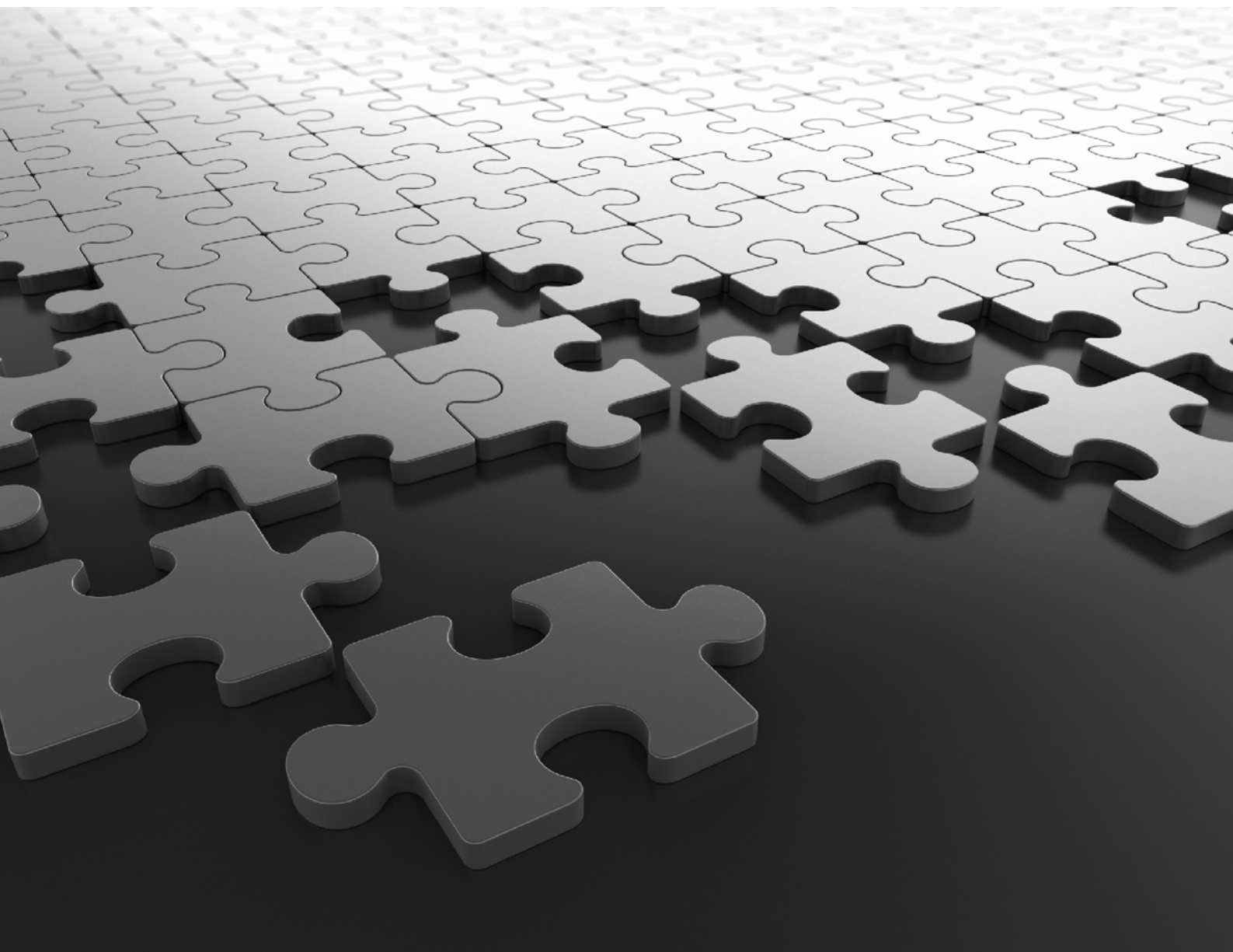


COSEC

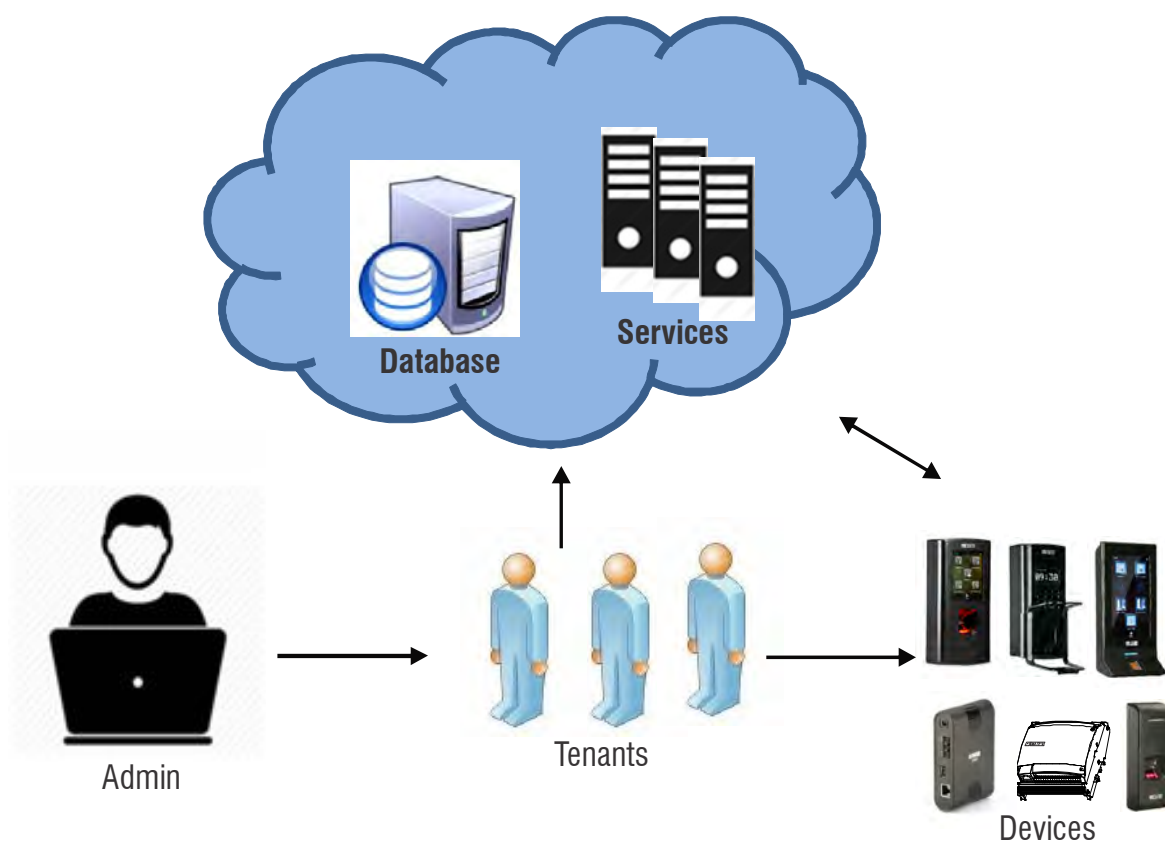
System Manual



COSEC CENTRA and COSEC VYOM

Right People in Right Place at Right Time

System Manual



Documentation Disclaimer

Matrix Comsec reserves the right to make changes in the design or components of the product as engineering and manufacturing may warrant. Specifications are subject to change without notice.

This is a general documentation for all variants of the product. The product may not support all the features and facilities described in the documentation.

Information in this documentation may change from time to time. Matrix Comsec reserves the right to revise information in this publication for any reason without prior notice. Matrix Comsec makes no warranties with respect to this documentation and disclaims any implied warranties. While every precaution has been taken in the preparation of this system manual, Matrix Comsec assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Neither Matrix Comsec nor its affiliates shall be liable to the buyer of this product or third parties for damages, losses, costs or expenses incurred by the buyer or third parties as a result of: accident, misuse or abuse of this product or unauthorized modifications, repairs or alterations to this product or failure to strictly comply with Matrix Comsec operating and maintenance instructions.

Warranty

For product registration and warranty related details visit us at:
<http://www.matrixaccesscontrol.com/product-registration-form.html>

Copyright

All rights reserved. No part of this system manual may be copied or reproduced in any form or by any means without the prior written consent of Matrix Comsec.

Version 28

Release date: January 5, 2023

Contents

Introduction	1
Know Your COSEC System.....	5
<i>System Architecture CENTRA & VYOM</i>	<i>7</i>
<i>Configuring and Using COSEC</i>	<i>12</i>
Pre - Installation Information	18
COSEC Software Installation.....	21
<i>Installing Prerequisites</i>	<i>25</i>
<i>Installing COSEC</i>	<i>37</i>
Launching the COSEC Application	54
<i>Starting Monitor Service & Utility</i>	<i>69</i>
<i>Accessing Social Security Dongle in COSEC CENTRA</i>	<i>72</i>
<i>Maintenance Scheduling</i>	<i>75</i>
Getting Started With COSEC Devices.....	77
<i>Device Features</i>	<i>87</i>
<i>Network Configuration</i>	<i>92</i>
<i>Licensing for Premise Solution</i>	<i>97</i>
<i>Using COSEC Web Application</i>	<i>101</i>
<i>Account Setting</i>	<i>105</i>
System Administration.....	107
<i>Managing System Accounts</i>	<i>111</i>
<i>Defining Global Policies</i>	<i>121</i>
<i>Identification Server</i>	<i>186</i>
<i>SMS Configuration</i>	<i>208</i>
<i>Email Configuration</i>	<i>212</i>
<i>Renaming Groups</i>	<i>227</i>
<i>Setting Up the Enterprise Profile</i>	<i>229</i>
<i>Configuring Alert Messages</i>	<i>231</i>
<i>Sending Messages from COSEC</i>	<i>267</i>
<i>Configuring Custom Messages</i>	<i>268</i>
<i>Component Status</i>	<i>271</i>
<i>Blocked Workstations</i>	<i>272</i>
<i>Configuring Locations</i>	<i>273</i>
<i>Location Group</i>	<i>276</i>

Agreement Builder	277
Form Builder	285
Importing Data	295
Exporting Data	299
Third Party Export	310
Scheduling Tasks/Reports	321
Event Notification	350
Message Board	353
Manage Database	355
Generate Face Templates	358
Activity Log	359
Event View	361
Alert View	363
Scheduler Log	365
License Information	367
Download Manager	368
Users	375
User List	379
Configuring Users	382
Multi-User Configuration	440
User-Module Configuration	461
Users on Device	462
Enrolling Users	466
Set and Sync Credentials	474
Delete Credentials	477
Sync from Device	480
Reporting In-Charge	482
Approval Policy	484
In-Charge Permissions	489
Import Users	491
Invite User	494
Changing Group	507
Exceptional Face Authorization	510
Deleting Users	517
Blocked Users	519
ESS Role Rights	522
IMEI Authorization	525
User Events	527
Assigning Alerts To Users	529
Blacklist Cards	531
Blacklisting Users	533
Changing User ID	535
Health	536
Get Location Details	538
User Details Export	541
User Reports	546
Devices	564
Getting Door Online	573
Device List	581
NGT Door	587
PVR Door	621
ARC Door	669
ARC IO-800	714
PATH Door	727

Door Controllers	762
Door FMX	808
VEGA Door	849
Wireless Door	916
ARGO Door	951
Panel200	1008
MODE Door	1059
ARGO FACE Door	1080
Special Functions	1132
Import Devices	1140
Milestone Integration	1141
Managing Sites	1145
Device Group	1147
Card Formats	1150
Reader Mode Scheduler	1152
Wiegand Output Format	1155
Card Personalization	1158
Device Status	1163
Device Reports	1174
Shifts and Schedule	1180
Shift Configuration	1184
Week Off Group	1194
Holiday Schedule	1197
Shift Schedule	1201
Restricted Holidays	1206
Manage Shift	1210
Change Schedule	1218
Change Week-Off	1220
Sync Change to Device	1222
Manual Schedule Import	1224
Monthly Shift Schedule	1225
Monthly Schedule	1226
Shifts & Schedule Reports	1228
Enterprise Structure	1231
Configuring Groups	1236
Organization	1237
Branch	1240
Department	1243
Designation	1246
Section	1249
Category	1252
Grade	1255
Custom Group1	1258
Custom Group2	1262
Custom Group3	1266
Group Associations	1270
Renaming Groups	1273
Enterprise Group Reports	1274
Access Control	1276
Absentee Rule	1279
Occupancy Control	1282
Use Count Control	1298
Dead Man Zone	1302

<i>Do Not Disturb</i>	1308
<i>Man Trap</i>	1313
<i>VIP Access</i>	1323
<i>Visitor Escort</i>	1325
<i>Anti-Pass Back</i>	1326
<i>Guard Tour</i>	1335
<i>Access Route</i>	1338
<i>Functional Group</i>	1343
<i>Time Schedule</i>	1344
<i>Time Schedule Group</i>	1345
<i>Elevator Configuration</i>	1347
<i>Elevator Floor Group</i>	1350
<i>Access Profile</i>	1352
<i>Access Profile Assignment</i>	1356
<i>2 Person Group</i>	1359
<i>2 Person Rule Assignment</i>	1362
<i>First In User</i>	1364
<i>First In User Assignment</i>	1366
<i>Smart Access Route</i>	1369
<i>Smart Identification</i>	1374
<i>Access Rule Profile</i>	1377
<i>Assign/Revoke</i>	1381
<i>View Alarm Log</i>	1384
<i>Cluster Access Details Export</i>	1387
<i>Access Control Reports</i>	1389
Time and Attendance	1408
<i>Attendance Policy</i>	1414
<i>Absentee Policy</i>	1447
<i>Overtime Policy</i>	1451
<i>Net-Work Hours Policy</i>	1483
<i>Late-IN Policy</i>	1491
<i>Early-OUT Policy</i>	1496
<i>C-OFF Policy</i>	1501
<i>In/Out Reasons</i>	1509
<i>Bus Route</i>	1510
<i>Overtime Code</i>	1511
<i>Attendance Summary</i>	1512
<i>Daily Attendance View</i>	1514
<i>N-Punch View</i>	1521
<i>Late-IN/Early-OUT Allowed</i>	1524
<i>Overtime/C-OFF Entry</i>	1526
<i>Previous Adjustment</i>	1529
<i>Attendance Correction</i>	1531
<i>Manual Status Correction</i>	1543
<i>Mark Group Attendance</i>	1545
<i>Manage Attendance</i>	1553
<i>Shift-Wise Management</i>	1568
<i>Change Policy</i>	1570
<i>User-Wise Attendance Restriction</i>	1573
<i>Advance Overtime Application</i>	1575
<i>Authorization or Approval</i>	1580
<i>Short Leave/Official In-Out Approval</i>	1581
<i>Overtime/C-OFF Approval</i>	1589
<i>Daily Attendance Approval</i>	1600
<i>Attendance Correction Approval</i>	1606

Event Authorization	1614
Advance Overtime Authorization	1619
Processing Attendance	1625
Attendance Register Export	1628
Site-Wise Head Count/Man Hours Export	1635
Short Leave/Official Out Time Export	1637
Group-Wise Shift Head Count Export	1640
Enterprise Group-Wise Presence Count Export	1643
Monthly Hours Summary Export	1645
Site Wise Monthly Summary Export	1648
Muster Roll Export	1652
Time and Attendance Reports	1656
Leave Management.....	1691
Configuring Leaves	1697
Tours	1719
Leave Group	1723
Accrual Policy	1726
Leave Credit/Debit/Encashment	1731
C-OFF Encashment	1738
Overflow Management	1740
Import Leave Balance	1743
Leave Application/Approval	1744
Tour Application/Approval	1760
C-OFF Application/Approval	1774
Leave Balance	1786
Leave Balance Process	1788
Leave Register Export	1789
Leave Reports	1792
Cafeteria Management	1797
Items	1802
Menus	1804
POS Devices Configuration	1806
Cafeteria Usage Policy	1808
Cafeteria Settings	1816
Recharge	1821
Payment	1824
Manual Adjustment	1825
Blocked Users	1830
Left Over Balance	1832
Pre-ordered Meals	1833
Correction Approval	1834
Manual Correction	1837
Transaction Summary	1841
Process-Monthly Payments	1845
Cafeteria Reports	1847
Visitor Management.....	1856
Visitor Profile List	1862
Visitor Profile	1864
Visit Components	1880
Station Location	1884
Visitor Template	1896
Invite Visitor	1899
Pre-Registration	1902

Visit Registration Approval	1912
Security Approval	1920
Visitor Login Authorization	1923
Visit Approval	1927
Form Summary	1934
Set and Sync Credentials	1936
Delete Credentials	1940
Sync From Device	1943
Visitor Events	1945
Entry/Exit Correction	1949
Frequent Visitors	1951
Watchlist/Blacklist	1957
Visitor History	1962
Enrollment	1964
Authorized Host Users	1969
Visit Request Handling	1970
Delete Frequent Visitors	1972
Import Visitor and Visit	1973
Visitor Management Reports	1976
Contract Worker Management.....	1983
Contractor Types	1989
Contractor Profile	1990
Induction Levels	1994
Approval Stages	1995
Work Order Types	1998
Work Order List	1999
Work Order	2000
Skills	2004
Personal Protective Equipment	2005
Worker List	2006
Worker Profile	2008
Worker Profile- Devices	2014
Worker Profile- Credentials	2017
Worker Profile- Group	2027
Worker Profile- T&A	2029
Worker Profile-Access Control	2034
Worker Profile-ESS	2036
Worker Profile-Cafeteria	2039
Worker Profile-CWM	2041
Worker Profile-Job Costing	2046
Worker Profile-Field Visit Management	2048
Worker Profile-Face Recognition	2049
Worker Profile-Visitor Management	2056
Worker Profile-Events	2058
Worker Assignment	2063
Enrollment	2066
Import Workers	2073
Blacklist	2076
Manage Workers	2079
Work Order Progress	2081
Induction Approval	2083
CWM Reports	2085
Job Processing and Costing	2091
Cost Centre	2095

<i>Job</i>	2096
<i>Job Group</i>	2099
<i>Phase</i>	2100
<i>Project</i>	2101
<i>Site Mapping</i>	2105
<i>Location Mapping</i>	2107
<i>Job Status</i>	2109
<i>Daily Job View</i>	2111
<i>Time Sheet Correction</i>	2113
<i>Time Sheet Correction Authorization</i>	2120
<i>Award Penalty Authorization</i>	2125
<i>Job Costing Process</i>	2131
<i>Daily Timesheet</i>	2132
<i>Job Processing and Costing Reports</i>	2134
Field Visit Management	2140
<i>Task</i>	2144
<i>Field Visit Schedule</i>	2145
<i>Field Visit Status</i>	2153
<i>Field Visit Correction</i>	2156
<i>Field Visit Correction Authorization</i>	2159
<i>Field Visit Management Reports</i>	2165
Report Builder	2167
<i>Report Configuration</i>	2170
<i>Designing Report</i>	2182
<i>Customized Report Page</i>	2223
Appendix	2226
<i>GDPR Reflections</i>	2229
<i>Technical Specifications</i>	2250
<i>Disposal of Products/Components after End-Of-Life</i>	2254
<i>Open Source Licensing Terms and Conditions</i>	2255
<i>Troubleshooting</i>	2261

Welcome

Thank you for choosing the Matrix COSEC Multi-door Access Control System! We are sure you will be able to make optimum use of this feature rich, Integrated Access Control and Time and Attendance system. Please read this document carefully to get acquainted with the product before installing and operating it.

About this System Manual

This is a common document providing detailed information and instructions for installing and configuring the **COSEC CENTRA** i.e. COSEC on Premise solution and **COSEC VYOM** i.e. COSEC on Cloud Solution. It includes COSEC Access Control System hardware components as well as the software installation and configuration of the COSEC application. This manual includes sufficient information to install and configure all the components of the Matrix COSEC Access Control System.

The COSEC application is a powerful web based multi-user Access Control cum Time and Attendance system that provides all the features required for medium to large size enterprises. A host of modules are available making the COSEC application a comprehensive, menu-driven software application.

This system manual is a common documentation for all variants of COSEC Controllers - PANEL, DOOR Controllers and their variants. This manual also includes sufficient information to install and interconnect the controllers on various network topologies. This manual must be read, and its contents clearly understood, before proceeding with any work relating to the COSEC Web Application.

Intended Audience

This System Manual is aimed at:

- **System Engineers**, who will install, maintain and support the COSEC system. System Engineers are persons who are responsible for configuring the COSEC system to meet the requirements of the organization/users. It is assumed that they are experienced in installing an Access Control System and are familiar with the cabling of such systems. They are expected to be aware of how it works, and the various technical terms and functions associated with it. The SE must have undergone training in the installation and configuration of the COSEC system. No one, other than the System Engineer is permitted to make any alterations to the configuration of the COSEC system.
- **System Administrators**, who are persons who will monitor and control the COSEC system after installation. Generally, an employee of the IT/HR designation in an organization or establishment is selected as the System Administrator. It is assumed that the System Administrator has some previous experience in configuring and deploying a security cum Time and Attendance system. The System Administrators are not expected to setup and install the system hardware, but only the configuration of the

system including its functionalities and features, defining the access levels for various users and the extraction of various reports.

- **Users**, persons/organizations who will use the COSEC system. They may be executives, include personnel of small and medium businesses, large enterprises, front desk and service staff of Hotels/Motels, hospitals, and other commercial and public organizations/institutions.

Organization of this Document

This system manual contains the following topics:

- **Introduction** - gives an overview of this document, its purpose, intended audience, organization, terms and conventions used to present information and instructions.
- **Know Your COSEC** - describes the system and its design, different network topologies, system architecture, and the interfaces with COSEC web application.
- **Pre-Installing COSEC Devices** - gives step-by-step instructions for pre- installing information for the COSEC devices, selection of installation location, the safety measures for protecting the system and persons handling the installation and maintenance, and packaging contents.
- **Getting Started with COSEC** - provides information about Panel/Panel lite/Panel200 and Door terminals, describes the COSEC modules and provides license information.
- **Launching the COSEC application** - provides a step by step instruction for installing the various components required to run the COSEC application as well as the various components. This section also includes instructions for launching the desktop and the web modules of the COSEC application.
- **Appendix** - Contains additional information related to the document. These include Technical Specifications of the Product, Glossary of terms, Product Warranty Statement, and Contact details.

How to Read this System Manual

This document is organized in a manner to help you get familiar with the COSEC system, learn how to install it, connect it in various network topologies, connect the external devices, and power up the hardware systems. The manual also covers the installation and configuration of the COSEC application and its dependent components.

This System Manual is presented in a manner that will help you find the information you need easily and quickly.

You may use the table of contents and the Index to navigate through this document to the relevant topic or information you want to look up.

- **Instructions**

The instructions in this document are written in a step-by-step format, as follows. Each step, its outcome and indication/notification, wherever applicable, have been described.

- **Notices**

The following symbols have been used for notices to draw your attention to important items.



Important: to indicate something that requires your special attention or to remind you of something you might need to do when you are using the system.



Caution: to indicate an action or condition that is likely to result in malfunction or damage to the system or your property.



Warning: to indicate a hazard or an action that will cause damage to the system and or cause bodily harm to the user.



Tip: to indicate a helpful hint giving you an alternative way to operate the system or carry out a procedure, or use a feature more efficiently.

Terminology used in this System Manual

The technical terms and Acronyms used in this Manual are standard terms, commonly used in the access control and Time and Attendance industry. However, considering the broad group of intended users of this manual, wherever possible, use of jargon has been avoided.

- **COSEC VYOM** is referred as **COSEC on Cloud**. **COSEC CENTRA** is referred as **COSEC on Premise**. The features which are common to COSEC CENTRA as well as COSEC VYOM are explained in generic way pointing to COSEC CENTRA or COSEC Server. The features which are explicitly available or not available in CENTRA or VYOM; are notified respectively.
- **COSEC Panel**, **COSEC Panel lite** (Vega Panel -Lite) and **COSEC Panel200** (Standalone Panel lite) are all master controllers. The term Panel or Panel lite is used interchangeably. COSEC Panel is supported in COSEC Centra only.



If you are accessing the COSEC Server GUI, Device Module> Device Configuration > Click Add Button, there are three options related to Panel, namely Panel, Panel Lite and Panel200.

The term Panel refers to COSEC Panel200/Panel Lite. The feature access may differ as per the Panel variant.

Panel Lite V2 has been renamed as Panel200, hence the screens for Panel Lite V2/Panel200 represent the same.

- **PANEL DOOR** (Door controller connected through Panel/ Panel lite/ Panel200) and **DIRECT DOOR** (Door controller connected to server directly) are used to refer the **COSEC DOOR** (including their variants) respectively.

The term **device** is a general term referring collectively to any or all of the above controllers.

Using this Manual in conjunction with the **COSEC PANEL Lite** and **Doors** Quick start, we hope, you will be able to set up, configure and make optimum use of this feature packed COSEC access control system.

Getting Help

Our online help will provide you with immediate and context-related help. Click on the **Help** button, found in all the system windows. A help file will open up which enables the user to navigate to the relevant topic of interest. To get a more focused and context sensitive help click on the “?” symbol located on the upper right half of the web page.

Technical Support

If you cannot find the answer to your question in this manual or in the Help files, we recommend you to contact your system installer. Your installer is familiar with your system configuration and should be able to answer any of your questions.

If you need additional information or technical assistance with the COSEC system and other Matrix products, contact our Technical Support Help desk, Monday to Saturday 9:00 AM to 6:00 PM (GMT +5:30) except company holidays.

Phone	(+91)18002587747
Internet	www.MatrixComSec.com
E-mail	Tech.Support@MatrixComSec.com

Time-Attendance defines the productivity of an organization and Access Control defines security of the valuable assets. These two areas are inherently human-oriented, complex and challenging to automate. Productivity of any organization depends on its effectiveness in putting the right people in the right place at the right time.

For this, Matrix COSEC provides a comprehensive, end-to-end Time-Attendance and Access Control Solution with an adaptive, modular, scalable and function-rich Time-Attendance and Access Control solution designed for Small Office Home Office (SOHO), Small and Medium Businesses (SMB), Small and Medium Enterprises (SME) and Large Enterprises (LE).

Key features of COSEC Application Software are:

- Layered Architecture
- Real-Time Processing of Events
- Latest Status View and Reports
- Web-based, Multi-User Application
- Live Monitoring and Supervision
- Remote Views and Reports
- Calender-Based Views
- Automatic Finger Template Distribution
- Past Adjustments of User Records

The Matrix COSEC is designed to deliver high level of flexibility at various levels such as

- Physical Interfaces- RS485 and Ethernet
- Door Controller Connectivity with Application Server- Direct or through Panel
- Readers- Card, Finger and PIN in any combination

Variants of COSEC DOORS

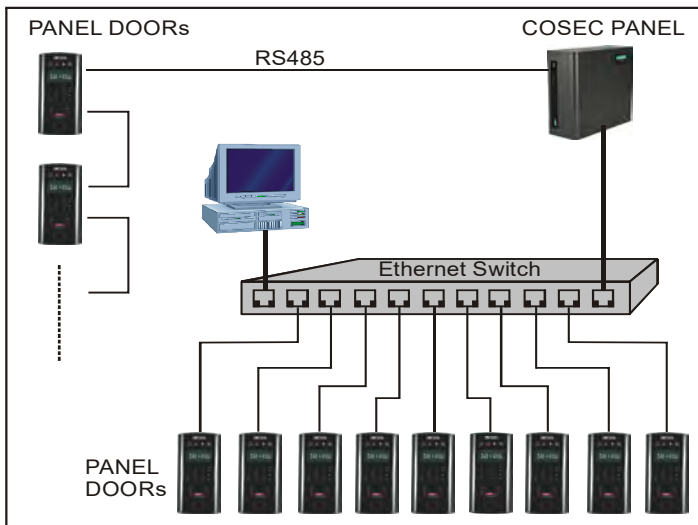
The Matrix COSEC Door is available with the following configurations depending on the firmware resident on the DOORS.

- **PANEL DOOR**
- **DIRECT DOOR**

All COSEC Doors are by default shipped with the DIRECT Door configuration. However, based on the mode set while configuring the COSEC application the appropriate modes will be enabled on the Doors. In the event of the Door being set in Panel mode the COSEC Panel downloads the Panel Door firmware to all the Doors on the network whose MAC addresses have been defined in the Door Controller settings of the COSEC application as explained later in this manual.

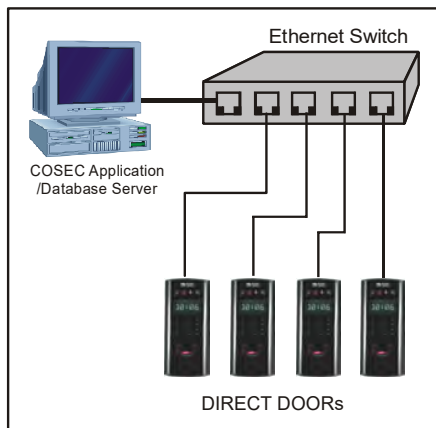
PANEL DOOR

The PANEL DOOR, as the name suggests connects to the COSEC PANEL which in turn connects to the COSEC Monitor application. A typical setup looks as follows.



DIRECT DOOR

The DIRECT DOOR, as the name suggests connects directly to the COSEC Monitor application. A typical setup looks as follows.



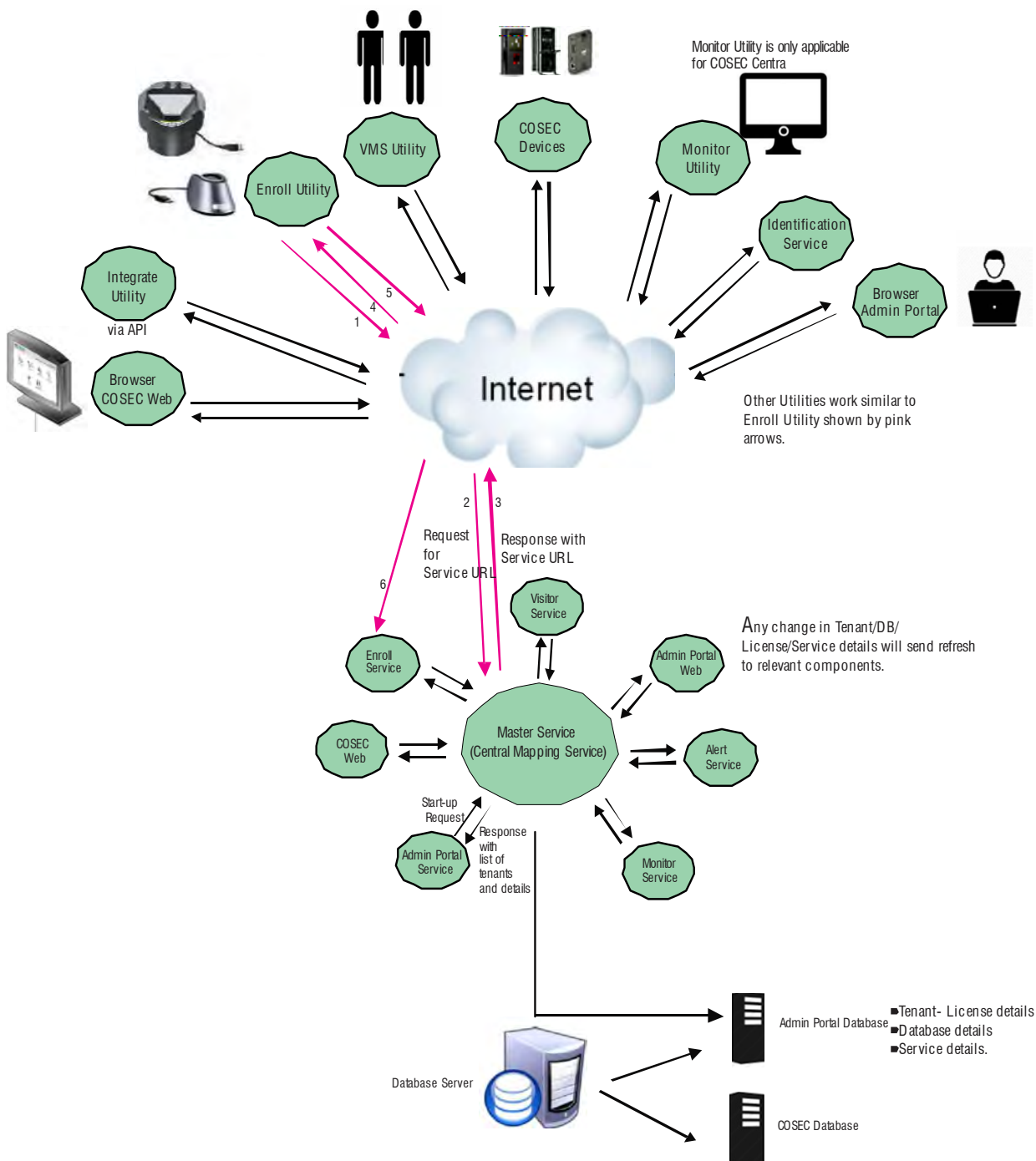
Also DIRECT DOORS have limited functionality as compared to the PANEL DOORS. For a functionality-based comparison of all COSEC devices, [See "Device Features" on page 87.](#)

For installation details on COSEC Doors, refer to COSEC Door Quick Start guides.

System Architecture CENTRA & VYOM

The COSEC access control system has a layered architecture with intelligent components at each level.

At the top is the **COSEC Utilities** at the user end, **COSEC Services** along with central Master Service and the Database servers hosting **Admin Portal database** and **COSEC database**. This gives the flexibility to install these components at one location or separate locations.



For COSEC on Premise solution; the complete system shown above has to be installed. For COSEC on Cloud solution; only the utilities has to be installed at the client side.

Database

The **Database Server Layer** involves the installation and management of Admin Portal database and COSEC database.

The **Admin Portal database** consist of:

- Tenants details
- License details
- Services Assignment
- Database backup/Upgrade- maintain records.

For Premise solution, there will be only 1 tenant in Admin Portal.

The **COSEC database** is the client specific database. For COSEC on Cloud solution; the database will be available at the cloud server and managed by the Tenant portal administrator. For COSEC on Premise solution; the database will be locally configured by the client.

COSEC Services

Master Service

- Handles request from all other components.
- Provides updated Tenant/DB/license details to all services.
- On Premise- Responsible for license Management for both modes- Dongle on Server as well as Dongle on Device.
- On Premise- Responsible for COSEC DB upgrade as well.
- Responsible for Admin Portal DB Upgrade.

Monitor Service is required for communicating with COSEC devices.

Admin Portal Service is required for following functions:

- Database upgrade (COSEC DBs)
- Post, Retrieve and Remove records.



The Admin Portal Web has no dependency on the status of Admin Portal Service. The Admin Portal Web can be accessed even if Admin Portal Service is not running. This service must be running for above mentioned functions.

Alert Service is required for sending notification alert.

Enroll Service and **Visitor Service** handles the request of the Enroll Utility and Visitor Utility respectively.

To know about the installation of the above Services, refer the ServicesUserGuide..

COSEC Utilities

The COSEC Utilities include — COSEC Enroll, COSEC VMS, COSEC Monitor, COSEC Integrate, COSEC Tracker.

To know more about these Utilities refer their respective manuals:

Utilities	User Manuals
COSEC Enroll	EnrollUserGuide

Utilities	User Manuals
COSEC Enroll	VisitorUserGuide
COSEC Monitor	MonitorUserGuide
COSEC Integrate	IntegrateUserGuide
COSEC Tracker	Tracker User Guide



COSEC Monitor and COSEC Tracker are applicable only for Premise solution.

COSEC Devices

COSEC Panel/ Panel-lite/Vega Panel-lite manages multiple door controllers and is a local bridge between the door controllers and the COSEC application software.

See Devices Section for supported devices.

Door Controllers and their readers are front end terminals, guarding and monitoring the entry and exit points. However, for time-attendance applications, Door Controllers can be connected directly with COSEC application software.

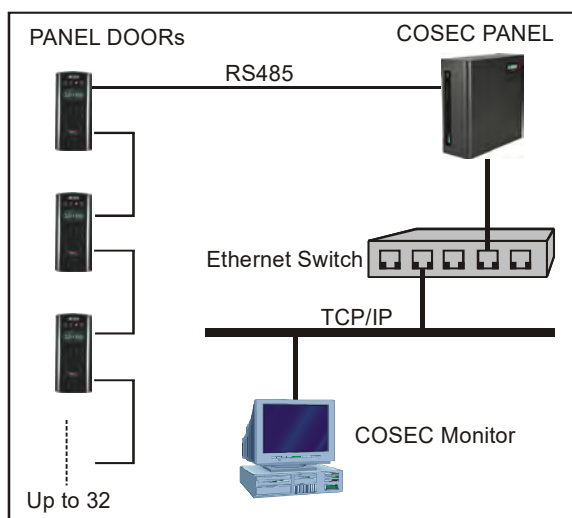
The COSEC Access Control System is based on the **Master-Slave architecture**.

The COSEC Panel/Panel Lite/Vega Panel Lite (Panel200) is the central processing unit which acts as **Master** and Door controllers act as **Slave**.

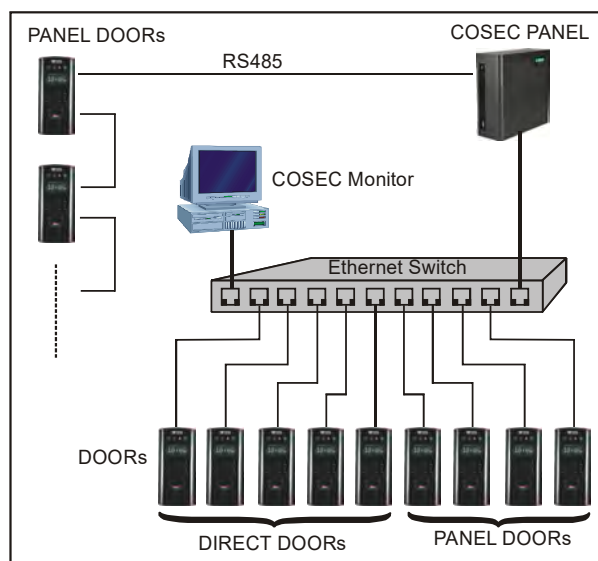
The Panel/Panel Lite/Panel200 stores complete user information, access policies, user events, door controller software and all the connected door controller's configuration settings. The Panel lite is programmed to apply certain access policies on users accessing the facility where the Access Control System (ACS) is installed.

Various Network Topologies

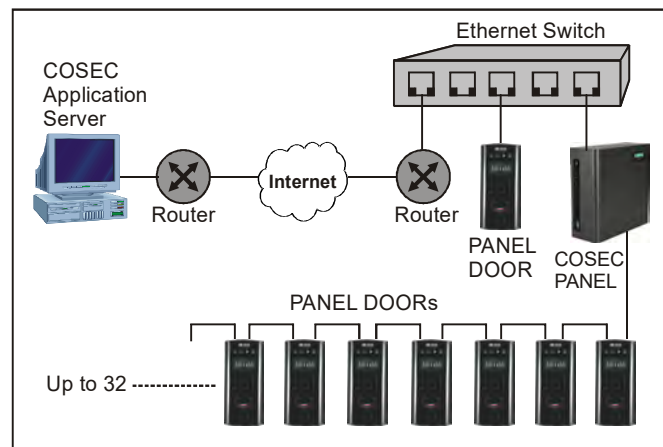
All PANEL Doors (up to 32) connected to PANEL on a RS-485 Loop



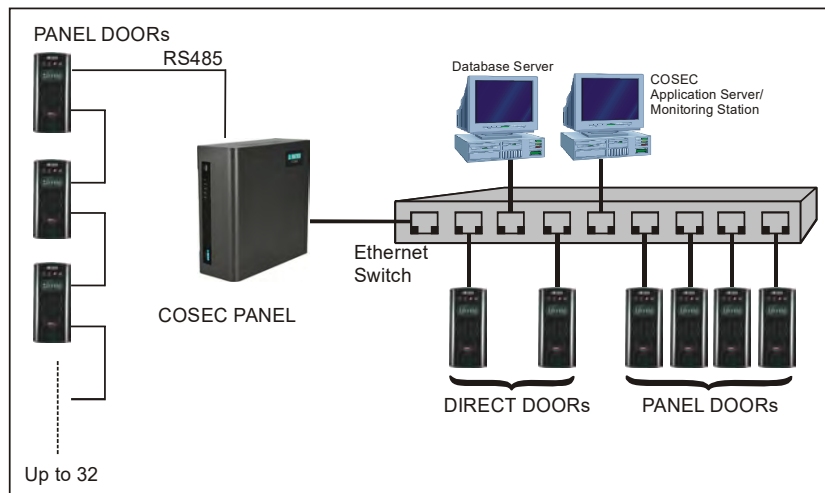
Some PANEL DOORS & DIRECT DOORS connected to the PANEL on the Ethernet and all other PANEL DOORS on the RS-485 loop.



Connecting remote sites



Typical Heterogeneous Network Topology



A maximum of 255 COSEC PANEL DOORS can be connected to a single PANEL in any combination. The MSSQL Database can be installed on the same computer as the application and the monitoring software.

Configuring and Using COSEC

Follow the below steps to configure new user in COSEC and assign devices and policies to him.

“Step1”: Create a user from User module.

“Step2”: Connect COSEC Device and add to the COSEC Web Server.

“Step3”: Assign Devices to User.

“Step4”: Enroll Credentials of the user.

“Step5”: Create and Assign Shift Schedule to the user.

“Step6”: Create and Configure Time Attendance Policies

“Step7”: Assigning Groups (Reporting, Leave, Week-Off) to the user.

Step1

From “User” module of Web server, add a user and select the type as T&A. Mention the Joining date and other details of the user.

Step2

Apply Power and Ethernet connection to the COSEC door.

Give available IP address to the door and set Server address and Port as the IP and Port of your computer where COSEC Monitor is installed. You can get the IP and Port from COSEC Monitor Properties.

Eg: 192.168.104.122 is the IP address of your Device and 192.168.104.23 is the Server address and 11000 is the Port.

Manual Addition

From “Devices” module in Web server, add the desired device by specifying its MAC address. Once the door is connected, it will come Online and IP address will be automatically displayed.

The status of door connection can be viewed from COSEC Monitor and also from Device Status page of Devices Module in Web Server.

Auto Addition

Enable “Auto add New Devices” from Global Policy of Admin Module. If you have set the server IP address in your device then the device will be automatically added in the server.

Step3

Method1: To a Device Group, assign user/ users

Create Device Group from Devices> Masters> Device Group. Add devices to the group. Then assign the user to the device group.

If “ Auto Assign new device to Device Group” is enabled from Global Policy then new devices added to the COSEC Server will be added automatically to the device group. And hence the user will be assigned to that device group.

Method2: To a Device, assign user

From Device Configuration> Additional> Assigned Users tab. Select the device from the device list to which the user is to be assigned. Then select the particular user from the picklist and Save.

Method3: To a User, assign device or Device Group

Create User. From User Configuration> Devices, assign Device group or individual device.

Step4

Enrolling when new user is created: Go to User Module> After creating the user, Select Credentials tab. Click Enroll Credentials and select the door on which credential is to be enrolled. From here you can enroll the credential directly on the door which will be later synced with other devices.

Enrollment of Multiple Users: When you have a device with you and want to enroll multiple users then go to Users module> Credential Management> Enrollment. Select a Door on which you want to enroll one by one user credential. Now select the user and perform enroll operation on device after selecting the type of enrollment.

Once the credentials are enrolled at one door, it gets automatically synced to other doors of the group. So the user can access other devices installed at the premises.

Depending on the device/door available you can enroll the finger template, palm template or card for the user/employee.

Finger Enrollment



Palm Enrollment



Card Enrollment



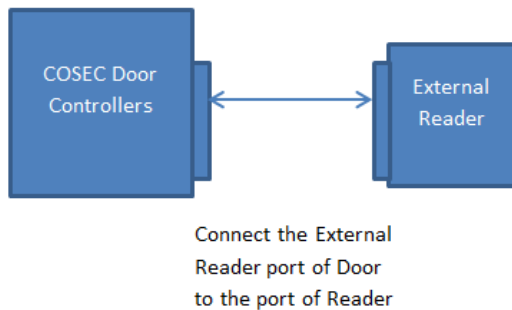
Using COSEC Enroll: When a person(say Receptionist or HRD person) is assigned the role of enrolling credential of new employees. Then the credentials can be enrolled using COSEC Enroll as the desktop application. Using

desktop application, you can easily enroll the finger/palm/card from the respective enrollment station. See COSEC Enroll Manual for details.



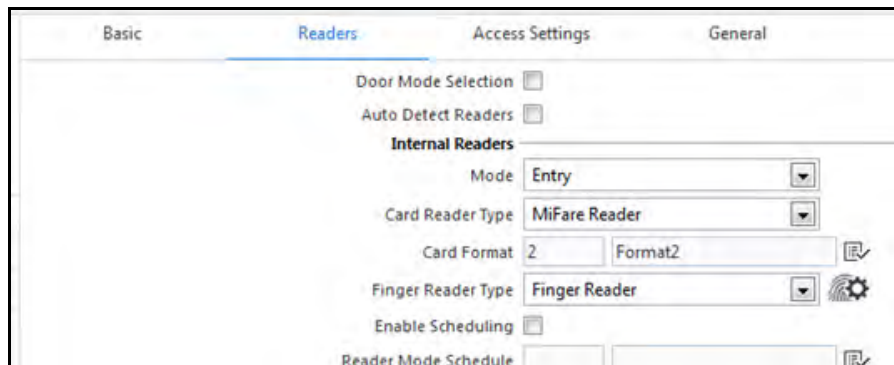
Enrolling Smart Card for User:

1: Configure the device with Internal or External Reader: For Internal reader, connect the reader module inside the device. For External reader, connect the 15 pin connector of door controller (Eg:Vega) with the connector of Reader as shown below:



2: Configure the device profile for Reader: Make the configuration changes as per the physical connection of the reader.

If you have connected Mifare reader, then select the **card reader type** as Mifare. Also ensure that you have Mifare card for enrollment.



Similarly make the configuration as per your reader selection.

Then select the **card format** from the picklist as per which the Parity, CSN and FC will be written on the card.

Note: Card Personalization works for HID-iclass and Mifare cards only.

3: Enroll the Smart Card for user: Select the User> Credentials. Click on Enroll Credentials. Select the Door where enrollment is to be done. For the enrollment type Smart Card, click Enroll and show your card on device. The card will get enrolled after the successful enrollment. The card number will be shown in Access Card field.

Enrollment of Special Card: In a factory when workers want to use special function (for eg: Short leave), then they can take the card which is enrolled for that special function and show to the device. In this way worker can activate the short leave function on door using the special function card. Once the function is active, he can access the door using his credential.

To enroll the special function card, Go to Users module> Credential Management> Enrollment> Special Card. Select a door for which special function card is to be enrolled. You can enroll Read only card or Smart card for any of the special functions available from the drop down list.

Step5

The user is assigned Shift Schedule, not the individual shift.

Creating Shift: First you have to create shifts eg: GS(General Shift), NS(Night Shift) etc. Define the timing of the shift. You can specify the working hours required to complete half day and full day.

Break Details and Grace details for the shift can be specified.

If Break deviation is not allowed, then the break Late-in and/or break early-out can be added to total late-in and/or total early-out respectively.

Create Shift Schedule Group: Add the required shifts to the created schedule group. You can specify the days for a particular shift to repeat. Eg: a schedule group has GS and NS shifts in which GS shift repeats for 7 days and NS shift repeats for 4 days.

Week-off days can be set in the shift. If both Off Day configuration and Week Off Group are defined for a user, then week off will be given as per the Week Off group. [See “Step6” on page 15.](#)

Assigning Shift Schedule to User: Select the User to whom the shift schedule is to be assigned.

Go to User Configuration> Access Control> Basic.

Select “Shift Schedule” to be assigned to the user. Then select “Start Shift” as the shift from which the schedule is to be started.

You can also create holiday schedule from Shifts and Schedule module and assign it to the user.

Process Schedule: Finally Go to Shifts and Schedule module> Process> Monthly Schedule. Select the user and the month for which shift-schedule is to be processed. If any existing schedule is available for the user, then you can overwrite the same by current schedule by enabling the respective box.

After processing the schedule, you can view from Shift and Schedule module> Utilities> Monthly Shift Schedule.

Step6

If you want to assign Time Attendance policies to user then Go to T&A module> Policies. You can configure various policies as per your organization requirement.

Configure Attendance Policy: The Attendance Policy is the configuration of rules as per which attendance of the employee is recorded and processed. For details see [“Attendance Policy”](#)

Configure Network hours Policy and OT Policy: If you want to pay for the extra work hours of an employee, then you must calculate overtime hours of the employee. For details see [“Net-Work Hours Policy”](#) and [“Overtime Policy”](#)

Configure Late-IN Policy: To allow the user for flexibility in late-incoming to the organization, you can configure Late-IN policy and assign to the user. For details see [“Late-IN Policy”](#)

Configure Early OUT Policy: To allow the user for flexibility in going out early from the organization, you can configure Early-OUTN policy and assign to the user. For details see [“Early-OUT Policy”](#)

Configure Absentee Policy: When the Employee takes leave before or after Week off/Public holiday, then to consider him as absent will depend on the configured Absentee Policy. For details see [“Absentee Policy”](#)

Configure C-OFF Policy: If Overtime hours of an employee are to be rewarded by the C-OFF, then the C-OFF policy can be configured and assigned to the user. For details see [“C-OFF Policy”](#)

Note: For assigning new policies (other than Attendance Policy) to user, Go to T&A module> Utilities> Change Policy. Select a single user or multiple users and assign the desired policy to the user.

To change Attendance Policy of the user, Go to User> User Configuration> T&A> Policy.

Step7

Additional to the basic configuration described above, the user can be assigned Reporting Group, Leave Group and Week-Off Group.

1) Creating Reporting Group: From User module> Reporting In-charge> Reporting Group, you can create a group with upto 5 in-charges. The users are then assigned this group. The authorization mode for the group can be selected as Any One, All or All Sequential.

Eg: Geeta, Dinesh, Aakash, Shruti and Khushbu are members of reporting group QA. The incharge1 is Shruti and incharge 2 is Khushbu. The authorization mode is All Seand final authority in Incharge2. In this case any application (leave application/ attendance correction/Cafeteria correction application) by user Geeta will require authorization by both incharges. And final verdict will be given by incharge2.

In case of Any One mode, authorization by any of the two incharges will be allowed.

In case of All Sequential mode, first incharge will authorize. Only after the verdict of first incharge or due to auto forward, the application will go to second incharge for the final verdict.

Assigning Reporting Group: Select the User to whom the reporting group is to be assigned.

Go to User Configuration> T&A> Group. Select the “Reporting Group” from the pick-list to be assigned to the user.

Eg : The new user Sheetal is assigned the group QA. So Shruti and Khushbu who are in-charges of QA group will become the Reporting In-Charges of Sheetal.

2) Creating Leave Group: From Leave Management module> Leave Group

Create a new leave group and add the leaves in the group. But you must configure the leaves first.

If you Enable pro-rata for a leave group, then the leave will be given to the user as per the no. of working days.

Assigning Leave Group: Select the User to whom the leave group is to be assigned.

Go to User Configuration> T&A> Group. Select the “Leave Group” from the picklist to be assigned to the user.

Crediting Leave:

To avail the leave, the user must have leave balance. For this you must credit the leaves to the user. Go to Leave Management> Balance Management> Credit/Debit/Encashment.

You can credit the selected leave to one/more user on monthly or yearly basis.

- For a fixed value of leave, Pro-rata can be applied. This implies that the leave will be given as per the no. of working days.

Eg: The user has joined a company on 21st of month. You are crediting 10 leaves but actually 3.5 leaves will be credited to the user.

The rounding of credited leaves can be configured from Leave Rounding Parameters.

- Using Accrual Policy, you can credit advanced leaves for monthly or yearly period in fixed mode (fixed number of leave) or calculated mode (calculation based on attendance of previous month).

3) Creating Week-Off Group: From Shifts and Schedules module> Week Off Group

You can create week off group with two week-offs. The 2nd week-off can be customized to give off for alternate week or any particular week or all the weeks.

Eg: IT Company gives 2nd week-off as Saturday on all weeks so select Saturday as Off day2 and check all the boxes. Some other company may give Off on second (W2) and fourth Saturday (W4).

WO Rotation:

The week off group can have one or both week-offs rotating. This implies if Off Day 1 is Sunday and Off Day2 is Friday and rotation count is 10 days. So WO Sunday will become Monday after 10 days. Eg: 1st July is Sunday (WO-1). After 10 days i.e. on 11th July you will have WO on Monday (WO-1). Similarly WO-2 will be rotated.

Note: WO Rotation will be disabled for Auto Week off assignment.

Assigning Week-Off Group: Select the User to whom the Week Off group is to be assigned.

Go to User Configuration> T&A> Group. Select the "Week Off Group" from the pick-list to be assigned to the user.

Installation Precautions

It is very important for the installer to read and understand all the instructions in this manual before starting the installation process. For each stage in the controllers' installation and commissioning procedures a brief description is given of its purpose, complete with detail drawings, flow diagrams and/or other graphics, wherever possible, to make the instructions easy to follow. Before installing the Matrix COSEC Access Control Units, you must first ensure that the following criteria have been met. Failure to do so may not only result in damage to the equipment, but may also cause problems when commissioning the system and may adversely affect its performance.

Product Inspection

The COSEC Access Control Units are simple to install and commission if the procedures as described in this System Manual, and the Installation and Commissioning sections of this manual, are followed.



Follow all installation instructions described in this manual. These instructions must be understood and followed to avoid damage to the controllers and associated equipment.

Checking the Controller for Damage

Before attempting to install your Panel/ Panel Lite/ Panel200 you should do the following:

1. Remove the PANEL from its packaging, and check for any damage that may have been caused during transit. Any missing item/part or damaged component should be reported immediately.



*In the unlikely event that the PANEL has been damaged in transit, you **MUST NOT** install it but contact your supplier for their return procedure.*

What to do if you Suspect the PANEL is Damaged

The procedure described below tells you what to do in the unlikely event that the supplied equipment has been damaged after leaving the factory. However, if you have problems regarding the quality of any supplied order items including the PANEL, its ancillaries or this manual, or items are missing, follow the procedure below.

1. If, after removing the PANEL from its packaging, a visual inspection reveals that it has been damaged, you **MUST NOT** continue with the installation but contact your supplier for advice on what to do next. Similarly, if the product is found to be faulty during installation contact your supplier immediately.

2. To aid your supplier you are requested to note all the details relevant to your complaint, clearly stating details of any technical problems, date of receipt, packaging condition, etc. and forward this to your supplier.
3. Where the product needs to be returned to your supplier, you are requested to use the original packaging wherever possible.

Do's and Don'ts:

Prior to selecting a location for the COSEC PANELs and DOORs, Do make sure that:

- a. The ambient temperature is in the range: +5 deg C to 35 deg C.
- b. The relative humidity is between: 5% and 95% (non-condensing).
- c. The COSEC PANELs and DOORs are wall mounted in a position which allows clear visibility of display and easy access to operating controls. The height above floor level should be chosen such that the middle of the COSEC PANEL is just above normal eye level (approximately 1.5 meters) while that of the COSEC DOOR should be approximately 1.0 meter.
- d. Do not locate the COSEC PANELs and DOORs where they are exposed to high levels of moisture.
- e. Do not locate the COSEC PANELs and DOORs where there are high levels of vibration or shock.
- f. Do not mount the COSEC PANELs where there would be restricted access to the internal equipment and cabling/wiring connections.

Safety Instructions

NEVER INSTALL THE EQUIPMENT DURING A LIGHTNING STORM!

The Installer should always take basic safety instructions to reduce the risk of fire, electric shock and injury to personnel and system. The following points need to be taken into account:

1. The COSEC PANEL should be installed and used within a pollution free environment and at a safe and secure indoor location.
2. The equipment is FIXED and PERMANENTLY CONNECTED and is designed to be installed by authorized Service Persons only. The COSEC PANEL comes installed in a metallic cabinet.
3. Do not place the product at a location from where it can fall and cause damage to the product.
4. The product should be operated with appropriate power voltage supply as mentioned in the specification sheet.
5. Cable splices can cause trouble. Make sure you measure your runs and order sufficient cable for unspliced runs. If splicing is required, solder the splices together, rejoin the shielding the best you can, and restore (heat shrink) the cable insulation.
6. Label each cable run and each individual wire. Make sure you don't cross cables at splices or junctions. Color coded cable makes life easier and assures straight through connections.
7. Make sure the site's electrical system is properly grounded.
8. Internal wiring must be routed in a manner that prevents:

- Excessive strain on wire and on terminal connections;
 - Loosening of terminal connections;
 - Damage of conductor insulation.
9. It is the end-user's and/or installer's responsibility to ensure that the disposal of the used batteries is made according to the waste recovery and recycling regulations applicable to the intended market.
10. There are **no serviceable parts within the equipment**. For any issues or queries regarding the equipment please contact your installer.



Disconnect Power before Servicing.

COSEC Software Installation

Before commencing the installation, make sure that the computers on which the software will be installed meets the necessary requirements.



The COSEC setup installation is explained for Premise based solution. For Cloud based solution; setup installation will be done at cloud server.

System Requirements

Make sure that the computer on which you are installing the software meets the following requirements:

- **Operating Systems:** Windows7 Professional and above
- **Processor:** Recommended is dual core processor and above
- **RAM:** Minimum available is 4GB
- **Hard disk:** Minimum available is 40 GB
- **Screen resolution:** Minimum Recommended is 1366 x 768
- **DVD/CD-ROM** drive
- **Network Interface card:** 10/100 Base-T network adapter
- Recommended **IIS** ver 6.0 or higher
- **Microsoft .Net Framework** ver 4.5
- **Internet Explorer** 9.0 - 11.0
- Requires **USB2.0** or higher Port for license dongle



Please ensure that you have installed the IIS ver 6.0 or higher, prior to proceeding with the installation of the application as described in the following section. The user needs to ensure that the .Net Framework 4.5 is installed only after the installation of the IIS component to enable appropriate registration of the asp.net with IIS. To check if IIS is installed on the computer, open the web browser (Internet Explorer) and type in <http://localhost> in the address field. The IIS home page must appear.



SQL database is supported for SQL server 2008 R2 and above. Oracle database is supported from version 10g upto version 19c.

Pre-Requisites for Face Recognition and Face Enrollment

Face Recognition and Face Enrollment System Requirement support for windows application development targets 3 major platforms: x86 (CPU), x64 (CPU) and x64 (NVIDIA GPU).

Computer Hardware Platform

For Windows with CPU:

- 6th and above generation Intel Core processors and Intel Xeon processors.
- Intel Xeon processor E family (formerly code named Sandy Bridge, Ivy Bridge, Haswell and Broadwell)
- 3rd generation Intel Xeon Scalable processor (formerly code named Cooper Lake)
- Intel Xeon Scalable processor (formerly Skylake and Cascade Lake).

For Windows with GPU:

- Nvidia GeForce GTX 1050 Ti-4 GB onwards

Operating System

Microsoft Windows 10 64-bit

Recommendations for Liveness Verification

Below mentioned recommendations for Liveness Verification is applicable for all Matrix's Cameras.

- Custom ROI of Height ~= 1000 px and Width ~= 700 px.
- Good and evenly distributed light is required on person's face.
- Good lighting is required at setup location facing person's front. Back light degrades acceptance rate of real person.
- Person's distance from camera when marking attendance must be between 1 to 2 ft (For Moderate and Advance Face Anti-Spoofing Mode) and more than 3 ft (For Basic Face Anti-Spoofing Mode).
- Face horizontal shift must be between -30% to 30% which means faces looking more left or right are rejected.
- Face coordinates must not exceed 10% area near left and right edges and 5% area near top and bottom edges of input image.
- Face touching image's border is rejected.
- Face must cover less than 70% area of valid image region. Faces very close to camera are also rejected.

Recommendations for Face Recognition

- User's distance from camera when marking attendance must be between 1 to 3 ft (i.e. Face Height should be more than 80px).
- Good and evenly distributed light is required on user's face.
- Shadow / Under Exposure / Over Exposure lighting should be avoided.
- Motion Blur / Over Image Compression / Environmental Noise should be avoided.
- Any type of Occlusions like Sunglasses / Mask / Helmet / Cloths covering the face should be avoided.
- Face Angle should not be more than 30 degree horizontal and 10 degree vertical.

Recommended Camera Settings for Liveness Verification

The below mentioned recommendations are applicable to SATATYA MIDR20FL28CWS or Wall mounted Cogniface Cameras.

Name	Value
Profile No.	4
CODEC	MJPEG
Resolution	720p
Bit Rate Control	VBR (For all Modes)
Bit Rate	1024 kbps
FPS	10
Lens Correction	Off

Security Setup for COSEC¹

If you are having any security concerns then make sure you manually configure the changes as per the steps given below along with installation of the COSEC package:

Step 1:

It is expected that wwwroot folder contains only Cossec Web Applications i.e. COSEC, COSECAdmin, COSECVisitor. If there are any other applications in wwwroot folder then placing/updating web.config file may impact other application too.

If your www.root folder does not have the **web.config**, then follow the steps mentioned below:

- You need to copy the **web.config** file from the COSEC Setup/Prerequisites and place it in the root folder.
Path of the root folder: C:\inetpub\wwwroot.

1. These settings need to be done if COSEC is to undergo security testing via any third party to evaluate that the software is free from security vulnerability. These tests help validate the software's security controls and measures against real world's attacks, for example VAPT.

- Open this file in notepad, and replace the **matrixvyomqa.com** text with the IP or Domain which the user wants to use.

If your www.root folder already has the **web.config**, then follow the steps mentioned below:

- Copy the **web.config** file from the COSEC Setup/Prerequisites and place it on the desktop.
- Open this file in notepad, and replace the **matrixvyomqa.com** text with the IP or Domain which the user wants to use.
- Then copy the content from the dummy file and append it in your web.config file.

Step 2:

Uncomment the **httpCookies** tag in the following config files of COSEC.

- COSEC Path: C:\inetpub\wwwroot\COSEC\Web.config
- COSEC Admin Path: C:\inetpub\wwwroot\COSECADMIN\Web.config
- COSEC Visitor Web Path: C:\inetpub\wwwroot\COSECVisitor\Web.config

Step 3:

Enable TLS1.2 in the Server.

Port Requirement

The Default Ports for running different COSEC services for SSL and Non SSL communication are as follows:

1. **Master Service:** Non-Secure = 15001 & Secure = 15010
2. **Alert Service:** Non-Secure = 13001 & Secure = 13010
3. **Enroll Service:** Non-Secure = 12001 & Secure = 12010
4. **Monitor Service:**
 - Communication with Master Service: Non-Secure = 11001 & Secure = 11010
 - Communication with Device: Non-Secure = 11000 & Secure = 11009
 - Communication with Monitor Utility: 11003
5. **Admin Portal Service:** Non-Secure = 14001 & Secure = 14010
6. **Visitor Service:** Non-Secure = 16001 & Secure = 16010

Installing Prerequisites

The following Prerequisites should be installed (not included in setup) by user who is using Premise based solution (COSEC Centra) before running the COSEC Installation Setup:

1. Install Internet Information Services (IIS).

For Installing Internet Information Services (IIS) click on ["Installing IIS on the Windows Operating System \(Windows10\)"](#)

2. Install .Net Framework ver. 4.5 (mandatory).

For Installing .Net Framework click on [".Net Framework Installation"](#)

3. Microsoft SQL Server 2008 R2 SP2 or above.

For Starting Microsoft SQL Server click on ["Microsoft SQL Server"](#)

4. Oracle database server- upto version 19C. For Starting Oracle click on ["Oracle Installation"](#)

Installing IIS on the Windows Operating System (Windows10)

To install the IIS on the Windows operating systems, the administrator needs to open the Windows Features dialog by performing the following steps.



To know about IIS installation procedure in different operating systems, read the Help topic from the installation Setup.

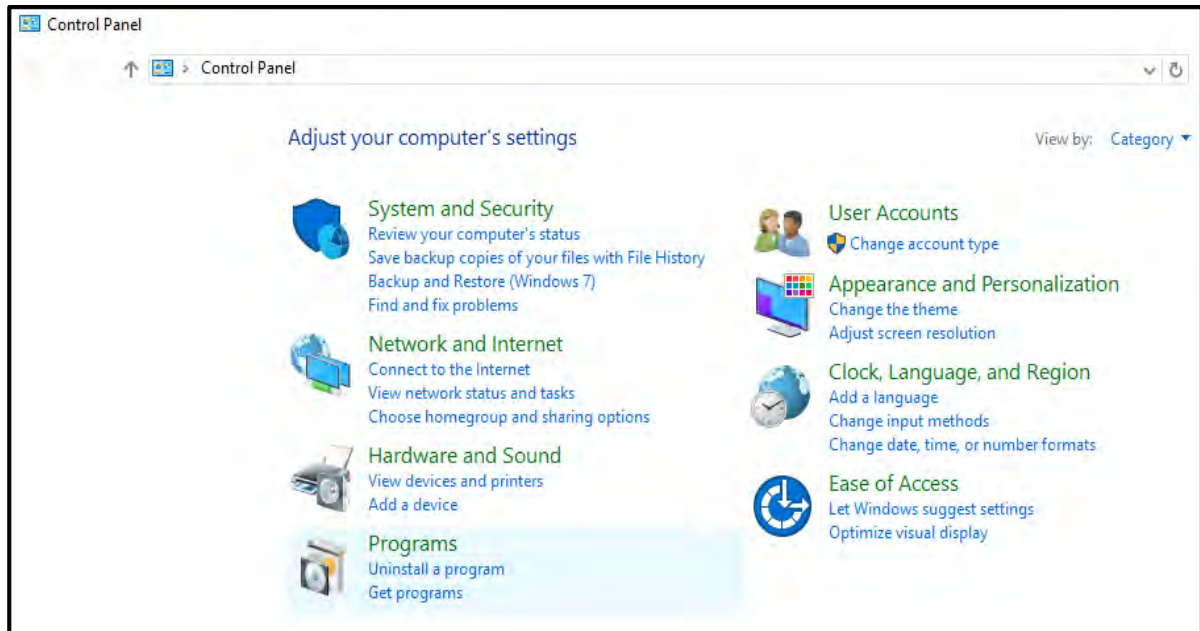
The following IIS components must be enabled for Windows 10 and above.

- "WCF-HTTP-Activation45"
- "IIS-WebServerRole"
- "IIS-WebServer"
- "IIS-ApplicationDevelopment"
- "IIS-NetFxExtensibility46"
- "IIS-ASPNET46"
- "IIS-ISAPIExtensions"
- "IIS-ISAPIFilter"
- "IIS-CommonHttpFeatures"
- "IIS-DefaultDocument"
- "IIS-DirectoryBrowsing"
- "IIS-HttpErrors"
- "IIS-HttpRedirect"
- "IIS-StaticContent"
- "IIS-Performance"
- "IIS-HttpCompressionStatic"
- "IIS-HttpCompressionDynamic"
- "IIS-Security"
- "IIS-RequestFiltering"
- "IIS-WindowsAuthentication"
- "IIS-WebServerManagementTools"
- "IIS-ManagementConsole"
- "IIS-IIS6ManagementCompatibility"
- "IIS-Metabase"
- "IIS-WMICompatibility"
- "IIS-LegacyScripts"

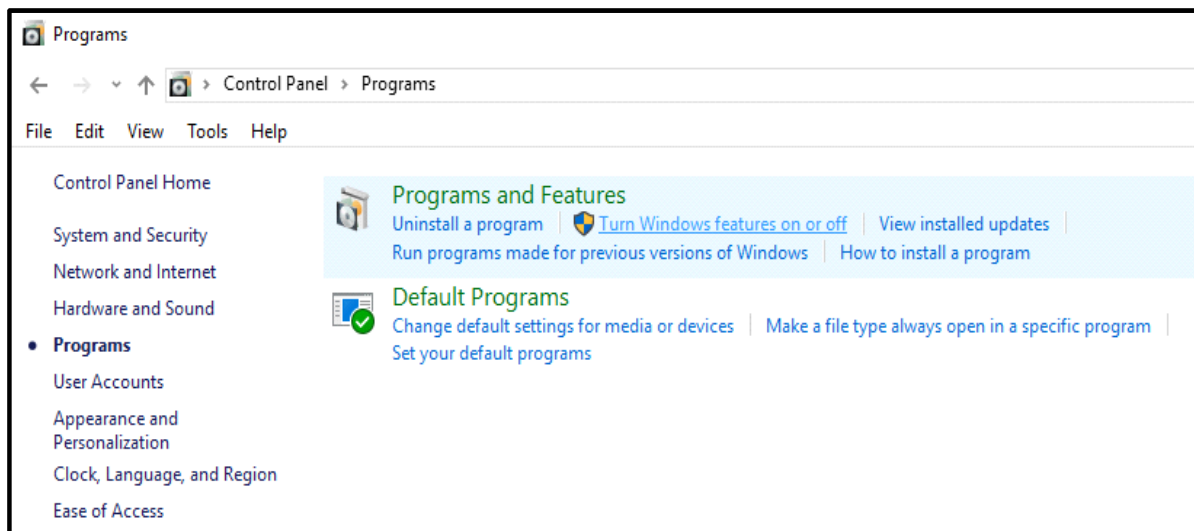
"IIS-LegacySnapIn"

The figures depict the screens as they appear on the **Windows 10** Operating system. However, the same procedure may be followed to activate IIS on other Windows Operating system.

- Navigate to Control Panel by typing it in “Search the Web and Windows” field. The Windows Control Panel appears as shown below. Now click on **Programs** as shown in the figure.

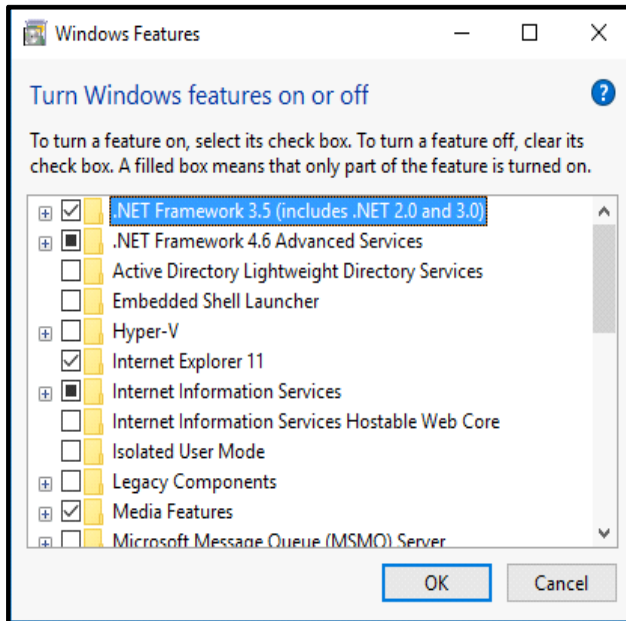


- The Control Panel **Programs and features** options are displayed.

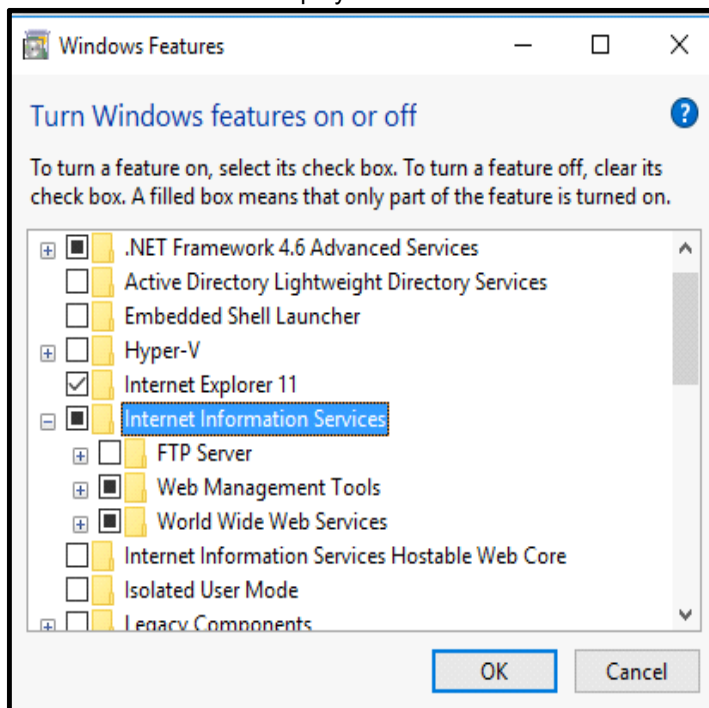


- Click on **Turn Windows features on or off**. You may receive the Windows Security warning at this point. Click **Continue** to continue.

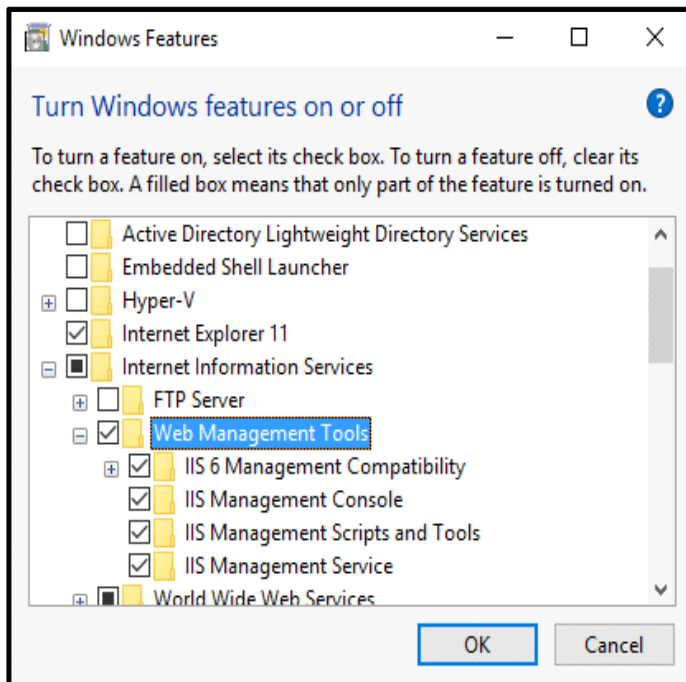
The Turn Windows Features on or off window will be displayed as shown below:



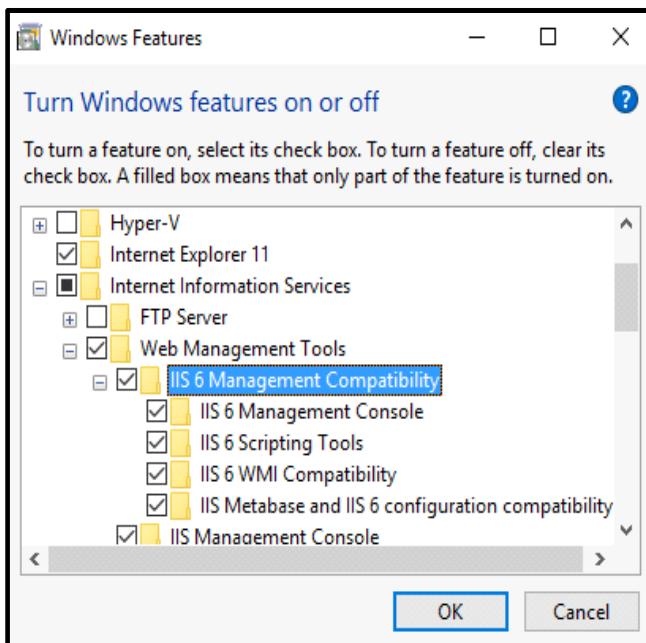
- The IIS default install features are shown as selected. Click on **Internet Information Services**. Additional IIS features will be displayed as shown.



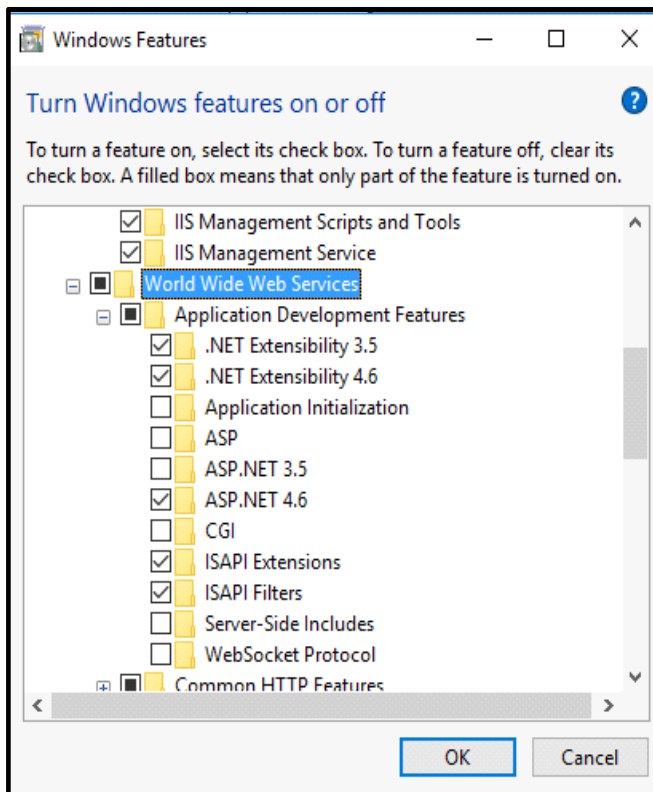
- Click on **Web Management Tools** to view the available features. Check the boxes against the features to be turned on as shown below.



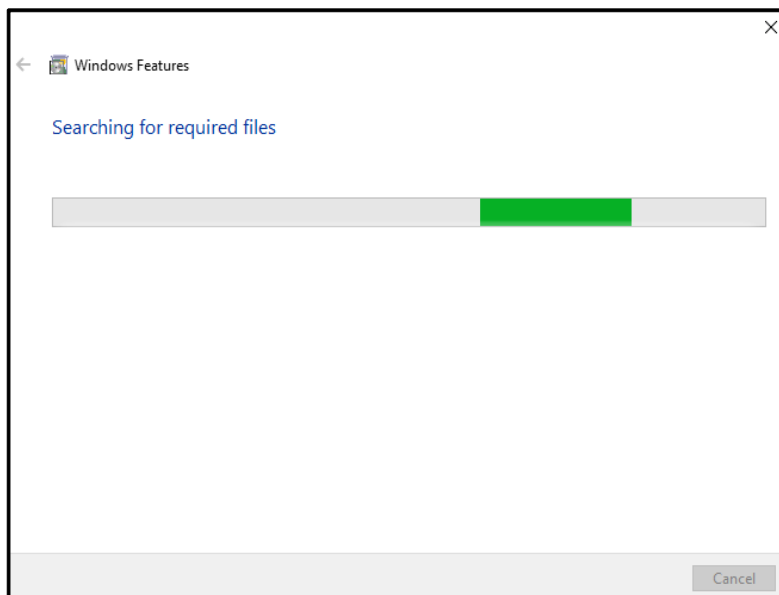
- Click on the **IIS 6 Management Compatibility** (Version depends on OS) and check the boxes against the features as shown.

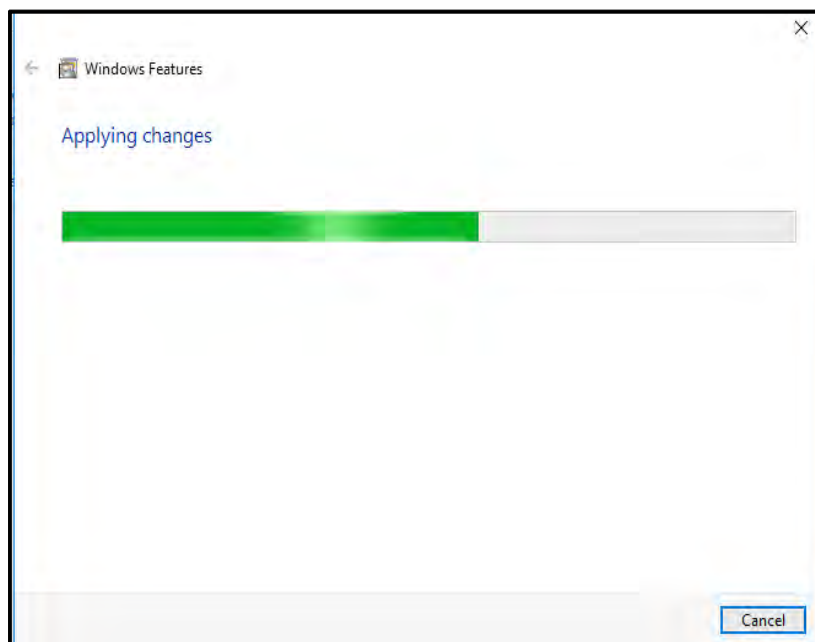


- Now click on **World Wide Web Services** and then on the **Application Development Features** option. Check the boxes against the features as shown.



- After selecting the IIS features as described above, click OK to start installation. The following Progress window will be displayed.





When the installation completes, the Windows Features dialog closes and you are returned to the Control Panel.

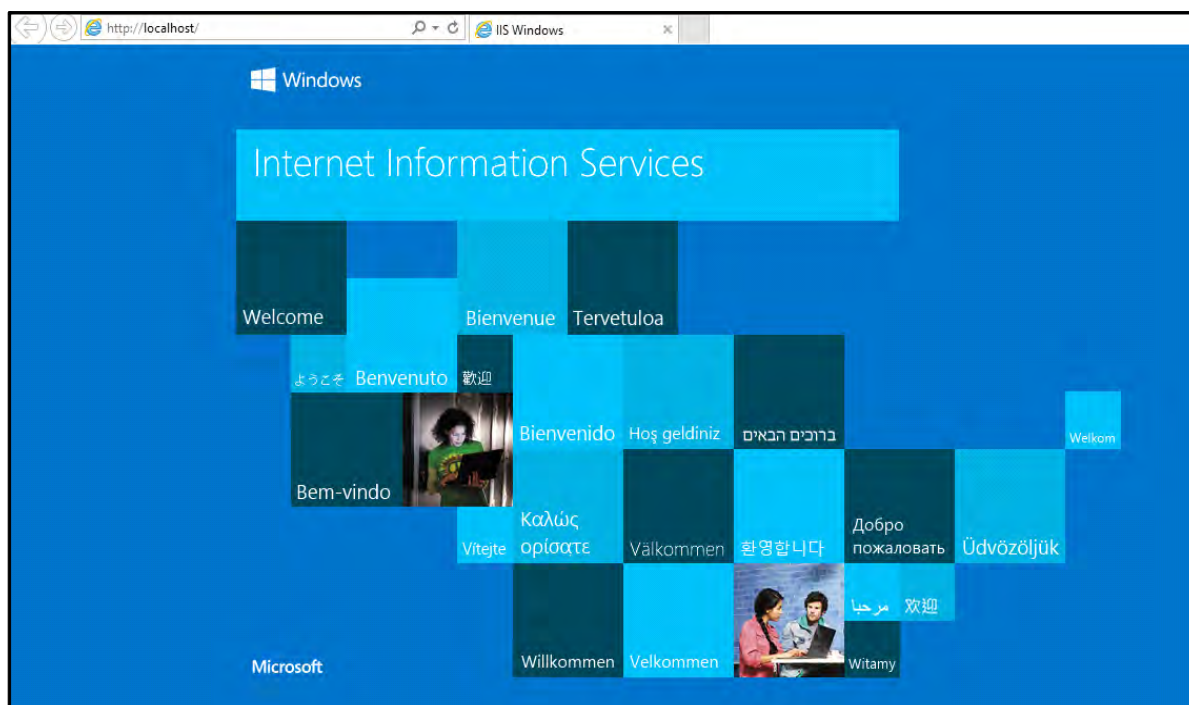


In order to perform a quick check to verify that IIS is installed:

*Start Internet Explorer web browser and enter the address <http://localhost/>
You should see the default IIS “Welcome” page.*



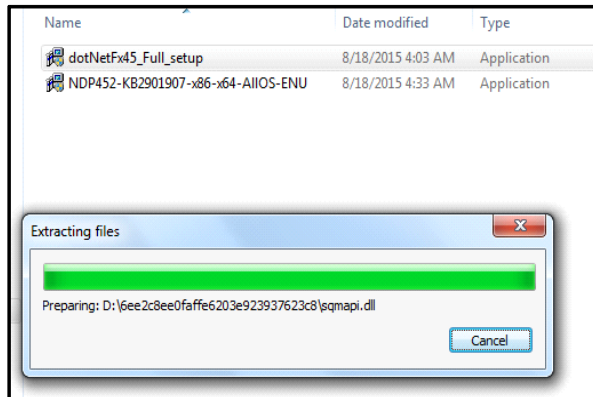
IIS version may change depending on the software updation and Windows in your Computer.



.Net Framework Installation

In the absence of the **.Net Framework**, user must install it before proceeding with COSEC installation.

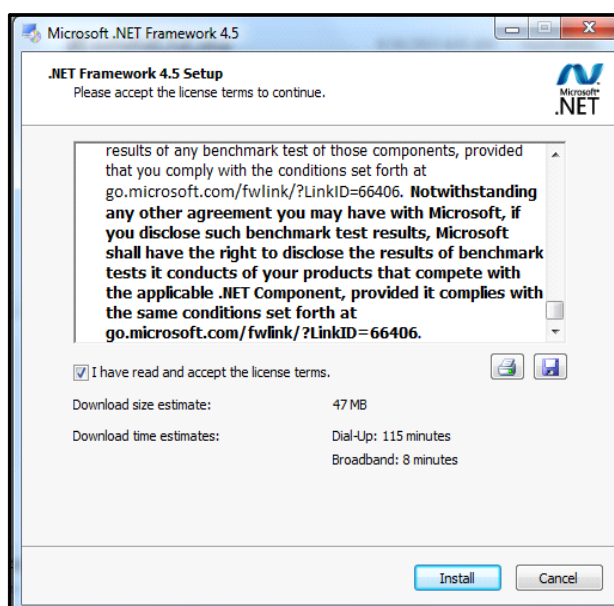
Name	Date modified	Type	Size
dotNetFx45_Full_setup	8/18/2015 4:03 AM	Application	982 KB
NDP452-KB2901907-x86-x64-AIIOS-ENU	8/18/2015 4:33 AM	Application	68,359 KB



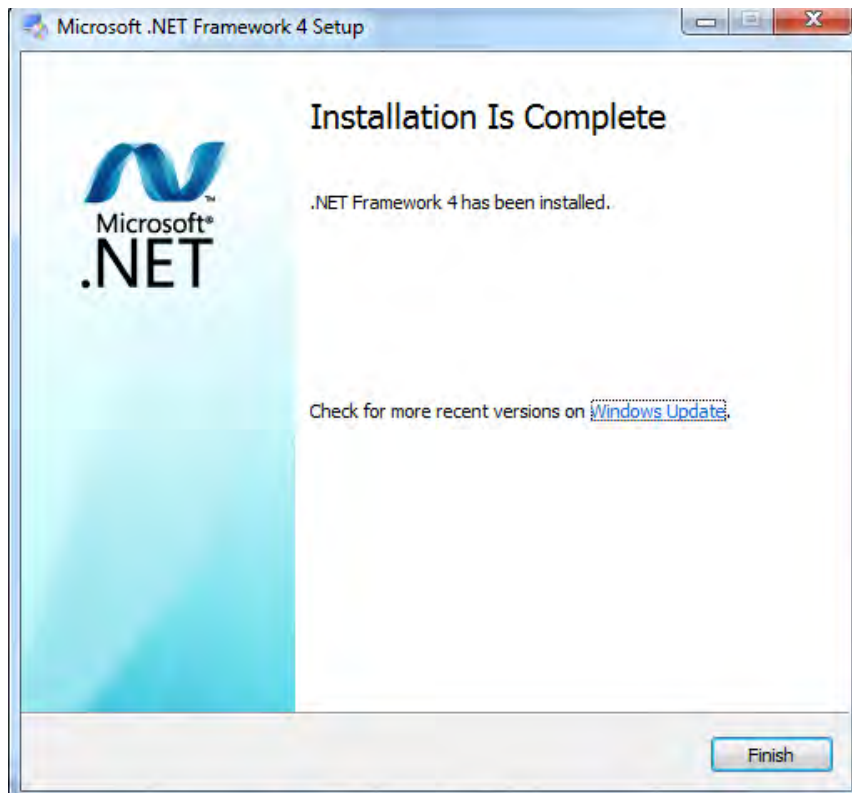
Browse the set and run the application.



Click on **Install** to install Microsoft .NET Framework. The Installation will begin.

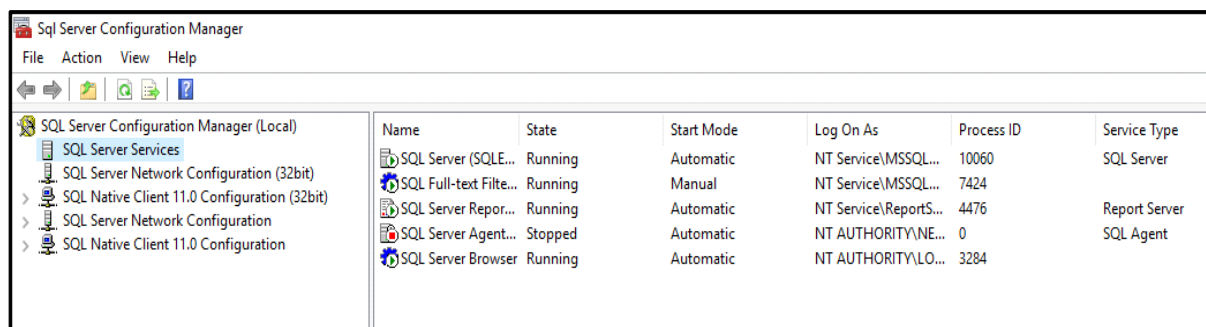


After installation is complete Click on **Finish** to exit the setup.

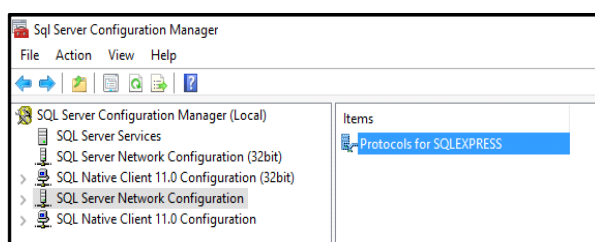


Microsoft SQL Server

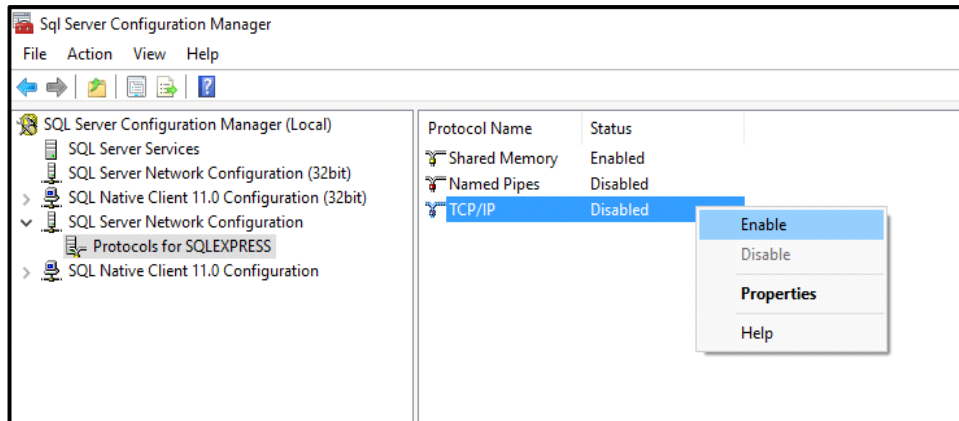
Now the installer needs to enable the appropriate protocols from the **SQL Server Configuration Manager** to allow the connectivity to the SQL server. For example; Navigate to the SQL Server 2014 Configuration Manager by typing it in “Search the web and Windows” option.



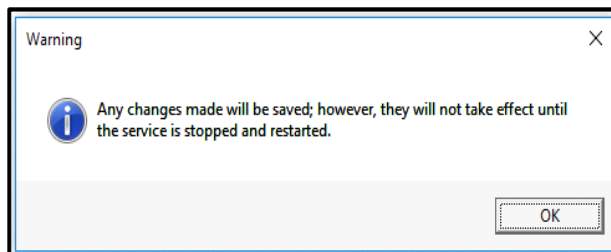
Go to **SQL Server Network Configuration > Protocols for SQLEXPRESS** option as shown in the figure.



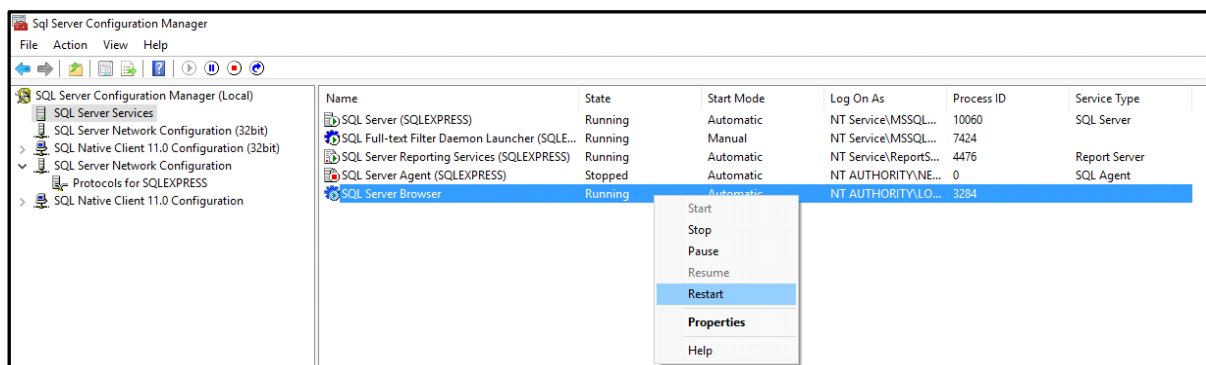
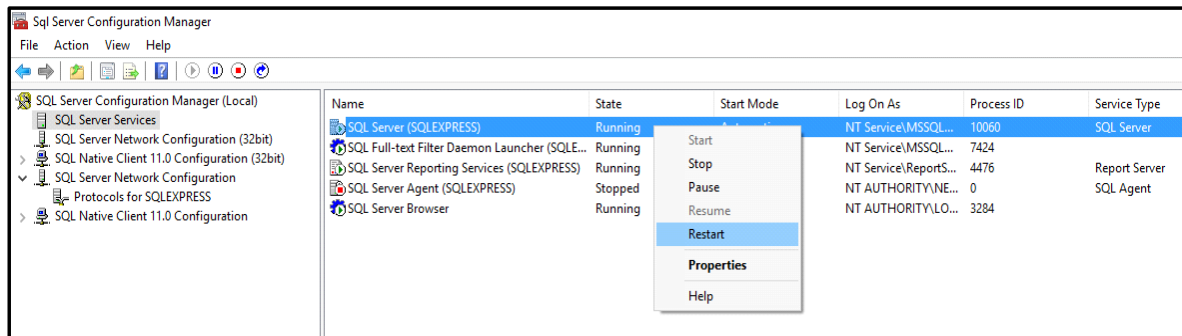
Click on the **Protocols for SQLEXPRESS** option in the left pane. The protocol options appear in the right pane as shown.



Right click on the **TCP/IP** option in the right pane and select the **Enable** option. The System will display the warning that the changes have been saved but it will take effect only after the service is restarted. Click OK to continue.

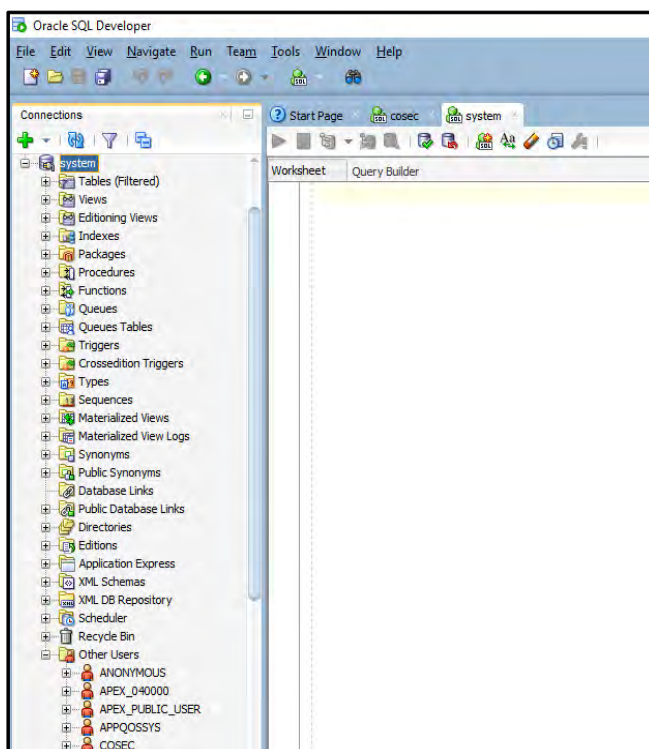


Select the **SQL Server Services** in the left pane. Restart the **SQL Server** and the **SQL Server Browser** services by right clicking on the options and selecting the **Restart** option as shown below:

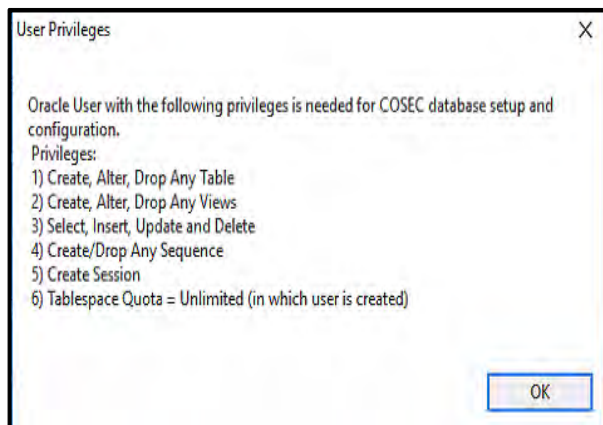
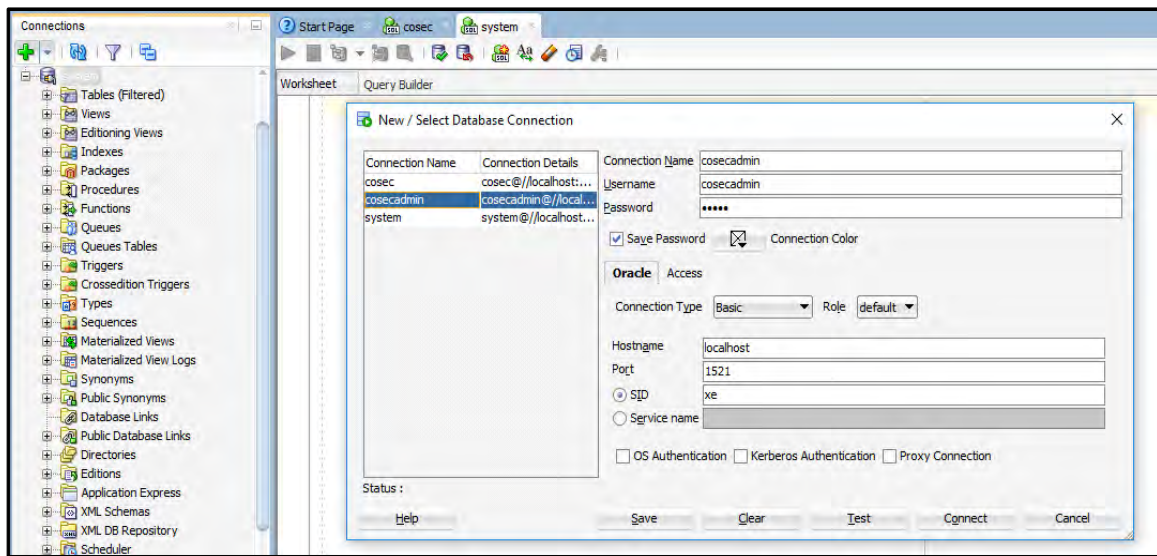


Oracle Installation

For Oracle database, Oracle setup must be installed as shown below.



Then you must create the user and assign the required privileges as shown below.

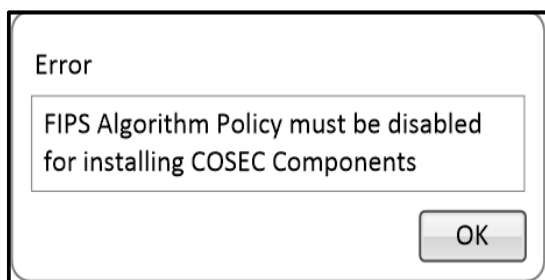


From PC where COSEC Web is installed - Execute msi file available at following path of Setup folder:
Setup\Prerequisites\SqlLocalDB\x64 OR x86 (as per 64-bit OR 32-bit system respectively)

Now once the Oracle user is created, you can start with the COSEC installation.

FIPS Algorithm Policy Check

To Install COSEC Component the FIPS Algorithm Flag must be disabled. If the FIPS Algorithm flag is enabled then following pop up will appear while installing the setup.



To disable FIPS Algorithm policy go to Registry Editor by typing regedit from the start menu of your computer.

Then go to the path:

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy.

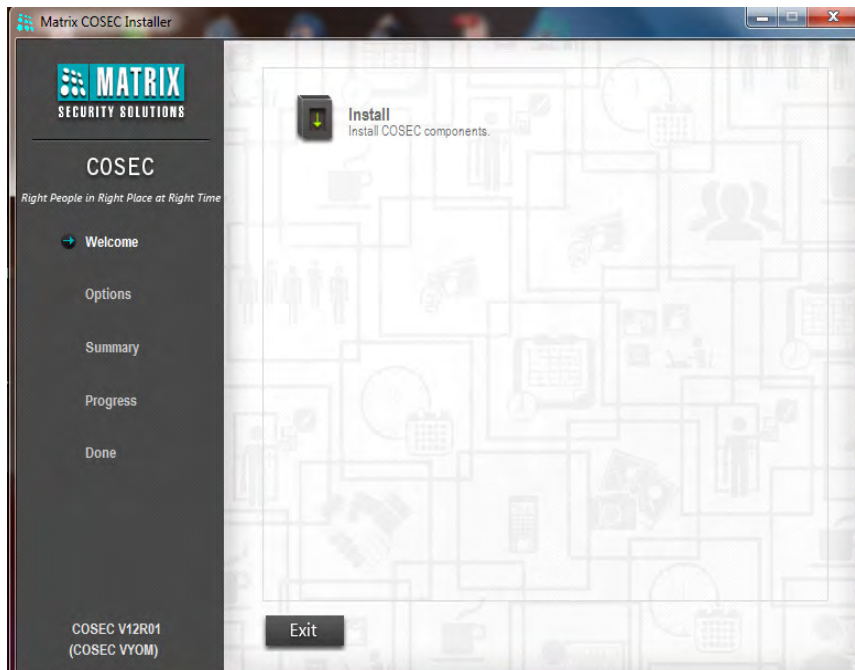
Now you can disable the FIPS Algorithm policy. Then Reset IIS Server and install the setup.

Installing COSEC

In order to install the COSEC application:

- Open the COSEC **Setup** folder in your PC.
- Double-click the COSEC Installer Application.
- The **Matrix COSEC Installer** page opens.

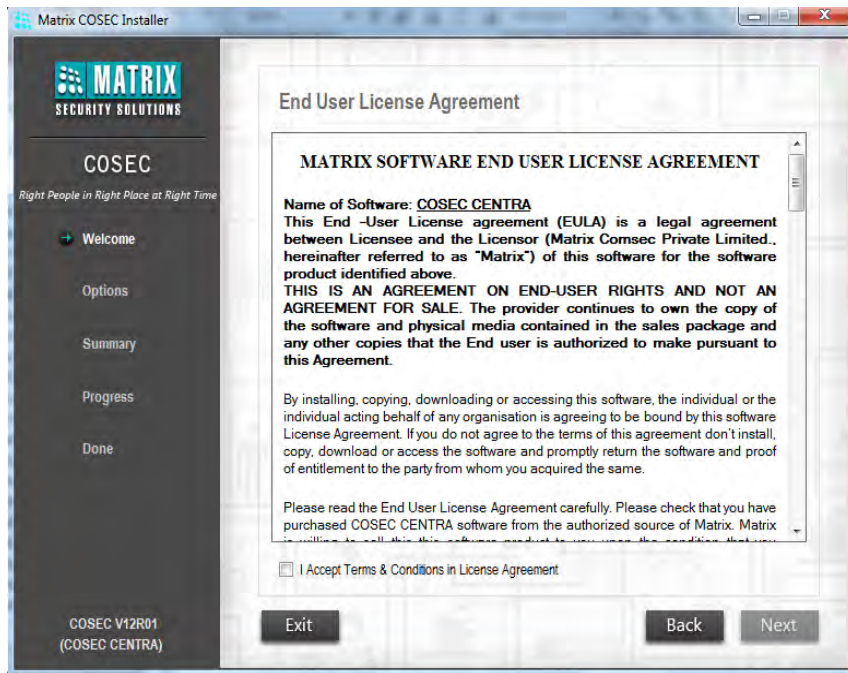
Name	Date modified	Type	Size
Help	09-12-2021 10:33	File folder	
Release Document	29-10-2021 14:54	File folder	
Setup	09-12-2021 10:47	File folder	
autorun.inf	16-08-2010 19:49	Setup Information	1 KB
COSECInstaller.exe	04-08-2017 11:23	Application	1,352 KB



This Installer automatically checks the computer for the prerequisites required for the installation of the applications prior to starting the installation process. Prior to running the Installer utility it is necessary to ensure that the logged in user has administrator rights on the computers where the various COSEC components are to be installed.

The COSEC application requires the Microsoft .Net Framework ver 4.0 to be installed prior to its installation on the application server. The COSEC Installer utility automatically detects the presence or absence of this component and the same must be installed in its absence.

Click on **Install** to initiate the installation process.



The End User License Agreement page will appear when new installation is done.

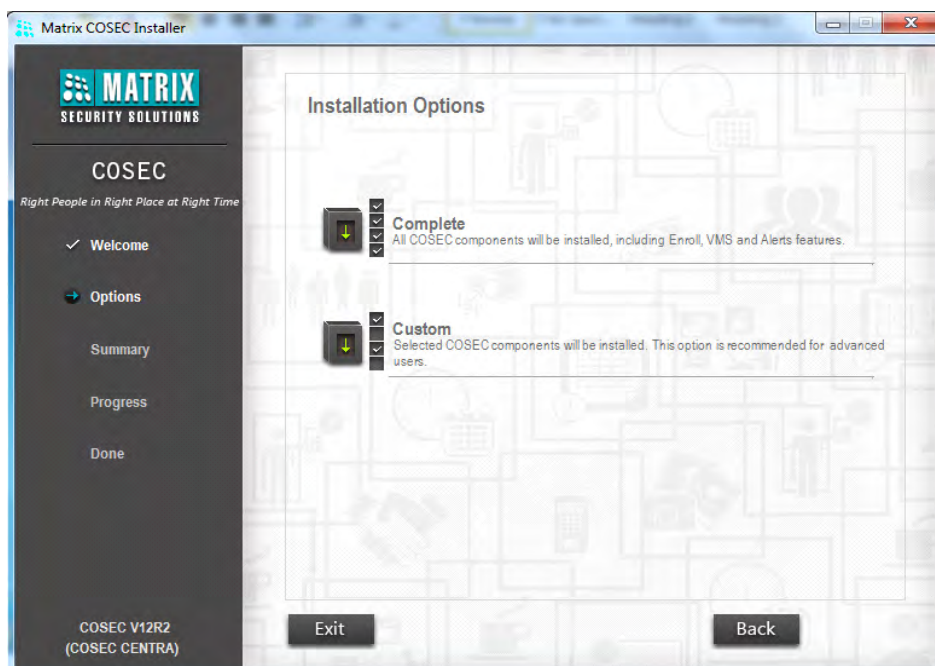


The **Annual Upgrade Package** for COSEC must be updated. Only then you can access COSEC. When the package gets expired; then you must have to get it upgraded through the Matrix channel partners.

Click on "I Accept Terms and Conditions" and click Next. The window appears with the following installation options:

Complete: Installs all the components of the COSEC application.

Custom: Enables the installer to select the components to be installed on a particular computer.



Select the appropriate installation option to continue.

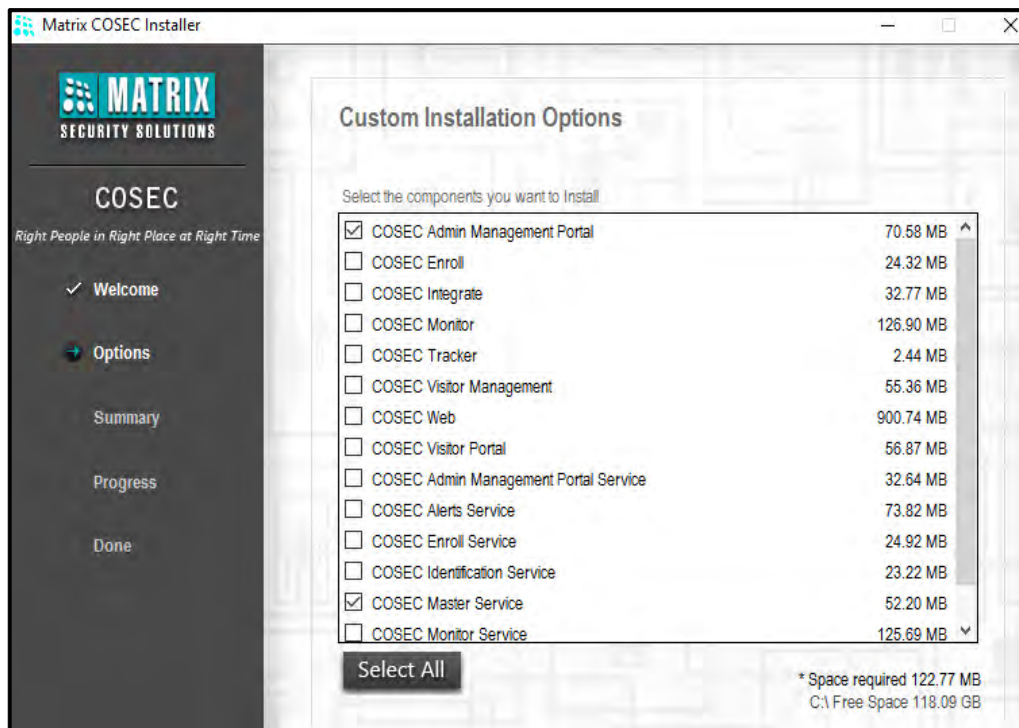
The grid on the left displays the progress of the installation process. Click on the **Exit** button to close the COSEC Installer. The **Back** button is provided and enables the user to go a step backwards in the installation process.

Custom Installation

The **Custom Installation** option provides flexibility in selecting the components to be installed by checking the boxes against the relevant options and click on **Next** to continue.

If you select Master Service is the custom options; then database creation page will appear from where you can configure Admin Management Database and COSEC Database which is explained in Complete Installation section.

If the custom options selected does not include Master service, then directly installation can be proceeded.



Complete Installation

The **Complete Installation** option will install all the COSEC components. Click on **Complete** option. The Database creation page will appear from where you can configure Tenant Admin Database and COSEC Database as shown below.

COSEC Admin Management Portal DB Details

Enter the details to configure Admin Management Portal Database.

Matrix COSEC Installer

COSEC
Right People in Right Place at Right Time

✓ Welcome
➔ Options
Summary
Progress
Done

COSEC 14.3.1
(COSEC CENTRA)

Complete Installation Options

COSEC Admin Management Portal DB Details:

Database Type: MS SQL
Server Address: sheetalraval\sqlexpress
Authentication: SQL Authentication
User Name: sa
Password: *****
Database Name: AdminPortalDB_V14R3

Create new database or Upgrade existing one

Test Connection

COSEC Web URL: localhost/COSEC
Location of COSEC Web folder

COSEC Visitor Portal URL: localhost/COSECVisitorPortal
Location of COSEC Visitor Portal folder

Note: Do not mention protocol http or https in URL.

Exit Back Next

Database Type: Select the database type as **MS SQL** or **ORACLE** to configure and connect the Admin Management portal database.

Matrix COSEC Installer

COSEC
Right People in Right Place at Right Time

✓ Welcome
➔ Options
Summary

Complete Installation Options

COSEC Admin Management Portal DB Details:

Database Type: Oracle
Server Address: 192.168.104.12
Authentication: SQL Authentication
User Name: cosecadmin
Password: *****
Database Name:

Create new database or Upgrade existing one.

Test Connection

NOTE: Oracle Server Setup has NOT been provided within the installer, please make sure Oracle is installed and USER is created in advance with defined [privileges](#)

COSEC Web URL: localhost/COSEC
Location of COSEC Web folder

COSEC Visitor Portal URL: localhost/COSECVisitorPortal
Location of COSEC Visitor Portal folder

Note: Do not mention protocol http or https in URL.

Success

i Test Connection Successful

OK

Server Address: Enter the server address where the database of Admin Management Portal is to be created. Eg: sheetalraval\sqlexpress for sql database and 192.168.104.12 for oracle database.

Authentication: Select the authentication type as SQL Authentication or Windows Authentication for connecting Tenant Admin Portal database for MS SQL database.

SQL database type

- For **SQL authentication**:
 - **User Name**: Specify the user name as created during sql server instance. Eg: sa
 - **Password**: Specify the password as created during sql server instance. Eg: matrix_1
- For **Windows authentication**: The Username and Password will be disabled.

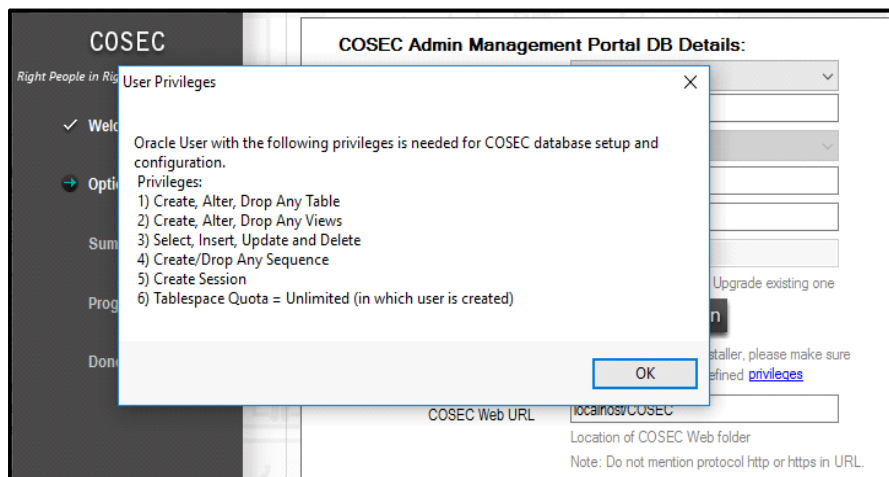
Oracle database type

In this Authentication field will be disabled. But you have to enter the User Name and Password to connect with the oracle database.

- **User Name**: Specify the user name as the name of the user created from Oracle system. Eg: cosecadmin
- **Password**: Specify the password as created while creating the user in Oracle. Eg: admin



Before connecting COSEC with ORACLE; you must create the user in ORACLE with following privileges.



Database Name: Enter the name with which Tenant Admin database is to be created in the server.

Test Connection: Click Test connection to establish connection with the configured SQL database or ORacle database.

COSEC Web URL: Enter the URL through which COSEC Web is to be accessed. If you are installing COSEC Web in PC2 and accessing from PC1; then give IP of PC2 where Web is installed. If Web is to be accessed locally then IP or localhost can be given in URL.

COSEC Visitor Portal URL: Enter the URL through which COSEC Visitor Portal is to be accessed.

MATRIX
SECURITY SOLUTIONS

COSEC
Right People in Right Place at Right Time

- ✓ Welcome
- ➔ Options
- Summary
- Progress
- Done

Complete Installation Options

COSEC Admin Management Portal DB Details:

Database Type: MS SQL

Server Address: sheetalravall/sqlexpress

Authentication: SQL Authentication

User Name: sa

Password: *****

Database Name: AdminPortalDB1

Create new database or Upgrade existing one

Test Connection

COSEC Web URL: localhost/COSEC
Location of COSEC Web folder

COSEC Visitor Portal URL: localhost/COSEC/VisitorPortal
Location of COSEC Visitor Portal folder

Note: Do not mention protocol http or https in URL.

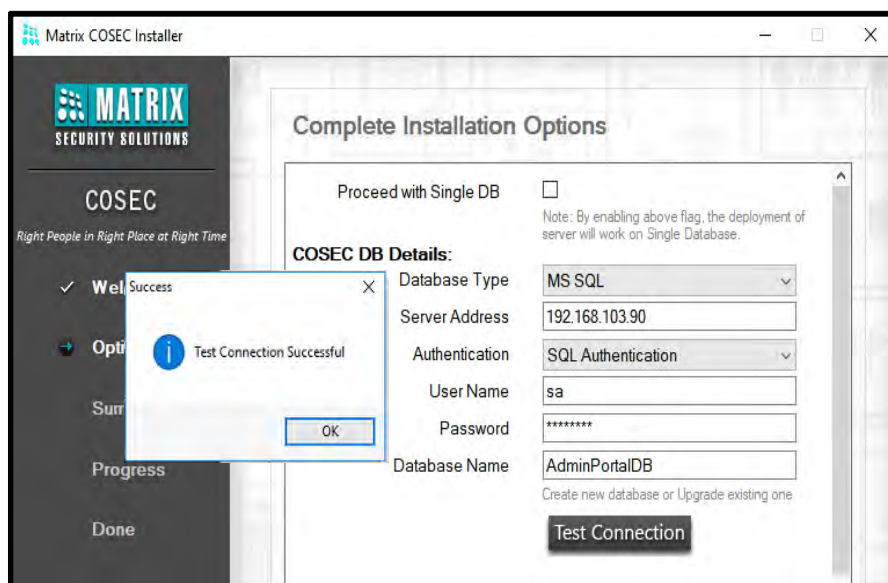
Now click on **Next** button.

COSEC DB Details

Enter the details to configure **COSEC Database**.



COSEC DB Details and **Company Details** must be configured only in **COSEC Centra** Solution.



Company Details:

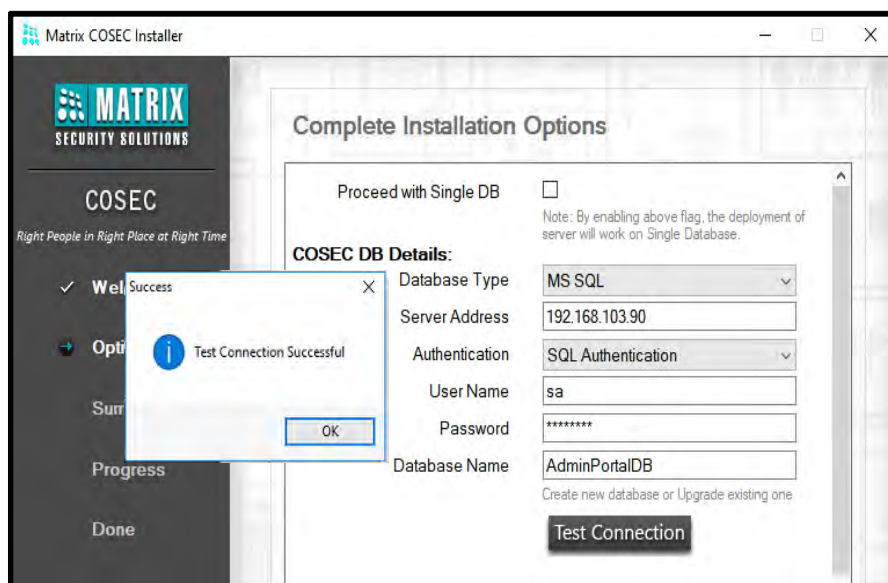
Name	sheetal
Email ID	sheetal.raval@matrixrd.org
Contact No.	9687624826
License Verification Mode	Server Based

Exit Back Next

Proceed with Single DB: Select this checkbox to complete the installation with creation of a single database. The details will be auto-filled similar to the details of [“COSEC Admin Management Portal DB Details”](#)

Database Type: Select the database type as **MS SQL** or **ORACLE** to configure the COSEC database.

Database Type is **MS SQL**



Company Details:

Name: sheetal

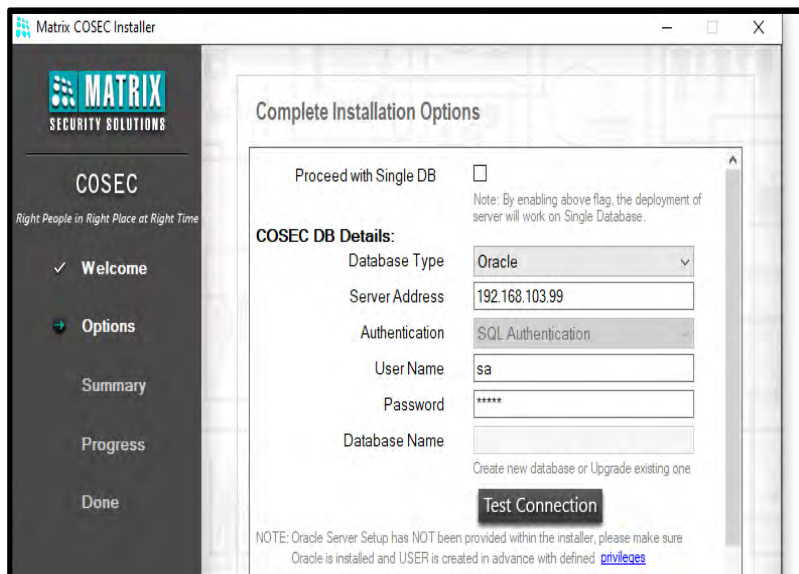
Email ID: sheetal.raval@matrixrd.org

Contact No.: 9687624826

License Verification Mode: Server Based

Exit Back Next

Database Type is Oracle



Server Address: Enter the server address where the COSEC database is to be created. Eg: SHEETALRAVAL\sqlcxpress for sql and 192.168.104.12 for oracle.

Authentication: Select the authentication type as SQL Authentication or Windows Authentication for connecting COSEC database with SQL server.

- For **SQL authentication:**
 - **User Name:** Specify the user name as created during sql server instance. Eg: sa
 - **Password:** Specify the password as created during sql server instance. Eg: matrix_1
- For **Windows authentication:** The Username and Password will be disabled.

For Oracle database type; Authentication field will be disabled. But you have to enter the User Name and Password to connect with the oracle database.

- **User Name:** Specify the user name as the name of the user created from Oracle system. Eg: cosecadmin
- **Password:** Specify the password as created while creating the user in Oracle. Eg: admin

Database Name: Enter the name with which COSEC database is to be created in the server.

Test Connection: Click Test connection to establish connection with the configured SQL database or Oracle database.

Company Details

Name: Enter the name of the company which will be created by default in the Admin Management Portal.



In COSEC Centra only one company will be created.

Email ID: Enter the Email ID of the company. This ID will appear in the Company configuration.

Contact No: Enter the Contact Number of the company. This contact number will appear in the Company configuration.

License Verification Mode: Select the option as **Server Based** or **Device Based** for verifying the license.

- For **Server based**: License will be verified from the dongle connected to the PC where Master service is installed.
- For **Device based**: License will be verified from the dongle connected to the COSEC device. This device will communicate with Master Service so that Master Service can fetch the license key from the dongle and all of the COSEC services will function.



Only Vega direct door and Panel200 in server mode can be used for Device based license verification. You must ensure that Vega and Panel200 are in CENTRA connection mode.

Once dongle is connected to the device (Vega or Panel200); enter the License Server URL (Default is 192.168.50.100) and License server Port (Default is 15025) in Server Settings from device or its webpage.

Server based License Reading

The dongle must be inserted in the computer where Master Service is running.

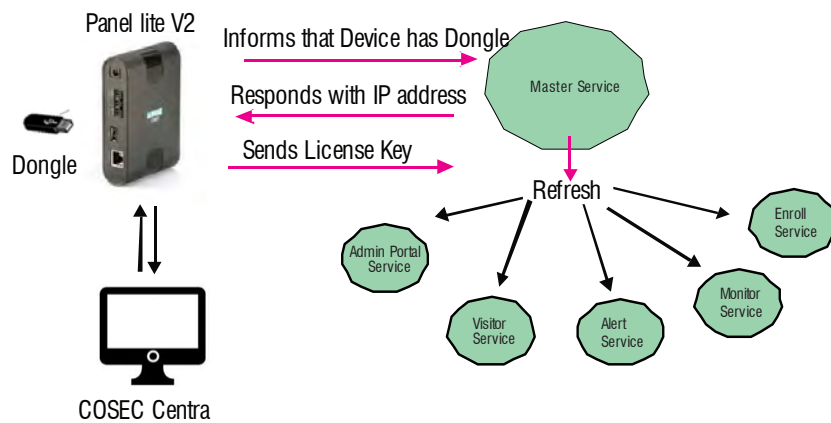
Master service checks for the presence of dongle. If dongle is available, then Master service sends Refresh command to all other services.

Device based License Reading & Writing

In device based licensing Vega direct door or Panel200 can be used. And the Tenant/ Company must be device based.

The license dongle is connected to either Vega direct door or Panel200.

- The device (Vega/Panel200) sends information to the Master service that device has license dongle.
- The Master Service responds to the device by sending the IP address of Master service.
- Now device sends license key to the Master service. The master service gets the license key and gives to other services.



When dongle is removed from the device, then immediate information is sent to the Master service and immediate refresh is sent to other services.

When device goes offline, then master service will continue working for a considerable time after which the master service and other services will get refresh.

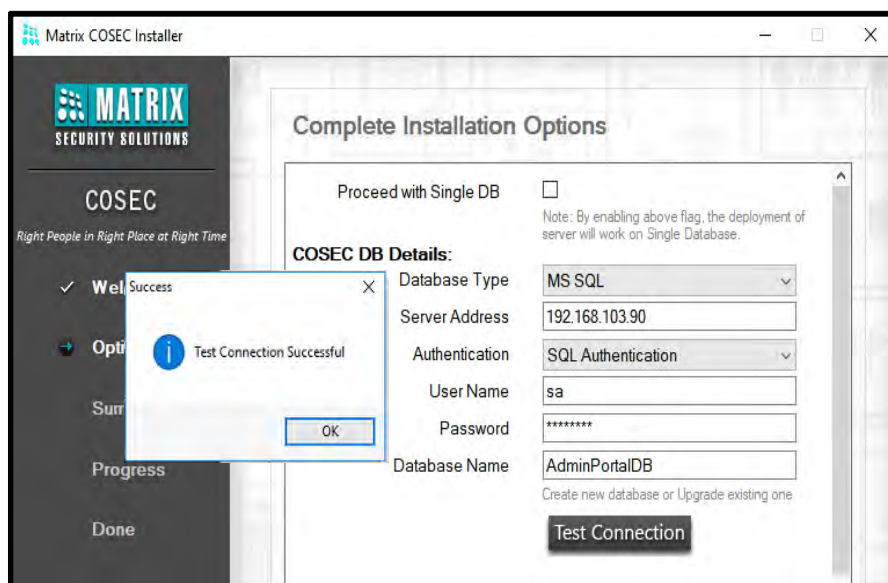
Any change or updation in license key will be fetched by the device when it is online. The updated license key will then be sent to the Master Service and hence other services.



In the Server Settings of Panel200; Enter the URL for COSEC Centra server as the IP address of the computer where Monitor Service is running.

And enter the License Server URL as the IP address of the computer where Master Service is running.

Once the license verification mode is selected and test connection is successful, click on **Next** button.



Company Details:

Name: sheetal

Email ID: sheetal.raval@matrixrd.org

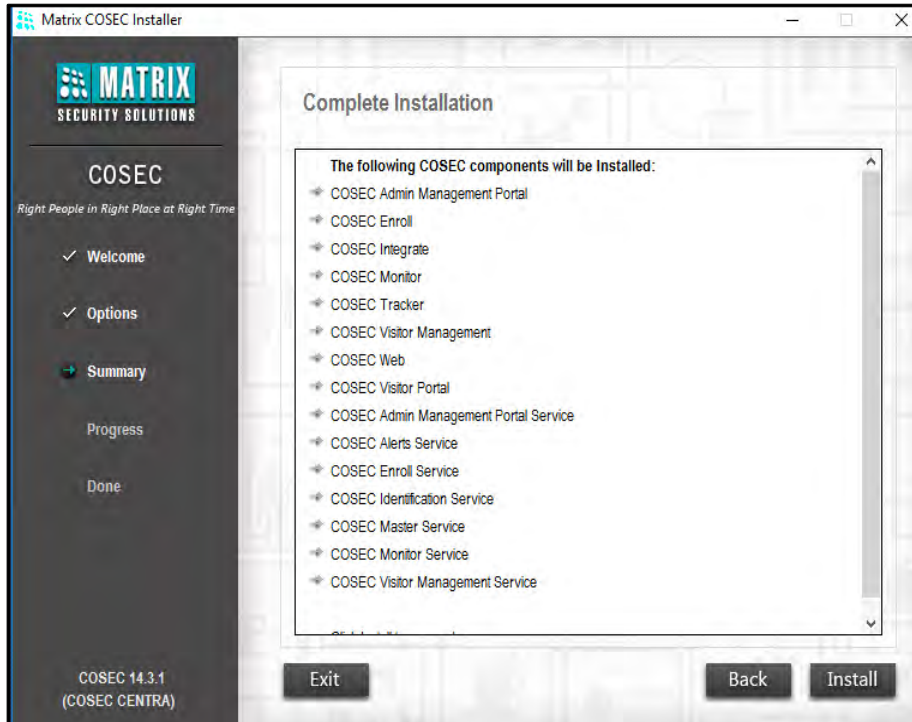
Contact No.: 9687624826

License Verification Mode: Server Based

Exit Back Next

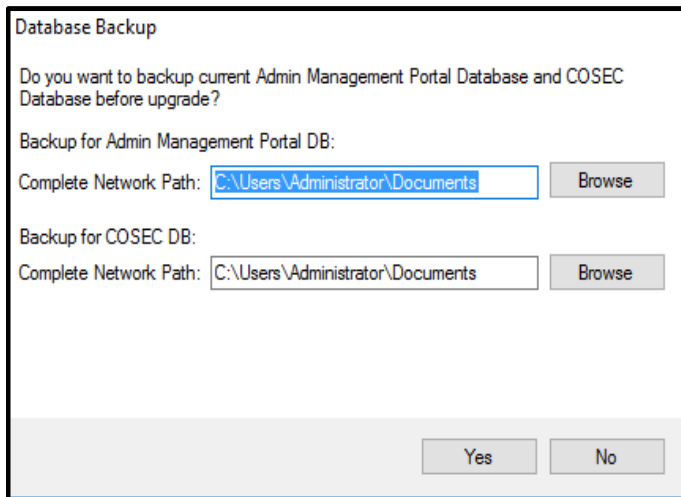
The selected components or all the components will be installed based on Custom or Complete installation respectively.

Click **Install** to start installation of components.

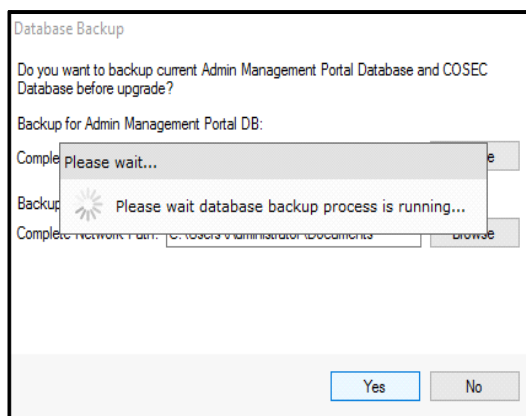
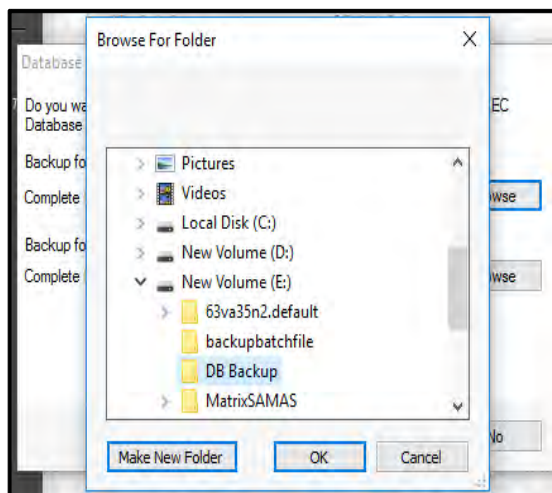


After the Installation is successful, Admin Portal database backup and COSEC database backup can be taken at desired network path.

The default network path where backup will be taken is of My documents folder.

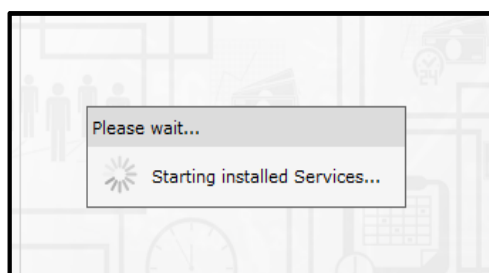


You can **Browse** and select the desired path where backup is to be taken.

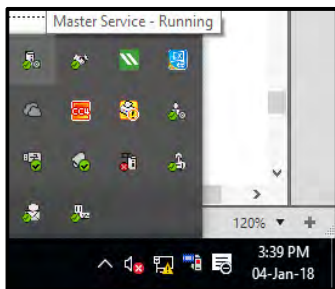


In case if the Backup fails at the time of installation then its log entry will be made in its backup log file which would be created at the same location as backup.

After taking the backup, the following services will be started automatically.



- COSEC Master Service
- COSEC Admin Management Portal Service
- COSEC Alert Service
- COSEC Enroll Service
- COSEC Monitor Service
- COSEC Identification Service
- COSEC VMS Services

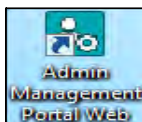


Once the services are started and license dongle is connected then you can login to Admin Portal and COSEC Web.

Login to Admin Portal

To access the Admin Management Portal, type the following link in your browser.

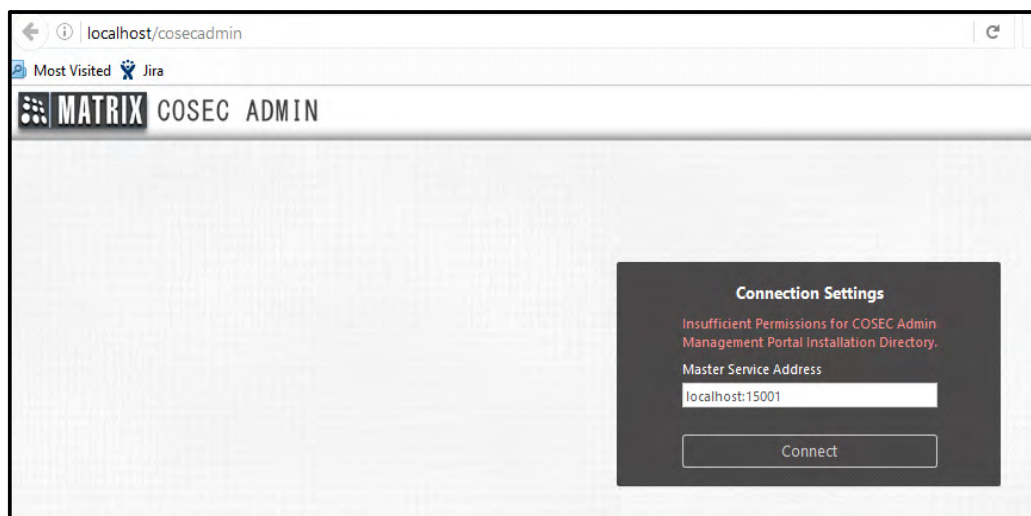
<http://localhost/cosecadmin>



OR click on

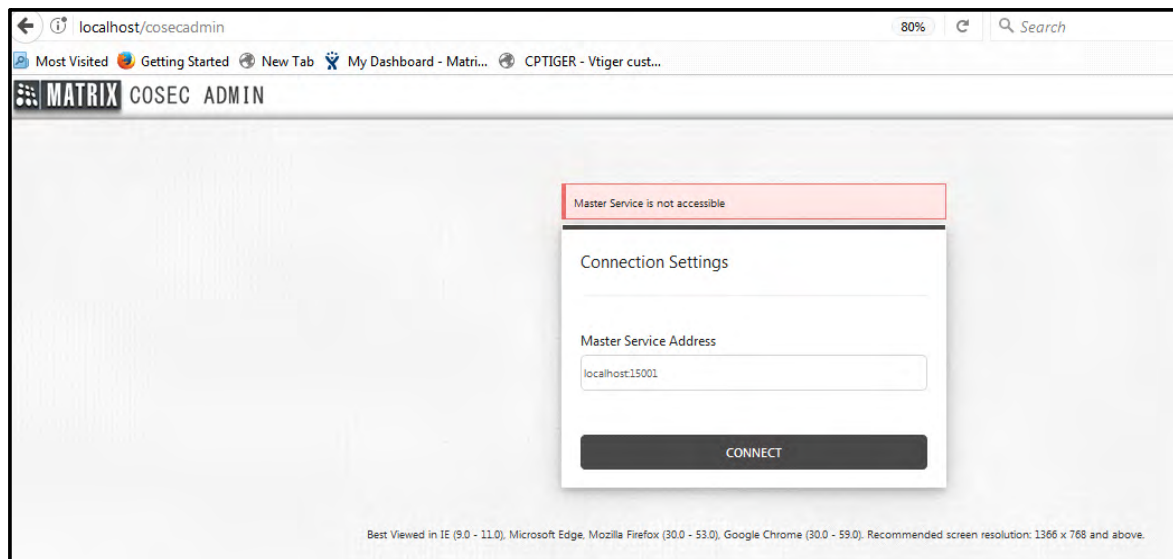


The COSECADMIN folder in inetpub must have administrator rights to access the Admin Portal.



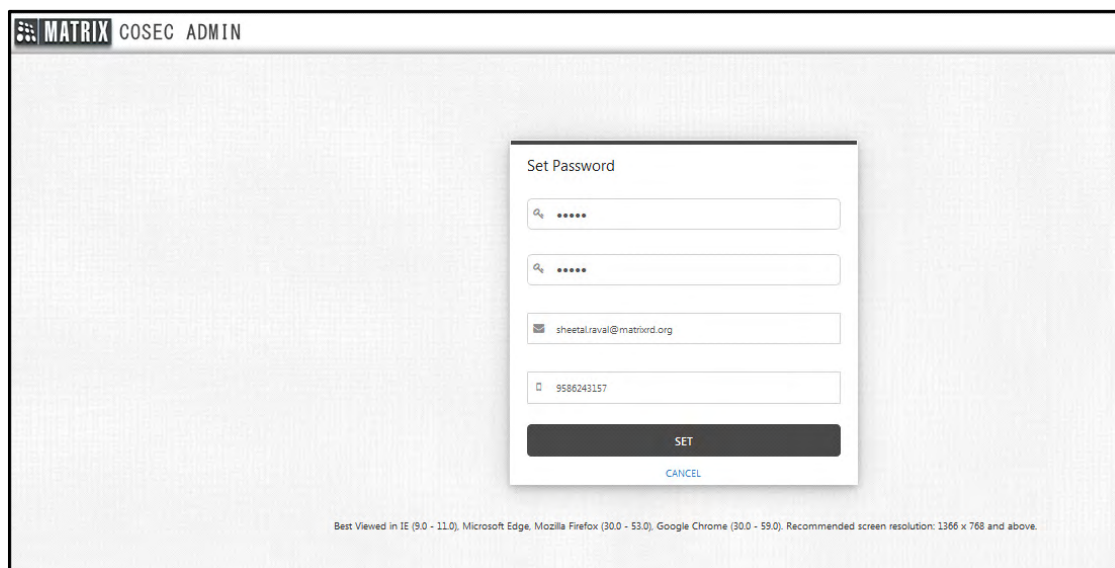
Check the rights on COSECADMIN folder. For this go to path C:\inetpub\wwwroot. The IIS user must be given full control rights. So click Edit and enable Full control checkbox. Then apply the changes. Now you can login to Admin Portal.

The Connection Settings page will appear as shown below:



Enter the **Master Service Address** to connect with the database and click **Connect**. The Admin Portal will get connected with its database through the Master service. Ensure that Master service is running.

Then login with default login ID “sa” and set the desired password.



The Admin Portal page will open as shown below.

MATRIX COSEC ADMIN

Company Configuration
 Profile
 License and Services
 Monitor Configuration
 COSEC Services
 Manage Database

Profile

ID *

Name *

Active ☒

Time Zone *

License Verification Mode *

Dongle Security URL *

Contact Details

Address Details

Database Configuration

Search

ID	Name	Status
1	Shalini	Active

For detailed information regarding Admin Portal read **Admin Mgt Portal User Guide** from the setup.

Login to COSEC Web

Now you can login to the COSEC Web using the Web URL say **192.168.104.12/cosec** or **localhost/cosec** in your browser. For login process "[COSEC Web](#)"

For detailed information regarding COSEC Web read **COSEC User Guide** from the setup.

Launching the COSEC Application

There are three components to start COSEC application.

- COSEC Master Service
- Admin Portal Web Server application
- COSEC Web server application

Master Service Connection

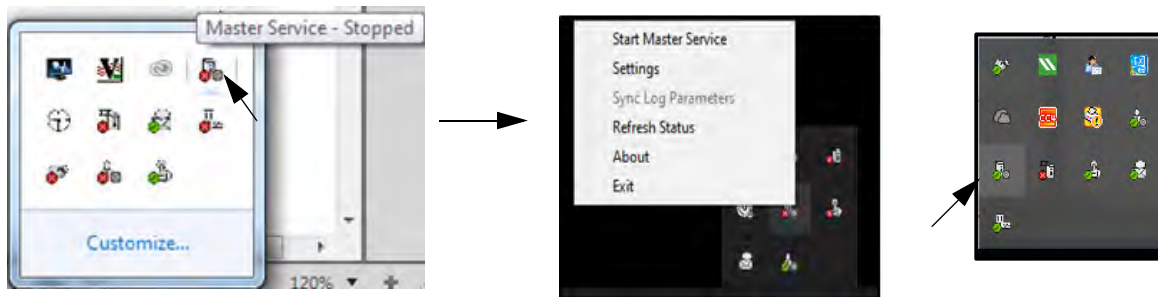
For Tenant Portal connection with Master Service, you must enter the Master Service URL in web configuration file at path **C: > inetpub > wwwroot > COSECADMIN>Web**

```
</system.web>
<appSettings>
<add key="MasterUrl" value="://localhost:15001/MasterService/" />
  <add key="HttpEnable" value="false" />
  <add key="IsSSL" value="false" />
  <add key="webpages:Version" value="3.0.0.0" />
  <add key="webpages:Enabled" value="false" />
  <add key="ClientValidationEnabled" value="true" />
  <add key="UnobtrusiveJavaScriptEnabled" value="true" />
  <add key="DomainName" value=".matrixvyom.com" />
  <add key="WebVirtualDir" value="Vyom" />
  <add key="Identity" value="" />
  <add key="IsInternal" value="true"/>
</appSettings>
```

For COSEC Web connection with Master Service, you must enter the Master Service URL in web configuration file at path **C: > inetpub > wwwroot > COSEC > Web**

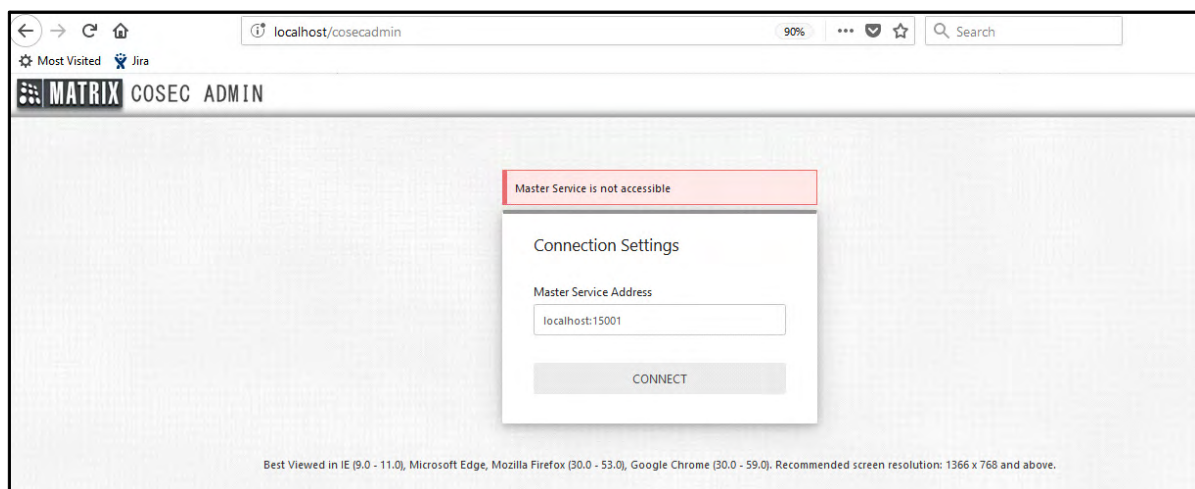
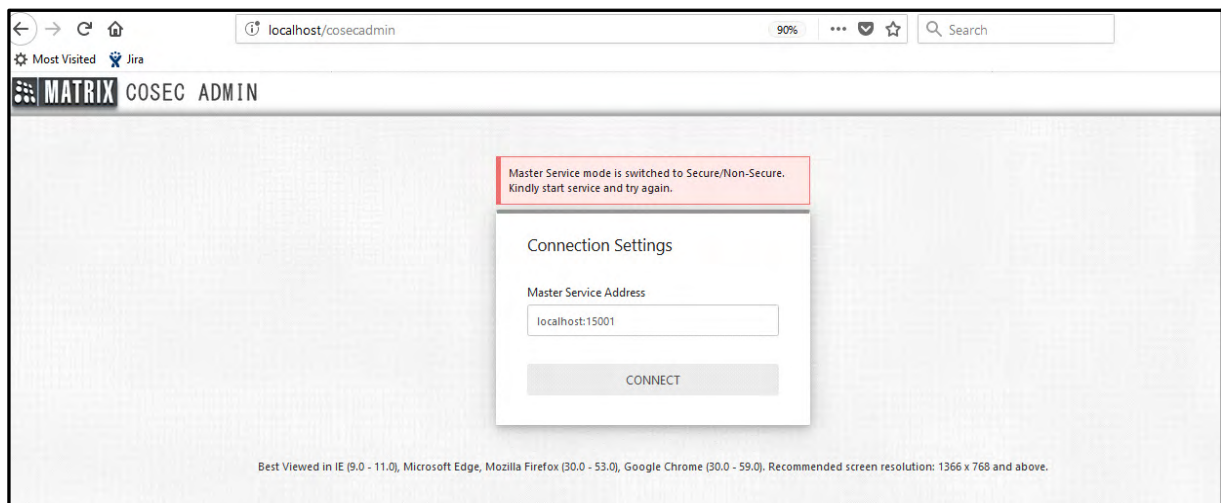
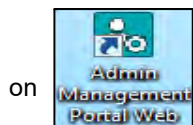
```
<appSettings>
  <add key="CrystalImageCleaner-AutoStart" value="true"/>
  <add key="CrystalImageCleaner-Sleep" value="60000"/>
  <add key="CrystalImageCleaner-Age" value="120000"/>
  <add key="ClientURL" value="www.sheelal.matrixvyom.com" />
  <add key="MasterUrl" value="://192.168.104.12:15001/MasterService/" />
  <add key="HttpEnable" value="false" />
  <add key="IsSSL" value="false" />
  <add key="baseUrl" value="http://192.168.104.12/cosec/" />
  <add key="isCloudApp" value="true" />
  <add key="Identity" value="" />
</appSettings>
```

The Master Service can be started from the Master Service icon from the system tray as shown below.



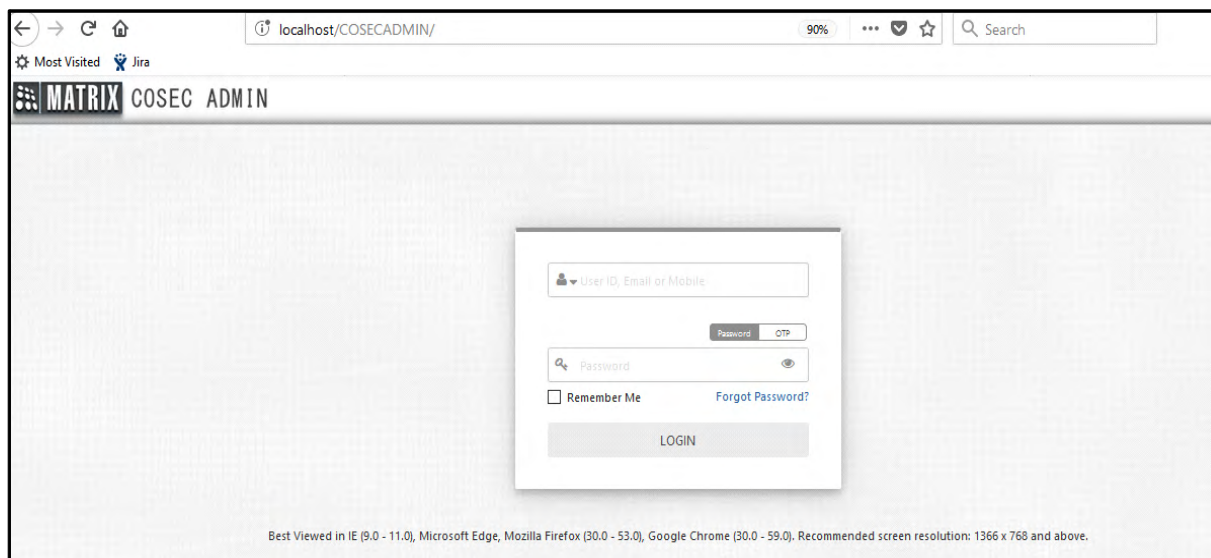
Admin Management Portal

Now login to the Tenant Admin Portal with URL **localhost/cosecadmin** or say 192.168.104.12/cosecadmin Or click



Connection Settings: Enter the Master Service URL to connect Tenant Admin Portal. Ensure that Master Service is running. Then click Connect button.

The Admin portal login page appears as shown below:



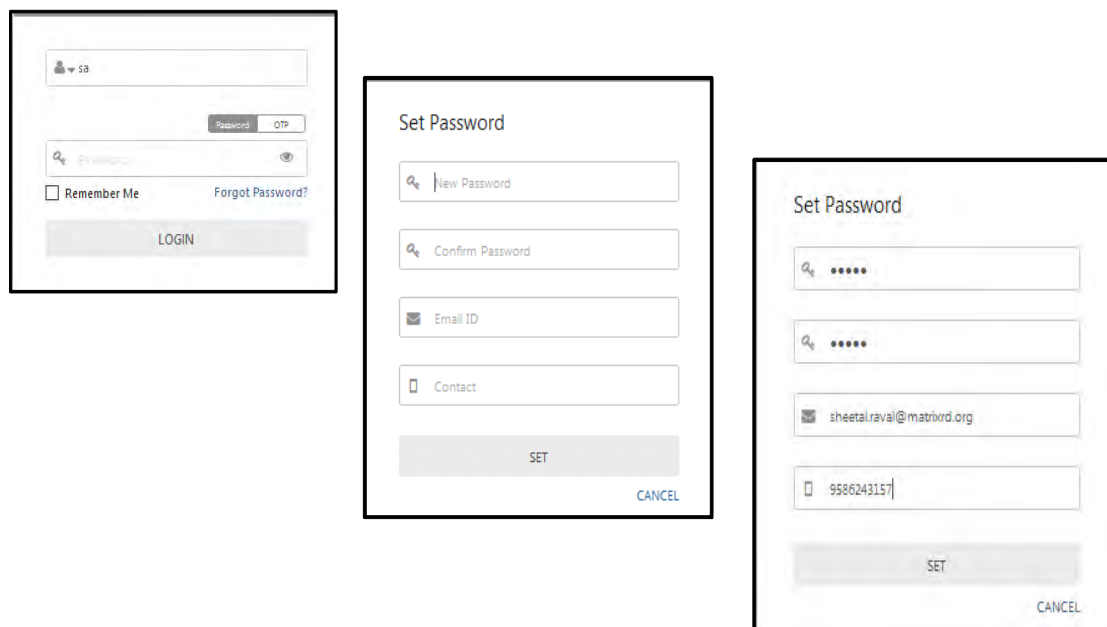
The screenshot shows a web browser window with the address bar displaying 'localhost/COSECADMIN/'. The page title is 'MATRIX COSEC ADMIN'. The login form is centered and contains the following elements:

- A text input field for 'User ID, Email or Mobile'.
- Buttons for 'Password' and 'OTP'.
- A text input field for 'Password' with a toggle for visibility.
- A checkbox for 'Remember Me' and a link for 'Forgot Password?'.
- A 'LOGIN' button.

At the bottom of the page, there is a footer text: 'Best Viewed in IE (9.0 - 11.0), Microsoft Edge, Mozilla Firefox (30.0 - 53.0), Google Chrome (30.0 - 59.0). Recommended screen resolution: 1366 x 768 and above.'

When you are accessing Admin portal for the first time; then enter the login ID as “sa”. Click Login and set the password for “sa” from the **Set Password** screen.

Enter the **Email ID** and **Contact** number through which you can retrieve your account when you forget your password. Also the OTP can be received on this Email ID and Contact number. Click **Set** to save the details.



The three screenshots illustrate the initial setup steps:

- Login Form:** Shows the login form with 'sa' entered in the 'User ID, Email or Mobile' field. The 'LOGIN' button is visible.
- Set Password Form (Initial):** Shows the 'Set Password' form with fields for 'New Password', 'Confirm Password', 'Email ID', and 'Contact'. The 'SET' button is visible.
- Set Password Form (Filled):** Shows the 'Set Password' form with fields for 'Password', 'Confirm Password', 'Email ID' (filled with 'sheetal.raval@matrixrd.org'), and 'Contact' (filled with '9586243157'). The 'SET' button is highlighted.

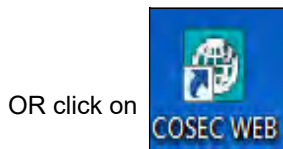
Then Enter the **Login ID** and **Password/OTP** to login into Admin Portal. You can use Login ID as **User ID/Mobile Number/Email ID**. The login process is similar to that described in “[COSEC Web](#)” section. The detailed description for login into Admin Portal is given in Admin Portal Manual.

The Admin Portal Profile page opens and the tenant would be created with name as entered in Company details.

ID	Name	Status
1	sheetal	Active

COSEC Web

Now you can login to the COSEC Web using the Web URL **localhost/cosec** or say **192.168.104.12/cosec** in your browser.



The login page appears as shown below.

You can login with the default User Names **sa** in the Login ID field.

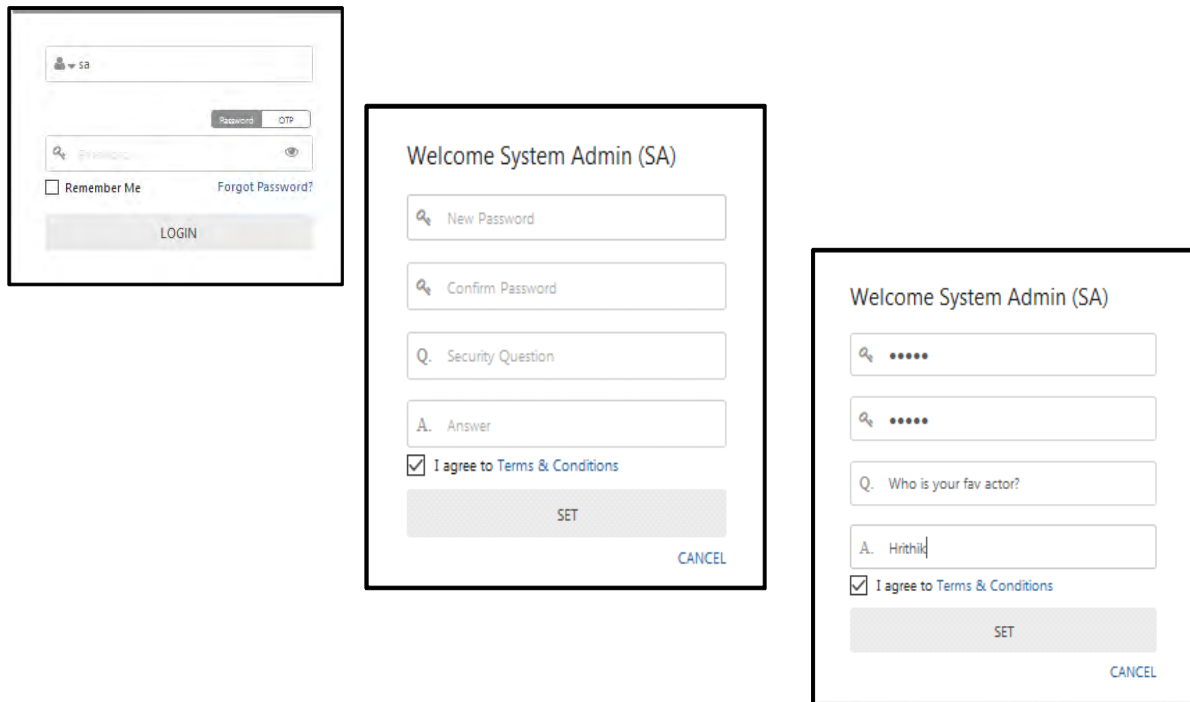
The **se** and **so** login are inactive by default. You can activate these login account from System Accounts page once you have logged in using **sa** login.

sa- System Administrator having unlimited access rights

se- System Engineer has access rights limited to access control and back up related pages

so- System Operator has the minimum access rights

When any of the system account user logs in for the first time, they need to enter just the Login ID and directly click on Login. The password setting page will appear from where password can be set.



Set the **New Password** for System Admin from the login page. You can enter the **security question** and its answer to retrieve the login account in future.

Click **Set**. Then Enter the **Login ID** as **User ID/Mobile Number/Email ID** to login into COSEC using the newly created password. You can login using OTP once Alert configurations are done.



By default the Login policy will be enabled for **Password or OTP**. So user can login using password or OTP. To enable 2 step verification; the option in login policy must be selected as **Password Then OTP**.

If you configure the Login policy as **Password or OTP** or **Password Then OTP**, make sure that you have linked an ESS user for the **SA** account. Refer **Admin Module > System Accounts > Optional > Linked ESS User**. For more details, refer **Linked ESS User** in **"Optional"**.

Refer **Maximum OTP Generation Attempts** in **"Password Policy"** for generation of OTP.



The valid characters for Login ID are **"A-Z a-z 0-9 @ _ \ : . / + -"**

You can view the password characters by clicking on **View Password**  button.

You can select **Remember Me** option which will remember the password during future login sessions.

You can click on **Forgot password** if you have forgotten your login password which will enable to get new password. "[Forgot Password](#)".

You must ensure that the Login ID being used has the respective correct icon. "[Icon of Login ID](#)".


Password or OTP

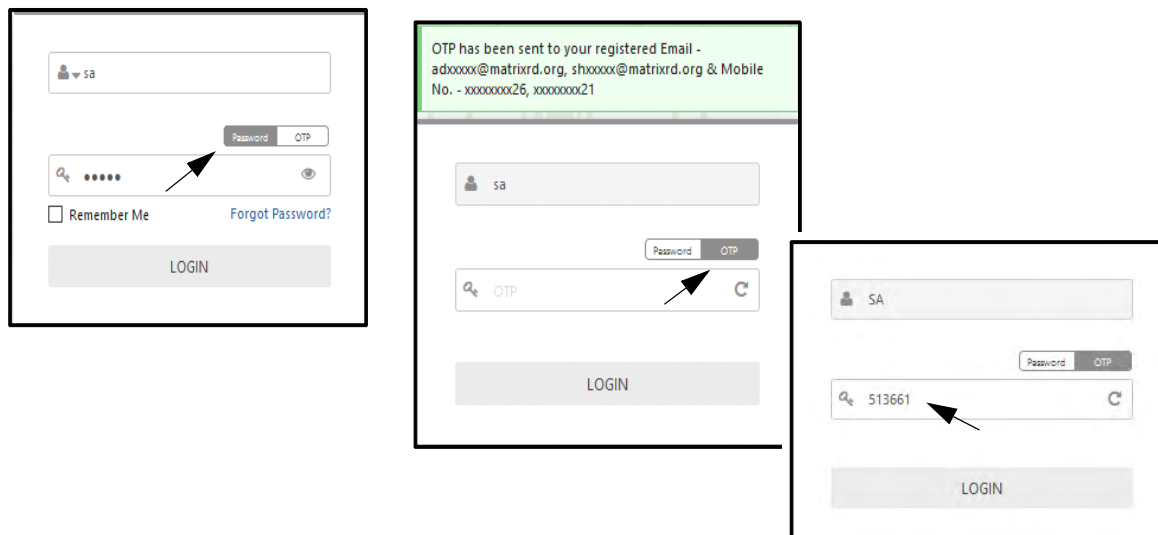
In this authentication mode, you can enter either Password of login ID or OTP for accessing the COSEC Web.

User ID with Password or OTP

Enter the **User ID** of login user. Then enter the password and click **Login** button to login into COSEC Web.

You can also login using OTP by clicking OTP button once Email/SMS configuration and OTP alert is configured. The OTP is sent to the contact details (Email ID and Mobile number as available in User Configuration) of login user. Enter the OTP and click **Login** button to login into COSEC Web.

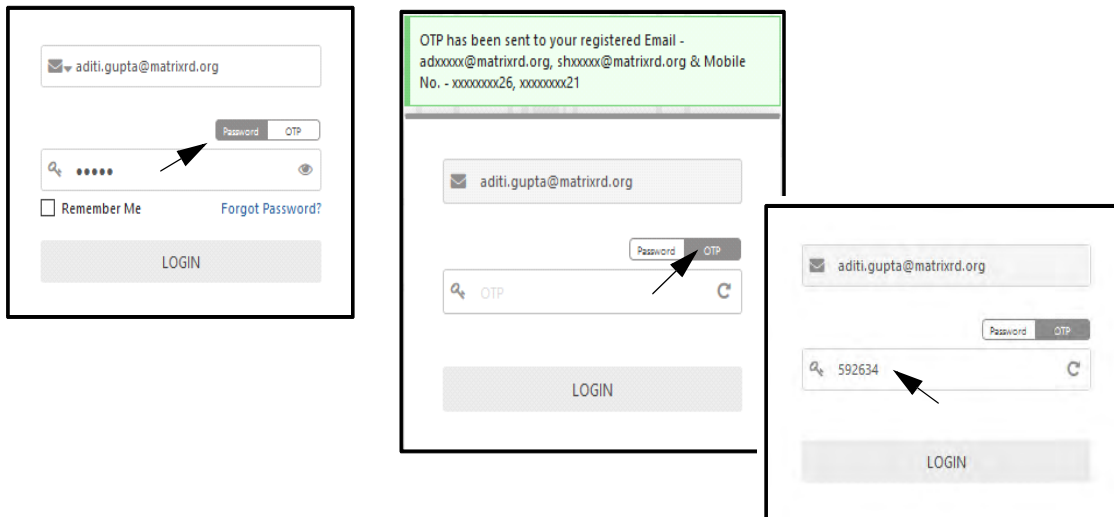
You can click on Resend OTP  button if OTP is to be sent again.



User entering Active Directory ID cannot login with OTP. They can log in with Password only.

Email ID with Password or OTP

Similar to User ID, you can login with your **Email ID**. Then enter the login password or OTP which is sent to the registered contact details. Then click Login to login into COSEC Web.




The login icon will be automatically changed when Email ID is entered.

The Email ID/Mobile No. must be available in the contact details of the System Account/ESS/CSS user.

For system account user; Email ID/Mobile No. of linked ESS user is considered. For eg: System Account user SA is linked to user Aditi having Email ID- aditi.gupta@matrixrd.org and Mobile number- 9667624826 So the user Aditi can login into COSEC using Email ID/Mobile number along with Password or OTP.

Using Password: Click on Password button. Enter the password in the field and click login.


Using OTP: Click on OTP button. The one time password will be sent to the registered Email ID/Mobile number. Enter that OTP in the field and click login. You can click on **Resend OTP** button  to send the OTP again.

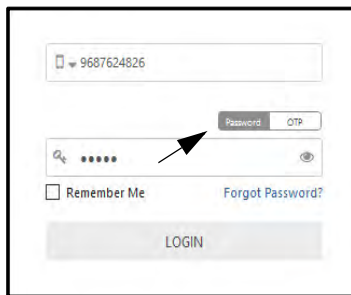
For sending OTP, "OTP Generated" Alert must be configured from Admin> System Configuration> Alert Message Configuration. Also Email/SMS Configuration must be done from Admin > System Configuration.

The screenshot shows the 'Alert Message Configuration' window. It has a title bar with standard window controls. Below the title bar, there are four fields: 'Alert Filter' with a dropdown menu set to 'System', 'Event' with a dropdown menu set to 'OTP Generated', 'Header Message' with the text 'Dear User,', and 'Footer Message' with the text 'From COSEC Software'. Below these fields is a section titled 'Additional Message Parameters' which contains two checkboxes: 'SMS' and 'Email', both of which are checked. At the bottom of the window is a 'Message Preview' section.

Mobile Number with Password or OTP

You can also login into COSEC using Mobile number similar to login using Email ID as described above. Enter the **Mobile number** of login user. Enter the Password or click OTP to get OTP number. Then enter OTP and click Login.

You can click on **Resend OTP** button  to send the OTP again.

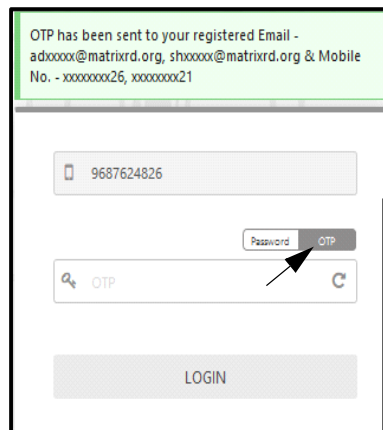


9687624826

Password OTP

Remember Me [Forgot Password?](#)

LOGIN

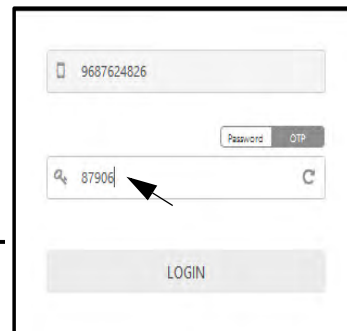


OTP has been sent to your registered Email -
adxxxxx@matrixrd.org, shxxxxx@matrixrd.org & Mobile
No. - xxxxxxxx26, xxxxxxxx21

9687624826

OTP

LOGIN



9687624826

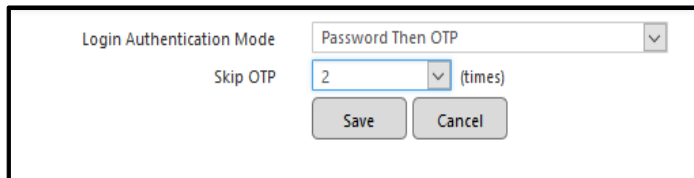
87906

LOGIN

Password Then OTP

If Login Authentication in Global Policy is set as Password Then OTP; then 2 step verification is enabled for login into COSEC. After entering the User ID/Mobile number/Email ID; you will have to enter the password and then OTP.

In case when you cannot enter the OTP in “Password Then OTP”; you can click on **SKIP OTP** which will skip the 2nd step of verification. The SKIP OTP can be done for the number of times defined in Global Policy.



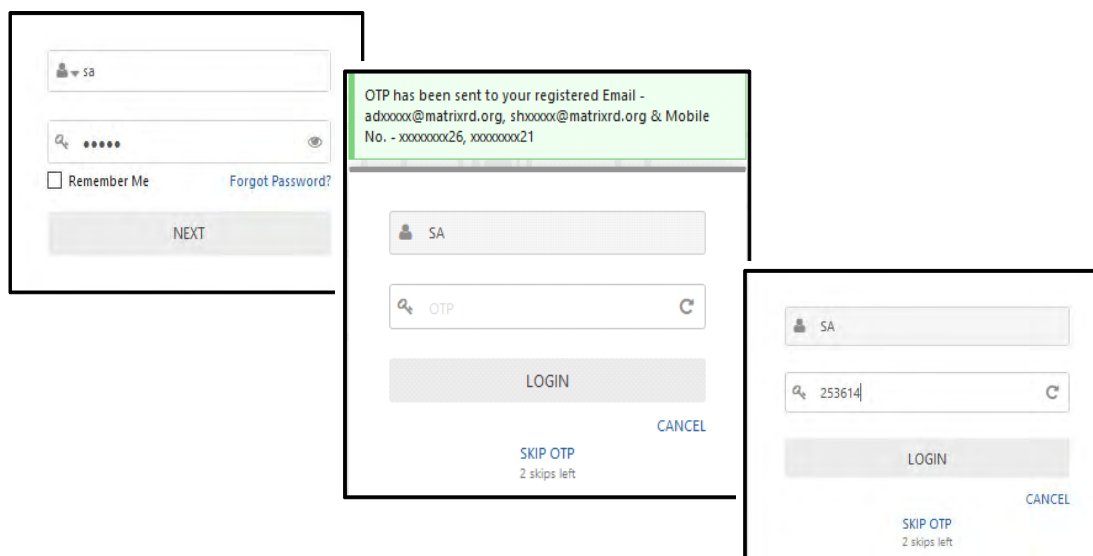
A configuration dialog box titled "Login Authentication Mode". It features a dropdown menu set to "Password Then OTP". Below this, there is a "Skip OTP" section with a numeric input field containing the value "2" and a "(times)" label. At the bottom of the dialog are two buttons: "Save" and "Cancel".

Eg: If Skip OTP is set as 2, the user can click on SKIP OTP for 2 times. When later if SKIP OTP in Global policy is changed to 5; then for 3 more times user can use SKIP OTP.

User ID with Password Then OTP

Enter the User ID of login user. Then enter the password and click **Next** button.

Now you will have to enter the OTP which is sent to the contact details of login user. After entering OTP click **Login** button to login into COSEC. If you click **Cancel** button; then it will go to the password page. You can also skip entering OTP by clicking on **SKIP OTP** link. This will directly login to COSEC Web without requiring OTP.



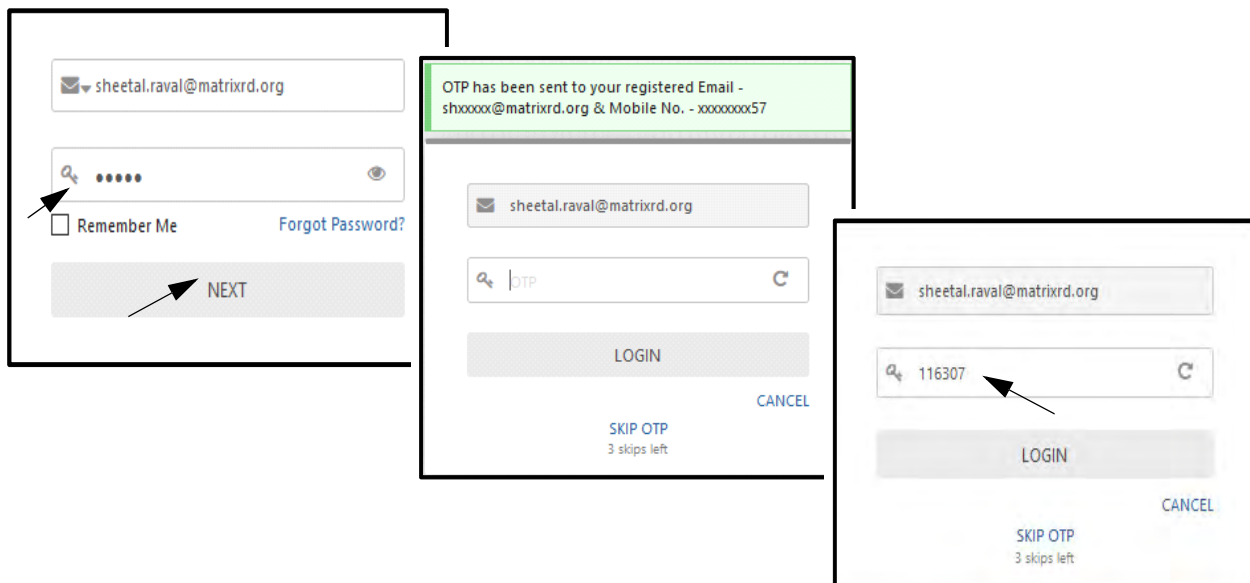
The image displays a sequence of three screenshots illustrating the login process:

- First Screenshot:** The initial login screen with fields for User ID (containing "SA") and Password (masked with dots). It includes a "Remember Me" checkbox, a "Forgot Password?" link, and a "NEXT" button.
- Second Screenshot:** A green notification banner at the top states: "OTP has been sent to your registered Email - adxxxxx@matrixrd.org, shxxxxx@matrixrd.org & Mobile No. - xxxxxxxx26, xxxxxxxx21". Below this, the screen shows the "SA" User ID, an "OTP" input field, a "LOGIN" button, a "CANCEL" button, and a "SKIP OTP 2 skips left" link.
- Third Screenshot:** The screen after the OTP is entered. The "OTP" field now contains the value "253614". The "LOGIN" button is highlighted, and the "SKIP OTP 2 skips left" link remains visible.

Email ID with Password Then OTP

Enter the **Email ID** of login user. Then enter the Password and click **Next** button.

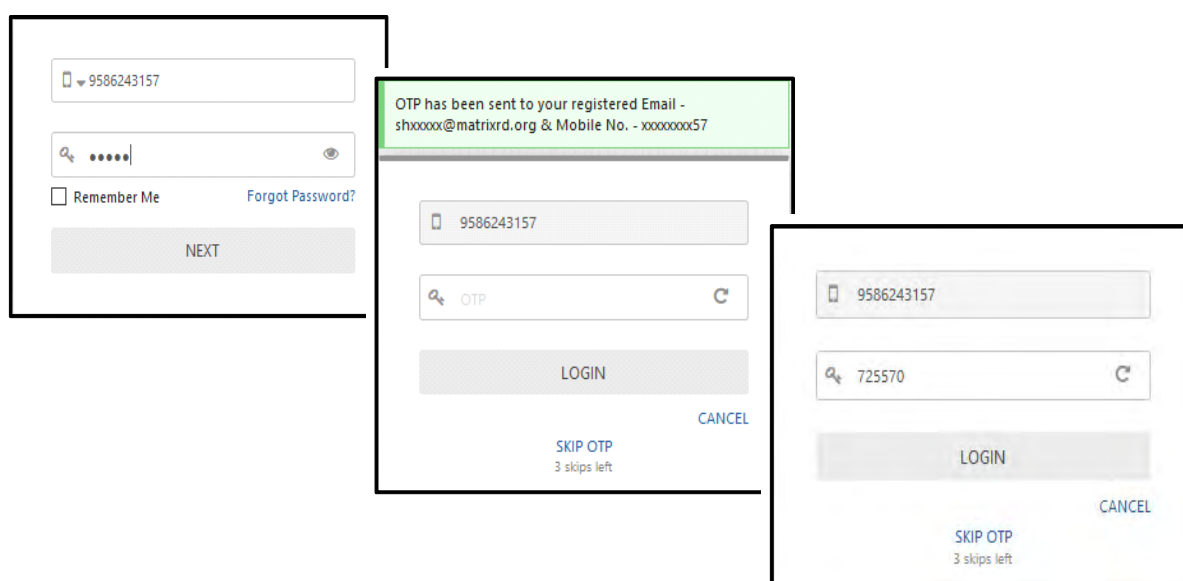
The OTP will be sent to the registered contact details. Then enter the OTP and click Login button to login to COSEC.



Mobile Number with Password Then OTP

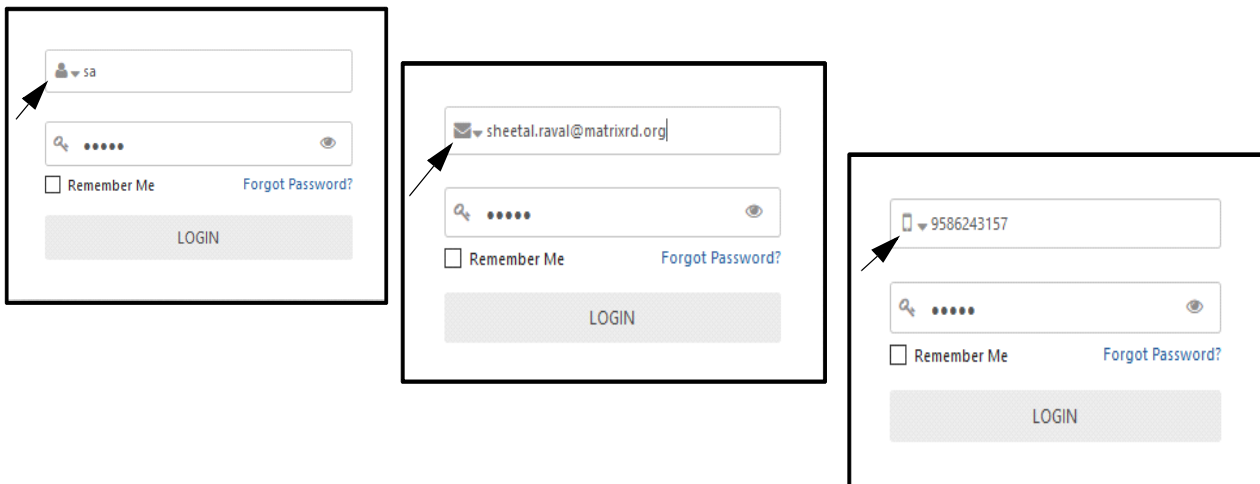
Enter the **Mobile number** of login user. Then enter the Password and click **Next** button.

The OTP will be sent to the registered Mobile Number/ Email ID. Then enter the OTP and click **Login** button to login to COSEC.



Password

You can select Login Authentication mode as "Password". This will require login ID with only password. Enter the login ID as User ID/ Email ID/ Mobile Number and the password. Then click Login to login into COSEC Web.

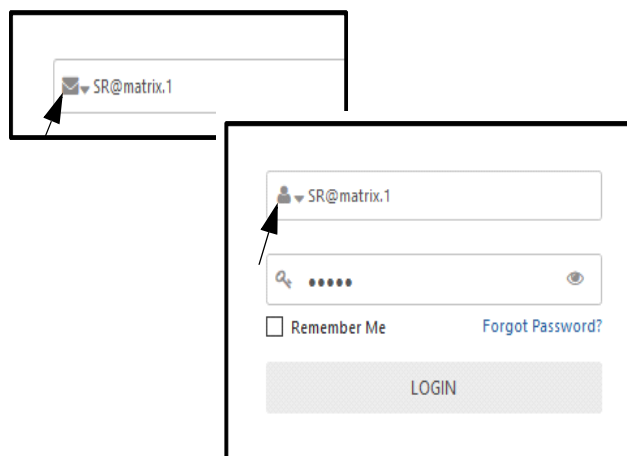


Icon of Login ID

Suppose you are logging into COSEC with your User ID which is similar to Email ID configuration.

eg: SR@matrix.1.

So the icon will automatically change to Email ID and it will try to login using Email ID. As there is no such Email ID; you will not be able to login. Hence you should manually click on the icon to change from Email ID to User ID.



Suppose you are logging into COSEC with your User ID which is of 10 characters eg: 8532621525 so as

there are 10 numeric characters; the icon will automatically change to Mobile number and it will try to login using Mobile number. As there is no such mobile number; you will not be able to login. Hence you should manually click on the icon to change from Mobile to User ID.



If the entered Mobile number/ Email ID is found for more than one user; then you will get the error "Unable to Identify the user. Please enter different Login ID". So Ensure that your Mobile Number/Email ID are entered correctly.

Link ESS User

For authentication mode equal to "Password Then OTP"; linked ESS user is mandatory. But when ESS user is not linked to System account user and system account user is trying to access COSEC then he will have to link the ESS user along with the contact details.

Enter the login ID and password. Click **Next** button.

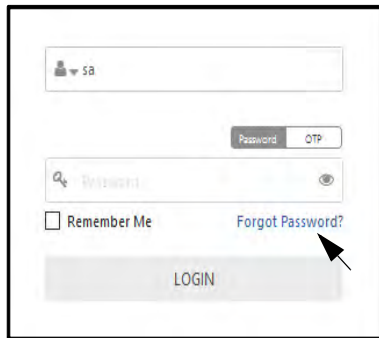
If ESS user is not linked, then **Link ESS ID** page will appear. Enter the **ESS User ID** who is to be linked. Then click on arrow; the name of the user will appear. Then click Next. The Contact details page will appear.

If ESS user is linked but contact details are not available, then directly Contact details page will appear where Email ID and Mobile number can be entered.

Enter the **Email ID** or **Mobile number** of the ESS user which will be stored as Official Email ID and Official Mobile number respectively. Then click **Get OTP**. The OTP will be sent to the registered contact details. Noe Enter that OTP and click **Login** button to login into COSEC Web.

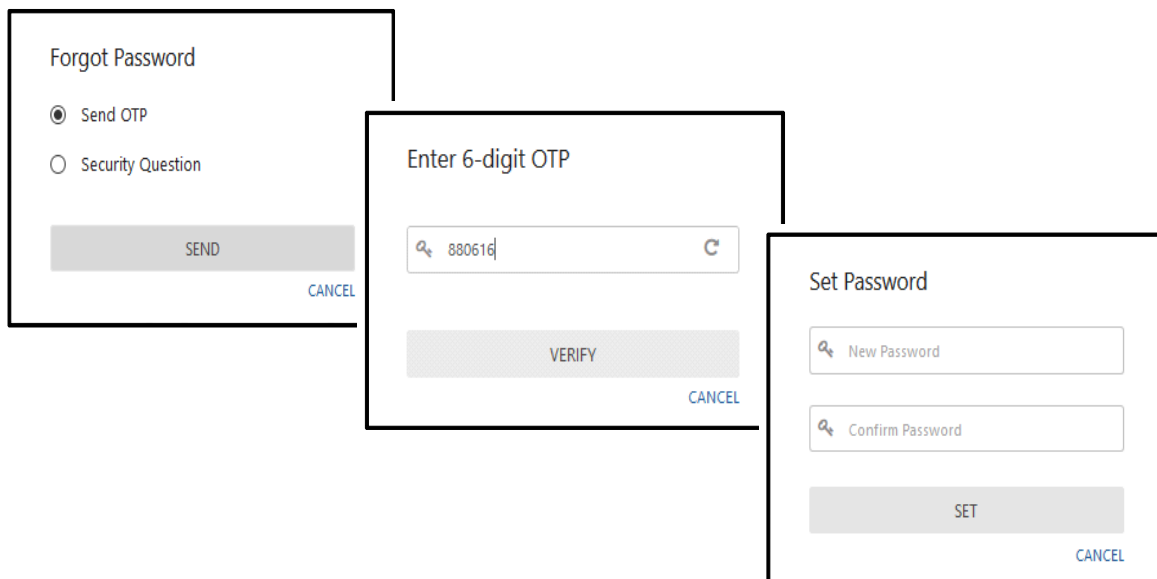
Forgot Password

Click on the Forgot password link from the login page to get a new password for your login ID. The password reset will be allowed if contact details of user, OTP generation alert, SMS Configuration, Email Configuration are available in the system.

A screenshot of the login interface. At the top, there's a field for 'sa' with a dropdown arrow. Below it are two tabs: 'Password' and 'OTP'. A password input field is shown with a toggle for visibility. Below the password field is a 'Remember Me' checkbox and a blue link labeled 'Forgot Password?'. An arrow points to this link. At the bottom is a 'LOGIN' button.

For “sa” login you can select Send OTP or Security Question. The **Send OTP** option will send an OTP to the registered contact detail. By entering this OTP you can set a new password.

Send OTP

A sequence of three screenshots illustrating the 'Send OTP' password reset process. The first screenshot, titled 'Forgot Password', shows two radio button options: 'Send OTP' (selected) and 'Security Question'. It includes a 'SEND' button and a 'CANCEL' link. The second screenshot, titled 'Enter 6-digit OTP', shows a text input field containing '880616', a 'VERIFY' button, and a 'CANCEL' link. The third screenshot, titled 'Set Password', shows two text input fields for 'New Password' and 'Confirm Password', a 'SET' button, and a 'CANCEL' link.

You can select **Security Question** which will ask you the question as entered during the first login. By entering the answer of the security question, you can set a new password.

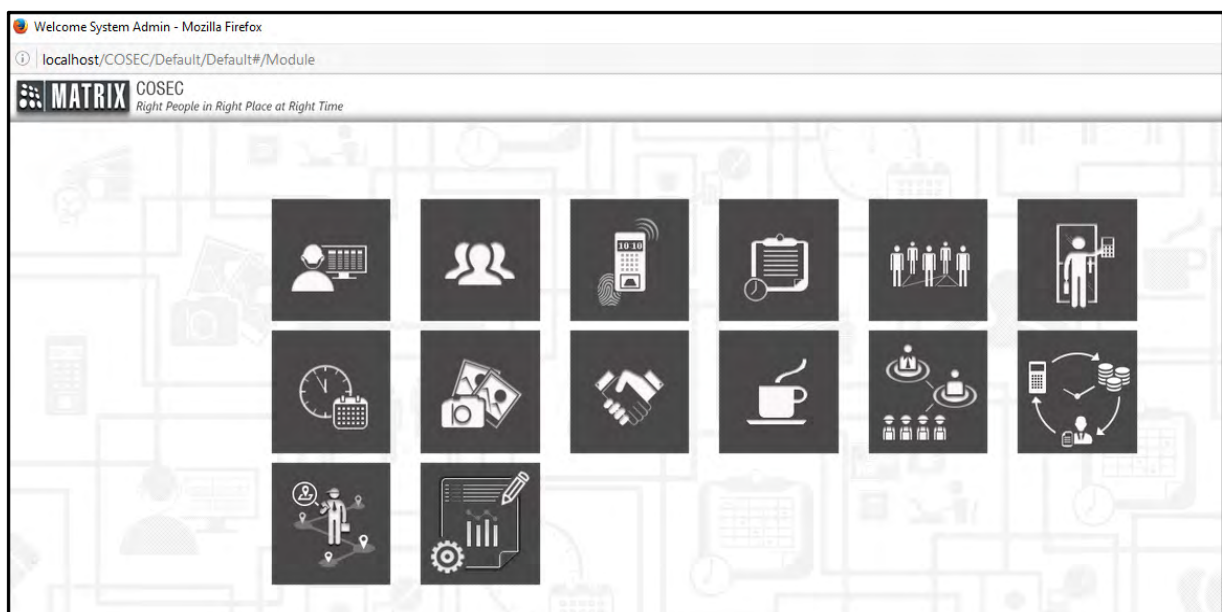
Security Question

The first screenshot, titled 'Forgot Password', shows two radio buttons: 'Send OTP' (unselected) and 'Security Question' (selected). Below them are 'NEXT' and 'CANCEL' buttons. The second screenshot, titled 'Security Question', asks 'fav actor?' with a text input field containing 'A. Hrithik' and 'NEXT'/'CANCEL' buttons. The third screenshot, titled 'Set Password', has two password input fields labeled 'New Password' and 'Confirm Password', followed by 'SET' and 'CANCEL' buttons.

For system account users other than “sa” or ESS/ CSS users, when Forgot password link is clicked then Forgot Password screen will appear as shown below. Clicking on **Send** will send an OTP to the registered contact detail. By entering this OTP you can set a new password.

The first screenshot shows a login form with fields for 'se' (username) and a toggle for 'Password' or 'OTP'. It includes a 'Remember Me' checkbox, a 'Forgot Password?' link (indicated by an arrow), and a 'LOGIN' button. The second screenshot, titled 'Forgot Password', states 'A 6-digit OTP will be sent to your registered Email Id.' and features a 'SEND' button and a 'CANCEL' link.

Now Login with UserID/Email ID/Mobile number with Password/OTP. Then click **Login** button. The home page of COSEC will open as shown below.





The administrator needs to ensure that the COSEC USB dongle key has been inserted in the USB port of the application server prior to the launching of the COSEC application.



The COSEC Database can be upgraded from the Admin Management Portal Utility. For details see the Admin Portal Manual.

The home page consists of the list of modules which are available as per the license. The user can now select the appropriate module and configure the parameters as per the site requirements.

Now user can start the online **COSEC Monitor** and Control application. The COSEC Monitor Utility connects with the Panel lite and Doors on the TCP port. This enables the COSEC application to connect to the COSEC controllers and upload and download configuration changes.

COSEC Monitor Service must be running to add devices to COSEC Web application. For more information on COSEC Monitor, [“Starting Monitor Service & Utility”](#)

Starting Monitor Service & Utility

The COSEC Monitor application consists of two components:

- Monitor Service
- Monitor Utility

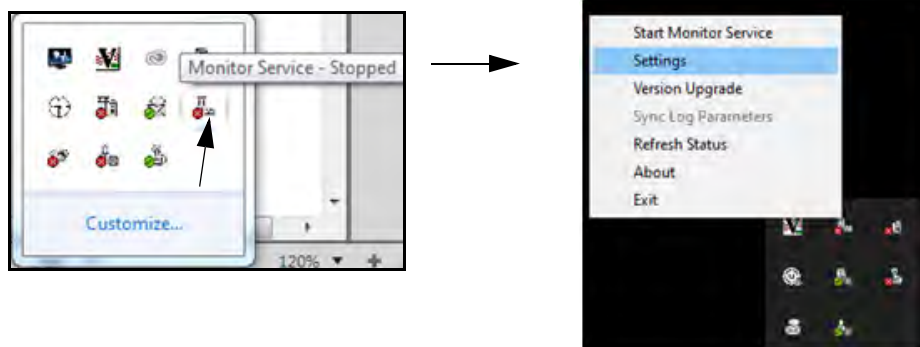
Monitor Service

For COSEC Centra, Monitor Service has to be started for using the Monitor Utility. For COSEC VYOM, Monitor Service will be running at Cloud so user can access the Monitor Utility directly.

The **Monitor Service** connects with the configured COSEC devices. This service starts up each time the computer is restarted.

After the Installation of COSEC Centra (Premise based setup), you can start the COSEC Monitor Service by browsing the folder from *C:\Program Files (x86)\Matrix\COSEC Monitor Service*.

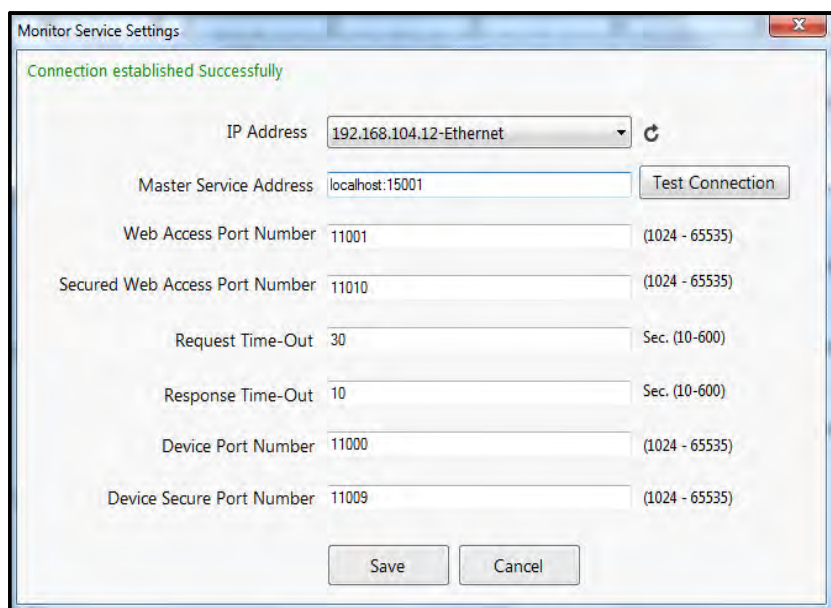
When the Monitor Service is started, an icon will be visible in the system tray as shown below. Then Right click on icon to configure the settings and start the service.



On the **Monitor Service Settings** window select the **IP Address** of the PC where Monitor service is to be started. Enter the **Master Service Address** as the URL of the system where Master service is running.



1. Refer Monitor Service in ServiceUserGuide for details.
2. Monitor Service will be active and running only if Master service is running.

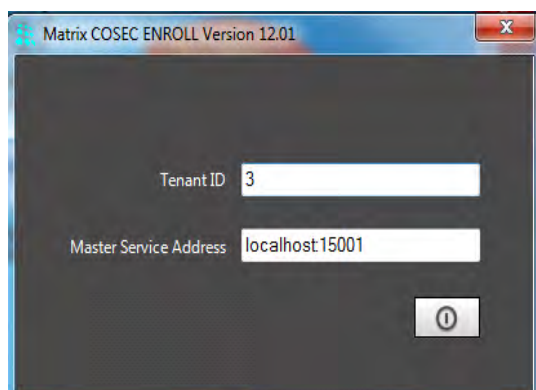


Monitor Utility

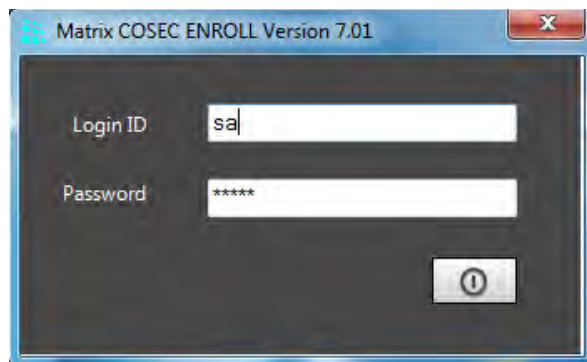
The Monitor application is used to send commands to the COSEC devices as well as monitor and control the device and user events.

Once the Monitor Service is running, the COSEC Monitor Utility can be accessed through the COSEC Monitor icon

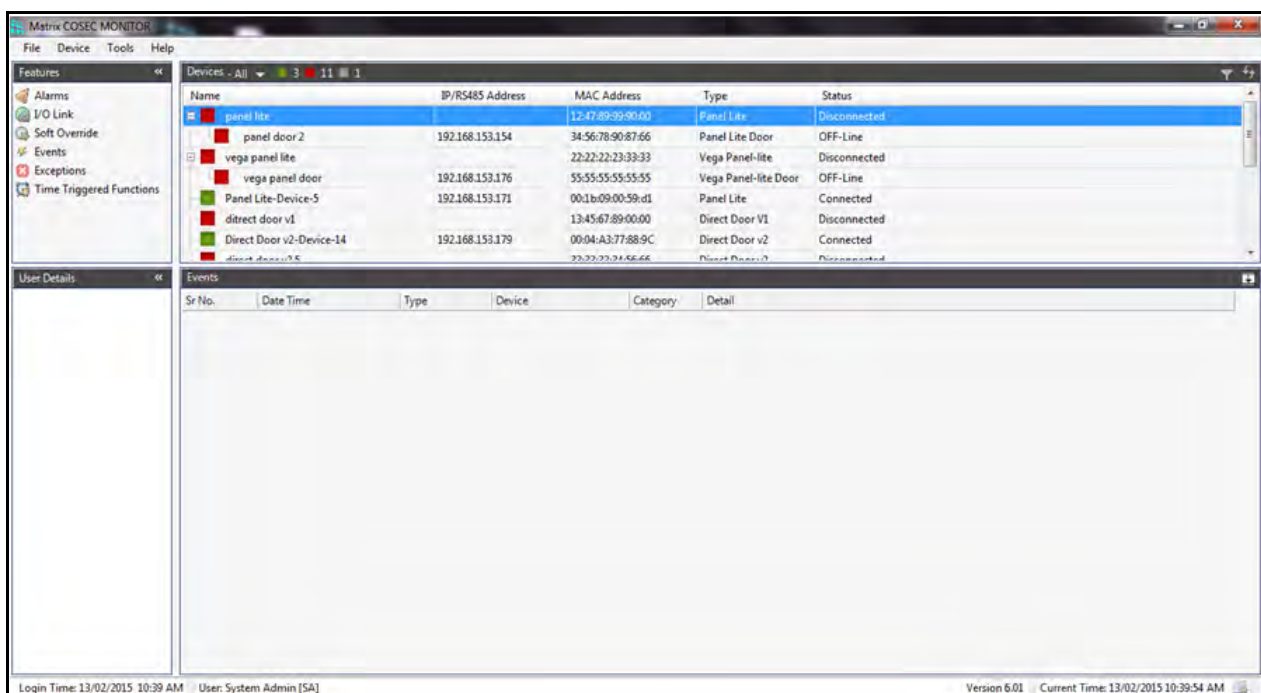
on the desktop.



For COSEC VYOM, Enter the **Tenant ID** and **Master Service Address** as shown above. Both the parameters are available in Tenant activation Email sent to the Tenant by the Tenant administrator.



Then enter the **Login ID** and **Password** as set in the web application module. For COSEC Centra directly login ID and password has to be entered. The COSEC Monitor window appears as shown.



Accessing Social Security Dongle in COSEC CENTRA

In COSEC CENTRA, License dongle is required for accessing the COSEC application.

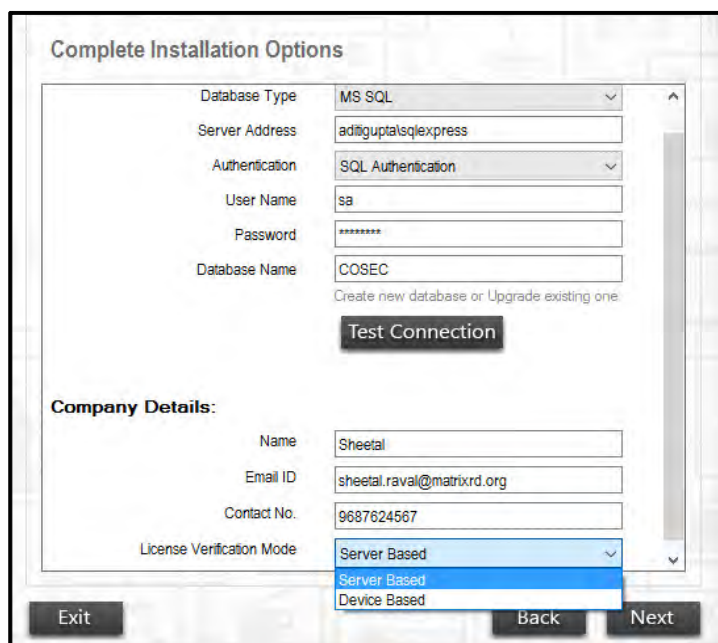
If the License verification from the dongle is not done, then the application will show license verification failed as shown below:



The license dongle verification can be done by following 2 modes:

- **Server based:** License will be verified from the dongle connected to the PC where Master service is installed.
- **Device based:** License will be verified from the dongle connected to the COSEC device. This device will communicate with Master Service so that Master Service can fetch the license key from the dongle and all of the COSEC services will function.

The mode of license verification can be selected while installing the COSEC setup.



Only Vega direct door and Panel200 in server mode can be used for Device based license verification. You must ensure that Vega and Panel200 is in CENTRA connection mode.

Once dongle is connected to the device (Vega or Panel200); enter the License Server URL (Default is 192.168.50.100) and License server Port (Default is 15025) in Server Settings from device or its webpage.

The screenshot shows the 'MATRIX VEGA Door' web interface. The left sidebar contains a 'Settings' menu with options: Basic Profile, LAN Settings, Wi-Fi Settings, Mobile Broadband Settings, Bluetooth Settings, **Server Settings**, CCC Settings, Identification Server Settings, Date-Time Settings, Cafeteria Settings, Multi Language Support, Manage, and View. The main content area is titled 'Server Settings - COSEC CENTRA'. It includes a note: 'This will be used to communicate with Monitor Service'. Under 'Connectivity Status', it shows 'via Ethernet' with a green dot. The 'Encryption (SSL)' section has an unchecked checkbox. The 'Configuration' section has 'Basic' selected. The 'URL' field is set to '192.168.104.13' and the port is '11000'. The 'License Server' section shows 'Connectivity Status' as 'Disconnected' with a red dot, and 'License Dongle' as 'Unavailable' with a red dot. The 'URL' field is '192.168.50.100' and the port is '15025'. The 'Web Server' section has an unchecked 'Encryption (HTTP)' checkbox, 'Ethernet' selected for 'Network Interface', 'URL' set to '192.168.104.13' with port '80', and 'Directory Name' set to 'cosec'.

You can use COSEC Utilities in different computer by accessing Master service from the PC where license dongle is connected.


Suppose Master Service and License dongle are connected in PC (192.168.104.12) and COSEC Integrate is installed in PC(192.168.104.24). Then start the COSEC Integrate application in PC(192.168.104.24) and enter the Master Service Address as the URL of the PC where Master service is running.

The screenshot shows the 'COSEC Integrate Version 13.01' application window. It has a blue title bar with a close button. The main area has a label 'Master Service Address' followed by a text input field containing '192.168.104.12:15001'. Below the input field is a dark grey button labeled 'Next'.

The Master Service settings in PC are as below. If the IP address and Port are changed in Settings; then the URL also must be changed.

Master Service Settings

DB Settings

IP Address 192.168.104.12-Ethernet 

Database Type MS SQL

Authentication SQL Authentication

Server Address sheetalraval\sqlexpress

Database Name AdminPortalDB1

Username sa

Password Test Connection

Connection Timeout 30 sec. (15-600)

Command Timeout 1200 sec. (30-1800)

General Settings

Port Number 15001 (1024-65535)

Secure Port Number 15010 (1024-65535)

Request Time-Out 30 sec. (10-600)

Response Time-Out 10 sec. (10-600)

Device Port Number 15005 (1024-65535)

Device Secure Port Number 15025 (1024-65535)

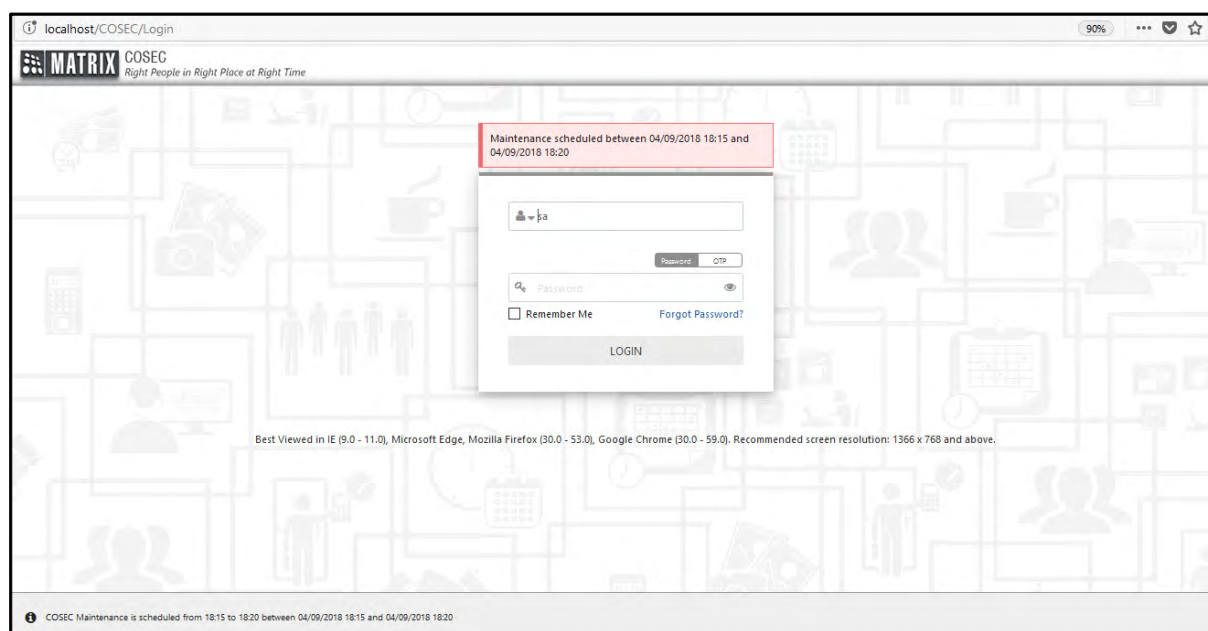
Save Cancel

Maintenance Scheduling

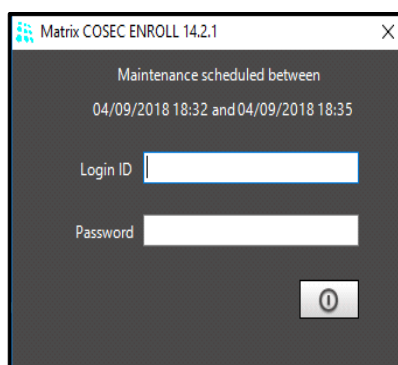
The COSEC system requires maintenance time for upgrading the version. During this time the user cannot access COSEC application. So the admin can configure the Maintenance duration in advance from the COSEC Admin Portal which will be displayed on the login page of COSEC Web, COSEC Enroll Utility and COSEC VMS Utility.

To configure the maintenance information go to the System Configuration> Maintenance Configuration of the Admin Portal.

When the user tries to login into COSEC Web within the maintenance duration then he will not be allowed to access: the application.



The Maintenance duration can also be reset from the Admin Portal if the maintenance gets completed before the scheduled time.



COSEC VMS

Maintenance scheduled between
04/09/2018 18:32 - 04/09/2018 18:35

Login ID

Password

Login

Getting Started With COSEC Devices

The Matrix COSEC Application is truly scalable, allowing a customer to start with smaller configuration and expand step-by-step as the organisation grows. One PANEL(Site Controller) can control from 1 to 255 Door Controllers. An Enterprise can deploy up to 1000 such PANELs and 10000 Door Controllers, managing over 1 million users.

The COSEC Panel is designed to operate off-line, making access control decisions independently from a PC or other controlling device. It can also be connected to a host computer for system configuration, alarm monitoring and direct control. Connectivity to the host computer is accomplished via TCP/IP network connection. Another key feature of the Matrix COSEC Panel is its completely distributed database. All information regarding cards, time zones, relay control and alarm points are loaded into its memory, enabling the unit to operate independently of any other equipment.

The **COSEC PANEL/PANEL LITE** and its variant is designed to support following major features.

- PANEL is a stand alone unit with multiple PANEL Door that work as slave controllers.
- Finger Print templates storage on PANEL for easy replacement of door controllers.
- PANEL communicates with RS-485 and Ethernet interface with PANEL Doors simultaneously.
- PANEL Doors IP address assignment and configuration through PANEL.
- Automatic Door firmware upgrade from PANEL.
- Automatic verification of Doors' firmware at start-up.
- “[Degraded Mode](#)” support on PANEL Doors for Exit by default and for Entry through configuration selection.
- Network clock synchronization of all PANEL Doors with PANEL.



Specification	COSEC PANEL/ PANEL LITE
Total Door Controllers supported	255
Door Controllers supported on Ethernet	255
Door Controllers supported on RS 485	32
User database support	25,000 users per Panel/Panel lite
No. of Events that can be stored in the memory	5,00,000 Events

The **COSEC DOOR** is designed to support following major features.

- The COSEC Door can be configured as a PANEL Door or DIRECT Door.
- COSEC doors support a 128 x 64 pixel LCD display as well as a 16 key cap sense type keypad. However, the Panel doors are available in variants without the LCD display and Keypad (Standard Panel Door).
- Panel Doors depend on the PANEL for configuration while DIRECT Doors are configured directly from the COSEC application platform.
- DIRECT DOORS have limited functionality as compared to the PANEL DOORS



The basic configuration of COSEC Doors is given in following topics links.

[“Degraded Mode”](#)

[“Connecting the COSEC RF Module”](#)

[“Connecting the Door Locking Device”](#)

[“External Reader Wiring”](#)

[“Powering the COSEC DOOR”](#)

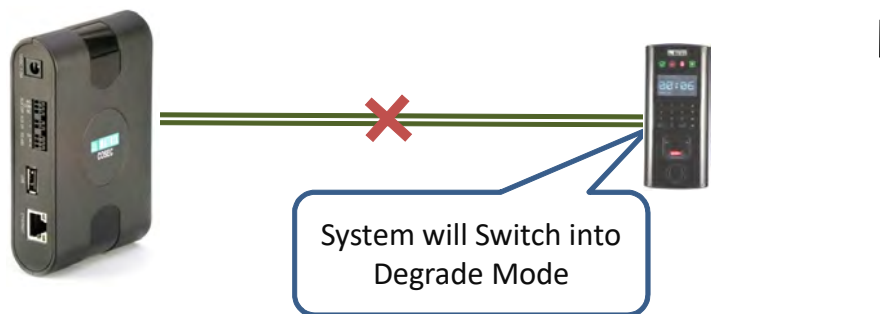
[“Setting the IP Address of the Direct DOOR”](#)

[“Default Initialization of the DOOR”](#)

[“Connection Diagram for the COSEC DOOR”](#)

[“Connection Diagram for COSEC PANEL DOOR \(Standard\)”](#)

Degraded Mode



The Degraded mode of PANEL DOOR can be defined as a mode of operation, where the DOOR starts working in standalone mode.

This mode will allow users to have access to controlled area by providing their credentials. However the user access rights are not verified while allowing the access to these areas and hence it is known as Degraded Mode.

In degraded mode, the PANEL DOOR performs the following functions.

1. Read the user credentials through any of its reader ports. If required communicate with user for further inputs (Card with FP stored on card for 1:1 match)
2. Identify the user based on credentials provided by user.
3. If request is for exit, allows user without any validation.
4. If request is for entry, then identify the user as a valid user for the facility.
 - In case of Proximity cards with FC, user is identified as collective users allowed.
 - In case of smart cards/FP templates, the user is identified with user ID, FC, ASC and hence the user is individually validated with enhanced security.
5. Store all events in non-volatile memory and send it to COSEC PANEL on restoration of network.
6. Monitor the door sense and activate the Door Relay according to degraded mode settings received.



The degraded mode has to be enabled at the PANEL (Advance Parameters) as well as the Access Zone level for the PANEL DOOR to be able to operate in this mode.

Connecting the COSEC RF Module

The COSEC DOOR enclosure has a connector for connecting the COSEC RF module. This female connector is located on the rear of the enclosure. The RF module has a corresponding male connector as shown. Place the RF module in the slot provided on the back of the door enclosure and apply a gentle pressure on the module and ensure that it is set properly in the slot.

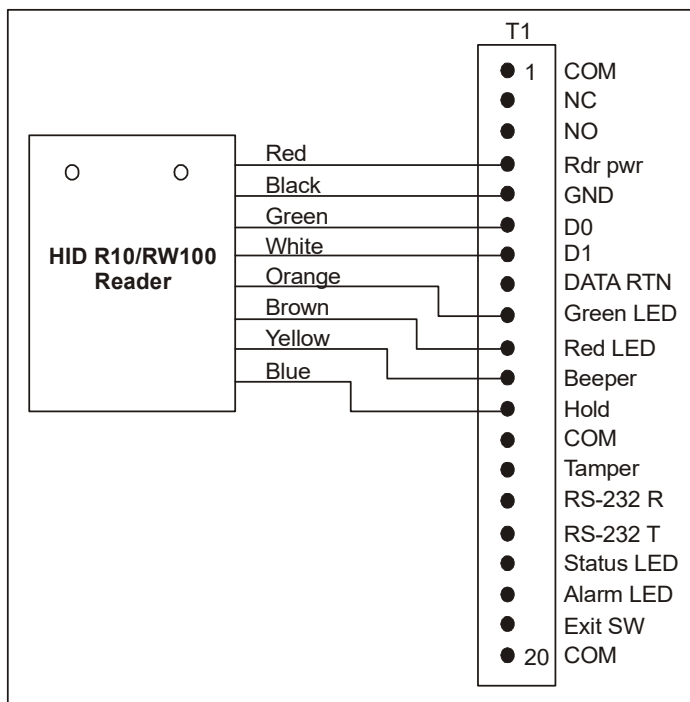
Terminal no.	Wire Color	Connects to Door Terminals
C5-1	Blue	COM
C5-2	Yellow	NC
C5-3	Orange	NO
C5-4	Red	Power Out +
C5-5	Black	Power Out -
C5-6	Black	Power Out -
C5-7	Brown	Lock Tamper IN+
C5-8	Black	COM
C5-9	White	Door Status IN+
C5-10	Black	COM

External Reader Wiring

The COSEC DOOR supports a maximum of 3 readers (2 internal and one External). The External reader port supports a single reader with Wiegand / Serial interface. To fully utilize Wiegand reader port, a shielded 13-conductor cable (18-22 AWG) is required. The maximum recommended length of wiring is 500 feet per reader. The COSEC system offers the following external reader options:

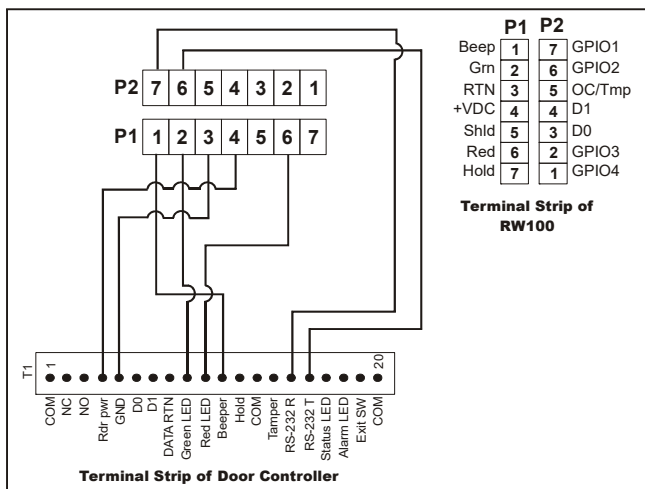
- HID Prox Reader R10 (Wiegand)
- HID Prox Reader RW10 (Wiegand / serial)
- COSEC Reader RFR (Serial)
- COSEC Reader FPR (Serial)

Connecting the Wiegand HID R10 / RW100 Prox Reader: The HID R10 and RW100 readers come with the Pigtail option which has color coded conductors as specified in the following connection diagram:

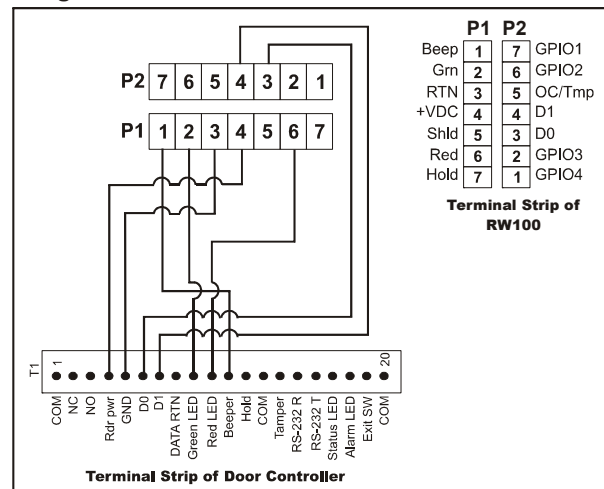


In the absence of the pigtail option on the RW100 reader the following are the connection diagrams for the serial and the Wiegand readers.

Serial Reader



Wiegand Reader



Connecting the red wire lead (or power lead) of a 5 VDC reader to the 12 VDC terminal may damage the reader. Refer the reader installation procedure for proper power connection.



For further connection details on External Readers, Refer COSEC DOOR Quick Start.

Powering the COSEC DOOR

The COSEC DOOR can be powered using any one of the following three options:

- Connect the adapter giving an output of 12VDC @ 1A-1.5A to the terminals 39 and 40 on the COSEC DOOR Controller Unit.
- A 2 conductor cable can be drawn from the terminals on the power supply unit and can be connected to the terminals 39 and 40 of the DOOR terminal strip.
- Connect the two cables coming from the Matrix PSBB - Universal Mains Power supply(13.8 VDC @ 2A) with Battery Backup to the terminals 39 and 40 of the DOOR controller.

On powering up the COSEC DOOR it goes through the power on sequence and displays the booting message along with the following information:

- Matrix Logo
- Firmware Version
- RS-485 address as set on the DIP switch of the DOOR
- Mac address of the DOOR (Note the address to be used in COSEC application)
- Hardware Version of the DOOR

Setting the IP Address of the Direct DOOR

There are two ways to configure the IP Settings of the Direct DOOR:

From the Direct DOOR Display

After powering up the Direct DOOR, the user need to navigate to the Admin option using the keypad and display. Navigate to Admin > LAN Settings > IP. Change the IP by pressing 1 on keypad and enter the new IP.

From the Direct DOOR Web Page

Type `http://192.168.50.50` in the Address field of internet browser. Enter admin as default user and password to login to the COSEC DOOR Web page. Navigate to Network Configuration and change the IP settings.

Default Initialization of the DOOR

The COSEC DIRECT DOOR configuration comes with three DIP switches on the rear of the DIRECT DOOR as shown which can be used to initialize the **IP settings**, **Password** and **System Parameters** of the DIRECT DOOR to factory defaults.



The DOOR reconfigures its network settings to the factory defaults whenever the DIP Switch number 1 is set to the ON position and the DIRECT DOOR is powered up again.

Use the Network Defaults DIP switch (1) to correct potential errors in a DIRECT DOOR's network configuration. In order to reset the IP address of the DIRECT DOOR to default settings:

- Power down the DOOR.
- Set the DIP Switch no. 1 to ON position.
- Power up the DOOR.
- The DOOR goes through the IP default process and indicates on the display that the IP has been defaulted.

The IP address settings of the DOOR are now set back to default as follows:

DOOR IP address: **192.168.50.50**

Subnet Mask: **255.255.255.0**

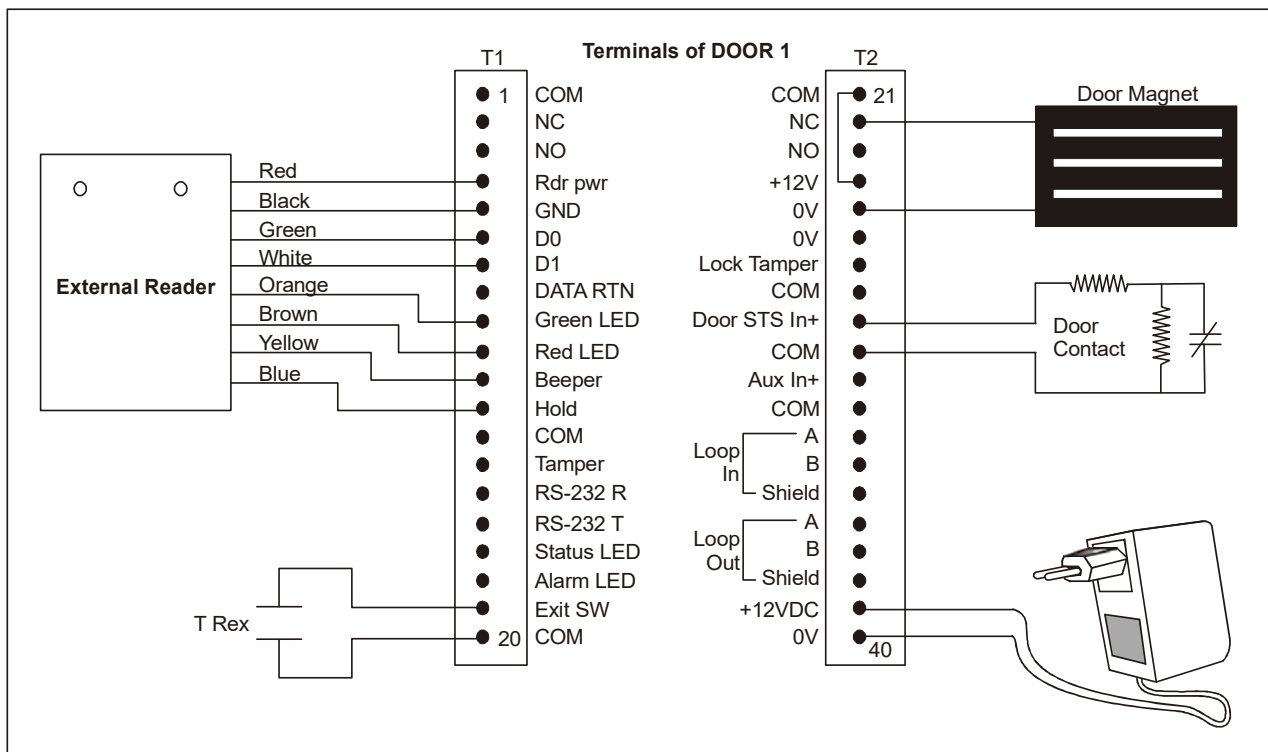
Push the DIP switch 1 back to Off position to ensure that the IP does not go back to default again the next time you power up the DOOR.

Similarly, DIP Switch no. 2 and 3 are used for resetting the Password and the system parameters respectively by following the same procedure as enumerated above.

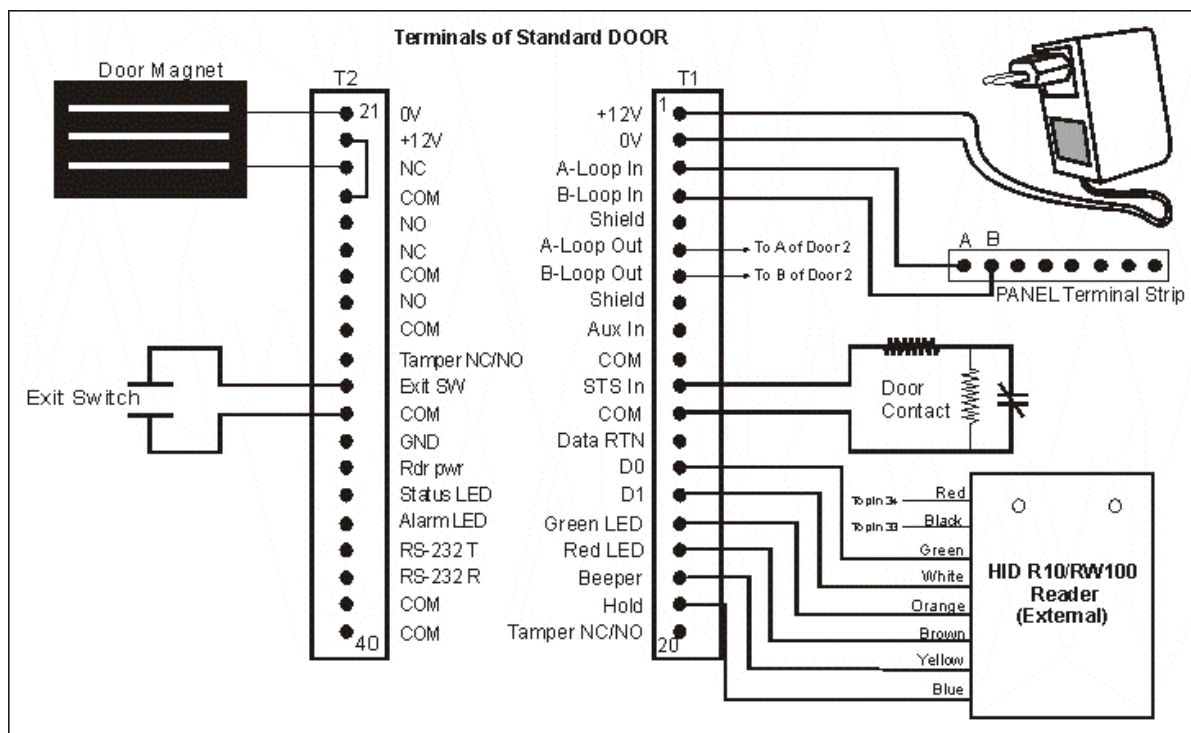


Please use the System default setting only in exceptional cases as it will erase all configuration and event data from the DOOR.

Connection Diagram for the COSEC DOOR



Connection Diagram for COSEC PANEL DOOR (Standard)



Color code mapping for the Wire-to-Board Connectors of Wireless and PVR DOOR

Terminal C2 (External Reader)

Terminal no.	Wire Color	Connects to
C2-1	Violet	Alarm LED
C2-2	Light Brown	Status LED
C2-3	Grey	RS232 Tx
C2-4	Pink	RS232 Rx
C2-5	Light Blue	Tamper
C2-6	White Red	COM
C2-7	Blue	Hold
C2-8	Yellow	Beeper
C2-9	Brown	Red LED
C2-10	Orange	Green LED
C2-11	White Blue	DATA RTN
C2-12	White	Wiegand Data1
C2-13	Green	Wiegand Data0
C2-14	Black	Ground
C2-15	Red	Reader Power

Terminal C3 (Exit Switch)

Terminal no.	Wire Color	Connects to
C3-1	White	Exit Switch IN+
C3-2	Black	COM

Terminal C4 (AUX I/O)

Terminal no.	Wire Color	Connects to
C4-1	Brown	AUX Relay COM
C4-2	Blue	AUX Relay NC
C4-3	Yellow	AUX Relay NO
C4-4	NA	Unused
C4-5	White	AUX IN+
C4-6	Black	COM

Terminal C5 (Door Lock Connectors)

Terminal no.	Wire Color	Connects to
C5-1	Blue	COM
C5-2	Yellow	NC
C5-3	Orange	NO

Terminal no.	Wire Color	Connects to
C5-4	Red	Power Out +
C5-5	Black	Power Out -
C5-6	Black	Power Out -
C5-7	Brown	Lock Tamper IN+
C5-8	Black	COM
C5-9	White	Door Status IN+
C5-10	Black	COM

Device Features

Features and functionality supported by the different COSEC doors and panels are listed in the table below:
The * marked features have given disclaimers at the bottom of table.

Sr. No	Feature Name / Product	Direct Doors									Panel/ Panel-Lite	Vega Panel-Lite (Panel2 00)	Panel Door
		Door V1	Door V2	V2 e-Cante en	NGT	Wireless Door/ Door V3/ Door V4	PVR Door	Vega Door	FMX Door	ARGO Door			
1	2-Person Rule	x	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	Absentee Rule	x	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	Access Group	x	x	x	x	x	x	x	x	x	✓	✓	✓
4	Access Level*	x	x	x	x	x	x	x	x	x	✓	✓	✓
5	Access Modes*	✓	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
6	Access Policies*	✓	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	Access Request Response (ARR)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
8	Access Route	x	x	x	x	x	x	x	x	x	✓	✓	✓
9	Access Zone	x	x	x	x	x	x	x	x	x	✓	✓	✓
10	Additional Security Code	✓	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
11	Anti Pass Back	x	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
12	Auto Alarm Acknowledge	x	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
13	Auto Relock	✓	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
14	Aux IN	✓	✓	✓	✓	✓	✓	✓	✓	x	✓	✓	✓
15	Backup and Update	x	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
16	Blocked User	x	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
17	Buzzer Mute	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
18	Communication with ACMS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	x
19	CDC Exit Reader Support	x	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
20	Daylight Saving Time	x	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
21	Date and Time	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
22	Dead Man Zone	x	x	x	x	x	x	x	x	x	✓	✓	✓

Sr. No	Feature Name / Product	Direct Doors									Panel/ Panel-Lite	Vega Panel-Lite (Panel2 00)	Panel Door
		Door V1	Door V2	V2 e-Canteen	NGT	Wireless Door/ Door V3/ Door V4	PVR Door	Vega Door	FMX Door	ARGO Door			
23	Default Configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
24	Degraded Mode*	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓
25	DND Zone	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓
26	Door Alarm Configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
27	Door Controller Configurations	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
28	Door Monitoring and Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
29	Duress Detection	✗	✓	✗	✗	✓	✓	✗	✗	✗	✓	✓	✓
30	HVR / NVR Integration	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
31	Cafeteria*	✗	N.A	N.A	✓	✓	✗	✓	✓	✓	✗	✗	✗
32	Enrollment	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
33	Event Configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
34	Facility Code	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓
35	First IN User Rule	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
36	Functional Groups	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓
37	Function Key	✗	✓	✗	✗	✓	✓	✗	✗	✗	✓	✓	✓
38	Display Greeting Message	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
39	Greetings (NGT) (Image+ Audio)	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
40	Guard Tour	✗	✗	✗	✓	✗	✗	✗	✓	✗	✓	✓	✗
41	Holiday Schedule	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
42	Input /Output Ports & Linking	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
43	Inter Digit Wait Timer (IDWT)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
44	Login Access Privileges	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
45	Mantrap	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓

Sr. No	Feature Name / Product	Direct Doors									Panel/ Panel-Lite	Vega Panel-Lite (Panel200)	Panel Door
		Door V1	Door V2	V2 e-Canteen	NGT	Wireless Door/ Door V3/ Door V4	PVR Door	Vega Door	FMX Door	ARGO Door			
46	Master Slave	x	x	x	✓	x	x	x	x	x	✓	✓	✓
47	Menu	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
48	Mobile Broadband	x	x	x	✓	✓	✓	✓	✓	✓	✓	✓	x
49	Network Settings	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
50	Network Interface Priority	x	x	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
51	Occupancy Control	x	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
52	Palm Predictive Algorithm (per user per template)	x	x	x	x	x	✓	x	x	x	x	x	x
53	Panel Route Access	x	x	x	x	x	x	x	x	x	✓	✓	✓
54	Password*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
55	Password Change from monitor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
56	Request To Exit	✓	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
57	RS-485 Assignment (manual)	✓	x	✓	x	x	x	x	x	x	✓	✓	✓
58	RS-485 Assignment (auto)	x	x	x	x	x	x	x	x	x	✓	✓	✓
59	Shift Schedule	x	x	x	✓	x	x	x	x	x	✓	✓	✓
60	Smart Card Based Route Access	x	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
61	Smart Identification	x	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
62	Soft override	x	x	x	✓	x	x	x	x	x	✓	✓	✓
63	Special Functions	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
64	System Timers	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
65	Tamper Detection*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Sr. No	Feature Name / Product	Direct Doors									Panel/ Panel-Lite	Vega Panel-Lite (Panel2 00)	Panel Door
		Door V1	Door V2	V2 e-Cante en	NGT	Wireless Door/ Door V3/ Door V4	PVR Door	Vega Door	FMX Door	ARGO Door			
66	Time Triggered Function	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
67	Time Stamping	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
68	Time Zone	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
69	UHF Reader Support	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗
70	USB Flash	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
71	Use Count Control	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
72	User Configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
73	VIP Access	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
74	Visitor Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
75	Voice Guidance	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
76	Wireless Connection*	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
77	IP Camera Integration	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗
78	Auto Hide Menu	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗
79	Punch marking via Bluetooth	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗
80	Elevator Access Control	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
81	Face Recognition *	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗



- *The Access Level function in Direct Door would come into picture only with smart secure access.*
- *Access Modes for Panel and Panel-Lite are applicable at zone level, while for Direct Doors, they are applicable to the particular Direct Door only.*
- *Direct Doors have limited Access Policies applicable as compared to Panel Doors.*
- *The Degraded Mode feature needs to be enabled for Panels at the zone level, but comes into use in Panel Doors only.*
- *V1, V2, V3 and V4 Cafeteria Direct Doors can be converted into Panel Doors by manual RS-485 address assignment.*
- *NGT has 6 digit password field whereas all other door has 4 digit password field.*
- *Tamper Detection is present in Panel and not in Panel-Lite.*
- *CDC Exit Reader Support in FMX door is without FP reader.*
- *In Wireless door there is inbuilt Wi-Fi. which is not there in Door V3/V4. But in Door V3/V4; if dongle is inserted then it will work with wireless Wi-Fi.*
- *Wiegand Out feature is supported only in Door V4 out of all Door Controllers i.e. Door V1, Door V2, Door V3.*
- *COSEC MODE Device is specially designed for Face Recognition feature which uses in-built camera of Mobile device for capturing the face. See MODE Door for detailed configuration. COSEC Vega, COSEC FMX and COSEC ARGO supports face recognition by using IP camera for capturing the face.*

Network Configuration

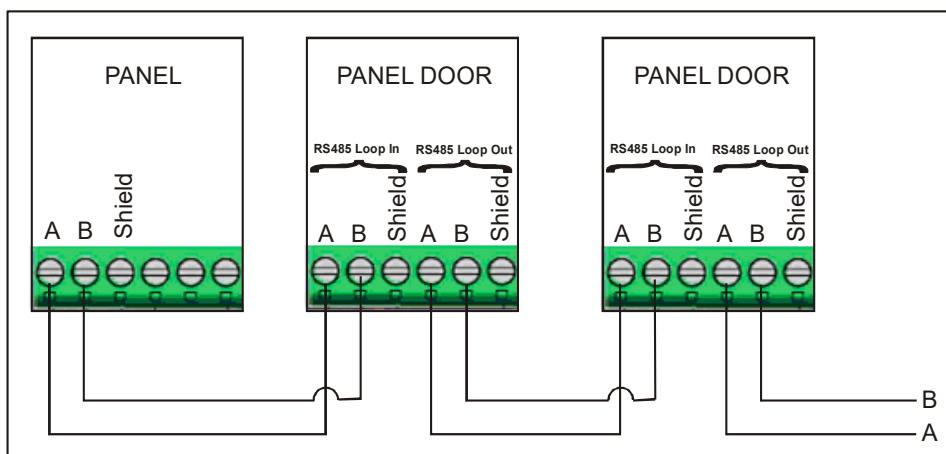
The COSEC PANELS and DOORs come with the following networking options:

- TCP/IP
- RS485

However, in the event of the DOOR being configured as a DIRECT DOOR, only the TCP/IP option will be available for communication. The DIRECT DOORs communicate directly with the COSEC Monitor application over the TCP/IP network while the PANEL DOORs communicate with the PANEL over the TCP/IP network or the RS485 loop.

Connecting the PANEL DOOR to the RS-485 Bus

The PANEL DOORs are linked together through their RS-485 Loop in and Loop Out terminals in the event of a RS485 loop connection with the COSEC PANEL. The interface allows the wiring of a Multidrop communication network of up to 4,000 feet (1200 m) in length from the last PANEL DOOR to the COSEC PANEL. Only one host COSEC PANEL per RS485 loop is supported as shown in the following figure.



The RS-485 communication loop should be wired using a two conductor cable (see cable specifications Belden 1227A or equivalent). The RS-485 loop can operate from 1,200 to 115,200 baud, under normal conditions. The baud rate depends on the loop length and the environment. DIP switch positions 1-5 are used to select the Controller's address on the network. Refer to **Table 1** for DIP switch setting information.

Switch **SW3** is provided at the bottom right on the rear face of the Premium DOORs for supplying end-of-line termination for the RS-485 network. The board ships with the switch in the non-termination mode. Push the switch to the **ON** position on the last Controller in the RS485 loop to provide end of line termination. Similarly on the Standard DOOR Models the switch is located just above the terminal strip on the rear face of the DOOR.



0 is ALSO a valid address for a DOOR controller in the RS485 loop.

DIP Switch Settings: Table 1

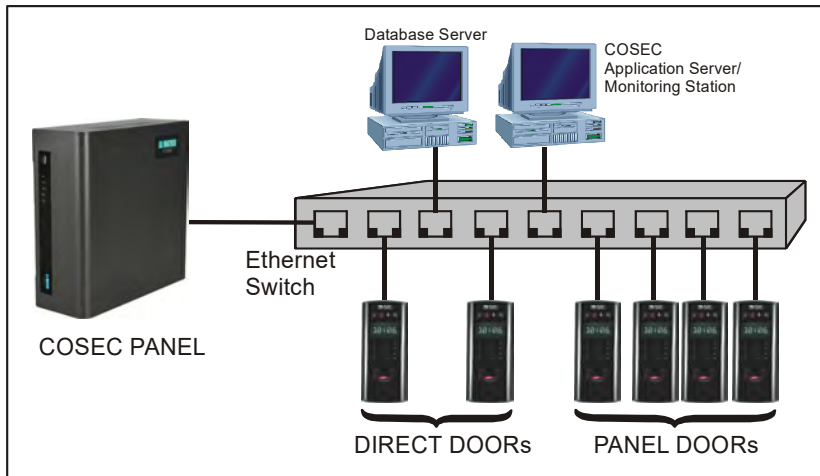
S1	S2	S3	S4	S5	Controller Address
Off	Off	Off	Off	Off	0
On	Off	Off	Off	Off	1

S1	S2	S3	S4	S5	Controller Address
Off	On	Off	Off	Off	2
On	On	Off	Off	Off	3
Off	Off	On	Off	Off	4
On	Off	On	Off	Off	5
Off	On	On	Off	Off	6
On	On	On	Off	Off	7
Off	Off	Off	On	Off	8
On	Off	Off	On	Off	9
Off	On	Off	On	Off	10
On	On	Off	On	Off	11
Off	Off	On	On	Off	12
On	Off	On	On	Off	13
Off	On	On	On	Off	14
On	On	On	On	Off	15
Off	Off	Off	Off	On	16
On	Off	Off	Off	On	17
Off	On	Off	Off	On	18
On	On	Off	Off	On	19
Off	Off	On	Off	On	20
On	Off	On	Off	On	21
Off	On	On	Off	On	22
On	On	On	Off	On	23
Off	Off	Off	On	On	24
On	Off	Off	On	On	25
Off	On	Off	On	On	26
On	On	Off	On	On	27
Off	Off	On	On	On	28
On	Off	On	On	On	29
Off	On	On	On	On	30
On	On	On	On	On	31

Ethernet Connectivity with the COSEC PANELS and DOORS

If the COSEC controllers are used in a LAN-enabled corporate setting, use the RJ-45 Ethernet port to connect the controllers to the corporate network. This method uses the existing network cabling for data exchange between the

Application server and the COSEC PANEL and the DIRECT DOORS as well as between the COSEC PANEL and PANEL DOORS.



The COSEC PANELs as well as the DOORS come with an on-board RJ-45 Connector.

The **PANELs** come factory configured with a default IP address of **192.168.50.1** while the **DIRECT DOORS** come pre-configured with a default IP address of **192.168.50.50**.

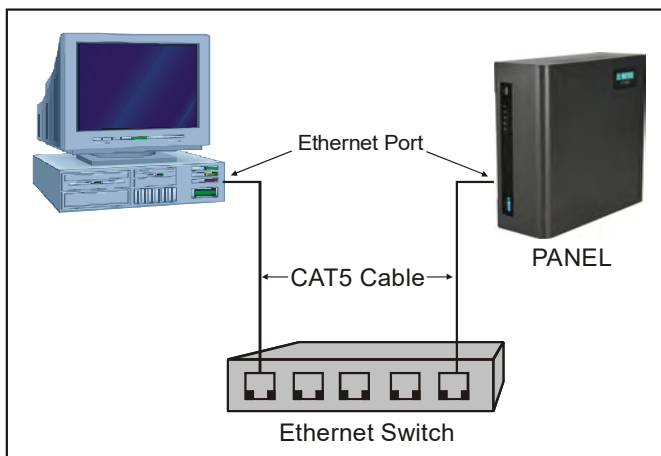
However, in the event of the DOORS being configured as PANEL DOORS, the IP addresses are assigned by the COSEC PANEL based on the **Slave network** parameters.

In order to change the IP address of the COSEC PANEL in line with the site requirements, change the IP settings of one of the computers on your LAN to **192.168.50.x** (where "x" can be any number from 2 to 254) by following the steps as described hereunder:

Connecting the COSEC PANEL to the Monitoring PC

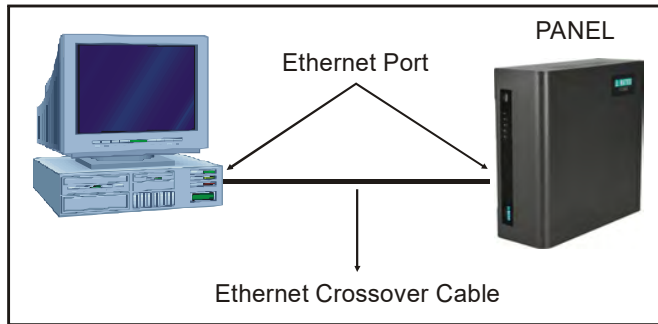
1. Connect your computer's Ethernet port and the PANEL's Ethernet Port by using either of two below mentioned methods:

Option 1: Connect both the computer's Ethernet port and the PANEL's Ethernet port to an Ethernet hub with standard straight-through Ethernet patch cables.



Option 2: Connect the computer's Ethernet port directly to the PANEL's Ethernet port with an Ethernet straight/crossover cable. A crossover cable is a cable that maps all output signals on one connector to the

input signals on the other connector. This allows the computer and the PANEL to perform full-duplex Ethernet communication.



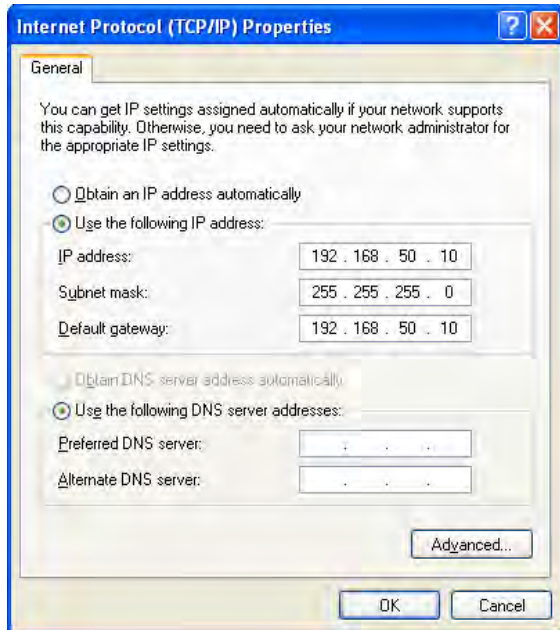
2. Configure the computer's network connection:

- a. Select **Start → Settings → Control Panel** from the Windows Desktop.
- b. Click **Network Connections**. The Network Connections window appears.
- c. Identify your local Ethernet connection (commonly labeled **Local Area Connection**), and click the icon to display the **Local Area Connection Status** window.
- d. Click on the **Properties** button to display the **Local Area Connection Properties** Window.

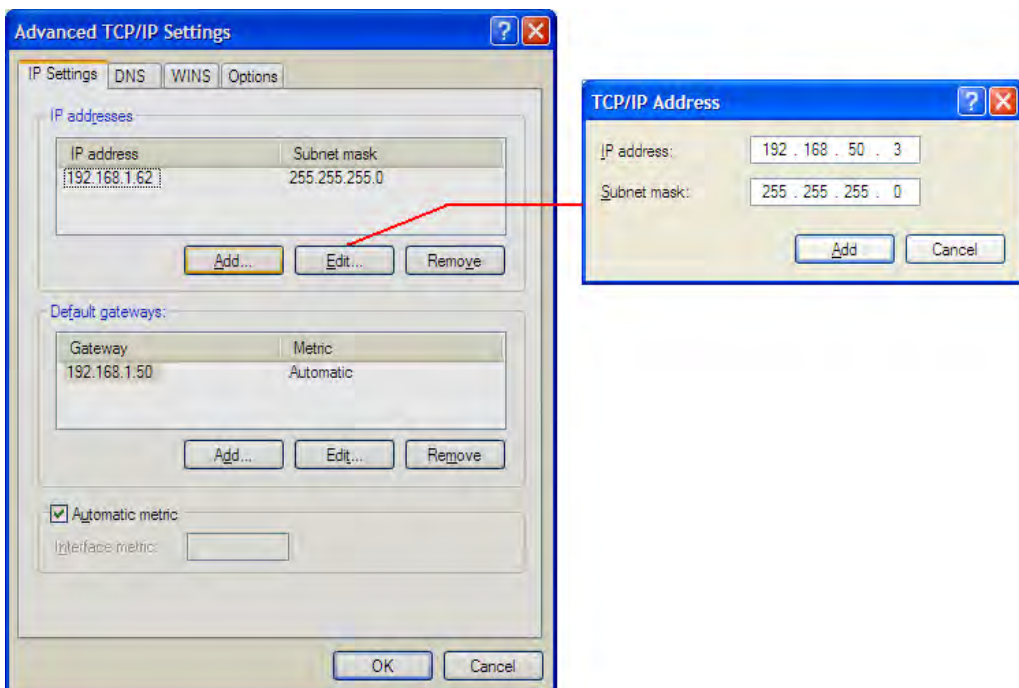


- e. Select the **Internet Protocol (TCP/IP)** option.

- f. Click **Properties** to display your system's current Internet Protocol properties.



- g. Click on **Advanced** to access the Advanced TCP/IP Settings window as shown below.



- h. Click on Add in the above window and enter "192.168.50.x" in the IP address field where "x" can be any number from 2 to 254.
- i. Enter "255.255.255.0" in the Subnet mask field.
- j. Click on Add to add the IP address to the list.

Click **OK** to save the settings.

Licensing for Premise Solution

The COSEC application platform has been partitioned into different modules to cater to the specific end user requirements.

The COSEC Application Platform has been categorized under the following licensing pattern based on the number of application users and door capacity. In addition to the above, the users can opt for the following modules at the time of placement of orders.

- **Platform/Basic Licence** - Admin + User + Device + Enterprise + Report Builder
- **T&A Licence** - Basic + T&A + Shift + Enterprise + Leave
- **ACS Licence** -Basic + Access Control
- **ESS Licence** - Used with T&A or Cafeteria
- **Cafeteria Licence** - Basic + Cafeteria
- **VMS Licence** - Basic +VMS
- **CWM Licence**- Basic +CWM including CSS+ Enterprise (CWM is recommended with T&A Licence)
- **JPC License**- Basic + T&A + JPC
- **FVM License**- Basic + T&A + FVM



The Licensing for Cloud based solution is based on user days for the particular license voucher. The voucher activation is done by the Tenant portal administrator.

In the event of the **Basic** COSEC platform license, the following options will be available on the home page after logging into the web application.

- Admin
- Users
- Devices
- Enterprise
- Report Builder



With Basic License; Report Builder will have only Events Template as default template. Other default templates of Report builder will be available with T&A license.

With the **Access Control** add on module the following options will be available on the home page after logging into the web application.

- Admin
- Users
- Devices
- Shifts & Schedules
- Access Control

The COSEC home page with only **Time and Attendance** add on module will have the following options available on the home page after logging into the web application.

- Admin
- Users
- Devices
- Shifts & Schedules
- Time & Attendance
- Leave management

The **Leave Management** module comes along with the Time and Attendance module and enables you to perform the following operations:

- Define Leave Policies
- Leave Opening Balance management
- Record Leave Adjustment transactions
- Record Leave Encashment transactions
- Leave application and approval
- View Reports

The **Visitor Management** module enables you to perform the following operations:

- Visitor Pre-Registration
- Maintain record of Blocked and Frequent Visitors
- Create Visitor E-Pass and Paper Pass
- View Reports

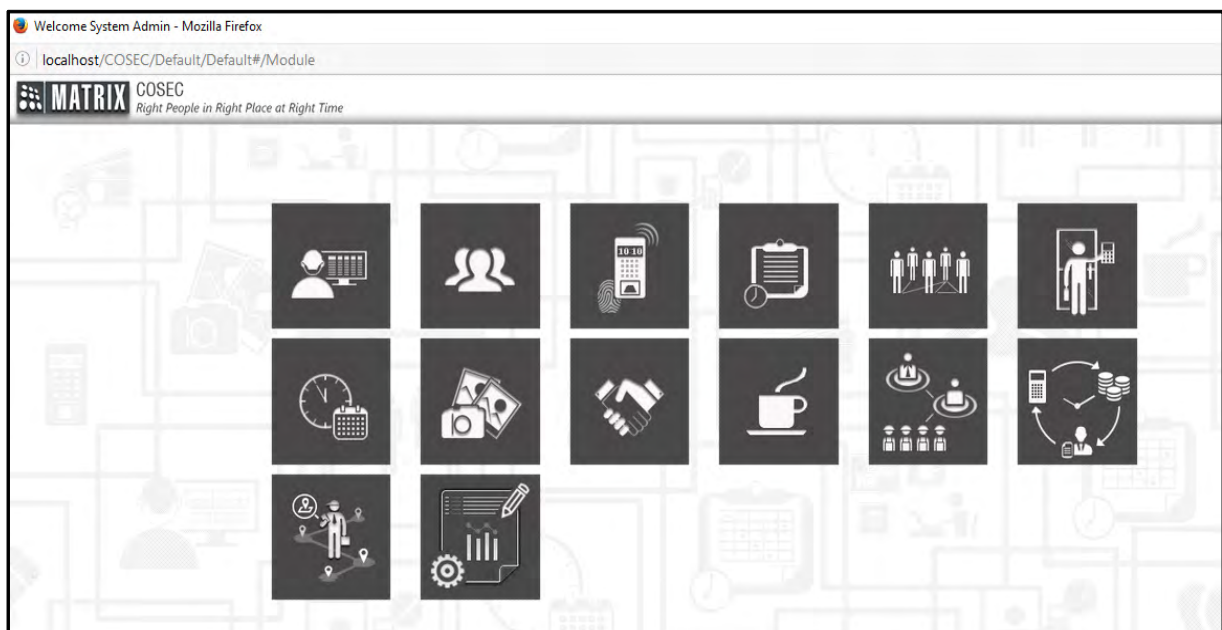
The **Contractor Worker Management** needs the Time and Attendance module to monitor contractor and workers and enables you to perform the following operations:

- Assign work orders to contractors
- Add and enroll contract workers and manage their credentials
- Manage worker assignments
- Approve, Reject, Blacklist contract workers
- Monitor daily and monthly work

The **Job Processing and Costing** Module enables to Create Project and Add Phases and Jobs to it, Assign Users to various Jobs. Also Monitor Daily Jobs and User's Time sheet.

The **Field Visit Management** Module enables to create task, assign task and location to some time slot. And monitor the user visiting the field.

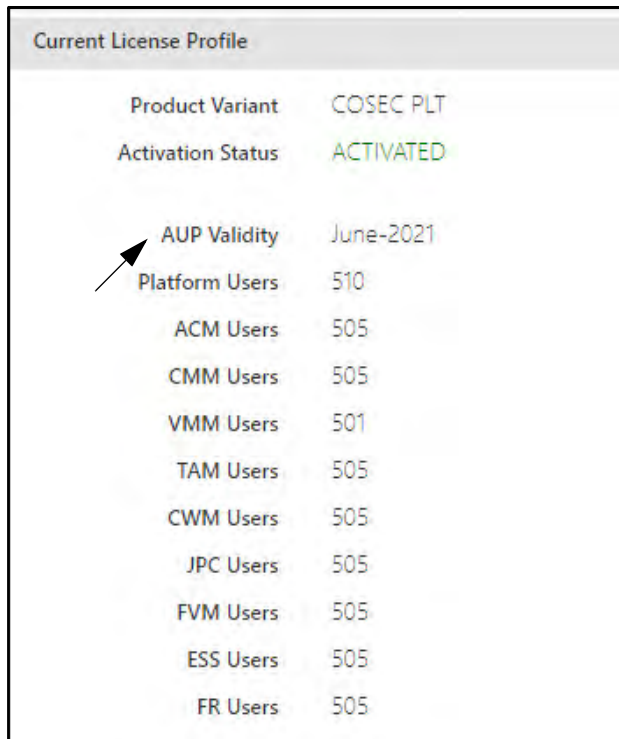
A full COSEC application license will have the following home page.



Thus, with the addition of module licenses, access to the various options are enabled.

Application Upgrade Package (AUP) Validity

COSEC AUP License allows you to upgrade the firmwares available before the time period specified in the Application Upgrade Package (AUP) Validity in **COSEC Centra Admin> Company Configuration> License and Services> Current License Profile> AUP Validity**.



Current License Profile	
Product Variant	COSEC PLT
Activation Status	ACTIVATED
AUP Validity	June-2021
Platform Users	510
ACM Users	505
CMM Users	505
VMM Users	501
TAM Users	505
CWM Users	505
JPC Users	505
FVM Users	505
ESS Users	505
FR Users	505

You will be allowed to upgrade the firmwares released before Month-Year specified in the Application Upgrade Package (AUP). These firmware upgradations are free of cost.

To upgrade the firmwares after this time period, you must renew the COSEC AUP License. As soon as you activate the License, AUP Validity date will be updated.

For Example:

In a system, AUP Validity is displayed as June-2021.

If a new firmware is released on March 2021, then the system can be upgraded with this firmware free of cost.

Similarly, if a new firmware is released on July 2021, and you wish to upgrade the system, then you must renew the COSEC AUP License.

To take the above example further, if a new firmware is released on July 2023 and the AUP Validity displayed in your system is July 2021, if you wish to upgrade the system, you must renew the COSEC AUP License twice.

Upgrading the COSEC License

For COSEC CENTRA, the COSEC application is shipped with the Generic license dongle. The License has to be updated with COSEC CENTRA PLT Voucher and Module specific vouchers based on User count as per your need.

Then activate the voucher against the Generic key in the Dongle.

Follow the Steps to upgrade the COSEC to new License structure(V14R1 onwards)

1. Ensure Application Upgrade Package (AUP) is available for upgrading to desired version.
2. Take Database Backup before upgrading.
3. Upgrade COSEC Software. Open COSEC Web login page/COSEC Admin Portal- License and Services page.
4. On License and Services page, SA user can accept and upgrade to new licensing structure. Once accepted; your license will be ported to new structure.



Once new License structure is upgraded, you cannot move back to older license structure.

The Login User name and Password will be provided by License Support team.

For more information on buying and upgrading license, Contact Matrix Channel Partners or Matrix Technical Support.

Using COSEC Web Application

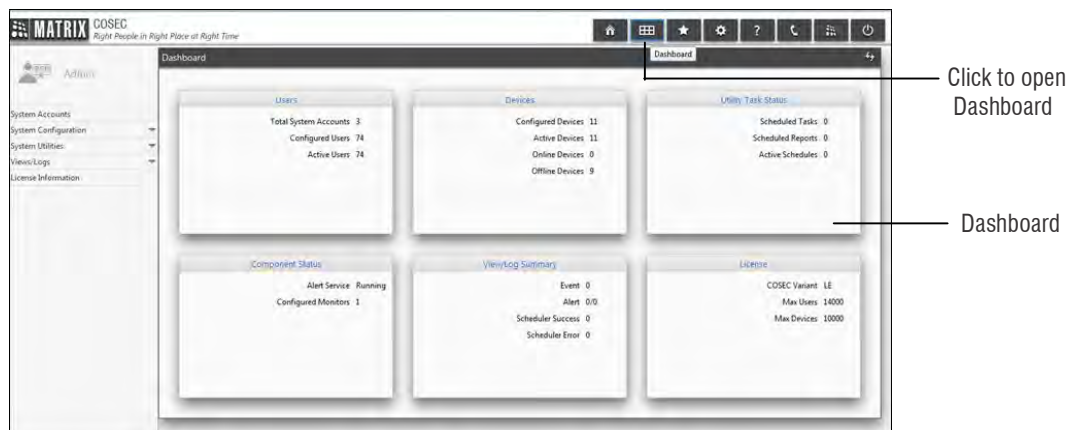
The COSEC Web application enables the users to log in to the web application from local or remote computers and configure the various parameters available in the functional modules. After the installation of the COSEC web application on the computer, the users can access the application by entering the following URL in the web browser:

`http://(ip address of web server computer)/cosec`

OR click on




From the home page of COSEC Web Application, the user can log into the various modules as supported by the License. The first page of any Module opens to the **Dashboard** as shown below which displays the information about the respective Module. On clicking the information links, the user can view additional details, or is directed to the corresponding configuration page.

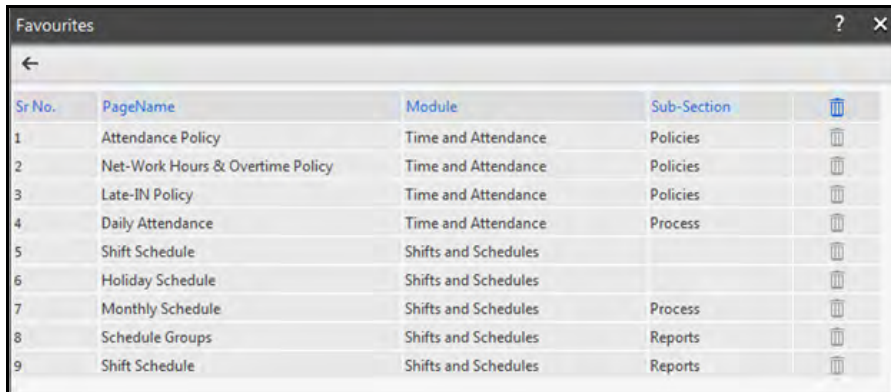











The Other interfaces are shown in below figure:



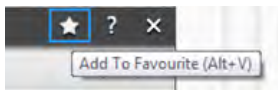
The **Menu Bar** at the top right side of window consist of following Icons:


- **Home:** Allows to go back to the Home Page.
- **Dashboard:** Allows to go to the dashboard page of the selected module.
- **Favourites:** Click on the **Favourites**  button from the Menu bar. This redirect to the Favourites Page as shown below.



Sr No.	PageName	Module	Sub-Section	
1	Attendance Policy	Time and Attendance	Policies	
2	Net-Work Hours & Overtime Policy	Time and Attendance	Policies	
3	Late-IN Policy	Time and Attendance	Policies	
4	Daily Attendance	Time and Attendance	Process	
5	Shift Schedule	Shifts and Schedules		
6	Holiday Schedule	Shifts and Schedules		
7	Monthly Schedule	Shifts and Schedules	Process	
8	Schedule Groups	Shifts and Schedules	Reports	
9	Shift Schedule	Shifts and Schedules	Reports	

- It shows the pages which are marked as favorites from pages of different modules by clicking on **Add to Favourite** button as shown below.



- The Favourite page can contain list of maximum 25 favourite pages. The user can remove the page from favourite list by clicking on delete button.
- **Account Settings:** Click on the Account Setting  button from the Menu bar. For more information, refer [“Account Setting”](#).
- **Help:** Gives the information about the COSEC Web Application.
- **Contact Us:** Gives the contact details of Matrix Comsec Pvt. Ltd. You can click on **Visit Us** link to view the Matrix website.
- **About:** Gives the details regarding the Product version, Product Variant and the Data Protection Manager. To configure and know more about the details of Data Protection Manager, refer [“Data Protection Manager”](#)
- **Logout:** Enables to log out from the application.

The **Title Bar** at the top right side of all module sub-options page consist of following Icons:

- **Refresh:** When you change any string in the language file and its reflection is required in the COSEC so click the Refresh button to get immediate reflection or else the changes will be reflected when you restart the system.
- **Add to favorites:** Enables to add the current page to favorites list.

- **Help:** Gives the information about the current page. For cross reference details refer to the complete System Manual.
- **Close:** Enables to close the current page and goes back to the selected module Dashboard.

The pages of the COSEC Web application have the following **Control/Command** buttons which are used to perform the functions as described below:

- **Back:** Allows to back to the previous page.
- **New/Add:** Allows creation of a new record for the selected option.
- **Edit:** Allows user to edit an already existing record.
- **Delete:** Allows user to delete the selected record.
- **Save:** Allows user to save the changes to the system.
- **Cancel:** Allows user to remove the data selected.



The COSEC application basic platform consists of the modules mentioned earlier in this manual. In order to get the COSEC BASIC application up and running, the administrator needs to configure the parameters in the following order:

Admin>Device Configuration> User Configuration



In presence of other modules follow the configuration order as:

Admin>Device Configuration> Configure T&A Policies, Leaves, Enterprise Structure, Shifts & Schedules

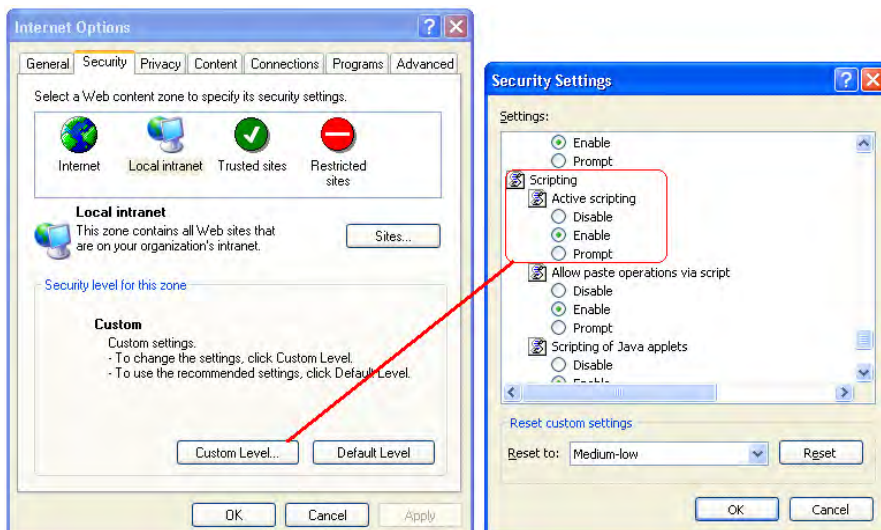
>Then configure User configuration

> Configure at last Access Control,Canteen and Visitor Modules



*Administrator needs to ensure that Java scripting is enabled in the security settings of the web browser application. In Internet Explorer this is done by selecting **Internet Options** from the **Tools** menu.*

*On the Internet options page go to the **Security** tab and click on the **Custom Level** button. Enable the Active Scripting option as shown.*



Initial Configuration with Device

To begin with COSEC Web Application, first configure the device by setting the LAN IP and Server port in the Network parameters of Door. The LAN IP should be the IP of the PC where COSEC Monitor is installed.

Now in the COSEC Web application go to **Device List**> Click on **New** and select the device or select **Device Module**> **Device Configuration**> **Profile**> **Basic**: Enter the MAC Address of the device to be connected in the

MAC Address field. While saving the MAC, the IP from the device will be fetched by the web application and the device will get activated.

OR

There is easy option of Automatically addition of new device by checking the box **Auto Add New Device**. For enabling this feature go to **Admin Module> System Configuration> Global Policy>Device**.

If the Auto addition feature is enabled then there is no need to enter the MAC address. The application will automatically configure the parameters and the device will be added.




For connecting the door as PANEL Door, auto addition has to be disabled. Then define the PANEL door manually then connect to the server. For details refer Devices Section.

Now configure the Device with Basic and Advanced parameters from the Device Module. For more details see Devices Module.

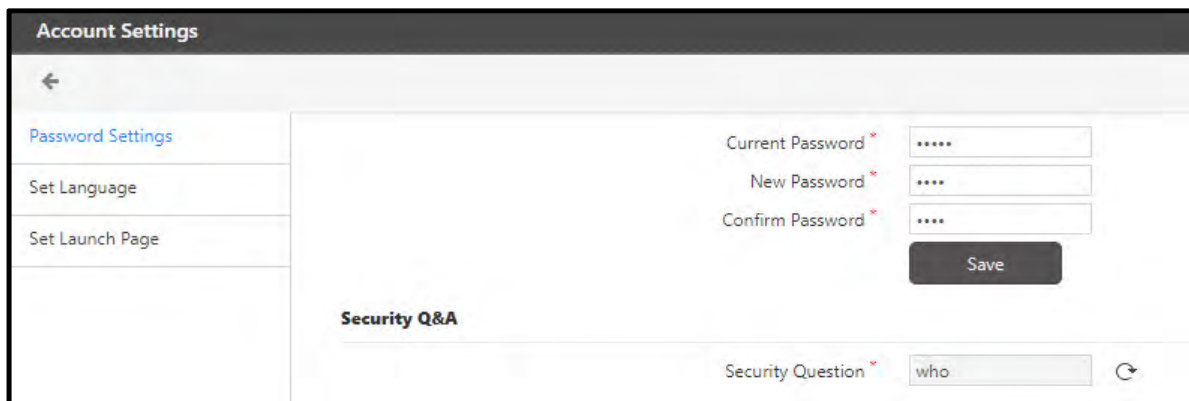
The COSEC system enables the administrator to define **sites** which are to be used for reporting purposes. The Door Controllers can then be assigned to the defined sites.

For defining Sites go to **Device Module> Masters> Site**.


Account Setting

Account Settings: Click on the Account Setting  button from the Menu bar. This enables the user to change the password, set the preferred language and to set the launch page for the login user.

- **Password Settings**
 - You can set new password from the Password Settings tab.



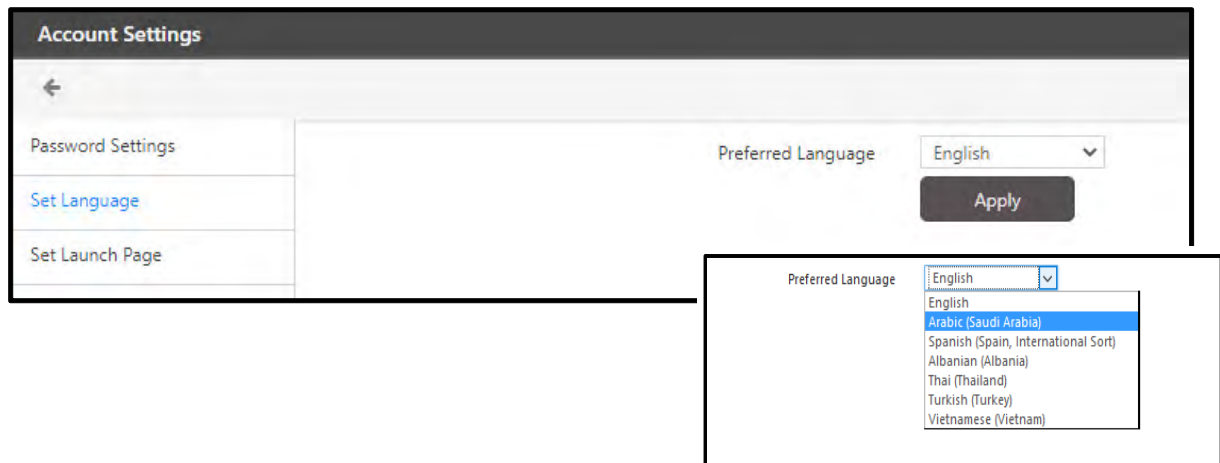
You can enter maximum 128 characters in password.

- **Security Q&A**
 - Security Q&A section will initially show a Security Question with the value of already fed security question at the time of page access.
 - Click on the **Reset Security Q&A**  Icon placed along with it and configure the following parameters to change Security Question and Answer for System Administrator login.

Security Question
Security Answer
Confirm Security Answer
Current Password

Then click on the **Save** button.

- **Set Language**
 - You can set the language by selecting the preferred language.

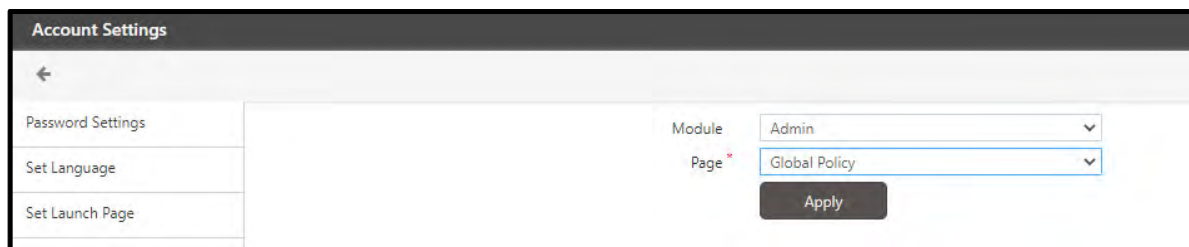


The screenshot shows the 'Account Settings' interface. On the left, there is a sidebar with options: 'Password Settings', 'Set Language' (highlighted in blue), and 'Set Launch Page'. The main area displays 'Preferred Language' with a dropdown menu currently set to 'English' and an 'Apply' button. A callout box shows the expanded dropdown menu with the following options: English, Arabic (Saudi Arabia), Spanish (Spain, International Sort), Albanian (Albania), Thai (Thailand), Turkish (Turkey), and Vietnamese (Vietnam).



The Language translation can be done via Multi-Language Utility. To know more, refer to the Multi-Language Utility User Guide.

- **Set Launch Page**
 - You can select the launch page i.e. the page which will appear directly after logging into COSEC.




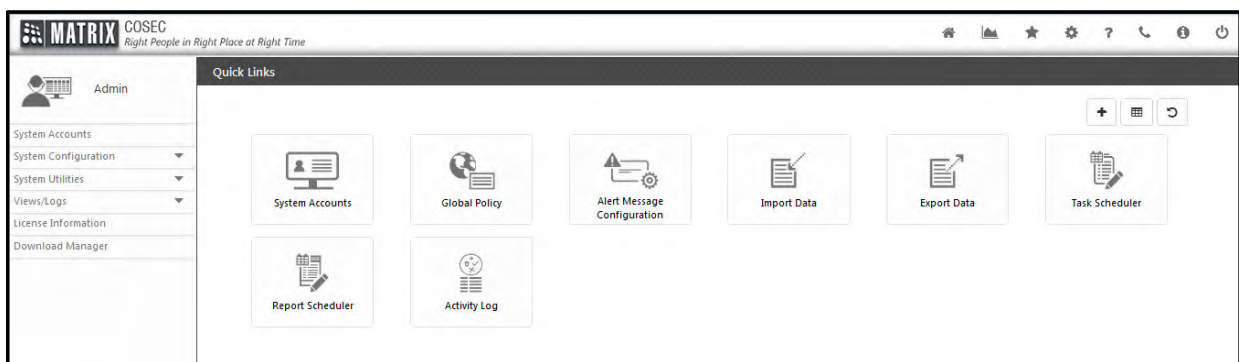
The screenshot shows the 'Account Settings' interface. On the left, there is a sidebar with options: 'Password Settings', 'Set Language', and 'Set Launch Page' (highlighted in blue). The main area displays 'Module' (set to 'Admin') and 'Page' (set to 'Global Policy') dropdown menus, with an 'Apply' button below them.

The **Admin** module allows the System Administrator to define users who will be using the COSEC application. Using this module, system rights and other information for the users of the COSEC application can be specified based on their roles. In addition, each user can be assigned a unique set of IDs and Passwords. It is recommended that this module be configured before starting the configuration of the COSEC Controllers for other applications.



A system administrator can set all parameters related to the use of the COSEC application and its modules. The administrator can also set the data export format based on certain database views which are provided by default along with the COSEC application. This would thus enable exporting of data which can be used as an input to external applications like Payroll.


This module also has the License Information option which allows the administrator to view the license details as well as enter new license string for updating the application and add more application user licenses as well as other modules.

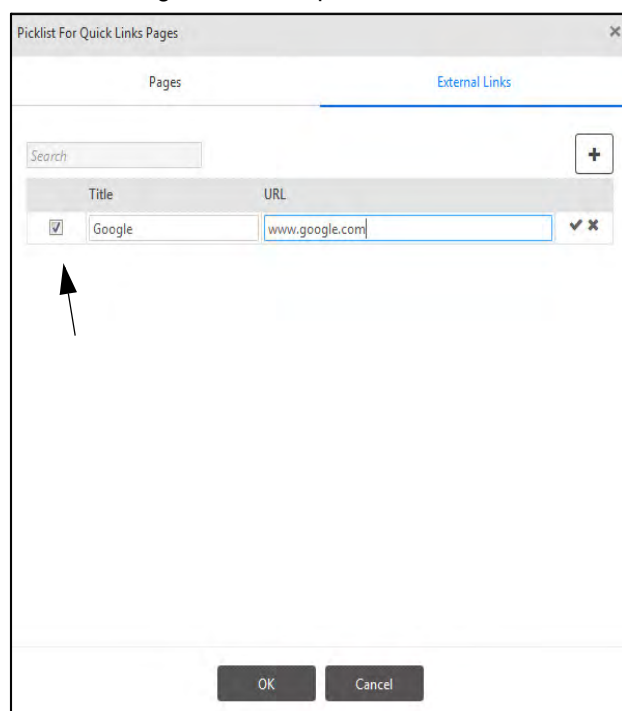
To use the system administration functionality, select the **Admin** module icon  on the module selection page. The **Admin** module page appears on the screen as shown below.



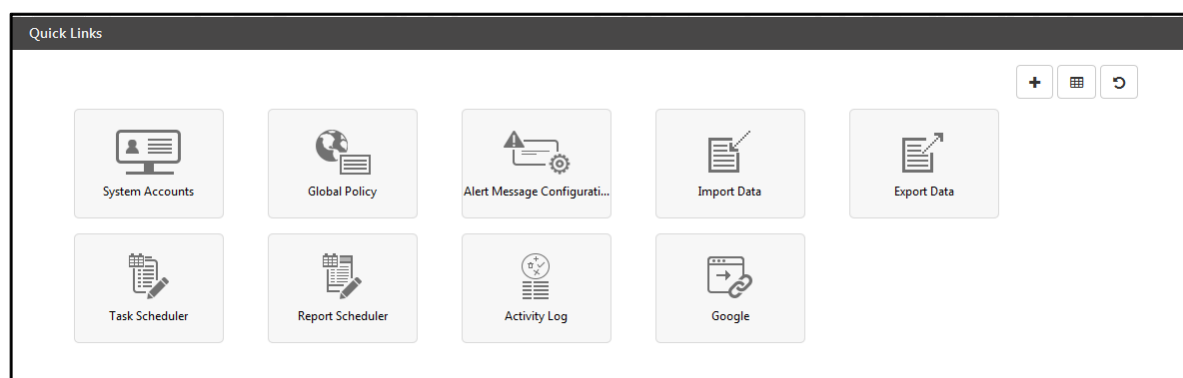
The page displays a menu and **Quick Links** to go to the required page in just one click. Quick Links are shortcuts to reach to a specific page easily. It also contains following three buttons:



- **Add Quick Link:** Click  button to add a quick link. A picklist for Quick Link pages appears for selecting the page or External Link for which the quick link is to be created. Maximum **20** quick links can be added.
- For Adding **Pages** in Quick Link, Select the Pages and click on OK
- For Adding **External Links**, Select External Link tab, click on  button to add new external link.

- Configure the **Title** and **URL** of the external link under the respective fields. click on checkbox to get the configured link on quick link screen as shown below. To save the configuration click on .



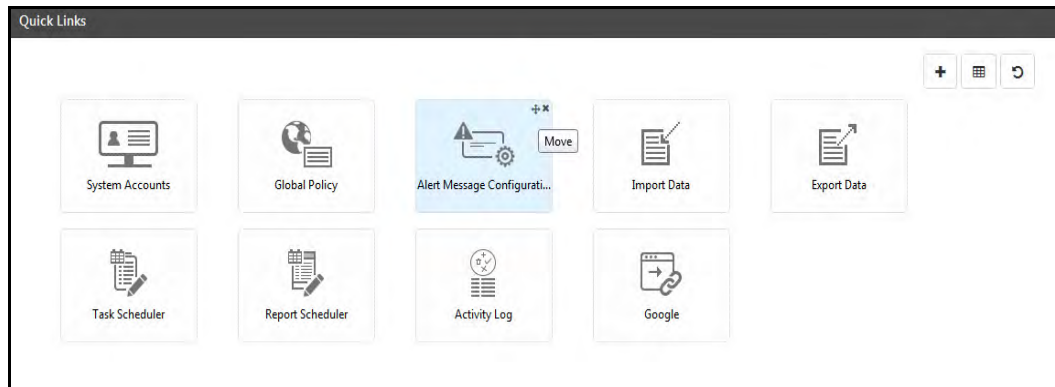
- To edit the saved configuration, click on .
- Click on OK to save the link configuration on Quick Link screen. The external link will be displayed as shown below:



- **Select Layout:** Click  button to select a layout for the quick links. You can select 5x4 or 4x5 layout to manage the quick links.
- **Reset Quick Links:** Click  button to reset the quick links to the default quick links.

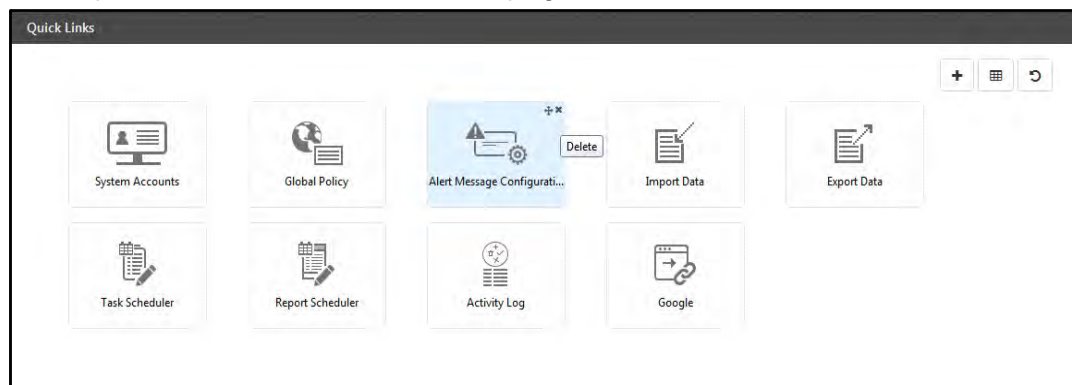
Move the Link

To move the link from one place to another, hover on the link on top right corner and click on “Move” icon as shown below. Then drag the quick link to the desired place. It will be placed at the desired location on the quick links page.




Delete the Link

To delete a particular link, hover on the link on top right corner and click on “Delete” icon as shown below.

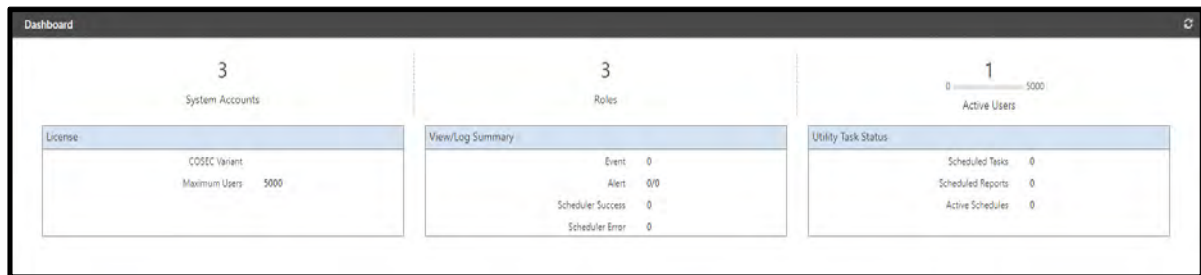


Quick links are displayed as per rights given to System Account and ESS users.

Admin Dashboard

The Admin Dashboard presents an overview of system information along with current system status. It also displays the total number of created Users in System Account, total number of created Roles and total number of active users. To view the Dashboard, click the Dashboard button  on the **Admin** page. It appears with the following information:

- System Accounts- Displays the number of system accounts created in the COSEC.
- Roles- Displays the number of Roles created in the COSEC.
- Active Users- Displays the number of active users created in the COSEC.



License


- Maximum Users - Maximum number of users allowed per license.

View/Log Summary

- Event - No. of event views made on the current day.
- Alert - No. of SMS Alerts/No. of e-mail alerts for the current day.
- Scheduler Success - No. of scheduled tasks completed successfully on the current day.
- Scheduler Error - No. of scheduled tasks which failed on the current day.

Utility Task Status

- Scheduled Tasks - Total tasks that are configured in scheduler.
- Scheduled Reports - Total reports that are configured in scheduler.
- Active Schedules - Total number of scheduled tasks and reports that are currently active.

For more information on the above Dashboard options, click the respective information links on the Dashboard. The Latest values on Dashboard are updated on clicking the Refresh  button.

Managing System Accounts

Every system account on COSEC is associated with a login role and a login user.

A login role on COSEC is a pre-defined role that determines how a user associated with it may login or perform certain activities on the COSEC application. For example, a Human Resources (HR) Manager in an organization may be assigned the login role of a system administrator, thus enabling him to administer system policies for an organization.

COSEC identifies three types of system-defined login roles which determine the login and system operation rights for each user. These are -

- System Administrator (SA)
- System Engineer (SE)
- System Operator (SO)



SE and SO account will be inactive by default during first login after installation. SA user can login and activate the SE and SO accounts.

In addition to these, Admin can add new login roles and configure role rights for each role. Based on these role rights, all login users associated with a login role can perform specific activities on COSEC.

You can create On Behalf System Accounts Users also. On Behalf Users can perform specific activities such a Leave Applications, Attendance Corrections, Apply for Shout Leaves etc on behalf of other users. For details refer to [“On Behalf System Account User”](#).

To view System Accounts page go to **Admin module > System Accounts** and the following screen appears.

The screen displays two tabs namely:

- [“System Accounts”](#)
- [“Roles and Rights Configuration”](#)


System Accounts

This tab enables to create login users.

To add a new login user to the system, go to **Admin module > System Accounts > System Accounts** tab and the following screen appears.

ID	Name
Aahar	Aahar
Canteen	Canteen
cosecdevic	COSEC Device
custom	custom
Devanand	Devanand
Enroll	Enroll
FR	Face Recognition
IDS	IDS
jayesh	jayesh
kanul	kanul

The page displays a **tool-bar** for creating, editing, deleting, saving, canceling and resetting password for a user along with configurations on the left hand side and a grid containing a list of created users on the right hand side. One can also search a particular user from the grid using **Search** field.

1. Click the **New**  icon on the **System Accounts** page.
2. Configure the following options as required:
 - **Login ID** - Assign a unique ID for the Login User.
 - **Name** - Enter a name for the login user.
 - **Role** - Select a login role from the drop-down list. One can also create a new login role from the Role Configuration tab or by clicking on the pick list button. Refer [“Roles and Rights Configuration”](#).
 - **Active** - Select to mark the status of the user as active. On enabling, the user becomes an active user.
3. Configure the remaining parameters on this page as described in the following sections.
4. Once the new system account is configured, click **Save** to add the new login user to the COSEC database.

Optional

This section allows the administrator to perform additional configurations for defining a login user on COSEC. To do this,

Under **System Accounts**, expand the **Optional** collapsible panel as shown below.

The screenshot shows a configuration window with the following elements:

- Linked ESS User:** Two input fields for 'ID' and 'Name'.
- Preferred Language:** A dropdown menu currently showing 'English'.
- Email:** A text input field.
- Enable API Access:** An unchecked checkbox.
- Report Export Output in PDF Only:** An unchecked checkbox.
- Set Launch Page:** A section containing two dropdown menus for 'Module' and 'Page', both currently set to '-Select-'.

Enter the following details:

- **Linked ESS User:** Select an ESS user using the picklist to link with the System Account. This allows selected employees to be assigned login rights to COSEC web system accounts. On logging into the respective system account, the user is now also able to access his/her ESS page directly from the COSEC Web module selection page.
- **Preferred Language:** Select the language to be preferred from the dropdown list. On selecting a specific language all the labels of the COSEC will change into that particular language. E.g. if Urdu language is selected, then all the labels get changed into Urdu.
- **Email:** Configure the Email ID to be link with the System Account and to be mapped with the attributes received in the SSO response. After successful SSO configuration, through this Email ID the SSO User will be able to login.
- **Enable API Access:** Select this checkbox allow the System Account user to use an *Application Programming Interface* (API) to access or update the COSEC database. While accessing COSEC through API you will need to enter the API login credentials for devices as mentioned in Global Policy.
- **Report Export Output in PDF Only:** Enable this checkbox to restrict exporting reports to the PDF format only. This will prevent risks of data manipulation using any other output format.

Login Via Active Directory

This feature will be active only if the same parameter is also enabled at the Global system level (*Admin module > System Configuration > Global Policy > Login*). Select the checkbox to enable system account users to login using their Active Directory credentials.

Enter the Active Directory **Username**. For eg: admin123

Specify the **Domain** name. For e.g. if the domain name is matrix.com the domain name is specified as: dc=matrix,dc=com.

Click the **Default Domain** button to set the domain name as saved in Global Policy configuration.

Set Launch Page

The user who accesses only one particular page in COSEC on a daily basis can be assigned that page as the launch page i.e. when the user logs into COSEC; the launch page will directly appear.

Module: Select the Module from the drop down list whose page is to be set as launch page.

Page: Select the page belonging to the selected module which will directly appear after login into COSEC.

Click **Save** button.



1. If a page is set to Launch page; then afterwards if the page view rights are made disabled or the respective Module rights are enabled to "Hide" then selection of Module and Page will get reset to default.

2. If Customized report is set to Launch page; then afterwards if the customized report is being deleted then selection of Module and Page will get reset to default.

Assigning Group-Wise Rights

The administrator can assign all or specific enterprise groups to each login user. The login user will then have access rights only to the user records belonging to the assigned group.

To assign group-wise rights,

- Under **System Accounts**, expand the **Group-Wise Rights** collapsible panel as shown below.

ID	Name	Group	
1	MatrixComsec	Organization	

- Select Users:** Select users dropdown list provides two options:
 - Group Wise: To specify users based on the selected enterprise group using a picklist.
 - All: To select all active users on the system.
- Select Group:** If All is selected, then the default enterprise groups will be assigned as per the assignment in the Enterprise Module.

If Group Wise option is selected, select the desired enterprise group from the dropdown list — Organization, Branch, Department, Designation, Section, Category, Grade, Custom Group1/2/3.

System Accounts Roles And Rights Configuration

Group-Wise Rights

Select Users: Group Wise

Select Group: Organization

Organization * ID Name

Search

ID	Name	Group	Default	
2	ORG2	Organization	<input checked="" type="checkbox"/>	
3	organization-3	Organization	<input type="checkbox"/>	
2	Branch 2	Branch	<input checked="" type="checkbox"/>	
1	Department-1	Department	<input checked="" type="checkbox"/>	
1	Designation-1	Designation	<input checked="" type="checkbox"/>	
2	section-2	Section	<input checked="" type="checkbox"/>	
1	Category-1	Category	<input checked="" type="checkbox"/>	

1 - 7 of 11 records

« < 1 2 > »

For each enterprise group — Organization, Branch, Department, Designation, Section, Category, Grade, Custom Group1/2/3, click the corresponding picklist to select the desired option/s.

Picklist For Organization Master

Total Selected: 2 Records

Search Show Selected

<input type="checkbox"/>	ID	Name
<input type="checkbox"/>	1	DADB
<input checked="" type="checkbox"/>	2	ORG2
<input checked="" type="checkbox"/>	3	organization-3

OK Cancel

Click **OK**.

System Accounts

Roles And Rights Configuration

Active ☒

Optional ▼

Group-Wise Rights ▲

Select Users

Group Wise ▼

Select Group

Organization ▼

Organization *

ID

Name

☰

Search

🔍

ID	Name	Group ▲	Default	🗑️
1	Custom Group 2	Custom Group 2	<input checked="" type="checkbox"/>	🗑️
1	Custom Group 3	Custom Group 3	<input checked="" type="checkbox"/>	🗑️
2	ORG2	Organization	<input checked="" type="checkbox"/>	🗑️
3	organization-3	Organization	<input type="checkbox"/>	🗑️

8 - 11 of 11 records

«

<

1

2

>

»

If there are multiple options available in each group, you can also set the default option as per your requirement.

For example: If you have 3 organizations — ORG1, ORG2 and ORG3, then ORG1 will be assigned as default. If you wish to set ORG3 as default, select the corresponding check box under Default.

The SA User will have rights to these groups only. New users created using his/her SA login, will be assigned these groups as their default groups.

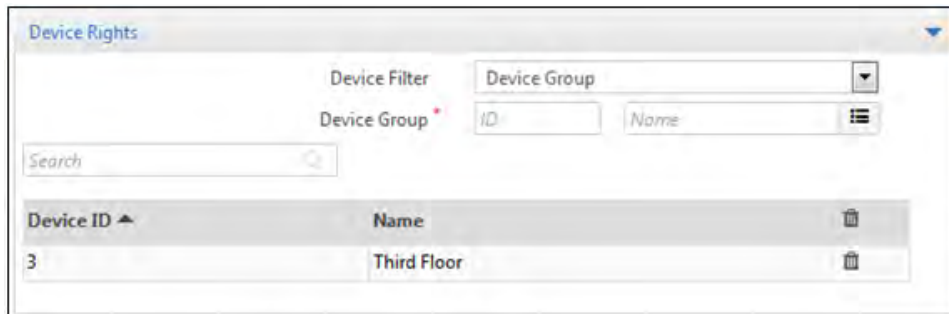
- These selected groups get displayed in the grid below the parameters. If required they can be deleted also by clicking on **Delete** icon.

Assigning Device Rights

A login user can also be assigned rights to access only selected devices or device groups on COSEC.

To do this,

- Under **System Accounts**, expand the **Device Rights** collapsible panel as shown below.



Device ID	Name
3	Third Floor

- **Device Filter:** Select devices/device groups from the dropdown list.
- **Device/Device Groups:** Based on the option selected from the Device Filter select the devices/device groups using the picklist for which the rights are to be assigned. The selected devices/device groups are displayed in the grid below the table. One can also search devices/device groups using the **Search** field.
- Click **Save** button.



Predefined System Account Login Roles (SA, SE or SO) are non-editable.

Once the user is created, the password for ESS User can be reset by clicking on **Reset ESS Password** button located in the toolbar. On clicking the button a message stating **Password Reset Successfully** gets displayed on the screen.



On Behalf System Account User

If in a certain scenario a user/worker is not able to access the system and subsequently fails to apply for a leave application, attendance correction or any other similar requests, in that case the On Behalf System Account User will be able to do so for that user/worker.

The On Behalf System Account User will have rights equivalent to that of a System Admin to execute the desired request of a User/Worker. You can modify the Roles and Rights assigned to this user as per your requirement.

To create the On Behalf System Account User follow the steps mentioned under [“System Accounts”](#) and for the roles and rights to be assigned to this user, refer to [“Roles and Rights Configuration”](#)

The On Behalf System User can either further the request of the application to the respective RIC or, the request can be considered for auto approval depending on the **Auto Approve** checkbox selection in Admin> [“Roles and Rights Configuration”](#)

The On Behalf System User can perform the following:

- "Attendance Correction Application"
- "Short Leave/Official IN-OUT Application"
- "Advance Overtime Application"
- "Leave Application/Approval"
- "Tour Application/Approval"
- "C-OFF Application/Approval"
- "Manual Correction"
- "Field Visit Correction"
- "Time Sheet Correction"
- "Pre-Registration"

Roles and Rights Configuration

Login Roles can be created in COSEC and each role can be assigned rights by the system administrator to access and perform specific functions in the COSEC Web Application or COSEC Desktop Apps. To do this,




- Under **System Accounts**, click the Role pick-list button in the **New/Edit** mode or click the **Role Configuration** tab as shown in the screen below.

Page Right

The screenshot shows the 'Roles And Rights Configuration' window. On the left, there's a sidebar with 'System Accounts' and a list of roles: System Administrator, System Engineer, System Operator, CAFETERIA, Security, test, Test SA, and ONBEHALF. The main area is titled 'Roles And Rights Configuration'. It has a 'Role' field set to 'System Administrator' and a 'Copy Right As Per' field set to 'Name'. Below these is a 'Module' dropdown set to 'Admin'. There are icons for 'View', 'Add', 'Edit', 'Delete', 'Print', and 'Auto Approve'. A table lists various system configuration options with checkboxes for each of these actions. The table has columns: Menu, Parent Menu, View, Add, Edit, Delete, Print, and Auto Approve. The table lists various system configuration options like Dashboard, System Accounts, Global Policy, Identification Server Configuration, SMS Configuration, Email Configuration, Rename Group, Enterprise Profile, Alert Message Configuration, and Custom Message. The 'View' column has checkboxes for all items. The 'Add', 'Edit', 'Delete', 'Print', and 'Auto Approve' columns have checkboxes for some items. At the bottom, it says '1 - 10 of 29 records' and there are pagination controls.

- **Role:** Enter a name for the Login Role.
- **Copy Right As Per:** If role rights are to be copied from another role then select a created role using the picklist button. **E.g.** If a new role Employee is created and the Copy Right As Per value is SA. Then all the rights of SA are copied to Employee. So, now even Employee role has the same rights as SA role.

After you select the desired option in Copy Right As Per, if required you can manually change/modify the View, Add, Edit Delete, Print or Auto Approve options for the desired Module's Menu options.

- **Module:** Select a module from the drop-down list for which rights are to be assigned to the Login Role.
- Select the type of rights to be assigned to the role from **Page Rights**  / **Module Rights**  / **Application Rights**  section by clicking on the respective icons.

- Further, as per the selected rights you can assign the View, Hide, Add, Edit, Delete, Print and Auto Approve login rights to the login role by selecting the respective check boxes against each function.
- **Auto Approve:** Select this check box, if you want the applications made by the On Behalf System Account User to be pre-approved. Clear this check box if you want the applications made by the On Behalf System Account User to be sent to the respective RIC for approval. To know more about On Behalf System Account User, refer to ["On Behalf System Account User"](#)



If no role rights are assigned to a system account, for a particular module (say, Leave Management), user can check the **Hide Module** option to hide this module from the login user's view for the same system account.

- Click **Save** button.
- All saved Login Roles can be viewed in the list on the left hand side. One can also search a login role using **Search Role** field.

Module Rights

The screenshot shows the 'Roles And Rights Configuration' window. On the left, there is a 'System Accounts' sidebar with a search field and a list of roles: System Administrator, System Engineer, and System Operator. The main area is titled 'Roles And Rights Configuration'. It features a 'Role' dropdown set to 'System Administrator' and a 'Copy Right As Per' dropdown set to 'Name'. Below this is a table with columns: Module Name, Hide, View, Add, Edit, Delete, and Module Rights. The table lists 14 modules: Admin, Access Control, Time and Attendance, Leave Management, Visitor Management, Cafeteria Management, Users, Devices, Shifts and Schedules, and Enterprise Structure. Each module has checkboxes for Hide, View, Add, Edit, and Delete. The 'Module Rights' column contains a small icon for each module. At the bottom, it says '1 - 10 of 14 records' and has a pagination control showing '1' and '2'.



If you select the Hide check box of any Module then that Module will not be visible on the Home page of COSEC Web, however its reflections in other Modules will be visible. For example if you select the Hide check box for Visitor Management, then Visitor Management will not be visible on the Home page but the Visitor Management tab in the User > User Configuration will be visible.

If you want to remove any Module and its reflections from COSEC Web, it can be done from the COSEC Admin Portal > Company Configuration > License and Services. For details, refer to the Admin Mgt Portal User Guide

Application Rights


The screenshot shows the 'Roles And Rights Configuration' window. On the left, there is a 'System Accounts' sidebar with a search field and a list of roles: System Administrator, System Engineer, and System Operator. The main area is titled 'Roles And Rights Configuration'. It features a 'Role' dropdown set to 'System Administrator' and a 'Copy Right As Per' dropdown set to 'Name'. Below this is a table with columns: Application Name, View, Add, Edit, Delete, and Application Rights. The table lists 6 applications: Cosec, COSEC Enroll, COSEC Monitor, COSEC Alert, COSEC VMS, COSEC Identification Server, and COSEC Visitor Portal. Each application has checkboxes for View, Add, Edit, and Delete. The 'Application Rights' column contains a small icon for each application. At the bottom, it says '1 - 10 of 14 records' and has a pagination control showing '1' and '2'.

Defining Global Policies

Global Policies are general administrative policies that are applicable all across the COSEC system and define the governing parameters for all COSEC system account users. In COSEC, the system administrator has the rights to define such general system policies as per the organization's norms, practices and requirements. The different sets of policies that COSEC allows the administrator to configure are:

- *"Basic Policy"*
- *"User Policy"*
- *"Login Policy"*
- *"Password Policy"*
- *"Device"*
- *"Access Control Policy"*
- *"Time Attendance Policy"*
- *"Reports Policy"*
- *"Visitor Management Policy"*
- *"CWM"*
- *"Job Costing"*
- *"Field Visit Management"*
- *"ESS"*
- *"SSO Configuration"*
- *"Face Recognition"*

To define Global System Policies,

1. Go to **Admin module > System Configuration > Global Policy**
2. Configure different global system policies as described in the following sections.
3. Once all policies are defined as per requirement, click **Save**  button.

Basic Policy

These policies govern the general working of the COSEC system.

To configure Basic Policy, go to **Admin module > System Configuration > Global Policy > Basic** and the following screen appears.

The screenshot displays the 'Global Policy' configuration window with the 'Basic' tab selected. The left sidebar contains a list of navigation items: Basic, User, Login, Password Policy, Device, Access Control, Time Attendance, Reports, Visitor Management, CWM, Job Costing, Field Visit Management, ESS, SSO Configuration, and Face Recognition. The main content area is divided into several sections:

- Basic:** Includes checkboxes for 'Create Activity Log' (checked) and 'Auto Login To COSEC Monitor' (unchecked), and a 'System Date Format' dropdown set to 'dd/mm/yyyy'.
- Multi-Language Parameters:** Includes a checked 'Support Multi-Language Input' checkbox and an 'Input Alignment' dropdown set to 'Left To Right'.
- Change Background:** Features a 'Background' selection area with an information icon.
- Google API Key:** Includes a 'Get Location Details' checkbox (unchecked) and an 'API Key' text input field.
- General Data Protection Regulation:** Includes checkboxes for 'Personal Data Protection' (unchecked) and 'Custom Fields' (unchecked), with an information icon next to the latter.
- Data Protection Manager:** A section with a note: 'Note: It is advisable to take backup of Database before updating value of Personal Data Protection.' Below this is a form with fields for Name, Designation, Organization Name, Organization Address, Email ID, Contact No, and Privacy Policy, each with a corresponding input field.

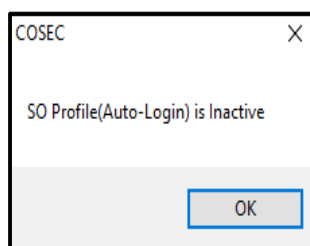
The parameters for configuring this system policy are as follows:

- **Create Activity Logs:** Select to enable the system to create and maintain an audit trail of all login user activity. The audit trail will have details of the login user id, activity date, activity time, key field information and activity description. Wherever applicable, it will also have the old and new values of the edited parameters.

To know more about viewing *Activity Logs*, go to *Admin Module > Views/Logs > Activity Log*.

- **Auto Login to COSEC Monitor:** Enable to allow users to directly login to the Desktop Monitoring application without going through the login process, once they login to the COSEC Web application.

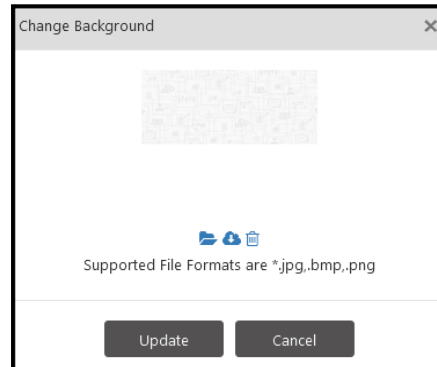
When this check-box is disabled and **SO** login is inactive (default on installation) then on direct login of COSEC monitor utility, following warning will be displayed. clicking on OK will allow to login through **SA** account.



- **System Date Format:** Set the system date format as per the site requirements from the dropdown list.

Change Background

- **Background:** To change, download or remove the background of COSEC Web pages, click on background image. The pop up will open. Browse and select the image to be uploaded and Save from the toolbar. The uploaded image will be applied to the background of Web.



Google API Key

- **Get Location Details:** Select this checkbox to perform Reverse Geo Coding, which is a process of converting a latitude and longitude coordinates into corresponding street address or human readable address using Google Maps. To perform Reverse Geo Coding process, refer [“Get Location Details”](#)
- Enter the **API Key** for displaying location on Google map. The maximum characters for API key are 100.

Multi-Language Parameters

- **Support Multi-language Input:** The users around the world can use COSEC system in their regional languages. So check this box to enable the multi-language input functionality which will enable you to enter the input in your own language.

Data input from server side and device side and storing the same in database will support UTF-8 characters.



Multi-language is not supported in Alert Messages sent via Email/SMS/App Notification.

Multi-language is not supported in Reports generated via Report Builder.

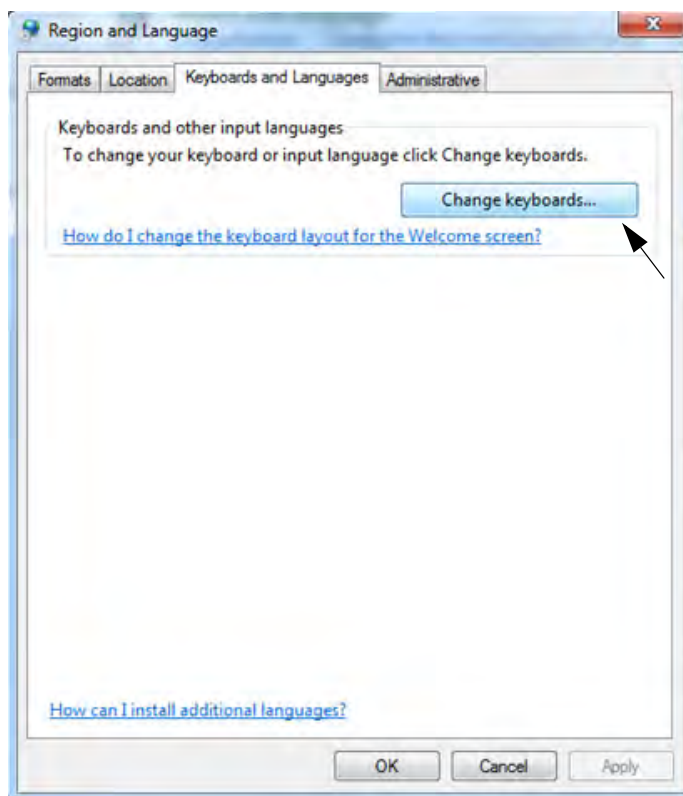
- **Input Alignment:** Select the orientation of multi-language input data from “Left to right” or “Right to left”. **E.g.** If “Right to Left” option is selected, then the input is entered from right side of the text-box and goes to left.

The invalid characters are as follows:

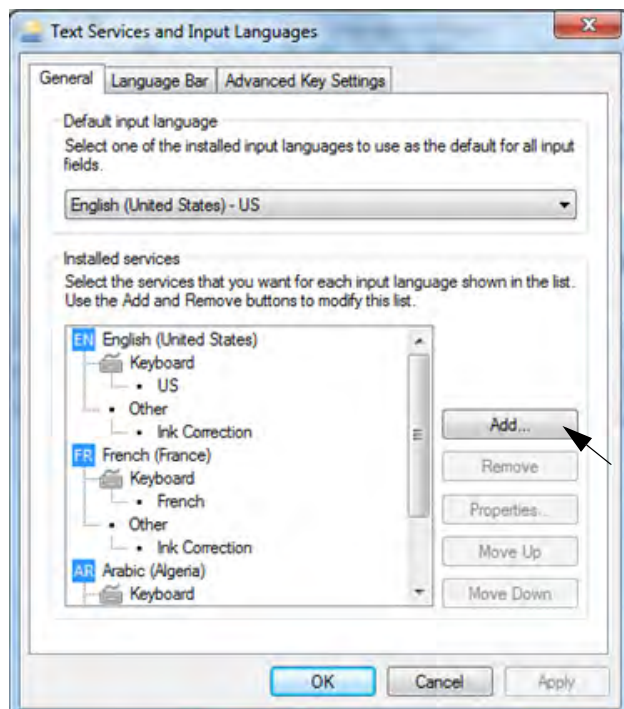
% ^ = ' " { } | ; < > ? & *

To configure the Multi-language input functionality:

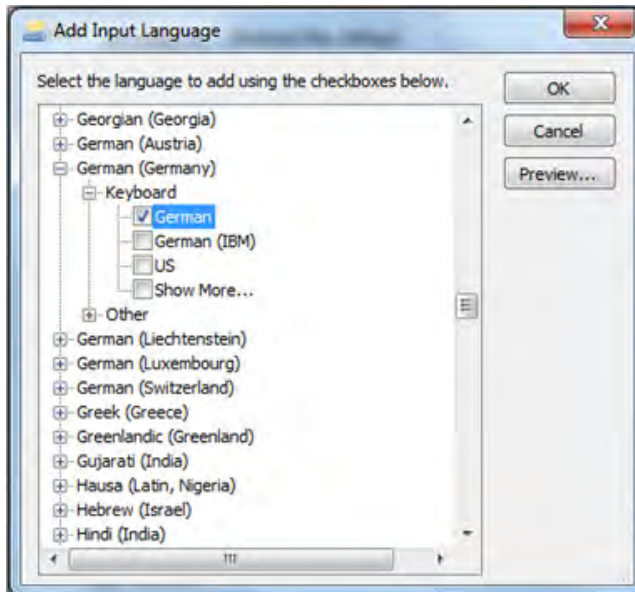
- Go to **Control Panel**.
- Select the “Clock, Language and Region”. Now click on “Change keyboards and other input methods”. The Region and Language window opens as shown below.



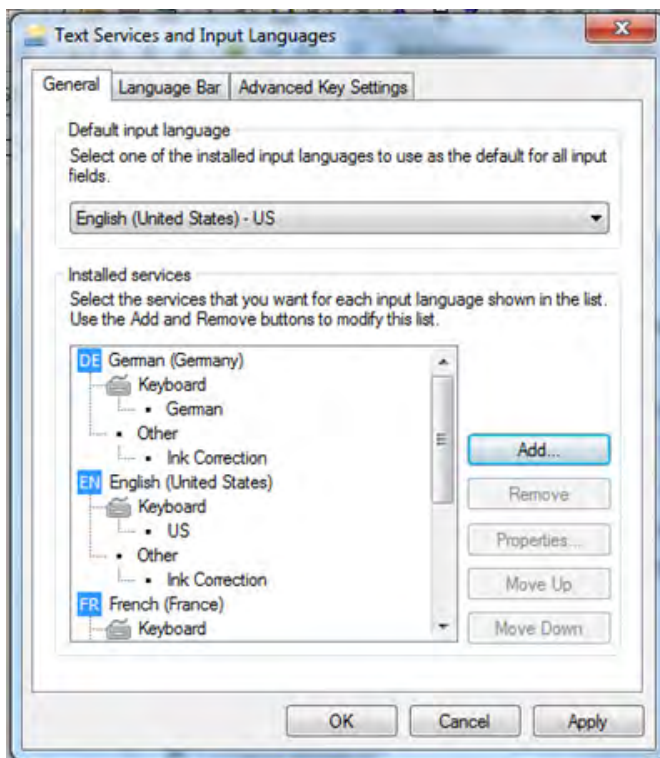
- Click on **Change Keyboards**. The Text Services and Input Languages window appears as shown below.



- Click on **Add** button. The Add Input Language window appears. Select the language to be added in the list. Click OK.



- The German language will be added as shown below.



- Finally click **OK**. The Language bar can be viewed in toolbar as shown below.



- You can select the language as Germany from language bar. The on-screen keyboard will be converted from English to German language

English language Keyboard

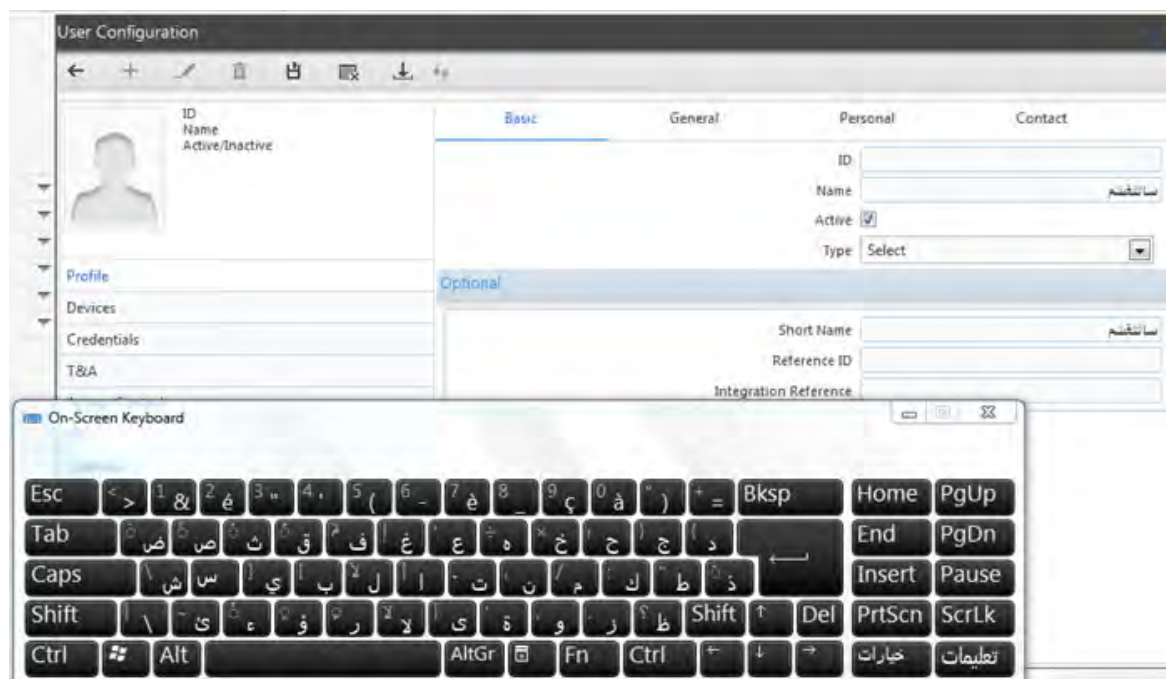


German Language keyboard



Example: The language input is selected as **right to left**. The language is selected as **Arabic**.

The user name is entered through on-screen keyboard in Arabic language as shown below:



Similarly the other parameters can be entered in the desired language.

General Data Protection Regulation

General Data Protection Regulation (GDPR) aims in providing safety and privacy to users¹ data. They limit the access to the users personal data.

By enabling GDPR, the personal information of the users will be masked and the data will be encrypted, accordingly a dummy image shall be displayed in place of the user's profile picture.

The following will be able to View/Edit/Add data:

- System Administrator whether System defined or User defined having the roles and rights of the System Administrator.
- OR**
- System Administrator whether System defined or User defined having rights of View as well as Add/Edit for User Configuration, Worker Profile as well as respective rights of the pages of the Visitor Management Module. For details, refer to ["GDPR Reflections"](#).

1. Users include Workers and Visitors also.

Personal Data Protection: Select the checkbox to impose **General Data Protection Regulation**.



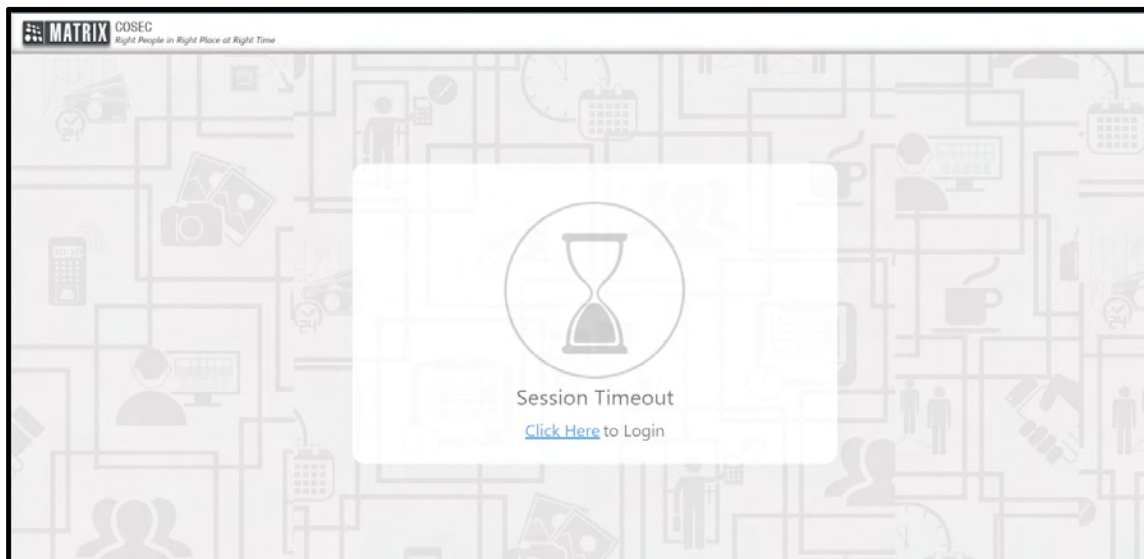
Make sure while enabling/disabling GDPR all the services are running successfully.

Before proceeding with the GDPR process (before enabling), make sure you have taken the backup of the existing database. Refer to Manage Database in the Admin Mgt Portal User Guide.

If you take the backup of the data after enabling GDPR and after the GDPR process is completed, the backup database will be encrypted. We recommend you to take the backup before enabling GDPR.

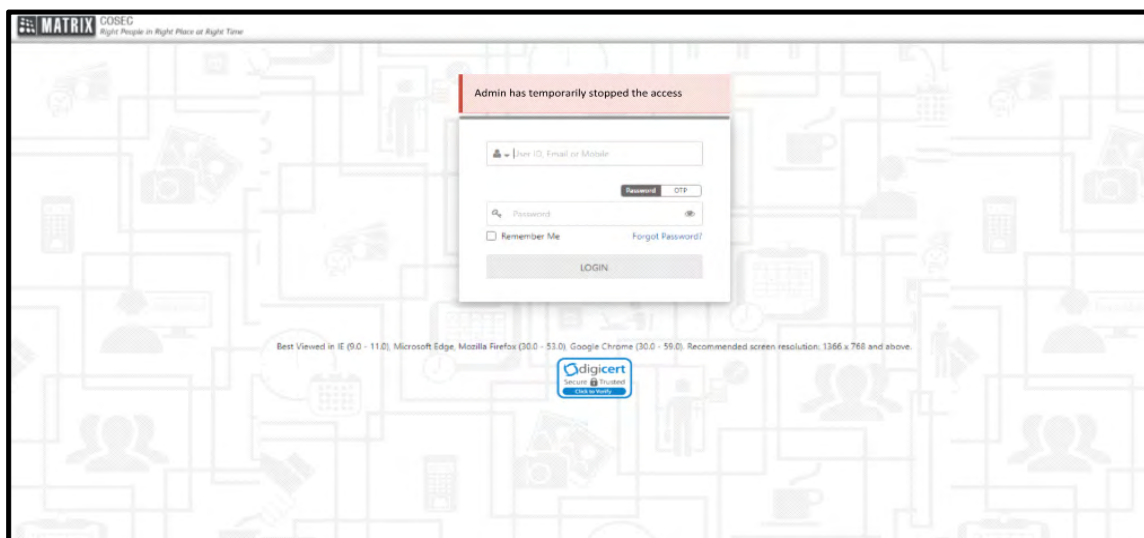
A pop- up stating necessary **Terms and Conditions** appears. Select **Agree** to proceed.

You will be re-directed to the **Session Timeout** page.



To re-login, click on the **Click Here** link.

The following screen appears, if the masking/encryption process is in-progress.



Else, you will be able to login successfully using your credentials and you can continue configuring the GDPR parameters.



Make sure the login details are correctly entered, else login will fail.

It is recommended to restart the IIS, all the services and utilities for swift functioning on successful completion of GDPR Process.

If you encounter a failure during the GDPR Process, the screen will display the error message "Processing Failed. Kindly contact Administrator." or if the GDPR process remains in in-progress state for a prolonged period, there is a provision to Reset the GDPR Process. For details, refer to Company Configuration > Profile > Reset Personal Data Protection Process Flag in the **Admin Mgt Portal User Guide**.

Custom Fields: Select the check box if you desire masking the personal data provided in the customized fields.




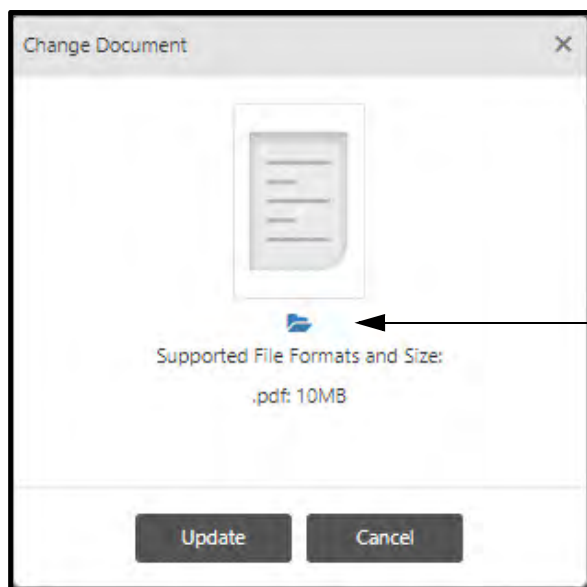
The custom fields masking will be applicable to Users, Visitors and Contractors.

Data Protection Manager


You need to update the details of the Data Protection Manager in this section

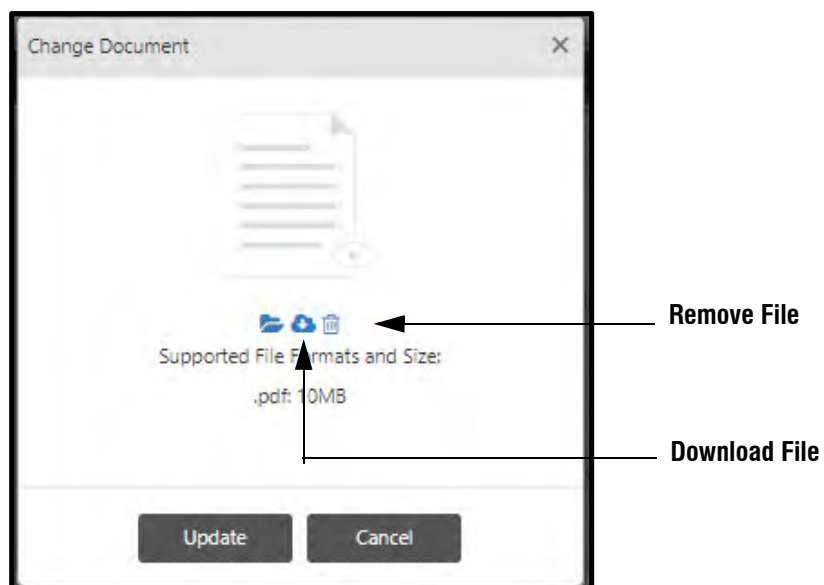
The screenshot shows a web form titled "Data Protection Manager". It contains several input fields for configuration: "Name", "Designation", "Organization Name", "Organization Address", "Email ID", and "Contact No". Each field is represented by a text box. Below these fields is a "Privacy Policy" label followed by an "Upload" icon (a small square with an upward arrow).




- Configure the **Name**, **Designation**, **Organization Name**, **Organization Address**, **Email ID** and **Contact No** of the Data Protection Manager.
- You can upload the **Privacy Policy** if you desire. To do so, click **Upload**  icon. The **Change Document** pop-up appears as shown below.



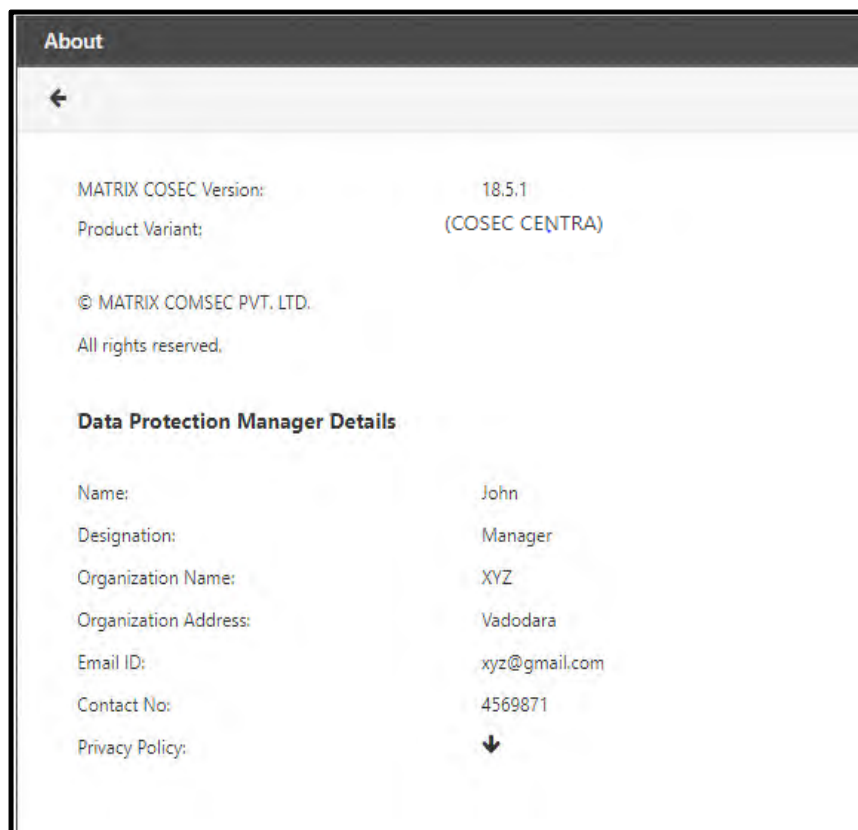
Browse File

- Click **Browse File**  and select the desired file as per the supported formats and size from your local PC.
- Click **Update**.



- After uploading the file, if you wish to upload a different file instead of the current uploaded file, click **Browse File**  again and select the desired file from your local PC. The previously uploaded file will get replaced with the new file.
- To download the uploaded file, click **Download File** .
- To remove the uploaded file, click **Remove File** .
- Then click **Update**.
- Click **Save**

The details of the Data Protection Manager will be displayed in **About**. To view the details, click the **About**  icon on the top bar. To know more, refer [“Using COSEC Web Application”](#)



Enabling GDPR will have an impact on the various modules. For details, refer to [“GDPR Reflections”](#).

For specific module details refer to the links mentioned below.

- [“User Module”](#)
- [“Contract Worker Management”](#)
- [“Time and Attendance”](#)
- [“Visitor Management Module”](#)



To know more about GDPR reflections in Enroll Utility refer, COSEC Enroll User Manual.

Masking will not be applicable for the VMS Web Portal and VMS Utility, only relevant data will be encrypted.

Masking will not be applicable for CSS Web Login as well as ESS/RIC Login, only relevant data will be encrypted.

For ESS/RIC user login, the data will be encrypted and as per the relevant user login the relevant fields will be visible.

For Host user login, relevant data will be masked as well as encrypted. Refer to the ESS manual for details.

User Policy

These policies define the credential limitations for users.

To configure User Policy, go to **Admin module > System Configuration > Global Policy > User** which is shown in next page.

User policy consists of:

- *"Custom Fields"*
- *"Job Costing"*
- *"Sensor Calibration"*
- *"QR Scan Feature"*
- *"Generate User ID"*
- *"Temperature and Symptoms Configuration"*
- *"Invite User"*

Global Policy

Basic

User

Login

Password Policy

Device

Access Control

Time Attendance

Reports

Visitor Management

CWM

Job Costing

Field Visit Management

ESS

SSO Configuration

Save FP Image ☒

Template Per Finger

Single Template/Finger

Maximum No. of Fingers

Two

Fingers On Device Per User

Two

Maximum No. of Palm Templates

Ten

Palm Templates On Device Per User

Ten

Maximum No. of Faces *

10

Self-Enrollment Retry Count *

5

Auto Add/Update Enrolled Face as Profile Photo ☒

Custom Fields

Field No.	Active	Field Name	Type	Upload	Mandatory	
1	Yes	Field 1	Textbox	Yes	No	
2	Yes	Field 2	Textbox	Yes	No	
3	Yes	Field 3	Textbox	Yes	No	
4	Yes	Field 4	Textbox	Yes	No	
5	No	Field 5	Textbox	No	No	

1 - 5 of 10 records

<<

<

1

>

>>

Job Costing

Job Assignment Level

Department

Sensor Calibration

Fingerprint Security Level - Suprema

Level 4

Fingerprint Security Level - Lumidigm

High

Fingerprint Fast Mode ☒

Palm - False Rejection Ratio

Normal

QR Scan Feature

Add/Update User/Worker through Aadhaar Scan ☒

Aadhaar Number Mandatory ☐

Generate User ID

Auto Generate User ID ☐

ID Format *

Numeric Value Length *

0

Zero Padding required ☐

Temperature and Symptoms Configuration

Temperature Configuration

Enable ☒

Temperature Unit

Fahrenheit (°F)

Temperature Threshold *

99.5

Symptoms Configuration

Enable ☒

+

Symptoms	
Fever	
Cough	
Difficulty in Breathing	

Symptoms Threshold

Any one

Warning Message

Message *

Health declaration parameter exceeded threshold. Consult the Doctor

Page Number

The parameters available under User Policy are:

- **Save FP Image:** Enable the checkbox to store the source of your **FP templates** to avoid re-enrollment in case of changes in FP template format.
- **Template Per Finger:** Select the number of template copies to be stored at the DOOR Controllers for each enrolled finger from the drop-down list.

In the event of selecting the Dual Template/Finger option the Door Controllers would maintain an additional copy of the enrolled finger template, which would be updated as and when a change is detected in the fingerprints of the users.



After making changes to this parameter the administrator needs to use the Restore Finger Print Template option from the Configuration tab of the COSEC Monitor application and restore the FPs to all the PANELs and DIRECT Doors.

- **Max No. Of Fingers:** Select the number of fingerprint templates that can be enrolled per user and stored in COSEC database from the dropdown list. One can select maximum 10 fingers.
- **Fingers On Device Per User:** Based on the configured max no. of fingers, select the number of finger templates that will be sent to each device per user. This parameter limits the device to enroll not more than the set number of finger templates.

When the parameter “Fingers on Device per user” is changed, a pop-up is displayed giving a warning message to understand the necessary follow up step needed to be done later.

- **Max No. Of Palm Templates:** This field determines the number of palm templates that can be enrolled per user and stored in COSEC database. You can select maximum 10 palm templates.
- **Palm Templates On Device Per User:** Based on the configured max no. of palm templates, select the number of palm templates that will be sent to each device per user from the dropdown list. This parameter limits the device to enroll not more than the set number of palm templates.
- **Max No. Of Faces:** This field determines the number of Face templates that can be enrolled per user and stored in COSEC database. The valid range for Max No. Of Faces is 1-30.
- **Self-Enrollment Retry Count:** Specify the maximum retry count for self-enrollment. The user gets locked, if the retry count exceeds the limit.
- **Auto Add/Update Enrolled Face as Profile Photo:** Enrolled Image of a User/ Worker/ Visitor can be set as the Profile Photo automatically on successful Face Enrollment.

Select the **Auto Add/Update Enrolled Face as Profile Photo** checkbox to set User/ Worker/ Visitor Profile Photo automatically.

If the checkbox is disabled, then only Manual Photo Upload method will be applicable to set Profile Photo for the User.

**For System Administrator:**

- The system will consider the enrolled face image located at index number 0 of Enroll / VMS Utility to set it as Profile Photo.
- So to update an Enrolled face as Profile Photo, first delete the previously enrolled face image located at index number 0 via Enroll/ Visitor Utility and enroll a new image at the same location.

Custom Fields

- **Field Name 1 - 10:** These are fields that can be customized as per your requirements (e.g. ID Proof, Security Number etc.). These field names will later be available for user/worker configuration on the COSEC Web as well as for ESS application (only for Users). These can also be used for third party integration purposes. The Field Names can be upto 20 alphanumeric characters (space, -, . and “comma” allowed).

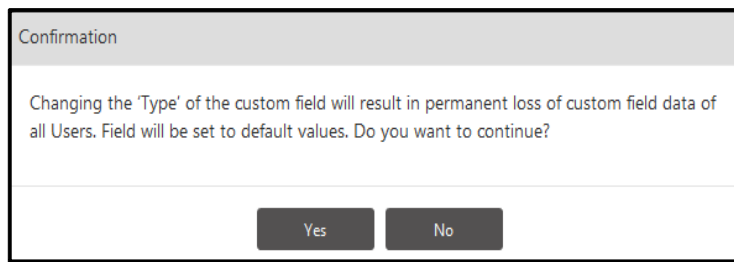
Custom Fields						
Field No.	Active	Field Name	Type	Upload	Mandatory	
1	Yes	Security Number	Textbox	Yes	No	
2	Yes	ID Proof	Textbox	Yes	Yes	
3	Yes	Nominee Name	Textbox	No	Yes	
4	Yes	Field 4	Textbox	Yes	No	
5	No	Field 5	Textbox	No	No	

- **Field No:** It displays the serial number and order of the field.
- **Active:** Select the check-box for this field to be visible in User/ Worker Profile.
- **Field Name:** Enter the desired Name. For example: Security Number.
- **Type:** Select the desired type of the field—Textbox and Date.
- **Upload:** Select the check-box if the configured field requires a provision to upload a document.
- **Mandatory:** Select the check-box for this field to be mandatory.

You can always edit this custom field by clicking the **Edit** button.

Custom Fields						
Field No.	Active	Field Name	Type	Upload	Mandatory	
1	<input checked="" type="checkbox"/>	Spouse Name	Textbox	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Yes	Spouse Birthdate	Date	Yes	No	
3	Yes	Aadhar No.	Textbox	Yes	No	
4	Yes	Field 4	Textbox	Yes	No	
5	No	Field 5	Textbox	No	No	

Click on the **Ok**  button and the pop-up appears.



Click the **Yes** button to save the configuration else click the **No** button.

The configured custom fields for Users will be visible in the **Users> User Configuration> Profile> General**.
The configured custom fields for Workers will be visible in the **CWM> Workers> Worker Profile> Profile> General**.

Job Costing

- **Job Assignment Level:** Selecting an Enterprise Group here will affect Site and Enterprise Group mapping in the **Job Costing And Processing** module. The group selected in *Global Policy* will be applicable to Enterprise Group-specific job assignment on the Site-mapping page.

Sensor Calibration

User Identification can occur from COSEC Enroll application or it can occur on the back end via Identification Server. From the desktop applications, identification is done using an API. To manage all qualities of FP/Palm template, sensor calibration fields must be configured from the Global Policy.

These below fields enable to improve the probability of finding the correct user match for an FP template in cases where there fingerprint mismatch occurs.

- **Fingerprint Security Level- Suprema:** You can select the security level for suprema sensor from the options of Level1 to Level7. The False Acceptance Ratio (FAR) varies as per the selection of levels.
 - For Level 1: FAR is below 1%
 - Level 2: Below 0.1%
 - Level 3: Below 0.01%
 - Level 4: Below 0.001%
 - Level 5: Below 0.0001%
 - Level 6: Below 0.00001%
 - Level 7: Below 0.000001%
- **Fingerprint Security Level- Lumidigm:** You can select the security level for Lumidigm sensor from the options of Lowest to Highest. The default value of security level is set to High.
 - Lowest
 - Low
 - Normal
 - High
 - Highest

If the user is enrolling via Suprema, then Fingerprint Security level- Suprema will be considered for Enroll Utility and VMS Utility.

If the user is enrolling via Lumidigm, then Fingerprint Security level- Lumidigm level will be considered for Enroll Utility and VMS Utility.



1. If existing user has set the security level ≤ 5 , then the user will continue with existing security level.
2. If existing user has set the security level > 5 , then security level will be set to "Highest" in Fingerprint Security level - Lumidigm dropdown.

- **Fingerprint Fast Mode:** Select to enable the fingerprint fast mode. This mode will then be used to identify the user from a template. It will also be considered when Verification button is clicked from desktop application (Enroll) or when Identification feature is involved via Identification API.
- **Palm-False Rejection Ratio:** Select the option as Normal, Highest, High, low or lowest. In COSEC Enroll Palm Identification method will use the value of FRR configured in Global Policy.

QR Scan Feature

This feature allows user to enable the Aadhar Card scanning facility in order to fill up the required details while configuring the users and workers.

QR Scan Feature

Add/Update User/Worker through Aadhaar Scan ☒

Aadhaar Number Mandatory ☐

- **Add/Update User/Worker through Aadhaar Card:** By enabling the check-box, an option for scanning of the 'Aadhar Card QR Code' at user/worker configuration page will become visible.
- **Aadhar Number Mandatory:** Enable the check-box to make the 'Aadhar Card QR Code' scanning mandatory for the configuration of new users.



In CSS module, 'Worker Assignment from CSS' option must be checked On to enable the QR Scan feature for the configuration of CSS Workers.

Generate User ID

User can configure the required format of the User ID and accordingly, the User ID will be generated automatically while configuring a new user. The format can be configured as shown below.

Generate User ID

Auto Generate User ID ☒

ID Format *

Numeric Value Length *

Zero Padding required ☒

- **Auto Generate User ID:** Enable the check-box to make the user id to be generated automatically for the configuration of new users at Users module. If disabled then, the user ID needs to be entered manually.
- **ID Format:** Configure the required format of the ID as by selecting the 'Numeric Value Format' and/or other Value Formats in any order as per the requirement. You can also enter the fixed value which will always print at User ID for every user.

To select the different format for the ID, Enter the * in **ID Format** box and the drop-down list containing different Value format list will appear as shown below. Select the required one from the drop-down list.



The NUMVAL (Numeric Value) is mandatory to be selected.

The drop-down list contains different formats for; Branch Code (BRCCODE), Organization Code (ORGCODE), Branch ID (BRCID), Department ID (DPTID), Numeric value (NUMVAL) etc. You can select the multiple formats by entering * after choosing the one.

Example:

As shown in above image, the fixed value 'MATRIX' is entered as a company name, BRCID and DPTCODE is selected which can vary as per the assigned 'Branch' and 'Department' for new configured users. The NUMVAL is selected which will provide a unique 'Numeric number' at the end of the ID.

Now, at the user configuration page while configuring the new (say first) user, the Branch is assigned as 4 (say Waghodia) and the Department is assigned as Documentation.

So, once the user is configured and saved, the unique User ID **"MATRIX4DOC1"** will get automatically generated and assigned. **[MATRIX4DOC1]**

[Fixed Value, Branch ID, Department Code, Numeric Value]



Numeric Value for each User ID will generate as per the next available number.

- **Numeric Value Length:** Enter the desired quantity of the digits from 1 to 15 till which the 'NUMVAL' will be generated. For example: 4

- **Zero Padding Required:** Enable the check-box to allow the addition of zeros before the 'NUMVAL' value to satisfy the Numeric value length.

For Example: As explained in above example, the new user id is supposed to be generated as 'MATRIX4DOC1' then by enabling Zero Padding, it will generate as 'MATRIXDOC0001' to fulfill the numeric value length=4.

Click on the **Save** button to save the configuration.

Temperature and Symptoms Configuration

This feature allows to configure the "Temperature" and "Symptoms" parameters for users. The configured parameters will be compared with the 'Health Parameters' declared by a user (*in Users > Utilities > Health > Health Declaration*) according to which, an Alert and a Warning Message will be generated if required.

• Temperature Configuration

Check the **Enable** box **On** to configure temperature parameters as shown below.

Temperature Unit: Select unit of the temperature from the drop down list. The options are '**Fahrenheit**' and '**Celsius**'.

Temperature Threshold: Define the threshold (maximum) temperature value, beyond which a warning message and an alert should be generated for a user if configured.

For Example: The specified Temperature Threshold = '99.8 Fahrenheit' and if the user's self declared value is equal to or greater than 99.8 Fahrenheit, then a warning message and an alert will be generated.

The screenshot displays the 'Global Policy' configuration window. On the left is a sidebar menu with options: Basic, User (selected), Login, Password Policy, Device, Access Control, Time Attendance, Reports, Visitor Management, CWM, Job Costing, Field Visit Management, ESS, and SSO Configuration. The main area is titled 'Temperature and Symptoms Configuration' and contains two sections:

- Temperature Configuration:**
 - Enable:** A checkbox that is checked (blue square).
 - Temperature Unit:** A dropdown menu set to 'Fahrenheit (°F)'.
 - Temperature Threshold:** A text input field containing '99.5'.
- Symptoms Configuration:**
 - Enable:** An unchecked checkbox.
 - Symptoms:** A table with three rows: 'Fever', 'Cough', and 'Difficulty in Breathing'. Each row has edit and delete icons to its right. A '+' button is at the top right of the table.
 - Symptoms Threshold:** A dropdown menu set to 'Any one'.
- Warning Message:**
 - Message:** A text input field containing 'Health declaration parameter exceeded threshold. Consult the Doctor'.

• Symptoms Configuration

Check the **Enable** box **On** to configure symptoms parameters as shown below.

Symptoms: This field enables to define a new symptom. The configured symptoms will appear for users in order to declare their health status.

To add a new symptom, click on the **Add** button and specify the symptom name. For example: Fever, Cough
Symptoms can be edited/renamed by **Edit** option and can also be removed permanently by **Delete** button.
Click on the **Save** button to save the added/edited symptom or **Discard** button to cancel the symptom.

Symptoms Threshold: Select the required threshold value from the drop-down list.

A warning message and an alert will be generated if the number of symptoms declared by the user is equal to or greater than the predefined symptoms threshold.



User will be notified by an Alert if the declared temperature and/or symptoms value is equal to or exceeding the predefined threshold values. Also an alert will be generated for a user only if it is configured in Admin > System Configuration > Alert Message Configuration.

For ESS/Mobile Application users the Health Module will be visible only if the user is assigned the right for the same. Refer [“ESS Role Rights”](#) for details.

Warning Message: Enter the warning message which is to be displayed, if the Temperature and/or Symptoms parameters declared by the user reaches/exceeds the predefined threshold value.

Invite User

Invite User enables you to pre-determine the information that you need to collect from the on boarding employees prior to their physically joining the organization. To know more refer [“Invite User”](#), Users>Utilities> Invite User.

After you determine the parameters a link will be sent to the on boarding employee to collect the information.

To determine the desired parameters:

- Click **Invite User** collapsible panel.

Parent Name	Field Name	Active	Mandatory
Basic	Profile Photo	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Basic	Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Basic	Full Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Basic	Short Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Basic	Face Image	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
General	Date of Birth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
General	Joining Date	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
General	Vehicle Registration No.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
General	Driving License	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
General	Passport No.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- **Link Expiry:** Enter the number of days after which the link will expire.
- A list of default parameters that will be sent to the on boarding employee will be displayed. You can customize the parameters as per your requirement.

- Select the respective **Active** check boxes of the desired parameters. Only Active parameters will be visible in the link.
- If you wish to make the parameter compulsory, select the **Mandatory** check box.
- Here, you can also add customize fields as per your requirement. Refer to [“Custom Fields”](#). (Admin module > System Configuration > Global Policy > User > Custom Fields)

Login Policy

These policies define the time till which the users can login to the system.

To configure Login Policy, go to **Admin module > System Configuration > Global Policy > Login** and the following screen appears.

Following are the parameters for configuration under Login Policy:

- **Login Policy:** Enable to allow administrator for enforcing the login policy for the system. If enabled the system will limit the period for which the user does not login to the system.
 - This period is specified in the **Maximum Days allowed without Login** parameter. If the user does not have successive logins within the period as specified then the user account is disabled.
- **Restrict ESS Local Login:** Select this check box to restrict the ESS Local Login for the Users.
- **Login via SSO:** Select this check box to enable the user to login into the ESS via SSO and/or for the System Account User to login via SSO. Configure the following parameters:
 - **SSO Certificate (.pfx):** Click **Choose File** and select the certificate to be uploaded from the local PC.
 - **Password:** Enter the password for accessing the certificate.

For Login via SSO to function, make sure you have configured the parameters — ACS Endpoint and ACS Logout Endpoint under IDP Configuration. For details of the SSO and IDP parameter configurations, refer to [“SSO Configuration”](#).



The System Administrator will not be able to Login via SSO in APTA.

- **Login Via Active Directory:** Select this check box, to enable ESS enabled users to login using their active directory credentials for COSEC Centra.
- **Secure Connection:** Select this checkbox to enable secure connection with the Active Directory Server.
- **Active Directory Server Address:** Specify the IP Address or the network name of the Domain Controller along with the port number, if configured.
- **Domain Name:** Specify the domain name here. For e.g. if the domain name is matrix.com the domain name is specified as: dc=matrix,dc=com.
- **Enable Notification:** Select this checkbox to enable notifications to be sent to a user on ESS.
- **RSA Key Size:** Specify the Key size to generate a public encryption key for securely sending credentials from a third party application using RSA encryption (for *Direct Login to ESS*). Select the key size from the dropdown list and click the **Generate Key** button to generate the public key **modulus** as shown below.

RSA Key Size	512	Generate Key
Modulus	2DORRZ5uhdTkeQB4f2KYw+4eYwBsf3VomxpZ7 YrBPpyNQk/7d9Mc371KJ+PJrsX /o9wISKGcEhKEIF5KNaLX3qcKEVOz1bh0n5IwHSi2 +fg9/C9CWXS3RJPc/sF+BNr	
Exponent	AQAB	



The higher the RSA Key Size, the more secure is the transmission.



Once a new key is generated from this page, all data that was encrypted using the previous key, will not be decrypted.

- **Login Authentication Mode:** Select the option to allow users to login into system via Password, Password OR OTP or Password Then OTP.

Login Authentication Mode	<div> Password OR OTP </div> <div> Password Password OR OTP Password Then OTP </div>
---------------------------	--

If **“Password OR OTP”** or **“Password Then OTP”** is selected; then you must configure OTP generated Alert in Alert Message Configuration to get OTP on SMS and or Email. And hence SMS Configuration and or Email Configuration must be done.

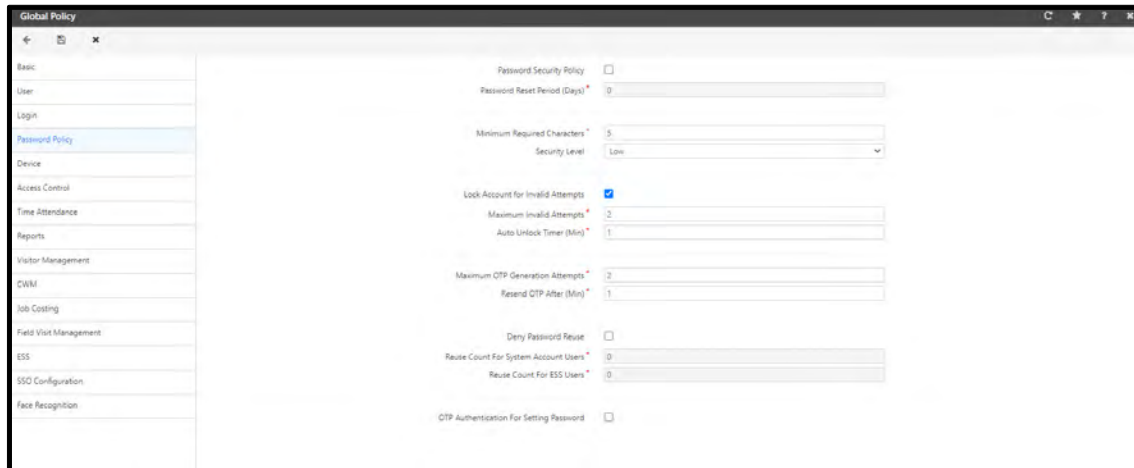
- **Skip OTP:** You can select the number of times for which OTP will be skipped when **“Password Then OTP”** is selected.

Login Authentication Mode	Password Then OTP	▼
Skip OTP	2	▼ (times)

Password Policy

This page allows to define policies for password.

To configure Password Policy, go to **Admin module > System Configuration > Global Policy > Password Policy** and the following screen appears.



The screenshot displays the 'Global Policy' configuration window with the 'Password Policy' tab selected. The settings are as follows:

- Password Security Policy:** ☐
- Password Reset Period (Days):** 0
- Minimum Required Characters:** 5
- Security Level:** Low
- Lock Account for Invalid Attempts:** ☒
- Maximum Invalid Attempts:** 2
- Auto Unlock Timer (Min):** 1
- Maximum OTP Generation Attempts:** 2
- Resend OTP After (Min):** 1
- Deny Password Reuse:** ☐
- Reuse Count For System Account Users:** 0
- Reuse Count For ESS Users:** 0
- OTP Authentication For Setting Password:** ☐

- **Password Security Policy:** Enable to enforce the Application user to change password after the expiry of configured period as specified in the **Password Reset Period (days)** field.
- **Minimum Required Characters:** Specify the minimum character count that is mandatory for setting a new password for any user account. Valid range is 5-45.
- **Security Level:** There can be 3 security levels allowed for setting a password:
 - **Low:** No restriction. All characters allowed in password.
 - **Medium:** 1 lowercase (a-z) character and 1 number (0-9) mandatory in password.
 - **High:** 1 uppercase (A-Z) character, 1 lowercase (a-z) character, 1 number (0-9) and 1 special character (` ~ ! @ # \$ % ^ & * () - = _ + [\] | ; ' : " , . / < > ?) mandatory.
- **Lock Account For Invalid Attempts:** Enable this check-box to lock a user account after a certain number of consecutive failed login attempts.
- **Maximum Invalid Attempts:** Specify the maximum number of invalid attempts after which the account will get locked for the time specified in "Auto Unlock Timer". Valid range is 1-15.

If Login Authentication Mode is set as Password or OTP/ Password Then OTP in Global Policy> Login tab; then Invalid Login Attempts count will be incremented when wrong password or wrong OTP is entered. When this count reaches "Max Invalid Login Attempts" then account will get locked.

- **Auto Unlock Timer (Min):** Specify the time in minutes after which the locked user account will be automatically unlocked or you can request the system administrator to reset the password. Valid range is 0-999.



*While configuring **Auto Unlock Timer (Min)**, do not specify the value as 0. If you specify the value as 0, the account will be permanently locked and to unlock the account you will have to contact the **Support Team**.*

- **Maximum OTP Generation Attempts:** Specify the maximum number of invalid attempts to regenerate/ resend OTP for Forgot Password, Login and/or Password Setting. Valid range is 0-15.



*If the value of **Maximum OTP Generation Attempts** is configured as 0, then users will have infinite OTP generation attempts.*

- **Resend OTP After (Min):** Specify the time in minutes after which the user will be able to regenerate OTP after **Maximum OTP Generation Attempts** are over. Valid range is 1-999.
- **Deny Password Reuse:** Enable to restrict a user from setting a new password that is same as a specific number of previously used passwords.
- **Reuse Count for System Account Users:** Specify the count of previously used passwords for System Account users. E.g.: If Reuse count for a System Account user is set to “3”, then a new password cannot be same as either of the last three used password.
- **Reuse Count for ESS Users:** Specify the count of previously used passwords for ESS users. E.g. if Reuse count for an ESS user is set as “2”, then a new password cannot be same as either of the last two used passwords.
- **OTP Authentication For Setting Password:** Select to enable OTP authentication for setting password. If enabled, the ESS user has to go through OTP Authentication for setting password while logging in for the first time in his/her ESS account.

Process

Ensure that Email ID / mobile number of the ESS user is available and entered in Contact Details of User Configuration. And Receive Alerts on Mobile/Email is enabled.

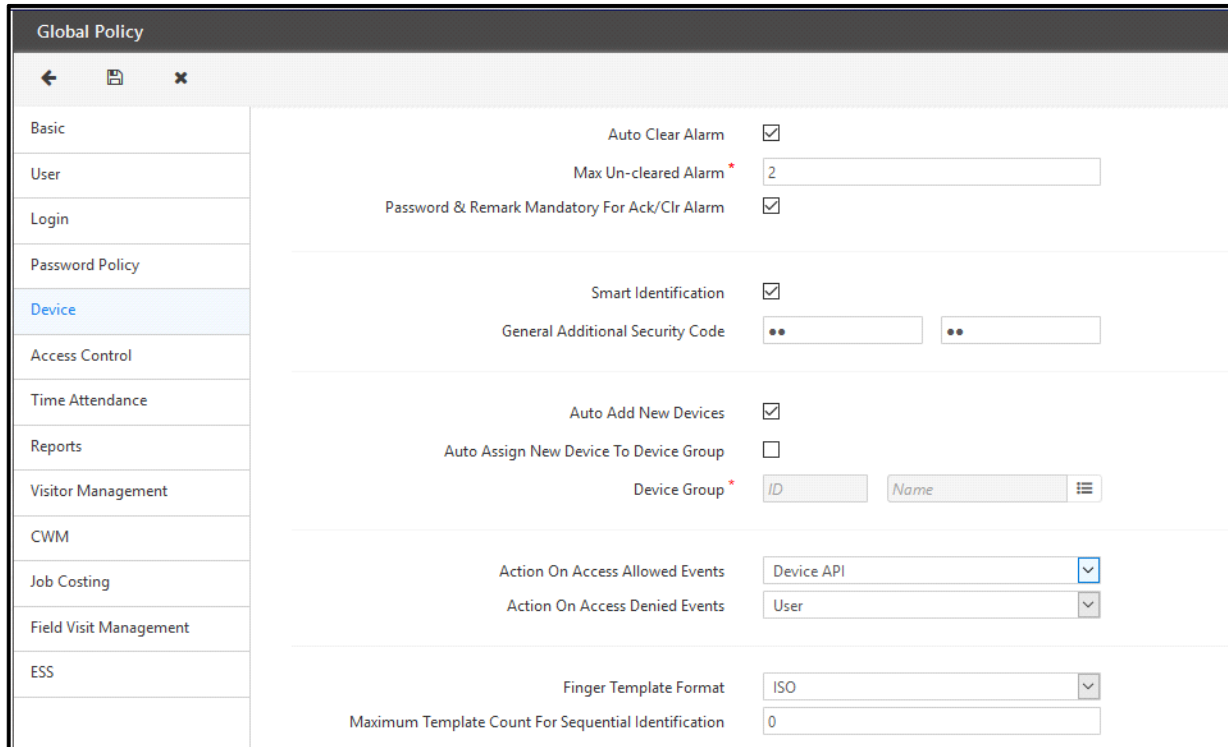
The Alert Message Configuration for SMS/Email for System Alert Event “OTP Generated” must be enabled. See “Configuring Alert Messages”.

To receive OTP on SMS, you have to do SMS setting and to receive OTP on Email, you have to do Mail Setting in The Alert service must be started for sending Email and SMS notification.

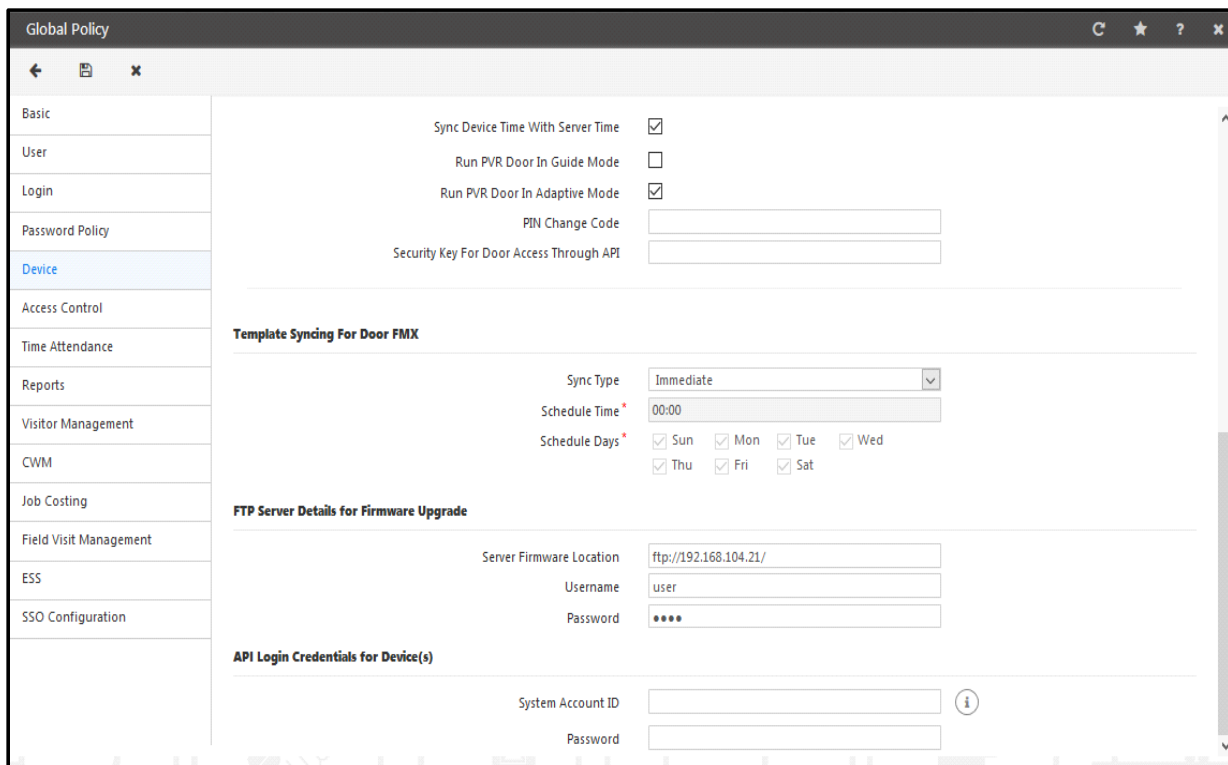
Device

This page allows to define policies for device.

To configure Device Policy, click **Admin module > System Configuration > Global Policy > Device** and the following screen appears.



Basic	Auto Clear Alarm	<input checked="" type="checkbox"/>
User	Max Un-cleared Alarm *	2
Login	Password & Remark Mandatory For Ack/Clr Alarm	<input checked="" type="checkbox"/>
Password Policy		
Device	Smart Identification	<input checked="" type="checkbox"/>
Access Control	General Additional Security Code	•• ••
Time Attendance	Auto Add New Devices	<input checked="" type="checkbox"/>
Reports	Auto Assign New Device To Device Group	<input type="checkbox"/>
Visitor Management	Device Group *	ID Name
CWM		
Job Costing	Action On Access Allowed Events	Device API
Field Visit Management	Action On Access Denied Events	User
ESS	Finger Template Format	ISO
	Maximum Template Count For Sequential Identification	0



Basic	Sync Device Time With Server Time	<input checked="" type="checkbox"/>
User	Run PVR Door In Guide Mode	<input type="checkbox"/>
Login	Run PVR Door In Adaptive Mode	<input checked="" type="checkbox"/>
Password Policy	PIN Change Code	
Device	Security Key For Door Access Through API	
Access Control		
Time Attendance		
Reports		
Visitor Management		
CWM		
Job Costing		
Field Visit Management		
ESS		
SSO Configuration		

Template Syncing For Door FMX

Sync Type	Immediate
Schedule Time *	00:00
Schedule Days *	<input checked="" type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat

FTP Server Details for Firmware Upgrade

Server Firmware Location	ftp://192.168.104.21/
Username	user
Password	****

API Login Credentials for Device(s)

System Account ID	
Password	

Auto Clear Alarm: Select this check box, if you wish to Auto Clear the Alarms triggered on the devices connected into the system.

Maximum Un-cleared Alarm: Specify the number of Alarms which will be kept uncleared on the devices connected into the system.

Let us understand this with an example:

The number of **Maximum Uncleared Alarm** is set at 2 and total devices connected are 10. Any device alarm gets activated and after sometime the second device alarm also gets activated. Now, when any third device alarm gets activated, then the first device alarm will get deactivated automatically.

Password & Remark Mandatory For Ack/Clr Alarm: Enable this option if password and remark is to be provided mandatory for acknowledging or clearing an alarm.

Smart Identification: Select to enable the Smart Identification (SI) functionality at the system level. Under this functionality, users defined in the system are assigned smart cards by enrolling at the [“COSEC Enrollment station”](#). Access to these users is granted based on the information written on the smart cards.

General Additional Security Code: To take the security level a step higher, an Additional Security Code can be added. This Additional Security Check is possible only with Smart Cards which will prevent the duplicacy of card and restrict unauthorized access to the facility. Configure the Additional Security Code (ranging from 1 to 65535) and Re-enter the code to confirm.



SI and ASC feature will work independently.

However, the user needs to ensure that the functionality is enabled at the device level. It is essential to install either a Mifare or an HID i-Class serial reader at the Door devices for this functionality to work. SI users need not be assigned any devices and need to be enrolled from the COSEC ENROLL application only.

COSEC Enrollment station



Auto Add New Devices: Enable to automatically add new devices on the COSEC system on first-time detection.

The devices will be added but will be inactive. To connect the device to the network enable the Active checkbox in Device > Device Configuration > Profile of the desired devices.

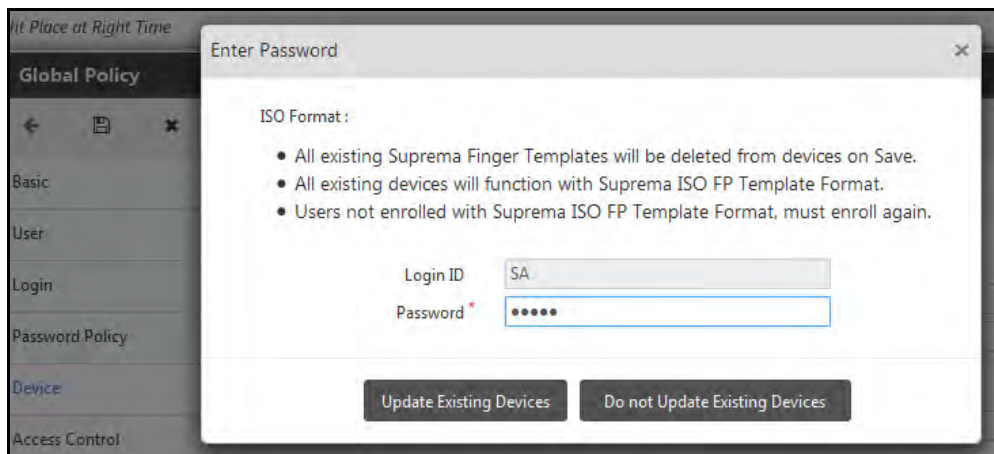
Auto Assign New Device To Device Group: Select to enable the system to automatically assign any auto-added device to a specified device group.

Device Group: Select and specify a device group by clicking the device group picklist button, to which the system can automatically assign auto-added devices.

Action On Access Allowed Events: Select the event types as **All, User, Devices API** whose occurrence will trigger actions as per IO Linking and Satatya Integration configuration defined in the COSEC Web Application. See *Device Configuration > Video Surveillance and Input/Output* for details.

Action On Access Denied Events: Select the event types as **All, User, Devices API** whose occurrence will trigger actions as per IO Linking and Satatya Integration configurations defined in the COSEC Web Application.

Suprema/Lumidigm Finger Template Format: COSEC Devices, by default, support a proprietary format for fingerprint templates. However, users also have the option to switch to the ISO format in Global Policy for saving templates. Changing from Proprietary to ISO format (and vice versa) will remove all existing fingerprint templates from the COSEC database and devices on saving, and finger enrollment for all users must be done again. Login credentials are required to save any changes in finger template format.



Maximum Template Count for Sequential Identification: This allows configuring Maximum Template Count on global level for all devices (PVR as Direct Door).

Device has a limited memory capacity for storage of templates so we need Identification Server which will store the more number of templates and respond to device when asked for identification.

The Identification Server is connected to many device. At a time, many device will request the Server for identification and the response by the server will consume more time. So at a small installation site with less number of users; your device locally can respond for the Identification.

Specify the “Maximum Template Count for Sequential Identification” as the maximum number of templates upto which identification will be done locally through device after which request is forwarded to the Identification Server.

Example:

- Suppose 10 templates are stored at device, and “Max Template count for Sequential Identification” set value is 60. When user punches on device, his template will be identified locally from the device first. If he is not identified by 10 templates, then identification will be done from server.
- Suppose 10 templates are stored, and Max Value is 8. Then Identification is done through both device and server.

Sync Device Time with Server Time: This parameter enables the system to synchronize the system time of the COSEC Monitor computer with that of the connected devices. This is enabled by default.

Run PVR Door in Guide Mode: PVR doors can be used with or without hand guides, depending on which, the enrollment and identification of palm credentials vary. Hence, COSEC enables the system administrator to run the

PVR in two modes, the Guide Mode and the Non-guide mode (default mode). Palm templates are saved and identified by the device differently, depending on the mode selected.

The **Run PVR Door in Guide Mode** check-box is available only to login users with system administrator rights. Enable this option to remove all existing palm templates from COSEC and for all future palm enrollment and identification to be performed in the Guide mode only. On saving this option, the system administrator will be prompted to enter his login credentials for authentication as displayed below.

Auto Assign New Device To Device Group ☒

Device Group * 1 Device Group-RnD

Run PVR Door In Guide Mode ☒ All existing palm templates will be deleted. Palm enrollment must be done again for all users. Note : All PVR Doors will re-boot.

Enter Password

PVR Guide Mode :

- All existing palm templates will be deleted.
- Palm enrollment must be done again for all users.
- All PVR Doors will re-boot.

Login ID SA

Password *

Update Existing Devices Do not Update Existing Devices

Run PVR Door in Adaptive mode: Enable the check-box to run the PVR door in an Adaptive mode. In this mode, the new enrolled 'Palm Templates' will allow to be saved into the 'Smart Card' for the enrollment type; 'Smart Card' / 'Biometric then Card', which is selected in **User module > Enrollment**. The users will then allow to be identified by their Palm Credentials through the smart card if configured.



Mifare 4K smart card is mandatory for the Palm Template to be saved.

If 'Run PVR in Adaptive Mode' checkbox is disabled then also the previously saved (compressed) Palm Templates will remain present into the COSEC Server.

PIN Change Code: Enter the PIN Change Code which will be used by the employees to change their own code.

Example: If PIN change code is 11 and employee code is 1220 which is required to be changed to 1320 then you have to enter 11 on device. Then you will have to enter old code as 1220 and new code as 1320. If new PIN is unique, then it will be updated.

Security Key For Door Access Through API: This is required, to get access on door through APTA/MODE Application. That is, it is required for authenticating the API.

Template Syncing for Door FMX

PIN Change Code	*****
Security Key For Door Access Through API	

Template Syncing For Door FMX

Sync Type	Immediate
Schedule Time *	00:00
Schedule Days *	<input checked="" type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat

Sync Type: Select the template sync type option as **Immediate** or **Scheduled**.

In **Immediate** option, the templates will get sync from server to device immediately with the enrollment. The user template will be identified immediately.

In **Scheduled** option, the templates will get sync from server to device based on the **schedule Time** and **Schedule Days**. The enrollment of the template will be done but the identification will be done once the template gets synced.

FTP Server Details for Firmware Upgrade

FTP Server Details for Firmware Upgrade	
Server Firmware Location	ftp://matrixtelecomsolutions.com
Username	cosecforread
Password	*****

Server Firmware Location: It is the location of FTP where device firmware files would be available for upgrade.

- For **COSEC VYOM**; default location is ftp://matrixtelecomsolutions.com.
- For **COSEC CENTRA** you can specify the desired FTP path. For this you have to create the folder structure for keeping Firmware files on FTP path. You must specify the URL path up- till COSEC_ DEVICE folder. i.e. if your COSEC_ DEVICE folder is at path ftp://192.168.107.15/Softwares/COSEC_DEVICE then your URL would be ftp://192.168.107.15/Softwares

[See “Example: Firmware upgrade from FTP” on page 1169. on Device Status page.](#)

The folder structure for keeping Firmware files on FTP path is:

```
COSEC_DEVICE_NEW > GateController > CENTRA
COSEC_DEVICE_NEW > NGT > CENTRA
COSEC_DEVICE_NEW > PVR > CENTRA
COSEC_DEVICE_NEW > FMX > CENTRA
COSEC_DEVICE_NEW > WirelessDoor > CENTRA
COSEC_DEVICE_NEW > V3 > CENTRA
COSEC_DEVICE_NEW > V4 > CENTRA
COSEC_DEVICE_NEW > VegaPanel200 > CENTRA
COSEC_DEVICE_NEW > VEGA > CENTRA
COSEC_DEVICE_NEW > V4 > CENTRA
```


COSEC_DEVICE_NEW > PathV2 > CENTRA
COSEC_DEVICE_NEW > ARCDC200 > CENTRA
COSEC_DEVICE_NEW > VegaPanel200BLE > CENTRA
COSEC_DEVICE_NEW > ARGO > CENTRA
COSEC_DEVICE_NEW > ARGOFACE > CENTRA



Before trying to Update Firmware for Centra (OnPremise Solution) above mentioned folder structure must be available on client side.



The file structure is Case Sensitive. So the folder structure must be created as specified.

User Name: Enter the Username for accessing the FTP location in COSEC CENTRA. For COSEC VYOM default Username is cosecforread.

Password: Enter the password for accessing the FTP location in COSEC CENTRA. For COSEC VYOM default password is Cosec@341



The valid values for above three fields are

A-Z

a-z

0-9 !\"#\$%&'()*+,-./:;<=>?@[\]^_`{|}~

API Login Credentials for Devices

This section enables to configure the API login credentials for the system account user and the same credentials can be used by devices. Only SA user can configure these parameters.

System Account ID: Enter the ID of system account type of user for whom API access is enabled. You can enable API access for a user from *Admin module > System Accounts > Optional*.

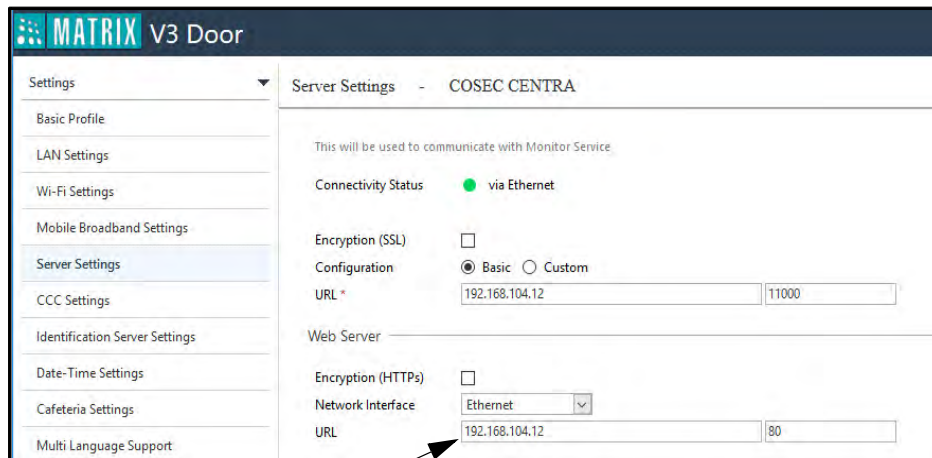
Password: Enter the password of the system account user with minimum 128 characters.

For APIs other than e-Canteen Account details; you have to enter the System Account ID and Password. Thus, whenever API is fired, if API's credentials don't match with the configured ID password in the global policy, then the request will get denied.



If the System Account ID or Password are changed (refer "[Managing System Accounts](#)"), then these changes will not be reflected in API Login Credentials for Devices automatically. You need to update the changes manually.

If System Account ID and Password are not entered, then only e-Canteen Account Details API will work. For getting Cafeteria Account details the URL of COSEC server must be specified in Web Server section of device webpage as shown below.



The screenshot displays the 'MATRIX V3 Door' web interface. On the left, a sidebar lists settings categories: Settings, Basic Profile, LAN Settings, Wi-Fi Settings, Mobile Broadband Settings, Server Settings (highlighted), CCC Settings, Identification Server Settings, Date-Time Settings, Cafeteria Settings, and Multi Language Support. The main content area is titled 'Server Settings - COSEC CENTRA'. It includes a note: 'This will be used to communicate with Monitor Service.' Below this, the 'Connectivity Status' is shown as 'via Ethernet' with a green dot. The 'Encryption (SSL)' checkbox is unchecked. The 'Configuration' section has 'Basic' selected with a radio button. The 'URL' field is set to '192.168.104.12' and the port is '11000'. The 'Web Server' section has 'Encryption (HTTPs)' unchecked, 'Network Interface' set to 'Ethernet', and the 'URL' field set to '192.168.104.12' with port '80'. An arrow points to the 'URL' field in the Web Server section.



In COSEC VYOM, Encryption in Web Server is must to enable to fetch the account details in API.

Access Control Policy

This page allows to define policies for access control.

To configure Access Control Policy, go to **Admin module > System Configuration > Global Policy > Access Control** and the following screen appears.

Smart Card Based Access Route: Select to enable access route based on smart card. For further configuration refer **Access Control Module > Smart Access > Smart Access Route** page

Access Route Type: If Smart Card Based Access Route is enabled, select the Access Route type as incremental by selecting **Level 0 is lowest level** and decremental by selecting **Level 0 is highest level**.

Smart Card Key Settings

You can either use the default Matrix Key for Smart Cards or customize the Smart Card key. You can change the Smart Card key as many times as you want or revert to the default Matrix Smart Card key.

You can define two custom keys—one for HID and one for MIFare cards. To use a custom key, select the type of Smart card to be used and enter the desired key in hexadecimal digits.

Customize HID iClass Card Key

Check the box to enable HID iClass Card Key configuration.

Enter **16 Digit Hexadecimal Key** as a custom key which will be used for all the sectors of Card.

Select the **Auto Update Key Change On Cards** check box to update all Smart Cards with the new (custom) key, when they communicate with the devices connected with COSEC.



Auto Update Key Change On Cards checkbox will be enabled only if “Customize HID iClass Card Key” / and “Customize MiFare Card Key” checkbox is enabled.

Customize MiFare Card Key

Check the box to enable Mifare Card Key configuration.

Card Type: You can select the Card type as **MiFare 1K** or **MiFare 4K**.

Key Type: You can select the Key type as **Global** or **Sector-Wise**.

For Global Key-Type:

All the sectors of card will be assigned same key.

Enter **12 Digit Hexadecimal Key** as custom key for the selected MiFare Cards.

For Sector-Wise Key-Type:

Smart cards are used for multiple purposes like storing user details for access control, his cafeteria details etc. So, in-order to ensure that all the information in card is not getting vulnerable to security threats like unauthenticated data access, different keys for different sectors of smart cards can be defined.

Save Sector-Wise Keys in DB: If this checkbox is **enabled**, configured sector-wise key sets will be saved in database and simultaneously sent to devices as commands.

If this checkbox is **disabled**, configured sector-wise key sets will not be stored in database but will be sent to devices as commands. If there are any old sector-wise keys' in database, then it will be removed.



If there are no keys saved in database, then COSEC Utilities (VMS, Enroll) will work with Default Keys for all the sectors. (FFFFFFFFFFFF).



Sector-wise configuration of keys in MiFare cards is supported in following Direct Doors:
Wireless Door, Door V3, Door V4, NGT Direct Door, PVR Door, Vega Controller and Door FMX.

Configuring sector-wise keys for different sectors.

Customize MIFare Card Key <input checked="" type="checkbox"/>										
Card Type	MiFare 1K									
Key Type	Sector-Wise									
Save Sector-Wise Keys in DB <input checked="" type="checkbox"/>										
Search										
Start Sector	End Sector	Key A						Read Using	Write Using	
8	12	D	E	2	4	A	3	Key A	Key A	✓ ✕
		A	F	C	0	8	F			

Start Sector: Select the starting sector of card. If Card type selected is Mifare 1K; then you can select from 0 to 15 sectors for defining key. If Card type selected is Mifare 4K; then you can select from 0 to 39 sectors for defining key.

End Sector: Select the ending sector of card. If Card type selected is Mifare 1K; then you can select from 0 to 15 sectors for defining key. If Card type selected is Mifare 4K; then you can select from 0 to 39 sectors for defining key.



The End Sector will be always greater than or equal to the option value selected in Start Sector.

Key A: Enter the Custom key value in hexadecimal format (0 to 9 & A to F)

Read Using: This field displays Key A as default. The hexadecimal Key A will be used for reading the selected Mifare card.

Write Using: This field displays Key A as default. The hexadecimal Key A will be used for writing on the card.



1. If Key is kept blank, then the grid will show as blank for the corresponding key.

2. If previously key is defined for sector 0 to 10 and new key is defined for sector 8 to 12. Then the new key will be assigned to sector 8 to 12. And the previous key will be marked for sector 0 to 7. *See below image.*

3. If previously key is defined for sector 0 to 10 and new key is defined for sector 3 to 8. Then the new key will be assigned to sector 3 to 8. And the previous key will be marked for 0 to 2 and 9 to 10.

Customize MIFare Card Key ☒

Card Type

MiFare 1K

Key Type

Sector-Wise

Save Sector-Wise Keys in DB ☒

Search

+

Start Sector	End Sector	Key A	Read Using	Write Using	
0	10	A2DC3F4DACBF	Key A	Key A	

After defining new key for sector 8-12, the previous key is marked to 0-7

Search

+

Start Sector	End Sector	Key A	Read Using	Write Using	
0	7	A2DC3F4DACBF	Key A	Key A	
8	12	DF0903EADF2B	Key A	Key A	

Click **Add** button to save the key configuration to the grid. The newly defined keys for sector8 to 12 will be listed along with previously defined keys for Sector 0 to 7 as shown above.

Time Attendance Policy

This page allows to define policies for time attendance.

To configure Time Attendance Policy, go to **Admin module > System Configuration > Global Policy > Time Attendance** and the following screen appears.

- **Auto Run Daily Process:** Select this checkbox for the system to run the daily attendance process automatically at 12:00 AM. The attendance status will be updated for the previous day only.

Example:

- Current Date and Day: 04/09/2021, Saturday (Week Off for users)
- **Auto Run Daily Process:** Enabled
- The system will run the daily process on 05/09/2021, Sunday at 12:00 AM.
- The attendance status of 04/09/2021, Saturday will be updated as WO.

Attendance Process Calibration

These Attendance processing parameters can be calibrated to determine how a punch is posted in the COSEC system. These can be set by the administrator as per organizational preferences in terms of recording attendance behaviour of employees. The parameters are as follows:

- **Max Early-IN Allowed (Hrs):** Maximum number of hours before shift-start time during which a punch should be considered as an Early-IN punch. Default value is 02:00 hours.
- **Max Late-OUT Allowed (Hrs):** Maximum number of hours after shift-end time during which a punch should be considered as a Late-OUT punch. Default value is 02:00 hours.
- **Priority:** This parameter assigns posting priority to an intermediate punch between two shifts. The administrator can determine whether such a punch is to be posted as an Early-IN punch for the next shift or a Late-OUT punch for the previous shift.
- **Max Working Hours Per Day (Hrs):** The maximum number of working hours to be considered per day for punch posting. All punches falling within this duration will be posted for the same day as per shift-based priority (if any). Default value is 16:00 hours.



If Attendance Process Calibration parameters are defined on both the Global Policies page and Attendance Policy page of Time and Attendance module, then only the Attendance Policy will be considered for a user.

The working of the Attendance Calibration parameters is explained below:

Assume the shift timing of an employee for the night shift from 19:30 hrs to 04:00 hrs.

Employee is entering the organization on 18th February at 19:31hrs and leaving at 04:30 hrs on 19th February, thus total working hours is 08:59 hrs.

Scenario1: With default parameters, The Punch 2 is in the Late out duration of the shift. So it will be posted on the same day(18th Feb).

Scenario2: If Late Out allowed is changed to 00:00 hrs, then the punch at 04:30 hrs comes under maximum working hrs. So OUT punch will be posted on the same day(18th Feb).

Scenario3: Now with Late Out allowed as 00:00 hrs and Max working hrs changed to 08:00 hrs, So according to the priority, punch at 04:30 hrs will be posted on next day(19th Feb) as IN punch.

If here, priority is changed to Late out, then punch at 04:30 hrs will be posted as OUT punch for same day(18th Feb).



When the user is assigned non-FB/RD shifts that end on FB/RD day, then in that case, process considers global policy parameters Max Early IN, Max Late OUT, Max Work Hours and priority with respect to Shift start-end time.

Reports Policy

This page allows to define policies for reports.

To configure Reports Policy, go to **Admin module > System Configuration > Global Policy > Reports** and the following screen appears.

Global Policy	
Basic	Sorting Field In Reports: User ID
User	Report Print Output: Printer
Login	Report Font: Courier New
Password Policy	Report Export Output In PDF Only: <input checked="" type="checkbox"/>
Device	Show Company Logo: <input checked="" type="checkbox"/>
Access Control	
Time Attendance	
Reports	



These report policies except 'Report Export Output in PDF only' will not have impact on the customized reports generated from Report builder.

If the checkbox "Report Export Output in PDF only" is enabled; then only PDF export option will be available in Report builder Export options.

Sorting Field In Reports: Select the option based on which the listing in the reports will be sorted in ascending order. The options available are: User ID and Name.

Report Print Output: Specify whether the report output is to be **Printed** on paper or as a **PDF** document.

Report Font: Select the font style from the drop down options in which the report is to be generated. If the selected font is not available then report will be generated in default “Courier New” font.



Depending on the font style selected, the report may overlap or get misaligned.

In case of multi-lingual content, unsupported characters will be displayed as garbage values.

Report Export Output in PDF Only: Select to restrict exporting reports to the PDF format only. This will prevent risks of data manipulation using any other output format.

Show Company Logo: Select to allow the “Company Logo” uploaded in “Enterprise Profile” page to be shown in the Reports.

For details go to *Admin Module > System Configuration > Enterprise Profile*.

Visitor Management Policy

This page allows to define policies for managing visitors.

To configure Visitor Management Policy, select **Admin module > System Configuration > Global Policy > Visitor Management** and the following screen appears.

- **Authorization For Visitor Pre-Registration:** When Visitor Pre-Registration request is initiated by host, it will be sent to the host's RIC for authorization.

Select the desired option from the dropdown list — Always, Not Required or When Visit Outside The Shift.

- **Always:** Select this option to always send all the Visitor Pre- Registration requests initiated by the host to the RIC for authorization.

All visit applications must be approved by the RIC irrespective of the visit time. That is, whether it is within or outside the shift timing of the host.

- **Not Required:** Select this option if you do not wish to send the Visitor Pre- Registration requests initiated by host to the RIC for authorization.
- **When Visit Outside The Shift:** Select this option to send all the Visitor Pre- Registration requests having visit time outside the shift timing of the host, to RIC for authorization.

If you select this option, Pre-registration requests within the shift timing of the host do not require approvals from the RIC.

An example with different cases is explained below for Visitor Pre-Registration initiated by both Host and Visitor. Refer [“Examples”](#).

For Visit Pre-Registrations, refer [“Pre-Registration”](#).

- **Authorization for Visitor Initiated Visit:** When a visit application is initiated by a visitor, it will be sent to the authorized host (of the visitor) for approval.

Once the host approves the visit application, this application will be sent to the host's RIC for authorization which depends on the option selected from the dropdown list.

Select the desired option from the dropdown list — Always, Not Required or When Visit Outside The Shift.

- **Always:** Select this option to always send all the visitor initiated visit applications (after the host authorizes) to the RIC for authorization.

All the visit applications must be approved by RIC irrespective of the visit time if it is within or outside the shift timing of the host.

- **Not Required:** Select this option if you do not wish to send the Visit application initiated by the Visitor for authorization to the RIC.
- **When Visit Outside the Shift:** Select this option to send all the visit requests having visit time outside the shift timing of the host to the RIC for authorization.

If you select this option, visitor initiated visit requests within the shift timing of the host do not require approvals from the RIC.

An example with different cases is explained below for Visitor Pre-Registration initiated by both Host and Visitor. Refer [“Examples”](#).

- **Send OTP for Verification:** If this checkbox is enabled, OTP will be sent to the visitor's mobile number for verifying the number provided by the visitor.

This is to verify that the visitor is genuine and the mobile number available in the system matches with the number of the visitor.



The OTP Verification will be applicable only when Pass is created from VMS Utility.

1. For Sending OTP to visitor, SMS configuration must be done in Admin module> System Configuration > SMS Configuration.
2. The OTP message alert must be configured from Alert Message Configuration by selecting “OTP Visitor Verification” event.
3. Visitor Service and Alert Service must be running for sending OTP.

Once this verification is done, visitor pass can be created from the VMS utility.

- **Security Approval for Visitor E- Pass:** Enable this Check-box if the Security Approval For Visitor E-Pass generation is required.
- **Required Visitor Acceptance:** Select this checkbox if the Visitor Acceptance is required.

If this checkbox is enabled then after approval of an appointment from RIC or system account user, appointment will be forwarded to visitor associated with appointment for the approval & Visitor Pre-Registration Alert will be dispatched to Visitor with approval links.

- **Allow E-Pass Generation Before Duration:** Enter the duration in minutes i.e. the duration before the system allows to generate Visit E-Pass. Only numeric value is allowed to enter upto 3 digits. Max Limit is 999 minutes.
- **Alert for Pass Expiration After Duration:** Enter the duration in minutes i.e. the duration after which the system generates an alert for visitor pass expiration. Only numeric value is allowed to enter up to 3 digits. Max Limit is 999 minutes.
- **Dynamic PIN On Pass Creation:** Select this checkbox to auto-generate a unique Dynamic PIN on Pass Creation for Visitor during his/her visit and assign this PIN to a Visitor Profile.

When **Dynamic PIN On Pass Creation** is enabled, then

- a. define the length of Dynamic PIN in **PIN Length**.
- b. during check-in, when Visitor Profile is assigned to a Visitor, then a Dynamic PIN as per set length will be auto-generated for the Visitor Profile.
- c. visitor will gain access to the devices assigned to that Visitor Profile via entering the Dynamic PIN.

If disabled, then PIN configured on Visitor Profile will be assigned to the Visitor during check-in.

To manually configure the PIN for Visitor Profile, refer "[Credentials](#)" under Visitor Profile.

- **Access via QR:** Select **Access via QR** checkbox to permit the visitor to access via QR Code.

During the check-in time of a visitor, when a Visitor Profile is assigned to a visitor, the Dynamic ID will be auto-generated and that Dynamic ID will be inserted in the QR Code which will be further added in the Visitor Pass Alert Message as well as in the visitor e-pass.

Dynamic ID will be set as the **Access Card 2** value for that Visitor Profile.

Once the Dynamic ID value is set in the **Access Card 2**, the **Access Card 2** will not be configurable from *Visitor Management> Visitor Profile> Credentials* and the **Card 2** will not be configurable from *Visitor Management> Utilities> Set and Sync Credentials> Credentials*.

When the visitor displays the QR Code in front of the device (with a Wiegand reader), the device scans the QR Code and check for the Dynamic ID inserted in the QR Code. If the Dynamic ID matches then the access is granted, else the access is denied.

Access will be denied if the visitor tries to access the device before/after the visit duration.

In any case, if the Dynamic ID is not generated or the **Access via QR** checkbox is disabled, then the Appointment ID will be generated and inserted in the QR Code.



It is recommended not to change the Access Card 2 value from the Device Module to avoid overwriting the Dynamic ID value set as the Access Card 2.

- **Auto Profile Assignment:** Visitor Profiles can be assigned to the visitors automatically. To do so, make sure the Visitor Profiles are created beforehand as per your requirement. To know more about the Visitor Profile, refer "[Visitor Profile](#)" in *Visitor Management> Visitor Profile*.

The system assigns these pre-configured profiles to the visitors as per certain matching criteria.

For Auto Assignment of Visitor Profiles, follow the steps given below:

- Select the **Auto Profile Assignment** checkbox. Once enabled, then configure **Matching Level**.
- To set the matching criteria for selection of the visitor profile which is to be assigned to the visitor, select the desired parameters' checkboxes in **Matching Level**.

Matching Level consists of different Groups such as Organization, Branch, Department etc. These are also configured for the Hosts.

The system will compare the selected criteria for the Visitor with the Groups assigned to the Host (in *User > User Configuration > Group*) and assign the best matched Visitor Profile to the Visitor automatically.

Along with the Profile, the visitor will also be granted access to the devices configured in the respective profile.

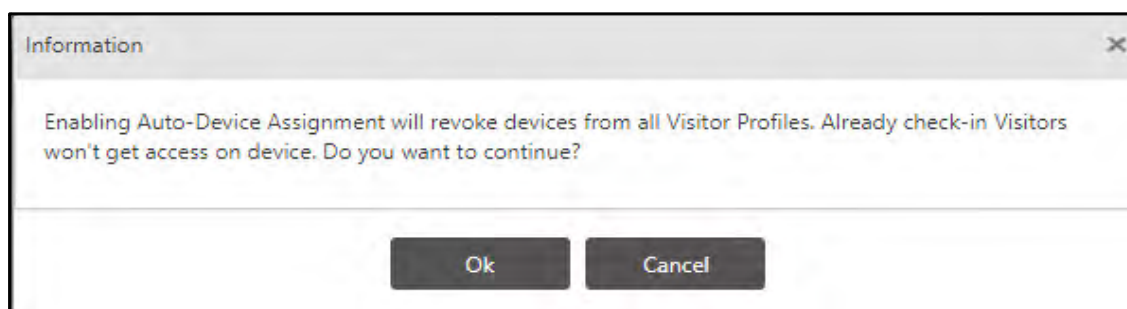
If **Auto Profile Assignment** is disabled, then the system will assign the first free Visitor Profile to the Visitor.

To understand this feature with the help of an example, refer Example 2 under [“Examples”](#).

- **Auto Device Assignment:** Select this checkbox to provide access to the devices assigned to the Host of a visitor, instead of the devices configured in the Visitor Profile (assigned to the visitor).

You can provide access to the devices assigned to the Host from the *User > User Configuration > Visitor Management*. For more information, refer [“Visitor Management”](#).

When you enable this feature, a pop-up will be displayed with an information as shown below:



Click **OK** if you want to continue, else click **Cancel** to discard the changes.

Once you click **OK**, all the devices will be revoked from the free as well as from the occupied Visitor Profiles.

If **Auto Device Assignment** is disabled, then the Visitor will be assigned devices configured in *Visitor Management > Visitor Profile > Devices*.

To understand this feature with the help of an example, refer Example 3 under [“Examples”](#).

Visit Creation Restriction

You can impose restriction on the Host/Visitor for Visit creation application by configuring minimum or maximum days as per your requirement.

Visit creation restriction will also be applied to rescheduled visits as well as inviting visitors via Invite Link, refer Reschedule Visit in [“Visit Approval”](#) and [“Invite Visitor”](#).

Configure the following parameters to impose restriction.

Visit Creation Restriction	
Minimum Days Before Allowing Visit	<input type="text" value="Days"/>
Maximum Days Before Allowing Visit	<input type="text" value="5"/>
Apply Restriction On	<input type="button" value="Both"/>

- **Minimum Days before Allowing Visit Creation:** Enter the minimum number of days before which the Host/Visitor needs to apply for the Visit creation.

For example: If **Minimum Days before Allowing Visit Creation** value is set to 2 and current date is 01/11/2020, then the visit start date cannot be before 03/11/2020.

If minimum days are not configured, then Visit creation will not be restricted.

- **Maximum Days Before Allowing Visit Creation:** Enter the maximum number of days before which the Host/Visitor needs to apply for the Visit creation.

For example: If **Maximum Days Before Allowing Visit Creation** is set to 10 and current date is 01/11/2020, then visit start date cannot be after 11/11/2020.

If maximum days are not configured, then Visit creation will not be restricted.

- **Apply Restriction On:** Apply the above configured restrictions on Host and/or Visitor which will be effective during a visit creation.

Select the desired option from the dropdown list — Both, Host only or Visitor only.

- **Host Only:** The restriction will be applied only when Host is creating the visit.
- **Visitor Only:** The restriction will be applied only when Visitor is creating the visit.
- **Both:** The restriction will be applied on both Visitor and Host while creating the visit.



The values for these parameters set in Global Policy will be considered as default values while creating a new user/worker. For more information refer [“Visitor Management”](#) and [“Worker Profile-Visitor Management”](#).

Visit creation application can also be created for the current date. To know more, refer Visit Creation on Current Date in [“Station Location”](#).

Default Host User:

Select the authorized host user from the picklist.

Visitor Custom Fields

- **ID Proof1 & ID Proof2:** Enter the name of ID Proof which will be printed on the visitor pass. The availability of these proofs need to be verified before the Visitor enters the premises. The ID Proofs specified here will appear in VMS Utility.
- **Custom Field 1 - 5:** These are fields that can be customized as per your requirements (e.g. ID Proof, Security Number etc.) which will be printed on the Visitor Pass from VMS Utility. These fields will be available for visitor configuration in the Visitor Management module of COSEC Web as well as for VMS Utility.

Visitor Custom Fields

ID Proof 1 *
ID Proof 2 *

Field No.	Active	Field Name	Type	Upload	Mandatory	
1	Yes	Security Number	Textbox	Yes	No	
2	Yes	Address Proof	Textbox	Yes	No	
3	Yes	Custom Field 3	Textbox	Yes	No	
4	Yes	Custom Field 4	Textbox	Yes	No	
5	Yes	Custom Field 5	Textbox	Yes	No	


- **Field No:** It displays the serial number and order of the field.
- **Active:** Select this check box, if you wish to display this field in Visitor Profile.
- **Field Name:** Enter the desired Field Name. For example: Security Number.
- **Type:** Select the desired type to be assigned to the field—Textbox and Date.
- **Upload:** Select the check box, if the configured field requires a provision to upload a document.
- **Mandatory:** Select the check box to mandate this field.

You can always edit this custom field by clicking **Edit**

Visitor Custom Fields

ID Proof 1 *
ID Proof 2 *

Field No.	Active	Field Name	Type	Upload	Mandatory	
1	<input checked="" type="checkbox"/>	Spouse Name	Textbox	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Yes	Spouse Birthdate	Date	Yes	No	
3	Yes	Custom Field 3	Textbox	Yes	No	
4	Yes	Custom Field 4	Textbox	Yes	No	
5	Yes	Custom Field 5	Textbox	Yes	No	

Click **OK**  and the pop-up appears.

Confirmation

Changing the 'Type' of the custom field will result in permanent loss of custom field data of all Users. Field will be set to default values. Do you want to continue?

Yes

No

Click **Yes** to save the configuration else click **No**.






The configured Visitor Custom Fields here will be displayed in **VMS Utility> New Visitor> Additional Details** and in **VMS Utility> Visitor Details> Additional Details** on the home page of VMS Utility.

The configured custom fields for Visitor will be visible in the **Visitor Management> Visitor Template> Details**.

The configured custom fields for Visitor will be visible in the **Visitor Management> Utilities> Frequent Visitor> Additional Details**.

The configured custom fields for Visitor will be visible in the **Visitor Management> Utilities> Watchlist> Additional Details**.

Visit Custom Fields

Visit Custom Fields						
Field No.	Active	Field Name	Type	Upload	Mandatory	
1	Yes	Field 1	Textbox	Yes	No	
2	Yes	Field 2	Textbox	Yes	No	
3	Yes	Field 3	Textbox	Yes	No	
4	Yes	Field 4	Textbox	Yes	No	
5	Yes	Field 5	Textbox	Yes	No	

1 - 5 of 10 records

«

<

1

2

>

»

- **Custom Field 1-10:** These fields can be customized as per your requirement. For detailed information, refer ["Visitor Custom Fields"](#).

The configured Visit Custom Fields here will be displayed in **VMS Utility> Home Page> Visit Details**.

The configured custom fields for Visitor will be visible in the **Visitor Management> Visit Template> Additional Details**.

The configured custom fields for Visitor will be visible in the **Visitor Management> Pre- Registration> Visit Details**.

The configured custom fields for Visitor will be visible in the **Visitor Management> Utilities> Visitor History**.

Examples

Example 1: Visitor and Host initiated Visit Requests

- Consider following data for Shift: GS
Shift Start Time:08:00
Shift End Time:17:00
- Consider following data for Shift: ES
Shift Start Time:18:00
Shift End Time:02:00
- Consider following data for host: H1
Date:12/10/2020
Shift:GS

Case 1: Visitor Initiated Visit Request

- Consider that visitor, V1 initiates a visit request as follows:
Visit Date:12/10/2020
Visit Start Time:18:00
Visit End Time:19:00
Host: H1
- This visit request when initiated successfully will be sent to the host for visit approval.
- Once the host approves this visit, then based on one of the following selected value for **Authorization For Visitor Initiated Visit** in *Admin> System Configuration> Global Policy > Visitor Management*, the request should proceed —
 - *Always*

This request application will be sent for RIC Approval.

- *Not Required*

This request application will not be sent for RIC Approval.

- *When Visit Outside The Shift*

This request application, for the above case, is outside the host's shift timings. Hence, as per the host's Reporting Group configurations it will be considered for RIC Approval.

Ex- RIC can approve from *Visitor Management > Visit Approval* page

- **Case 2: When Host's Shift is changed**

- Now, let us consider that in the above example the **Authorization For Visitor Pre-Registration** is selected as *When Visit Outside The Shift*, and shift for H1 is changed from GS to ES.
- Then only for upcoming visit request applications, ES will be applicable. No changes in previous Visitor Pre-Registration request applications.

- **Case 3: When either Visitor/Host Reschedules the Visit**

Visit can be rescheduled by —

1. *Visitor*

- If rescheduled by the visitor, then the request application will be sent to the host for acceptance.
- Once the host approves, then based on **Authorization For Visitor Initiated Visit** value, the application will be considered for RIC Approval.

2. *Host*

- If rescheduled by the host, then it will be sent to the visitor for acceptance and once the visitor accepts (depends on the value of the option **Required Visitor Acceptance**), then it should be considered for RIC approval based on the value set in **Authorization For Visitor Pre-Registration**.

3. *SA*

- Rescheduled visit by SA will be pre-approved.

• **Case 4: When Visit Transfer is done**

On visit transfer to another host can be done by —

1. *Visitor*

- If the visit is transferred by the visitor, then the request application will be sent to the new host for acceptance. (Host changed by Visitor)
- Once this new host approves, then based on **Authorization For Visitor Pre-Registration** dropdown value, the application will be considered for RIC Approval.

2. *Host itself*

- If the visit is transferred by the host, then it should be sent to the new host for acceptance. Once this new host approves the application, then it will be considered for RIC approval (of this new host) based on the value set in **Authorization For Visitor Pre-Registration**.

3. *SA*

- Visit transferred by SA will be pre-approved.

• **Case 5: Values of Authorization For Visitor Pre-Registration and Authorization For Visitor Initiated Visit change**

- When **Authorization For Visitor Pre-Registration** and/or **Authorization For Visitor Initiated Visit** value is changed then it will be applicable for upcoming visit request applications. There will be no change in previous Visitor Pre-Registration applications.

Example 2: Auto Profile Assignment

Case 1:

- A Visitor creates a visit for Host 1 and checks-in
- **Auto Profile Assignment** = Enabled
- **Matching Level** = Organization, Department, Section

	Host 1	Visitor Profile 1	Visitor Profile 2	Visitor Profile 3
Organization	Matrix	Matrix	Matrix	Matrix
Branch	R&D	HO	R&D	HO
Department	PMT	MKTG	PMT	PMT
Section	TL	TL	Member	TL
Category	C1	C1	C1	C4
Grade	G1	G2	G1	G4
Designation	D1	D2	D1	D4

- Here, as Matching Level is set as Organization, Department and Section, the Visitor Profile's groups should be matching with the values of host's groups.
- Hence, the profile Visitor Profile 3 will be assigned to the visitor.

Case 2: Multiple Profiles Match

- A Visitor creates a visit for Host 1 and checks-in
- Auto Profile Assignment = Enabled
- Matching Level = Department
- As per the configurations of Table 1, two profiles would be available for the visitor i.e. Visitor Profile 2 and Visitor Profile 3.
- In this case, any one of the profiles will be selected randomly for the visitor.

Case 3: No Profile Matches

- A Visitor creates a visit for Host 1 and checks-in
- Auto Profile Assignment = Enabled
- Matching Level = Section

	Host 1	Visitor Profile 1	Visitor Profile 2	Visitor Profile 3
Organization	Matrix	Matrix	Matrix	Matrix

	Host 1	Visitor Profile 1	Visitor Profile 2	Visitor Profile 3
Branch	R&D	HO	R&D	R&D
Department	PMT	MKTG	PMT	PMT
Section	TL	Member	Member	Member
Category	C1	C1	C1	C4
Grade	G1	G2	G1	G4
Designation	D1	D2	D1	D4

- As per the configurations of Table 2, no profile would be available for the visitor.
- In this case, no profile would be assigned to the visitor.

Case 3: No Profile Available

- A Visitor creates a visit for Host 1 and checks-in.
- Auto Profile Assignment = Enabled
- Matching Level = Department
- In this case, no profile would be available to assign to the visitor if all the profiles are occupied.

Case 4: Auto Profile Assignment is Disabled

- When **Auto Profile Assignment** is disabled, the first free visitor profile will be assigned to the visitor.

Example 3: Auto Device Assignment

Case 1:

- A Visitor creates a visit for Host 1 and checks-in.
- Auto Device Assignment = Enabled
- Then the devices assigned to the Host in the *Users> User Configuration> Visitor Management* will be assigned to the visitor.

Case 2: No Device Assigned

- A Visitor creates a visit for Host 1 and checks-in.
- Auto Device Assignment = Enabled
- When no device is assigned to the Host in the *Users> User Configuration> Visitor Management*, the Visitor visiting the host won't be allotted any device.

Case 2: Auto Device Assignment is disabled

- When Auto Device Assignment is disabled, the devices configured for a Visitor Profile from *Visitor Management> Visitor Profile> Devices* page will be assigned to the visitor.

CWM

This page allows to define policies for managing contract workers.

To configure CWM Policy, go to **Admin module > System Configuration > Global Policy > CWM** and the following screen appears.

- **Worker Assignment from CSS:** Enable to provide rights to Contractors for adding workers or assigning work orders using their Contractor Self Service (CSS) account.
- **Assignment Approval:** Select a Worker Approval type from the dropdown list to determine the process by which workers assigned by a Contractor can be approved by an organization. There are two options:
 - **Direct** - Approval Requests are directly sent to the system administrator.
 - **Approval Stage** - Approval Requests are sent to all the assigned *Approving In-Charges* either serially, or in a Parallel order (as per the *Approval Stage*). To set an approval scheme, select **Approval Stage** and select **Serial** or **Parallel** option from **Approval Scheme** dropdown list.



For more information on the Worker Approval process, go to: *Contract Worker Management > Work Order > Approval Stages*.

- **Approval Required For Existing Workers:** Select this checkbox if an existing worker is also required to go through the configured approval process, when assigned to a new work order. If unchecked, the worker assignment will be directly approved.

Custom Fields For Contractors

- **Field Name 1 - 10:** These are fields that can be customized as per your requirements. (e.g. ID Proof, Security Number etc.). These field names will later be available for Contractor configuration on the COSEC Web as well as for CSS application. These can also be used for third party integration purposes. The Field Names can be upto 20 alphanumeric characters (space, -, . and “comma” allowed).

Field No.	Active	Field Name	Type	Upload	Mandatory	
1	Yes	Security Number	Textbox	No	No	
2	No	Field 2	Textbox	No	No	
3	No	Field 3	Textbox	No	No	
4	No	Field 4	Textbox	No	No	
5	No	Field 5	Textbox	No	No	

- **Field No:** It displays the serial number and order of the field.
- **Active:** Select the check-box for this field to be visible in Contractor Profile.
- **Field Name:** Enter the desired Name. For example: Security Number.
- **Type:** Select the desired type of the field—Textbox and Date.
- **Upload:** Select the check-box if the configured field requires a provision to upload a document.
- **Mandatory:** Select the check-box for this field to be mandatory.

You can always edit this custom field by clicking the **Edit** button.

Field No.	Active	Field Name	Type	Upload	Mandatory	
1	<input checked="" type="checkbox"/>	<input type="text" value="Security Number"/>	Textbox	<input type="checkbox"/>	<input type="checkbox"/>	
2	No	Field 2	Textbox	No	No	
3	No	Field 3	Textbox	No	No	
4	No	Field 4	Textbox	No	No	
5	No	Field 5	Textbox	No	No	

Click on the **Ok** button and the pop-up appears.

Confirmation

Changing the 'Type' of the custom field will result in permanent loss of custom field data of all Users. Field will be set to default values. Do you want to continue?

Yes No


Click the **Yes** button to save the configuration else click the **No** button.

The configured custom fields for Contractor will be visible in the **CWM> Contractor> Contractor Profile> Details**.

Generate Worker ID

This section allows user to enable the Worker IDs to be generated Automatic while configuring new workers.

Enable 'Auto Generate Worker ID' check-box and configure '**ID Format**', '**Numeric Value Length**' and '**Zero Padding Required**' parameters the same ways as configured for 'Generate User ID' in **Global Policy > Users** tab at [page 138](#).

Click on the  button located besides the ID Format box to copy the same format which is configured for User ID.

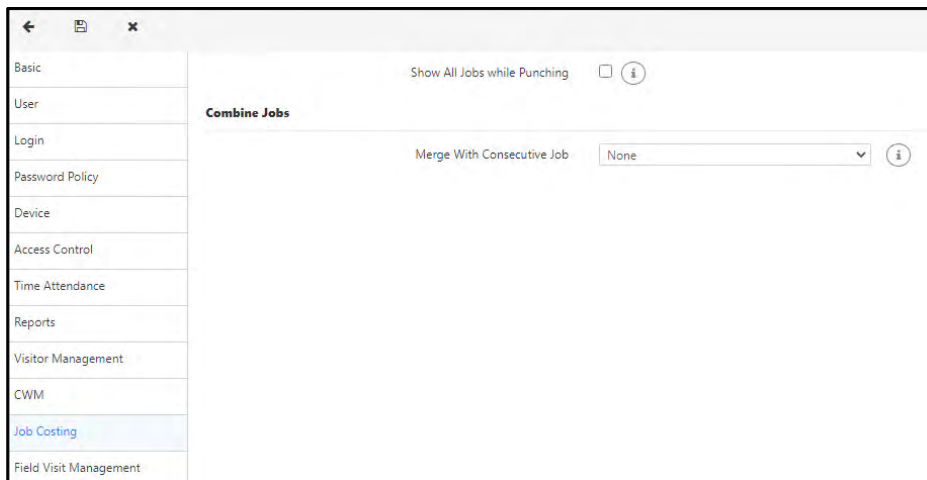
- **Worker ID Range:** Enter a range for allowed Worker IDs to define new workers in COSEC. The maximum allowed range is 1 - 9999999. Any prefix defined here will be added before all system-generated Worker IDs by default. For e.g. If prefix defined is "CWM", Worker IDs for approved workers will appear as shown below.

CWM35	Ramesh Pai
CWM32	Anil Aggarwal
CWM31	Ranjan Parmar
CWM3	Raju R.

Job Costing

When a user shifts from one site to another, the hours spent in the transition are to be added in the **Preceding** or **Succeeding** Job transaction.

To access Job Costing, go to **Admin module > System Configuration > Global Policy > Job Costing** and the following screen appears.



Show All Jobs while Punching: Select this check box if you want all the jobs present in the system to be displayed to the users. All jobs will also be displayed in **ESS login /APTA** Jobs drop-down when a user wants to punch.



The **ESS Assignment** check box at the following locations will not be displayed:

- User Module > Multi-User Options > User Configuration > Multi-User Configuration > Job Costing > Default Jobs
- User Module > Multi-User Options > User Configuration > Multi-User Configuration > Job Costing
- Enterprise Structure > Enterprise Groups > Job Costing
- Contract Worker Management > Worker Profile > Job Costing > Default Jobs

Combine Jobs

Merge with Consecutive Job: Select the desired option — None, Preceding, Succeeding.



If few transactions were made and then value in **Merge With Consecutive Job** drop-down is changed, its reflection in existing transactions will be made once “Daily Process” has been done.

Field Visit Management

This page allows to define policies for managing field visits.

To configure Field Visit Management Policy,

Click **Admin > System Configuration > Global Policy > Field Visit Management** and the following page appears.

Scheduling Reporting In-Charge: Select the Scheduling Reporting In-Charge from the drop down list—Group In-Charge1, Group In-Charge 2, Group In-Charge 3, Group In-Charge 4 or Group In-Charge 5 to give the rights for creating the Field Visit Schedule. The selected Reporting In-Charge can create/modify/ import/export the field schedules whereas the other Reporting In-Charges can only view the schedule.

Schedule Lock Out Period: Select the time duration (days) after the Schedule Date, for which the editing of the past schedules will be allowed.

If Lock Out Period is set as 0, then schedule can be edited on the schedule date only.

Example:

Consider Schedule Lock Out Period = 20 days

Current Date = 30/09/2015

If Schedule Date = 15/09/2015, field schedule will be in Edit Mode.
If Schedule Date = 05/09/2015, field schedule will be in View Mode.

ESS

To access ESS, go to **Admin module > System Configuration > Global Policy > ESS** and the following screen appears.

The screenshot shows the 'Global Policy' configuration window. On the left is a sidebar with the following menu items: Basic, User, Login, Password Policy, Device, Access Control, Time Attendance, Reports, Visitor Management, CWM, Job Costing, Field Visit Management, ESS (highlighted in blue), SSO Configuration, and Face Recognition. The main content area is titled 'Special Functions Configuration'. At the top right of this area is a checkbox labeled 'Refresh & Run Monthly Process', which is checked. Below this is a section titled 'Allowed Special Functions' containing a list of functions with checkboxes: Regular IN (checked), Official Work IN (checked), Short Leave IN (unchecked), Break End (checked), Overtime IN (unchecked), Regular OUT (checked), Official Work OUT (checked), Short Leave OUT (unchecked), Break Start (checked), and Overtime OUT (unchecked).

Refresh & Run Monthly Process: Select this checkbox for Refresh icon to be visible at “Current Month” and “Previous Month” section of ESS dashboard.

You can disable this checkbox to prevent the ESS users from refreshing or processing the monthly attendance period which creates ambiguities in attendance data of user.

Allowed Special Functions: Select the desired special functions for allowing ESS users to configure these special functions while punch marking.

SSO Configuration

To access SSO Configuration, go to **Admin module > System Configuration > Global Policy > SSO Configuration** and the following screen appears.



Make sure you have enabled Login via SSO, refer to [“Login Policy”](#).

Relaystate URL: Enter the relaystate URL.

IDP Profile Details: Specify the Details of IDP Profile by selecting Identity provider from drop-down list from options- OKTA, Pingone, ADFS and Azure. For Custom IDP, select *other* option from the drop-down list.



The dimensions of the Logo for IDP should be 32 x 32 pixels with its size less than or equal to 100kb.

COSEC Connections: Specify the details related to service provider by mentioning SP Identity ID. You may download COSEC Public certificate on click of **Signing Certificate** icon.

If the 'Sign Authentication Request' check-box is enabled for IDP profile as ADFS then, the COSEC Public certificate is mandatory to be uploaded at the ADFS. The User will be notified with an error; 'SSO Login Failed' while login with IDP, if the certificate is not found at the ADFS.



If the certificate is expired then in that case login response from IDP will be failure and user needs to re new or upload new certificate.

COSEC Connection

SP Identity ID *

Signing Certificate

Sign Authentication Request

IDP Configuration

Attribute Mapping

IDP Configuration: Configure IDP in this collapsible panel by adding ACS Endpoint, ACS Logout Endpoint, SSO Login and SSO Logout URLs.

For SSO based login to work, make sure you have configured the:

- **ACS (Assertion Consumer Service) Endpoint:** Enter the Domain URL for COSEC Login. The SSO Token will be sent to this location.
- **ACS (Assertion Consumer Service) Logout Endpoint URL:** Enter the Domain URL for COSEC Logout. The logout requests will be sent to this location.
- **SSO Login URL:** The URL entered in the SSO Login URL must be the URL where the user should be redirected.
- **SSO Logout URL:** The URL entered in SSO Logout URL must be the URL that should hit just after the user logout from COSEC.
- **IDP Entity ID:** The URL entered in the IDP Entity ID must be the URL which should be used to identify the IDP to which the SSO request to be send.
- **Upload the IDP Certificate:** Click **Browse** to select the certificate to be uploaded from the local PC.



If any of the URL or certificate uploaded are invalid or does not exist then SSO should fail.

IDP Configuration

ACS Endpoint <Domain URL for COSEC Login> /Login/ReceiveSSO

ACS Logout Endpoint <Domain URL for COSEC Login> /Login/ReceiveSLO

SSO Login URL *

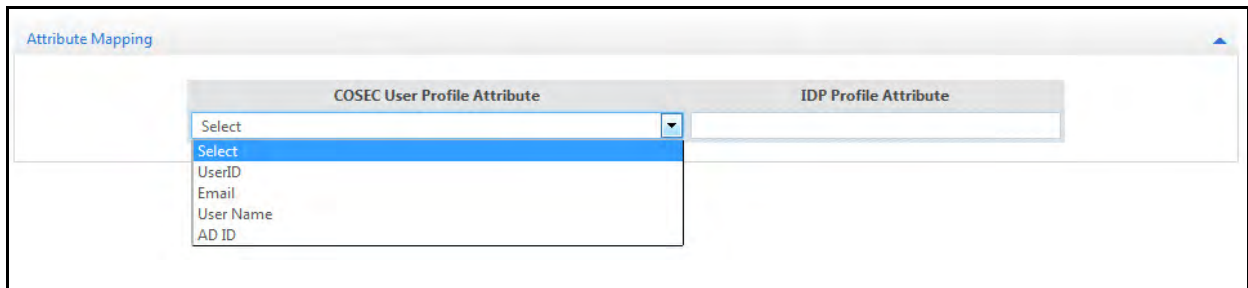
Enable Logout From IDP

SSO Logout URL *

IDP Entity ID *

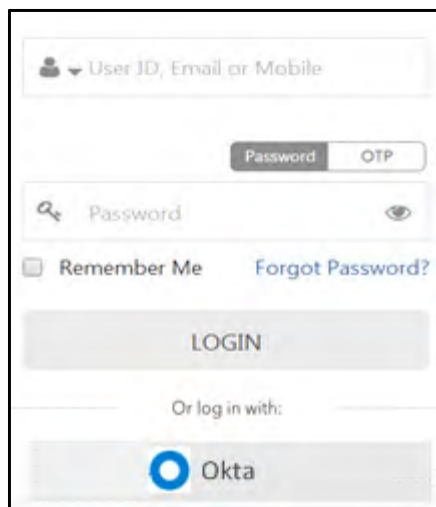
Upload IDP Certificate * **Browse...** No file selected.

Attribute Mapping: To identify which user wants to access COSEC from the respective IDP, Attribute Mapping is used. Map the Attribute such as User ID, Email, User Name and AD ID to be received in SSO Response.



The image shows a window titled "Attribute Mapping". It contains two columns: "COSEC User Profile Attribute" and "IDP Profile Attribute". The "COSEC User Profile Attribute" column has a dropdown menu that is open, showing the following options: "Select", "Select", "UserID", "Email", "User Name", and "AD ID". The "IDP Profile Attribute" column is currently empty.

After successful SSO Configuration, the Login page will be have additional option under Log in with as shown in figure below:



The image shows a login page. It has a text input field for "User ID, Email or Mobile". Below it are two tabs: "Password" and "OTP". The "Password" tab is selected. There is a password input field with a toggle icon. Below the password field are two links: "Remember Me" and "Forgot Password?". A large "LOGIN" button is below these links. At the bottom, there is a section "Or log in with:" followed by an "Okta" logo and text.

Face Recognition

To access Face Recognition, go to **Admin module > System Configuration > Global Policy > Face Recognition**, and the following screen appears.

The screenshot shows the 'Global Policy' configuration window for 'Face Recognition'. The left sidebar lists various system modules, with 'Face Recognition' selected. The main area contains several configuration sections:

- Conflict Matching Threshold:** A slider set to 93%.
- Group FR:** Includes a 'Group FR' checkbox (unchecked) and a 'Matching Threshold (Face) for Group Attendance' slider set to 98%.
- Exceptional Face:** Includes 'Exceptional Face Enrollment' (unchecked), 'Exceptional Face Clustering Threshold' (98%), and 'Exceptional Face On Device Per Cluster' (5).
- Mask Coverage:** Includes 'Face Mask Coverage' (98%) and 'Visible Face' (99%).
- Adaptive Face Enrollment:** Includes 'Adaptive Face Templates Per User' (5).
- APTA Anti-Spoofing:** Includes 'APTA Face Anti-Spoofing Mode' (Advanced) and 'APTA Face Anti-Spoofing Threshold' (62%).

A note at the bottom states: 'Note : For Group FR/ Exceptional Face Enrollment feature to work, ensure that Identification Service is defined in Cosoc Admin's License and Service'.

- **Conflict Matching Threshold:** Enter the desired Conflict Matching Threshold value in percentage.

The system will consider this value while comparing the face with the face templates already present in the database.

If a conflict is found, that is, if the system detects a face template in the database similar to the new face, then a conflict error will be displayed.

Make sure a higher value is set for this parameter, as it will result in less equivalent matches with the face templates available in the database.



Make sure the *Conflict Matching Threshold* is set lower than *Matching Threshold* in *Admin module > System Configuration > Identification Server Configuration*.

Example: Face Enrollment of Suresh

- **Conflict Check** checkbox is selected.
- **Conflict Matching Threshold** is set as 93%.

Now during the face enrollment of Suresh, the system will check in its database if his face matches with faces of other users available in the database.

- **Case 1:** If Suresh's face matches 92% with Ram, then the system will allow to enroll Suresh's face.
- **Case 2:** If Suresh's face matches 94% with Shyam, then the system will display the conflict error while enrolling Suresh's face.

Group FR



For Group FR ("[Mark Group Attendance](#)") **Exceptional Face Enrollment** and **Face Enrollment via Web** feature to work, ensure that **Identification Service** is defined in **COSEC Admin > License and Service**. For more details refer *Admin Management Portal User Manual*.

- **Group FR:** Select this checkbox to enable face recognition feature for multiple users for marking attendance at the same time.
- **Matching Threshold (Face) for Group Attendance:** Enter the matching threshold value, which will be used by the COSEC Server to match faces of users from the uploaded group image (having faces of different users) for group attendance. Image can be uploaded by Admin as well as by RIC. To know how to upload a group image, refer "[Mark Group Attendance](#)".

Exceptional Face

- **Exceptional Face Enrollment:** During face recognition, if a user is not identified by his/her face credential, the system will consider that face as an exceptional face.

Exceptional faces can be found in the following cases:

1. User and face both are not enrolled
 2. User is enrolled but face is not enrolled
 3. User and face are enrolled
- Then the system will capture this exceptional face image and send it to the Admin.
 - Admin will authorize these exceptional face images and once authorized, Admin can enroll the face against the respective user manually or discard it.
 - In case the exceptional face image received is of a new user, then the Admin can create a new user profile and enroll that image against that profile. For more information refer "[Exceptional Face Authorization](#)" in Users> Utilities.
 - Select this checkbox to enable **Exceptional Face Enrollment**.



If you have enabled the **Exceptional Face Enrollment** feature then make sure that you schedule a task of **Delete Exceptional Face** in **Admin > System Utilities> Task Scheduler** to avoid storage of excess data in the database.

If you are using Cogniface EBS, make sure you have a centralized IDS installed for this feature to function.

- **Exceptional Face Clustering Threshold:** Multiple exceptional faces of a single user can be recognized by the system. Such faces will be saved in a cluster for a user.
 - Enter the Exceptional Face Clustering Threshold value which is basically a matching threshold based on which the system will identify whether two exceptional faces recognized, belong to the same user or not.
 - These two exceptional faces will be kept in the same cluster if matching threshold between them is equal to or greater than the value entered by the Admin.

- **Exceptional Face On Device Per Cluster:** Select the number of exceptional faces of an unidentified user that should be received from each device available in a cluster.

Select the number of exceptional faces to be received from each device present in a cluster



When the number of exceptional faces received from a device in a cluster exceeds the value you entered, then before adding a new exceptional face from the same device, the exceptional face with the highest matching threshold from that device needs to be removed.

Let's understand with the help of an example:

Value set for **Exceptional Face On Device Per Cluster** = 5

Cluster ID = 1

Exceptional faces from device 1 = 4

Exceptional faces from device 2 = 5

- Case 1: A new exceptional face from device 1 is matched with cluster 1. So new face should be directly added in cluster 1.
- Case 2: A new exceptional face from device 2 is matched with cluster 1. So here new exceptional face should be matched with all 5 exceptional faces. The face having highest matching threshold should be replaced by the new exceptional face from device 2 in cluster 1.

Mask Coverage

- **Face Mask Coverage:** Enter the minimum percentage required for considering face mask in Face Mask Compulsion at the time of user identification.

Set higher percentage values for accurate face mask detection.

- **Visible Face:** Enter the maximum percentage required for the face to be visible during user enrollment/identification.

Set higher percentage value to identify or enroll face without mask accurately.

Setting lower value will increase false acceptance.

This parameter is applicable for Face Enrollment from Enroll Utility, Adaptive Face Enrollment and identification when Face Mask Compulsion is enabled.



*Make sure you have selected the Enable FR checkbox in **Device Configuration> Identification Server> Face Recognition**.*

*If Face Mask Compulsion is disabled in **Device Configuration> Advanced> Settings> Face Mask Compulsion**, then Face Mask Coverage will not be applicable.*

Adaptive Face Enrollment

- **Adaptive Face Templates Per User:** Select the desired number of Adaptive Face Templates that can be enrolled against a user from the drop-down list.

APTA Anti-Spoofing

- **APTA Face Anti-Spoofing Mode: Face Anti-Spoofing** feature prevents false face verification by using a photo, video, mask or a different substitute for an unauthorized person's face.

Along with the configurations to be done for Face Anti-Spoofing you also need to take care of the recommended settings for liveness verification and for face recognition, refer [“Recommendations for Liveness Verification”](#) and [“Recommendations for Face Recognition”](#).

Select the desired Face Anti-Spoofing Mode for liveness detection via COSEC APTA Application from the following:

1. **Moderate:** This mode analyzes the texture of face. Select this option when the distance between Camera and Face is less than 2 feet
 2. **Advance:** Select this option when the distance between Camera and Face is more than 1 feet and less than 2 feet.
- **APTA Face Anti-Spoofing Threshold:** Enter the Face Anti-Spoofing threshold value in percentage within the range from 1.00 to 99.99 to identify user's face liveness via COSEC APTA Application for considering him/her as a genuine person.

Identification Server

Identification Server is a server which enables to identify the credentials (Finger/Palm/Face) faster in comparison to local identification. COSEC Device do not have heavy storage capacity for credential templates so Identification Server (IDS) can be used which can be installed on 64 bit PC with high storage capacity.

The Identification Service must be installed from the COSEC Setup and configured with Master Server Settings.

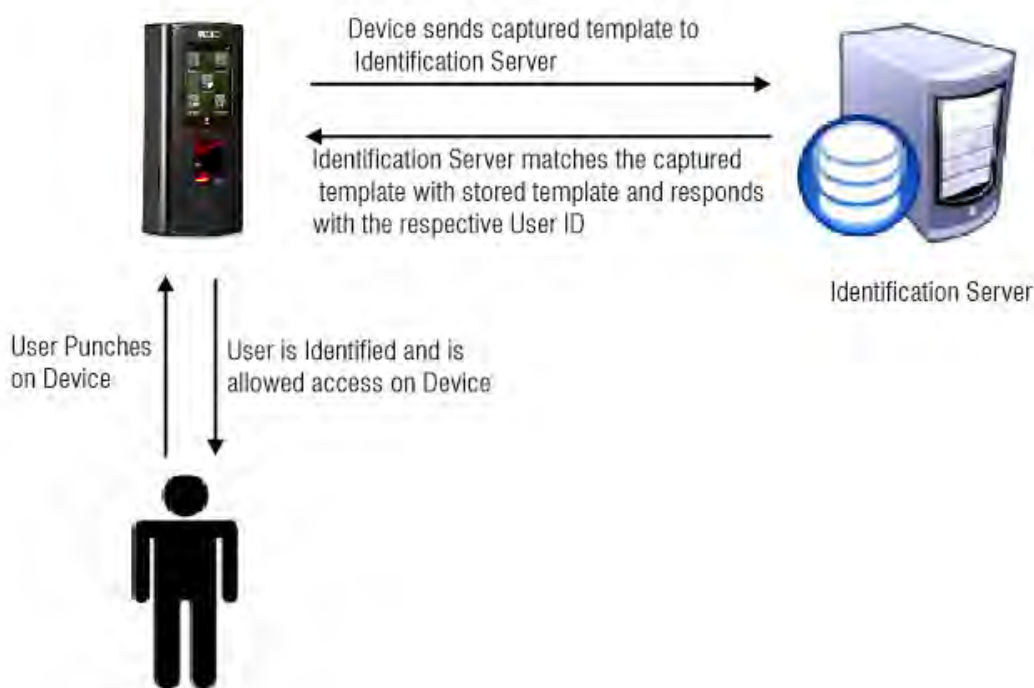


For Identification Server to work smoothly, ensure that ports specified in Master Service and Identification Service are opened in the Firewall settings.

When you start the Identification Service; then Identification Server Configuration will be added in Admin module > System Configuration with the IP address and MAC address of the PC where Identification Service is installed.

Identification of Credential

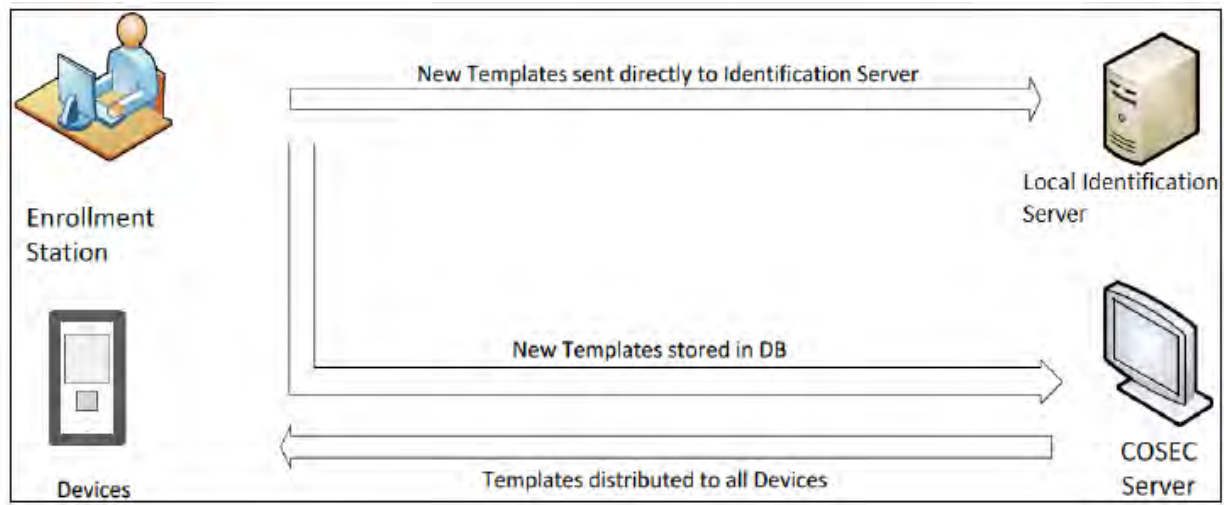
The Identification Server runs as a service of the COSEC Application and enables the COSEC server to perform both centralized as well as localized finger, palm and face template identification across a multi-site installation. Multiple Identification servers can be configured at multiple locations for a single COSEC installation where credentials are maintained locally based on enterprise group assignment. This ensures a faster identification process as matching of credentials is performed only against locally stored templates on each identification server.



Each Identification Server can be configured for a specific location and assigned specific devices and enterprise groups for which it will perform local identification. This will ensure that only the templates of users at this location are available with the Identification Server. You can configure the Identification Server parameters from **Identification Server Configuration** page in the Admin module. For details, refer "[Identification Server Configuration](#)".

On completion of Identification Server configuration, whenever an enrollment is performed at an Enrollment station (or at a door controller), the enrolled templates shall be sent both to the COSEC database as well as the local identification server configured for the site. Now, when a user shows a palm or swipes a finger at any of the

assigned door controllers, the local Identification Server shall respond with a User ID for which the template is matching.



To assign a device to an Identification Server, go to **Devices > Device Configuration > Identification Server**

A local Identification Server will have two databases for storing finger/palm/face templates:

- A **local** database - This stores only the templates of local users and will be used for location-based user identification. This can be set up at the time of server configuration.
- A **global** database - This stores the templates of all COSEC users and will be used at the time of finger/palm enrollment of all COSEC users from an enrollment station.



For Group FR ("[Mark Group Attendance](#)"), [Exceptional Face Enrollment](#) and [Face Enrollment via Web](#) feature to work, ensure that Identification Service is defined in COSEC Admin > License and Service. For more details refer Admin Management Portal User Manual.

The following process enables you to collaboratively setup and configure the Identification Service:

- ["Installing Identification Server"](#)
- ["Starting Identification Service"](#)
- ["Identification Server Configuration"](#)

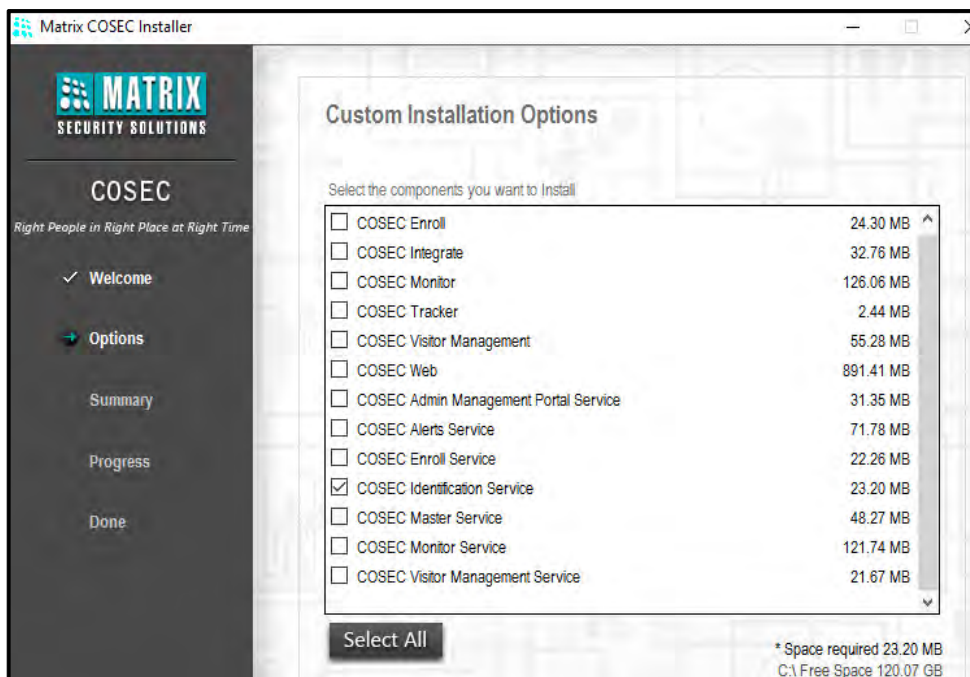
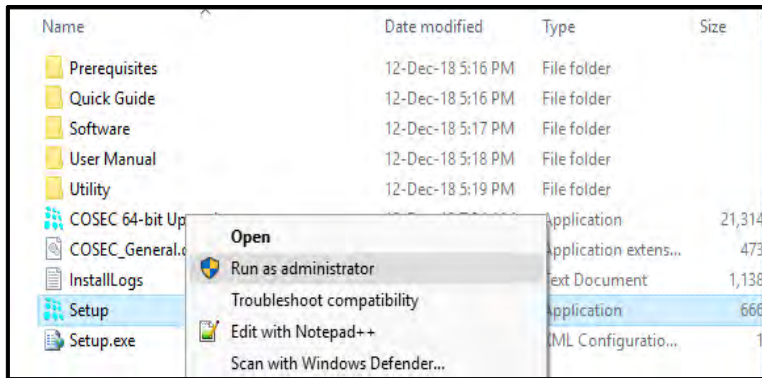
Installing Identification Server

The Identification Server runs as a service of the COSEC Application. You can install the Identification service from the Custom Installation of COSEC Installer directly or from the COSEC Setup> Software> COSEC_Identification.

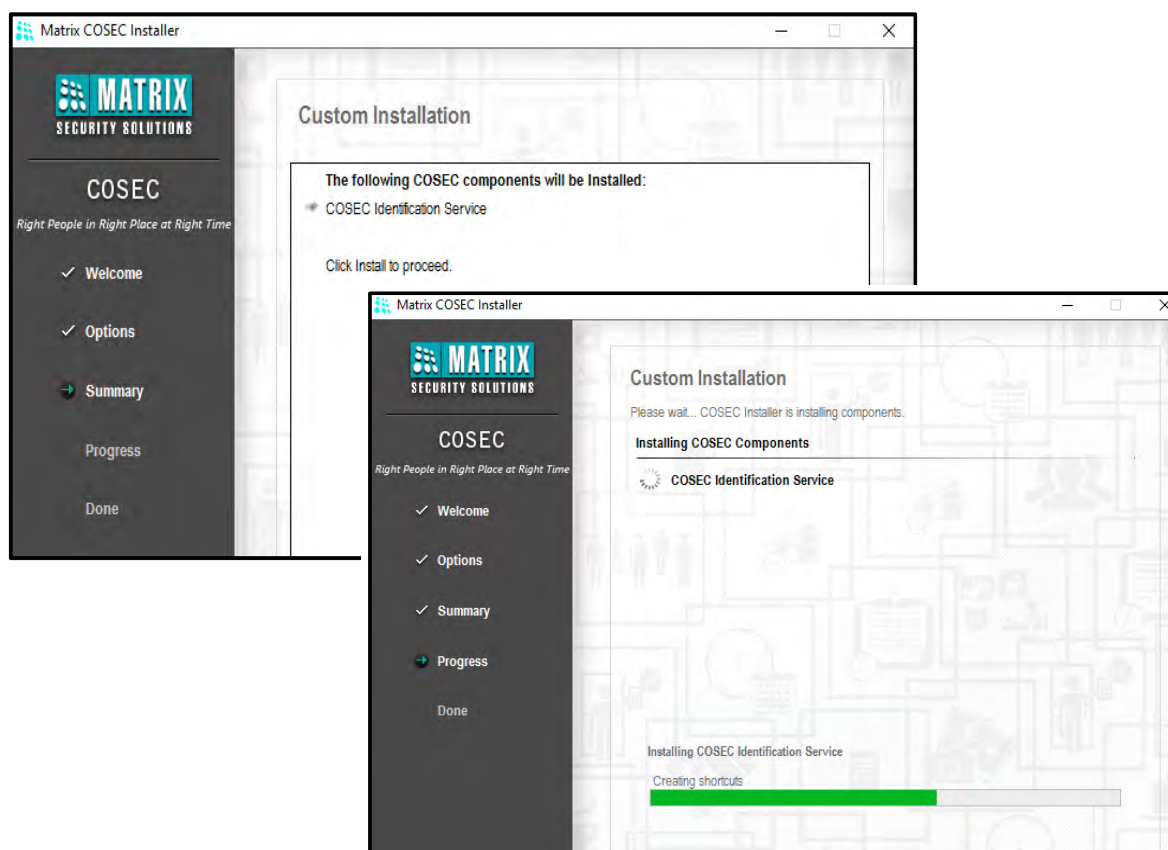
To install the Identification Service right click on the **Setup** and click **Run as Administrator** option as shown in the screen below.



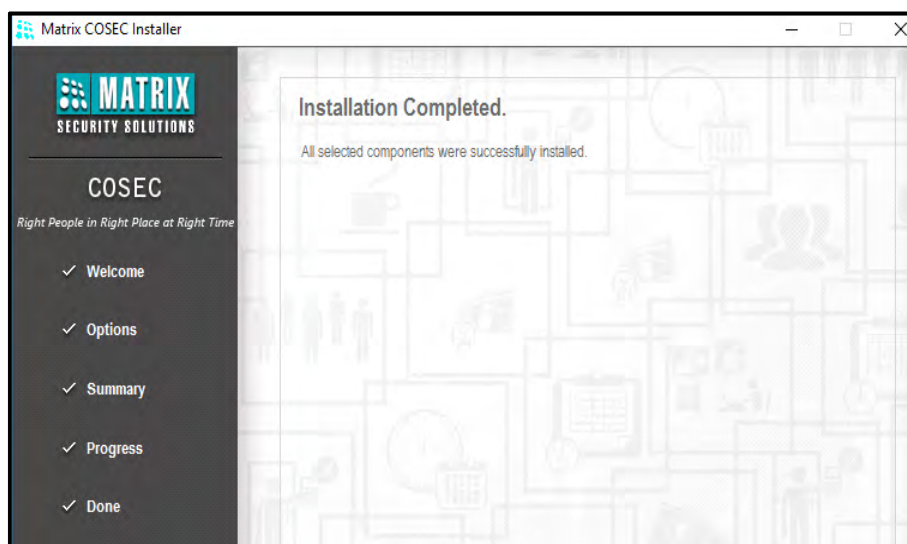
The Identification Service must be installed on 64 bit computer with high configuration.



Select **COSEC Identification Service** and proceed for installation.




Once the installation gets over the following screen appears.




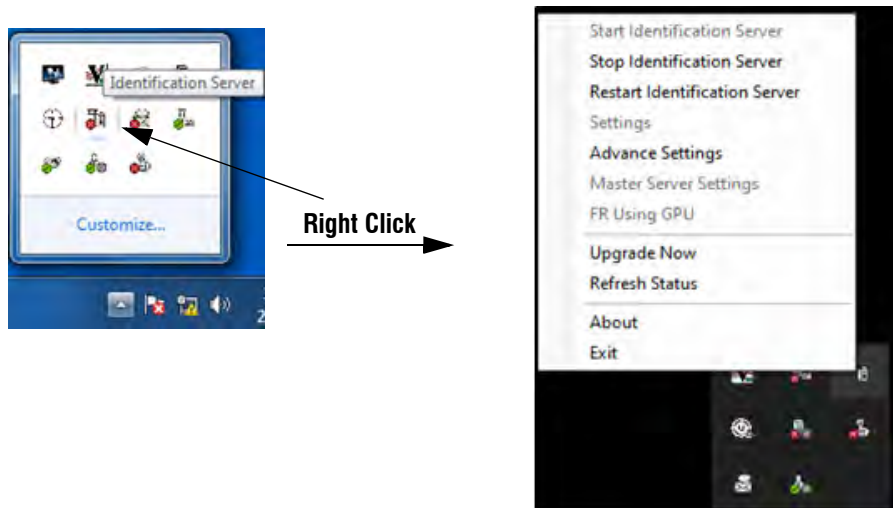
The Identification Sever is installed successfully and click **Close** button to exit the wizard. Now, you need to start the service which is described in the following section.

Starting Identification Service

After the installation, you can start the COSEC Identification Service Application by browsing the folder from **C:\Program Files (x86)\Matrix\COSEC Identification Service**

When Identification Service starts, Identification Service's  icon will be displayed in the System Tray (Notification area) on the right side of the taskbar.

Right click on the  icon.



The options displayed are — Start Identification Service, Stop Identification Service, Restart Identification Server, Settings, Advance Settings, Master Server Settings, FR Using GPU, Version Up-To Date, Refresh Status, About and Exit.

- To start this service through the Service Manager Tray, click on **Start Identification Service**.
- To configure the settings of Identification Service, first stop this service by clicking **Stop Identification Service**, and then click **Settings**. To know more, refer [“Settings”](#).
- To restart this service, click **Restart Identification Service**.
- To configure the settings of logs and tenants in the Identification Service, click **Advance Settings**. To know more, refer [“Advance Settings”](#)
- To configure the settings of Master Service, first stop the Identification Service, then click **Master Service Settings**. To know more, refer [“Master Service Settings”](#)
- To run FR with GPU, you require a graphic card installed in your PC, then click **FR with GPU**. If the graphic card is not available, then the system will continue the FR process without GPU.
- To upgrade the version of Identification Service, click **Version Up-To-Date**.
- To refresh the status of this service, click **Refresh Status**.
- To view the service details, click **About**.
- To close the Service Manager Tray window, click **Exit**.



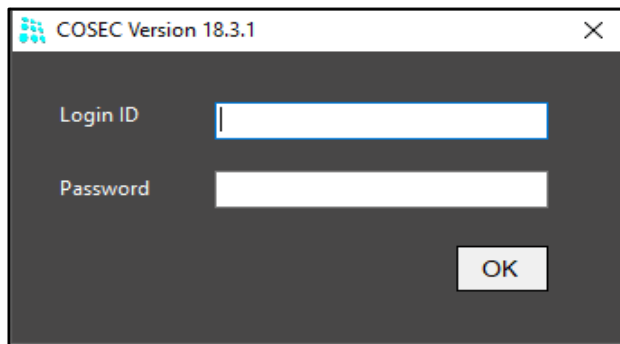
When service is running and Admin database loses connectivity or is unavailable then the service will keep running for 24 hours by default after which it will stop.

The maximum hours allowed for service is given as the configurable tag in Settings.xml file from **C:\Program Files (x86)\Matrix\COSEC Identification Service**.

Settings

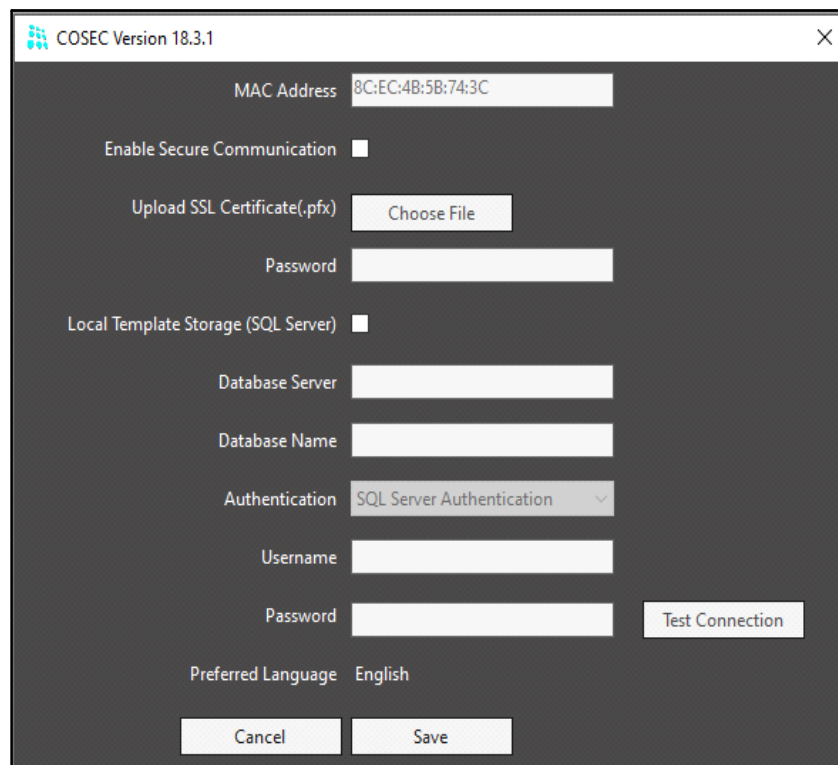
To configure the settings of Identification Service, first stop this service, then click on **Settings** from the Service Manager Tray option.

Login page appears.



- Enter the **Login ID** and **Password** same as configured in the COSEC Web.
- Click **OK**.

Identification Service's Settings window appears as shown below.



Configure the following parameters:

- **MAC Address:** It displays the MAC address of the system corresponding to the IP address selected from the Tenant Settings screen.
- **Enable Secure Communication:** Select this checkbox to enable secure communication with the COSEC database.
- **Upload SSL Certificate (.pfx):** For secured communication, SSL Certificate is to be uploaded.
- **Password:** Enter the password for accessing SSL Certificate file.
- **Local Template Storage (SQL Server):** Select this checkbox to allow the template storage in the local database for the retention of stored templates when the service gets restarted.
- **Database Server and Database Name:** Enter the server address of the database and its name.



*The Database Server name should be specified using the following syntax:
Server IP Address\instance name of SQL Server.*

E.g. 192.168.104.24\squlexpress. Here, IP Address is of the system on which the Database Server is installed and sqlexpress is the instance name given to the SQL Server.

- **Authentication:** Select the desired authentication mode — SQL Server Authentication or Windows Authentication.
- **Username and Password:** Enter the user name and the password of the database.

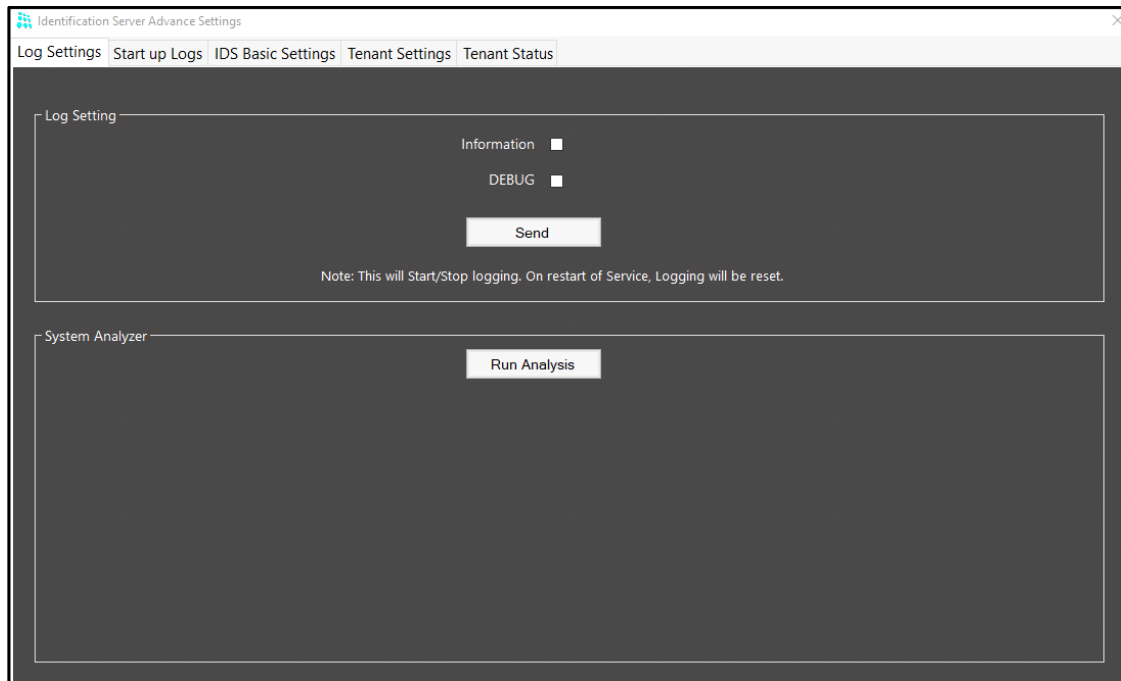
Click **Test Connection** to test the connection of Identification Service with the database.

- **Preferred Language:** It displays the language selected for the COSEC Web for a specific System Account User.

Click **Save** to save the settings or click **Cancel** to discard.

Advance Settings

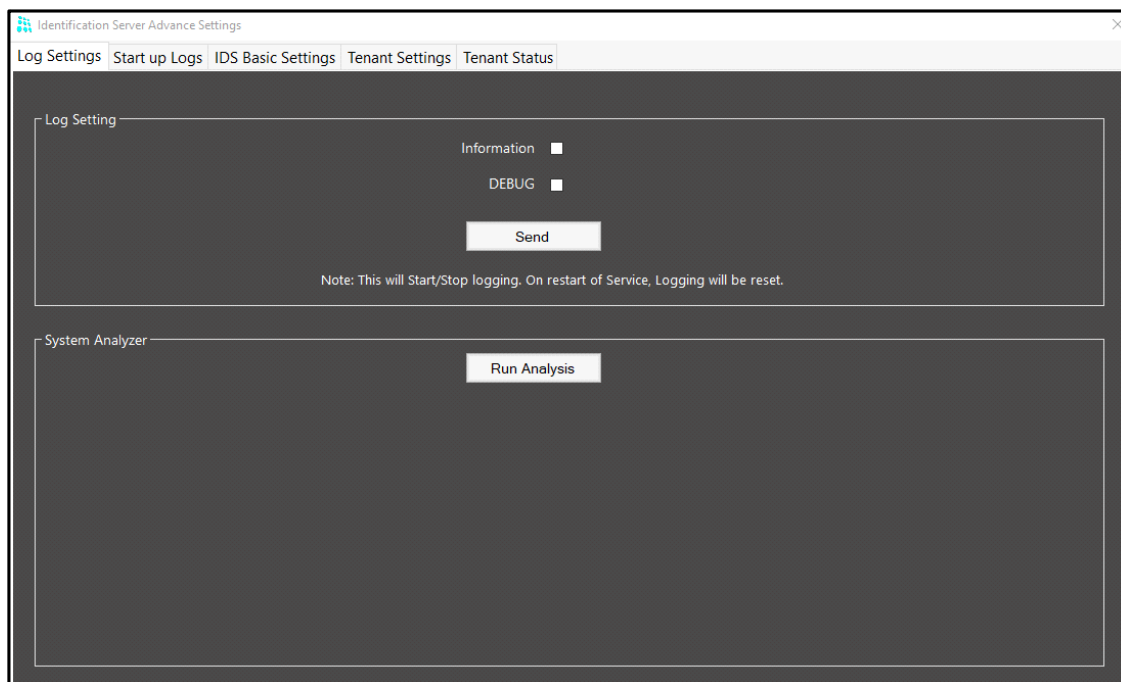
In order to configure the settings of logs and tenants in the Identification Service, click **Advance Settings** from the Service Manager Tray option. The **Identification Server Advance Settings** page appears as below:



Before you start the configurations, you can check if your PC is compatible and the required pre-requisites for the installation of the Identification Server are fulfilled.

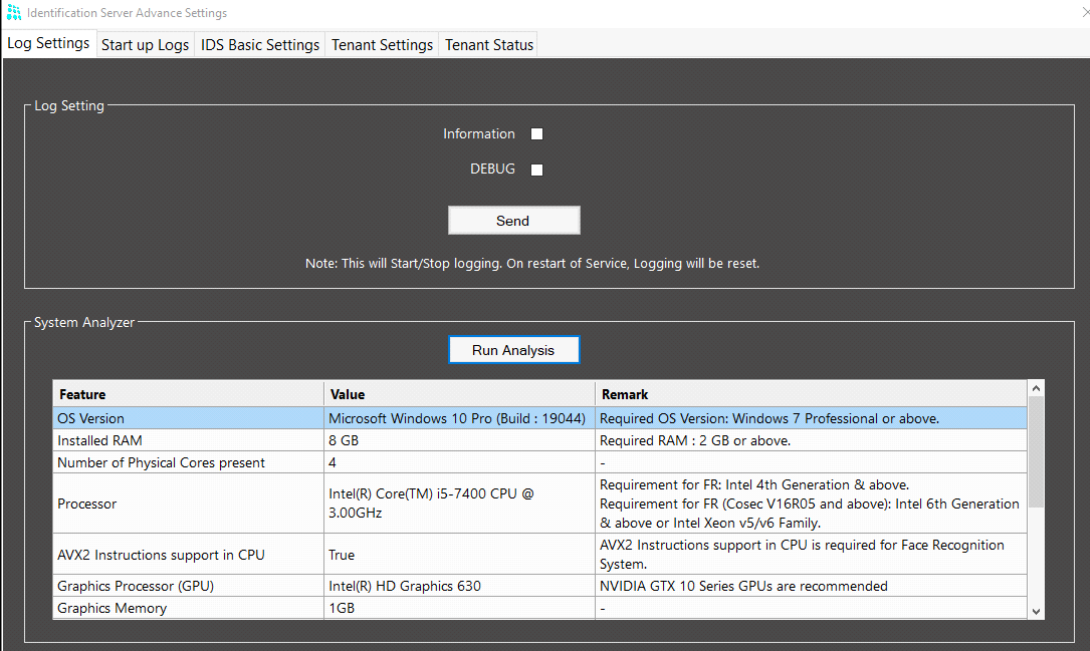
To check the compatibility,

- In the System Analyzer section, click **Run Analysis**.



After the process completes, it displays a table with the three columns Feature, Value and Remarks.

Value mentions the current systems details for each Feature and the Remark column displays what is required for the IDS to function.



Identification Server Advance Settings

Log Settings | Start up Logs | IDS Basic Settings | Tenant Settings | Tenant Status

Log Setting

Information ☐

DEBUG ☐

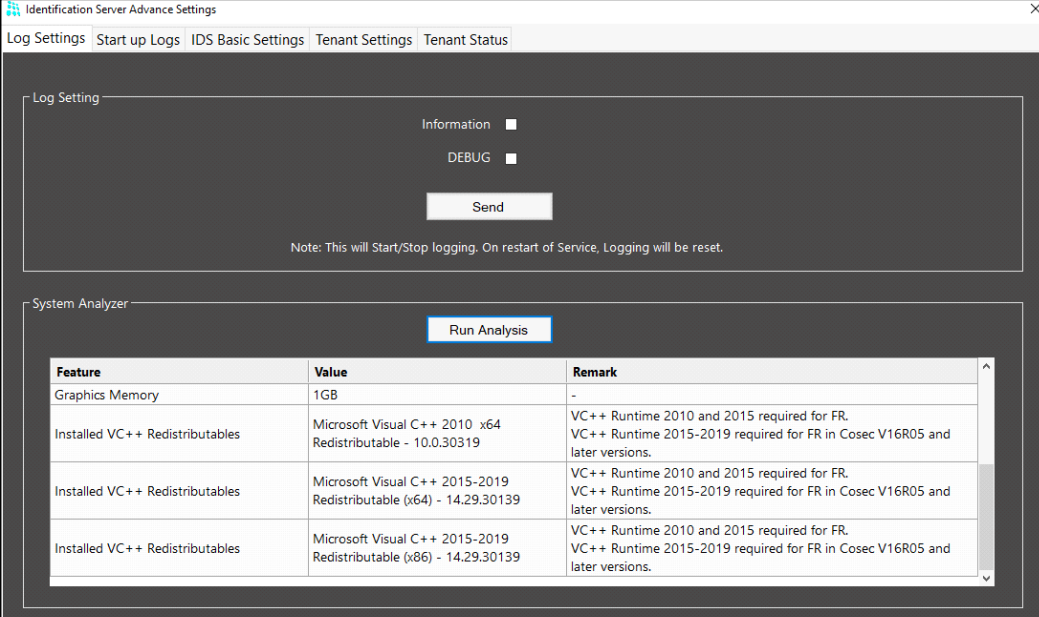
Send

Note: This will Start/Stop logging. On restart of Service, Logging will be reset.

System Analyzer

Run Analysis

Feature	Value	Remark
OS Version	Microsoft Windows 10 Pro (Build : 19044)	Required OS Version: Windows 7 Professional or above.
Installed RAM	8 GB	Required RAM : 2 GB or above.
Number of Physical Cores present	4	-
Processor	Intel(R) Core(TM) i5-7400 CPU @ 3.00GHz	Requirement for FR: Intel 4th Generation & above. Requirement for FR (Cosec V16R05 and above): Intel 6th Generation & above or Intel Xeon v5/v6 Family.
AVX2 Instructions support in CPU	True	AVX2 Instructions support in CPU is required for Face Recognition System.
Graphics Processor (GPU)	Intel(R) HD Graphics 630	NVIDIA GTX 10 Series GPUs are recommended
Graphics Memory	1GB	-



Identification Server Advance Settings

Log Settings | Start up Logs | IDS Basic Settings | Tenant Settings | Tenant Status

Log Setting

Information ☐

DEBUG ☐

Send

Note: This will Start/Stop logging. On restart of Service, Logging will be reset.

System Analyzer

Run Analysis

Feature	Value	Remark
Graphics Memory	1GB	-
Installed VC++ Redistributables	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.30319	VC++ Runtime 2010 and 2015 required for FR. VC++ Runtime 2015-2019 required for FR in Cosec V16R05 and later versions.
Installed VC++ Redistributables	Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.29.30139	VC++ Runtime 2010 and 2015 required for FR. VC++ Runtime 2015-2019 required for FR in Cosec V16R05 and later versions.
Installed VC++ Redistributables	Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.29.30139	VC++ Runtime 2010 and 2015 required for FR. VC++ Runtime 2015-2019 required for FR in Cosec V16R05 and later versions.

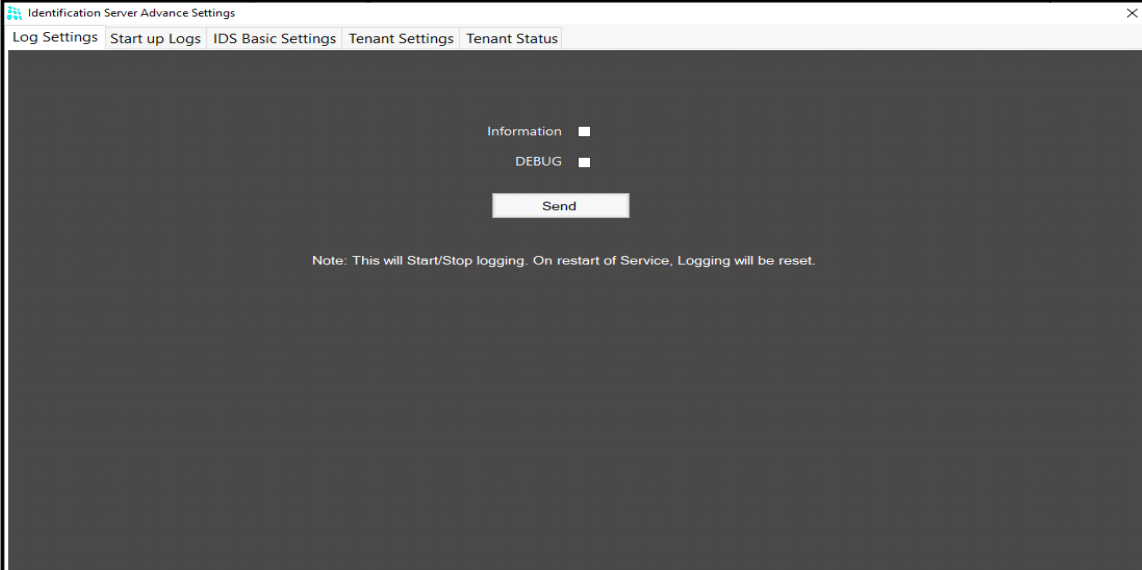
If all Values are as per the Remarks the IDS will be functional. If not you need to update the system as per the Remarks.

Now, you can continue with the configuration, the screen displays the following tabs:

- “Log Settings”
- “Start up Logs”
- “IDS Basic Settings”
- “Tenant Settings”
- “Tenant Status”

Log Settings

Click the **Log Settings** tab to enable logs of the IDS Service.



The screenshot shows a window titled "Identification Server Advance Settings" with a tabbed interface. The "Log Settings" tab is selected. The main area contains two checkboxes: "Information" and "DEBUG", both of which are currently unchecked. Below these checkboxes is a "Send" button. At the bottom of the window, a note states: "Note: This will Start/Stop logging. On restart of Service, Logging will be reset."

Select the check box of the desired option — **Information**, **DEBUG**.

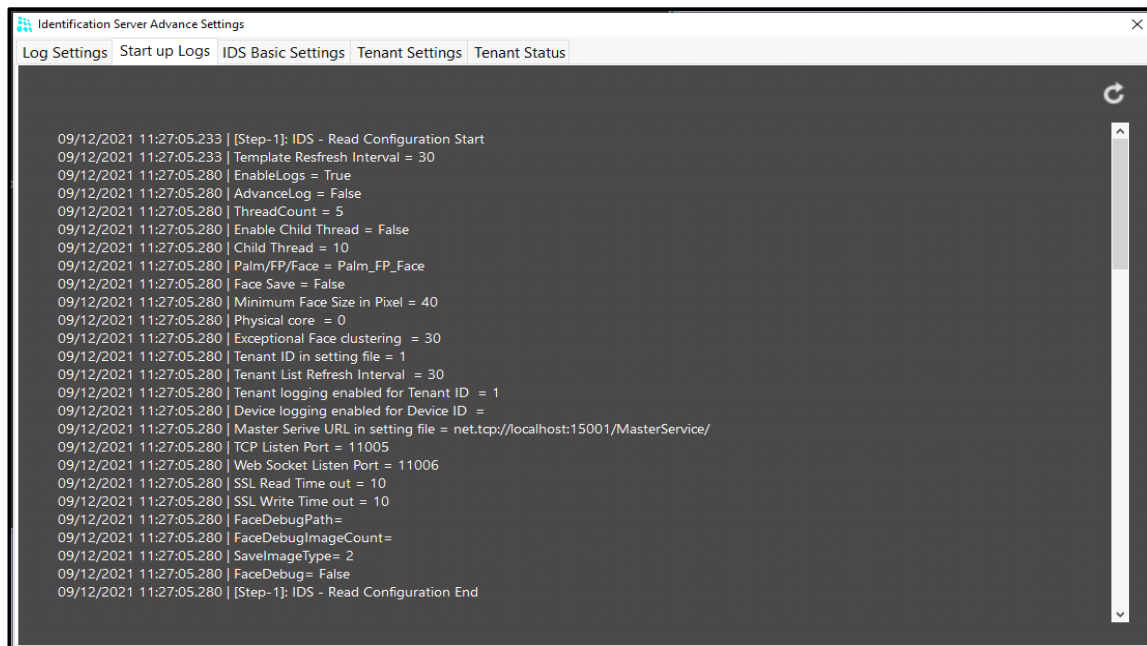
Click **Send** and the respective logs will be stored in the COSEC Identification Server in the Logs folder. These logs can be used for troubleshooting issues related to IDS by the Support Team.



If in case you restart the Identification Service, the configured log settings will be reset. You need to configure it again.

Start up Logs

Click the **Start up Logs** tab if you desire viewing the previous start-up logs of the identification Service. The **Start up logs** page appears as below:



If you stop and then start the IDS, the previous logs will be replaced with the current logs.

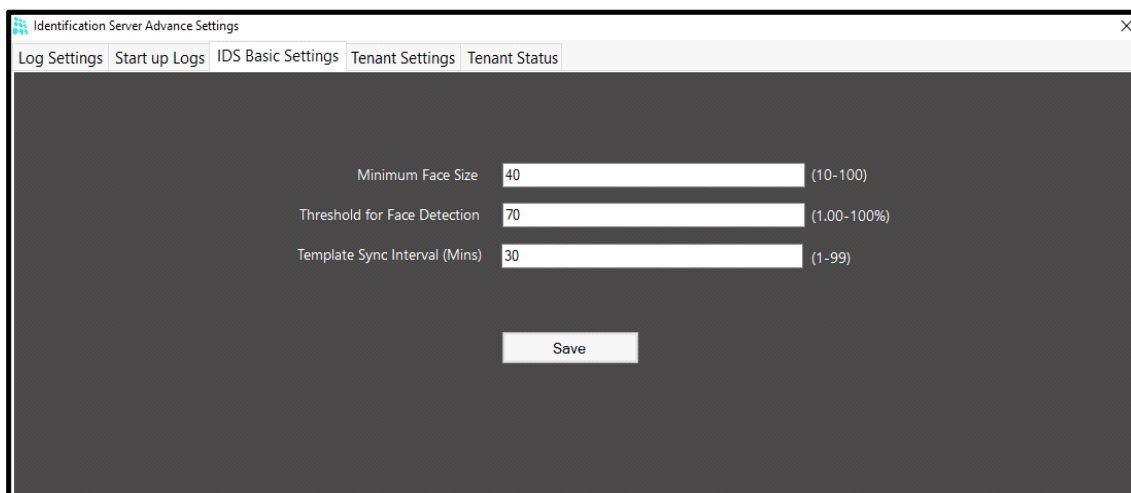
Click **Reload**  , to refresh the logs on the page.



In the event, when user stops IDS and starts immediately, logs may not be displayed because, before IDS could complete its stopping task, the start command was executed in that case the user will have to reload logs after some time.

IDS Basic Settings

Click the **IDS Basic Settings** tab, in order to configure the basic settings of the Identification Service. The page appears as below:

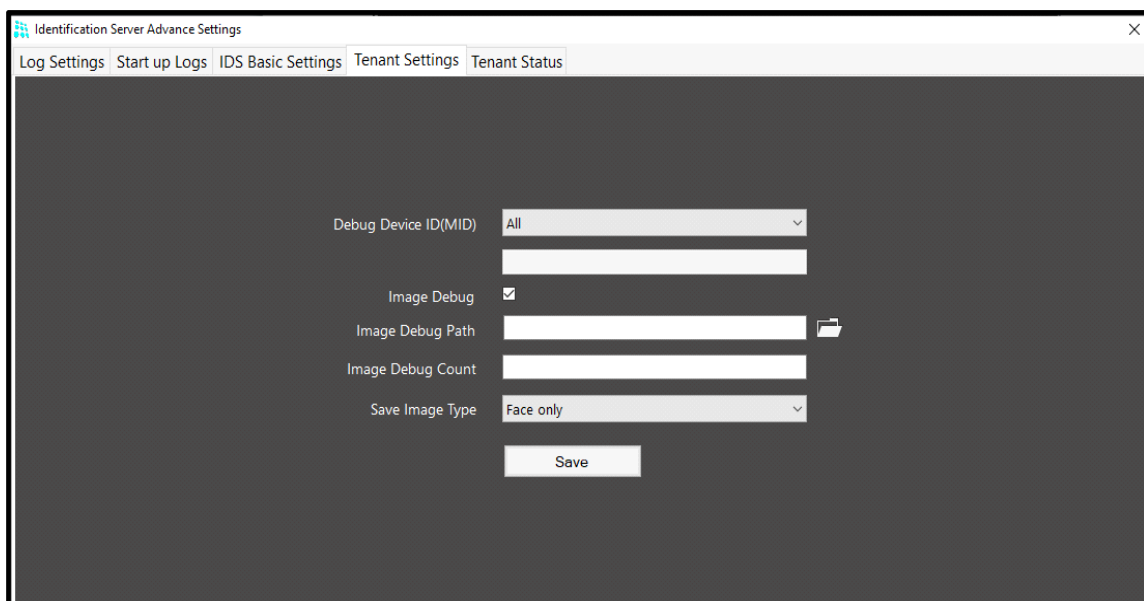


Configure the parameters:

- **Minimum Face Size:** Specify the minimum percentage value of face mandatory in the frame, for the face to be detected.
- **Threshold for Face Detection:** Specify the desired threshold value in percentage to detect a face.
- **Template Sync Interval:** Specify the desired time after which the Identification Service will request the Enroll Service to sync the face template.

Tenant Settings

Click **Tenant Settings** tab, to configure the parameters of the tenant. The **Tenant Settings** page appears as shown below.



Configure the parameters:


- **Debug Device ID(MID):** You can select the desired device/s from which you intend to get logs as well as face images.

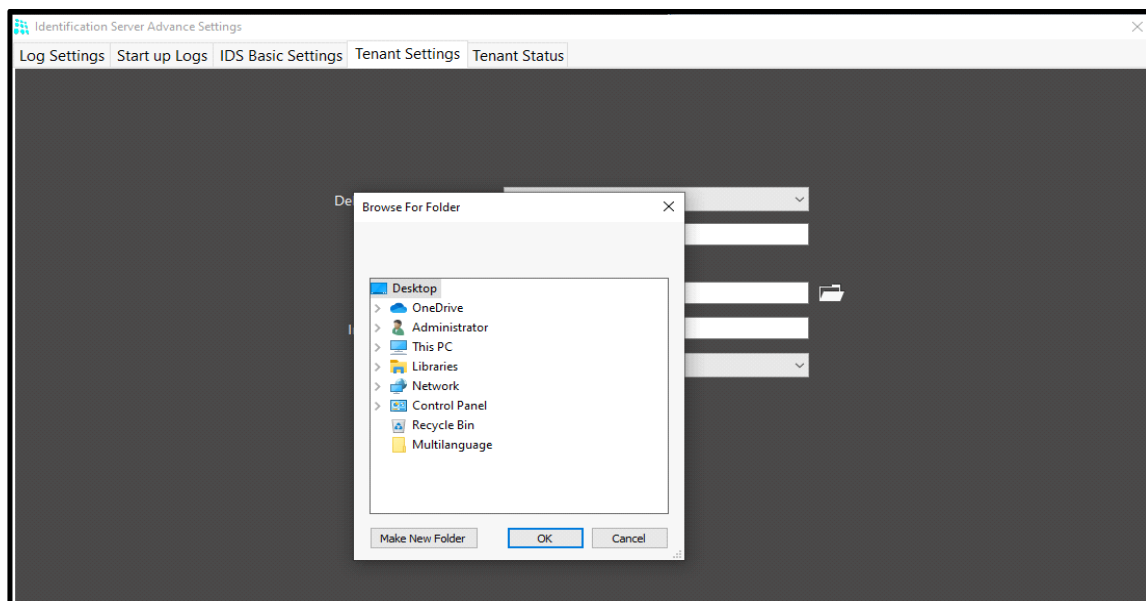
From the dropdown list:

- Click **All** if you desire logs from all the devices.
- Click **Selected** if you desire logs from a specific device. Enter the Device ID in the text box.



To debug multiple devices make sure you specify Device ID as comma-separated values. For example, if you desire logs/image templates of three devices, that is, 15, 05, 44 then select **Selected** as the Debug Device ID (MID) option and in the text box enter the values as 15, 5, 44.

- **Image Debug:** Select the checkbox to enable image debugging.
- **Image Debug Path:** If you have enabled the **Image Debug** checkbox, mention the path where you wish to store the images. Click on the icon  and a pop up appears, browse and select the respective folder. Click **OK**.

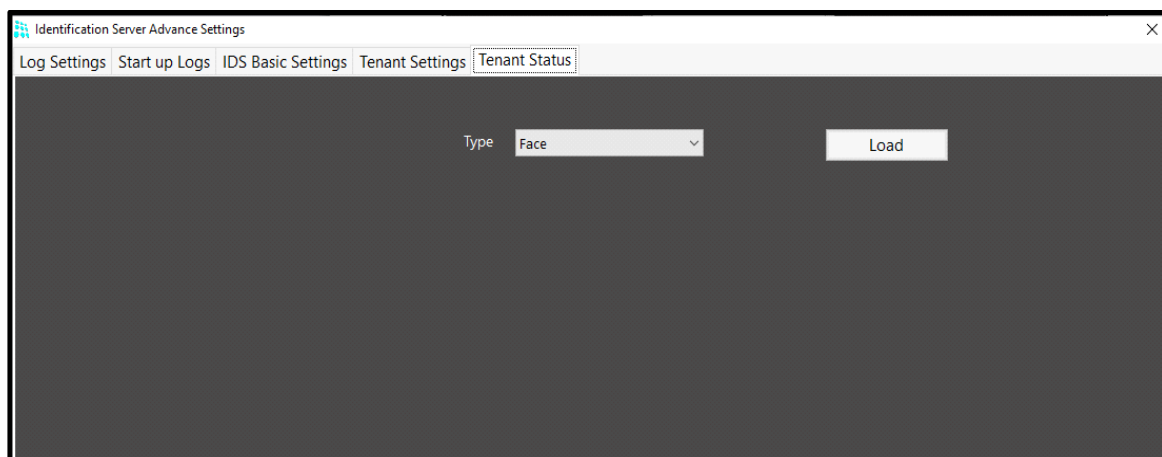


- **Image Debug Count:** Specify the desired number of images you wish to store in the folder on the above mentioned path.
- **Save Image Type:** Select the image type from the drop down list.
 - Select **Face only** if you desire saving only images with face.
 - Select **All** if you desire saving all images, that is, with or without face.

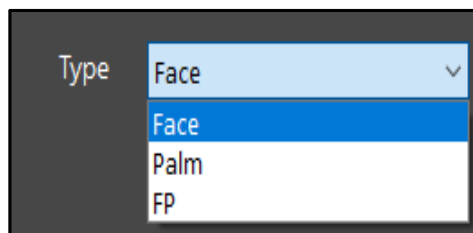
Click **Save** to save the configured parameters.

Tenant Status

Click the **Tenant Status** tab in order to configure the type of tenant status. The **Tenant Status** page appears as shown below:



- **Type:** From the drop down list select the desired type of tenant status —**Face**, **Palm** or **FP**.



- Click **Load**. According to the **Type** selected the information regarding the tenant will be displayed. The following screen appears.

Identification Server Advance Settings

Log Settings Start up Logs IDS Basic Settings Tenant Settings Tenant Status

Type: Face Load

STAGE: Running STARTUP DATE TIME: 09/12/2021 11:27:34

QUEUE IN

0

NAME	STATE	LAST ACTIVITY TIME
FACEPT_1_1	Idle	-
FACEPT_2_1	Idle	-
FACEPT_3_1	Idle	-
FACEPT_4_1	Idle	-
FACEPT_5_1	Idle	-

QUEUE OUT

0

0 User Face Template 09/12/2021 05:51:23

0 Visitor Face Template 09/12/2021 05:51:23

0 All Face Template N/A

0 Palm Template 09/12/2021 11:20:30

0 Finger Template 09/12/2021 11:20:30

Master Service Settings

Master Server Settings

Tenant ID: 1

Master Service Address: 192.168.103.155:15001

IP Address: 192.168.103.155-Ethernet

Login ID: sa

Password: *****

OK

Configure the following parameters of Master Service:

- **Tenant ID:** Enter the COSEC Tenant ID.
- **Master Service Address:** Enter the IP Address or URL of the Master Service.
- **IP Address:** If your PC is having multiple network connections, the IP Addresses of these networks will be displayed in the drop down list.

Select the desired IP Address.

The IP Address of the enabled network will be set as the default IP Address for this service.



If none of the network connections are enabled, then IP Address of the running service will get updated to 127.0.0.1 - Localhost and the services will continue running.

To restore the IP Address to the desired one, you must first enable the connection from network connections and then select its IP Address from the drop down list manually.




As the Windows10 PC boots up fast, so services will check and retry for the availability of assigned IP address before finally moving to 127.0.0.1



If more than one network connections are enabled then the first enabled network connections IP Address will be assigned to all the services on service startup after installation.



If the PC is assigned a DHCP Addressing scheme, then whenever the IP Address changes, the same will be updated against every service.

Click **Refresh IP List**  to update the list of all network adapters (network connections).

- **Login ID and Password:** Enter the Login ID and Password same as configured in the COSEC Web.

Click **Save** to save the settings.



Existing COSEC users must upgrade to COSEC V9R3 for the Identification Service feature to function as expected. On upgrading to COSEC V9R3, any Identification Server configuration performed from the device Web page shall be reset and will require to be re-configured from the COSEC Web application. It is recommended that all Identification Server configuration be performed from the COSEC Web application only.

Identification Server Configuration

This page enables the administrator to configure multiple Identification Servers and assign devices and enterprise groups to each of them. An Identification Server can be assigned to multiple enterprise groups (i.e. department, branch etc.) at a time. However a device can be assigned to only one Identification Server at a time.



For Group FR ("Mark Group Attendance"), Exceptional Face Enrollment and Face Enrollment via Web feature to work, ensure that Identification Service is defined in COSEC Admin > License and Service. For more details refer Admin Management Portal User Manual.

To configure an Identification Server,

Go to **Admin module > System Configuration > Identification Server Configuration** and the following screen appears.

Identification Server Configuration

← + ✎ 🗑️ 💾 ✕ ↺

ID * 1 Identification - 4CCC6A15649C

MAC Address * 8C : EC : 4B : 4C : 53 : CC

Server Address 192.168.103.27

Support Global Identification ☐

Enable Secure Communication ☐

Matching Threshold(Face) * 94.00 %

Biometric Group Based Identification ▼

Assign Groups ▼

Assign Devices ▼

- When an Identification Server and the COSEC Server both are installed on the same system, then the identification server will get automatically added on the Identification Server Configuration page.
- You only need to configure other required parameters. But if an identification server is installed on the other system then you need to configure it manually by clicking **New** button and providing the following parameters as described below.
- **Name:** Enter a suitable name for the Identification Server.
- **MAC Address:** Enter MAC Address of the PC where Identification Server is installed.
- **Server Address:** Enter IP Address of the system where Identification Server is installed.
- **Support Global Identification:** Select the check-box to enable identification of all the COSEC users whose finger/palm has been enrolled from an enrollment station.
 - If not selected then templates of only those users will be identified which are stored locally.
- **Enable Secure Communication:** Select the check-box to establish secure communication with server.
- **Matching Threshold (Face):** Enter the Matching Threshold in percentage for Face identification. It also accepts upto two decimal points.

Example: If you set Matching threshold as low (e.g.: 20%) then your Face may match with other person. But if you set matching at high percentage (e.g.: 90%) then more accurate matching of your template will be done and accordingly access will be granted or denied.

Biometric Group Based Identification

In the Biometric Group Based Identification panel, configure the required parameters for minimizing the search time of template by classifying the templates based on user's biometric group number. Also, configure parameters for handling Roaming Users template.



The firmware (V10R2) of Identification Server and Devices must be upgraded to work in sync for searching templates in threads.

- **Enable:** Select the checkbox to activate the biometric group based identification feature. If enabled, Identification Server will maintain the biometric group wise user templates.
- **Extended Search:** Select the checkbox to do extended search, if the user's biometric group specific template match is below the configured matching threshold.
- **Extended Search In:** If extended search is enabled, select the group for which Extended Search In should be done, i.e. Roaming Group or All.
- **Matching Threshold Palm/FP:** Enter the Matching Threshold in percentage for Palm identification. Also, select the Matching Threshold (FP) for finger print to be configured for matching the FP template.

If you set Matching threshold as low (Example: 20%) then lose matching may be found. i. e. your template may match with other person. But if you set matching at high percentage (Example: 70%) then more accurate matching of your template will be done and accordingly access will be granted or denied.

Example:

The Biometric group number of Device at R&D is 1 and HO is 2. The default Biometric group number of users belonging to R&D is 1 and those of HO is 2.

A user Ashish (roaming user) belonging to HO (biometric group no.2) when regularly punches on device at HO, then his templates are searched from thread handling group number2. The Identification server stores the Roaming user templates at 0.

When Ashish punches at R&D then his template is searched from group1. If you have enabled Extended search and selected Roaming group, then the template will specifically search from Roaming user templates. This will reduce the time for identification. If you select option for extended search to All, then templates will be searched from all the threads.

Assign Groups

In the **Assign Groups** panel, select enterprise groups to be assigned to the Identification Server. For e.g. Admin can select the Group “Branch” in User Filter and select users of Branch-1 to be assigned to the current Identification Server. Similarly all users of Branch-2 can be assigned to a different Identification Server.

Assign Groups

Select Users: Group Wise

Select Group: Organization

Organization* ID: Name: [Picklist]

Search

ID	Name	Group	
1	Organization-1	Organization	[Delete]

Assign Devices

Similarly, in the **Assign Devices** panel, select one or multiple devices to be assigned using the picklist button.

Assign Devices

Face Recognition

Device ID: Name: [Picklist]

Search

MID	Name	Type	
1	ARGO-Device-1	ARGO	[Delete]

Other Biometric Credentials

Device ID: Name: [Picklist]


Search

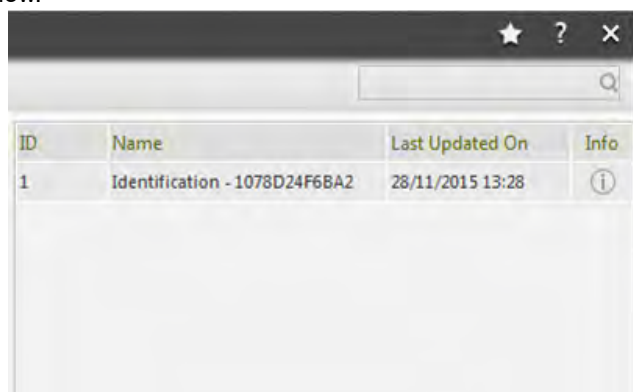
MID	Name	Type	
No Data			


- **Face Recognition:** Select the Device from the pick-list and assign it to the Identification Server at where the Face templates will be saved.
- **Other Biometric Credentials:** Select the Device from the pick-list and assign it to the Identification Server where the Other Biometric credentials will be saved.



The configuration done in Assign Devices for Face Recognition and Other Biometric Credentials will also be updated into the Device Configuration > Identification Server section.

Click **Save** . The new Identification Server will appear in the grid list on the right hand side of the page as shown below.

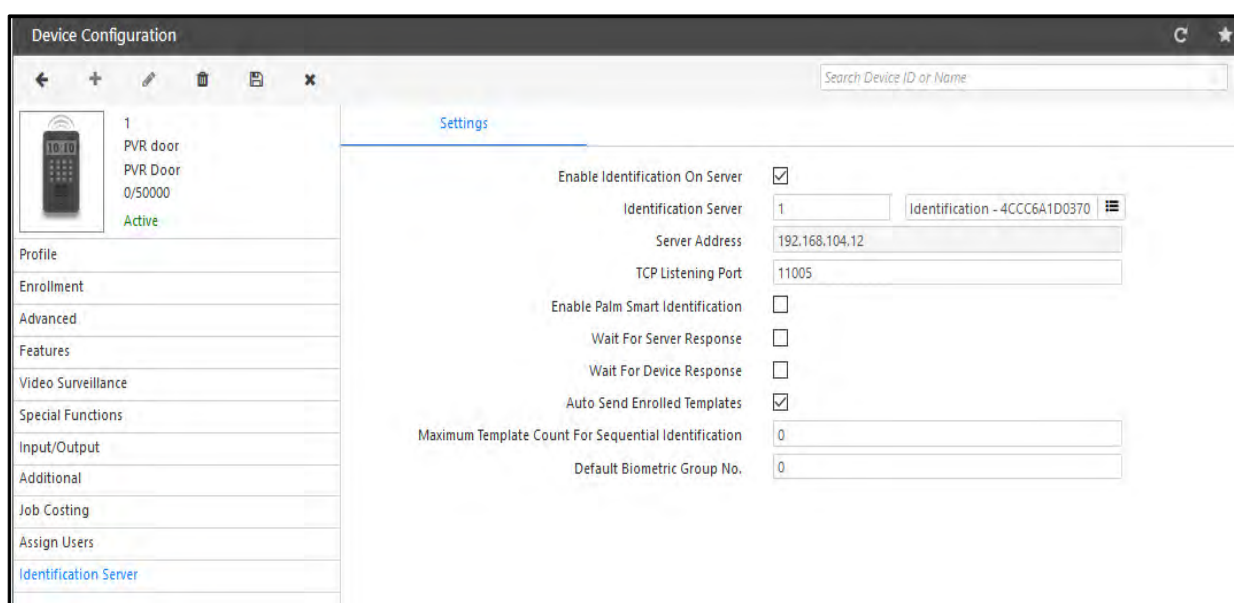


ID	Name	Last Updated On	Info
1	Identification - 1078D24F6BA2	28/11/2015 13:28	

The **Last Updated On** column displays the date and time at which the server last came online. Hover your mouse on the **Info** icon to view the time duration since the server last came online.

After the IDS configuration has been done in System Configuration, you now need to configure the parameters in the desired devices.

The COSEC device (Eg: PVR door) on which identification of user is to be done through IDS; must be assigned the IDS settings from Device Configuration> Identification Server.



10.10

1

PVR door

PVR Door

0/50000

Active

Profile

Enrollment

Advanced

Features

Video Surveillance

Special Functions

Input/Output

Additional

Job Costing

Assign Users

Identification Server

Settings

Enable Identification On Server

☒

Identification Server

1

Identification - 4CCC6A1D0370

Server Address

192.168.104.12

TCP Listening Port

11005

Enable Palm Smart Identification

☐

Wait For Server Response

☐

Wait For Device Response

☐

Auto Send Enrolled Templates

☒

Maximum Template Count For Sequential Identification

0

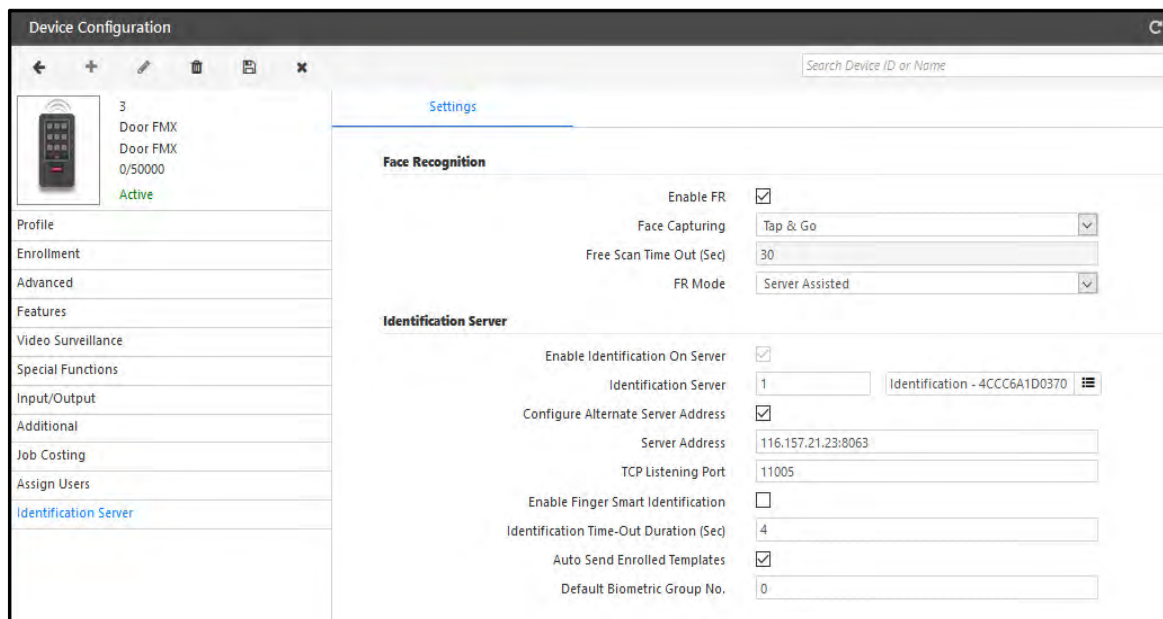
Default Biometric Group No.

0

The enrolled templates of user are stored in Identification server.

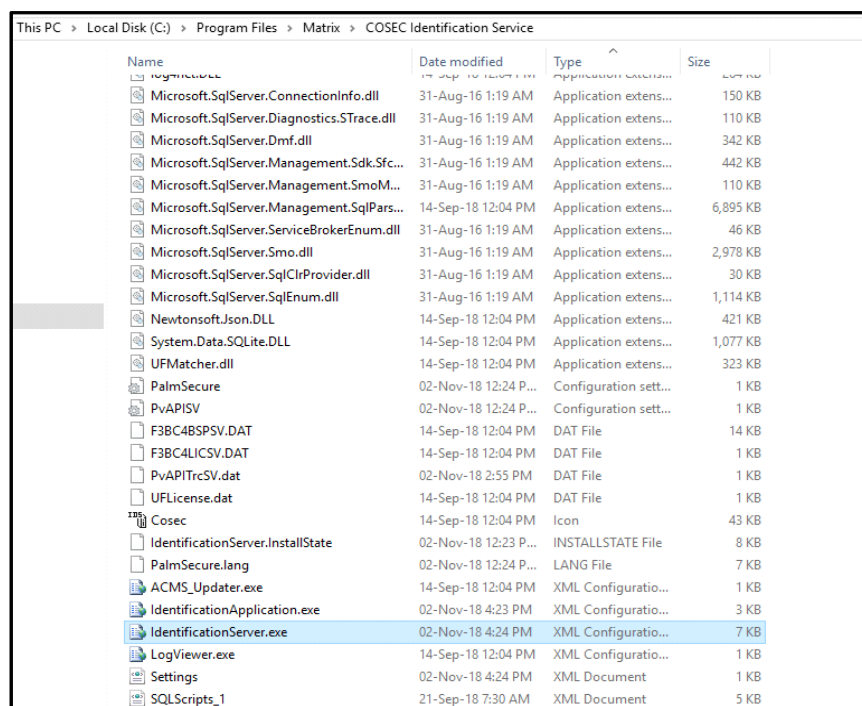
Now when a user punches on PVR door, his palm template will go to Identification server for matching. The Identification server matches the palm template with the stored templates and gives the response to device and hence user is identified/rejected accordingly.

When new template of user is enrolled, it can be sent to the identification server if “Auto Send Enrolled Templates” checkbox is enabled. Also Identification server automatically checks for new templates after every 2 minutes (by default).



For Devices such as FMX, Vega, ARGO and MODE, the identification of Face can be done through Local as well as Server Assisted Mode. For Server Assisted Mode; FR server must be installed and its IP address and Port must be specified in the Configuration file as explained below.

The **Settings** File and **Configuration** File is available in Program files as shown below.




```

73 <appSettings>
74 <add key="DBRetryInterval" value="10" />
75 <add key="ListenPort" value="11005" />
76 <add key="EnableIdsLogs" value="true" />
77 <add key="EnableLogs" value="false" />
78 <add key="AdvanceLog" value="false" />
79 <add key="ThreadCount" value="5" />
80 <add key="EnableChildThread" value="false" />
81 <add key="ChildThreadCount" value="10" />
82 <add key="RefreshMinute" value="30" />
83 <add key="EnrollMinute" value="1" />
84 <add key="PopulationSource" value="1" />
85 <add key="GroupLimit" value="999" />
86 <add key="MaxFRRRequested" value="0" />
87 <add key="GuideModeRefresh" value="60" />
88 <add key="PalmOrFP" value="2" />
89 <add key="FPGroupLimit" value="500" />
90 <add key="FPSecurityLevel" value="4" />
91 <add key="FPFastMode" value="false" />
92 <add key="FPMaxResult" value="1" />
93 <add key="FPTemplateFormat" value="1" />
94 <add key="ClientSettingsProvider.ServiceUri" value="" />
95 <add key="RefreshOnContinuesSocketClose" value="false" />
96 <add key="SocketCloseCount" value="12" />
97 <add key="SocketCloseMinut" value="2" />
98 <add key="SocketLogExe" value="false" />
99 <add key="SocketLog" value="false" />
100 <add key="log4net.internal.Debug" value="false" />
101 <add key="IsInternal" value="true" />
102 <add key="HttpEnable" value="0" />
103 <add key="IsSSL" value="False" />
104 <add key="TenantID" value="1" />
105 <add key="MasterUrl" value="net.tcp://localhost:15001/MasterService/" />
106 <add key="FaceServerIP" value="" />
107 <add key="FaceServerPort" value="" />
108 <add key="FaceTCPortHTTP" value="" />
109 </appSettings>

```

You can edit the tag as per your requirement. The description of tag can be viewed in **Parameter Description** comments when the particular tag is selected.

Some of the tags are described here:

DBRetryInterval: When Identification service loses connectivity with database server; then it is required to connect again so Identification service will retry to connect with Database after every 10 seconds of interval. You can edit this interval.

ThreadCount: It is the number of Identification requests handled by Identification server at once. The default is 5 i.e. at a time identification can be done through 5 devices.

EnrollMinute: When new enrollment is done; then after every 2 minutes (default) the templates will be updated in Identification server. You can edit this time for updating the enrolled templates to identification server.

GroupLimit: When there are more than 4000 Palm templates in Identification server then templates can be grouped which will reduce the time for identification. Suppose there are 10,000 templates in a server and the algorithm can run for 3999 templates at once so the templates will be divided into 3999,3999 and 2002 for faster identification in group. The default grouping is for 999 templates.

PalmOrFP: The default value is 2 = Palm+ FP. To include Face credential change this parameter to 6 = Palm + FP + Face.

FPGroupLimit: When there are more than 50000 FP templates in Identification server then templates can be grouped which will reduce the time for identification. The default grouping is for 500 templates.

FPSecurityLevel: Default is 4, max is 7 and minimum is 1

FPTemplateFormat: FP Template Format(0-Proprietary , 1- ISO) : Default is 0

FaceServerIP: IP address of face server. The Face server must be installed for identification to be done through FR Mode as Server Assisted.

FaceServerPort: Port number of the face server.

FaceTCPorHTTP: 0=TCP, 1=HTTP

SMS Configuration

This tab enables to configure parameters for sending SMS using one the selected SMS service providers.

To view SMS Configuration page, go to **Admin module > System Configuration > SMS Configuration** and the following screen appears.

The screenshot shows the 'SMS Configuration' window. At the top, there's a title bar with 'SMS Configuration' and standard window controls. Below the title bar, there's a left arrow icon. The main content area contains the following fields and controls:

- Service Provider:** A dropdown menu showing 'SMS Lane' with a '+' button to add a new provider.
- Active:** A checkbox that is checked.
- User Name:** A text input field containing 'sa'.
- Password:** A text input field containing '*****'.
- Sender ID:** A text input field containing 'KUNAL'.
- Flash Message:** A checkbox that is unchecked.
- Account Type:** A dropdown menu showing 'Promotional'.
- Alert Cycle:** A text input field containing '10', with a label 'Seconds (1-120)' to its right.
- Retry Count:** A text input field containing '3', with a label '3-99' to its right.
- Active Days:** A text input field containing '1', with a label '1-9' to its right.
- Disable Sending SMS:** A checkbox that is unchecked.
- www.smslane.com:** A link to the service provider's website.
- Save** and **Cancel** buttons.
- Test Message** section with a sub-header and two input fields:
 - Phone Number:** An empty text input field.
 - Template ID:** An empty text input field.
 - Send** button.

The page displays configurations for the added service providers. The pre-defined service providers are: SMS Gateway Center, SMS Lane, Business SMS, Bulk SMS, Smart Life Tech and SNOWEBS.

To set SMS configurations provide the following parameters:

- **Service Provider:** Select the service provider to be used for sending SMS from the dropdown list. One can also add a new Service Provider by clicking on **Add Service Provider** + button and the following API Configuration pop-up window appears.

The screenshot shows the 'API Configuration' window with the following fields and tables:

- Service Provider Name:** way2sms
- Service Provider URL:** http://way2sms.com
- Base URL:** localhost/way2sms/login
- Search:** (empty)
- API Arguments Table:**

API Argument	Argument Value	Custom Value
enc	Custom	1
msg	Message	
pwd	Password	
number	Phone No.	
sid	Sender ID	
uname	User Name	
- Argument Separator:** ;
- Request Method:** Post
- Request Preview:** localhost/way2sms/login?uname=test;pwd=test;sid=test;number=test;msg=test;enc=1
- Balance Check:** ☐
- Search:** (empty)
- API Response Table:**

API Response	COSEC Response
0	Failure
1	Success
- Buttons:** Save, Cancel

Enter the following parameters as given in the API document of the service provider:



The API Document of the service provider is mandatory for configuring the below parameters.

- **Service Provider Name:** Enter the name of SMS service provider.
- **Service Provider URL:** Enter the url of the service provider. This url is displayed on the main SMS configuration page.
- **Base URL:** Enter the base url of the service provider. E.g: localhost/way2sms/login
- Click Add button to associate **API Arguments** with the **Argument value** selected from the dropdown list. These API arguments are available in the API document of the service provider.
- **Argument Separator:** Enter the argument separator to be used for firing a command. E.g.: & or ;. Also, select the method to be used for sending the message from the dropdown list.
- **Request Preview:** Displays the preview of the url with arguments.
- **Balance Check:** Select to allow balance check, if the service provider needs to use it.
- Click **Add** button and provide the **API Response** for failure or success of the COSEC response.

Click **Save** button to save the above API configurations and return to the main page where you need to configure the remaining below given parameters.

- **Active:** Enable to activate the selected service.
- **User Name:** Enter the username.
- **Password:** Enter the password.



Contact the administrator to get user name and password for using the SMS service.

- **Sender ID:** Enter the registered sender ID.
- **Flash Message:** Enable the checkbox to flash the message at the time of arrival.
- **Alert Cycle:** Specify the time in seconds between successive send attempts when the system tries to send the pending messages.
- **Retry Count:** Specify the number of times the system needs to try to send the message. The retry count can be from 3 to 99.
- **Active Days:** Specify the number of days till which the pending messages are treated as active in the event of the Alert service being temporarily stopped. Maximum 9 active days can be specified.
- **Disable Sending SMS:** Select to temporarily disable the SMS sending functionality.

The URL displayed is a link to the website of the selected service provider. Click on the link and login with your user-name and password to connect with service provider.

Click **Save**, once all the configurations are done. The created service provider gets displayed in the dropdown list as shown below.

Test Message

- **Phone Number:** Enter the mobile number to send the test message for testing the settings.
- **Template ID:** As per TRAI Regulation, an enterprise which sends messages to customers like OTP, communication message, promotional messages via SMS, have to register their entity and the content template to avoid Spam, fake and fraudulent communication through SMS.

It is mandatory for an Admin to register the SMS content template prior with your Service Provider which will be verified before it is delivered to the users.

Once registered, the Service Provider will provide a Template ID against the registered SMS content.

Here, a test message content is pre-defined, which has to be registered with the Service Provider.

The test message which is to be registered is — **Hello this is a test message.**

The Service Provider will provide a Template ID against this test message.

Enter the Template ID provided by the Service Provider.



If you have multiple Service Providers, then make sure the required templates are registered with all the desired Service Providers. Hence for each template you will have multiple Templates IDs. Also make sure you maintain a record of all the registered Message Templates with their respective Template IDs for reference.

Click **Send** to link the phone number and the test template ID with the respective Service Provider.



For each tenant, you can send upto 10 test messages in one minute. Thereafter the message “Maximum count reached. Please try after sometime” will be displayed.

Email Configuration

This tab enables to set email configurations. Before configuring ensure that an SMTP Server has been set up on the network.

To view Email Configuration page, go to **Admin module > System Configuration > Email Configuration** and the following screen appears.

The screenshot shows the 'Email Configuration' page. It has a title bar with a back arrow, refresh, star, and help icons. The main content area contains the following fields:

- SMTP Server* (text input)
- SMTP Port Number* (text input, value: 25)
- Incoming Mail Protocol (radio buttons: POP3 selected, IMAP)
- POP3 Server* (text input)
- POP3 Port Number* (text input)
- Sender E-mail ID* (text input)
- Sender Display Name (text input)
- Authentication (dropdown menu: Basic Authentication)
- User Name* (text input)
- Password* (text input)
- Alert Cycle (Sec)* (text input, hint: Seconds (1-120))
- Retry Count* (text input, hint: 3-99)
- Active Days* (text input, hint: days (1-9))
- Enable SSL (checkbox)
- Disable Sending Mail (checkbox)
- Email Reading Interval* (text input, value: 30, hint: Minutes (1-30))
- Delete Mail (dropdown menu: All, hint: i)
- Auto Forward E-mail ID (text input, hint: i)

At the bottom, there is a 'Test Mail' section with an 'Email ID*' field and 'Save' and 'Cancel' buttons.

Enter the following parameters:

- **SMTP Server:** Specify the IP Address or name of the configured SMTP server. Check the server availability with your network administrator.



You can use Gmail SMTP Server if Internet connection is available.

- SMTP server : smtp.gmail.com
- SMTP Port: 587(POP3)/993 (for imap)
- Email ID: gmail id of the user
- **SMTP Port Number:** Specify the TCP port for the SMTP service as set on the SMTP server.
- **Incoming Mail Protocol:** In the event of activating the approve/reject links in the leave application alerts the user needs to specify the mail protocol for the incoming mails.
- **POP3/IMAP Server:** Specify the IP Address or name of the configured POP3 or IMAP server.
- **POP3/IMAP Port Number:** Specify the appropriate incoming port for the SMTP service as set on the SMTP server.

- **Sender E-mail ID:** Mention the Email ID of the sender.
- **Sender Display Name:** Specify the user name as to be displayed in the emails.
- **Authentication:** Select a desired method of authentication from the drop down list — Basic Authentication and Modern Authentication.
 - **Basic Authentication:** It provides a simple mechanism to perform authentication.

Basic Authentication works by prompting a web server user for a username and password.

It repeatedly sends username and password on each request which will be stored in the server to avoid constantly prompting the user for their credentials.

Also, all the information is sent over the network in an unencrypted format.

Any password sent using Basic Authentication can easily be decoded making it vulnerable to replay attacks which proves, it is not a secure method of authentication.

If you select Basic Authentication, configure the following:

- **User Name:** Specify the user name as set in the outlook account.
- **Password:** Specify the password as set in the outlook account.
- **Modern Authentication:** It is a combination of authentication and authorization between client and server.

The screenshot displays the configuration window for Modern Authentication. At the top, three dropdown menus are set to 'Modern Authentication', 'Microsoft Office 365', and 'Authorization Code'. Below these is a 'Get Token' button. The main configuration area includes fields for 'Authorization URL' (https://login.microsoftonline.com/common/oauth2/v2.0/authorize), 'Access Token URL' (https://login.microsoftonline.com/common/oauth2/v2.0/token), 'Client ID', 'Client Secret', 'Redirect URL' (https://<Domain URL for COSEC Login>/Oauth/AccessToken), 'Scope' (offline_access https://outlook.office.com/POP.AccessAsUser.All https://), and 'Client Credentials' (In Basic Auth Header). A 'Get Token' button is located below these fields. The bottom section contains fields for 'Access Token', 'Refresh Token', 'Alert Cycle (Sec)' (with a hint 'Seconds (1-120)'), 'Retry Count' (with a hint '3-99'), 'Active Days' (with a hint 'days (1-9)'), 'Enable SSL' (checkbox), 'Disable Sending Mail' (checkbox), and 'Delete Mail' (dropdown set to 'All').

Pre-requisites for Modern Authentication

Microsoft 365 Configuration

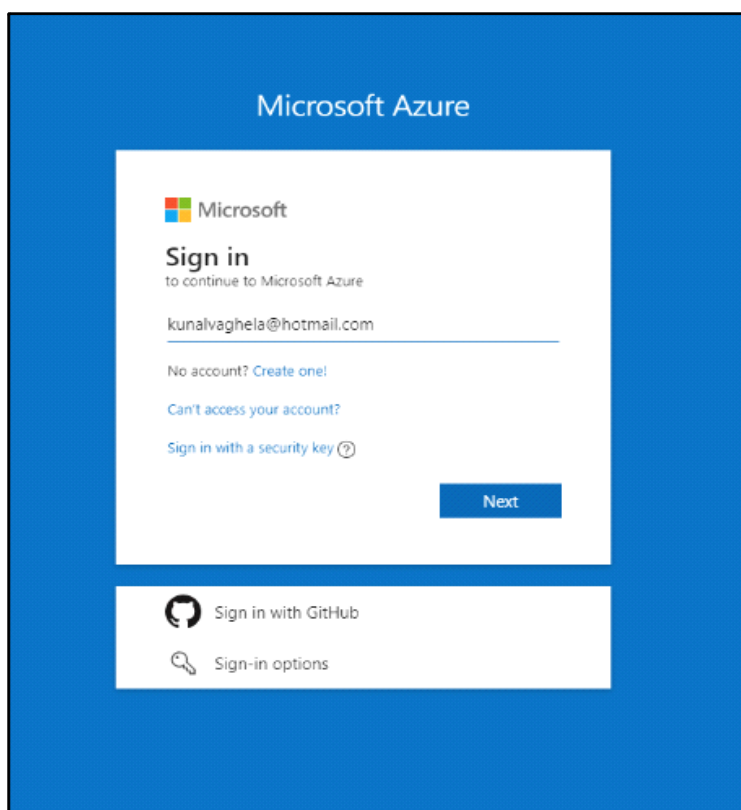


Make sure you have Internet connectivity in your PC.

- Enter the **portal.azure.com** in your Web Browser.



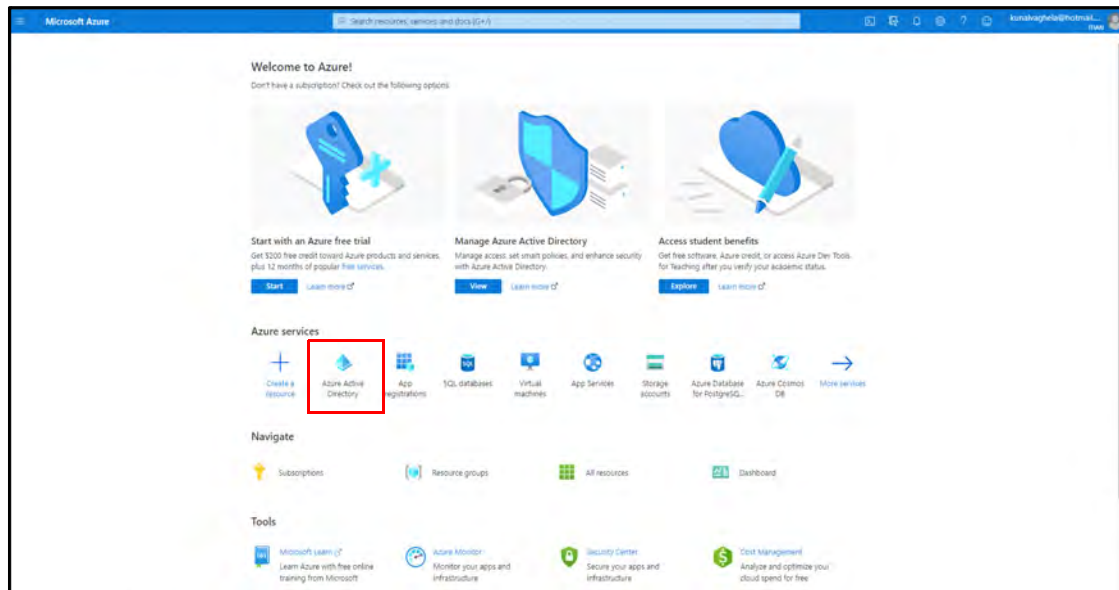
- Create Microsoft Azure Account.



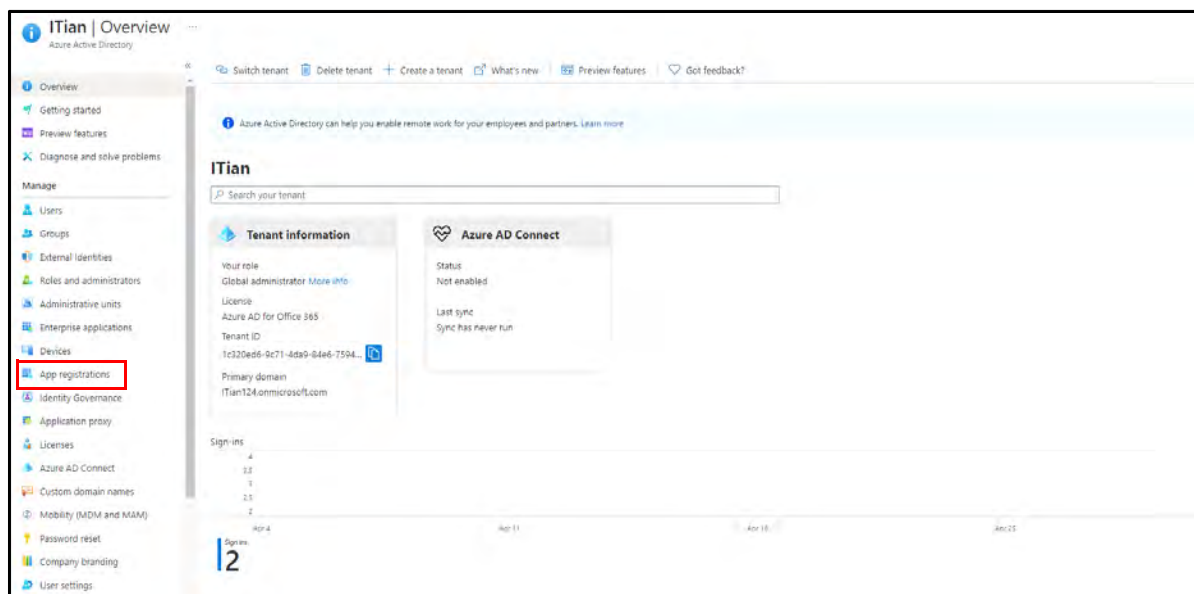
*Make sure the **Sender Email ID** in COSEC Server and the Microsoft Account Email ID are same.*

- Login in to Microsoft Azure Account.

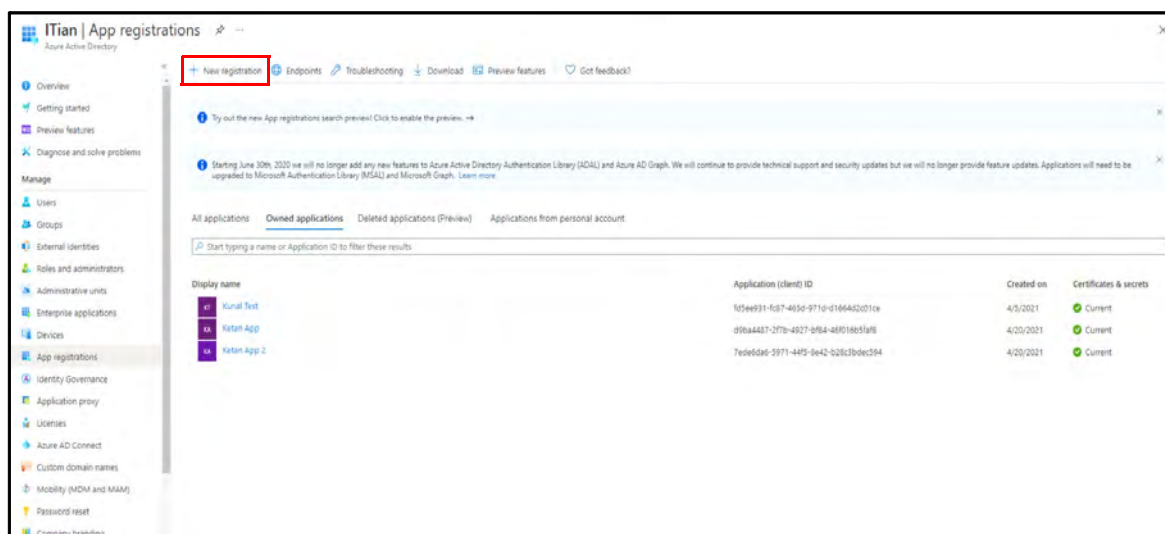
- Click **Azure Active Directory**.



- Click **App Registration** on the left pane.



- Click **New Registration**.



Configure the parameters as mentioned below:

- In **Name**, enter the name you wish to assign.
- Under **Supported Account Types**, select the options **Accounts in any organizational directory (any Azure AD Directory + Multitenant)** and **personal Microsoft Account (eg. Skype, Xbox)**
- **Redirect URI (Optional)**, select the options **Public client/native (mobile & desktop)** and enter the IP Address/Domain Name of the Cossec Server in the format **https://172.16.2.175/cosec/login/ReceiveAuthorizationToken**.

Home > ITian >

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

Athira Application ✓

Supported account types

Who can use this application or access this API?

☐ Accounts in this organizational directory only (ITian only - Single tenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
☒ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile ... ^ https://localhost/cosec/Login/ReceiveAuthorizationToken ✓

Public client/native (mobile & desktop)
Web
Single-page application (SPA)

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#) ☐

Register

- Click **Overview** in the left pane and the Client ID and Tenant ID is visible.

Athira Application ...

Search (Ctrl+J) Delete Endpoints Preview features

Overview Quickstart Integration assistant Manage Branding Authentication Certificates & secrets Token configuration API permissions

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : Athira Application

Application (client) ID : ea31bb05-4865-4b16-b1fd-2b0a850c34e

Directory (tenant) ID : 1c320e96-9c71-4da9-94e6-759482b6a034

Object ID : a0999c03-7987-4e7a-a27e-00a069eeec71

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Supported account types : All Microsoft account users

Redirect URIs : 0 web, 0 spa, 1 public client

Application ID URI : Add an Application ID URI

Managed application in L : Athira Application

- Click **Endpoints**.
- You can view the Access Token URL and Authorization URL

Endpoints



OAuth 2.0 authorization endpoint (v2)

← **Authorization URL**

Copy to clipboard

<https://login.microsoftonline.com/common/oauth2/v2.0/authorize>

OAuth 2.0 token endpoint (v2)

← **Access Token URL**

<https://login.microsoftonline.com/common/oauth2/v2.0/token>

OAuth 2.0 authorization endpoint (v1)

<https://login.microsoftonline.com/common/oauth2/authorize>

OAuth 2.0 token endpoint (v1)

<https://login.microsoftonline.com/common/oauth2/token>

OpenID Connect metadata document

<https://login.microsoftonline.com/common/v2.0/.well-known/openid-configuration>

Microsoft Graph API endpoint

<https://graph.microsoft.com>

Federation metadata document

<https://login.microsoftonline.com/6941876e-c5ea-4c83-a513-96698357096a/federationmetadata/2007-06/federationmetadata.xml>

WS-Federation sign-on endpoint

<https://login.microsoftonline.com/6941876e-c5ea-4c83-a513-96698357096a/wsfed>

SAML-P sign-on endpoint

<https://login.microsoftonline.com/6941876e-c5ea-4c83-a513-96698357096a/saml2>

SAML-P sign-out endpoint

<https://login.microsoftonline.com/6941876e-c5ea-4c83-a513-96698357096a/saml2>



If any user is having multiple tenants then replace the word **common** with the tenant ID in Authorization URL and Access Token URL.

- Click **API Permissions** in the left pane and then click **Add Permission**.

Athira Application | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. [Add MPN ID to verify publisher](#)

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your org.

Configured permissions

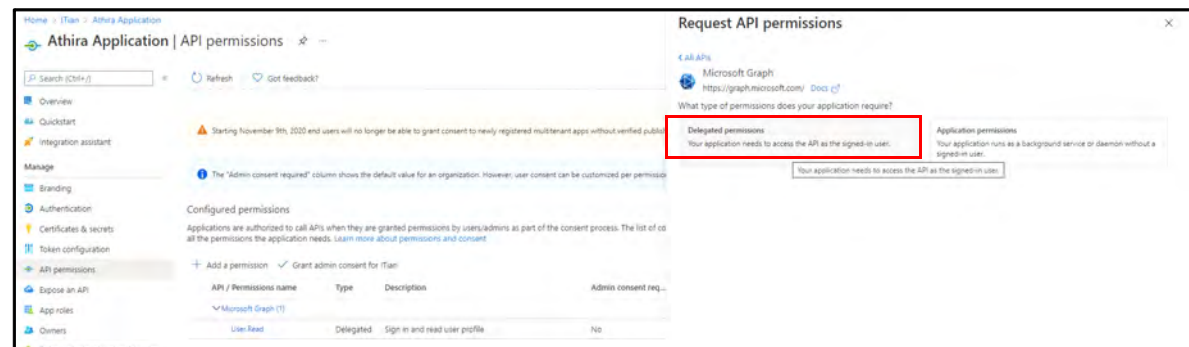
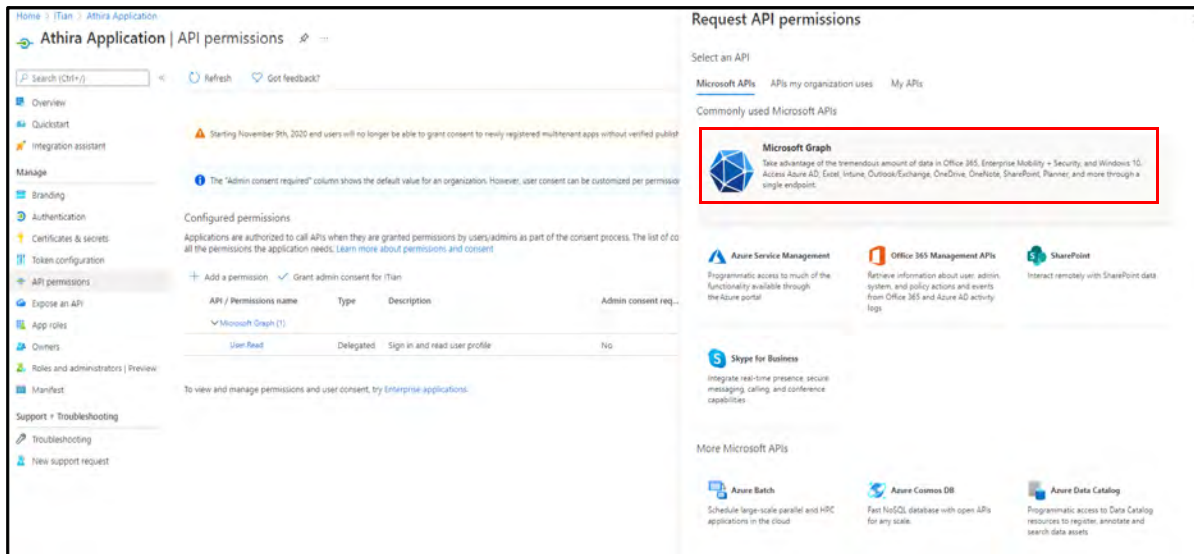
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) ☒ Grant admin consent for ITun

API	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage permissions and user consent, try [Enterprise applications](#).

- In Request API permissions window, click **Microsoft Graph**, then click **Delegated Permissions**.

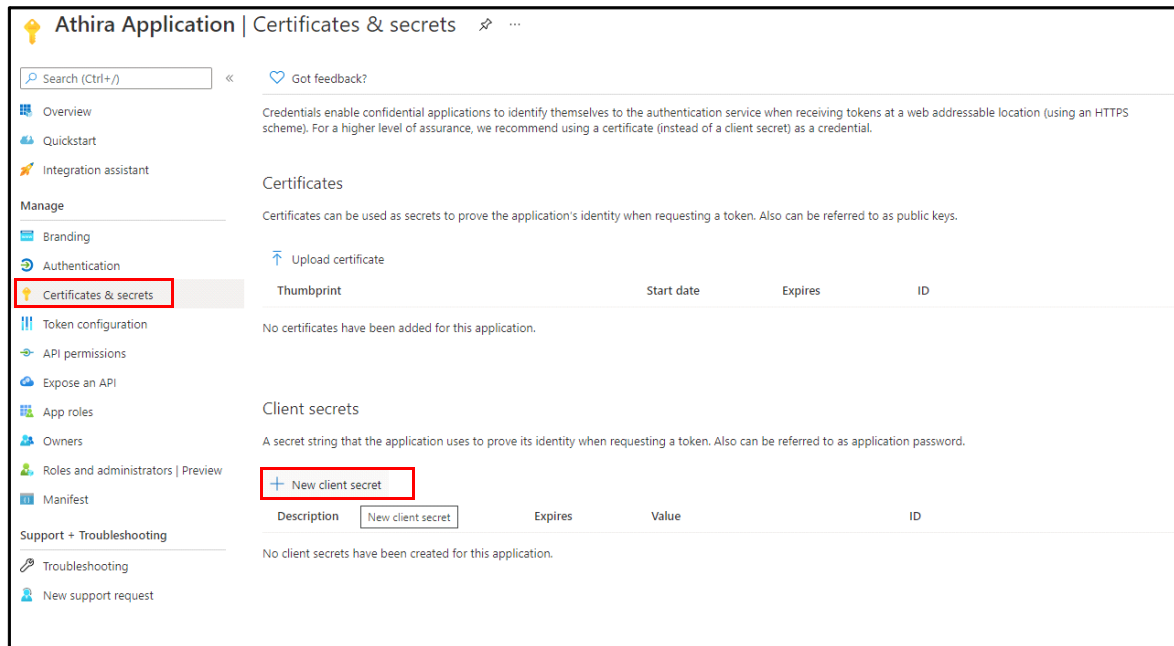


- Select the check boxes of the list of permissions displayed in the below screen.

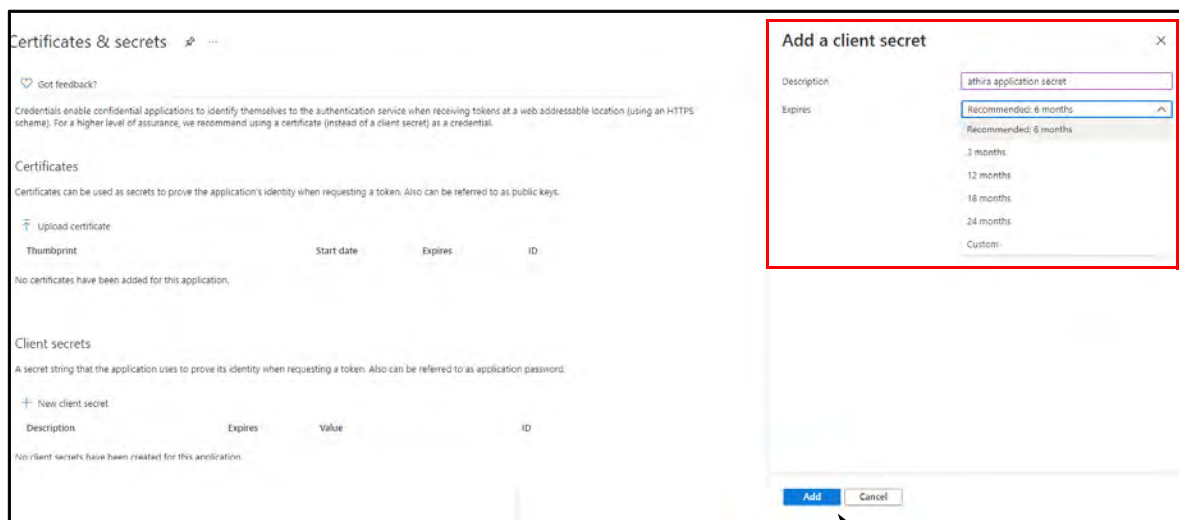
+ Add a permission ✓ Grant admin consent for matrix					
API / Permissions name	Type	Description	Admin consent req...	Status	
▼ Microsoft Graph (10)					
email	Delegated	View users' email address	No	✓ Granted for matrix	...
IMAP.AccessAsUser.All	Delegated	Read and write access to mailboxes via IMAP.	No	✓ Granted for matrix	...
Mail.Send	Delegated	Send mail as a user	No	✓ Granted for matrix	...
Mail.Send	Application	Send mail as any user	Yes	✓ Granted for matrix	...
offline_access	Delegated	Maintain access to data you have given it access to	No	✓ Granted for matrix	...
openid	Delegated	Sign users in	No	✓ Granted for matrix	...
POP.AccessAsUser.All	Delegated	Read and write access to mailboxes via POP.	No	✓ Granted for matrix	...
profile	Delegated	View users' basic profile	No	✓ Granted for matrix	...
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No	✓ Granted for matrix	...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for matrix	...

Once the permissions are added, click **Grant admin consent for matrix**.

- Click **Certificates and secret** on the left pane. Then click **New Client secret**.



- Enter the **Client Secret description** and **Expires**. Then click **Add**.



- The secret will be visible short time period, hence make sure you copy the same.

Athira Application | Certificates & secrets

Search (Ctrl+/) << Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators | Preview
Manifest

Support + Troubleshooting
Troubleshooting
New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	ID
No certificates have been added for this application.			

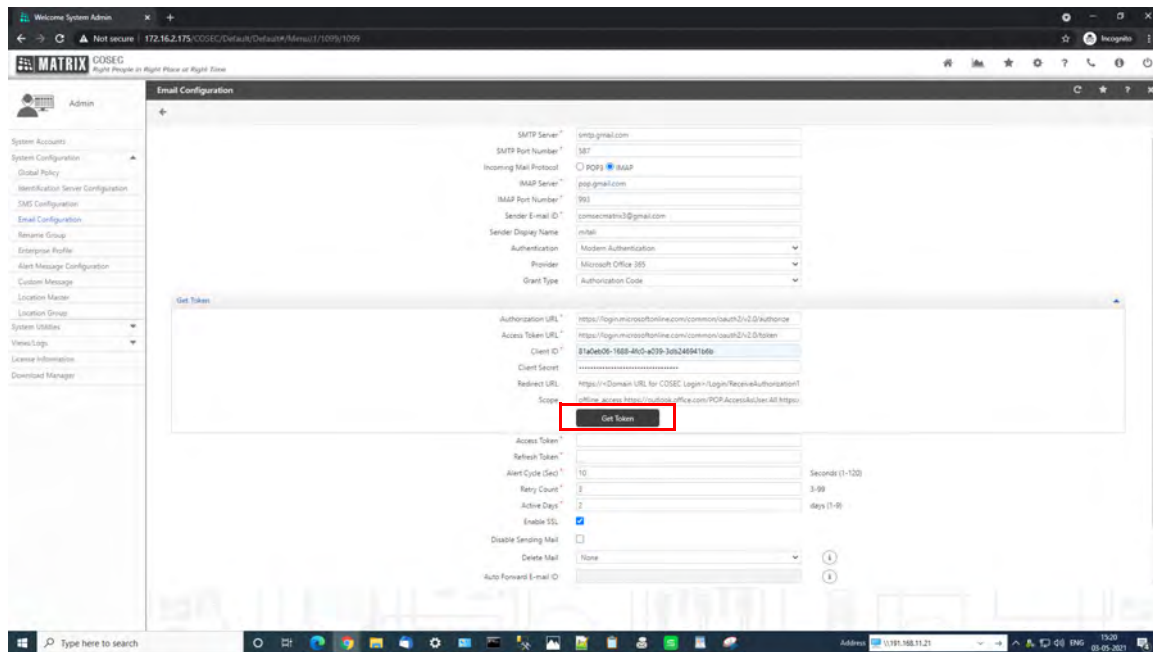
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

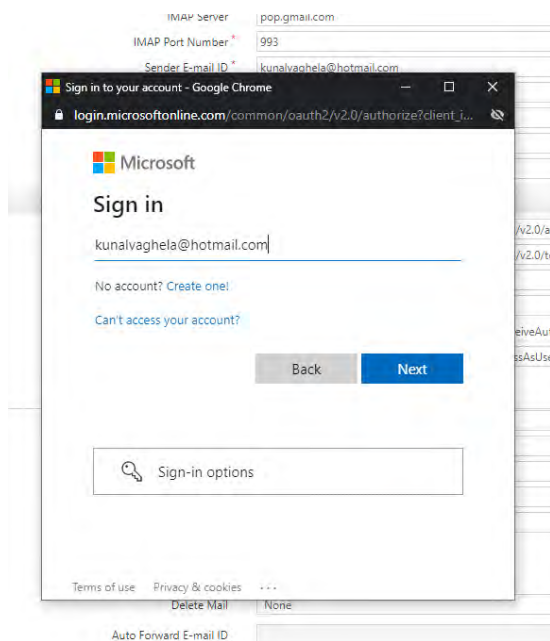
+ New client secret

Description	Expires	Value	ID
athira application secret	11/4/2021	DT0~py55kn2Da5pe2uCl~rcae-szxwd~r	afcbfb1a-790a-4699-9242-9c9b945cf722

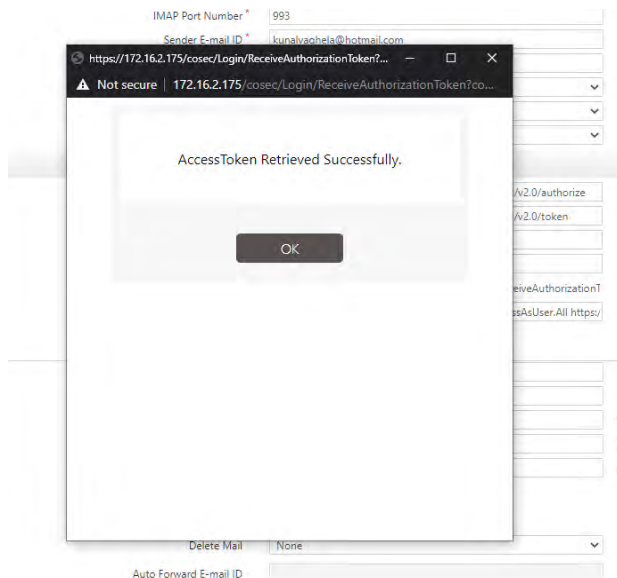
- Now, in the Cospec Server click **Admin module > System Configuration > Email Configuration** (refer *"Modern Authentication - Microsoft 365 Configuration"* and enter the following details as displayed in the screen below:
 - Authorization URL
 - Access Token URL
 - Client ID
 - Client Secret
 - Redirect URL
 - Scope



- Click **Get Token**.
- The **Microsoft Sign in** pop ups appears. Enter the **Microsoft Email ID** and then enter the **Password**.



- Click **Allow** (this is to grant the Read/Write Permission). Then the Access Token Retrieved Successfully pop up appears.



- Click **OK**.

The Access Token and Refresh Token will be updated automatically in the Email Configuration page in the Cossec Server.

Modern Authentication - Microsoft 365 Configuration

Modern Authentication does not allow servers to save Microsoft 365 account details.

To authenticate, a user needs to log in to their account using standard Microsoft 365 login and accept the application's request to access the account.

Access is granted on the basis of tokens which gives a strictly defined permission scope which is accepted by the user.

User receives two tokens namely — Access Token and Refresh Token.

- **Access Token:** This is the most important Token, as on the basis of this, the third party application is allowed access to user data as well as gain access to O365 services.

This token needs to be sent by the client as a parameter or as a header in the request to the third party resource server.

It has a limited lifetime, which is defined by the authorization server.

It must be kept confidential to restrict its misuse by unauthorized entity.

- **Refresh Token:** This token is issued along with the Access Token but unlike the latter, it is not to be sent in each request from the client to the third party resource server.

When an Access Token expires, the Office client will present the Refresh Token to Azure Active Directory (Azure AD) and request for a new Access Token.



We recommend you to use Modern Authorization to avoid any security breach.

Configure the following parameters for Modern Authentication:

- **Provider:** It displays the name of the provider which is Microsoft Office 365.
- **Grant Type:** It refers to the way an application gets an Access Token.

This field is non-configurable and displays Authorization Code as the Grant Type.

Authorization Code is used only to be returned to exchange for an Access Token. It keeps this token hidden from the user client as it could be potentially exposed to the malicious agents trying to steal the token for nefarious means.

When you select Modern Authentication as a method of Authentication, you need to configure Get Token parameters.

Get Token

- **Authorization URL:** This command sends the URL to the endpoint of the Authorization Server that authenticates user credentials.

Enter the URL of the authorization endpoint.

Format: *https://login.microsoftonline.com/common/oauth2/v2.0/authorize*

- **Access Token URL:** This command sends the URL to the endpoint of the Authentication Server that is used to exchange the Authorization Code for Access Token.

Enter the Access Token URL.

Format: *https://login.microsoftonline.com/common/oauth2/v2.0/token*

- **Client ID:** Enter the application's Client ID, issued during the client application registration provided by the Azure AD.
- **Client Secret:** Client Secret is a secret string that the application uses to prove its identity while requesting a token. It is also known as Application Password.

It ensures that the request to get the Access Token is made only from the application and not from a potential attacker that may have intercepted the authorization code.

Enter the application's Client Secret. The Client Secret is issued to the client during the Application registrations process.

It will be in an encrypted format like a Password field.

- **Redirect URL:** It tells the authorization server where to send the user back to after they approve the request.

It extracts the Authorization Code/ Access Token.

The Redirect URL will be displayed in this field. The authentication response will be returned to the configured URL after successfully authenticating the user.

Redirect URL: *https://<Domain URL for COSEC Login>/Login/ ReceiveAuthorizationToken*

- **Scope:** It is one or more space-separated strings indicating the permissions, the application is requesting. The specific OAuth API you are using will define the scopes that it supports.

Scopes are set of permissions granted for each Client to access a specific data. It may have space-delimited values.

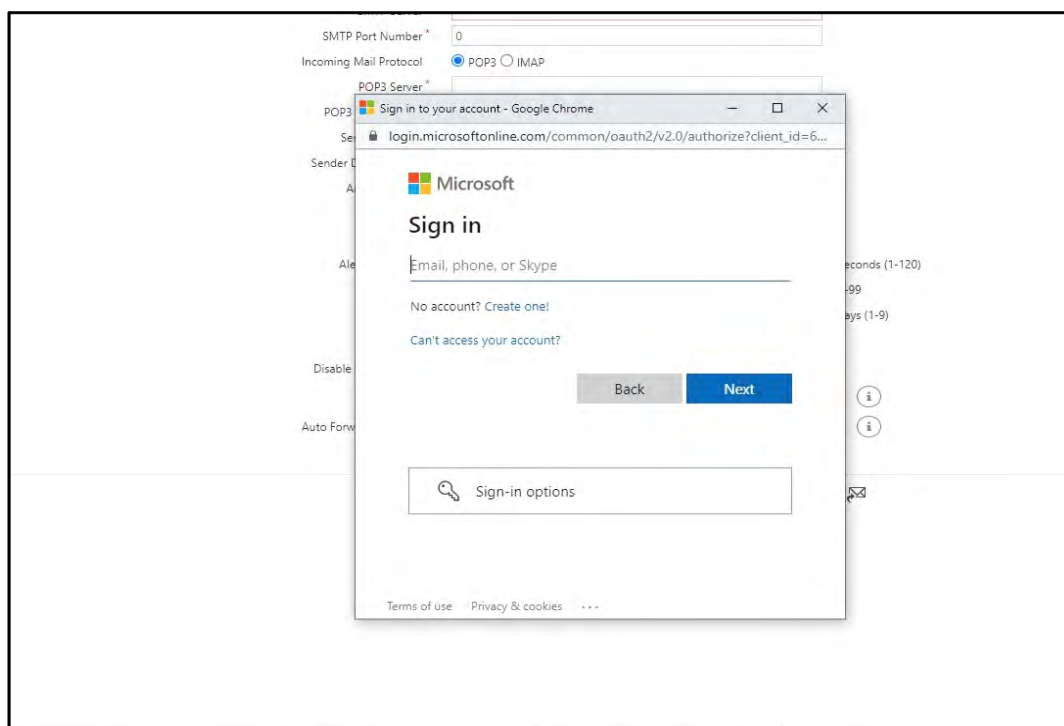
Enter Scope of the access request.

Format: *offline_access https://outlook.office.com/POP.AccessAsUser.All https://outlook.office.com/IMAP.AccessAsUser.All https://outlook.office.com/SMTP.Send https://outlook.office.com/Mail.Read*

- **Client Credential:** It defines whether to send client credentials as basic authorized header or as a plain text in the request body.

Select a desired option from the drop down list — In Basic Auth Header or Request Text.

Click **Get Token**. Once you click this button, you need to sign in to your Microsoft account and then all the parameters in the request will be verified ensuring the Authentication Code has not expired and that the Client ID and Client Secret is a match.



After the verification process is completed, the Authorization Server will generate and return the Access Token and Refresh Token in the response.

- **Access Token:** It displays the Access Token received in the response received from the Authorization Server or Access Token Server. To know more about Access Token, refer Access Token under Modern Authentication on [page 223](#).


- **Refresh Token:** It is obtained in the response received from the Authorization Server or Access Token Server. To know more about Refresh Token, refer Refresh Token under Modern Authentication on [page 223](#).
- **Alert Cycle:** Specify the time in seconds between successive send attempts when the system tries to send the pending messages.
- **Retry Count:** Specify the number of times the system needs to retry to send the same Email message in the event of an unsuccessful attempt.
- **Active Days:** Specify the number of days the system needs to keep the unsent messages active in the event of the service being stopped.
- **Enable SSL:** If you are using an external SMTP server like Gmail, then select the check box to enable.
- **Disable Sending Mail:** Select the check box to temporarily disable the email sending functionality.
- **Email Reading Interval:** Specify the desired duration (in minutes). This is the duration after which the Alert Service to fetch the data from the database.
- **Delete Mail:** Select the desired option from the drop-down list. Options are **All**, **Server**, **None**.
 - Select **All** to delete all the mails related to the Server and personal. This is applicable if the set **Email Reading Interval** is less than or equal to 30 minutes.
 - Select **None** to delete none of the mails. This is applicable if the set **Email Reading Interval** is equal to 30 minutes.
 - Select **Server** to delete all the emails from the server as soon as they are downloaded by the client. This is applicable if the set **Email Reading Interval** is equal to 30 minutes.
- **Auto Forward Email Id:** If a user selects either delete mail as **All** or **Server**, before deleting the mails, it will be auto forwarded to the configured email ID.

If mail is successfully forwarded, then the mail will be deleted from the inbox of the Server & log will be added in Alert view in **Admin> Views/Logs> Alert view**.

If mail is not forwarded due to incorrect E-mail Id (with valid characters), then the mail will be deleted from the inbox of the Server & log will be added in Alert view in **Admin> Views/Logs> Alert view**.

Once the above settings are done click **Save** button.

Test Mail

- **E-mail ID:** Specify the email id on which the test mail can be sent. Click  **Send Test Mail** button to send the test mail.



For each tenant, you can send upto 10 test emails in one minute. Thereafter the message "Maximum count reached. Please try after sometime" will be displayed.

Renaming Groups

The COSEC application defines 7 enterprise groups with default group labels and 3 custom groups. These are:

- Organization
- Branch
- Department
- Section
- Category
- Grade
- Designation
- Custom Group1
- Custom Group2
- Custom Group3

However, COSEC administrators can rename these group labels as per the site requirements. For e.g. some sites would need to refer to the **Organization** group as 'Company' or 'Condominium'.

Administrators can also rename the following entities in COSEC :

All modules

- User (e.g. "User" can be re-labelled as "Employee")

Contract Worker Management module

- Worker
- Work Order
- Contractor

Job Processing and Costing module

- Cost Centre
- Project
- Phase
- Job

Also **Quick Links** group can be renamed as required which will be reflected on the dashboard of modules.

To rename a group, Go to **Admin module > System Configuration > Rename Group** and the following screen appears.

Rename Group

Search

Rename Group: Organization

Rename As: Organization

Default Group Name	Renamed As
Organization	Organization
Branch	Branch
Department	Department
Section	Section
Category	Category
Grade	Grade
Designation	Designation
User	User
Worker	Worker
Work Order	Work Order
Contractor	Contractor
Cost Centre	Cost
Project	Project
Phase	Phase
Job	Job

1 - 15 of 16 records

1 2

Rename Group: Select a **Group** from the list view that is to be renamed. The selected Default Group Name appears in the field.

Rename As: Enter the new Group Name/label in the field.

Click the **Save** button.

The new Group name/label will appear in the list view under the **Renamed As** column as shown below.

Rename Group Saved Successfully

Search

Rename Group: User

Rename As: Employee

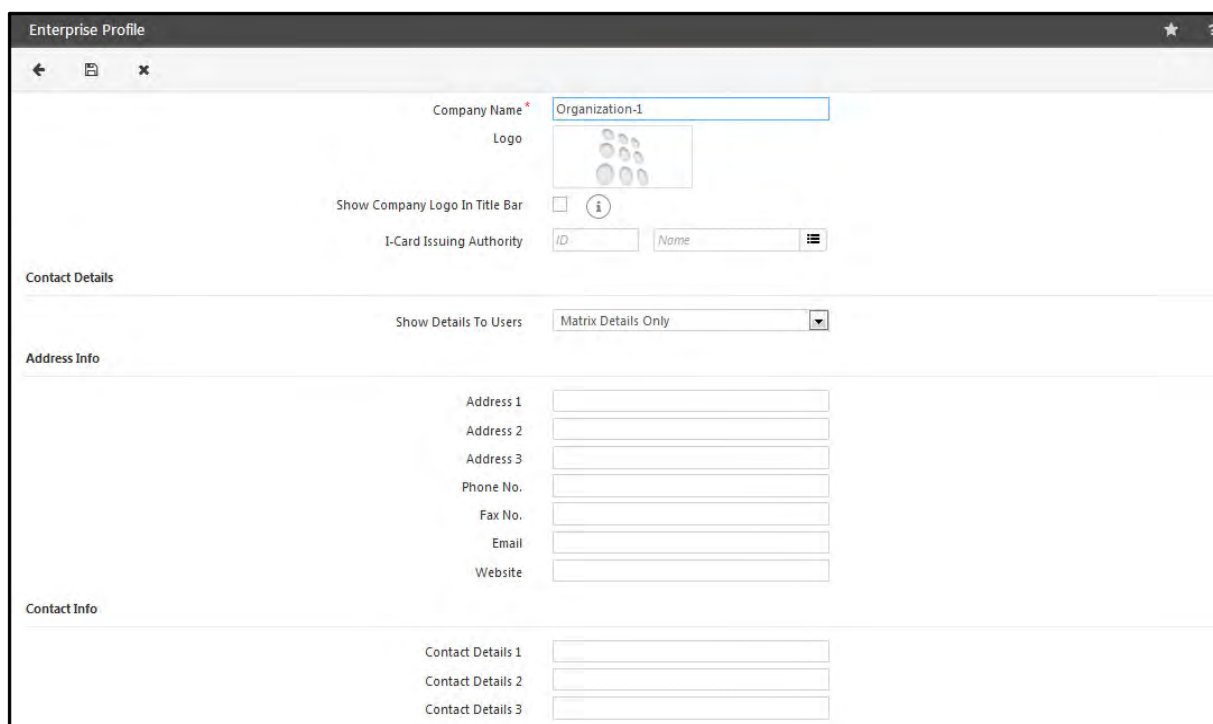
Default Group Name	Renamed As
Organization	Organization
Branch	Branch
Department	Department
Section	Section
Category	Category
Grade	Grade
Designation	Designation
User	Employee
Worker	Worker
Work Order	Work Order
Contractor	Contractor
Cost Centre	Cost
Project	Project
Phase	Phase
Job	Job

The updated label gets reflected all across the COSEC system.

Setting Up the Enterprise Profile

The system administrator can define how the profile of an enterprise appears on the COSEC home page. This representative profile can be set up to display the company logo, the contact information as well as other descriptive details about the company.

To set up the enterprise profile, select **Admin module > System Configuration > Enterprise Profile** and the following screen appears.



Company Name: Enter the name of the company in the field.

Uploading Logo

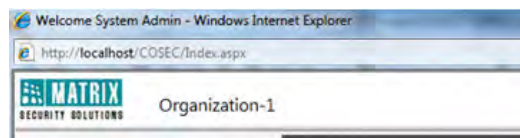
Logo: Click to add an image for the company logo.

Show Company Logo in Title Bar: Select the box to show company logo in title bar.



Company Logo with size 96 pixels in width and 48 pixels in height will display properly otherwise it is possible that logo will not fit properly. If image with transparency has been uploaded as company logo then it will not be displayed properly in reports.

The uploaded company logo will be shown in title bar when you login again.



I-card Issuing Authority: Select the User as the I-card Issuing Authority using the picklist.

Contact Details


Show Details To Users: Select an option from the dropdown list to make the company profile information visible to the employees.

- **Matrix Details Only:** If this value is selected, the user will be able to view only the Matrix Details on the "Contact Us" page.
- **Enterprise Details Only:** "Only the details configured in the "Address Info" and "Contact Info" will be displayed.
- **Both:** If this option is selected, both the "Matrix Contact Details" and "Enterprise Contact Details" will be displayed.

In the **Address Info** section, enter the company's correspondence **address, phone no., fax no., email address** and **website** as per the fields requested.

In the **Contact Info** section, you can define additional contact information to be provided.

In the **About Company** Section, add a brief description about the company.

Click **Save** button. The saved information will be now be updated on the COSEC Web application home page as well as the **Contact**  page.

Configuring Alert Messages

In order to send an alert message from the COSEC system, the **Alert Messages** option needs to be enabled while configuring a door controller. To do this, refer to [“Device List”](#).



When client is situated in a time zone other than Alert Service's time zone; Alert Service will take tenant's time zone into consideration while processing scheduled tasks or generating scheduled reports.



Multi-language is not supported in Alert Messages sent via Email/SMS/App Notification.

To configure an alert message, Go to **Admin module > System Configuration > Alert Message Configuration** and the following screen appears.

The screenshot shows the 'Alert Message Configuration' window. On the left, there are configuration fields: 'Alert Filter' (set to 'All'), 'Event' (set to 'Select Event'), 'Header Message', and 'Footer Message'. Below these are expandable sections for 'Additional Message Parameters', 'Message Preview', and 'Assign Alert'. On the right, there is a table of events with columns 'ID' and 'Event'. The table lists 17 events, including 'Monthly Attendance', 'Leave Approval', 'Leave Rejection', 'User Events', 'Leave Application', 'Missing In Punch - Users', 'Missing In Punch - Group Incharge', 'Missing Out Punch - Users', 'Missing Out Punch - Group Incharge', 'User Allowed', 'User Denied', 'Door Force Open', 'New Joining - Confirmation', 'Visitor Arrival', and 'Visitor Pre-Registration'. At the bottom right, it shows '1 - 15 of 51 records' and a pagination control.

ID	Event
1	Monthly Attendance
2	Leave Approval
3	Leave Rejection
4	User Events
5	Leave Application
6	Missing In Punch - Users
7	Missing In Punch - Group Incharge
8	Missing Out Punch - Users
9	Missing Out Punch - Group Incharge
10	User Allowed
11	User Denied
12	Door Force Open
15	New Joining - Confirmation
16	Visitor Arrival
17	Visitor Pre-Registration

The grid on the right side displays events for which the alert message can be configured. Click on the event from the grid for which the alert message is to be configured.

Alert Filter: You can also select the specific module from Alert filter options based on which event can be selected. (list depends on the available license).

Event: Firstly select an event from the dropdown list for which the alert message is to be configured. The events in the dropdown list depends on the available license. For eg: for Devices filter, Door Offline event can be selected. Each event allows a particular alert message to be sent to the users.



Please refer the Examples for few Alert Filters and its events described in upcoming pages.

Header Message: Enter the required text to be displayed in the header of the message (For e.g. "Dear User,").

Footer Message: Enter the required text to be displayed in the footer of the message (For e.g. "From COSEC Software").

The 'Alert Message Configuration' window displays the following fields:

- Alert Filter:** A dropdown menu currently set to 'All'.
- Event:** A dropdown menu with 'Select Event' highlighted.
- Header Message:** An empty text input field.
- Footer Message:** An empty text input field.
- Additional Message Parameters:** A collapsible section, currently collapsed.
- Message Preview:** A collapsible section, currently collapsed.
- Assign Alert:** A collapsible section, currently collapsed.

If the selected event has additional parameters to be defined, click on the **Additional Message Parameters** section.

Additional Message Parameters

The Additional Message Parameters collapsible panel provides the following options: The parameters under Additional Message Parameters are dependent on the configured Event.

The 'Alert Message Configuration' window shows the 'Additional Message Parameters' section expanded. The configuration is as follows:

- Alert Filter:** Visitor Management
- Event:** Visitor Pre-Registration
- Header Message:** Dear User/Visitor,
- Footer Message:** From COSEC Software
- Additional Message Parameters:**
 - Message Selection:** ☒ SMS, ☐ Email, ☒ App Notification
 - Template ID:** [Empty text field]
 - Calendar Invite:** ☐
 - Approval Links:** ☐
 - Approval Acknowledgment:** ☐
 - Send Alert To:** ☒ Host, ☒ Visitor
- Message Preview:** [Collapsible section]

- **Message Selection:** Select the **SMS** or **Email** checkbox to determine the type of message to be sent. You can also enable **App Notification** check-box to receive the 'Push Notifications' for the APTA mobile application for its related events.
- **Template ID:** As per TRAI Regulation, an enterprise which sends messages to customers like OTP, communication message, promotional messages via SMS, have to register their entity and the content template to avoid Spam, fake and fraudulent communication through SMS.

It is mandatory for an Admin to register the SMS content template beforehand with your Service Provider which will be verified before it is delivered to the users.

Once registered, the Service Provider will provide a Template ID against the registered SMS content.

For every different Alert messages, a unique Template ID will be provided by the Service Provider.

Enter the respective Template ID for the configured alert message which is to be send to users via SMS. Make sure **SMS** is enabled in **Message Selection** to configure Template ID.



If you have multiple Service Providers, then make sure the required templates are registered with all the desired Service Providers. Hence for each template you will have multiple Templates IDs. Also make sure you maintain a record of all the registered Message Templates with their respective Template IDs for reference.

- **Calendar Invite:** When **Message Selection** is Email, select this checkbox to attach icalender (.ics) file in the Email invitation along with the details of the scheduled visit to a visitor.

ICS file is an universal calender format which enables the users to publish and share calendar information over Email.

By attaching the .ics file in the Email invitation, all scheduled visit details will get imported directly in to the calendar of the invited visitors, provided it has an email reader with calendar application.

Recipients of the .ics file will get a notification from the calendar event for the scheduled visit before the start time of the visit.

An .ics file includes — Summary of the Visit, Visitor and Host Information, Date and Time of the Visit, Unique ID (UID), Location, Description of the Visit etc.

Calendar Invite is not applicable if **Message Selection** is SMS or App Notification.

- **Approval Links:** Make sure you have enabled **Email** checkbox to configure Approval Links checkbox.

Select this checkbox to send the application alert to the RIC of the user for his/her approval. The RIC can Approve/Reject the application via the link in the Email. The verdict will be based on the authorization mode — Any One, All or All Sequential. For details refer to [“Approval Policy”](#) and [“Reporting Group”](#).

- **Approval Acknowledgment:** Select this checkbox to send Acknowledgment email.

Make sure you have enabled **Email** and **Approval Links** checkboxes to configure **Approval Acknowledgment**.

ID	Event
1	Monthly Attendance
2	Leave Approval
3	Leave Rejection
4	User Events
5	Leave Application
6	Missing In Punch - Users
7	Missing In Punch - Group Incharge
8	Missing Out Punch - Users
9	Missing Out Punch - Group Incharge
10	User Allowed
11	User Denied
12	Door Force Open
15	New Joining - Confirmation
16	Visitor Arrival
17	Visitor Pre-Registration



The System Alert “Pending Applications For Approval” will be available with **T&A license OR VMS license**.

The counts of Time sheet Correction Authorization, Award/Penalty Application, FVM Correction Application and VMS Pre-Registration Application will depend upon their corresponding license availability.

- **Include Attachment:** Select this checkbox to send an attachment including Medical Certificate/Tour document along with the alert message to the RIC.

Include attachment is applicable only when you select **Email** as the **Message Selection** option.

- **Alert for Normal Shift Update:** Enable to send alert for normal shift update.
- **Alert for Field Break Shift Update:** Enable to send an alert for updating everyone about the field break shift.
- **Alert for Rest Day Shift Update:** Enable to send an alert for updating everyone about the rest day shift.
- **Send Alert To:** Select the desired checkboxes — **User, Reporting In-charge, Group, System Account, Host, Visitor, Security** and/or **Additional Host** — to define the recipient type for the message.
- **Send Alert As Per:** Select **Send Alert As Per — Schedule Time of the Day** and **Shift End Time** from the given dropdown.
 - **Schedule Time of the Day:** Select this option from the dropdown to schedule an exception alert generation at a fix time of a day, for which you will have to specify the **Schedule Time** and **Schedule Day**.
 - **Post Shift Time:** Select this option to generate an exception alert after the shift ends. Specify the time after which the alert of exception should be generated.

For example: Value of this parameter is set to 120. Shift of Ram ends at 18:00. If any exception occurs for Joy, its alert should be sent at 20:00.

- **Exceptions:** Select one/many exceptions from the list provided for Alert which are to be sent to the RIC/ User.

If you select **Send Alert To RIC**, then only single message will be sent containing details about all user for whom the same exception has occurred.

For each exception, a different alert will be sent.

Exceptions will be calculated separately for each user.

- **Event Check Period (In Minutes)**

- **Event Check Period:** Specify the Event Check Period. Enter the Start Time (HH:MM format) and the End Time (HH:MM format).

You can configure multiple alerts at different times on weekdays and holidays. The Event alerts can be configured for events like User Allowed, User Denied, Door Force Open, Door Offline, Door Abnormal, Identification Server Inactive.

Maximum configuration limit for a single alert is **99**.

Start Time	End Time	Active Days
09:00	18:30	Mon Tue Wed Thu Fri
11:00	16:00	Sat Sun

- **Active Days:** Select the days of the week or holidays to be considered as active days.
- **Tolerance Period:** Enter the tolerance time in seconds after which the alert message is to be sent. Eg. If 60 seconds is set, and if the door goes offline for 60 seconds then alert message is sent.

Confirmation Period (In Days)

- **Confirmation:** Specify the days after joining for which alert is to be sent.

Reminder Period (In Days/Hours)

- **Days before Expiry:** Specify the number of days before which the alert is to be sent.
- **Set Reminder:** Days before confirmation.
- **Reminder Time:** Time at which Alert is to be sent.
- **Schedule Time:** Specify the time to be scheduled for sending an alert message.
- **Processing Period:** Select the period for processing alert message from the dropdown list.
- **Alert Reporting In-Charge:** Enable to send alert messages to the reporting in-charge.

- **Pre -Shift End (Minutes):** Set the time period in minutes prior to the shift end time that the system should consider to trigger a **Missing Out Punch** alert.
- **Post Shift End (Minutes):** Set the time period in minutes after the shift ends that the system should consider to trigger a **Missing Out Punch** alert.

Example:

Supposing your shift ends at 18:00 P.M. And you have not marked punch.

Considering, the following are configured:

Pre -Shift End: 60 min

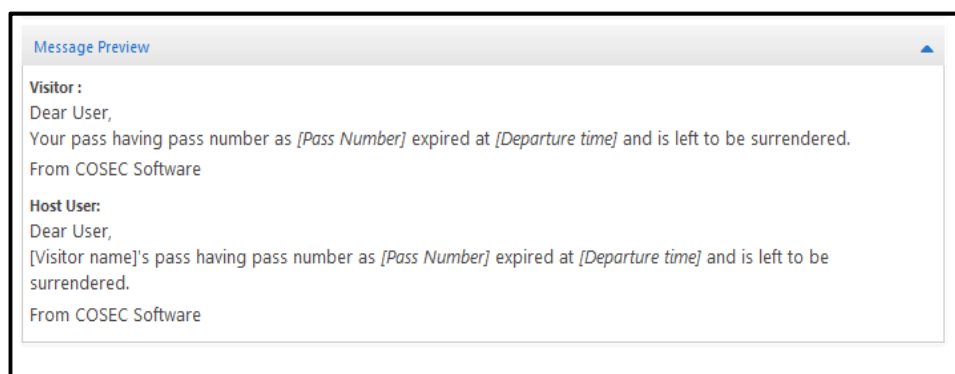
Post Shift End: 60 min

In this case an alert of **Missing Out Punch** will be triggered between time interval 17:00 - 19:00.

- **Post Shift Start (Minutes):** Set the desired time in minutes to send an alert after the shift begins.
- **Reminder Prior Hours:** Set the desired hours to send an alert before the configured time ends.
- **Reminder Prior Days:** Set the desired days to send an alert before the configured time ends.

Message Preview

You can preview the configured message in this field. It allows the user to customize the message. It also allows to reset the message to default value. The figure below shows a preview of Visitor Pass Expired Alert message:

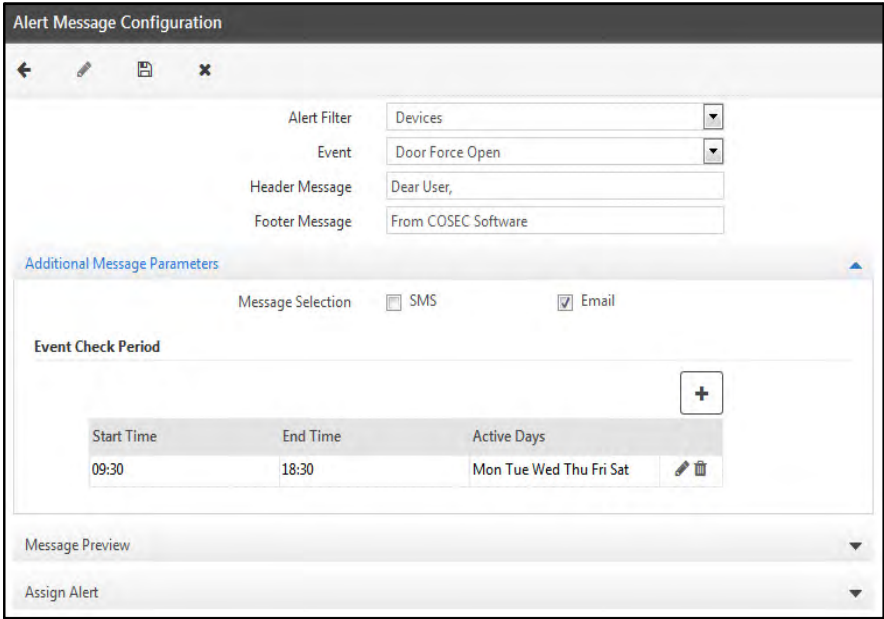


Similarly, you can preview the message for other events also.

Assign Alert

This feature is available to users if the event selected for alert can be assigned to users. For e.g. Events such as "Door Force Open" can be assigned to a users.

Enable the **SMS** and/or **Email** check boxes to send the SMS or Email to the selected users. Enter the timing and select the days on which the alert message is to be sent to the users under **Event Check Period**.



Alert Message Configuration

Alert Filter: Devices
 Event: Door Force Open
 Header Message: Dear User,
 Footer Message: From COSEC Software

Additional Message Parameters

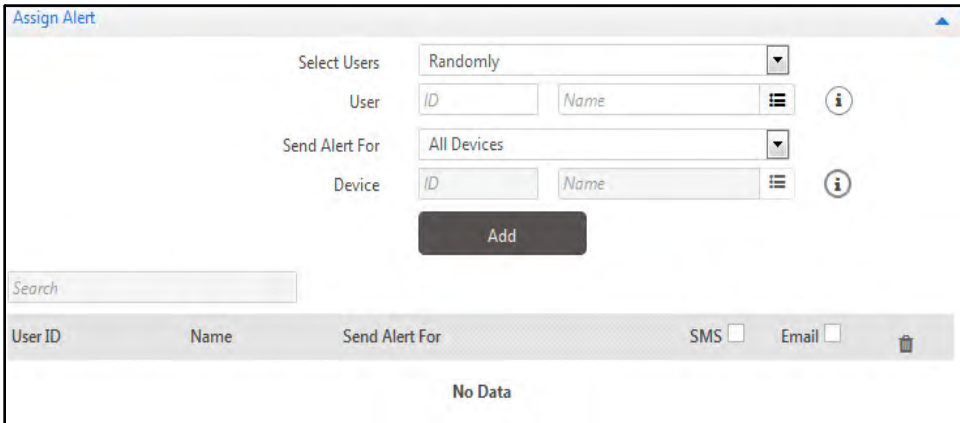
Message Selection: ☐ SMS ☒ Email

Event Check Period

Start Time: 09:30 End Time: 18:30 Active Days: Mon Tue Wed Thu Fri Sat

Message Preview
 Assign Alert

Users can be selected from **Select Users**, either **All** or **Randomly**, as shown below:




Assign Alert

Select Users: Randomly
 User: ID Name
 Send Alert For: All Devices
 Device: ID Name

Add

Search

User ID	Name	Send Alert For	SMS	Email	
No Data					

User: Click on  and choose the users from the pick-list.



*If **All** is selected in Selected User dropdown, then User pick-list will be disabled.*

Send Alert For: Choose any one options from **All Devices**, **Selected Devices** and **Selected Device Groups** for which alert is to be send to users. On selecting All Device from the drop-down, Device pick-list will be disabled.

Devices: Select the Device or Device Group for which alert is to be send.

Click on **Add** to view the configured users as shown below:

Assign Alert

Select Users: Randomly

User: ID Name

Send Alert For: All Devices

Device: ID Name

Add

Search

User ID	Name	Send Alert For	SMS <input checked="" type="checkbox"/>	Email <input checked="" type="checkbox"/>	
1	Exl	Selected Devices (2)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
2	Anmol	Selected Devices (2)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
2192chiraglkdhf	2192chirag2192chirag2192chirag2192chirag2192c	Selected Devices (2)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
25	fyfy	Selected Devices (2)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
3	nisha	Selected Devices (2)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

1 - 5 of 10 records

« < 1 2 > »



Before configuring SMS and Email alert for the user, the mobile number and Email address of the user must be provided in **User Configuration > Profile > Contact**. Also “Receive Alert On” must be enabled for the user.

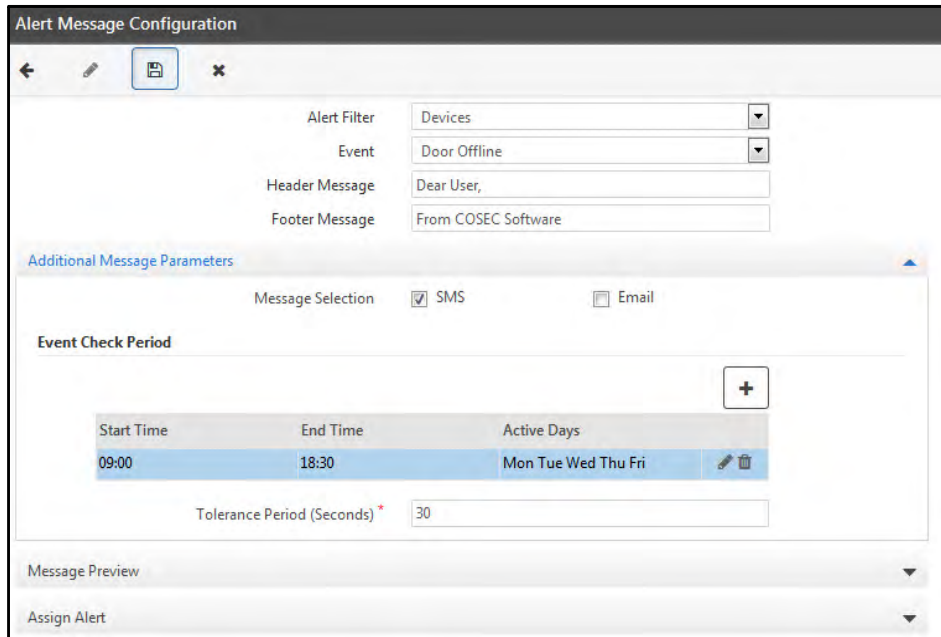
The SMS configuration must be done from **Admin module > System Configuration > SMS Configuration**.
The Email configuration must be done from **Admin module > System Configuration > Email Configuration**.

The “Alert Messages” checkbox in **Device Configuration > Profile > Basic** must be enabled to send the device based events alert.

Ensure that Alert Service is running so that alert message can be sent to the assigned user.

Example1: Door Offline Alert

The Door Offline Alert is used to send alert through SMS or Email when door is found offline with Panel within some defined timings say from 9:00 to 18:30 hours for tolerance duration (say 30 seconds) and on selected days (Monday to Friday).



Alert Message Configuration

Alert Filter: Devices
 Event: Door Offline
 Header Message: Dear User,
 Footer Message: From COSEC Software

Additional Message Parameters

Message Selection: ☒ SMS ☐ Email

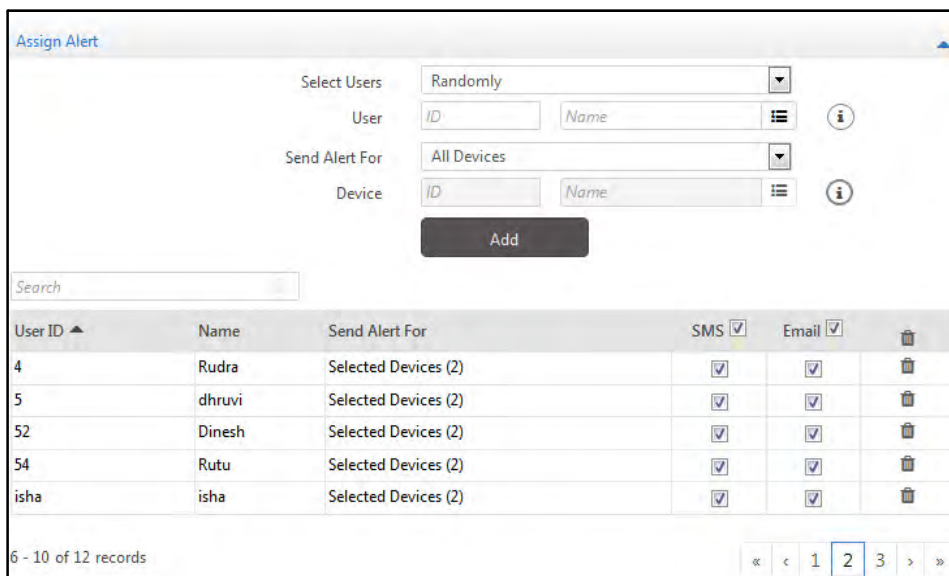
Event Check Period

Start Time	End Time	Active Days
09:00	18:30	Mon Tue Wed Thu Fri

Tolerance Period (Seconds): 30

Message Preview
 Assign Alert

The alert is sent to the users who are assigned the alert by selecting the users from the picklist. And you can select the devices from drop down options for whom the alert is to be sent.



Assign Alert

Select Users: Randomly
 User: ID Name
 Send Alert For: All Devices
 Device: ID Name

Add

Search

User ID	Name	Send Alert For	SMS	Email	
4	Rudra	Selected Devices (2)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
5	dhruvi	Selected Devices (2)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
52	Dinesh	Selected Devices (2)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
54	Rutu	Selected Devices (2)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
isha	isha	Selected Devices (2)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

6 - 10 of 12 records

If Tolerance period is 0 seconds, alert will be sent immediately when the door offline event is generated. Once the alert is sent, its logs will be visible in Admin > View/Logs > Alert View page.

Direct Door as Panel Door

For generating the sequential In/Out events direct door can connect with server and panel simultaneously. When **Connect to Panel** checkbox is enabled; device display reflects the connectivity status as per connectivity with panel.

When the Direct Door is connected to Server and Panel;

MATRIX PVR Door - PVR Door-Device-7 (7)

Settings ▾

- Basic Profile
- LAN Settings
- Wi-Fi Settings
- Mobile Broadband Settings
- Server Settings**
- CCC Settings
- Identification Server Settings
- Date-Time Settings
- Multi Language Support
- Manage ▶
- View ▶

Server Settings - COSEC CENTRA

This will be used to communicate with Monitor Service

Connectivity Status ● via Ethernet

Encryption (SSL) ☐

Configuration ☒ Basic ☐ Custom

URL * 192.168.104.12 11000

Panel

Connectivity Status ● Connected

Connect to Panel ☒

Interface Selection ☒ Auto ☐ Manual

Network Interface Ethernet

IP Address * 192.168.104.111 11000

Submit Cancel Default

And when **Connect to Panel** is disabled it reflects the connectivity status as per connectivity with server.

MATRIX PVR Door - PVR Door-Device-7 (7)

Settings ▾

- Basic Profile
- LAN Settings
- Wi-Fi Settings
- Mobile Broadband Settings
- Server Settings**
- CCC Settings
- Identification Server Settings
- Date-Time Settings
- Multi Language Support
- Manage ▶
- View ▶

Server Settings - COSEC CENTRA

This will be used to communicate with Monitor Service

Connectivity Status ● via Ethernet

Encryption (SSL) ☐

Configuration ☒ Basic ☐ Custom

URL * 192.168.104.12 11000

Panel

Connectivity Status ● Disconnected

Connect to Panel ☐

Interface Selection ☒ Auto ☐ Manual

Network Interface Ethernet

IP Address * 192.168.104.111 11000

Saved Successfully

Submit Cancel Default

This door offline alert will be sent to as SMS or Email to the selected users.
This event will be generated for Wireless door, NGT, FMX, Vega and PVR door.

Alert Log

Date * 06/04/2018 06/04/2018
View

Filter

Alert E-mail
E-mail ID

Search

E-mail ID	Message	Date Time	Error/Status
sheetal.raval@matrixrd.org	Dummy Door found Offline on 06/04/2018 03:04:13 PM sinc...	06/04/2018 15:04:23	
sheetal.raval@matrixrd.org	Dummy Door found Offline on 06/04/2018 03:04:13 PM sinc...	06/04/2018 15:04:23	
sheetal.raval@matrixrd.org	PVR Door-Device-7 found Offline on 06/04/2018 02:42:14 ...	06/04/2018 14:42:25	
sheetal.raval@matrixrd.org	PVR Door-Device-7 found Offline on 06/04/2018 02:42:14 ...	06/04/2018 14:42:25	

Example2: Alert for Validity/Expiry date of Documents

Whenever the ID proof documents such as Visa, Driving License, Passport etc. are going to be expired, the users must get notified in advance in order to renew them. By creating the **Validity/Expiry Date alert**, user will able to configure Reminder Period for important documents as explained below.

Select Alert Filter as a 'User', event as a 'Validity/Expiry Date' and update the Header-Footer if required.

Alert Message Configuration

Alert Filter Test FP15s
Event Validity/Expiry Date
Header Message Dear User,
Footer Message From COSEC Software

Additional Message Parameters

Message Selection ☒ SMS ☒ Email
Send Alert To ☒ Test FP15 ☒ Reporting Incharge

Reminder Period (In Days)

Send Alert For	Document	Days Before Expiry	Reminder Time	Repeat Reminder	Repeat Interval(In Days)	
Yes	Visa	5	15:30	No	1	
No	Driving License	0	00:00	No	1	
<input checked="" type="checkbox"/>	Passport	5	15:30	<input checked="" type="checkbox"/>	10	
No	Aadhar Card	0	00:00	No	1	

Message Preview
Assign Alert

Enable the 'Message Selection' and 'Send Alert to' check-boxes and configure **Reminder Period (In Days)** columns as described below.

- **Send Alert For:** Enable the check-box for which the Alert is to be send as a notification. For example: Visa and Passport.

- **Document:** This field shows the type of documents for which Alert is to be configured. The configured custom fields will also be available for the selection.

Note: Only the custom fields which are configured with their **type; Date**, will be visible in the Document column. For the configuration of Custom Fields, See ["Custom Fields" on page 136](#).

- **Days Before Expiry:** Enter the number of days before which the user will get notified about the expiry of documents validity. You can enter the days from 1 to 99. For Example:5
- **Reminder Time:** Define the Time of the reminder in 24hrs format at when the notification will get generated. For Example: 15:30
- **Repeat Reminder:** Enable the check box if the configured reminder is to be repeated again.
- **Repeat Interval (In days):** Define the number of days in between 1 to 99. The reminder will repeat till the entered number of days. For example: 10

Click on the **Ok** button to Save and **Cancel** button to **Cancel** the Reminder Period configuration. Click on the **Edit** button to **Edit** the reminder.

Now, after previewing the Message and configure the assign Alert, click on the **Save** button to save the Alert message Configuration.

So, as per the above configuration, the reminder will get generated at 15:30 before 5 days of Visa and Passport expires and will repeat for next 10 days.

Example3: Login Account Locked Alert

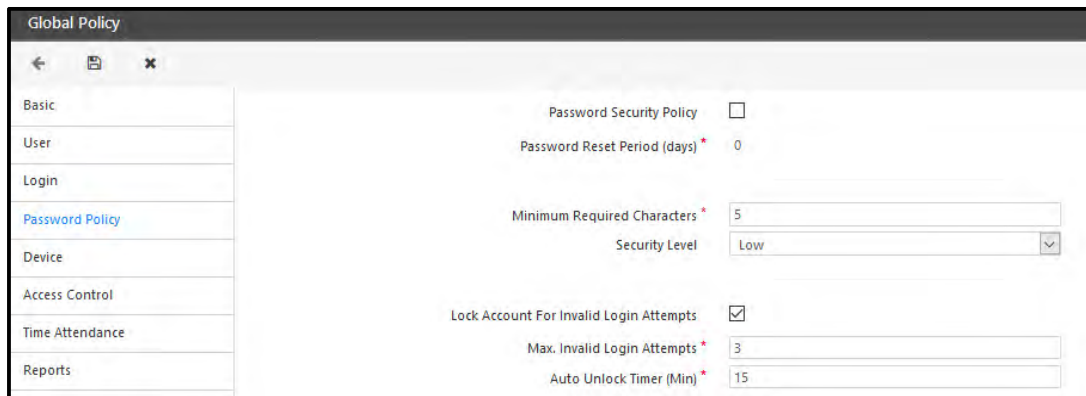
When the user logs into COSEC with wrong password for a specified number of times; then his account can be locked for defined duration of time. When the account gets locked; the locked account alert will be generated.

ID	Event
1	Monthly Attendance
2	Leave Approval
3	Leave Rejection
4	User Events
5	Leave Application
6	Missing In Punch - Users
7	Missing In Punch - Group Incharge
8	Missing Out Punch - Users
9	Missing Out Punch - Group Incharge
10	User Allowed
11	User Denied
12	Door Force Open
15	New Joining - Confirmation
16	Visitor Arrival
17	Visitor Pre-Registration

This alert will be generated if

- Global Policy > Password Policy > "Lock Account For Invalid Login Attempts" is enabled.

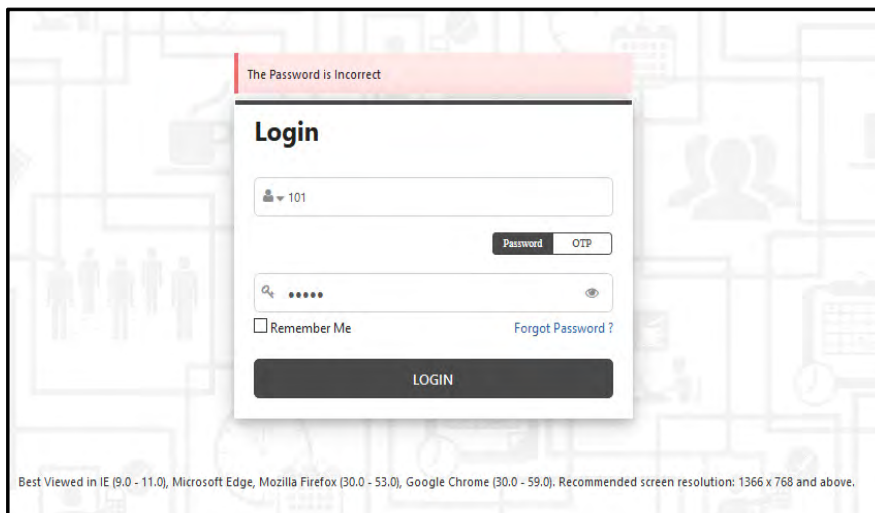
- No. of Failed Login Attempts against user is equal to "Max. Invalid Login Attempts" count as specified in Password Policy.



The alert can be sent to all the active users who are trying to login in COSEC. (Either as System Account User, ESS User or CSS User)

- **ESS User Login-** The "Receive Alerts On" for the user must be configured in User profile to send the SMS or Email to Personal/Official contact.
- **System Account User Login-** If a System Account has "Linked ESS User" configured, then alert will be sent to that ESS User's saved contact details considering all the conditions mentioned in ESS User Login section for ESS user satisfy.
- **CSS User Login-** The "Receive Alerts On" for the contractor must be configured in User profile to send the SMS or Email to Personal/Official contact.

Example: Here the ESS user 101 is trying to login into COSEC. When the number of attempts is equal to 3 as specified in Password Policy; then account will get blocked to 15 minutes as defined.



Unlock My Account

The alert email will be sent as shown below. In the Alert mail; “Unlock My Account” button will be available. On click of this button, a reply mail will be sent to COSEC server with Subject having 'Account-Locked-Date-Time' to unlock the account.



A single mail will be used only once to unlock that user's account. Same mail will not be used multiple times to unlock a user's account.

Subject	From
COSEC - Login Account Locked	Aditi-Matrix
Test Mail	Sheetal-Matrix
Door Offline	Sheetal-Matrix
Door Offline	Sheetal-Matrix
Door Offline	Sheetal-Matrix
Door Offline	Sheetal-Matrix

From: Aditi-Matrix <aditi.gupta@matrixrd.org>
 Subject: COSEC - Login Account Locked
 To: Me

Dear User,

Your ESS Account has been locked due to maximum failed login attempts.
 To unlock your account, please click the button below.

[Unlock my Account](#)

Instructions:
 1) Do NOT Change the subject in the reply mail.

From COSEC Software

Example4: OTP Generated Alert

OTP Generated Alert generates the alert for set/reset password, login authentication, pass creation and visitor registration verification.

To view details on OTP alert for Set/Reset Password and Login Authentication see Chapter: Launching COSEC Application

The screenshot shows the 'Alert Message Configuration' window. It has a title bar with standard window controls. Below the title bar, there are four fields: 'Alert Filter' set to 'System', 'Event' set to 'OTP Generated', 'Header Message' set to 'Dear User,', and 'Footer Message' set to 'From COSEC Software'. Below these fields is a section titled 'Additional Message Parameters' which contains two checkboxes: 'SMS' and 'Email', both of which are checked. At the bottom of the window is a 'Message Preview' section.

Example 5: 'Auto Sign-in' Alert for COSEC APTA Mobile Application

User can configure the Alert for download and sign in to the COSEC APTA application. For this, an ESS rights must be allocated to the user.

Select the Alert filter as 'All' or 'System', an event as 'APTAAuto Sign-in Configuration' as shown below. Update the Header and Footer message if required.

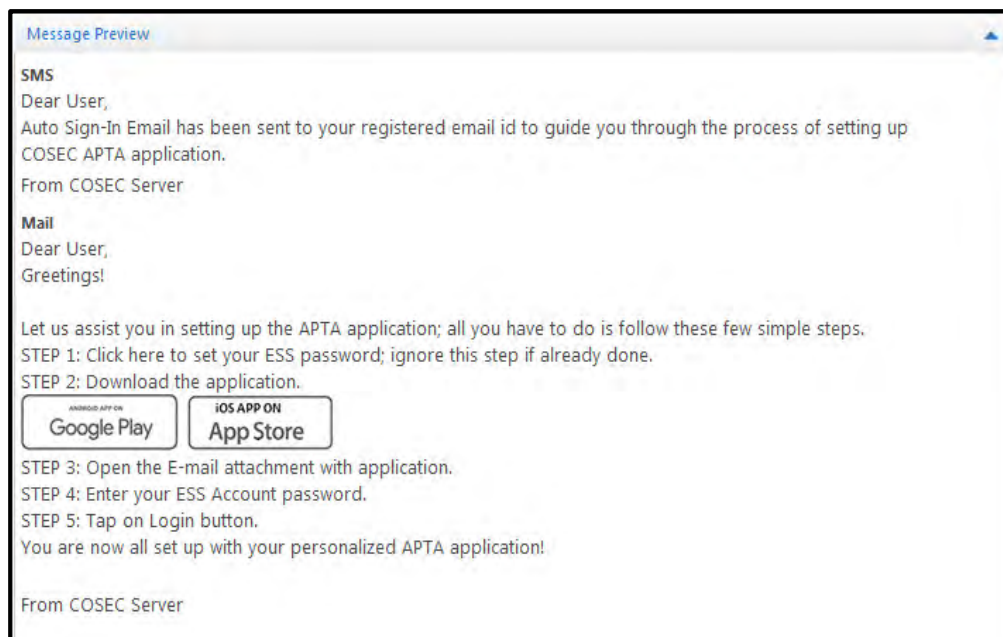
This screenshot shows the 'Alert Message Configuration' window with different settings. The 'Alert Filter' is 'System' and the 'Event' is 'APTAAuto Sign-In Configuration'. The 'Header Message' is 'Dear User,' and the 'Footer Message' is 'From COSEC Server'. The 'Additional Message Parameters' section shows both 'SMS' and 'Email' checkboxes checked. Below this section are 'Message Preview' and 'Send Alert' buttons.

Enable the respective checkbox for **SMS** and **Email** through which the alert message is to be sent.

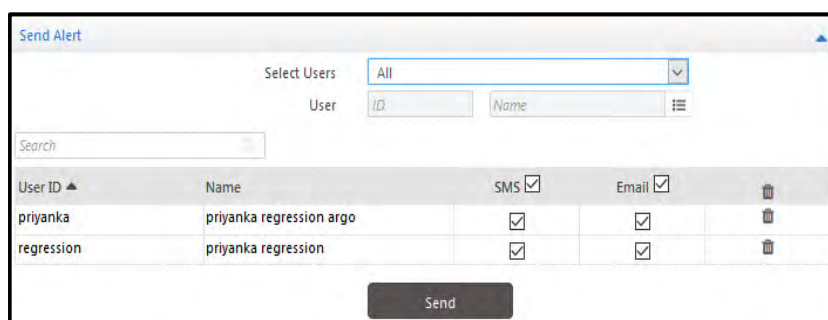


The respective links to download the application and, auto sign in configuration file will be sent through the email.

The Message preview with the necessary steps for downloading the APTA Application and Sign In are as shown below.



Expand the **Send Alert** tab and select the users to which the Auto Sign in email is to be sent.



Click on the **Send** button to send the configured Alert message to the selected users.

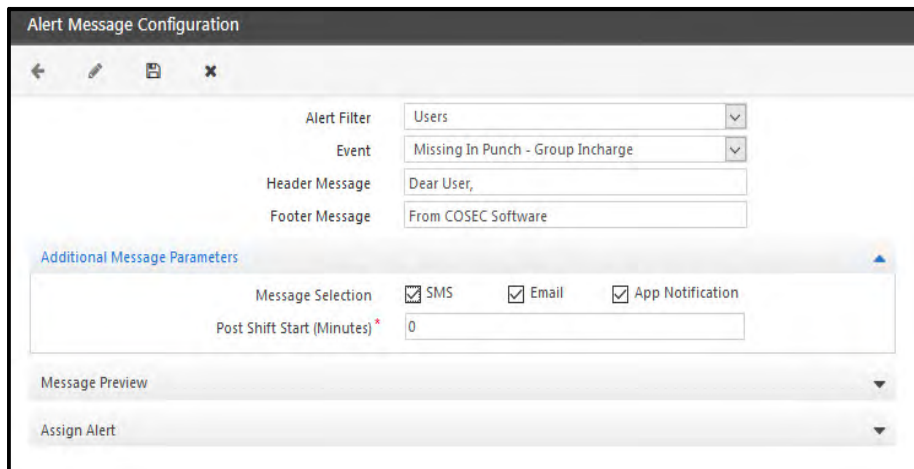
Note: An email will have a configuration file as an attachment. Open the file on COSEC APTA application to sign.

Example 6: Receive 'Push Notifications' to the COSEC APTA Mobile Application

User can configure an alert to receive the Push notifications on the APTA user's smartphone for the Alert Filter; User, Leave Management and Time & Attendance for below list of events.

- Missing In/Out Punch
- Attendance Correction Application / Approval / Rejection
- Short Leave/Official Hours Application
- Short Leave/Official Hours Approval / Rejection
- Shift Change
- OT / C-OFF Authorization
- Event Authorization
- Leave Application / Approval / Rejection
- Leave Cancellation/Approval / Rejection
- Leave Credit / Debit
- Leave Modification Application / Approval / Rejection

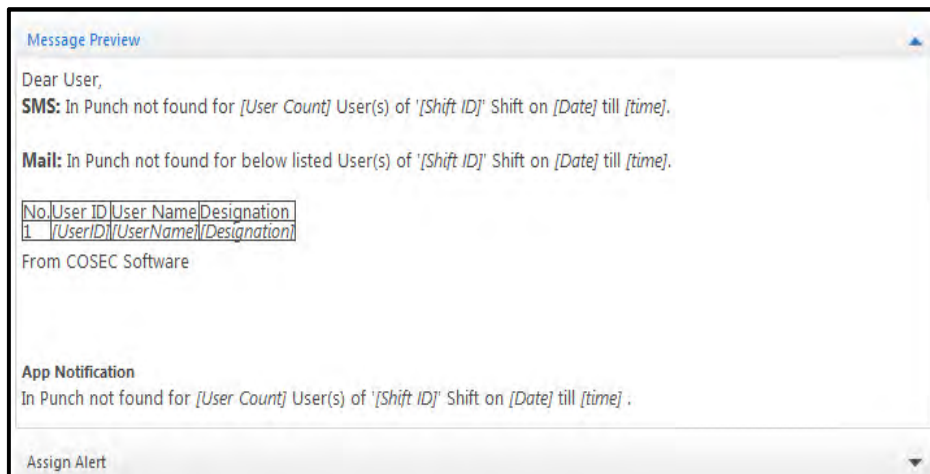
Overtime Limit Exceeded - Group-Incharge
Overtime Limit Exceeded - User



The 'Alert Message Configuration' window is shown. It has a title bar with standard window controls. Below the title bar, there are four fields: 'Alert Filter' (set to 'Users'), 'Event' (set to 'Missing In Punch - Group Incharge'), 'Header Message' (set to 'Dear User,'), and 'Footer Message' (set to 'From COSEC Software'). Below these is a section titled 'Additional Message Parameters' with a blue arrow icon. Inside this section, there are three checkboxes: 'SMS' (checked), 'Email' (checked), and 'App Notification' (checked). Below the checkboxes is a field for 'Post Shift Start (Minutes)' with the value '0'. At the bottom of the window, there are two tabs: 'Message Preview' and 'Assign Alert', both with dropdown arrows.

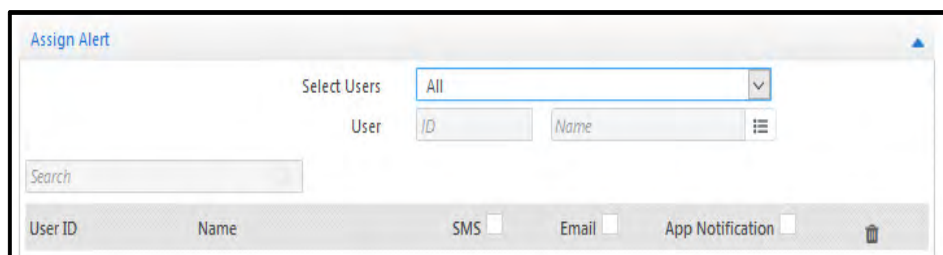
Enable the 'App Notification' checkbox from the **Additional Message Parameters** to receive the Alert as a Push Notification on user's smartphone.

The Preview message for SMS, Email and App Notification is as shown below.



The 'Message Preview' window is shown. It displays the message content for SMS, Mail, and App Notification. The message content is as follows:
Dear User,
SMS: In Punch not found for [User Count] User(s) of '[Shift ID]' Shift on [Date] till [time].
Mail: In Punch not found for below listed User(s) of '[Shift ID]' Shift on [Date] till [time].
[Table with 4 columns: No, User ID, User Name, Designation]
1 [UserID] [UserName] [Designation]
From COSEC Software
App Notification
In Punch not found for [User Count] User(s) of '[Shift ID]' Shift on [Date] till [time].
At the bottom, there is an 'Assign Alert' button.

Expand the **Assign Alert** tab and select the required users to which the Alert is to be configured and, enable the App Notification checkbox for the respective one.



The 'Assign Alert' window is shown. It has a title bar with standard window controls. Below the title bar, there is a 'Select Users' dropdown menu set to 'All'. Below this is a table with two columns: 'User ID' and 'Name'. Below the table is a 'Search' field. At the bottom, there are three checkboxes: 'SMS', 'Email', and 'App Notification', all of which are unchecked. To the right of these checkboxes is a trash icon.

Click on the **Save** button to save the configuration.

Example 7: Alert for Overtime Limit Exceeds for User/Group In-charge.



If for Authorizing Overtime, the Weekly/Monthly overtime option is enabled for WO, PH, WO/PH as well as Daily overtime is enabled for the same day, then in this case the Alert would be sent twice to the respective user.

You can configure an Alert to notify a user/group in-charge about the Overtime Limit if it exceeds as described below.

Select the Alert Filter as a 'Time and Attendance', an event as a **Overtime Limit Exceeded-User/Overtime Limit Exceeded-Group In-charge** for which the alert is to be configured. Update the **Header** and **Footer** if required.

Enable the respective checkbox for **SMS** and/or **Email** and/or **App Notification** through which the alert is to be sent from the 'Additional Message Parameters'.

Configure the **Template ID** only if you have enabled **SMS** as the **Message Selection** option.

Configure the **Schedule Time** to send the Alert.

The screenshot shows the 'Alert Message Configuration' window. It has a title bar with a back arrow, edit icon, save icon, and close icon. The main content area includes:

- Alert Filter:** A dropdown menu set to 'Time and Attendance'.
- Event:** A dropdown menu set to 'Overtime Limit Exceeded - Group Incharge'.
- Header Message:** A text input field containing 'Dear User,'.
- Footer Message:** A text input field containing 'From COSEC Software'.
- Additional Message Parameters:** A section with a blue header and a collapse arrow. It contains:
 - Message Selection:** Three checkboxes for 'SMS', 'Email', and 'App Notification', all of which are checked.
 - Template ID:** A text input field.
 - Schedule Time:** A text input field with a red asterisk, containing '00:00'.
 - Processing Period:** A section with a bold header and a dropdown menu set to 'Previous'.
- Message Preview:** A section with a downward arrow.
- Assign Alert:** A section with a downward arrow.

Alert Message Configuration

Alert Filter: Time and Attendance

Event: Overtime Limit Exceeded - Group Incharge

Header Message: Dear User,

Footer Message: From COSEC Software

Additional Message Parameters

Message Selection: ☐ SMS ☐ Email ☐ App Notification

Template ID:

Schedule Time: 00:00

Processing Period

Processing Period: Previous

Message Preview

Assign Alert

- **Processing Period:** Select the processing period which is to be considered for the overtime calculation and generate an alert.

The Preview Message for **User** is as shown below.

Message Preview

SMS

Dear User,

[Daily OT limit exceeded on] [<AttendanceDate>], [Daily Permissible OT:] [<AllowedOT>], [Daily Actual OT:] [<ActualOT>], [Weekly/Monthly] [OT limit exceeded for] [<WeekStartDate to WeekEndDate> / <MonthStartDate to MonthEndDate>], [<Weekly/Monthly> Permissible OT:] [<AllowedOT>], [<Weekly/Monthly> Actual OT:] [<ActualOT>].

From COSEC Software

Mail

Dear User,

[Daily OT limit exceeded on][<AttendanceDate>].

[Daily Permissible OT:] [<AllowedOT>]

[Daily Actual OT:] [<ActualOT>]

[<Weekly/Monthly> OT limit exceeded for] [<WeekStartDate to WeekEndDate> / <MonthStartDate to MonthEndDate>].

[<Weekly/Monthly> Permissible OT:] [<AllowedOT>]

[<Weekly/Monthly> Actual OT:] [<ActualOT>]

From COSEC Software

The Preview Message to the **Group In-charge** about users is as shown below.

Message Preview

SMS
Dear User,

[Daily OT limit exceeded for] [<User1Count>User1(s) on] [<AttendanceDate>]. [Weekly OT limit exceeded for] [<User1Count> User1(s) for] [<WeekStartDate to WeekEndDate>]. [Monthly OT limit exceeded for][<User1Count> User1(s) for] [<MonthStartDate to MonthEndDate>].

From COSEC Software

Mail
Dear User,

Overtime limit exceeded for below listed User1(s):

Exceeded Daily Overtime					
No.	Date	User1 ID	User1 Name	Permissible OT	Actual OT
1	<attendance-date>	<User1-id>	<User1-name>	<permissibleOT>	<actualOT>
2	<attendance-date>	<User1-id>	<User1-name>	<permissibleOT>	<actualOT>

Exceeded Weekly Overtime						
No.	Week Start Date	Week End Date	User1 ID	User1 Name	Permissible OT	Actual OT
1	<week-start-date>	<week-end-date>	<User1-id>	<User1-name>	<permissibleOT>	<actualOT>
2	<week-start-date>	<week-end-date>	<User1-id>	<User1-name>	<permissibleOT>	<actualOT>

Exceeded Monthly Overtime						
No.	Month Start Date	Month End Date	User1 ID	User1 Name	Permissible OT	Actual OT
1	<month-start-date>	<month-end-date>	<User1-id>	<User1-name>	<permissibleOT>	<actualOT>
2	<month-start-date>	<month-end-date>	<User1-id>	<User1-name>	<permissibleOT>	<actualOT>

From COSEC Software



The Alert includes information about exceeded Overtime for Daily, Weekly and/or Monthly will be as per the configuration done in an **Time and Attendance Module > Overtime Policies**.

Configure the **Assign Alert** tab by selecting Users and the respective checkbox; **SMS/Email** for them through which they will be notified as shown below.

Assign Alert

Select User1s:

User1:

Search:

User1 ID ▲	Name	SMS <input checked="" type="checkbox"/>	Email <input checked="" type="checkbox"/>	
001A	priyanka thakur	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
002A	noshift	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
003A	fb	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
003CC	DONOTDELETE-KHUSHBU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
004A	ot	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

1 - 5 of 114 records

« < 1 2 3 ... 23 > »

Click on the **Save** button to save the configuration.

Example 8: Seamless VMS

a) Visitor Pre-Registration Alert

License required: Basic (For Alert Message Configuration page) & VMS (For Pre-Registration Alert)

The screenshot shows the 'Alert Message Configuration' window. On the left, the 'Alert Filter' is set to 'Visitor Management' and the 'Event' is 'Visitor Pre-Registration'. The 'Header Message' is 'Dear User/Visitor,' and the 'Footer Message' is 'From COSEC Software'. Under 'Additional Message Parameter', 'Message Selection' has 'App Notification' checked. 'Send Alert To' has 'Host' and 'Visitor' checked. On the right, a list of events is shown, with 'Visitor Pre-Registration' (ID 17) highlighted. The list shows 1-15 of 86 records.



It is mandatory for Authorized System Users to configure SMS and Email configuration for visitors of visitor Portal to send OTP on the Mobile number/Email Address Entered by the visitor.

b) Visitor Pre-Registration Approval/Rejection Alert

License required: Basic (For Alert Message Configuration page) & VMS (For Pre-Registration Alert)

The screenshot shows the 'Alert Message Configuration' window. On the left, the 'Alert Filter' is 'Visitor Management' and the 'Event' is 'Visitor Pre-Registration Approval/Rejection'. The 'Header Message' is 'Dear User/Visitor,' and the 'Footer Message' is 'From COSEC Software'. Under 'Additional Message Parameters', 'Message Selection' has 'SMS', 'Email', and 'App Notification' all checked. On the right, a list of events is shown, with 'Visitor Pre-Registration Approval/Rejection' (ID 58) highlighted. The list shows 46-55 of 55 records.

This alert will be dispatched to Host user associated with respected pre-registration application.

App Notification will be dispatched to Device ID mapped against respected Host / Visitor and Security User through cloud messaging notification provider.

Mobile Device Token will be user's / visitor's App Notification Token mapped in User Master Table & VMS Visitor Master table respectively.

c) Security Clearance Alert

The screenshot shows the 'Alert Message Configuration' window. The 'Alert Filter' is set to 'Visitor Management' and the 'Event' is 'Security Clearance'. The 'Header Message' is 'Dear User,' and the 'Footer Message' is 'From COSEC Software'. Under 'Additional Message Parameters', 'Message Selection' has 'SMS', 'Email', and 'App Notification' checked. 'Approval Links' and 'Approval Acknowledgment' are also checked. The 'Message Preview' section is empty. On the right, a list of events is shown, with 'Security Clearance' (ID 59) highlighted. The list shows 46 - 55 of 55 records, with page 4 selected.

ID	Event
50	Identification Server Inactive
51	Award/Penalty Application
52	Pending Applications For Approval
53	Schedule Unavailable - Users
54	Schedule Unavailable - Group Incharge
55	Schedule Modified
56	COSEC - Login Account Locked
57	Integrate Import/Export
58	Visitor Pre-Registration Approval/Rejection
59	Security Clearance

d) Visitor Pass Expired Alert

The screenshot shows the 'Alert Message Configuration' window. The 'Alert Filter' is 'Visitor Management' and the 'Event' is 'Visitor Pass Expired'. The 'Header Message' is 'Dear User/Visitor,' and the 'Footer Message' is 'From COSEC Software'. Under 'Additional Message Parameters', 'Message Selection' has 'SMS' and 'Email' unchecked, while 'Send Alert To' has 'Host', 'Visitor', and 'Security' checked. The 'Reminder Period (Minutes)' is set to 0. The 'Message Preview' section is empty. On the right, a list of events is shown, with 'Visitor Pass Expired' (ID 46) highlighted. The list shows 31 - 45 of 55 records, with page 3 selected.

ID	Event
35	Short Leave/Official Hours Application
36	Short Leave/Official Approval/Rejection
37	Duress
38	Shift Based Access Violations
39	Shift Change
40	Password Generated
41	Overtime/C-OFF Authorization
42	Worker Assignment
43	Worker Approval
44	Dead Man Zone Violation
45	Visitor Pass Expiry Reminder
46	Visitor Pass Expired
47	Self-Enrollment Notification
48	Work Order Expiry
49	OTP Generated

For any appointment, if Visit State is other than Check-OUT and Pass Expiry Time is reached, then this alert should be dispatched to Host / Visitor / Security based on Send Alert To selection.

e) Visitor Pass Alert

The screenshot shows the 'Alert Message Configuration' window. The 'Alert Filter' is set to 'Visitor Management' and the 'Event' is 'Visitor Pass'. The 'Header Message' is 'Dear Visitor,' and the 'Footer Message' is 'From COSEC Software'. Under 'Additional Message Parameters', 'Message Selection' has 'SMS' and 'Email' unchecked, and 'App Notification' checked. 'Scan Code' has 'QR' checked and 'Barcode' unchecked. The 'Message Preview' section is empty. On the right, a table lists 17 events, with 'Visitor Pre-Registration' at the bottom. The table has columns 'ID' and 'Event'. The bottom right shows '1 - 15 of 60 records' and a pagination control with '1' selected.

ID	Event
1	Monthly Attendance
2	Leave Approval
3	Leave Rejection
4	User Events
5	Leave Application
6	Missing In Punch - Users
7	Missing In Punch - Group Incharge
8	Missing Out Punch - Users
9	Missing Out Punch - Group Incharge
10	User Allowed
11	User Denied
12	Door Force Open
15	New Joining - Confirmation
16	Visitor Arrival
17	Visitor Pre-Registration

Once visit request is approved then visitor can generate Pass by themselves. Hence, the alert 'Visitor Pass' will notify visitors for Visit Pass via SMS & Email.



Visitor Pass Alert will be dispatched only when Visitor has applied Check-IN from Mail, Generate E-Pass from Mobile Application or from COSEC Visitor Portal and if security does creates pass from VMS Utility.

This 'Visitor Pass alert' includes Message, QR Code, Barcode and visit pass. Along with these, visitor will also get **Access PIN** of Visitor Profile which is assigned to visitor while Pass creation.

f) Visit Transfer Alert

The screenshot shows the 'Alert Message Configuration' window. The 'Alert Filter' is 'Visitor Management' and the 'Event' is 'Visit Transfer'. The 'Header Message' is 'Dear User/Visitor/Security,' and the 'Footer Message' is 'From COSEC Software'. Under 'Additional Message Parameters', 'Message Selection' has 'SMS' and 'App Notification' unchecked, and 'Email' checked. There is a 'Template ID' field with an information icon. 'Calendar Invite' has an information icon. 'Approval Links' is unchecked. 'Approval Acknowledgment' is unchecked. 'Send Alert To' has 'Host', 'Visitor', and 'Security' all unchecked. The 'Message Preview' section is empty. On the right, a table lists 17 events, with 'Visitor Pre-Registration' at the bottom. The table has columns 'ID' and 'Event'. The bottom right shows '1 - 15 of 86 records' and a pagination control with '1' selected.

ID	Event
1	Monthly Attendance
2	Leave Approval
3	Leave Rejection
4	User Events
5	Leave Application
6	Missing In Punch - Users
7	Missing In Punch - Group Incharge
8	Missing Out Punch - Users
9	Missing Out Punch - Group Incharge
10	User Allowed
11	User Denied
12	Door Force Open
15	New Joining - Confirmation
16	Visitor Arrival
17	Visitor Pre-Registration

A host user can transfer his visit Request to another Host & new Host may now Accept/Reject visits request. The 'Visit Transfer Alert' notifies the transferred host user about the transferred visit.

g) Visit State Change Alert

The screenshot shows the 'Alert Message Configuration' window. The 'Alert Filter' is set to 'Visitor Management' and the 'Event' is 'Visit State Change'. The 'Header Message' is 'Dear User/Visitor,' and the 'Footer Message' is 'From COSEC Software'. Under 'Additional Message Parameters', 'Message Selection' has 'Email' and 'App Notification' checked. 'Send Alert To' has 'Host', 'Visitor', and 'Security' checked. The 'Message Preview' section is empty. On the right, a table lists 17 events, with 'Visit State Change' at the top. The table has columns 'ID' and 'Event'.

ID	Event
1	Monthly Attendance
2	Leave Approval
3	Leave Rejection
4	User Events
5	Leave Application
6	Missing In Punch - Users
7	Missing In Punch - Group Incharge
8	Missing Out Punch - Users
9	Missing Out Punch - Group Incharge
10	User Allowed
11	User Denied
12	Door Force Open
15	New Joining - Confirmation
16	Visitor Arrival
17	Visitor Pre-Registration

Once the visit is requested, then there can be various state of application (such as Host Approval/Rejection, Security Clearance, Check-In, Start, On Hold, Resume, Stop, Check-OUT) which can be provided by any Visitor, Host or Security. This state change is notified by Visit State Change alert.

h) Visitor Pass Expiry Reminder

The screenshot shows the 'Alert Message Configuration' window. The 'Alert Filter' is set to 'Visitor Management' and the 'Event' is 'Visitor Pass Expiry Reminder'. The 'Header Message' is 'Dear User,' and the 'Footer Message' is 'From COSEC Software'. Under 'Additional Message Parameters', 'Message Selection' has 'SMS' and 'Email' checked. 'Expiry Reminder (Minutes)' is set to 10. 'Send Alert To' has 'Host', 'Visitor', and 'Security' checked. The 'Message Preview' section is empty. On the right, a table lists 17 events, with 'Visitor Pass Expiry Reminder' at the top. The table has columns 'ID' and 'Event'.

ID	Event
1	Monthly Attendance
2	Leave Approval
3	Leave Rejection
4	User Events
5	Leave Application
6	Missing In Punch - Users
7	Missing In Punch - Group Incharge
8	Missing Out Punch - Users
9	Missing Out Punch - Group Incharge
10	User Allowed
11	User Denied
12	Door Force Open
15	New Joining - Confirmation
16	Visitor Arrival
17	Visitor Pre-Registration

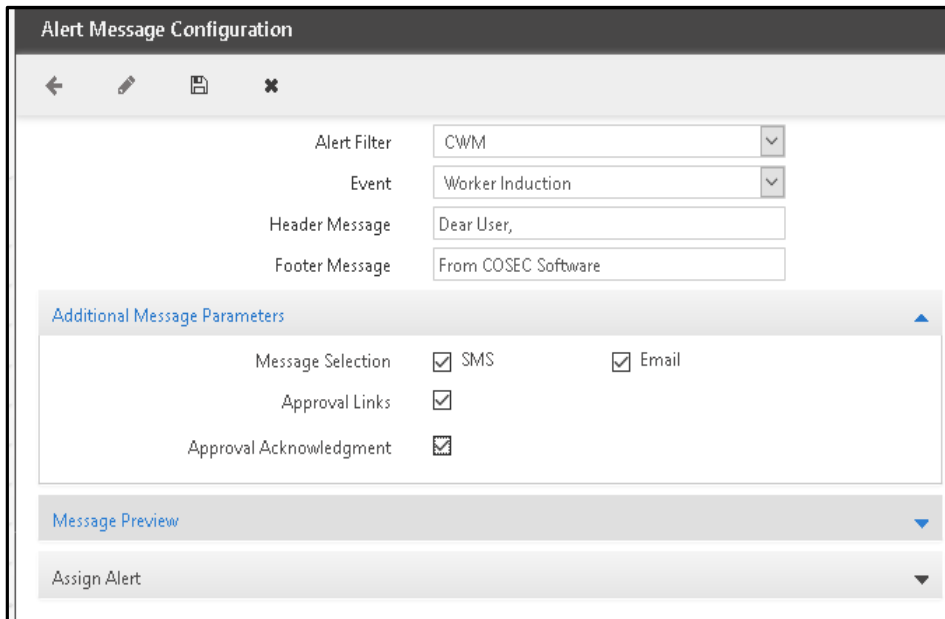
The Visitor Pass Expiry Reminder notifies the assigned Host/Visitor/Security when the Visitor Pass is about to expire.

Example 9: To get an alert for Worker Induction

(a) Worker Induction

This alert allows user to get notified about the Induction Approval application, created by the contractor for respective workers. User can also **Approve/Reject** the Induction application from the notified email if configured the same.

Select the alert filter as 'CWM', an event as a 'Worker Induction' and configure the Additional Message Parameters as shown below.



Alert Message Configuration

Alert Filter: CWM

Event: Worker Induction

Header Message: Dear User,

Footer Message: From COSEC Software

Additional Message Parameters

Message Selection: ☒ SMS ☒ Email

Approval Links: ☒

Approval Acknowledgment: ☒

Message Preview

Assign Alert

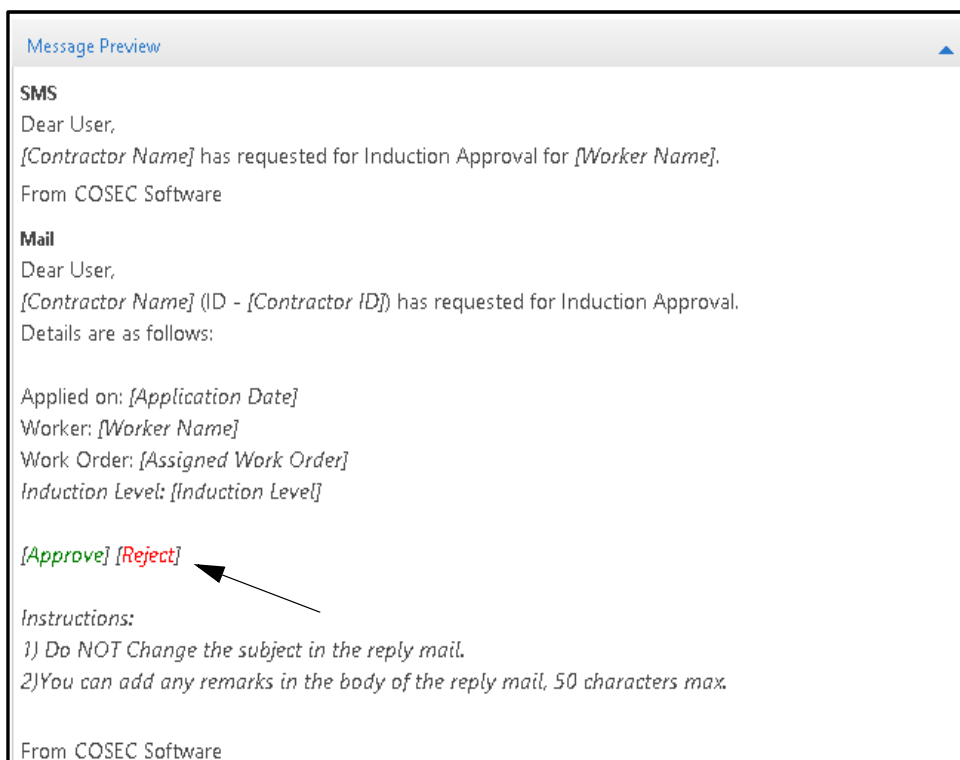
Select the required checkbox; **SMS** and/or **Email** through which the user will get notified.

Enable the **Approval Links** checkbox to include particular links into email body by which user can Approve/Reject the application. Enable **Approval Acknowledgment** checkbox to get an Acknowledgment email (*reply*) of the application if it is Approved/Rejected by respective user.



The 'Approval Links' and 'Approval Acknowledgment' can be enabled only if the Email option is checked On in 'Additional Message Parameters' as the link will be sent only on configured email address.

The Preview of the message is as shown below.



Message Preview

SMS

Dear User,

[Contractor Name] has requested for Induction Approval for [Worker Name].

From COSEC Software

Mail

Dear User,

[Contractor Name] (ID - [Contractor ID]) has requested for Induction Approval.

Details are as follows:

Applied on: [Application Date]

Worker: [Worker Name]

Work Order: [Assigned Work Order]

Induction Level: [Induction Level]

[Approve] [Reject]

Instructions:

1) Do NOT Change the subject in the reply mail.

2) You can add any remarks in the body of the reply mail, 50 characters max.

From COSEC Software

By clicking on the respective link; **Approve / Reject** the application can be approved or rejected.

Suppose the Application is approved by In-charge 1, then the 2nd alert will be sent to the In-Charge 2 for the verdict. If the In-charge 2 approves the application then the 3rd alert will be sent to the In-charge 3 and then so on, until the final verdict is not given by the last In-charge.

If the application is getting rejected by any of the In-Charge then, the final verdict will be considered as Rejected and alert will not be dispatched to the next In-Charge.

Configure the **Assign Alert** tab and assign an alert to the users as explained in above examples.

Assign Alert

Select Users: Randomly

User: ID Name

Search

User ID ▲	Name	SMS <input checked="" type="checkbox"/>	Email <input checked="" type="checkbox"/>	
DS_0	DS_0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
DS_1	DS_1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
DS_10	DS_10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Click on the **Save** button to save the configured alert.

(b) Worker Induction Approval/Rejection

You can create an another Alert for the 'Approval' or 'Rejection' of worker Induction. For this, select the Alert filter as 'CWM' and an event as 'Worker Induction Approval/Rejection'.

Alert Message Configuration

Alert Filter: CWM

Event: Worker Induction Approval/Rejection

Header Message: Dear User,

Footer Message: From COSEC Software

Additional Message Parameters

Message Preview

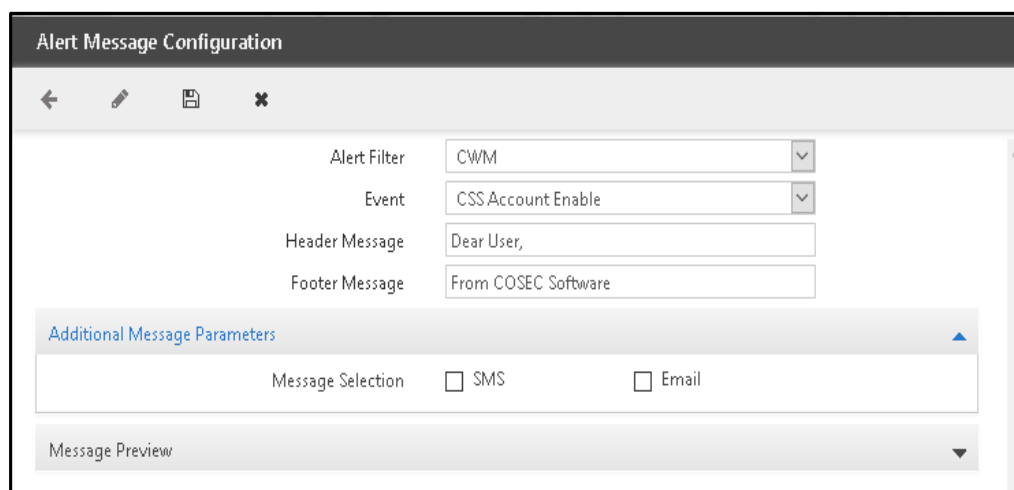
Assign Alert

Configure the rest parameters as explained above in '**(a) Worker Induction**'.

Example 10: To get an alert for the CSS account enabled

This alert allows you to get a notification through SMS and Email, once the CSS Account is enabled for the contractor.

Select the Alert Filter as '**CWM**' and Event as a '**CSS Account Enable**' as shown below.



The 'Alert Message Configuration' window displays the following settings:

- Alert Filter: CWM
- Event: CSS Account Enable
- Header Message: Dear User,
- Footer Message: From COSEC Software

The 'Additional Message Parameters' section includes:

- Message Selection: ☐ SMS ☐ Email

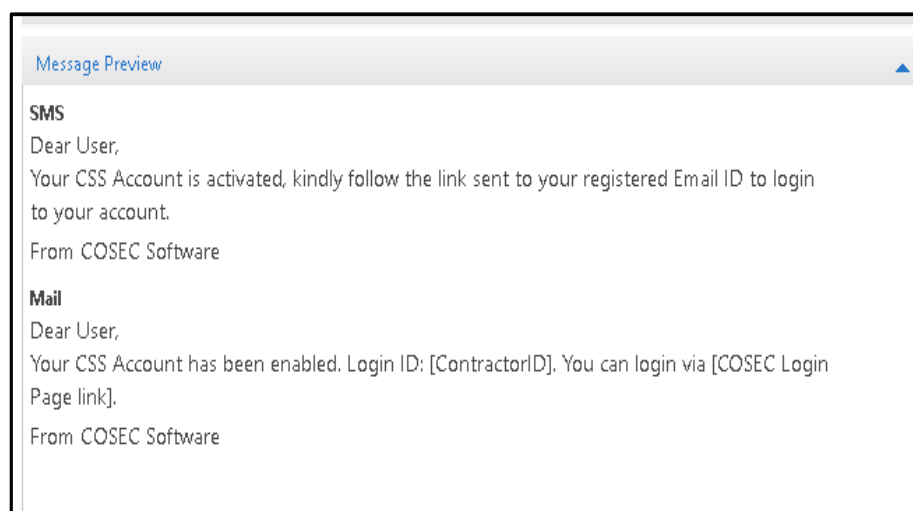
A 'Message Preview' section is located at the bottom of the configuration window.

Update the Header and Footer if required and configure the 'Additional Message Parameters' by enabling the respective checkbox; **SMS** and/or **Email** through which the user will get notified.



The Contractor Login ID and COSEC Login link can be sent only on user's email ID.

The preview of the message is as shown below.



The 'Message Preview' window shows the following content:

SMS
Dear User,
Your CSS Account is activated, kindly follow the link sent to your registered Email ID to login to your account.
From COSEC Software

Mail
Dear User,
Your CSS Account has been enabled. Login ID: [ContractorID]. You can login via [COSEC Login Page link].
From COSEC Software

Click on the **Save** button to save the configured alert.

Example 9: Birthday Greeting

'Birthday Greetings' allows you to configure an Alert which will send birthday wishes to the user as well as notify the same to the reporting In-charge and group through **SMS** and/or **Email**.

Select the alert filter as 'User', an Event as 'Birthday Greetings' and configure Additional message parameters as required.

Additional Message Parameters

Message Selection ☒ SMS ☐ Email

Send Alert To ☒ User ☐ Reporting In-Charge ☒ Group

Select Group

- ☒ Organization
- ☐ Branch
- ☒ Department
- ☐ Designation
- ☐ Section
- ☐ Category

Additional Recipients

Schedule Time * 06:00

Birthday Card

Upload Card

The message preview is as shown below.

Message Preview

SMS
Dear [UserName]
Greetings, matrix wishes you a very happy birthday and a great year ahead.ksjghkdgfdhk0 [User]
From COSEC Software

Mail
Dear [UserName]
[OrganizationName] wishes you a very Happy Birthday!

**May your birthday be the start of a year with full of happiness and brings you much success.
All the best. Have a good day**

Attached Birthday Card

From COSEC Software

You can also configure the **Assign Alert** tab as explained in above example.

Click on the **Save** button to save.

Example 13: Contractor Validity

This Alert is used to send alert message to both Users and Contractors, informing them about upcoming Contractor validity end date via SMS and email.

Select **Alert Filter** as “ALL or CWM” and **Event** as “Contractor Validity”

The screenshot shows the 'Alert Message Configuration' window. The 'Alert Filter' is set to 'All'. The 'Event' dropdown menu is open, showing a list of events. 'Contractor Validity' is highlighted in blue. Other events in the list include 'CSS Account Enable', 'Award/Penalty Application', 'Pending Applications For Approval', 'Schedule Unavailable - Users', 'Schedule Unavailable - Group Incharge', 'Schedule Modified', 'Login Account Locked', 'Integrate Import/Export', 'Visitor Pre-Registration Approval/Rejection', 'Security Clearance', 'Visit Transfer', 'Visitor Pass', 'Visit State Change', 'Event Authorization', 'Visitor - Login without OTP', 'Overtime Limit Exceeded - User', 'Overtime Limit Exceeded - Group Incharge', 'Worker Induction', 'Worker Induction Approval/Rejection', and 'CSS Account Enable'.

Additional Message Parameters

Expand the tab and Enable the respective checkboxes; Message Selection and Send Alert according to which the alert will be generated. Also, set the **Reminder Period (In Days)** which will allow you to set a particular scheduled time to resend an alert message to the user and contractor regarding the expiry of Contractor's Validity.

The screenshot shows the 'Alert Message Configuration' window with the 'Additional Message Parameters' tab expanded. The 'Alert Filter' is set to 'CWM' and the 'Event' is set to 'Contractor Validity'. The 'Header Message' is 'Dear User,' and the 'Footer Message' is 'From COSEC Software'. The 'Message Selection' section has checkboxes for 'SMS' and 'Email', both of which are checked. The 'Send Alert To' section has checkboxes for 'User' and 'Contractor', with 'User' checked. The 'Reminder Period (In Days)' section contains a table with the following data:

Days Before Validity End Date	Reminder Time	Repeat Reminder	Repeat Interval (In Days)
5	11:34	No	1

Preview:

Message Preview

User:

SMS:

Dear User,
Validity End Date is approaching for [Contractor Count] Contractor(s).
From COSEC Software

MAIL:

Dear User,
Validity End Date is approaching for following Contractor(s):

Sr. No.	Contractor Type ID	Contractor ID	Contractor Name	Validity End Date	Days Remaining
1	[ConTypeID]	[ConID]	[ConName]	[EndDate]	[days]

From COSEC Software

Contractor:

Dear User,
Your Validity End Date is approaching in [days] day(s). / Your Validity End Date is today.

From COSEC Software

Expand the **Assign Alert tab** and select the required users to which the Alert is to be configured and, enable the App Notification checkbox for the respective one.

Assign Alert

Select Users

Randomly

User

ID

Name

Select Contractors

Randomly

Contractor

ID

Name

Add

Search

User ID	Name	Contractor ID	Contractor Name	SMS	Email
E01	Utsav Pal	E11	RAVI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

You can also configure the **Assign Alert** tab as explained in above example.

Click on the **Save** button to save.

Example 14: Contractor Details Alert

This alert event is used to send the message to the **User** and **Contractor** regarding the validity and expiration date as per the custom field's.

Alert Message Configuration

←
✎
📄
✕

Alert Filter

CWM

Event

Contractor Details Alert

Header Message

Dear [User/ContractorName]

Footer Message

From COSEC Software

Additional Message Parameters

▼

Message Preview

▼

Assign Alert

▼



Custom field will be only shown in table if there type is mentioned as “Date” in the global policy.

Additional Message Parameters

Message Selection

☐ SMS
 ☒ Email

Send Alert To

☒ User
 ☐ Contractor

Reminder Period (In Days)

Send Alert For	Field Name	Days Before Expiry	Reminder Time	Repeat Reminder	Repeat Interval(In Days)	
Yes	txt	1	12:00	Yes	1	✎
No	Custom Field 2	0	00:00	No	1	✎
No	Custom Field 3	0	00:00	No	1	✎
No	Custom Field 4	0	00:00	No	1	✎

Message Preview

▼

Assign Alert

▼

Message Preview:

Message Preview

User:
SMS:
Dear [User/ContractorName],bye
Expiry Date is approaching for documents of [Contractor Count] Contractor(s).
From COSEC Software.....
EMAIL:
Dear [User/ContractorName],bye
Expiry Date is approaching for documents of following Contractor(s):

Sr. No.	Contractor ID	Contractor Name	Field Name	Validity End Date	Days Remaining
1	[ConID]	[ConName]	[FldLabel]	[EndDate]	[days]

From COSEC Software.....
Contractor:
SMS:
Dear [User/ContractorName],bye
[Validity of your few documents is going to expire./ Validity of your few documents is going to expire today.]
From COSEC Software.....
EMAIL:
Dear [User/ContractorName],bye
[Validity of following documents is going to expire:/ The validity of following documents is going to expire today:]

Sr. No.	Field Name	Validity End Date	Days Remaining
1	[FldLabel]	[EndDate]	[days]

From COSEC Software.....

Assign Alert

Configure the **Assign Alert** tab by selecting Users and the respective checkbox; **SMS/Email** for them through which they will be notified as shown below

Assign Alert

Select Users

Randomly

User

ID

Name

Select Contractors

Randomly

Contractor

ID

Name

Fields Approaching Expiry Date

☐ txt

☐ Custom Field 2

☐ Custom Field 3

☐ Custom Field 4

Add

Search

User ID	Name	Contractor ID	Contractor Name	Fields Approaching Expiry Date	SMS	Email	
001A	priyanka thakur	1204	Matrix_contractor	Custom Field 2, Custom Field 3, Custom Field 4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Now, after previewing the Message and configure the assign Alert, click on the **Save** button to save the Alert message Configuration.

Example 15: Guard Tour Violation

This alert is used to send a message regarding the violation occurred during Guard Tour.

Alert Filter	Access Control
Event	Guard Tour Violation
Header Message	Dear User,
Footer Message	From COSEC Software
Additional Message Parameters	
Message Preview	
Assign Alert	

Additional Parameter

Additional parameter enables to select the modes of alert to be sent i.e via SMS, E-mail or/and App Notification. It also allows you to send configured alert to the User and/or Reporting Incharge if required on each guard tour violation.

Additional Message Parameters			
Message Selection	<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> App Notification
Send Alert To	<input checked="" type="checkbox"/> User	<input type="checkbox"/> Reporting Incharge	

Message Preview

It shows the final message preview before sending it to the user and/or report-in-charge.

Message Preview	
SMS	
Dear User,	
Guard Tour Violated by [Username] ([User ID]) on [Door Count] Door(s) at [date-time].	
From COSEC Software	
Email	
Dear User,	
Guard Tour Violated by [Username] ([User ID]) on below [Door Count] Door(s) at [date-time].	
Door ID	Name
[Door ID]	[Door Name]
App Notification	
Guard Tour Violated by [Username] ([User ID]) on [Door Count] Door(s) at [date-time].	

Message can also be edited by clicking on the message line as shown below.

Once the modifications are done, click on **OK** button to save or **Default** to reset the message.

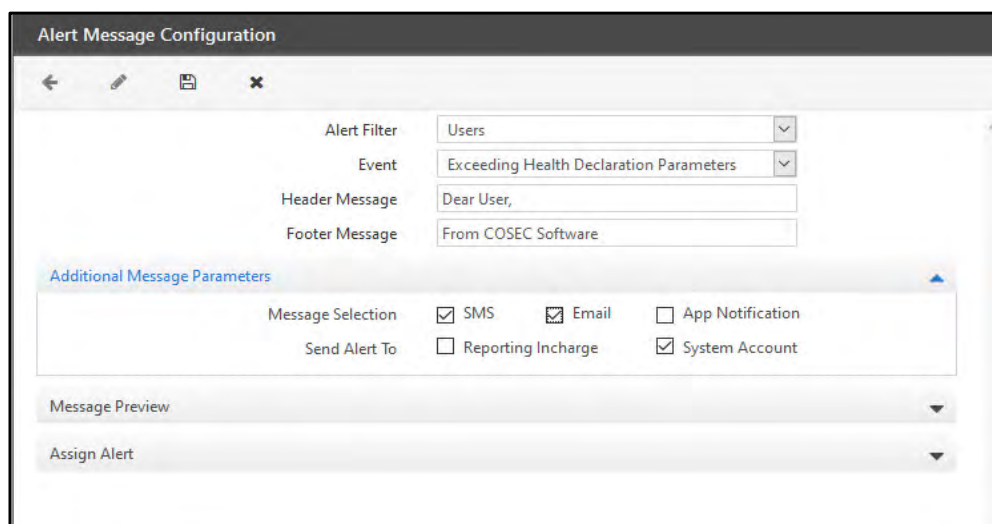
Assign Alert

Configure the **Assign Alert** tab by selecting Users and the respective checkbox; **SMS**, **Email**, **App Notification** through which they will be notified as shown below.

Click on the **Save** button to save or **Cancel** to cancel the Alert configuration.

Example 16: Exceeding Health Declaration Parameters

This alert is used to get notified about the health parameters of users if they are exceeding from their specified threshold value.



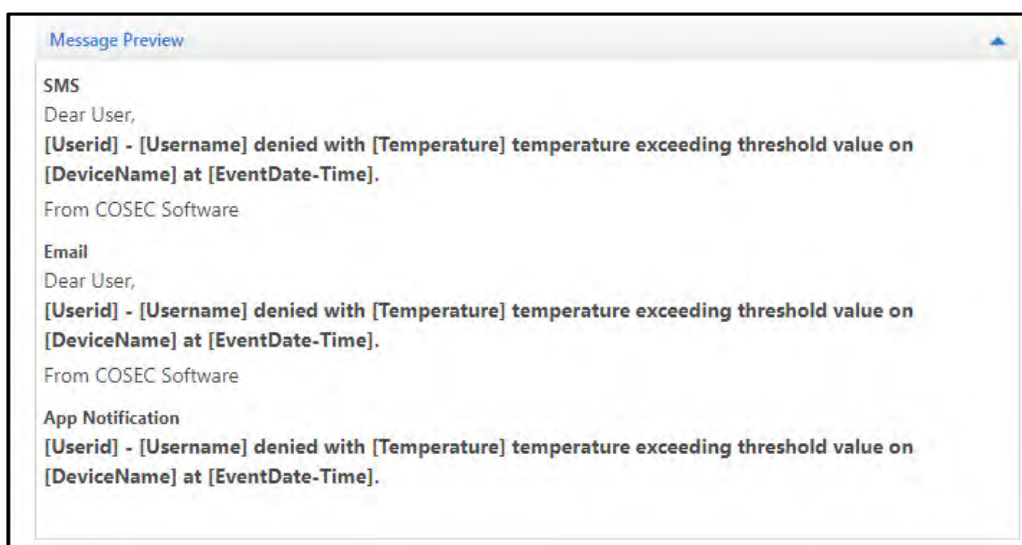
The 'Alert Message Configuration' window is a modal dialog with a title bar and standard window controls. It contains the following fields and options:

- Alert Filter:** A dropdown menu set to 'Users'.
- Event:** A dropdown menu set to 'Exceeding Health Declaration Parameters'.
- Header Message:** A text input field containing 'Dear User,'.
- Footer Message:** A text input field containing 'From COSEC Software'.
- Additional Message Parameters:** A section containing:
 - Message Selection:** Three checkboxes: 'SMS' (checked), 'Email' (checked), and 'App Notification' (unchecked).
 - Send Alert To:** Two checkboxes: 'Reporting Incharge' (unchecked) and 'System Account' (checked).
- Message Preview:** A button with a dropdown arrow.
- Assign Alert:** A button with a dropdown arrow.

This alert can be sent to Report-in-charge and System Administrator.

In the same way alerts can be configured for the events like Health Declaration Pending, User Denied/allowed-Threshold Temperature Exceeded.

Message Preview



The 'Message Preview' window displays the formatted alert message for the selected configuration. It shows three sections: SMS, Email, and App Notification, each with the same content:

```

SMS
Dear User,
[Userid] - [Username] denied with [Temperature] temperature exceeding threshold value on
[DeviceName] at [EventDate-Time].
From COSEC Software

Email
Dear User,
[Userid] - [Username] denied with [Temperature] temperature exceeding threshold value on
[DeviceName] at [EventDate-Time].
From COSEC Software

App Notification
[Userid] - [Username] denied with [Temperature] temperature exceeding threshold value on
[DeviceName] at [EventDate-Time].
  
```

The message can also be edited if required.

Assign Alert

Assign Alert

Select Users Randomly

User ID Name

Search

User ID	Name	SMS	Email	App Notification	
1087	KALPESH DIYORA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
1095	ABHAY JOSHI	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Once the configurations are done, Click on the **Save** button to save the alert.

Sending Messages from COSEC

The COSEC system can be configured to send preset alerts or customized messages to its users in response to certain predefined user events. If such a predefined user event occurs, it will trigger off an alert message to be sent to the relevant user or users via SMS or e-mail. A system administrator may also choose to send custom messages to selected users. COSEC allows you to configure both alert messages and custom messages.

- [“Configuring Alert Messages”](#)
- [“Configuring Custom Messages”](#)

Configuring Custom Messages

Custom messages unlike alert messages are not predefined in their formats. These are customizable messages that the system administrator can send to employees on events, other than those predefined for alert message configuration.



1. Before configuring the Custom messages, it is required to configure the SMS and Email settings to send the custom message successfully via Email and SMS. The configuration can be done from the path: **Admin Module > System Configuration > SMS/Email Configuration** pages.

2. It is also required that Alert services must be running prior to sending the Custom Messages.

To send a Custom Message,

Go to **Admin Module > System Configuration > Custom Message** and the following screen appears.

This page allows the user to configure the following parameters:

Message Header - Enter the required message for the message header.

Message Footer - Enter the required message for the message footer.

Message - Enter the message body.

Subject- Enter the message subject.

Send Message Via- Select the mode via which the message is to be sent to recipients. The dropdown list contains three options — **SMS**, **Email** and **SMS & Email**.

Template ID: As per TRAI Regulation, an enterprise which sends messages to customers like OTP, communication message, promotional messages via SMS, have to register their entity and the content template to avoid Spam, fake and fraudulent communication through SMS.

Template ID will be applicable only when **Send Message Via** is selected as SMS/ SMS & Email.

An Admin needs to register the SMS content template beforehand with your Service Provider which will be verified before it is delivered to the users.

Once registered, the Service Provider will provide a Template ID against the registered SMS content.

Template ID will be visible and needs to be configured only for newly added Service Providers. To know more, refer Service Provider under “SMS Configuration”.

For Custom Messages, if the Service Provider supports sending a SMS without Template ID, messages will be delivered to the users. Contact your Service Provider for details.



If you have multiple Service Providers, then make sure the required templates are registered with all the desired Service Providers. Hence for each template you will have multiple Templates IDs. Also make sure you maintain a record of all the registered Message Templates with their respective Template IDs for reference.

Select Users

Select Users: Select the group from the dropdown list to whom this message is to be sent. The options available are:

Select Users

User *

User Wise

Group Wise

All

Send

User Wise - To select users. Users available in the picklist are configured in the **Users** Module.

Select Users

User *

User Wise

ID

Name

Send

Group Wise - To select a group of users. Groups and their respective user available in the dropdown and picklist are configured in the **Enterprise Structure** Module.

Select Users

Group Wise

Select Group

Organization

Organization *

ID

Name

Send

ALL - To select all active users on the system.

Click the **Send** button to send the message to the specified recipients.

If the message is not sent due to any reason and **Error List** will be provided which displays the reason why the message was not sent to the user.

Error List	
Search	
User ID	Status
RI1	Mobile No. not configured

If the Custom Message was sent successfully, then you can check its status from *Admin> System Configuration> View/Logs> Alert View*.

Alert Log			
Date * 04/06/2021 04/06/2021			
View			
Filter			
Search			
Phone Number	Message	Date Time	Error/Status
7405309208	SDTE&TEvtTemplatelD=1543532532	04/06/2021 11:08:58	The remote name could not be resolved: '...
74050353792	SDTE&TEvtTemplatelD=1543532532	04/06/2021 11:08:58	The remote name could not be resolved: '...
46874635745	GHJFJHDJD	04/06/2021 11:00:02	The remote name could not be resolved: '...

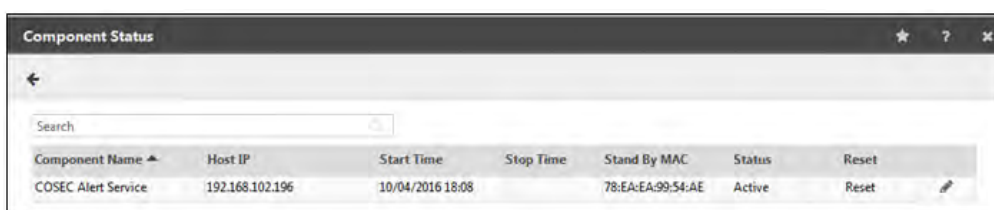
Component Status

The Component Status option enables the administrator to view the details of the *COSEC Alerts Service* running on the network as also to reset the status of the application in the event of the application crashing on the network. The COSEC system allows only one instance of the above components to run on the network at a time.

In the event of a crash the component status can be reset using this functionality which would thus enable the administrator to run the component from another computer on the network. The reset option however is not required in the event of restarting the component on the same computer.

In order to access this functionality,

1. Go to **Admin module > System Configuration > Component Status** and the following screen appears displaying the status of the COSEC Alerts Service application as displayed below.



Component Name	Host IP	Start Time	Stop Time	Stand By MAC	Status	Reset
COSEC Alert Service	192.168.102.196	10/04/2016 18:08		78:EA:EA:99:54:AE	Active	Reset

2. Apart from the **Component Name** it also displays the following information:
 - **Host IP:** Displays the IP Address of the computer where the application is or was last run.
 - **Start Time:** Displays the time when the application was last started.
 - **Stop Time:** Displays the time when the application was last stopped in the event of the status being inactive.
 - **Stand By MAC:** This field enables the administrator to enter the MAC address of Stand by Monitor.
 - **Status:** Displays the current activity status of the application.
 - **Reset:** This field enables the administrator to reset the activity flag of the application in the event of an application crash which would then enable the administrator to start the application from another computer on the network. This option however does not allow the administrator to stop an application which is running on the network.
3. Click the **Edit** icon corresponding to each **Component Name** to update or cancel the changes done to the Stand By MAC field.

Blocked Workstations

COSEC is a web-based application. Hence it is crucial that the system administrator is able to supervise all workstations that can login to the application, granting and denying access to specific workstations. This functionality enables the administrator to create a denial list of workstations which will be blocked from accessing the application.

To block a workstation, Go to **Admin module > System Configuration > Blocked Workstations** and the following screen appears.

ID	Name
No Data	

Click the **New** button to add the details of the workstation that is to be denied the access.

Blocked Workstation: Enter the name of the workstation. The ID will be generated by the system while saving the workstation.

IP Address: Enter the IP Address of the workstation which is to be denied the access.

Click the **Save** button to save the configured workstation.

ID	Name
1	System1

The blocked workstations grid displays all workstations which have been blocked from accessing the COSEC . The COSEC responds only to those workstations that are not displayed in this list.

All other workstations on the network would by default be able to access the COSEC application from their respective web browsers. So the administrator should include in this list, only those workstations which are to be denied permanent or temporary access to the application.

Configuring Locations

This feature enables COSEC to detect and record the source location for all punch events submitted from a mobile device using the ESS Application. This can be done by pre-configuring a set of locations on the Web Application. This will ensure that only punches entered by an employee from a pre-configured location radius are authenticated by the system as valid punches.

Geographical areas such as the office campus, branch offices, workshops, client offices etc. may be identified as valid locations for accepting attendance punches from employees. Hence, an employee who has entered the office campus area as per shift timings, may submit a punch from his current location, without having to physically approach the device.

To access configure locations on the COSEC Web Application,

Go to **Admin module > System Configuration > Location Master** and the following screen appears.

The screenshot displays the 'Location Master' configuration interface. On the left is a sidebar menu with options like System Accounts, System Configuration, Global Policy, Identification Server Configuration, SMS Configuration, Email Configuration, Rename Group, Enterprise Profile, Alert Message Configuration, Custom Message, Location Master (highlighted), Location Group, System Utilities, Views/Logs, License Information, and Download Manager. The main panel is titled 'Location Master' and contains a form with the following fields:

- Code ***: Text input with 'ID' entered.
- Location Name ***: Text input with 'Name' entered.
- Type**: Dropdown menu with 'GPS' selected.
- BLE Code**: Text input with '4 characters. 1111 to 9999' as a hint.
- BLE Name**: Text input with 'BLE Name' as a hint.
- Latitude ***: Text input with '8 characters. -90.0000 to +90.0000' as a hint and a location pin icon.
- Longitude ***: Text input with '9 characters. -180.0000 to +180.0000' as a hint.
- Location Radius (Meters) ***: Text input with '0' entered.
- Wi-Fi MAC Address**: Text input with a hint showing the format ' : : : : '.
- Address**: Text input.
- Mode**: Dropdown menu with 'Attendance' selected.
- Device**: Two text inputs, 'ID' and 'Name', with a list icon next to 'Name'.
- Alternate Address**: Text input.
- Port No. (HTTPS)**: Text input.
- Event Type**: Dropdown menu with 'Entry' selected.


To add a new location click the **New** button.

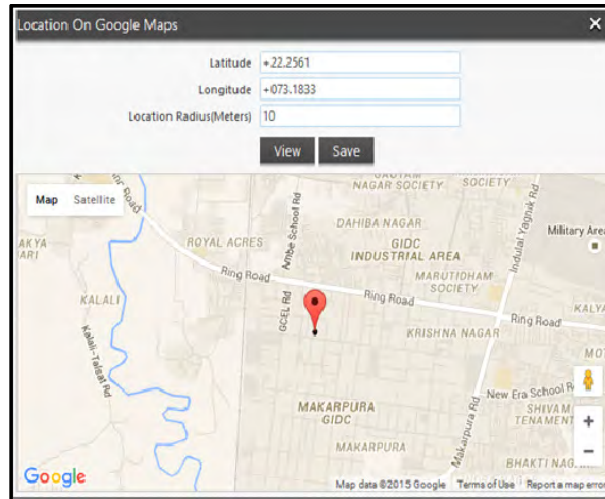
Every location is configured with a **Code** and **Location Name**.

Type: Select the type from the drop down options based on which location is to be defined.

- **GPS:** Enter the Latitude, Longitude and location radius.
- **Wi-Fi:** Enter the Wi-Fi MAC address of a specific Wi-Fi access point to define the coverage area.
- **BLE- Beacon:** Enter the **BLE Code** for configuring location based on bluetooth enabled beacon. Select the Mode as Attendance and or Access Control.
- **BLE- Device:** Enter the **BLE Name**. Valid characters are maximum 10 alphanumeric characters. Mode will be set as Attendance automatically.

A location can be defined by recording its geographical details such as **Latitude**, **Longitude** and **Location Radius** i.e. the radius in meters over which the area would be spread.

Click the  button to view and edit the coverage area, as per requirement.



Navigate and click a location on the map to select its latitude and longitude. You can also manually enter the location details and click the **View** button to view the location. Edit the location radius, if required.

Address: You can specify the address of the location.

Device: When Mode is selected as Access Control or Both then you can select the direct doors and Panel200 doors from the picklist.

Alternate Address: It is the external network (public network) IP address of device.

If Door V3 is selected for Location1. The IP address (Internal Address) of Door V3 is 192.168.104.114. The Alternate Address of Door V3 is 173.183.4.11:43.

When the door is accessed from external network then alternate address will be used for communication.

If you are using APTA in the external network at Location1 and tries to access Door V3, then it will be accessed through 173.183.4.11:43. In Door API response to APTA, alternate IP address will be sent in response.

The communication between the device and the external network takes place via device port configured in **Port No. (HTTPS)**.

Port No. (HTTPS): Enter the Device Port number for secure communication between the device and the external network.



The Device must be Wi-Fi enabled so that it can be accessed through external network.

Event Type: Select the event type as **Entry** or **Exit** which will identify the events from the BLE-Beacon or BLE-Device based locations as Entry event or Exit event.



The In-built bluetooth is supported in VEGA door only.

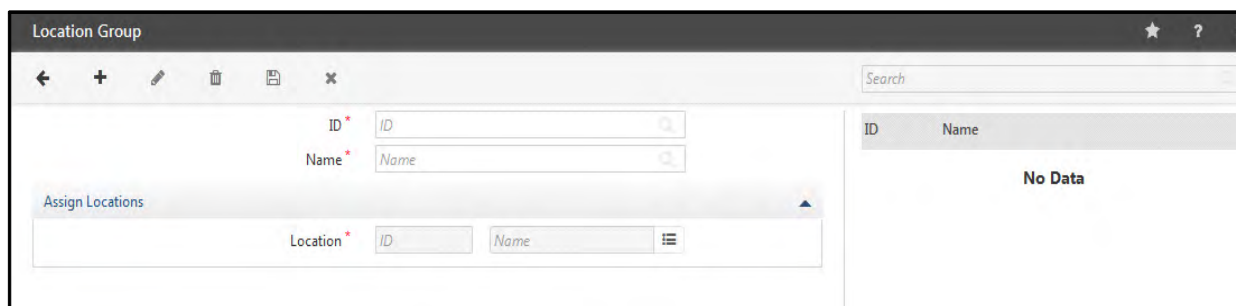
Click the **Save** button from the toolbar to save the Location Master configuration.

Location Group

This page allows defining location groups as collection of multiple locations. Location group can then be used while defining Field Visit Schedule for users.

To create location group, Select the **Admin module> System Configuration> Location Group**.

The **Location Group** page appears as shown below.



Location Group

ID *

Name *

Assign Locations

Location *

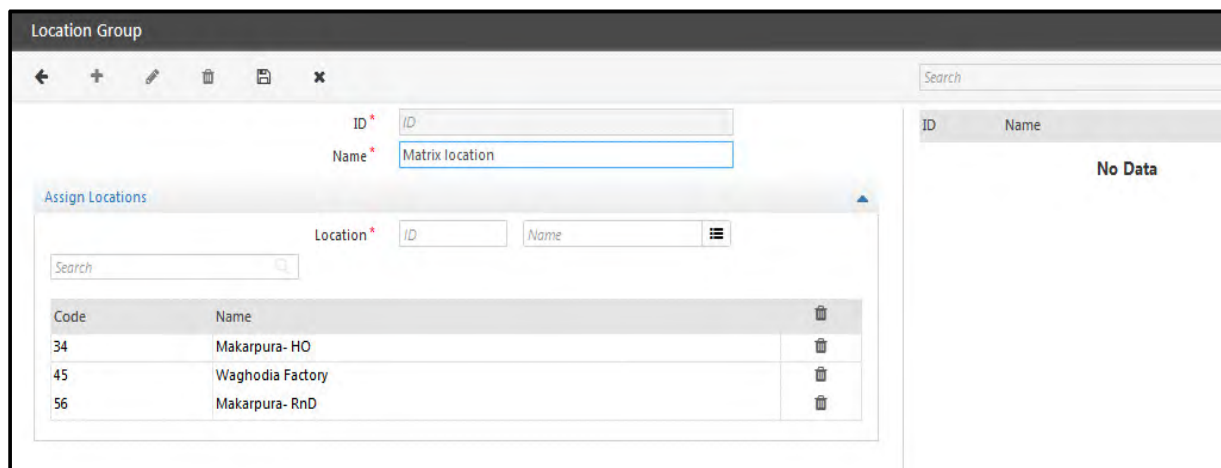
ID	Name
No Data	

Click the **New** button to configure a new location group.

ID: The ID will be generated automatically after saving the location group.

Name: Specify a name of the location group.

Location: Click the picklist button and select the locations to include in the location group. The locations can be configured in the Location Master.



Location Group

ID *

Name *

Assign Locations

Location *

Code	Name
34	Makarpura- HO
45	Waghodia Factory
56	Makarpura- RnD

ID	Name
No Data	

Click on **Save** button to save the configured location group.



1. You can assign multiple locations to one location group.
2. Same location can be added in multiple location groups.



System sends Field Schedule Modified Alert to User for schedule dates whose records have been affected by addition or removal of location from location group.

Agreement Builder

The Visitor Portal is used for — creating visit by visitor, for checking-in and checking-out of visitors as well as maintaining visit logs of the visitors.

To enhance the utility of the Visitor Web Portal, the provision for displaying an Agreement and /or a Form (Questionnaire) has been added. To be able to use this functionality, you need to configure the Agreement and Form parameters in COSEC Web.

You can configure the content of the Agreements/Forms as per your requirement. You can also link any Agreement with a Form. You can determine the placement of the Agreement/Forms — Login, Check-in, Check-out. The Agreement/Forms configured here will be displayed in the Visitor Web Portal.

You can send Alert Messages when Forms are executed by Visitors. To do so, click **Admin Module > Alert Configuration**. In **Alert Filter** make sure you select **Visitor Management** and in the **Event** you select **Visitor Form Execution**. For details, refer to [“Configuring Alert Messages”](#).

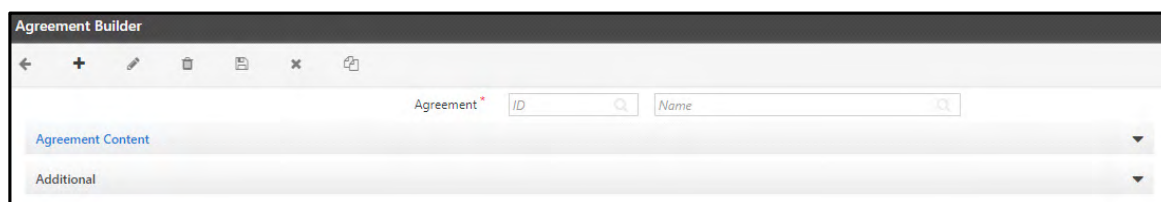
To create the form, select the **Admin Module> System Configuration> Form Builder**. For details refer to, [“Form Builder”](#).

To determine the placement of the Agreement/Forms — Login, Check-in, Check-out of Visitor as per your requirement. For details refer to [“Station Location”](#).


Agreement Builder

To create the agreement, select the **Admin Module> System Configuration> Agreement Builder**.

The **Agreement Builder** page appears.



To add a new Agreement,

- Click the **New**  icon. You can add upto 99 different agreements.
- **ID**: The ID is auto-generated by the system. It will be displayed after you save the agreement.
- **Name**: Assign a name to the agreement.

The Agreement is divided into — Agreement Content and Additional.

Agreement Content

Click the **Agreement Content** collapsible panel to configure the parameters. This section is divided into three sub-sections — Header, Content and Footer.

- **Header:** This will be displayed on top before the Agreement Content. This is the Title you wish to provide. Maximum 100 characters.
- **Content:** You can add text or media here.

The text can be in the form of Terms and Conditions or any Contract requirements or Non Disclosure Agreements or any text as per your requirement. Maximum 5000 characters.

In Media, you can upload an image, pdf or video relevant to the agreement.



You can either upload an image/pdf or video. Both cannot be uploaded.

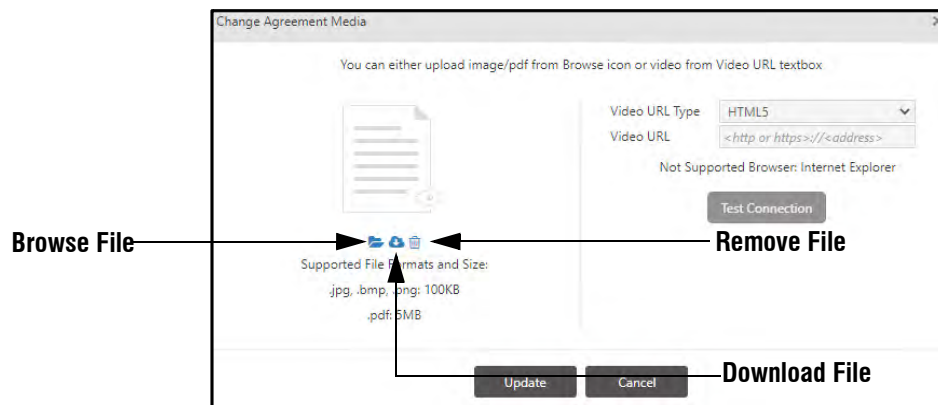
Uploading Image/PDF

- Clicking **Upload**  . The **Change Agreement Media** pop-up appears.


- Click **Browse File**  .


To upload, select the desired file from your local PC.


Make sure the image size is not more than 100KB and the pdf is upto 5MB. The supported formats are .jpg, .bmp, .png, pdf




After uploading the file, if you wish to upload a different file instead of the current uploaded file, click

Browse File  again and select the desired file from your local PC. The previously uploaded file will get replaced with the new file.

To download the uploaded file, click **Download File** .

To remove the uploaded file, click **Remove File** .

Then click **Update**.

The document will be uploaded and you can preview it by clicking the **Preview**  icon.



PDF can be viewed only after it is downloaded.

Uploading Video

You can also upload a relevant video. To do so,

- Select the desired option for uploading the **Video URL Type** — **HTML5, FTP, YouTube, Vimeo, Wistia, Custom Embed (iFrame)**.

If you select **FTP**, in **Video URL** enter the desired FTP URL from where the COSEC will fetch the video. To access the FTP URL, you need to enter the FTP credentials. Enter the **User Name** and **Password**. **User Name** can be a maximum of 40 characters and **Password** can be a maximum of 128 characters.

Change Agreement Media

You can either upload image/pdf from Browse icon or video from Video URL textbox

Video URL Type: **FTP**

Video URL:

FTP File Formats: .mp4, .mov.

FTP Size: 100 MB.

Username:

Password:

Not Supported Browser: Internet Explorer

Test Connection

Supported File Formats and Size:

.jpg, .bmp, .png: 100KB

.pdf: 5MB

Update Cancel

If you select **YouTube, HTML5, Vimeo** or **Wista**, in **Video URL** enter the desired URL from where the COSEC will fetch the video.

Change Agreement Media

You can either upload image/pdf from Browse icon or video from Video URL textbox

Video URL Type: **YouTube**

Video URL:

Test Connection

Supported File Formats and Size:

.jpg, .bmp, .png: 100KB

.pdf: 5MB

Update Cancel

If you select **Custom Embed (iFrame)**, in **Video URL** enter the video URL which is the extracted URL from embed code which belongs to any video on web platform.

Follow the steps given below to extract the URL from the embed code, for example to extract the URL from a YouTube video:

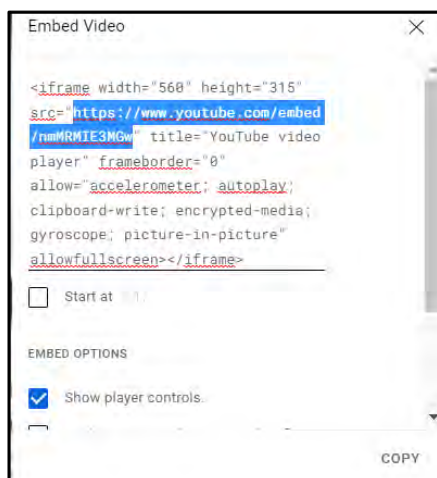
- Click on the desired Video.



- Click **Share**.



- Click **Embed**.



- In the **Embed Video** pop-up select the link as shown above. Paste this link in the **Video URL**.

Similarly, you can copy the link from any other web video and paste the same in the Video URL.



- File formats supported for FTP/Web[HTML5, YouTube, Vimeo, Wistia, Custom Embed(iFrame)] are .mp4 and .mov.
- For a video to be displayed using the FTP link make sure the file size is 100MB.
- Make sure the Web Video URL's — HTML5, YouTube, Vimeo, Wistia, Custom Embed(iFrame) do not have any type of authentication.
- Click **Test Connection** to check the connectivity, to fetch the video data from the configured URL.



If the Test Connection is Successful, it only depicts that there is connectivity till the Video URL link. The video may or may not be functional.

- Click **Update**. The video will be uploaded.
- **Footer:** You can add the desired text. This will be displayed at the end of the Agreement, before the Signature. Maximum 100 characters.

Additional

Click the **Additional** collapsible panel and configure the following parameters:

- **Signature:** Select the check box, if you want the user to add their signature along with their confirmation.
- **Confirmation Style:** This defines the way in which the confirmation to the drafted agreement would be provided. Select the desired **Confirmation Style** as **Agree Checkbox** or **Buttons (Accept/Decline)**.

If you select **Agree Checkbox**, a check box will be provided to agree with the Terms and Conditions.

If you select **Buttons (Accept/Decline)**, two buttons — 'Accept' and 'Decline' will be provided to agree with the Terms and Conditions.

Click **Save** to save the configuration. The Agreements you add appear in the right pane.

Sample of Agreement if you select **Agree Checkbox**, as displayed in the VMS Portal.

MATRIX

Check-In Form

Profile

Visit

Visit Form Agreement

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Quis ipsum suspendisse ultrices gravida. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Quis ipsum suspendisse ultrices gravida. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Quis ipsum suspendisse ultrices gravida.

☒ I agree with terms and condition.

NEXT >

Sample of Agreement if you select **Buttons (Accept/Decline)** as displayed in the VMS Portal.

MATRIX

Check-In Form

Profile

Visit


Visit Form Agreement


Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Quis ipsum suspendisse ultrices gravida. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Quis ipsum suspendisse ultrices gravida. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Quis ipsum suspendisse ultrices gravida.


DECLINE ACCEPT


Top Panel Functionality

After the Agreements have been created, you can perform the following:

Click **Add** , to add a new Agreement.

Click the desired agreement from the list of agreements in the right pane. Click **Edit** , if you wish to make modifications in the existing agreement.

Click the desired agreement from the list of agreements in the right pane. Click **Delete** , if you wish to delete the agreement.

Click the desired agreement from the list of agreements in the right pane. Click **Duplicate** , if you wish to replicate the agreement.

Form Builder

We all know that collecting feedback, opinions, data etc via Forms is an important aspect for every organization.

The Form Builder allows you to customize the design of the questionnaire in the form of different formats, convey messages as well as provide feedback. You can customize the content of the Forms as per your requirement. You can also link any Agreement with a Form. For details related to Agreements, refer to [“Agreement Builder”](#).

You can determine the placement of the Agreement/Forms — Login, Check-in, Check-out of Visitor as per your requirement. For details refer to [“Station Location”](#).

For displaying the Form and Agreement on Visitor Web Portal, you need to configure the Form and Agreement parameters in the COSEC Web.

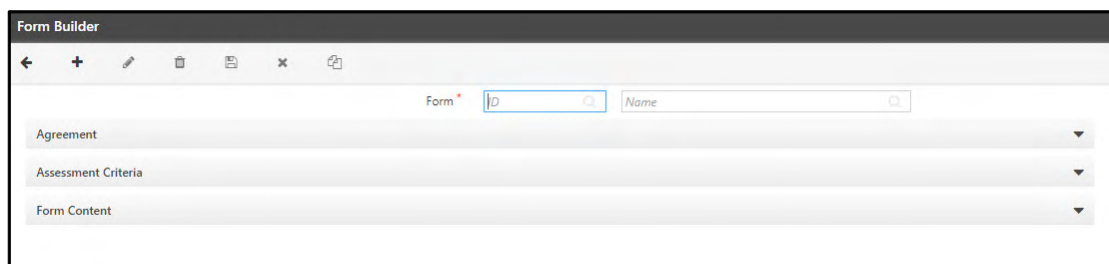
After the Form is submitted by the Visitor, the details are displayed in the Form Summary. For details refer to [“Form Summary”](#).

You can send Alert Messages when Forms are executed by Visitors, to do so click **Admin Module> System Configuration> Alert Message Configuration**. Select Visitor Event from the Alert filter drop-down list and Visitor Execution from the event drop-down list. For details, refer to [“Configuring Alert Messages”](#).


To configure the Form parameters:

Click **Admin Module> System Configuration> Form Builder**.

The **Form Builder** page appears.



To add a new Form,

Click the **New**  icon. You can add upto 99 different Forms.

- **ID:** The ID is auto-generated by the system. It will be displayed after you save the form.
- **Name:** Assign a name to the form.

The Form Builder is divided into three sections— **Agreement**, **Assessment Criteria** and **Form Content**.

Agreement

Click the **Agreement** collapsible panel and configure the following parameters:

- **Agreement Selection:** Click the picklist to select and bind a pre-configured agreement with this form.
- **Position At:** Select the position — Starting, Ending — at which you want the agreement to be displayed.

If you select **Starting**, the agreement will be displayed before the form.

If you select **Ending**, the agreement will be displayed after the form is filled-in.

Assessment Criteria

This defines the eligibility criteria on the bases of which the further functionality would be executed.

Click the **Assessment Criteria** collapsible panel and configure the following parameters:

- **Approve On:** Select the desired eligibility criteria for further action — All Correct, Minimum Percentage, Any Condition.

All Correct: If you select this option, the visitor will be allowed further course of action only if all the questions are answered correctly.

Minimum Percentage: If you select this option, the visitor will be allowed further course of action only when the defined percentage value cut-off score is achieved as the score after answering the questions.


Any Condition: If you select this option, the visitor will be allowed further course of action without fulfillment of any condition.

- **Display Score to User:** Select this check box if you wish to display the score to the visitor after the questionnaire is filled-in.

Form Content

In the Form Content, you first need to add Sections. In each Section you can then add different types of questions as Multi-Choice, Single-Choice, Text Answer Only, Fixed Content, Rating.

Create a list of Sections and the questions to be added in each Section manually as after you have completed a Section and its questions and then add a new Section, you will not be able to add other questions in the previous Section.


If you still wish to do so, you will have to add the desired question in the current Section and then click Move  or drag and drop it to the desired Section.






Click the **Form Content** collapsible panel and configure the following parameters:

A screenshot of the 'Form Content' panel. It has a title bar 'Form Content' and a main area with the text 'No data added yet. Click '+' to start.' and a plus icon in the bottom right corner.

Section

To add a **Section**,

A screenshot of the 'Form Content' panel. It shows a section titled 'Section 1' with a plus icon and a trash icon. Below it, there is a question: '(1) Multiple Choice Question' with the text 'Which are the products of Matrix Comsec company?'. A context menu is open on the right side of the section, showing options: Multi-Choice, Single-Choice, Text Answer Only, Fix Content, Rating, and Section.


- Click **Add**  and select **Section**. The **Section** will be added. You can add upto 10 Sections.
- By default, the name assigned is Section 1. Click **Edit**  to assign the desired name to the Section you added. Click **Save**  to save the assigned name or click **Cancel** .
- Click **Merge**  if you wish to merge one section with another.



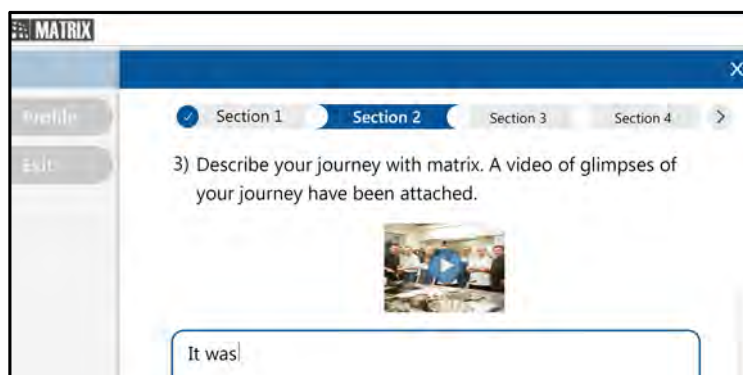
Merge will be visible only when you add multiple Sections.

Merge is not applicable for individual questions.

If questions in current Section and questions in the Section to be merged exceeds 10, then sections cannot be merged.

- Click **Discard**  if you wish to discard the complete Section along with its questions.


Sample of Sections as displayed in the VMS Portal.

A screenshot of the VMS Portal interface. It shows a window titled 'MATRIX' with a sidebar containing 'Profile' and 'Exit' buttons. The main area displays a list of sections: 'Section 1', 'Section 2' (selected), 'Section 3', and 'Section 4'. Below the sections, there is a question: '3) Describe your journey with matrix. A video of glimpses of your journey have been attached.' followed by a video player showing a group of people. At the bottom, there is a text input field with the text 'It was'.



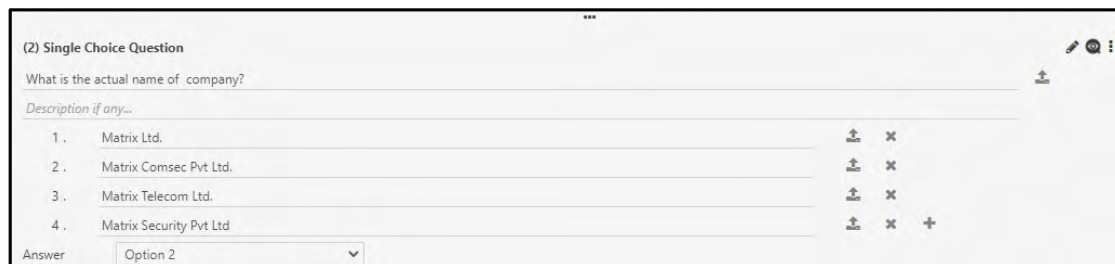
All of the samples are samples of Check-In Form as displayed in the VMS Portal. It will vary according to the configurations done by you in Station Location for Login, Check-In and Check-Out. For details refer to [“Form”](#) under Station Location.

Adding Questions within Sections

- Click **Add**  again and select the type of question you wish to add — Multi-Choice, Single-Choice, Text Answer Only, Fixed Content, Rating in this Section. You can add upto 10 questions in each Section.

Multi-Choice/Single-Choice

If you select Multi-Choice/Single-Choice, configure the following:

- Question:** Configure a **Question**. You can add the text and/or media —image, pdf or video.

The text can be a maximum of 100 characters.




You can either upload an image/pdf or video. Both cannot be uploaded.

To add media, click **Upload** . Refer to [“Uploading Image/PDF”](#) and [“Uploading Video”](#).

- Description:** Add a brief **Description** for the question if required. The text can be of maximum 100 characters.
- Options:** You can add text and/or media —image, pdf or video.

The text can be a maximum of 50 characters. You can add upto 10 options.

To add media, click **Upload** . Refer to [“Uploading Image/PDF”](#) and [“Uploading Video”](#).

To add another answer as an option, click **Add** .

To remove an existing option, click **Remove** ✕ .

To change the sequence of the options, click **Move** ↕ .

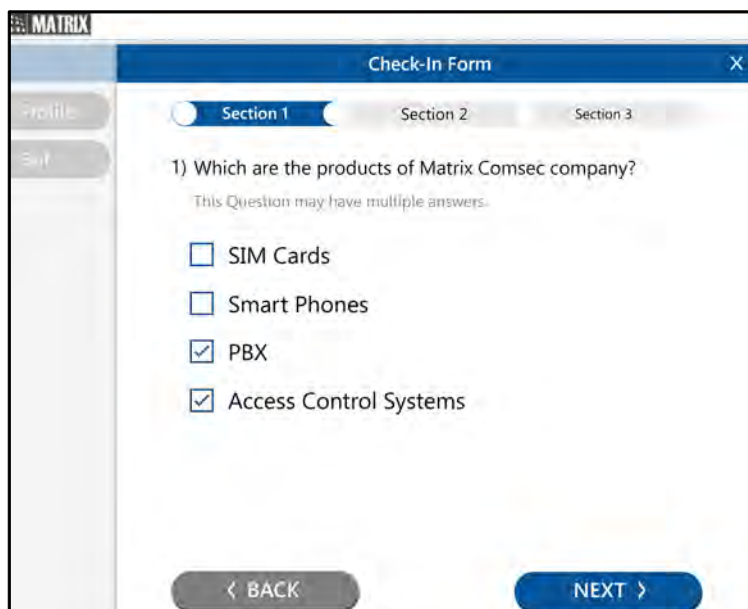
- **Answer:** For **Multi-Choice**, all the options added appear as answers in the drop-down list. You can select a single option or multiple options as the answer or to select all the options as the answer click **Check All**.

The ⓘ icon will display the correct option.

For **Single-choice**, all the options added appear as answers in the drop-down list. You can select only one option as the answer.

Click **Save** ✔ to save the configurations done or click **Cancel** ✕ to discard the changes.

Sample of Multi-Choice as displayed in the VMS Portal.

The screenshot shows a web application window titled 'MATRIX' with a 'Check-In Form' header. The form has three tabs: 'Section 1' (active), 'Section 2', and 'Section 3'. Under 'Section 1', there is a question: '1) Which are the products of Matrix Comsec company?'. Below the question, it says 'This Question may have multiple answers.' There are four options with checkboxes: 'SIM Cards' (unchecked), 'Smart Phones' (unchecked), 'PBX' (checked), and 'Access Control Systems' (checked). At the bottom of the form, there are two buttons: '< BACK' and 'NEXT >'. The left sidebar of the application shows 'Profile' and 'Self' buttons.

Sample of Single-Choice as displayed in the VMS Portal.

Text Answer Only

If you select this option the answers can be in text format only. Configure the following parameters:

- **Question:** Configure a **Question**. You can add the text and/or media —image, pdf or video.

The text can be a maximum of 100 characters.



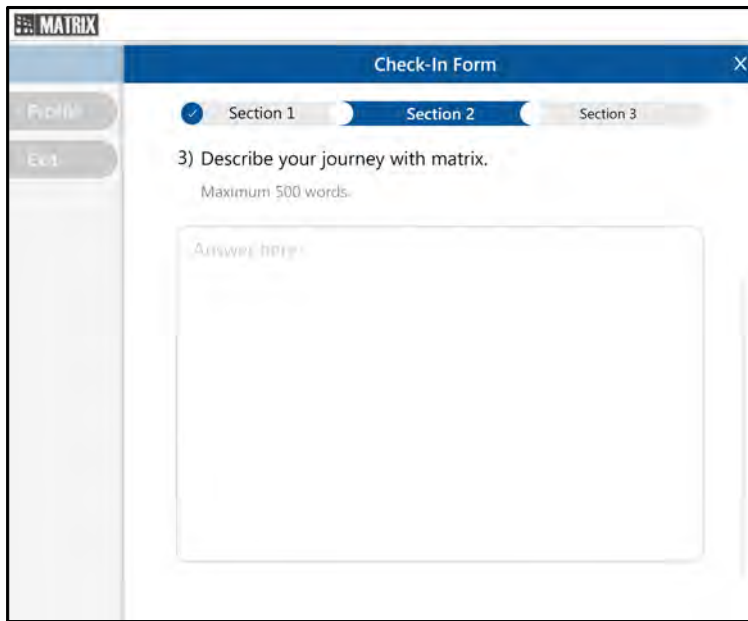
You can either upload an image/pdf or video. Both cannot be uploaded.

To add media, click **Upload** . Refer to [“Uploading Image/PDF”](#) and [“Uploading Video”](#).

- **Description:** Add a brief **Description** for the question if required. The text can be of maximum 100 characters.
- **Input Type:** Select the type of input — All Characters, Alpha Numeric or Numeric — you wish to allow.
Valid characters for Alpha Numeric: - A-Z a-z 0-9 +
Valid Range for Numeric - 0-9 +
- **Input Length:** This is the maximum input length to be allowed as the answer. Valid Range: 1 to 999.

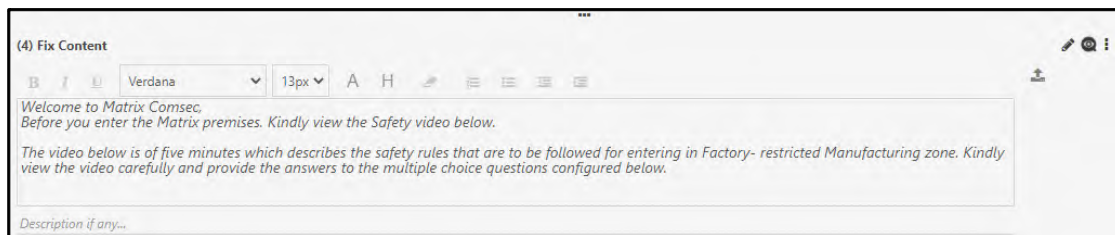
Click **Save**  to save the configurations done or click **Cancel**  to discard the changes.

Sample of Text Answer Only as displayed in the VMS Portal.

A screenshot of a web application titled "MATRIX" with a "Check-In Form" window. The form has three sections: "Section 1" (completed), "Section 2" (active), and "Section 3". Section 2 contains the question "3) Describe your journey with matrix." with a "Maximum 500 words" limit. Below the question is a large text input area with the placeholder text "Answer here".

Fix Content

If you select this option, you can display fixed content along with a description. Configure the following parameter:

A screenshot of a configuration window titled "(4) Fix Content". It features a rich text editor with a toolbar containing icons for Bold, Italic, Underline, Font Color, Background Color, Text Color, Text Size, and Text Style. The text area contains the following content: "Welcome to Matrix Comsec. Before you enter the Matrix premises. Kindly view the Safety video below. The video below is of five minutes which describes the safety rules that are to be followed for entering in Factory- restricted Manufacturing zone. Kindly view the video carefully and provide the answers to the multiple choice questions configured below." Below the text area is a label "Description if any...".

- **Fix Content:** You can add the text and/or media —image, pdf or video for the question.

You can add text as well as format it as per your requirement.

You can add the text using different font, font- size, font color, highlight color and remove formatting. You can customize your content according to different font layouts like Bold, Italic, Underlined, Ordered List, Unordered List, Outdent and Indent.

All characters are allowed.



You can either upload an image/pdf or video. Both cannot be uploaded.

To add media, click **Upload** . Refer to ["Uploading Image/PDF"](#) and ["Uploading Video"](#).

- **Description:** Add a brief **Description** for the question if required. The text can be a maximum of 100 characters.

Click **Save** ✓ to save the configurations done or click **Cancel** ✕ to discard the changes.

Sample of Fix Content as displayed in the VMS Portal



Rating

If you select this option, after the question and description, five Stars icons will be displayed to the visitor to provide the rating. Below each Star the Labels you configured will be displayed. Configure the parameters as per your requirement:

A screenshot of a configuration form for a 5-star rating system. The form has a title '(5) Rating' and a description 'Rate your journey with our company.' Below the description is a text input field labeled 'Description if any...'. Below this are five rows, each with a star icon and a label input field. The labels are: 1. Worst, 2. Bad, 3. Good, 4. Label if any..., and 5. Label if any....

- **Question:** Configure a **Question**. You can add the text and/or media —image, pdf or video.

The text can be a maximum of 100 characters.




You can either upload an image/pdf or video. Both cannot be uploaded.



To add media, click **Upload** . Refer to “[Uploading Image/PDF](#)” and “[Uploading Video](#)”.

- **Description:** Add a brief **Description** for the question if required. The text can be of maximum 100 characters.
- **Labels:** You can add upto 5 labels. Each label can be a maximum of 15 characters. This will be visible below each Star icon.

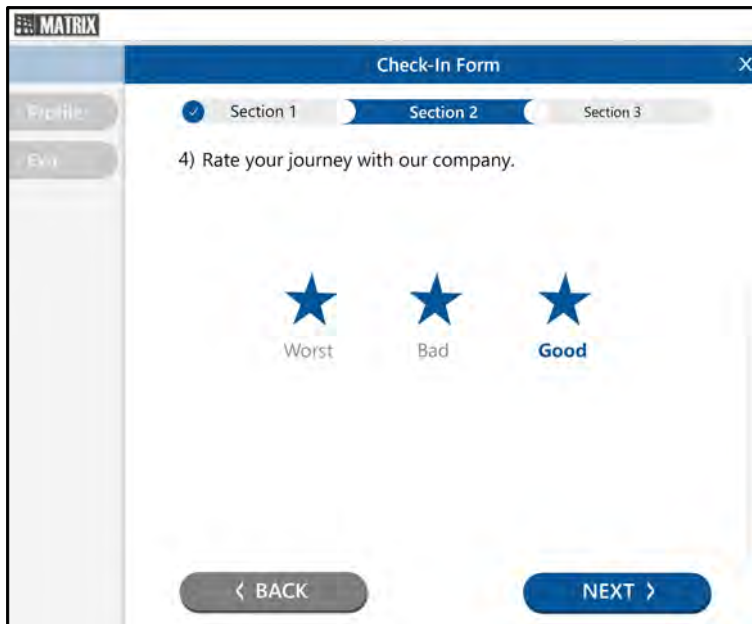


The five configurable labels are not mandatory.

- To change the sequence of labels, click **Move** .





Click **Save**  to save the configurations done or click **Cancel**  to discard the changes.

Sample of Rating as displayed in the VMS Portal.



Common Functionality for all types of Questions


After you have saved the Question and Answer along with the Options, you can:


- **Move:** You can re-arrange the sequence of the questions within a particular Section or across a Section, if required. To do so, click **Move**  or drag and drop the questions as per your the required sequence. The numbering will be changed automatically. Sections cannot be moved.
- Click **Edit** , if you wish to edit the details.
- Click **Hide** , if you wish to hide a question. This will not be visible to the visitor. Once you select **Hide** the available option will toggle to **Un-hide**.
- Click **Additional Options**  to view other options:
 - **Set as Mandatory:** Select this option, if you wish to make this question compulsory. Once you select **Set as Mandatory** the available option will toggle to **Set as Non-Mandatory**.
 - **Duplicate:** Select this option, if you wish to create a copy of the question along with the options.

- **Discard:** Select this option, if you wish to delete the question along with the options.


Top Panel Functionality


After the Forms have been created, you can perform the following:

Click **Add** , to add a new Form.

Click the desired form from the list of forms in the right pane. Click **Edit** , if you wish to make modifications in the existing form.

After the form is edited and the response is submitted by the visitor, then if you edit the form, it will be considered as edit count 1. Such edits can be done upto 99 times.

Click the desired form from the list of forms in the right pane. Click **Delete** , if you wish to delete the form.

Click the desired form from the list of forms in the right pane. Click **Duplicate** , if you wish to replicate the form.

Importing Data

The COSEC application has an inbuilt utility for enabling users to import data from excel files with predefined format. This would thus save the end user a lot of time and effort in having to make individual data entries at the application level.



*In the event of the **COSEC Application Basic Platform** license as well as the **Access Control add on module**, only the User data with some of the fields can be imported.*

To import data from a file follow the steps given below:

Select **Admin module > System Utilities > Import Data** and the following screen appears.

Import Data

←

Import Data For: User

File Format: XLS

Import File: Choose File No file chosen

Upload Import Data

Select Devices To Assign To User


Configure the following parameters:

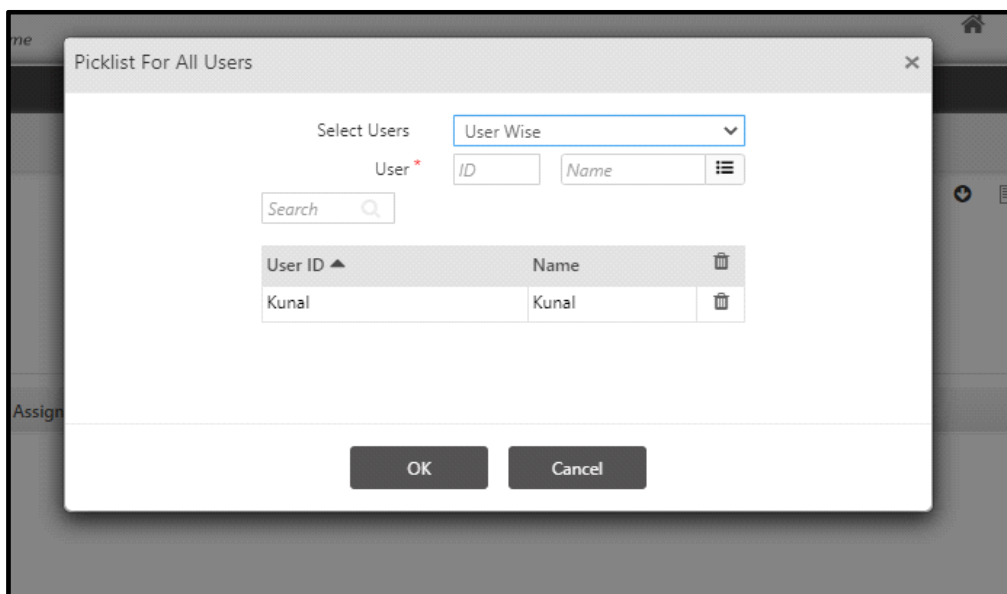
- **Import Data For** - Select the option from the dropdown list for which the data is to be imported. You can download sample import file by clicking on **Download Sample Import file** button. The downloaded import sheet displays the fields required for importing specific data.

	A	B	C	D	E
1	ID	CODE	NAME	EMAIL	DESCRIPTION
2	2323	A4	Anup		
3	6897	S5	Mahesh		
4	3553	F2	Mithesh		
5	3333	N5	Jithesh		

You can even refer to the Import Data Document Guidelines in the downloaded import sheet.

	Import Data Document Guidelines				
1					
2	General Guidelines				
3					
4	1 The sheet name should not be changed or the sheet will not be identified for import.				
5	2 The column names and the column position also should not be changed.				
6	3 For all date columns, the cell format should be "text" and date format should be same as configured in Web Server.				
7					
8					
9					
10	USER Import Fields				
11	Basic License	ACS License	T&A License	ACS + T&A License	
12	Organization	All fields	NA	All fields	All fields
13	Branch	All fields	NA	All fields	All fields
14	Department	All fields	NA	All fields	All fields
15	Section	All fields	NA	All fields	All fields
16	Category	All fields	NA	All fields	All fields
17	Grade	All fields	NA	All fields	All fields
18	Designation	All fields	NA	All fields	All fields
19	Custom Group1	All fields	All fields	All fields	All fields
20	Custom Group2	All fields	All fields	All fields	All fields
21	Custom Group3	All fields	All fields	All fields	All fields
	User	UserId UserName Full Name ShortName Gender BloodGroup Father/Spouse Name BirthDate Joining Date Leaving Date	Basic ScheduleGroupID StartShift	Basic ScheduleGroupID StartShift LeaveGroup WeekOffGroupID ReportingGroupID ApprovalPolicyID	Basic + ACS + T&A

If **Import Data For** is selected as User/Worker then you can download a detailed data sheet, to do so click on **Download Detailed Data Sheet**  button. On clicking this button, a pop-up will be displayed as shown below:



Select Users: Select the desired option — User Wise, Group Wise or All. If you select User Wise or Group Wise the select the desired users/groups from the picklist.

Click **OK** button to download the Data Sheet or click on **Cancel** button to abort the process.

The Detailed Data Sheet will be as per the selected option.

If the **Import Data For** option is selected as Visitor and Visit, then configure **Import Data Of**.

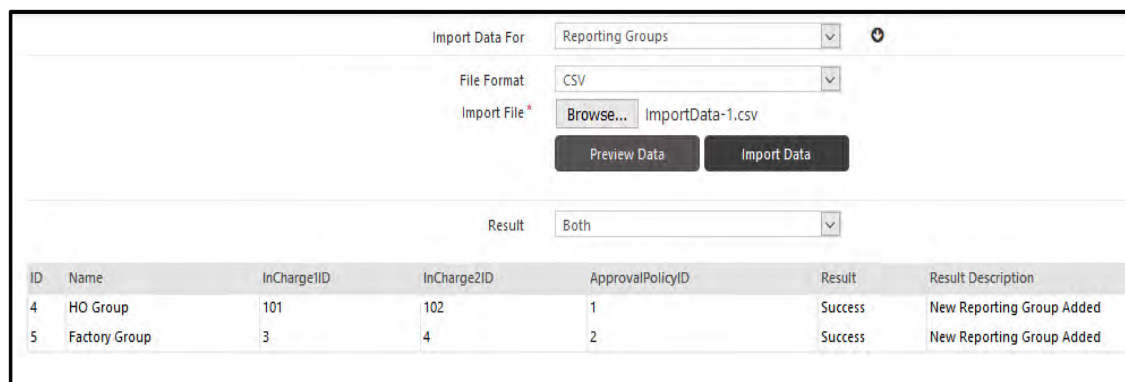
- **Import Data Of** - To import data of a Visitor and/or a Visit, select the desired option — Visitor Only, Visit Only or Both.
- **File Format** - Select the file format of the specific file from the dropdown list. The options available are XLS or CSV.
- **Import File** - Browse the path of the file from which the data is to be imported.

Click **Upload** button. The file will be saved and you can preview the data.

The Preview Data enables the administrator to view the uploaded data to confirm if it is in order before giving the import command. Click on **Preview Data** button. The preview data of reporting In-charge is shown as below.

ID	Name	InCharge1ID	InCharge2ID	ApprovalPolicyID
4	HO Group	101	102	1
5	Factory Group	3	4	2

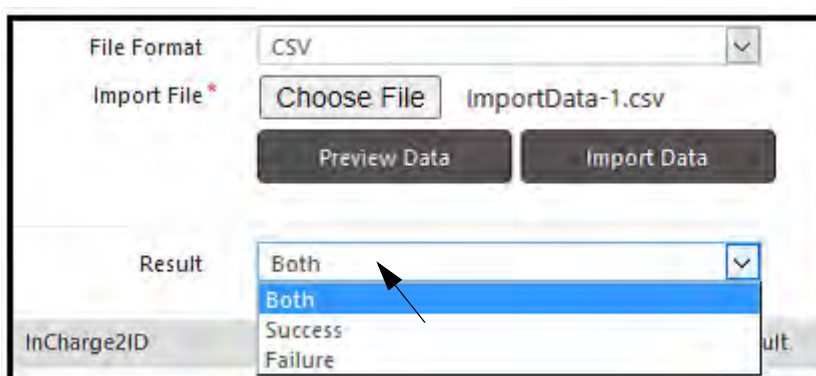
Now click on **Import Data** to start importing the uploaded data. The result of import is shown as Success or Failure along with result description as shown.



The screenshot shows the 'Import Data' interface. At the top, there's a dropdown for 'Import Data For' set to 'Reporting Groups'. Below it, 'File Format' is set to 'CSV'. The 'Import File' section shows a 'Browse...' button and the filename 'ImportData-1.csv'. There are 'Preview Data' and 'Import Data' buttons. Below this, a 'Result' dropdown is set to 'Both'. At the bottom, a table displays the import results:

ID	Name	InCharge1ID	InCharge2ID	ApprovalPolicyID	Result	Result Description
4	HO Group	101	102	1	Success	New Reporting Group Added
5	Factory Group	3	4	2	Success	New Reporting Group Added

You can also filter import result records on the basis of their Success, Failure or Both using the **Result** drop-down options.



This screenshot is a close-up of the 'Result' dropdown menu. The menu is open, showing three options: 'Both', 'Success', and 'Failure'. The 'Both' option is currently selected and highlighted in blue. An arrow points to the 'Both' option. The background shows parts of the 'File Format' (CSV) and 'Import File' (Choose File, ImportData-1.csv) sections.

Once the data is imported successfully, data will be added or updated in COSEC Web.



Administrator needs to ensure that the ASP.NET user has full rights on the folder containing the Excel or .csv file for the import data operation.

Exporting Data

This functionality enables the user to export data to external applications based on the pre-configured data templates. The user has the flexibility to select the output formats and Type of Users. User can select Output formats from one of the following:

- Excel
- Text
- CSV
- XML

To access this functionality, go to **Admin Module > System Utilities > Export Data** and the following screen appears.

Name	Value
Name	
UserID	
UserName	
ProcessDate	
Punch1	
Punch2	

1 - 5 of 10 records

« < 1 2 > »

Export Parameters

Date * From Date To Date

File Format Excel Files

File Name *

Select Users User Wise

User * ID Name

Generate Export For All Users

Export

The page displays two tabs namely:

- “Export”
- “Templates”

Export

To export data following are the configurations:

The 'Export Data' window displays the following configuration options:

- Template Type:** Custom
- Template:** API_Template_Daily
- Export Fields List:** A list of fields including API_Template_Daily, API_Template_Monthly, API_Template_ATDEvents, API_Template_ACSEvents, Template_Daily, Template_Monthly, Template_ATDEvents, and Template_ACSEvents. The first item is selected.
- Export Parameters:** A collapsible panel containing:
 - Date:** From Date and To Date (with calendar icons).
 - File Format:** Excel Files
 - File Name:** (empty text field)
 - Select Users:** User Wise
 - User:** ID and Name (with a list icon).
 - Export:** A button to execute the export.

Template Type: Select the type of template to be used for exporting data from the dropdown list. There are two types of templates: Custom Templates and System Defined.

Before exporting the data based on Custom Template, it is required that the templates are pre-configured. [See "Templates" on page 302.](#)

Template: Based on template type, select the templates from the dropdown list for data export. For Custom Template type, select the template which is configured from section: [See "Templates" on page 302.](#)

Export Fields List: This displays the fields that are selected and added to the template from ["Export Field Configuration"](#)

Export Parameters

Click on Export Parameters collapsible panel and configure the following:

The 'Export Parameters' panel displays the following configuration options:

- Header:** 300 chars
- Export Date-Range:** ☐
- Export Generation Date-Time:** ☐
- Date:** From Date and To Date (with calendar icons).
- File Format:** Excel Files
- File Name:** (empty text field)
- Select Users:** User Wise
- User:** ID and Name (with a list icon).
- Generate Export For:** All Users
- Export:** A button to execute the export.

Header: Enter header details which is to be displayed in Header of Export Sheet. It is a Custom header. You can enter alphanumeric characters in header.

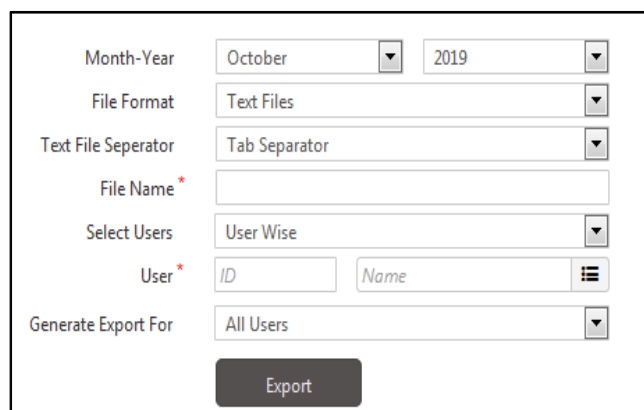
Export Date-Range: It allows to decide whether configured From Date & To Date is to be displayed in Export Sheet or not. This check-box is available when the selected Template is of Daily basis. If this check-box is checked, then the configured From Date & To Date will be displayed in Export sheet.

Export Generation Date-Time: This check-box is used for displaying details regarding when (at which date & time) the sheet is exported. If this check-box is checked, then the Date -Time of when the sheet is exported will be displayed in Export sheet.

Date/ Month: Select the date range or the month for the data that is to be exported based on the template selected. The Date and Month-Year field appears as per selection of template.

File Format: Select the format of the file to be exported from the options of **Excel**, **Text**, **CSV** and **XML** file formats.

Text File Separator: In the event of the **Text files** option being selected, specify the separator type. Based on the site requirements, select the **Text File Separator** as shown below:

A screenshot of a web-based export configuration form. The form contains several fields: 'Month-Year' with dropdowns for 'October' and '2019'; 'File Format' with a dropdown for 'Text Files'; 'Text File Separator' with a dropdown for 'Tab Separator'; 'File Name' with a text input field; 'Select Users' with a dropdown for 'User Wise'; 'User' with two input fields labeled 'ID' and 'Name'; and 'Generate Export For' with a dropdown for 'All Users'. An 'Export' button is located at the bottom of the form.

Text File Separator field will be available only when **File Format** is selected as **Text Files** format.

File Name: Specify a filename by which the exported data is to be saved.

Event Selection: Select the desired options — All, Allowed Events or Denied Events.

- Select **Both**, if you want all Allowed and Denied events to be exported.
- Select **Allowed Events**, if you want only Allowed events to be exported.
- Select **Denied Events**, if you want only Denied events to be exported.



Event Selection is applicable when Template selected is API_Template_ATDEvents or API_Template_ACSEvents or Template_ATDEvents or Template_ACSEvents.

Select Users: Select the User as **User Wise**, **Group Wise** or **All**. Then select the users accordingly whose data is to be exported.

Generate Export for: Select the users as **All**, **Active** or **Inactive** for which data is to be exported.

Click on the **Export** button. Open or Save the export file by specifying the location. The below shown file is in Excel format.

	A	B	C	D	E	F	M	N
1	UserID	UserName	PYear	PMonth	PRDays	ABDays		
2	1782	Nidhi	2017	4	1.5	3.5		
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								

Templates

The COSEC system enables the administrator to define templates for export of data in a customizable format. Select the **Templates** tab on the **Export Data** home page and the following page appears.

Seq. No.	Field Type	Field Name	Up/Down		
1	Database Field	UserID	▼		
2	Database Field	UserName	▲▼		
3	Database Field	ProcessDate	▲▼		
4	Database Field	Punch1	▲▼		
5	Database Field	Punch2	▲▼		
6	Database Field	WorkingShift	▲▼		
7	Database Field	LateIn	▲▼		
8	Database Field	EarlyOut	▲▼		
9	Database Field	Overtime	▲▼		
10	Database Field	WorkTime	▲		

To add a new template, click the **New**  button and the following screen appears.

Template: Enter a user-friendly name for the new template to be defined (e.g. “*Template_Canteen*”, “*Template_DailyEvents*” etc.).

Database View: Select a corresponding Database View from the dropdown list.

Click the **Add Field** button. The following pop-up window: **Export Field Configuration** appears for the configuration of Export fields.

Export Field Configuration

Field Type: Select the type of field to be exported from the below options and then click **Save** button to add the fields in the template:

- **Database Field-** If any of the database field is to be modified.
- **Static Field** - To keep a field or column static (fixed).
- **Custom Field** - To create user defined field. Eg: User ID+UserName to be merged as a single field.

Field Type as Database Field

Display Name: The name to be displayed as the header of the column is display name.

Fields: Select the fields to be displayed in the Export sheet. The fields in the dropdown depends upon the selection of Database View type.



When the "Leave Type" field is selected; then the count of leaves based on the leave code will be displayed in the exported file. Suppose SL and PL are both Paid leaves; then count of SL and PL will be shown separately. [See "Exporting Leave Details" on page 308.](#)

Field Condition: To change the field condition i.e. to replace the existing value of a field with new value, you must enable this.

Field Value: Specify the value of the field to be edited.

Replace Value: Specify the new value to replace the existing field value in database.

Export Field Configuration

Field Type: Database Field
 Display Name: Canteen Name

Fields: USERID
 Field Condition: ☒
 Field Value:
 Replace Value:

Add

Search

Field Value	Replace Value	
1220	1220001	

Save **Cancel**

Eg: The User ID having Field Value 1220 is replaced by value 1220001. The exported sheet will be shown as below. The display name will be shown as column header.

A	B	C	D
Research Employee	Employee ID	Edited ID	Joining
SHEETAL RAVAL	1220	1220001	2013/06/17

Field Type as Static Field

User can select Field Type as Static field when he wants to display the same (static) field against all the other variable fields such as Employee Name.

Export Field Configuration

Field Type: Static Field
 Display Name: Company Name

Field Name: Company Name
 Field Value: Matrix
 Data Type: Alpha-Numeric
 Data Length: 20

Save **Cancel**

Display Name: The name to be displayed as the header of the column is display name. Eg: “Company Name” is set as Display name.

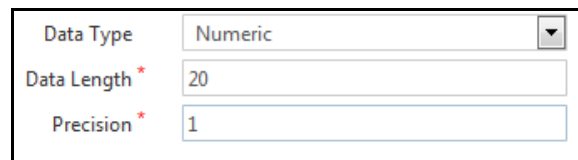
Field Name: Specify any field name.

Field Value: This is the value of the field which will remain static or same for all records. Eg: “Matrix” is the company name which remains static for all the users of the company.

Data Type: Select the data type as Alpha-numeric, Numeric or Date-time according to the field value.

Data Length: Specify the length of data which is to be used to map with the data length in destination tables of COSEC Integrate used for exporting data in other database.

Precision: If Data Type is selected as **Numeric**, then you will have to specify Precision also. For Eg: If the user wants to display the Working hours of the employee as static Field value, then user can select Data Type as Numeric and will have to define Precision of decimal as the value of Working hours may result in decimal.

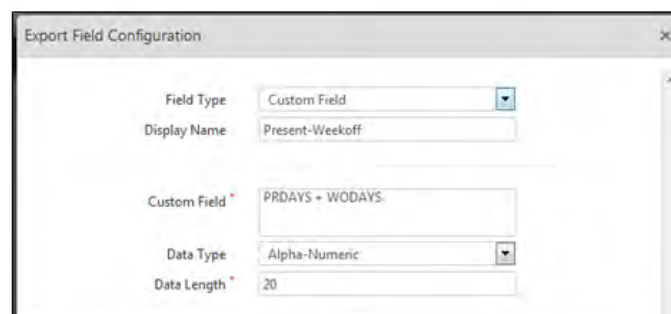


A screenshot of a configuration form. It has three fields: 'Data Type' with a dropdown menu showing 'Numeric', 'Data Length *' with a text input containing '20', and 'Precision *' with a text input containing '1'.

Eg: The Static Field Value “Matrix” with Display Name “Company Name” is shown below in the exported excel file:

A	B
Company Name	Employee Name
MATRIX	JAY K DOSHI
MATRIX	MANOJ DETROJA
MATRIX	HARSHIT PATEL
MATRIX	ANIL TAILOR
MATRIX	VJAYKUMAR
MATRIX	KAUSHAL KADAKIA
MATRIX	VISHAL DHANANI
MATRIX	MANTHAN PATEL
MATRIX	ANIL MODI
MATRIX	SATISH RAJE
MATRIX	SHUBHANGINI
MATRIX	PARTH SUTARIYA
MATRIX	SATISH JHA
MATRIX	TANMAY SHAH

Field Type as Custom Field



A screenshot of a dialog box titled 'Export Field Configuration'. It contains several fields: 'Field Type' with a dropdown menu showing 'Custom Field', 'Display Name' with a text input containing 'Present-Weekoff', 'Custom Field *' with a text input containing 'PRDAYS + WODAYS', 'Data Type' with a dropdown menu showing 'Alpha-Numeric', and 'Data Length *' with a text input containing '20'.

- **Custom Field:** Provide custom field to display two or more fields in one column or to concatenate the fields and display in single column. The Allowed Length for the Custom Field control for Oracle is 2000; and for SQL is 4000.



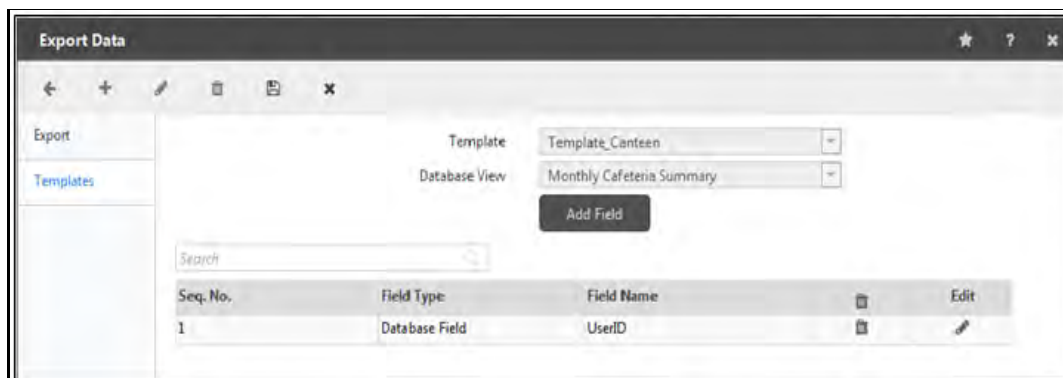
The custom fields specified here are those included in the Database View selected for the template.

For other fields See “Field Type as Static Field” on page 305.

Eg: Present days and Weekoff days are added and shown in single column with Display name “Present-Weekoff”. Also Birthdate and Joining date are shown together.

A	B	C	D	E
Company Name	Employee Name	Company	Present-Weekoff	Birthdate-Joindate
MATRIX	SHEETAL RAVAL	Matrix Comsec Pvt.	27.5	27/11/198717/06/2013
MATRIX	SHRUTI PATKI	Matrix Comsec Pvt.	29.0	08/07/199010/06/2014
MATRIX	AKHILESH DUBEY	Matrix Comsec Pvt.	23.0	14/08/199018/05/2015

- On clicking **Save** button in the Export Field Configuration pop-up window, the fields get displayed in the grid on the main Export page as shown in the screen below:



- To edit a field click the corresponding icon.
- Click **Save** to save the export template configuration. This new custom template will now be available for selection in the **Export** section.
- The following screen illustrates a sample Excel file that was exported using the new custom template:

	A	B	C	D
1	Canteen	Canteen door n	Menu location	User discount I
2	27	Canteen Factory	3	1
3	27	Canteen Factory	3	1
4	27	Canteen Factory	3	1
5	27	Canteen Factory	3	1
6	27	Canteen Factory	3	1
7	27	Canteen Factory	3	1
8	27	Canteen Factory	3	1
9	27	Canteen Factory	3	2
10	27	Canteen Factory	3	2
11	16	Canteen HO	1	1
12	27	Canteen Factory	3	1
13	27	Canteen Factory	3	1
14	27	Canteen Factory	3	1
15	16	Canteen HO	1	1
16	27	Canteen Factory	3	1
17	27	Canteen Factory	3	1
18	27	Canteen Factory	3	1
19	27	Canteen Factory	3	2
20	27	Canteen Factory	3	1

Exporting Leave Details

Suppose a custom template of Database view Monthly Attendance Summary is created. The UserID, UserName, PMonth, PYear, LeaveDays-SL and LeaveDays-PL are selected from Database field.

For example: LeaveDays-SL field is added as shown below.

Export Field Configuration

Field Type: Database Field

Display Name: Sick Leave

Fields: LeaveDays-SL

Field Condition: ☒

Field Value: SL

Replace Value: Availed SL

Add

Field Value: SL

Replace Value: Availed SL

Save Cancel

Export Field Configuration

Field Type: Database Field

Display Name: Sick Leave

Fields: LeaveDays-SL

Field Condition: ☒

Field Value: SL

Replace Value: Availed SL

Add

Field Value: SL

Replace Value: Availed SL

Save Cancel

Now similarly other fields are added in the template.

Seq. No.	Field Type	Field Name	Up/Down		
1	Database Field	UserID	▼		
2	Database Field	UserName	▲▼		
3	Database Field	PMonth	▲▼		
4	Database Field	PYear	▲▼		
5	Database Field	LeaveDays-SL	▲▼		
6	Database Field	LeaveDays-PL	▲		

Now the fields in the template can be exported by configuring Export details.

Export Parameters

Month-Year: September 2018

File Format: Excel Files

File Name: UserLeaveDetails

Select Users: All

Export

The Exported file shows the count of Sick Leave and Privilege Leave (both PL type of leave) separately.

	A	B	C	D	E	F	G	H	I
1	User ID	User Name	Punch Month	Punch Year	Sick Leave	Privilege Leave			
2	1583	Shilpa	9	2018	0.0	3.0			
3	2	Chirag	9	2018	0.5	1.0			
4									
5									
6									

Similarly count of different leaves of same leave type can be exported through COSEC Integrate Utility also.

Third Party Export

This functionality enables the COSEC system to export attendance data in predefined formats which can be recognized and imported by a third party application. COSEC can integrate with *three* third party applications for data export - **Tally**, **Relyon** - **Saral PayPack** and **IDS**.

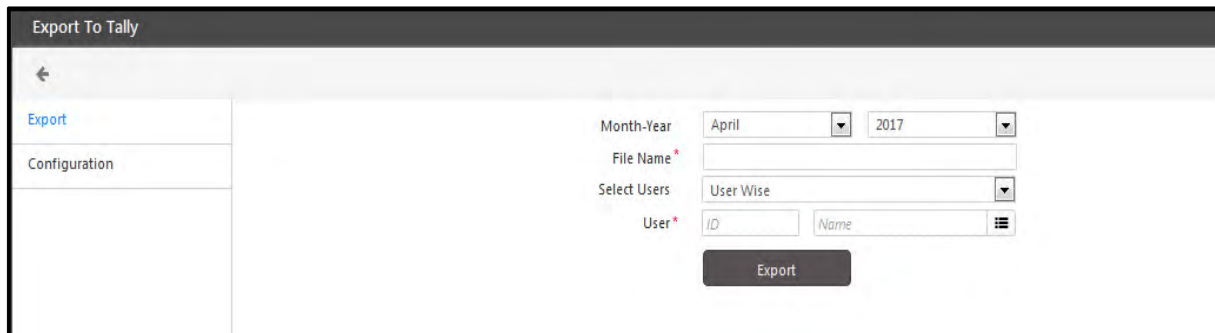
Read the following sections to configure all third party export options using the COSEC Web Application:

- [“Export to Tally”](#)
- [“Export To Relyon”](#)
- [“Export to IDS”](#)

Export to Tally

This functionality enables the COSEC system to export attendance data in an XML format which can be recognized and imported by the Tally application. Importing attendance data from the COSEC system into the Tally payroll module would allow user to directly generate attendance vouchers which then can be used to maintain Employee accounts. Tally having its own data format does not allow direct import of attendance data from COSEC, hence has to be exported as well imported in an intermediate XML format.

In order to configure the parameters for exporting data, go to **Admin > System Utilities > Third Party Export > Export to Tally** and the following page appears.



Before exporting, Configuration has to be done. See [“Export To Tally Configuration” on page 312](#).

Month-Year: Select the Month & Year to specify the time period for which the data is to be exported.

File Name: Specify a filename for the XML file that is to be created.

Select Users: Select users/groups as per the option selected from the dropdown list. The options are:

- User Wise
- Group Wise (*Available only with the Time & Attendance add on module*)
- All

Click the **Export** button. The system prompts the user to browse to the folder path where the specified file will be saved.

Guide to Tally

The following points are needed to be taken care of while configuring the Tally application.

Create all the employees whose data is to be imported from the COSEC application.



User needs to take care and configure one of the following to ensure proper mapping of data:

- Enable aliases for employee and enter the User I.D. (as in COSEC application) in the alias field.
- Enter User I.D. (as in COSEC application) in the Cost Centre field of Account Info.

The Tally Tags can be created using the following options:

Gateway of Tally > Masters > Payroll Info > Units (Work): Create the necessary units required for different attendance types. For ex: Hrs, Mins, etc.

Gateway of Tally > Masters > Payroll Info > Attendance/Production Types: Create the required Attendance Types, for ex: Present, Absent, etc. The user needs to take care to use these Attendance Types while creating Tally Tags in COSEC application with appropriate Attendance Type.

The Payroll Info parameters as defined here should match the parameters as specified in the **Export to Tally** option of the COSEC web application.

Refer the Tally user manual for more details. The import process can be initiated from the Tally application by going to **Gateway of Tally > Utility > Import of Data > Vouchers**.

Export To Tally Configuration

On the **Export To Tally** page, select the **Configuration** tab.

To configure export to tally click **New** button and the following screen appears.

The screenshot shows the 'Export To Tally' application window. On the left is a sidebar with 'Export' and 'Configuration' tabs. The 'Configuration' tab is selected. The main area contains a form with the following fields:

- ID:** A text input field.
- Tally Voucher Name:** A text input field with the value 'Attendance'.
- Tag Type:** A dropdown menu with 'Production' selected.
- Tally Tag:** A text input field with the value 'month'.
- COSEC Fields:** A text input field with the value 'Overtime' and a 'Select' button to its right.
- Production Unit Name:** A text input field with the value 'Waghodiya'.

Below the form is a search bar and a table. The table has the following columns: ID, Voucher Name, Tally Tags, COSEC Fields, and Tag Type. The table is currently empty, displaying 'No Data'.

Enter the following parameters:

- **ID:** The ID will be auto generated.
- **Tally Voucher Name:** Enter a voucher name for tally.
- **Tag Type:** Select the tag type from the options of With Pay, Without Pay or Production.
- **Tally Tag:** Enter tally tag.
- **COSEC Fields:** Select the COSEC fields to be exported by clicking on **Select** button.
- **Production Unit Name:** Specify the name of production unit for production tag type.
- Click **Save** button and the created voucher gets displayed in the grid as shown in the screen below.

Export To Tally

✓ Saved Successfully

Export

Configuration

ID

1

Tally Voucher Name *

Attendance

Tag Type

Production

Tally Tag *

month

COSEC Fields *

Overtime

Production Unit Name *

Waghodiya

Select

Search

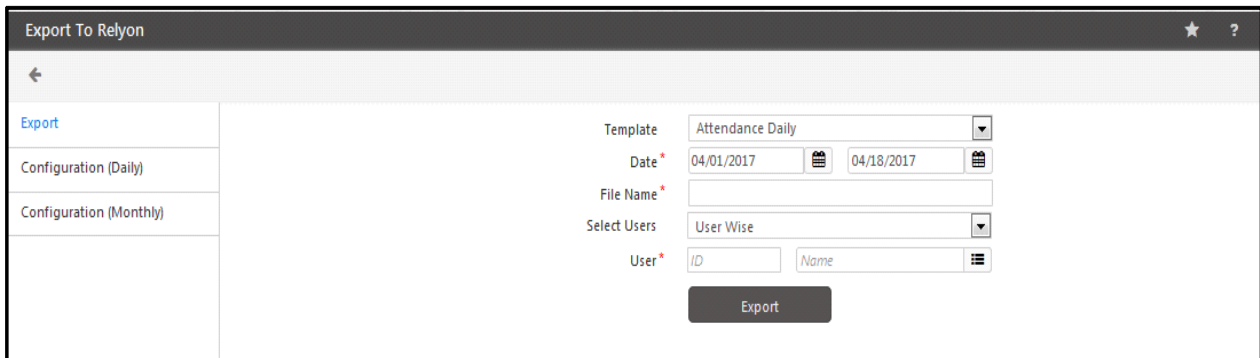
ID ▲	Voucher Name	Tally Tags	COSEC Fields	Tag Type
1	Attendance	month	Overtime	Production

Export To Relyon

This functionality enables the COSEC system to export attendance data in Excel format which can be recognized and imported by the Relyon's application. The Relyon application needs the following two kinds of attendance data outputs from the COSEC application:

- Daily Attendance
- Monthly Attendance

In order to configure the parameters for exporting data, go to **Admin > System Utilities > Third Party Export > Export to Relyon** option and the following page appears.

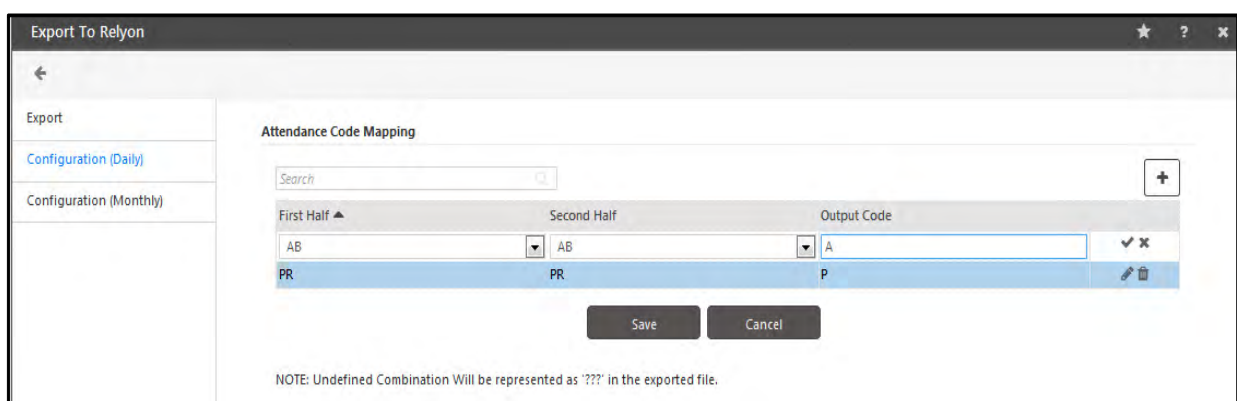


Before exporting, Configuration has to be done. See [“Daily Attendance Configuration”](#) and [“Monthly Attendance Configuration”](#)

Daily Attendance Configuration

Select the **Configuration (Daily)** tab to configure the export parameters for the daily attendance data.

Click **Add** button to add a new output code for various combinations of attendance status codes.



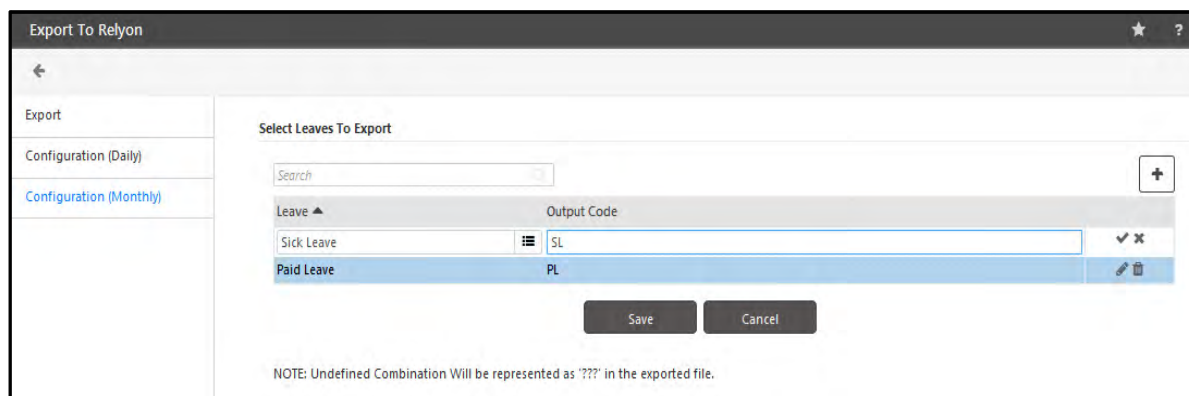
- Select the **First half** and **Second half** codes from the dropdown list and specify the **Output Code** for the combination as shown in the above figure.
- Click OK to save the code mapping.

- Define all the applicable combinations as per the site requirements and click **Save** button once done.

Monthly Attendance Configuration

Click on the **Configuration (Monthly)** tab to configure the export parameters for the monthly attendance data.

The user can now map the Leave name to the Column name of the exported Excel file. Click **Add** button to add a new leave to export and the following screen appears.



Export To Relyon

Export

Configuration (Daily)

Configuration (Monthly)

Select Leaves To Export

Search

Leave	Output Code
Sick Leave	SL
Paid Leave	PL

Save Cancel

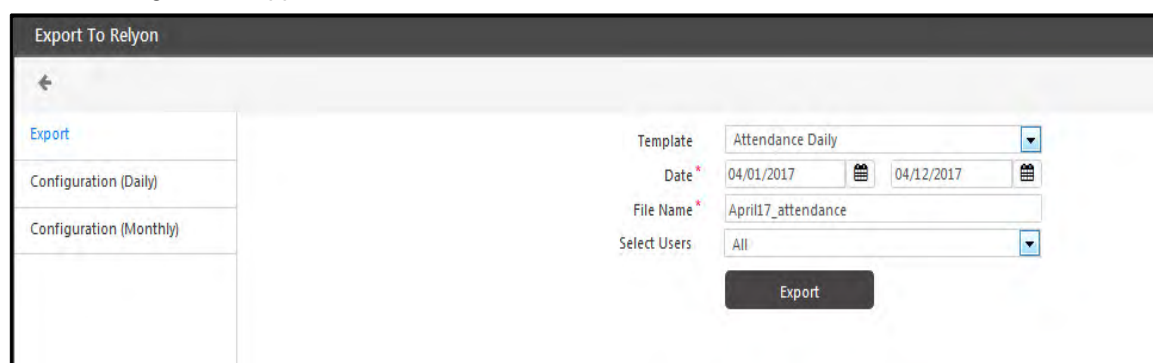
NOTE: Undefined Combination Will be represented as '???' in the exported file.

- Select the **Leave** from the picklist and specify the **Output Code** for the leave.
- Click OK to save the code mapping of leaves.
- Define all the applicable leaves to be exported and click **Save button** once done.

Export

Once the daily and monthly configurations for the export are done, data can be exported to Relyon.

To export data to relyon, go to **Admin > System Utilities > Third Party Export > Export to Relyon > Export** tab and the following screen appears.



Export To Relyon

Export

Configuration (Daily)

Configuration (Monthly)

Template: Attendance Daily

Date: 04/01/2017 to 04/12/2017

File Name: April17_attendance

Select Users: All

Export

- **Template:** Select an export template as Attendance Daily or Attendance Monthly.
- **Date:** Select the date range in the given fields, for which the data is to be exported.

- **File Name:** Specify a filename for the exported data file.
- **Select Users:** Select single or multiple users whose data is to be exported based on filter options of:
 - User Wise
 - Group Wise
 - All
- Click the **Export** button. The system will prompt the user to open or save the file. The exported file is shown as below.


A	B	C	D	E
EMPID	REFNO	ATTENDANCEDATE	OUTPUTCODE	OT(hh.mm)
07	7	01-Apr-17	A	0.0
101	101	01-Apr-17	A	0.0
1567	1567	01-Apr-17	P	0.0
1782	1782	01-Apr-17	A	0.0
2	2	01-Apr-17	A	0.0
DVD	1786	01-Apr-17	A	0.0
07	7	02-Apr-17	????	0.0
101	101	02-Apr-17	????	0.0
1567	1567	02-Apr-17	????	0.0
1782	1782	02-Apr-17	????	0.0
2	2	02-Apr-17	????	0.0
DVD	1786	02-Apr-17	????	0.0
07	7	03-Apr-17	A	0.0
101	101	03-Apr-17	A	0.0
1567	1567	03-Apr-17	P	0.0
1782	1782	03-Apr-17	A	0.0
2	2	03-Apr-17	A	0.0
DVD	1786	03-Apr-17	A	0.0
07	7	04-Apr-17	A	0.0
101	101	04-Apr-17	A	0.0
1567	1567	04-Apr-17	????	0.0
1782	1782	04-Apr-17	P	0.0
2	2	04-Apr-17	A	0.0
DVD	1786	04-Apr-17	A	0.0
07	7	05-Apr-17	A	0.0
101	101	05-Apr-17	A	0.0
1567	1567	05-Apr-17	P	0.0
1782	1782	05-Apr-17	????	0.0
2	2	05-Apr-17	A	0.0

Export to IDS

This functionality enables the COSEC system to export attendance data in a flat line sequential file format which can be recognized and imported by the IDS application.

In order to configure the parameters for exporting data, go to **Admin > System Utilities > Third Party Export > Export to IDS > Configuration** and the following page appears.

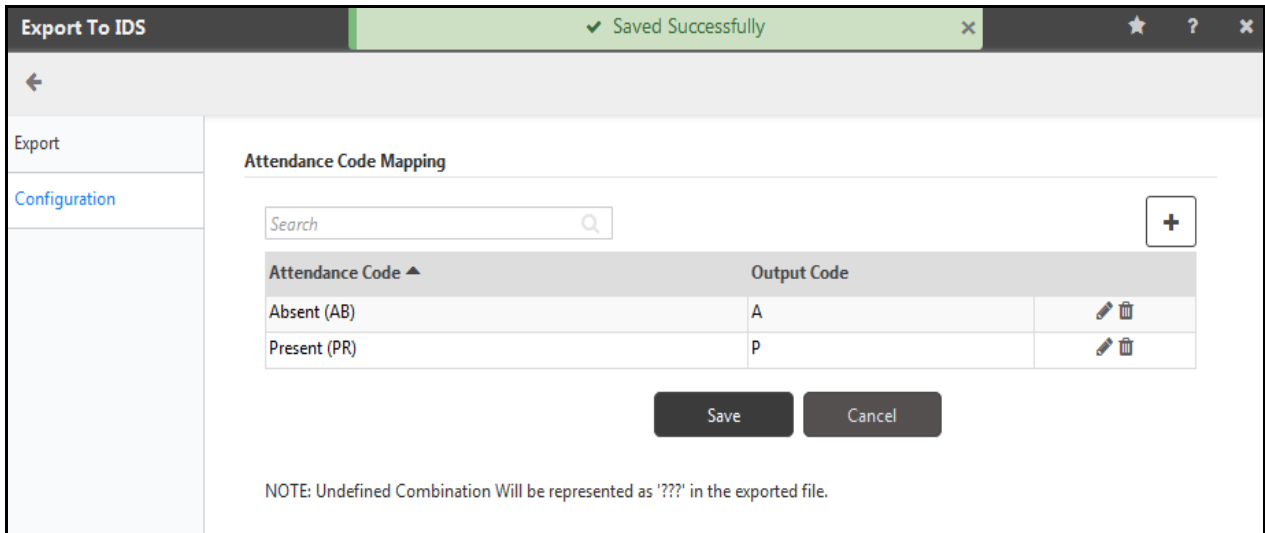
This tab enables the user to map the Attendance Code of the COSEC application to an Output Code as per the site requirements.

Click **Add**  button to add a new leave to export and the following screen appears.

Attendance Code: Select the **Attendance Code** from the dropdown list.

Output Code: Enter an Output Code to map against the **Attendance Code** (e.g. “P” can be the output code defined for “Present”).

Click on  icon to save the mapping. The defined mapping code appears in the bottom grid as shown below.



Export To IDS

✓ Saved Successfully

←

Export

Configuration

Attendance Code Mapping

Search

Attendance Code ▲	Output Code	
Absent (AB)	A	
Present (PR)	P	

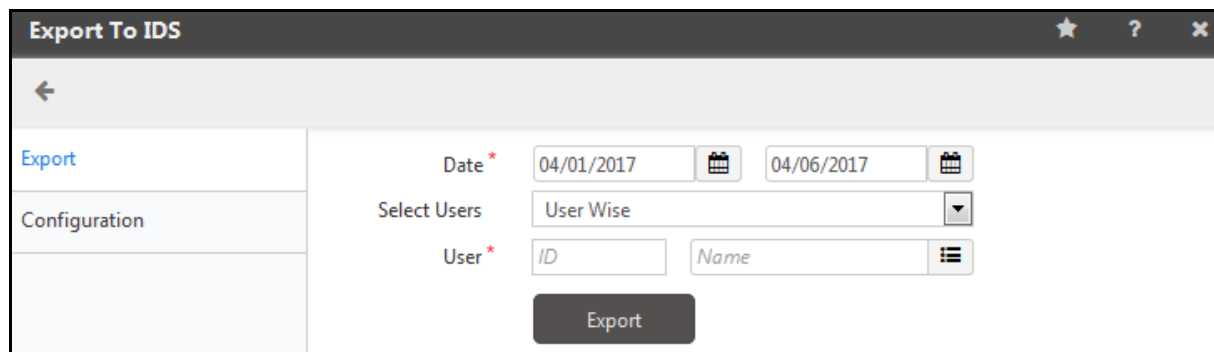
Save Cancel

NOTE: Undefined Combination Will be represented as '???' in the exported file.

Define all the applicable mappings as per the site requirements and click **Save** button once done.

The user can now export the data in required format from the COSEC application.

Click on the **Export** tab and the following screen appears as below:



Export To IDS

←

Export

Configuration

Date * 04/01/2017 04/06/2017

Select Users User Wise

User * ID Name

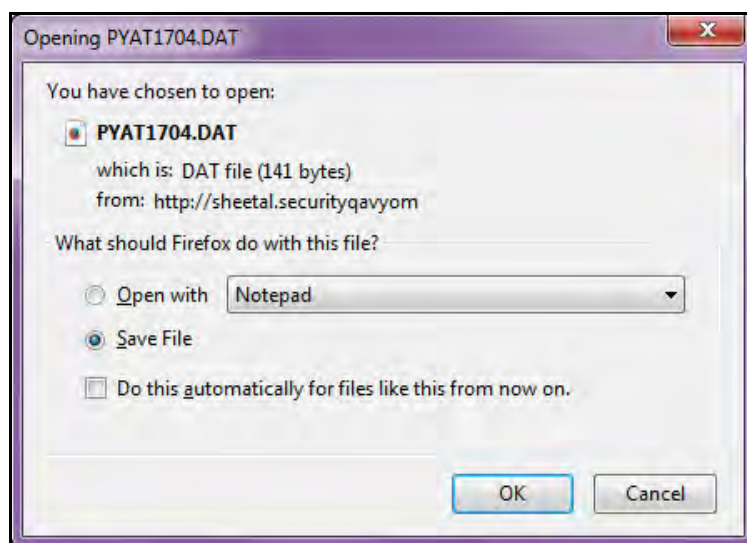
Export

- **Date:** Specify the date range for which the data is to be exported, by selecting the start and the end date.
- **Select Users:** Select single or multiple users whose data is to be exported from dropdown list. The administrator can select from the following options:
 - User Wise
 - Group Wise (*Available only with the Time & Attendance add on module*)
 - All

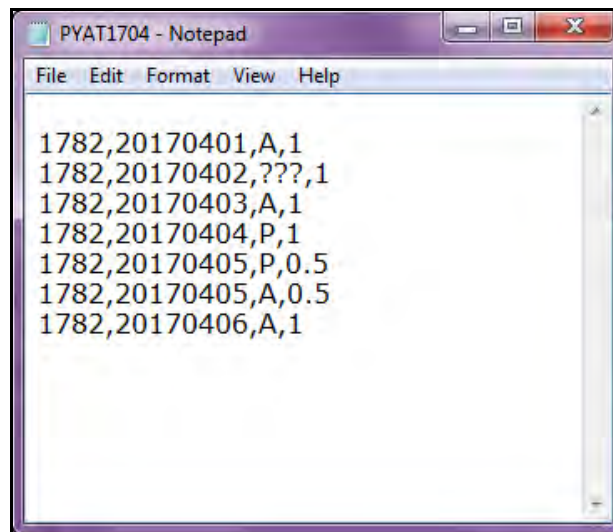
User ID	Name
1782	Nidhi

Click the **Export** button. The system prompts to browse to the folder path where the specified file is to be saved. The filename is automatically generated by the system as per the following format:

PYATYYMM.DAT (where YY stands for Year and MM stands for month).



The Exported File will display the user's Attendance Data in the following format.



The file generated contains the comma separated values in the sequence: **User ID**, Date in **YYYYMMDD** format, **Output Code**, 1/ 0.5 (Full Day/Half day).

For the better understanding, consider the following example and the screenshot above.

Example1:

1782,20170401,A,1 - This value denotes that the user with ID:**1782** on Date: 1st April 2017 (**20170401**) was Absent (**A**) for the full day (**1**).

Example2:

1782,20170404,P,1 - This value denotes that the user with ID:**1782** on Date: 1st April 2017 (**20170401**) was Present (**P**) for the full day (**1**).

Example3:

1782,20170405,P,0.5
1782,20170405,A,0.5

The above two values are generated for the same day (**20170405**), as the user was Present (**P**) in the first half (**0.5**) and Absent (**A**) in the second Half (**0.5**).

Example4:

1782,20170402,???,1 - In this value, "???" denotes that the Out put Code has not been mapped with the Attendance Code in the **Configuration** tab.

Scheduling Tasks/Reports

Scheduling refers to the process of setting up certain functions on the COSEC system to take place automatically at a scheduled time, without the need of manual intervention.

The *Scheduler* option in the COSEC application enables the administrator to perform the following functions:

- “Scheduling Tasks”
- “Scheduling Reports”
- “Scheduling Data Export”

To view a log of all scheduled reports/data exports/tasks and their status for a specific period, go to **Admin > Views/Logs > Scheduler Log**. For more information on generating such logs, refer to “Scheduling Tasks”.



The Alert Service must be running to run schedulers.

Scheduling Tasks

The *Task Scheduler* functionality in the COSEC Application enables the system to be scheduled for performing certain pre-defined tasks. Some of these tasks involve -

- Periodic database backup.
- Running the monthly schedule process on the scheduled day of the month.
- Running the monthly attendance process on the scheduled day of the month.
- Crediting leaves to user account on the scheduled day of the month.
- Configuring actions related to User relieving process like revoking devices etc.

To schedule a task, go to **Admin module > System Utilities > Task Scheduler** and the following screen appears.

The page displays configurations on the left hand side and to the right is a grid containing scheduled tasks.

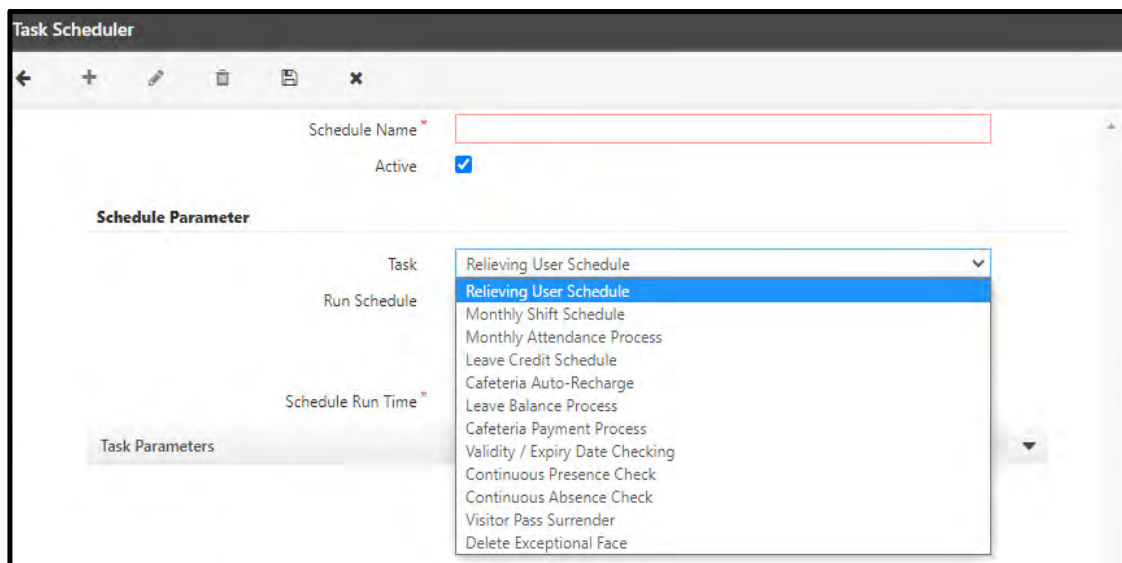
The configurations are:

- **Schedule Name:** Enter a unique name for the new task schedule to be defined.
- **Active:** Select this check-box to activate the scheduler.

Schedule Parameter

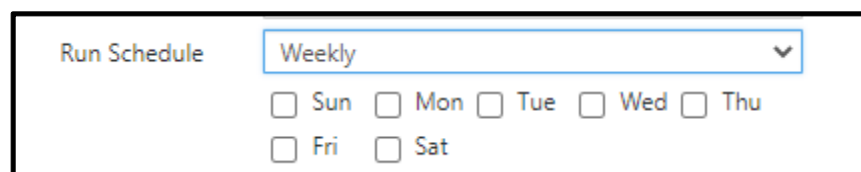
This section enables the user to set the schedule of the task.

- **Task:** Select a task from the dropdown list for which the scheduler is to be run (as shown).



The screenshot shows the 'Task Scheduler' window. At the top, there is a 'Schedule Name' text field and an 'Active' checkbox which is checked. Below this is the 'Schedule Parameter' section. It contains a 'Task' dropdown menu which is open, showing a list of tasks: 'Relieving User Schedule' (highlighted), 'Monthly Shift Schedule', 'Monthly Attendance Process', 'Leave Credit Schedule', 'Cafeteria Auto-Recharge', 'Leave Balance Process', 'Cafeteria Payment Process', 'Validity / Expiry Date Checking', 'Continuous Presence Check', 'Continuous Absence Check', 'Visitor Pass Surrender', and 'Delete Exceptional Face'. There is also a 'Run Schedule' dropdown and a 'Schedule Run Time' text field. A 'Task Parameters' section is partially visible at the bottom left.

- **Run Schedule:** Select the days or months to run the schedule from the drop-down.
- If Weekly is selected, then check the box of any 1 or more days as shown below.



The screenshot shows the 'Run Schedule' section. It features a dropdown menu set to 'Weekly'. Below the dropdown are checkboxes for the days of the week: Sun, Mon, Tue, Wed, Thu, Fri, and Sat. The checkboxes for Sun, Mon, Tue, and Wed are currently checked.

- If monthly is selected, then enter the day of the month for which the task has to be scheduled.

- **Schedule Run Time:** Specify the time at which the task schedule will run by COSEC in 24 hours format.



*If you have enabled the **Exceptional Face Enrollment** feature then make sure that you schedule a task of **Delete Exceptional Face** in Admin > System Utilities> Task Scheduler to avoid storage of excess data in the database.*

Task Parameters

This section lists the task parameters for the task scheduler configuration, depending on the type of task scheduled.

- **For Relieving User Schedule:** For relieving user schedule, task parameters will be about to execute relieving process either by deactivating a User or Delete User and also an option (enable/disable) to revoke assigned device.
- If the user relieving date is before the schedule run time then user will be relieved i.e. de-activated and the devices which were assigned to him would be revoked. E.g.: User relieving date is entered in his profile as 5th Feb 2018, and relieving schedule is run on 6th Feb 2018; then user will be relieved.

Schedule Parameter

Task: Relieving User Schedule

Run Schedule: Weekly

☐ Sun ☒ Mon ☐ Tue ☐ Wed ☐ Thu
☐ Fri ☐ Sat

Schedule Run Time *: 12:00

Task Parameters

Execute Relieving Process

Process: De-activate User

Revoke Assigned Devices: De-activate User

- The Filter can be used to specify users for whom the new schedule should be applicable.
- Click Save button to save the task scheduler configuration. The created scheduled task gets displayed in the grid on the right hand side.
- **For Monthly Shift Schedule:** Specify the processing period in Task Parameter as Current, Current +1, Current +2 etc.

E.g.: If Current month is June 2016, Processing period selected is Current +3, then monthly schedule for September 2016 will run on 1st Sept at 12 pm.

Schedule Parameter

Task: Monthly Shift Schedule

Run Schedule: Monthly

Every(Day Of The Month): 1

Schedule Run Time *: 12:00

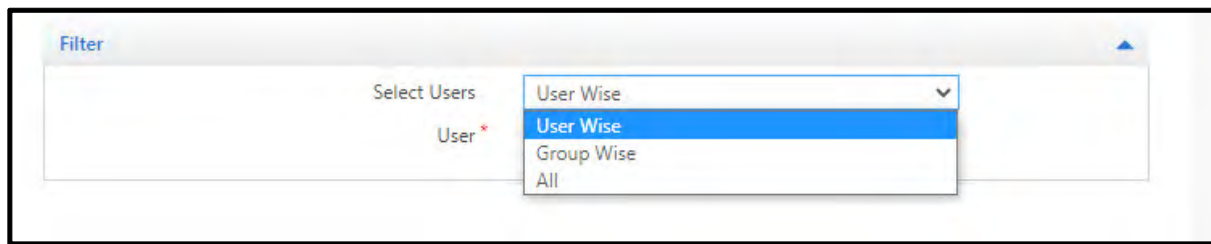
Task Parameters

Processing Period

Processing Period: Current

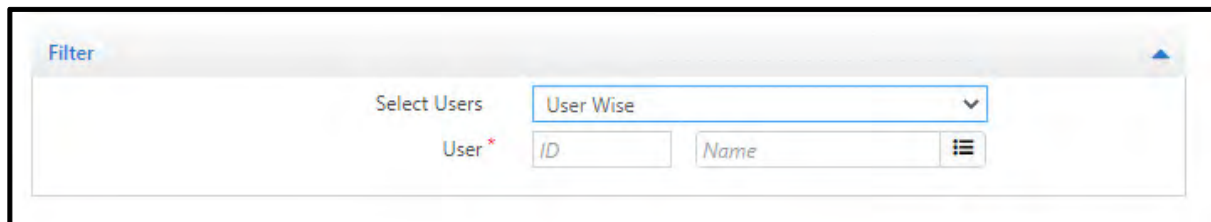
Filter: [Dropdown]

Filter: Apply the filters as per the selection of Users; User-wise, Group-Wise, All.



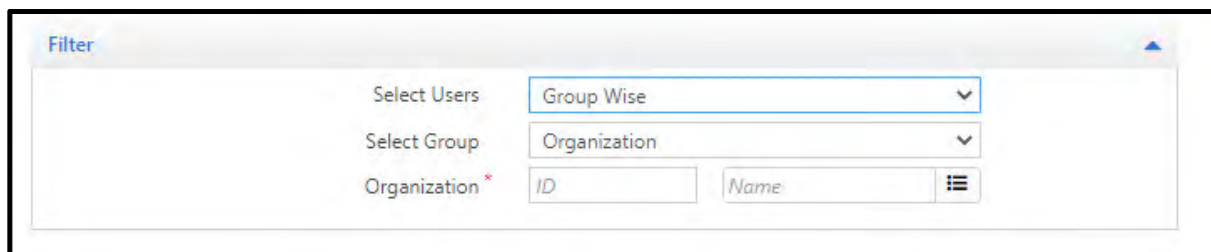
The screenshot shows a 'Filter' dialog box with a 'Select Users' dropdown menu. The dropdown is open, showing the following options: 'User Wise' (highlighted), 'Group Wise', and 'All'. The 'User' label is marked with a red asterisk.

When User Wise is selected, select the desired user id from the pick-list provided.



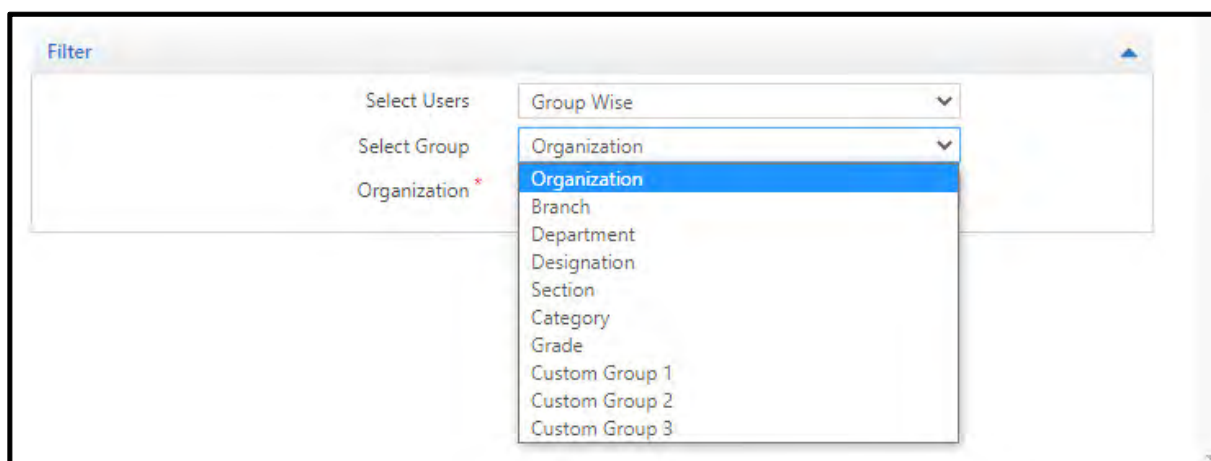
The screenshot shows the 'Filter' dialog box with 'User Wise' selected in the 'Select Users' dropdown. Below it, the 'User' label is marked with a red asterisk, and there are two input fields: 'ID' and 'Name'. A pick-list icon is visible next to the 'Name' field.

When Group Wise is selected, select the required type of group from the drop-down list provided.



The screenshot shows the 'Filter' dialog box with 'Group Wise' selected in the 'Select Users' dropdown. Below it, the 'Select Group' dropdown menu is open, showing the following options: 'Organization' (highlighted), 'Branch', 'Department', 'Designation', 'Section', 'Category', 'Grade', 'Custom Group 1', 'Custom Group 2', and 'Custom Group 3'. The 'Organization' label is marked with a red asterisk.

As per the selection of the group, select the particular group's name from the pick-list provided.
E.g. If the type of Group selected is Organization, then select any organization's name and ID from the provided pick-list.



The screenshot shows the 'Filter' dialog box with 'Group Wise' selected in the 'Select Users' dropdown. Below it, the 'Select Group' dropdown menu is open, showing the following options: 'Organization' (highlighted), 'Branch', 'Department', 'Designation', 'Section', 'Category', 'Grade', 'Custom Group 1', 'Custom Group 2', and 'Custom Group 3'. The 'Organization' label is marked with a red asterisk.



The Filter parameter is same as the Monthly Shift Schedule for all the Tasks available in the drop-down list.

Filter Parameter is not available for Relieving User Schedule, Validity/Expiry Date Checking and Visitor Pass.

- **For Monthly Attendance Process:**
 - **Send Alert Message to Users:** Enable to send alert message to users while processing the monthly attendance.
 - **Processing Period:** Select the period to perform the task.

The screenshot shows a web form titled "Schedule Parameter". It contains several fields and sections:

- Task:** A dropdown menu with "Monthly Attendance Process" selected.
- Run Schedule:** A dropdown menu with "Monthly" selected.
- Every(Day Of The Month):** A dropdown menu with "1" selected.
- Schedule Run Time:** A text input field with "HH:MM" and a red border, indicating it is required.
- Task Parameters:** A section with a blue header and a collapse arrow. It contains a checkbox labeled "Send Alert Message to Users" which is currently unchecked.
- Processing Period:** A section with a header and a dropdown menu showing "Previous".
- Filter:** A dropdown menu at the bottom of the form.

- **For Leave Credit Schedule:**
 - **Credit Method:** Select the method to credit leave as **Fixed** or **Policy**.
 - **Leave:** Select the **Leave** from the dropdown list.
 - **No. of Days:** Specify the number of days after which the leave should be credited for Fixed credit method.

Schedule Parameter

Task: Leave Credit Schedule

Run Schedule: Monthly

Every(Day Of The Month): 1

☒ Jan
 ☒ Feb
 ☒ Mar
 ☒ Apr
☒ May
 ☒ Jun
 ☒ Jul
 ☒ Aug
☒ Sep
 ☒ Oct
 ☒ Nov
 ☒ Dec

Schedule Run Time: 12:00

Task Parameters

Leave Selection

Credit Method: Fixed

Leave: Select

No of Days: 1

Apply Pro-rata: ☒

Processing Period

Processing Period: Current

Filter

- **Accrual Policy:** Select the policy using the pick-list for Policy credit method.
- **Apply Pro-rata:** Select to enable leave credit on pro-rata basis (i.e. based on the actual number of days worked).
- **Processing Period:** Select the period to process leave credit from the dropdown list.
- **No. of Hours** (This option is only available for Hourly based leaves): Specify **No. of Hour(s)** that should be credited leave for Fixed credit method (i.e. like *Hourly Paid Leave*, as shown in the figure)

Task Parameters

Leave Selection

Credit Method: Fixed

Leave: Hourly Paid Leave

No of Hour(s): HHH : MM

Apply Pro-rata: ☐

Processing Period

Processing Period: Current

Filter

- **For Cafeteria Auto-Recharge:**
 - **Recharge Amount:** Specify the amount to recharge the cafeteria account automatically.

Schedule Parameter

Task

Cafeteria Auto-Recharge

Run Schedule

Weekly

☐ Sun
☒ Mon
☐ Tue
☐ Wed
☐ Thu
☐ Fri
☐ Sat

Schedule Run Time *

12:00

Task Parameters

Recharge Amount *

100

- **For Leave Balance Process:**

- **Processing Period:** Select the period to process Leave Balance from the dropdown list

Schedule Parameter

Task

Leave Balance Process

Run Schedule

Monthly

Every(Day Of The Month)

1

Schedule Run Time *

12:00

Task Parameters

Processing Period

Current

Current

Next

Filter

- **For Cafeteria Payment Process:**

- **Processing Period:** Select the period to process monthly Cafeteria Payment from the dropdown list.

Schedule Parameter

Task: Cafeteria Payment Process

Run Schedule: Monthly

Every(Day Of The Month): 1

Schedule Run Time *: 12:00

Task Parameters

Processing Period: Previous (dropdown menu open showing Previous, Previous, Current)

Filter

- **For Validity/Expiry Date Checking:**
 - **Execute Relieving Process:** Select the required Check Field for User's Id Proof such as **Visa, Driving License, Passport** and configured **Custom Fields** to either **De-activate** or **Delete User**.
 - **Revoke Assigned Devices:** Enable this check-box to revoke the devices assigned to the user.

Schedule Parameter

Task: Validity / Expiry Date Checking

Run Schedule: Weekly

☐ Sun ☒ Mon ☐ Tue ☐ Wed ☐ Thu
☐ Fri ☐ Sat

Schedule Run Time *: 12:00

Task Parameters

Execute Relieving Process

Check Fields: Visa, Driving License, Passport

Process: De-activate User (dropdown menu open showing De-activate User, Delete User)

Revoke Assigned Devices



Only the Custom Fields which are configured as a 'Date' type will be displayed in the Check Fields list.

- **For Continuous Presence Check**

This task will check for the continuous number of present days of a user according to the assigned shift/hours as shown below.

- **Check For (Present Days):** Enter the number of days till which the presence of a user will be checked continuously from the scheduled date.
- **Schedule Run Time:** Set particular time at which task executes.

Schedule Parameter

Task: Continuous Presence Check

Check For (Present Days) *: 1

Schedule Run Time *: 12:00

Task Parameters

Processing Period

Processing Period: Current

Consider half day PR as Full Day PR: ☒ *i*

Days to consider as Present

Days	<input type="checkbox"/>			HH:MM
AB	<input type="checkbox"/>	Always	▼	HH:MM
Leave	<input type="checkbox"/>	Always	▼	HH:MM
WO	<input type="checkbox"/>	Always	▼	HH:MM
PH	<input type="checkbox"/>	Always	▼	HH:MM
FB	<input type="checkbox"/>	Always	▼	HH:MM
RD	<input type="checkbox"/>	Always	▼	HH:MM
IN	<input checked="" type="checkbox"/>	Always	▼	HH:MM

i

- **Processing Period:** Select the period to perform the task.
- **Consider half day PR as full day PR:** Enable the check-box to consider a day as full day present even if a user is present for half of the total working hours.
- **Days to consider as Present:** Select the days to be considered as present as per Shift based or Skip that day or Custom hours or Always.

Days to consider as Present

Days	<input checked="" type="checkbox"/>			HH:MM
AB	<input checked="" type="checkbox"/>	Shift Based	▼	HH:MM
Leave	<input checked="" type="checkbox"/>	Always	▼	HH:MM
WO	<input checked="" type="checkbox"/>	Skip	▼	HH:MM
PH	<input checked="" type="checkbox"/>	Shift Based	▼	HH:MM
FB	<input checked="" type="checkbox"/>	Custom Hours	▼	HH:MM
RD	<input checked="" type="checkbox"/>	Always	▼	HH:MM
IN	<input checked="" type="checkbox"/>	Always	▼	HH:MM

i

For the Configuration of rest parameters and related example, [See “Example: Continuous Absence/Presence” on page 340.](#)

- **Filter:** You can also apply filter by selecting Users as well as their respective shifts, as shown below:

For Example: If you select **PH** from the ‘Consider Work Hours For Full Day Present’, and set the parameters as ‘Custom Hours’ which is defined as “03:00” which means, by attending 3:00 hours on a Public Holiday will be considered as a Full Day Present.

- **For Continuous Absence Check**

This task will count the continuous number of absence days of the user according to the assigned shift/hours as shown below.

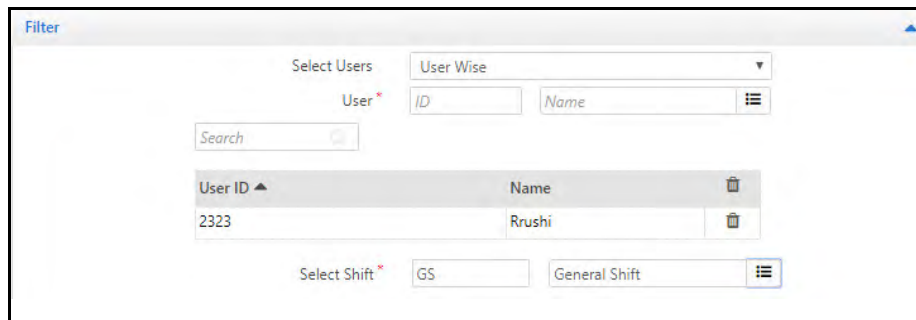
- **Check For (Absent Days):** Enter the number of days till which the absence of a user will be checked continuously from the scheduled date.
- **Schedule Run Time:** Set particular time at which task executes.

Task Parameters:

- **Processing Period:** Select the period to perform the task.
- **Consider half day PR as full day PR:** Enable the check-box to consider a day as full day present even if a user is present for half of the total working hours.

For the Configuration of rest parameters and related example, See [“Example: Continuous Absence/Presence” on page 340.](#)

- **Filter:** You can also apply filter by selecting Users as well as their respective shifts, as shown below:

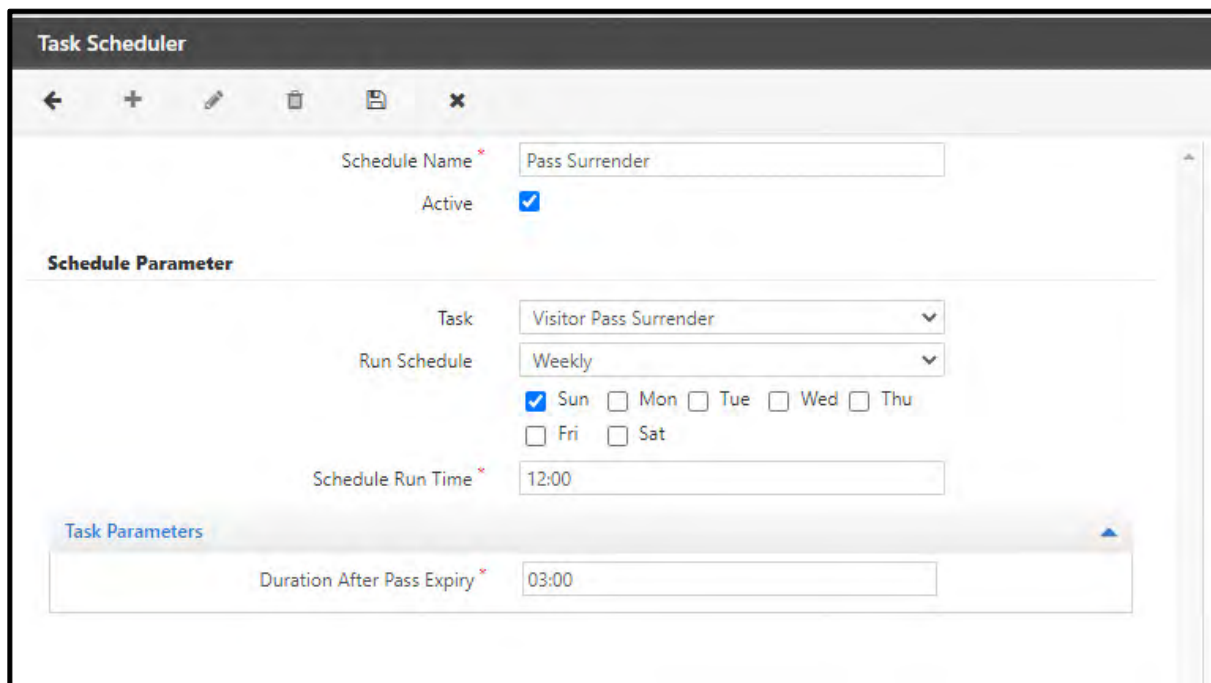


The screenshot shows a 'Filter' window with the following elements:

- Select Users:** A dropdown menu set to 'User Wise'.
- User:** Fields for 'ID' and 'Name' with a search icon.
- Search:** A text input field with a search icon.
- User List:** A table with columns 'User ID' and 'Name'. It contains one entry: User ID 2323, Name Rrushi.
- Select Shift:** A dropdown menu set to 'GS' (General Shift).

For Example: If you select **AB** from the 'Consider Work Hours For Full Day Present', and set the parameters as 'Custom Hours' which is defined as "03:00" which means, by attending 3:00 hours on a day of absence will be considered as a Full Day Present.

- **For Visitor Pass Surrender:** This task will surrender the pass for those visitors by default by system whose visit has ended and they have yet to checkout on their own through visitor portal or via security gate.



The screenshot shows the 'Task Scheduler' window with the following configuration:

- Schedule Name:** Pass Surrender
- Active:** ☒
- Schedule Parameter:**
 - Task:** Visitor Pass Surrender
 - Run Schedule:** Weekly
 - Days:** ☒ Sun, ☐ Mon, ☐ Tue, ☐ Wed, ☐ Thu, ☐ Fri, ☐ Sat
 - Schedule Run Time:** 12:00
- Task Parameters:**
 - Duration After Pass Expiry:** 03:00

Run Schedule: Select from the given options **Weekly/Monthly** to run this scheduled task.

Schedule Run Time: Enter the time to execute this scheduled task.

Task Parameter

Duration After Pass Expiry: Set the minimum time duration after Visitor Pass expiry which will be considered for Auto surrendering of the Visitor Pass.

This time will be a buffer to provide some time to the visitor to submit the pass. If the visitor still doesn't submit then this scheduler will surrender the pass.

For example 1:

If a Visitor's Visit time is from 9:00 AM to 11:00 AM.

Scheduled Run Time: 12:00 PM

Duration After Pass Expiry: 03:00 Hours

Now when the visitor checks out at 11:00 AM through Visitor portal or via Security Portal, Visitor Pass will be surrendered.

For example 2:

If a Visitor's Visit time is from 9:00 PM to 11:00 PM.

Scheduled Run Time: 12:00 PM

Duration After Pass Expiry: 03:00 Hours

In this case, if the Visitor due to any reason hasn't checked out even after 11:00 PM, then the system will wait for 03 Hours as set in Duration After Pass Expiry and if still the Visitor doesn't checkout, the system will auto surrender the particular Visitor's Pass.

Scheduling Reports

The *Report Scheduler* functionality enables e-mail reports to be sent to selected users as per configured schedules. The system uses the *COSEC Alerts* service settings to send the e-mails.

To schedule a report, select **Admin module > System Utilities > Report Scheduler** and the following screen will appear.

The screenshot shows the 'Report Scheduler' web application window. It features a sidebar with navigation icons and a search bar. The main content area is divided into two sections. The left section contains form fields for scheduling a report: 'Scheduler Type' (set to 'Reports'), 'Schedule Name' (empty), 'Active' (checked), 'Module' (set to 'All'), 'Parent Menu' (set to 'All'), 'Report' (set to 'Select Report'), 'Send Email Notification' (checked), 'Email ID' (empty), 'Report Format' (set to 'PDF'), 'Message' (empty), 'Schedule Run Time' (set to 'HH:MM'), 'Schedule Run Day' (set to 'Weekly'), and 'Report Parameters' (empty). The right section displays a table with columns 'ID' and 'Schedule Name', showing 'No Data'.

Click the **New** button and provide the following parameters.

- **Scheduler Type:** Select the scheduler type as **Report** from the dropdown list.
- **Schedule Name:** Enter a unique name for the new report schedule to be defined.
- **Active:** Enable to activate the scheduler.
- **Module:** Select the module name from the dropdown list, for which this scheduler would apply. Select **All** if you desire to schedule reports of all the modules.
- **Parent Menu:** As per the selected module, the options (sub module) will be available into the dropdown list. Select the desired one of which the report is to be selected for schedule. If the **Module** selected is **All**, then select **All**, to schedule the report of all the sub modules.
- **Report:** Select a report type from the dropdown list, for which the schedule is assigned. This list is dependent on the **Module** selected.

Send Email Notification

This section offers the following options:

- **Send Report To:** Select the desired option from the given drop-down.
- 1. **Configured Email ID:** When Configured Email ID is set, then the report will be sent to the respective Email ID only.

Make sure you configure the desired **Email ID**.

- **Email ID:** If you have selected **Configured ID** as the **Send Report To** option, enter the email address of the recipient to whom the specific report is to be sent. In the event of multiple email ids, use a comma as the separator between the ids.



Report will be sent only to those recipients whose email address is already stored in the system database.

Under the **Filter** section:

- In **Send Report To**, select the desired option.
 - User Wise: Select the desired users from the picklist.
 - Group Wise: Select the desired groups from the picklist. The reports will be sent to the users within the group.
 - All
- In **Generate Report For**, select the desired option
 - All Users
 - Active Users
 - Inactive Users
- 2. **Reporting In-Charge:** When Reporting In-Charge is set, then the report will be sent to the Reporting In-Charge of the user for whom this report is being generated.

You can send report to selected RIC users or selected RIC users within a group.

To set the desired option, under the **Filter** section in **Send Report To** select the desired option.

- User Wise: Select the desired RIC users from the picklist.
- Group Wise: Select the desired groups from the picklist. The reports will be sent to the RIC users within the group.

In case the Email ID of Reporting In-Charge is not available or is invalid, then the report will not be sent. Make sure the Reporting Group is configured for the user otherwise the report will not be sent.

- 3. **Assigned User Itself:** When Assigned User itself is set, then the report will be sent to respective user for whom the report is being generated.

You can send report to selected users or selected users within a group.

To set the desired option, under the **Filter** section in **Send Report To** select the desired option.

- User Wise: Select the desired users from the picklist.

- **Group Wise:** Select the desired groups from the picklist. The reports will be sent to the users within the group.
- **All**

In case the Email ID of the users is not available or is invalid, then the report will not be sent.

- **Report Format:** Select the format in which the report is to be mailed to the recipients in one of the three formats - PDF, XLS or CSV.
- **Message:** Enter relevant description regarding the report in the **Message** field with maximum 500 characters. The subject line for the scheduled reports will be as follows:

<Report Name>: Generated on - <schedule run date-time (dd/mmm/yyyy - hh:mm)>

Schedule Parameter

This section enables the user to set the schedule of the reports or tasks.

The screenshot shows the 'Schedule Parameter' form. It has a title bar 'Schedule Parameter'. Below it, there are two main fields: 'Schedule Run Time *' with a text input field containing 'HH:MM', and 'Schedule Run Day' with a dropdown menu set to 'Weekly'. Below the dropdown, there are seven checkboxes for the days of the week: Sun, Mon, Tue, Wed, Thu, Fri, and Sat. All checkboxes are currently unchecked.

- **Schedule Run Time:** Specify the time at which you want the report to be generated.
- **Schedule Run Day:** You can schedule reports **Weekly** or **Monthly** or **Bi-weekly**.
 - For **Weekly** reports, you can select the days of the week.
 - For **Monthly**, you can select any day of the month.

The screenshot shows the 'Schedule Parameter' form with 'Schedule Run Day' set to 'Monthly'. Below the dropdown, there is a field 'Every (Day Of the Month)' with a text input field containing '1'.

- For **Bi-Weekly** reports, you can select a day of the week.as well select the desired week of the year.

The screenshot shows the 'Schedule Parameter' form with 'Schedule Run Day' set to 'Bi-Weekly'. Below the dropdown, there are seven checkboxes for the days of the week: Mon, Tue, Wed, Thu, Fri, Sat, and Sun. The 'Mon' checkbox is checked. Below these, there is a field 'Week of the Year' with a dropdown menu set to 'Odd Weeks'. There is also an information icon (i) to the right of the dropdown.

- In **Week of the Year** select the desired option as **Odd Weeks** or **Even Weeks**.

Report Parameters

This section lists some additional parameters for the report scheduler configuration, depending on the type of report scheduled.

- The **Processing Period** enables the administrator to set the time period of the selected report. Some reports will have only the **For Date** option while others will have the **Start Date** and the **End Date** options.
- **For Date**: Specify the day prior to the scheduled day for which the report is required. If report for current date of scheduled day is required then set the value as 0. If scheduled day is set as Friday and the number of days specified is 2 then system will send the report of Wednesday every Friday.
- **Start and End Date**: Specify the time period prior to the scheduled day for which the report is required. For reports relating to month wise data, specify the month prior to the scheduled month for which the report is required. If the number specified in this field is 1, then system will send report of the previous month.
- **Group By Selection**: Select the group from the **Group By** dropdown list for which the report is to be scheduled.
- **Application Type Filter**: Select the **Application Type** from the dropdown list for which the report is to be scheduled.
- **List Selection**: Select the type of applications from the **Select** dropdown list for which the report is to be scheduled. One can select multiple applications.

The below figure illustrates the **Report Parameters** for an example, where a Leave Application report is being scheduled by a Leave Management module user:

Report Scheduler

←

+

✎

🗑

💾

✕

Scheduler Type

Reports

Schedule Name *

Absence Check

Active

☒

Module

Leave Management

Parent Menu

None

Report

Leave Application

Send Email Notification

Email ID *

sheetal@matrix.com

Report Format

PDF

Message

Leave Application Report

Schedule Parameter

Schedule Run Time *

12:00

Schedule Run Day

Weekly

☐ Sun

☒ Mon

☐ Tue

☐ Wed

☐ Thu

☐ Fri

☐ Sat

Report Parameters

Processing Period

Start Days Before Scheduled Day *

1

End Days Before Scheduled Day *

1

Group by Selection

Group By

Organization

Application Type Filter

Application Type

All

Group By Selection

Group By

Date

List Selection

Select *

☒ Pending

☐ Approved

☐ Rejected

thSelect Leave/Tour el

All

For the customized report, the 'Processing Period' will include **Other Option** parameters (Filter) if the 'Optional Parameters' option is enabled in the *Report Configurations > Report Builder*.



"Filter Events" option will available only for the report with Report Type = Events.

For the detailed configuration of Other Option, [See "Example: Events Report Template placed in User module" on page 2223.](#)

Filter

This section enables you to specify the users to whom the reports need to be sent. The users can be filtered based on individual users or users belonging to various groups as configured in the COSEC application.

Refer to ["Send Email Notification"](#) for more details.

Click the **Save** button to save the report schedule. All created report schedules are displayed in the list on the right hand side of the page.



*You must configure Email settings from **Email Configuration** page of **System Configuration** tab to send the Email notification.*



The Access Control- Elevator Access Control Report requires Basic + ACS License.

Example: JPC module- Project Summary report scheduler

Report Scheduler

Scheduler Type: Reports

Schedule Name*: JPC

Active: ☒

Module: Job Processing and Costing

Parent Menu: Work Summary

Report: Project Summary

Send Email Notification

Email ID: Email Address

Report Format: PDF

Message: Email Body 500(chars)

Schedule Parameter

Schedule Run Time*: 12:00

Schedule Run Day: Weekly

☐ Sun ☒ Mon ☐ Tue ☐ Wed ☐ Thu
☐ Fri ☐ Sat

Example: Device module- Device Wise Events report scheduler

Report Scheduler

Scheduler Type: Reports

Schedule Name*: DevicewiseEvents

Active: ☒

Module: Devices

Parent Menu: None

Report: Device-Wise Events

Send Email Notification

Email ID: Email Address

Report Format: PDF

Message: Email Body 500(chars)

Schedule Parameter

Schedule Run Time*: 12:00

Schedule Run Day: Monthly

Every(Day Of The Month): 1

Example: Continuous Absence/Presence

The continuous Absence/Presence report allow you to generate the attendance summary of user, if he/she is absent or present continuously for how many days.

Select "Time and Attendance" as **Module**, "Absenteeism" as **Parent Menu** and "Continuous Absence/Presence" as **Report**

Report Scheduler

Scheduler Type: Reports

Schedule Name: AB-PR

Active: ☒

Module: Time and Attendance

Parent Menu: Absenteeism

Report: Continuous Absence/Presence

Send Email Notification

Email ID: Email Address

Report Format: PDF

Message: Email Body 500(chars)

Schedule Parameter

Schedule Run Time: 20:00

Schedule Run Day: Weekly

☒ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu
☐ Fri ☐ Sat

Consider below Report Parameters for Report Type = “Continuous Absence”

Report Parameters

Processing Period

Start Days Before Scheduled Day: 1

End Days Before Scheduled Day: 1

Report Template

Report Type: Continuous Absence

Continuous Absent Days: 1

Select Shift: All

Consider half day PR as full day PR: ☒

Days to consider as Absent

Days			
<input checked="" type="checkbox"/> AB	Always		HH:MM
<input checked="" type="checkbox"/> WO	Always		HH:MM
<input checked="" type="checkbox"/> PH	Always		HH:MM
<input checked="" type="checkbox"/> Leave	Always		HH:MM
<input checked="" type="checkbox"/> FB	Always		HH:MM
<input checked="" type="checkbox"/> RD	Always		HH:MM
<input type="checkbox"/> IN	Always		HH:MM

Report Template

- **Continuous Absent Days:** Enter the minimum number of days for 'Absence' which is required to be counted as 'Continuous Absent Days'. Suppose, 3 days are specified, then the counting will be started and shown into the report only if user is absent for 3 or more days. The absence of less than 3 days will not be considered as Continuous Absent Days.
- **Select Shift:** Select 'All' option if the report to be generated is of all the Shifts. In case of requirement of report of particular shifts like 'Report of only General Shift' or 'Report of Night Shift', select the option 'Shift-wise'. Multiple shifts can be selected from the pick-list provided.
- **Consider half day PR as full day PR:** Enable the check-box to consider a day as full day present even if the user is present for half day.

Days to Consider as Absent

Enable the respective check-boxes for the days which should be consider as a Absent. Also select the required option from the dropdown list located besides the day column as shown below.

Always: Select the option to count the entire day as 'Absent'.

Skip: Select to Skip the day from counting of continuous absence. .

Shift Hours: Select to check for assigned work hours of a user. If the work hours for the day are equal or greater than the assigned hours, then count as present else count the day in number of total continue absent days.

Custom Hours: Select and specify the custom work hours which is required to be completed on the day. If the work hours are equal or greater than the specified hours then, count as present else count the day in number of total continue absent days.

Configure the Filter tab and click on the save button to Save the scheduled report.



Kindly consider below example for the report generation of Continuous Absence.

Let consider below weekly attendance details of a User-1 for which the 'Continuous Absence' report is to be generated.

01/06/2020 - PR - PR
 02/06/2020 - PR - PR
 03/06/2020 - AB - AB
 04/06/2020 - PR - PR
 05/06/2020 - PR - PR
 06/06/2020 - PR - PR
 07/06/2020 - WO - WO

The 'Schedule Run Time' is 20.00 hrs and 'Schedule Run Day'; Sunday is configured as shown below:

Schedule Parameter

Schedule Run Time * 20:00

Schedule Run Day Weekly

☒ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu
☐ Fri ☐ Sat

Report Parameters

Filter

The 'Report Template' and 'Days to Consider as Absent' is configured as shown below:

Report Template

Report Type Continuous Absence

Continuous Absent Days * 1

Select Shift All

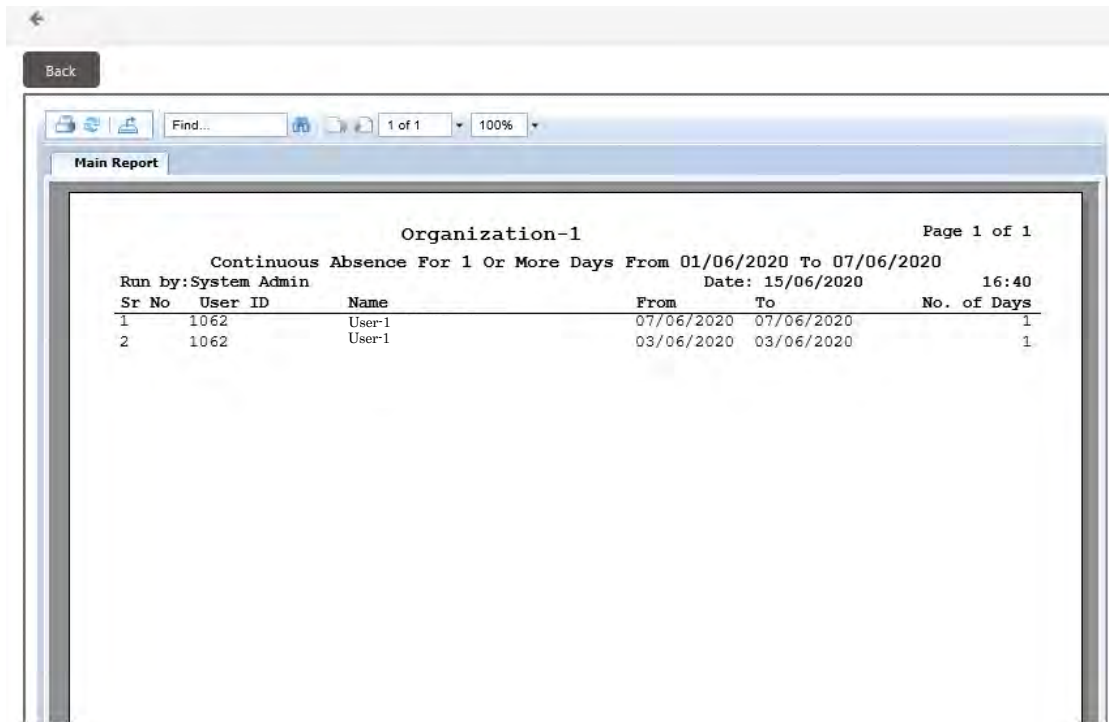
Consider half day PR as full day PR ☒ ⓘ

Days to consider as Absent

<input type="checkbox"/> Days				
<input checked="" type="checkbox"/> AB	Always		HH:MM	
<input checked="" type="checkbox"/> WO	Always		HH:MM	
<input checked="" type="checkbox"/> PH	Always		HH:MM	
<input checked="" type="checkbox"/> Leave	Always		HH:MM	
<input checked="" type="checkbox"/> FB	Always		HH:MM	
<input checked="" type="checkbox"/> RD	Always		HH:MM	
<input type="checkbox"/> IN	Always		HH:MM	ⓘ

Save the configuration.

Now as per the User-1's weekly attendance and configuration, the scheduled report (on Sunday) will be run as shown below.



The same way you can configure the parameters for the Report Type = "Continuous Presence" as shown below.

Report Scheduler

Processing Period

Start Days Before Scheduled Day * 1

End Days Before Scheduled Day * 1

Report Template

Report Type Continuous Presence

Filter Based On Days

Continuous Present Days * 1

Select Shift All

Consider half day PR as full day PR ☒ ⓘ

Days to consider as Present

<input type="checkbox"/> Days			
<input type="checkbox"/> AB	Always	▼	HH:MM
<input type="checkbox"/> WO	Always	▼	HH:MM
<input type="checkbox"/> PH	Always	▼	HH:MM
<input type="checkbox"/> Leave	Always	▼	HH:MM
<input type="checkbox"/> FB	Always	▼	HH:MM
<input type="checkbox"/> RD	Always	▼	HH:MM
<input checked="" type="checkbox"/> IN	Always	▼	HH:MM ⓘ

Filter ▼

Report Template

- **Continuous Present Days:** Enter the minimum number of days for 'Presence' which is required to be counted as 'Continuous Present Days'. Suppose, 4 days are specified, then the counting will be started and shown into the report only if user is present for 4 or more days. The presence of less than 4 days will not be considered as Continuous Present Days.
- **Consider half day PR as full day PR:** Enable the checkbox to consider a day as full day present even if the user is present for half day.

Days to Consider as Present

Enable the respective checkboxes for the days which should be consider as a Present. Also select the required option from the dropdown list located besides the day column as shown below.

Always: Select the option to count the entire day as Present.

Skip: Select to Skip the day from counting of continuous Present.

Shift Hours: Select to check for assigned work hours of a user. If the work hours for the day are equal or greater than the assigned hours, then count as present else count the day in number of total continue absent days.

Custom Hours: Select and specify the custom work hours which is required to be completed on the day. If the work hours are equal or greater than the specified hours then, count as present else count the day in number of total continue absent days.

Configure the Filter tab and click on the save button to Save the scheduled report.



Kindly consider below example for the report generation of Continuous Presence.

Let consider below weekly attendance details of a User-1 for which the 'Continuous Presence' report is to be generated.

01/06/2020 - PR - PR
02/06/2020 - PR - PR
03/06/2020 - AB - AB
04/06/2020 - PR - PR
05/06/2020 - PR - PR
06/06/2020 - PR - PR
07/06/2020 - WO - WO

The 'Schedule Run Time' is 20.00 hrs and 'Schedule Run Day'; Sunday is configured as shown below:

Schedule Parameter

Schedule Run Time * 20:00

Schedule Run Day Weekly

☒ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu
☐ Fri ☐ Sat

Report Parameters

Filter

The 'Report Template' and 'Days to Consider as Present' is configured as shown below:

Report Template

Report Type: Continuous Presence

Filter Based On: Days

Continuous Present Days *: 1

Select Shift: All

Consider half day PR as full day PR: ☒ *i*

Days to consider as Present

Days			
<input type="checkbox"/> Days			
<input type="checkbox"/> AB	Always		HHMM
<input type="checkbox"/> WO	Always		HHMM
<input type="checkbox"/> PH	Always		HHMM
<input type="checkbox"/> Leave	Always		HHMM
<input type="checkbox"/> FB	Always		HHMM
<input type="checkbox"/> RD	Always		HHMM
<input checked="" type="checkbox"/> IN	Always		HHMM <i>i</i>

Save the configuration.

Now as per the User-1's weekly attendance and configuration, the scheduled report (on Sunday) will be run as shown below.

Back

Find... 1 of 1 100%

Main Report

Organization-1 Page 1 of 1

Continuous Presence For 1 Or More Days From 01/06/2020 To 07/06/2020

Run by: System Admin Date: 15/06/2020 17:05

Sr No	User ID	Name	From	To	No. of Days
1	1062	User-1	04/06/2020	06/06/2020	3
2	1062	User-1	01/06/2020	02/06/2020	2

Example: Visitor History Report

Select “**Visitor Management**” as Module and “**Visitor History**” as Report.

Scheduler Type	Reports ▼
Schedule Name *	Visitor Report
Active	<input checked="" type="checkbox"/>
Module	Visitor Management ▼
Report	Visitor History ▼

This Report parameters will change according to **Report Type**.

Report Parameters	
Processing Period	
Start Days Before Scheduled Day *	1
End Days Before Scheduled Day *	1
Group by Selection	
Group By	Organization ▼
Group Needed In Report	<input type="checkbox"/>
Station	All ▼


Enabling the check-box “**Group Needed In Report**” will display the name for that particular group in the generated report.

Then Fill up the filter:

Select Users: Select All or User Wise depending on your requirement.

User: If you select “Select Users : User Wise”, then you have to mention that particular user.

Generate Report For: Select for whom you want to generate the report.

Filter	
Send Report Of	
Select Users	User Wise ▼
User *	ID <input type="text"/> Name <input type="text"/> 
Generate Report For	All Users ▼

Click on **Save icon** after you are done with the configuration.

Scheduling Data Export

This scheduler enables data export templates to be sent by e-mail to selected users as per configured schedules. The system uses the *COSEC Alerts* service settings to send the e-mails.

To schedule a data export, go to **Report Scheduler** page and click the **New** button.

ID	Schedule Name
5	Attendance Report
2	Monthly OT Report
1	Leave Application Schedule

- **Scheduler Type:** Select the scheduler type as **Export Data** from the dropdown list.
- **Schedule Name:** Enter a unique name for the new report schedule to be defined.
- **Active:** Enable to activate the scheduler.
- **Template:** Select template from the dropdown list based on which the report is to be exported.
- Setup the required e-mail and schedule configurations for the scheduler. Refer “Scheduling Reports”
- The **Export Parameters** section for data export scheduler will vary depending on the template selected. This section primarily defines the time range for which the data must be exported and the export file details.

For daily data, specify the number of days prior to the Scheduled Day for the **Start Date** as well as the **End Date** as shown. Here, the data from 1 day before the scheduled date to 1 day1s before the scheduled date is specified for export:

Export Parameters

Start Date (Days Before Scheduled Day) *

1

End Date (Days Before Scheduled Day) *

1

File Format

XLS

Filename *

Export Data

For month-wise data, specify the month before the scheduled day for which data must be exported. If the number specified in this field is 1, then system will send data of the previous month.

- **File Format:** Specify the export file format.
- **Filename:** Specify a name for the file to be exported.



If number of rows and columns are found to be more than 65535 and 255 respectively then Export Data would generate .xlsx file.

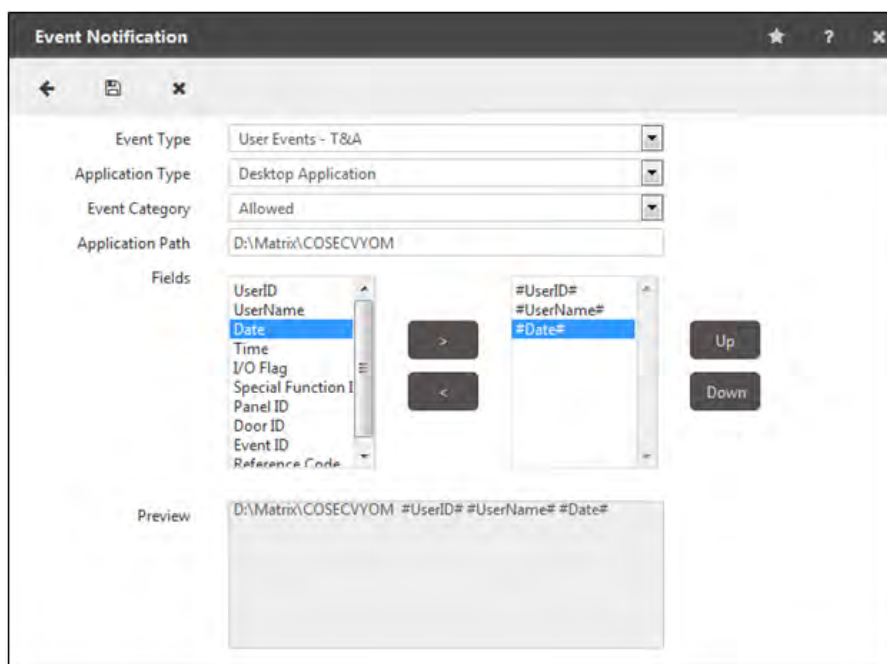
- In the **Filter** section, specify the users whose data is to be exported (if required).
- Click the **Save** button to save the schedule.

Event Notification

The Event Notification feature enables third party application to access and display the COSEC events which is only displayed in COSEC monitor.

It enables to pass pre-defined fields from live events coming from the COSEC Panel-lite and door controllers to an external application, which in turn can place it in another database. The external application could be any third party desktop or a web application.

To access this functionality, Go to **Admin> System Utilities > Event Notification** and the following screen appears.



- **Event Type:** Select the type of event from the dropdown list. The options available are:
 - User Events - T&A (*Available only with the Time & Attendance add on module*)
 - User Events - All
- **Application Type:** Select the Application Type from the dropdown list.
- **Event Category:** Select the **Event Category** from the drop down list. The options available are:
- **Application Path:** Specify the application path in the following formats:
 - For Desktop application: **C:\Program Files\XYZ\XYZ.exe**
 - For Web Application: **http://localhost/XYZ/default.aspx**

The desktop application has to incorporate command line arguments while in the case of the web application query strings need to be incorporated in the external application.



The application path is the path of third party application as required by the customer.

- **Fields:** The grid displays the fields whose live values are available for export as shown.

Select the fields one at a time and click on the right arrow button. The selected fields will be visible on the right grid as shown above. Click on the **Up** or **Down** button to change the order of the selected fields.

Refer the “[Field Values](#)” section of this topic for the values which will be sent for the various user events.

- Click **Save** on the menu bar to commit the changes. The administrator needs to ensure that the COSEC Monitor application is running for this functionality to work. In order to stop the exporting process the administrator needs to blank out the **Application Path** parameter from the page.

Field Values

The export events option will send the following values based on the user event.

- I/O Flag:** This flag represents the IN or OUT status. The following values can be sent:
 - 0 = Entry
 - 1 = Exit
- Special Function ID:** The following special function code values will be sent based on the special function associated with the user event.

Special Function Name	Special Function Code
Official Work-IN Marking in T&A	1
Official Work-OUT Marking in T&A	2
Short Leave-IN Marking in T&A	3
Short Leave-OUT Marking in T&A	4
Clock - IN Marking in T&A	5
Clock - OUT Marking in T&A	6
Post Lunch-IN Marking in T&A	7
Pre Lunch -OUT Marking in T&A	8
Over time - IN Marking in T&A	9
Over time - OUT Marking in T&A	10
Late -IN Allowed Marking in T&A	11
Early - OUT Allowed Marking in T&A	12
Access in Degrade Mode Marking	99

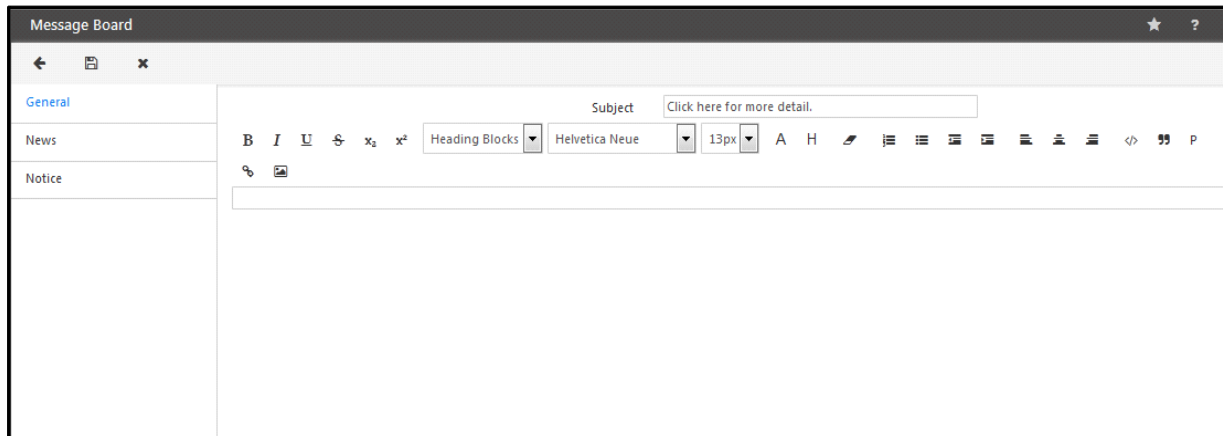
- **Event ID:** This value will depend on the User category as well as the type of user event as follows:

Event ID	Event Description
101	User Allowed
102	User Allowed - with Duress
103	User Allowed - Anti-Pass Back-soft
104	User Allowed - Dead-man Zone
105	User Allowed - Door Not open
151	User Denied - User Invalid
152	User Denied - Occupancy Control
153	User Denied - 2-Person Rule
154 '	User Denied - Time Out
155	User Denied - Visitor Escort Rule
156	User Denied - Anti-Pass Back
157	User Denied - Disabled User
158	User Denied - Blocked User
159	User Denied - First IN User
160	User Denied - DND Enabled
161	User denied - Control zone
162	User Denied - Door Lock
163	User Denied - Invalid Access Group

Message Board

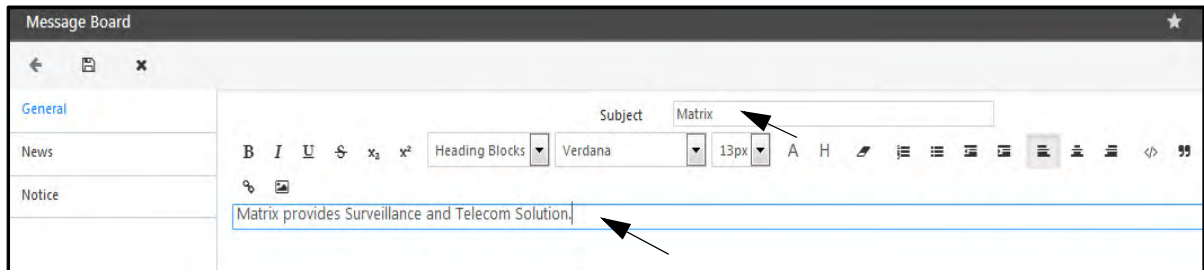
The Message board has been provided to enable the administrator to specify messages which should be displayed on the *Employee Self Service* application home page when ESS users login to the application.

To access this option, go to **Admin module > System Utilities > Message Board** and the following screen appears.



The page displays the following tabs:

- **General** - This tab allows to configure and display general messages of interest.
- **News** - This tab allows to configure and display latest news items.
- **Notice** - This tab allows to configure and display notices for all employees.



Select the appropriate tab based on the type of message to be configured and enter the message for the ESS users.

Enter the **Subject** and the related message in the box as shown above.

Click the **Save** button to save the entries.

The ESS user can view the **Notice**, **News** and **General** message by clicking on it on the scrolling information from the bottom of home page as shown below.

The screenshot displays the 'Member Details' page for a user named Chirag. The page is divided into three main sections:

- Work Hours Detail:** Shows attendance data for 04/18/2017. The table includes columns for Work Hours, Net Work Hours, Actual OT, Authorized OT, Late In, and Early Out. The values are: Work Hours: 1, Net Work Hours: 0.75, Actual OT: 0.5, Authorized OT: 0.25, Late In: 0, Early Out: 0.
- Pending Approvals / Authorization 0:** A table showing various approval types and their counts:

0	0	0	0
Leave	Tour	C-OFF	Attendance Correction
0	0	0	0
Attendance	Short Leave/Official IN-OUT	Overtime/C-OFF	Timesheet Correction
- Daily Attendance Summary:** Shows attendance data for 04/18/2017. The table includes columns for Reported, Absent, On Leave, On Tour, On Holiday, On Field Break, and On Rest Day. The values are: Reported: 0, Absent: 0, On Leave: 0, On Tour: 0, On Holiday: 0, On Field Break: 0, On Rest Day: 0.

At the bottom of the page, there is a navigation bar with buttons for Notice, News, and General. An arrow points to the 'General' button.

Click on General. The general message will be displayed as shown below.

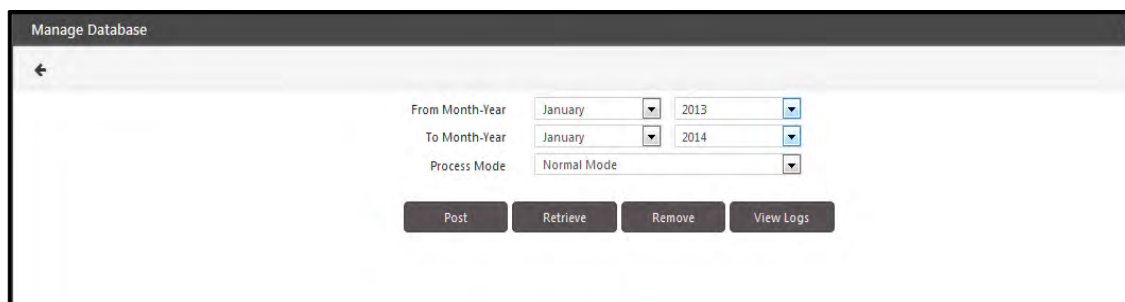
The screenshot shows a 'Message Board' window with a 'General' message. The message text is: 'Matrix provides Surveillance and Telecom Solution.' At the bottom of the window, there are three buttons: Notice, News, and General.

You can click on Notice and News button to read the respective message.

Manage Database

Manage Database allows the posting, retrieval and erasing of data from the database. The Post/Retrieve/Remove request is submitted in a queue which will be processed on server side in a parallel manner.

To access this functionality, go to **Admin Module > System Utilities > Manage Database** and the following screen appears.



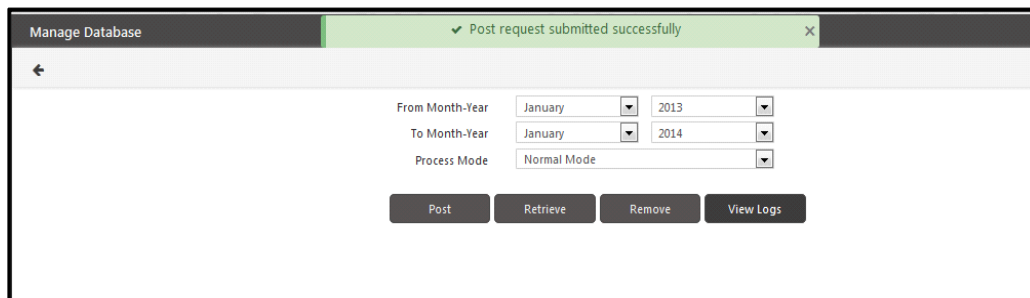
The screenshot shows the 'Manage Database' window. It contains three dropdown menus: 'From Month-Year' (set to January 2013), 'To Month-Year' (set to January 2014), and 'Process Mode' (set to Normal Mode). Below these are four buttons: 'Post', 'Retrieve', 'Remove', and 'View Logs'.

Select the **From month- year** as well as the **To month-year** whose data is to be posted. This functionality removes the transactions of the selected period from the current transaction table and posts it to another table thus reducing the load on the current transaction table.

Select the **Process Mode** as Normal mode or Advanced mode (overwrite destination).

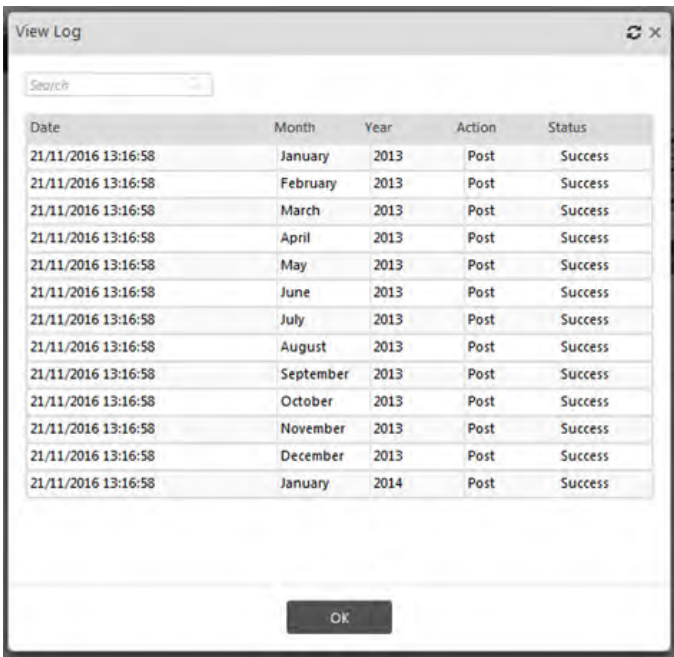
Click on the **Post** button. The utility will post the data to the backup table and will display the status in the bottom grid.

The Post request with log details is shown as below.



This screenshot shows the same 'Manage Database' window as before, but with a green notification bar at the top stating '✓ Post request submitted successfully'. The dropdown menus and buttons remain the same.

Click on the **View Log** button to view the status of the transaction.



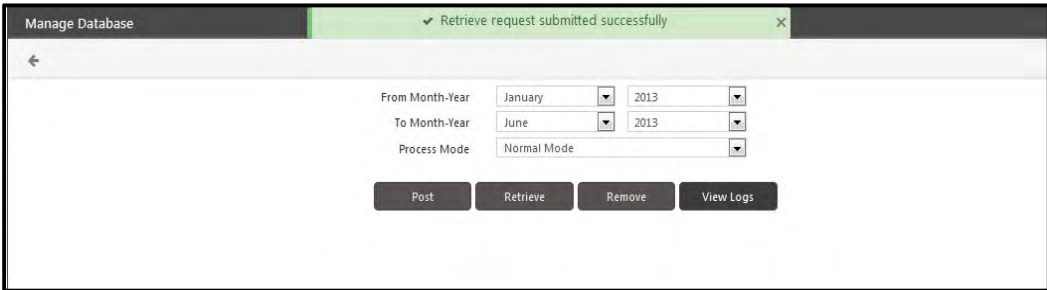
The 'View Log' window displays a table with the following data:

Date	Month	Year	Action	Status
21/11/2016 13:16:58	January	2013	Post	Success
21/11/2016 13:16:58	February	2013	Post	Success
21/11/2016 13:16:58	March	2013	Post	Success
21/11/2016 13:16:58	April	2013	Post	Success
21/11/2016 13:16:58	May	2013	Post	Success
21/11/2016 13:16:58	June	2013	Post	Success
21/11/2016 13:16:58	July	2013	Post	Success
21/11/2016 13:16:58	August	2013	Post	Success
21/11/2016 13:16:58	September	2013	Post	Success
21/11/2016 13:16:58	October	2013	Post	Success
21/11/2016 13:16:58	November	2013	Post	Success
21/11/2016 13:16:58	December	2013	Post	Success
21/11/2016 13:16:58	January	2014	Post	Success



Data posting cannot be done for data of the last three months, for posting data select the time period before three months.

The **Retrieve** functionality restores the transactions of the selected month from the backup table to the current transaction table and is thus the reverse of the Posting process.



The 'Manage Database' window shows a green status bar: 'Retrieve request submitted successfully'. Below, there are dropdowns for 'From Month-Year' (January 2013) and 'To Month-Year' (June 2013), and a 'Process Mode' dropdown (Normal Mode). At the bottom are buttons for 'Post', 'Retrieve', 'Remove', and 'View Logs'.



The 'View Log' window displays a table with the following data:

Date	Month	Year	Action	Status
21/11/2016 14:45:18	January	2013	Retrieve	Success
21/11/2016 14:45:18	February	2013	Retrieve	Success
21/11/2016 14:45:18	March	2013	Retrieve	Success
21/11/2016 14:45:18	April	2013	Retrieve	Success
21/11/2016 14:45:18	May	2013	Retrieve	Success
21/11/2016 14:45:18	June	2013	Retrieve	Success
21/11/2016 13:16:58	January	2013	Post	Success
21/11/2016 13:16:58	February	2013	Post	Success

The **Remove** option permanently deletes the transactions of the selected month from the table.



If Process mode is selected as **Normal**, then on clicking **Post**, the data which are already present in Backup table will be skipped when data are transferred. If the Process Mode is selected as **Advance**, then on clicking **Post**, the data which are already present in Backup table will be overwritten when data are transferred.



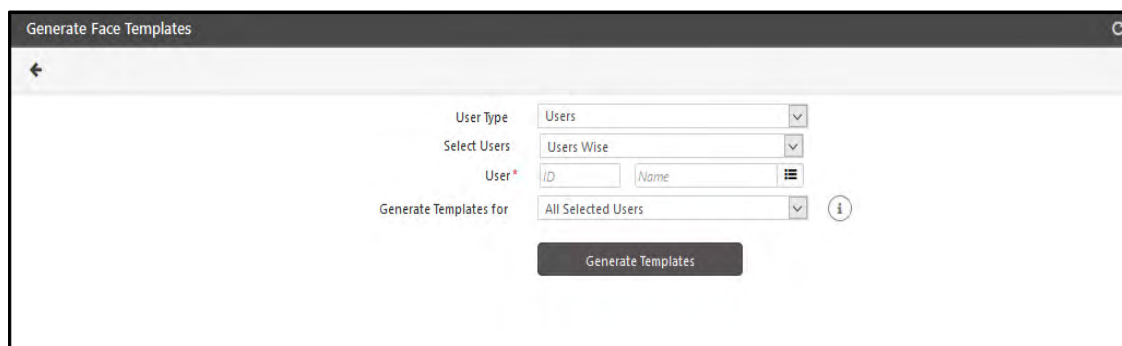
If Process mode is selected as **Normal**, then on clicking **Retrieve**, the data which are already present in Current table will be skipped when data are transferred. If the Process Mode is selected as **Advance**, then on clicking **Retrieve**, the data which are already present in Current table will be overwritten when data are transferred.

Generate Face Templates

When Matrix FR algorithm is to be used for identification process, it requires face templates for identification and recognition process. So if the images are converted into templates during enrollment of faces, then it reduces the duration required for template conversion at Identification Service restart.

This page enables to convert face into templates.

To access this functionality, go to **Admin Module > System Utilities > Generate Face Templates** and the following screen appears.

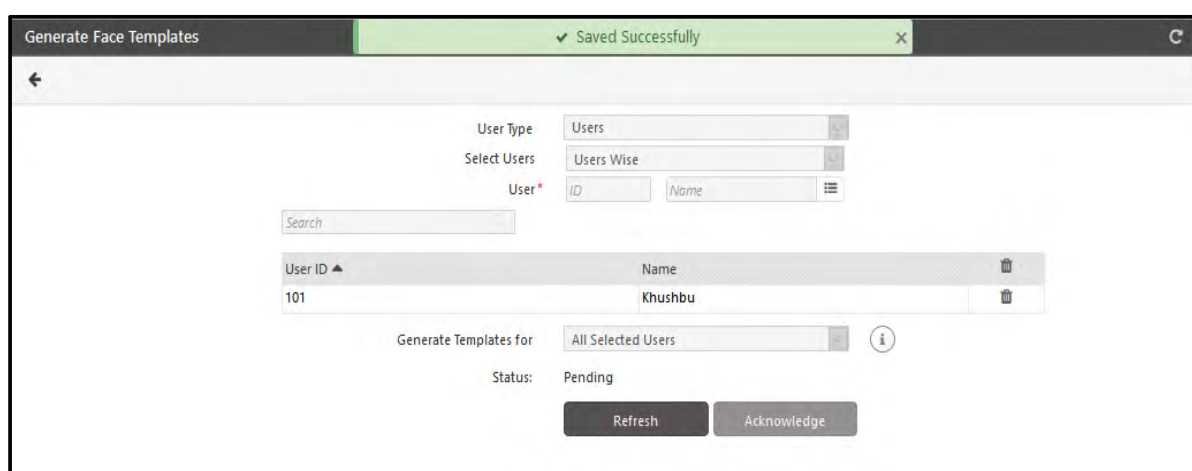


User Type: Select the User type as Users, Visitors or Both.

Select Users/Visitors: Based on selection of User Type, select the User, Visitor or Both individually, Group wise or All. The picklist will contain only FR enables user/visitor.

Generate Templates for: Select the option for generating template for All Selected Users or Differential Users. Selecting Differential Users will generate templates for users out of selected users, whose templates have not been generated previously.(For Users displayed in the error list)

Then click on **Generate Templates** button to process the conversion of enrolled faces into templates.



On start of Alert Service, it will pick up the records that are in pending state and the records change to "In Progress" state. If the process of generating templates is complete, the status is displayed as "Process Completed".



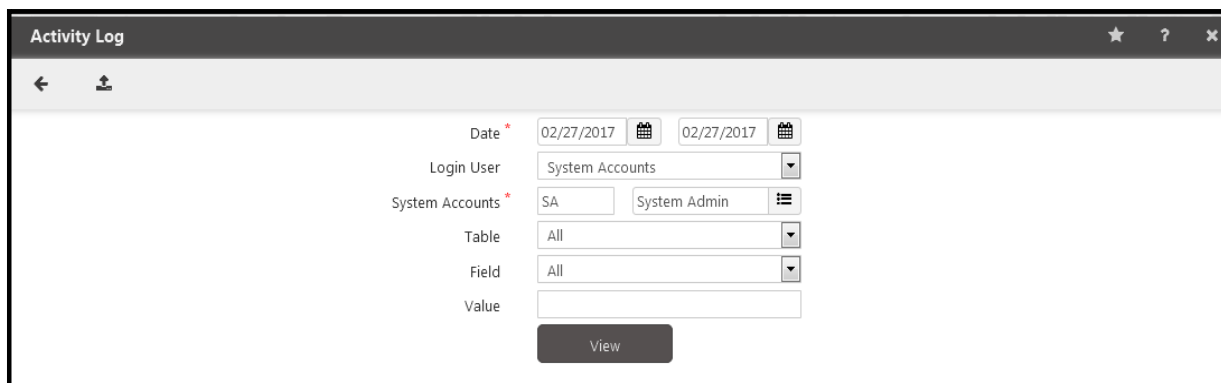
Generate Face Templates is not tested in 32 bit Computer

Activity Log

This option enables the user to view activity logs which provide information about all the actions performed by login users with key field information. The system thus maintains an audit trail of all actions performed by the Login users and this information can be viewed by the system administrator.

To view the activity logs,

1. Go to the **Admin module > Views/Logs > Activity Log** and the following screen appears.



2. Select the time period for which the activity log is to be displayed by defining the start and the end **date**.
3. The other three filtering options available for viewing the audit trail are as follows:
 - **Login User:** Select the Login user whose activities need to be displayed. Available options for Login User are: All, System Accounts, User.
 - **User/System Accounts:** For the Login User type selected, specify a user/System Accounts from the user picklist. The Label will be changed to **System Accounts** in case of Login User = System Accounts as shown in the screenshot above.
 - **Table:** Select the data table for which you would like to view the change history.
 - **Field:** Select the field for which you would like to view the change history. User can Select the field from the drop down list and specify the Value for the field as an additional filtering criteria.
4. Click the **View** button.

The following screenshot illustrates an *Activity Log* for a system administrator:

Activity Log

←

⬆

Date *

02/27/2017

02/27/2017

Login User

System Accounts

System Accounts *

SA

System Admin

Table

All

Field

All

Value

View

Search

Q

User ID	Date ▼	Action	Table	Key Field	Key Value	Host IP	Details
SA	02/27/2017 17:30:33	Add	Project Phase Detail	Project Code	open	192.168.104.13	⋮
SA	02/27/2017 17:30:29	Add	Phase Master	Phase ID	10	192.168.104.13	⋮
SA	02/27/2017 17:28:12	Edit	Leave Credit Policy Master	LCPLCID	5	192.168.104.15	⋮
SA	02/27/2017 17:27:53	Edit	Leave Credit Policy Master	LCPLCID	5	192.168.104.15	⋮
SA	02/27/2017 17:27:24	Edit	Leave Credit Policy Master	LCPLCID	5	192.168.104.15	⋮

1 - 5 of 1034 records

«

<

1

2

3

...

207

>

»

You can click the **Details** icon to view detailed information of each entry.

Detail Information

Search

Q

Field ▲	Old Value	New Value
Type		7
Panel ID		11
Home zone ID		1
VIP Feature Enable		0
Access Group ID		1
Functional Group ID		1
Absentee Rule Enable		0
Max Absent Allowed		60
Ref Index		11
Enable		1

1 - 10 of 15 records

«

<

1

2

>

»

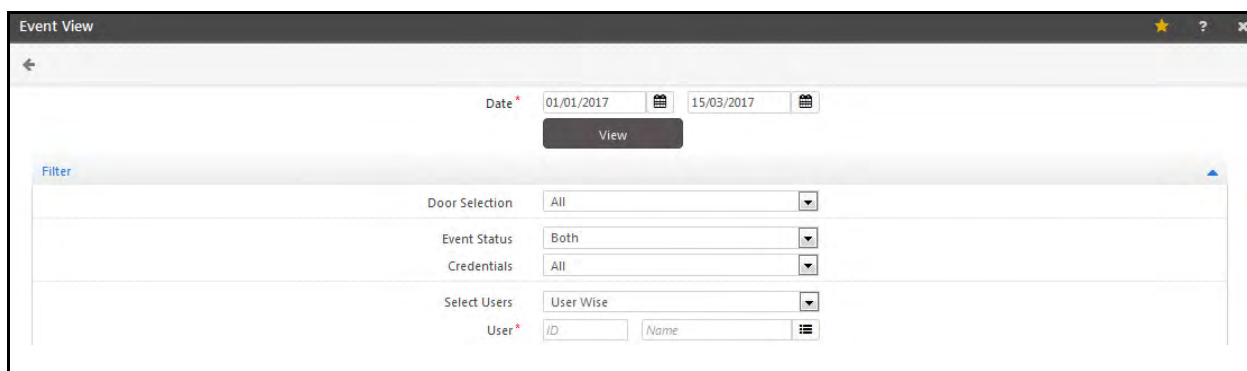
Close

Event View

The COSEC system interfaces with specific video recorder devices such as the *Matrix HVR/NVR* and enables the user to grab images triggered by user events at the respective doors. Doors such as the *NGT door controller* also have a built-in camera which can be configured to capture user images based on an event trigger. To know more about configuring doors for *Visual Tagging*, refer to “[Device List](#)”. These user events and related images can be viewed using the **Event View** option under the *Admin* module.

To access this feature,

Go to **Admin module > Views/Logs > Event View** and the following screen appears.

The screenshot shows the 'Event View' web application interface. At the top, there's a title bar with 'Event View' and standard window controls. Below the title bar, there's a search bar with a magnifying glass icon. The main content area is divided into two sections. The top section contains date selection fields: 'Date' with a red asterisk, followed by two date pickers showing '01/01/2017' and '15/03/2017', and a 'View' button. The bottom section is titled 'Filter' and contains several dropdown menus: 'Door Selection' (set to 'All'), 'Event Status' (set to 'Both'), 'Credentials' (set to 'All'), and 'Select Users' (set to 'User Wise'). Below these, there's a 'User' section with a red asterisk, followed by 'ID' and 'Name' input fields, and a list icon.

On the **Event View** page, specify a date range using the **Date** fields, for which user event records are to be retrieved.

Filter

You can filter the Event view by configuring the following fields in the **Filter** section:

Door selection: Select the doors for which events are to be viewed.

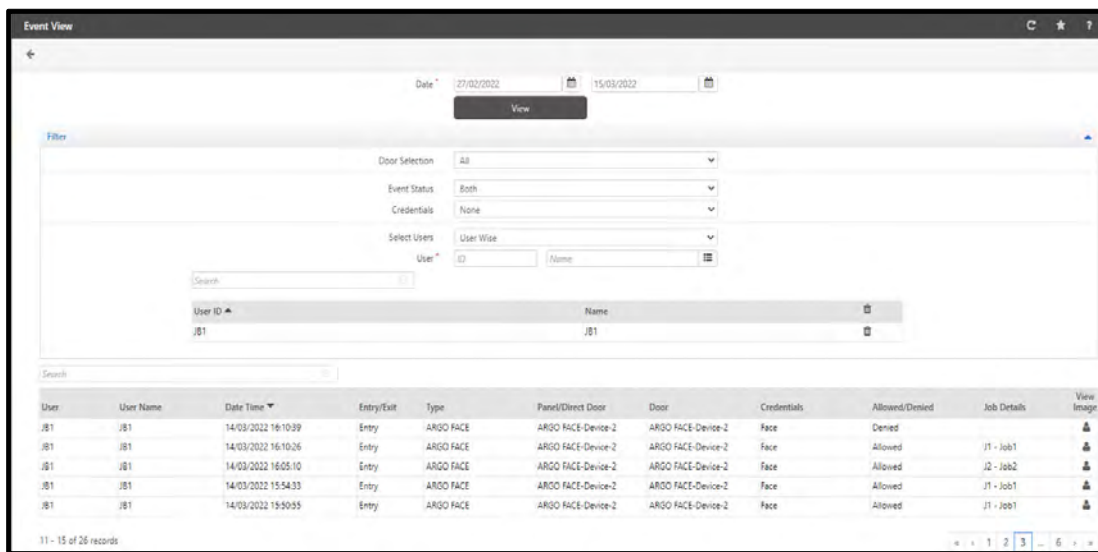
Event Status: Select the event status to view events which are Allowed, Denied or Both.



Credentials: Select the option to view events based on the type of credentials used.

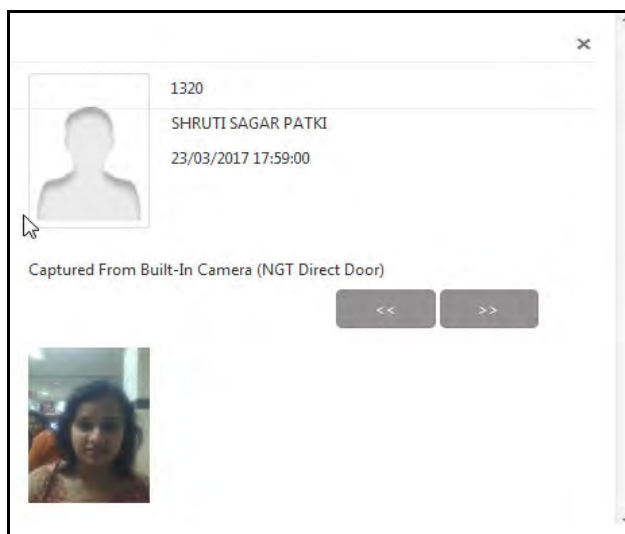
Select Users: Select the users for whom events are to be viewed. You can select users from the option: User wise, Group Wise and ALL.

Click the **View** button.

A detailed list of all specified events is displayed in the grid as shown in the screen below.



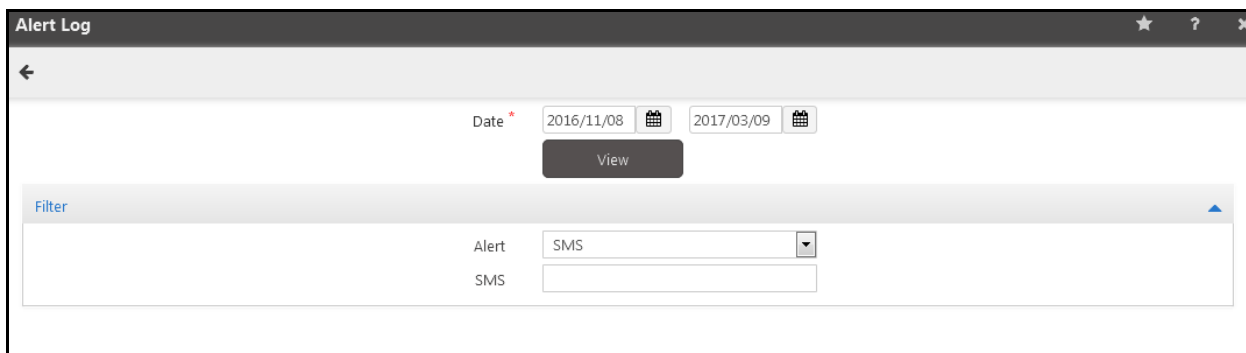
Click on the  icon under the **View Image** column against the relevant user event and view the associated snapshot image, if available. Click on the  button to view images captured for the successive events.



Alert View

This tab enables the user to view alert logs generated by the SMS and E-mail alerts on the COSEC system.

To view alert logs Go to **Admin module > Views/Logs > Alert View** and the following screen appears.



The screenshot shows the 'Alert Log' window. At the top, there's a title bar with a back arrow, a star, a question mark, and a close button. Below the title bar, there's a date selection area with two date pickers: '2016/11/08' and '2017/03/09', each with a calendar icon. A 'View' button is centered below the date pickers. Below the 'View' button is a 'Filter' section. The 'Filter' section has a dropdown menu for 'Alert' set to 'SMS' and a text input field for 'SMS'.

Select the time period for which the alert log needs to be displayed by defining the **start** and the **end date**.

Expand the **Filter** panel to set the following:

- **Alert:** Select **SMS** or **E-mail** as the alert mode for which the log is to be viewed.
- **SMS/E-mail ID:** Depending on the alert selected, an additional filter can be applied on the log view in the form of a specific sms or e-mail address.

Click the **View** button.

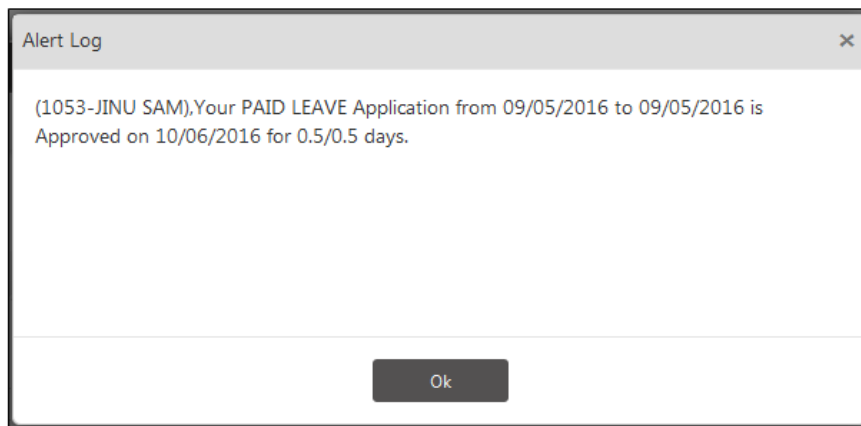
The system displays the logs of all the alerts which meet the specified filter criteria as shown in the following screen.

Phone Number ▲	Message	Date Time	Error/Status
09687204569	(1053 - JINU SAM), Your PAID LEAVE Application from 09/05/...	10/06/2016 17:07:40	
09765727827	(1053 - JINU SAM), Your PAID LEAVE Application from 09/05/...	10/06/2016 17:07:40	
9327736565	1053 - JINU SAM has Applied TOUR from 10/06/2016 to 10...	10/06/2016 11:56:48	
9327736565	1053 - JINU SAM has Applied TOUR from 09/05/2016 to 10...	10/06/2016 11:57:11	
9327736565	1053 - JINU SAM has Applied TOUR from 10/03/2016 to 10...	10/06/2016 11:57:32	

1 - 5 of 10 records

1 2

- Double click on an entry in any of the columns except the **Date Time** column to get a detailed view of the content as shown below.



Scheduler Log

The Scheduler Log enables the user to view details of all scheduled **tasks** and **reports** in the COSEC system for a defined date range. These details include the scheduling and completion status of all report and task schedules.



This section displays the logs of the **Task Scheduler** or **Report Scheduler** created from the path: **Admin Module > System Utilities > Task/Report Scheduler**.

To view Scheduler Logs, Go to **Admin module > Views/Logs > Scheduler Log** and the following screen appears.

Date: Select the time period for which the scheduler log needs to be displayed by defining the start and the end Date.

Filter

Expand the **Filter** panel to set the following parameters:

Scheduler Activity - Select an activity (such as Leave Credit, Blocked User, etc) to filter the scheduler log for specific results.

Status - Select a **Status** type for the scheduled activity from the dropdown list. The options available are: Succeed, Failed and Both.

Click the **View** button.

The *Scheduler Log* appears in a grid as shown in the figure below.

Scheduler Log

← ↑

Date * 01/01/2017 28/03/2017 View

Filter

Scheduler Activity All

Status Both

Search

Task/Report Name	Scheduled Date-Time	Completion Date-Time	Status	Status Description
Cafeteria users CSV Weekly	08/02/2017 16:00	08/02/2017 16:00	Succeed	
Cafeteria Sales XLS Weekly	08/02/2017 17:00	08/02/2017 17:00	Succeed	
Cafeteria Credit debit CSV Wee	08/02/2017 17:00	08/02/2017 17:01	Succeed	No Data Found
Visitor history XLSWeek	08/02/2017 19:00	08/02/2017 19:00	Succeed	
Visitor history XLS Week	08/02/2017 19:00	08/02/2017 19:00	Failed	

121 - 125 of 503 records

« < 1 ... 101 > »

You can also Export the Scheduler Logs in the **xls format** by clicking on the **Export** button as shown with the arrow above.

The Scheduler Logs will be saved in xls format as shown below:

SchedulerLog_export [Protected View] - Microsoft Excel

Protected View This file originated from an Internet location and might be unsafe. Click for more details. Enable Editing

	A	B	C	D	E	F
	Task/Report Name					
60	Cafeteria Sales PDF	2017/02/07 10:00	2017/02/07 10:00	Succeed		
61	Cafeteria USer PDF	2017/02/07 10:00	2017/02/07 10:00	Succeed		
62	Visitor history PDF Week	2017/02/07 10:00	2017/02/07 10:00	Succeed	No Data Found	
63	Visitor Expired PDF	2017/02/07 10:00	2017/02/07 10:00	Succeed		
64	Cafeteria Blocked users	2017/02/07 11:00	2017/02/07 11:00	Succeed	No Data Found	
65	Relieving User Sch Deacti	2017/02/07 11:00	2017/02/07 11:00	Succeed	Users not found for Process	
66	VM	2017/02/07 12:00	2017/02/07 12:00	Failed		
67	Visitor history CSV Week	2017/02/07 12:00	2017/02/07 12:00	Succeed		
68	Visitor history XLS Week	2017/02/07 12:00	2017/02/07 12:00	Failed		
69	Visitor head Count XLS	2017/02/07 12:00	2017/02/07 12:00	Succeed		
70	Relieving User Sch Delete	2017/02/07 12:00	2017/02/07 12:00	Succeed	Users not found for Process	
71	new invalid events	2017/02/07 12:10	2017/02/07 12:10	Failed		
72	Relie User Sch De-act	2017/02/07 12:30	2017/02/07 12:30	Succeed	Users not found for Process	
73	Cafeteria Headcount PDF	2017/02/07 13:00	2017/02/07 13:00	Failed	Incorrect syntax near ')	
74	Cafeteria Sales CSV	2017/02/07 13:00	2017/02/07 13:00	Succeed		
75	Visitor head count CSV	2017/02/07 15:00	2017/02/07 15:00	Succeed		
76	Visitor Expired CSV	2017/02/07 15:00	2017/02/07 15:00	Succeed		
77	Cafeteria users CSV	2017/02/07 16:00	2017/02/07 16:00	Succeed		
78	Cafeteria Sales XLS	2017/02/07 17:00	2017/02/07 17:00	Succeed		
79	Cafeteria Credit debit CSV	2017/02/07 17:00	2017/02/07 17:01	Succeed	No Data Found	
80	Visitor history XLSWeek	2017/02/07 19:00	2017/02/07 19:00	Succeed		

Sheet1

Ready

License Information

The page displays the license information of the COSEC web application.

To view the license details, Go to **Admin module > License Information** and the following screen appears.

License Information

Product Variant: COSEC PLT

License Key: 3B86-2228-B22D-06A2-06B0-A690-43C6-9F41-6DB0-0821-B4B2-C9E8-5508-0499-4580-A412-9609-0B40-4

License Details

Annual Upgrade Package Validity: October-2018

Module	Current Usage	Allowed Limit
Platform Users	4	100000
ACM Users	4	100000
CMM Users	0	100000
VMM Users	2	100000
TAM Users	2	100000
CWM Users	1	100000
JPC Users	0	100000
FVM Users	0	100000
ESS Users	1	100000
FR Users	1	100000

[End User License Agreement](#)

The page displays the existing license profile and lists the following information:

- **Product Variant:** It displays the COSEC product variant licensed to the user. For example: COSEC PLT.
- **License Key:** It displays 56 or 128 (excluding the separators) characters valid license key string.

License Details

- **Annual Upgrade Package Validity:** It displays the Month - Year for the validity of the package after which the package is required to be upgraded.
- **Modules:** It shows the modules in the license along with Current usage and Allowed limit.
 - **Current Usage-** It displays the number of users active in the system.
 - **Allowed Limit-** It is displayed as per the license key.

End User License Agreement- By clicking on this link, you can read the end user license agreement.

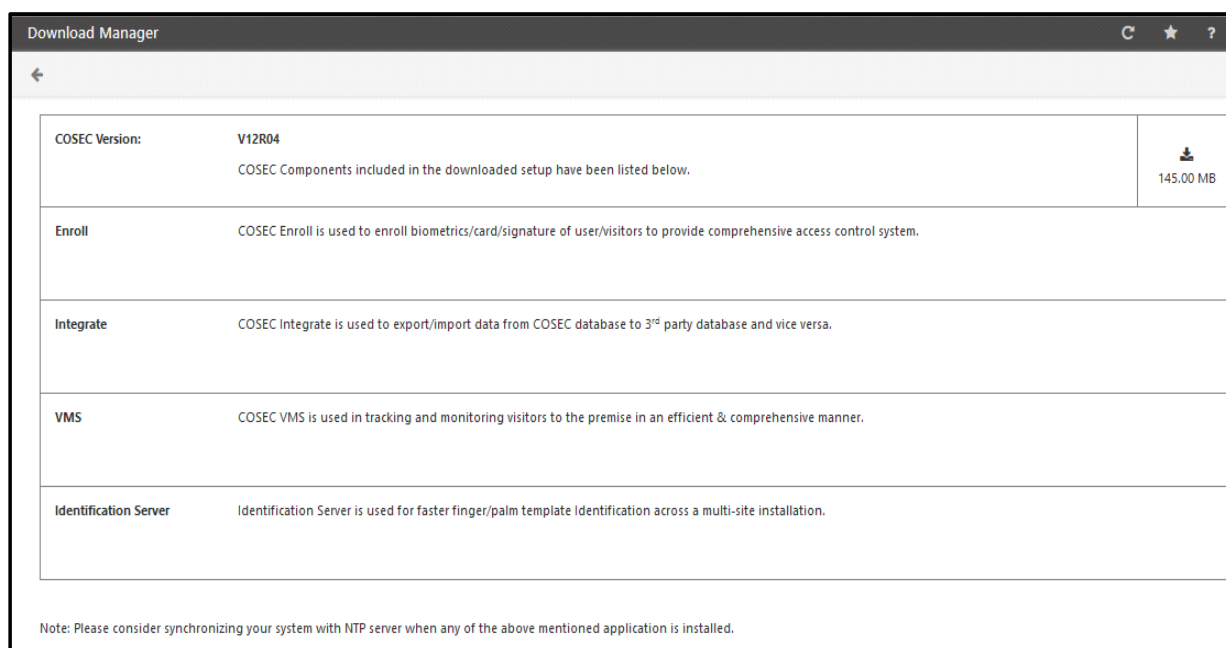
Download Manager

Download Manager is a page that enables to download COSEC Enroll, COSEC Integrate, COSEC VMS and Identification Server applications. Before installing the COSEC applications refer, “[System Requirements](#)” to ensure the prerequisites are fulfilled.



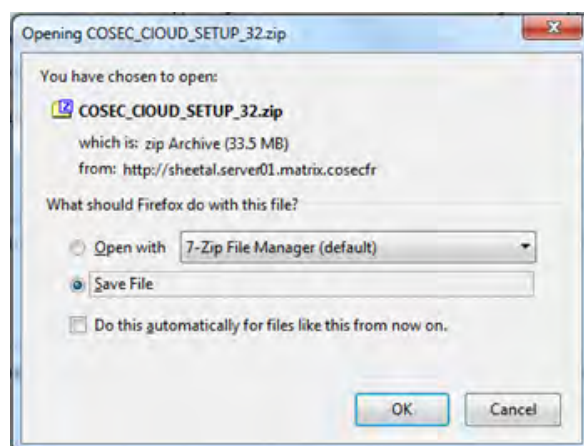
After the installation, if you are upgrading the IDS, Enroll, VMS, or Alert Services from the Service Tray App (refer to the Services User Guide to know more) you will need to update the FR libraries manually. To do so,

- Copy the desired FR files from the downloaded package, that is from MxFRSDK > MxFRSDK_x64_CPU or MxFRSDK_x64_GPU.
- Paste the same into the respective library folder in the setup folder in your local PC.

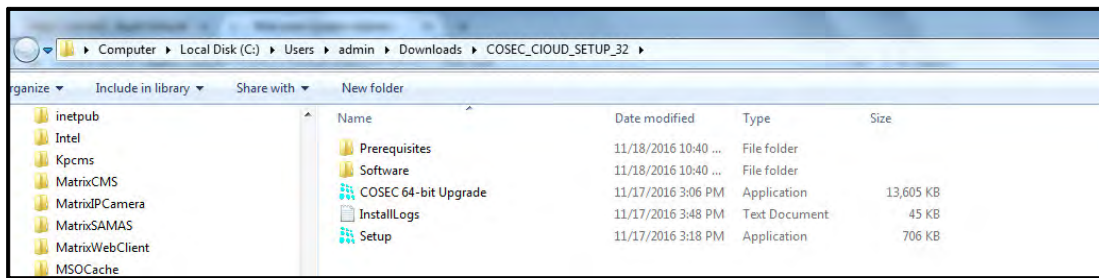


To install any of the above applications click  download icon.

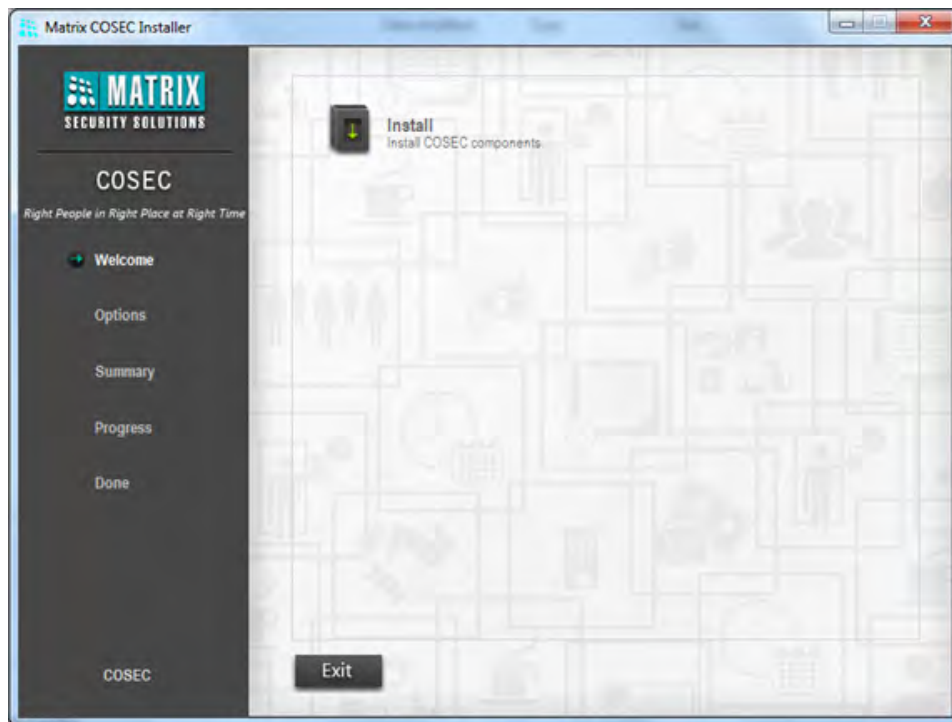
The Cloud download Setup window appears as shown below.



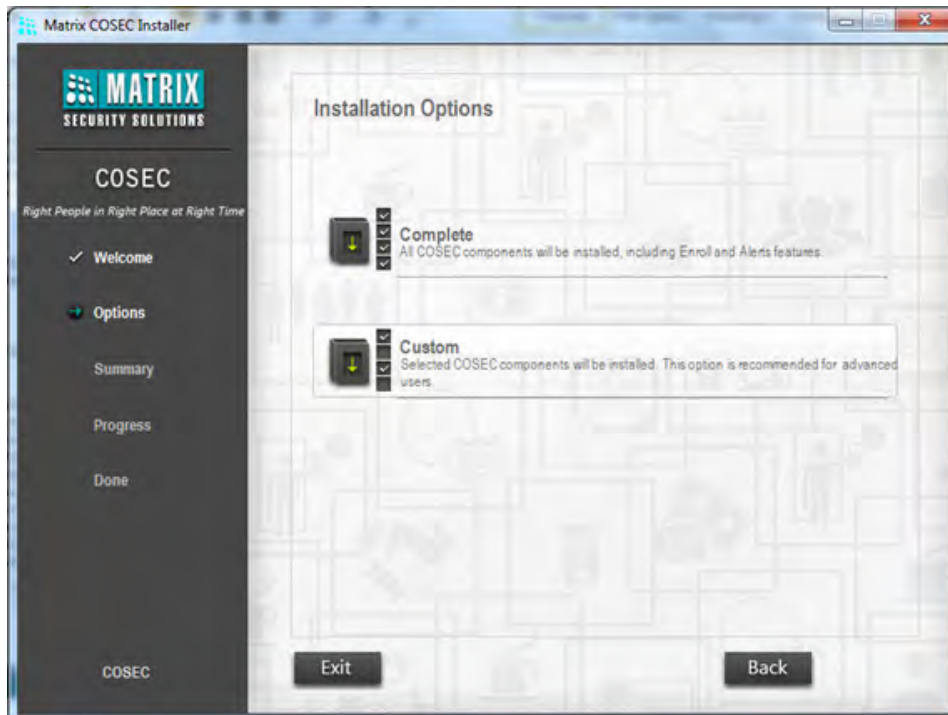
Open the Zip folder or Save the folder. Open the folder as shown below.



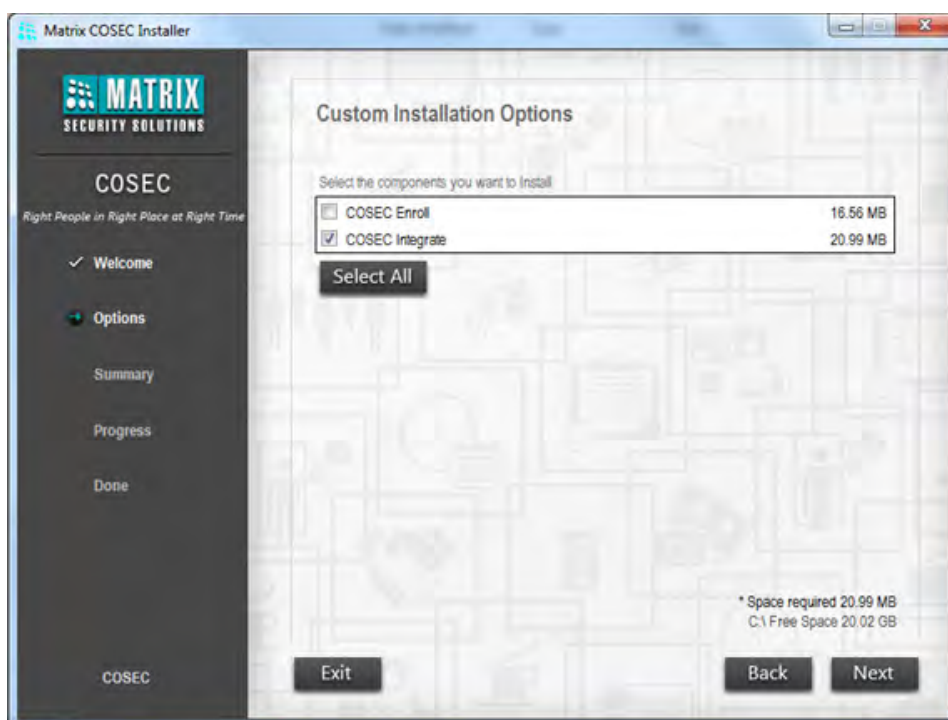
Click on Application Setup. The COSEC Installer is shown as below.



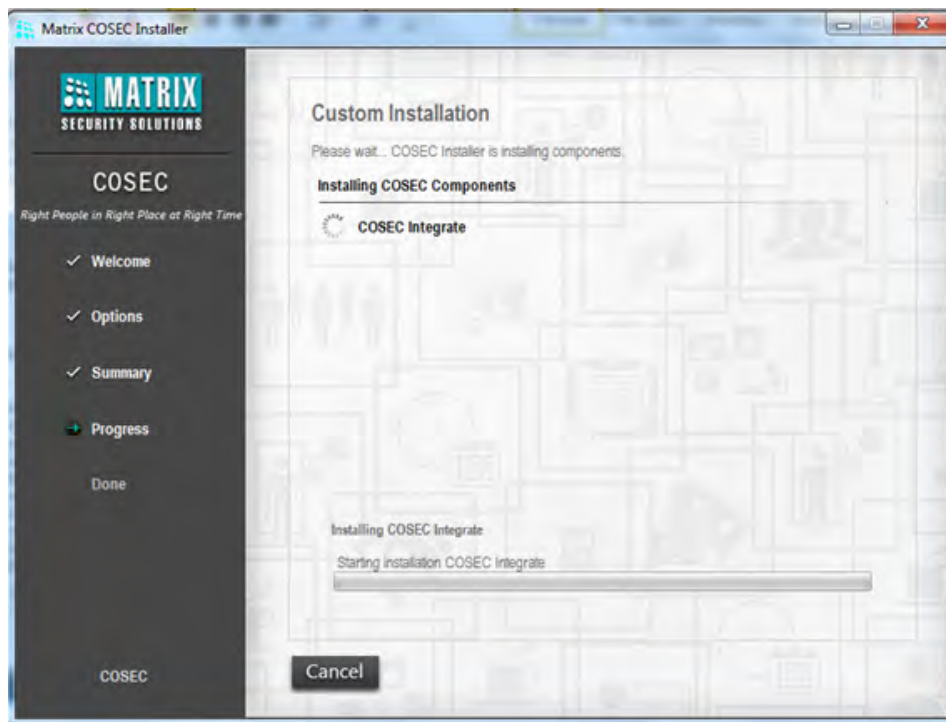
Click Install. The Installation options are shown as below.



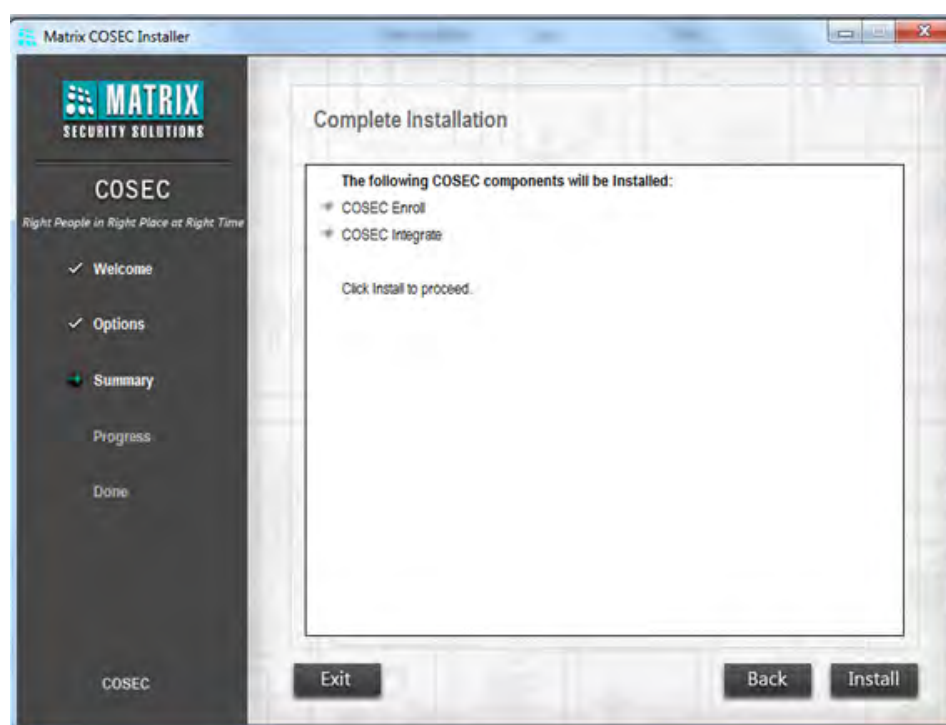
You can select the Custom option and select the desired component to be installed.

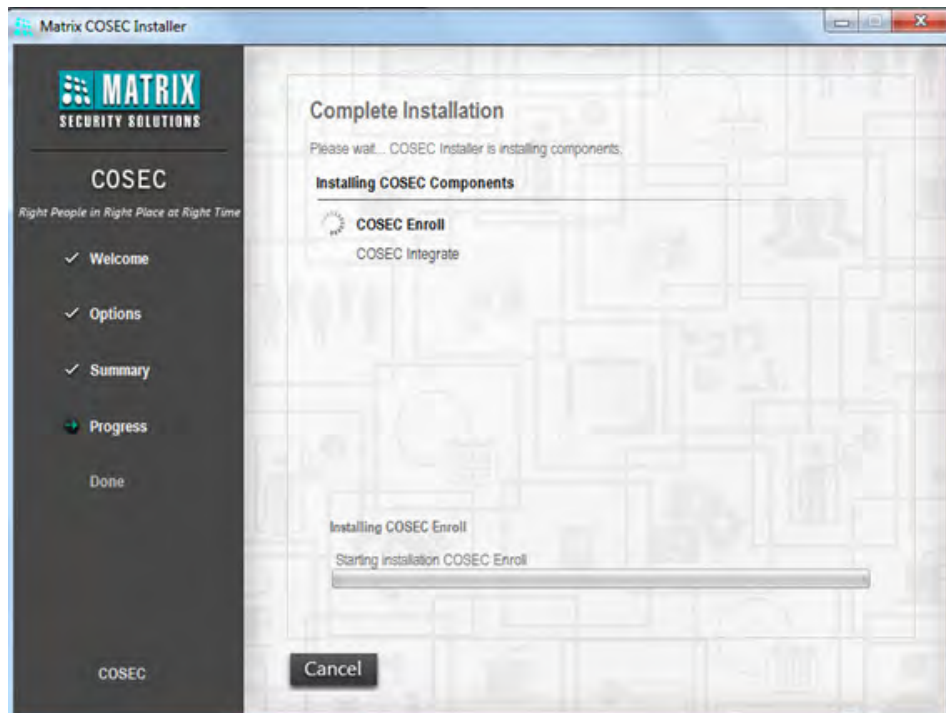


After selecting a component, click Next to install. The Custom Installation is shown as below.

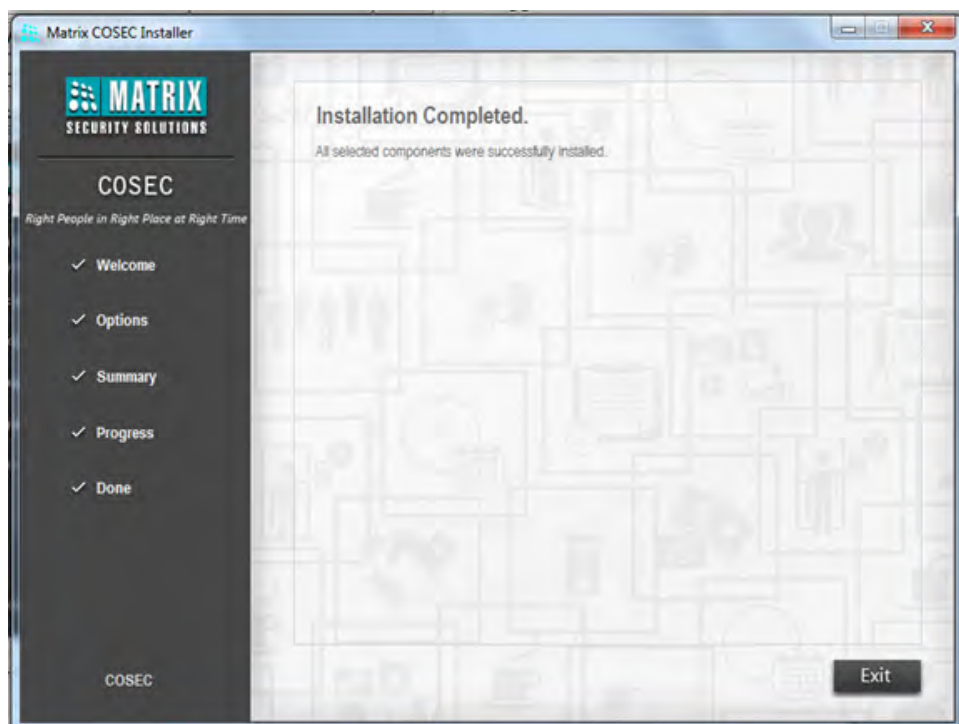


The Complete Installation is shown as below.





After completing the installation, Installation Completed window will be shown as below.

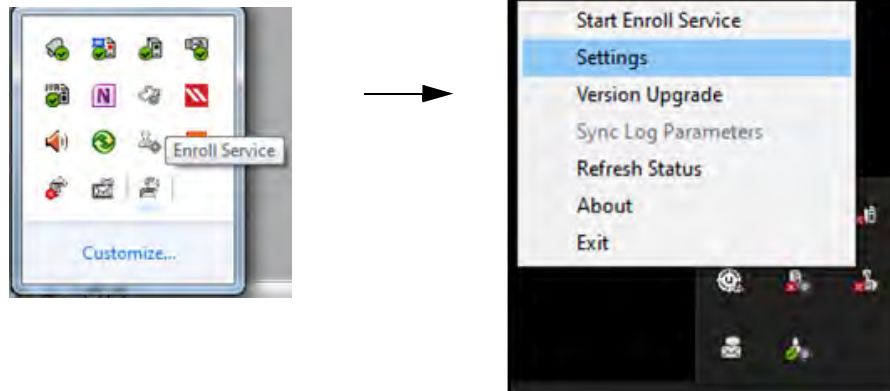


Enroll Service

After the Installation, a shortcut icon  will be created on your desktop.

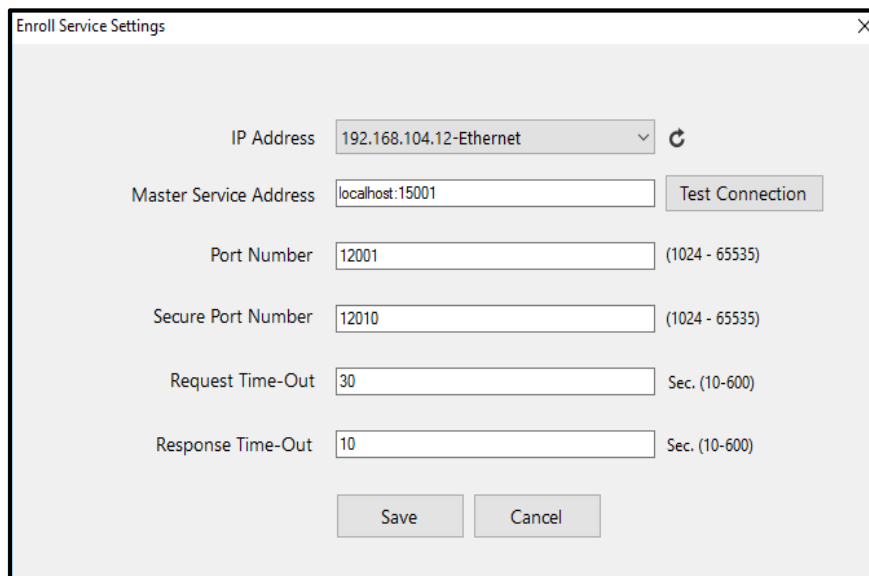
Also you can start the Enroll Service Application by browsing the folder from **All Programs> Matrix> Enroll Service**.

When the Enroll Service is started, an icon will be visible in the system tray as shown below. Then Right click on icon to configure the settings and start the service.



If the service entry is not found on general settings table then service will self-register itself. When Master Service URL in Tenant Portal> System Configuration > General Settings is blank then service will self-register itself.

At the time of self-registration MAC-Address, IP Address, URL (generated), Port Number and Domain Name from general settings should be passed as parameters.

The image shows a dialog box titled 'Enroll Service Settings'. It contains several input fields and buttons. The fields are: 'IP Address' with a dropdown menu showing '192.168.104.12-Ethernet' and a refresh icon; 'Master Service Address' with a text box containing 'localhost:15001' and a 'Test Connection' button; 'Port Number' with a text box containing '12001' and a range '(1024 - 65535)'; 'Secure Port Number' with a text box containing '12010' and a range '(1024 - 65535)'; 'Request Time-Out' with a text box containing '30' and a range 'Sec. (10-600)'; and 'Response Time-Out' with a text box containing '10' and a range 'Sec. (10-600)'. At the bottom are 'Save' and 'Cancel' buttons.

Master Service Address: Enter the IP Address or URL of the Master Service.

On Changing / Updating the Master Service Address, connection should be tested with the master service on click of Test Connection button. Eg: localhost:15001

Click **Test Connection** to test the connection with Master service.

Port Number: This is the port number of the computer at which device will do enrollment.

Secure Port Number: This is the port number of the computer at which device will do enrollment.


Specify the **Request time-out** duration in seconds.

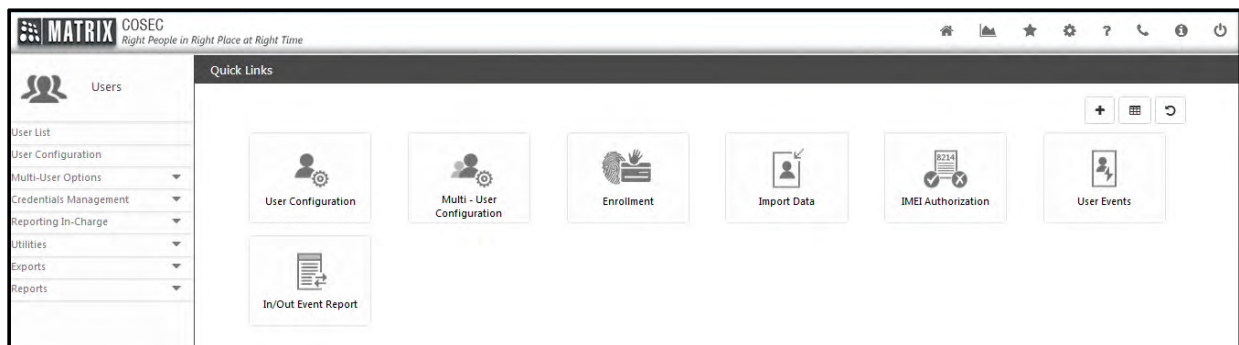
Specify the **Response time-out** duration in seconds.

Click **Save** button to save the settings.



User Configuration is a consolidation of the user information at one place to manage and to obtain details whenever needed. It enables the creation of a user database that allows the system to consider the configured user as a valid user of the system.


It is necessary to create a user database that shall have the information about him/her like employee ID, general details, personal details, access privileges detail, contact details etc. Having the user details organized makes it simpler to manage the system and the details of any user can be obtained whenever needed.

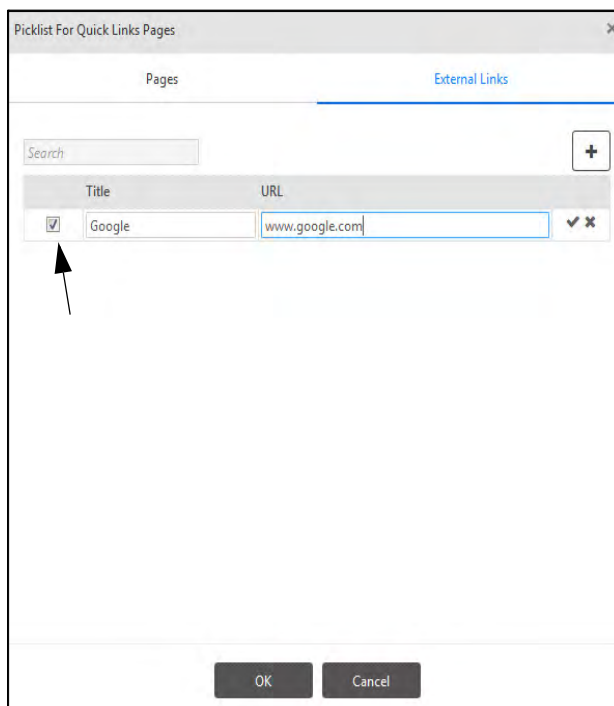
To access the **Users** module with the COSEC Web Application, select the **Users**  icon on the module selection page. The **Users** page will appear on your screen as shown below.



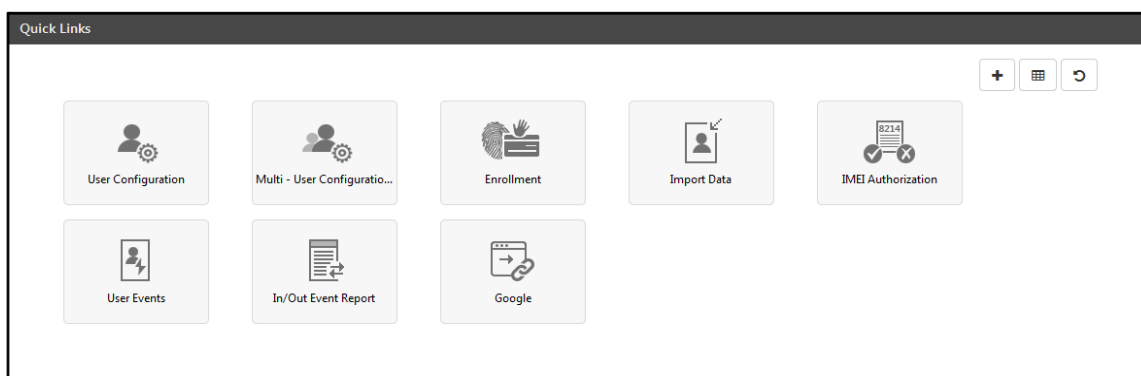
The page displays a menu and **Quick Links** to go to the required page in just one click. Quick Links are shortcuts to reach to a specific page easily. It also contains following three buttons:



- **Add Quick Link:** Click  button to add a quick link. A picklist for Quick Link pages appears for selecting the page or External Link for which the quick link is to be created. Maximum **20** quick links can be added.
- For Adding **Pages** in Quick Link, Select the Pages and click on OK
- For Adding **External Links**, Select External Link tab, click on  button to add new external link.

- Configure the **Title** and **URL** of the external link under the respective fields. click on checkbox to get the configured link on quick link screen as shown below. To save the configuration click on .



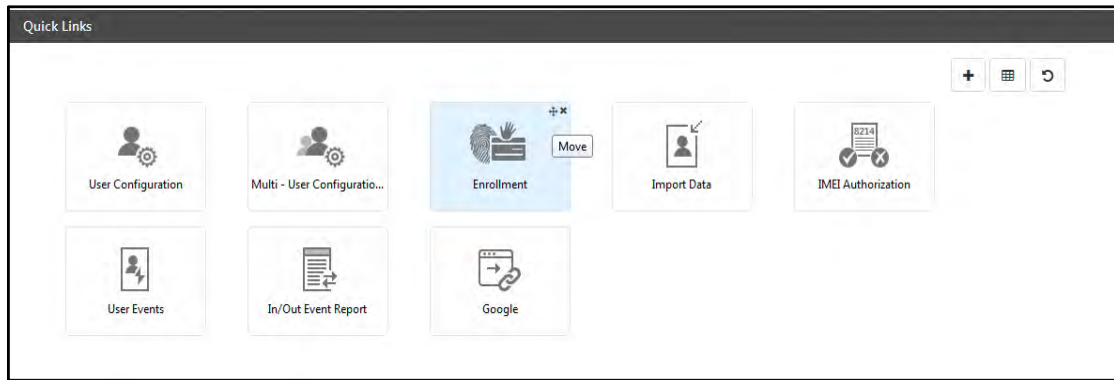
- To edit the saved configuration, click on .
- Click on OK to save the link configuration on Quick Link screen. The external link will be displayed as shown below:



- **Select Layout:** Click  button to select a layout for the quick links. You can select 5x4 or 4x5 layout to manage the quick links.
- **Reset Quick Links:** Click  button to reset the quick links to the default quick links.

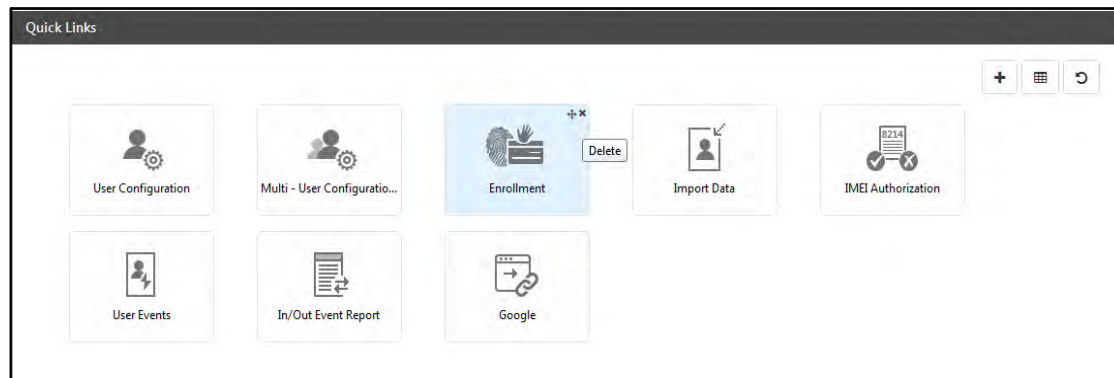
Move the Link

To move the link from one place to another, hover on the link on top right corner and click on “Move” icon as shown below. Then drag the quick link to the desired place. It will be placed at the desired location on the quick links page.




Delete the Link

To delete a particular link, hover on the link on top right corner and click on “Delete” icon as shown below.




Quick links are displayed as per rights given to System Account and ESS users.

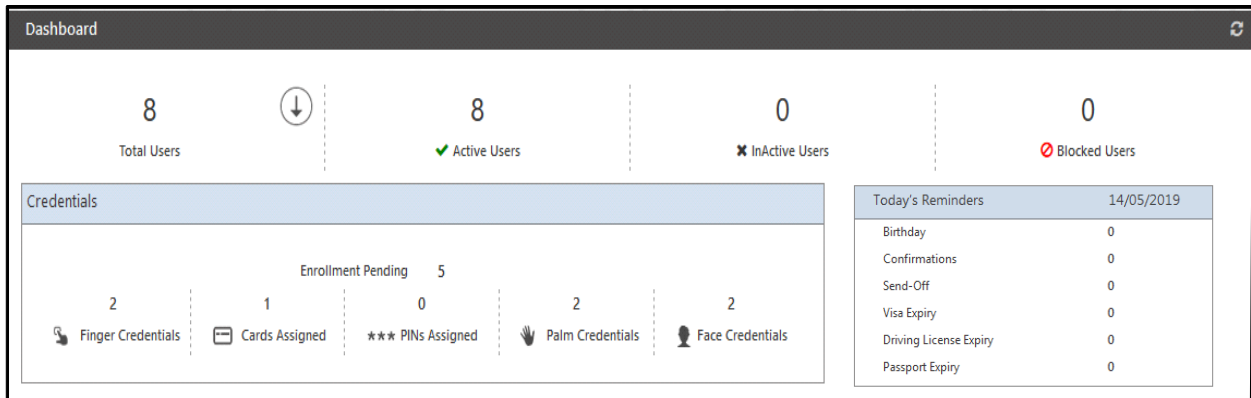
Users Dashboard

To view the Dashboard, click the Dashboard button  on the **Users** page.

It displays the basic information on Users relating to the COSEC Software under three groups:

Users

- Total Users- Total no. of ESS Users (employees) created in COSEC.
-  Click on the Import Users button to go to the Import users page.
- Active Users- Total no. of Users (employees) currently that are active.
- Blocked Users- Total no. of Users (employees) that are blocked.



Enrollment Status

- Enrollment Pending- Total no. of users whose enrollment is not done at all.
- Finger Credentials- Total no. of users with one or more fingers enrolled.
- Cards Assigned- Total no. of users with one or more cards assigned.
- PIN's Assigned- Total no. of users with PIN assigned.
- Palm Credentials- Total no. of users with at least one palms enrolled.
- Face Credentials- Total no. of users whose faces are enrolled.

Reminder

- Birthday- Total no. of users whose birthday is on the current day.
- Confirmations- Total no. of users whose confirmation date is on the current day.
- Send-off- Total no. of users whose leaving date is on the current day.
- Visa Expiry- Total no. of users whose visa expires on the current day.
- Driving License Expiry- Total no. of users whose driving license expires on the current day.
- Passport Expiry- Total no. of users whose passport expires on the current day.

For more information on the above Dashboard options, click the respective information links on the Dashboard. The

Latest values on Dashboard are updated on clicking the Refresh  button.

User List

COSEC allows you to add new users to its database via the Users Module. This functionality can be used by administrators to add new employee information, define employee profiles and contact details.

To define a new user, Select the **Users module > User List**.

The **User List** page opens as follows:

User ID	Name	Short Name	Reference ID	Status
NP	Nisha	Nisha	1783	Active
4	Sweta	Sweta	4	Active
3	Isha	Isha	3	Active
2	Chirag	Chirag	2	Active
1782	Nidhi	Nidhi	1782	Active
1678	Supriya	Supriya	1678	Active
1567	Sheetal	Sheetal	1567	Active
123	123	123	123	Active
101	Khushbu	Khushbu	101	Active
1	Shalini	Shalini	1	Active
07	Aditi	Aditi	7	Active

The User List will display only those users for which rights are assigned to the SA, that is as per the enterprise groups assigned to the users.

For example, if for User1 in Groups, Organization is ORG1 and if the rights for ORG1 are not assigned to the SA, then through the SA login the User List will not display User1.

For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#) as well as [“Group”](#) under [“Configuring Users”](#).

Click the **New** button to add a new user.

The **User Configuration** page will appear as shown below. Also you can directly click on **User Configuration** option from where the user Profile can be configured as described below:

User Configuration

Search User ID or Name

Basic General Personal Contact

ID * 15 chars

Name * 45 chars

Active ☒

Optional

Full Name 200 chars

Short Name * 15 chars

Reference ID * 8 chars

Integration Reference 20 chars

Profile

Devices

Credentials

Group

T&A

Access Control

ESS

Cafeteria

Job Costing

Field Visit Management

The user can be added by entering the ID and Name of the user. Then click on Save button to save the user. The other configurations can be done by selecting the respective tab or section. Then click the edit button to configure the user details.

For more details See [“Configuring Users” on page 382.](#)

User Configuration

Search User ID or Name

Basic General Personal Contact

ID * 3

Name * Sheetal

Active ☒

Optional

Full Name Sheetal Pradip Pandya_Ahmd

Short Name * Sheetal

Reference ID * 3

Integration Reference 20 chars

Profile

Devices

Credentials

Group

T&A

Access Control

ESS

Cafeteria

Job Costing

Field Visit Management

Now once the user gets added, you can view the users in the **Photo view** as shown below:

Configuring Users

COSEC allows you to add new users from the Users Module. This functionality can be used by administrators to add new employee information, define employee profiles and contact details.

The User configuration options can be viewed from:

- *["Profile"](#)*
- *["Adding User Photo"](#)*
- *["Devices"](#)*
- *["Credentials"](#)*
- *["Group"](#)*
- *["T&A"](#)*
- *["Access Control"](#)*
- *["ESS"](#)*
- *["Cafeteria"](#)*
- *["Contract Worker Management \(CWM\)"](#)*
- *["Job Costing"](#)*
- *["Field Visit Management"](#)*
- *["Face Recognition"](#)*
- *["Visitor Management"](#)*
- *["Events"](#)*

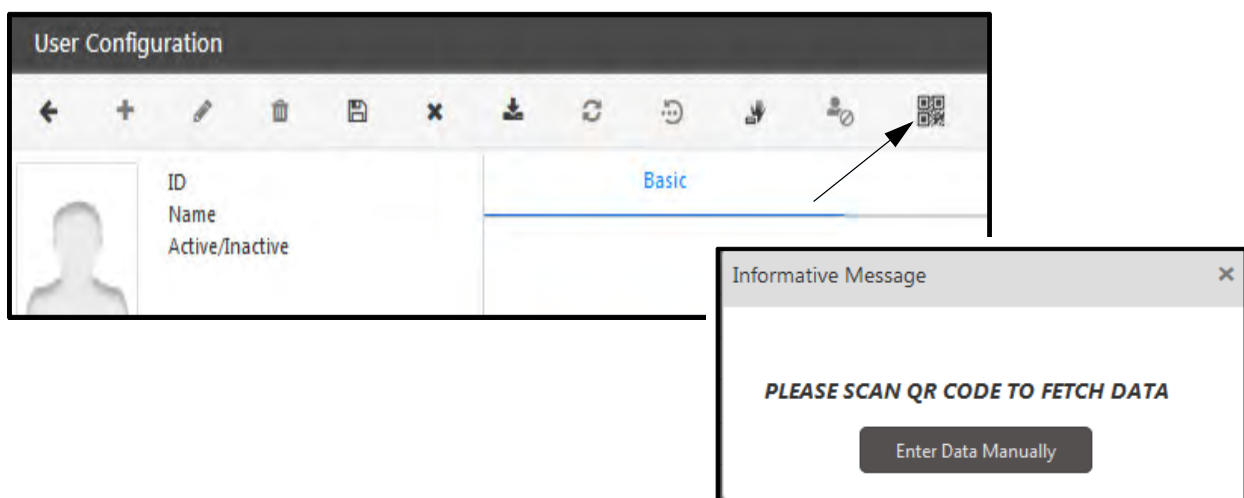
Profile

To configure a User Profile, follow the below steps.

- *“Basic”*
- *“General”*
- *“Personal”*
- *“Contact”*

The details can also be fetched directly from user's Aadhar Card. By Scanning the QR Code of Aadhar Card through 'QR Code Scanner', the information like Name, Gender, DoB, Address etc. available in Aadhar Card will be automatically fetched, and filled into the respective fields of above listed sections.

From the Top menu Bar click on the **QR Code** button and the Pop-up will open as shown below.



Scan the user's Aadhar Card QR through the QR Code scanner or click on the **Enter Data Manually** button to enter the details manually into a pop-up window.

Once the Aadhar Card is scanned and information is received by COSEC Server, the fetched details including Aadhar Number will display as shown below.

×

Aadhaar No.

702351944240

Name

Bindu Singh

Gender

Female

▼

Date Of Birth

15/09/1987

📅

Address

A2-92-Sanidhya Township, Behin

d Dasalad, Ajwa Road, Vadodara

Street

Waghodiya Road

City-Pincode

Vadodara

-

390019

State

Gujarat

Country

India

Father/Spouse Name

Roopnarayan Singh

OK

Cancel

User can edit the details if required.

The Aadhar Number must be unique from existing users to configure a new one.

Click on the **OK** button to Save the details or **Cancel** to cancel the configuration.

Once saved, the details will be placed into the fields of respective sections.

If the Admin has configure QR Code scanning optional then, the above step can be skipped and the details can be added manually as describe below.

384

Matrix COSEC System Manual

Basic

The **Basic** section is displayed as follows:

The screenshot shows the 'User Configuration' window with the 'Basic' tab selected. The sidebar on the left lists various configuration options: Profile, Devices, Credentials, Group, T&A, Access Control, ESS, Cafeteria, Job Costing, Field Visit Management, Face Recognition, and Events. The main content area displays the following fields:

- ID ***: 1687
- Name ***: Aditi Ajay Gupta
- Active**: ☒
- Optional** section:
 - Full Name**: Aditi Ajay Gupta
 - Short Name ***: Aditi Ajay Gupt
 - Reference ID ***: 1687
 - Integration Reference**: 20 chars

The following parameters appear here for configuration:



When Full name of user is entered and Name and Short name are blank then Name will be auto updated with 45 characters of full name excluding special characters and Short name will be updated with 15 characters of full name.

ID - Specify a unique User ID. It can have an alphanumeric value. If the Admin has configured a User ID to be generated automatically then, a user does not need to specify this field. Once the further details are configured and saved, the unique ID will be automatically allocated to the user.

Name - Enter a name in this field that identifies the user (maximum upto 45 characters)

Active - Select this checkbox to activate the user. Whenever a user is made inactive (i.e. **Active** checkbox is unchecked), say, on the last day of employment, the admin will be prompted to choose whether all assigned devices should be revoked from the user or not.

Optional

Full Name- You can also specify the Full name of the user with maximum 200 characters. The supported values are: **A-Z, a-z, 0-9, () , [], _ (underscore), - (Hyphen), . (full Stop), /, &, , (comma), @, ' (single quote), [space]**



A function name followed by (bracket is invalid in full name. Eg: Thomas S/O Round (will be invalid.

Short Name - Specify an alternative short name for the user which will be displayed on the COSEC doors whenever there is an event related to this user. (maximum up to 15 characters).

Reference ID - The system allots a random sequential Reference Code based on the last reference code allotted (numeric value with a maximum of 8 digits). This option is used to provide a linkage ID in the event of an organization using a different user ID format in another software application for e.g. the payroll application.

Integration Reference - This field is provided for integration with third party applications where the user ID has to be alphanumeric and up to 20 characters.

General

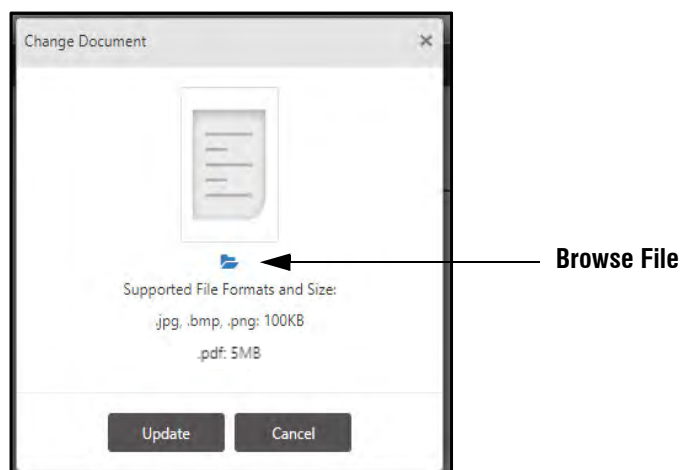
This section allows you to add general information about a user. The **General** page appears as follows:

Basic	General	Personal	Contact
<div>Date Of Birth <input type="text"/></div> <div>Birthday Message <input type="checkbox"/></div> <div>Joining Date <input type="text"/></div> <div>Confirmation Date <input type="text"/></div> <div>Leaving Date <input type="text"/></div> <div>Reason For Leaving <input type="text"/></div>			
<div>Vehicle Registration No. <input type="text"/></div>			
<div>Driving License <input type="text"/></div> <div>Driving License Expiry <input type="text"/></div>			
<div>Passport No. <input type="text"/></div> <div>Passport Expiry <input type="text"/></div>			
<div>PAN <input type="text"/></div> <div>Aadhaar No. <input type="text"/></div> <div>PF No <input type="text"/></div> <div>UAN <input type="text"/></div> <div>ESI No <input type="text"/></div> <div>Voter ID <input type="text"/></div>			
<div>Visa <input type="text"/></div> <div>Visa Expiry <input type="text"/></div>			

Security Number	<input type="text"/>	
ID Proof *	<input type="text"/>	
Nominee Name *	<input type="text"/>	
Field 4	<input type="text"/>	

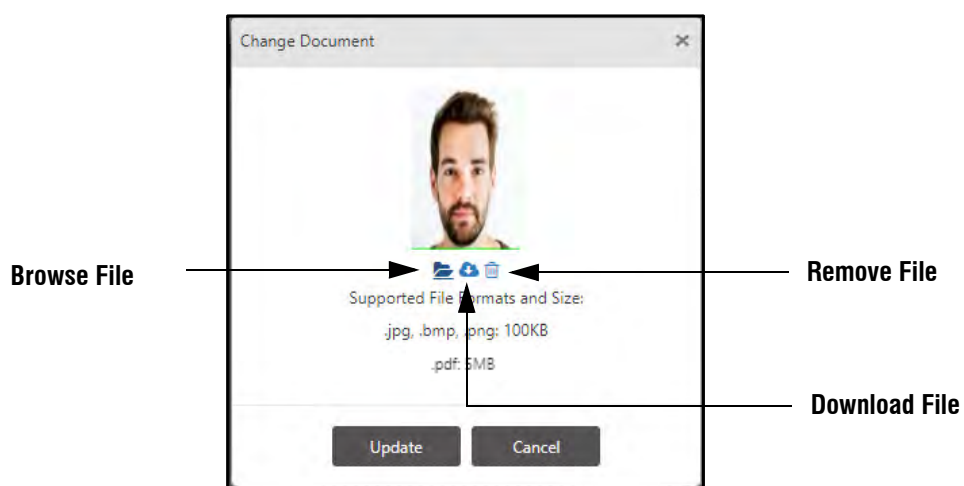
Enter the relevant employee information — Date of Birth, Joining Date, Confirmation Date etc.— either manually or by clicking the date selection button as shown in the above images.

In certain parameters like Driving License, Passport No., PAN, etc, you can upload the documents by clicking **Upload** button. Then **Change Document** pop-up appears as shown below.





Click **Browse File**  .


To upload, select the desired file as per the supported formats and size (.jpg, .bmp, .png, pdf) from your local PC.




After uploading the file, if you wish to upload a different file instead of the current uploaded file, click **Browse File**

 again and select the desired file from your local PC. The previously uploaded file will get replaced with the new file.


To download the uploaded file, click **Download File**  .

To remove the uploaded file, click **Remove File**  .

Then click **Update**.


The document will be uploaded and can be previewed by clicking the **Preview**  icon.

There are 10 additional fields in which you can enter the desired details of the users as per your requirement. These are visible only after they are configured from **Admin> System Configuration> Global Policy> User**. For details refer *“Custom Fields”*. For example Security Number, ID Proof, Nominee Name, etc.

Click on the **Upload**  button and select the image of respective document.

Select the desired file as per the supported formats (.jpg, .bmp, .png, pdf).

Then click **Update**.

The document will be uploaded and can be previewed by clicking on **Preview**  button.

Personal

This section allows you to add personal information about a user. The **Personal** page appears as follows:

Basic	General	Personal	Contact
Nationality <input type="text" value="Indian"/>			
Qualification <input type="text" value="B.E-E.C"/>			
Experience <input type="text" value="3 years"/>			
Gender <input type="text" value="Female"/>			
Blood Group <input type="text" value="A+"/>			
Height (cms) <input type="text" value="180"/>			
Weight (kgs) <input type="text" value="55.0"/>			
Medical History <input type="text"/>			
Marital Status <input type="text" value="Married"/>			
Father/Spouse Name <input type="text" value="N M Raval"/>			

Enter the relevant personal details — Nationality, Qualification, Experience etc. — of an employee in the following fields either manually or by choosing from the respective drop-down lists:

Contact

This section allows you to add contact information about a user. The **Contact** page appears as follows:

Enter the relevant contact and address details of the employee in the **Contact Info** and **Address** tabs.

Basic	General	Personal	Contact
<div> <div>Contact Info</div> <div> <div>Personal</div> <div> <div>Phone</div> <div>9682624826</div> </div> <div> <div>Mobile</div> <div>8611224120</div> </div> <div> <div>Email</div> <div>aditigupta@gmail.com</div> </div> </div> <div> <div>Official</div> <div> <div>Phone</div> <div>9825278780</div> <div>-</div> <div>680</div> </div> <div> <div>Mobile</div> <div>8762422620</div> </div> <div> <div>Email</div> <div>aditigupta@matrixcomsec.com</div> </div> </div> <div> <div>Receive Alert On</div> <div> <div>Personal Mobile</div> <div><input checked="" type="checkbox"/></div> </div> <div> <div>Personal Email</div> <div><input checked="" type="checkbox"/></div> </div> <div> <div>Official Mobile</div> <div><input type="checkbox"/></div> </div> <div> <div>Official Email</div> <div><input checked="" type="checkbox"/></div> </div> </div> </div>			
<div> <div>Address</div> <div></div> </div>			

Basic	General	Personal	Contact
<div> <div>Contact Info</div> <div> <div>Address</div> <div> <div>Local</div> <div> <div>Address</div> <div>302, shivam Residency</div> </div> <div> <div>Street</div> <div>Manjalpur</div> </div> <div> <div>City-Pincode</div> <div>390011</div> <div>-</div> <div>Pincode</div> </div> <div> <div>State</div> <div>Gujarat</div> </div> <div> <div>Country</div> <div>India</div> </div> </div> <div> <div>Permanent</div> <div> <div>Address</div> <div>CTM</div> </div> <div> <div>Street</div> <div>Ahmedabad</div> </div> <div> <div>City-Pincode</div> <div>380002</div> <div>-</div> <div>Pincode</div> </div> <div> <div>State</div> <div>Gujarat</div> </div> <div> <div>Country</div> <div>India</div> </div> </div> </div> </div>			

Click on the **Save** button to save the user's profile.

This user will now be reflected in the list of users on the **User List** page.

To further add or edit any user details, go to **Users module > User List**.

Select the user from the **User List** by searching the user through ID or name. Also the user can be searched by specifying the ID or Name in User Configuration page.

The **User Configuration** page opens with the selected user details as shown below.

The screenshot shows the 'User Configuration' window with a sidebar on the left and a main content area. The sidebar contains a user profile icon and a list of configuration tabs: Profile, Devices, Credentials, Group, T&A, Access Control, ESS, Cafeteria, Job Costing, Field Visit Management, Face Recognition, and Events. The 'Profile' tab is selected. The main content area has four tabs: Basic, General, Personal, and Contact. The 'Basic' tab is active, showing fields for ID (1687), Name (Aditi Ajay Gupta), and Active status (checked). Below these is an 'Optional' section with fields for Full Name (Aditi Ajay Gupta), Short Name (Aditi Ajay Gupta), Reference ID (1687), and Integration Reference (20 chars).

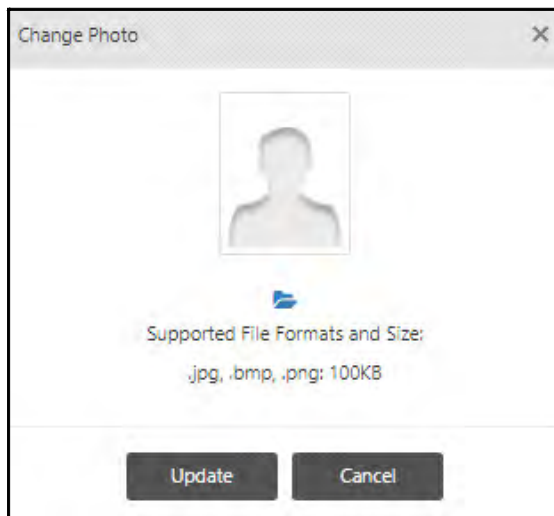
The User Configuration page provides various options for detailed configuration of the new user. Once the Profile tab is configured, the administrator can proceed to configure the other sections.


Adding User Photo

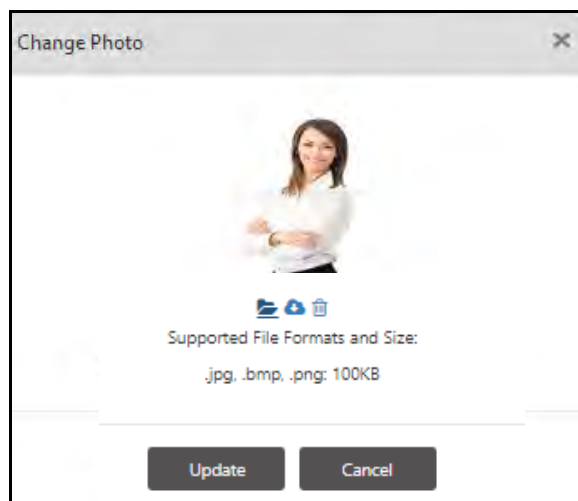
The administrator can add a profile photograph for each user defined in the COSEC system. The allowed size limit for uploading an image file is 100 KB.

This screenshot is similar to the previous one, but with an arrow pointing to the profile photo icon in the sidebar. The main content area shows the same user details for Aditi Ajay Gupta, with the 'Basic' tab selected. The 'Optional' section is also visible, showing fields for Full Name, Short Name, Reference ID, and Integration Reference.

To add an image as the profile photograph for a user, click the image icon. The Change Photo window appears as shown below.



Click  to browse the image file. The Supported File Formats are *.jpg, .bmp and .png. Once the required image file is selected, click the **Update** button.



Then click **Save** button. The user photo will be successfully updated on the **User Configuration** page as shown below.

User Configuration

1687
Aditi Ajay Gupta
Active

Basic | General | Personal | Contact

ID * 1687
Name * Aditi Ajay Gupta_Ahmedabad
Active ☒

Optional

Full Name Aditi Ajay Gupta_Ahmedabad
Short Name * Aditi Ajay Gupta
Reference ID * 1687
Integration Reference 20 chars

Profile
Devices
Credentials
Group
T&A
Access Control
ESS
Cafeteria
Job Costing
Field Visit Management

Devices

This option enables the administrator to assign the user to the Panel200, Direct doors and Device groups defined in the system.



The COSEC devices must be configured before assigning users on devices.

Assign

Assign | Configure

Device Group ID Name
Device Name

Search

DGID	Device Group Name	Action
1	Group1	

Search

Device Name	Type	Restrict Access	Restrict Attendance	Action
ARGO	ARGO	<input type="checkbox"/>	<input type="checkbox"/>	
Door PVR	PVR Door	<input type="checkbox"/>	<input type="checkbox"/>	
FMX	Door FMX	<input type="checkbox"/>	<input type="checkbox"/>	
PATH	Path V2	<input type="checkbox"/>	<input type="checkbox"/>	

Profile
Devices
Credentials
Group
T&A
Access Control
ESS
Cafeteria
Job Costing
Field Visit Management
Face Recognition
Events

Device Group: To assign a device group or Super group to the user, click the device group picklist and select the group. Super group is a group made up of device groups.

You can also unassign the particular device from the assigned Device Group by clicking on icon. Click on the icon to assign the device again.

Device Name ▲	Type	Restrict Access	Restrict Attendance	Action
ARGO	ARGO	<input type="checkbox"/>	<input type="checkbox"/>	
Door PVR	PVR Door	<input type="checkbox"/>	<input type="checkbox"/>	
FMX	Door FMX	<input type="checkbox"/>	<input type="checkbox"/>	
PATH	Path V2	<input type="checkbox"/>	<input type="checkbox"/>	

Click to Assign

Device: To assign a single device to the user; click the device picklist and select the device. The device can be deleted by clicking on **Delete** button.



The device appearing in the device picklist will be Panel, Panel Lite, Panel200 Doors & Direct Doors only.

Click the **OK** button.

Select the corresponding **Restrict Access** and **Restrict Attendance** check-boxes to enable these restrictions for the selected user on the selected device as shown.

Device Group

ID Name

Device

Name

Search

DGID ▲	Device Group Name	Action
1	Group1	

Search

Device Name ▲	Type	Restrict Access	Restrict Attendance	Action
ARGO	ARGO	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Door PVR	PVR Door	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
FMX	Door FMX	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
PATH	Path V2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

- It implies that the user Aditi is restricted for access on Door ARGO and PATH V2. The punches of Aditi on this door will be considered for attendance only and the door will not be opened for access.
- For Door PVR and Door FMX, the restriction is for Attendance. This means the punch on door will open the door for access but will not be calculated for attendance.

Click the **Save** button to save the device selection for assigning to the user.



If any device or a device belonging to any device group is un-assigned against any user or is selected for deletion but is a part of the Access Rule which is assigned to that user, then those door(s) will be retained against that user.

Configure



The parameters for “Configure” varies for different type of devices.

The screenshot shows the 'User Configuration' window with the 'Configure' tab selected. On the left, a sidebar lists various configuration options: Profile, Devices (highlighted), Credentials, Group, T&A, Access Control, ESS, Cafeteria, Job Costing, and Field Visit Management. The main area displays configuration for user '1687 Aditi Gupta' (Active). The 'Device' is set to 'NGT Direct Door-Device-10' and the 'Type' is 'NGT Direct Door'. Both 'Active' and 'Cafeteria Device' checkboxes are checked.

Device: Select a device from the Device drop down list. This list displays all devices on which the selected user is assigned.

Active: The Active checkbox is selected by default to enable the user credentials on the selected device.

Configuration of Panel200 is shown below:

This screenshot shows the configuration settings for a 'Panel Lite V2' device. The 'Device' is 'Panel Lite V2-Device-1' and the 'Type' is 'Panel Lite V2'. The 'Active' checkbox is checked, while 'VIP', 'Absentee Rule', and 'Absent Day(s) Count' (set to 60) are not. Other settings include 'Access Profile' (Group-1), 'Functional Group' (Staff), 'Home Zone' (Zone-1), 'Visit Zone' (Select), and 'Access Route' (Select).

VIP: Check the VIP box if the user is to be given unrestricted access rights.

Absentee rule: Check this box to enable Absentee rule feature at user level for each Panel200 and Direct door. However, this option needs to be first enabled at the Panel200 and Direct door levels.

- **Absent Days Count:** Specify the days count ranging from 1 to 365 for which if the user remains absent, he will be marked inactive.

Access Profile: Select the Access Profile to be assigned to the user for the selected Panel200.

Functional Group: Select the Functional Group to be assigned to the user for the selected Panel200.

Zone: Select the user's **Home Zone** and the **Visit Zone** for the selected Panel200.

Access Route: The administrator can also assign a defined access route to the user. Select the access route from the drop down list if required.

Select another device and configure the access control options as applicable.



*This option is only available with the **Access Control** add on module.*

Credentials

The Credentials option enables the configuration and enrollment of user credentials for the selected user.

The screenshot shows a web application window titled "User Configuration". On the left is a sidebar menu with options: Profile, Devices, Credentials (selected), Group, T&A, Access Control, ESS, Cafeteria, Job Costing, Field Visit Management, Face Recognition, and Events. The main area displays the "Credentials" configuration for user "SK8 Shailee" (Active). The fields are as follows:

Field	Value
PIN	[Empty]
Biometric Group No.	42
Roaming User	<input type="checkbox"/>
Access Card 1	[Empty]
Access Card 2	[Empty]
Enrolled Fingers (Suprema Proprietary)	0
Enrolled Fingers (Suprema ISO)	0
Enrolled Fingers (Lumidigm ISO)	0
Enrolled Fingers (Lumidigm Proprietary)	0
Enrolled Palm	0
Enrolled Face	0
Enable Self-Enrollment	<input type="checkbox"/>

The following parameters are available for configuration for the selected user:

PIN: Specify the PIN no. for the user. User PIN should be a numeric value ranging from 1 digit to a maximum of 15 digits. The value entered in this field will only be visible to the "SA" user. For all other login users the value in this field will be masked.

Biometric Group No.: Specify the Biometric group number to be assigned to the user if applicable. It is a number allotted to a group of users assigned on a device. This enables the device to match a template against only those users who are part of the same Biometric Group thus reducing processing time.

This value is used for Palm/Face Identification of user on Identification Server in shorter time span considering user first specifies Group No and then punches on the device.

Identification Server will be allocating templates to its child threads on the basis of this field.

Roaming User: You can mark the user as roaming user for the users who are field engineers, partners etc who report to office rarely. When such users mark their punch after pressing 0 on door, then they will be identified from the Roaming user group.

The Identification server will maintain a list of users along with their templates to be considered as roaming/remote users.

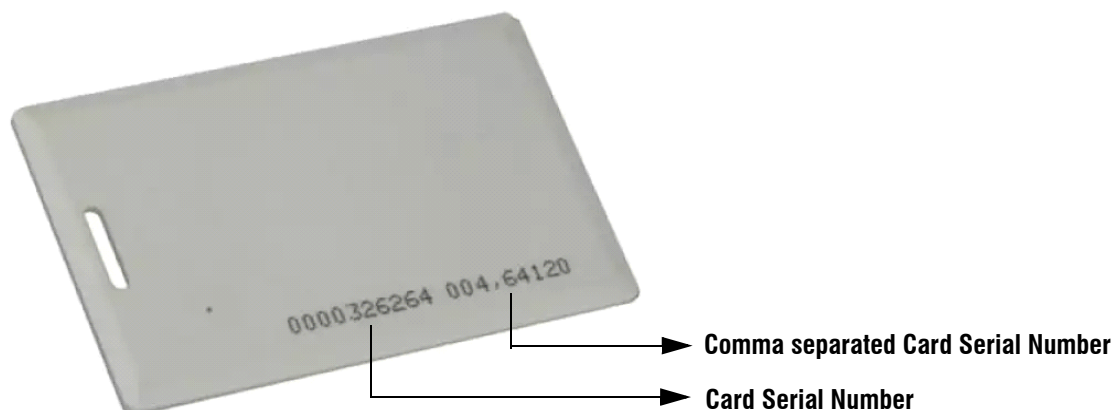


If Enterprise Group Mapping is done then on user configuration page by default status of 'Roaming User' will be loaded as per mapped enterprise group.

Access Card 1: Enter a Card Serial Number (CSN) or a Comma separated CSN which is to be assigned to the user.

Format:

- **Card Serial Number** = 1343933547.
- **Comma separated CSN** = 12,345789



The maximum character limit for Card Serial Number (CSN) is 20 digits. While the maximum character limit for Comma separated CSN is 21 digits.

To configure a comma separated card value, make sure you configure a 26-bit card format in the system and then assign the same to the device. To know more, refer [“Card Formats”](#).

If there is any discrepancy while entering the Access Card number (CSN), the system will display an error.

This Access Card number will be synced with the devices to allow/deny access to users.

COSEC accepts up to two cards per user. So if required and available, enter the **Access Card 2** number.

Once you save the configurations, hover your mouse over the Comma separated CSN value of any Access Card, the system will display an encoded (converted) value of Comma separated CSN.

While importing the data of users, make sure you enter the correct Access Card details in the desired format — Card Serial Number (CSN) or Comma separated CSN. To know more about importing users, refer [“Import Users”](#).

Enrolled Fingers: This option displays the number of fingerprint templates enrolled against the selected user.

- **FP Template Type-** If Credential is selected as FP Template; then you can select the Type of FP Template which is to be deleted. The options of template are Suprema Proprietary, Suprema ISO, Lumidigm ISO, Lumidigm Proprietary and All.

Enrolled Palm: This option displays the number of palm vein templates enrolled against the selected user.

Enrolled Face: This option displays the number of Face templates enrolled against the selected user.


Enable Self-Enrollment: Select this checkbox to enable the Self-Enrollment feature for the selected user.

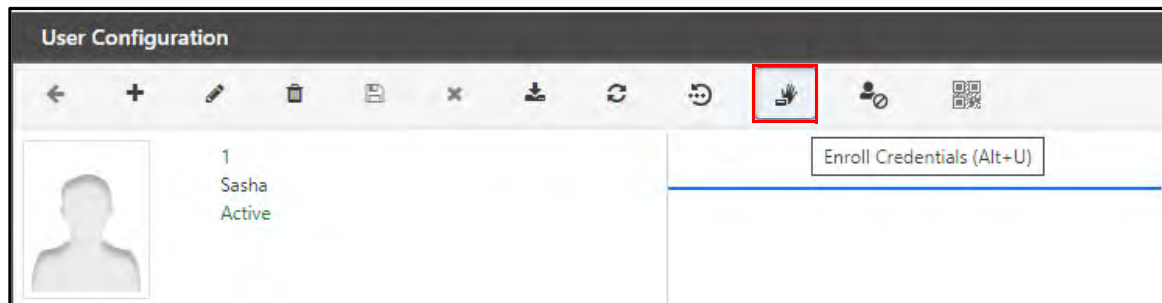
The *Self-Enrollment* feature enables the user to enroll himself/herself at a COSEC door controller using an already provided access PIN, without the help of any operator or HR executive. This feature is applicable for Wireless Door, PVR Door, NGT Controller, Vega Controller, Door V3 and Door V4.

To enable Self- Enrollment at door; select *Device Configuration> Enrollment > Settings*.

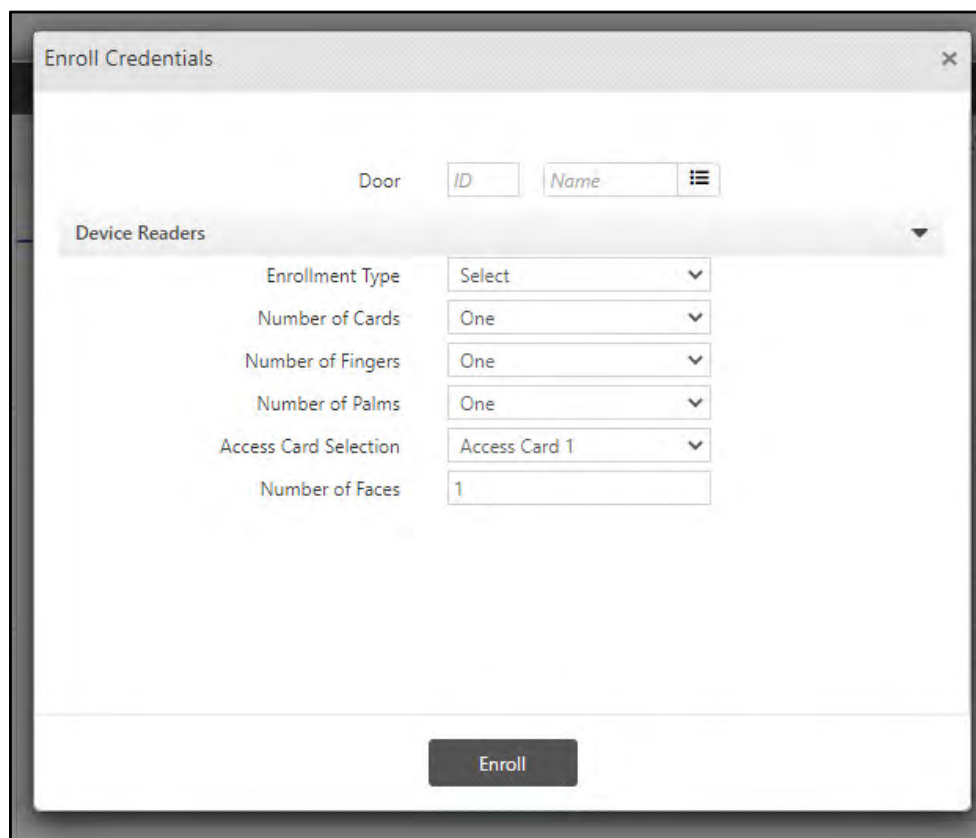
An alert message containing the access PIN will be sent to the user once this feature is enabled for this user. To configure the access PIN to be sent in Alert message, [See “Configuring Alert Messages” on page 231](#). Self-Enrollment can be especially beneficial for organizations with large number of employees.

Enroll Credentials

The Administrator can enroll credentials for the user by clicking **Enroll Credentials**  as shown below.



The **Enroll Credentials** window appears as shown below:



- **Door:** Select the desired door from the pick-list on which the enrollment is to done.

Device Readers

Device Readers displays the information of the readers configured in the selected **Door**.

Enroll Credentials

Door

Device Readers

Card Reader

Biometric Reader

External Reader

Enrollment Type

Number of Cards

Number of Fingers

Number of Palms

Access Card Selection

Number of Faces

Enroll

Card Reader, Biometric Reader and External Reader information are displayed here.

Enroll Credentials

Door

Device Readers

Card Reader

Biometric Reader

External Reader

Enrollment Type

Number of Cards

Enroll

- **Enrollment Type:** From the dropdown list, select the desired enrollment type — **Read Only Card, Smart Card, Face, Biometrics, BiometricsThenCard, Mobile, or Duress Finger.**

Based on the selection of the **Door** and **Enrollment Type**, below parameters will be displayed for configuration.



When Enrollment Type selected is Smart card or BiometricThenCard, Duress Finger Templates will not be written in the Smart Card.

Below parameters also depend on the Readers configured in the Door. To configure the desired Reader, refer Readers section under Devices > Device Configuration (of the desired Door) > Profile > Readers.

1. Enrollment Type = Read Only Card

Number of Cards: Select the desired number of cards from the drop-down list.

2. Enrollment Type = Smart Card

Number of Cards: Select the desired number of cards from the drop-down list.

Details on Smart Card

Select the desired check boxes of the parameters — **User ID**, **Facility Code (FC)**, **Additional Security Code (ASC)** — which are to be displayed on the Smart Card.

Select the desired number of **Finger Templates** from the drop-down list.

If the **Door** is selected as PVR Door, **Palm Templates** parameter will be visible. Select the check box of this parameter if you wish to display it on the smart card.

To store palm templates, MiFare 4k reader must be configured in the PVR Door.



Door PVR must be set in the Adaptive mode (configure from Admin> System Configuration> Global Policy) for the palm templates to be saved into the Smart Card.

Additional Details on Smart Card

Other than the parameters mentioned in the Details on Smart Card, you can display additional details on Smart Card.

Select the desired check boxes of the parameters — **Short Name, Branch, Department, Designation, Emergency Contact, Blood Group** and **Medical History**— which are to be displayed on the Smart Card.

The values of these additional details are displayed as well. Make sure the values of these additional details are not blank for successful enrollment process.

3. Enrollment Type = Face

Number of Faces: Select the desired number of faces from the dropdown list.

The screenshot shows a window titled "Enroll Credentials". Inside, there are several input fields: "Door" with the value "13", "Device Readers" with a dropdown menu showing "ARGO-Device-", "Enrollment Type" with a dropdown menu showing "Face", and "Number of Faces" with a dropdown menu showing "1". At the bottom of the window is a button labeled "Enroll".

4. Enrollment Type = Biometrics

Number of Fingers/ Number of Palms: Select the desired number of fingers or palms from the dropdown list.

The image displays two screenshots of a configuration interface, likely for a security system. Both screenshots show a 'Door' configuration section with a dropdown menu for 'Device Readers' expanded. The top screenshot shows 'Door' set to 3, 'ARGO' selected, 'Enrollment Type' set to Biometrics, and 'Number of Fingers' set to One. The bottom screenshot shows 'Door' set to 1, 'PVR' selected, 'Enrollment Type' set to Biometrics, and 'Number of Palms' set to One.

5. Enrollment Type = BiometricsThenCard

Number of Cards: Select the desired number of cards from the dropdown list.

Number of Fingers/ Number of Palms: Select the desired number of fingers or palms from the dropdown list.

Details on Smart Card

Select the desired check boxes of the parameters — **User ID**, **Facility Code (FC)**, **Additional Security Code (ASC)** — which are to be displayed on the Smart Card.

Select the desired number of **Finger Templates** from the drop-down list.

If the **Door** is selected as PVR Door, **Palm Templates** parameter will be visible. Select the check box of this parameter if you wish to display it on the smart card.

To store palm templates, MiFare 4k reader must be configured in the PVR Door.



Door PVR must be set in the Adaptive mode (configure from Admin> System Configuration> Global Policy) for the palm templates to be saved into the Smart Card.

Additional Details on Smart Card

Other than the parameters mentioned in the Details on Smart Card, you can display additional details on Smart Card.

Select the desired check boxes of the parameters — **Short Name, Branch, Department, Designation, Emergency Contact, Blood Group** and **Medical History**— which are to be displayed on the Smart Card.

The values of these additional details are displayed as well. Make sure the values of these additional details are not blank for successful enrollment process.

6. Enrollment Type = Mobile



To select **Enrollment Type** as **Mobile**, the particular device must have BLE support and ensure Bluetooth is ON in the mobile.

Access Card Selection: Select the desired Access Card from the drop-down list.

Facility Code (FC): Select this check box to enroll the Facility Code (FC) against the user.

Click **Enroll** to initiate the enrollment process.

Enroll Credentials

✓ Enrollment Command Sent

Door: 3 ARGO

Device Readers: [Dropdown]

Enrollment Type: Mobile

Access Card Selection: Access Card 1

Facility Code (FC): ☐

Enroll

To know more about enrolling credentials of users, refer [“Enrolling Users”](#).

7. Enrollment Type = Duress Finger

Number of Fingers: Select the desired number of fingers that you want to enroll as **Duress Finger** from the drop-down list— **One** or **Two**.

Enroll Credentials

Door: 1 ARGO Device

Device Readers: [Dropdown]

Enrollment Type: Duress Finger

Number of Fingers: [Dropdown: One, Two, Three]

Enroll

Click **Enroll** to initiate the enrollment process.

Group

This option enables to assign the Enterprise groups, Reporting group, Approval Policy, Leave group and Week off group to the user.

The screenshot shows the 'User Configuration' window with the 'Group' tab selected. The user profile on the left shows ID 1687, name Aditi Ajay Gupt, and status Active. The main configuration area contains the following fields and their assigned values:

Field	Value
Organization	1
Branch	1
Department	1
Section	1
Category	1
Grade	1
Designation	1
Custom Group 1	1
Custom Group 2	1
Custom Group 3	1
Reporting Group	1
Approval Policy	2
Leave Group	1
Week Off Group	ID

This page will be available with the Time & Attendance add on module.

The default groups will be shown in the respective fields. Click on the picklist buttons and select the appropriate enterprise groups (Organization, Branch, Department, Section, Category, Grade, Designation, Custom Groups) to assign the user.



The Enterprise Groups changed from here will be effective from the current date only. For the changed group to be effective from previous date, change the group from User module> Utilities> Change Group.

The picklist options that appear in each enterprise group will be as per the rights assigned to the SA. For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#).

- **Reporting Group:** Select the group from the pick-list to be assigned as reporting group for the user. The In-charge of the selected group will be the in-charge of the user. The different applications of user will require authorization of the in-charge of the group.

To create the Reporting group; click *Users module> Reporting In-Charge> Reporting Group*. For details, refer to [“Reporting Group”](#)

- **Approval Policy:** When Reporting Group is assigned to the user only then you can select the Approval Policy from the pick-list to assign to the user.

The Approval policy is created from *Users module> Reporting In-Charge> Approval Policy*. Refer to [“Approval Policy”](#).

- **Leave Group:** Select the leave group from the pick-list to assign a group of leaves to the user.



To assign the new leave to the user, add the leave to the Leave group and assign the leave group to the user.

- **Week Off Group:** Select the week off group from the picklist to assign the configured week offs to the user.



To create the Week Off group, go to Shifts and Schedule module > Week Off Group



If 'Shift Based Access' flag is enabled in User Configuration, then effect of Week Off group assigned to user differently won't be effective.

Also if flag of 'Deny Access On Week Off' is enabled in Shift Schedule assigned to user, then user won't be granted access though user did not have week off based on Week Off group.

T&A

This tab will be available only for the *Time and Attendance* license. Here, the administrator can enter the attendance and the working policy related information for the user.

The screenshot shows the 'User Configuration' window with the 'T&A' tab selected. The left sidebar lists various configuration options: Profile, Devices, Credentials, Group, T&A (selected), Access Control, ESS, Cafeteria, Job Costing, Field Visit Management, Face Recognition, and Events. The main area is divided into 'Attendance' and 'Policy' sections. The 'Attendance' section includes: 'Enable Attendance Calculation' (checked), 'Restrict Half Day Considerations' (unchecked), 'Attendance Marking Type' (Normal), 'Max Punches To Be Considered' (Select), 'Bypass Finger/Palm/Face For Attendance' (unchecked), 'Max Short Leaves Allowed' (None), 'OT/C-OFF Eligibility' (None), 'Authorize C-OFF On' (WO, PH, WO/PH, FB, RD, Normal Day), 'Bus Route' (ID, Name), 'Enable Site Based Auto Tour Application' (unchecked), 'Tour' (Select), 'Base Site Selection' (ID, Name), and 'Auto Authorize Site Based Tour Application' (unchecked).

This close-up shows the 'Enable Location Based Auto Tour Application' (checked) section. It includes: 'Tour' (T2 - Tour2), 'Base Location Assignment' (Selected), 'Location' (Code, Name), 'Location Group' (ID, Name), 'Auto Authorize Location Based Tour Application' (checked), and 'Show Attendance Details On Device' (checked).



If the Attendance Policy for the user is configured then assign that policy to the user. There is no need to configure same parameters i.e. "Max Punches to be considered" and "Max Short Leaves Allowed" here. Still If configured, then parameters configured here will be applicable for the user.

Attendance

In the **Attendance** section, configure the following parameters:

The screenshot shows the 'Attendance' section of the configuration. It includes: 'Enable Attendance Calculation' (checked), 'Restrict Half Day Considerations' (unchecked), 'Attendance Marking Type' (Normal), 'Max Punches To Be Considered' (Select), 'Bypass Finger/Palm/Face For Attendance' (unchecked), 'Max Short Leaves Allowed' (None), and 'OT/C-OFF Eligibility' (None). A dropdown menu for 'Attendance Marking Type' is open, showing options: Normal, First Punch Only, Executive, Flexible, and Present.

Enable Attendance Calculation - This field is checked by default. Uncheck this box if you want to disable attendance calculation for this User. This option has to be enabled for configuring any of the other parameters on this page.

Restrict Half Day Considerations - Enabling this option will restrict the half day markings and will consider only the full day attendance calculations.

For Example:

If the user has completed only the half of the required working hours, and **Restrict Half Day Considerations** is enabled for him, then his attendance will be considered as full day absent and the half day consideration will be restricted.

Attendance Marking Type - In case the attendance calculation is enabled then the user needs to select the attendance marking type from the drop down list.

The following options are available:

- **Normal:** type will be default for all users.
- **First Punch Only:** type users need only entry punch at the start of the shift. In this case the system will assume that the shift end time is the last out Punch for the day. All other calculations remain the same as for normal type users.
- **Executive:** type users will be marked full day present if at least one punch (entry/exit) is available in the day. There will not be any late/early & overtime calculation like it is done for normal and single punch type users.
- **Present:** category users do not require any punch for them to be marked full day present. All users belonging to this category are marked present by default.
- **Flexible:** category users' working will be checked against required minimum working and if it is more than required, full day attendance will be marked. In this case the minimum working hours required in a day for full day attendance and half day attendance can also be defined for each user as explained below.
- **Minimum Working Hours Required** - In the event of selecting the Flexible type for a user the administrator can also specify the minimum working hours required in a day to be marked **Full Day** or **Half Day** present. Specify the hours in hh:mm format.

Attendance	Policy
Enable Attendance Calculation	<input checked="" type="checkbox"/>
Restrict Half Day Considerations	<input type="checkbox"/> ⓘ
Attendance Marking Type	Flexible ▼
Min Working Hours Required	
Half Day	02:00
Full Day	04:00
Max Punches To Be Considered	2 ▼
Bypass Finger/Palm/Face For Attendance	<input type="checkbox"/>

Max Punches to be Considered - This parameter specifies the maximum entry/exit events per user to be considered in a day for attendance calculation.

Specify a value in this field if the value defined at the global level is to be overridden for this user. The options available are 2, 4, 6, 8, 10, 12 and N-Punch. N-Punch allows unlimited number of punches in IN/OUT pair.

The screenshot shows a configuration form with several fields. The 'Max Punches To Be Considered' field has a dropdown menu open, displaying options: 2, 4, 6, 8, 10, 12, and N-Punch. The 'Bypass Finger/Palm/Face For Attendance' field is checked. Other fields include 'Max Short Leaves Allowed', 'OT/C-OFF Eligibility', 'Authorize C-OFF On', 'Bus Route', and 'Enable Site Based Auto Tour Application'. To the right, there are checkboxes for 'WO/PH' and 'Normal Day'.

Bypass Finger/Palm/Face For Attendance - On checking this option, the user can punch in or out using any of the assigned credentials and the same will be considered for attendance calculation. On selection of this option, finger/palm/face identification is not required for marking attendance. The user can use pin or card to mark the attendance.

Max Short Leaves Allowed - This parameter specifies the maximum number of short leaves (personal hours) to be allowed to selected users in an attendance period. This parameter is also defined at the global system configuration level and can be overridden for specific users using this option. The administrator can specify a value of a maximum two digits in this field.

OT/C-OFF Eligibility: This parameter enables the administrator to determine whether the overtime authorization for this user is to be done in one of the following ways:

- **None** - Extra work cannot be authorized as overtime or C-OFF for user.
- **Only Overtime** - Extra Work can only be authorized as overtime.
- **Only C-OFF** - Extra Work can only be authorized as C-OFF.
- **Both** - Extra Work can be authorized both as overtime and C-OFF.

On selecting **Both**, user can set the extra hours to be authorized as OT or C-OFF separately for Normal Day, WO, PH, WO/PH, FB and RD.

The screenshot shows the 'Authorize C-OFF On' section of the configuration form. It includes checkboxes for 'WO', 'PH', 'WO/PH', 'FB', 'RD', and 'Normal Day'. The 'Both' option is selected in the 'OT/C-OFF Eligibility' dropdown. An arrow points to the 'WO' checkbox.



For detailed configuration to authorize OT/C-OFF, [See "Configuration to give OT and C-OFF to user" on page 1502.](#)

If only Compensatory off is to be given to the user, then you must select Only C-OFF option.

To know more about authorization of extra hours as OT/C-OFF, [See "Overtime/C-OFF Approval" on page 1589.](#)

Bus Route: Click on the Picklist button and select the bus route to be assigned to the user.

Enable Site Based Auto Tour Application: Select this checkbox so that tour application will be automatically applied for a particular user, if he punches from some site other than the Base Site.

- **Tour:** Select the tour application from the drop-down list which will be automatically applied.
- **Base Site Selection:** Select the base site to be assigned to the user.
- **Auto Authorize Site Based Tour Application:** Select this checkbox to automatically authorize the tour application for a particular user, if auto tour application feature is enabled.
- **Enable Location Based Auto Tour Application:** Select this checkbox so that tour application will be automatically applied for a particular user, if he punches from some location other than the Base location.

If a user goes for official activity to some location other than base location; then new location can be assigned to the user and tour application will be automatically applied for that day when event is generated from the new location.

- **Tour:** Select the tour application from the drop-down list which will be automatically applied when user goes to other location. The Tour application will be available in the drop-down only if it is added in the leave group assigned to the user.
- **Base Location Assignment:** Select the base location to be assigned to the user as **All** or **Selected**.
 1. For **All** option; all the locations configured in Location Master will be assigned to the user. When new location is added to Location master then it will be automatically assigned to the user if “All” is selected.
 2. For **Selected** option; Location and Location Group will be enabled for the selection which is to be assigned to the user.
 - **Location-** Select the Location pick-list and select the locations to be assigned to the user.
 - **Location Group-** Select the Location group pick-list and select the groups to be assigned to the user. If Selected Location groups are assigned to user and whenever new location is added to the location group then newly added location in location group will also be assigned to the user.

- **Auto Authorize Location Based Tour Application:** Select this checkbox to automatically authorize the auto generated tour application for a particular user who has punched from location other than base location. The auto approved application will appear in the Approved list. As it is automatically approved; no sms or email will be sent for approval to reporting in-charge.

Example: Consider a user Chirag for whom “Location Based Auto Tour Application” is enabled. Tour1 is selected and one location (HO) is assigned as the base location.

The screenshot shows a configuration form for 'Enable Location Based Auto Tour Application'. The form includes the following fields and values:

- Enable Location Based Auto Tour Application:** ☒
- Tour:** TR - Tour1
- Base Location Assignment:** Selected
- Location:** Code: [empty], Name: [empty]
- Location Group:** ID: [empty], Name: [empty]
- Auto Authorize Location Based Tour Application:** ☐
- Show Attendance Details On Device:** ☒

A 'Picklist For Location' dialog is open, showing a list of locations with 'HO' (Head Office) selected. The dialog indicates '1 selected of 3 records'.

Code	Name
<input checked="" type="checkbox"/> HO	Head Office
<input type="checkbox"/> HOM	HO Matrix
<input type="checkbox"/> RnD	RnD Makarpura

When user punches from location other than assigned base location then event will be generated as shown below.

The screenshot shows the 'User Events' interface. The top section displays filters for Date (27/06/2018), Filter By (All), and Group/User (ID, Name). Below the filters, there is a 'View' button and a table of 'Attendance Events (1)'.

User ID	User Name	Date-Time	Device Name	I/O	Access	Source	Source Details	Location Details	View Image
1	Chirag	27/06/2018 15:45		Entry	Allowed	Others		+22.2575, +073.1851	

Below the attendance events, there are sections for 'Access Control Events (0)' and 'Visitor Events (0)'.

This event will automatically generate the tour application. The reporting in-charge of the user can view the application and give the verdict.

Tour Application Approval

Show All Pending Applications

Tour Date: ☐ From Date: To Date:

Filter Users:

Group/User:

Pending (1)

User	Name	From Date	To Date	Tour	Application Type	Application Date	Posted Days	Approve	Reject	Remark	Details
1	Chirag	27/06/2018	27/06/2018	Tour1	New	27/06/2018	1.0	<input type="checkbox"/>	<input type="checkbox"/>		<input type="button" value="Details"/>

Click on **Details** button to view the tour application details.

Tour Application Detail

User:

Tour:

Application Details

Application Date:

Half Day Consideration:

From Date:

To Date:

Applied Days:

Posted Days:

Reason:

Address:

Contact Number:

Location Details:

The SMS and Email Alert can be configured from Alert Message configuration which will notify the reporting in-charge of the user who has punched from location other than base location. The SMS and Email must be configured from SMS configuration and Email configuration respectively.



1. Ensure that Email ID and Mobile number are specified in User profile of Reporting in-charge.
2. Ensure that Alert service must be properly assigned from the Admin Portal and Alert service must be running to get the alert notification.



Posting of Tour Application

1. If user is marked as 'PR' on one of the half day then Tour will be applied for other half of the day.
2. If leave application is pending for either half of day then tour will be applied on another half of day.
3. If leave application is pending for either half of day and approved C-OFF application for another half of day; then tour will not be applied on that day.

Show Attendance Details on Device: Select the check-box to display the attendance summary of the user on Vega direct door and FMX door. Hence the Vega/FMX direct doors assigned to the user will display the current month's data (as per device time) when the user is allowed access to the door.

See details in Device Configuration> Advanced > Settings (of Vega Door/ FMX door)

In the **Policy** section assign different Policies to the selected user. This page will be available only with the **Time & Attendance** add on module.

The default policies will automatically be assigned to the new user. It will be displayed in the respective fields as shown above.

To change the policies from current date, click the respective picklist and select the policy to be assigned to the user. If the policies (other than Attendance Policy) are to be assigned from previous date, then go to T&A > Utilities > Change Policy.



To configure the Policies go to T&A> Policies.

Access Control

On selection of the **Access Control** tab, the following page is displayed:

The screenshot shows the 'User Configuration' window with the 'Access Control' tab selected. The left sidebar lists various configuration options, with 'Access Control' highlighted. The main area is divided into 'Basic' and 'Advance' sections. The 'Basic' section includes fields for 'Bypass Finger', 'Bypass Palm', 'Access Validity', 'Access Validity Date', 'Access Level', 'Shift Schedule', 'Start Shift', 'Holiday Schedule', and 'Access Cluster Checking'. The 'Advance' section is currently empty.

Section	Field	Value
Basic	Bypass Finger	<input type="checkbox"/>
	Bypass Palm	<input type="checkbox"/>
	Access Validity	<input type="checkbox"/>
	Access Validity Date	<input type="text"/>
	Access Level	8
	Shift Schedule	Schedule Group
	Start Shift	General Shift
	Holiday Schedule	Schedule 1
	Access Cluster Checking	<input type="checkbox"/>
Advance		

Basic

In the **Basic** section, the administrator can define access parameters for the selected user. This tab offers the following sections for configuration:

Bypass Finger - This option can be enabled in the event of the Finger Print image not being in order and the system thus has problems identifying the user. In such cases, the system administrator can disable the Finger Print check for the user thus enabling the user to gain access using either the assigned pin or card.

Bypass Palm - This option can be enabled in the event of the Palm Vein image not being in order and the system thus has problems identifying the user. In such cases, the system administrator can disable the Palm vein check for the user thus enabling the user to gain access using either the assigned pin or card.

Access Validity - Enable this option if the user credential is to be activated for a predefined period.

Access Validity Date - Specify the end date of the validity in this field.

Access Level - Specify the access level for which the Smart Identification feature will be applicable to the user.

Shift Schedule - Assign a shift schedule to the selected user from the drop-down list.

Start Shift - In case of multiple shifts in the schedule group, the starting shift needs to be selected from the drop down list.

Holiday Schedule - Select the Holiday schedule to be assigned to the user from the drop down list.

Access Cluster Checking - Select this checkbox to enable checking for access cluster restrictions for the selected user. It is available only with the Access Control add-on license.

Advance

The **Advance** section is available only with the Access Control add-on module. Here, the administrator can define access parameters for the selected user. The **Advance** page appears as follows:

The screenshot shows the 'User Configuration' window with the 'Advance' tab selected. On the left, a sidebar lists various configuration options: Profile, Devices, Credentials, Group, T&A, Access Control (highlighted), ESS, Cafeteria, Job Costing, Field Visit Management, and Events. The main area displays the 'Advance' settings for user '1687 Aditi Gupta' (Active). The settings include: 'Enable Advance Access Control' (checked), 'Shift Based Access' (unchecked), 'Smart Access Route' (with input fields for ID and Name), 'Max Route Level' (set to 75), 'Enable Elevator Access Control' (checked), and 'Elevator Floor Group' (set to 1 with a picklist for 'RnD Elevator Group').

Enable Advance Access Control: Check this box to enable the advance access control feature.

Shift based Access: This parameter allows the administrator to enable user access based on the shift working time of the user.



*In the event of not selecting the **Shift Based Access** option then the system will apply the **Default Access Settings** as defined on a Panel200 as the access settings for the user.*

Smart Access Route - Select the Smart Access Route to be assigned to the user from the Access Route picklist window. The user can access the assigned route using the smart card enrolled with Smart Access Route. The card can be configured to include Smart Access Route from Card Personalization.

Max Route Level: Select the route level up to which the user is to be allowed access from the drop down list.

Enable Elevator Access Control: Check this box to enable the Elevator access control feature for the user.

Elevator Floor Group: Click the picklist and select the Elevator floor group to be assigned to the user. The user can access the floors of the Elevators included in Elevator Floor Group.

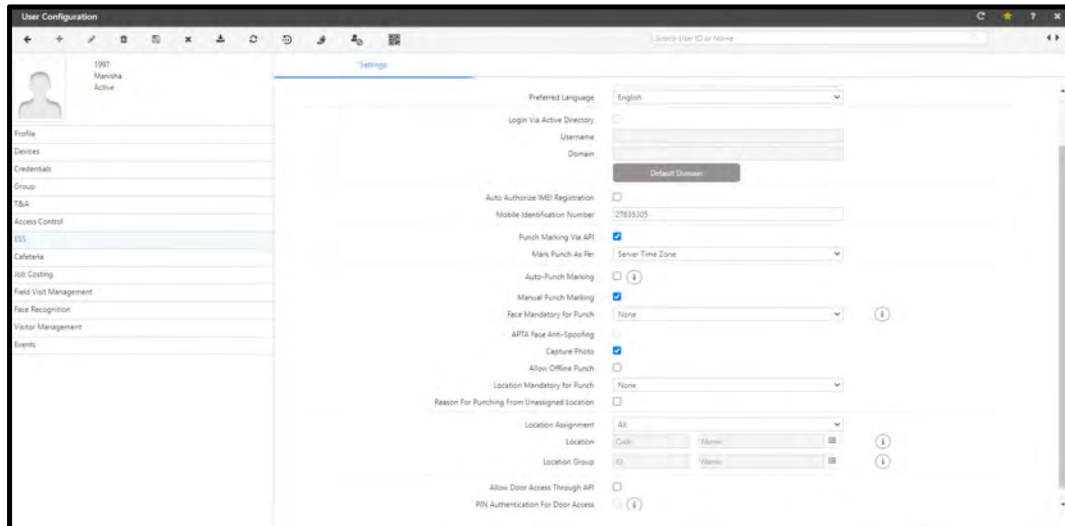
The Elevator Floor group is created from Access Control> Elevator Access Control> Elevator floor group



Certain parameters when configured for a specific user may over-ride corresponding parameters pre-defined at the Global Policy level.

ESS

To enable and configure ESS account access for the selected user. On selection of the **ESS** tab, the following page is displayed:



Settings

The **Settings** section under the **ESS** tab offers the following parameters for configuration:

Enable Account - Select this checkbox to enable ESS account access for the selected user.

Edit Basic Details - Select this checkbox to enable the selected users to edit basic details on their respective ESS accounts.

Punch marking via ESS - Select this checkbox to enable users to mark their attendance punch manually from their respective ESS accounts.

ESS Role Rights- Select the Role Rights from the picklist to be assigned to the user.

Preferred Language- Specifies the language preferred for the selected ESS Users as *English, Arabic, Spanish, Albanian, Turkish or Vietnamese*.

Login via Active Directory - Select this checkbox to enable the selected ESS user to login using his Active Directory credentials.

- **Username** - Assign a username to the selected ESS user for Active Directory login.
- **Domain** - Specify the Active Directory domain name in this field for Active Directory login.

Auto -Authorize IMEI Registration -Select this checkbox to automatically authorize the user request through device with registered IMEI number in COSEC database.

Mobile Identification Number - Specify the Mobile Identification Number which is the unique number of the mobile device from which the ESS application is to be used. This can consist of maximum 40 alphanumeric characters.

Punch Marking Via API - Select this checkbox to enable user to mark punches by firing API. Auto-Punch and Manual-Punch marking checkbox will be activated only if Punch marking via API is enabled.

Mark Punch As Per- Select the option of Time Zone which is to be applied for punch time (punch marked from API)

- **Server Time Zone-** The date- time of the punch will be as per the server time zone.
- **Local Time Zone-** The date-time of the punch will be as per the time zone of the place from where the punch is marked.

Auto-Punch Marking - Select this checkbox to enable the auto-attendance marking feature for the selected user from the COSEC APTA mobile application. On enabling this feature, if the user's current location matches any of the assigned locations; a punch will be marked automatically for the user from the mobile application.

Manual Punch Marking - Select this checkbox to enable manual punch marking from the COSEC APTA mobile application.

Face Mandatory For Punch - When Manual Punch Marking and Face Recognition feature is enabled for user then you can select the specific option for which face is to be made mandatory for the punch. The options are **Attendance, Access Control, Both** and **None**.

For Access Control and Both option; you must enable **Allow Door Access Through API** checkbox.

APTA Face Anti-Spoofing: When **Manual Punch Marking** is enabled and **Face Mandatory For Punch** is selected as — **Attendance, Access Control** or **Both** — then select **APTA Face Anti-Spoofing** checkbox to enable **Face Anti-Spoofing** feature via COSEC APTA Application to prevent false face verification by using a photo, video, mask or a different substitute for an unauthorized person's face.

Capture Photo - This checkbox is activated only when **Punch marking via API** and **Manual Punch Marking** are enabled. This allows the user to capture snapshot while punching through COSEC APTA.

Allow Offline Punch - This checkbox is activated only when "Punch marking via API" and "Manual Punch Marking" are enabled. This allows users to apply for offline punches.

In Mobile devices, when there is no connectivity between server and the Mobile device, the punches, with their timings can be stored through offline punch and send to server when connectivity is restored.

Location Mandatory For Punch - This field determines if information regarding the source location from where the punch has been marked should accompany a punch marking by user.

- Select **None** if location information should not accompany a punch.
- For *Manual Punch Marking*, select **Any Location** (locations need not be configured).
- For *Auto-Punch Marking* (auto-attendance feature), select **Configured Locations Only** (locations must be configured on "Location Master").

Reason For Punching From Unassigned Location: This checkbox will be activated only when 'Location Mandatory For Punch' has either **None** or **Any Location** as values. By enabling this checkbox, the Incharge Users can know the reason for which the punch is made from unassigned location by the employee user.

Location Assignment- Select the option as "All" or "Selected" for assigning location to user.

1. For **All** option; all the locations configured in Location Master will be assigned to the user. When new location is added to Location master then it will be automatically assigned to the user if "All" is selected.

2. For **Selected** option; Location and Location Group will be enabled for the selection which is to be assigned to the user.

- **Location**- Select the Location pick-list and select the locations to be assigned to the user.
- **Location Group**- Select the Location group pick-list and select the groups to be assigned to the user. If Selected Location groups are assigned to user and whenever new location is added to the location group then newly added location in location group will also be assigned to the user.



Locations can be configured from *COSEC Web Application > Admin > System Configuration > Location Master*.

Allow Door Access Through API- Select this check box to allow the access to device through API.

PIN Authentication For Door Access- Enable this check-box for Dual Authentication with PIN when Bluetooth or QR based access is used for Access control feature in COSEC APTA mobile application.



Pin Authentication For Door Access can be enabled only when Allow Door Access Through API is enabled.

Cafeteria

The cafeteria section allows to enable the cafeteria account for the user and configure the related parameters.

The screenshot displays the 'User Configuration' window for user 'u1' (Active). The left sidebar lists various configuration categories, with 'Cafeteria' highlighted. The main area shows the 'Settings' tab for the Cafeteria section. The settings include:

- Enable Account:** A checked checkbox.
- Enable Offline Transaction:** A dropdown menu set to 'Allow With Discount'.
- Discount Level:** A dropdown menu set to 'None'.
- Account Type:** A dropdown menu set to 'Pre-Paid'.
- Balance Management:** A dropdown menu set to 'Server Based'.
- Device-Server Balance Check:** An unchecked checkbox.
- Cafeteria Usage Policy:** Two input fields labeled 'ID' and 'Name'.

Settings

Enable Account - Select this checkbox to enable Cafeteria account access for the selected user.

Enable Offline Transaction- Select the desired option from the drop-down list for the user to perform the offline transaction

- Select **None**, if you do not want to allow transactions to be made by the user when the device is in offline mode.

- Select **Allow With Discount**, if you want to allow transactions with discount to be made by the user, when the device is in offline mode.
- Select **Allow Without Discount**, if you want to allow transactions without discount to be made by the user, when the device is in offline mode.

Enable Account	<input checked="" type="checkbox"/>
Enable Offline Transaction	<div> <div>Allow With Discount</div> <div>None</div> <div>Allow With Discount</div> <div>Allow Without Discount</div> </div>
Discount Level	

Discount Level - Select the appropriate discount level from the drop down list as shown.

Discount Level	<div> <div>None</div> <div>None</div> <div>Discount Level 1</div> <div>Discount Level 2</div> <div>Discount Level 3</div> <div>Discount Level 4</div> </div>
Account Type	

Account Type - Specify the account type as **Pre-Paid** or **Post-Paid** by selecting from the drop down list.

Pre-paid Account

- For **Pre-Paid** account type, specify whether the **Balance Management** should be **Device-based** or **Server-based**.
- When Balance Management is selected as **Server based**, then you can enable **Device-Server Balance Check**. This will allow Device to check Server-side balance before allowing transaction. For this, Device and Server must be connected.

Post-paid Account

- For **Post-Paid** account type, enter the **Allowed Usage Per Month** based on which monthly dues for the user can be calculated.

Enable Account	<input checked="" type="checkbox"/>
Enable Offline Transaction	None
Discount Level	None
Account Type	Post-Paid
Allowed Usage Per Month *	0.00
Cafeteria Usage Policy	<div>ID</div> <div>Name</div>

Cafeteria Usage Policy- Select the cafeteria usage policy to assign to the user based on which cafeteria transaction restrictions will be applied to the user.

Contract Worker Management (CWM)

This tab is available for configuration only for the *Contract Worker Management (CWM)* module user when a existing worker is selected from the *User List*. This enables the administrator to assign Contractor, Work Order, Skills and PPE (Personal Protective Equipment) to the selected worker as well as add ID Proof and Address Proof.

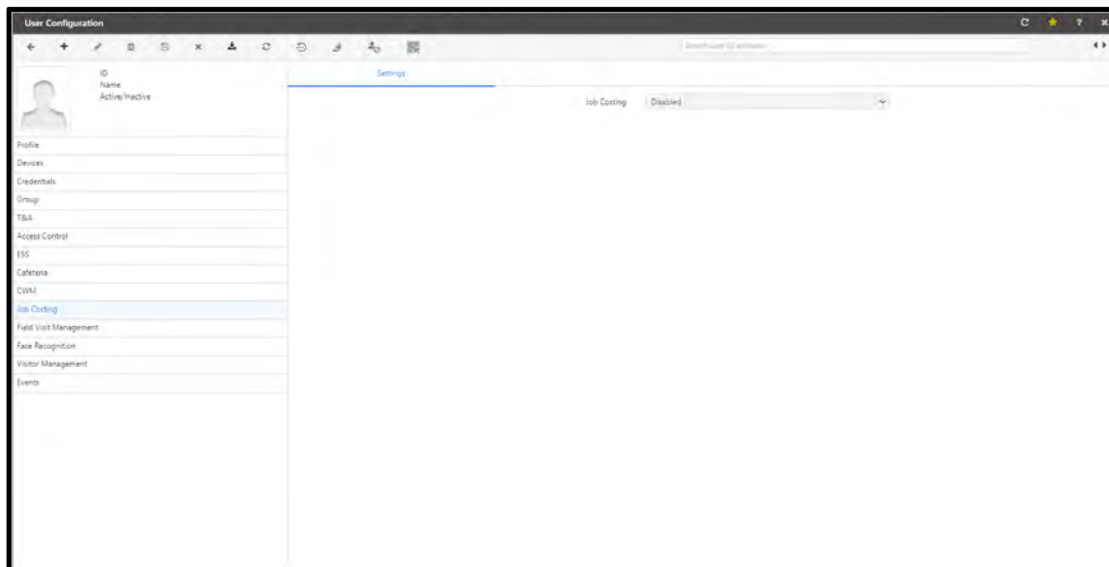
The CWM tab for the worker is shown as below.

The screenshot shows the 'User Configuration' window for a user named 'Parth parth' who is 'Active'. The left sidebar lists various configuration tabs: Profile, Devices, Credentials, Group, T&A, Access Control, ESS, Cafeteria, **CWM** (highlighted), Job Costing, and Field Visit Management. The main area is divided into two sections: 'Assignment' and 'Other Details'. The 'Assignment' section is currently active and shows fields for Skill (1), Contractor (Ct2), Work Order (W11), Assignment Period (31/03/2017 to 04/05/2017), Assignment Status, and Approval Stage (1). The 'Other Details' section shows fields for Skill-1, Contractor2, Work order1, and Approval Stage-1. Below these sections is a table with columns: Level, Induction Level Name, Status, and Details. The table currently displays 'No Data'.



To know about the configuration of worker in CWM tab for Assignment and Other Details ,see CWM section in [“Worker Profile”](#)

Job Costing



To assign the user for job costing feature, select the Job costing tab. The following page appears.

Job Costing- Select the option **Enabled** from the drop down list to enable Job Costing feature for the user.




The Job costing events for the past dates will be reflected only when the Reprocess Attendance events is enabled while processing daily attendance.

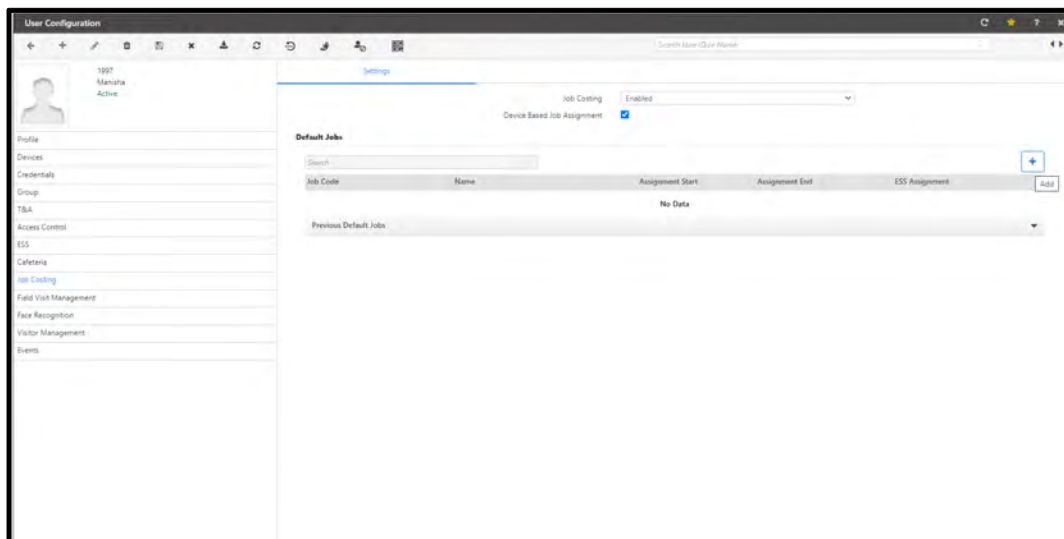
Device based Job Assignment- Enable this checkbox so that Job codes are assigned to the user as per device configuration on which user punches.

If Job Costing is enabled and “Device based job assignment” is checked, then it will work in mixed mode.

In this user can be working a default job even when assignment type is device-based. This will allow existing job selection from device along with few additional options like 'Continue Current Job' and 'Start Default Job'.

Default Jobs: Click **Add**  to assign default jobs to the user.

The Multiple default jobs can be assigned with non-overlapping Assignment Date Ranges. Only 'In Progress' Jobs can be assigned.

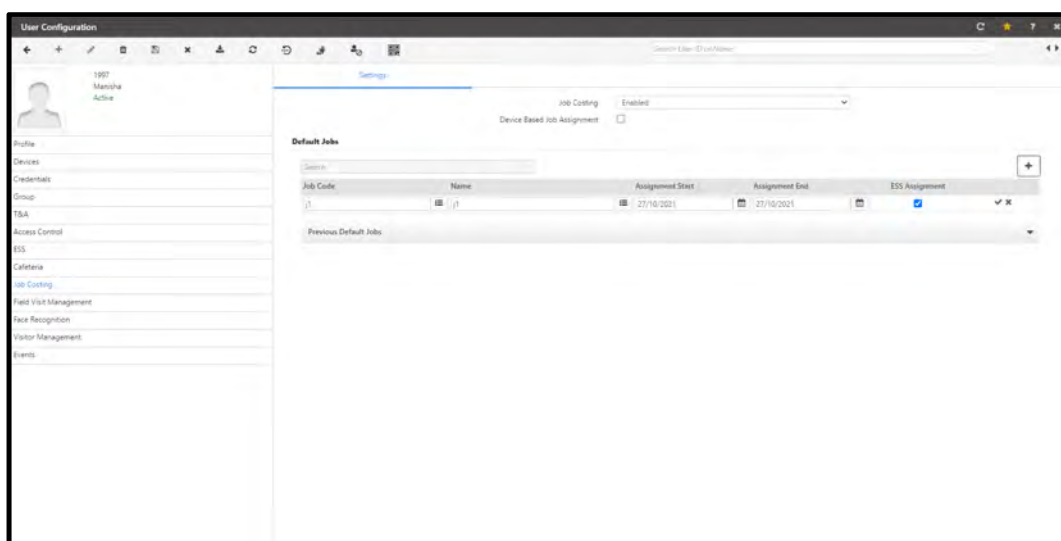



- **Job Code:** Select the desired Job Code from the pick list.
- **Name:** Select the desired Name from the pick list.
- **Assignment Start** and **Assignment End:** Define the start date and End date for the selected job from the calendar.
- **ESS Assignment:** The check box is enabled by default. This Job will be displayed in the list of Jobs assigned to the user through the ESS login. If you do not want this job to be displayed, clear the check box.



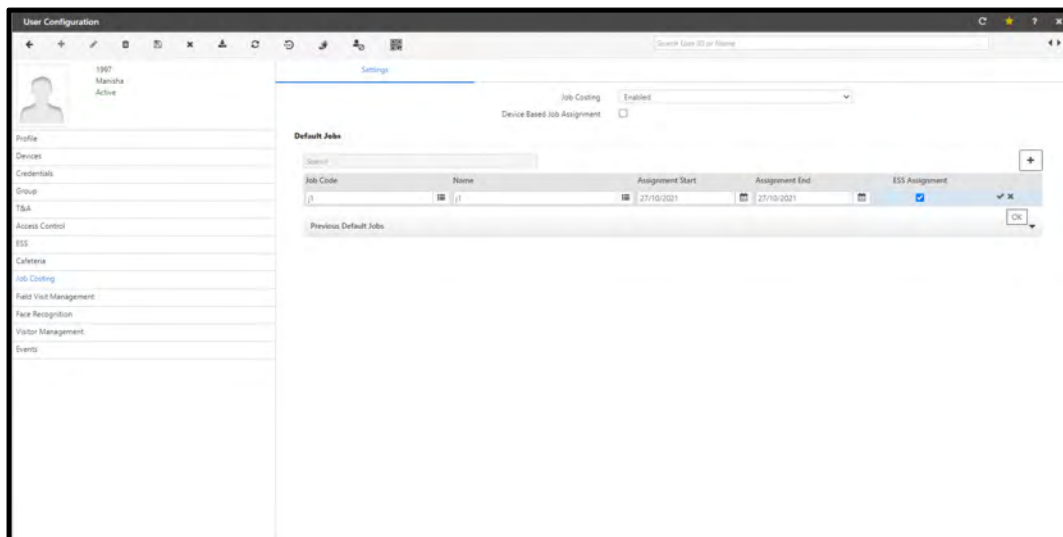
The Jobs created here which are In-progress, Assigned and have the ESS Assignment check box enabled will be displayed in the **ESS login > Job** drop-down while Marking a Punch.

The ESS Assignment column will not be displayed if the **Show All Jobs while Punching** check box is enabled. For details, refer to “[Job Costing](#)” in “[Defining Global Policies](#)”.



Click **OK**  to save the details.

Default Jobs Grid will consist of currently assigned default jobs (i.e. Current Date is within the Assignment End Date).



Jobs are created from Job Processing and Costing module > Project Management> Job.



When job code is not assigned to user and user punches with that job code using Special function from door; then Reprocess Events should be enabled during Job Costing process to assign the actual job code to the job.

Example:

On date 15/01/2017, Assign Job-1 (15/01/2017 - 31/03/2017) as default.

On date 25/03/2017, Same Job-1 will be visible in default jobs grid.

Since date 01/04/2017 i.e. after the assignment end date, Job-1 will be moved from Default jobs grid to Previous Jobs Grid.

The applicable devices are:

- DOOR V3
- Wireless DOOR
- PVR
- NGT
- Vega Controller
- Door V4



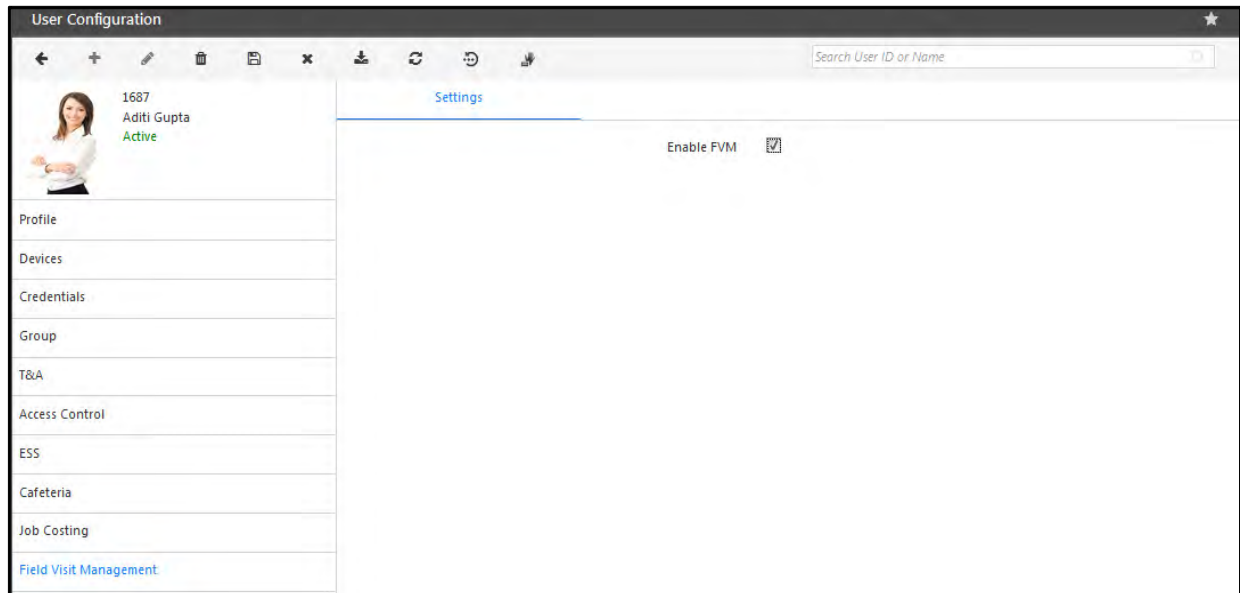
User configuration will be resent to devices only when there is some change in Job Assignment.

When new user is added or existing user's Enterprise group is changed. Then if user is assigned to the Enterprise group with which Job costing parameters are associated, then the configured job costing parameters will be reflected in User Configuration > Job Costing Tab

Field Visit Management

In this module, you can assign schedules to the users and keep a track of their activities, while on site and also check if the assigned tasks are being fulfilled correctly or not.

The Field Visit Management tab appears as shown below:

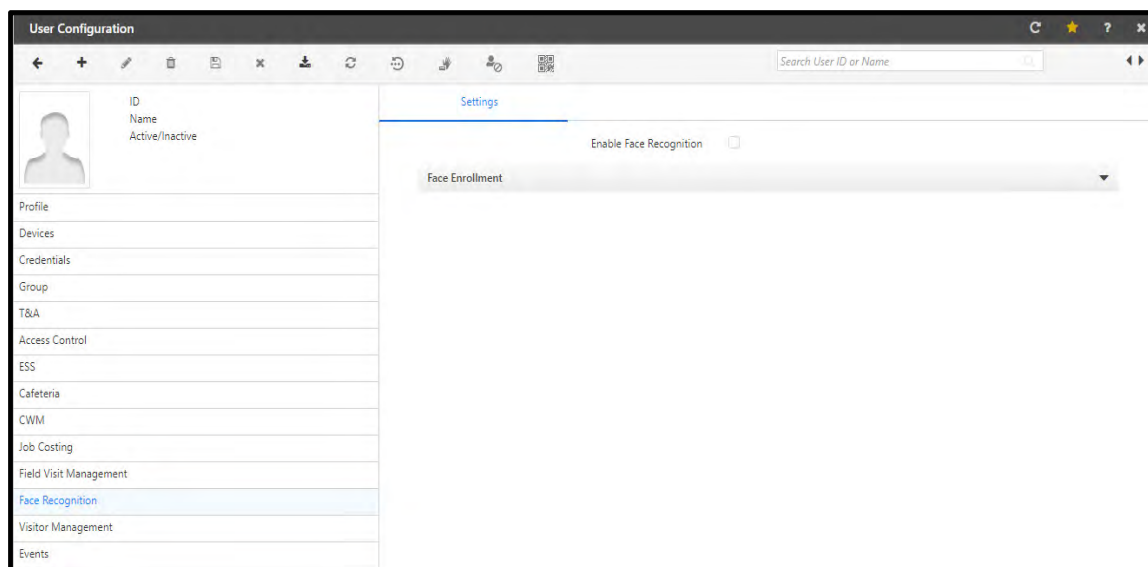


In the **Settings** tab, check the **Enable FVM** box to consider the selected user as FVM user. Then click **Save** button to save the changes.

Face Recognition

In this feature, user can access the device or mark the attendance by verifying his Face as the credential.

The Face Recognition tab appears as shown below:



Settings

Enable Face Recognition: Check this box to enable Face Recognition feature for the user.

1. Create a User. Enable Face Recognition feature.
2. Assign Vega, FMX, ARGO or AGRO FACE door to the user.
3. Connect the FR module and IP Camera to the network. Ensure that COSEC Device, FR Module and IP Camera are in the same subnet.

If you are connecting the ARGO FACE device, it has an in-built FR Module and camera.

4. Configure IP camera to be used for capturing face credential. Select the Capturing device as IP Camera in Video Surveillance section of Device Configuration and configure the snapshot URL.
5. Configure FR settings on Device. Go to Identification Server of Device Configuration. Enable FR and select the Face capturing mode. Select the FR mode as Local/Server-Assisted. Enter the FR Server Address as the IP address of FR module. Enter FR Server Port as 12000 which is default port for Identification Service.
6. Now Tap on Device screen. The motion streaming of camera will appear on COSEC Device.
7. Now Enroll the user for Face credential using Enroll Utility.
8. When you show your face in front of camera, the camera will capture your face and identify with the enrolled template. If it matches, you will be allowed access on the door.

The screenshot displays the Matrix COSEC MONITOR software interface. The top menu bar includes File, Device, Tools, and Help. The left sidebar contains a 'Features' section with icons for Alarms, I/O Link, Soft Override, Events, Exceptions, Time Triggered Functions, and EMAP. The main window is divided into two panes. The top pane, titled 'Devices - All', shows a table of devices with columns for Name, Site, IP/R5485 Address, MAC/UUID, Type, and Status. The bottom pane, titled 'Events', shows a table of events with columns for Sr.No., Date Time, Type, Device, Category, and Detail. The 'User Details' section on the left shows a user profile for 'User ID: 2' with a photo and the name 'Sheetal'. The 'Device' section shows 'Vega Controller-Device-5' with a status of 'Allowed'.

Name	Site	IP/R5485 Address	MAC/UUID	Type	Status
Panel Lite V2-Device-1		192.168.104.111	00:18:09:04:65:D1	Panel Lite V2	Disconnected
PVR as Panel Door	Site-1	192.168.104.113	00:18:09:03:F2:B0	Panel Lite V2 Door	Off-Line
NGT Direct Door	Site-1		DF:E4:36:35:43:EB	NGT Direct Door	Disconnected
Wireless Door	Site-1		DF:DD:47:E5:FB:C5	Wireless Door	Disconnected
PVR Door- Direct Door	Site-1		34:36:37:75:E5:54	PVR Door	Disconnected
Vega Controller	Site-1		CD:E6:73:56:F5:65	Vega Controller	Disconnected
Vega Controller-Device-5	Site-1	192.168.104.71	00:18:09:05:B6:89	Vega Controller	Connected
Panel V2 Device-1	Site-1	192.168.104.114	00:18:09:05:3E:E7	Panel V2	Disconnected

Sr.No.	Date Time	Type	Device	Category	Detail
527	07/12/2018 06:51:06 PM	Vega Controller	Vega Controller-Device-5	Request	← Login Request Received.
528	07/12/2018 06:51:06 PM	Vega Controller	Vega Controller-Device-5	ACK	→ Login Success Poll Duration: 3 Poll Interval: 2
529	07/12/2018 06:51:06 PM	Vega Controller	Vega Controller-Device-5	Request	← Message Request Received
530	07/12/2018 06:51:06 PM	Vega Controller	Vega Controller-Device-5	Command	→ Event Request for RollOver: 0 Event Seq. No.: 113
531	07/12/2018 06:51:06 PM	Vega Controller	Vega Controller-Device-5	Other	← Start Of Event
532	07/12/2018 06:51:07 PM	Vega Controller	Vega Controller-Device-5	Command	→ Set Date & Time
533	07/12/2018 06:51:07 PM	Vega Controller	Vega Controller-Device-5	ACK	← Set Date & Time Command Successful
534	07/12/2018 06:51:07 PM	Vega Controller	Vega Controller-Device-5	Other	→ End Of Message
535	07/12/2018 06:52:23 PM	Vega Controller	Vega Controller-Device-5	User	→ Allowed with FACE. User ID: 2 [3] Event Date Time: 07/12/2018 06:52:22 PM
536	07/12/2018 06:52:23 PM	Vega Controller	Vega Controller-Device-5	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 113
537	07/12/2018 06:52:25 PM	Vega Controller	Vega Controller-Device-5	System	→ Camera Event for Time Stamp [Fail] received for Event Sequence No: 113 and Rollover: 0 Event Date...
538	07/12/2018 06:52:25 PM	Vega Controller	Vega Controller-Device-5	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 114

Face Enrollment

This functionality enables the SA to enroll face/s against a user. Face Enrollment can be done by either directly uploading the images of the desired user or by capturing and then uploading the images.



To use the capture functionality for images, make sure you have a secure login, that is you have logged in using HTTPS.

Using Face Enrollment you can:

- replace existing images (if any) with new images
- add new images
- remove enrolled images

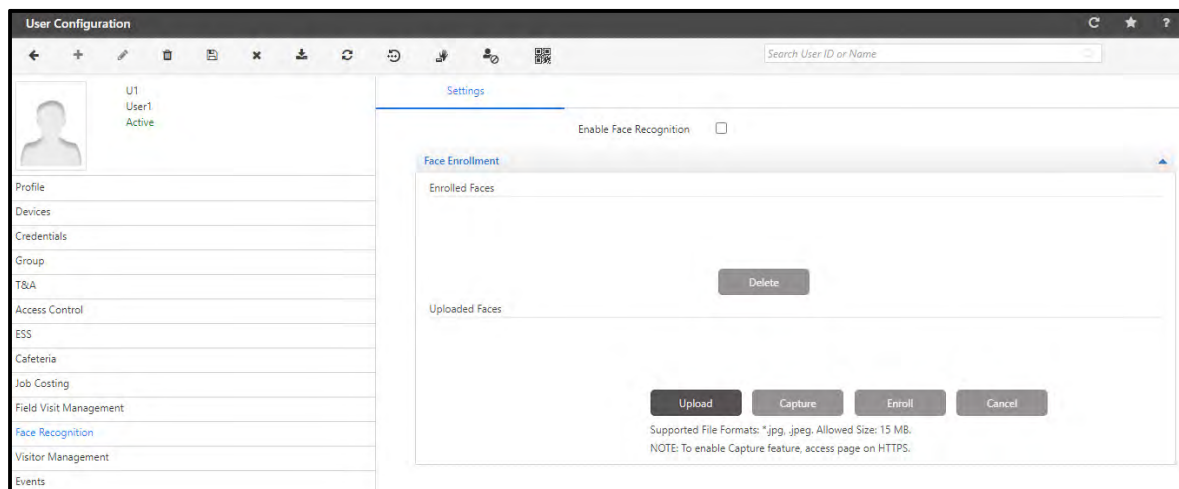
Click the **Face Enrollment** collapsible panel in order to enroll faces against a user.



For Face Enrollment via Web feature to work, ensure that Identification Service is defined in COSEC Admin > License and Service. For more details refer Admin Management Portal User Manual.

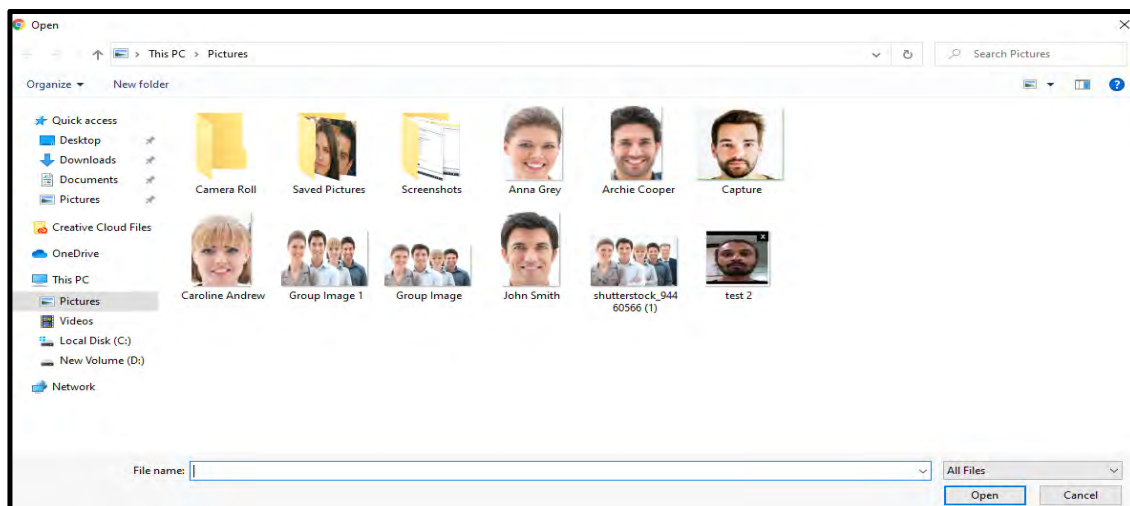
To Upload the images directly, refer **“Upload”**

To Capture and then upload the images, refer **“Capture”**

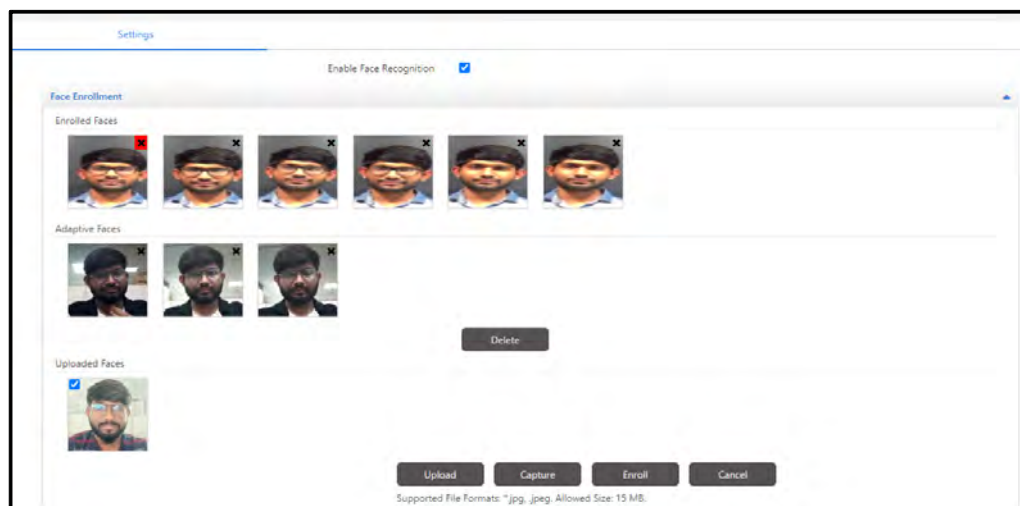


Upload

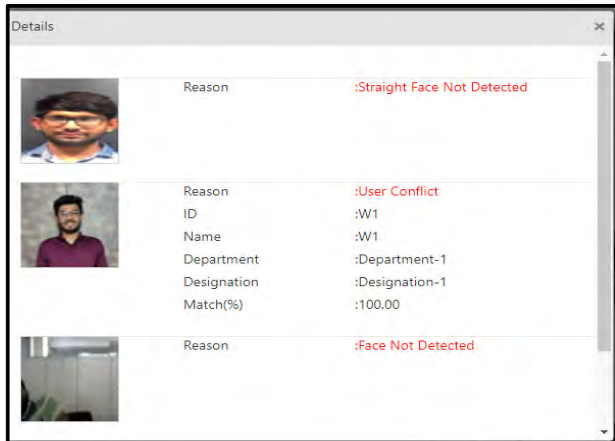
- In order to upload face/s against a user click **Upload** in **Face Enrollment**.
- Browse to select the desired file from your local PC wherein the image is stored.
- Make sure the selected image is in the .jpg or .jpeg format.
- Click **Open**.



- All the faces that are uploaded will be reflected in **Uploaded Faces** Grid.
- Select the face/s that you want to enroll by clicking the checkbox provided on the top left corner of the uploaded face.

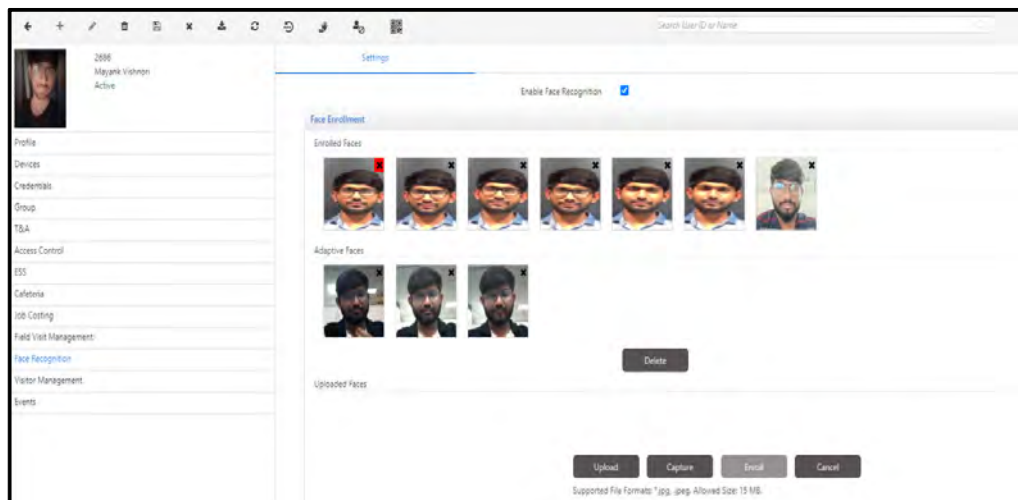


- While uploading a face if any error occurs, the **Info** icon will be displayed.
- On clicking the **Info** icon a pop up with the discarded face/s will be displayed along with the possible reason for discarding the image.

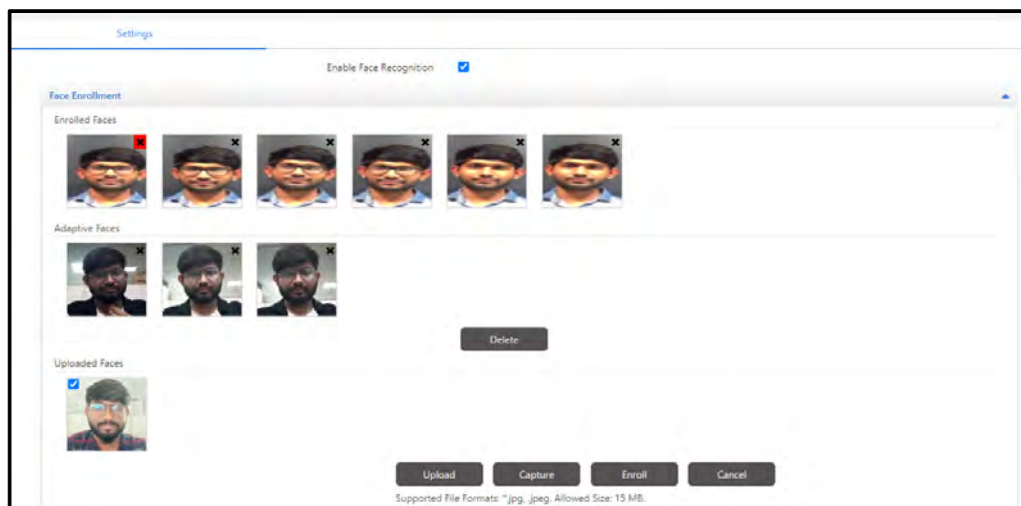


Let us understand this with the help of an example, you have uploaded 5 faces out of which 3 got discarded and then again you upload 5 more faces out of which 2 got discarded then the pop-up will display all the 5 discarded faces with the probable reasons for discarding.

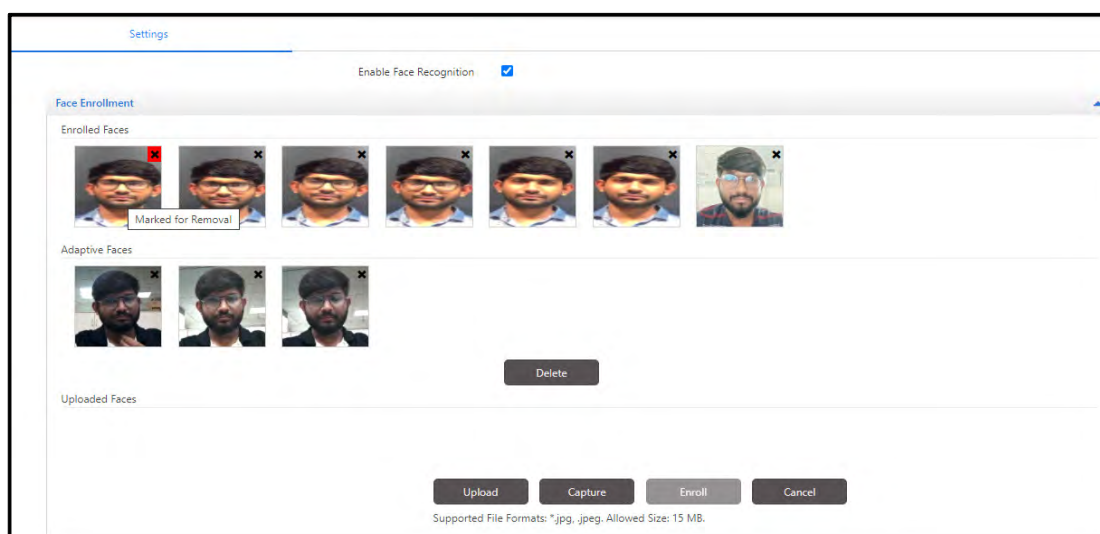
- To add the new image as the enrolled face,
- Select the check box of the desired image under **Uploaded Faces**.
- Click **Enroll** in order to enroll the selected face/s. The selected face/s will be reflected in the **Enrolled Faces** grid.




- To replace an existing enrolled faces,
- Click on the desired image, the red cross icon appears on the top right corner of the face under **Enrolled Faces**.
- Select the check box of the desired image under Uploaded Faces.
- Click **Enroll**.





- To remove an existing enrolled faces,
 - Click on the desired image, the red cross icon appears on the top right corner of the face under **Enrolled Faces**.
 - Click **Delete**.



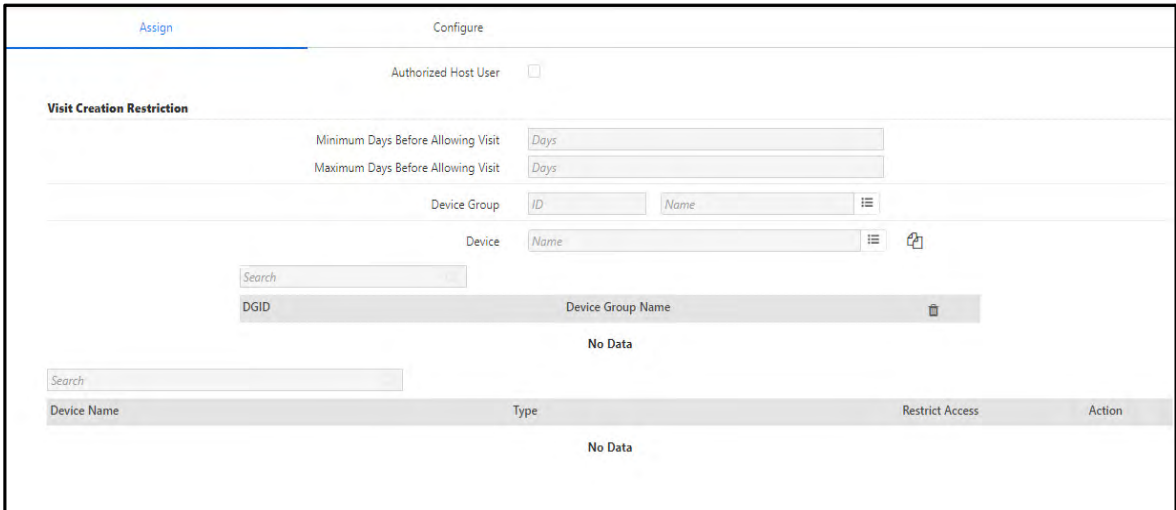
*Make sure the number of faces you consider for enrollment is lesser than or equal to the defined value in **Maximum No. of Faces** in Admin >System configuration> Global Policy >User.*

- If there is an occurrence of an adaptive face, it will be displayed under the **Adaptive Faces** grid, a sub-section under **Enrolled Faces** grid. If you desire, you may delete the image. To do so, follow the same instructions as mentioned above.
- Click the Save  in order to save all the enrolled faces. The faces will be successfully saved and considered for face recognition.

- If the image captured is appropriate click the icon  . Now, you can again capture a new image if required.
- If the image clicked is not appropriate then click the icon  and a retake will be considered.
- After completing the capture, click **OK** to upload the image. Click **Cancel** if you desire to restart the **Capture**.
- The uploaded faces will be reflected in **Uploaded Faces** Grid.
- Now, refer to “[Upload](#)” for further instructions.

Visitor Management

In this page you can authorize a host user, restrict the visitor pre-registration on the basis of no.of days and assign device groups and devices to the visitors.



The screenshot shows the 'Configure' tab of the Visitor Management interface. It includes a checkbox for 'Authorized Host User'. Under 'Visit Creation Restriction', there are two input fields for 'Minimum Days Before Allowing Visit' and 'Maximum Days Before Allowing Visit'. Below these are sections for 'Device Group' and 'Device', each with a search bar and a list icon. At the bottom, there are two tables, both displaying 'No Data'.

Assign

- **Authorized Host User:** Select the checkbox to authorize a Host user. Once you authorize the host, the host user will be added in the list of Authorized Host Users in *Visitor Management> Utilities> Authorized Host Users*. For more information, refer “[Authorized Host Users](#)”.

Visit Creation Restriction

- **Minimum Days before Allowing Visit:** The minimum days configured in *Admin> System Configuration> Global Policy> Visitor Management* will be displayed here as the default value.

You can change the number of minimum days as per your requirement.


For more details, refer “[Visit Creation Restriction](#)” in *Admin> System Configuration> Global Policy> Visitor Management*.

- **Maximum Days Before Allowing Visit:** The maximum days configured in *Admin> System Configuration> Global Policy> Visitor Management* will be displayed here as the default value.

You can change the number of maximum days as per your requirement.

For more details, refer [“Visit Creation Restriction”](#) in *Admin> System Configuration> Global Policy> Visitor Management*.

- **Device Group:** Select the desired device group/s from the picklist to assign it to the Visitor.
- **Device:** Select the desired device/s from the picklist.

To add devices which are assigned to the host, click **Add Host's Devices** .

Configure

This option enables the Admin to change the settings of the devices assigned to the Visitor.

To know more about the configurations, refer [“Configure”](#) in *User> User Configuration> Devices*.

Panel Door

Assign	Configure
Device	Panel
Type	Panel
Active	<input checked="" type="checkbox"/>
VIP	<input type="checkbox"/>
Access Profile	Access Group-1
Functional Group	Staff
Home Zone	Zone-1
Visit Zone	Select
Access Route	Select

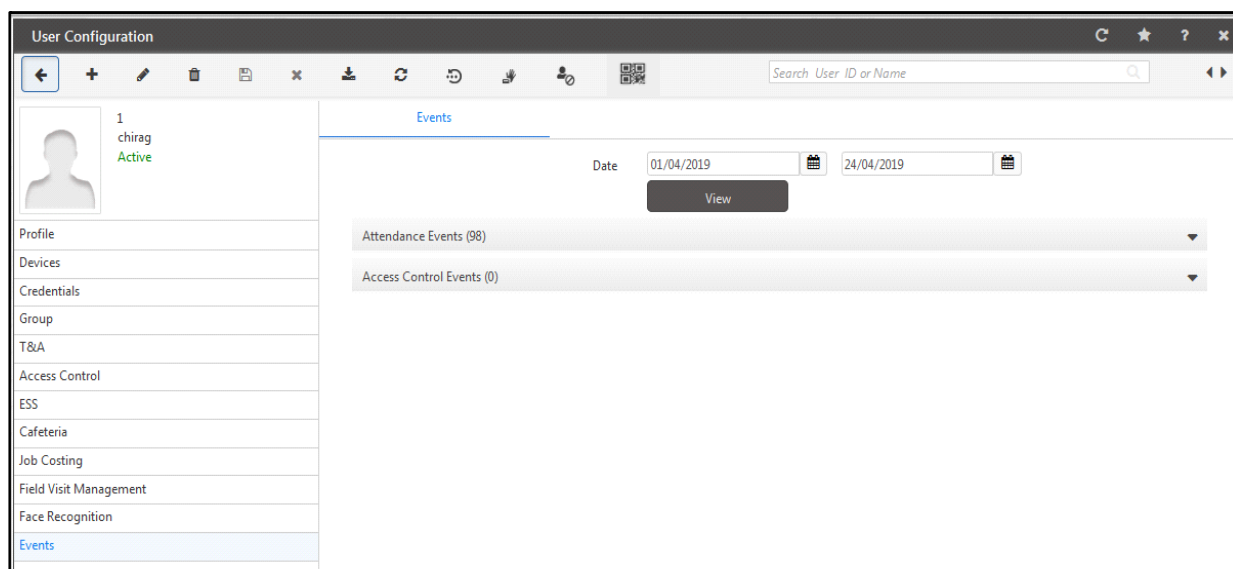
Direct Door

Configure	
Device	Argo Door
Type	ARGO
Active	<input checked="" type="checkbox"/>
VIP	<input type="checkbox"/>

Events

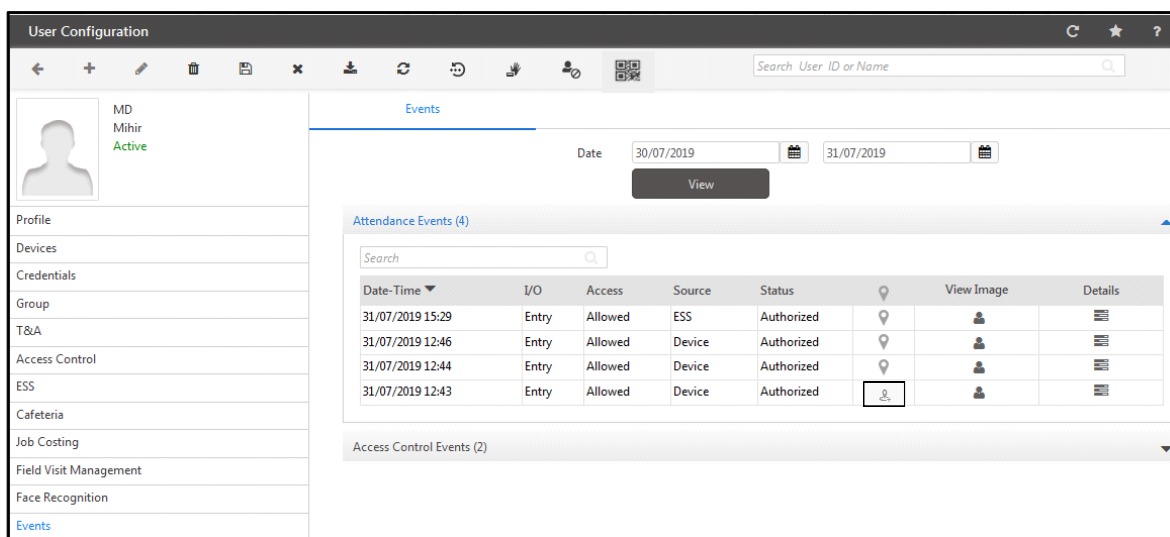
The Events tab is used for the security purpose by monitoring the users in the organization. The Attendance Events and Access Control Events can be viewed by filtering the date range.

In cases of infringement or suspicion; the security supervisor can blacklist, delete or inactivate the user creating problems in the organization.



Date: Select the date range for which events are to be viewed.

Click on **View** button to view the Attendance events and Access Control events.

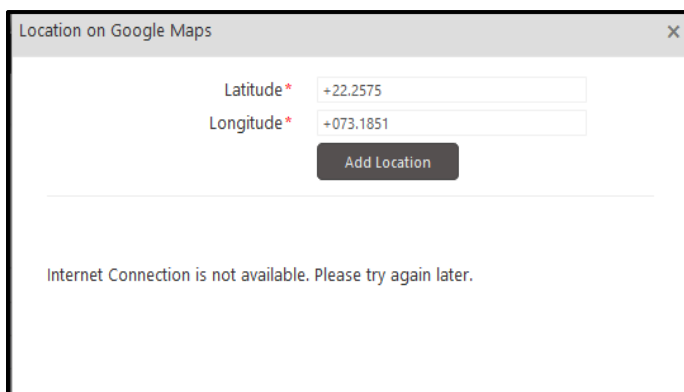


The Attendance Events shows the Date and time when the event is generated along with the I/O, Access, Source, Status and Location details. It also displays Image and Details of the punch.

The location details will display Latitude/Longitude or MAC address from where event has generated.

- You can view the location on Map if the GPS/GSM location is configured in Location Master by clicking on View Map icon.
- If the location is not configured in Location Master then you can add this location by clicking on **Add this Location** icon shown in above figure.

Now click on **Add Location** button which will redirect to Location Master page from where you can add this location.




Location on Google Maps

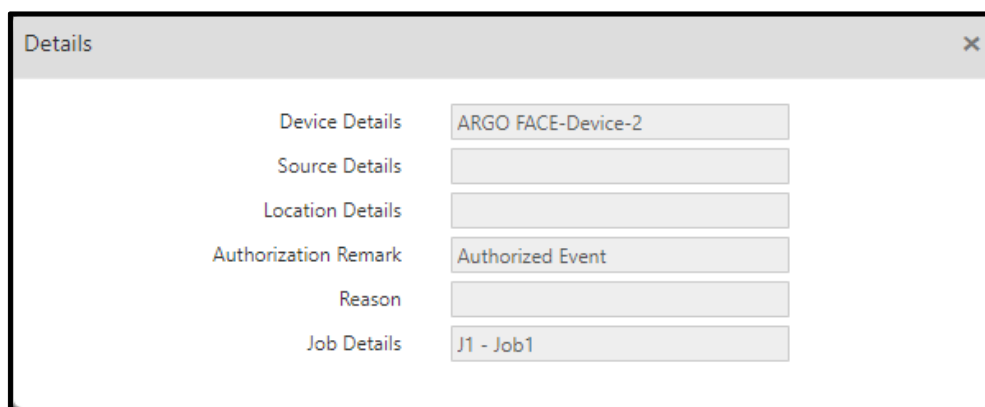
Latitude* +22.2575

Longitude* +073.1851

Add Location

Internet Connection is not available. Please try again later.

Click the **Details**  icon to view the event details of the corresponding user.



Details

Device Details ARGO FACE-Device-2

Source Details

Location Details

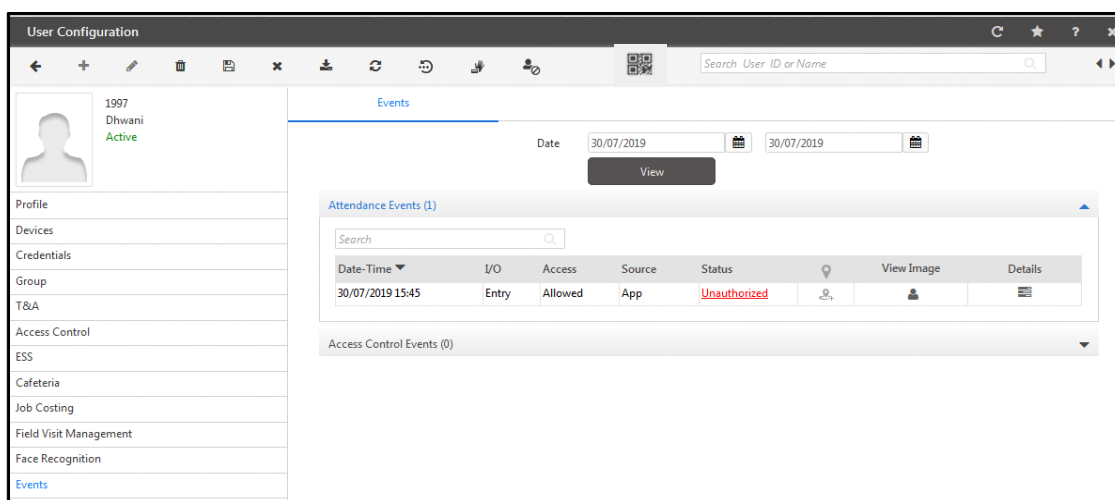
Authorization Remark Authorized Event

Reason

Job Details J1 - Job1

The Status of event, i.e. whether it is authorized or unauthorized is displayed under Status.

- If the status is Unauthorized, it will display a link as shown below, which on clicking will be redirected to Events Authorization Page as per login user's rights.



User Configuration

1907 Dhwani Active

Profile

Devices

Credentials

Group

T&A

Access Control

ESS

Cafeteria

Job Costing

Field Visit Management

Face Recognition

Events

Events

Date 30/07/2019 30/07/2019

View

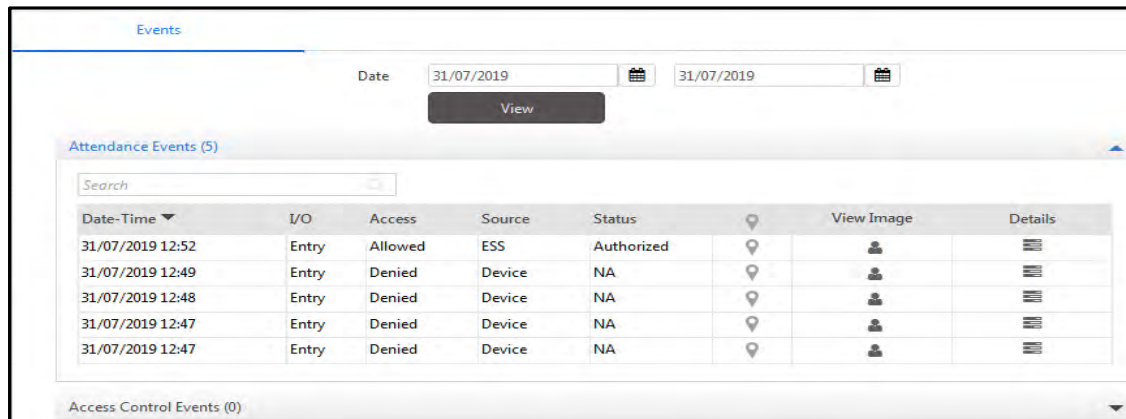
Attendance Events (1)

Search

Date-Time	I/O	Access	Source	Status	View Image	Details
30/07/2019 15:45	Entry	Allowed	App	Unauthorized		

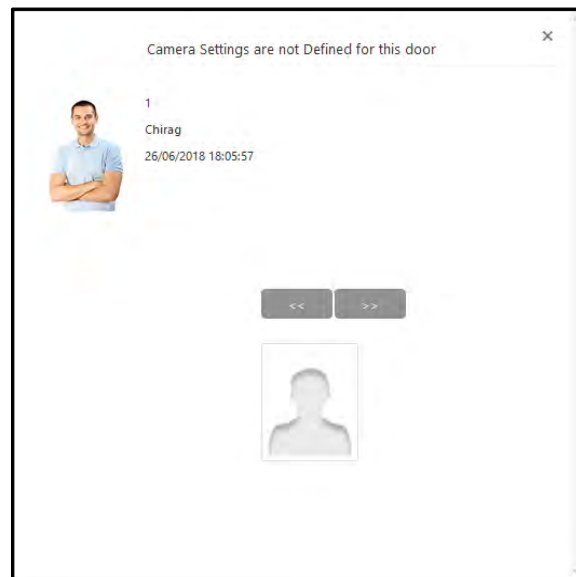
Access Control Events (0)

- If the status is shown as NA, then Authorized status will be Null and the access will be shown as **Denied** as shown below:




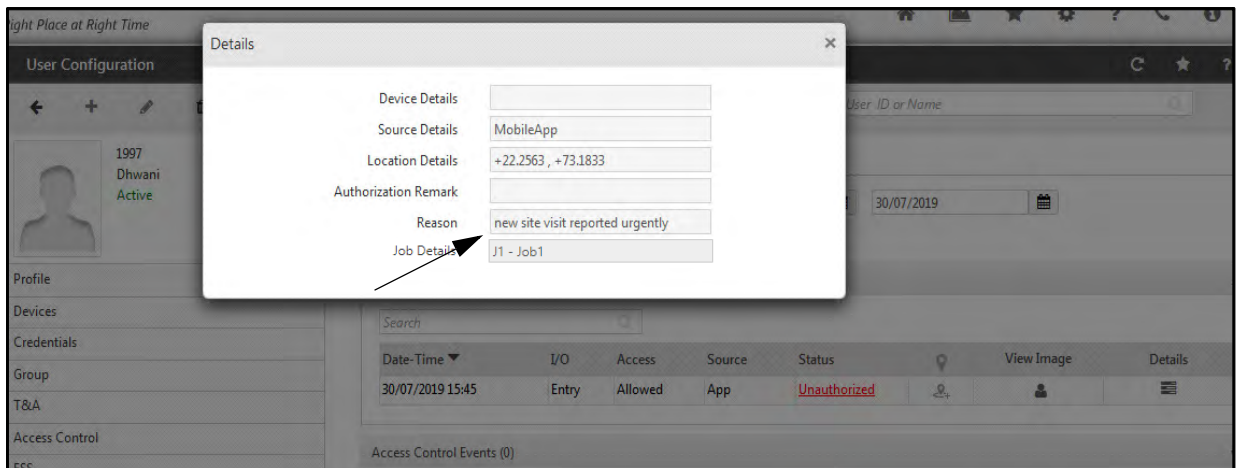
You can view the image captured by the Built-In Camera by clicking on **View Image** icon.

If there is camera to capture the image of the user punching on door; then his image will be captured and can be viewed for that event by clicking on View Image icon.



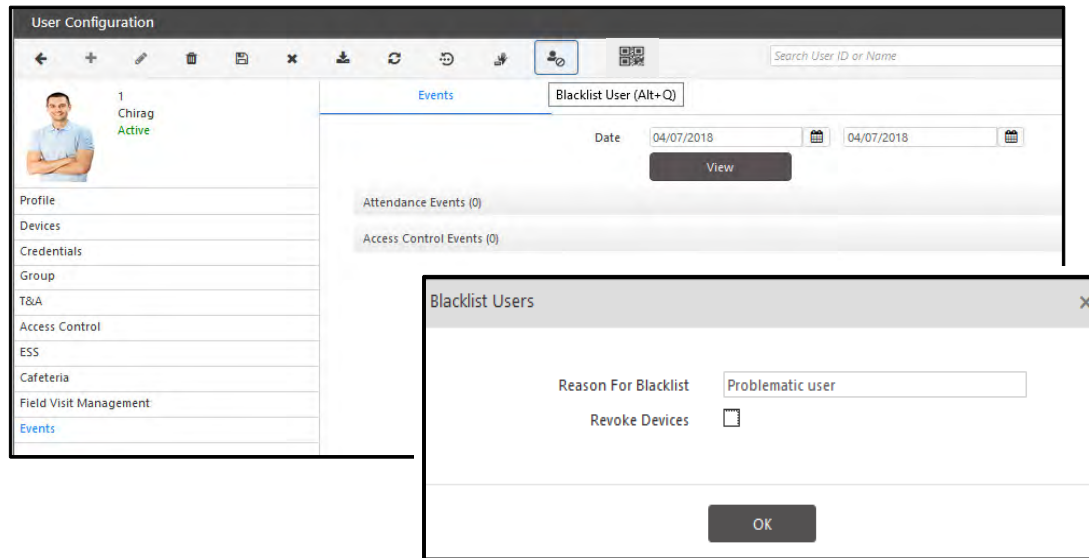
If the event is generated by API then there will not be any image popup window on clicking View Image icon.

The Reason for punching from unassigned location can be known by clicking on Details icon  as shown in the figure below:



Blacklist

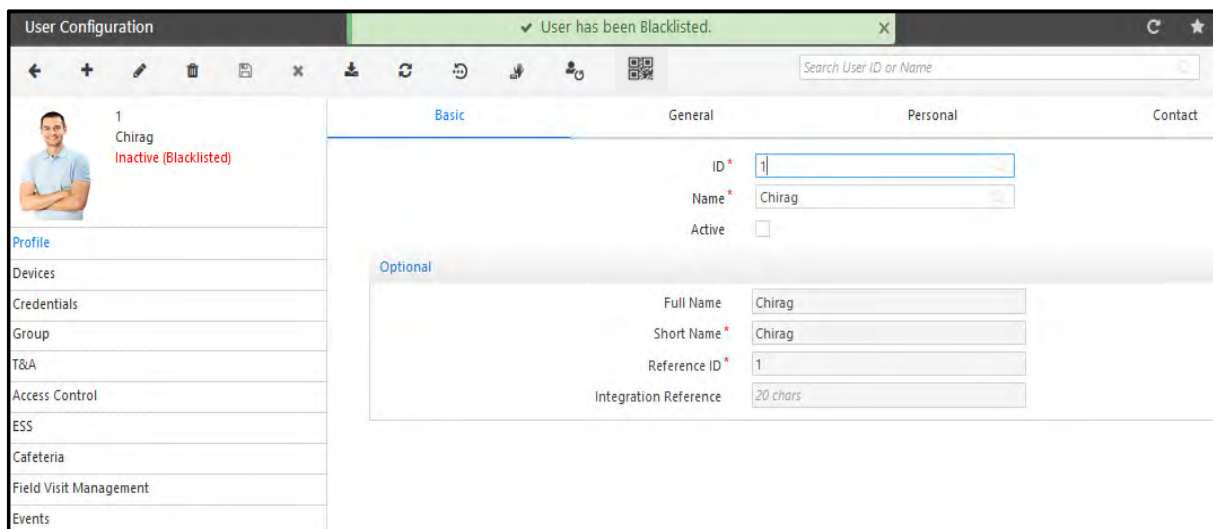
Click on the **Blacklist User** button. The Blacklist Users window appears.



Enter the **Reason** for Blacklisting the user.

Click on **Revoke Devices** to remove the assignment of devices from the user.

Click **OK** and **Save** button to save the changes. The user will be blacklisted and Inactive as shown below.



The blacklisted user can be revoked by clicking **Restore and Activate User** button. It will make the user active.

User Configuration

+
✖

1

Chirag

Inactive (Blacklisted)

Profile

Devices

Credentials

Group

T&A

Access Control

ESS

Cafeteria

Field Visit Management

Events

Basic

Restore and Activate User (Alt+Q)

Personal

Contact

ID *

Name *

Active

Optional

Full Name

Short Name *

Reference ID *

Integration Reference

1

Chirag

☐

Chirag

Chirag

1

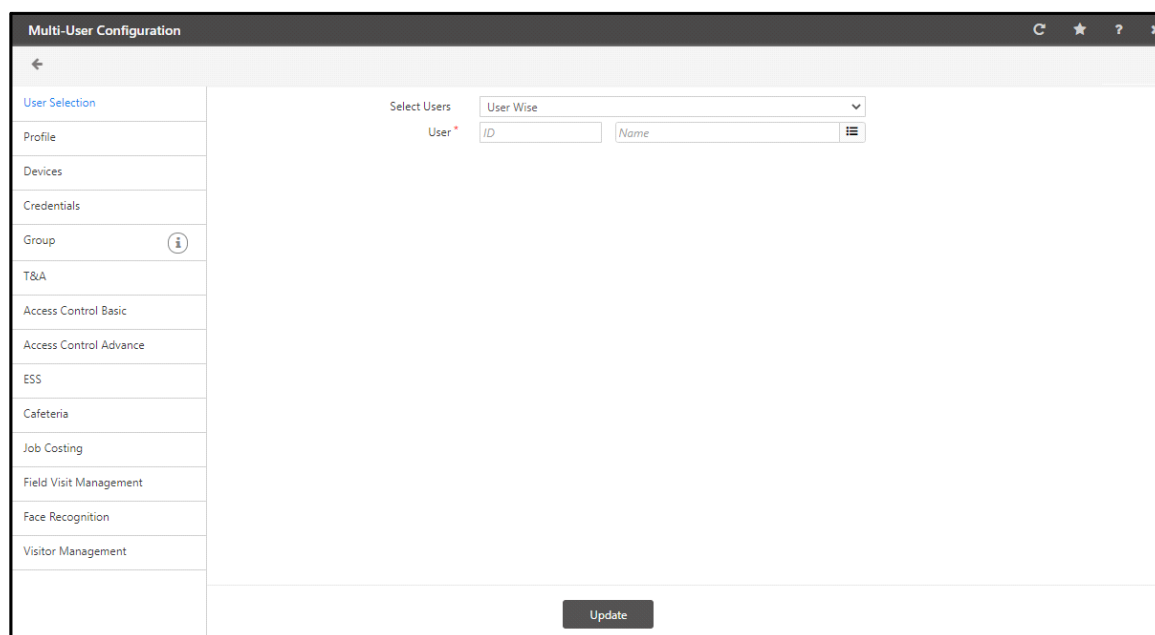
20 chars

Multi-User Configuration

COSEC provides the option for an HR administrator to apply a common configuration to multiple users at one go. This is not only convenient, but also saves the time required to configure each user individually. This feature can be useful when the same user configuration is applicable to more than one user defined in the COSEC database.

To access this functionality, select the **Users module > Multi-User Options > User Configuration**.

The **Multi-User Configuration** page opens as shown below.



User Selection

Select the users based on the filters of

- **User Wise:** Select random users by selecting the user from picklist.
- **Group Wise:** Select all users in an enterprise group using the **Select Group** drop down list.
- **ALL:** Select all active users in the system.

Click the **Update** button to apply all configurations on the selected users.



Configurable parameters on the **Multi-User Configuration** page can be activated using the **Update** checkbox for each option. Selecting this checkbox will make the parameter enabled for modification using the **Set New Value** column.

Update	Field Name	Set New Value
<input checked="" type="checkbox"/>	Active	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Birthday Message	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Personal Mobile	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Personal Email	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Official Mobile	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Official Email	<input checked="" type="checkbox"/>

The **Multi-User Configuration** page is divided into following sections. Select the individual sections and set the necessary configuration for the selected multiple users. The detailed configuration has been explained in the following sections.

- [“Profile”](#)
- [“Devices”](#)
- [“Credentials”](#)
- [“Group”](#)
- [“T&A”](#)
- [“Access Control Basic”](#)
- [“Access Control Advance”](#)
- [“ESS”](#)
- [“Cafeteria”](#)
- [“Job Costing”](#)
- [“Field Visit Management”](#)
- [“Face Recognition”](#)
- [“Visitor Management”](#)

To configure the parameters of the following tabs, you need to first select the **Update** checkbox of the desired parameter.

Profile

To update the profile of multiple users, select **Multi-User Configuration > Profile**.

Update	Field Name	Set New Value
<input checked="" type="checkbox"/>	Active	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Birthday Message	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Personal Mobile	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Personal Email	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Official Mobile	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Official Email	<input checked="" type="checkbox"/>

Update

1. Select the **Active** checkbox to activate all selected users.
2. Enable the **Birthday Message** checkbox for the selected users to receive a birthday message on NGT direct door.
3. Select the appropriate checkboxes to specify which contact details must be enabled for alert messages to be sent to selected users.
4. Click on **Update** to update the profile for selected users.

Devices

The **Devices** section enables the administrator to add and assign/revoke a device group and/or randomly selected devices to multiple users at the same time.

To access this configuration, On the **Multi-User Configuration** page, select the **Devices** section as shown below.

To assign Device/Device Group to multiple users at the same time,

- Select the **Assign Device/Device Group** option.
- Under **Update**, select the **Device Group** check box to enable.


Under **Set New Value**, select the desired device group from the **Device Group** picklist you wish to assign to the selected users.

The selected device group appears in the grid as shown above.

- You can also select individual devices. By default, under **Update** the **Device** check box is enabled.

Under **Set New Value** from the **Device** picklist, select the desired devices you wish to assign to the selected users.

The selected devices appear in the grid as shown above.

- Click **Configure**  to configure the selected device for multiple users.

The Configuration page of the selected Device appears as shown below.

Panel Lite V2 - Configuration

Device: Panel Lite V2

Type: Panel Lite V2

Active: ☒

VIP: ☐

Absentee Rule: ☐

Absent Day(s) Count: 60

Access Profile: Group-1

Functional Group: Staff

Home Zone: Zone-1

Visit Zone: Select

Access Route: Select

OK Close



The Device and Type will be shown as per the device selected from the grid.

You can enable and configure Access Control features from the Configuration page.

- Click **OK**.
- Click **Update** to assign the selected devices/device groups with configuration to multiple users.

Similarly to revoke Device/Device Group from multiple users at the same time,

- Select the **Revoke Device/Device Group** option.
- Under **Update**, select the **Device Group** check box to enable.

Under **Set New Value**, select the desired device group from the **Device Group** picklist you wish to revoke from the selected users.

The selected device group appears in the grid.

- You can also select individual devices. By default, under **Update** the **Device** check box is enabled.

Under **Set New Value** from the **Device** picklist, select the desired devices you wish to revoke from the selected users.

The selected devices appear in the grid as shown above.

- Click **Update** to revoke the selected devices/device groups from multiple users.

Credentials

To update the credentials for multiple user, select the **Credentials** section as shown below.

The screenshot shows the 'Multi-User Configuration' interface. On the left is a sidebar with a back arrow and a menu containing 'User Selection', 'Profile', 'Devices', 'Credentials' (highlighted in blue), and 'Group'. The main area contains a table with three columns: 'Update', 'Field Name', and 'Set New Value'. The table has three rows: 'Biometric Group No.' with a checked 'Update' checkbox and a text input field containing '123'; 'Roaming User' with a checked 'Update' checkbox and a checked checkbox; and 'Enable Self-Enrollment' with a checked 'Update' checkbox and a checked checkbox. An 'Update' button is located at the bottom right of the table area.

Update	Field Name	Set New Value
<input checked="" type="checkbox"/>	Biometric Group No.	<input type="text" value="123"/>
<input checked="" type="checkbox"/>	Roaming User	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Enable Self-Enrollment	<input checked="" type="checkbox"/>

Update

1. Enter the **Biometric group number** to be assigned to the users. It is a number allotted to a group of users assigned on a device. This enables the device to match a finger/palm credential against only those users who are part of the same Biometric Group thus reducing processing time.

This value is used for Finger/Palm Identification of user on Identification Server in shorter time span considering user first specifies Group No and then punches on the device.

Identification Server will be allocating templates to its child threads on the basis of this field.

2. You can mark the user as **Roaming user** for the users who are field engineers, partners etc who report to office rarely. When such users mark their punch after pressing 0 on door, then they will be identified from the Roaming user group.

The Identification server will maintain a list of users along with their templates to be considered as roaming/remote users.

3. Select the **Enable Self-Enrollment** checkbox to allow users to enroll themselves in COSEC using already provided access cards/PIN. The self-enrollment feature can be especially beneficial for organizations with large number of employees.

Group

This section enables the administrator to select Enterprise groups, Reporting group, Approval Policy, Leave group and Week off for assigning to multiple users. To access this configuration, select the **Group** section as shown.

	Update	Field Name	Set New Value	
			ID	Name
Organization	<input type="checkbox"/>		ID	Name
Branch	<input type="checkbox"/>		ID	Name
Department	<input type="checkbox"/>		ID	Name
Section	<input type="checkbox"/>		ID	Name
Category	<input type="checkbox"/>		ID	Name
Grade	<input type="checkbox"/>		ID	Name
Designation	<input type="checkbox"/>		ID	Name
Custom Group 1	<input type="checkbox"/>		ID	Name
Custom Group 2	<input type="checkbox"/>		ID	Name
Custom Group 3	<input type="checkbox"/>		ID	Name
Reporting Group	<input checked="" type="checkbox"/>		2	ACTA Group
Approval Policy	<input checked="" type="checkbox"/>		5	Matrix Approval Policy
Leave Group	<input type="checkbox"/>		ID	Name
Week Off Group	<input type="checkbox"/>		ID	Name

Update

1. Select a group from the respective group picklist to be assigned to the user.
2. Click on **Update** to update the group change for the users.



The **Leave Group** and **Week Off Group** option is available for multi-user configuration only with the **T&A** add-on module.

For detailed description refer to User Configuration> Group

The picklist options that appear in each enterprise group will be as per the rights assigned to the SA. For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#).

T&A

The T&A section enables the administrator to set attendance configuration for multiple users and to specify T&A policies to be assigned. This section is available only with a *Time and Attendance* add-on module license.

To access this configuration, select the **T&A** section as shown below.

Update	Field Name	Set New Value
<input type="checkbox"/>	Enable Attendance Calculation	<input type="checkbox"/>
<input type="checkbox"/>	Restrict Half Day Considerations	<input type="checkbox"/> ⓘ
<input type="checkbox"/>	Attendance Marking Type	Normal
<input type="checkbox"/>	Min Working Hours Required For Full Day	
<input type="checkbox"/>	Min Working Hours Required For Half Day	
<input type="checkbox"/>	Max Punches To Be Considered	Select
<input type="checkbox"/>	Bypass Finger/Palm/Face For Attendance	<input type="checkbox"/>
<input type="checkbox"/>	Max Short Leaves Allowed	
<input type="checkbox"/>	OT/C-OFF Eligibility	None
<input type="checkbox"/>	Authorize C-OFF On	<input type="checkbox"/> WO <input type="checkbox"/> PH <input type="checkbox"/> WO/PH <input type="checkbox"/> FB <input type="checkbox"/> RD <input type="checkbox"/> Normal Day
<input type="checkbox"/>	Bus Route	ID Name
<input type="checkbox"/>	Enable Site Based Auto Tour Application	<input type="checkbox"/>
<input type="checkbox"/>	Tour	Select
<input type="checkbox"/>	Base Site Selection	ID Name ⓘ
<input type="checkbox"/>	Auto Authorize Site Based Tour Application	<input type="checkbox"/>

<input type="checkbox"/>	Enable Location Based Auto Tour Application	<input type="checkbox"/>
<input type="checkbox"/>	Tour	Select
<input type="checkbox"/>	Base Location Assignment	All
<input type="checkbox"/>	Location	Code Name ⓘ
<input type="checkbox"/>	Location Group	ID Name ⓘ
<input type="checkbox"/>	Auto Authorize Location Based Tour Application	<input type="checkbox"/>
<input type="checkbox"/>	Show Attendance Details On Device	<input type="checkbox"/>
<input type="checkbox"/>	Attendance Policy	ID Name
<input type="checkbox"/>	Late-IN Policy	ID Name
<input type="checkbox"/>	Overtime Policy	ID Name
<input type="checkbox"/>	Absentee Policy	ID Name
<input type="checkbox"/>	Early-OUT Policy	ID Name
<input type="checkbox"/>	C-OFF Policy	ID Name

Update

1. Select the **Enable Attendance Calculation** checkbox to enable attendance calculation on the system for the selected users. This option has to be enabled for configuring any of the other parameters in this section.
2. In case the attendance calculation is enabled then the user needs to select the **Attendance Marking Type** from the drop down list.

The following options are available:

- **Normal:** This type will be default for all users.
 - **First Punch Only:** This type users need only entry punch at the start of the shift. In this case the system will assume that the shift end time is the last out Punch for the day. All other calculations remain the same as for normal type users.
 - **Executive:** This type users will be marked full day present if at least one punch (entry/exit) is available in the day. There will not be any late/early & overtime calculation like it is done for normal and single punch type users.
 - **Flexible:** This category of users working will be checked against required minimum working and if it is more than required, full day attendance will be marked. In this case the minimum working hours required in a day for full day attendance and half day attendance can also be defined for each user as explained below.
 - **Present:** category users do not require any punch for them to be marked full day present. All users belonging to this category are marked present by default.
3. The **Min Working Hours Required** section is enabled for configuration only when the *Flexible* Attendance Marking type is selected for a user. The administrator can specify the minimum working hours required in a day for users to be marked *Full Day* or *Half Day* present. Specify the hours in *HH:MM* format as shown below.

Update	Field Name	Set New Value
<input checked="" type="checkbox"/>	Enable Attendance Calculation	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Attendance Marking Type	Flexible
<input checked="" type="checkbox"/>	Min Working Hours Required For Full Day	08:00
<input checked="" type="checkbox"/>	Min Working Hours Required For Half Day	04:00
<input type="checkbox"/>	Max Punches To Be Considered	Select

4. The **Max Punches to be Considered** parameter specifies the maximum entry/exit events per user to be considered in a day for attendance calculation.

<input checked="" type="checkbox"/>	Max Punches To Be Considered	Select	
<input type="checkbox"/>	Bypass Finger/Palm/Face For Attendance	Select	
<input type="checkbox"/>	Max Short Leaves Allowed	2	
<input type="checkbox"/>	OT/C-OFF Eligibility	4	
<input type="checkbox"/>	Authorize C-OFF On	6	
<input type="checkbox"/>		8	
<input type="checkbox"/>		10	
<input type="checkbox"/>	Bus Route	12	
<input type="checkbox"/>	Enable Site Based Auto Tour Application	N-Punch	
<input type="checkbox"/>	Tour	Select	

☐ WO/PH
☐ Normal Day

Specify a value in this field if the value defined at the global level is to be overridden for this user. The options available are 2, 4, 6, 8, 10,12 and N-Punch. N-Punch allows unlimited number of punches in IN/ OUT pair.

5. On checking the **Bypass Finger/Palm/Face For Attendance** option, the user can punch IN or OUT using any of the assigned credentials and the same will be considered for attendance calculation. On selection of this option, finger/palm /face identification is no longer must for marking attendance.

6. The **Max Short Leaves Allowed** parameter specifies the maximum number of short leaves (personal hours) to be allowed to selected users in an attendance period. This parameter is also defined at the global system configuration level and can be overridden for specific users using this option. The administrator can specify a value of a maximum of two digits in this field.
7. The **OT/C-OFF Eligibility** parameter enables the administrator to define whether the overtime authorization for this user is to be done as:

- None
- Only Overtime
- Only Compensatory Off
- Both

For **Both** option you can select the days on which C-OFF is to be authorized.

8. Click the **Bus Route** picklist button and select the bus route to be assigned to selected users.
9. **Enable Site Based Auto Tour Application:** Select this checkbox so that tour application will be automatically applied for a particular user, if he punches from some site other than the Base Site.

<input checked="" type="checkbox"/>	Enable Site Based Auto Tour Application	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Tour	T1 - tour1
<input checked="" type="checkbox"/>	Base Site Selection	ID <input type="text"/> Name <input type="text"/>
<input checked="" type="checkbox"/>	Auto Authorize Site Based Tour Application	<input checked="" type="checkbox"/> 1 Site(s) are Selected

- **Tour:** Select the tour application from the dropdown list which will be automatically applied.
 - **Base Site Selection:** Select the base site to be assigned to the user.
 - **Auto Authorize Site Based Tour Application:** Select this checkbox to automatically authorize the tour application for a particular user, if auto tour application feature is enabled.
10. **Enable Location Based Auto Tour Application:** Select this checkbox so that tour application will be automatically applied for a particular user, if he punches from some location other than the Base location.

If a user goes for official activity to some location other than base location; then new location can be assigned to the user and tour application will be automatically applied for that day when event is generated from the new location.

<input checked="" type="checkbox"/>	Enable Location Based Auto Tour Application	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Tour	T2 - tour2
<input checked="" type="checkbox"/>	Base Location Assignment	Selected
<input checked="" type="checkbox"/>	Location	Code <input type="text"/> Name <input type="text"/>
<input checked="" type="checkbox"/>	Location Group	ID <input type="text"/> Name <input type="text"/>
<input checked="" type="checkbox"/>	Auto Authorize Location Based Tour Application	<input checked="" type="checkbox"/> 1 Location(s) are selected

Access Control Basic

This section enables the administrator to configure basic access control parameters for multiple users. To access this configuration, select the **Access Control Basic** section as shown below.

The screenshot displays the 'Multi-User Configuration' interface. On the left is a sidebar menu with options: User Selection, Profile, Devices, Credentials, Group, T&A, Access Control Basic (highlighted), Access Control Advance, ESS, Cafeteria, Job Costing, Field Visit Management, Face Recognition, and Visitor Management. The main area contains a table with three columns: 'Update' (checkboxes), 'Field Name', and 'Set New Value'. The table lists various access control settings. At the bottom right of the main area is an 'Update' button.

Update	Field Name	Set New Value
<input type="checkbox"/>	Bypass Finger	<input type="checkbox"/>
<input type="checkbox"/>	Bypass Palm	<input type="checkbox"/>
<input type="checkbox"/>	Access Validity	<input type="checkbox"/>
<input type="checkbox"/>	Access Validity Date	<input type="text"/>
<input type="checkbox"/>	Access Level For Smart Identification (SI)	8
<input type="checkbox"/>	Shift Schedule	Schedule Group
<input type="checkbox"/>	Start Shift	General Shift
<input type="checkbox"/>	Holiday Schedule	Schedule 1
<input type="checkbox"/>	Access Cluster Checking	<input type="checkbox"/>

1. The **Bypass Finger** option can be enabled in the event of the Finger Print image not being in order and the system thus has problems identifying the user. In such cases, the system administrator can disable the Finger Print check for the user thus enabling the user to gain access using either the assigned pin or card.
2. The **Bypass Palm** option can be enabled in the event of the Palm Vein image not being in order and the system thus has problems identifying the user. In such cases, the system administrator can disable the Palm vein check for the user thus enabling the user to gain access using either the assigned pin or card.
3. Enable the **Access Validity** option if the user credential is to be activated for a predefined period.

Specify the end date of the validity in the **Access Validity Date** field.

4. Specify an access level from the **Access Level For Smart Identification (SI)** drop down list, for which the Smart Identification feature will be applicable to the selected users.
5. Assign a **Shift Schedule** to the selected users from the dropdown list.

In case of multiple shifts in the schedule group, the **Start Shift** needs to be selected from the drop down list.

6. Select the **Holiday Schedule** to be assigned to the user from the drop down list.
7. Select the **Access Cluster Checking** option to enable checking for access cluster restrictions for the selected users.

Access Control Advance

This section enables the administrator to set advance access control parameters for multiple users. The **Access Control Advance** section is available only with the *Access Control* add-on module license. To access this configuration, select the **Access Control Advance** section as shown below.

The screenshot shows the 'Multi-User Configuration' window with a sidebar on the left containing the following menu items: User Selection, Profile, Devices, Credentials, Group, T&A, Access Control Basic, and Access Control Advance (highlighted in blue). The main area displays a table with three columns: 'Update', 'Field Name', and 'Set New Value'.

Update	Field Name	Set New Value
<input checked="" type="checkbox"/>	Enable Advance Access Control	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Shift Based Access	<input type="checkbox"/>
<input type="checkbox"/>	Smart Access Route	ID: <input type="text"/> Name: <input type="text"/>
<input type="checkbox"/>	Max Route Level	75
<input checked="" type="checkbox"/>	Enable Elevator Access Control	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Elevator Floor Group	1 RnD Elevator Group

1. **Enable Advance Access Control:** Check this box to enable the advance access control feature.
2. The **Shift Based Access** parameter allows the administrator to enable user access based on the shift working time of the users.



*In the event of not selecting the **Shift Based Access** option, the system will apply the default access settings applicable to the user.*

3. Select the **Smart Access Route** to be assigned to the user from the *Access Route* picklist.
4. Select the route level up to which the user is to be allowed access from the **Max Route Level** drop down list.
5. **Enable Elevator Access Control:** Check this box to enable the Elevator access control feature for the users.
6. **Elevator Floor Group:** Click the picklist and select the Elevator floor group to be assigned to the users. The users can access the floors of the Elevators included in Elevator Floor Group. The Elevator Floor group is created from Access Control> Elevator Access Control> Elevator floor group



Some parameters, when configured for a specific user, may over-ride corresponding parameters pre-defined at the Global Policy level.

ESS

The **ESS** section is available only with the ESS add-on module license. It enables the administrator to set up ESS accounts for new users. To access this configuration, select the **ESS** section as shown.

The screenshot shows the 'Multi-User Configuration' window. On the left, a sidebar lists various configuration categories: Profile, Devices, Credentials, Group, TBA, Access Control Basic, Access Control Advance, **ESS** (highlighted), Cafeteria, Job Costing, Field Visit Management, Face Recognition, and Visitor Management. The main area is divided into three columns: 'Update', 'Field Name', and 'Set New Value'. The 'Update' column has checkboxes for various features, with 'ESS' checked. The 'Field Name' column lists features like 'Enable Account', 'Edit Basic Details', 'Punch Marking Via ESS', 'Mark Punch As Per', 'Auto-Punch Marking', 'Manual Punch Marking', 'Face Mandatory for Punch', 'APTA Face Anti-Spoofing', 'Capture Photo', 'Allow Offline Punch', 'Location Mandatory for Punch', 'Reason For Punching from Unassigned Location', 'Location Assignment', 'Location', 'Location Group', 'Allow Door Access Through API', 'PIN authentication For Door Access', 'Domain', 'Auto Authorize (ME) Registration', 'Reset Password', and 'Preferred Language'. The 'Set New Value' column shows dropdown menus for 'Server Time Zone' (set to 'None') and 'Language' (set to 'English'). An 'Update' button is at the bottom right.

1. Select the **Enable Account** check-box to enable ESS account access for the selected users.
2. Select the **Edit Basic Details** check-box to enable the selected users to edit basic details on their respective ESS accounts.
3. Select the **Punch Marking Via ESS** check-box to enable users to mark their attendance manually from their respective ESS accounts.
4. Select the **Punch Marking Via API** check-box to enable user to mark punches by firing API. Auto-Punch and Manual-Punch marking check-box will be activated only if Punch marking via API is enabled.
5. Select the **Mark Punch As Per** check-box to select the time zone which is to be applied for punch time (punch marked from API)
 - **Server Time Zone**- The date- time of the punch will be as per the server time zone.
 - **Local Time Zone**- The date-time of the punch will be as per the time zone of the place from where the punch is marked.
6. Select the **Auto-Punch Marking** check-box to enable the auto-attendance marking feature for the selected user from the COSEC APTA mobile application. On enabling this feature, if the user's current location matches any of the assigned locations; a punch will be marked automatically for the user from the mobile application.



Locations can be configured from *COSEC Web Application > Admin > System Configuration > Location Master*.

- **Location Assignment**- Select the option as “**All**” or “**Selected**” for assigning location to users.
 - For **All** option; all the locations configured in Location Master will be assigned to the users. When new location is added to Location master then it will be automatically assigned to the users if “All” is selected.

- For **Selected** option; Location and Location Group will be enabled for the selection which is to be assigned to the users.
 - **Location**- Select the Location pick-list and select the locations to be assigned to the users.
 - **Location Group**- Select the Location group pick-list and select the groups to be assigned to the users. If Selected Location groups are assigned to users and whenever new location is added to the location group then newly added location in location group will also be assigned to the users.
7. Select the **Manual Punch Marking** check-box to enable manual punch marking from the COSEC APTA mobile application.
 8. **Face Mandatory For Punch** - When Manual Punch Marking and Face Recognition feature is enabled for user then you can select the specific option for which face is to be made mandatory for the punch. The options are **Attendance, Access Control, Both** and **None**.
For Access Control and Both option; you must enable "Allow Door Access Through API" checkbox.
 9. **APTA Face Anti-Spoofing**: When **Manual Punch Marking** is enabled and **Face Mandatory For Punch** is selected as — **Attendance, Access Control** or **Both** — then select **APTA Face Anti-Spoofing** checkbox to enable **Face Anti-Spoofing** feature via COSEC APTA Application to prevent false face verification by using a photo, video, mask or a different substitute for an unauthorized person's face.
 10. **Capture Photo**- This checkbox is activated only when **Punch marking via API** and **Manual Punch Marking** are enabled. This allows the user to capture snapshot while punching through COSEC APTA.
 11. **Allow Offline Punch** - This checkbox is activated only when **Punch marking via API** and **Manual Punch Marking** are enabled. This allows users to apply for offline punches.
In Mobile devices, when there is no connectivity between server and the Mobile device, the punches, with their timings can be stored through offline punch and send to server when connectivity is restored.
 12. The **Location Mandatory For Punch** field determines if information regarding the source location from where the punch has been marked should accompany a punch marking by user. Select **None** if location information should not accompany a punch. For *Manual Punch Marking*, select **Any Location** (locations need not be configured). For *Auto-Punch Marking* (auto-attendance feature), select **Configured Locations Only** (locations must be configured on "Location Master").
 13. **Reason For Punching From Unassigned Location**: This checkbox will be activated only when 'Location Mandatory For Punch' has either **None** or **Any Location** as values. By enabling this checkbox, the Incharge Users can know the reason for which the punch is made from unassigned location by the employee users.
 14. **Location Assignment**- Select the option as "All" or "Selected" for assigning location to users.
 - For **All** option; all the locations configured in Location Master will be assigned to the users. When new location is added to Location master then it will be automatically assigned to the users if "All" is selected.
 - For **Selected** option; Location and Location Group will be enabled for the selection which is to be assigned to the users.
 - **Location**- Select the Location pick-list and select the locations to be assigned to the users.
 - **Location Group**- Select the Location group pick-list and select the groups to be assigned to the users. If Selected Location groups are assigned to users and whenever new location is added to the location group then newly added location in location group will also be assigned to the users.

15. Select the **Allow Door Access Through API** to allow the access to device through API.
16. Select the **PIN Authentication For Door Access** for Dual Authentication with PIN when Bluetooth or QR based access is used for Access control feature in COSEC APTA mobile application.
17. Specify the Active Directory domain name in the **Domain** field for Active Directory login.
18. Select the **Auto-Authorize IMEI Registration** checkbox to enable automatic authorization of IMEI numbers newly registered on COSEC, for the selected users.
19. The administrator can click the **Reset Password** button to reset the selected ESS users' login password.
20. Specify the **Preferred Language** for the selected ESS Users as *English, Arabic, Spanish, Albanian, Turkish or Vietnamese*.

Cafeteria

This section is available only with the Cafeteria add-on module license. To access this configuration, select the **Cafeteria** section as shown.

Update	Field Name	Set New Value
<input type="checkbox"/>	Enable Account	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Enable Offline Transaction	None
<input checked="" type="checkbox"/>	Discount Level	None
<input checked="" type="checkbox"/>	Account Type	Pre-Paid
<input type="checkbox"/>	Balance Management	Device Based
<input type="checkbox"/>	Device-Server Balance Check	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Cafeteria Usage Policy	ID: <input type="text"/> Name: <input type="text"/>

1. Select the **Enable Account** checkbox to enable Cafeteria account access for the selected user.
2. Select the desired option to perform offline transaction from the **Enable Offline Transaction** drop down list.
 - Select **None**, if you do not want to allow transactions to be made by the users when the device is in offline mode.
 - Select **Allow With Discount**, if you want to allow transactions with discount to be made by the users, when the device is in offline mode.
 - Select **Allow Without Discount**, if you do not want to allow transactions without discount to be made by the users, when the device is in offline mode.
3. Select the appropriate discount level from the **Discount Level** drop down list.

4. Select the **Account Type** as **Pre-Paid** or **Post-Paid**.

- For **Pre-Paid** account type, specify whether the **Balance Management** should be Device-based or Server-based.
- When Balance Management is selected as **Server based**, then you can enable **Device-Server Balance Check**. This will allow Device to check Server-side balance before allowing transaction. For this, Device and Server must be connected.
- For **Post-Paid** account type, enter the **Allowed Usage Per Month** based on which monthly dues for the user can be calculated.

5. **Cafeteria Usage Policy**- Select the cafeteria usage policy to assign to the multiple users based on which cafeteria transaction restrictions will be applied to the users.

Job Costing



In case the job added is same as existing job assigned to the user and the date range provided is also the same, then only the ESS Assignment flag is updated for users through Multi User Configuration.

To assign new job through Multi User Configuration, make sure that the new job does not fall within the date range of already assigned job(s).

This section is available with Job Processing and Costing license. To set Job costing related parameters for multiple users, click **User Module >Multi-User Options >User Configuration >Job Costing**.

Update	Field Name	Set New Value
<input checked="" type="checkbox"/>	Job Costing	Enabled
<input type="checkbox"/>	Device Based Job Assignment	
<input type="checkbox"/>	Job	

- **Job Costing**: Select the check box under **Update** to enable. Select **Enabled** from the drop-down under **Set New Value**.

- **Device Based Job Assignment-** Select the check box under **Update** to enable. Select the check box under **Set New Value**. Job codes will be assigned to the user as per device configuration on which user punches.

- **Job-** Select the desired job from the pick list.

The Multiple default jobs can be assigned with non-overlapping Assignment Date Ranges. Only 'In Progress' Jobs are assigned.

- **Assignment Date-** Define the start date and end date for the selected job from the calendar.
- **ESS Assignment-** Select the check box to Enable. This job will be displayed in the list of Jobs assigned to the user through the ESS login. If you do not want this job to be displayed, clear the check box.



*The ESS Assignment check box will not be displayed if the **Show All Jobs while Punching** check box is enabled. For details, refer to ["Job Costing"](#) in ["Defining Global Policies"](#).*

- After configuring **Job Costing** parameters, select the user from **User Filter**. Click **Update** to apply **Job Costing** configurations for the selected user.

The screenshot shows the 'Multi-User Configuration' window with the 'Job Costing' tab selected in the left sidebar. The main area contains a table with columns 'Update', 'Field Name', and 'Set New Value'. The table has four rows: 'Job Assignment Type' (Enabled), 'Device Based Job Assignment' (checked), 'Job' (1), and 'Assignment Date' (10/12/2021). There is an 'Update' button at the bottom right.

Update	Field Name	Set New Value
<input checked="" type="checkbox"/>	Job Assignment Type	Enabled
<input checked="" type="checkbox"/>	Device Based Job Assignment	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Job	1
<input checked="" type="checkbox"/>	Assignment Date	10/12/2021



*Jobs are created from **Job Processing and Costing module > Project Management> Job**.*

Field Visit Management

In this module, you can assign schedules to the users and keep a track of their activities, while on site and also check if the assigned tasks are being fulfilled correctly or not.

The screenshot shows the 'Multi-User Configuration' window with the 'Field Visit Management' tab selected in the left sidebar. The main area contains a table with columns 'Update', 'Field Name', and 'Set New Value'. The table has one row: 'Enable FVM' (checked). There is an 'Update' button at the bottom right.

Update	Field Name	Set New Value
<input checked="" type="checkbox"/>	Enable FVM	<input checked="" type="checkbox"/>

Check the **Enable FVM** box to consider multiple user as FVM user.

Face Recognition

In this feature, user can access the device or mark the attendance by verifying his Face as the credential. The Face Recognition tab appears as shown below:

The screenshot shows the 'Multi-User Configuration' window with the 'Face Recognition' tab selected in the left sidebar. The main area contains a table with three columns: 'Update', 'Field Name', and 'Set New Value'. The table has one row with 'Enable Face Recognition' checked in both the 'Update' and 'Set New Value' columns. An 'Update' button is at the bottom right.

Update	Field Name	Set New Value
<input checked="" type="checkbox"/>	Enable Face Recognition	<input checked="" type="checkbox"/>

Update

Enable Face Recognition: Check this box to enable Face Recognition feature for the user.

Visitor Management

In this feature you can authorize a host user, restrict the visitor pre-registration on the basis of no.of days and assign device groups and devices to the visitors.

The screenshot shows the 'Multi-User Configuration' window with the 'Visitor Management' tab selected in the left sidebar. The main area contains two tables. The first table has columns 'Update', 'Field Name', and 'Set New Value' with rows for 'Authorized Host User', 'Minimum Days Before Allowing Visit', and 'Maximum Days Before Allowing Visit'. The second table has columns 'Update', 'Field Name', and 'Set New Value' with rows for 'Device Group' and 'Device'. Below the tables are radio buttons for 'Assign Device/Device Group' (selected) and 'Revoke Device/Device Group'. An 'Update' button is at the bottom right.

Update	Field Name	Set New Value
<input type="checkbox"/>	Authorized Host User	<input type="checkbox"/>
<input type="checkbox"/>	Minimum Days Before Allowing Visit	Days
<input type="checkbox"/>	Maximum Days Before Allowing Visit	Days

☒ Assign Device/Device Group ☐ Revoke Device/Device Group

Update	Field Name	Set New Value
<input type="checkbox"/>	Device Group	ID Name
<input checked="" type="checkbox"/>	Device	Name

Update

- Under **Update**, select the **Authorized Host User** check box to enable. Under **Set New Value**, select the check box to enable the selected users to function as Authorized Host Users.
- To restrict the visitor pre-registration on the basis of number of days,

- Under **Update**, select the **Minimum Days Before Allowing Visit** check box to enable. Under **Set New Value** configure the desired number of days.
- Under **Update**, select the **Maximum Days Before Allowing Visit** check box to enable. Under **Set New Value** configure the desired number of days.
- To assign Device/Device Group to multiple users at the same time,
 - Select the **Assign Device/Device Group** option.
 - Under **Update**, select the **Device Group** check box to enable.


Under **Set New Value**, select the desired device group from the **Device Group** picklist you wish to assign to the selected users.

The selected device group appears in the grid as shown above.

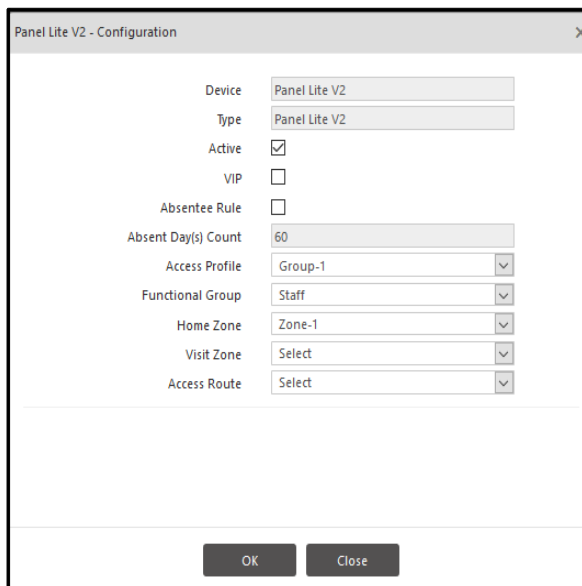
- You can also select individual devices. By default, under **Update** the **Device** check box is enabled.

Under **Set New Value** from the **Device** picklist, select the desired devices you wish to assign to the selected users.

The selected devices appear in the grid as shown above.

- Click **Configure**  to configure the selected device for multiple users.

The Configuration page of the selected Device appears as shown below.




The Device and Type will be shown as per the device selected from the grid.

You can enable and configure Access Control features from the Configuration page.

- Click **OK**.

- Click **Update** to assign the selected devices/device groups with configuration to multiple users.
- Similarly to revoke Device/Device Group from multiple users at the same time,
 - Select the **Revoke Device/Device Group** option.
 - Under **Update**, select the **Device Group** check box to enable.

Under **Set New Value**, select the desired device group from the **Device Group** picklist you wish to revoke from the selected users.

The selected device group appears in the grid.

- You can also select individual devices. By default, under **Update** the **Device** check box is enabled.

Under **Set New Value** from the **Device** picklist, select the desired devices you wish to revoke from the selected users.

The selected devices appear in the grid as shown above.

- Click **Update** to revoke the selected devices/device groups from multiple users.

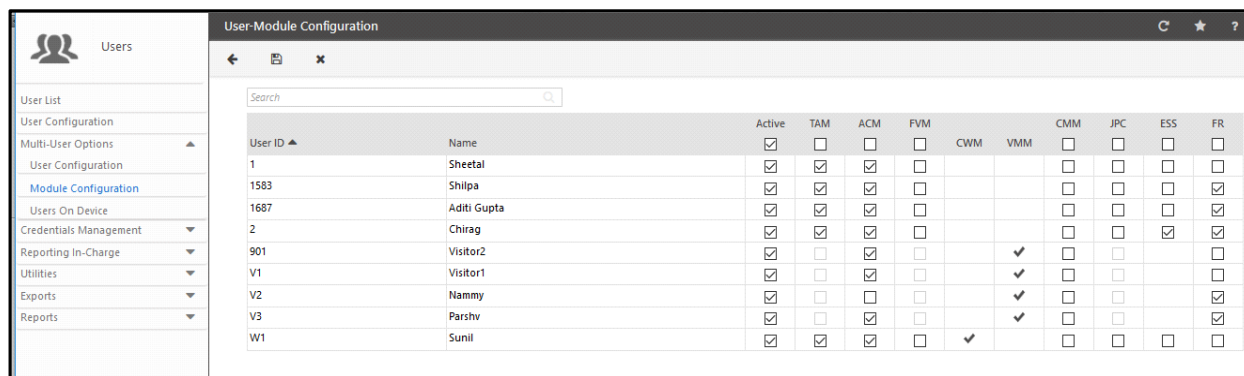
For more information about the configurations, refer "[Visitor Management](#)" in *Users> User Configuration> Visitor Management*.

User-Module Configuration

COSEC provides the option to activate/deactivate different modules for multiple users at the same time. You can Enable/Disable Attendance Calculation, Cafeteria Account, Job Costing Account, FVM Account, ESS and Face Recognition for multiple users.

To access this functionality, select the **Users module > Multi-User Options > Module Configuration**.

The **Module Configuration** page opens as shown below.



User ID	Name	Active	TAM	ACM	FVM	CWM	VMM	CMM	JPC	ESS	FR
1	Sheetal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1583	Shilpa	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1687	Aditi Gupta	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Chirag	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
901	Visitor2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
V1	Visitor1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
V2	Nammy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
V3	Parshv	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
W1	Sunil	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Check the **Active** box to configure the module for the user. The ACM box will get checked. Now you can enable TAM and ESS module.

If TAM module license is activated then you can enable FVM and JPC module.



For a user, when checkbox is checked but disabled in grid for a particular module; then it indicates that user does not have rights for accessing that module.

For visitor; if Active box is enabled; then you can enable CWM module.

You can also enable CMM module and FR module for the required user.



When check-box of FR is enabled for a user then Face Recognition check-box will get enabled for that user in User Configuration> Face Recognition and “Face Recognition For” drop down will be set as “**For Both**” for the user.

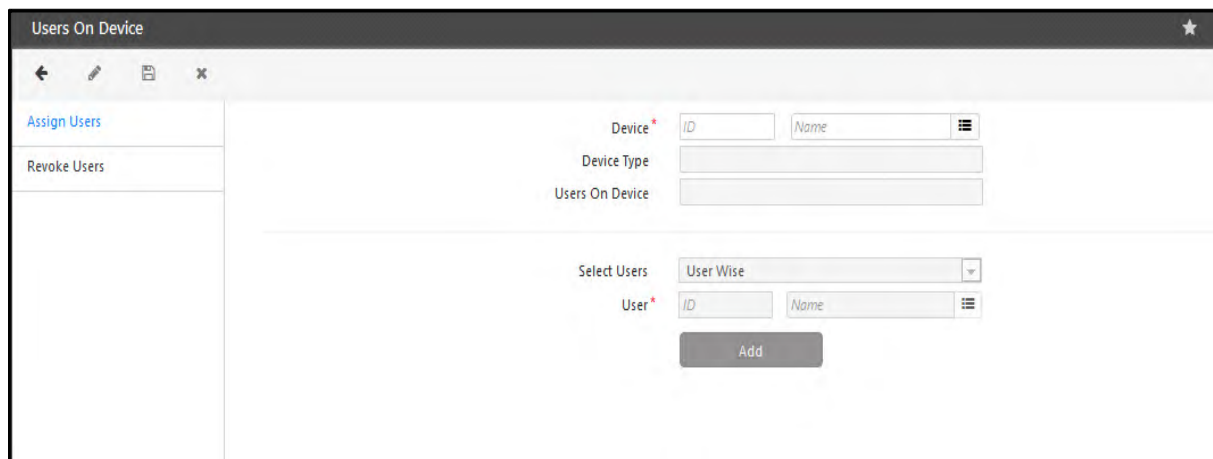
Users on Device

The **Users** module allows the system administrator to assign multiple users to a selected Panel200 or Direct Door device at a time.

To do this, Select the **Users module > Multi-User Options > Users On Device**.

Assign Users

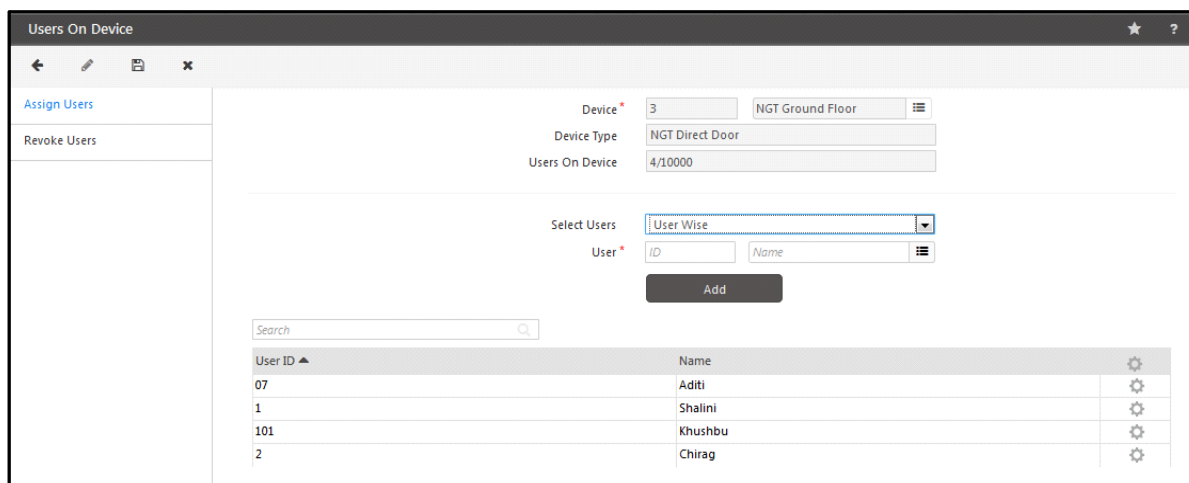
The **Users On Device** page appears on your screen as follows:



Device: Select a Device from the picklist to which users are to be assigned.

On selection of a device, the **Device Type** and **Users On Device** (number of users on the device) will be displayed in the respective fields as shown below.

The already assigned users on the device is also shown in the grid.



User ID	Name	
07	Aditi	⚙
1	Shalini	⚙
101	Khushbu	⚙
2	Chirag	⚙

Select Users: Select the users from the filter options of User Wise, Group Wise or All.

Select Users: User Wise

User* ID Name

Search

User ID ▲	Name	
1678	Supriya	
3	Isha	
NP	Nisha	

Add

Search

User ID ▲	Name	
07	Aditi	
1	Shalini	
101	Khushbu	
2	Chirag	

Click the **Add** button. The selected users will appear in the grid list. Click on **Save** button to save the assignment of users on device.

Now click the **Settings** icon next to a user to additionally configure *Access Control* parameters for the device. The following pop up window appears on your screen:

User ID ▲	Name	
07	Aditi	
1	Shalini	
101	Khushbu	
1678	Supriya	
2	Chirag	

Device Options

Device Name* NGT Ground Floor

User ID 1678

Active ☒

VIP ☐

Absentee Rule ☐

Day(s) Count* 60

Save Cancel

You can edit and save the *Device Options*, if required.

Click the **Save** button to assign the selected users on device successfully.

Revoke Users

To revoke a user from the selected device, select the **Revoke Users** tab.

The screenshot shows the 'Users On Device' window with the 'Revoke Users' tab selected. The sidebar on the left has 'Assign Users' and 'Revoke Users' tabs. The main area contains the following fields:

- Device ***: ID (text input), Name (text input with a menu icon)
- Device Type**: (text input)
- Users On Device**: (text input)
- Select Users**: User Wise (dropdown menu)
- User ***: ID (text input), Name (text input with a menu icon)
- Select**: (button)

Device: Select a Device from the picklist from which users are to be removed.

On selection of a device, the **Device Type** and **Users On Device** (number of users on the device) will be displayed in the respective fields as shown below.

The assigned users on the device is shown in the grid.

The screenshot shows the 'Users On Device' window with the 'Revoke Users' tab selected. The 'Device' field is filled with '4' and 'Vega Direct Door'. The 'Device Type' is 'Vega Controller' and 'Users On Device' is '4/50000'. The 'Select Users' dropdown is set to 'User Wise'. Below the form is a table of users with columns 'User ID', 'Name', and 'Revoke'.

User ID	Name	Revoke
07	Aditi	<input type="checkbox"/>
1	Shalini	<input type="checkbox"/>
101	Khushbu	<input type="checkbox"/>
2	Chirag	<input type="checkbox"/>

Select Users: Select the users from the filter options of User Wise, Group Wise or All.

Now click on **Revoke** button for the user who is to be revoked from the device.

User ID	Name	Revoke
07	Aditi	<input type="checkbox"/>
1	Shalini	<input type="checkbox"/>
101	Khushbu	<input type="checkbox"/>
2	Chirag	<input type="checkbox"/>

Click the **Save** button to revoke the selected users successfully. The user will be removed from the assigned list as shown below.

The screenshot shows a web application window titled "Users On Device". At the top, a green notification bar displays "✓ Saved Successfully". The interface includes a sidebar with "Assign Users" and "Revoke Users" (highlighted in blue). The main area contains form fields for "Device" (4), "Device Type" (Vega Controller), and "Users On Device" (3/50000). Below these is a "Select Users" section with a dropdown set to "User Wise" and a table of users with columns for "ID", "Name", and "Revoke". A "Select" button is positioned below the user selection table.

User ID ▲	Name	Revoke
1	Shalini	<input type="checkbox"/>
101	Khushbu	<input type="checkbox"/>
2	Chirag	<input type="checkbox"/>

Enrolling Users

Once the users have been added to the database the administrator can start the enrollment process and assign credentials to the users. Enrollment can be defined as a process wherein the COSEC system accepts and stores the user credentials against a particular user. The COSEC access control system supports enrollment of user cards, finger print templates, palm templates and special cards.

The enrollment process can be initiated either from the COSEC application as described here or from the Door Controller by using special cards or Menu. However, the administrator needs to ensure that the **COSEC Monitor** application is running before starting the enrollment process.



The Smart Card Detail section will not be available with the COSEC Application basic platform license.

To start the enrollment process, select the **Users module > Credentials Management > Enrollment**.

User Enrollment

Select the **User** tab for enrolling user credentials on selected device.

The page opens as follows:

- **Door:** Select the desired door from the pick-list on which the enrollment is to done.

Device Readers

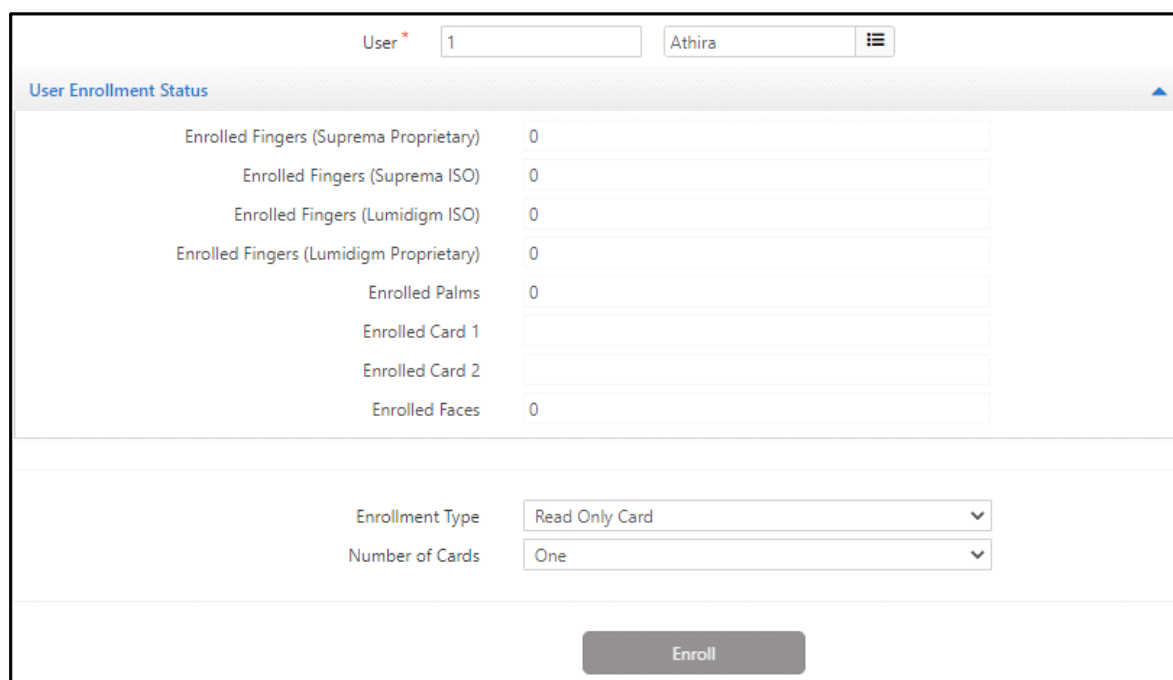
Device Readers displays the information of the readers configured in the selected **Door**.



Device Readers	
Card Reader	MiFare Reader
Biometric Reader	None
External Reader	MiFare-U Reader

Card Reader, Biometric Reader and External Reader information are displayed here.

- **User:** Select the desired user from the pick-list for whom the enrollment is to be done.



User * 1 Athira

User Enrollment Status	
Enrolled Fingers (Suprema Proprietary)	0
Enrolled Fingers (Suprema ISO)	0
Enrolled Fingers (Lumidigm ISO)	0
Enrolled Fingers (Lumidigm Proprietary)	0
Enrolled Palms	0
Enrolled Card 1	
Enrolled Card 2	
Enrolled Faces	0

Enrollment Type Read Only Card

Number of Cards One

Enroll

User Enrollment Status

User Enrollment Status displays the information related to the number of already enrolled credentials of the user like fingers, palms, cards and faces.

Details like — **Enrolled Fingers (Suprema Proprietary)**, **Enrolled Fingers (Suprema ISO)**, **Enrolled Fingers (Lumidigm ISO)**, **Enrolled Fingers (Lumidigm Proprietary)**, **Enrolled Palms**, **Enrolled Card 1**, **Enrolled Card 2** and **Enrolled Faces** — are displayed here.

- **Enrollment Type:** From the dropdown list, select the desired enrollment type — **Read Only Card**, **Smart Card**, **Face**, **Biometrics**, **BiometricsThenCard**, **Mobile**, or **Duress Finger**.

Based on the selection of the **Door** and **Enrollment Type**, below parameters will be displayed for configuration.



When Enrollment Type selected is Smart card or BiometricThenCard, Duress Finger Templates will not be written in the Smart Card.

Below parameters also depend on the Readers configured in the Door. To configure the desired Reader, refer Readers section under Devices > Device Configuration (of the desired Door) > Profile > Readers.

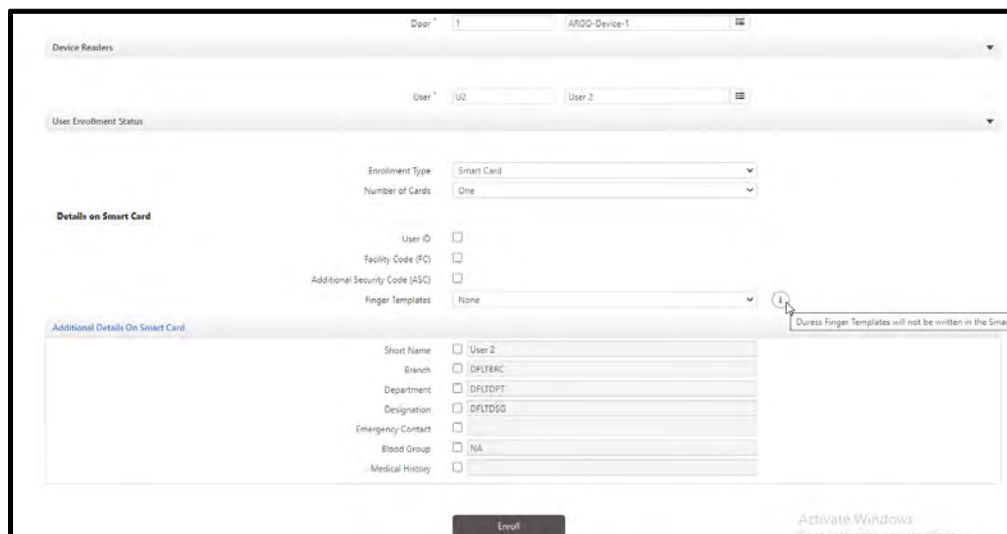
1. Enrollment Type = Read Only Card

Number of Cards: Select the desired number of cards from the drop-down list.

Enrollment Type	Read Only Card
Number of Cards	One

2. Enrollment Type = Smart Card

Number of Cards: Select the desired number of cards from the drop-down list.



The screenshot shows a web-based enrollment form for a Smart Card. At the top, there are fields for 'Door' (set to 1) and 'ARMO-Device-1'. Below this is a 'Device Readers' section. The main form area is titled 'User Enrollment Status' and contains two user selection fields, 'User 1' and 'User 2', both set to 'U2'. Under 'Details on Smart Card', there are dropdown menus for 'Enrollment Type' (set to 'Smart Card') and 'Number of Cards' (set to 'One'). Below these are checkboxes for 'User ID', 'Facility Code (FC)', and 'Additional Security Code (ASC)', all of which are unchecked. A dropdown for 'Finger Templates' is set to 'None'. An information icon next to this dropdown has a tooltip that reads: 'Duress Finger Templates will not be written in the Smart Card'. At the bottom, there is an 'Additional Details On Smart Card' section with a table of fields: 'Short Name' (User 2), 'Branch' (DPLTBAC), 'Department' (DPLTDPT), 'Designation' (DPLTDSG), 'Emergency Contact', 'Blood Group' (NA), and 'Medical History'. Each field has a checkbox, all of which are unchecked. At the bottom right of the form is an 'Activate Windows' watermark. A large 'Enroll' button is at the bottom center.

Details on Smart Card

Select the desired check boxes of the parameters — **User ID**, **Facility Code (FC)**, **Additional Security Code (ASC)** — which are to be displayed on the Smart Card.

Select the desired number of **Finger Templates** from the drop-down list.

If **Door** is selected as PVR Door, **Palm Templates** parameter will be visible. Select the check box of this parameter if you wish to display it on the Smart Card.

To store the palm templates, MiFare 4k reader must be configured in the PVR Door.



Door PVR must be set in the Adaptive mode (configure from Admin> System Configuration> Global Policy) for the palm templates to be saved into the Smart Card.

Additional Details on Smart Card

Other than the parameters mentioned in the Details on Smart Card, you can display additional details on Smart Card.

Select the desired check boxes of the parameters — **Short Name, Branch, Department, Designation, Emergency Contact, Blood Group** and **Medical History**— which are to be displayed on the Smart Card.

The values of these additional details are displayed as well. Make sure the values of these additional details are not blank for successful enrollment process.

3. Enrollment Type = Face

Number of Faces: Select the desired number of face from the dropdown list.

Enrollment Type	Face
Number of Faces	1

4. Enrollment Type = Biometrics

Number of Fingers/ Number of Palms: Select the desired number of fingers or palms from the dropdown list.

Enrollment Type	Biometrics
Number of Fingers	One

Enrollment Type	Biometrics
Number of Palms	One

5. Enrollment Type = BiometricsThenCard

Number of Cards: Select the desired number of cards from the drop-down list.

Number of Fingers/ Number of Palms: Select the desired number of fingers or palms from the drop-down list.

Details on Smart Card

Select the desired check boxes of the parameters — **User ID**, **Facility Code (FC)**, **Additional Security Code (ASC)** — which are to be displayed on the Smart Card.

Select the desired number of **Finger Templates** from the drop-down list.

If the **Door** is selected as PVR Door, **Palm Templates** parameter will be visible. Select the check box of this parameter if you wish to display it on the Smart Card.

To store palm templates, MiFare 4k reader must be configured in the PVR Door.



Door PVR must be set in the Adaptive mode (configure from Admin> System Configuration> Global Policy) for the palm templates to be saved into the Smart Card.

Additional Details on Smart Card

Other than the parameters mentioned in the Details on Smart Card, you can display additional details on Smart Card.

Select the desired check boxes of the parameters — **Short Name**, **Branch**, **Department**, **Designation**, **Emergency Contact**, **Blood Group** and **Medical History**— which are to be displayed on the Smart Card.

The values of these additional details are displayed as well. Make sure the values of these additional details are not blank for successful enrollment process.

6. Enrollment Type = Mobile



To select **Enrollment Type** as **Mobile**, the particular device must have **BLE** support and ensure **Bluetooth** is **ON** in the mobile.

Access Card Selection: Select the desired Access Card from the drop-down list.

Enrollment Type: Mobile
Access Card Selection: Access Card 1
Facility Code (FC): ☐

Facility Code (FC): Select this check box to enroll the Facility Code (FC) against the user.

7. **Enrollment Type** = Duress Finger

Number of Fingers: Select the desired number of fingers that you want to enroll as **Duress Finger** from the drop-down list— **One** or **Two**.

The screenshot shows the Matrix COSEC System Manual enrollment interface. The 'Enrollment Type' is set to 'Duress Finger'. The 'Number of Fingers' dropdown menu is open, showing options for 'One' and 'Two'. The 'Enroll' button is visible at the bottom of the dropdown.

Click Enroll to initiate the enrollment process.

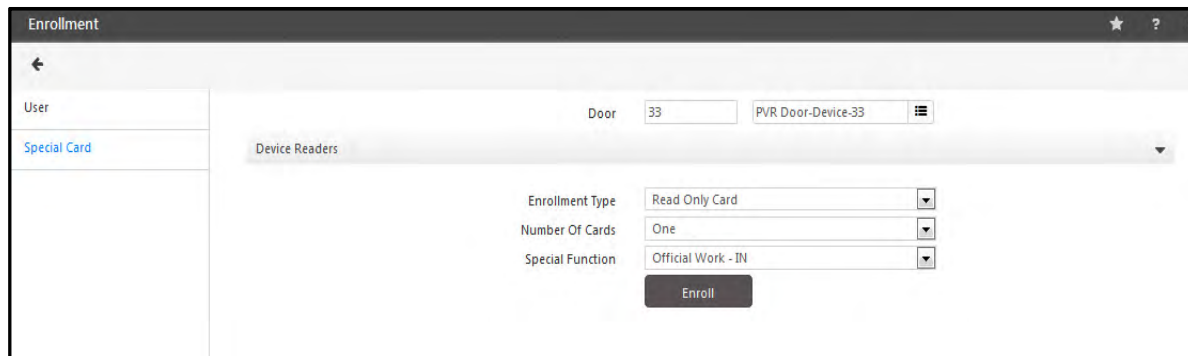
After the enrollment process, the user must tap on **Tap to Register > Matrix Device** from the ACS Application installed on respective mobile phone and select the same configured Door from **Available Doors**. Thereafter, that user can access the device through ACS application for Access Control purpose.

The value in Access Card selected will be consider as Access ID of the user. If Access Card selected has no value i.e blank, then after the enrollment process, the system will auto-generate 18 digits number as user Access ID and store the same value as shown below:

Enrolling Special Cards

This functionality enables the Administrator to enroll special cards for activated special functions. To know more about special cards, refer to [“Special Cards”](#).

To enroll *Special Cards*, select the **Special Card** tab as shown below:

The screenshot shows a web application window titled "Enrollment". On the left is a sidebar with a "User" tab and a "Special Card" tab (which is selected). The main area has a header with "Door" set to "33" and a dropdown for "PVR Door-Device-33". Below this is a "Device Readers" panel. To the right of the panel are three dropdown menus: "Enrollment Type" (set to "Read Only Card"), "Number Of Cards" (set to "One"), and "Special Function" (set to "Official Work - IN"). At the bottom right is an "Enroll" button.

Select a **Door** on which the special card enrollment is to be performed.

Expand the **Device Readers** panel to view the Internal and External Reader information for the selected device.

In the **Enrollment Type** drop-down list, specify whether a **ReadOnlyCard** or **SmartCard** is to be enrolled as a special card.

Specify the **Number of Cards** to be enrolled for a special function from the drop-down list. A maximum of upto four cards can be enrolled for a single special function.

Select a **Special Function** from the drop-down list for which the special card is to be enrolled.

Click the **Enroll** button to initiate the Enrollment process at the selected Panel200 or door.

Set and Sync Credentials

The COSEC system has six major types of user credentials which can be assigned to users:

- PIN
- Cards (Read only and Smart Cards)
- Fingerprint Templates (Finger print and Duress)
- Palm Templates
- User Photo
- Face Template

The **Set and Sync Credential** option provides a simple method of setting user credentials to devices. However the administrator needs to ensure that the users have been created on the system using the **User Configuration** option of the Basic module.

To access this functionality, Select the **Users module > Credential Management> Set and Sync Credentials**.

The **Set and Sync Credentials** page appears on your screen as follows:

Single User

Set And Sync Credentials

Single User

Multiple Users

User* 03 Arushi

Credential FP Template

FP Templates (Suprema Proprietary) 1

FP Templates (Suprema ISO) 0

FP Templates (Lumidigm ISO) 0

Sync To Device

Search

All Devices

ID	Name	Type
51	NGT Direct Door-Device-51	NGT Direct Door

Set And Sync Credentials

- **User** - Select a user from the user picklist whose credentials are to be set.
- **Credential** - Select a user credential from this drop down list which is to be set for the selected user. the options are -
 - PIN
 - Cards
 - FP Template (Finger print and Duress)
 - FP Template
 - Palm Template
 - User Photo
 - Face Template

- Depending on the credential selected, one of the following options will appear-
 - **PIN Number** - Enter the PIN Number to set the PIN.
 - **Card1/Card2** - Enter the Card Serial Number (CSN) or a Comma separated CSN. To know about the format of entering the Card details, refer **Access Card 1** in *"Credentials"* under *Users> User Configuration> Credentials> Access Card 1*.
 - **FP Templates** - The number of FP templates enrolled with different sensor devices will be displayed. This will include the finger templates of Duress Finger also.
 - **Palm Templates** - The number of Palm templates will be displayed.
 - **Enrolled Faces** - The number of face templates will be displayed.

The screenshot shows a web interface for user configuration. At the top, there are fields for 'User' (1583) and 'Shilpa'. Below these, a 'Credential' dropdown menu is set to 'Face Template'. Underneath, 'Enrolled Faces' is displayed as '4'. A section titled 'Sync To Device' contains a search bar and a 'Select All' checkbox. Below this is a table with columns for selection, ID, Name, and Type. The table lists two devices: 'Vega Door' (ID 3, Vega Controller) and 'MODE Device1' (ID 6, MODE). A 'Set And Sync Credentials' button is located at the bottom of the table.

	ID	Name	Type
<input checked="" type="checkbox"/>	3	Vega Door	Vega Controller
<input checked="" type="checkbox"/>	6	MODE Device1	MODE

- **Sync To Device**- Select the devices where the specified credentials are to be set for the selected user. The options available will depend on the credential selected or the Sync Type.
- Click the **Set and Sync Credentials** button to set the user credential successfully on all the specified devices.

Multiple Users

The screenshot shows a web application window titled "Set And Sync Credentials". On the left, there is a sidebar with two options: "Single User" and "Multiple Users", with "Multiple Users" selected. The main area contains the following elements:

- Credential**: A dropdown menu currently set to "FP Template".
- Select Users**: A dropdown menu currently set to "User Wise".
- User ***: Two input fields, "ID" and "Name", with a search icon to the right.
- Search**: A text input field.
- User List Table**: A table with columns "User ID", "Name", and a delete icon.

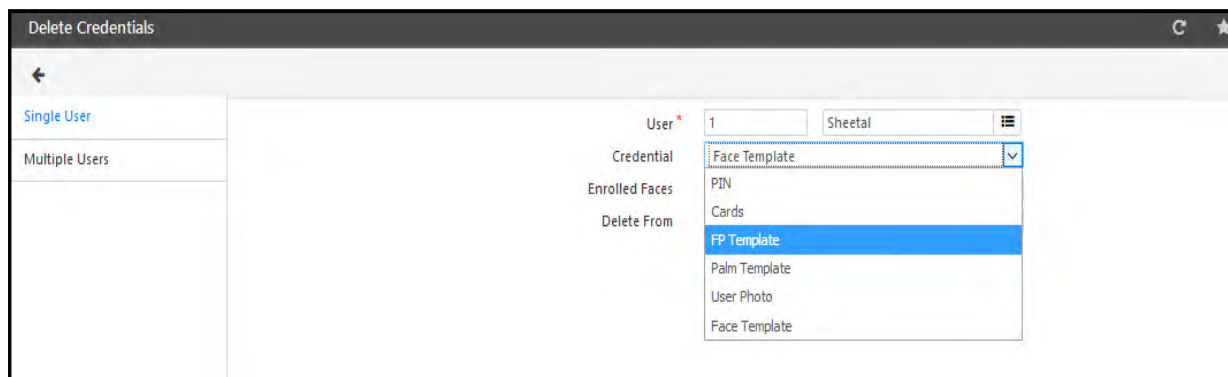
User ID	Name	
03	Arushi	
1320	SHRUTI SAGAR PATKI	
1421	Isha Shah	
- Sync To**: A dropdown menu currently set to "All Allotted Devices".
- Set And Sync Credentials**: A button at the bottom right.

- **Credential** - This option supports following types of user credentials -
 - FP Template (Finger print and Duress)
 - Palm Template
 - User Photo
 - Face Template
 -
- **Select User** - Specify multiple users using this dropdown list. Choose from the following options -
 - **User Wise** - Select random users from the user picklist.
 - **Group Wise** - Select a group of users from the **Select Group** drop down list.
 - **ALL** - Select all users active on the system.
- **Sync To** - Use this drop down list to specify the devices where the specified credentials are to be set for the selected user. The options available will depend on the credential selected or the Sync Type.
 - **All Allotted Devices** - This option appears for FP Template only. Select this to set credentials on all allotted devices.
 - **All Allotted PVR Devices** - This option appears for Palm Template only. Select this to set credentials on all allotted PVR devices.
 - **All Allotted NGT & Vega Controllers** - This option appears for User Photo only. Select this to set credentials on all allotted NGT and Vega controllers.
 - **All Allotted MODE, Vega and FMX Devices** - This option appears for Face Template only. Select this to set face credential on all MODE, Vega and FMX devices.
- Click the **Set** button to set the user credential successfully on all the specified devices for the selected multiple users.

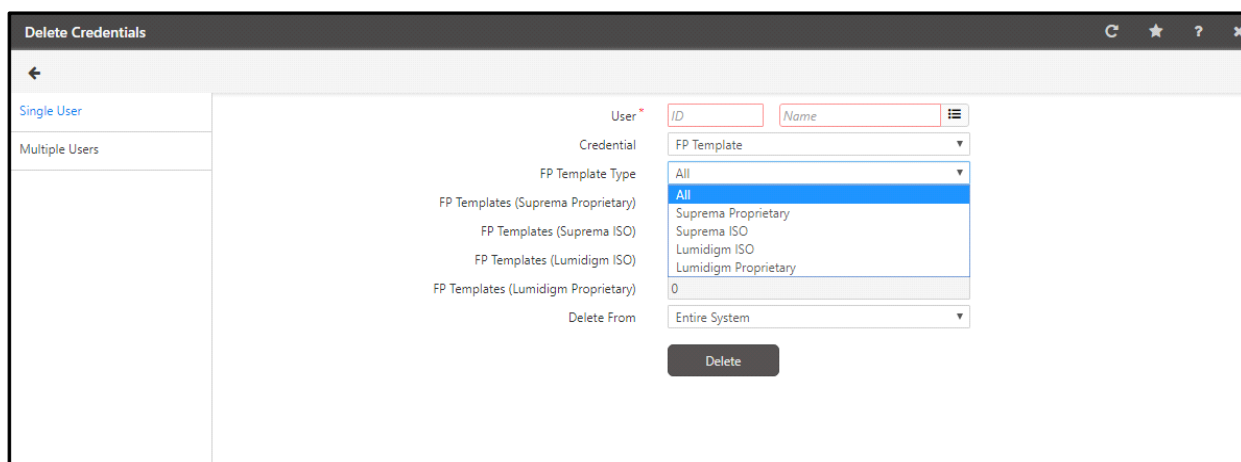
Delete Credentials

The **Delete Credential** option provides a simple method of Deleting user credentials from devices. To access this functionality, Select the **Users** module. Select **Credential Management > Delete Credentials**.

The **Delete Credentials** page appears on your screen as follows:



Single User



- **User** - Select a user from the user picklist whose credentials are to be deleted.
- **Credential** - Select a user credential from this drop down list which is to be deleted for the selected user.
The options are -
 - PIN
 - Cards
 - FP Template (Finger print and Duress)
 - Palm Template
 - User Photo
 - Face Template

- **FP Template Type-** If Credential is selected as FP Template; then you can select the Type of FP Template which is to be deleted. The options of template are Suprema Proprietary, Suprema ISO, Lumidigm ISO, Lumidigm Proprietary and All. This will include the finger templates of Duress Finger also.

The screenshot shows the 'Delete Credentials' window with the 'Single User' tab selected. The form contains the following fields:

- User ***: 1687
- Credential**: FP Template
- FP Template Type**: Suprema Proprietary
- FP Templates (Suprema Proprietary)**: 1
- FP Templates (Suprema ISO)**: 0
- FP Templates (Lumidigm ISO)**: 0
- Delete From**: Entire System

A 'Delete' button is located at the bottom right of the form.

- **Enrolled Faces-** If Credential is selected as Face Template; then the number of enrolled face templates for the selected user will be displayed.
- **Delete From-** Use this drop down list to specify the devices from where the specified credentials are to be deleted for the selected user.
- Click the **Delete** button to delete the user credential successfully on all the specified devices.

Multiple Users

The screenshot shows the 'Delete Credentials' window with the 'Multiple Users' tab selected. The form contains the following fields:

- Credential**: FP Template
- FP Template Type**: All
- Select Users**: All
- Delete Credentials For**: Active Users
- Delete From**: All Allotted Devices

A 'Delete' button is located at the bottom right of the form.

- **Credential** - This option supports the deleting of following user credentials -
 - PIN
 - Cards
 - FP Template (Finger print and Duress)
 - Palm Template
 - User Photo
 - Face Template

- **FP Template Type-** If Credential is selected as FP Template; then you can select the Type of FP Template which is to be deleted. The options of template are Suprema Proprietary, Suprema ISO, Lumidigm ISO, Lumidigm Proprietary and All. This will include the finger templates of Duress Finger also.
- **Select User** - Specify multiple users using this dropdown list. Choose from the following options -
 - **User Wise** - Select random users from the user picklist.
 - **Group Wise-** Select a group of users from the **Select Group** drop down list.
 - **ALL** - Select all users active on the system.
- **Delete From** - Use this drop down list to specify the devices from where the specified credentials are to be deleted for the selected user. The options available will depend on the credential selected.
- Click the **Delete** button to delete the user credential successfully on all the specified devices for the selected multiple users.

Sync from Device

This option enables the COSEC system to synchronize user credential details between the COSEC database and the devices. This functionality enables the system to pull (**Sync from Device**) the credentials from the Devices.

Single User

The screenshot shows a web interface titled "Sync From Device". On the left, there is a sidebar with two options: "Single User" (highlighted in blue) and "Multiple Users". The main content area is titled "Sync From Device" and contains two rows of input fields. The first row has a "Device" field with the value "1" and a "Credential" dropdown menu with "Cards" selected. The second row has a "User" field with the value "1581" and a text field with the value "Kinchit". Below these fields is a dark "Sync" button.

- **Device** - Click the device selection picklist button and select the device from the pop up window.
- **Credential** - Select a user credential from the drop down list. This feature supports following credentials:
 - Cards
 - FP Templates (Finger print and Duress)
 - Palm Templates

Sync From Device

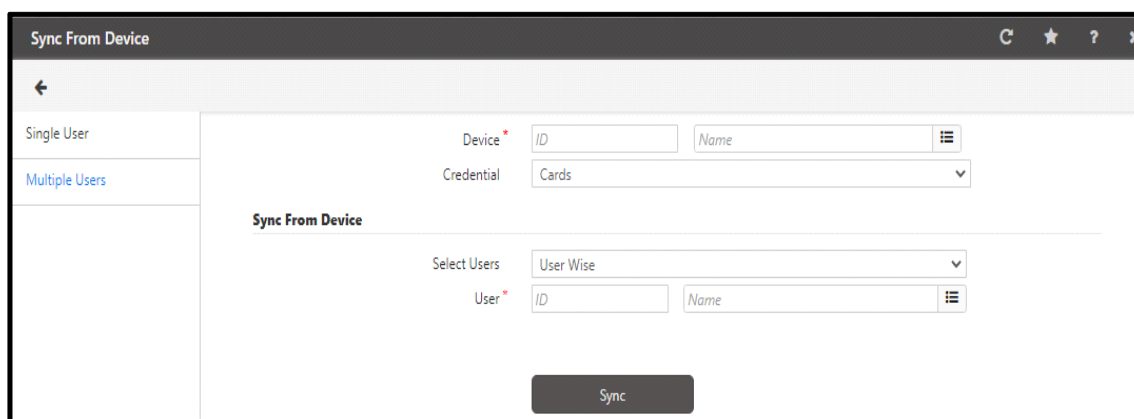
- **User** - Select a user from the user selection picklist whose credentials are to be synchronized.
- Click the **Sync** button to pull the specified credentials to the COSEC database successfully.



*If **Sync From Device** is done for **FP Templates** including **Duress Detection** templates from the Duress supported devices (V4, VEGA, ARGO, PATH V2 and ARC DC200 Direct Doors and V4, VEGA, ARGO, PATH V2 and ARC DC200 Panel Doors) to devices that do not support Duress, then the synced templates will be overwritten as normal templates.*

*And, if the **FP Templates** are synced from devices that do not support Duress, then all the templates will be synced as normal templates only, to all the devices.*

Multiple User



- **Device** - Click the device selection picklist button and select the device from the pop up window.
- **Credential** - Select a user credential from the drop down picklist. The options will differ as per the selected device. This feature supports following credentials -
 - Cards
 - FP Templates (Finger print and Duress)
 - Palm Templates

Sync From Device

- **User Filter** - Specify multiple users using this dropdown list. Choose from the following options -
 - **User Wise** - Select random users from the user picklist.
 - **Group Wise** - Select a group of users from the **Select Group** drop down list.
 - **ALL** - Select all users active on the system.
- Click the **Sync** button to pull the specified credentials for multiple users to the COSEC database successfully.



*If **Sync From Device** is done for **FP Templates** including **Duress Detection** templates from the Duress supported devices (V4, VEGA, ARGO, PATH V2 and ARC DC200 Direct Doors and V4, VEGA, ARGO, PATH V2 and ARC DC200 Panel Doors) to devices that do not support Duress, then the synced templates will be overwritten as normal templates.*

*And, if the **FP Templates** are synced from devices that do not support Duress, then all the templates will be synced as normal templates only, to all the devices.*

Reporting In-Charge

A large number of organizations are structured in a way that employees are grouped functionally and each group of employees is assigned to report everyday to a designated officer for efficient management purposes. This *Reporting In-Charge*, also known as Officer In-Charge or Reporting Manager, is responsible for overseeing and managing the reporting group assigned under him/her. COSEC allows the system administrator to assign employees to such reporting groups and also to define reporting in-charges from amongst active COSEC users.

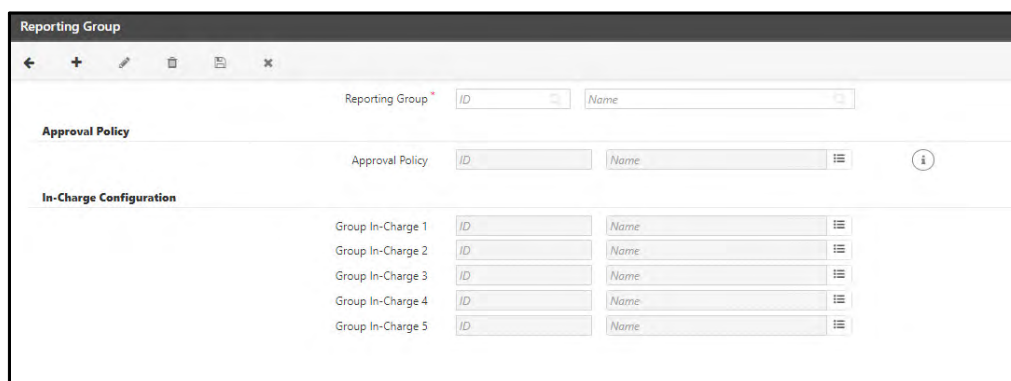
Once defined, this in-charge can perform certain authorizations and sanctioning to all users who are in the same reporting group. A Reporting In-Charge can manage multiple *Reporting Groups* but a user can belong to only one reporting group as a member. There is a provision to add upto five Reporting In-Charges for a Reporting Group along with its Approval Policy.

Reporting Group

To configure the Reporting Group parameters,

Click **Users > Reporting In-Charge > Reporting Group**.

The **Reporting Group** page appears.



Click **New**, to create a new Reporting Group. You can create upto 9999 Reporting Groups.

- **Reporting Group:** Enter a Name for the Reporting Group. The ID will be displayed after you save the Reporting Group.
- **Approval Policy:** Click the picklist to select the desired Approval Policy or enter the ID/Name of the Approval Policy manually.



If no Approval Policy is selected then, Reporting Group will work as per Any One Authorization Mode.

Reporting Group will work on AnyOne Authorization Mode irrespective of policy selected if selected in-charge from Approval Policy is not configured on this page.

- **In-Charge Configuration:** You can assign upto five in-charges for a single Reporting Group.



Selecting at least one Group In-Charge is mandatory.

Make sure the desired Reporting In-Charge/s (RIC) are configured as Users. For details, refer to [“Configuring Users”](#).

- **Group In-Charge 1 to Group In-Charge 5:** To assign each group in-charge, click the picklist to select the desired group in-charge or enter the ID/Name of the group in-charge manually.

The applications will be sent for approval to the Reporting Group In-Charge/s as per the Authorization Mode selected. The sequence in which it will be sent will depend on the configuration done in **Group In-Charge 1 to Group In-Charge 5**.

Click **Save**, to save the new Reporting Group.

The new Reporting Group will appear in the right pane of the page.



If the application is Pending and any Reporting In-Charge is deleted/deactivated from the system, then the application will still remain Pending with all the remaining Reporting In-Charge/s.

If the application is Approved/Rejected and any Reporting In-Charge is deleted/deactivated from the system, then there will be no change in the application as the final verdict has already been given.

If set of Reporting In-Charge configured in Reporting Group Page and Approval Policy page matches exactly with each other, then the application will be processed based on Approval Policy.

If set of Reporting In-Charge configured in Reporting Group Page has more In-Charge than set of Reporting In-Charge configured in Approval Policy Page then system will check if set of Reporting In-Charge configured in Approval Policy page is same as configured in Reporting Group page.

- If yes, then application will be processed based on Approval Policy selected for both pending and new application.
- If no, then all new applications process will get updated to Any One Authorization Mode (and the application will be sent to RIC configured in respective Reporting Group).

If number of Reporting In-Charge configured in Reporting Group page is less than number of Reporting In-Charge configured in Approval Policy. If yes, then application flow for all applications will get updated to Any One Authorization Mode (and application will be sent to Reporting In-Charge configured in respective Reporting Group).

If set of Reporting In-Charge configured in Reporting Group page and set of Reporting In-Charge configured in Approval Policy page for exception application does not match exactly with each other then application flow for exceptions application will get updated to Any One Authorization Mode (application will be sent to Reporting In-Charge configured in respective Reporting Group).

Approval Policy

Approval Policy enables to create different Approval Policies and to select the applications for which the Policy will be applicable.

To configure the Approval Policy parameters,

Click **Users > Reporting In-Charge > Approval Policy**.

The Approval Policy page appears.


ID	Name
1	AnyOne
2	All Sequential
3	All Final-1
4	All Final-2

By default there are four policies created — AnyOne, All Sequential, All Final-1, All Final-2.



If you are upgrading the system and you have existing users, then the Approval Policies (default as well as custom created) will remain the same. That is, the default policies will be — AnyOne, 1then2, Both Final-1 and Both Final-2.

For the default policies — All Sequential, All Final-1, All Final-2 — Short Leave/Official In-Out and Daily Attendance are listed in exception with Authorization Mode as Any One.

You can select the default policies and Edit the same by clicking **Edit**  or you can add a new policy.

To add a new policy,

Click **New**  . You can create upto 999 Approval Policies.

- **Approval Policy:** Enter a Name for the Approval Policy. The ID will be displayed after you save the Approval Policy.
- **Authorization Mode:** Select the Authorization Mode from the drop-down list — Any One, All, All Sequential

- **Any One:** If you select this option, then the authorization is done by any In-Charge among the selected associated Reporting In-Charge/s. The application will be sent to all the selected Reporting In-Charges and any In-Charge can provide the verdict. The In-Charge who gives the verdict first will be considered as the final verdict and the application status changes to the respective state as per the provided verdict. The verdict details will be displayed in the respective approval page. If you select this option, you also need to configure the **Reporting In-Charge**.
- **Reporting In-Charge:** Select the Reporting In-Charge/s from the drop-down list. Click **Check All** if you wish to select all the Reporting In-Charges. The application will be sent to the selected Reporting In-Charge/s.
- **All:** If you select All, the application will be sent to all the Reporting In-Charges for authorization and the verdict of the Final In-Charge will be considered as the final verdict. The application status changes to the respective state as per the provided verdict. The verdict details will be displayed in the respective approval page. If you select this option, you also need to configure the **Reporting In-Charge** and the **Final In-Charge**.
- **Reporting In-Charge:** Select the Reporting In-Charge/s from the drop-down list. Click **Check All** if you wish to select all the Reporting In-Charges. The application will be sent to the selected Reporting In-Charge/s.
- **Final In-Charge:** Select the Final In-Charge from the selected associated Reporting In-Charges. After the Final In-Charge provides the verdict, the application status changes to the respective state as per the provided verdict. The verdict details will be displayed in the respective approval page.
- **All Sequential:** If you select All Sequential, the application will be sent to all the Reporting In-Charges for authorization in the defined sequence. The application will only be sent from first Reporting In-Charge to the second Reporting In-Charge after the verdict of the first Reporting In-Charge is received and so on.

There is a provision to Auto Forward the application to the next Reporting In-Charge also. In this case, if the verdict is not provided by a Reporting In-Charge within the defined days, then the application will automatically be forwarded to the next Reporting In-Charge.

If you select this option, you also need to configure the **Reporting In-Charge** as well as **Auto Forward** parameters.

- **Reporting In-Charge:** Select the Reporting In-Charges from the drop-down list. Click **Check All** if you wish to select all the Reporting In-Charges. The application will be sent to all the selected Reporting In-Charges in a sequential manner.
- **Auto Forward:** To enable Auto Forward, configure the following parameters.

Reporting In-Charge	Auto Forward	Auto Forward After (Days)	Action
In-Charge 1	<input type="checkbox"/>		Approve ▼
In-Charge 2	<input type="checkbox"/>		Approve ▼
In-Charge 3	<input type="checkbox"/>		Approve ▼
In-Charge 4	<input type="checkbox"/>		Approve ▼
In-Charge 5	<input type="checkbox"/>		Approve ▼

- **Reporting In-Charge:** It displays the name of the Reporting In-Charge in a sequential manner.
- **Auto Forward:** Select the check box to enable the Auto Forward for the Reporting In-Charge.

- **Auto Forward After (Days):** Specify the duration in days after which the application should be sent to the next Reporting In-Charge if the verdict is not provided by this Reporting In-Charge.
- **Action:** Configure the Action from the drop-down list — Approve or Reject to be provided for the application.

After the last Reporting In-Charge has provided the verdict, the application status changes to the respective state as per the last Reporting In-Charge's verdict. The verdict details will be displayed in the respective approval page.



An application will be forwarded automatically after the specified days with the logic; [Application Date + Auto Forward configured days + 1]. For example: The application date=10 and configured Auto Forward days=1 then, the application will be forwarded automatically on date [10 + 1 + 1 = 12] =12.

For Reporting In-Charge 2, the date on which an application is received will be considered as the application date.

If the Reporting In-Charge 1, has Approved/Rejected an application manually before the specified Auto Forward days then, the application date for Reporting In-Charge 2 will be the date on which an application is approved or rejected.

If any Reporting In-Charge has rejected the application and the previous Final Reporting In-Charge is deactivated/deleted from the system and later the Reporting In-Charge who has rejected the application changes his/her verdict then the final application verdict will be of System Administrator.

Exceptions

Click **Add +** if you wish to add any applications in **Exceptions** list i.e. the applications for which Authorization Mode is to be set other than the default mode.

- **Application(s):** Select the desired Application(s) from the drop-down list to be added in Exceptions.
- **Customize Based On:** Select the field from the drop-down list to display the basis on which application needs to be customized.
- **Range:** Enter the From and To (Hours/ Days) on the basis of which the application will be selected.



The parameters **Customize Based On** and **Range** are visible depending upon the application which you select.

- **Authorization Mode:** Select the desired Authorization Mode from the drop-down list— Any One, All, All Sequential. Refer to the details mentioned above in Authorization Mode.

Click **Add** to add the application to the **Exceptions** table.

Click **Cancel** if you wish to remove all the configurations.

The **Exceptions** table displays the following parameters:

Exceptions						
<input type="text" value="Search"/>						
<div>+</div>						
Application(s) ▲	Range	Authorization Mode	Reporting In-Charge	Final In-Charge		
Unpaid Leave - UP UnpaidLeave	1.0 - 3.0 Days	All Sequential	In-Charge 1, In-Charge 3, In-Charge 5	In-Charge 5		
Unpaid Leave - UP UnpaidLeave	5.0 - 6.0 Days	All Sequential	In-Charge 2, In-Charge 3, In-Charge 4, In-Charge 5	In-Charge 5		
Unpaid Leave - UP UnpaidLeave	>= 6.0 Days	All Sequential	In-Charge 1, In-Charge 2, In-Charge 3, In-Charge 4, In-Charge 5	In-Charge 5		

- **Application(s):** It displays the Application(s) added in **Exceptions**.
- **Range:** It displays the From and To (Days/Hours) on the basis of which the application will be selected.
- **Authorization Mode:** It displays the selected pattern of approval for any application— Any One, All, All Sequential.
- **Reporting In-Charge:** It displays the selected Reporting In-Charge/s from whom approval needs to be taken.
- **Final In-Charge:** It displays the selected Final In-Charge when authorization mode is selected as **All** or **All Sequential**.
- **Delete:** Click **Delete**, if you wish to delete the particular application from the **Exceptions** table.

Exceptions

+

Application(s) ▲	Range	Authorization Mode	Reporting In-Charge	Final In-Charge	
Unpaid Leave - UP UnpaidLeave	1.0 - 3.0 Days	All Sequential	In-Charge 1, In-Charge 3, In-Charge 5	In-Charge 5	
Unpaid Leave - UP UnpaidLeave	5.0 - 6.0 Days	All Sequential	In-Charge 2, In-Charge 3, In-Charge 4, In-Charge 5	In-Charge 5	
Unpaid Leave - UP UnpaidLeave	>= 6.0 Days	All Sequential	In-Charge 1, In-Charge 2, In-Charge 3, In-Charge 4, In-Charge 5	In-Charge 5	

Application(s)

Select

Customized Based On

Duration

Range

1 Days - 3 Days

Authorization Mode

All Sequential

Reporting In-Charge *

Select

Reporting In-Charge	Auto Forward	Auto Forward After (Days)	Action
In-Charge 1	<input checked="" type="checkbox"/>	1	Approve
In-Charge 2	<input type="checkbox"/>		Approve
In-Charge 3	<input checked="" type="checkbox"/>	5	Approve
In-Charge 4	<input type="checkbox"/>		Approve
In-Charge 5	<input checked="" type="checkbox"/>	7	Approve

Update

Cancel

Select any of the application from the **Exceptions** table and click **Update** if you wish to edit the application.

The application will be updated in the **Exceptions** table.

Error List

If there are any issues while configuring the applications (that is overlaps) in the **Exceptions**, then an Error List will be generated.

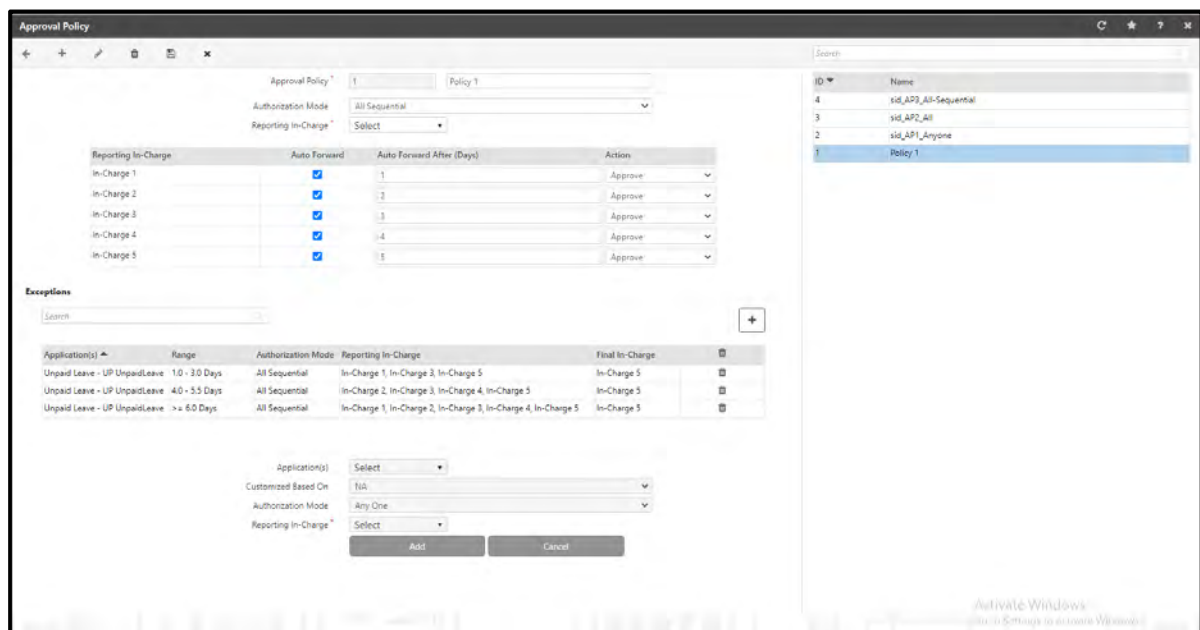
Click **Error List** collapsible panel. It displays the following parameters.



Application(s)	Status	Description
Paid Leave - PL Paid Leave	Failed to configure	Customize based on range overlap with existing Paid Leave - PL Paid Leave

- **Application(s):** It displays the Application type.
- **Status:** It displays the status of the application as failed to configure.
- **Description:** It displays the reason for failure of the application configuration.

Click **Save**, to save the Approval Policy. The new Approval Policy will appear in the right pane of the page.



The screenshot shows the 'Approval Policy' configuration window. It includes a search bar, a table for 'Reporting In-Charge' with columns for 'Auto Forward', 'Auto Forward After (Days)', and 'Action'. Below this is an 'Exceptions' section with a search bar and a table for 'Application(s)', 'Range', 'Authorization Mode', 'Reporting In-Charge', and 'Final In-Charge'. At the bottom, there are dropdown menus for 'Application(s)', 'Customized Based On', 'Authorization Mode', and 'Reporting In-Charge', along with 'Add' and 'Cancel' buttons. On the right side, there is a list of policies with columns 'ID' and 'Name'.

After creation of the Approval Policy, it can be assigned to the Reporting Group from **Reporting In-Charge >Reporting Group**. For more details, refer ["Reporting Group"](#).

In-Charge Permissions

This functionality facilitates the administrator to assign specific permissions to a particular Reporting In-charge defined on the system.

To assign In-Charge Permissions, Select the **Users module > Reporting In-Charge > In-Charge Permissions**.

The **In-Charge Permissions** page appears as shown below.

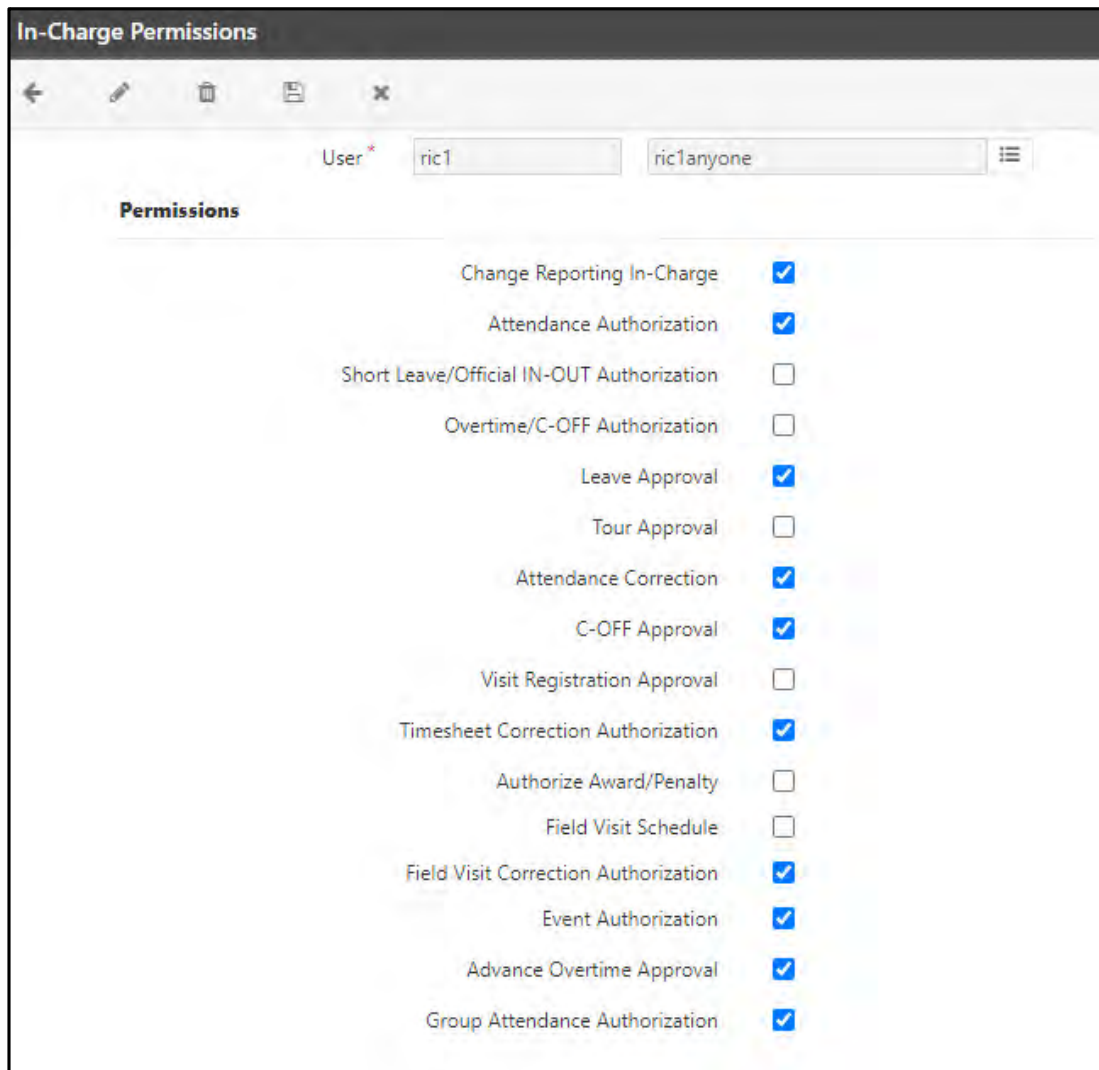
In-Charge Permissions

User* Name

Permissions

Change Reporting In-Charge	<input type="checkbox"/>
Attendance Authorization	<input type="checkbox"/>
Short Leave/Official IN-OUT Authorization	<input type="checkbox"/>
Overtime/C-OFF Authorization	<input type="checkbox"/>
Leave Approval	<input type="checkbox"/>
Tour Approval	<input type="checkbox"/>
Attendance Correction	<input type="checkbox"/>
C-OFF Approval	<input type="checkbox"/>
Visit Registration Approval	<input type="checkbox"/>
Timesheet Correction Authorization	<input type="checkbox"/>
Authorize Award/Penalty	<input type="checkbox"/>
Field Visit Schedule	<input type="checkbox"/>
Field Visit Correction Authorization	<input type="checkbox"/>
Event Authorization	<input type="checkbox"/>
Advance Overtime Approval	<input type="checkbox"/>
Group Attendance Authorization	<input type="checkbox"/>

- Select a Reporting In-Charge from the list on the right.



Permissions	Enabled
Change Reporting In-Charge	<input checked="" type="checkbox"/>
Attendance Authorization	<input checked="" type="checkbox"/>
Short Leave/Official IN-OUT Authorization	<input type="checkbox"/>
Overtime/C-OFF Authorization	<input type="checkbox"/>
Leave Approval	<input checked="" type="checkbox"/>
Tour Approval	<input type="checkbox"/>
Attendance Correction	<input checked="" type="checkbox"/>
C-OFF Approval	<input checked="" type="checkbox"/>
Visit Registration Approval	<input type="checkbox"/>
Timesheet Correction Authorization	<input checked="" type="checkbox"/>
Authorize Award/Penalty	<input type="checkbox"/>
Field Visit Schedule	<input type="checkbox"/>
Field Visit Correction Authorization	<input checked="" type="checkbox"/>
Event Authorization	<input checked="" type="checkbox"/>
Advance Overtime Approval	<input checked="" type="checkbox"/>
Group Attendance Authorization	<input checked="" type="checkbox"/>

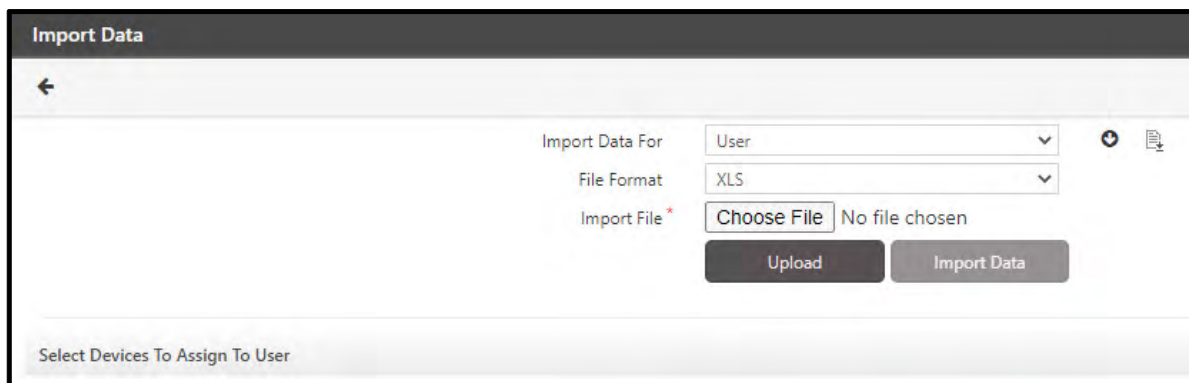
- Under **Permissions**, select the desired check boxes for the relevant permissions which are to be enabled for the selected Reporting In-Charge. This will permit the Reporting In-Charge to authorize the applications.
- Click **Save** button to save the permissions for the Reporting In-Charge.

Import Users

The COSEC application has an inbuilt utility for enabling users to import data from *Excel* files with predefined format. This would thus save the end user a lot of time and effort in having to make individual data entries at the application level.


To import user data from a file, select the **Users module > Utilities > Import Users**

The **Import Data** page appears as shown.




Configure the following parameters:

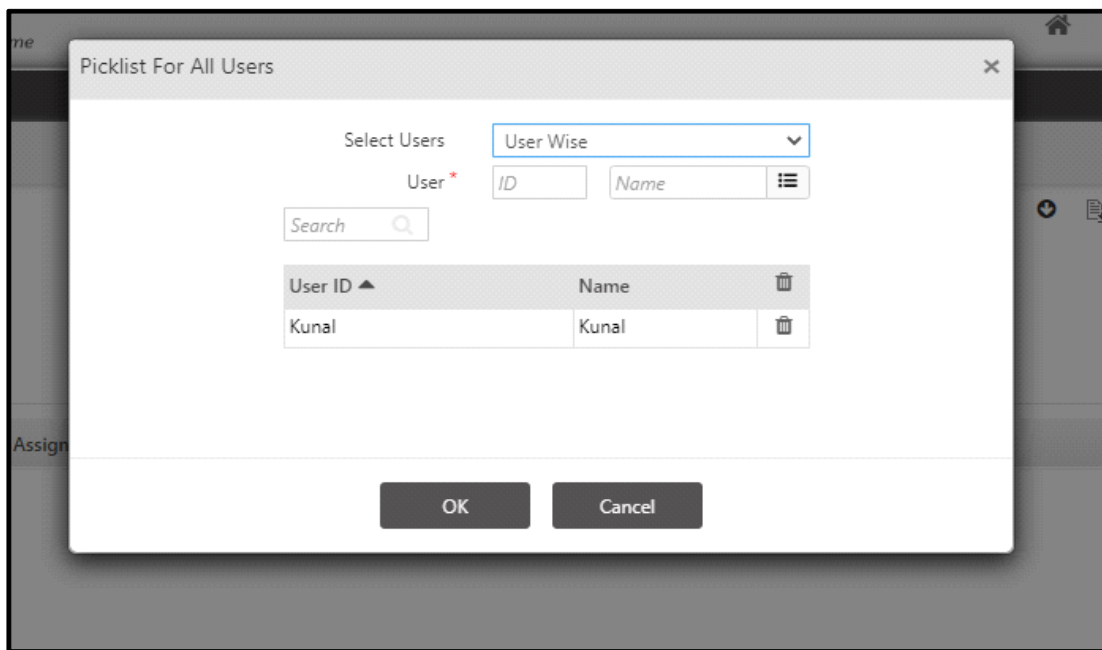
- **Import Data For** - Select the option from the dropdown list for which the data is to be imported.

You can download sample import file by clicking on **Download Sample Import file**  button. The import sheet displays the fields required for importing specific data.

The mandatory fields list is given in **Document guidelines** section of Import sheet.

	BK	BL	BM	BN	BO	BP	BQ	BR	BS	BT	BU	BV	BW	BX	BY
1	WorkProfileID	RosterPolicyID	HourExceptionID	LeaveGroup	WeekOffGroupID	Field1	Field2	Field3	Field4	Field5	Field6	Field7	Field8	Field9	Field10
2	1	452		22	6										
3	2	565		33	5										
4	3	899		44	4										
5	4	555		55	2										
6	5	454		66	1										

To download detailed sheet, click on **Download Detailed Data Sheet**  button. On clicking this button, a pop-up will be displayed as shown below:

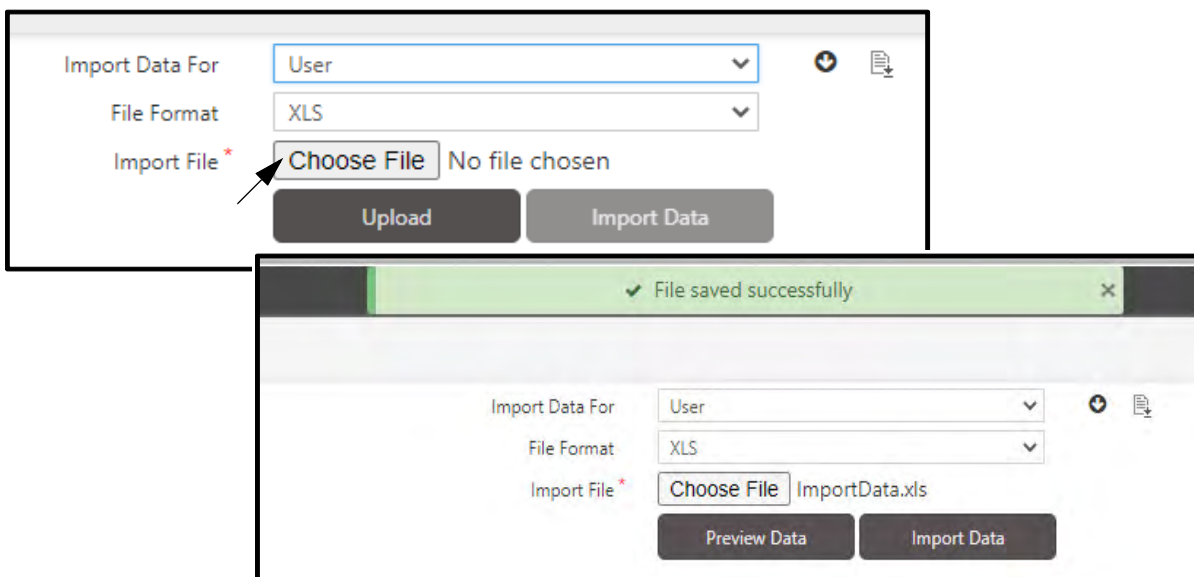


Select Users: Select the desired option — User Wise, Group Wise or All. If you select User Wise or Group Wise the select the desired users/groups from the picklist.

Click **OK** button to download the Data Sheet or click on **Cancel** button to abort the process.

The Detailed Data Sheet will be as per the selected option.

- **File Format** - Select the file format of the specific file from the dropdown list. The options available are XLS or CSV.
- **Import File** - Browse the path of the file from which the data is to be imported.



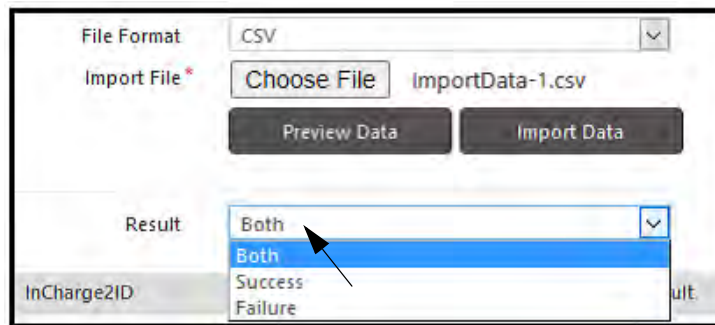
Click on **Upload** to save the file.

Click on **Preview Data** button to view the data in the respective worksheets to confirm that the data is in order prior to giving the import command.

Now click on **Import Data** to start importing the uploaded data. The result of import is shown as Success or Failure along with result description.

Select the device controllers to be assigned to the imported users by checking the boxes against the relevant controllers and click on **Import**. The system will import all the relevant valid entries from the sheet and will display the status in the bottom grid.

You can also filter import result records on the basis of their Success, Failure or Both using the **Result** drop-down options.



Once the data is imported successfully, data will be added or updated in User Profile in COSEC Web.



Administrator needs to ensure that the ASP.NET user has full rights on the folder containing the Excel or .csv file for the import data operation.



When new user is added or existing user's Enterprise group is changed. Then if user is assigned to the Enterprise group with which Job costing parameters are associated, then the configured job costing parameters will be assigned to the User.



When a new User/ Worker is created via Import Data for User and Worker then the user and worker configuration will be set according to the configuration set in Association Groups assigned to the user and worker.

Invite User

The Employee On Boarding Portal enables you to collect all the required details of the on boarding employees prior to their physically joining the organization.

To collect the required information, you need to:

- pre-determine all the details that you need to collect from the new on boarding employee. Refer to [“Invite User”](#).
- create a link that will be sent to the new on boarding employee for the collection of the details. For details refer to [“Generating the Invite Link”](#).
- set the alerts, refer to [“Configuring Alert Messages”](#).
 - To configure an alert message, click **Admin Module >System Configuration > Alert Message Configuration**. In Alert Filter make sure that you select *Users* from the drop-down list and in Event select *Invite User* from the drop down list.
 - To generate an OTP alert, click **Admin Module >System Configuration > Alert Message Configuration**. In Alert Filter make sure that you select *System* from the drop-down list and in Event select *OTP Generated* from the drop down list.
 - To configure an alert message for **User Onboarding- On Submit**, click **Admin Module >System Configuration > Alert Message Configuration**. In Alert Filter make sure that you select *Users* from the drop-down list and in Event select *User Onboarding- On Submit* from the drop down list. The alert message can also be configured from **Users Module> Utilities >Alert Assignment**, refer [“Assigning Alerts To Users”](#).
 - To configure an alert message for **User Onboarding- Schedule Time**, click **Admin Module >System Configuration > Alert Message Configuration**. In Alert Filter make sure that you select *Users* from the drop-down list and in Event select *User Onboarding- Schedule Time* from the drop down list. The alert message can also be configured from **Users Module> Utilities >Alert Assignment**, refer [“Assigning Alerts To Users”](#).



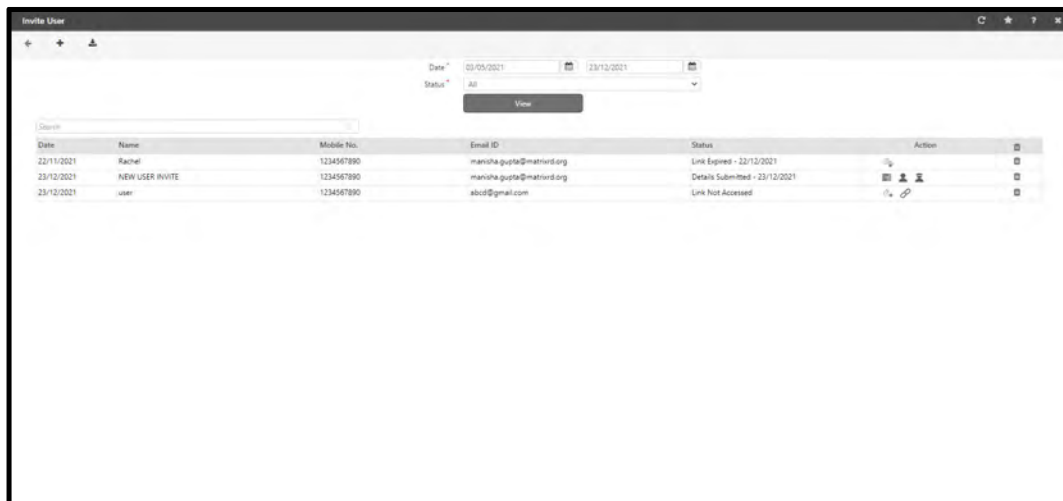
For the Invite Link to be accessible from the external network, make sure you have configured the COSEC Web URL (external) while installing the COSEC software.

Make sure you have configured COSEC Web URL (external) in System Configuration > General Settings in the Admin Web Portal.

Generating the Invite Link


- Click **Invite User**.

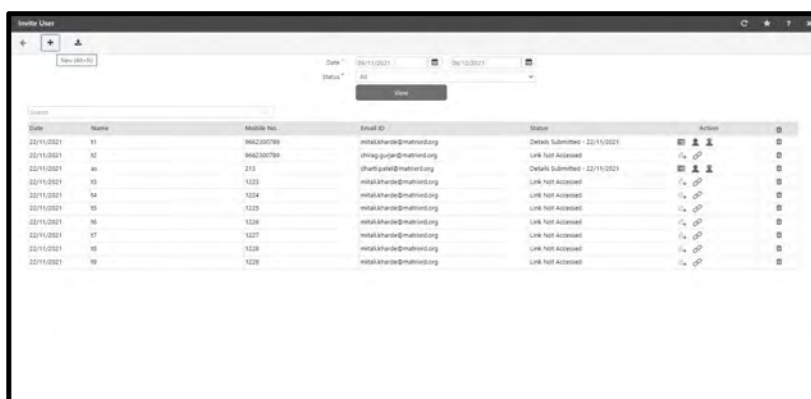
The **Invite User** page appears.



- You can enter the data manually or you can import a file.

Entering the data manually,

- To create a new invite link, click **New** .



- The **Invite User** pop-up appears.



- Click **Add** .

- Enter the details - **Name**, **Mobile Number** and **Email ID**.

Click **OK** to save or **Cancel** to abort the changes.

Click **Send Link**. The link will be created and sent to the new on boarding employee.

To import the file,


- Click **Import** .

Date	Name	Mobile No.	Email ID	Status	Action
18/10/2021	abcd	1234567890	abcd@gmail.com	Link Not Accessed	
19/10/2021	efgh	9876543210	efgh@gmail.com	Link Not Accessed	
20/10/2021	ij	2345678901	ijklm@gmail.com	Link Not Accessed	
21/10/2021	New joined	1234567890	manisha.gupta@matillion.org	Link Not Accessed	

- The **Import Invite User** pop-up appears.

- Select the desired **File Format** as - **XLS**, **CSV** or **XLSX**.



- Click **Download Sample Import File**  . A sample file will be downloaded with the name, **Import Data**.



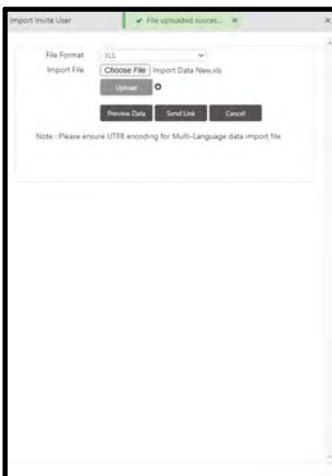
- Open the file.
- Click the **Invite User Sheet**.
- Enter the **Name**, **Mobile No** and **Email ID** of the new on boarding employee.
- Save the details.



- Now, click **Choose File** and select the **Import Data** file from the location on the PC.
- The selected file name appears as shown below. Click **Upload**.



- The confirmation message appears.



- Click **Preview Data**. The details are displayed under **Description**.

Import Invite User

File Format: CSV

Import File: Choose File ImportData.xls

Previous Data Send Link Cancel

Note : Please ensure UTF8 encoding for Multi-Language data import file

Description

Name	Mobile No.	Email ID
Nayan Kanya	8733953281	nayan.kanya@matrind.org
Hiral Radia	436789	hiral.radia@matrind.org

- Click **Send Link** to send the on boarding employee invite link to the **Mobile No.** and **Email ID**.
- The confirmation message appears.

Import Invite User Processing Completed

File Format: CSV

Import File: Choose File ImportData.xls

Previous Data Send Link Cancel

Note : Please ensure UTF8 encoding for Multi-Language data import file

Description

Name	Mobile No.	Email ID	Success	Description
Nayan Kanya	8733953281	nayan.kanya@matrind.org	Yes	Send Link Successfully
Hiral Radia	436789	hiral.radia@matrind.org	Yes	Send Link Successfully

- After the link is sent, the **status** of the links will update in the grid below.

Matrix COSEC

Invite User

Date: 22/11/2021 Status: All

Date	Name	Mobile No.	Email ID	Status	Action
22/11/2021	Nayan Kanya	8733953281	nayan.kanya@matrind.org	Link Accepted	22/11/2021
22/11/2021	Hiral Radia	436789	hiral.radia@matrind.org	Link Accepted	22/11/2021

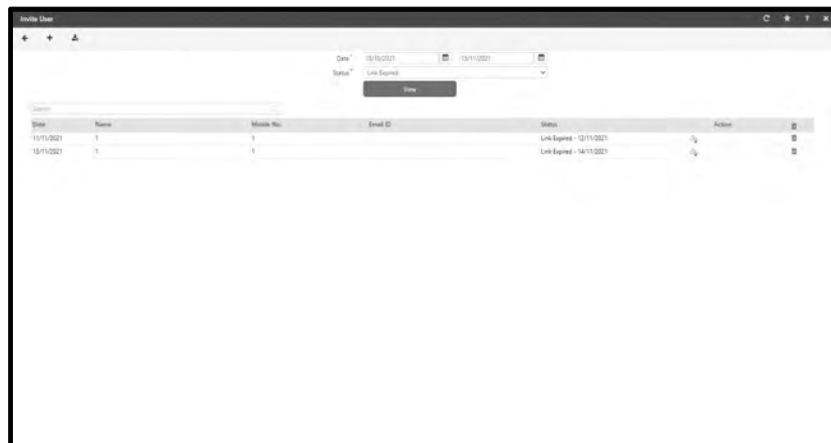
Filtering the records as per Status


You can filter the records by setting the following parameters as per your requirement:

Date: Select the start and end date.

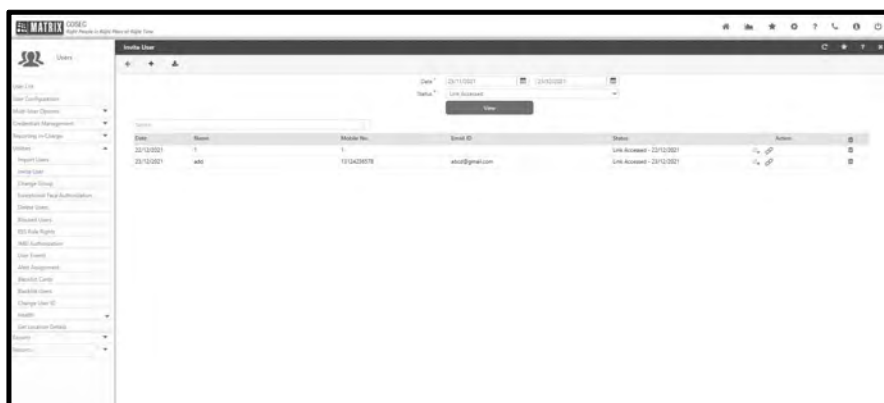
Status: Select the desired status from the drop down list — All, Link Not Accessed, Link Expired, Link Accessed, Details Submitted.

If you select **Link Expired** and click **View**.



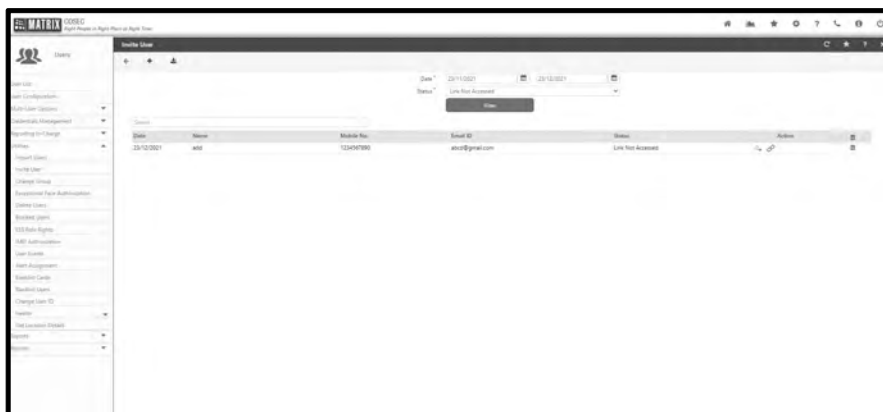
- The records whose links have expired will be displayed.
- If you wish to regenerate the link, click **Regenerate**  .



If you select **Link Accessed** and click **View**.



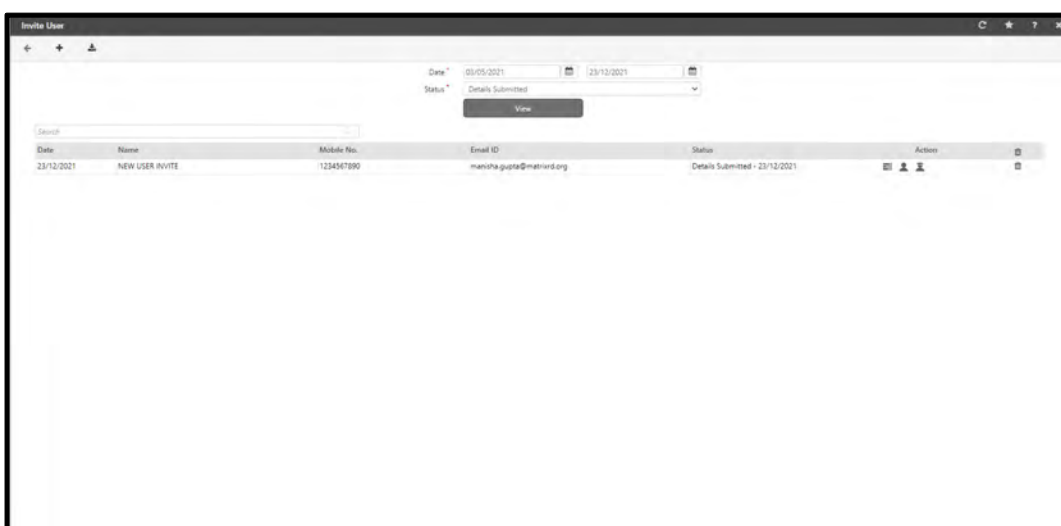
- The records of accessed links will be displayed.
- If you wish to resend the link, click **Resend**  or if you wish to copy the link, click **Copy**  .




If you select **Link Not Accessed** and click on **View**



- The records whose links have not been accessed will be displayed.
- If you wish to resend the link, click **Resend**  or if you wish to copy the link, click **Copy** .

If you select **Details Submitted** and click **View**.



- The records whose documents have been submitted will be displayed.
- If you wish to view the submitted details, click **Details** .
- If you wish to add the on boarding employee as a new user, click **Add User** .
- OR
- if you wish to add the on boarding employee as a worker, click **Add Worker** .

If you select **All** and click **View**.

Date	Name	Mobile No.	Email ID	Status	Actions
23/10/2021	ADIN USER ADITE	1234567890	manishgupta@matrixindia.org	Details Submitted - 23/10/2021	[Icons]
23/10/2021	user	1234567890	abc@gmail.com	Details Submitted - 23/10/2021	[Icons]
23/10/2021	Adin User	1234567890	manishgupta@gmail.com	Details Submitted - 23/10/2021	[Icons]
23/10/2021	adit	1234567890	abc@gmail.com	Link Not Activated	[Icons]

- All the records will be displayed.

Accessing the Link

New Employee

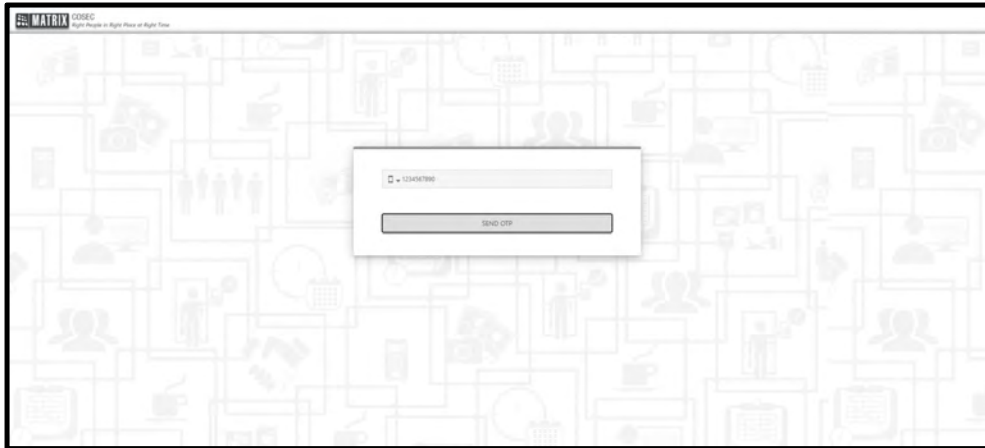
The new on boarding employee will receive an invitation link on the Mobile Number/ Email ID.

- Click the link received on the Mobile/Email.

Sample for Email is given below:



- The new on boarding employee is directed to the following page.



- Select the option - **Mobile** or **Email** on which the OTP is to be sent.
- Click **Send OTP**.
- The following page appears.



- Enter the received **OTP**.
- Click **LOGIN**.



- The new employee on boarding details page appears.
- The new employees must enter the **Basic, General, Personal** and **Contact** details.

Face Image: You can **Upload** the image directly from the local PC or you can **Capture** the image first and then click **Upload**.

At most four images can be Uploaded/ Captured.



To capture the image, make sure the camera is connected.

- Click **Save** to save all the details.
- The **Information** pop-up appears. Click **OK**.

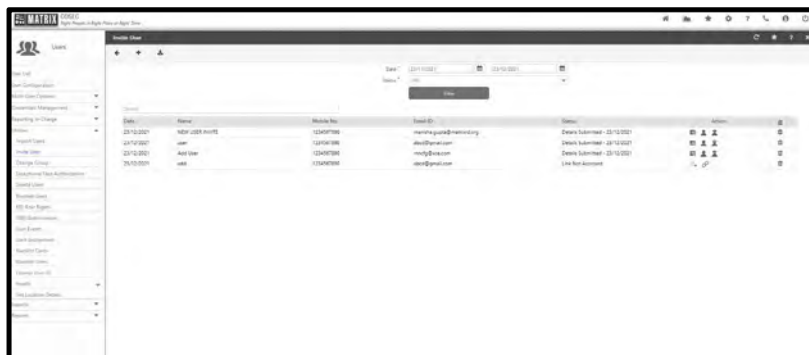
- The filled details are displayed.

- Click **Submit**.
- **Information** pop-up appears. Click **OK**.

- The new on boarding employee is logged out.
- Confirmation message appears.

Admin

To view **Status** of links, click **Users > Utilities > Invite Users**.



You can filter the records by settings the following parameters as per your requirement:

Date: Select the start and end date to specify the duration.

Status: Select the desired status from the drop down list. Refer [“”](#).

Changing Group

The Users Module provides a functionality whereby the user has the option to change the groups like Organization, Branch, Department, Section, Category, Grade, Designation, Custom Groups and Reporting Group to which an employee is currently linked. This change can be applied for a user-definable time period. The system also maintains the group change records for each user. User group changes can be assigned both for a single user or multiple users at a time.



The Group of any user can be changed **99999** times.

Single User

To change group for a single user, Select the **Users module > Utilities > Change Group**.

The **Change Group** page will open as follows:

User ID: Select a user from the user selection picklist, for whom the group change should apply.

Select the **Additional Details** section to view the group details for the selected user as shown below.

Change Group: Select the group from the options of Enterprise groups and Reporting Group to be changed for the selected user.

Date: Select the start and end date to specify the duration for which the group change is to be done.

New Group: Select the new group from the picklist to be assigned to the user.

Remark: You can add a Remark for the change to be done.

Click **Apply** to apply the changes for the selected user.

The changes can be viewed by clicking **User Group Change Records** as shown below.

The screenshot shows a web application interface for managing user group changes. At the top, there is a form with the following fields: 'User ID *' with the value '1687', a user name 'Aditi Gupta', and a dropdown menu. Below this is a section titled 'Additional Details' containing: 'Change Group *' with a dropdown set to 'Company', 'Date *' with a date range from '03/10/2017' to '31/10/2017', 'New Group *' with a dropdown set to '1' and a label 'Matrix', and a 'Remark' field with the text 'Organization change for October'. There are 'Apply' and 'Clear' buttons. Below the form is a section titled 'User Group Change Records' with a search bar and a table showing the change history.

User ID ▲	Group Type	From	To	New Group
1687	Company	01/01/2009	31/12/2099	Organization2
1687	Company	09/05/2017	31/12/2099	Organization2
1687	Company	03/10/2017	31/10/2017	Matrix
1687	ReportingGroup	28/03/2017	31/12/2099	ri1



*When existing user's Enterprise group is changed. Then if user is assigned to the Enterprise group with which **Job costing** parameters are associated, then the configured job costing parameters will be assigned to the user.*

Multiple Users

To change group for multiple users, Select the **Users Module > Utilities > Change Group > Multi User**

The **Multi User** page will appear as follows:

The screenshot shows the 'Change Group' form with the 'Multi User' tab selected. The form contains the following fields and controls:

- Group Type:** A dropdown menu set to 'ReportingGroup'.
- Date:** Two date pickers showing '04/07/2017' and '12/31/2099'.
- New Group:** A text input with '3' and a picklist showing 'Hardware Repo Group'.
- Remark:** A text input field.
- Select Users:** A dropdown menu set to 'User Wise'.
- User:** Two input fields for 'ID' and 'Name'.
- Apply:** A button at the bottom.

Group Type: Select a group type from the dropdown list for which the change is to be done.

Date: Select the start and end date to specify the duration for which the group change is to be done.

New Group: Select the new group from the picklist to be assigned to the user.

Remark: You can add a Remark for the change to be done.

This screenshot shows the 'Change Group' form with the 'Multi User' tab selected. The 'Select Users' section is expanded, showing a list of users. The 'User' dropdown is set to 'User Wise'. The list of users is as follows:

User ID	Name	
2	Chirag	
3	Isha	
4	Sweta	

An 'Apply' button is located at the bottom of the form.

Select Users: Select the users by filtering the option of User Wise, Group Wise or All.

Click the **Apply** button to apply the changes.

Exceptional Face Authorization

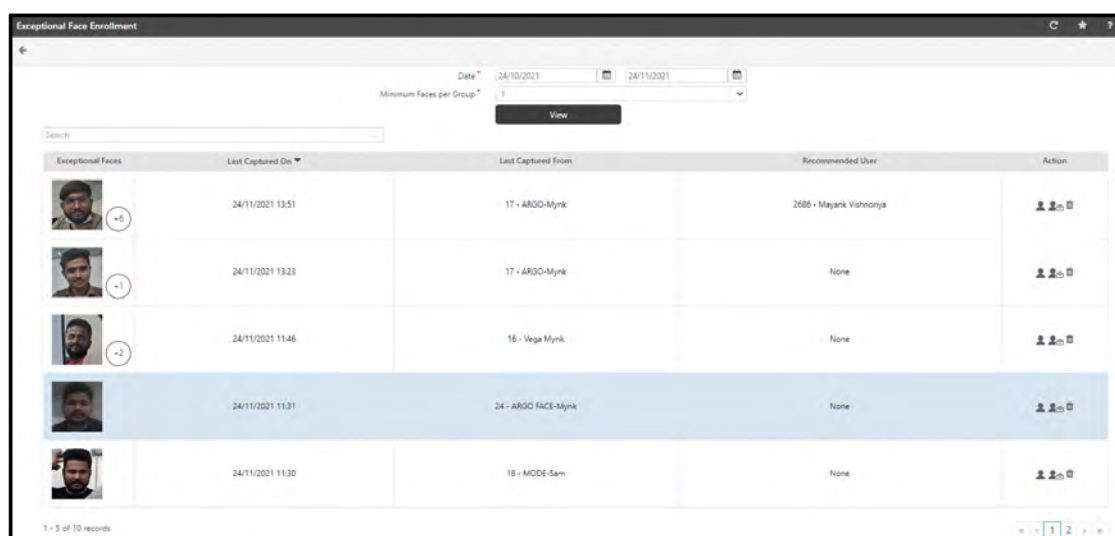
During face recognition, if a user is not identified by his/her face credential, the system will consider this face as an Exceptional Face. These exceptional or unidentified faces are stored in the database.

The system may store a single face or multiple faces of the same user (known as cluster).
















The System Admin can view the details and accordingly perform action— enrolling these exceptional faces against an existing/new user/visitor or can delete them.

To view exceptional face, click **Users > Utilities> Exceptional Face Authorization**.

The **Exceptional Face Authorization** page appears as below:



The screenshot shows the 'Exceptional Face Enrollment' interface. At the top, there are date range filters (24/10/2021 to 24/11/2021) and a 'Minimum Faces per Group' dropdown set to 1. A 'View' button is present. Below is a table with columns: Exceptional Faces, Last Captured On, Last Captured From, Recommended User, and Action. The table contains five rows of face images with associated data. The fourth row is highlighted in blue. At the bottom left, it says '1 - 5 of 10 records'.

Exceptional Faces	Last Captured On	Last Captured From	Recommended User	Action
 +5	24/11/2021 13:51	17 - ARGO-Mynk	2588 - Mayank Vishnoria	 
 -1	24/11/2021 13:23	17 - ARGO-Mynk	None	 
 -2	24/11/2021 11:46	18 - Vega Mynk	None	 
	24/11/2021 11:31	24 - ARGO FACE-Mynk	None	 
	24/11/2021 11:30	18 - MODE-Sam	None	 

Setting the Filters

- **Date:** Select the desired date range to display the captured exceptional faces during that duration.
- **Minimum Faces per Group:** There can be multiple images of a single unidentified user stored in a cluster. There can be multiple clusters of different unidentified users.

Select the desired value in **Minimum Faces per Group**. As per the number set here the system will filter records of clusters equal to and greater than this number.

- Click **View**. The records will appear as per the set filters.

Filtered Records

The grid displays the exceptional faces of unidentified users with the following details:

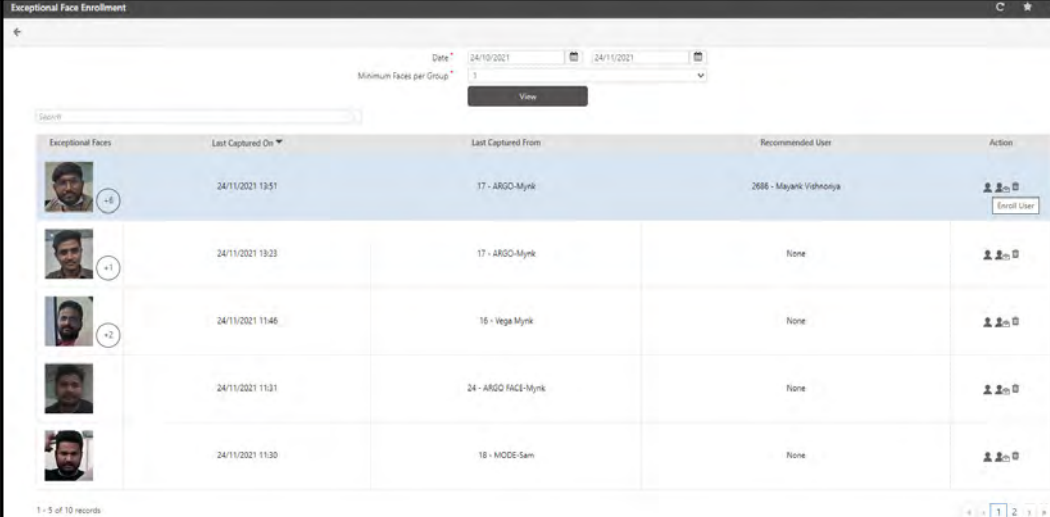
- **Exceptional Faces:** It displays the latest captured image of the user in the cluster along with the total count of captured exceptional faces.
- **Last Captured On:** Displays the date and time of the last captured image.











- **Last Captured From:** Displays the Device ID and the Device Name from which the last image has been captured.
- **Recommended User:** Displays the best match found User ID and User Name from the database for the unidentified user.
If there is no match found for the unidentified user image in the database, then it displays **None**.
- **Action:** The System Admin can perform the following actions:
 - **Enroll User/Visitor:** Exceptional faces in a cluster can be enrolled against an existing or new user/visitor. Refer [“Enrolling the Exceptional Face”](#)
 - **Remove:** Exceptional faces from the cluster can be removed or deleted. Refer [“Deleting the Exceptional Face”](#)

Enrolling the Exceptional Face

Enrolling Users

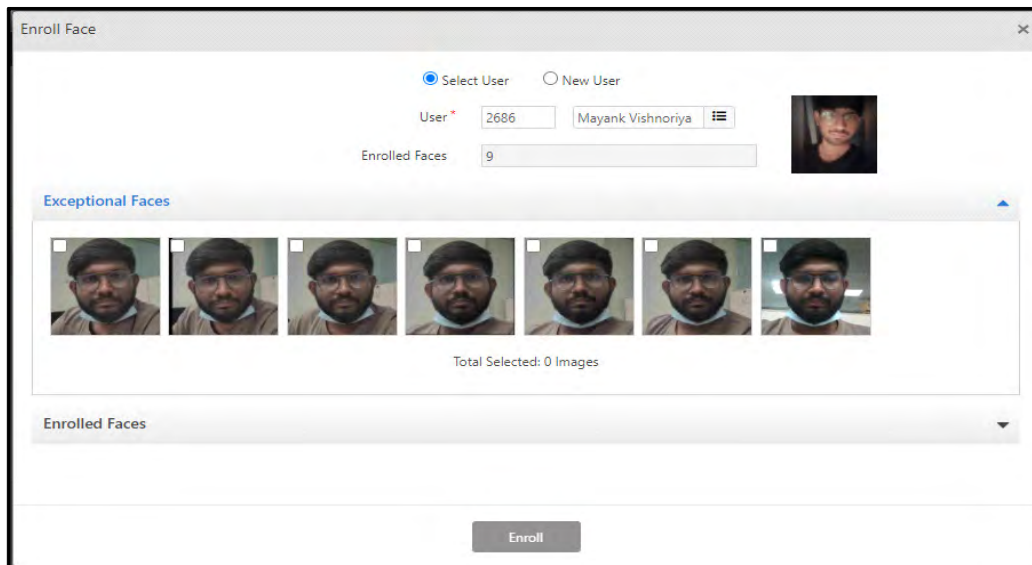
Click Enroll  icon to enroll a User.



Exceptional Faces	Last Captured On	Last Captured From	Recommended User	Action
 +6	24/11/2021 13:51	17 - ARGO-Myrk	2686 - Mayank Vishnoria	 Enroll User
 +1	24/11/2021 19:23	17 - ARGO-Myrk	None	 Enroll User
 +2	24/11/2021 11:46	16 - Vega Myrk	None	 Enroll User
	24/11/2021 11:31	24 - ARGO FACE-Myrk	None	 Enroll User
	24/11/2021 11:30	18 - MODE-Sam	None	 Enroll User

1 - 5 of 10 records

An **Enroll Face** pop-up appears as shown below:



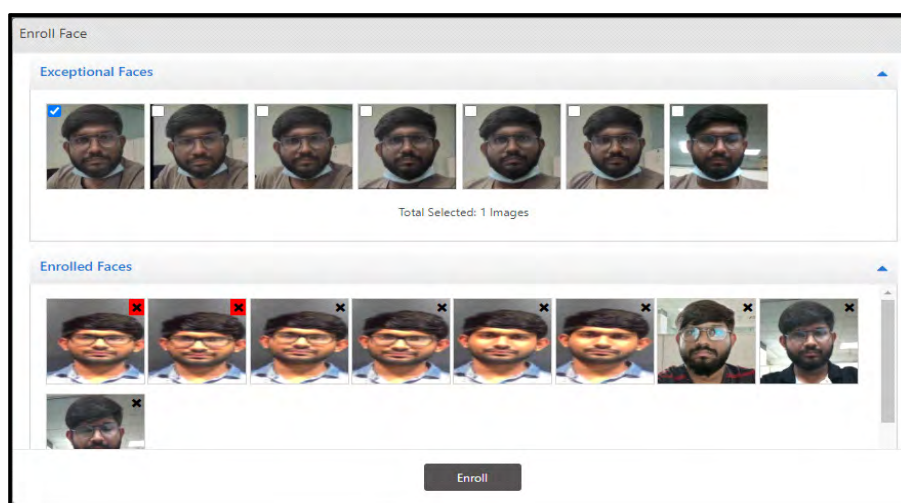
- If you want to enroll the images against an existing user, click **Select User**.
- **User**: Select the user from the pick list.
- **Enrolled Faces**: Displays the number of already enrolled faces against the user in the database.
- **Exceptional Faces**: Click the **Exceptional Faces** collapsible panel. It displays all the captured exceptional faces against this user. Select the check boxes of the desired exceptional face images that you wish to add to the list of enrolled face of the user.

The number of exceptional face images selected will be displayed as the **Total Selected** images.



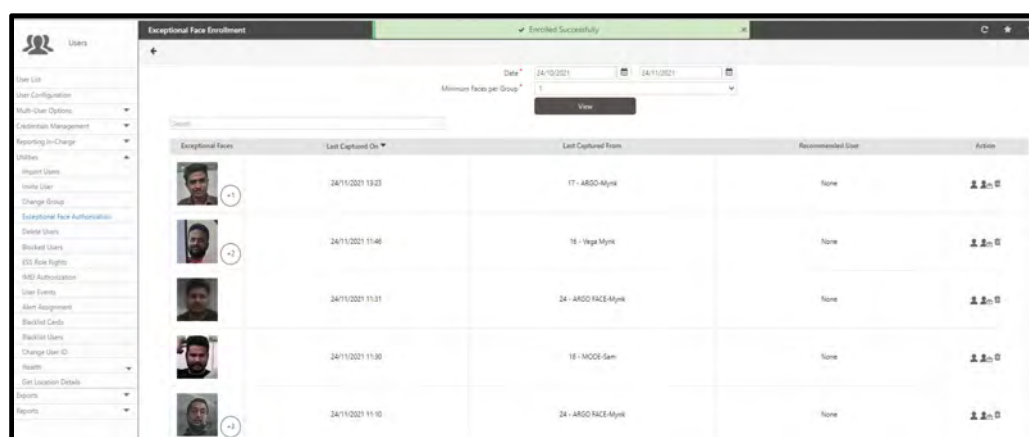
*Make sure the number of faces you consider for enrollment is lesser than or equal to the defined value in **Maximum No. of Faces** in Admin >System configuration> Global Policy >User.*

- **Enrolled Faces**: Click the **Enrolled Faces** collapsible panel. It displays the enrolled images of the user currently in the database.



- Click **Enroll**. The selected Exceptional Faces will now be considered as Enrolled Faces.
- To replace an existing enrolled faces,
 - Click on the desired image under **Enrolled Faces**, the red cross icon appears on the top right corner of the image.
 - Select the check box of the desired image under **Exceptional Faces** that you wish to add.
 - Click **Enroll**.

The image with the cross icon in Enrolled Faces will be replaced with the desired Exceptional Face image.



- If you want to enroll the images against a new user, click **New User**.


The screenshot shows the 'Enroll Face' window. At the top, there are two radio buttons: 'Select User' (unselected) and 'New User' (selected). Below these are input fields for 'ID' and 'Name'. A section titled 'Exceptional Faces' contains two face images. Below the images, it says 'Total Selected: 0 Images'. At the bottom, there is an 'Enroll' button.

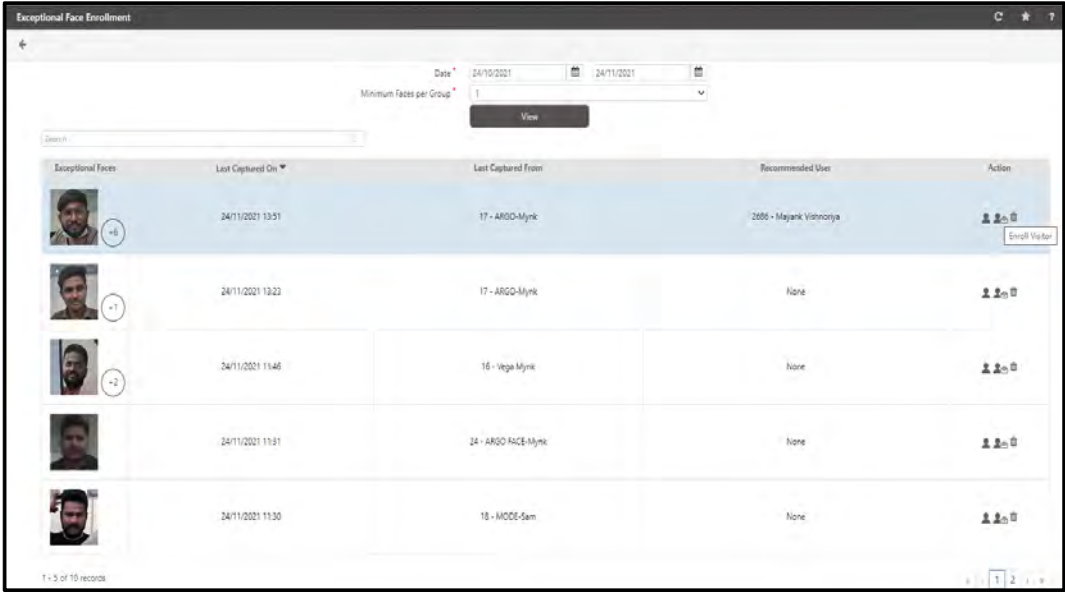
- **ID:** Enter the ID of the new user.
- **Name:** Enter the name of the new user.
- **Exceptional Faces:** Click the **Exceptional Faces** collapsible panel. It displays all the captured exceptional faces against this user. Select the check boxes of the desired exceptional face images that you wish to add to the list of enrolled face of the user.
















The number of exceptional face images selected will be displayed in **Total Selected**.

- Click **Enroll**. The selected Exceptional Faces will now be considered as Enrolled Faces.

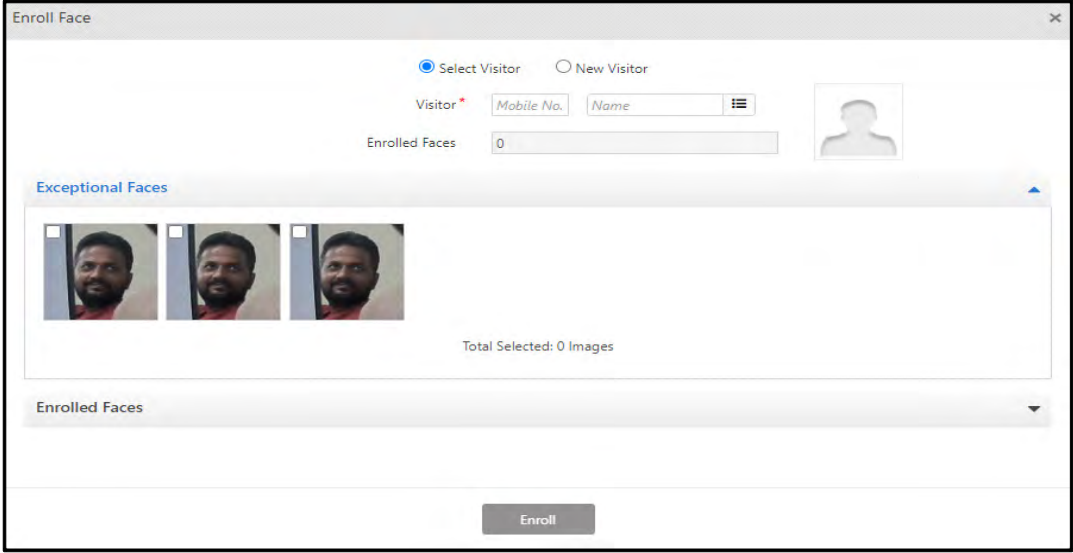
Enrolling Visitor

Click  icon to enroll a Visitor.



Exceptional Faces	Last Captured On	Last Captured From	Recommended User	Action
 +6	24/11/2021 13:51	17 - ARGO-Mynk	2686 - Majank Vinnoraya	 
 +1	24/11/2021 13:23	17 - ARGO-Mynk	None	 
 +2	24/11/2021 11:46	16 - Vega Mynk	None	 
	24/11/2021 11:31	24 - ARGO FACE-Mynk	None	 
	24/11/2021 11:30	18 - MOOS-Sam	None	 

An **Enroll Face** pop-up will appear as shown below:



Enroll Face

☒ Select Visitor ☐ New Visitor

Visitor *

Enrolled Faces

Exceptional Faces

Total Selected: 0 Images

Enroll

- If you want to enroll the images against an existing visitor, click **Select Visitor**.
- Visitor:** Select the visitor from the pick list.
- Enrolled Faces:** Displays the number of already enrolled faces against the visitor.

- **Exceptional Faces:** Click the **Exceptional Faces** collapsible panel. It displays all the captured exceptional faces against this visitor. Select the check boxes of the desired exceptional face images that you wish to add to the list of enrolled face of the visitor.

The number of exceptional face images selected will be displayed in **Total Selected** images.


- **Enrolled Faces:** Click the **Enrolled Faces** collapsible panel. It displays the enrolled images of the visitor currently in the database.
- Click **Enroll**. The selected Exceptional Faces will now be considered as Enrolled Faces.
- To replace an existing enrolled faces,
 - Click on the desired image under **Enrolled Faces** the red cross icon appears on the top right corner of the image.
 - Select the check box of the desired image under **Exceptional Faces** that you wish to add.
 - Click **Enroll**.

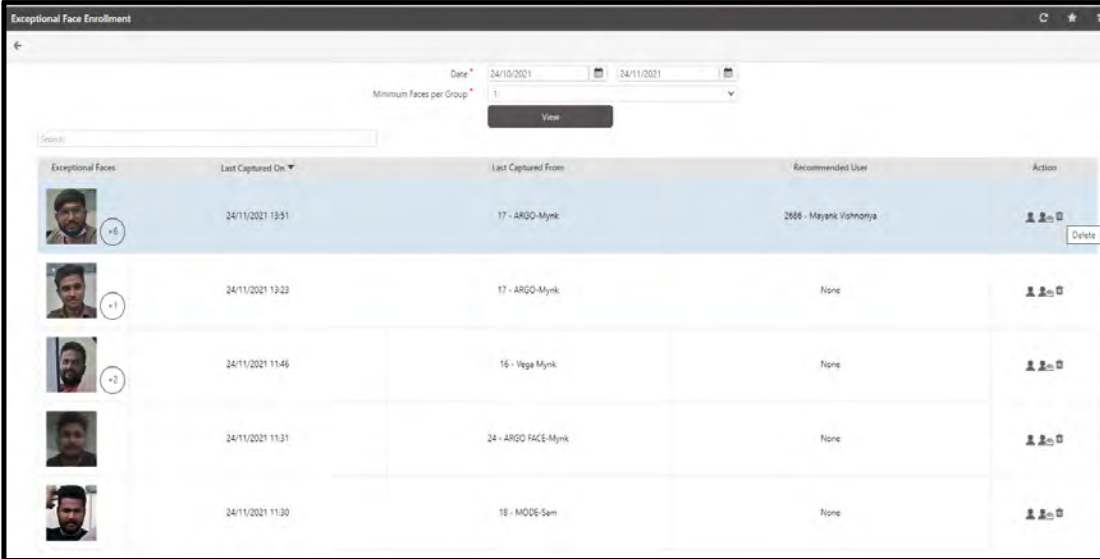
The image with the cross icon in Enrolled Faces will be replaced with the desired Exceptional Face image.





















- If you want to enroll the images against a new Visitor, then click **New Visitor**

- **Mobile No:** Enter the mobile number of the new visitor
- **Name:** Enter the name of the new visitor.
- **Exceptional Faces:** Click the **Exceptional Faces** collapsible panel. It displays all the captured exceptional faces against this visitor. Select the check boxes of the desired exceptional face images that you wish to add to the list of enrolled face of the visitor.
- Click **Enroll**. The selected Exceptional Faces will now be considered as Enrolled Faces.

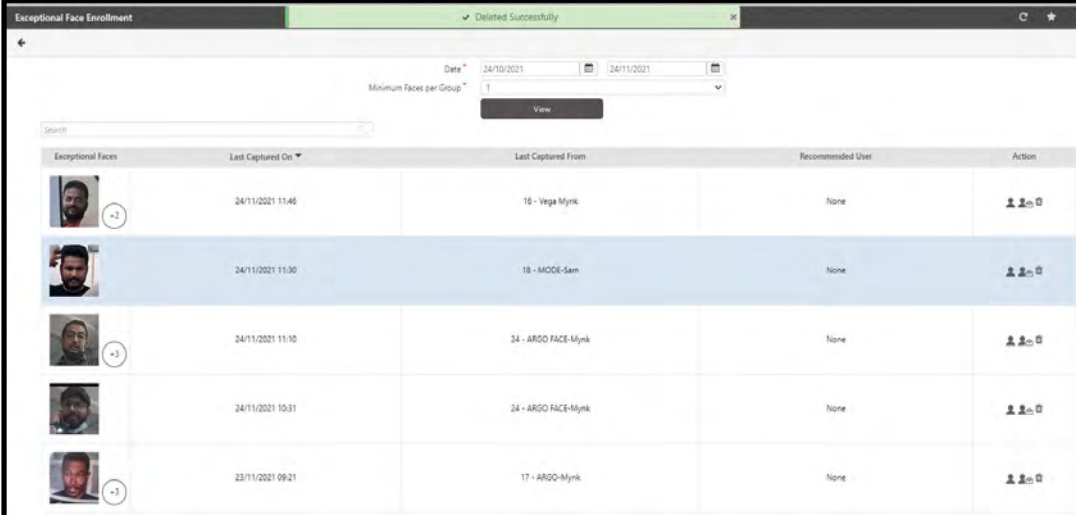
Deleting the Exceptional Face





















Click  icon to remove an exceptional face.



Exceptional Faces	Last Captured On	Last Captured From	Recommended User	Action
 +6	24/11/2021 13:31	17 - ARGO-Myrik	2686 - Mayank Vishnootiya	   Delete
 +1	24/11/2021 13:23	17 - ARGO-Myrik	None	  
 +2	24/11/2021 13:46	16 - Vega Myrik	None	  
 +1	24/11/2021 11:31	24 - ARGO FACE-Myrik	None	  
 +1	24/11/2021 11:30	18 - MODE-Sam	None	  

The exceptional face will be successfully deleted from the database.



Exceptional Faces	Last Captured On	Last Captured From	Recommended User	Action
 +2	24/11/2021 11:46	16 - Vega Myrik	None	  
 +1	24/11/2021 11:30	18 - MODE-Sam	None	  
 +3	24/11/2021 11:10	24 - ARGO FACE-Myrik	None	  
 +1	24/11/2021 10:31	24 - ARGO FACE-Myrik	None	  
 +3	23/11/2021 09:21	17 - ARGO-Myrik	None	  

Deleting Users

This option enables the administrator to delete single or multiple users from the COSEC database.



This is an irreversible process. Proceed with caution.

To delete users from the system, Select the **Users Module > Utilities > Delete Users**.

The **Delete Users** page appears as follows:

The user needs to re-enter the logged in user credentials to access this critical functionality as shown.

The administrator can now select the user or the group of users to be deleted from the COSEC database using the **User Filter** drop down list as shown.

The **User Filter** section allows you the following options for multiple user selection:

- **User Wise:** Enables administrator to randomly select users by clicking the **Select Users** button.
- **Group Wise:** Enables the administrator to select all users belonging to a particular group.
- **All:** Enables administrator to select all active users in the database.

To apply all the changes made, click the **Apply** button.

The system will successfully delete all the selected users from the COSEC database.

Blocked Users

Users whose credentials have been temporarily blocked due to inactivity for prolonged periods are referred to as *Blocked Users*. This could happen in the event of the Absentee rule being applied to the user or unauthorized access attempts exceeding the defined limit.

Blocking a user only deactivates the credential and does not result in the deletion of user information from the database.



*This functionality is available only with the **Access Control** add on module.*



The Alert Service must be running to generate the Block User event.

To access this functionality, Select the **Users module > Utilities > Blocked Users**.

The **Blocked Users** page appears as shown:

ID	Name	Panel/Direct Door	Block DateTime	Reason for Block	Remark	Restore
1	Shinjini	PVR Door-Device-1	08/11/2017 23:59:27	Absentee Rule		
2	Nikita	PVR Door-Device-1	09/11/2017 00:00:00	Absentee Rule		

Restored User (0)

Suppose Absentee rule is configured for user Shinjini for 15 days. And she is absent for 15 days; when she punches on 16th day (roll-over of date) then she will be denied access with reason: “User is Blocked”. And she will be listed in the Blocked user list as shown above.

- Click the **Blocked User** section to view details of blocked users such as name of the user, name of the door, block date and time, reason for blocking etc. along with the option to restore selected users from their “blocked” status.
- The administrator can re-activate any of the users in the blocked list by clicking on the **Restore** option against the selected user in the list.
- There is a provision for adding **remarks** which can be viewed later for reporting and analysis as well as deciding the future course of action.

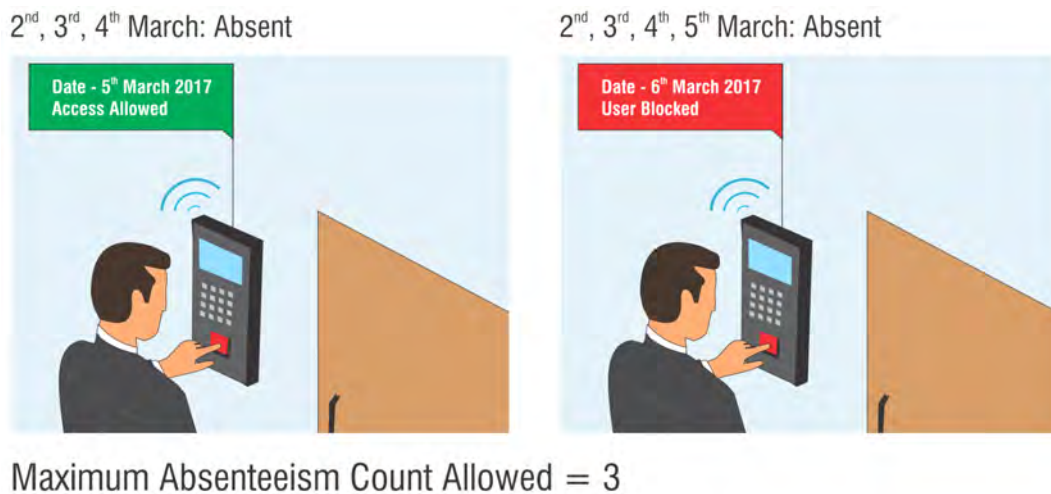
Blocked User						
Blocked User (2)						
ID	Name	Panel/Direct Door	Block DateTime	Reason for Block	Remark	Restore
1	Shinjini	PVR Door-Device-1	08/11/2017 23:59:27	Absentee Rule	User is restored	
2	Nikita	PVR Door-Device-1	09/11/2017 00:00:00	Absentee Rule		
Restored User (0)						

The restored user will be shown in **Restored User** list as shown below.

Blocked User						
Blocked User (1)						
Restored User (1)						
ID	Name	Panel/Direct Door	Application Restore DateTime	Controller Restore DateTime	Remark	
1	Shinjini	PVR Door-Device-1	09/11/2017 16:04:36		User is restored	

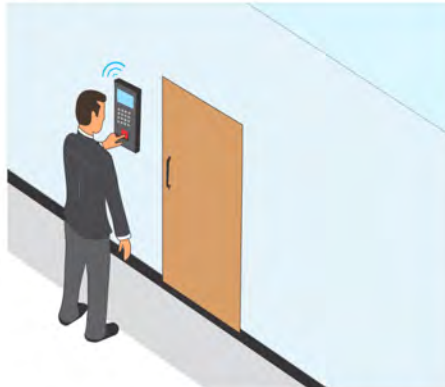
- The reason for the de-activation of the user credential is displayed in the **Reason for Block** column. The possible reasons for deactivation are:

1. Absentee rule being applied to user

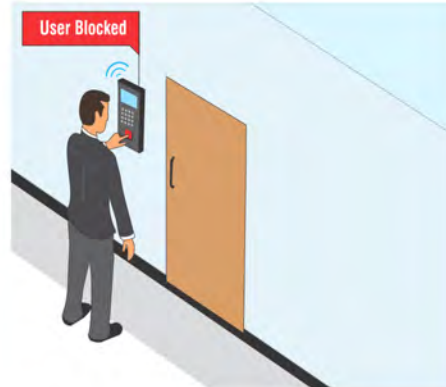


2. The Use Count Control rule has been violated.

Time - 11:01
Attempt - 1



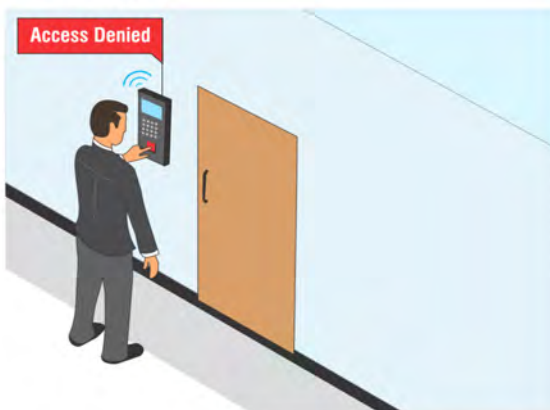
Time - 11:01
Attempt - 4



Maximum Attempts Allowed Per Minute = 3

3. Failed Access attempts.

1st Attempt



6th Attempt



Maximum Attempts Allowed at an Unauthorized Zone = 5



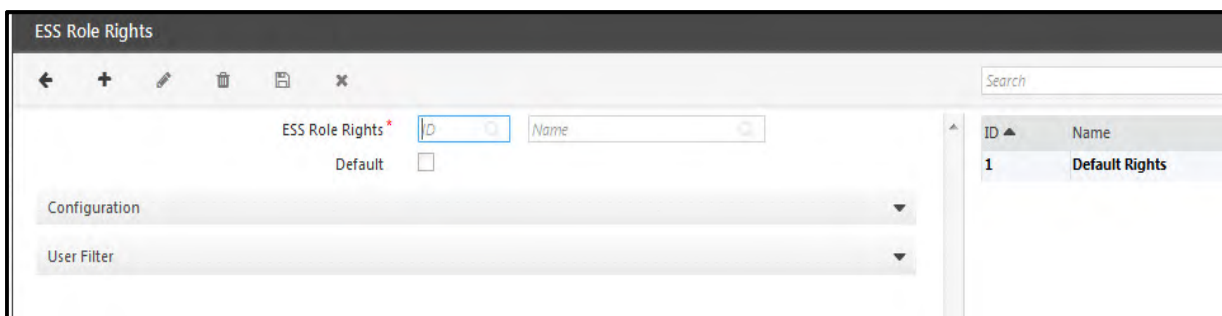
For other conditional violations that may lead to blocking of a user, go to **Device Configuration (Panel200) > Features > Set 1 > Block Users**. Also, [See "Enabling Access Control Features" on page 21.](#)

ESS Role Rights

The ESS Role Rights is used to restrict user(s) access for some options in ESS login. (Like viewing other User's basic details, attendance correction applications etc.). The administrator can create up to 99 role rights configurations, which will specify the pages to be enabled for ESS users and can choose which rights configuration should be applicable to a user.

To configure the rights for ESS pages, select the **Users module > Utilities > ESS Role Rights**.

The **ESS Role Rights** page appears as shown below.



ID	Name
1	Default Rights

Click on **New** button to create the new role rights.

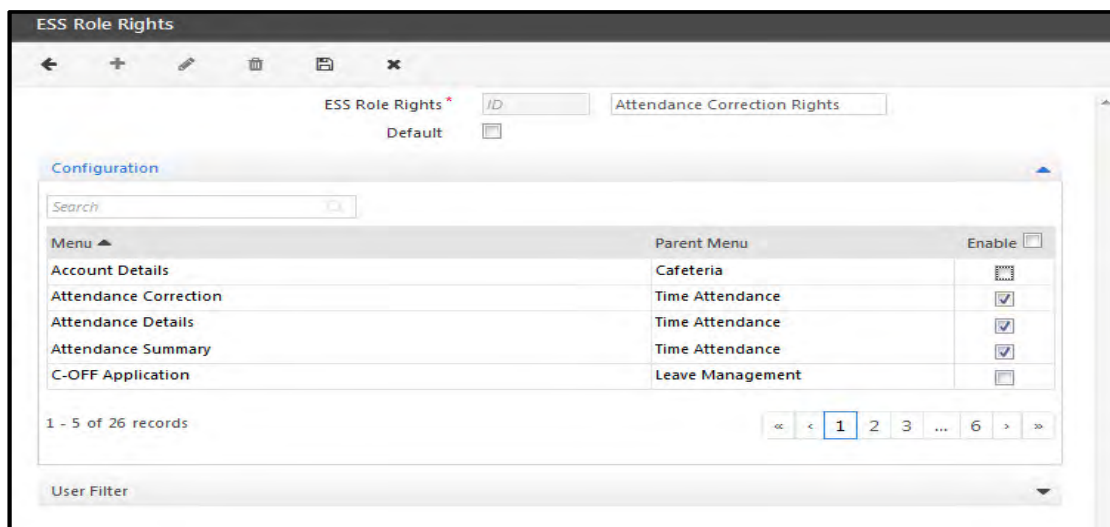
ESS Role Rights: Enter the name of the Rights. For Eg: attendance correction rights can be given to specific users. Cafeteria access rights can be given to some users.

Default: Enable the checkbox to make the particular ESS role rights as default.

Configuration

Enable/Disable the check-box for the options mentioned in the configuration list to assign/deny the role rights to the respective user.

Eg1: For Attendance Correction rights, Attendance Correction, Attendance Details and Attendance Summary are enabled as shown below. The users assigned to Attendance Correction Rights can access these features.



Menu	Parent Menu	Enable
Account Details	Cafeteria	<input type="checkbox"/>
Attendance Correction	Time Attendance	<input checked="" type="checkbox"/>
Attendance Details	Time Attendance	<input checked="" type="checkbox"/>
Attendance Summary	Time Attendance	<input checked="" type="checkbox"/>
C-OFF Application	Leave Management	<input type="checkbox"/>



The User Basic Details page in the collapsible Configuration panel provides the option of **Advanced Rights Configuration** from where you can hide or show the Attendance Status and Last Punch related details of the user from the ESS > Basic > User Basic Details.

Menu	Parent Menu	Enable	Configure
Short Leave/Official In-Out	Time Attendance	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Timesheet Correction Application	Job Costing	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Tour Application	Leave Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Transaction Correction	Cafeteria	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User Basic Details	Basic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Show Attendance Status ☒

Show Last Punch Details ☒

Save

User Filter

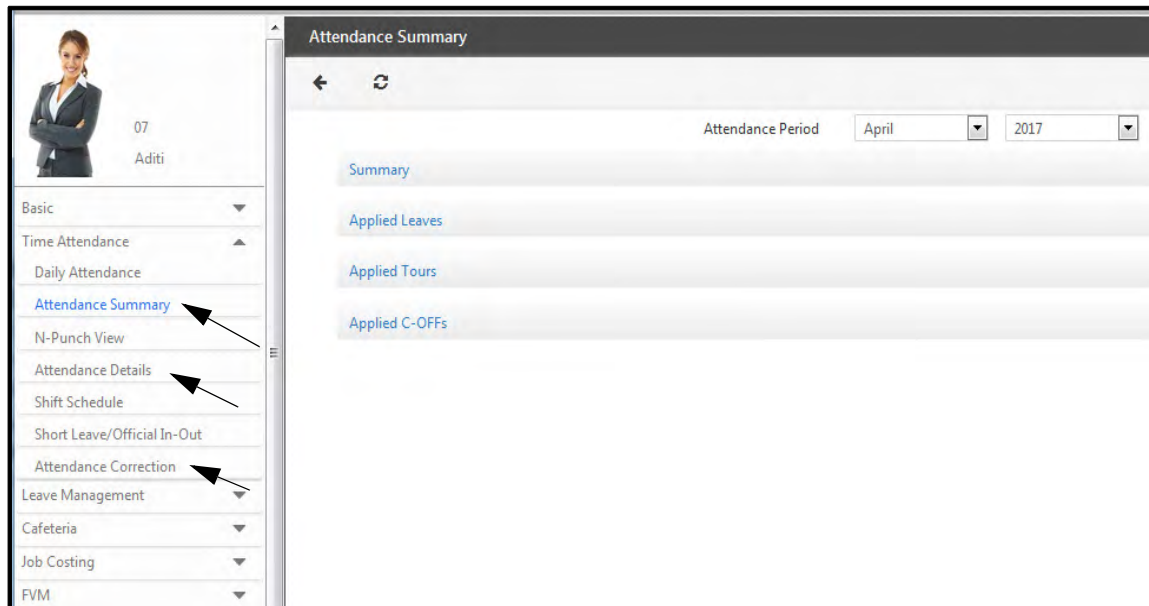
Select the User filter section. Select the users from the pick-list eg. Aditi. The users will be listed in the grid.

ID	Name	
07	Aditi	
1	Shalini	
101	Khushbu	
1567	Sheetal	
1678	Supriya	

Click on **Save** button to add the role rights. The **Rights ID** will be automatically generated.

Menu	Parent Menu	Enable
Account Details	Cafeteria	<input type="checkbox"/>
Attendance Correction	Time Attendance	<input checked="" type="checkbox"/>
Attendance Details	Time Attendance	<input checked="" type="checkbox"/>
Attendance Summary	Time Attendance	<input checked="" type="checkbox"/>
C-OFF Application	Leave Management	<input type="checkbox"/>

Hence the user Aditi when logs into her ESS account will have rights for Attendance Correction, Attendance Details and Attendance Summary as shown below.



In the same way, other role rights can be assigned/denied to the required users from the configuration panel of ESS Role rights tab.

IMEI Authorization

ESS Mobile Apps can be used on mobile devices. To ensure that a user can install and use the app from a single authenticated device, the device IMEI number is stored in the Database. An ESS user can apply for an IMEI number authorization request, and a System Account user can authorize or reject these requests.

You can view all the pending request at one go as well as you can authorize/reject the IMEI request of ESS mobile users.

Select the **Users module > Utilities > IMEI Authorization**.

The **IMEI Authorization** page appears as shown.

You can either:

- view all the pending applications for IMEI Authorization
- set the filters — Date, Filter Users — to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Authorized** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To know more, refer to [“Pending Applications”](#).



The population on this page depends on the server's database. It might take time to load all pending applications.

Applications according to Set Filters

To Set the Filters,

- **Date:** Select this option to enable the date filter. Specify the start and end dates by clicking the respective date selection buttons. This defines the period for which IMEI Applications approval status is to be viewed.
- **Filter Users:** You can filter records according to the desired Enterprise Group, All or for an Individual.

Select **All**, to view authorization status of the applications of all the active users on the system.

Select **Individual**, to view authorization status of the applications of a single user. Click the picklist to select the desired User ID/Name.

Select the desired Enterprise Group — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Group1/2/3 and then click the picklist to select the desired group's ID/Name, to view authorization status of these applications.

Click **View**. The Pending, Authorized and Rejected collapsible panels appear.

Pending Applications

- Click the **Pending** collapsible panel. All the applications in pending state appear.



The screenshot shows a web interface titled "Pending (1)". It contains a search bar and a table with the following data:

Request Date	User ID	Name	IMEI Number	Approve	Reject
01/09/2022	MVR5	MVR5	39de45fd-f9c0-49cb-bb44-f26315635dab	<input type="checkbox"/>	<input type="checkbox"/>

- To approve the application, select the **Approve** check box of the desired entry. This application will then appear under the **Authorized** collapsible panel.
- To reject the application, select the **Reject** check box of the desired entry. This application will then appear under the **Rejected** collapsible panel.

Authorized Applications

Click the **Authorized** collapsible panel. All the authorized applications with their details are displayed.



The screenshot shows a web interface titled "Authorized (4)". It contains a search bar and a table with the following data:

Request Date	User ID	Name	IMEI Number	Authorization Date
31/08/2022	MVR1	MVR1	48abac71-7f63-4b67-b60e-d432c14d5957	31/08/2022
31/08/2022	MVR2	MVR2	a8d5bb0a-e731-4889-a327-24983b1caa88	31/08/2022
31/08/2022	MVR3	MVR3	39de45fd-f9c0-49cb-bb44-f26315635dab	31/08/2022
31/08/2022	MVR4	MVR4	48abac71-7f63-4b67-b60e-d432c14d5957	31/08/2022

Rejected Applications

Click the **Rejected** collapsible panel. All the rejected applications with their details are displayed.



The screenshot shows a web interface titled "Rejected (1)". It contains a search bar and a table with the following data:

Request Date	User ID	Name	IMEI Number	Rejection Date
01/09/2022	MV1	MV1	39de45fd-f9c0-49cb-bb44-f26315635dab	01/09/2022

User Events

This functionality enables the COSEC system administrator to view the attendance events, access events as well as visitor events (if any) for one or more selected users. Details of entry and exit punches, allowed/denied status of access as well as the source details of a punch (*Device, App, ESS* etc.) can be viewed.

To view the User Events, Select the **Users module > Utilities > User Events**.

The **User Events** page appears as shown below.

The screenshot shows the 'User Events' interface. At the top, there are date pickers for 'Date' set to '21/03/2017'. Below this is a 'Filter By' dropdown menu set to 'Individual'. Underneath, there are input fields for 'User' with 'ID' and 'Name' labels. A 'View' button is positioned below the user fields. At the bottom, there are three expandable sections: 'Attendance Events (0)', 'Access Control Events (0)', and 'Visitor Events (0)'.

Specify the **date** range for which events are to be viewed.

Select the **user** based on Filter options of *Individual, Device or Department*.

Click the **View** button to get the specified records. Select the **Attendance Events** section to view the attendance events of employees.

The screenshot shows the 'User Events' interface with the 'Attendance Events (7)' section expanded. It displays a table of attendance events for user '2' (Anmol) on '31/07/2019'. The table has columns for User ID, User Name, Date-Time, I/O, Access, Source, Status, Location, View Image, and Details. The events are as follows:

User ID	User Name	Date-Time	I/O	Access	Source	Status	Location	View Image	Details
2	Anmol	31/07/2019 16:11:50	Entry	Allowed	App	Unauthorized			
2	Anmol	31/07/2019 16:05:08	Entry	Allowed	ESS	Unauthorized			
2	Anmol	31/07/2019 12:52:06	Entry	Allowed	ESS	Authorized			
2	Anmol	31/07/2019 12:49:43	Entry	Denied	Device	NA			
2	Anmol	31/07/2019 12:48:53	Entry	Denied	Device	NA			

Below the table, it indicates '1 - 5 of 7 records' and provides pagination controls. At the bottom, there are sections for 'Access Control Events (0)' and 'Visitor Events (0)'.

The Attendance Events shows the Date and time when the event is generated along with the I/O, Access, Source, Status and Location. It also displays Image and Details of the punch.

The Status of event, i.e. whether it is Authorized or Unauthorized is displayed under Status.

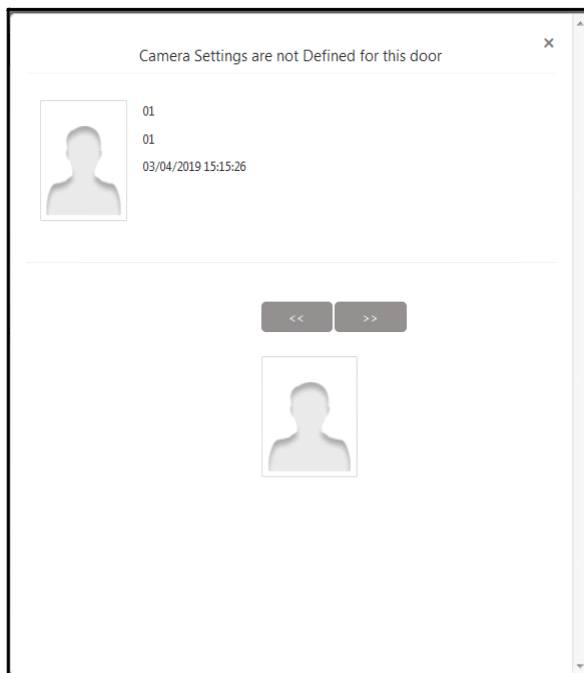
- If the status is Unauthorized, it will display a link which on clicking will be redirected to **Events Authorization** Page as per login user's rights.
- If the status is shown as NA, then Authorized status will be Null and the access will be shown as **Denied**.

Click the  button to view source location details for an entry or exit event.



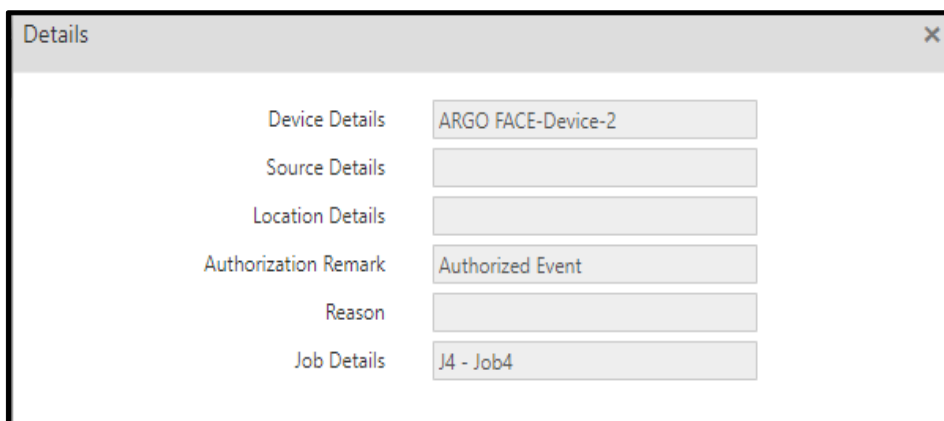
If Map is not loaded; check the network connection of your PC or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

Clicking on View Image icon will display the captured image of user as shown below. If no image is captured, then on clicking icon nothing will be displayed.



If the event is generated by API then there will not be any image popup window on clicking View Image icon.

On clicking  icon, **Details** regarding user event will be displayed.



Assigning Alerts To Users

The **Alert Assignment** function enables the system administrator to assign multiple alerts for a particular active user in the COSEC system. To know more about Alert messages, refer to [“Configuring Alert Messages”](#).

For example, this functionality can be used to enable a user to receive SMS or E-mail alerts whenever the events such as his leave application has been approved, for missing punches, for changes in shifts etc are generated.

To assign alerts to users, Select the **Users module > Utilities > Alert Assignment**.

The **Alert Assignment** page appears as shown below.

The screenshot shows the 'Alert Assignment' window. At the top, there are search fields for ID, Name, and Type, and a 'Reporting In-Charge' field. Below these is a search bar. The main area contains a table with columns: Assigned (checkbox), ID (dropdown), Alert, SMS (checkbox), Email (checkbox), and App Notification (checkbox). The table lists five alerts: Monthly Attendance, Leave Approval, Leave Rejection, User Events, and Leave Application. At the bottom, it shows '1 - 5 of 38 records' and a pagination control with '1' selected. A 'Receive Alerts on' dropdown is at the bottom left.

Assigned	ID	Alert	SMS	Email	App Notification
<input type="checkbox"/>	1	Monthly Attendance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2	Leave Approval	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	Leave Rejection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	User Events	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	Leave Application	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Select a user from the right side grid as shown below for whom the alerts are to be assigned.

The User ID, Name and Type will be displayed in the respective fields.

If the selected user is Reporting Incharge of any group, then it will show Yes otherwise No.

The screenshot shows the 'Alert Assignment' window with a user selected. The ID field is '001', Name is 'KAJAL', Type is 'T&A', and Reporting In-Charge is 'No'. The table below shows six alerts, all of which are assigned (checkbox checked). The alerts are: Monthly Attendance, Leave Approval, Leave Rejection, User Events, and Missing In Punch - Users. At the bottom, it shows '1 - 5 of 25 records' and a pagination control with '1' selected.

Assigned	ID	Alert	SMS	Email	App Notification
<input checked="" type="checkbox"/>	1	Monthly Attendance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	2	Leave Approval	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	3	Leave Rejection	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	4	User Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	6	Missing In Punch - Users	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Now check the box for the events for which the alert is to be sent to the user. Enable the **SMS**, **Email** and/or **App Notification** checkbox by which the alert will be sent to the user.



The ESS rights must be allocated to the user to access the COSEC APTA mobile application and receive the alert.

- For example, the User KAJAL will get the SMS, Email alerts on Monthly Attendance, User Events and Leave Application events. Also she will get Push Notifications on COSEC APTA Application on her smartphone for Approval/Rejection of the applied leave as selected above.

Select the **Receive Alerts on** section and select the appropriate checkboxes to define which contact numbers or E-mail addresses for the selected users should be considered for sending the alerts.

Assigned <input checked="" type="checkbox"/>	ID ▲	Alert	SMS <input type="checkbox"/>	Email <input type="checkbox"/>	App Notification <input type="checkbox"/>
<input checked="" type="checkbox"/>	1	Monthly Attendance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	2	Leave Approval	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	3	Leave Rejection	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	4	User Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	6	Missing In Punch - Users	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

1 - 5 of 25 records

« < 1 2 3 4 5 > »

[Receive Alerts on](#)

Personal Cell ☒

Personal Email ☒

Official Cell ☒

Official Email ☒

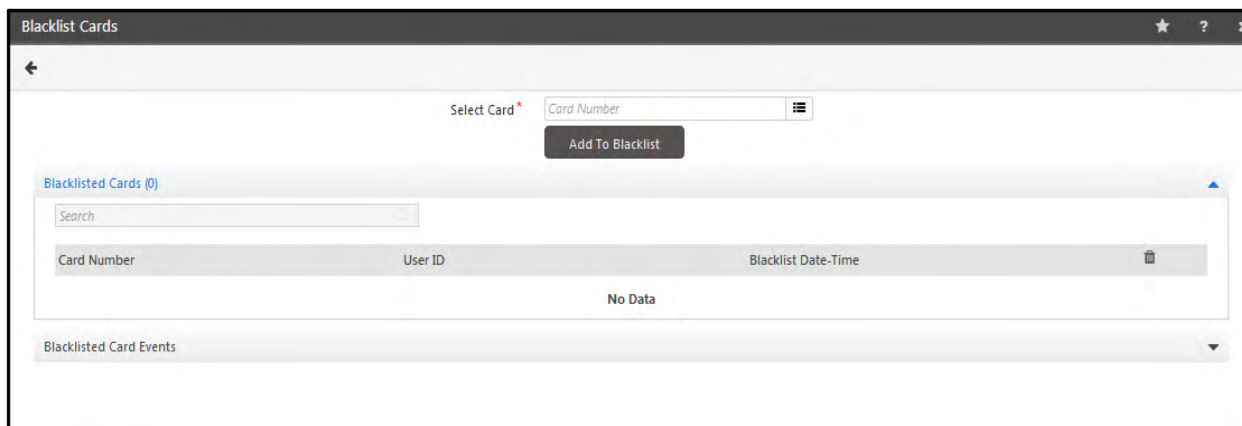
Click **Save** button to assign the alerts successfully to this user.

Blacklist Cards

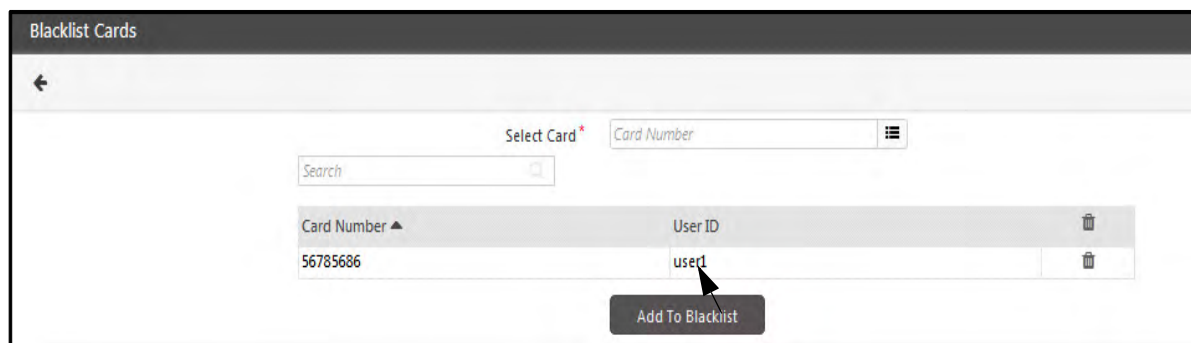
In COSEC, various credentials such as finger print templates, palm templates as well as access cards can be associated with a user. Each user can be assigned two access cards. In case a user's access card is stolen or lost, the blacklisting feature enables the administrator to add this card to a Watchlist and track its usage.

To blacklist a card, Select the **Users module > Utilities > Blacklist Cards**.

The page will open as shown below.



Select one or more cards using the card picklist to blacklist.



Click the **Add to Blacklist** button.

If you enter a Comma separated CSN, then the system will first encode (convert) the value of this CSN and then add it to the blacklist. To know more about the Comma separated CSN, refer Access Card 1 under [“Credentials”](#) in Users> User Configuration> Credential.

The blacklisted cards will appear in the **Blacklisted Cards** panel as shown.

Blacklist Cards

←

Select Card *

Card Number

⋮

Add To Blacklist

Blacklisted Cards (1)

Search

Card Number ▲	User ID	Blacklist Date-Time	
56785686	user1	2017/09/03 12:31:47	<div></div> <div></div>

Blacklisted Card Events

Once blacklisted, access cards can be tracked based on card events. To view card events for a selected period, click the **Blacklisted Card Events** section.

Event date: Select the From and To date to view the events of cards.

If some user is trying to access the device using blacklisted card, then the event will be displayed in blacklisted card events.

Click the **View** button to view the blacklisted card events for the selected date range as shown below.

Blacklisted Card Events

Event Date

2017/03/09

2017/03/09

View

Search

Card Number ▲	User ID	Blacklist Date Time	Event Date Time	Device Name
590570823	user1	2017/03/09 14:27:27	2017/03/09 14:29:25	WIRELESS DOOR DEVICE 8 SWETAAA
590570823	user1	2017/03/09 14:27:27	2017/03/09 14:29:26	WIRELESS DOOR DEVICE 8 SWETAAA
590570823	user1	2017/03/09 14:27:27	2017/03/09 14:29:29	WIRELESS DOOR DEVICE 8 SWETAAA
590570823	user1	2017/03/09 14:27:27	2017/03/09 14:29:30	WIRELESS DOOR DEVICE 8 SWETAAA

Blacklisting Users

This page allows blacklisting users, thereby limiting their rights, access, etc., until the user is restored. You can also restore a blacklisted user from the same page. Along with this, you can also view the list of users who have been blacklisted/ restored.

To blacklist a user, Select **Users module > Utilities> Blacklist Users**

The screenshot shows the 'Blacklist Users' interface. At the top, there's a 'Select Users' dropdown set to 'User Wise'. Below it, there are input fields for 'User *' (with sub-fields for 'ID' and 'Name') and 'Reason' (with a '50 Char' limit). An 'Add To Blacklist' button is present. Below the form, there's a section for 'Blacklisted Users (0)' with a search bar and a table. The table has columns: 'User ID', 'Name', 'Blacklist Date-Time', 'Reason For Blacklisting', and 'Restore'. It currently shows 'No Data'. At the bottom, there's a section for 'Restored Users (1)'.

User: You can select the user by filtering the user as **User Wise**, **Group Wise** or **All**. According to the filter selected You can

- select the user randomly from the picklist,
- select the enterprise group and select particular groups or

Reason: You can specify the reason behind blacklisting a user.

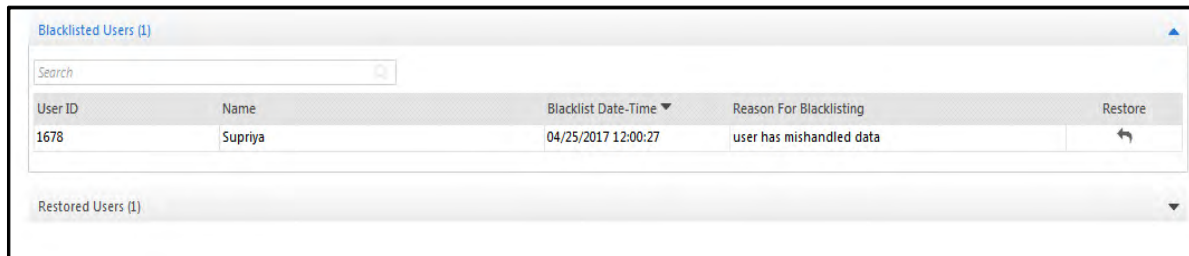
The screenshot shows the 'Blacklist Users' interface with a user selected. The 'Select Users' dropdown is still 'User Wise'. The 'User *' field now shows '1678' in the 'ID' sub-field and 'Supriya' in the 'Name' sub-field. The 'Reason' field is filled with 'user has mishandled data'. The 'Add To Blacklist' button is still visible. The 'Blacklisted Users' table is still empty.

Then click on **Add to Blacklist** button. A warning appears.

The screenshot shows a 'Warning' dialog box with the text: 'Would you like to revoke devices (as per device-wise rights)?'. There are two buttons: 'Yes' and 'No'.

If you select **Yes**, then user will become inactive and user's data will be removed from the devices.
If you select **No**, then user will become inactive but user data will still be there on assigned devices.

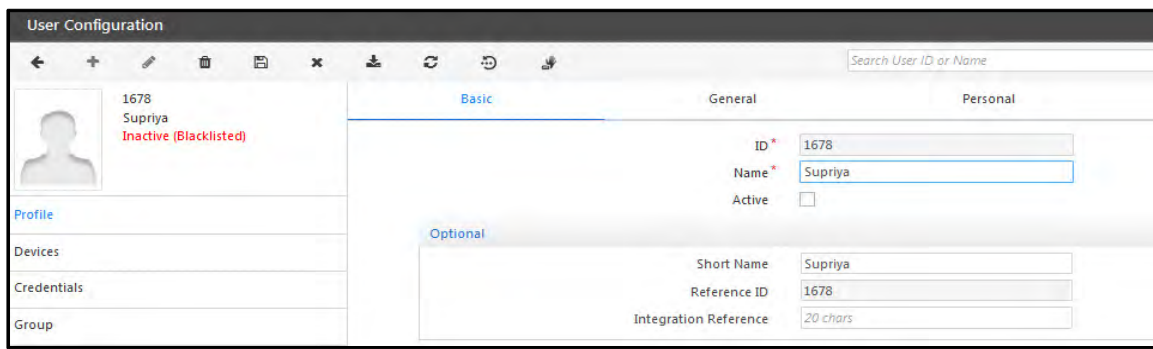
The user will get listed in Blacklisted Users section as shown below.



User ID	Name	Blacklist Date-Time	Reason For Blacklisting	Restore
1678	Supriya	04/25/2017 12:00:27	user has mishandled data	

Restored Users (1)

The blacklisted user will be made inactive in the system. The user profile displays the user being Inactive and blacklisted as shown below.



User Configuration

1678
Supriya
Inactive (Blacklisted)

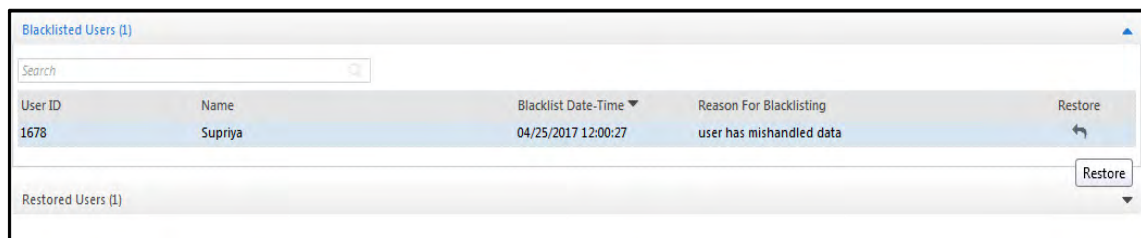
Basic | General | Personal

ID * 1678
Name * Supriya
Active ☐

Optional

Short Name Supriya
Reference ID 1678
Integration Reference 20 chars

To restore the blacklisted user, click on **Restore** button to remove the user from the blacklist. The user will be restored to the normal state and shown in the Restored section.



User ID	Name	Blacklist Date-Time	Reason For Blacklisting	Restore
1678	Supriya	04/25/2017 12:00:27	user has mishandled data	

Restored Users (1)

Restore



User ID	Name	Restore Date-Time	Reason For Blacklisting
1678	Supriya	04/25/2017 12:32:51	user has mishandled data
AP	Aakash	03/29/2017 11:55:25	Caught stealing company property



The restored user remains inactive. You have to enable the checkbox to make him active user.

Changing User ID

Certain firms have the practice of assigning temporary User IDs to new employees for a certain period of time before they can be given a permanent ID. COSEC provides the option for HR administrators to assign a temporary User ID to new users. These users can later be migrated to a new COSEC User ID for permanent use. The *Change User ID feature* ensures that none of the existing user data is erased on assigning a new ID.

To change User ID for a user, select the **Users module > Utilities > Change User ID**.

The page will open as shown below.

Change User ID

←

Authorize Process

Username *

Password *

Select User

User *

New User ID *

Process

Enter the administrator's login credentials to authorize the process.

Select the **user** for whom User ID is to be changed

Enter the **new User ID** to replace the existing User ID.

Click the **Process** button to change User ID.

Change User ID

←

Authorize Process

Username *

Password *

Select User

User *

New User ID *

Process

Health

This functionality enables the user to declare his/her health status and on the basis of that, it will be helpful for the firm as well as for user to keep track of their employee's/one's health on the daily basis.

To access this functionality, Select **Users module> Utilities> Health**

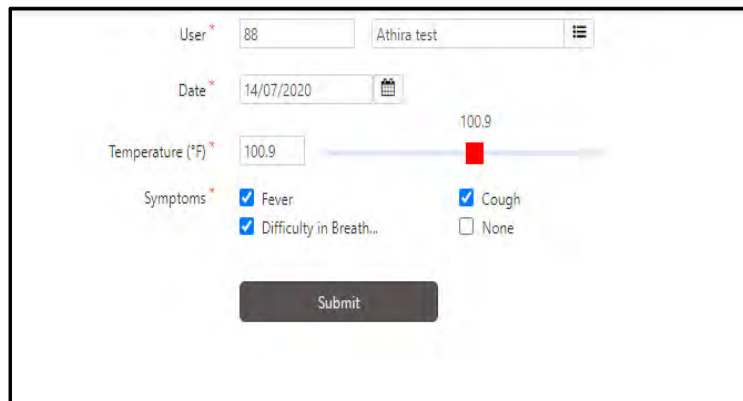
This page consists of 2 important parameters. They are:

- "Health Declaration"
- "Health Record"

Health Declaration

User can enter his/her Temperature in a unit predefined by Admin as well as different Symptoms options provided by Admin.

Below shown image is the Health declaration page appeared on User's screen.



The screenshot shows a web form for health declaration. At the top, there are two input fields: 'User' with the value '88' and a dropdown menu showing 'Athira test'. Below these is a 'Date' field with the value '14/07/2020' and a calendar icon. The 'Temperature (°F)' field has a value of '100.9' and a slider control. The 'Symptoms' section has three checkboxes: 'Fever' (checked), 'Cough' (checked), and 'Difficulty in Breathing...' (checked). There is also a 'None' option. A 'Submit' button is located at the bottom of the form.

Select the **User** and particular **Date** for which the health parameters are to be declared.

Enter the **Temperature** and select the **Symptoms** which belongs to the user.

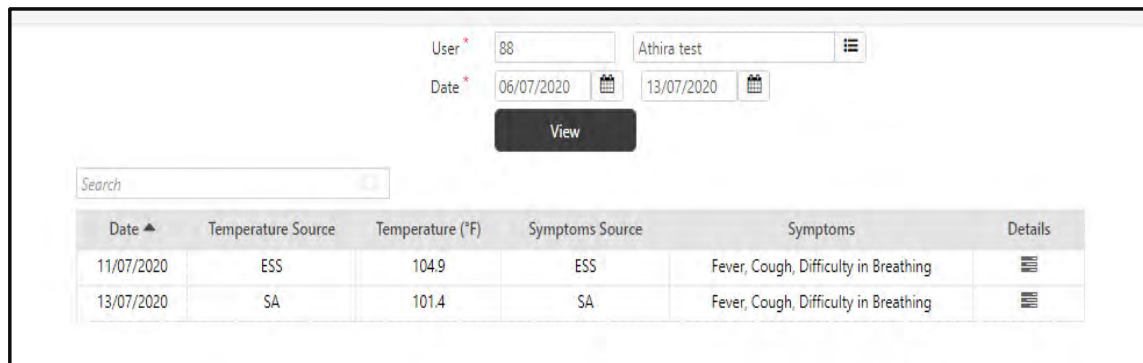


The symptoms displayed for selection, will be as configured by the Admin in Admin > Global Policy > User.

Once the configuration is done, click on the **Submit** button to Save the details. You can check the records in Health Records as described below.

Health Record

It shows all the health records of a user of each day for which the date range has to be mentioned. Report includes date, source of entering the data (SA or ESS), temperature and symptoms.



The screenshot displays a web interface for viewing health records. At the top, there are filter fields: 'User' with the value '88', 'Athira test' with a menu icon, 'Date' with a range from '06/07/2020' to '13/07/2020' and calendar icons, and a 'View' button. Below the filters is a search bar labeled 'Search'. The main content is a table with the following data:

Date ▲	Temperature Source	Temperature (°F)	Symptoms Source	Symptoms	Details
11/07/2020	ESS	104.9	ESS	Fever, Cough, Difficulty in Breathing	⋮
13/07/2020	SA	101.4	SA	Fever, Cough, Difficulty in Breathing	⋮



If the health declaration is entered more than once on same day, then the system will consider only the last declared health parameters which will reflect on the health record.

Health Declaration and Health Record will only be configurable by the user if the Admin has assigned role and rights for the same.

Get Location Details



To access this page, make sure you enable **Get Location Details** checkbox from *Admin > System Configuration > Global Policy > Basic Policy*.

Admin is unable to understand the exact location of his users/ workers with the help of GPS latitude and longitude coordinates. S/He needs to enter these coordinates on Maps to search the location details manually which is quite time consuming and even tedious to check location details for multiple events.

To overcome this issue, COSEC is providing **Get Location Details** page.

In this page, the system performs **Reverse Geo Coding** process using Google Maps (Internet required).

Reverse Geo Coding: It is process of converting a latitude and longitude coordinates into corresponding street address or human readable address.

To perform this process, following things are required:

- Longitude and Latitude Coordinates
- Google API Key

Longitude and Latitude Coordinates:

There are 2 types of Longitude and Latitude Coordinates — GPS Latitude-Longitude and GSM Latitude-Longitude.

- For events having GPS latitude-longitude, GPS latitude-longitude will be consider for processing.
- For events having GSM latitude-longitude, GSM latitude-longitude will be consider for processing.
- For events having both GPS and GSM latitude-longitude, GPS latitude-longitude will be consider for processing.
- For events having GPS latitude or GPS longitude and GSM latitude-longitude, GPS latitude/longitude will be consider for processing.

Google API Key

Enable the **Get Location Details** checkbox from *Admin > System Configuration > Global Policy > Basic Policy*.

Then enter the **Google API Key**.

This page then displays the converted location to the Admin.

To access this functionality, select *Users > Utilities > Get Location Details* and the following page appears:

Configure the following parameters:

- **Date:** Select a desired date range to define the period for which location details are to be processed.



To avoid long processing time, it is recommended to select the date range as per the events available with your system.

- **Process:** Select a desired option — Pending Events or All Events.

Pending Events: Select this option to consider the pending events available with the system which do not have the location address against the coordinates during get location process.

All Events: Select this option to consider all the events available with the system during get location process. When you run the get location process for all events, the events which are already processed, will also be reprocessed.

User Selection

- **Select Users:** Select a desired option — User-wise, Group-wise or All for whom the location is to be processed.

If you select the User-wise, select the desired User from the picklist.

If you select the Group-wise, select the desired Group from the picklist.

Click **Process** to start processing location details for selected users.

Once processed, the details will be displayed in the **Result** table.

The **Result** table displays details like — User ID & Name, Event Date & Time, Coordinates, Location, Status (Success or Failure) and Status Description.

Result Table:

Get Location Details

Process Completed

Date

19/04/2021

19/05/2021

Process

☐ Pending Events

☒ All Events

User Selection

Select Users

User Wise

User

ID

Name

Search

User ID	Name	
1	Richa	
2807	Santosh Ramani	

Process

Result

Search

User	Event Date & Time	Coordinates	Location	Status	Status Description
2807-Santosh Ramani	18/05/2021 18:02	+22.2562 , +73.1834	Eva Mall Rd Ghanshyam Nagar Society	Success	
2807-Santosh Ramani	18/05/2021 18:15	+22.2562 , +73.1834		Failure	Server not reachable
2807-Santosh Ramani	18/05/2021 18:25	+22.2562 , +73.1834		Failure	Server not reachable

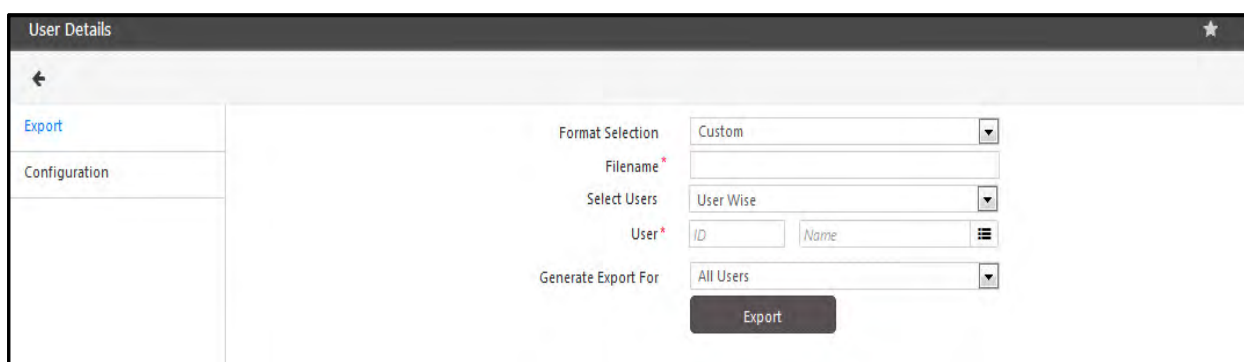
User Details Export

This functionality enables the administrator to export user profile data such as the user's personal information, contact information, official information etc. in the Excel format. The administrator can either use a system-defined format or customize the export format by selecting the required user fields.

To access this functionality, Select the **Users module > Exports > User Details**

Export

The **User Details** page opens as follows:

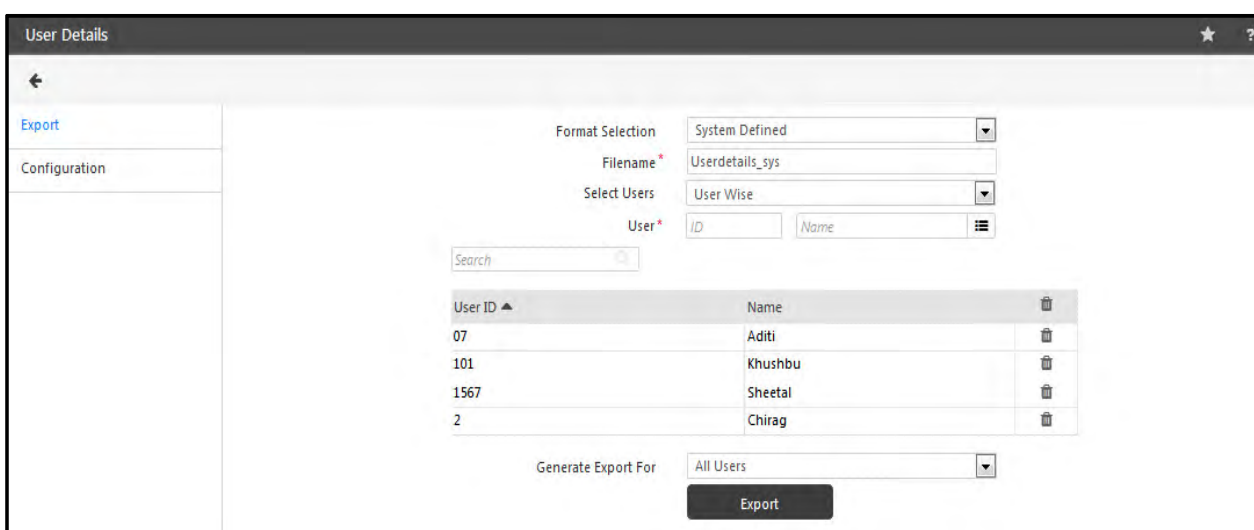


The screenshot shows the 'User Details' export interface. On the left, there is a sidebar with 'Export' and 'Configuration' tabs. The main area contains the following fields:

- Format Selection:** A dropdown menu set to 'Custom'.
- Filename:** A text input field with a red asterisk, currently empty.
- Select Users:** A dropdown menu set to 'User Wise'.
- User:** Two input fields labeled 'ID' and 'Name', each with a red asterisk. The 'Name' field has a list icon to its right.
- Generate Export For:** A dropdown menu set to 'All Users'.
- Export:** A dark button at the bottom right.

Format Selection: In the Export tab, Select the format as **Custom** or **System Defined**. To configure the custom export template, See ["Configuration" on page 544](#).

System Defined Format



The screenshot shows the 'User Details' export interface with the 'System Defined' format selected. The fields are populated as follows:

- Format Selection:** A dropdown menu set to 'System Defined'.
- Filename:** A text input field with a red asterisk, containing the value 'Userdetails_sys'.
- Select Users:** A dropdown menu set to 'User Wise'.
- User:** Two input fields labeled 'ID' and 'Name', each with a red asterisk. The 'Name' field has a list icon to its right.
- Generate Export For:** A dropdown menu set to 'All Users'.
- Export:** A dark button at the bottom right.

Below the 'User' fields, there is a search bar and a table of users:

User ID ▲	Name	
07	Aditi	🗑️
101	Khushbu	🗑️
1567	Sheetal	🗑️
2	Chirag	🗑️

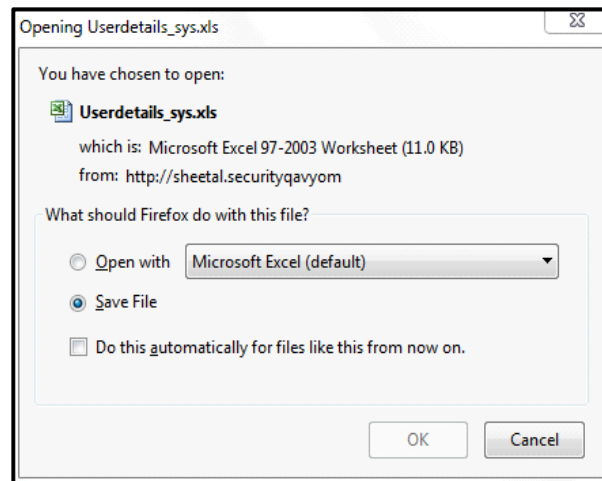
Filename: Enter an appropriate Filename for the export file as shown.

Select Users: Select the user based on following filters:

- **User Wise**- To select users randomly using the user picklist.
- **Group Wise** - To select all users associated with a particular enterprise group using the Group Wise dropdown list.
- **ALL** - To select all users in the system.

Generate Export for: You can Generate Export For All Users, Active Users or Inactive users.

Click the **Export** button. You can open or save the exported file at a desired location.



The **System defined** exported file for the selected users is shown below. It displays all the details like User ID, User Name, ReferenceID, ShortName, BloodGroup etc.

Userdetails_sys [Compatibility Mode] - Microsoft Excel														
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	UserID	UserName	ReferenceID	ShortName	Gender	BloodGroup	BirthDate	JoiningDate	LeavingDate	LocAddress1	LocAddress2	LocStreet	LocCity	LocCountry
1	07	Aditi	7	Aditi	Female	AB+	02/09/1993	12/07/2016						
2	101	Khushbu	101	Khushbu	Female	B+	11/16/1993			D-91, Nandanvan Soc.	Vadsar	GIDC-Makarpara	Vadodar	India
3	1567	Sheetal	1567	Sheetal	Female	A+	11/27/1987	06/17/2013						
4	2	Chirag	2	Chirag	Male	A+	05/09/1990	04/01/2016						

Custom Format

User Details

←

Export

Configuration

Format Selection: Custom

Filename*: Userdetails_custom

Select Users: User Wise

User*: ID Name

Search

User ID	Name
07	Aditi
101	Khushbu
1567	Sheetal
2	Chirag

Generate Export For: All Users

Export

The configuration of custom export template is done in Configuration section. See [“Configuration” on page 544](#).

Once the configuration is done, configure the fields in Export section and click on **Export** button.

The custom export file is shown as below. Here the fields will be displayed as per the selection in Configuration section.

	A	B	C	D	E	F	G	H	I	J	K	L	M
	User ID	User Name	Birth Date	Joining	Gender	Marital Status	Personal	Personal Mobile	Personal Email	Official Mobile	Official Email		
1	07	Aditi	02/09/1993	12/07/2016	Female		8722212444	8612352302					
2	101	Khushbu	11/16/1993		Female	Married		9686423523		9787624826	khushbu.g@matrixrd.org		
3	1567	Sheetal	05/12/1987	06/11/2013	Female	Married	9878675678	9682634526	sheetal.raval@gmail.com	8699925301	sheetal.raval@matrixrd.org		
4	2	Chirag	05/09/1990	04/01/2016	Male	UnMarried	9872433367						
5													
6													

Configuration

The User Details Export can be customized to determine which data appears in the exported file (applicable only for the **Custom** Format Selection).

To do this, On the **User Details** page, select the **Configuration** tab as shown.

The screenshot shows the 'User Details' configuration page. On the left, there is a sidebar with 'Export' and 'Configuration' tabs, with 'Configuration' selected. The main area is titled 'Personal Info' and contains a 'Select Fields To Export' section. This section has a search bar and a table of fields with checkboxes. The fields listed are: Fields, User ID, User Name, Reference ID, Birth Date, and Joining Date. The checkboxes for User ID, User Name, Birth Date, and Joining Date are checked. A black arrow points to the checkbox for 'Joining Date'. Below the table, it says '1 - 5 of 21 records' and there is a pagination control with numbers 1 through 5, where 1 is highlighted. At the bottom of the page, there are sections for 'Contact Info' and 'Official Info', and a 'Save' button.

This screenshot shows the same 'User Details' configuration page, but with a different set of fields selected in the 'Personal Info' section. The 'Select Fields To Export' section now shows: Fields, Father/Spouse Name, Driving License Expiry, and Passport Expiry. The checkboxes for Driving License Expiry and Passport Expiry are checked. Below the table, it says '21 - 23 of 23 records' and the pagination control shows numbers 1 through 5, with 5 highlighted. The 'Contact Info' and 'Official Info' sections and the 'Save' button are also visible.

Select the sections **Personal Info**, **Contact Info** and **Official Info** and select the required fields to include them in the new custom export template.

Personal Info

Contact Info

Select Fields To Export

Search

Fields

Fields	
Personal Phone	<input checked="" type="checkbox"/>
Personal Mobile	<input checked="" type="checkbox"/>
Personal Email	<input checked="" type="checkbox"/>
Local Address	<input type="checkbox"/>
Local Street	<input type="checkbox"/>

1 - 5 of 15 records

« < 1 2 3 > »

Official Info

Save

Personal Info

Contact Info

Official Info

Select Fields To Export

Search

Fields

Fields	
Official Phone	<input type="checkbox"/>
Official Extn	<input type="checkbox"/>
Official Mobile	<input checked="" type="checkbox"/>
Official Email	<input checked="" type="checkbox"/>
Organization	<input type="checkbox"/>

1 - 5 of 14 records

« < 1 2 3 > »

Save

Click **Save** button to save the configuration. Now go to Export section to export the user details in excel file.

User Reports

User Reports can be accessed and generated via the **Reports** section under the COSEC Users module. This section is classified into the following categories of reports:

- “Device-wise Reports”
- “User Info”
- “Others”
- “User Events”

Device-wise Reports

- **Panel Wise** - Generates a Panel wise list of the users along with the panel doors on which users are assigned in the system as shown below.

Panel-Wise Users

User Selection

Select Users: Group Wise

Select Group: Panel

Panel * ID: Name:

Search

ID	Name	Group
4	Panel Lite V2-Device-4	Panel

Generate Report For: All Users

Generate Report

Panel-Wise Users

Back

Find... 1 of 1 100%

Main Report

Organization-1
Panel-Wise Users

Run by: System Admin Date: 07/03/2018 18:00

User ID	Name	Index	VIP	Access	Route	Home Zone	Access Group	Visit Zone	Functional Group
Panel Lite V2-Device-4-Panel Lite V2 Door									
1	Chirag	1	No			Zone-1	Group-1		Staff
101	Khushbu	2	No			Zone-1	Group-1		Staff
1687	Aditi Gupta	3	No			Zone-1	Group-1		Staff
2	Priyank	4	No			Zone-1	Group-1		Staff
FVM1	Jinu	5	No			Zone-1	Group-1		Staff
JPC1	Trisha	6	No			Zone-1	Group-1		Staff
JPC2	Priya Mistry	7	No			Zone-1	Group-1		Staff
PVR as Panel door-Panel Lite V2 Door									
1	Chirag	1	No			Zone-1	Group-1		Staff
101	Khushbu	2	No			Zone-1	Group-1		Staff
1687	Aditi Gupta	3	No			Zone-1	Group-1		Staff
2	Priyank	4	No			Zone-1	Group-1		Staff
FVM1	Jinu	5	No			Zone-1	Group-1		Staff
JPC1	Trisha	6	No			Zone-1	Group-1		Staff
JPC2	Priya Mistry	7	No			Zone-1	Group-1		Staff
Door V3 as Panel Door-Panel Lite V2 Door									
1	Chirag	1	No			Zone-1	Group-1		Staff
101	Khushbu	2	No			Zone-1	Group-1		Staff
1687	Aditi Gupta	3	No			Zone-1	Group-1		Staff
2	Priyank	4	No			Zone-1	Group-1		Staff
FVM1	Jinu	5	No			Zone-1	Group-1		Staff
JPC1	Trisha	6	No			Zone-1	Group-1		Staff
JPC2	Priya Mistry	7	No			Zone-1	Group-1		Staff

- **Door Wise** - Generates a Door wise list of users assigned to the Direct Doors along with their details as shown.

Door-Wise Users

Back

Find...

1 of 1

100%

Main Report

Organization-1

Door-Wise Users

Page 1 of 1

Run by: System Admin

Date: 06/04/2018

20:57

Sr No	User ID	Name	Status	Department	Designation
ARC as Direct Door					
1	1	Chirag	Active	Department-1	Designation-1
2	101	Khushbu	Active	Department-1	Designation-1
3	1687	Aditi Ajay	Active	Department-1	Designation-1
Gupta_Ahmedabad					
Door FMX					
1	1	Chirag	Active	Department-1	Designation-1
2	101	Khushbu	Active	Department-1	Designation-1
3	1687	Aditi Ajay	Active	Department-1	Designation-1
Gupta_Ahmedabad					
Door V3					
1	1	Chirag	Active	Department-1	Designation-1
2	101	Khushbu	Inactive	Department-1	Designation-1
3	1687	Aditi Ajay	Active	Department-1	Designation-1
Gupta_Ahmedabad					
NGT Direct Door-Device-2					
1	1	Chirag	Active	Department-1	Designation-1
2	101	Khushbu	Active	Department-1	Designation-1
3	1687	Aditi Ajay	Active	Department-1	Designation-1
Gupta_Ahmedabad					
4	3	Sheetal Pradip	Active	Department-1	Designation-1
Pandya_Ahm					
5	JPC1	Darshna	Active	Department-1	Designation-1

- **User Wise Controllers** - Generates a user-wise list of assigned door controllers. It also shows the Active/Inactive status of user for the particular door which is configured from User Configuration > Devices> Configure.

User-Wise Controllers				
Back				
Find... 1 of 1 100%				
Main Report				
Organization-1				
User-Wise Controllers				
Run by: System Admin			Date: 06/04/2018 20:55	
Sr No	Panel/Door Name	Index	Status	
1 - Chirag				
1	NGT Direct Door-Device-2	1	Active	
2	Panel Lite V2	2	Active	
3	Wireless Door	2	Active	
4	Door V3	2	Active	
5	Door FMX	2	Active	
6	FVR Door-Device-7	2	Active	
7	ARC as Direct Door	2	Active	
8	Path as direct door	2	Active	
9	Vega as Direct Door	2	Active	
101 - Khushbu				
1	NGT Direct Door-Device-2	2	Active	
2	Panel Lite V2	3	Active	
3	Wireless Door	3	Active	
4	Door V3	3	Inactive	
5	Door FMX	3	Active	
6	FVR Door-Device-7	3	Active	
7	ARC as Direct Door	3	Active	
8	Path as direct door	3	Active	
9	Vega as Direct Door	3	Active	

- **Blocked Users** - Generates a list of blocked users on specified devices. For eg: If the Absentee rule for user is configured for 15 days on PVR door and if the user remains absent for 15 days; then on changing the date to 16th day; he will be listed in Blocked Users list. When user punches on 16th day or after that on PVR door he will be denied the Access with Blocked user event.

Blocked Users						
Back						
Find... 1 of 1 100%						
Main Report						
Organization-1				Page 1 of 1		
Blocked User				Date: 06/04/2018 20:20		
Run by: System Admin						
Sr No	User ID	Name	Blocked Date	Reason	Panel/Door	
1	1	Chirag	13/04/2018 00:00:00	Absentee Rule	PVR Door-Device-7	
2	5	Priyank	10/04/2018 00:00:00	Absentee Rule	PVR Door-Device-7	

- **Device Assignment Information** - This report shows the information related to device assignment to user, Revoke, Device Deleted and Device Reuse for the selected dates.

Device Assignment Information

Date *

01/02/2018

06/02/2018

Optional Parameters

Group By

Organization

Action

☒ Assign
☒ Revoke
☒ Device Delete
☒ Device Reuse

User Selection

Select Users

All

Generate Report For

All Users

Generate Report

- The information for Action= Assign is shown when device is assigned to a user.
- The information for Action= Revoke is shown when device assignment for the user is removed.
- The information for Action= Device Delete is shown when device is deleted from the Device Configuration.
- The information for Action= Device Reuse is shown when the previously deleted device is added again manually in Device Configuration on the same Device ID. Eg: Device ID-1 PVR HO Door is previously assigned and then deleted. Then same door is added with another name PVR RnD Door on Door ID-1 which is shown in the report as Reuse.

Note: As the Device ID is same; the previous name of door will be replaced by the new name.

The Source can be Web application, API, Alert Service or Monitor Service which shows the source from where the Action was taken.

Device Assignment Information										
Back										
Find... 1 of 1 100%										
Main Report										
Organization-1										
Organization-Wise Device Assignment Information Report From 07/01/2018 To 06/02/2018										
Run by: System Admin										
User ID	User Name	Device ID	Device Name	Device Type	Action	Date	Source	System User ID	System User Name	Date: 06/02/2018 18:25
Organization-1										
1	Chirag	1	FVR RnD Door	FVR Door	Revoke	06/02/2018 15:20:23	Web	SA	System Admin	
1	Chirag	1	FVR RnD Door	FVR Door	Assign	05/02/2018 16:27:13	Web	SA	System Admin	
101	Khushbu	1	FVR RnD Door	FVR Door	Assign	05/02/2018 16:27:13	Web	SA	System Admin	
101	Khushbu	4	Door-Device-4	NGT Direct Door	Assign	06/02/2018 16:21:26	Monitor Service			
2	Priyank	1	FVR RnD Door	FVR Door	Revoke	06/02/2018 18:24:39	Alert Service			
2	Priyank	1	FVR RnD Door	FVR Door	Assign	06/02/2018 18:05:51	Web	SA	System Admin	
2	Priyank	4	Door-Device-4	NGT Direct Door	Revoke	06/02/2018 18:24:39	Alert Service			
2	Priyank	4	Door-Device-4	NGT Direct Door	Assign	06/02/2018 18:05:51	Web	SA	System Admin	
		1	FVR RnD Door	FVR Door	Reuse	06/02/2018 15:31:02	Web	SA	System Admin	
		1	FVR RnD Door	FVR Door	Delete	06/02/2018 15:24:09	Web	SA	System Admin	
		2	FVR Door-Device-2	FVR Door	Delete	06/02/2018 15:26:15	Web	SA	System Admin	
		3	FVR Door-Device-2	FVR Door	Delete	06/02/2018 15:28:25	Web	SA	System Admin	

Monitor Service in Source

When a user is assigned a Device group. Eg: Khushbu is assigned device group DG1. And In Global policy Auto add new devices is enabled. Also Auto assign new device to device group is enabled and DG1 is selected. So when new device is added source will appear as Monitor Service.

Alert Service in Source

When a user is relieved through a scheduler task "Relieving User Schedule" (Admin> System Utilities> Task Scheduler) then the revoking of device is done and source is shown as Alert Service.

The device assignment (Assign/Revoke) to the visitors can be done from VMS Utility and will be reflected in the report as shown below.

Device Assignment Information										
Back										
Find... 1 of 1 100%										
Main Report										
Organization-1										
Organization-Wise Device Assignment Information Report From 16/10/2018 To 15/11/2018										
Run by: System Admin										
User ID	User Name	Device ID	Device Name	Device Type	Action	Date	Source	System User ID	System User Name	Date: 15/11/2018 12:06
Organization-1										
V1	Visitor1	1	Panel Lite V2-Device-1	Panel Lite V2	Assign	15/11/2018 11:53:47	Web	SA	System Admin	
V1	Visitor1	1	Door V3-Device-1	Door V3	Assign	15/11/2018 11:53:47	Web	SA	System Admin	
V1	Visitor1	2	MODE1	MODE	Assign	15/11/2018 11:54:11	VMS Utility	SA	System Admin	

User Info

- **Access Profile** - Generates a list of the access related information of selected users as shown.

Access Profile

Back

Find... 1 of 1 100%

Main Report

Organization-1 Page 1 of 1

Run by: System Admin Organization-Wise User Access Profile Date: 28/06/2021 10:54

Sr No	User ID	Name	Card	Enrolled Fingers	Enrolled Palm	Enrolled Faces	PIN Finger	Bypass Palm	Shift Check	Shift Schedule	Start Shift	Holiday Schedule	Access Valid Till
1	111	RIC-1		0	0	0	No	No	No	1	GS	1	
2	R11	R11111		0	0	0	No	No	No	1	GS	1	
3	R12	R11112		0	0	0	No	No	No	1	GS	1	
4	U1	User1	346436 346,46 346346 346	0	0	8	No	No	No	1	GS	1	01/01/2022
5	U2	User2		0	0	0	No	No	No	1	GS	1	01/01/2022
6	U3	User3		0	0	0	No	No	No	1	GS	1	01/01/2022
7	U4	User4		0	0	0	No	No	No	1	GS	1	01/01/2022
8	U5	User5		0	0	0	No	No	No	1	GS	1	01/01/2022
9	U6	User6		0	0	0	No	No	No	1	GS	1	
10	U7	User7	12336, 474343 643345 433 464364 6,7457 745543 453	0	0	0	No	No	No	1	GS	1	

- **Personal Info** - Generates a list of the personal information of selected users.

Personal Info

Back

Find... 5 of 10 100%

Main Report

Organization-1 Page 5 of 10

Run by: System Admin OrganizationS-Wise User Personal Info Date: 23/01/2018 16:29

User ID :19617	Name :User 5040
Reference Code :19617	Nationality :
Birth Date :	Marital Status :Married
Blood Group :A+	Gender :Male
Qualification :	
User ID :19618	Name :User 5041
Reference Code :19618	Nationality :
Birth Date :	Marital Status :NA
Blood Group :A+	Gender :Male
Qualification :	
User ID :19619	Name :User 5042
Reference Code :19619	Nationality :
Birth Date :	Marital Status :NA
Blood Group :A+	Gender :Male
Qualification :	
User ID :19620	Name :User 5043
Reference Code :19620	Nationality :
Birth Date :	Marital Status :NA
Blood Group :A+	Gender :Male
Qualification :	
User ID :19621	Name :User 5044
Reference Code :19621	Nationality :
Birth Date :	Marital Status :NA

- **Contact Info** - Generates a listing of the contact information of selected users.

Contact Info

Back

Find... 1 of 1 100%

Main Report

Organization-1

Page 1 of 1

Run by: System Admin

Organization-Wise User Contact Info

Date: 30/04/2018 11:44

Sr No	User ID	Name	Address (Local-Permanent) / Contact Number / Email	Reference Code
Organization-1				
1	1	Chirag		1
2	101	Khushbu	Personal: Email:sheetal.raval@matrixrd.org	101
3	1687	Aditi Ajay Gupta_Ahmedabad	Personal: Cell:919687624826 Email:aditi.gupta@matrixrd.org Official: Cell:919429063421	1687
4	3	Sheetal Pradip Pandya_Ahm		3
5	JPC1	Darshna		102
6	JPC2	Akshay		103
Organization-2				
1	5	Priyank		5
2	6	Rohit Jain	Personal: Cell:9654231585 Official: Email:rohit.jain@gmail.com	6

- **Official Info** - Generates a list of the official information of selected users.



The details of Reporting Group, OFF Day1 and OFF Day2 will not be available in Basic License.

Official Info									
Back									
Find... 1 of 1 100%									
Main Report									
Organization-1									
Organization-Wise User Official Info									
Run by: System Admin									
Sr No	User ID	Name	Reporting Group	DPT	DSG	CTG	Off Day 1	Qualification	Date: 30/04/2018 11:46
	Joining Dt			BRC	SEC	GRD	Off Day 2	Experience	Reference Code
ORG1									
1	1	Chirag	QA Group	DPT1	DSG1	CTG1	Sunday		1
				BRC1	SEC1	GRD1	None		
2	101	Khushbu		DPT1	DSG1	CTG1	Sunday		101
				BRC1	SEC1	GRD1	None		
3	1687	Aditi Ajay Gupta_Ahmedabad		DPT1	DSG1	CTG1	Sunday		1687
			QA Group	BRC1	SEC1	GRD1	None		
4	3	Sheetal Pradip Pandya_Ahm		DPT1	DSG1	CTG1	Sunday		3
				BRC1	SEC1	GRD1	None		
5	JPC1	Darshna	QA Group	DPT1	DSG1	CTG1	Sunday		102
				BRC1	SEC1	GRD1	None		
6	JPC2	Akshay	QA Group	DPT1	DSG1	CTG1	Sunday		103
				BRC1	SEC1	GRD1	None		
ORG2									
1	5	Priyank	QA Group	DPT1	DSG1	CTG1	Sunday		5
				BRC1	SEC1	GRD1	None		
2	6	Rohit Jain		DPT1	DSG1	CTG1	Sunday		6
				BRC1	SEC1	GRD1	None		

- **Retirement Info** - Displays the list of all employees who are going to retire in the defined time period as shown below. The official age for retirement can be specified in the **Retirement Age** field. Eg: Here the retirement age is 30 years. The person who is completing 30 years in the date range from 25-4-2018 to 30-4-2018 will be listed in retirement info report. The calculation of 30 years is counted from the specified birthdate in user profile.

Retirement Info

←

Date * 25/04/2018 30/04/2018

Retirement Age 30

Optional Parameters

Group By Organization

User Selection

Select Users All

Generate Report For All Users

Generate Report

Retirement Info

←

Back

Find... 1 of 1 100%

Main Report

Organization-1 Retirement Info Page 1 of 1

Run by: System Admin Date: 30/04/2018 11:54

Sr No	User ID	Name	Designation	Grade	Birth Dt	Join Dt	Retire Dt
1	1	Chirag	Designation-1	Grade-1	28/04/1988	02/05/2013	28/04/2018
2	3	Sheetal Pradip Pandya_Ahm	Designation-1	Grade-1	30/04/1988	01/08/2011	30/04/2018

- **Enrollment Info** - Generates a list of all users who have been enrolled against a particular credential. You can select the credentials for which enrollment information report is to be viewed. Also you can enable "Not Enrolled Credentials" which will display the users who are not enrolled for even single credential.

Enrollment Info

←

Optional Parameters

Credentials

Card1 ☒ Card2 ☐ PIN ☒ FP ☒ Template(Supren) ☐

Not Enrolled Credentials ☒

User Selection

Select Users All

Generate Report

Enrollment Info

Back

Find... 1 of 1 100%

Main Report

Organization-1 Page 1 of 1

Enrollment Info

Run by: System Admin Date: 06/09/2018 14:24

User ID	Name	Card1	Card2	PIN	Enrolled Fingers			Enrolled Palm	Enrolled Faces	Enrollment Date-Time
					Suprema Proprietary	Suprema ISO	Lumidigm ISO			
user_1	User_1	Not Enrolled	Not Enrolled	Not Enrolled	0	0	0	0	0	
User_1	User_1	Not Enrolled	Not Enrolled	Not Enrolled	0	0	0	0	0	
user1	user1	Not Enrolled	Not Enrolled	Not Enrolled	0	0	0	0	0	

- **Change Group** - Generates a list of specific users whose reporting groups have been changed within the specified date range as shown below.

Change Group

Date * 30/04/2018 30/04/2018

User Selection

Select Users All

Generate Report For All Users

Generate Report

Change Group

Back

Find... 1 of 1 100%

Main Report

Organization-1 Page 1 of 1

Change Group From 30/04/2018 To 30/04/2018

Run by: System Admin Date: 30/04/2018 17:35

Sr No	Group Type	Change From	Change Till	New Group
5 - Priyank				
1	Reporting Group	30/04/2018	31/12/2099	ACTA Group

- **Biometric Enrollment Report:** This report provides an information about the total number of enrolled fingers of user as per the selection of 'Finger Enrollment Format Type' and its 'Quality'.

Configure the **Optional Parameters** and **User Selection** as shown below.

Optional Parameters

Finger Template Format Type Consideration

Suprema Proprietary ☒

Suprema ISO ☒

Enrollment Quality %

User1 Selection

Select User1s

User1 *

Search

User1 ID	Name	
006A	Shallee	
005A	admin	
001A	priyanka thakur	
002A	noshift	
002CC	regression	

1 - 5 of 20 records

« < 1 2 3 4 > »

Generate Report For

Generate Report

- Configure the **Finger Template Format Type Consideration** by choosing the required 'Finger Enrollment Format' as **Suprema Proprietary** and/or **Suprema ISO**.
- You can also choose the required quality of the Finger templates for which the report is to be generated. Select the appropriate formula and specify the value for it (in percentage) to configure the desired **Enrollment Quality**.



If the option 'Select' is selected as an Enrollment Quality then the Templates of all quality types will be considered into the report.

- Configure the **User Selection** Tab and click on the Generate Report button to generate the "Biometric Enrollment Report" as shown below.

Biometric Enrollment Report

Back

Find... 1 of 1 100%

Main Report

Organization-1		Suprema Proprietary		Suprema ISO		Date: 11/02/2020 18:13
Biometric Enrollment Report						
User1 ID	Name	No of Enrolled Fingers	Quality	No of Enrolled Fingers	Quality	
006A	Shallee	0		8	69, 63, 67, 70, 75, 48, 51, 48	

Page 1 of 1

Others

- **Former Users** - Generates records of all or group-wise former employees whose leaving dates fall within the specified month and year as shown below. Leaving date is specified in User profile.

Former Users

←

Back

Find...

1 of 1

100%

Main Report

Organization-1

Page 1 of 1

Former Users

Run by: System Admin

Date: 30/04/2018 7:40

User ID	Name	Department	Designation	Joining Date	Confirmation Date	Leaving Date	Reason	Active	Inactive
6	Rohit Jain	Department-1	Designation-1	02/05/2017		27/04/2018		Yes	
JPC1	Darshna	Department-1	Designation-1	11/10/2017		11/04/2018		Yes	

- **New Joining** - Generates a list of users whose joining date is within the specified date range. Joining date is specified in User profile.

New Joining

Back

Find...

1 of 1

100%

Main Report

Organization-1

Page 1 of 1

Run by: System Admin

Date: 21/02/2018 12:10

Organization-Wise New Joining From 01/02/2018 To 21/02/2018

User ID

Name

Department

Joining Date

Creation Date-Time

Leaving Date

Active

1 - Organization-1

101

Khushbu

Department-1

01/02/2018

01/02/2018 - 11:41

Yes

4

Sudeshna

Department-1

21/02/2018

21/02/2018 - 12:09

Yes

- **Pending Confirmation** - Generates a listing of all users whose employment confirmation is due within the specified date range.

If the Joining date of user is say 21/2/2018 and confirmation period is 5 days. It means within 5days user will be confirmed. So if confirmation date i.e. 26/2/2018 is within the selected date range then report will show that pending confirmation user.

Pending Confirmation

←

Date* 21/02/2018 28/02/2018

Confirmation Period (Days) 5

Optional Parameters

User Selection

Select Users All

Generate Report For All Users

Generate Report

Pending Confirmation

Back

Find... 1 of 1 100%

Main Report

Organization-1 Page 1 of 1

Pending Confirmation From 21/02/2018 To 28/02/2018

Run by: System Admin Date: 21/02/2018 18:17

User ID	Name	Department	Designation	Joining Date	Days Remaining	Confirmation On
4	Sudeshna	Department-1	Designation-1	21/02/2018	5	26/02/2018

- **Reporting Groups** - Generates a list of all reporting groups with the details of Reporting In-charge and their respective members.

Reporting Groups

←

Show Group-Wise Users ☒

Reporting Group Selection

Select Reporting Groups Reporting Group Wise

Reporting Group* ID Name

Search

ID	Name	Group	
1	QA Group	Reporting Group	
2	ACTA Group	Reporting Group	

Generate Report

Reporting Groups

←

Back

Find...

1 of 1

100%

Main Report

Organization-1

Page 1 of 1

Reporting Group-Wise Users

Run by: System Admin

Date: 30/04/2018 18:07

Sr No	User ID	Name	Department	Status	Type
1	QA Group				
1	101	Khushbu	Department-1	Active	T&A
1	1	Chirag	Department-1	Active	T&A
2	1687	Aditi Ajay	Department-1	Active	T&A
		Gupta_Ahmedabad			
3	JPC1	Darshna	Department-1	Active	T&A
4	JPC2	Akshay	Department-1	Active	T&A
2	ACTA Group				
1	102	Shruti Patki	Department-1	Active	T&A
1	5	Priyank	Department-1	Active	T&A

- **Users without Reporting In-charge** - Enlists all users on the system who have not been assigned under any Reporting In-charge.

Users Without Reporting In-Charge					
Main Report					
Organization-1					
Users Without Reporting In-Charge					
Run by: System Admin					
Date: 30/04/2018 18:20					
Sr No	User ID	Name	Organization	Department	Designation
1	101	Khushbu	Organization-1	Department-1	Designation-1
2	102	Shruti Patki	Organization-1	Department-1	Designation-1
3	2	Isha Shinde	Organization-1	Department-1	Designation-1
4	3	Sheetal Pradip Pandya_ Ahm	Organization-1	Department-1	Designation-1
5	4	Shinjini Ghosh	Organization-1	Department-1	Designation-1
6	6	Rohit Jain	Organization-2	Department-1	Designation-1

- **User Wise Policy Assignment**- It shows the users along with the policies assigned to the user.

User-Wise Policy Assignment

Back

Find...

1 of 2

100%

Main Report

Organization-1

Page 1 of 2

User-Wise Policy Assignment

Run by: System Admin

Date:21/02/2018 11:28

User :1 Chirag

Attendance Policy : 1-Attendance Policy-1 Early-OUT Policy : 1-Early Out Policy-1

Absentee Policy : 1-Absentee Policy-1 C-OFF Policy : 1-COFF Policy-1

Ntwk & OT Policy : 1-OverTime Policy-1 OT/C-OFF Eligibility: None

Late-IN Policy : 1-Late In Policy-1

User :101 Khushbu

Attendance Policy : 1-Attendance Policy-1 Early-OUT Policy : 1-Early Out Policy-1

Absentee Policy : 1-Absentee Policy-1 C-OFF Policy : 1-COFF Policy-1

Ntwk & OT Policy : 1-OverTime Policy-1 OT/C-OFF Eligibility: None

Late-IN Policy : 1-Late In Policy-1

User :1687 Aditi Ajay Gupta Ahmedabad

Attendance Policy : 1-Attendance Policy-1 Early-OUT Policy : 1-Early Out Policy-1

Absentee Policy : 1-Absentee Policy-1 C-OFF Policy : 1-COFF Policy-1

Ntwk & OT Policy : 1-OverTime Policy-1 OT/C-OFF Eligibility: None

User Events

- **In/Out Event** - Generates a list of all entry and exit events of users within the specified date and time range as shown in the sample report below.

Organization-1							Page 2 of 2	
Organization-Wise IN/OUT Event From 12/07/2021 00:00 To 12/07/2021 23:59							Date: 12/07/2021 17:39	
Run by: User ID	System Admin Name	Punch Time	I/O Type	Device/Source Detail	Location	Punch Mode	Event Status	Special Function
117	mayank	13:59:40	IN	13 : ARGO FACE-Device-7		API	Allowed	
117	mayank	13:59:50	IN	13 : ARGO FACE-Device-7		API	Allowed	
117	mayank	14:00:32	IN	13 : ARGO FACE-Device-7		API	Allowed	
117	mayank	14:00:47	IN	13 : ARGO FACE-Device-7		API	Allowed	
117	mayank	14:00:53	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:01:00	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:01:04	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:01:08	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:01:11	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:01:14	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:01:17	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:01:22	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:01:26	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:01:29	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:02:06	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:02:09	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:32:31	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:32:36	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:41:07	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:41:11	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:41:30	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:41:35	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:41:39	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:41:42	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:41:47	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:41:53	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:42:01	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:42:12	IN	13 : ARGO FACE-Device-7		Face	Allowed	
117	mayank	14:42:17	IN	13 : ARGO FACE-Device-7		Face	Allowed	
chirag	chirag	17:16:26	IN	ESS			Allowed	Regular - IN
chirag	chirag	17:16:28	IN	ESS			Allowed	Overtime - IN
chirag	chirag	17:17:10	OUT	ESS			Allowed	Official Work - OUT
chirag	chirag	17:17:12	OUT	ESS			Allowed	Regular - OUT
chirag	chirag	17:17:16	OUT	ESS			Allowed	Overtime - OUT
chirag	chirag	17:17:19	IN	ESS			Allowed	Short Leave - IN

- **In/Out Summary** - Generates a summary statement of the compiled data on the entry and exit events of users of selected group on the selected date.

In/Out Summary

←

Date * 30/04/2018

User Selection

Select Users

Group Wise

Select Group

Organization

Organization *

ID

Name

Search

ID

Name

Group

1

Organization-1

Organization

Generate Report For

All Users

Generate Report

Organization-1							Page 1 of 1	
Department-Wise IN/OUT Summary For 30/04/2018							Date: 30/04/2018 18:26	
Run by:	System Admin			Total Users				
Sr No	Department	Entered	Exited	Total Inside				
1	Department-1	2	0	2				

- **Access Denied** - Generates a list of punch events where the identified users have been denied access along with the reason for the same.

Access Denied

Date: 14/09/2020 14/09/2020

Optional Parameters

Enterprise Group In Report: Organization

Denied Events:

- ☒ Invalid Input
- ☐ Occupancy Control
- ☒ 2-Person Rule
- ☐ Time Out
- ☐ Visitor Escort

Organization Name in Header As Per: User Selection

User Selection

Select Users: User Wise

User: ID Name

Generate Report For: All Users

Generate Report

Access Denied

Back

Find... 1 of 1 100%

Main Report

Organization-1 Page 1 of 1

Access Denied From 03/05/2018 To 03/05/2018

Run by: System Admin

Sr No	User ID	Name	Organization	Credential	Time	IN/OUT	Date: 03/05/2018 14:39	Reason
03/05/2018								
Door V3 as Panel Door								
1	1	Chirag	Organization-1	Finger	14:31	IN		Denied - Time Out
2	1	Chirag	Organization-1	Finger	14:35	IN		Denied - Time Out
3	1	Chirag	Organization-1	Card	14:35	IN		Denied - Time Out
4	101	Khushbu	Organization-1	Finger	14:31	IN		Denied - 2-Person Rule
5	101	Khushbu	Organization-1	Finger	14:34	IN		Denied - Time Out
6	1687	Aditi Ajay	Organization-1	Card	14:35	IN		Denied - 2-Person Rule
7	4	Gupta_Ahmedabad Shinjin Ghosh	Organization-1	Finger	14:35	IN		Denied - Time Out

- **Doors Accessed By User** - Generates a date-wise list of all users who have punched at various doors.

Doors Accessed by User

Back

Find... 1 of 1 100%

Main Report

Organization-1 Page 1 of 1

Doors Accessed By User From 01/04/2018 To 30/04/2018

Run by: System Admin Date: 30/04/2018 18:33

Sr No	User ID	Name	Department	Time	I/O Type
17/04/2018					
Door V3 as Panel Door					
1	1	Chirag	Department-1	14:52	IN
2	1	Chirag	Department-1	14:53	IN
19/04/2018					
Door V3 as Panel Door					
1	1	Chirag	Department-1	17:43	IN
30/04/2018					
PVR Door-Device-12					
1	JPC1	Darshna	Department-1	18:32	IN
2	JPC1	Darshna	Department-1	18:32	IN
3	JPC1	Darshna	Department-1	18:32	IN
Door V3 as Panel Door					
1	1	Chirag	Department-1	15:40	IN
2	1687	Aditi Ajay Gupta_Ahmedabad	Department-1	15:47	IN

- **Door Usage** - Generates a user-wise detailed list of door usage over the specified period as shown.

ORGANISATION 1. Page 1 of 23

Door Usage from 01/01/2013 to 01/01/2013

Run by: System Admin Date: 30/01/2014 10:43

Sr No	Date	In Door	In Time	Out Door	Out Time	Duration
1001 - ANKITKUMAR SOHLIYA						
1	01/01/2013	RnD Basement V2	09:28	RnD Basement WL	14:01	04:33
2	01/01/2013	RnD 4th Flr	14:50	RnD 4th Flr	14:55	00:05
3	01/01/2013	RnD 3rd Palm	14:56	RnD 3rd Palm	19:59	05:03
4	01/01/2013	RnD Basement V2	20:00			
Total Hours :						09:41
1002 - MEGHA H SHUKLA						
1	01/01/2013	RnD Basement V2	09:21	RnD Basement V2	09:23	00:02
2	01/01/2013	RnD 3rd Palm	09:24	RnD Basement V2	14:16	04:52
3	01/01/2013	RnD 4th Flr	19:05	RnD 3rd Palm	19:15	00:10
4	01/01/2013	RnD 3rd Palm	19:51	RnD Basement V2	19:53	00:02
Total Hours :						05:06
1003 - UMESH M TALANPURI						
1	01/01/2013	Main Entry 2	09:14	Main Entry 1	19:03	09:49
Total Hours :						09:49

- **Who Is In** - Displays a list of all cardholders who have “punched-in” over the last 24 hours but have not “punched-out” i.e. a list of users still within the premises.

Who Is In

Optional Parameters

IN Punch Consideration Period (Hours) 24

Door Selection

Select Doors Door Wise

Door * ID Name

Search

ID	Name	Group	
2	PVR Door-Device-12	Door	
17	Door V3 as Panel Door	Door	
18	Door V3 as Panel Door	Door	

Generate Report

Who Is In

Back

Find... 1 of 1 100%

Main Report

Organization-1 Page 1 of 1

Who Is In as on 03/05/2018 15:15:52

Run by: System Admin Date: 03/05/2018 15:15

Sr No	User ID	Name	Door	IN Date-Time
Department-1				
1	1	Chirag	Door V3 as Panel Door	03/05/2018 14:31
2	101	Khushbu	Door V3 as Panel Door	03/05/2018 14:31
3	JPC1	Darshna	PVR Door-Device-12	03/05/2018 09:06

- **Out Time** - Displays a detailed list of Out Time for users during the specified period i.e. the time duration for which user has been outside the office premises.



The **Out Time** report generated will only display the User's Device punches.

Out Time

Date * 04/05/2018 04/05/2018

User Selection

Select Users All

Generate Report For All Users




Generate Report

When the user punches out at 10:30 hours and comes again with In punch of 11:30 hours; then OUT time will be 1:00 hour. Similarly other transactions are recorded with individual out time duration. Also the total OUT time will be added and displayed as shown below.



Out Time

←

Back



Find...



1 of 1

100%

Main Report

Organization-1

Page 1 of 1

Out Time From 04/05/2018 To 04/05/2018

Run by: System Admin

Date: 04/05/2018 15:33

Sr No	Date	OUT Door	IN Door	OUT Time	IN Time	Duration
102 - Shruti Patki						
1	04/05/2018	Door V3 as Panel Door	FVR Door-Device-12	10:30	11:30	01:00
2	04/05/2018	Door V3 as Panel Door	FVR Door-Device-12	11:50	12:30	00:40
Total OUT Time						01:40

- **User Events Interval-** Displays entry and exit events of user with time interval.

User Event Interval

←

Date * 03/05/2018 03/05/2018
Time 00:00 23:59

Optional Parameters

User Selection

Select Users All

Generate Report

User Event Interval

Back

Find...

1 of 1

100%

Main Report

Organization-1

Run by: System Admin

User Events Interval From 03/05/2018 To 03/05/2018

Date: 03/05/2018 15:20

Late-IN/

Early-OUT

Event Date-Time	Device	Site	Entry/Exit	Interval
1 - Chirag				
03/05/2018 09:07:52	FVR Door-Device-12	Site-1	Entry	00:00:00
03/05/2018 19:19:20	Door V3 as Panel Door	Site-1	Exit	10:11:28
03/05/2018 19:19:38	Door V3 as Panel Door	Site-1	Exit	00:00:18
101 - Khushbu				
03/05/2018 09:09:54	FVR Door-Device-12	Site-1	Entry	00:00:00
03/05/2018 19:19:38	Door V3 as Panel Door	Site-1	Exit	10:09:44
JPC1 - Darshna				
03/05/2018 09:06:21	FVR Door-Device-12	Site-1	Entry	00:00:00

The Devices module is available to all users of the COSEC Basic Platform License. You can view, define and configure all the parameters related to COSEC Devices in this module. It is important to configure this module correctly because it precedes the process of user enrollment and formulation of advanced HR policies such as *Time and Attendance* or *Access Control* policies.



VEGA Series

DOOR Series

PATH Series

ARC Series

The various COSEC devices have capacity to support the following number of users:

S. No.	COSEC Device	No. of Users Supported
1	Direct Door V1	500
2	Direct Door V2	2000
3	Direct Door V3	50,000
4	Direct Door V4	50,000
5	NGT Direct Door	10,000
6	Wireless Door	50,000
7	PVR Door	50,000
8	PATH Door	10,000
9	ARC DC100	10,000
10	ARC DC200	50,000
10	ARC IO 800	NA

S. No.	COSEC Device	No. of Users Supported
11	Panel	10,000
12	Panel-Lite	25,000
13	Panel200	25,000
14	Vega Controller	50,000
15	Door FMX	50,000
16	MODE Device	50,000
17	ARGO	50,000
18	ARGO FACE	50,000



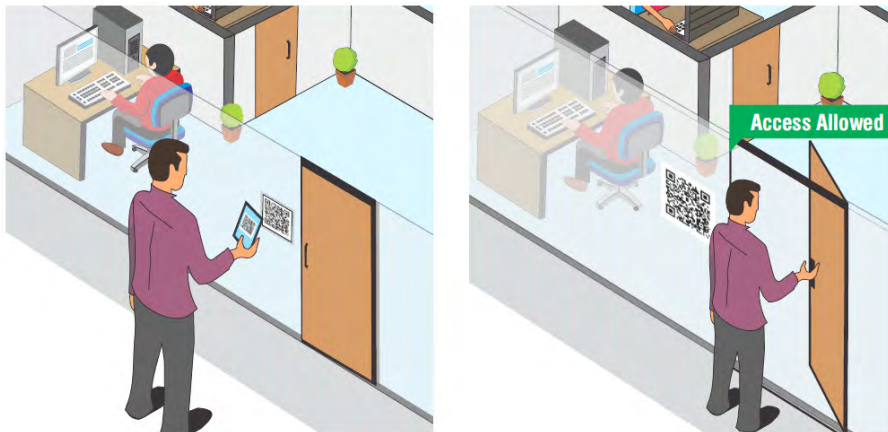
The Direct Door V1, Direct Door V2, PATH Door, ARC DC100, ARC DC200, ARC IO 800, Panel and Panel lite are not supported in COSEC VYOM.

You can access the COSEC Devices using PIN Number, Biometric Credentials, Smart Cards, Mobile based Access like QR Code Access and Bluetooth based Access. You can also open COSEC Doors using Matrix SARVAM UCS by dialing a number from the keypad. To know more refer to *COSEC Integration* in the SARVAM UCS System Manual.

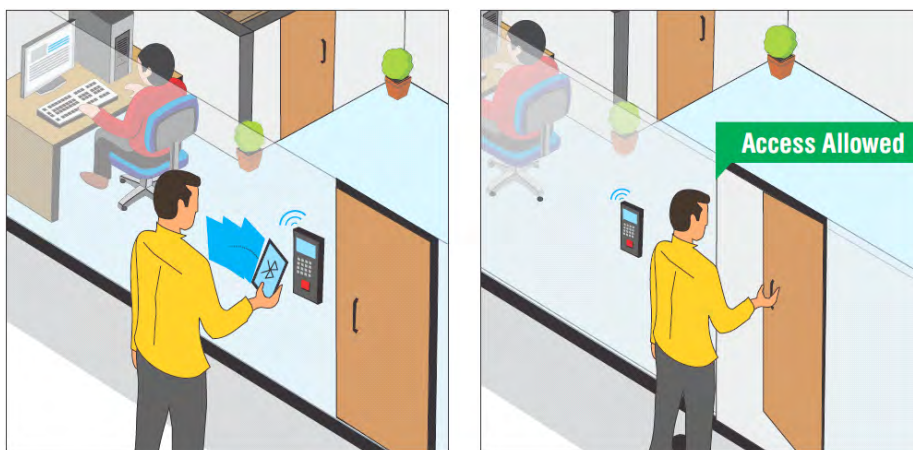
PIN, Biometric Credentials, Card



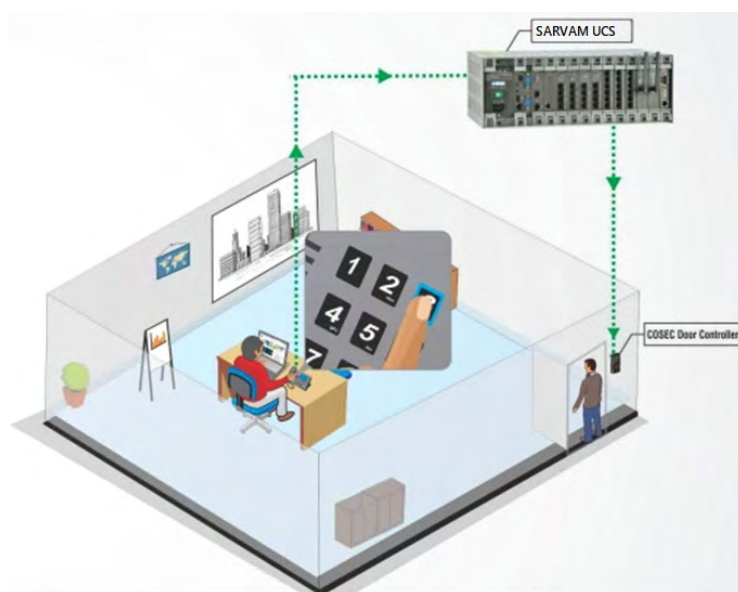
QR based Access



Bluetooth based Access



Access using SARVAM UCS




Face Recognition

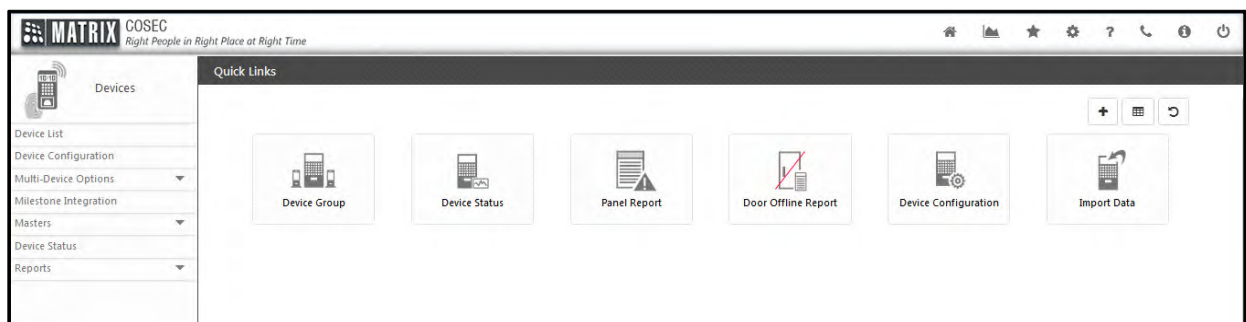
Face Recognition today is the need of the hour and Matrix offers the following devices to choose from as per your requirement:

- The ARGO FACE with built-in facial recognition and liveness detection support for Access Control, Time Attendance & Cafeteria. For details refer to [“ARGO FACE Door”](#).
- The MODE Device is designed for Face Recognition feature which uses in-built camera of the Mobile device for capturing the face. For details, refer to [“MODE Door”](#).
- COSEC Vega, COSEC FMX and COSEC ARGO supports face recognition by using IP camera for capturing the face. For details refer to [“ARGO Door”](#), [“Door FMX”](#) and [“VEGA Door”](#).






To access the **Devices** module,

- Click **Devices**  module on the Home page. The **Devices** page appears.



The page displays a menu and **Quick Links** to go to the required page in just one click. Quick Links are shortcuts to reach to a specific page easily. It also contains following three buttons:

- **Add Quick Link:** Click  to add a quick link. A picklist for Quick Link pages appears for selecting the page or External Link for which the quick link is to be created. Maximum **20** quick links can be added.
- For Adding **Pages** in Quick Link, select the Pages and click on **OK**.
- For Adding **External Links**, select External Link tab, click on  to add new external link.
- Configure the **Title** and **URL** of the external link under the respective fields. Click on checkbox to get the configured link on quick link screen as shown below. To save the configuration click on .


Picklist For Quick Links Pages

Pages External Links

Search +

	Title	URL	
<input checked="" type="checkbox"/>	Google	www.google.com	✓ ✕

OK Cancel



- To edit the saved configuration, click on  .
- Click on **OK** to save the link configuration on Quick Link screen. The external link will be displayed as shown below:

Quick Links

+ [Grid Icon] ↺

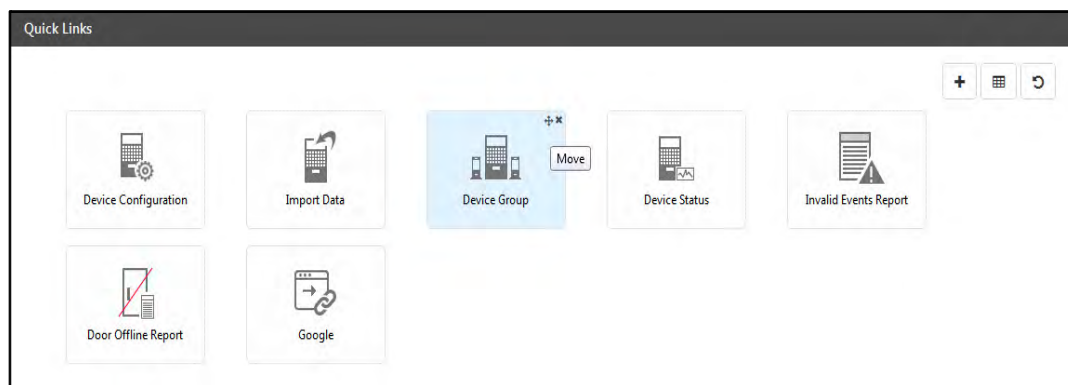
Device Configuration Import Data Device Group Device Status Invalid Events Report

Door Offline Report Google

- **Select Layout:** Click  to select a layout for the quick links. You can select 5x4 or 4x5 layout to manage the quick links.
- **Reset Quick Links:** Click  to reset the quick links to the default quick links.

Move the Link

To move the link from one place to another, hover on the link on top right corner and click on **“Move”** as shown below. Then drag the quick link to the desired place. It will be placed at the desired location on the quick links page.



Delete the Link

To delete a particular link, hover on the link on top right corner and click on “Delete” icon as shown below.



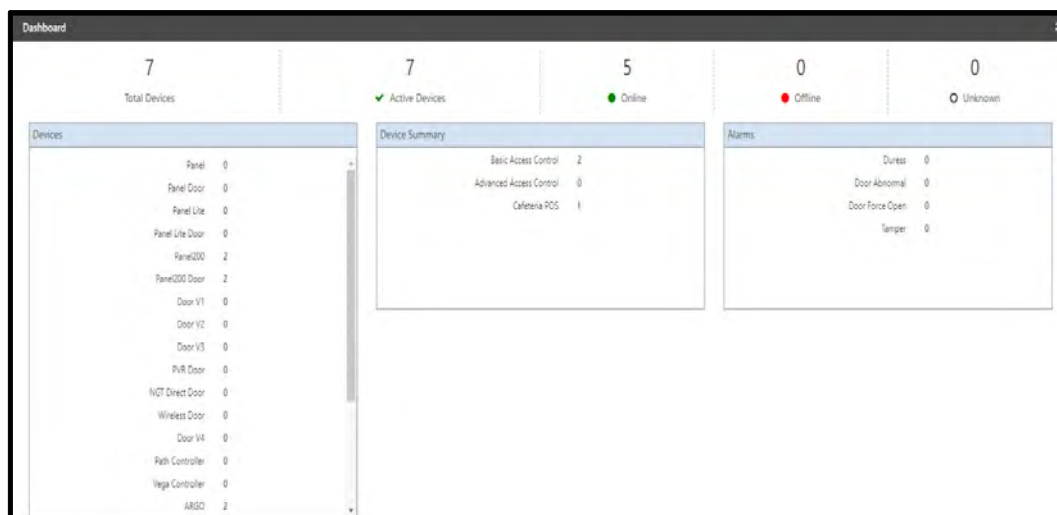
Quick links are displayed as per rights given to System Account and ESS users.

Devices Dashboard

To view the Dashboard,

- Click **Dashboard**  on the **Devices** page.

It displays the following information of the Devices — Device Status, List of Devices, Device Summary and Device Alarms.



Device Status

- **Total Devices:** Total number of devices configured in COSEC.
- **Active Devices:** Total number of devices that are currently active.
- **Online Devices:** Total number of devices that are currently online with server.
- **Offline Devices:** Total number of devices that are currently offline with server.
- **Unknown Devices:** Total number of devices whose status is not known to the server.

Devices

- This displays the list of various device types configured on the system, along with their individual counts.

Device Summary

- **Basic Access Control:** Total number of devices that are configured for Basic Access Control.
- **Advanced Access Control:** Total number of devices that are configured for Advanced Access Control.
- **Cafeteria POS:** Total number of devices that are configured for Cafeteria application.

Alarms

- **Duress:** Total number of Duress Alarm that are currently unacknowledged.
- **Door Abnormal:** Total number of currently unacknowledged Door Abnormal events of the doors.
- **Door Force Open:** Total number of currently unacknowledged Force Open events of the doors.
- **Tamper:** Total number of currently unacknowledged tampering events of the doors.



To configure an alert message for **Duress** click **Admin Module > System Configuration > Alert Message Configuration**. In Alert Filter, make sure that you select **All/Devices** from the drop-down list and in Event select **Duress** from the drop-down list. For more details, refer "[Configuring Alert Messages](#)".

Maximum 2 fingers can be enrolled as Duress Fingers. To configure the **Maximum No. of Fingers** enrolled click **Admin Module > System Configuration > Global Policy > Maximum No. of Fingers**.

For more information on the above Dashboard options, click the respective information links on the Dashboard.

Clicking **Refresh**  , to update the values on the Dashboard.

The **Devices** Module allows you to add and configure different devices and their corresponding variants. These are as follows:

Direct Doors

- Door V1
- Door V2
- Door V3
- Door V4
- NGT Direct Door
- Wireless Door
- PVR Door
- Vega Controller
- Door FMX
- Path Controller
- ARC DC100
- ARC DC200
- ARC IO800
- ARGO
- ARGO FACE

Panels

- Panel
- Panel Lite
- Panel200

Panel Doors

- Path Panel Door
- PVR Panel Door
- Vega Controller Panel Door
- ARC DC100 Panel Door
- ARC DC200 Panel Door
- ARC IO800 Panel Door
- Door V1/V2/V3/V4 Panel Door
- ARGO Panel Door
- ARGO FACE Panel Door

Although the basic configuration of all devices is a generic process, certain functionalities or configurations may not be available for all devices or all user licenses. For example, Cafeteria configurations are available only for Door V2, Door V3, Door V4, NGT Direct Door, Wireless Door, Door FMX, Vega and ARGO, ARGO FACE devices with a Cafeteria module license. Please refer to the respective device configuration topics for further details.



For all existing Panel200 devices, it is must for the Admin to update firmware before using PVR as a Panel Door.

Auto Adding New Devices

It is necessary to add a new device in the COSEC application before proceeding further with configuring it. These devices can be added manually as well as automatically using the **Auto Add New Devices** option.

To add the devices automatically, the administrator must enable the **Auto Add New Devices** check box in Admin Module > System *Configurations* > *Global Policy* > Device. The new devices connected with the COSEC Server

are automatically detected and defined in the COSEC database with a default ID and Name. For details, refer to [“Device”](#) in Global Policy.

For a new device to be auto-detected by the COSEC Server, the administrator must configure the **Server IP Address**, **LAN Settings** and **Port** configurations for the device from the physical Device Menu or Device Web page. For more information, refer to the respective device documents.

You can also auto-add devices that are to be assigned to a particular Device Group by default. Hence, any user and user credentials assigned to the default Device Group can be inherited by the new device automatically without manual intervention.



*If you wish to add a device as a Panel Door, we recommend you to add the same manually in the system if you have enabled **Auto Add New Devices**. This is to prevent the device from being added automatically as a Direct Door when the device comes online.*

While adding a device make sure the Monitor Service is running.

After a new device is added, you must upgrade its firmware, set it to Default factory settings and then Restore the Configurations.

Getting Door Online

Devices will be online when their connectivity is established with the Server.

Server - COSEC CENTRA

Let us consider the following example, to connect COSEC Door V3 with COSEC Server (CENTRA),

- Log into the **Admin Portal** (to do so, enter the following in the web browser: 192.168.101.88/cosecadmin/login. Then, enter the set Username and Password.)
- Click **Monitor Configuration**. The Monitor Configuration page appears.

ID	Monitor Name	Total no. Of Devices
3	MonitorService-309C23443DA7	67

ID	Name	Type
No Data		

- If the Monitor Settings have been configured, the details of the Monitor Service appears. Make sure the Monitor Service is running.



*Make sure the Master Service and Admin Portal Service configurations are done and these are running. For details refer to the **Services User Guide**.*

- Click **Service Configuration**, the details of the various services including Monitor Service are displayed.

For details refer to the **Services User Guide**.

- Click **Company Configuration > License and Services**.

The **License and Services** page appears.

MATRIX COSEC ADMIN

Company Configuration
 Profile
License and Services
 Monitor Configuration
 Service Configuration
 Manage Database

License and Services

Company * [matrix]
 Database Name COSEC_V20R1.1_SV Rack_17_Oct_2022

License Key
 Current License Key E684-CD3C-BF18-3CF-0C07-7296-5DA1-980C-F3CB-C871-2A4C-2080-8C04-880E-E
 New License Key *
 [Update] [Cancel]

Services

Alert Service * 1 [AlertService - 309C234]
 Enroll Service * 4 [EnrollService - 309C234]
 Visitor Service 2 [VisitorService - 309C23]
 Identification Service 2 [Identification - 309C23]
 Monitor Service * ID [Name]

Search [X]

ID	Monitor Service Name	Default
3	MonitorService - 309C2343DA7	<input checked="" type="checkbox"/>

[Save] [Cancel]

Current License Profile

Product Variant COSEC PLT
 Activation Status ACTIVATED
 AUP Validity November-2022
 Platform Users 510
 ACM Users 505
 CMM Users 505
 VMM Users 501
 TAM Users 505
 CWM Users 505
 JPC Users 505
 FVM Users 505
 ESS Users 505
 FR Users 505

- Under **Services**, select the configured Monitor Service. For details refer to the **Admin Mgt Portal User Guide**.
- Now, enter the Default IP Address of COSEC DOOR V3 in the web browser and press the Enter Key.
- Select the **User Name** as **Admin** and enter the set **Password**.
- Click **Settings > LAN Settings**.

The **LAN Settings** page appears.

MATRIX V3 Door - COSEC Door V3 (18)

Settings
 Basic Profile
LAN Settings
 Wi-Fi Settings
 Mobile Broadband Settings
 Server Settings
 CCC Settings
 Identification Server Settings
 Date-Time Settings
 Cafeteria Settings
 Multi Language Support
 Reader Settings
 Logs
 Manage

LAN Settings

IP Assignment Static
 IP Address * 191.168.10.51
 Subnet Mask * 255.255.254.0
 Default Gateway 191.168.11.1
 Preferred DNS
 Alternate DNS
 MAC Address 00:1b:09:07:83:03

[Submit] [Cancel] [Default]

Enter URL
 [Test Connection]

- The default IP Address appears. You can change the IP Address, if required. Enter the **IP Address** you wish to assign to the door.
- Click **Settings > Basic Profile**.

The **Basic Profile** page appears.

MATRIX V3 Door - COSEC Door V3 (18)

Settings

Basic Profile

Connectivity Status: ● via Ethernet

Door Type: Direct Door

Server Connection: COSEC CENTRA

Firmware Version: V01R60.00 (Oct 28 2021 - 01:31:36)

Firmware Upgrade Time: Oct 17 2022 - 11:01:51

System Up-Time: 1 days 6 hrs 33 mins

Submit Cancel

Readers

Readers	Mode	Configured Reader	Detected Reader
Internal - Card	Entry	HID ICLASS-U Reader - Active	HID ICLASS-U Reader
Internal - Finger	Entry	Finger Reader - Active	Finger Reader
External - Card	Exit	None	None
External - Finger	Exit	None	None
External - BLE	Exit	None	None

- In **Server Connection**, select the **COSEC CENTRA** option.
- Click **Manage > Backup and Update**.

The **Backup and Update** page appears.

MATRIX V3 Door - COSEC Door V3 (18)

Settings

Manage

Change Password

Backup and Upgrade

Alarm Monitoring and Control

Door Monitoring and Control

Enrollment

Smart Card Key

View

Backup and Upgrade

Auto Firmware Upgrade

Upgrade For: Door

Upgrade Firmware: Choose a file

Restore Configurations: Choose a file

Backup Events: Download

The device firmware must be upgraded. To do so, select the file and click **Update**.

- Click **Settings > Server Settings**. The **Server Settings** page appears.

MATRIX V3 Door - Door V3 51 FOT HID-iClass None (18)

Settings

- Basic Profile
- LAN Settings
- Wi-Fi Settings
- Mobile Broadband Settings
- Server Settings**
- CCC Settings
- Identification Server Settings
- Date-Time Settings
- Cafeteria Settings
- Multi Language Support
- Reader Settings
- Logs
- Manage
- View

Server Settings - COSEC CENTRA

This will be used to communicate with Monitor Service

Connectivity Status: ● via Ethernet

Encryption (SSL): ☐

Configuration: ☒ Basic ☐ Custom

URL:

Web Server

Encryption (HTTPS): ☐

Interface Selection: ☒ Auto ☐ Manual

Network Interface:

URL:

Directory Name:

Panel

Connectivity Status: ● Disconnected

Connect to Panel: ☐

Interface Selection: ☐ Auto ☐ Manual

Network Interface:

IP Address:

- In **URL**, enter the COSEC CENTRA IP Address and Port.

Once the connection with the Server is established, the **Connectivity Status** will turn Green.

Now, enter the **COSEC Server IP Address** in the address bar of the web browser and press the Enter Key.

- Click **Device Module > Device Status**.



*Make sure you have enabled the **Auto Add New Devices** check box in Admin Module > System Configurations > Global Policy > Device.*

The **Device Status** page appears.

Device Status

Search

Device Type: Device Status: Group By:

Name	Status	IP	MAC Address	Device Type	Site
Door V3	● Connected	192.168.104.109	00:18:09:02:66:F3	Door V3	Site-1

- Refresh the Device Status page. The device Status displays Connected and the device will be online.

Server - COSEC VYOM

Let us consider the following example, to connect COSEC ARGO Door with COSEC Server (VYOM),

- Log into the **Admin Portal** (to do so, enter the following in the web browser: 192.168.101.88/cosecadmin/login. Then, enter the set Username and Password.)
- Click **Monitor Configuration**. The Monitor Configuration page appears.

ID	Name	Type
1	Argo-Device	ARGO

- If the Monitor Settings have been configured, the details of the Monitor Service appears. Make sure the Monitor Service is running.



*Make sure the Master Service and Admin Portal Service configurations are done and these are running. For details refer to the **Services User Guide**.*

- Click **Service Configuration**, the details of the various services including Monitor Service are displayed.

For details refer to the **Services User Guide**.

- Click **Tenant Configuration > Tenant - Service Assignment**.

The **Tenant Service Assignment** page appears.

ID	Monitor Service Name	Default
2	MonitorService - 8CEC4B78A4FC	

- Under **Services**, select the configured Monitor Service. For details refer to the **Admin Mgt Portal User Guide**.
- Now, enter the Default IP Address of COSEC DOOR V3 in the web browser and press the Enter Key.
- Select the **User Name** as **Admin** and enter the set **Password**.
- Click **Settings > LAN Settings**.

The **LAN Settings** page appears.

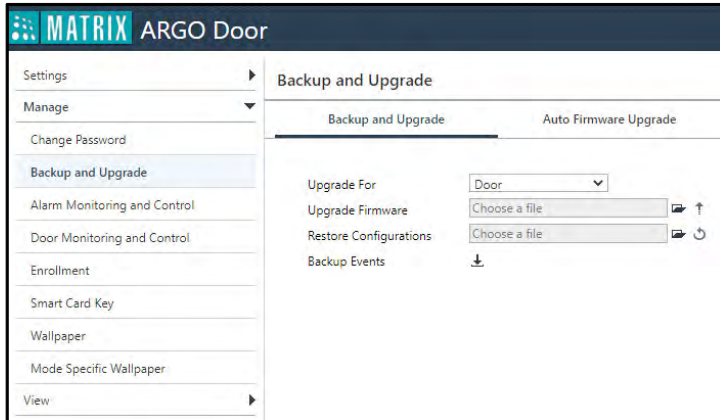
- The default IP Address appears. You can change the IP Address, if required. Enter the **IP Address** you wish to assign to the door.
- Click **Settings > Basic Profile**.

The **Basic Profile** page appears.

Readers	Mode	Configured Reader	Detected Reader
Internal - Card	Entry	EM Prox Reader - Inactive	HID ICLASS-U Reader
Internal - Finger	Entry	Finger Reader - Active	Finger Reader
External - Card	Exit	None	None
External - Finger	Exit	None	None
External - BLE	Exit	None	None

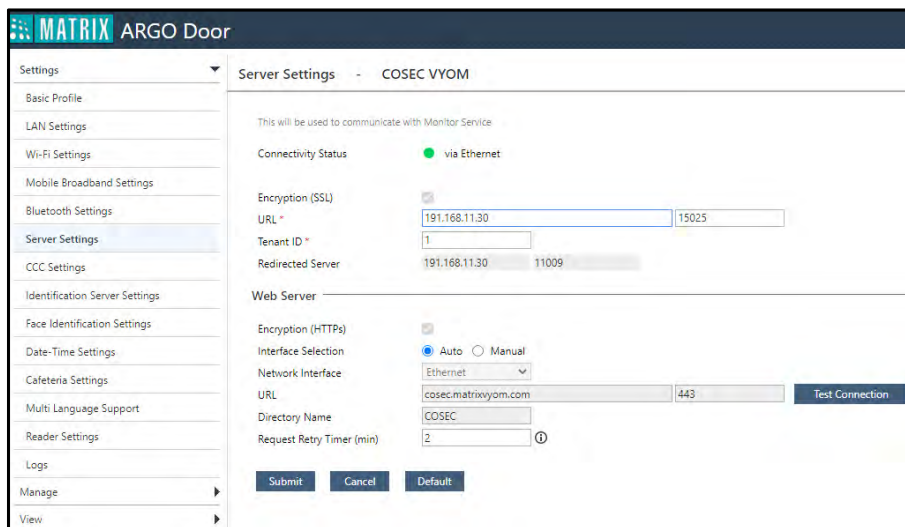
- In **Server Connection**, select the **COSEC VYOM** option.
- Click **Manage > Backup and Update**.

The **Backup and Update** page appears.



The device firmware must be upgraded. To do so, select the file and click **Update**.

- Click **Settings > Server Settings**. The **Server Settings** page appears.



- In **URL**, enter the COSEC VYOM IP Address and Port.
- In **Tenant ID**, enter the ID provided to you.

Once the connection with the Server is established, the **Connectivity Status** will turn Green.

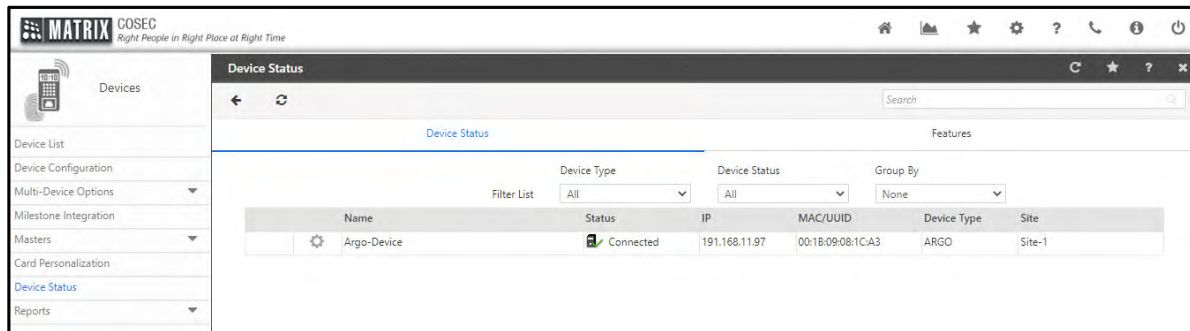
Now, enter the **COSEC Server IP Address** in the address bar of the web browser and press the Enter Key.

- Click **Device Module > Device Status**.



Make sure you have enabled the *Auto Add New Devices* check box in Admin Module > System Configurations > Global Policy > Device.

The **Device Status** page appears.



- Refresh the Device Status page. The device Status displays Connected and the device will be online.

Device List

The configuration procedure for every COSEC device is unique and depends on the type of device to be configured and the properties or regulations to be assigned to it.

Both Direct Door and Panel Door devices have considerably different configuration procedures as both follow separate approaches for communicating with the Server and other devices. While Direct Doors are independent doors that communicate individually with the COSEC Server.

Doors can also be connected as Panel Doors via Panel200. The Panel200 is a controlling device that can establish a centralized communication between the Server and other Panel Doors.

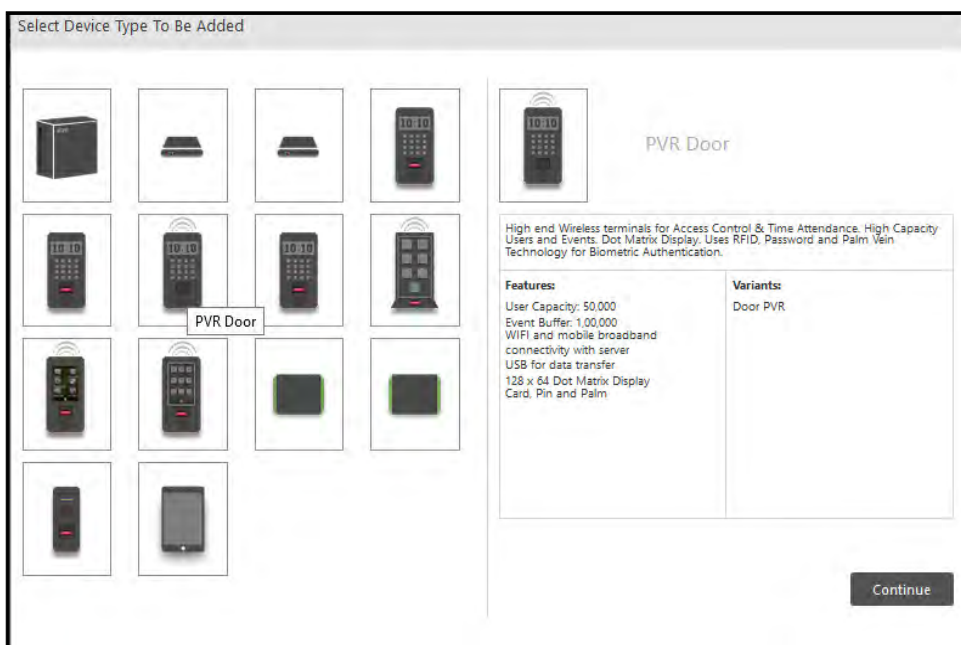
You can configure a COSEC Door as Direct Door or Panel Door.



Here, Panel refers to Panel/Panel Lite/Panel200.

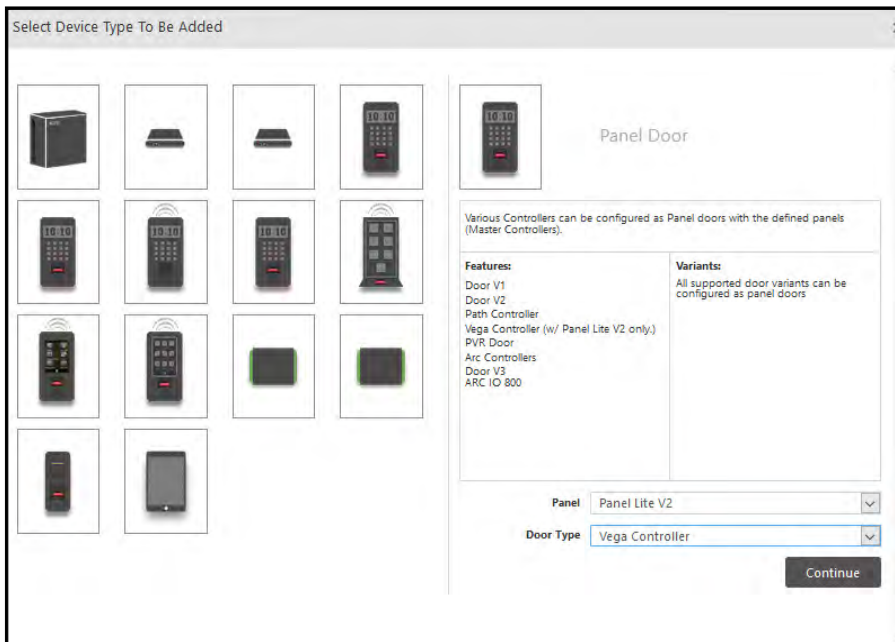
Adding and Configuring Doors

- **For Direct Door:** You can select any door from the options of Door Controller V1/V2/V3/V4, PATH Door, ARC Door, ARC IO800, PVR Door, NGT Door, Wireless Door, Vega Controller, ARGO or ARGO FACE and configure the door directly.
- Click **New**. Then click on the desired device.



- **For Panel Door:** You have to configure Panel200 first. Once Panel200 is configured, you can add the desired door by clicking the Panel Door option.

- Click **New**, then click **Panel Door**.
- Select the desired **Panel200** from the drop-down list.

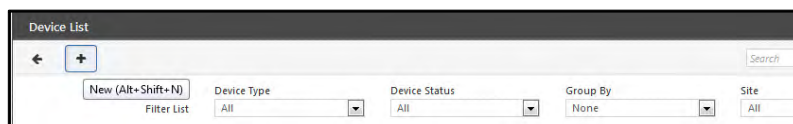


- Select the desired **Door Type** from the drop-down list— Door V1, Door V2, Door V3, Door V4, Path Controller, Vega Controller, PVR Door, ARC DC 100, ARC IO 800, ARC DC 200, ARGO, Path V2, ARGO FACE.

To configure doors,

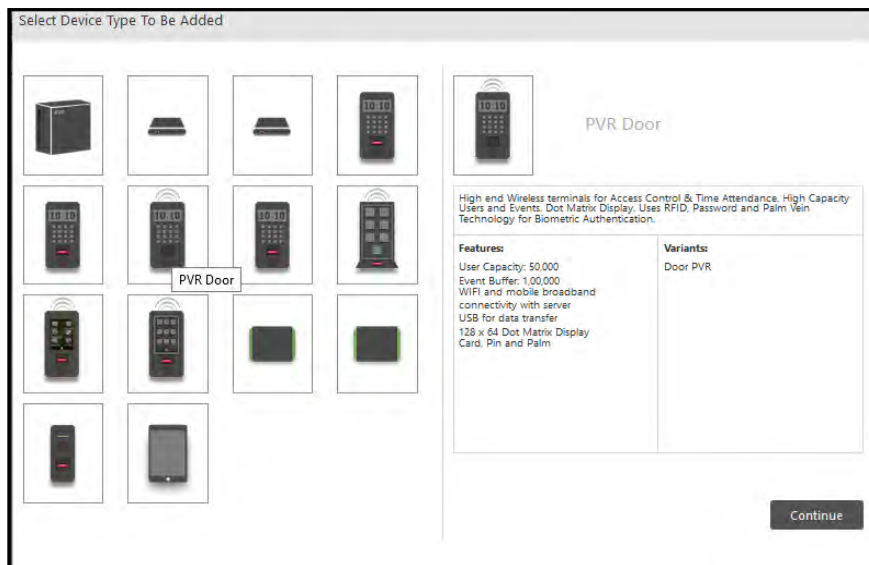
- Click **Devices module > Device List**.

The **Device List** page appears.



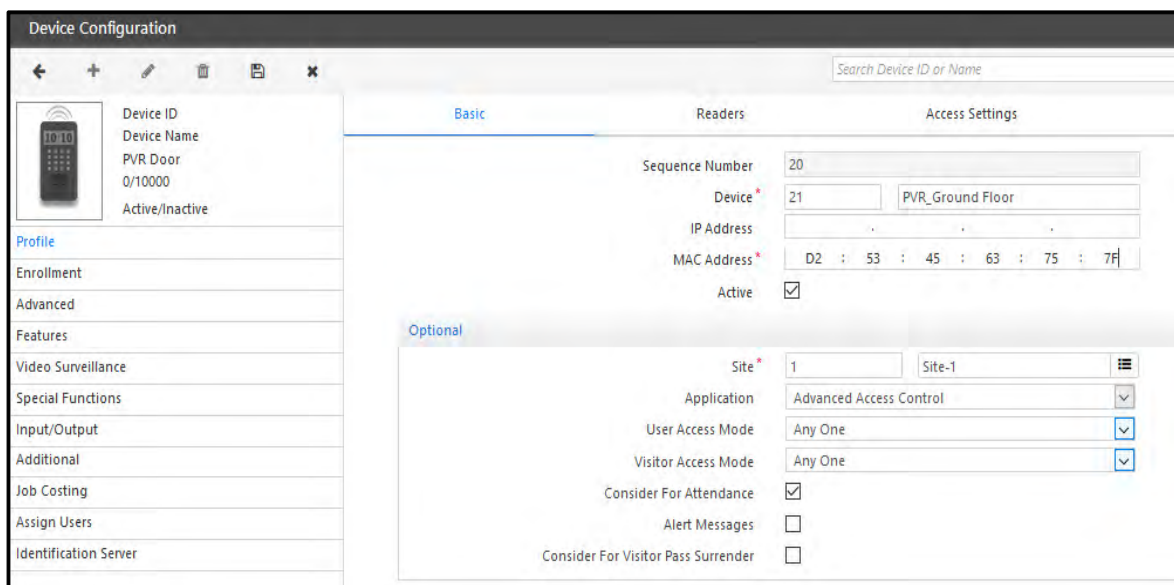
- Click **New**.

The **Select Device Type To Be Added** pop-up appears.



- Click on the desired Door Type.
- Click **Continue** to proceed.

The Device Configuration page appears.

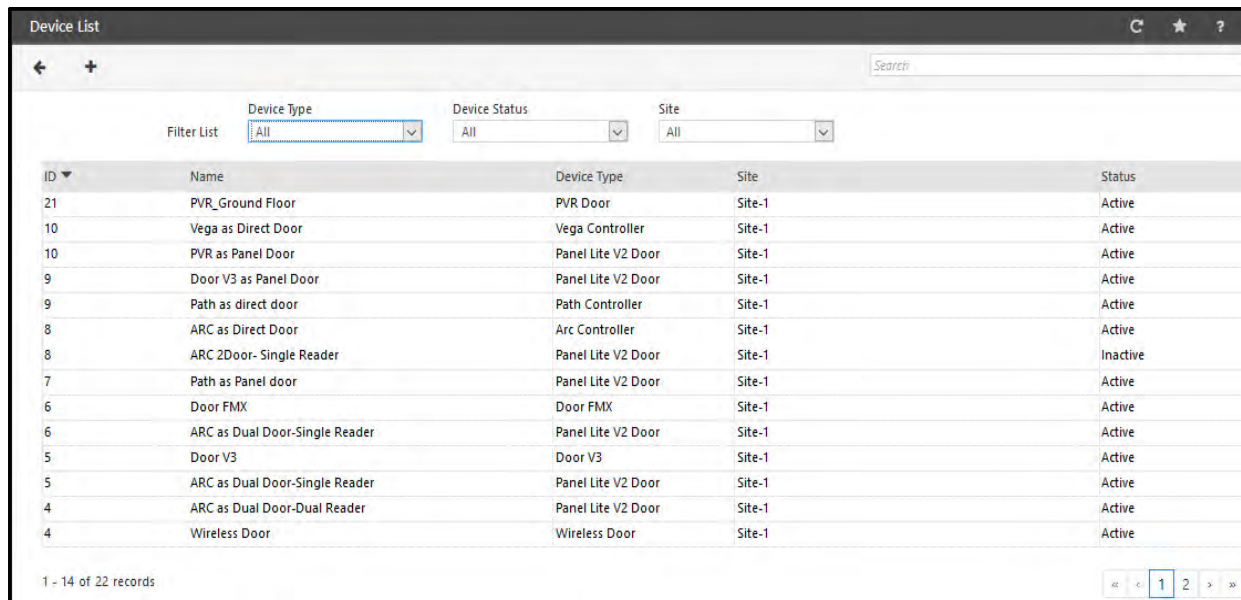


Refer to the respective topic for details.

- “NGT Door”
- “PVR Door”
- “ARC Door”
- “ARC IO-800”
- “PATH Door”
- “Door Controllers”
- “Door FMX”
- “VEGA Door”

- “Wireless Door”
- “ARGO Door”
- “ARGO FACE Door”
- “Panel200”
- “MODE Door”

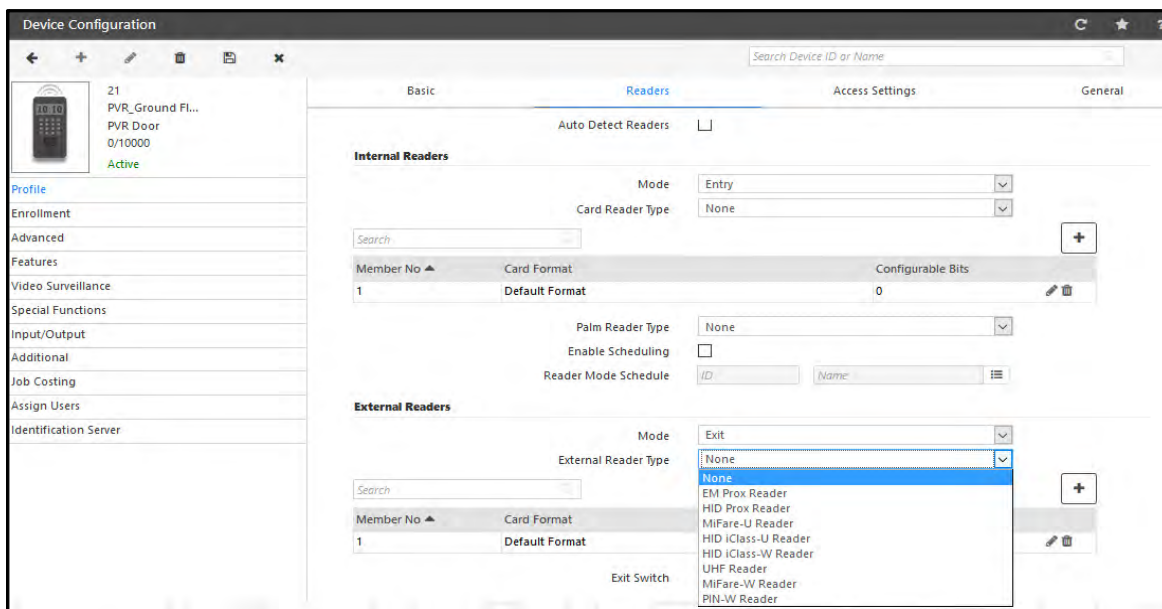
After configuring the devices, the **Device List** appears.



ID	Name	Device Type	Site	Status
21	PVR_Ground Floor	PVR Door	Site-1	Active
10	Vega as Direct Door	Vega Controller	Site-1	Active
10	PVR as Panel Door	Panel Lite V2 Door	Site-1	Active
9	Door V3 as Panel Door	Panel Lite V2 Door	Site-1	Active
9	Path as direct door	Path Controller	Site-1	Active
8	ARC as Direct Door	Arc Controller	Site-1	Active
8	ARC 2Door- Single Reader	Panel Lite V2 Door	Site-1	Inactive
7	Path as Panel door	Panel Lite V2 Door	Site-1	Active
6	Door FMX	Door FMX	Site-1	Active
6	ARC as Dual Door-Single Reader	Panel Lite V2 Door	Site-1	Active
5	Door V3	Door V3	Site-1	Active
5	ARC as Dual Door-Single Reader	Panel Lite V2 Door	Site-1	Active
4	ARC as Dual Door-Dual Reader	Panel Lite V2 Door	Site-1	Active
4	Wireless Door	Wireless Door	Site-1	Active

You can view the Device list based on the filters — **Device Type**, **Device Status** and **Site**.

You can connect **External Readers** to the door controller and configure it from **Device > Device Configuration > Profile > Readers > External Readers**.



Device Configuration

Basic | **Readers** | Access Settings | General

Auto Detect Readers ☐

Internal Readers

Mode: Entry
Card Reader Type: None

Search: []

Member No	Card Format	Configurable Bits
1	Default Format	0

Palm Reader Type: None
Enable Scheduling: ☐
Reader Mode Schedule: ID: [] Name: []

External Readers

Mode: Exit
External Reader Type: [None selected]

Search: []

Member No	Card Format
1	Default Format

Exit Switch: []

These Readers are used to read and detect cards and finger templates enrolled for the user.

You can use Read Only Card as well as Smart Card.

The External Reader type selection depends on the available card/credentials with you.

Reader Types and supported credentials

- **EM Prox Reader:** EM Prox Read Only Card
- **HID Prox Reader:** HID i-class Low Frequency Read Only Card.
- **MiFare-U Reader:** Mifare Smart Card.
- **HID iClass-U Reader:** HID i-class Smart Card.
- **HID iClass-W Reader:** HID i-class at Wiegand Interface; Read Only Card.
- **UHF Reader:** UHF Card at Wiegand Interface.
- **Combo Exit Reader:** Finger and any card (Type of Card is automatically detected by the Reader).
- **MiFare-W Reader:** Mifare at Wiegand Interface; Read Only Card.
- **PIN-W Reader:** Pin Reader.
- **CB U Reader:** Reader with BLE support.
- **CB W Reader:** Reader CB at Wiegand Interface.
- **ATOM RD300:** Pin, RFID Card, Mobile Credential over BLE and Fingerprint.
- **ATOM RD200:** RFID Card, Mobile Credential over BLE and Finger.
- **ATOM RD100:** Card and Mobile Credential over BLE.



Check for availability of ATOM reader variants.

COSEC PATH Readers

The variants; RDCE, RDCEP, RDCI, RDCM can be used as Combo Exit Readers, that is, you can use finger as well as card as the credential.

- **COSEC PATH Reader:** RDCE - EM Prox Cards
RDCP - HID- Prox Cards
RDCI - HID-iClass Cards
RDCM- Mifare Cards

- **COSEC ATOM Readers:** The type of card supported in each COSEC ATOM variants — RD300, RD200 and RD100 is dependent upon their sub-variants as described below.
 - **ATOM RD300**
 - ATOM RD300MFM - Mifare / Desfire / NFC / Combo Cards
 - ATOM RD300MFI - HID i - Class, Mifare / Desfire / NFC / Combo Cards
 - ATOM RD300SFE - Proximity Card
 - ATOM RD300MFE - Proximity Card
 - **ATOM RD200**
 - ATOM RD200MFM - Mifare / Desfire / NFC / Combo Cards
 - ATOM RD200MFI - HID i - Class, Mifare / Desfire / NFC / Combo Cards
 - ATOM RD200SFE - Proximity Card
 - ATOM RD200MFE - Proximity Card
 - **ATOM RD100**
 - ATOM RD100KM - Mifare / Desfire / NFC / Combo Cards
 - ATOM RD100KI - HID i - Class, Mifare / Desfire / NFC / Combo Cards
 - ATOM RD100M - Mifare / Desfire / NFC / Combo Cards
 - ATOM RD100I - HID i - Class, Mifare / Desfire / NFC / Combo Cards
 - ATOM RD100E - Proximity Card
 - ATOM RD100KE - Proximity Card

NGT Door

The Device Configuration page for NGT Door appears as shown below.

Device Configuration

Search Device ID or Name

1 NGT Direct Do...
NGT Direct Door
16/10000
Active

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Basic Readers Access Settings General

Sequence Number 1
Device 1 NGT Direct Door-Device-1
IP Address 192 . 168 . 104 . 84
MAC Address 00 : 1B : 09 : AB : CD : 51
Active ☒

Optional

Site 2 RnD Site
Finger Template Format Suprema Proprietary
Application Advanced Access Control
User Access Mode Any One
Visitor Access Mode Any One
Consider For Attendance ☒
Alert Messages ☐
Consider For Visitor Pass Surrender ☐

Enter the MAC address of the door. The IP address will be displayed automatically once the device comes Online in Monitor.

To add Devices automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the “Auto Add New Devices” check-box. Once the device is connected in network, it will come Online in COSEC Monitor.



The Monitor Service must be running while adding the device to COSEC.

Once the device is configured, click the **Save** button to save the configuration.

To know more about configuring devices, click on the links for different tabs of Device configuration.

- [“Profile”](#)
- [“Enrollment”](#)
- [“Advanced”](#)
- [“Features”](#)
- [“Video Surveillance”](#)
- [“Special Functions”](#)
- [“Input/Output”](#)
- [“Additional”](#)
- [“Job Costing”](#)

- *“Assign Users”*
- *“Cafeteria”*
- *“Identification Server”*

Profile

This section enables the user to set up the basic profile for any new device. Setting up a door profile involves defining basic parameters to set up any door controller device.

To do this, On the **Device Configuration** page, select the **Profile** tab. The Profile can be configured in the following sections:

- “Basic”
- “Readers”
- “Access Settings”
- “General”

Basic

The **Basic** section for “NGT door” is shown below:

The screenshot shows the 'Device Configuration' window with the 'Basic' tab selected. The left sidebar lists various configuration sections: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main area displays the configuration for 'NGT Direct Door-1' (ID 16/10000). The 'Basic' tab includes fields for Sequence Number (1), Device (NGT Direct Door-Device-1), IP Address (192.168.104.84), MAC Address (00:1B:09:AB:CD:51), and an 'Active' checkbox (checked). Below these are 'Optional' settings: Site (2), RnD Site (RnD Site), Finger Template Format (Suprema Proprietary), Application (Advanced Access Control), User Access Mode (Any One), Visitor Access Mode (Any One), Consider For Attendance (checked), Alert Messages (unchecked), and Consider For Visitor Pass Surrender (unchecked).

Configure the following options as required:

- **Sequence Number** - This is a system generated sequence number for each new device.
- **Device**- Specify a name that can be assigned to the door. The Door ID is auto-generated by the system.
- **IP Address** - This is the IP address assigned to the door. Once the device connection is established, this field will automatically display the door IP address.
- **MAC Address** - Specify the MAC Address of the door.



MAC address of door is required while manually adding the door to the COSEC Monitor. Note the MAC address from the device when it is powered on.

- **Active** - Check the box to activate the device on the network.



To add the Device automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the **“Auto Add New Devices”** checkbox.

The device will be added automatically but make sure you enable the **Active** checkbox in order to connect the device to the network. Once the device is connected to the network, it will come online in COSEC Monitor.

The **Basic** page also offers an **Optional** tab which provides optional configurations as shown below:

- **Site** - Select the site to which this door is to be assigned from the site pick list window. Site is created from Devices> Masters> Site.
- **Finger Template Format** - Select the format as Suprema Proprietary or Suprema ISO according to which the templates will be enrolled. For globally setting the template format, you can set from Global policy.
- **Application** - Select the application type for which the device is to be used. The options are **Basic Access Control**, **Advanced Access Control** and **Cafeteria**. All devices set to **Cafeteria** will subsequently be available for Cafeteria configuration.



The available license is ACS and Application is set to Basic Access Control. If this ACS voucher exhausts, then while dispatching Basic Configuration of device, application type will be sent as 'Advance Access Control'.

- **User/Visitor Access Mode** - Defines the type and combination of credentials required to identify and validate a user/visitor at the Door Controller. Select the appropriate credential combination from the drop down list.

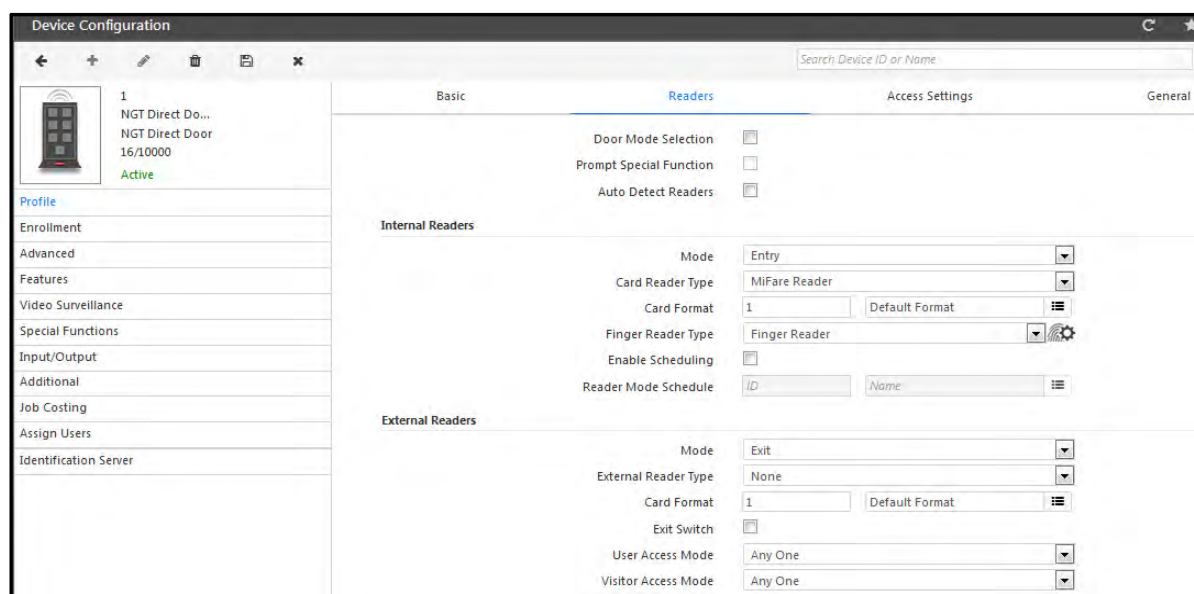
The options available are:

- Any one
 - Card
 - Card + Biometrics
 - Card + Biometrics + PIN
 - Card + PIN
 - Biometrics
 - Biometrics + PIN
 - Biometrics then Card
- **Consider for Attendance** - Select this checkbox if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as access control events.

- **Alert Messages** - Select this checkbox to enable the application to send alerts based on events from this door.
- **Consider for Visitor Pass Surrender:** Check the box to consider the selected device for visitor pass surrender. The Visitor can show his credential on this device to surrender the pass.

Readers

Readers are important hardware components in a biometric door device. They may be internal or external. This section enables the administrator to configure both internal and external readers for a door as shown.



The following parameters are available for configuration:

Door Mode Selection - If this option is enabled, then user will be prompted to select punch type as IN or OUT while punching on the device.

Eg: When a door is in Entry mode, your punches will always be in Entry side. But if you want to mark the punch in ext mode then you can select the door mode if “Door Mode Selection” is enabled.

If not selected, user will need to enable Scheduling to set reader mode of door as entry or exit as per user-defined schedules. For information on creating Reader Mode Schedules, **see Devices > Masters > Reader Mode Scheduler**.

Prompt Special Function- This will provide selection of special function on device screen and based on the selection of particular type of special function, job codes for JPC user will be prompted. This can be enabled only when “Door Mode Selection” is enabled.


Auto Detect Readers - Select this checkbox to enable auto detection of Readers on a door controller connected to the server.

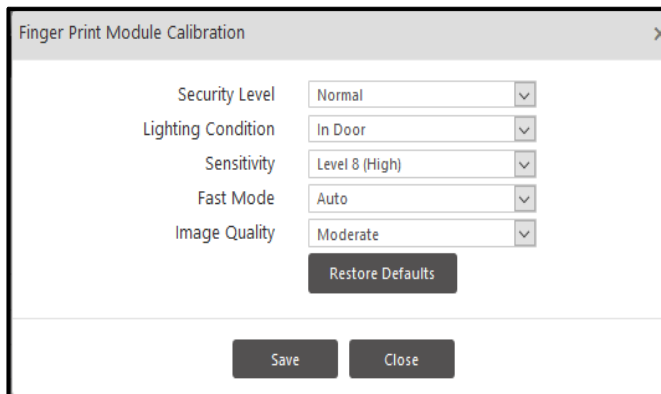
Internal Readers

This option allows the configuration of the Internal Reader for the selected door.

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop down list.
- **Card Reader Type;** Select the Card Reader Type from the following options:

- EM Prox Reader
 - HID Prox Reader
 - MiFare Reader
 - HID iClass-U Reader
 - HID iClass-W Reader
- **Card Format:** Select a card format to be applicable for internal readers of the device.
 - See Devices> Master> Card Format
 - Select the **Finger Reader Type** as **Finger Reader**.

Click the **FP Reader Configuration**  button to set the **Security Level**, **Lighting Condition**, **Sensitivity**, **Fast Mode**, **Image Quality** and **Restore Defaults** for the selected FP Reader as shown.



Finger Print Module Calibration

- **Security Level:** Security level specifies FAR (False Acceptance Ratio). Since FAR and FRR (False Rejection Ratio) is in inverse proportion to each other, FRR will increase with higher security levels.

For regular Time-Attendance system “**Normal**” level can be selected. For high security areas requiring complete or maximum matching of template, “**Highly Secure**” level must be selected. For approximate matching of template, “**Secure**” level can be selected.

- **Lighting Condition:** Optical sensors are sensitive to lighting condition. With this parameter, users can tune optical sensors to be adapted for their lighting environment. Select the In Door or Out Door option based on the device location.
- **Sensitivity:** Specifies sensor sensitivity to detect a finger. On high sensitivity, the module will accept the finger input more easily. Level 8 has the highest sensitivity.
- **Fast Mode:** Fast Mode parameter can be used to shorten the matching time with a little degradation of authentication performance. In typical cases, Fast Mode 1 is 2 to 3 times faster than Normal mode while Fast Mode 5 is 6 to 7 times faster than Normal mode. There is also an Auto mode.
- **Image Quality:** When a fingerprint is scanned, the module will check if the quality of the image is adequate for further processing. Image quality parameter specifies the strictness of this quality check. Strongest option might lead to higher number of finger rejections during the enrollment process.



Good quality of enrollment(around 70-75% quality) is recommended for proper identification of enrolled templates.

- Click on the **Restore Defaults** button to return the field values for this page to default values if needed.
- Click on the **Save** button.
- **Enable Scheduling:** Select this check box to **Enable Scheduling** to set reader mode of door as entry or exit as per user-defined schedules. For information on creating Reader Mode Schedules, **see Devices > Masters > Reader Mode Scheduler**.

External Readers

This option allows the configuration of the External Reader for the selected door.

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop down list.
- **External Reader Type:** Select the desired type of External Reader from the drop-down list.



Using PIN-W Reader; user can change their PIN number through devices.

- **Card Format** - Select a card format to be applicable for external readers of the device. This is applicable for all direct doors and all Panel doors.
- **Exit Switch** - Select this check box to enable the use of **Exit Switch**.
- **User/Visitor Access Mode** - Select the access mode from the options shown below:
 - Any One
 - Card
 - Biometrics
 - Card + Biometrics
 - Biometrics then Card
- **Access Control On Exit Mode** - Select this check box to enable the checking of the following access control policies on door when the external reader is in the 'exit' mode.
 - User enabled
 - User validity
 - Blocked user
 - Time Based Access Check
 - ASC
 - User Access Group

When this parameter is unchecked, all the following access control features will be checked on door (which are applicable and configured).

- User enabled
- Blocked user
- Time Based Access Check
- ASC
- User Access Group
- Deadman
- Door application mode
- Use count

- Mantrap
- Anti-pass back
- Panel Route access
- Smart card based route access
- 2-person
- Access mode
- Occupancy control
- Visitor escort rule

Access Settings

The **Access Settings** page appears as shown below:

- **Universal Time Zone** - Select the geographic time zone in which the DOOR will operate.
- **Time Format** - Specifies the time format to be displayed on Door Controller LCD display. The formats available are:
 - 24 Hours
 - 12 Hours

Select the relevant option from the drop down list as per the site requirements.

Auto Synchronize with NTP

If Date and time is to be automatically synchronized as per the **Preferred NTP Server** (predefined or user-defined NTP server address) selected by user, then you must enable **Auto Synchronize With NTP** checkbox.

Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from device webpage, which will be reflected on device display.

- When Auto Synchronization with NTP is disabled Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 1. You can specify the Preferred NTP server of your choice. In this case device will first try to get Date and Time from that server address.

If it does not get Date and Time in three tries; device will check from pre-defined NTP servers.

If you have entered one of the three pre-defined NTP servers(ntp1.cs.wisc.edu , time.windows.com , time.nist.gov); then device will first check that server first.

If it receives updated Date and Time then Updated Date and Time will be reflected on device web-page and display screen.

2. You can keep the Preferred NTP server as blank. In this case device will check for Date and Time from the first NTP server.
3. If user has manually entered Date and Time from web- page or Device Menu then those values of Date and Time will be reflected on device web-page and display screen.

In the case of the **Manual** option the administrator can manually update the time on the Door with that of the system time as and when required. This can be accomplished from the COSEC Monitor and control application.

- **Working Days** - Specify the days on which the default working hours should be applicable. Check the relevant boxes to specify the active days.
- **Working Hours (HH:MM)** - Define the default working hours in HH:MM format.
- **Holiday Schedule** - This section allows the administrator to assign up to four holiday schedules to the device by using the Holiday Schedule pick list.



If the same holiday schedule is configured for a user and for the door controller on which the user is assigned, then the user's attendance marking on this device, on any of the scheduled holidays will always be marked as a holiday.

General

The **General** page appears as follows. Enter all general details applicable to the device in this section.

The screenshot shows the 'Device Configuration' window for an 'NGT door'. The left sidebar contains a list of configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, and Assign Users. The main area is titled 'General' and contains the following settings:

- Mute Buzzer**: ☐
- Voice Guidance**: ☒
- Enable Display Messages**: ☒
- Display Message 1**: ☒
 - Schedule**: 00:00 to 11:59
 - Message**: Good Morning
- Display Message 2**: ☒
 - Schedule**: 12:00 to 15:59
 - Message**: Good Afternoon
- Display Message 3**: ☒
 - Schedule**: 16:00 to 20:59
 - Message**: Good Evening
- Display Message 4**: ☒
 - Schedule**: 21:00 to 23:59
 - Message**: Good Night

- **Mute Buzzer** - User can mute or unmute the door buzzer by checking or clearing the box respectively.
- **Voice Guidance** - Select this check box to enable Voice Guidance feature on door which will guide the user through voice.
- **Enable Display Messages** - This feature allows the user to enable display messages to be displayed on the door device. Upto 4 display messages can be configured for a door.
- **Display Message** - Enable each display message individually by selecting this checkbox.
- **Schedule** - For each message, the user needs to define the time period between which this message is to be displayed.
- **Message** - Enter the message to be displayed in this field. Maximum 21 characters allowed.
- **Multi-Language Support** - Select this check box to enable multi-language support for the selected device.

The **Display From** field shall display the reading order for the selected language.

Enrollment

The Enrollment page appears as shown below.

- **Enroll from Device** - Select this check-box to enable the enrollment of user from the door controller. When this check-box is enabled, 'Enroll User' special function on that device will get active as shown below.

If 'Enroll User' special function & 'Enroll From Device' check-box both are inactive in device configuration, then on activating 'Enroll User' special function, 'Enroll From Device' check-box will be enabled.

No.	Function Name	Active	JOB Selection	User Group	Card-1
1	Official Work - IN	Yes	Yes	All	
2	Official Work - OUT	Yes	Yes	All	
3	Short Leave - IN	Yes	Yes	All	
4	Short Leave - OUT	Yes	Yes	All	
5	Regular - IN	Yes	Yes	All	
6	Regular - OUT	Yes	Yes	All	
7	Break End	Yes	Yes	All	
8	Break Start	Yes	Yes	All	
9	Overtime - IN	Yes	Yes	All	
10	Overtime - OUT	Yes	Yes	All	
11	Enroll User	Yes	No	All	
12	Enroll Special Card	Yes	No	All	

- **Enrollment Mode** - Select the credential from the drop-down list that can be enrolled using the special function at the door. The options are **ReadOnlyCard**, **SmartCard**, **Biometrics** and **BiometricsThenCard**.
- **Template Per Finger** - This parameter displays the values as configured at the global level. This field is not user editable from this page.
- **Max Number of Fingers** - This parameter displays the values of the maximum number of fingers configured at the global level. This field is not user editable from this page.

- **Number of Fingers/Cards** - Select the number of cards or fingerprints to be enrolled based on the credential option selected in the Enrollment Mode parameter.
- **Enable Self-Enrollment** - Select this check-box to enable the self-enrollment feature on this door

Advanced

The Advanced tab allows the user to configure some advanced parameters such as access control settings, alarms and device timers.

To access this, After selecting the device, Select the **Advanced** tab from **Device Configuration** page. The advanced settings can be configured from following two sections:

- “Settings”
- “Timers”

Settings

The **Settings** page appears on your screen as shown below:

Device Configuration

Search Device ID or Name

1 NGT Direct Door
4/10000
Active

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Settings Timers

Generate Exit Switch Events ☐
Generate Invalid User Events ☒
Generate Sequential IN-OUT Events ☐
Two Credentials Required ☐
Show Pin ☒
Allow Exit When Door Lock ☐
Auto Relock ☐
Auto Relock Timer (Sec) 3
Alarms ☐
Tamper Alarm ☐
Enable Additional Security ☐ Disabled
Enable Smart Identification ☐
Access Level 8
Access Mode Card
Auto Acknowledge Alarm ☐
Auto Acknowledge Alarm (Sec) 10
Facility Code 1

Allow Access Through Mobile ☐
Mobile Entry Access Mode Mobile Only
Mobile Exit Access Mode Mobile Only

The following parameters are available for configuration:

- **Generate Exit Switch Events** - Select this checkbox to enable the door to generate events everytime the exit switch is used.

- **Generate Invalid User Events** - Select this checkbox to enable the door to generate events for invalid user inputs.
- **Generate Sequential IN-OUT Events** - Select this checkbox to generate user punches on device as the sequential IN-OUT events irrespective of whichever mode in which device is functioning.
- **Two Credentials Required**- Select this checkbox to enable the feature of verifying 2 credentials mandatorily for users allowed to By-pass finger/palm.
- **Show Pin**- Select this checkbox to display the characters of PIN when the PIN is entered on device.
- **Allow Exit when Door Lock** - Select this checkbox if users are to be allowed to exit even when the Door relay is in locked condition.
- **Auto Relock** - Select this checkbox to allow the door to relock immediately when the door status changes to close after normal open irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Relock Timer** - Specify the time in seconds for the Auto Relock operation.
- **Alarms** - Select this checkbox to set all door-based alarms as active.
- **Tamper Alarm** - Select this checkbox to activate the Tamper Alarm.
- **Enable Additional Security**- Select this checkbox to enable additional security at the selected Door Controller.
- **Additional Security Code** - Enter a code (ranging from 1 to 65535) in the field provided. Re-enter the code to confirm.



*Changing this value can affect the SI function. Click on the **Default Code** button to reset the **Additional Security Code** to the value set in the **Global Additional Security Code** field on the Global System Policy page.*

- **Enable Smart Identification** - Select this check box to enable this functionality at the selected Door Controller and select the **Access Level** and the **Access Mode** from the drop down list.
- **Auto Acknowledge Alarm** - Select this check box to enable the auto-acknowledgment of all alarms for this device.
- **Auto Acknowledge Alarm (sec)** - Set the time in seconds for the Auto Acknowledge Timer. The wait timer will start and on expiry of the timer, the alarm buzzer will stop automatically.
- **Facility Code** - Set a value for Facility Code to be set for access modes other than “Card”, if Facility Code is expected in Wiegand Output. This will be applicable to all direct doors.
- **Allow Access Through Mobile**- Check the box to allow the access to device using COSEC ACS App.

Allow Access Through Mobile	<input type="checkbox"/>
Mobile Entry Access Mode	Mobile Only
Mobile Exit Access Mode	Mobile Only

- **Mobile Entry/Exit Access Mode-** Select the entry and exit door access mode from the options of **Mobile Only** and **Mobile then Biometrics**.

Timers

This section allows the configuration of various types of pre-defined device timers which can trigger off specific responses. In COSEC, timers are often used to control door behaviour and for triggering alarms. The **Timers** page appears on your screen as shown below:

Timer	Value
Inter-Digit Wait Timer (Sec)	3
Multi-Input Wait Timer (Sec)	5
Door Open Pulse Timer (Sec)	5
Late-IN Early-OUT Active Timer (Min)	60

- **Inter-Digit Wait Timer (sec)** - Specify the time period in seconds between two key inputs on the device keypad. On expiry of this timer, the system considers the user input to be complete and is ready for the next input.
- **Multi-Input Wait Timer (sec)** - Specify the time in seconds for which system needs to wait for the second credential input from the user when more than one credential is to be used to grant access.



We recommend you to set the timer value as greater than or equal to 10 seconds to avoid access denial issues to users. This is applicable when the system reads the credentials (biometric) from the user's Smart Cards.

- **Door Open Pulse Timer (sec)** - Specify the time in seconds (3 to 99) for the door to be energized for a valid credential. If the opened door does not return to a closed state before the expiry of this timer, the door will generate a "Door Abnormal" alarm.
- **Late-IN Early-OUT Active Timer (min)** - Specify the time in minutes for which the Late-IN and Early-OUT special functions will remain active after being enabled at the Door Controller.

Door Access using QR code

The user can access the COSEC device using COSEC APTA installed in the mobile device. If the user has rights for COSEC APTA and the access to the device is allowed for the user, then he can use his mobile device to scan the QR code which constitute the details of the COSEC door.

There is icon for QR code on COSEC APTA application. Clicking that icon will open the camera in your mobile. Now you can show the mobile camera to scan the QR code. The COSEC door will get opened after verifying the security key and access policies of the user.

Steps to create a QR code

Step 1: Enter details in JSON format

```
{"version":"x","ip": "x.x.x.x","port":"x","pdid":"x","mode":"x"}
```

Valid values:

Field	Field range	Default Value	Remark
version	1-255	1	
ip	0.0.0.0-255.255.255.255	0.0.0.0	
port	0-65535	0	
pdid	0-255	0	If door is in direct door mode then, then PDID will be 0 If door is in panel door mode then, PDID will have values from 1-255
mode	0,1	0	0= for entry mode 1=for exit mode



Note:

Step1a. If door is in direct door mode enter IP & port of the direct door

b. If door is a panel door, then enter IP & port of the panel door and in the pdid specify the door id which is to be accessed.

Step 2: Encrypt the JSON string using key "matrix12" with simple DES/ECB mode.

Step 3: Encode the encrypted string using Base 64.

Step 4: Use this string to generate QR code through any third party software.

Features

The Features tab allows the user to enable certain Access Control features for a device



The Features tab is available only with the Access Control Module license.

To access this, After selecting the device, Select **Device Configuration> Features**. The access control features for the device can be set from the following two sections:

- "Set1"
- "Set2"

Set1

This page allows the configuration of three rules - **Absentee Rule**, **Occupancy Control** and **Use Count Control**. The page appears as shown below.

The screenshot shows the 'Device Configuration' window for 'Set1'. The left sidebar lists various configuration categories, with 'Features' currently selected. The main panel displays three rule configurations:

- Absentee Rule:** The 'Enable' checkbox is checked.
- Occupancy Control:** The 'Enable' checkbox is checked. Below it, 'Maximum Occupancy Limit' is set to 9, 'Minimum Occupancy Limit' is set to 1, and the 'Zero Occupancy' checkbox is checked.
- Use Count Control:** The 'Enable' checkbox is checked. Below it, 'Use Count Limit (Per minute)' is set to 5.

- **Absentee Rule** - Select this check box to **enable** this feature at the door. This rule sets the maximum number of days for non-use of a credential. On expiration of days limit, the user will be automatically blocked.
For configuring the rule *See Access Control> Absentee Rule*.
- **Occupancy Control** - Select this check box to **enable** the feature at the door and specify maximum number of users to be allowed within the controlled area after which a user exit is required to enable access to another user. Also specify the **Minimum Occupancy Limit** i.e. the minimum number of occupants the designated zone should have, and enable/disable the **Zero Occupancy** option to determine whether the designated zone should be allowed to be empty or not.
For configuring the rule *See Access Control> Occupancy Control*.
- **Use Count Control** - Select this check box to **enable** the feature at the door and specify the maximum number of uses per minute.
For configuring the rule *See Access Control> Use Count Control*.

Set2

This page allows the configuration of three rules - **First-IN User Rule**, **Anti-Pass-Back (APB)** and **2-Person Rule**. The page appears as shown below.

- **First-IN User Rule** - Select this check box to enable the feature at the direct door and select the First-In User group which would be valid at the door.
For configuring the rule See *Access Control> First- In User Rule> Assignment*
- **Anti-Pass Back (APB)** - Select this check box to enable the feature at the direct door.
For configuring the rule See *Access Control> Anti-Pass Back*
- **2-Person Rule** - Select this check box to enable the feature at the door and set the **wait time** in seconds after which the second person is allowed to punch on the door.
For configuring the rule See *Access Control> 2- Person Rule*

Video Surveillance

The Video Surveillance tab allows the user to configure parameters for video surveillance integration with the COSEC device.

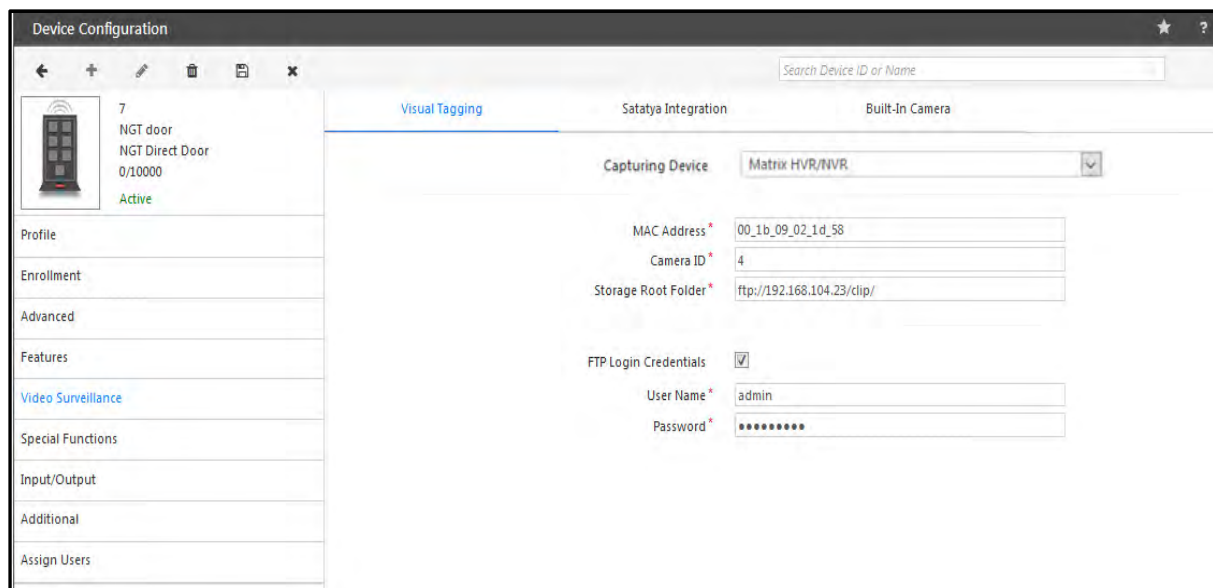
It is available in Basic License.

To access this, Go to **Device Configuration> Video Surveillance**.

- “Visual Tagging”
- “Satatya Integration”
- “Built-In Camera”

Visual Tagging

The COSEC application can interface with some supported hybrid and network video recording systems and grab images triggered by user events at the Doors. The **Visual Tagging** option enables the administrator to define the video recorder parameters. The **Visual Tagging** page appears as shown below.



The screenshot shows the 'Device Configuration' window with the 'Visual Tagging' tab selected. On the left, a sidebar lists various configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance (highlighted), Special Functions, Input/Output, Additional, and Assign Users. The main area displays settings for a device named '7 NGT door NGT Direct Door 0/10000', which is 'Active'. The 'Capturing Device' is set to 'Matrix HVR/NVR'. Other fields include 'MAC Address' (00_1b_09_02_1d_58), 'Camera ID' (4), 'Storage Root Folder' (ftp://192.168.104.23/clip/), and 'FTP Login Credentials' (checked). The 'User Name' is 'admin' and the 'Password' is masked with dots.



To view the user events and related images, go to **Admin > Views/Logs > Event View**. To know more about viewing events, refer to “Event View”.

The following parameters are available for configuration:

- **Capturing Device** - Select the video recording device type from the dropdown menu.

The compatible device types are:

- Matrix HVR/NVR
- Built-In Camera
- Milestone



For more information on integration with **Milestone** devices, refer to “[Milestone Integration](#)”.

- **MAC Address** - In the event of selecting the Matrix HVR/NVR, the administrator needs to specify the MAC address of the video recorder device using “_” (underscore) as the separator.
- **Camera ID** - Specify the camera number or camera ID for IP cameras. For analog cameras specify the camera number.
- **Storage Root Folder** - Specify the Root folder path or FTP Path where the uploaded images will be saved.
- **FTP Login Credentials** - Check this box to activate FTP login credentials for authentication.
- **Username** - Specify the FTP server username.
- **Password** - Specify the FTP server password.



Some COSEC devices do not support all the network connection options.

Satatya Integration

This functionality is available for configuration only when the Matrix HVR/NVR device type is selected as the **Capturing Device** (from *Visual Tagging*). It enables the configured COSEC devices to directly send commands to the SATATYA HVR/NVR devices as per the configuration on this page. The Satatya configuration page appears as shown below:

- **Integration type-** Select the integration type from the options of Wired and Network. In wired integration, door is physically connected with Satatya Device. In Network integration, connection can be by ethernet, wireless or broadband depending upon the COSEC device support.
- **Active-** Check the box to activate the connection.
- **Network Connection-** Select the Network connection from the options of Ethernet, Broadband, Wireless.
- **IP Address-** Specify the IP address of HVR/NVR if device is connected with Ethernet.
- **Port Number-** Specify the port number of HVR/NVR.
- **Name-**Specify a user friendly name for the integration function.
- **Active-** Check the Active box to enable the SATATYA integration functionality.
- **Schedule** - Specify a schedule for the function by specifying the start and the end time (*24 Hours format*) as well as checking the boxes against the applicable **days** of the week.
- **Event-** Select a COSEC event from the drop down list for which the resultant action is to be configured.

- **Mode-** Select the event mode from the options of Entry, Exit and Both from the drop down list wherever applicable.
- **Action-** Select the action for the Satatya device from the drop down list. The options available are:
 - Recording - Specify the duration in minutes.
 - Upload Image - This will be uploaded as per the ftp settings.
 - Video Pop-up - Specify the duration in seconds. The video pop up will be generated on the local client of Satatya device on the selected camera.
 - PTZ Preset - Specify the PTZ position number as defined on the SATATYA device.
 - Mail Image - Specify the email-ID.
- **Camera-** Select the relevant camera channels depending on the action selected.

Example1: For Access allowed event on COSEC Device, the video pop up of Camera 12 will be shown for 10 seconds.

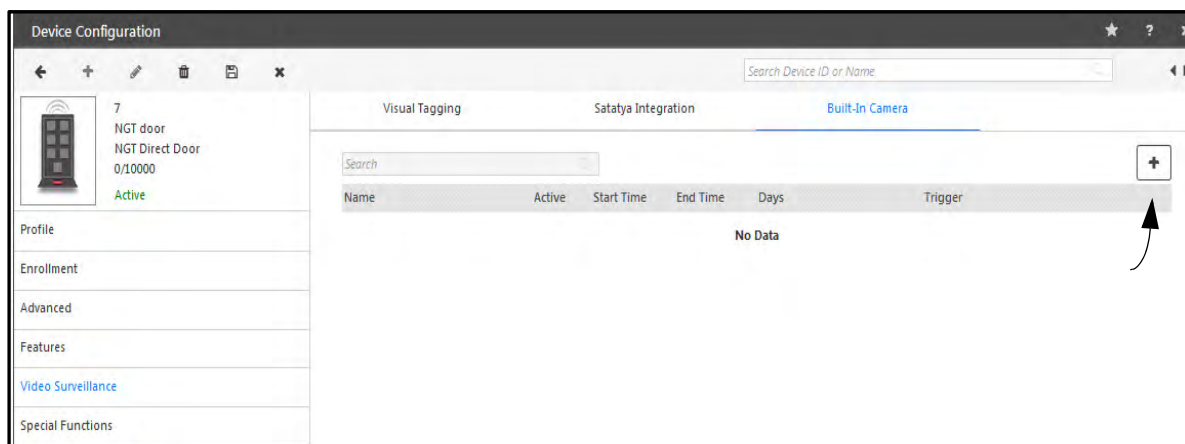
The screenshot shows a configuration window with the following fields and options:

- Event:** Access Allowed (dropdown menu)
- Mode:** Both (dropdown menu)
- Action:** Video Pop-Up (dropdown menu)
- Duration Sec.:** 10 (text input field)
- Camera:** A grid of checkboxes for cameras 1 through 24. Camera 12 is selected (checked).

- Click the **Add** button to finish the process of linking the event to the action. The user may configure another event-action linkage if required.

Built-In Camera

This functionality enables configuration and scheduling of image capturing using the in-built camera of an NGT door. The **Built-In Camera** configuration page appears as shown below.

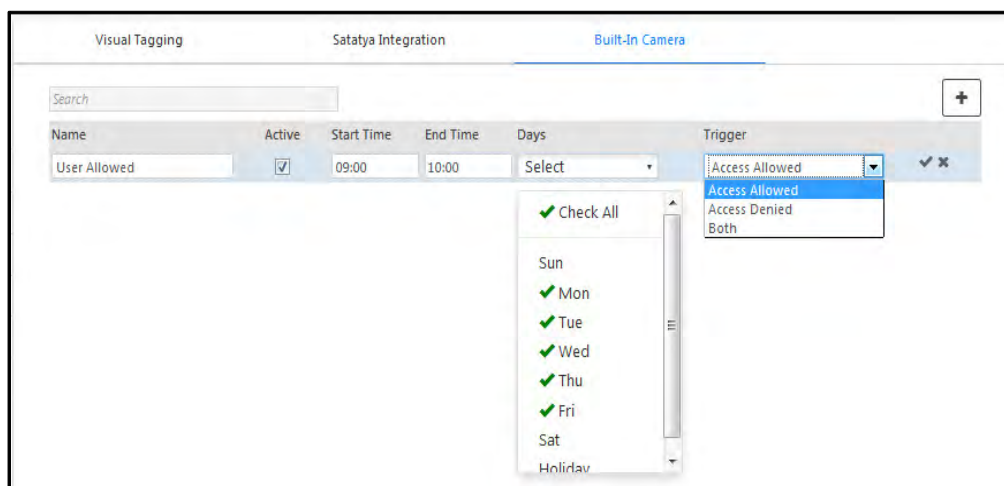


*This functionality is not available in the **Edit** mode for devices.*

The NGT Built-In Camera can be scheduled to capture images during scheduled periods and triggered by specific user events.

To configure a schedule click **Add** button as shown above.

- Specify the function **Name** and select the **Active** check box to enable it on the system.
- Specify a schedule by entering **Start** and **End Time**.
- Select the Applicable **days**.
- Select the user events from the drop down list by which the image capturing should be **triggered**. The options are Access Allowed, Access Denied and Both.



- Click the **OK** and **Save** button to save the schedule for the selected device.

Special Functions

To configure *Special Functions* for COSEC doors, refer to [“Special Functions”](#).

Input/Output

The Input/Output (I/O) configuration of a system determines how the output or response of a system is influenced by the input applied on it. In case of the COSEC Access Control System, the I/O configuration should enable the system to monitor and trigger a specific response to any changes in door state or event occurrences at the door device. This change of door state or occurrence of events may be considered as an input while the response or action that is generated by the system on detection of this input, may be defined as the output.



1. This functionality cannot be fully accessed in the Edit mode for a selected device.
2. This functionality is available only with the Access Control add-on module license.

To access this, After selecting the device, Select **Device Configuration> Input Output**. The Input Output parameters can be set from the following sections:

- “Configuration”
- “Linking”
- “Time Triggered”

Configuration

The **Configuration** section for a NGT Door appears as shown below.

The screenshot shows the 'Device Configuration' window for a 'NGT Direct Door'. The sidebar on the left lists various configuration sections: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, **Input/Output** (highlighted), Additional, Job Costing, Assign Users, and Identification Server. The main area has three tabs: 'Configuration' (selected), 'Linking', and 'Time Triggered'. Under the 'Configuration' tab, there are four sections: 'Door Sense' (Enable: checked, Supervised: unchecked, Sense Type: NC), 'Auxiliary Input' (Enable: checked, Supervised: checked, Sense Type: NO, Debounce Time (Sec): 5), 'Auxiliary Output' (Enable: checked, Output Wait Time (Sec): 2), and 'Accept External IO Linking' (Enable: unchecked).

The following parameters are available for configuration:

- **Door Sense** - The system by default can sense two states of a door - *Normally Open (NO)* and *Normally Closed (NC)* depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a *Door Abnormal* alarm.

Select the **Enable** checkbox to enable the system for such two-state monitoring.

Select the **Supervised** checkbox to enable the door for four-state monitoring where the door is also monitored for *door fault* and *door disconnection*. Specify the **Sense Type** as **NC** or **NO** (Default: NC).

- **Auxiliary Input** - Select the **Enable** checkbox option for Auxiliary Input (e.g. Smoke Detectors) depending on normal or supervised door state monitoring as described above.

Debounce Time (Sec) - Specify the Debounce time in seconds. Default value is 3 sec and range should be 0-99 sec. It defines the minimum time for which an input interface must be maintained in a given state before the system reports it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.

- **Auxiliary Output** - Select the **Enable** checkbox to enable Auxiliary Output (e.g. Fire Alarm) for the selected device. To set an additional waiting period before the Aux Output signal is sent, enter an **Output Wait Time (Sec)**.
- **Accept External IO Linking** - Select the Enable checkbox to enable device-to-device IO Linking i.e. input from one Direct Door can trigger output in another Direct Door.
- **Network Interface**- Select the interface option for IO linking with external devices. The options are
 - Ethernet
 - Wireless
 - Mobile Broadband

Linking

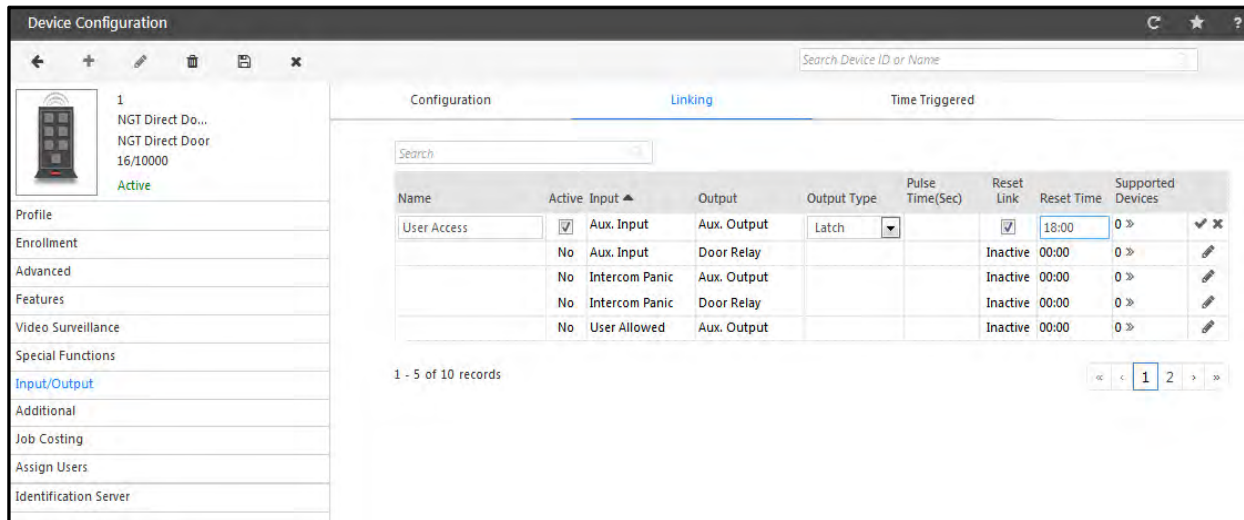
The **Linking** section appears as shown below.

The screenshot shows the 'Device Configuration' window with the 'Linking' tab selected. On the left, a sidebar lists various configuration options for a device named '1 NGT Direct Do...'. The main area displays a table of linking configurations. The table has the following columns: Name, Active, Input, Output, Output Type, Pulse Time(Sec), Reset Link, Reset Time, and Supported Devices. The table contains 5 rows of data, each representing a different linking configuration. The first row shows 'No' for Active, 'Aux. Input' for Input, 'Aux. Output' for Output, and 'Inactive' for Reset Link. The second row shows 'No' for Active, 'Aux. Input' for Input, 'Door Relay' for Output, and 'Inactive' for Reset Link. The third row shows 'No' for Active, 'Intercom Panic' for Input, 'Aux. Output' for Output, and 'Inactive' for Reset Link. The fourth row shows 'No' for Active, 'Intercom Panic' for Input, 'Door Relay' for Output, and 'Inactive' for Reset Link. The fifth row shows 'No' for Active, 'User Allowed' for Input, 'Aux. Output' for Output, and 'Inactive' for Reset Link. The table is paginated, showing '1 - 5 of 10 records'.

Name	Active	Input	Output	Output Type	Pulse Time(Sec)	Reset Link	Reset Time	Supported Devices
	No	Aux. Input	Aux. Output			Inactive	00:00	0 »
	No	Aux. Input	Door Relay			Inactive	00:00	0 »
	No	Intercom Panic	Aux. Output			Inactive	00:00	0 »
	No	Intercom Panic	Door Relay			Inactive	00:00	0 »
	No	User Allowed	Aux. Output			Inactive	00:00	0 »

The COSEC application supports the Input/Output Linking feature to activate an output port based on a trigger received from an input port on the same Direct Door. This option enables the administrator to define how an event or events (input port) will trigger an output on the selected door.

Select a Input-Output linking row and click edit button.



- **Name** - Specify a name for the new I/O linking program to be defined.
- **Output Type** - Specify the appropriate type of output from the following four options available in the drop down list:
 - **Pulse**: With this type of output, the user needs to define the Pulse time in seconds.
 - **Interlock**: With this option, the output follows the input. The relay output is triggered as long as the input is activated after which it returns to normal state.
 - **Latch**: With this option, it is denoted that the relay output will be in an energized condition for infinite period and needs to be reset manually.
 - **Toggle**: With this option, the output group toggles its state whenever an input group is activated.
- **Pulse Duration (sec)** - For a *Pulse* output type, specify the pulse duration in seconds.
- **Active** - Select this checkbox to activate this linking program.
- **Reset Link**- Select this checkbox to reset the link automatically after a defined time period.
- **Reset Time**- Enter the time period in hh:mm format at which the link will get reset automatically. Suppose, an IO Link gets activated on 21/04/2017 at 15:00. And Reset Time is set as 18:00. When Device Time is 18:00 then that IO link will get reset.
- **Supported Devices** - All devices supported for external IO Linking will appear in this picklist for selection. Upto 255 external devices can be added by the administrator.
- Click the **OK** button and **Save** the configuration.

Time Triggered

On the **Input Output** page, select the **Time Triggered** section as shown.

Function Name	Active	Time	Duration(Sec)	Days	Output
Siren Activate	<input checked="" type="checkbox"/>	00:00	10	Select	Aux O/P

- ✓ Check All
- ✓ Sun
- ✓ Mon
- ✓ Tue
- ✓ Wed
- ✓ Thu
- ✓ Fri
- ✓ Sat
- ✓ Holiday

This functionality enables the user to control the activity of an Output without manual intervention. The time triggered functions are used for activating events like door unlock and siren activation that are set as per the start time and for the configured time duration. This functionality is designed to energize outputs for predefined periods at the configured time. The COSEC access control system supports up to 20 Time Triggered functions on a Direct Door.

Function Name	Active	Time	Duration(Sec)	Days	Output
Siren Activate	Yes	00:00	10	Su Mo Tu We Th Fr Sa Ph	Aux O/P

Additional

This section lists some additional configurations that can be enabled for door controllers.

To access these configurations, Go to **Device Configuration > Additional**

The Additional parameters can be set from the following sections:

- “Greetings”
- “Daylight Saving”

Greetings

This functionality enables the administrator to define greeting messages triggered by user access events at the NGT DIRECT DOORS. The greeting messages can be in predefined visual as well as audio formats.

The screenshot shows the 'Device Configuration' window for an NGT door. The left sidebar lists various configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, and Assign Users. The 'Greetings' tab is selected. The main configuration area includes a 'Greeting Type' dropdown set to 'Custom Message', an 'Active' checkbox checked, and fields for 'Message Line1' (Welcome to Matrix), 'Message Line2' (Have a Good Day), and 'Date' (08/12/2016). Below these is an 'AV' section with 'Image' (Keep Smiling) and 'Audio' (Sunshine Piano) dropdowns. A 'User Selection' section is also present. At the bottom, there are 'Add' and 'Cancel' buttons, a search bar, and a table with columns: Greeting Type, Message 1, Message 2, AV, Active, and a delete icon. The table currently shows 'No Data'.

Configure the following options as required:

- Select the **Greeting Type** from the drop down list. The options available are:
 - Custom Message
 - Birthday Message
- Check the **Active** box to activate the greeting message on the selected door.
- Specify the message in alphanumeric format in the space provided against Message Line1 and Message Line2.
 - In the event of defining a *Custom Message*, select the **Date** on which the message is to be displayed by clicking on the date picklist button. In the event of defining a *Birthday Message*, date selection will be disabled.
- Expand the **AV** panel and select a predefined image and audio file from the respective drop down lists.
- When defining a *Custom Message*, select all users or specific users from the user picklist. This field will be disabled in the event of a *Birthday Message* and all users will be selected by default.
- Click the **Add** button to save the settings on the door.

Greeting Type	Message 1	Message 2	AV	Active	
Custom Message	Welcome to Matrix	Have a Good Day	AV	Yes	

Daylight Saving

Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. COSEC doors can be configured to be compatible with this procedure keeping the RTC of the system updated with such changes.

The **Daylight Saving** configuration can be done in 2 ways i.e. Day-Month wise or Date-Month wise.

- Select the **DST Type** as Day-Month wise or Date-Month wise. The **Disable** option when selected, disables the application of DST on the system time.
- On selection of the **Day-Month wise** option, the DST is set by the day of the month on which clock needs to be forwarded and reverted back to normal. Set the month, week number, day of the week, and time for both the **Forward Clock** and **Backward Clock** as shown.

- On selection of the **Date-Month wise** option, the DST is set by date of the month on which clock needs to be forwarded and reverted back to normal. Define the **Time Period** for the date-month wise DST

settings in *24-hours* format, and specify the **Month**, **Date** and **Time** for the **Forward Clock** and the **Backward Clock** as shown.

This DST Setting implies that on 1st sunday of November at 09:00 hours, the clock will be forwarded by 08:00 hours. And on 1st sunday of January at 10:00 hours, the clock will be reversed or backwarded by 08:00 hours.

- Click the **Save** button.

Job Costing

When user punches on any device, there will be an option to select the Job Code on which the user is working. Job Costing enables the admin to show or hide Job Code selection on device. It also enables the admin to assign default jobs on device.

Job Code	Name	Assignment Start	Assignment End	
INV	Inventory	22/05/2017	30/06/2017	
LAB	Labelling	22/05/2017	07/06/2017	
PSD-R	PSD Review	22/05/2017	17/06/2017	
PSD-S	PSD Study	22/05/2017	31/05/2017	
SAD	SAD study	08/05/2017	30/06/2017	

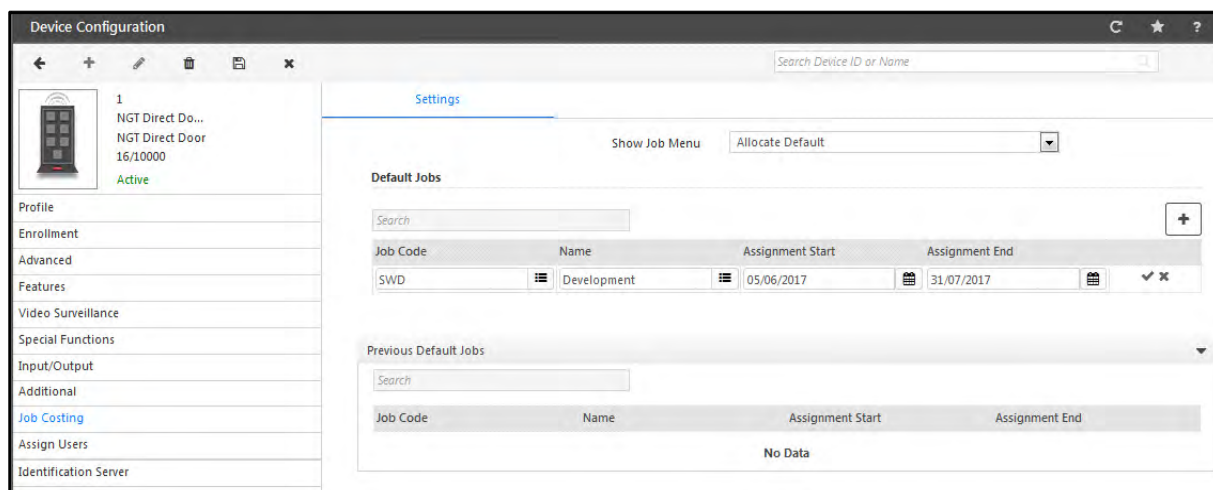
Show Job Menu: Select the option as **Show List** or **Allocate Default**.

When **Show List** is selected; then multiple jobs can be assigned to the device. The user can select the relevant job code while punching on the device. His job hours will be recorded for that job code.

- **Assign Jobs:** Select the Job group or individual job from the picklist. Then click on Save button. The jobs will be listed to the grid.

When **Allocate Default** is selected; then default jobs for the device can be selected.

- **Default Jobs:** Click Add button to add the default job on the door. Then click on the Job picklist button and select the job to be assigned to the device. The Job costing user can directly punch on this door for starting the default job.



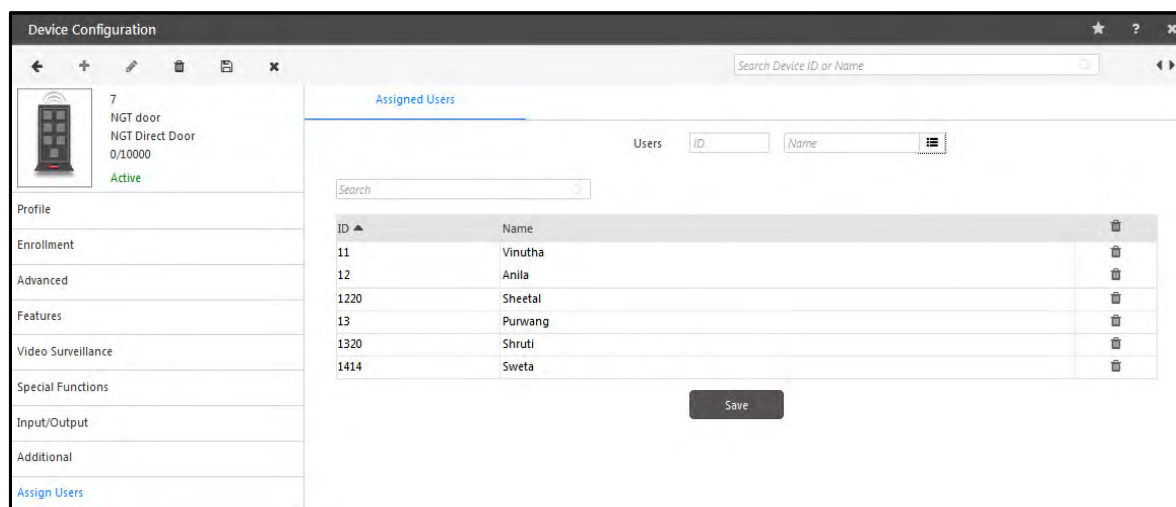
Finally click on **Save** button to save the configuration.

When the assignment date of the default job gets elapsed, then the respective job will be listed in **Previous Default Jobs** section.

Assign Users

To the configured device, you can select and assign the users.

Click the picklist button and select the users.

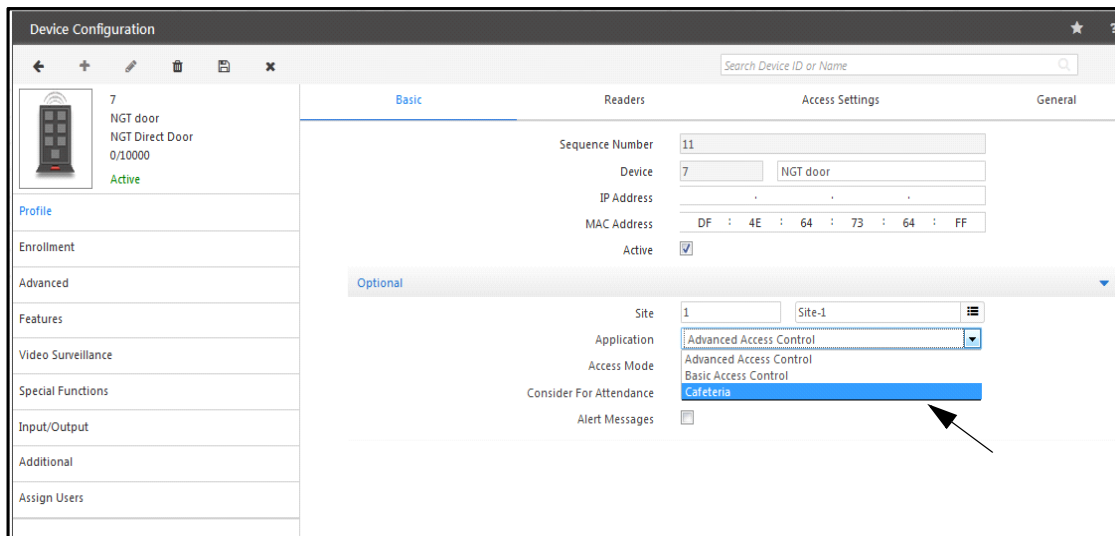


- Click the **Save** button to assign all the added users to the selected door.

Cafeteria

The COSEC system enables the user to configure devices which will be used by the Cafeteria management module.

To configure a door for Cafeteria application, select **Cafeteria** option in Device Profile> Basic> Application as shown below.



The Cafeteria tab will appear in Device Configuration page.

Select **Device Configuration> Cafeteria> Settings**

Settings

The Cafeteria configuration for NGT Door is shown as below.

The screenshot shows the 'Device Configuration' window for a device named 'NGT Direct Door'. The left sidebar contains a list of configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, Cafeteria (highlighted), and Identification Server. The main area is titled 'Settings' and contains a 'Menu' section with a 'Consecutive Transaction Delay (Sec)' field set to 0. Below this is the 'Printer Settings' section, which includes a 'Printer' dropdown menu (set to 'None'), a 'Connection Type' dropdown menu (set to 'RS232'), a 'Baud Rate' dropdown menu (set to '115200'), and text input fields for 'Company Name', 'Company Address', and 'Punch Line'. There is also an 'Exclude Price-Cost From Coupon' checkbox, which is currently unchecked.

- **Consecutive Transaction Delay (Sec):** Enter the time interval between two transactions, wherein any user transaction would be restricted.

Printer Settings

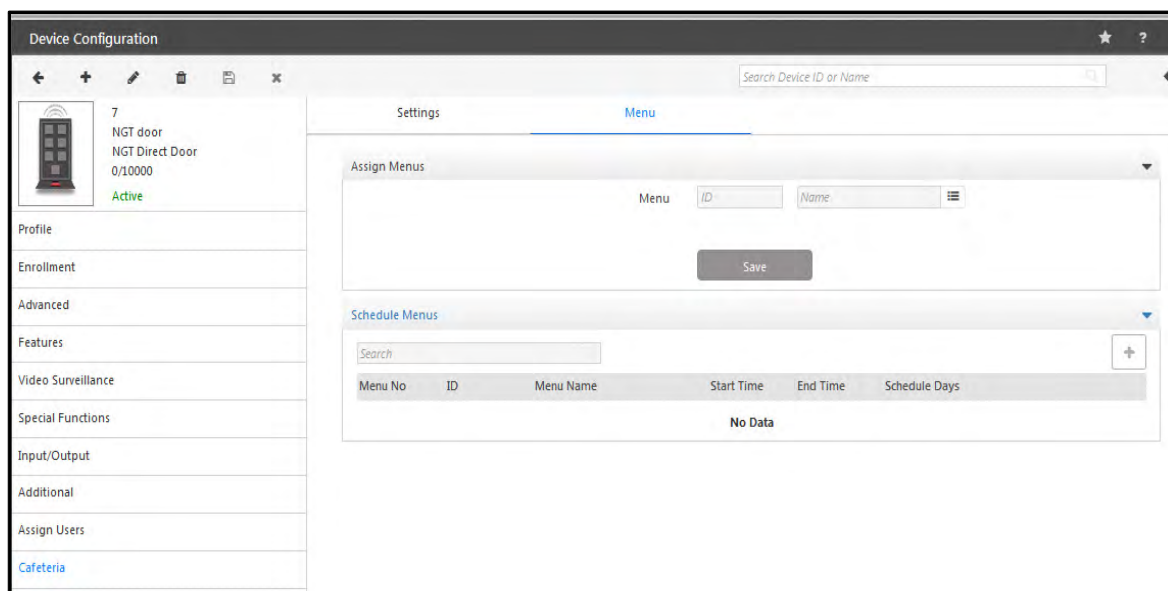
- **Printer:** Select the printer from the dropdown list based on the site requirements.
- **Connection Type:** Select the printer connection type from the drop down list. The options available are:
 - RS232 (serial)
 - USB
- **Baud Rate:** In the event of a serial printer, select the appropriate baud rate from the drop down list.
- Specify the **Company Name**, **Company Address** and the **Punch Line** as per the site requirements. These details will be printed on the receipt dispensed from the selected printer.
- Select the **Exclude Price-Cost From Coupon** check box if you want to exclude the price from the coupon.

Menu

COSEC allows the administrator to assign one or more cafeteria menus (Menu 1, Menu 2, Menu 3... upto 99.) to a device. These can be configured by selecting pre-defined menus from the Menu picklist.

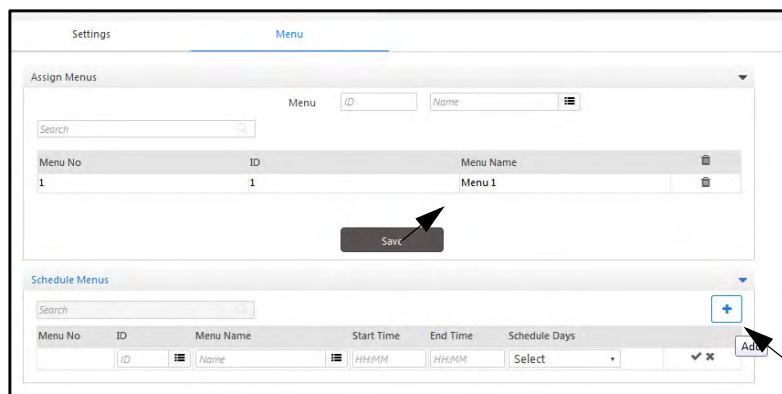


The Menu is created from Cafeteria module.



The Menu can be scheduled from Cafeteria module and is displayed in “Schedule Menus” in above screenshot.


If you have to assign another menu and schedule it on the door then select the Menu from the picklist. The Menu will be shown in the grid as shown below.



Now to schedule the menu click **Add** button as shown above.

Then select the menu to be scheduled from the **ID** picklist. Specify the **Start** and **End time** for which the Menu will be active and is available to users on the selected door. Select the **days** for which this menu will be available i.e. scheduled on the door.

Then click **OK** and **Save** the Menu schedule on the door.

 *Two Menus cannot be scheduled for same timing.*

Identification Server

This tab enables the selected device to be assigned to a pre-defined Identification Server. Device has a limited memory capacity for storage of templates so we need Identification Server which will store the more number of templates and respond to device when asked for identification.

For more information on Identification Servers, See *Admin> System Configuration> Identification Server Configuration*.

To access these configurations,

- On the **Device Configuration** page, select the **Identification Server** tab.

- **Enable Identification On Server:** Select the checkbox to enable the identification of palm/finger templates on this device.

- **Identification Server:** Select an Identification Server using the picklist button to which the device is to be assigned. The configuration of server is done from **Admin module > System Configuration > Identification Server Configuration**.
- **Server Address:** It displays the IP Address of the selected Identification Server.

- **Configure Alternate Server Address:** Enable this check-box to configure external IP address of Identification Server.
 - **Server Address:** Enter the external network IP address which will be used for accessing identification server.
- **TCP Listening Port:** Enter the TCP port number. The default port number is 11005.
- **Network Interface:** Select the interface through which the server is to be connected to the device. The options are: Ethernet, Wireless and Mobile Broadband.
- **Enable Finger Smart Identification:** For all other supported doors, select the checkbox to enable fingerprint templates identification through Identification Server.
- **Identification Time-Out Duration (Sec):** Specify the duration in seconds after which the fingerprint template identification will get time out.

Example: If 5 seconds is specified, then the identification server will try to identify the template till 5 seconds and if not found then it will show time-out to the user.
- **Auto Send Enrolled Templates:** Select the checkbox to enable any enrolled templates to be saved both on the COSEC database as well as saved locally on the configured Identification Server. This enables prompt identification of user on enrollment.
- **Default Biometric Group No.:** Specify the default biometric group number to be assigned to the device. It is a number allotted to a device to be assigned to the Identification Server. This enables the Identification Server to match the template against only those devices that belong to the corresponding biometric group. This reduces the false detection as well time to search template.

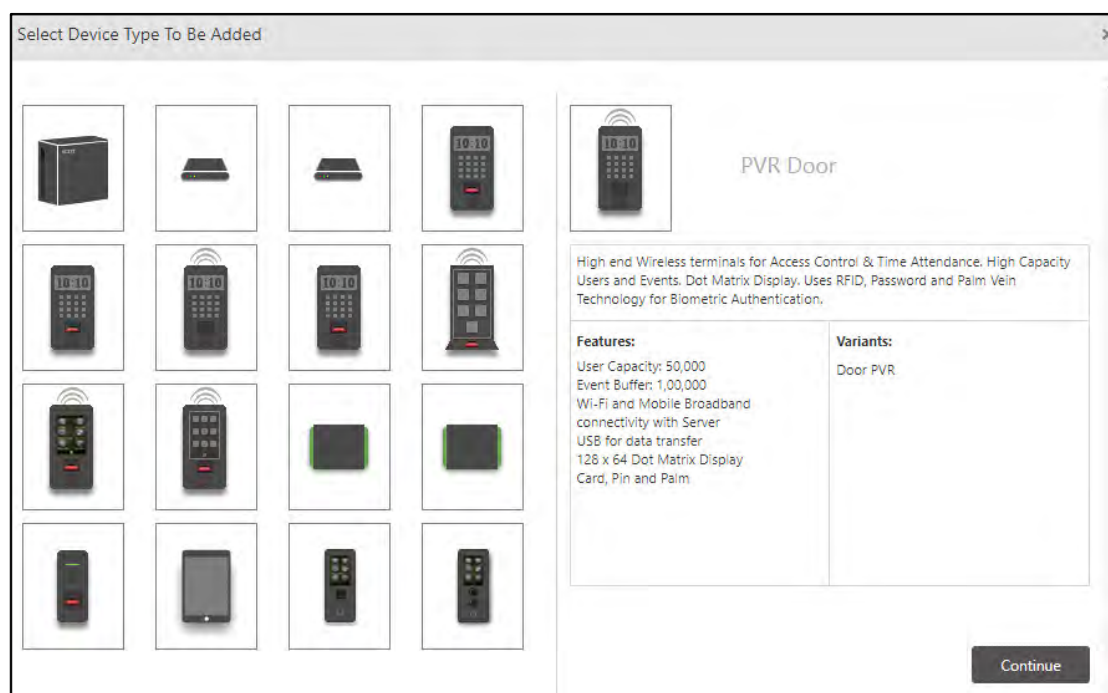
PVR Door

COSEC PVR Door uses a contactless technology that reads internal vascular pattern of the user palm and gives accurate result to provide utmost security.

PVR Door can be connected as **Direct Door** as well as **Panel Door**.

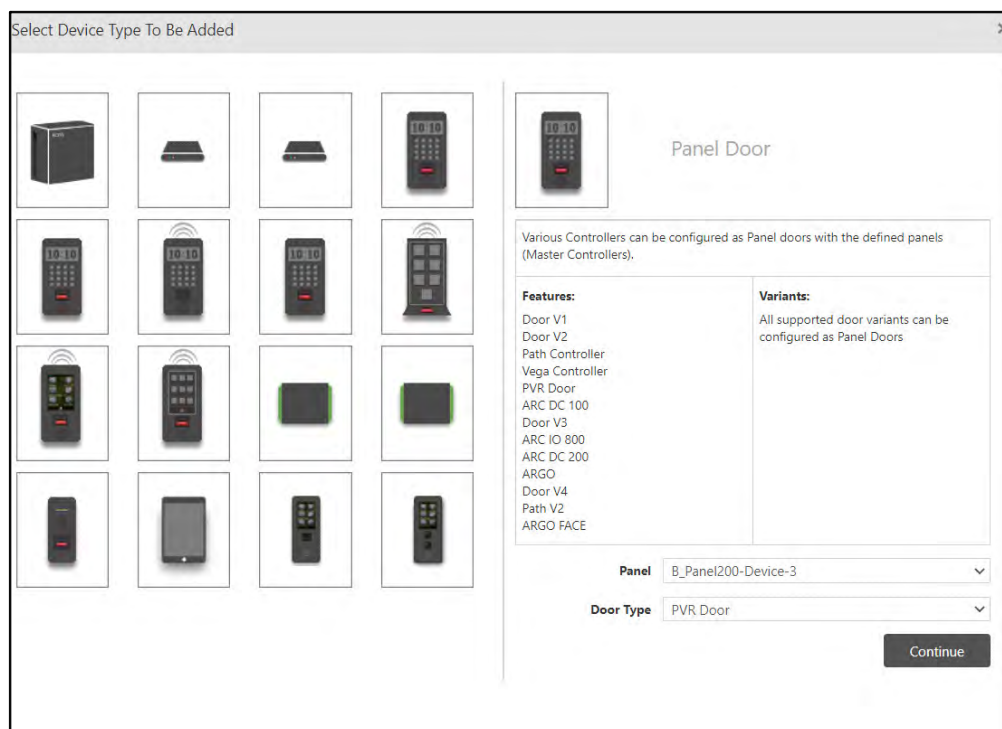


Click the PVR Door device from the Device List to add it as a **Direct Door**.



OR

Click Panel Door to add PVR Door device as a **Panel Door**.

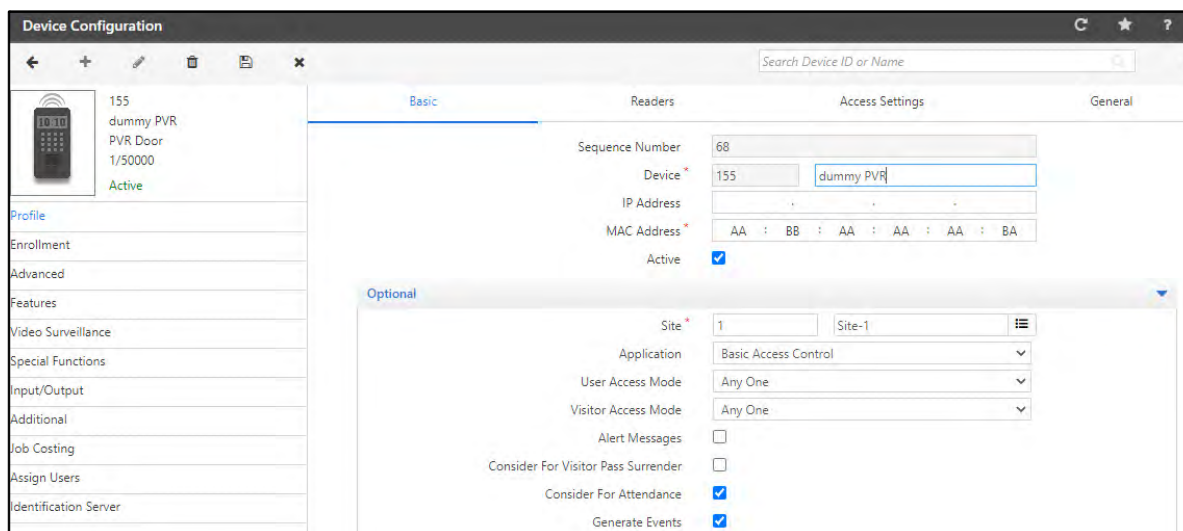


Panel: Select the desired Panel from the drop-down list with which you wish to connect the Door.

Door Type: Select **PVR Door** from the drop-down list.

Click **Continue**.

The **Device Configuration** page for PVR Door appears.



To add devices automatically, click **Admin Module > System Configuration > Global Policy > Device**. Select the **Auto Add New Devices** check box. Once the device is connected in the network, it comes online in COSEC Monitor.



While adding the device to COSEC Server, make sure the COSEC Monitor Service is running.

To know more about configuring devices, click on the links for different tabs of Device configuration.

- [“Profile”](#)
- [“Enrollment”](#)
- [“Advanced”](#)
- [“Features”](#)
- [“Video Surveillance”](#)
- [“Special Functions”](#)
- [“Input/Output”](#)
- [“Additional”](#)
- [“Job Costing”](#)
- [“Assign Users”](#)
- [“Identification Server”](#)

Profile

Setting up a door profile involves configuring basic parameters to set up any door controller device. This section enables the user to set up the basic profile for any new device.

To do this, on the **Device Configuration** page, click the **Profile** tab in the left pane.

The screenshot shows the 'Device Configuration' window with the 'Profile' tab selected in the left sidebar. The main area is divided into 'Basic' and 'Optional' sections. The 'Basic' section includes fields for Sequence Number (68), Device (155), IP Address, MAC Address (AA : BB : AA : AA : AA : BA), and an Active checkbox (checked). The 'Optional' section includes Site (1), Application (Basic Access Control), User Access Mode (Any One), Visitor Access Mode (Any One), Alert Messages (unchecked), Consider For Visitor Pass Surrender (unchecked), Consider For Attendance (checked), and Generate Events (checked).

To configure the Profile parameters, click the following links:

- “Basic”
- “Readers”
- “Access Settings”
- “General”

Basic

Click **Basic** tab. The **Basic** page appears.



Sequence Number, Device, IP Address, MAC Address and Active are applicable for both Direct Door and Panel Door.

For PVR as a **Direct Door**.

Configure the following parameters:

- **Sequence Number:** This is a system generated sequence number for each new device.
- **Device:** Specify a name that can be assigned to the door. The Door ID is auto-generated by the system.
- **IP Address:** This is the IP address assigned to the door. Once the device connection is established, this field will automatically display the door IP address.
- **MAC Address:** Specify the MAC Address of the door.



MAC address of door is required while manually adding the door to the COSEC Monitor. Note the MAC address from the device when it is powered on.

- **Active:** Select the check box to activate the device in the network.



To add the Device automatically, click **Admin Module > System Configuration > Global Policy > Device**. Select the **Auto Add New Devices** check box.

*The device will be added automatically but make sure you enable the **Active** check box in order to connect the device to the network. Once the device is connected to the network, it will come online in COSEC Monitor.*

Click the **Optional** collapsible tab, to configure the following parameters:

- **Site:** Select the site to which this door is to be assigned from the picklist. Site is created from **Devices > Masters > Site**.
- **Application:** Select the type of application for which the device is to be used from the drop-down list options— **Basic Access Control** or **Advanced Access Control**.
- **User/ Visitor Access Mode:** This defines the type and combination of credentials required to identify and validate a user at the Door Controller. Select the appropriate credential combination from the drop-down list.
 - Any one
 - Card
 - Card + PIN
 - Card + Biometrics
 - Card + PIN + Biometrics
 - Biometrics
 - Biometrics + PIN
 - Biometrics + Group
 - Biometrics then Card
 - Card then Biometrics
 - None
- **Alert Messages:** Select this check box to enable the application to send alerts based on events from this door.
- **Consider for Visitor Pass Surrender:** Select this check box to consider the device for visitor pass surrender. The Visitors can show their credentials on this device to surrender their passes.
- **Consider for Attendance:** Select this check box if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as Access Control events.
- **Generate Events:** By default, this check box is selected. Click to disable, if the server is not required to receive any events from this device.

For PVR as a **Panel Door**.

Basic	Readers	General
Sequence Number <input type="text" value="9"/>		
Device * <input type="text" value="6"/> <input type="text" value="Dummy PVR_PD"/>		
IP Address * <input type="text" value="192"/> . <input type="text" value="138"/> . <input type="text" value="103"/> . <input type="text" value="151"/>		
MAC Address * <input type="text" value="00"/> : <input type="text" value="1B"/> : <input type="text" value="2C"/> : <input type="text" value="CD"/> : <input type="text" value="46"/> : <input type="text" value="BA"/>		
Active <input checked="" type="checkbox"/>		
Optional		
Site * <input type="text" value="1"/> <input type="text" value="Site-1"/>		
Consider For Attendance <input checked="" type="checkbox"/>		
Alert Messages <input checked="" type="checkbox"/>		
Access Zone <input type="text" value="Zone-1"/>		
Access Cluster <input type="text" value="Cluster-1"/>		
Door Group <input type="text" value="None"/>		
Auto IP Assignment <input checked="" type="checkbox"/>		

Click the **Optional** collapsible panel, to configure the following parameters:

- **Site:** Select the site to which this door is to be assigned from the picklist. Site is created from **Devices > Masters > Site**.
- **Consider for Attendance:** Select this check box if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as Access Control events.
- **Alert Messages:** Select this check box to enable the application to send alerts based on events from this door.
- **Access Zone:** Select the desired Access Zone to be assigned to the door from the drop-down list.
- **Access Cluster:** Select the desired Access Cluster to be assigned to the door from the drop-down list.
- **Door Group:** The Door Group drop-down includes the list of all configured Door Groups on the corresponding Panel. An additional option as 'None' is available and selected by default. Select the desired Door Group to be assigned to the door from the drop-down list.
- **Auto IP Assignment:** Select this check box to assign the IP to the Panel Door from the device webpage.



Access Zone is configured while configuring Panel200.

Readers

Readers are important hardware components in a biometric door device. They may be internal or external. This section enables the user to configure both internal and external readers for a door.

Click the **Readers** tab. The **Readers** page appears.

Member No	Card Format	Configurable Bits
1	Default Format	0

Configure the following parameters:



Door Mode Selection, Prompt Special Function and Auto Detect Readers are applicable for Direct Door only.

- **Door Mode Selection:** Select this check box if you wish the user to select the punch type as IN or OUT while punching on the device.

For example, when a door is in Entry mode, your punches will always be in Entry side. But if you want to mark the punch in Exit mode, you can select the door mode if **Door Mode Selection** check box is enabled.

If not selected, the user needs to enable Scheduling to set reader mode of door as entry or exit as per user-defined schedules. For information on creating Reader Mode Schedules, refer **Devices > Masters > Reader Mode Scheduler**.

- **Prompt Special Function-** Select this check box to enable the selection of special functions on device screen, based on the selection of particular type of special function. This can be enabled only when **Door Mode Selection** is enabled. For more details, refer to “Special Functions”.
- **Auto Detect Readers:** Select this check box to enable the auto detection of Readers on a door controller connected to the server.

Internal Readers

This option allows the configuration of the Internal Reader for the door.

Click **Internal Readers** collapsible panel and configure the following parameters.

Internal Readers

Mode: Entry

Card Reader Type: EM Prox Reader

Search

Member No ▲	Card Format	Configurable Bits	
1	Default Format	0	
2	Format 1	64	
3	Format 2	32	

Palm Reader Type: Palm Vein Reader

Enable Scheduling: ☒

Reader Mode Schedule: ID Name



Mode, Card Reader Type and Card Format are applicable for both Direct Door and Panel Door.

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop-down list.
- **Card Reader Type:** Select the desired Card Reader Type from the drop-down list.
- **Card Format:** Single or multiple card formats can be assigned to the readers of the door. The default card format is assigned to device as shown in the grid. If no other card format is assigned to device, then this default format will be applied.



The formatting of card is described in Devices> Master> Card Format.

Multiple Card Format

- To assign multiple card formats to device click **Add**. Then click the picklist to select the card format and click **OK** to save the format.

Search

Member No ▲ Card Format Configurable Bits

1 Default Format 0

Search

Member No ▲ Card Format Configurable Bits

1 Default Format 0

- Similarly, you can add maximum 5 card formats. When the card format is saved, the configured bits of that format as configured from **Masters > Card Format** will be displayed here. Multiple Card format

configurations will be sent to the door separated by **Format ID** that is 'Member No.' along with all other format related parameters.

Member No	Card Format	Configurable Bits
1	Default Format	0
2	Format 1	64
3	Format 2	32



Palm Reader Type is applicable for both Direct Door and Panel Door.

- **Palm Reader:** Select the **Palm Reader Type** as **Palm Vein Reader**.

Click **Palm Reader Configuration**  to set the Palm identification configuration.

The **Palm Reader Configuration** pop-up appears.

Configure the following parameters:

- **Security Level:** Select the desired Security Level to be set for the Palm Reader Configuration from the drop-down list options—Normal, Highest, High, Low, Lowest. You can select **Normal** level for regular Time and Attendance system. You must select **High/Highest** level for high security areas that require complete or maximum matching of template. You can select **Low/Lowest** level for approximate matching of template.
- **Palm Matching Timeout:** Specify the duration in seconds for which the reader will match and identify the Palm template, after which it will show timeout.
- **Palm Template Quality:** Select the desired Palm Template Quality from the drop-down list options—Good, Moderate, Poor. You can select **Good** quality for Access Control system required in high security areas. You can select **Moderate** quality for normal Time and Attendance system.

Click **Restore Defaults**, to return the field values for this page to default values, if required.

Click **Save** to save the changes or **Close**, if you wish to discard the changes.



Enable Scheduling and Reader Mode Schedule are applicable for Direct Door only.

- **Enable Scheduling:** Select the check box to enable the automated control of an Internal Reader. This will set the reader mode of door as Entry or Exit as per user-defined schedules.
- **Reader Mode Schedule:** Select the Schedule for the Reader Mode which is to be assigned to this door from the picklist. With this the same reader can be configured to function both in Entry as well as Exit mode based on scheduled timings.

External Readers

This option allows the configuration of the External Reader for the door.



Mode, External Reader Type, Card Format and Exit Switch are applicable for both Panel Door and Direct Door.

Click **External Readers** collapsible panel and configure the following parameters.

Member No	Card Format	Configurable Bits
1	Default Format	0
2	Format 1	64

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop-down list.
- **External Reader Type:** Select the desired Card Reader Type from the drop-down list.



If you are using PIN-W Reader; users will be able to change their PIN number from the devices.



User Access Mode, Visitor Access Mode and Access Control on Exit Mode is applicable for Direct Door only.

- **Card Format:** Single or multiple card formats can be assigned to the readers of the door. The default card format is assigned to device as shown in the grid. If no other card format is assigned to device; then this default format will be applied. This is applicable for all Direct Doors and all Panel Doors. For details, refer ["Multiple Card Format"](#).
- **Exit Switch:** Select this check box to enable the use of **Exit Switch**.

- **User/Visitor Access Mode:** Select the desired **Access Mode** from the drop-down list options—Any One, Card, None, BLE.
- **Access Control On Exit Mode:** Select this check box to enable the checking of the following access control policies on door when the External Reader is in the **Exit** mode.
 - User enabled
 - User validity
 - Blocked user
 - Time Based Access Check
 - ASC
 - User Access Group

Access Settings



Access Settings are applicable for Direct Door only.

Click the **Access Settings** tab. The **Access Settings** page appears.

Configure the following parameters:

- **Universal Time Zone:** Select the geographic time zone in which the door will operate from the drop-down list.
- **Time Format:** Select the time format to be displayed on Door Controller LCD display from the drop-down list options —24 Hours or 12 Hours.
- **Auto Synchronize with NTP:** If Date and time is to be automatically synchronized as per the **Preferred NTP Server** (predefined or user-defined NTP server address) selected by user, then you must select the **Auto Synchronize With NTP** check box.

Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from device web page, which will be reflected on device display.

- When **Auto Synchronization with NTP** is disabled, **Preferred NTP Server** field will be disabled.
- When Auto Synchronization with NTP is enabled,

- You can specify the **Preferred NTP Server** of your choice. In this case, the device will first try to get Date and Time from that server address.

If it does not get Date and Time in three tries, device will check from pre-defined NTP servers.

If you have entered one of the three pre-defined NTP servers(ntp1.cs.wisc.edu, time.windows.com, time.nist.gov), then device will first check that server first.

If it receives updated Date and Time, then that Updated Date and Time will be reflected on device web page and display screen.

- You can keep the Preferred NTP Server as blank. In this case device will check for Date and Time from the first NTP server.



If user has manually entered Date and Time from device web page or Device Menu, then these values of Date and Time will be reflected on device web page and display screen.

*In the case of the **Manual** option, the administrator can manually update the time on the Door with that of the system time as and when required. This can be accomplished from the COSEC Monitor.*

- **Working Days:** Specify the days on which the default working hours should be applicable. Select the respective check boxes of the relevant days.
- **Working Hours (HH:MM):** Specify the default working hours in HH:MM format.
- **Holiday Schedule:** Select the desired Holiday Schedule from the picklist. The Administrator can assign upto four Holiday Schedules to the device.



If the same Holiday Schedule is configured for a user and for the door controller on which the user is assigned, then the user's attendance marking on this device, on any of the scheduled holidays will always be marked as a holiday.

General

Click the **General** tab. The **General** page appears.

Basic Readers Access Settings **General**

Mute Buzzer ☐

Allowed Acknowledgement

Display Duration (ms) 3000

LED - Buzzer Duration Long

Denied Acknowledgement

Display Duration (ms) 3000

LED - Buzzer Duration Long

Enable Display Messages ☐

Custom Birthday Message Happy Birthday

Display Message 1 ☐

Schedule 00:00 11:59

Message Good Morning

Display Message 2 ☐

Schedule 12:00 15:59

Message Good Afternoon

Display Message 3 ☐

Schedule 16:00 20:59

Message Good Evening

Display Message 4 ☐

Schedule 21:00 23:59

Message Good Night

Multi-Language Support ☐

Configure the following parameters:



Mute Buzzer, Allowed Acknowledgment and Denied Acknowledgment are applicable for both Direct Door and Panel Door.

- **Mute Buzzer:** Select the check box to enable door buzzer muting.
- **Allowed Acknowledgment**
 - **Display Duration (ms):** Specify the time duration for which the **Acknowledgment Allowed** message should be displayed. Valid Range is 500 to 3000 ms.
 - **LED - Buzzer Duration:** Select the time duration for the LED Buzzer from the drop-down list options—Long, Medium, Short.
- **Denied Acknowledgment**
 - **Display Duration (ms):** Specify the time duration for which the **Acknowledgment Denied** message should be displayed. Valid Range is 500 to 3000 ms.

- **LED - Buzzer Duration:** Select the time duration for the LED Buzzer from the drop-down list options—Long, Medium, Short.



Enable Display Messages, Custom Birthday Message, Display Message 1 to 4, Schedule, Message and Multi-Language Support are applicable for Direct Door only.

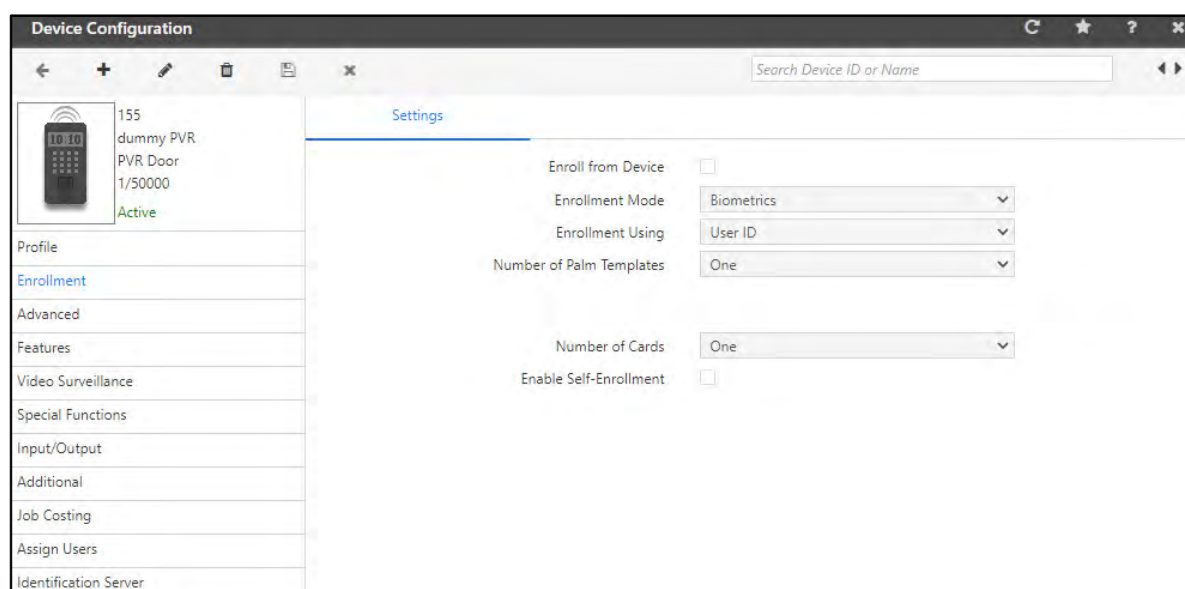
- **Enable Display Messages:** Select this check box, if you wish to customize the messages as well as display them on the device. You can configure and display the Birthday Message and 4 other Messages.
- **Custom Birthday Message:** Enter the birthday message to be displayed on the door to the user, when the user punches on the door on his/her birth date. The valid values are: A-Z a-z 0-9 `~!@#\$%^&*()_+-{}\\|/|:;?<>.,\`".
- **Display Message 1 to 4:** Select this check box to enable each display message. These check boxes are enabled automatically if you select the **Enable Display Message** check box.
- **Schedule:** Specify the time duration for which the display message should be displayed in HH:MM format.
- **Message:** Enter the message to be displayed. Maximum 21 characters are allowed.
- **Multi-Language Support:** Select this check box to enable multi-language support for the device.

Enrollment



Enrollment is applicable for Direct Door only.

On the **Device Configuration** page, click the **Enrollment** tab in the left pane.



Settings

Click the **Settings** tab. The **Settings** page appears

Settings

Enroll from Device ☐

Enrollment Mode Biometrics ▼

Enrollment Using User ID ▼

Number of Palm Templates One ▼

Number of Cards One ▼

Enable Self-Enrollment ☐

Configure the following parameters:

- **Enroll from Device:** Select this check box to enable the enrollment of user from the door controller. When this check box is enabled, **Enroll User** special function on that device will get activated.



*If **Enroll User** special function & **Enroll From Device** check box both are inactive in device configuration, then on activating **Enroll User** special function, **Enroll From Device** check box will be enabled.*

- **Enrollment Mode:** Select the credential to be enrolled using special function at the door from the drop-down list options —ReadOnlyCard, SmartCard, Biometrics or BiometricsThenCard.
- **Enrollment Using:** Select the desired option to be used for enrollment from the drop-down list options — User ID or Reference No.
- **Number of Palm Templates:** Select the Number of Palm Templates to be enrolled from the drop-down list, if the Enrollment Mode is **Biometrics** or **BiometricsThenCard**.
- **Number of Cards:** Select the Number of Cards to be enrolled from the drop-down list, if the Enrollment Mode is **ReadOnlyCard** or **SmartCard**.
- **Enable Self-Enrollment:** Select this check box to enable the Self-Enrollment feature on the door.

Advanced

The Advanced tab allows the user to configure some advanced parameters such as Access Control Settings, Alarms, Device Timers as well as Wiegand.

To do this, on the **Device Configuration** page, click the **Advanced** tab in the left pane.

The screenshot shows the 'Device Configuration' window with the 'Settings' tab selected. The left sidebar lists various configuration categories, with 'Advanced' currently selected. The main area displays a list of settings for a device named '155 dummy PVR' (PVR Door, ID 1/50000, Active).

Settings	Alarms	Timers	Wiegand
Generate Exit Switch Events	<input type="checkbox"/>		
Generate Invalid User Events	<input type="checkbox"/>		
Generate Sequential IN-OUT Events	<input type="checkbox"/>		
Two Credentials Required	<input type="checkbox"/>		
Show PIN	<input type="checkbox"/>		
Allow Exit when Door Lock	<input checked="" type="checkbox"/>		
Auto Relock	<input type="checkbox"/>		
Auto Relock Timer (Sec)	<input type="text" value="3"/>		
Enable Additional Security	<input type="checkbox"/> Disabled		
Enable Smart Identification	<input type="checkbox"/>		
Access Level	<input type="text" value="8"/>		
Access Mode	<input type="text" value="Card"/>		
Auto Acknowledge Alarm	<input type="checkbox"/>		
Auto Acknowledge Alarm (Sec)	<input type="text" value="10"/>		
Facility Code	<input type="text" value="1"/>		
Allow Access Through Mobile	<input type="checkbox"/>		
Mobile Entry Access Mode	<input type="text" value="Mobile Only"/>		
Mobile Exit Access Mode	<input type="text" value="Mobile Only"/>		

To configure the Advanced parameters click the following links:

- [“Settings”](#)
- [“Alarms”](#)
- [“Timers”](#)
- [“Wiegand”](#)

Settings

The **Settings** tab differs for both Direct Door and Panel Door.

Click **Settings** tab.

For configuring the settings for **PVR** as a **Direct Door**, refer to [“Settings- Direct Door”](#).

For configuring the settings for **PVR** as a **Panel Door**, refer to [“Settings- Panel Door”](#).

Settings- Direct Door

For PVR as **Direct Door**.

Settings	Alarms	Timers	Wiegand
Generate Exit Switch Events	<input type="checkbox"/>		
Generate Invalid User Events	<input type="checkbox"/>		
Generate Sequential IN-OUT Events	<input type="checkbox"/>		
Two Credentials Required	<input type="checkbox"/>		
Show PIN	<input type="checkbox"/>		
Allow Exit when Door Lock	<input checked="" type="checkbox"/>		
Auto Relock	<input type="checkbox"/>		
Auto Relock Timer (Sec)	<input type="text" value="3"/>		
Enable Additional Security	<input type="checkbox"/> Disabled		
Enable Smart Identification	<input type="checkbox"/>		
Access Level	<input type="text" value="8"/>		
Access Mode	<input type="text" value="Card"/>		
Auto Acknowledge Alarm	<input type="checkbox"/>		
Auto Acknowledge Alarm (Sec)	<input type="text" value="10"/>		
Facility Code	<input type="text" value="1"/>		
Allow Access Through Mobile	<input type="checkbox"/>		
Mobile Entry Access Mode	<input type="text" value="Mobile Only"/>		
Mobile Exit Access Mode	<input type="text" value="Mobile Only"/>		
Temperature Logging			
Enable	<input type="checkbox"/>		
Sensor Type	<input type="text" value="FEVOBOT"/>		
Sensor Interface	<input type="text" value="USB"/>		
Emissivity	<input type="text" value="0.95"/>		
Calibration Parameter	<input type="text" value="+"/> <input type="text" value="0.0"/>		
Approach to Sensor Wait-Timer (Sec)	<input type="text" value="3.0"/>		
Temperature Detection Time Out (Sec)	<input type="text" value="10"/>		
Tolerance between Consecutive Readings	<input type="text" value="0.5"/>		
Consecutive Readings Count within Tolerance	<input type="text" value="5"/>		
Temperature Threshold (°F)	<input type="text" value="99.5"/>		
Minimum Temperature for Access (°F)	<input type="text" value="95.0"/>		
Restriction Type	<input type="text" value="Soft"/>		
Bypass If Sensor Disconnected	<input type="checkbox"/>		

Configure the following parameters:

- **Generate Exit Switch Events:** Select this check box to enable the door to generate events every time the Exit Switch is used.
- **Generate Invalid User Events:** Select this check box to enable the door to generate events for Invalid User inputs.
- **Generate Sequential IN-OUT Events:** Select this check box to enable the door to generate user punches on device as the sequential IN-OUT events irrespective of whichever mode in which the device is functioning.

- **Two Credentials Required:** Select this check box to enable the feature. If both, **ByPass Finger/Palm/face for Attendance** (User Configuration > T&A > Attendance) and **Two Credentials Required** check boxes are enabled, then two credentials will be mandatory for the users and the door will verify both these credentials.
- **Show Pin:** Select this check box to display the characters of PIN when the PIN is entered on device.
- **Allow Exit when Door Lock:** Select this check box to enable the users to Exit even when the Door relay is in locked condition.
- **Auto Re-lock:** Select this check box to enable the door to re-lock immediately when the door status changes to close after normal open, irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Re-lock Timer:** Specify the time in seconds for the Timer to Re-lock automatically.
- **Enable Additional Security:** Select this check box to enable additional security at the Door.
 - **Additional Security Code:** Specify the Additional Security Code ranging from 1 to 65535.
 - **Re-enter Code:** Re- enter the **Additional Security Code** to confirm.



*Changing this value can affect the SI function. Click **Default Code** to reset the **Additional Security Code** to the value set in the **Global Additional Security Code** field on the Global System Policy page.*

- **Enable Smart Identification:** Smart Identification enables the identification of a user using the Smart Card even though the user is not registered on a device. Select this check box to enable Smart Identification at the door and select the **Access Level** and the **Access Mode** from the drop-down list.



*Door PVR must be in an Adaptive mode (System Configuration > Global Policy > Device > Run PVR Door In Adaptive Mode) to allow the Access through **Card + Biometric** and **Card + Biometric + PIN** mode of the Access.*

- **Auto Acknowledge Alarm:** Select this check box to enable the acknowledgment of all alarms for this device automatically.
- **Auto Acknowledge Alarm (sec):** Specify the time in seconds for the Auto Acknowledge Timer. On expiry of the timer, the alarm buzzer will stop automatically.
- **Facility Code:** Specify a value for Facility Code to be set for access modes other than **Card**, if Facility Code is expected in Wiegand Output.
- **Allow Access Through Mobile:** Select this check box to enable the Access to device using COSEC ACS App.
- **Mobile Entry/Exit Access Mode:** Select the **Entry and Exit** door **Access Mode** from the drop-down list options—Mobile Only, Mobile then Biometrics, Mobile then Card.



*If User Access Mode is selected as **None** in Zone Configuration and Mobile Access Mode is selected as **Mobile Then Biometrics** then door can be accessed through Mobile and then Biometric credential.*

Temperature Logging

- **Enable:** Select this check box to enable the temperature logging feature on the zone.
- **Sensor Type:** Select the type of thermal sensor integrated in the device from the drop-down list options—**AST, Web-Based** or **FEVOBOT**.
- **Sensor Interface:** Select the interface on which device will communicate with the sensor from the drop-down list.
For Sensor Type-AST, the Sensor Interface options will be: RS-232 and USB
For Sensor Type- Web-Based, the Sensor Interface options will be: HTTP/S
For Sensor Type-FEVOBOT, the Sensor Interface options will be: USB
- **Emissivity:** Specify the Emissivity for Sensor. This parameter is applicable when the Sensor Type is AST. The default value is 0.95.
- **Calibration Parameter:** Specify the Calibration Parameter for the thermal sensor. This parameter is applicable when Sensor Type is AST or Web-Based. On click of **+** the value increases by 0.1 and on click of **–** it decreases by 0.1.
- **Approach to Sensor Wait-Timer:** Specify the time for which the device will wait for user to approach the device before starting Temperature Detection.
- **Temperature Detection Time-Out:** Specify the time till which temperature detection will be done for the user and if valid temperatures are not found till the expiry of timer, then timeout will be declared.
- **Tolerance between Consecutive Readings:** Specify the time within which the consecutive readings are considered to be valid user temperature readings. This parameter is applicable when Sensor Type is AST or Web-Based.
- **Consecutive Readings Count within Tolerance:** Specify the number of readings within the Tolerance time for which the consecutive readings are considered to be valid user temperature readings. This parameter is applicable when Sensor Type is AST or Web-Based. For example: if the count is set as 5, then 5 readings are taken and the reading with the highest temperature is considered.
- **Temperature Threshold:** Specify the Threshold value of the Temperature.
- **Minimum Temperature for Access:** Specify the Minimum Temperature value for Access that should be detected to be considered as valid temperature.
- **Restriction Type:** Specify the Restriction Type from the drop-down list options —**Soft** or **Hard**.
- **Bypass if Sensor Disconnected:** Select this check box to enable bypassing the feature if sensor connectivity is lost or is disconnected.

Settings- Panel Door

For PVR as a **Panel Door**.

Settings	Alarms	Timers
<div>Auto Relock <input type="checkbox"/></div> <div>Auto Relock Timer (Sec) <input type="text" value="3"/></div>		
<div>Tail-Gating <input type="checkbox"/></div> <div>Reset Wait Timer <input type="text" value="On Door Lock"/></div>		
<div>Man Trap Timer - Internal Reader (Sec) * <input type="text" value="0"/></div> <div>Man Trap Timer - External Reader (Sec) * <input type="text" value="0"/></div>		
<div>Enable Man Trap Door Interlocking <input type="checkbox"/></div> <div>Select Doors for Interlocking</div> <div> <input type="text" value="ID"/> <input type="text" value="Name"/> <input type="button" value="⋮"/> <input type="button" value="i"/> </div>		

Configure the following parameters:

- **Auto Re-lock:** Select this check box to enable the door to re-lock automatically when the door status changes to close after normal open, irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Re-lock Timer:** Specify the time in seconds after which the door should re-lock automatically.
- **Tail-Gating:** Tailgating refers to an access violation which occurs when more than one person tries to enter a secured area using a single person's access credentials. If this option is enabled on the Panel Door, the occupancy count of a zone should be increased or decreased considering both the punch as well as the auxiliary input of the Panel Door. Select this check box to enable this feature.
- **Reset Wait Timer:** Select when the Wait Timer should be reset for tailgating from the drop-down list options—On Door Lock or Pulse Wait Timer.
- **Man Trap Timer- Internal Reader (Sec):** Specify the Man Trap Entry Timer within which the user should enter the next sequential door of a man-trap.
- **Man Trap Timer- External Reader (Sec):** Specify the Man Trap Exit Timer within which the user should exit the panel door to enter the next sequential door of a man-trap.
- **Enable Man Trap Door Interlocking:** Select this check box to enable the Door Interlock for the door (say Door1). This means if the Door1 is open, other doors will remain closed.
- **Select Doors for Interlocking:** Select the doors to be assigned for Interlocking from the picklist. For example, if Door 2 and Door 3 are selected for interlocking with Door 1, Door 2 and Door 3 will remain locked when Door 1 is open.

Door Interlocking feature will not work for Degraded mode.



For Example, when a door is in abnormal state and for that door interlocking is enabled, then user access to other doors of the interlocking group is allowed.

Alarms

Alarms tab differs for Direct Door and Panel Door.

Click **Alarms** tab. The **Alarms** page appears.

For PVR as **Direct Door**.

Settings	Alarms	Timers	Wiegand
Tamper <input type="checkbox"/>			
Door Abnormal <input type="checkbox"/>			
Door Force Open <input type="checkbox"/>			
Door Fault <input type="checkbox"/>			
Panic <input type="checkbox"/>			
Temperature Threshold <input type="checkbox"/>			

For PVR as a **Panel Door**.

Settings	Alarms	Timers
Duress <input type="checkbox"/>		
Tamper <input type="checkbox"/>		
Door Abnormal <input type="checkbox"/>		
Door Force Open <input type="checkbox"/>		
Door Fault <input type="checkbox"/>		
Panic <input type="checkbox"/>		
Door Held Open <input type="checkbox"/>		
Dead Man <input type="checkbox"/>		
Occupancy Violated <input type="checkbox"/>		
Tail-Gating <input type="checkbox"/>		
Man Trap Timer Violation <input type="checkbox"/>		
Access Denied - Anti-Pass Back <input type="checkbox"/>		
Access Denied - Access Route Violated <input type="checkbox"/>		
Access Denied - Other Reasons <input type="checkbox"/>		
User Unidentified <input type="checkbox"/>		
Multiple Unauthorized Attempts <input type="checkbox"/>		
Access Denied - Access Route Timer Violated <input type="checkbox"/>		

- Select the check boxes of the desired alarms you wish to enable.

Timers

This section allows the configuration of various types of predefined device timers which can trigger off specific responses. In COSEC Server, Timers are often used to control door behavior and for triggering alarms.

The **Timers** tab differs for both Direct Door and Panel Door.

Click **Timers** tab. The **Timers** page appears.

For PVR as **Direct Door**.

Settings	Alarms	Timers	Wiegand
Inter Digit Wait Timer (Sec) *		<input type="text" value="3"/>	
Multi-Input Wait Timer (Sec) *		<input type="text" value="5"/>	
Door Open Pulse Timer (Sec) *		<input type="text" value="5"/>	
Late-IN Early-OUT Active Timer (Min) *		<input type="text" value="60"/>	
Palm Enrollment Time Out (Sec) *		<input type="text" value="60"/>	

Configure the following parameters:

- **Inter-Digit Wait Timer (sec):** Specify the time in seconds within which two key inputs on the device keypad must be obtained. On expiry of this timer, the system considers the user input to be complete and is ready for the next input.
- **Multi-Input Wait Timer (sec):** Specify the time in seconds for which system needs to wait for the second credential input from the user when more than one credential is to be used to grant access.



It is recommended to set the timer value as greater than or equal to 10 seconds to avoid Access Denial issues to users. This is applicable when the system reads the credentials (Biometric) from the user's Smart Cards.

- **Door Open Pulse Timer (sec):** Specify the time in seconds for the door to remain open for a valid credential. If the opened door does not return to a closed state before the expiry of this timer, the door will generate a **Door Abnormal** alarm.
- **Late-IN Early-OUT Active Timer (min):** Specify the time in minutes for which the Late-IN and Early-OUT special functions will remain active after being enabled at the Door.
- **Palm Enrollment Time Out (sec):** Specify the time in seconds for which a Palm Enrollment command will be valid for credential input. Once this timer runs out, a new enrollment command will have to be generated.

For PVR as a **Panel Door**.

Settings	Alarms	Timers	Wiegand
Pulse Time (Sec)		<input type="text" value="5"/>	

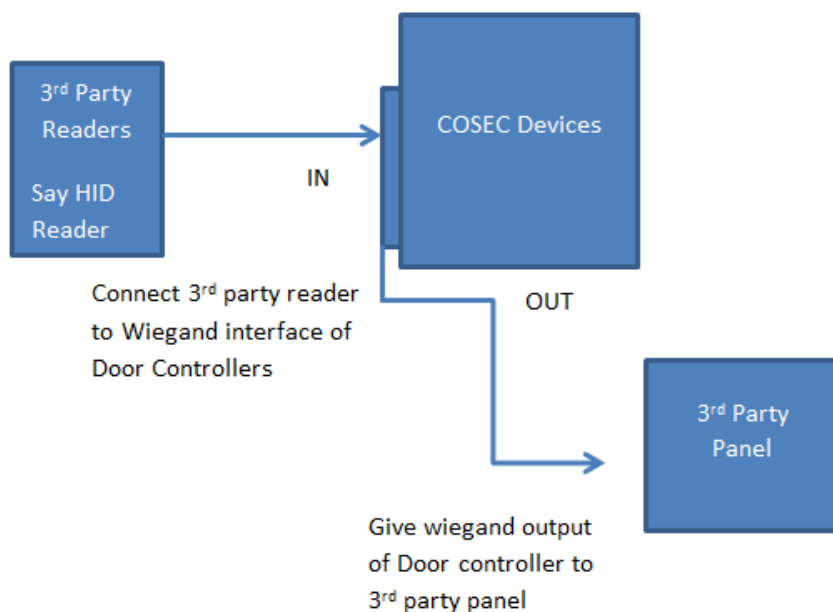
- **Pulse Time (sec):** Specify the time in seconds for the panel door to remain open for a valid credential.

Wiegand



Wiegand is applicable for Direct Door only.

Click the **Wiegand** tab. The **Wiegand** page appears.



- **Wiegand Interface:** The COSEC Device can be connected both as input devices (e.g. to receive data from a Wiegand Reader) or output devices (e.g. to support output to third party panel) via the Wiegand interface as shown above.

So select the interface of PVR Direct Door as **Output Mode** to work as Wiegand Output to Panel or **Reader Input** to take data from third party reader. If Reader Input option is selected, all the output mode parameters will be disabled.

If you select Output Mode then configure the **Output Mode Parameters**.

Output Mode Parameters

- **Wait For Panel Signal:** Select the check box to enable. If this option is enabled the PVR Door will wait for reply from the connected third party device before triggering any output. You need to configure the **Signal Wait Timer (Sec)**.
- **Signal Wait Timer:** Specify the time for which the PVR Door should wait for reply from the connected third party device before triggering any output.
- **Wait For User Verification:** Select the check box to enable. If this option is enabled, user verification will be requested on the third party device before triggering any output.
- **Wiegand Output Format:** Select the desired format — 26 Bit, 37 Bit, Actual or Custom

Settings Alarms Timers **Wiegand**

Wiegand Interface Output Mode

Output Mode Parameters

Wait For Panel Signal ☒

Signal Wait Timer (Sec) 20

Wait For User Verification ☒

Wiegand Output Format 26 Bit

Send From MSB Bit

If you select **Custom**, you can configure details of fields to be sent as output from the Wiegand reader that has been added.

Wiegand Format

For Allowed Events ID Name

Allowed Code

For Identified Events ID Name

Identified Code

For Denied With Invalid Biometric Events ID Name

Invalid Biometric Code

For Denied With Invalid Card Events ID Name

Invalid Card Code

For Denied With Invalid PIN Events ID Name

Invalid PIN Code

For Denied With Credential Time-Out Events ID Name

Credential Time-Out Code

Send From MSB Bit

- For each of the listed events, click the picklist to select the desired **Wiegand Output Format**.
- Assign an Access **Code** for each communication (for example Invalid PIN Code). This will depend on the number of output bits configured for Access Code in the selected Wiegand Output Format.
- **Send From:** Select the desired sending order for reader data — MSB or LSB Bit.

Features



The Features are available only with the Access Control Module license and are applicable for Direct Door only.

The Features tab enables the user to enable certain Access Control features for the device.

To do this, on the **Device Configuration** page, click the **Features** tab in the left pane.

The screenshot shows the 'Device Configuration' window with the 'Features' tab selected in the left sidebar. The main area is divided into 'Basic' and 'Optional' sections. The 'Basic' section includes fields for Sequence Number (68), Device (155, dummy PVR), IP Address, MAC Address (AA : BB : AA : AA : AA : BA), and an Active checkbox (checked). The 'Optional' section includes Site (1, Site-1), Application (Basic Access Control), User Access Mode (Any One), Visitor Access Mode (Any One), Alert Messages (unchecked), Consider For Visitor Pass Surrender (unchecked), Consider For Attendance (checked), and Generate Events (checked).

To configure the Features parameters, click the following links:

- [“Set1”](#)
- [“Set2”](#)

Set1

Click **Set1** tab. The **Set1** page appears.

Set1	Set2
Absentee Rule	
Enable	<input type="checkbox"/>
Occupancy Control	
Enable	<input type="checkbox"/>
Maximum Occupancy Limit	<input type="text" value="9"/>
Minimum Occupancy Limit	<input type="text" value="1"/>
Zero Occupancy	<input checked="" type="checkbox"/>
Use Count Control	
Enable	<input type="checkbox"/>
Use Count Limit (Per Minute)	<input type="text" value="5"/>
Duress Detection	
Duress Detection	<input type="checkbox"/> <input type="text"/>

Configure the following parameters:

Absentee Rule

- **Enable:** Select this check box to enable the feature on the door. This rule sets the maximum number of days for non-use of a credential. On expiration of days limit, the user will be automatically blocked. For configuring the rule, refer to [“Absentee Rule”](#).

Occupancy Control

- **Enable:** Select this check box to enable the feature on the door.
- **Maximum Occupancy Limit:** Specify the maximum number of users to be allowed within the controlled area, after which a user exit is required to enable access to another user.
- **Minimum Occupancy Limit:** Specify the minimum number of occupants to be present within the controlled area.
- **Zero Occupancy:** Select the check box to enable the controlled area to be empty. For configuring the rule, refer to [“Occupancy Control”](#).

Use Count Control

- **Enable:** Select this check box to enable the feature on the door.
- **Use Count Limit (Per Minute):** Specify the maximum number of times a user is allowed to access an area with valid credentials per minute. For configuring the rule, refer to [“Use Count Control”](#).

Duress Detection

- **Duress Detection:** Select this check box to enable Duress Detection on the door. The default duress detection code is displayed which is used to generate the duress alarm. Specify the desired duress code. This code informs that a user is forced to open the door under threat. Once this feature is enabled the system waits for the duress code after the User PIN and the right arrow key input before enabling the duress alarm. The keys have to be pressed in the following order: (User Pin Code) → (Right Arrow Key) → (2 digit Duress Code).

Set2

Click **Set2** tab. The **Set2** page appears.

Set1	Set2
First IN User Rule	
Enable	<input type="checkbox"/>
Reset On	<input checked="" type="radio"/> Day Change <input type="radio"/> Timer Expiry
Access Timer (Sec)	<input type="text" value="3"/>
First IN User Group	<input type="text" value="1"/> <input type="button" value="List 1"/>
Anti-Pass Back (APB)	
On Entry	<input type="checkbox"/>
On Exit	<input type="checkbox"/>
Hard/Soft	<input type="text" value="Soft"/>
Forgiveness	<input checked="" type="checkbox"/>
Reset After	<input checked="" type="radio"/> Day Change <input type="radio"/> Timer Expiry
Forgiveness Timer (Min)	<input type="text" value="1"/>
2-Person Rule	
Enable	<input type="checkbox"/>
Mode	<input type="text" value="Primary Must"/>
Primary Group	<input type="text" value="g1"/>
Secondary Group	<input type="text" value="None"/>
2nd Person Wait Timer (Sec)	<input type="text" value="5"/>

Configure the following parameters:

First-IN User Rule

- **Enable:** Select this check box to enable the feature on the door.
- **Reset On:** Select when the First-IN User rule should be reset from the options — **Day Change** or **Time Expiry**.

If you select **Time Expiry**, configure the **Access Timer (Sec)**.

- **Access Timer (sec):** Specify the duration for which the rule should be applied. After the expiry of this timer, the rule will be reset for all the users.
- **First-In User Group:** Select the desired group which should be valid at the door from the picklist. For configuring the rule, refer to [“First In User Assignment”](#).

Anti-Pass Back (APB)

- **On Entry:** Select this check box to enable the system to monitor the entry reader for APB violation.
- **On Exit:** Select this check box to enable the system to monitor the entry as well as the exit readers for APB violations.
- **Hard/Soft:** Select the restriction type from the drop-down list options—Soft or Hard.

Hard APB: If you select Hard APB, access will be denied if the exit is not registered first. It does not allow a second entry using the same card without an exit.

Soft APB: The access will be granted even if the exit is not registered. It allows a second entry of the same user without an exit; however, an event and a warning are generated that indicates the second entry.

- **Forgiveness:** Select this check box to enable the system to reset the APB status.

If **Forgiveness** is enabled, configure the following parameters.

- **Reset After Day Change:** This will reset the APB status of all the users to NULL at midnight. This enables a user, who left the building in the evening without exit punch, to use his/her card for entry in the next morning.
- **Reset After Timer Expiry:** This will reset the APB status of all the users after the expiry of defined time.

If **Reset After Timer Expiry** is selected, configure the following parameter.

- **Forgiveness Timer (Mins):** Specify the time duration in minutes after which Anti-Pass Back status will get reset and the pass will be in original state.

2-Person Rule

- **Enable:** Select this check box to enable the feature on the door.
- **Mode:** Select the Mode from the drop-down list options— Primary Must or Primary & Secondary Must.
- **Primary Group:** Select the desired group from the drop-down list.
- **Secondary Group:** Select the desired group from the drop-down list.
- **2nd Person Wait Timer (sec):** Specify the wait time in seconds after which the second person is allowed to punch on the door. For configuring the rule, refer to [“2 Person Rule Assignment”](#).

Video Surveillance



Video Surveillance is applicable for both Direct Door and Panel Door.

The **Video Surveillance** tab enables the user to configure parameters for video surveillance integration with the COSEC device. It is available in Basic License.

To do this, on the **Device Configuration** page, click the **Video Surveillance** tab in the left pane.

The screenshot shows the 'Device Configuration' window. On the left, a sidebar lists configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance (highlighted), Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main content area is titled 'Satatya Integration' and contains the following fields:

- Capturing Device:** A dropdown menu showing 'Matrix HVR/NVR'.
- MAC Address:** A text input field.
- Camera ID:** A text input field.
- Storage Root Folder:** A text input field.
- FTP Login Credentials:** A checkbox.
- User Name:** A text input field with the placeholder 'User Name'.
- Password:** A text input field with masked characters (dots).

To configure the Video Surveillance parameters, click the following links:

- [“Visual Tagging”](#)
- [“Satatya Integration”](#)

Visual Tagging

The COSEC application can interface with some supported Hybrid and Network Video Recorders and grab images triggered by user events at the Doors. The **Visual Tagging** tab enables the administrator to define the video recorder parameters.

Click the **Visual Tagging** tab. The **Visual Tagging** page appears.

Visual Tagging Satatya Integration

Capturing Device: Matrix HVR/NVR

MAC Address *

Camera ID *

Storage Root Folder *

FTP Login Credentials ☐

User Name *

Password *



To view the user events and related images, click **Admin > Views/Logs > Event View**. To know more about viewing events, refer to [“Event View”](#).

Configure the following parameters:

- **Capturing Device:** Select the video recording device type from the drop-down list options — Matrix HVR/NVR or Milestone.

For more information on integration with **Milestone** devices, refer to [“Milestone Integration”](#).

If you select Matrix HVR/NVR, then configure the following parameters.

- **MAC Address:** Specify the MAC address of the video recorder device using “_” (underscore) as the separator.
- **Camera ID:** Specify the Camera number or Camera ID for IP cameras. For analog cameras, specify the camera number.
- **Storage Root Folder:** Specify the Root Folder path or FTP Path where the uploaded images are to be saved.
- **FTP Login Credentials:** Select this check box to activate the FTP login credentials for authentication.
- **User name:** Specify the FTP Server User Name.
- **Password:** Specify the FTP Server Password.

Satatya Integration

This functionality is available for configuration only when the Matrix HVR/NVR device type is selected as the **Capturing Device** in **Visual Tagging** tab. It enables the configured COSEC devices to directly send commands to the SATATYA HVR/NVR devices as per the configuration on this page.

Click **Satatya Integration** tab. The **Satatya Integration** page appears.

Visual Tagging
Satatya Integration

Integration Type
Network

Active
☐

IP Address *

Port Number *
1024-65535

Schedule Name

Active
☐

Schedule Range *
00:00
23:59

Days *
☒ Sun
☒ Mon
☒ Tue
☒ Wed
☒ Thu
☒ Fri
☒ Sat
☒ Holiday

Event
Access Allowed

Mode
Both

Action
Recording

Duration Min. *

Camera *
☐ 1
☐ 2
☐ 3
☐ 4
☐ 5
☐ 6
☐ 7
☐ 8
☐ 9
☐ 10
☐ 11
☐ 12
☐ 13
☐ 14
☐ 15
☐ 16
☐ 17
☐ 18
☐ 19
☐ 20
☐ 21
☐ 22
☐ 23
☐ 24

Add
Cancel

Configure the following parameters:

- **Integration Type:** Select the **Integration Type** from the drop-down list options—Wired or Network.

If you select **Wired Integration**, door will be physically connected with the Satatya Device.

If you select **Network Integration**, connection can be by Ethernet, Wireless or Broadband depending upon the COSEC device support. If you select this option you need to configure the below mentioned parameters.

- **Active:** Select this check box to enable the SATATYA Integration functionality.
- **IP Address:** Specify the IP Address of HVR/NVR.
- **Port Number:** Specify the Port Number of HVR/NVR.
- **Schedule Name:** Specify a user friendly Name for the Integration function.
- **Active:** Select this check box to enable the schedule.
- **Schedule:** Specify the Start Time and End Time of the Schedule in HH:MM format.
- **Days:** Select the check boxes for the desired Days on which you wish to apply the Schedule.
- **Event:** Select a COSEC Event for which the action is to be configured from the drop-down list.
- **Mode:** Select the event Mode from the drop-down list options—Entry, Exit, Both if you select the Event as Access Allowed, Access Denied or Invalid User.

- **Action:** Select the Action for the Satatya device from the drop-down list options—Recording, Image Upload, Video Pop-up, PTZ Preset, Mail Image.

If you select **Recording**, specify the **Duration Min..**

If you select **Upload Image**, Images will be uploaded as per the FTP settings.

If you select **Video Pop-up**, specify the **Duration Sec.** The video pop up will be generated on the local client of Satatya device.

If you select **PTZ Preset**, specify the desired **Position No.**

If you select **Mail Image**, specify the **Email ID.**

- **Camera:** Select the check boxes of the desired camera channels depending on the Action selected.

Example 1: For Action as Video Pop up and the camera channel selected is 24, then the pop-up of Camera 24 will be shown for 10 seconds.

Example 2: For Access Allowed event on COSEC Device and the camera channel selected are 4,6,8 and 10, then recording of these cameras will be done for 10 seconds.

- Click **Add**. All the Events and Actions configured for them appear in a list.

Visual Tagging
Satatya Integration

Integration Type
Network

Active
☒

IP Address *
192 . 168 . 111 . 164

Port Number *
8711

Schedule Name

Active
☐

Schedule Range *
00:00
23:59

Days *
☒ Sun
☒ Mon
☒ Tue
☒ Wed
☒ Thu
☒ Fri
☒ Sat
☒ Holiday

Event
Access Allowed

Mode
Both

Action
Recording

Duration Min. *

Camera *
☐ 1
☐ 2
☐ 3
☐ 4
☐ 5
☐ 6
☐ 7
☐ 8
☐ 9
☐ 10
☐ 11
☐ 12
☐ 13
☐ 14
☐ 15
☐ 16
☐ 17
☐ 18
☐ 19
☐ 20
☐ 21
☐ 22
☐ 23
☐ 24

Add
Cancel

Search

Name	Event	Action	Start Time	End Time	Active	
New Schedule	Access Allowed	Recording	00:00	23:59	Yes	

Special Functions



Special Functions is applicable for both Direct Door and Panel Door.

On the **Device Configuration** page, click the **Special Functions** tab in the left pane.

No.	Function Name	Active	Job Selection	User Group	Card 1	Card 2	Card 3	Card 4	
1	Official Work - IN	Yes	Yes	All					
2	Official Work - OUT	Yes	Yes	All					
3	Short Leave - IN	Yes	Yes	All					
4	Short Leave - OUT	Yes	Yes	All					
5	Regular - IN	Yes	Yes	All					
6	Regular - OUT	Yes	Yes	All					
7	Break End	Yes	Yes	All					
8	Break Start	Yes	Yes	All					
9	Overtime - IN	Yes	Yes	All					
10	Overtime - OUT	Yes	Yes	All					
11	Enroll User	Yes	No	All					
12	Enroll Special Card	Yes	No	All					

The **Special Functions** page differs for both Direct Door and Panel Door.

For PVR as **Direct Door**.

Configuration		Shortcuts			Schedule			
No.	Function Name	Active	Job Selection	User Group	Card 1	Card 2	Card 3	Card 4
1	Official Work - IN	Yes	Yes	All				
2	Official Work - OUT	Yes	Yes	All				
3	Short Leave - IN	Yes	Yes	All				
4	Short Leave - OUT	Yes	Yes	All				
5	Regular - IN	Yes	Yes	All				
6	Regular - OUT	Yes	Yes	All				
7	Break End	Yes	Yes	All				
8	Break Start	Yes	Yes	All				
9	Overtime - IN	Yes	Yes	All				
10	Overtime - OUT	Yes	Yes	All				
11	Enroll User	Yes	No	All				
12	Enroll Special Card	Yes	No	All				

To configure Special Functions for PVR as Direct Door, refer to [“Special Functions”](#).

For PVR as a **Panel Door**.

Shortcuts	
▲ F1	None
▼ F2	None
► F3	None
◄ F4	None

To configure Special Functions for PVR as Panel Door, refer to [“Special Functions Shortcuts”](#).

Input/Output



Input/Output is applicable for both Direct Door and Panel Door.

The Configuration Tab is applicable for both Direct Door and Panel Door, whereas Linking and Time Triggered tab is applicable for Direct Door only.

This functionality is available only with the Access Control add-on module license.

The Input/Output (I/O) configuration of a door determines how the output or response of a system is influenced by the input applied on it. In case of the COSEC Access Control System, the I/O configuration should enable the system to monitor and trigger a specific response to any changes in door state or event occurrences at the door device. This change of door state or occurrence of events may be considered as an input while the response or action that is generated by the system on detection of this input, may be defined as the output.

On the **Device Configuration** page, click the **Input/Output** tab in the left pane.

The screenshot shows the 'Device Configuration' window with the 'Input/Output' tab selected in the left sidebar. The main area displays the following configuration options:

- Door Sense:**
 - Enable: ☐
 - Supervised: ☐
 - Door Sense Type: NC
- Auxiliary Input:**
 - Enable: ☐
 - Supervised: ☐
 - Sense Type: NO
 - Debounce Time (Sec): 5
- Auxiliary Output:**
 - Enable: ☐
 - Output Wait Time (Sec): 0
- Accept External IO Linking:**
 - Enable: ☐
 - Network Interface: Ethernet

To configure the Input/Output parameters, click the following links:

- [“Configuration”](#)
- [“Linking”](#)
- [“Time Triggered”](#)

Configuration



Configuration is applicable for both Direct Door and Panel Door.

Configuration tab differs for Direct Door and Panel Door.

Click **Configuration** tab. The **Configuration** page appears.

For PVR as **Direct Door**.

Configuration	Linking	Time Triggered
Door Sense		
Enable	<input checked="" type="checkbox"/>	
Supervised	<input type="checkbox"/>	
Door Sense Type	NC	
Auxiliary Input		
Enable	<input checked="" type="checkbox"/>	
Supervised	<input type="checkbox"/>	
Sense Type	NO	
Debounce Time (Sec)	5	
Auxiliary Output		
Enable	<input checked="" type="checkbox"/>	
Output Wait Time (Sec)	0	
Accept External IO Linking		
Enable	<input checked="" type="checkbox"/>	
Network Interface	Ethernet	

Configure the following parameters:

Door Sense

The system by default can sense two states of a door - Normally Open (NO) and Normally Closed (NC) depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a **Door Abnormal** alarm.

- **Enable:** Select the check box to enable the feature.
- **Supervised:** Select the check box to enable the door for four-state monitoring, where the door is also monitored for Door Fault and Door Disconnection.

- **Door Sense Type:** Select the Door Sense Type from the drop-down list options — NO or NC.

Auxiliary Input

- **Enable:** Select the check box to enable the feature.
- **Supervised:** Select the check box to enable the door for four-state monitoring, where the door is also monitored for Door Fault and Door Disconnection.
- **Sense Type:** Select the Sense Type from the drop-down list options — NO or NC.
- **Debounce Time (Sec):** Specify the Debounce Time in seconds. It defines the minimum time for which the door should remain in a given state to enable the system to take action on it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.

Auxiliary Output

- **Enable:** Select the check box to enable the feature.
- **Output Wait Time (Sec):** Specify the time in seconds that will be set as an additional waiting period before the Aux Output signal is sent.

Accept External IO Linking

- **Enable:** Select the check box to enable device-to-device IO Linking, i.e. input from one Direct Door can trigger output in another Direct Door.
- **Network Interface:** Select the interface option for IO linking with external devices from the drop-down list options—Ethernet, Wireless or Mobile Broadband.

For PVR as a **Panel Door**.

Configuration

Door Sense

Enable

☒

Supervised

☒

Door Sense Type

NC

Auxiliary Input

Enable

☒

Supervised

☒

Sense Type

NO

Debounce Time (Sec)

5

Auxiliary Output

Enable

☒

Output Group

1

DC Aux Ports

Relay Output

Output Group Number (Door Unlock)

2

Door Unlock

Output Group Number (Door Lock)

5

Panel Output

Configure the following parameters:

Door Sense

The system by default can sense two states of a door - Normally Open (NO) and Normally Closed (NC) depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a **Door Abnormal** alarm.

- **Enable:** Select the check box to enable the feature.
- **Supervised:** Select the check box to enable the door for four-state monitoring, where the door is also monitored for Door Fault and Door Disconnection.
- **Door Sense Type:** Select the Door Sense Type from the drop-down list options — NO or NC.

Auxiliary Input

- **Enable:** Select the check box to enable the feature.
- **Supervised:** Select the check box to enable the door for four-state monitoring, where the door is also monitored for Door Fault and Door Disconnection.
- **Sense Type:** Select the Sense Type from the drop-down list options — NO or NC.
- **Debounce Time (Sec):** Specify the Debounce Time in seconds. It defines the minimum time for which the door should remain in a given state to enable the system to take action on it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.

Auxiliary Output

- **Enable:** Select the check box to enable the feature.
- **Output Wait Time (Sec):** Specify the time in seconds that will be set as an additional waiting period before the Aux Output signal is sent.

Relay Output

- **Output Group Number (Door Unlock):** Select the Output Group Number to which the device output for Door Unlock is to be assigned from the picklist.
- **Output Group Number (Door Lock):** Select the Output Group Number to which the device output for Door Lock is to be assigned from the picklist.

Linking



Linking is applicable for Direct Door only.

The COSEC application supports the Input/Output Linking feature to activate an output port based on a trigger received from an input port on the same Direct Door. This option enables the administrator to define how an event or events (input port) will trigger an output on the door.

Click **Linking** tab. The **Linking** page appears.

Name	Active Input	Output	Output Type	Pulse Time(Sec)	Reset Link	Reset Time	Supported Devices
	No	Aux. Input	Aux. Output		Inactive	00:00	0 »
	No	Aux. Input	Door Relay		Inactive	00:00	0 »
	No	Duress	Aux. Output		Inactive	00:00	0 »
	No	Duress	Door Relay		Inactive	00:00	0 »
	No	Intercom Panic	Aux. Output		Inactive	00:00	0 »

1 - 5 of 12 records

« < 1 2 3 > »

Select a Input-Output linking row or click edit button.

- **Name:** Specify a Name for the new I/O linking program to be defined.
- **Active:** Select this check box to enable the IO Linking.
- **Output Type:** Specify the required type of Output from the drop-down list options—Pulse, Interlock, Latch, Toggle.

If you select **Pulse**, the output will be active for the defined pulse time, for example, 5 sec.

If you select **Interlock**, the output follows the input. The output will be active till the input is active, after which it returns to normal state.

If you select **Latch**, the relay output will be in energized condition for infinite period and needs to be reset manually. It means once the input is active, output will be active. It has to be reset manually. For example, during a Fire alarm, door should be unlocked permanently so Latch output can be used.

If you select **Toggle**, the output group toggles its state whenever an input group is activated.

- **Pulse Time (sec):** If you select the Output Type as **Pulse**, specify the time until which the output should be active.
- **Reset Link:** Select this check box to enable the system to reset the IO link.
- **Reset Time:** Specify the time after which the IO link should be reset in HH:MM format.
- **Supported Devices:** All devices supported for external IO Linking will appear in this picklist for selection. Select the required devices from the picklist. Upto 255 external devices can be added.

Click **OK** and then **Save** to save the configuration.

Time Triggered



Time Triggered is applicable for Direct Door only.

This functionality enables the user to control the activity of an Output without manual intervention. The output gets active without the status of input, i.e. the selected output is triggered based on the configured time and not the IO link.

The time triggered functions are used for activating events like door unlock and siren activation that are set as per the start time and for the configured time duration. This functionality is designed to trigger outputs for predefined periods at the configured time. The COSEC access control system supports up to 20 Time Triggered functions on a Direct Door.

Click **Time Triggered** tab. The **Time Triggered** page appears.

Function Name	Active	Time	Duration(Sec)	Days	Output
Function 1	Yes	00:00	10	Su Mo Tu We Th Fr Sa PH	Aux. Output

Click **Add**.

Configure the following parameters:

- **Function Name:** Specify a user friendly Function Name.
- **Active:** Select this check box to enable the Time Triggered function.
- **Time:** Specify the time when the Time Triggered function should be activated.
- **Duration:** Specify the time duration for which the Time Triggered function should be active.
- **Days:** Select the check boxes for the desired days on which you wish to apply the Time Triggered function from the drop-down list. Click **Check All**, if you wish to select all the days.
- **Output:** Select the Output on which the Time Triggered function should be applied from the drop-down list options—Aux Output or Door Relay.

Click **OK** and then **Save** to save the settings.

Additional



Additional is applicable for Direct Door only.

Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. COSEC doors can be configured to be compatible with this procedure keeping the RTC of the system updated with such changes

On the **Device Configuration** page, click the **Additional** tab in the left pane.

The screenshot shows the 'Device Configuration' window. On the left, a sidebar lists various configuration options, with 'Additional' highlighted. The main window displays the 'Daylight Saving' configuration page. At the top, there's a search bar for 'Device ID or Name'. Below it, the 'DST Type' is set to 'Day-Month wise' in a dropdown menu, and the 'Time Period' is '00:00'. The 'Forward Clock' section includes dropdowns for 'Month' (January), 'Week No.' (1st), and 'Day of Week' (Sunday), with a 'Time' field set to '00:00'. The 'Backward Clock' section has identical dropdowns for 'Month', 'Week No.', and 'Day of Week', with a 'Time' field set to '00:00'. A 'Save' button is located at the bottom right of the configuration area.

The **Daylight Saving** configuration can be done in 2 ways — Day-Month wise or Date-Month wise.

- **DST Type:** Select the **DST Type** as Day-Month wise or Date-Month wise. Select Disable, if you wish to disable the application of DST on the system time.

If you select the **Day-Month wise** option, configure the following parameters.

This is a close-up view of the 'Daylight Saving' configuration page. The 'DST Type' dropdown is set to 'Day-Month wise'. Below it, the 'Time Period' is '00:00'. The 'Forward Clock' section shows 'Month' as 'January', 'Week No.' as '1st', 'Day of Week' as 'Sunday', and 'Time' as '00:00'. The 'Backward Clock' section also shows 'Month' as 'January', 'Week No.' as '1st', 'Day of Week' as 'Sunday', and 'Time' as '00:00'. A 'Save' button is at the bottom.

- **Time Period:** Specify the time period by which the time period will be set forward or backward to achieve Daylight Saving.

Forward Clock

- **Month:** Select the month when the DST starts for the Forward Clock from the drop-down list.
- **Week No.:** Select the week of the month when the DST starts for the Forward Clock from the drop-down list. For example, if DST starts from 4th week of March, select 4th.
- **Day of Week:** Select the day of the week when the DST starts for the Forward Clock from the drop-down list.
- **Time:** Specify the time when the DST starts for the Forward Clock in HH:MM format.

Backward Clock

- **Month:** Select the month when the DST ends for the Backward Clock from the drop-down list.
- **Week No.:** Select the week of the month when the DST ends for the Backward Clock from the drop-down list. For example, if DST starts from 4th week of March, select 4th.
- **Day of Week:** Select the day of the week when the DST ends for the Backward Clock from the drop-down list.
- **Time:** Specify the time when the DST ends for the Backward Clock in HH:MM format.

Click **Save** to save the configurations.

If you select the **Date-Month wise** option, configure the following parameters.

The screenshot shows a configuration window titled "Daylight Saving". At the top, "DST Type" is set to "Date-Month wise" and "Time Period" is set to "00:00". Below this, there are two sections: "Forward Clock" and "Backward Clock". Each section has three fields: "Month" (set to "January"), "Date" (set to "1"), and "Time" (set to "00:00"). A "Save" button is located at the bottom center of the form.

- **Time Period:** Specify the time period by which the time period will be set forward or backward to achieve Daylight Saving.

Forward Clock

- **Month:** Select the month when the DST starts for the Forward Clock from the drop-down list.

- **Date:** Select the date of the month when the DST starts for the Forward Clock from the drop-down list.
- **Time:** Specify the time when the DST starts for the Forward Clock in HH:MM format.

Backward Clock

- **Month:** Select the month when the DST ends for the Backward Clock from the drop-down list.
- **Date:** Select the date of the month when the DST ends for the Backward Clock from the drop-down list.
- **Time:** Specify the time when the DST ends for the Backward Clock in HH:MM format.

Click **Save** to save the configurations.

Suppose, the DST period in a region is from Sunday, 27 March at 02:00:00 hours till Sunday, 30 October at 03:00:00. If DST is configured according to this period and the **Time Period** is specified as 1 hour, the clock will be forwarded by 01:00 hours on 27 March at 02:00:00 hours. The clock will be set back by 01:00 hours on 30 October at 03:00:00.

Job Costing



Job Costing is applicable for Direct Door only.

When user punches on any device, there will be an option to select the Job Code on which the user is working. Job Costing enables the Administrator to show or hide Job Code selection on device. It also enables the Administrator to assign default jobs on device.

On the **Device Configuration** page, click **Job Costing** tab in the left pane.

Job Code	Name	Assignment Start	Assignment End
J1	J1	01/12/2022	06/12/2022

Job Code	Name	Assignment Start	Assignment End
No Data			

Settings

Click **Settings** tab. The **Settings** page appears.

Job Code	Name	Assignment Start	Assignment End
J1	J1	01/12/2022	06/12/2022

Job Code	Name	Assignment Start	Assignment End
No Data			

- **Show Job Menu:** Select the Job Menu to be displayed from the drop-down list options— **Show List** or **Allocate Default**.

If you select **Show List**, configure the following parameters.

Settings

Show Job Menu: Show List

Retain Job Selection: ☒

Assign Jobs

Job Group: ID, Name

Job: ID, Name

Search

Job Code	Name	Assignment Start	Assignment End	
J1	J1	01/12/2022	06/12/2022	

- **Retain Job Selection:** Select this check box to retain the Job Code selected by a user which would be applicable for all the subsequent users until another job selection is done on the device.

Assign Jobs

- **Job Group:** Select the desired Job Group from the picklist.
- **Job:** Select the desired Job from the picklist.

Click **Save**. The jobs will be listed to the grid.

If you select **Allocate Default**, configure the following parameters.

Settings

Show Job Menu: Allocate Default

Retain Job Selection: ☐

Default Jobs

Search

Job Code	Name	Assignment Start	Assignment End	
J1	J1	01/12/2022	06/12/2022	

Previous Default Jobs

Search

Job Code	Name	Assignment Start	Assignment End
No Data			

Default Jobs

Click **Add**, to add the default job for the door.

- **Job Code:** Select the desired Job Code from the picklist. The Job Name appears once you select the Job Code.

- **Name:** Select the desired Name from the picklist. The Job Code appears once you select the Name.
- **Assignment Start:** The Assignment Start date appears once you select the Job Code or Name. You can also specify the Assignment Start date, if required.
- **Assignment End:** The Assignment End date appears once you select the Job Code or Name. You can also specify the Assignment End date, if required.

Click **OK** and then click **Save**.

When the assignment date of the default job gets elapsed, then the particular job will be listed in **Previous Default Jobs** section.

Assign Users



Assign Users is applicable for both Direct Door and Panel Door.

You can select and assign users to the door.


On the **Device configuration** page, click **Assign Users**. The Assign Users page appears.

ID	Name	
1111	Test_08	
105	Test_105	
1000	test_15	
1	ar3	

- **Users:** Click the picklist. The Picklist For All Users window appears.

Select the check boxes of the desired Users and click **OK**.

The grid displays the list of selected users.

If you wish to remove any assigned user, click the respective **Delete**  icon.

- Click **Save**.

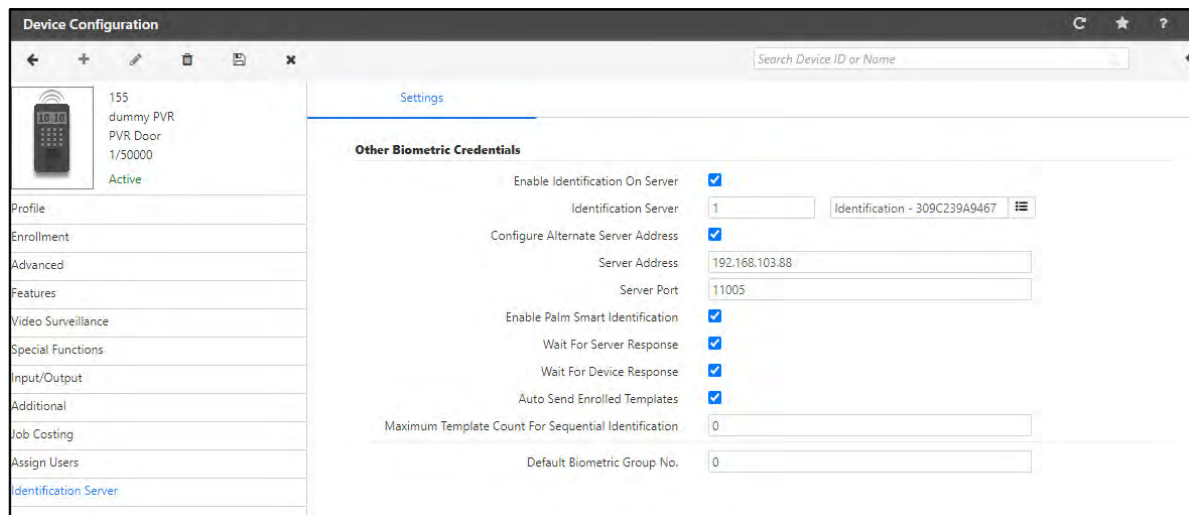
Identification Server

This tab enables the device to be assigned to a pre-defined Identification Server.

The door has a limited memory capacity for storage of templates so, we can assign an Identification Server which will store the templates for the door and will respond to the door when asked for identification.

For more information on Identification Servers, refer to [“Identification Server”](#).

On the **Device Configuration** page, click the **Identification Server** tab in the left pane.



Settings

Configure the following parameters:

Other Biometric Credentials

- **Enable Identification On Server:** Select this check box to enable identification of palm/finger templates on this device.
- **Identification Server:** Select an Identification Server using the picklist button to which the device is to be assigned. The configuration of Identification Server is done from **Admin module > System Configuration > Identification Server Configuration** and make sure you start the Identification Service from the service tray. This IP Address of this Identification Server is displayed in **Server Address**.
- **Configure Alternate Server Address:** Select this check box to configure an external IP Address of the FR Identification Server and configure the Server Address.
 - **Server Address:** By default it displays the IP Address of the selected Identification Server. Enter the external network IP address which will be used for accessing Identification Server.
- **Server Port:** Enter the TCP Port number. Default: 11005.
- **Enable Palm Smart Identification:** Select this check box to enable Palm templates Identification through Identification Server for this device.

- **Wait For Server Response:** Select this check box if the Identification Server should wait for response from the COSEC Server before identifying a user. If enabled, the Identification Server will request the device as well as the COSEC Server to search for the template and wait till the response is received from the COSEC Server (even if a matching palm template is found locally).
- **Wait For Device Response:** Select this check box if the Identification Server should wait for response from the COSEC Device before identifying a user. If enabled, the Identification Server will request the device as well as the COSEC Server to search for the template and wait till the response is received from the device.
- **Auto Send Enrolled Templates:** Select this check box to enable any enrolled templates to be saved both in the COSEC database as well as saved locally in the configured Identification Server. This enables prompt identification of user on enrollment.
- **Maximum Template Count for Sequential Identification:** Specify the Maximum number of Templates upto which identification will be done locally through device after which the request will be forwarded to the Identification Server. For details, "[Device](#)" in Global Policy.
- **Default Biometric Group No.:** Specify the default Biometric Group Number to be assigned to the device. It is a number allotted to a device to be assigned to the Identification Server. This enables the Identification Server to match the template against only those devices that belong to the corresponding biometric group. This reduces false detection as well time to search template.

Accessing the Door using QR code

The user can access the COSEC device using COSEC APTA installed in the mobile device. If the user has rights for COSEC APTA and access to this device is allowed to the user, then he can use his mobile device to scan the QR code which constitute the details of the door.

There is icon for QR code on COSEC APTA application. Clicking that icon will open the camera in your mobile. Now using the mobile camera you can scan the device QR code. The COSEC door will open after verifying the security key and access policies assigned to the user.

Steps to create a QR code

Step 1: Enter details in JSON format

```
{"version":"x","ip": "x.x.x.x","port":"x","pdid":"x","mode":"x"}
```

Valid values:

Field	Field range	Default Value	Remark
version	1-255	1	
ip	0.0.0.0-255.255.255.255	0.0.0.0	
port	0-65535	0	

Field	Field range	Default Value	Remark
pdid	0-255	0	If door is in direct door mode then, then PDID will be 0 If door is in panel door mode then, PDID will have values from 1-255
mode	0,1	0	0= for entry mode 1=for exit mode



Notes for Step1

- If door is in direct door mode enter IP and port of the direct door
- If door is a panel door, then enter IP and port of the panel door and in the pdid specify the door id which is to be accessed.

Step 2: Encrypt the JSON string using key "matrix12" with simple DES/ECB mode.

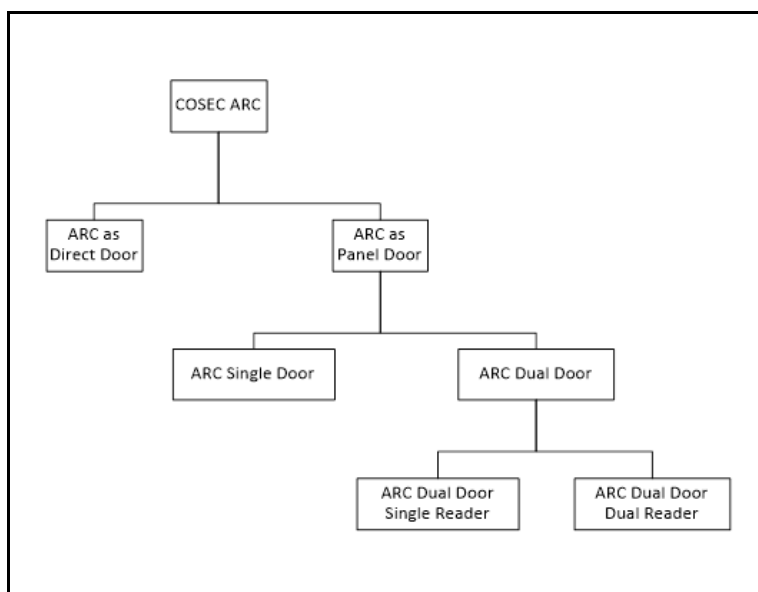
Step 3: Encode the encrypted string using Base 64.

Step 4: Use this string to generate QR code through any third party software.

ARC Door

COSEC ARC is an intelligent compact panel with PoE for two doors. The COSEC ARC can control two readers on Wiegand or RS-485, door lock and other auxiliary devices making it an ideal solution for any access control installation. **ARC DC100** and **ARC DC200** can be connected as **Direct Door** as well as **Panel Door**.

ARC DC100 and ARC DC200



To know more about configuring devices, click on the links for different tabs of Device configuration.

- [“Profile”](#)
 - [“ARC as Panel Door”](#)
 - [“ARC as Direct Door”](#)
- [“Enrollment”](#)
- [“Advanced”](#)
- [“Features”](#)
- [“Video Surveillance”](#)

- *“Special Functions”*
- *“Input/Output”*
- *“Additional”*
- *“Job Costing”*
- *“Assign Users”*
- *“Identification Server”*

Profile

This section enables the user to set up the basic profile for any new device. Setting up a door profile involves defining basic parameters to set up any door controller device.

On the **Device Configuration** page, select the **Profile** tab. The Profile can be configured in the following sections:

“ARC as Panel Door”

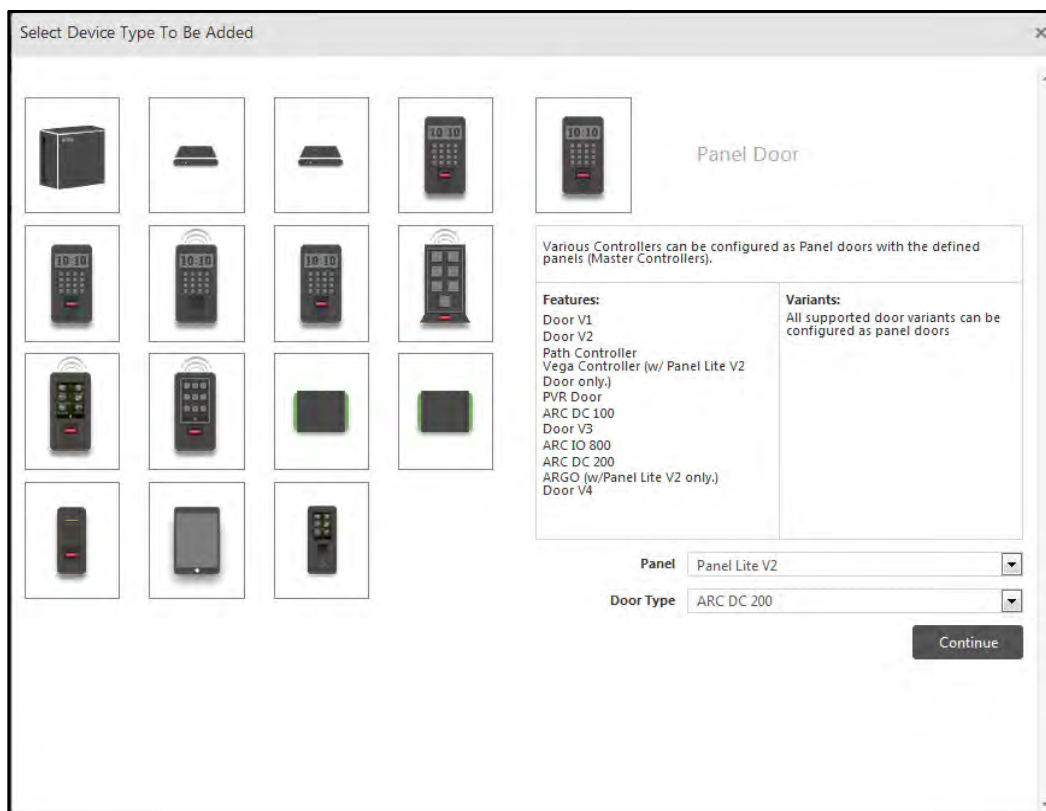
- *“Basic”*
- *“Readers”*
- *“General”*

“ARC as Direct Door”

- *“Basic”*
- *“Readers”*
- *“Access Settings”*
- *“General”*

ARC as Panel Door

To add ARC as Panel Door, click Panel Door from the device selection window and select the Panel as Panel Lite/ Panel200 and the door type as ARC DC100/ARC DC200. Then click Continue.



The Device Configuration window appears as shown below.

The screenshot shows the 'Device Configuration' window with the 'Basic' tab selected. On the left, a sidebar lists configuration sections: Profile, Advanced, Video Surveillance, Input/Output, Job Costing, and Assign Users. The main area is divided into 'Readers' and 'General' sections. Under 'Readers', fields include Sequence Number (3), Mode (Single Door), Connect Doors With (Dual Reader), Device (1), Connection Type (Ethernet), IP Address, MAC Address, and an Active checkbox. An 'Optional' section below contains Site (1), Consider For Attendance (checked), Alert Messages, Access Zone (Zone-1), Access Cluster (Cluster-1), Door Group (None), and Auto IP Assignment (checked).



The Monitor Service must be running while adding the device to COSEC.

Basic

Sequence Number - This is a system generated sequence number for each new device.

Mode: For connecting ARC as single door, select the mode as **Single Door**. For connecting ARC as dual door (ARC as 2door) select the Mode as **Dual Door**.

Connecting ARC as Single Door

This screenshot shows the 'Device Configuration' window with the 'Basic' tab selected. The left sidebar shows a list of devices, with '1 ARC as Single...' selected. The main area shows the configuration for this device. Under the 'Readers' section, the Mode is set to 'Single Door' (indicated by an arrow), and the Device name is 'ARC as Single Door'. The 'Optional' section shows Site set to '1' and 'Consider For Attendance' checked. Other settings like Access Zone, Access Cluster, and Door Group are also visible.

Connect Doors with: When Dual Door Mode is selected, you can connect doors with either **Single reader** or **Dual reader**.

Device: Specify the name of the door. The ID of the door is auto generated by the system.

Connection Type - Specify the connection type as Ethernet or RS485.

IP address/MAC address: Enter the IP address and MAC address respectively of ARC DC100/ARC DC200. The IP address and MAC address of both the doors of ARC-2 door is same.



MAC address of door is required while manually adding the door to the COSEC Monitor. You can note the MAC address from the device web page.

Active - Check the box to activate the device on the network.



*To add the Device automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the “**Auto Add New Devices**” checkbox.*

*The device will be added automatically but make sure you enable the **Active** checkbox in order to connect the device to the network. Once the device is connected to the network, it will come online in COSEC Monitor.*

Click **Save** button to save the configuration.

Optional

The optional tab shows the following configuration.

- **Site** - Select the site to which this door is to be assigned from the site picklist window. Site is created from Devices> Masters> Site.
- **Consider for Attendance** - Select this checkbox if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as access control events.
- **Alert Messages** - Select this checkbox to enable the application to send alerts based on events from this door.
- **Access Zone** (only for panel doors) - Assign an access zone to the door by selecting from the drop down menu.



Access Zone, Access Cluster, Door Group are configured while configuring Panel/Panel lite/Panel200.

- **Access Cluster** (only for panel doors) - Assign an access cluster to the door by selecting from the drop down menu.
- **Door Group:** Door Group drop down includes list of all configured Door groups on corresponding panel. An additional option as 'None' is available and selected by default.
- **Auto IP Assignment:** There is option where panel door can be assigned its IP from device webpage. To enable this check the Auto IP Assignment box.

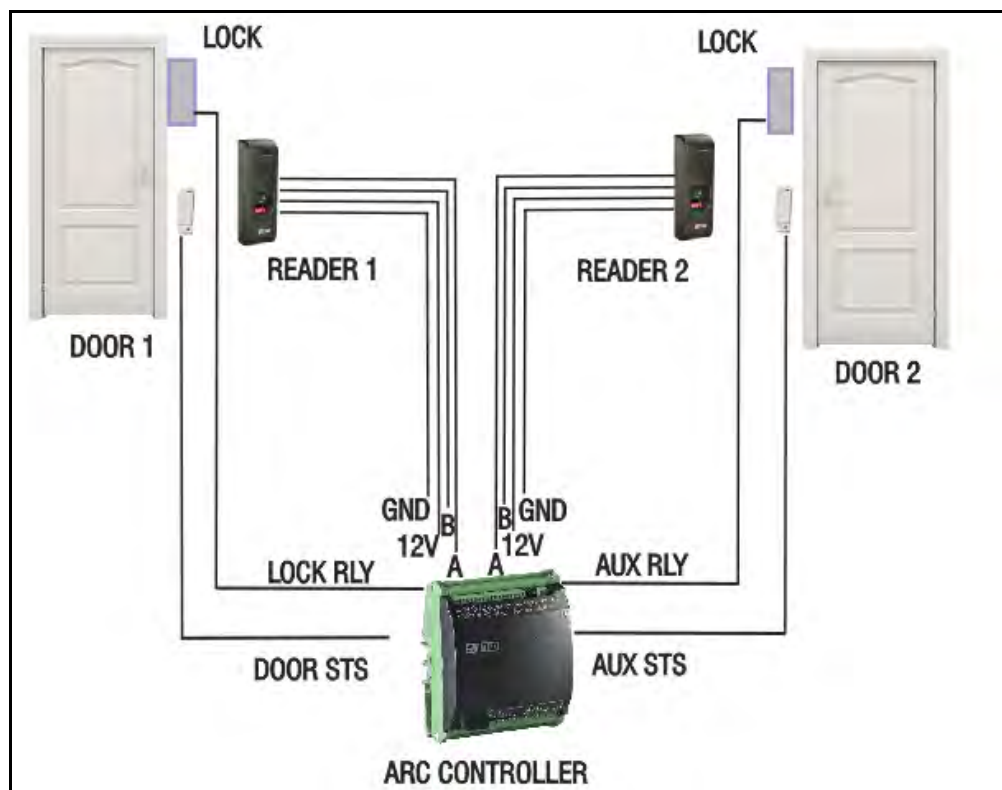
Connecting ARC as Dual Door

ARC-2 door can be connected as Panel door only. The 2 doors will have the same IP address and MAC address.

1. ARC Dual Door- Dual Reader- Working

Two readers connected to ARC-2-Door will point to 2 separate Panel doors virtually by the system so as to control two separate physical doors using a single arc-controller. You can connect PATH readers or any other supported readers to ARC DC100/ARC DC200.

- Both the readers will have the same MAC and IP Address.
- Both the readers can be assigned different zones, polices as per choice.
- As there will be only one reader per physical door hence both ENTRY/EXIT cannot be monitored on a physical door.
- The exit reader can only be connected with the reader1 since there is only one PIN available for this purpose.



Device Configuration

Device ID: [icon]
 Device Name: Panel Lite V2 Door
 ARC DC 200
 Panel Lite V2
 Active/Inactive

Basic

Sequence Number: 3
 Mode: Dual Door
 Connect Doors With: Dual Reader
 Device: 1
 Connection Type: Ethernet
 IP Address: 192 . 168 . 104 . 112
 MAC Address: 00 : 1B : 09 : 03 : E5 : 29
 Active: ☒

Optional

Site: 1 Site-1: Site-1
 Consider For Attendance: ☒
 Alert Messages: ☐
 Access Zone: Zone-1
 Access Cluster: Cluster-1
 Door Group: None
 Auto IP Assignment: ☒



Once the door is added and connected, it will be shown in Device Status as shown below. The IP address and MAC address of both the doors of ARC-2 door is same.

Device Status

Filter List: All Device Type: All Device Status: All Group By: None

Name	Status	IP	MAC Address	Device Type	Site
Panel lite V2			EF:54:76:8D:87:BF	Panel Lite V2	
Panel Lite V2-Device-4		192.168.104.111	00:1B:09:03:F3:83	Panel Lite V2	
PVR as Panel door		192.168.104.113	00:1B:09:03:F2:B0	Panel Lite V2 Door	Waghodia Site
Path as Panel door		192.168.105.2	54:76:8F:46:76:87	Panel Lite V2 Door	Waghodia Site
ARC as Single Door		192.168.105.3	DF:34:64:75:56:E3	Panel Lite V2 Door	Waghodia Site
ARC as Dual Door		192.168.104.112	00:1B:09:03:E5:29	Panel Lite V2 Door	Waghodia Site
ARC as Dual Door		192.168.104.112	00:1B:09:03:E5:29	Panel Lite V2 Door	Waghodia Site

Connection Example:

When a reader (eg: PATH reader) is connected to ARC DC100/ARC DC200, connect the cables as mentioned below.

ARC Reader2 terminal

A+
 B-
 12V
 GND

PATH RDFI terminal

Small connector - Blue
 Small connector - Brown
 Big connector- Red
 Big connector- Black

Aux o/p port in ARC DC must be used as door relay for reader 2.
 Aux i/p port in ARC DC must be used as door status for reader 2.
 Unused pin in ARC DC must be used as exit switch for reader 2.

Both the doors of Arc as dual door will act as individual doors.

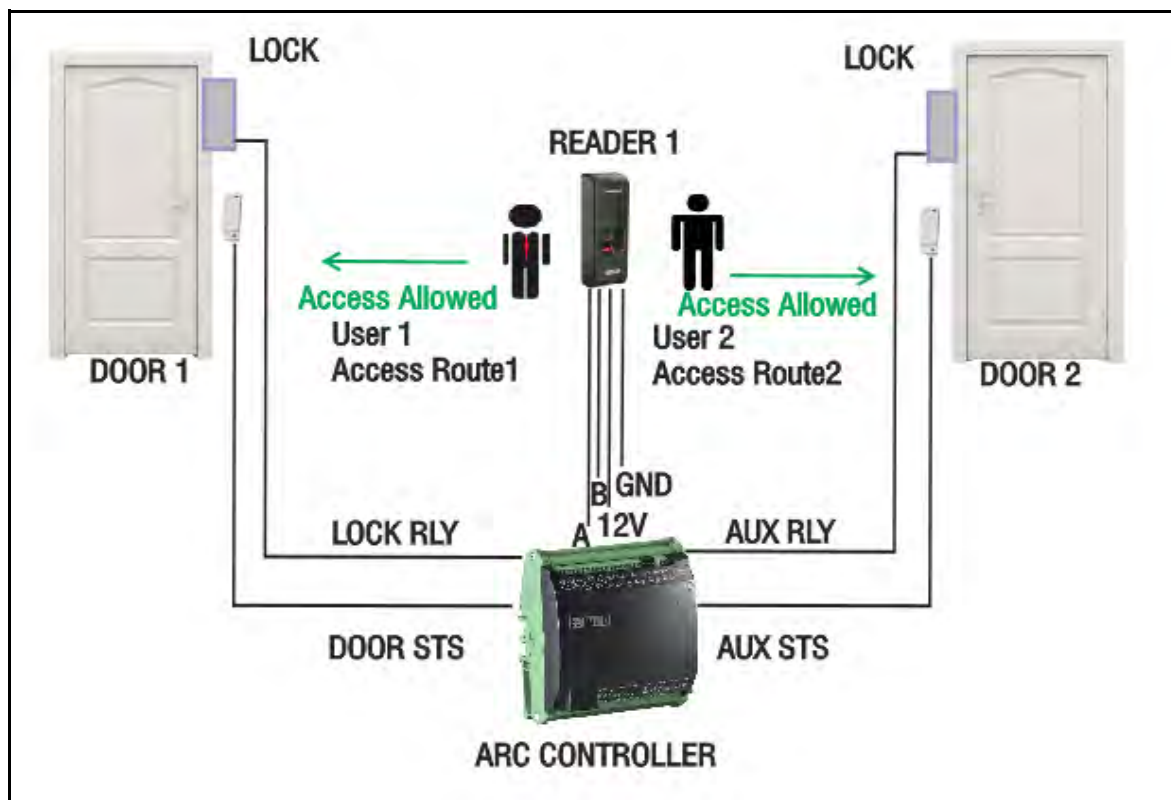
Thus, 2 sets of configurations will be generated and dispatched every-time whenever any of the parameters in one of the two door's (Dual Door) Configuration gets changed.

2. ARC Dual Door- Single Reader: Working

Single reader (Door controller) connected to ARC-2-Door will point to 2 separate Panel doors virtually by the system so as to control two separate physical doors using a single arc-controller. In this both the door will have same Reader Configuration except Exit Switch checkbox.

You can connect PATH readers or any other supported readers to ARC DC100/ARC DC200.

- The Door controller or the Reader must be connected to Reader1 port of ARC.
- LOCK Relay is connected to physical Door 1 and AUX Relay is connected to physical Door 2.
- As there is only 1 reader; If user punches on reader 1 and user is allowed on both doors then both doors will be opened simultaneously.
- If User1 is assigned Access Route1; then only Door1 will be opened when he punches on Reader1. similarly User 2 who is assigned Access Route2 can access Door2 only when he punches on Reader1.



Readers

Readers are important hardware components in a biometric door device. They may be internal or external. This section enables the administrator to configure both internal and external readers for a door as shown.

ARC as Single Door Dual Reader

Configure the following parameters for ARC DC200 as Single Door- Dual Reader:

- **Advertise Bluetooth-** Select this checkbox to enable Bluetooth of ARC DC200 and it will be visible to others. Then configure the following parameters.
- **Bluetooth Name-** By default, if the Device Name is configured then it will be displayed here.

If required, you can configure the bluetooth name as per your requirement. The Bluetooth Name can be a maximum of 10 characters.

- **Bluetooth Range-** The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m - 2m), Medium (5m - 7m) or Long (> 8m).

Reader Group1/ Reader Group2

Configure the following parameters for Reader 1 or Reader 2:

The screenshot displays the configuration interface for two reader groups. Each group has a search bar, a table for member configuration, and a mode dropdown. Reader Group 1 is set to 'Entry' mode, while Reader Group 2 is set to 'Exit' mode.

Member No	Card Format	Configurable Bits
1	Default Format	0

- **Wiegand Reader:** You can select **Short-Range Reader**, **Long-Range Reader**, **PIN-W Reader** or **CB W Reader**.

Select **Short-Range Reader** to identify the user from a short distance.

Select **Long-Range Reader** to identify the user from a long distance.

Long range reader is used at boom barriers where the user vehicle is identified by reading the tag on vehicle.

Select **PIN-W Reader** to support PIN pad device and accept the PIN from pin pad for identifying the user.

CB W Reader is a slave reader that works over BLE module.

Example: Punching on door via bluetooth technology of mobile.

- **RS-485:** Select the desired reader type to be connected on RS-485 port.

For the type of the supported Card/Credentials in the variants of each reader, refer [“Reader Types and supported credentials”](#)

- **Card Format:** For ARC as panel door; you can assign multiple card format.

To assign multiple card formats to device click on Add button. Then click the picklist to select the card format. And click OK to save the format.

Similarly you can add maximum 5 card formats. When the card format is saved, the Configurable bits of that format as configured from Masters> Card format will be displayed here.

Multiple Card format configurations will be dispatched to door separated by '**Format ID**' that is 'Member No.' along with all other format related parameters.

- **Configure Bluetooth from Server:** When you select **RS-485** as — CB U Reader, ATOM RD300, ATOM RD200 or ATOM RD100, select **Configure Bluetooth from Server** checkbox to enable Bluetooth feature of aforementioned readers.

The screenshot displays the 'Reader Group' configuration window, divided into two sections: 'Reader Group 1' and 'Reader Group 2'.

Reader Group 1:

- Wiegand Reader:** Short - Range Reader
- RS-485:** CB U Reader
- Search:** (Empty search bar)
- Table:**

Member No	Card Format	Configurable Bits
1	Default Format	0
- Mode:** Entry
- Configure Bluetooth From Server:** ☒
- Advertise Bluetooth:** ☐
- Bluetooth Name:** (Empty text field)
- Bluetooth Range:** Medium (5m - 7m)

Reader Group 2:

- Wiegand Reader:** Short - Range Rez
- RS-485:** ATOM RD300
- Search:** (Empty search bar)
- Table:**

Member No	Card Format	Configurable Bits
1	Default Format	0
- Mode:** Exit
- Configure Bluetooth From Server:** ☒
- Advertise Bluetooth:** ☐
- Bluetooth Name:** (Empty text field)
- Bluetooth Range:** Medium (5m - 7m)

Once you enable **Configure Bluetooth from Server**, configure the following Bluetooth parameters:

- **Advertise Bluetooth-** Select this checkbox to enable Bluetooth of the reader. Then configure the following parameters
- **Bluetooth Name-** By default, if the Device Name is configured then it will be displayed here along with the Mode. The prefix will be the Device Name and the suffix will be -IN or -OUT as per the set Mode.

- If required, you can configure the bluetooth name as per your requirement. The **Bluetooth Name** can be a maximum of 20 characters.
- **Bluetooth Range**- The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m-2m), Medium (5m-7m) or Long (>8m).

- **Mode**: Select the Mode as **Entry** or **Exit** for both the reader groups from the drop down list.
- **Enrollment Via**: Select the preferred enrollment option — Reader Group1, Reader Group2 or Device.



Make sure you have configured the desired Readers (as per the credentials you wish to enroll) in Reader Group 1 and Reader Group 2. To configure the Readers, refer "[Reader Group1/ Reader Group2](#)".

- **Exit Switch** - Select this checkbox to enable the use of **Exit Switch**.

ARC as Dual Door- Single Reader



In ARC as dual door; changing any of the control value in Reader of one Door will also change the value of this control in Reader of second door.

DOOR 1

The screenshot shows the configuration interface for Door 1, specifically the **Readers** tab. The interface is divided into three sections: **Basic**, **Readers** (active), and **General**.

Basic Section:

- Advertise Bluetooth:** A checkbox that is currently unchecked.
- Bluetooth Name:** A text input field.
- Bluetooth Range:** A dropdown menu set to "Medium (5m - 7m)".

Readers Section:

- Door Group:** A header for the reader configuration.
- Wiegand Reader:** A dropdown menu set to "Short - Range Reader".
- RS-485:** A dropdown menu set to "EM Prox Reader".
- Search:** A search bar with a magnifying glass icon.
- Member No:** A table with one row showing "1".
- Card Format:** A table with one row showing "Default Format".
- Configurable Bits:** A table with one row showing "0".
- Mode:** A dropdown menu set to "Entry".
- Enrollment Via:** A dropdown menu set to "Reader Group 1".
- Exit Switch:** A checkbox that is checked.

Configure the following bluetooth parameters for ARC DC200 Door 1:

Advertise Bluetooth- Select this checkbox to enable Bluetooth of ARC DC200 Door 1. Then configure the following parameters

Bluetooth Name- By default, if the Device Name is configured then it will be displayed here.

If required, you can configure the bluetooth name as per your requirement. The **Bluetooth Name** can be a maximum of 10 characters.

Bluetooth Range- The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m-2m), Medium (5m-7m) or Long (>8m).

Door Group

Select the **Wiegand reader** or **RS- 485** reader for connecting ARC with desired reader.

The default **card format** is assigned. to the reader. You can also assign multiple card formats. See section *ARC as Single door* for Card format description.

You can select the **Mode** of the reader as Entry or Exit.

You can enable the **Exit Switch** if required.

For Dual door with single reader, **Exit Switch** checkbox can be set differently for both doors i.e. for one door it can be enabled, while for the other door it can be disabled.

When you select **RS-485** as — CB U Reader, ATOM RD300, ATOM RD200 or ATOM RD100, select **Configure Bluetooth from Server** checkbox to enable Bluetooth feature of aforementioned external readers.

Once you enable **Configure Bluetooth from Server**, configure the following Bluetooth parameters:

Advertise Bluetooth- Select this checkbox to enable Bluetooth of the reader. Then configure the following parameters:

Bluetooth Name- By default, if the Device Name is configured then it will be displayed here along with the Mode. The prefix will be the Device Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the name of bluetooth as per your requirement. The **Bluetooth Name** can be a maximum of 20 characters.

Bluetooth Range- The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m-2m), Medium (5m-7m) or Long (>8m).

Click on the **Save** button.

DOOR 2

For 2nd Panel of ARC dual door, configure the Bluetooth parameters — Advertise Bluetooth, Bluetooth Name and Bluetooth Range.

The screenshot shows the 'Readers' configuration tab. At the top, there are three tabs: 'Basic', 'Readers' (selected), and 'General'. Under 'Readers', the 'Advertise Bluetooth' checkbox is checked. Below it, the 'Bluetooth Name' is set to 'device' and the 'Bluetooth Range' is set to 'Medium (5m - 7m)'. A 'Door Group' section is expanded, showing an 'Exit Switch' checkbox which is also checked.

Under the **Door Group**, select **Exit Switch** checkbox so that the door can be opened without checking for any access policies.

Click **Save**.

ARC as Dual Door- Dual Reader

Configure the following parameters of ARC DC200 as Dual Door - Dual Reader:

The screenshot shows the 'Readers' configuration tab for the ARC DC200. The 'Advertise Bluetooth' checkbox is unchecked. The 'Bluetooth Name' field is empty, and the 'Bluetooth Range' is set to 'Medium (5m - 7m)'. The 'Door Group' section is expanded, showing 'Wiegand Reader' set to 'Short - Range Reader' and 'RS-485' set to 'EM Prox Reader'. Below this is a search bar and a table with columns 'Member No', 'Card Format', and 'Configurable Bits'. The table has one row with '1' in the first column, 'Default Format' in the second, and '0' in the third. There are edit and delete icons for this row. Below the table, the 'Mode' is set to 'Entry'. At the bottom, 'Enrollment Via' is set to 'Reader Group 1' and the 'Exit Switch' checkbox is checked.

- **Advertise Bluetooth**- Select this checkbox to enable Bluetooth of ARC DC200 and it will be visible to others. Then configure the following parameters.
- **Bluetooth Name**- By default, if the Device Name is configured then it will be displayed here.

If required, you can configure the bluetooth name as per your requirement. It can be a maximum of upto 10 characters.

- **Bluetooth Range-** The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m - 2m), Medium (5m - 7m) or Long (>8m).

Door Group

- **Wiegand Reader:** Select a desired Wiegand Reader — **Short-Range Reader, Long-Range Reader, PIN-W Reader or CB W Reader.**

Select **Short-Range Reader** to identify the user from a short distance.

Select **Long-Range Reader** to identify the user from a long distance.

Long Range Reader is used at boom barriers where the user vehicle is identified by reading the tag on vehicle.



Select **PIN-W Reader** to support PIN pad device and accept the PIN from pin pad for identifying the user.

CB W Reader is a slave reader that works over BLE module.

Example: Punching on door via bluetooth technology of mobile.

- **RS-485:** Select the desired reader type to be connected on RS-485 port.

For the type of the supported Card/Credentials in the variants of each reader, refer [“Reader Types and supported credentials”](#)

- **Card Format:** For ARC as panel door; you can assign multiple card format. To assign multiple card formats to device click on Add button. Then click the picklist to select the card format. And click **OK**  to save the format and to discard the format, click **Cancel** .

Similarly you can add maximum 5 card formats. When the card format is saved, the Configurable bits of that format as configured from Masters> Card format will be displayed here.

Multiple Card format configurations will be dispatched to door separated by 'Format ID' that is 'Member No.' along with all other format related parameters.

- **Configure Bluetooth from Server:** When you select **External Reader Type** as — CB U Reader, ATOM RD300, ATOM RD200 or ATOM RD100, select **Configure Bluetooth from Server** checkbox to enable Bluetooth feature of aforementioned readers.

Once you enable **Configure Bluetooth from Server**, configure the following Bluetooth parameters:

- **Advertise Bluetooth-** Select this checkbox to enable Bluetooth of the reader. Then configure the following parameters:
- **Bluetooth Name-** By default, if the Device Name is configured then it will be displayed here along with the Mode. The prefix will be the Device Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the name of bluetooth as per your requirement. The **Bluetooth Name** can be a maximum of 20 characters.

- **Bluetooth Range-** The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m-2m), Medium (5m-7m) or Long (>8m).

- **Mode:** Select the Mode as **Entry** or **Exit** for the door groups from the drop down list.
- **Enrollment Via:** Select the preferred enrollment option — Reader Group1,Reader Group2 or Device.

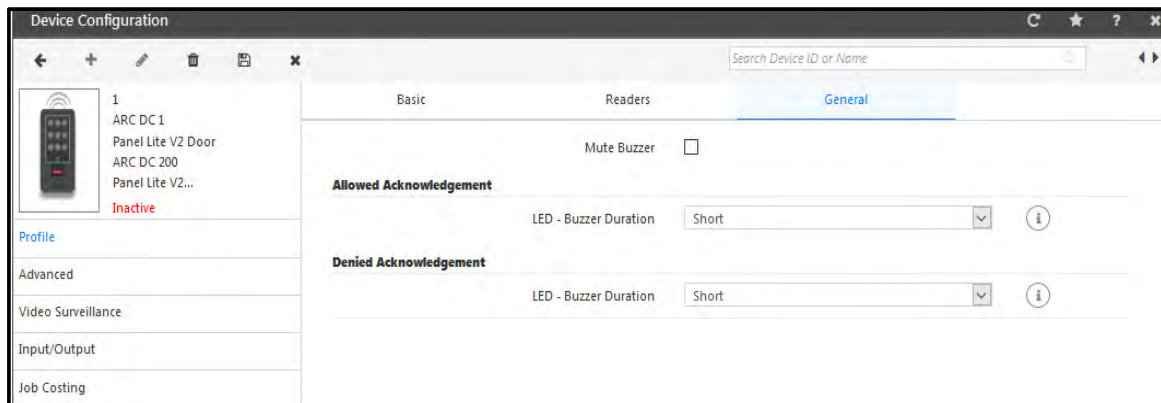


Make sure you have configured the desired Readers (as per the credentials you wish to enroll) in Reader Group 1 and Reader Group 2.

- **Exit Switch** - Select this checkbox to enable the use of **Exit Switch**.

General

The **General** page appears as follows.



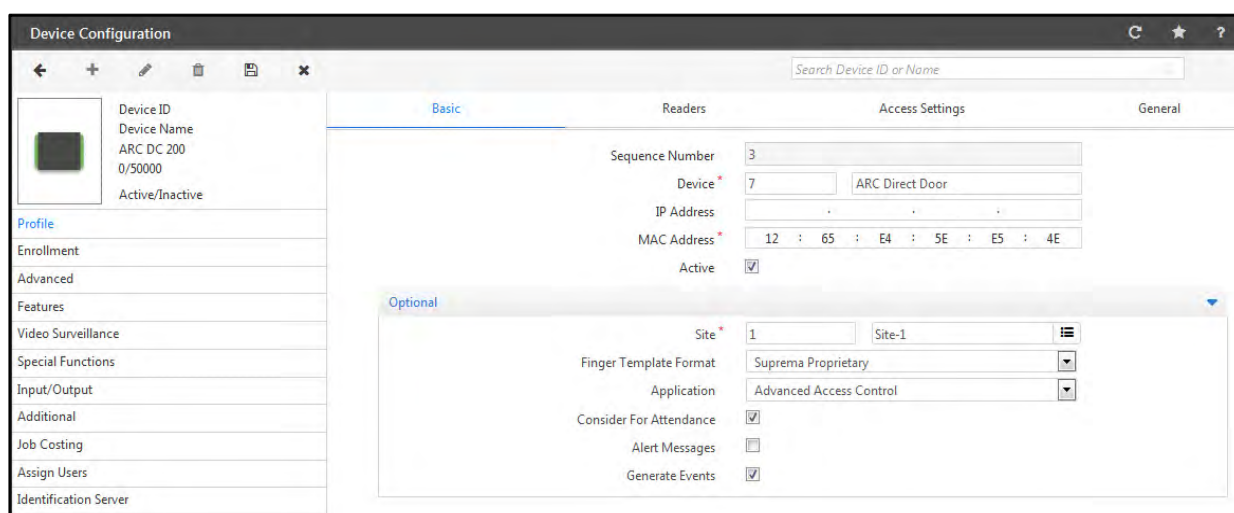
- **Mute Buzzer** - You can enable the check-box to mute the door buzzer.
- **Allowed Acknowledgment**
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.
- **Denied Acknowledgment**
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.

ARC as Direct Door



The Device Configuration page for ARC Door appears as shown below.

Basic



Sequence Number - This is a system generated sequence number for each new device.

Device: Specify the name of the door. The ID of the door is auto generated by the system.

Enter the **MAC address** of the door. The **IP address** will be displayed automatically once the device comes online in Monitor.

To add Devices automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the “Auto Add New Devices” check-box. Once the device is connected in network, it will come online in COSEC Monitor.

Active - Check the box to activate the device on the network.

Click **Save** button to save the configuration.



The Monitor Service must be running while adding the device to COSEC.

The **Basic** page also has an **Optional** tab which provides optional configurations as shown below:

- **Site** - Select the site to which this door is to be assigned from the site picklist window. Site is created from Devices> Masters> Site.
- **Finger Template Format** - Select the format as Suprema Proprietary or Suprema ISO according to which the templates will be enrolled. For globally setting the template format, you can set from Global policy.
- **Application** - Select the application type for which the device is to be used. The options are **Basic Access Control** and **Advanced Access Control**.



The available license is ACS and Application is set to Basic Access Control. If this ACS voucher exhausts, then while dispatching Basic Configuration of device, application type will be sent as 'Advance Access Control'.

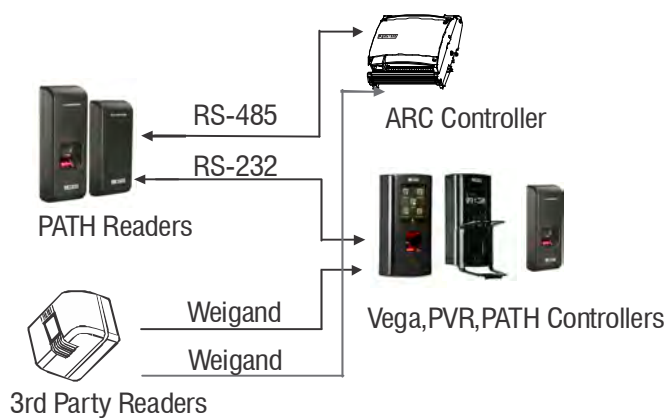
- **Consider for Attendance** - Select this checkbox if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as access control events.
- **Alert Messages** - Select this checkbox to enable the application to send alerts based on events from this door.
- **Generate Events**: For ARC DC200, this check-box is enabled by default. You can disable the check-box if the server is not required to receive any events from the respective devices.

Readers

Readers are important hardware components in a biometric door device. They may be internal or external. This section enables the administrator to configure both internal and external readers for a door as shown.

For Arc as Direct Door, configuration must be set separately for Reader Group 1 and Reader Group 2.

The screenshot displays the 'Readers' configuration page in the Matrix COSEC System. The left sidebar lists various system settings, with 'Readers' being the active section. The main configuration area is divided into tabs: Basic, Readers (selected), Access Settings, and General. Under the 'Readers' tab, there are checkboxes for 'Auto Detect Readers' and 'Advertise Bluetooth'. Below these are fields for 'Bluetooth Name' and a 'Bluetooth Range' dropdown menu set to 'Short (1m - 2m)'. The configuration is then split into two sections: 'Reader Group 1' and 'Reader Group 2'. Each group contains a table with columns for 'Member No', 'Card Format', and 'Configurable Bits'. For Reader Group 1, the 'Wiegand Reader' is set to 'Short - Range Reader' and the 'RS-485' is set to 'EM Prox Reader'. For Reader Group 2, the 'Wiegand Reader' is set to 'Short - Range Reader' and the 'RS-485' is set to 'CB U Reader'. Both groups have a 'Mode' dropdown set to 'Entry' and 'User Access Mode' and 'Visitor Access Mode' dropdowns set to 'Any One'. At the bottom of the configuration area, there are checkboxes for 'Enrollment Via', 'Exit Switch', and 'Access Control On Exit Mode'.



Auto Detect Readers - Select this checkbox to enable auto detection of Readers on a door controller connected to the server.

Advertise Bluetooth- Select this checkbox to enable Bluetooth of ARC DC200 Door 1. Then configure the following parameters

Bluetooth Name- By default, the **Device** Name assigned is displayed along with the set **Mode**. You can change it as per your requirement. Name can be a maximum of 10 characters.

Bluetooth Range- The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m-2m), Medium (5m-7m) or Long (>8m).

Reader Group1/ Reader Group2

- **Wiegand Reader:** You can select **Short-Range Reader**, **Long-Range Reader**, **PIN-W Reader** or **CB W Reader**.
The short-range reader is used where the user can access the door at short distance i.e. where the short distance identification can be done. Eg: Punching on the door by showing user credential on door. Long range reader is used at boom barriers where the user vehicle is identified by reading the tag on vehicle.
- **RS-485:** Based on the COSEC PATH Reader (RDFM, RDFE, RDFI, RDFF, RDCM, RDCE, RDCI) and Reader CB; Select the reader type to be connected on RS-485 port. (M- MiFare, E-EM Prox, I- HID iClass, P-HID Prox,CB U Reader).



*If Auto Detect Reader is enabled, then **Wiegand Reader** and **RS-485** parameters will not be visible.*

- **Card Format:** Only Single card format is applicable to ARC as direct door. The default card format is applied to ARC as direct door. To assign another card format for internal readers of the device; delete the default format and select another format from the picklist. **See Devices> Master> Card Format**
- **Mode:** Select the Mode as **Entry** or **Exit** for both the Reader groups.
- **User/Visitor Access Mode** - Select the desired user and visitor access mode for both reader groups.
- **Configure Bluetooth from Server:** When you select **External Reader Type** as — CB U Reader, ATOM RD300, ATOM RD200 or ATOM RD100, select **Configure Bluetooth from Server** checkbox to enable Bluetooth feature of aforementioned readers.

Once you enable **Configure Bluetooth from Server**, configure the following Bluetooth parameters:

- **Advertise Bluetooth-** Select this checkbox to enable Bluetooth of the reader. Then configure the following parameters:
- **Bluetooth Name-** By default, if the Device Name is configured then it will be displayed here along with the Mode. The prefix will be the Device Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the name of bluetooth as per your requirement. The **Bluetooth Name** can be a maximum of 20 characters.

- **Bluetooth Range-** The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m-2m), Medium (5m-7m) or Long (>8m).

- **Enrollment Via:** Select the preferred enrollment option — Reader Group1,Reader Group2 or Device.



Make sure you have configured the desired Readers (as per the credentials you wish to enroll) in Reader Group 1 and Reader Group 2. To configure the Readers, refer "[Reader Group1/ Reader Group2](#)".

- **Exit Switch** - Select this checkbox to enable the use of Exit Switch.
- **Access Control On Exit Mode** -Select this check box to enable the checking of the following access control policies on door when the external reader is in the 'exit' mode.
 - User enabled
 - User validity
 - Blocked user
 - Time Based Access Check
 - ASC
 - User Access Group

Access Settings

This section is available for direct doors. The **Access Settings** page appears as shown below:

The screenshot shows the 'Device Configuration' web interface. On the left is a sidebar with a list of configuration tabs: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, and Assign Users. The main area is titled 'Access Settings' and contains several configuration fields. At the top, there's a search bar for 'Search Device ID or Name'. Below that, the 'Universal Time Zone' is set to '(GMT+05:30)Chennai, Kolkata, New Delhi, Mumbai'. The 'Time Format' is set to '24 Hours'. The 'Auto Synchronize with NTP' checkbox is checked. Below this, the 'Preferred NTP Server' field is empty. Further down, the 'Working Days' section shows checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, Sat, and Holiday, all of which are checked. The 'Working Hours(HH:MM)' are set to '00:00' and '23:59'. At the bottom, there are four 'Holiday Schedule' entries, each with a number (1-4) and a corresponding 'Schedule' field with a calendar icon.

- **Universal Time Zone** - Select the geographic time zone in which the DOOR will operate.
- **Time Format** - Specifies the time format to be displayed on Door Controller LCD display. The formats available are:
 - 24 Hours
 - 12 Hours

Select the relevant option from the drop down list as per the site requirements.

Auto Synchronize with NTP

If Date and time is to be automatically synchronized as per the **Preferred NTP Server** (predefined or user-defined NTP server address) selected by user, then you must enable **Auto Synchronize With NTP** checkbox.

Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from device webpage, which will be reflected on device display.

- When Auto Synchronization with NTP is disabled Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 1. You can specify the Preferred NTP server of your choice. In this case device will first try to get Date and Time from that server address.
If it does not get Date and Time in three tries; device will check from pre-defined NTP servers.
If you have entered one of the three pre-defined NTP servers(ntp1.cs.wisc.edu , time.windows.com , time.nist.gov); then device will first check that server first.
If it receives updated Date and Time then Updated Date and Time will be reflected on device webpage and display screen.
 2. You can keep the Preferred NTP server as blank. In this case device will check for Date and Time from the first NTP server.

3. If user has manually entered Date and Time from webpage or Device Menu then those values of Date and Time will be reflected on device webpage and display screen.

In the case of the **Manual** option the administrator can manually update the time on the Door with that of the system time as and when required.

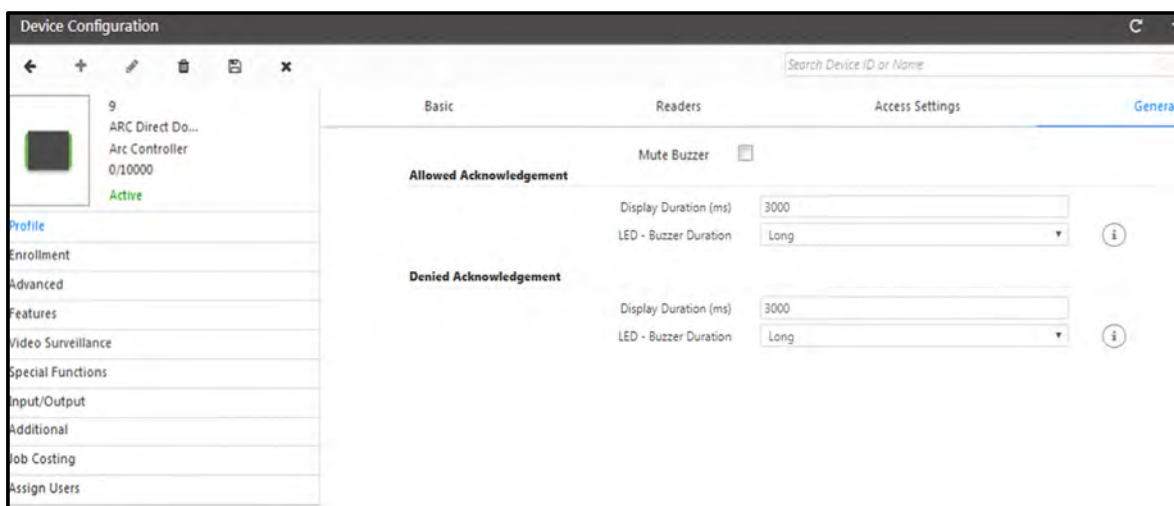
- **Working Days** - Specify the days on which the default working hours should be applicable. Check the relevant boxes to specify the active days.
- **Working Hours (HH:MM)** - Define the default working hours in HH:MM format.
- **Holiday Schedule** - This section allows the administrator to assign up to four holiday schedules to the device by using the Holiday Schedule picklist.



If the same holiday schedule is configured for a user and for the door controller on which the user is assigned, then the user's attendance marking on this device, on any of the scheduled holidays will always be marked as a holiday.

General

The **General** page appears as follows.



- **Mute Buzzer** - You can mute the door buzzer by checking the box respectively.
- **Allowed Acknowledgment**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgment Allowed' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.
- **Denied Acknowledgment**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgment Denied' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.

Enrollment



The Enrollment section is not available for panel doors.

The Enrollment page appears as shown below.

- **Enroll From Device** - Select this checkbox to enable the feature. This allows the user to specify the user credential that can be enrolled by using the enrollment devices such as DOOR Controllers.
- **Enrollment Mode** - Select the Credential from the drop-down list that can be enrolled using the special function at the DOOR. The options are **ReadOnlyCard**, **SmartCard**, **Biometric** and **BiometricthenCard**, and **DuressFinger**. Refer “[Enroll Credentials](#)” or “[Enrolling Users](#)” to enroll User/Worker. Refer “[Enrollment](#)” or “[Enroll Credentials](#)” to enroll Worker. Refer “[Enroll Credentials](#)” to enroll a Visitor.



DuressFinger is only applicable for User and Worker.

- **Template Per Finger** - This parameter displays the values as configured at the global level. This field is not user editable from this page.
- **Max Number of Fingers** - This parameter displays the values of the maximum number of fingers configured at the global level. This field is not user editable from this page.
- **Number of Fingers/Cards** - Select the number of cards or fingerprints to be enrolled based on the credential option selected in the Enrollment Mode parameter.

Advanced

The Advanced tab allows the user to configure some advanced parameters such as access control settings, alarms and device timers.

To access this, After selecting the device, Select the **Advanced** tab from **Device Configuration** page. The advanced settings can be configured from following two sections:

- “Settings”
- “Alarms”
- “Timers”

Settings

The **Advanced Settings** page for ARC as **Direct Door** appears on your screen as shown below:

Settings	Alarms	Timers
Device ID	Generate Exit Switch Events	
Device Name	Generate Invalid User Events	
ARC DC 200	Generate Sequential IN-OUT Events	
0/50000	Show PIN	
Active/Inactive	Allow Exit when Door Lock	
Profile	Auto Relock	
Enrollment	Auto Relock Timer (Sec)	
Advanced	Enable Additional Security	
Features	Reader Group 1-Tamper	
Video Surveillance	Reader Group 2-Tamper	
Special Functions	Enable Smart Identification	
Input/Output	Access Level	
Additional	Access Mode	
JobMS Costing	Auto Acknowledge Alarm	
Assign Users	Auto Acknowledge Alarm (Sec)	
Identification Server	Facility Code	
	Allow Access Through Mobile	
	Mobile Entry Access Mode	
	Mobile Exit Access Mode	

The following parameters are available for configuration:

- **Generate Exit Switch Events** - Select this checkbox to enable the door to generate events every time the exit switch is used.
- **Generate Invalid User Events** - Select this checkbox to enable the door to generate events for invalid user inputs.
- **Generate Sequential IN-OUT Events** - In ARC DC 200; select this checkbox to generate user punches on device as the sequential IN-OUT events irrespective of the mode in which device is functioning.
- **Show PIN** - Select this checkbox to display the characters of PIN when the PIN is entered on device.
- **Allow Exit when Door Lock** - Select this checkbox if users are to be allowed to exit even when the Door relay is in locked condition.
- **Auto Relock** - Select this checkbox to allow the door to relock immediately when the door status changes to close after normal open irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Relock Timer** - Specify the time in seconds for the Auto Relock operation.

- **Enable Additional Security** (for direct door) - Select this checkbox to enable additional security at the selected Door Controller.
- **Additional Security Code** - Enter a code (ranging from 1 to 65535) in the field provided. Re-enter the code to confirm.



*Changing this value can affect the SI function. Click on the **Default Code** button to reset the **Additional Security Code** to the value set in the **Global Additional Security Code** field on the Global System Policy page.*

- **Reader Group 1&2 - Tamper** - For **ARC Door** this option allows the configuration of tamper input for Reader Group 1 and Reader Group 2 and setting the default signal type as Normally Open (NO) or Normally Closed (NC).
- **Enable Smart Identification** - Select this checkbox to enable this functionality at the selected Door Controller and select the **Access Level** and the **Access Mode** from the drop down list.
- **Auto Acknowledge Alarm** - Select this checkbox to enable the auto-acknowledgment of all alarms for this device.
- **Auto Acknowledge Alarm (sec)** - Set the time in seconds for the Auto Acknowledge Timer. The wait timer will start and on expiry of the timer, the alarm buzzer will stop automatically.
- **Facility Code** - In ARC DC200, Set a value for Facility Code to be set for access modes other than "Card", if Facility Code is expected in Wiegand Output.
- **Allow Access Through Mobile**- Check the box to allow the access to device using COSEC ACS App.
- **Mobile Entry/Exit Access Mode**- Select the entry and exit door access mode from the options of **Mobile Only**, **Mobile then Biometrics**, **Mobile then Card** and **Mobile then PIN**.



If User Access Mode is selected as "None" in Zone Configuration and Mobile Access Mode is selected as "Mobile Then Biometrics" then door can be accessed through Mobile and then Biometric credential.

- **Advertise Bluetooth**- For ARC DC200; Check the box to enable Bluetooth of the device by which the device will be visible to others.
- **Bluetooth Name**- When "Advertise Bluetooth" checkbox is enabled, you can enter the bluetooth name. The default name is Matrix.
- **Bluetooth Range**- You can select the Bluetooth range as Short, Medium or Long based on which user can mark the attendance. Suppose if you select "Short" range; then user can mark the punch via Bluetooth from near by office premises only.
 - Short(1m-2m)
 - Medium(5m-7m)
 - Long (>8m)

By default, the range will be set to "Medium".
If you want to allow punch marking from long distance, then you can select "Long" range.

The **Advanced Settings** for ARC as **Panel door** is shown below:

For Single Door:

The screenshot shows the 'Advanced Settings' for a single door. On the left, a sidebar lists the device '1' as 'ARC DC 200 as...' and 'Panel Lite V2 Door'. The main area has three tabs: 'Settings', 'Alarms', and 'Timers'. The 'Alarms' tab is selected, showing the following settings:

- Auto Relock:** A checkbox that is currently unchecked.
- Auto Relock Timer (Sec):** A text input field containing the value '3'.
- Reader Group 1-Tamper:** A dropdown menu set to 'NO'.
- Reader Group 2-Tamper:** A dropdown menu set to 'NO'.
- Tail-Gating:** A checkbox that is currently unchecked.
- Reset Wait Timer:** A dropdown menu set to 'On Door Lock'.
- Man Trap Timer - Internal Reader (Sec):** A text input field containing the value '0'.
- Man Trap Timer - External Reader (Sec):** A text input field containing the value '0'.
- Enable Man Trap Door Interlocking:** A checkbox that is currently unchecked.
- Select Doors for Interlocking:** A section with two input fields labeled 'ID' and 'Name', followed by a list icon and an information icon.

For Dual Door:

The screenshot shows the 'Advanced Settings' for a dual door. On the left, a sidebar lists the device '1' as 'ARC DC 200 as...' and 'Panel Lite V2 Door'. The main area has three tabs: 'Settings', 'Alarms', and 'Timers'. The 'Alarms' tab is selected, showing the following settings:

- Auto Relock:** A checkbox that is currently unchecked.
- Auto Relock Timer (Sec):** A text input field containing the value '3'.
- Door Group - Tamper:** A dropdown menu set to 'NO'.
- Man Trap Timer - Internal Reader (Sec):** A text input field containing the value '0'.
- Man Trap Timer - External Reader (Sec):** A text input field containing the value '0'.
- Enable Man Trap Door Interlocking:** A checkbox that is currently unchecked.
- Select Doors for Interlocking:** A section with two input fields labeled 'ID' and 'Name', followed by a list icon and an information icon.

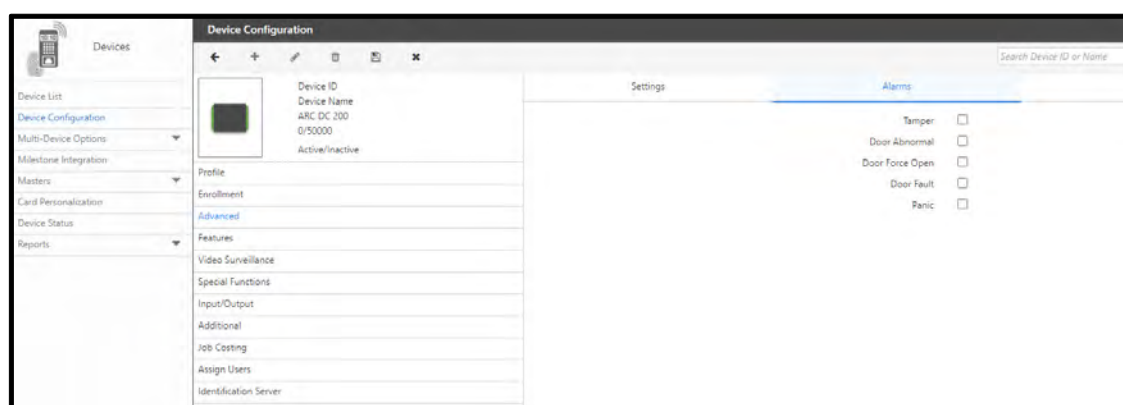
- **Auto Relock** - Select this checkbox to allow the door to relock immediately when the door status changes to close after normal open irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Relock Timer** - Specify the time in seconds for the Auto Relock operation.
- **Reader Group 1&2 - Tamper** - For **ARC as Single door**; this option allows the configuration of tamper input for Reader Group 1 and Reader Group 2 and setting the default signal type as Normally Open (NO) or Normally Closed (NC).
- **Door Group -Tamper** - For **ARC as Dual door**; this option allows the configuration of tamper input for dual doors and setting the default signal type as Normally Open (NO) or Normally Closed (NC).

- **Tail-Gating (For ARC as Single Door)**- Tail-gating refers to an access violation which occurs when more than one person tries to enter a secured area using a single person's access credentials. If this option is enabled on the panel door, the occupancy count of a zone should be incremented or decremented considering both the punch as well as the auxiliary input port of the panel door (say, input from a beam-counter). Set the wait timer for resetting the tailgating count (**Reset Wait Timer**) based on the door lock status or the door pulse wait timer (as configured).
- **Man Trap Timer -Internal Reader (Sec)** - This checkbox enables an alarm wait timer on the panel door to ensure that the user enters the next sequential door of a man-trap within a specific time-frame.
- **Man Trap Timer External Reader (Sec)** - This checkbox enables an alarm wait timer on the panel door to ensure that the user exits the panel door to enter the next sequential door of a man-trap within a specific time-frame.

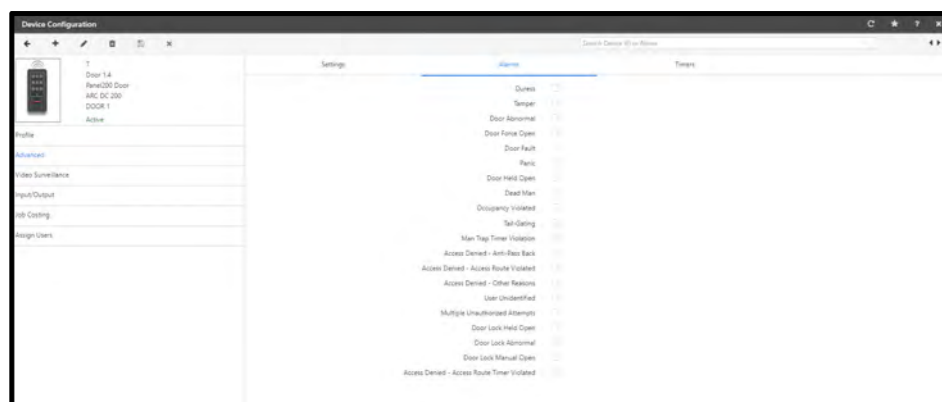
Alarms

In Alarm tab, you can assign below list of alarms to the door.

For Direct Door



For Panel Door



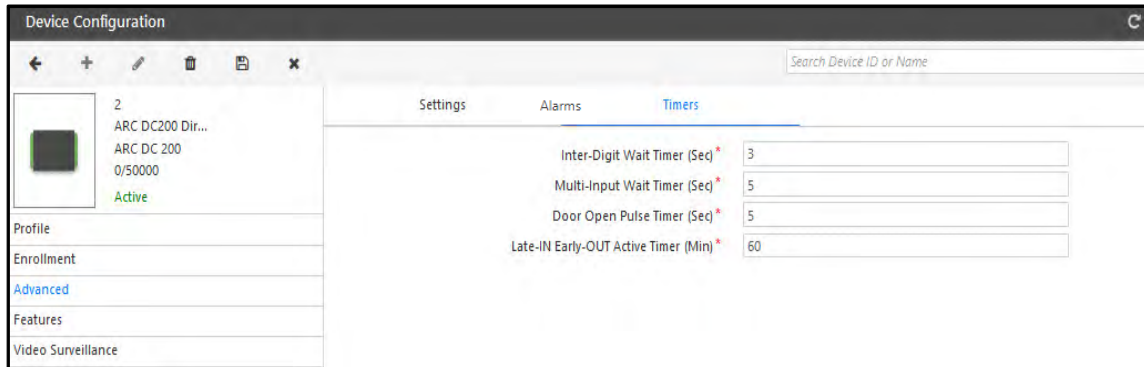
Select the respective checkbox of alarms which you want to enable.



The above list of alarms is available for the ARC DC 200. For ARC DC 100, the number of supported alarms may differ.

Timers

This section allows the configuration of various types of pre-defined device timers which can trigger off specific responses. In COSEC, timers are often used to control door behaviour and for triggering alarms. The **Timers** page appears on your screen as shown below:



- **Inter-Digit Wait Timer (sec)** - For ARC DC200, Specify the time period in seconds between two key inputs on the device keypad. On expiry of this timer, the system considers the user input to be complete and is ready for the next input.
- **Multi-Input Wait Timer (sec)** - Specify the time in seconds for which system needs to wait for the second credential input from the user when more than one credential is to be used to grant access.



We recommend you to set the timer value as greater than or equal to 10 seconds to avoid access denial issues to users. This is applicable when the system reads the credentials (biometric) from the user's Smart Cards.

- **Door Open Pulse Timer (sec)** - Specify the time in seconds (3 to 99) for the door to be energized for a valid credential. If the opened door does not return to a closed state before the expiry of this timer, the door will generate a "Door Abnormal" alarm.
- **Late-IN Early-OUT Active Timer (min)** - Specify the time in minutes for which the Late-IN and Early-OUT special functions will remain active after being enabled at the Door Controller.



The above features are available only for direct doors.

- **Pulse Time (sec)** - Specify the time in seconds for the panel door to be energized for a valid credential.



This feature is available only for panel doors.

Features

The Features tab allows the user to enable certain Access Control features for a device



The Features tab is available only with the Access Control Module license and is applicable only for direct doors.

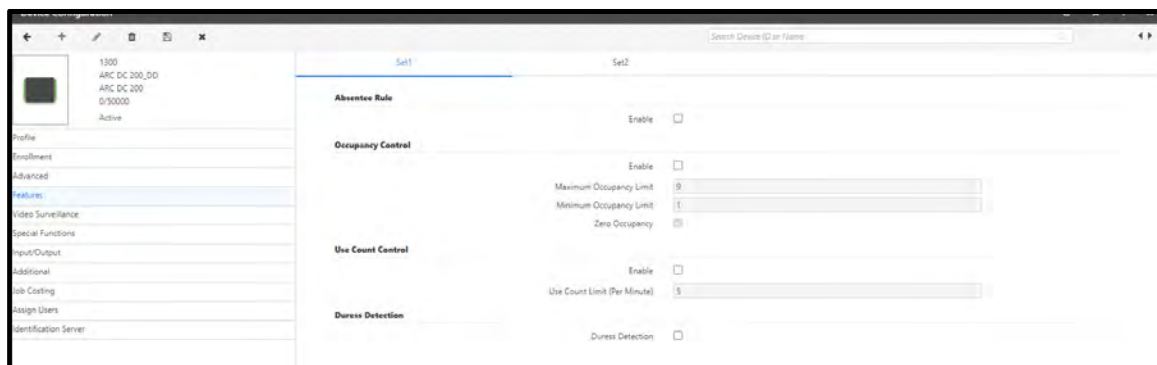
To access this, After selecting the device, Select **Device Configuration> Features**. The access control features for the device can be set from the following two sections:

- “Set1”
- “Set2”

Set1

This page allows the configuration of three rules - **Absentee Rule**, **Occupancy Control** and **Use Count Control**.

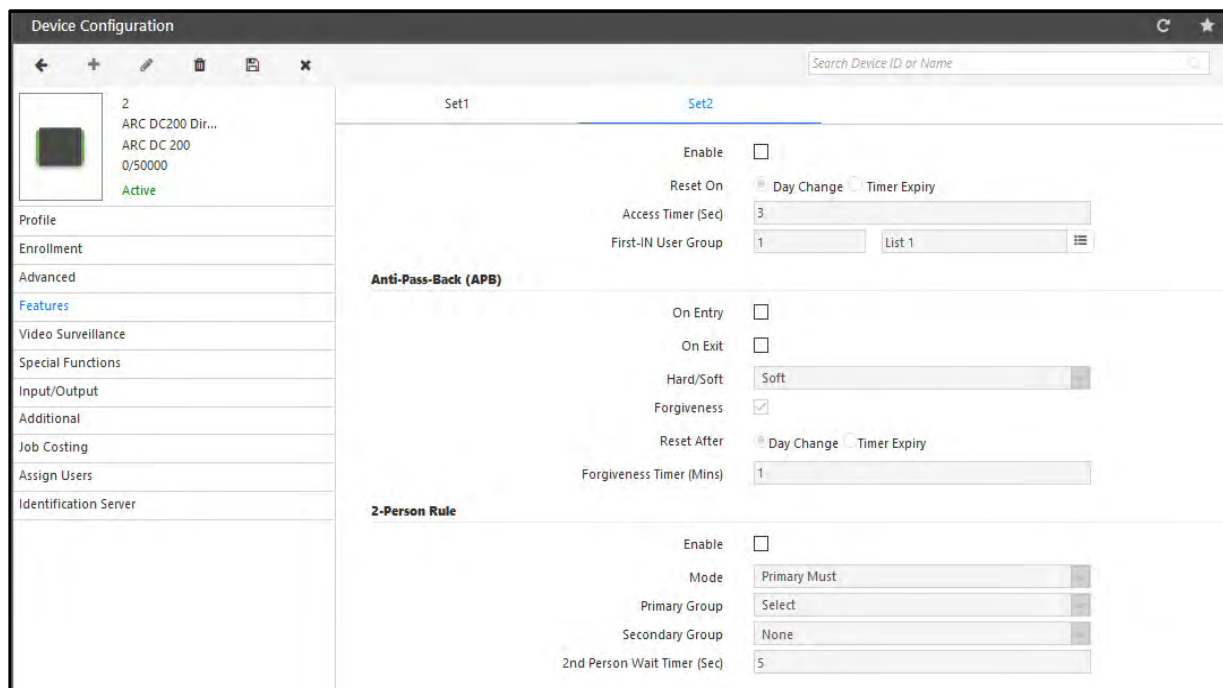
The page appears as shown below.



- **Absentee Rule** - Select this checkbox to enable this feature at the door. This rule sets the maximum number of days for non-use of a credential. On expiration of days limit, the user will be automatically blocked.
For configuring the rule See *Access Control> Absentee Rule*.
- **Occupancy Control** - Select this checkbox to enable the feature at the door and specify maximum number of users to be allowed within the controlled area after which a user exit is required to enable access to another user. Also specify the **Minimum Occupancy Limit** i.e. the minimum number of occupants the designated zone should have, and enable/disable the **Zero Occupancy** option to determine whether the designated zone should be allowed to be empty or not.
For configuring the rule See *Access Control> Occupancy Control*.
- **Use Count Control** - Select this checkbox to enable the feature at the door and specify the maximum number of uses per minute.
For configuring the rule See *Access Control> Use Count Control*.
- **Duress Detection** - Select the checkbox to enable the feature. Duress Detection is used to generate the duress alarm which informs that the user is forced to open the door under threat.

Set2

This page allows the configuration of three rules - **First-IN User Rule**, **Anti-Pass-Back (APB)** and **2-Person Rule**. The page appears as shown below.



- **First-IN User Rule** -Select this checkbox to enable the feature at the direct door and select the First-In User group which would be valid at the door.
For configuring the rule *See Access Control> First- In User Rule> Assignment*
- **Anti-Pass Back (APB)** - Select this checkbox to enable the feature at the direct door.
For configuring the rule *See Access Control> Anti-Pass Back*
- **2-Person Rule** - Select this checkbox to enable the feature at the door and set the **wait time** in seconds after which the second person is allowed to punch on the door.
For configuring the rule *See Access Control> 2- Person Rule*

Video Surveillance

The Video Surveillance tab allows the user to configure parameters for video surveillance integration with the COSEC device.

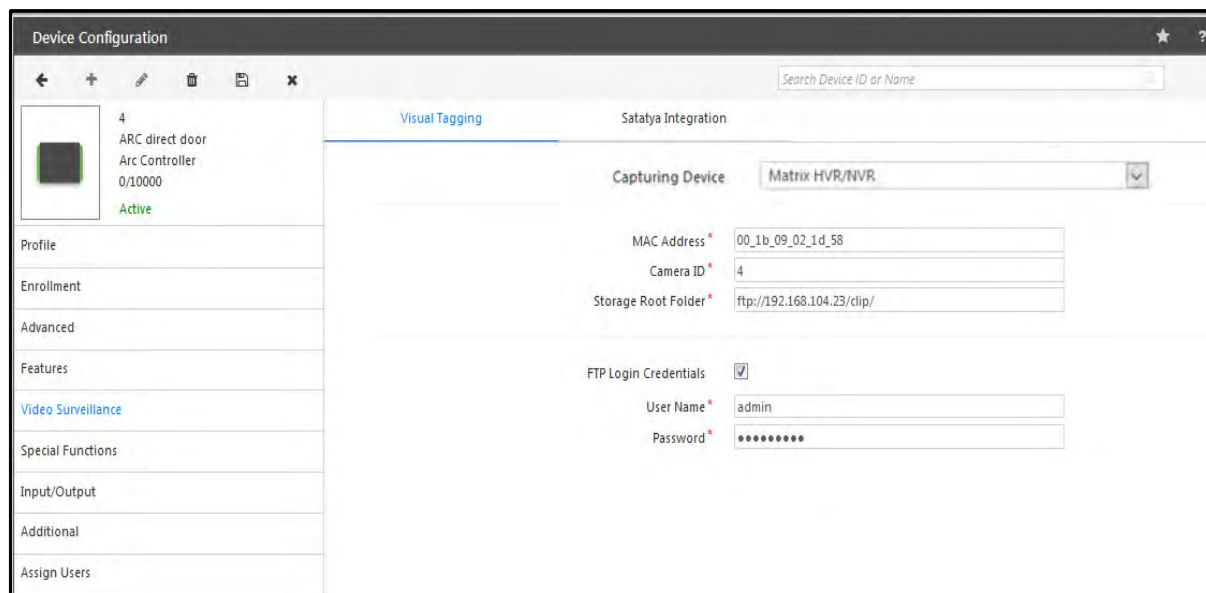
It is available in Basic License.

To access this, Go to **Device Configuration> Video Surveillance**.

- “Visual Tagging”
- “Satatya”

Visual Tagging

The COSEC application can interface with some supported hybrid and network video recording systems and grab images triggered by user events at the Doors. The **Visual Tagging** option enables the administrator to define the video recorder parameters. The **Visual Tagging** page appears as shown below.



The screenshot shows the 'Device Configuration' window with the 'Visual Tagging' tab selected. On the left, a sidebar lists various configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance (highlighted), Special Functions, Input/Output, Additional, and Assign Users. The main area is titled 'Satatya Integration' and contains the following fields:

- Capturing Device:** A dropdown menu showing 'Matrix HVR/NVR'.
- MAC Address:** A text field containing '00_1b_09_02_1d_58'.
- Camera ID:** A text field containing '4'.
- Storage Root Folder:** A text field containing 'ftp://192.168.104.23/clip/'.
- FTP Login Credentials:** A checkbox that is checked.
- User Name:** A text field containing 'admin'.
- Password:** A text field with masked characters (dots).



To view the user events and related images, go to **Admin > Views/Logs > Event View**. To know more about viewing events, refer to “Event View”.

The following parameters are available for configuration:

- **Capturing Device** - Select the video recording device type from the dropdown menu as shown. The compatible device types are:

- Matrix HVR/NVR
- Milestone

Matrix HVR/NVR

- **MAC Address** - In the event of selecting the Matrix HVR/NVR, the administrator needs to specify the MAC address of the video recorder device using “_” (underscore) as the separator.
- **Camera ID** - Specify the camera number or camera ID for IP cameras. For analog cameras specify the camera number.
- **Storage Root Folder** - Specify the Root folder path or FTP Path where the uploaded images will be saved.
- **FTP Login Credentials** - Check this box to activate FTP login credentials for authentication.
- **Username** - Specify the FTP server username.
- **Password** - Specify the FTP server password.



Some COSEC devices do not support all the network connection options.

Milestone



For more information on integration with **Milestone** devices, refer to “Milestone Integration”.

Satatya

This functionality is available for configuration only when the Matrix HVR/NVR device type is selected as the **Capturing Device** (from *Visual Tagging*). It enables the configured COSEC devices to directly send commands to the SATATYA HVR/NVR devices as per the configuration on this page. The Satatya configuration page appears as shown below:

- Integration type-** Select the integration type from the options of Wired and Network. In wired integration, door is physically connected with Satatya Device. In Network integration, connection can be by ethernet, wireless or broadband depending upon the COSEC device support.

- **Active**- Check the box to activate the connection.
- **Network Connection**- Select the Network connection from the options of Ethernet, Broadband, Wireless.
- **IP Address**- Specify the IP address of HVR/NVR if device is connected with Ethernet.
- **Port Number**- Specify the port number of HVR/NVR
- **Name**-Specify a user friendly name for the integration function.
- **Active**- Check the Active box to enable the SATATYA integration functionality.
- **Schedule** - Specify a schedule for the function by specifying the start and the end time (*24 Hours format*) as well as checking the boxes against the applicable **days** of the week.
- **Event**- Select a COSEC event from the drop down list for which the resultant action is to be configured.
- **Mode**- Select the event mode from the options of Entry, Exit and Both from the drop down list wherever applicable.
- **Action**-Select the action for the Satatya device from the drop down list. The options available are:
 - Recording - Specify the duration in minutes.
 - Upload Image - This will be uploaded as per the ftp settings.
 - Video Pop-up - Specify the duration in seconds. The video pop up will be generated on the local client of Satatya device on the selected camera.
 - PTZ Preset - Specify the PTZ position number as defined on the SATATYA device.
 - Mail Image - Specify the email-ID.
- **Camera**- Select the relevant camera channels depending on the action selected.

Example: For action as Mail Image, the image of Camera 8 will be mailed to the mentioned Email ID.

The screenshot shows a configuration form with the following fields:

- Event:** Access Allowed (dropdown)
- Mode:** Both (dropdown)
- Action:** Mail Image (dropdown)
- E-mail ID:** sheetalpandya2012@gmail.com (text input)
- Camera:** A grid of checkboxes for cameras 1 through 24. Camera 8 is selected.

- Click the **Add** button to finish the process of linking the event to the action. The user may configure another event-action linkage if required.

Name	Event	Action	Start Time	End Time	Active	
ARC HVR Integration	Access Allowed	Mail Image	09:00	12:00	Yes	


Special Functions

To configure *Special Functions* for COSEC doors, refer to “*Special Functions*”.

Input/Output

The Input/Output (I/O) configuration of a system determines how the output or response of a system is influenced by the input applied on it. In case of the COSEC Access Control System, the I/O configuration should enable the system to monitor and trigger a specific response to any changes in door state or event occurrences at the door device. This change of door state or occurrence of events may be considered as an input while the response or action that is generated by the system on detection of this input, may be defined as the output.



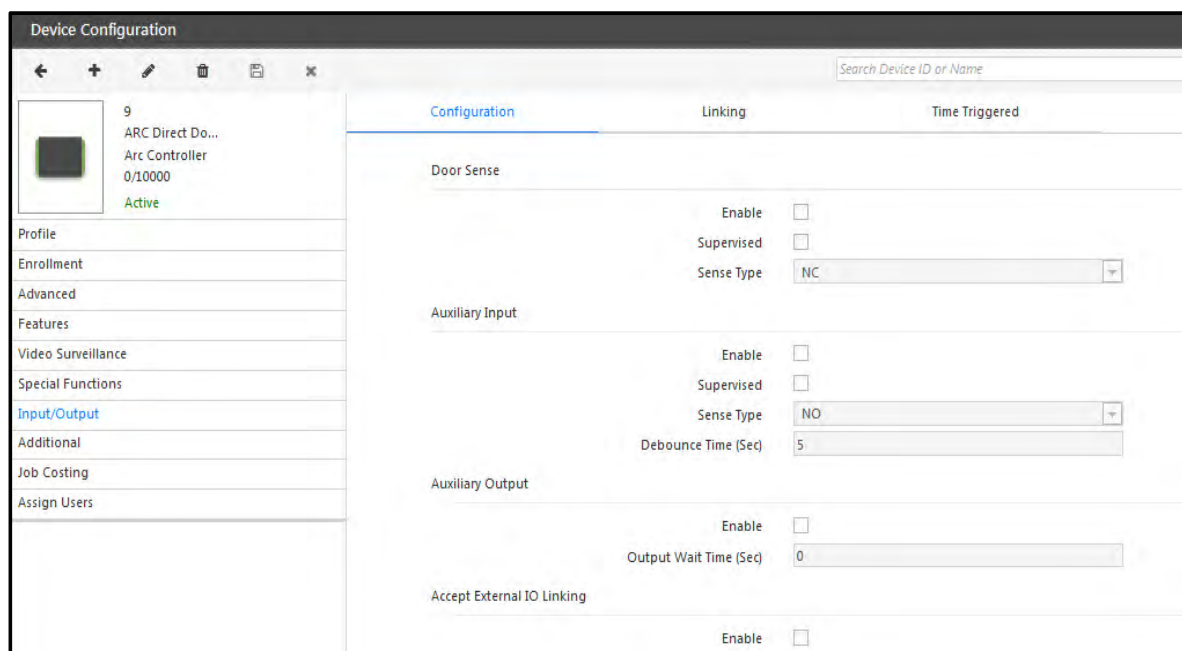
1. This functionality cannot be fully accessed in the Edit  mode for a selected device.
2. This functionality is available only with the Access Control add-on module license.

To access this, After selecting the device, Select **Device Configuration> Input Output**. The Input Output parameters can be set from the following sections:

- “Configuration”
- “Linking”
- “Time Triggered”

Configuration

The **Configuration** section for a **ARC DC100 Door** appears as shown below.

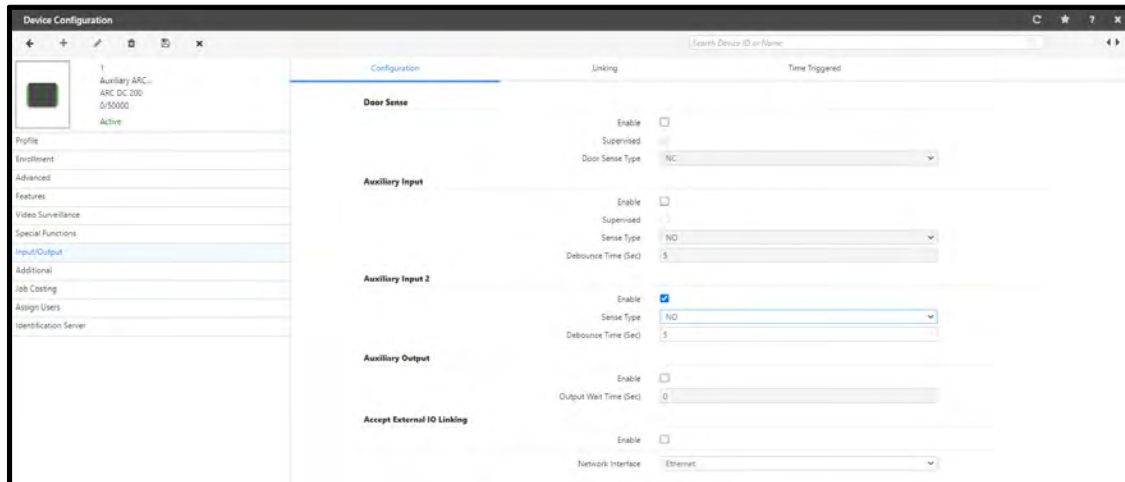


The screenshot shows the 'Device Configuration' window for an 'ARC Direct Door' (ID: 9, Arc Controller: 0/10000, Status: Active). The left sidebar lists various configuration sections: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, **Input/Output** (selected), Additional, Job Costing, and Assign Users. The main area displays the 'Configuration' tab with three sections: 'Door Sense', 'Auxiliary Input', and 'Auxiliary Output'. Each section has 'Enable' and 'Supervised' checkboxes, and a 'Sense Type' dropdown menu. The 'Door Sense' section has 'Sense Type' set to 'NC'. The 'Auxiliary Input' section has 'Sense Type' set to 'NO' and a 'Debounce Time (Sec)' of 5. The 'Auxiliary Output' section has 'Output Wait Time (Sec)' set to 0. At the bottom, there is an 'Accept External IO Linking' section with an 'Enable' checkbox.

Section	Enable	Supervised	Sense Type	Debounce Time (Sec)	Output Wait Time (Sec)
Door Sense	<input type="checkbox"/>	<input type="checkbox"/>	NC		
Auxiliary Input	<input type="checkbox"/>	<input type="checkbox"/>	NO	5	
Auxiliary Output	<input type="checkbox"/>				0

Accept External IO Linking: ☐

The **Configuration** section for a **ARC DC200 Door** appears as shown below.



The following parameters are available for configuration in both Direct door and Panel door:

- **Door Sense** - The system by default can sense two states of a door - **Normally Open (NO)** and **Normally Closed (NC)** depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a **Door Abnormal** alarm.

Select the **Enable** checkbox to enable the system for such two-state monitoring.

Select the **Supervised** checkbox to enable the door for four-state monitoring where the door is also monitored for **door fault** and **door disconnection**. Specify the **Door Sense Type** as **NC** or **NO**. Default value is **NC**.

- **Lock Sense** - The system by default can sense two states of lock - **Normally Open (NO)** and **Normally Closed (NC)** depending on which the output is determined. For example, any deviation of the lock from its normal state may lead to the trigger of a **Lock** event.

Select the **Enable** checkbox to enable the lock sense. When Lock Sense is enabled, then Exit Switch in Readers tab will get disabled.



1. The Lock Sense must be connected with Exit Switch-2.

2. For Single Door, the configuration of Lock must be considered as: Lock Sense 1 & Lock Sense Type 1.



For Dual Door, the configuration of Lock is

- For first device it will be: Lock Sense 1 & Lock Sense Type 1
- For second device it will be: Lock Sense 2 & Lock Sense Type 2

- **Auxiliary Input** - Select the **Enable** checkbox option for **Auxiliary Input** (e.g. Smoke Detectors) depending on normal or supervised door state monitoring as described above.

Select the **Supervised** checkbox to enable the door for four-state monitoring where the door is also monitored for **door fault** and **door disconnection**.

Specify the **Door Sense Type** as **NC** or **NO**. Default value is **NC**.

Debounce Time (Sec) - Specify the **Debounce Time** in seconds. Default value is **5 sec** and valid range is 0-99 sec. It defines the minimum time for which an input interface must be maintained in a given state before the system reports it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.

- **Auxiliary Input 2**- Select the **Enable** checkbox option for **Auxiliary Input 2**.

Specify the **Door Sense Type** as **NC** or **NO**. Default value is **NO**.

Debounce Time (Sec) - Specify the **Debounce Time** in seconds. Default value is **5 sec** and valid range is 0-99 sec. It defines the minimum time for which an input interface must be maintained in a given state before the system reports it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.



***Auxiliary Input 2** is only applicable for **ARC DC200 Direct** door and **ARC DC200 Single Door Dual Reader Panel** door.*

- **Auxiliary Output** - Select the **Enable** checkbox to enable Auxiliary Output (e.g. Fire Alarm) for the selected device. To set an additional waiting period before the Aux Output signal is sent, enter an **Output Wait Time (Sec)**.
- **Accept External IO Linking** - Select the Enable checkbox to enable device-to-device IO Linking i.e. input from one Direct Door can trigger output in another Direct Door.
- **Network Interface** - Select anyone network interface out of **Ethernet**, **Wireless** and **Mobile Broadband**.
- **Relay Output**

Output Group Number (Door Unlock)- Select the Output Group Number to which the device output for Door Unlock is to be assigned from the picklist.

Output Group Number (Door Lock)- Select the Output Group Number to which the device output for Door Lock is to be assigned from the picklist.



*The “**Accept External IO Linking**” and “**Network Interface**” features are available in direct door only.*



*For **ARC DC200 Dual Door SingleDual Reader Panel** door; only **Door Sense**, **Lock Sense** and **Relay Output** are applicable.*

ARC DC200 Dual Door SingleDual Reader Panel door.

Device Configuration

3

ARC Dual Door...
Panel Lite V2 Door
Arc Controller
Panel Lite V2

Active

Search Device ID or Name

Configuration

Door Sense

Enable ☒

Supervised ☐

Door Sense Type

NC

Lock Sense

Enable ☒

Lock Sense Type

NO

Relay Output

Output Group Number(Door Unlock)	2	Door Unlock	⋮
Output Group Number(Door Lock)	ID	Name	⋮

ARC DC200 Single Door Dual Reader Panel door.

Devices

Device List

- Device Configuration
- Multi-Device Options
- Milestone Integration
- Masters
- Card Personalization
- Device Status
- Reports

Device Configuration

S
PQ ARCDCA85 S...
Panel200 Door
ARC DC 200
Panel200 Devi...
Active

Profile

Advanced

Video Surveillance

Input/Output

Job Costing

Assign Users

Configuration

Door Sense

Enable ☐

Supervised ☐

Door Sense Type NO

Lock Sense

Enable ☐

Lock Sense Type NO

Auxiliary Input

Enable ☒

Supervised ☐

Sense Type NO

Debounce Time (Sec) 0

Auxiliary Input 2

Enable ☐

Sense Type NO

Debounce Time (Sec) 5

Auxiliary Output

Enable ☐

Output Group 6 door_unlock

Relay Output

Output Group Number (Door Unlock) 2 Door Unlock

Output Group Number (Door Lock) 40 Name

Search Device ID or Name:

Door Sense

Enable ☐

Supervised ☐

Door Sense Type NO

Lock Sense

Enable ☐

Lock Sense Type NO

Auxiliary Input

Enable ☒

Supervised ☐

Sense Type NO

Debounce Time (Sec) 0

Auxiliary Input 2

Enable ☐

Sense Type NO

Debounce Time (Sec) 5

Auxiliary Output

Enable ☐

Output Group 6 door_unlock

Relay Output

Output Group Number (Door Unlock) 2 Door Unlock

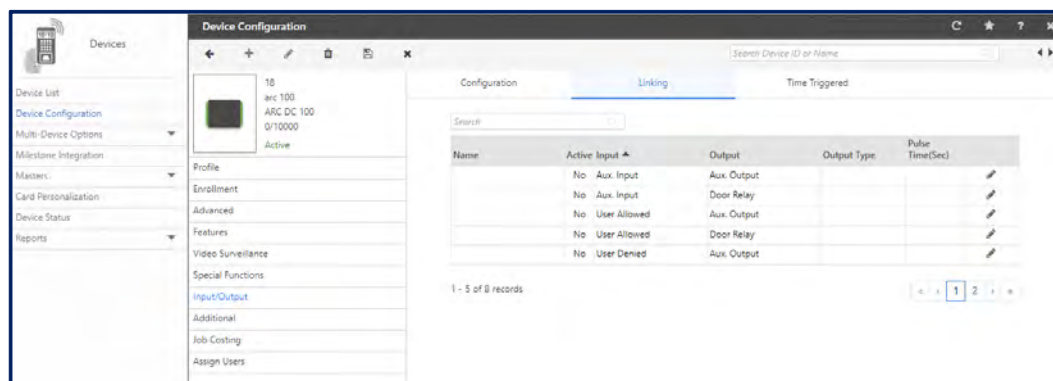
Output Group Number (Door Lock) 40 Name

Linking

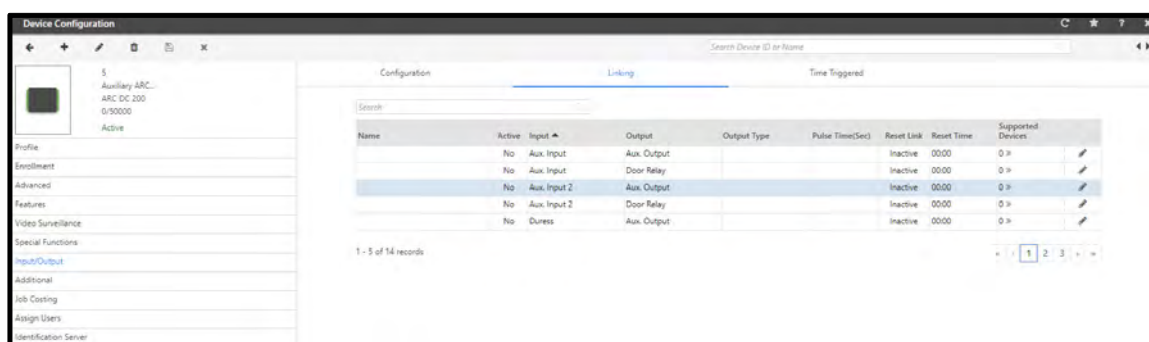


This section is only available for Direct door.

The **Linking** section for **ARC DC100** door appears as shown below.




The **Linking** section for **ARC DC200** door appears as shown below.

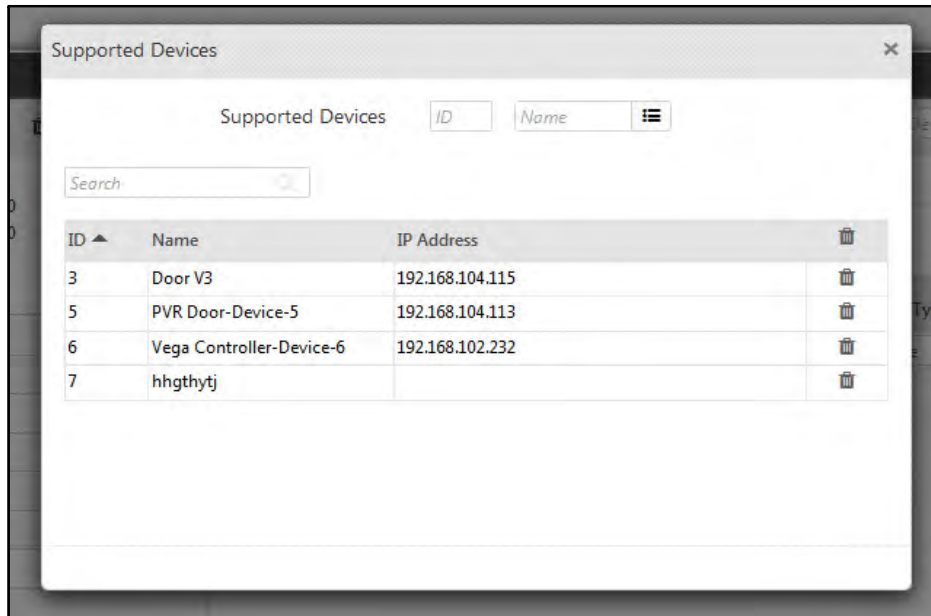


The COSEC application supports the Input/Output Linking feature to activate an output port based on a trigger received from an input port on the same Direct Door. This option enables the administrator to define how an event or events (input port) will trigger an output on the selected door.

Select a Input-Output linking row or click edit button.

- **Name** - Specify a name for the new I/O linking program to be defined.
- **Output Type** - Specify the appropriate type of output from the following four options available in the drop down list:
 - Pulse: With this type of output, the user needs to define the Pulse time in seconds.
 - Interlock: With this option, the output follows the input. The relay output is triggered as long as the input is activated after which it returns to normal state.
 - Latch: With this option, it is denoted that the relay output will be in an energized condition for infinite period and needs to be reset manually.
 - Toggle: With this option, the output group toggles its state whenever an input group is activated.

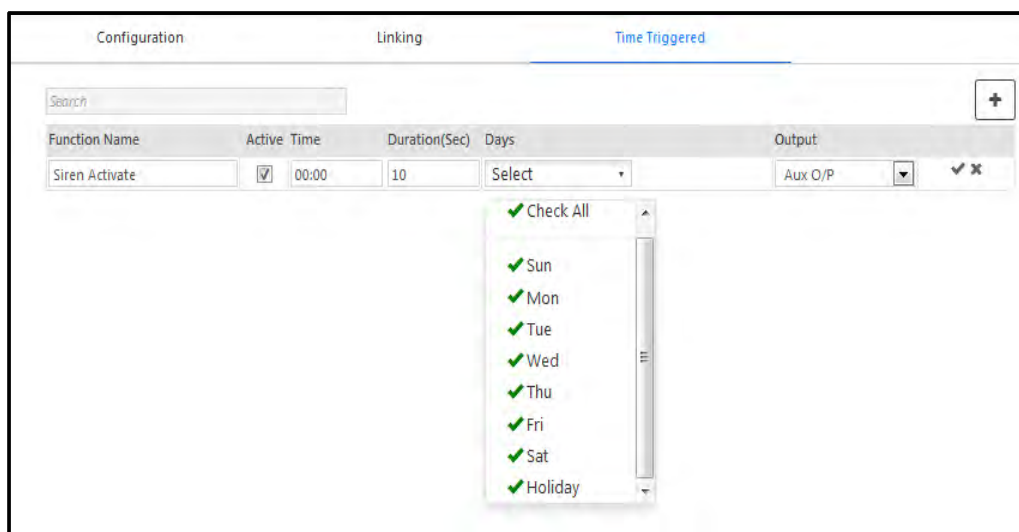
- **Pulse Duration (sec)** - For a *Pulse* output type, specify the pulse duration in seconds.
- **Reset Link** - Select this checkbox to activate this linking program as well as set the time from **Reset Time**.
- **Supported Devices**- By clicking on the  , the pop-up will arise as shown in figure below. Select the supported devices.



- Click the ☒ button and **Save** the configuration.

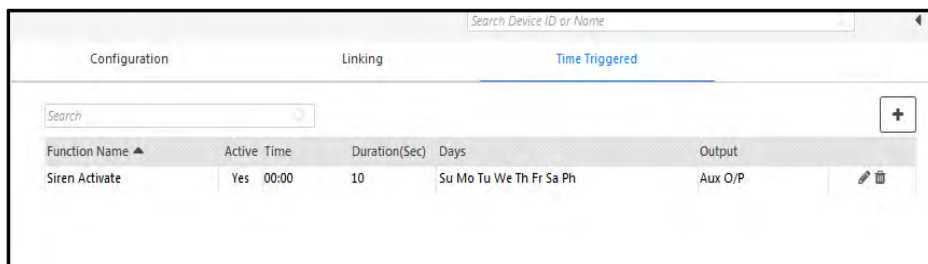
Time Triggered

On the **Input Output** page, select the **Time Triggered** section as shown.



This functionality enables the user to control the activity of an Output without manual intervention. The time triggered functions are used for activating events like door unlock and siren activation that are set as per the start time and for the configured time duration. This functionality is designed to energize outputs for predefined periods

at the configured time. The COSEC access control system supports up to 20 Time Triggered functions on a Direct Door.



Function Name ▲	Active Time	Duration(Sec)	Days	Output
Siren Activate	Yes 00:00	10	Su Mo Tu We Th Fr Sa Ph	Aux O/P

Additional

This section lists some additional configurations that can be enabled for door controllers.

To access these configurations, Go to **Device Configuration > Additional > Daylight Saving**

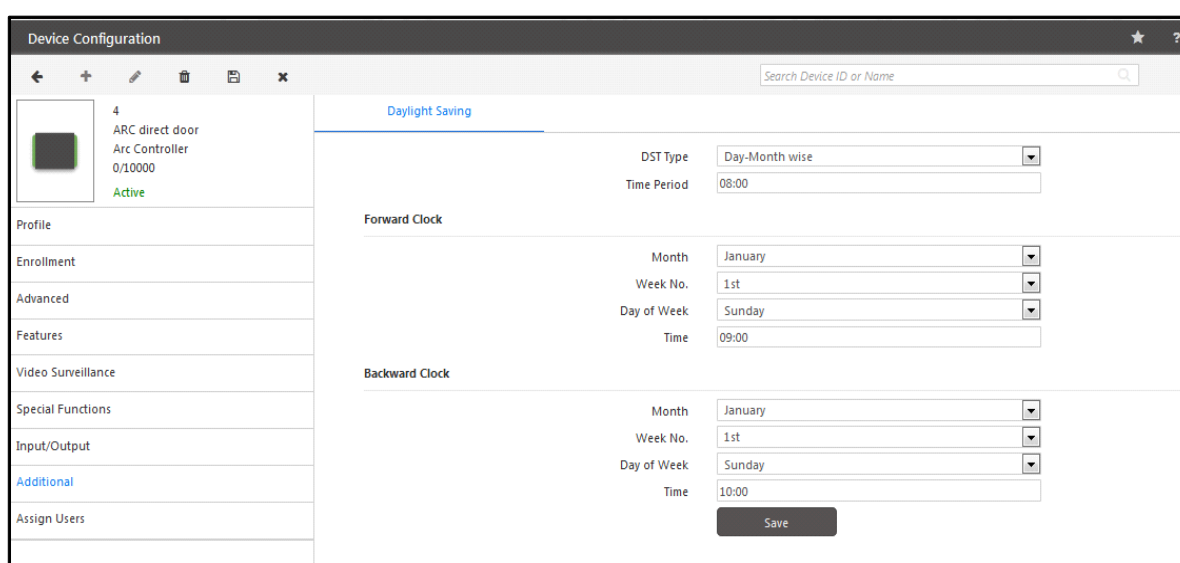


This section is available only for Direct Doors.

Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. COSEC doors can be configured to be compatible with this procedure keeping the RTC of the system updated with such changes.

The **Daylight Saving** configuration can be done in 2 ways i.e. Day-Month wise or Date-Month wise.

- Select the **DST Type** as Day-Month wise or Date-Month wise. The **Disable** option when selected, disables the application of DST on the system time.
- On selection of the **Day-Month wise** option, the DST is set by the day of the month on which clock needs to be forwarded and reverted back to normal. Set the month, week number, day of the week, and time for both the **Forward Clock** and **Backward Clock** as shown.



Device Configuration

Search Device ID or Name

4 ARC direct door Arc Controller 0/10000 Active

Profile

Enrollment

Advanced

Features

Video Surveillance

Special Functions

Input/Output

Additional

Assign Users

Daylight Saving

DST Type: Day-Month wise

Time Period: 08:00

Forward Clock

Month: January

Week No.: 1st

Day of Week: Sunday

Time: 09:00

Backward Clock

Month: January

Week No.: 1st

Day of Week: Sunday

Time: 10:00

Save

- On selection of the **Date-Month wise** option, the DST is set by date of the month on which clock needs to be forwarded and reverted back to normal. Define the **Time Period** for the date-month wise DST

settings in 24-hours format, and specify the day of the week, date and time for the **Forward Clock** and the **Backward Clock** as shown.

This DST Setting implies that on 1st sunday of November at 09:00 hours, the clock will be forwarded by 08:00 hours. And on 1st sunday of January at 10:00 hours, the clock will be reversed or backwarded by 08:00 hours.

The screenshot shows the 'Daylight Saving' configuration page for device 4. The left sidebar lists various configuration categories, with 'Additional' selected. The main area contains the following settings:

- DST Type:** Date-Month wise
- Time Period:** 08:00
- Forward Clock:**
 - Month: January
 - Date: 1
 - Time: 09:00
- Backward Clock:**
 - Month: January
 - Date: 1
 - Time: 10:00

A 'Save' button is located at the bottom right of the configuration area.

- Click the **Save** button.

Job Costing



Job Costing is applicable for ARC DC200 Direct Door only.

Job Costing enables the admin to assign default jobs on the ARC DC200.

The screenshot shows the 'Settings' configuration page for device 9. The left sidebar lists various configuration categories, with 'Job Costing' selected. The main area contains the following settings:

- Show Job Menu:** Allocate Default
- Default Jobs:**

Job Code	Name	Assignment Start	Assignment End
SWD	Development	02/06/2017	31/07/2017
- Previous Default Jobs:** No Data

Show Job Menu: It is disabled for ARC DC200.

Default Jobs: Click Add button to add the default job on the door. Then click on the Job pick-list button and select the job to be assigned to the device. The Job costing user can directly punch on the reader of this door for starting the default job.

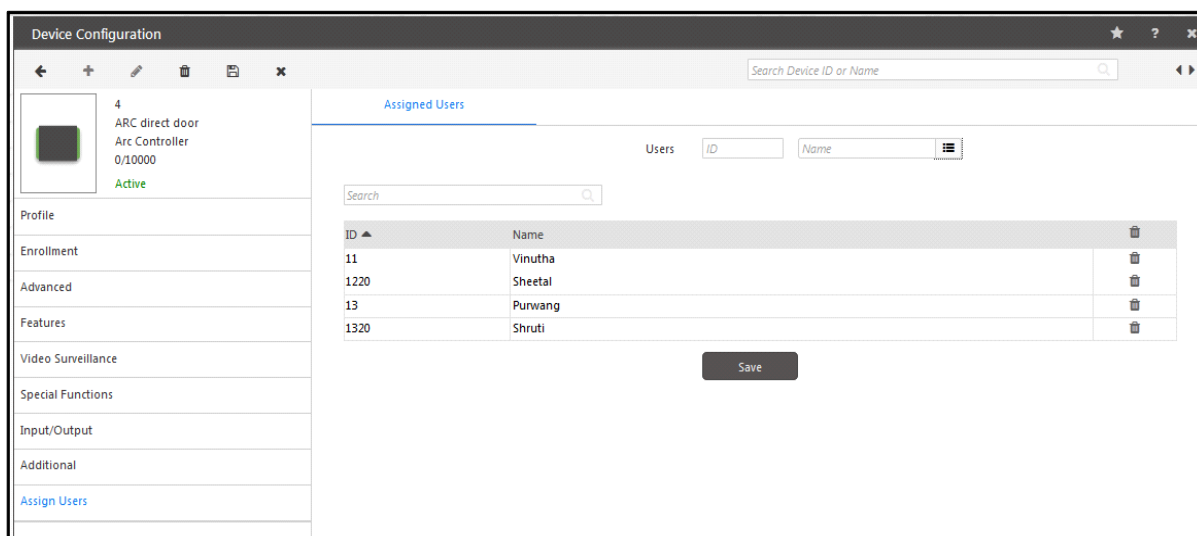
Finally click on **Save** button to save the configuration.

When the assignment date of the default job gets elapsed, then the respective job will be listed in **Previous Default Jobs** section.

Assign Users

To the configured device, you can select and assign the users.

Click the picklist button and select the users.



Click the **Save** button to assign all the added users to the selected door.

Identification Server

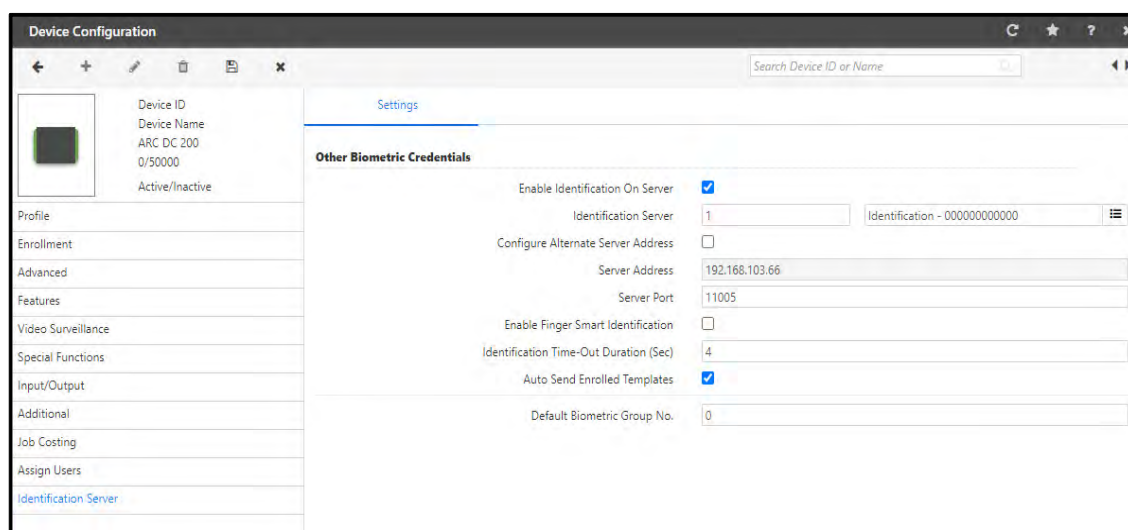
This tab enables the ARC DC200 to be assigned to a pre-defined Identification Server.

Device has a limited memory capacity for storage of templates so we need Identification Server which will store the more number of templates and respond to device when asked for identification.

For more information on Identification Servers, See *Admin> System Configuration> Identification Server Configuration*.

To access these configurations,

- On the **Device Configuration** page, select the **Identification Server** tab.



Other Biometric Credentials

- **Enable Identification On Server:** Select the checkbox to enable the identification of finger templates on this device.
- **Identification Server:** Select an Identification Server using the picklist button to which the device is to be assigned. The configuration of server is done from **Admin module > System Configuration > Identification Server Configuration** and the Identification Service must be started from the service tray.
- **Configure Alternate Server Address:** Enable this checkbox to configure the alternate Server Address.
- **Server Address:** It displays the IP Address of the selected Identification Server.
- **Server Port:** Enter the server port number. The default port number is 11005.
- **Enable Finger Smart Identification:** For all other supported doors, select the checkbox to enable fingerprint templates identification through Identification Server.
- **Identification Time-Out Duration (Sec):** Specify the duration in seconds after which the fingerprint template identification will get time out.
Example: If 5 seconds is specified, then the identification server will try to identify the template till 5 seconds and if not found then it will show time-out to the user.
- **Auto Send Enrolled Templates:** Select the checkbox to enable any enrolled templates to be saved both on the COSEC database as well as saved locally on the configured Identification Server. This enables prompt identification of user on enrollment.
- **Default Biometric Group No.:** Specify the default biometric group number to be assigned to the device. It is a number allotted to a device to be assigned to the Identification Server. This enables the Identification Server to match the template against only those devices that belong to the corresponding biometric group. This reduces the false detection as well time to search template.

ARC IO-800

COSEC ARC IO800 is an input and output controller to control multiple inputs and outputs of third party devices to perform multiple applications. ARC IO800 can be connected as **Direct Door** as well as **Panel Door**.



The Device Configuration page for ARC IO-800 appears as shown below.

Enter the MAC address of the door. The IP address will be displayed automatically once the device comes online in Monitor.

To add Devices automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the “Auto Add New Devices” check-box. Once the device is connected in network, it will come online in COSEC Monitor.



The Monitor Service must be running while adding the device to COSEC.

Once the device is configured, click the **Save** button to save the configuration.



ARC IO 800 (Direct door) is restricted to be added to the configured Device group even if the checkbox “Auto Assign New Device To Device Group”. is enabled.

To know more about configuring devices, click on the links for different tabs of Device configuration.

- [“Profile”](#)
- [“Video Surveillance”](#)
- [“Input/Output”](#)

Profile

This section enables the user to set up the basic profile for any new device. Setting up a door profile involves defining basic parameters to set up any door controller device.

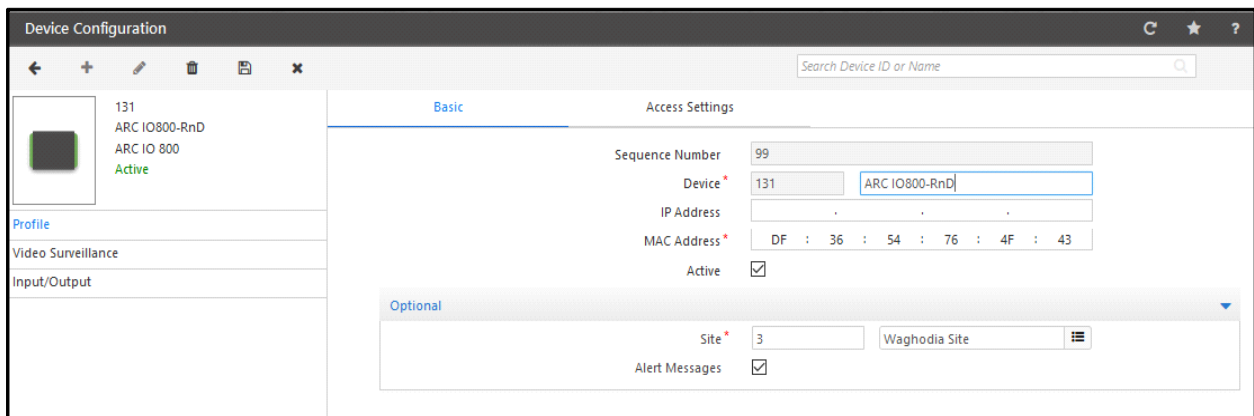
To do this, On the **Device Configuration** page, select the **Profile** tab. The Profile can be configured in the following sections:

- “Basic”
- “Access Settings”

Basic

The **Basic** section for “ARC IO800 as Direct door and Panel door” is shown below:

ARC IO800 as Direct Door



Device Configuration

Search Device ID or Name

131
ARC IO800-RnD
ARC IO 800
Active

Profile

Video Surveillance

Input/Output

Basic

Access Settings

Sequence Number: 99

Device: 131

IP Address: . . .

MAC Address: DF : 36 : 54 : 76 : 4F : 43

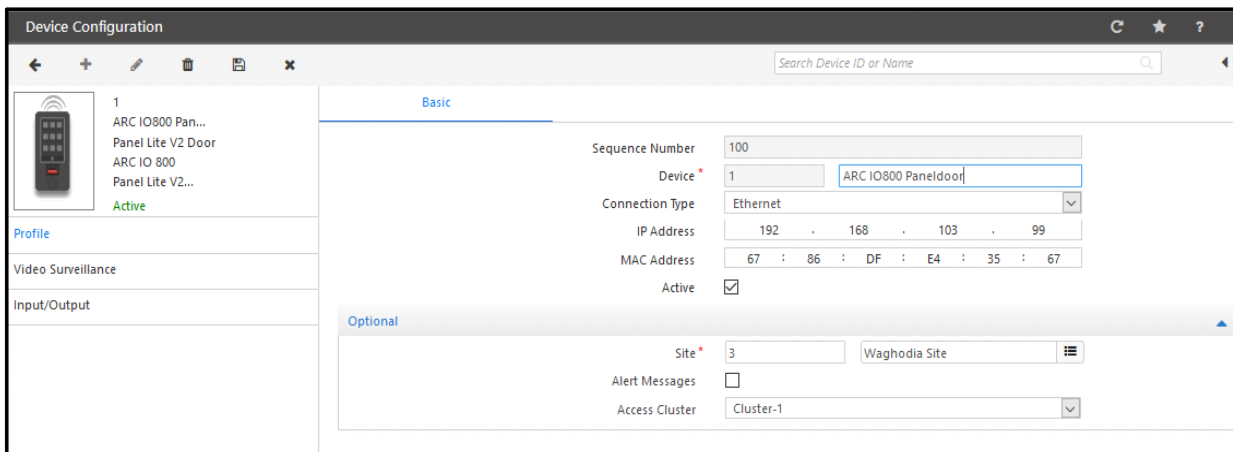
Active: ☒

Optional

Site: 3

Alert Messages: ☒

ARC IO800 as Panel Door



Device Configuration

Search Device ID or Name

1
ARC IO800 Pan...
Panel Lite V2 Door
ARC IO 800
Panel Lite V2...
Active

Profile

Video Surveillance

Input/Output

Basic

Sequence Number: 100

Device: 1

Connection Type: Ethernet

IP Address: 192 . 168 . 103 . 99

MAC Address: 67 : 86 : DF : E4 : 35 : 67

Active: ☒

Optional

Site: 3

Alert Messages: ☐

Access Cluster: Cluster-1

Configure the following options as required:

Sequence Number - This is a system generated sequence number for each new device.

Device: Specify the name of the door. The ID of the door is auto generated by the system.

Connection Type - Applicable only for Panel Doors. Specify the connection type as Ethernet or RS485.

IP address/MAC address: Enter the IP address and MAC address respectively of ARC IO800.



MAC address of door is required while manually adding the door to the COSEC Monitor. You can note the MAC address from the device web page.

Active - Check the box to activate the device on the network.



*To add the Device automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the “**Auto Add New Devices**” checkbox.*

*The device will be added automatically but make sure you enable the **Active** checkbox in order to connect the device to the network. Once the device is connected to the network, it will come online in COSEC Monitor.*

Click **Save** button to save the configuration.

The **Basic** page also has an **Optional** tab which provides optional configurations as shown below:

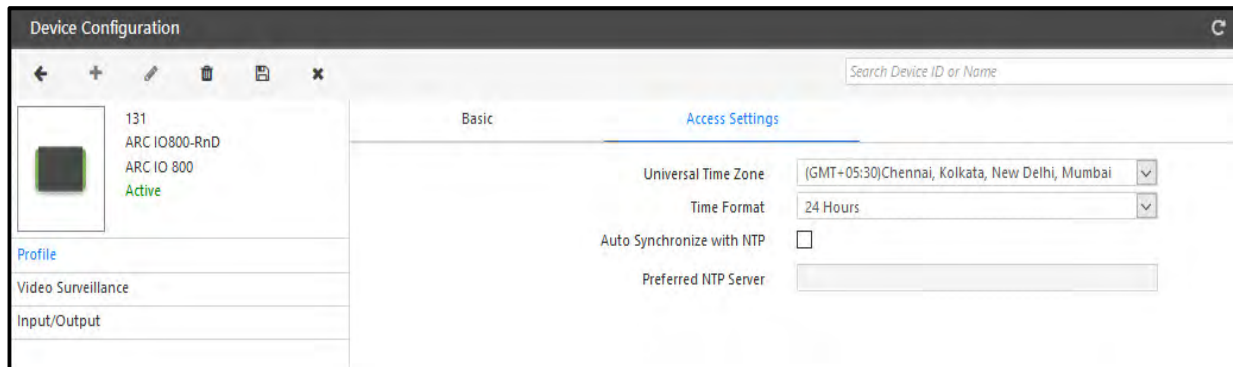
- **Site** - Select the site to which this door is to be assigned from the site picklist window. Site is created from Devices> Masters> Site.
- **Alert Messages** - Select this checkbox to enable the application to send alerts based on events from this door.
- **Access Cluster** (only for panel doors) - Assign an access cluster to the door by selecting from the drop down menu.



Access Cluster is configured while configuring Panel/Panel lite/Panel200.

Access Settings

This section is available for direct door only. The **Access Settings** page appears as shown below:



- **Universal Time Zone** - Select the geographic time zone in which the DOOR will operate.
- **Time Format** - Specifies the time format to be displayed on Door Controller LCD display. The formats available are:
 - 24 Hours
 - 12 Hours

Auto Synchronize with NTP

If Date and time is to be automatically synchronized as per the **Preferred NTP Server** (predefined or user-defined NTP server address) selected by user, then you must enable **Auto Synchronize With NTP** checkbox.

Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from device webpage, which will be reflected on device display.

- When Auto Synchronization with NTP is disabled Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 1. You can specify the Preferred NTP server of your choice. In this case device will first try to get Date and Time from that server address.
If it does not get Date and Time in three tries; device will check from pre-defined NTP servers.
If you have entered one of the three pre-defined NTP servers(ntp1.cs.wisc.edu , time.windows.com , time.nist.gov); then device will first check that server first.
If it receives updated Date and Time then Updated Date and Time will be reflected on device webpage and display screen.
 2. You can keep the Preferred NTP server as blank. In this case device will check for Date and Time from the first NTP server.
 3. If user has manually entered Date and Time from webpage or Device Menu then those values of Date and Time will be reflected on device webpage and display screen.

In the case of the **Manual** option the administrator can manually update the time on the Door with that of the system time as and when required.

Video Surveillance

The Video Surveillance tab allows the user to configure parameters for video surveillance integration with the COSEC device.

It is available in Basic License.

To access this, Go to **Device Configuration> Video Surveillance**.

- “Visual Tagging”
- “Satatya”

Visual Tagging

The COSEC application can interface with some supported hybrid and network video recording systems and grab images triggered by user events at the Doors. The **Visual Tagging** option enables the administrator to define the video recorder parameters. The **Visual Tagging** page appears as shown below.



To view the user events and related images, go to **Admin > Views/Logs > Event View**. To know more about viewing events, refer to “Event View”.

The following parameters are available for configuration:

- **Capturing Device** - Select the video recording device type from the dropdown menu as shown.

The compatible device types are:

- Matrix HVR/NVR
- Milestone



For more information on integration with **Milestone** devices, refer to “[Milestone Integration](#)”.

- **MAC Address** - In the event of selecting the Matrix HVR/NVR, the administrator needs to specify the MAC address of the video recorder device using “_” (underscore) as the separator.

- **Camera ID** - Specify the camera number or camera ID for IP cameras. For analog cameras specify the camera number.
- **Storage Root Folder** - Specify the Root folder path or FTP Path where the uploaded images will be saved.
- **FTP Login Credentials** - Check this box to activate FTP login credentials for authentication.
- **Username** - Specify the FTP server username.
- **Password** - Specify the FTP server password.



Some COSEC devices do not support all the network connection options.

Satatya

This functionality is available for configuration only when the Matrix HVR/NVR device type is selected as the **Capturing Device** (from *Visual Tagging*). It enables the configured COSEC devices to directly send commands to the SATATYA HVR/NVR devices as per the configuration on this page. The Satatya configuration page appears as shown below:

- **Integration type**- Select the integration type from the options of Wired and Network. In wired integration, door is physically connected with Satatya Device. In Network integration, connection can be by ethernet, wireless or broadband depending upon the COSEC device support.
- **Active**- Check the box to activate the connection.
- **Network Connection**- Select the Network connection from the options of Ethernet, Broadband, Wireless.
- **IP Address**- Specify the IP address of HVR/NVR if device is connected with Ethernet.
- **Port Number**- Specify the port number of HVR/NVR
- **Name**-Specify a user friendly name for the integration function.

- **Active-** Check the Active box to enable the SATATYA integration functionality.
- **Schedule** - Specify a schedule for the function by specifying the start and the end time (*24 Hours format*) as well as checking the boxes against the applicable **days** of the week.
- **Event-** Select a COSEC event from the drop down list for which the resultant action is to be configured.
- **Mode-** Select the event mode from the options of Entry, Exit and Both from the drop down list wherever applicable.
- **Action-** Select the action for the Satatya device from the drop down list. The options available are:
 - Recording - Specify the duration in minutes.
 - Upload Image - This will be uploaded as per the ftp settings.
 - Video Pop-up - Specify the duration in seconds. The video pop up will be generated on the local client of Satatya device on the selected camera.
 - PTZ Preset - Specify the PTZ position number as defined on the SATATYA device.
 - Mail Image - Specify the email-ID.
- **Camera-** Select the relevant camera channels depending on the action selected.

Example: For action as Mail Image, the image of Camera 8 will be mailed to the mentioned Email ID.

The screenshot shows a configuration form with the following fields:

- Event:** Access Allowed (dropdown)
- Mode:** Both (dropdown)
- Action:** Mail Image (dropdown)
- E-mail ID *:** sheetalpandya2012@gmail.com (text input)
- Camera *:** A grid of checkboxes for cameras 1 through 24. Camera 8 is checked.


- Click the **Add** button to finish the process of linking the event to the action. The user may configure another event-action linkage if required.

Name	Event	Action	Start Time	End Time	Active	
ARCIO800HVR Integration	Aux. Input 1	Mail Image	09:00	12:00	Yes	

Input/Output

The Input/Output (I/O) configuration of a system determines how the output or response of a system is influenced by the input applied on it. In case of the COSEC Access Control System, the I/O configuration should enable the system to monitor and trigger a specific response to any changes in door state or event occurrences at the door device. This change of door state or occurrence of events may be considered as an input while the response or action that is generated by the system on detection of this input, may be defined as the output.



1. *This functionality cannot be fully accessed in the Edit  mode for a selected device.*
2. *This functionality is available only with the Access Control add-on module license.*

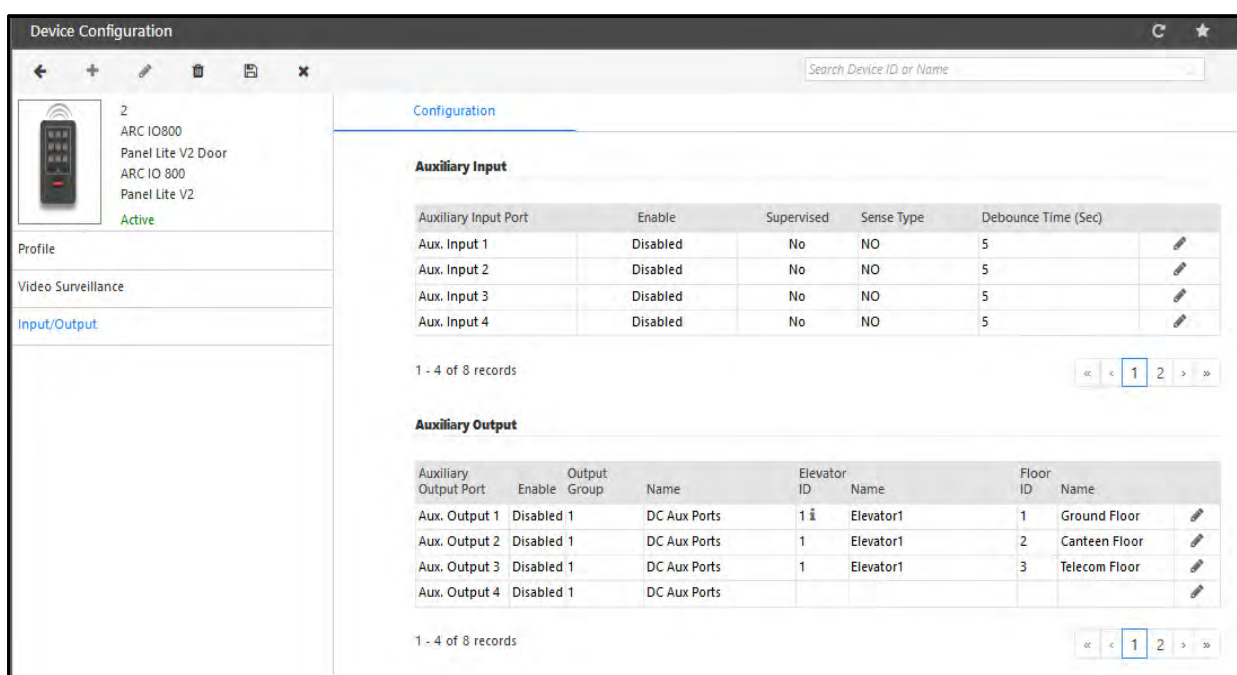
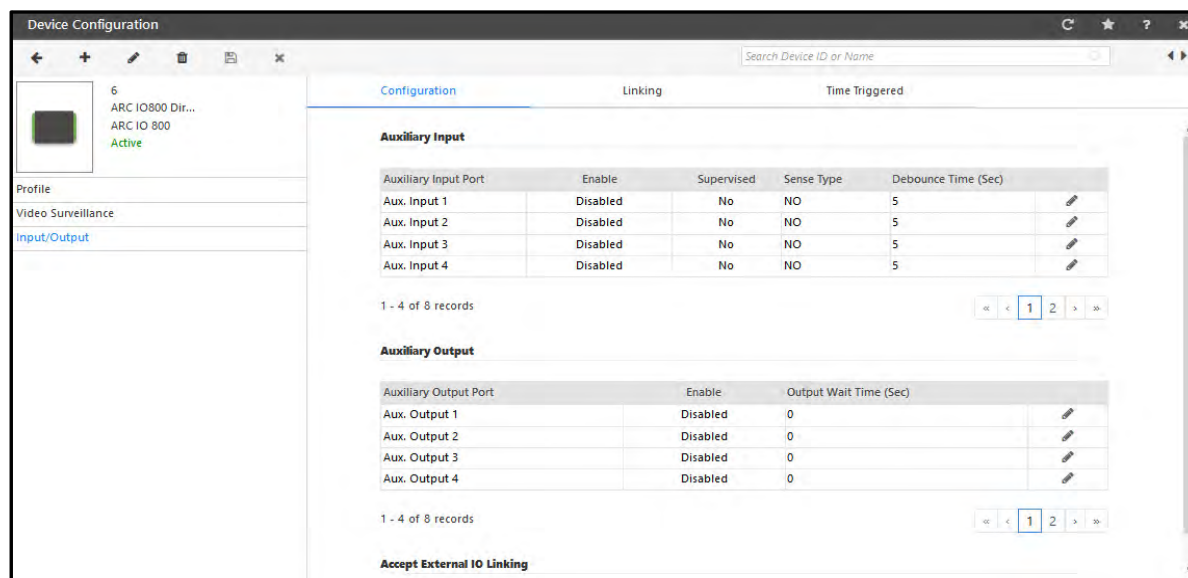
To access this, After selecting the device, Select **Device Configuration> Input Output**. The Input Output parameters can be set from the following sections:

- [“Configuration”](#)
- [“Linking”](#)
- [“Time Triggered”](#)

Configuration

In ARC IO800 as Direct door- Configuration, Linking and Time Triggered sections are available. In ARC IO800-Panel200 door- only Configuration section is available.

The **Configuration** section for a ARC IO800 appears as shown below.



The following parameters are available for configuration in both Direct door and Panel door:

Auxiliary Input Port	Enable	Supervised	Sense Type	Debounce Time (Sec)
Aux. Input 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	NO	5
Aux. Input 2	Disabled	No	NO	5
Aux. Input 3	Disabled	No	NO	5
Aux. Input 4	Disabled	No	NO	5

1 - 4 of 8 records

Auxiliary Input

- Click the **Edit** button and select the **Enable** checkbox to enable the system for such two-state monitoring.
- Select the **Supervised** checkbox to enable the door for four-state monitoring where the door is also monitored for *door fault* and *door disconnection*. Specify the **Sense Type** as **NC** or **NO**.
- Debounce Time (Sec)** - Specify the Debounce time in seconds. Default value is 3 sec and range should be 0-99 sec. It defines the minimum time for which an input interface must be maintained in a given state before the system reports it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.
- Click **OK** and **Save** to save the Auxiliary Input settings.

Auxiliary Output

- Click the **Edit** button and select the **Enable** checkbox to enable Auxiliary Output (e.g. Fire Alarm) for the selected device. To set an additional waiting period before the Aux Output signal is sent, enter an **Output Wait Time (Sec)**.

Direct Door

Auxiliary Output Port	Enable	Output Wait Time (Sec)
Aux. Output 1	<input checked="" type="checkbox"/>	5
Aux. Output 2	Disabled	0
Aux. Output 3	Disabled	0
Aux. Output 4	Disabled	0

1 - 4 of 8 records

Accept External IO Linking

Enable ☒

- Click **OK** and **Save** to save the Auxiliary Output settings.
- Accept External IO Linking** - Select the Enable checkbox to enable device-to-device IO Linking i.e. input from one Direct Door can trigger output in another Direct Door.



This feature is available in direct door only.

Panel Door

Auxiliary Output Port	Enable	Output Group	Name	Elevator ID	Name	Floor ID	Name	
Aux. Output 1	Disabled	1	DC Aux Ports	1	Elevator1	1	Ground Floor	
Aux. Output 2	Disabled	1	DC Aux Ports	1	Elevator1	3	Telecom Floor	
Aux. Output 3	Disabled	1	DC Aux Ports	2	Elevator2	2	Surveillance FI	
Aux. Output 4	Disabled	1	DC Aux Ports					

1 - 4 of 8 records

« < 1 2 > »

The Auxiliary Output ports are mapped with floors of same or different Elevators as shown above.

If multiple floors are mapped with one Auxiliary Output port; then one floor mapping will be shown in Floor ID- Name column and other mappings will be shown on hovering over Info icon.

Example: Ground Floor and Canteen Floor of Elevator1 are mapped with Aux Output1 so the Floor column shows Ground Floor and Info icon shows Canteen Floor as shown below.

Auxiliary Output Port	Enable	Output Group	Name	Elevator ID	Name	Floor ID	Name	
Aux. Output 1	Disabled	1	DC Aux Ports	1	Elevator1	1	Ground Floor	
Aux. Output 2	Disabled	1	DC Aux Ports	1	Elevator1	3	Telecom Floor	
Aux. Output 3	Disabled	1	DC Aux Ports	2	Elevator2	2	Surveillance FI	
Aux. Output 4	Disabled	1	DC Aux Ports					

1 - 4 of 8 records

« < 1 2 > »



1. If the Auxiliary Output port is not mapped with any floor; then Elevator ID= Name and Floor ID-Name will be blank.

2. If Auxiliary Output port is mapped with more than 1 floors of same Elevator; then Floor No.- Name will be shown as the first entry data as per Floor No.

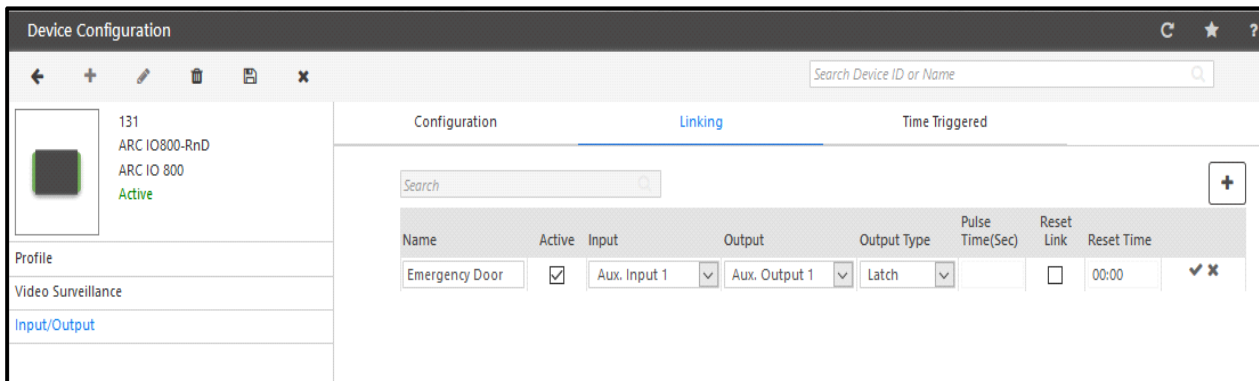
3. If Auxiliary Output port is mapped with more than 1 floors of different Elevator; then Elevator ID - Name will be shown as the first entry data as per Elevator ID and display its corresponding floor ID - Name.

Linking



This section is available in direct doors only.

The **Linking** section appears as shown below.



The COSEC application supports the Input/Output Linking feature to activate an output port based on a trigger received from an input port on the same Direct Door. This option enables the administrator to define how an event or events (input port) will trigger an output on the selected door.

Select a Input-Output linking row or click edit button.

- **Name** - Specify a name for the new I/O linking program to be defined.
- **Active** - Select this checkbox to activate this linking program.
- **Input/Output**- Select the **Auxiliary Input** and **Auxiliary Output** for which the IO link is to be set.
- **Output Type** - Specify the appropriate type of output from the following four options available in the drop down list:
 - Pulse: With this type of output, the user needs to define the Pulse time in seconds.
 - Interlock: With this option, the output follows the input. The relay output is triggered as long as the input is activated after which it returns to normal state.
 - Latch: With this option, it is denoted that the relay output will be in an energized condition for infinite period and needs to be reset manually.
 - Toggle: With this option, the output group toggles its state whenever an input group is activated.
- **Pulse Time (sec)** - For a *Pulse* output type, specify the pulse duration in seconds.
- **Reset Link**- Select this checkbox to reset the link automatically after a defined time period.
- **Reset Time**- Enter the time period in hh:mm format at which the link will get reset automatically. Suppose, an IO Link gets activated on 21/04/2017 at 15:00. And Reset Time is set as 18:00. When Device Time is 18:00 then that IO link will get reset.
- Click the **OK** button and **Save** the configuration.

Time Triggered

On the **Input Output** page, select the **Time Triggered** section as shown.

The screenshot shows the 'Time Triggered' configuration window. It has tabs for 'Configuration', 'Linking', and 'Time Triggered'. Below the tabs is a search bar and a table. The table has columns: 'Function Name', 'Active', 'Time', 'Duration(Sec)', 'Days', and 'Output'. The first row shows 'Siren Activate' with 'Active' checked, 'Time' as '00:00', 'Duration(Sec)' as '10', 'Days' as 'Select', and 'Output' as 'Aux O/P'. A dropdown menu is open for the 'Days' column, showing options: 'Check All', 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', and 'Holiday', all with green checkmarks.

This functionality enables the user to control the activity of an Output without manual intervention. The time triggered functions are used for activating events like door unlock and siren activation that are set as per the start time and for the configured time duration. This functionality is designed to energize outputs for predefined periods at the configured time. The COSEC access control system supports up to 20 Time Triggered functions on a Direct Door.

The screenshot shows the 'Time Triggered' configuration window with the 'Days' dropdown menu closed. The table now shows 'Siren Activate' with 'Active' as 'Yes', 'Time' as '00:00', 'Duration(Sec)' as '10', 'Days' as 'Su Mo Tu We Th Fr Sa Ph', and 'Output' as 'Aux O/P'. There are edit and delete icons at the end of the row.

PATH Door

Compact, robust and cost-effective PATH series door controllers; '**PATH V1**' and '**PATH V2**' assure reliable and long term performance as at the building gates and doors for Access Control application. PATH Doors can be connected as **Direct Door** as well as **Panel Door**.



The Configuration of PATH Controller and PATH V2 is similar. In this manual; configuration of PATH Controller (V1) is explained for reference.

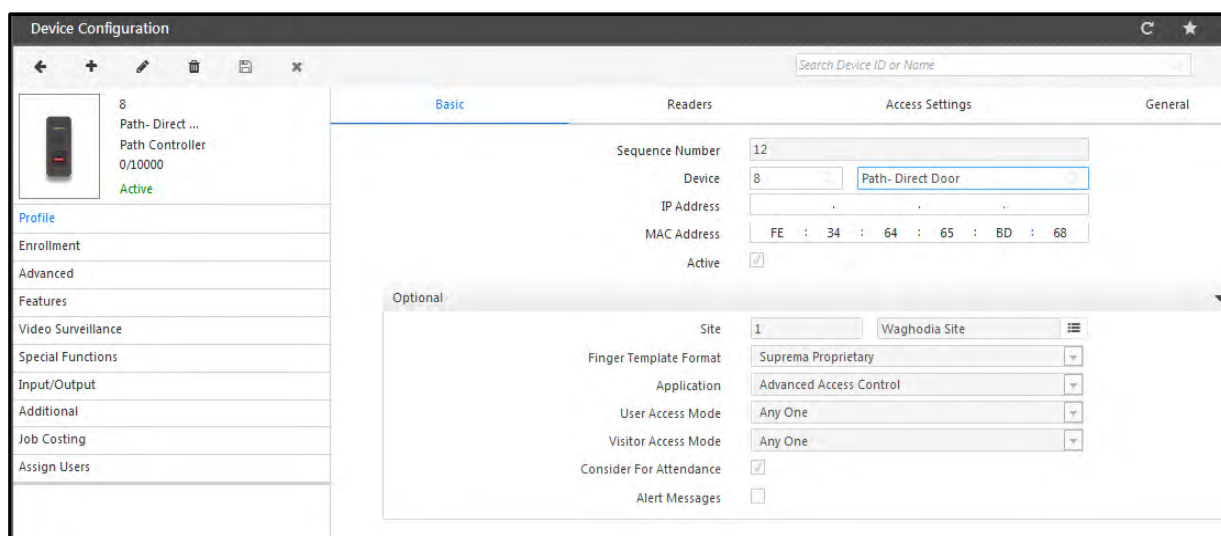


The difference between PATH V1 and PATH V2 is the number of 'user capacity' and 'event storage'. PATH V1 supports 10,000 storage capacity and PATH V2 supports 50,000 user storage capacity. Also PATH V2 supports the Wi-fi as well as Bluetooth connectivity.



In addition, the PATH V1 contains PIC32 processor whereas PATH V2 runs with the AM3352 processor.

The Device Configuration for Path Controller V1 appears as shown below.



The screenshot shows the 'Device Configuration' window. On the left is a sidebar with a device icon and a list of configuration tabs: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, and Assign Users. The main area is divided into four sections: Basic, Readers, Access Settings, and General. The 'Basic' section is active, showing fields for Sequence Number (12), Device (8), IP Address, and MAC Address (FE : 34 : 64 : 65 : BD : 68). The 'Readers' section shows the device name 'Path- Direct Door'. The 'Access Settings' section shows Site (1), Waghodia Site, Finger Template Format (Suprema Proprietary), Application (Advanced Access Control), User Access Mode (Any One), Visitor Access Mode (Any One), Consider For Attendance (checked), and Alert Messages (unchecked).

Enter the MAC address of the door. The IP address will be displayed automatically once the device comes online in Monitor.

To add Devices automatically, select *Admin Module> System Configuration> Global Policy> Device*.

Enable the “Auto Add New Devices” checkbox. Once the device is connected in network, it will come online in COSEC Monitor.



The Monitor Service must be running while adding the device to COSEC.

Once the device is configured, click the **Save** button to save the configuration.

To know more about configuring devices, click on the links for different tabs of Device configuration.

- [“Profile”](#)
- [“Enrollment”](#)
- [“Advanced”](#)
- [“Features”](#)
- [“Video Surveillance”](#)
- [“Special Functions”](#)
- [“Input/Output”](#)
- [“Additional”](#)
- [“Job Costing”](#)
- [“Assign Users”](#)
- [“Identification Server”](#)

Profile

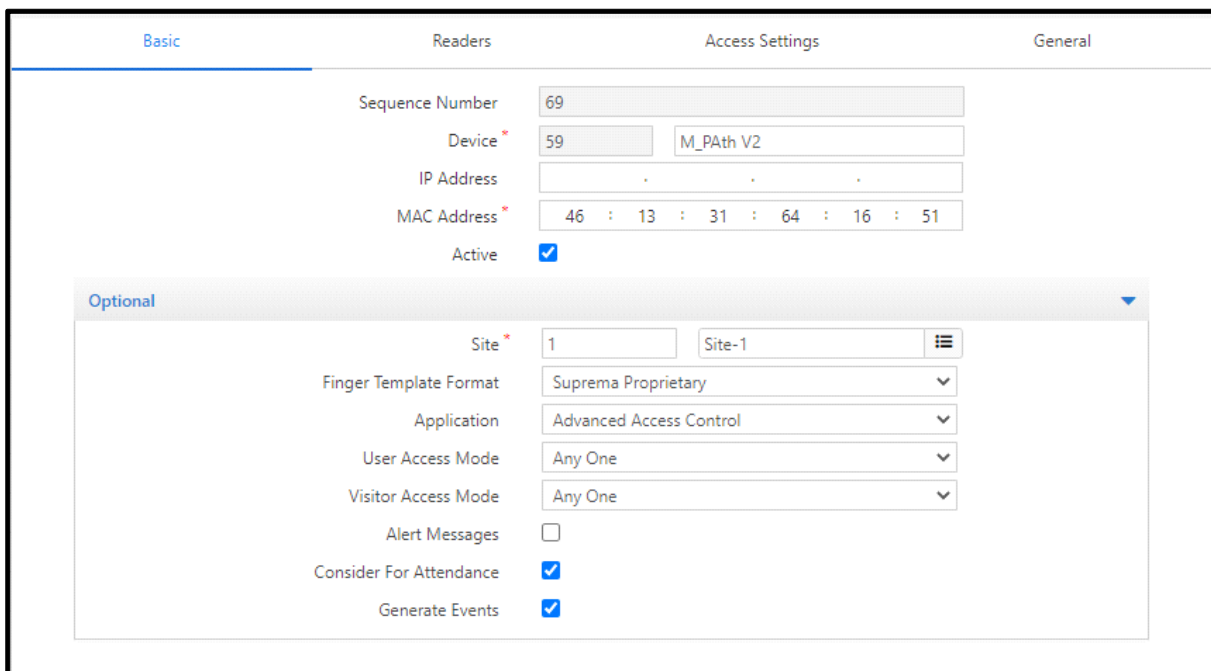
This section enables the user to set up the basic profile for any new device. Setting up a door profile involves defining basic parameters to set up any door controller device.

To do this, select **Device Configuration> Profile**. The Profile can be configured in the following sections:

- “Basic”
- “Readers”
- “Access Settings”
- “General”

Basic

The **Basic** section for PATH as Direct door is shown below:



Configure the following options as required:

- **Sequence Number** - This is a system generated sequence number for each new device.
- **Device**- Specify a name that can be assigned to the door. The Door ID is auto-generated by the system.
- **Connection Type** - Applicable only for Panel Doors. Specify the connection type as **Ethernet** or **RS485**.
- **IP Address** - This is the IP address assigned to the door. Once the device connection is established, this field will automatically display the door IP address.
- **MAC Address** - Specify the MAC Address of the door.



MAC address of door is required while manually adding the door to the COSEC Monitor. Note the MAC address from the device when it is powered on.

- **Active** - Check the box to activate the device on the network.



To add the Device automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the “**Auto Add New Devices**” checkbox.

The device will be added automatically but make sure you enable the **Active** checkbox in order to connect the device to the network. Once the device is connected to the network, it will come online in COSEC Monitor.

For PATH as Direct door, the **Optional** tab shows the following configuration.

Optional	
Site	1 Waghodia Site
Finger Template Format	Suprema Proprietary
Application	Advanced Access Control
User Access Mode	Any One
Visitor Access Mode	Any One
Consider For Attendance	<input checked="" type="checkbox"/>
Alert Messages	<input type="checkbox"/>

- **Site** - Select the site to which this door is to be assigned from the site picklist window. Site is created from Devices> Masters> Site.
- **Finger Template Format** - Select the format as Suprema Proprietary or Suprema ISO according to which the templates will be enrolled. For globally setting the template format, you can set from Global policy.
- **Application** - Select the application type for which the device is to be used. The options are **Basic Access Control**, **Advanced Access Control** or **Enrollment**.



The available license is ACS and Application is set to Basic Access Control. If this ACS voucher exhausts, then while dispatching Basic Configuration of device, application type will be sent as 'Advance Access Control'.

- **User/Visitor Access Mode** - Defines the type and combination of credentials required to identify and validate a user/visitor at the Door Controller. Select the appropriate credential combination from the drop down list.

The options available are:

- Any one
- Card
- Card + Biometrics
- Card + Biometrics + PIN
- Card + PIN
- Biometrics
- Biometrics + PIN
- Biometrics then Card
- Card then Biometric
- **Consider for Attendance** - Select this checkbox if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as access control events.

- **Alert Messages** - Select this checkbox to enable the application to send alerts based on events from this door.
- **Generate Events:** This check-box is enabled by default. You can disable the check-box if the server is not required to receive any events from the respective devices.



'Generate Events' option is available only for PATH V2 variants.

For PATH as Panel door, the **Optional** tab shows the following configuration.

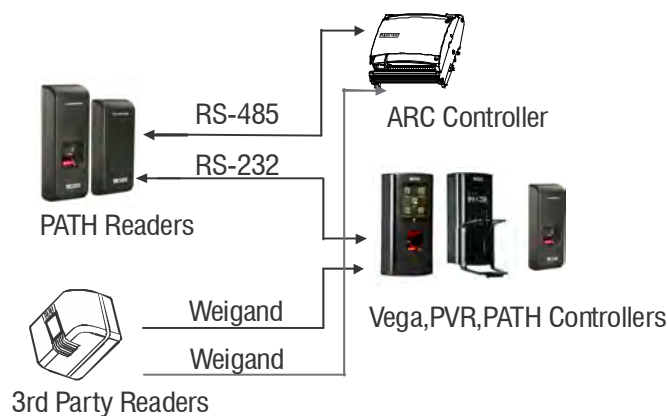
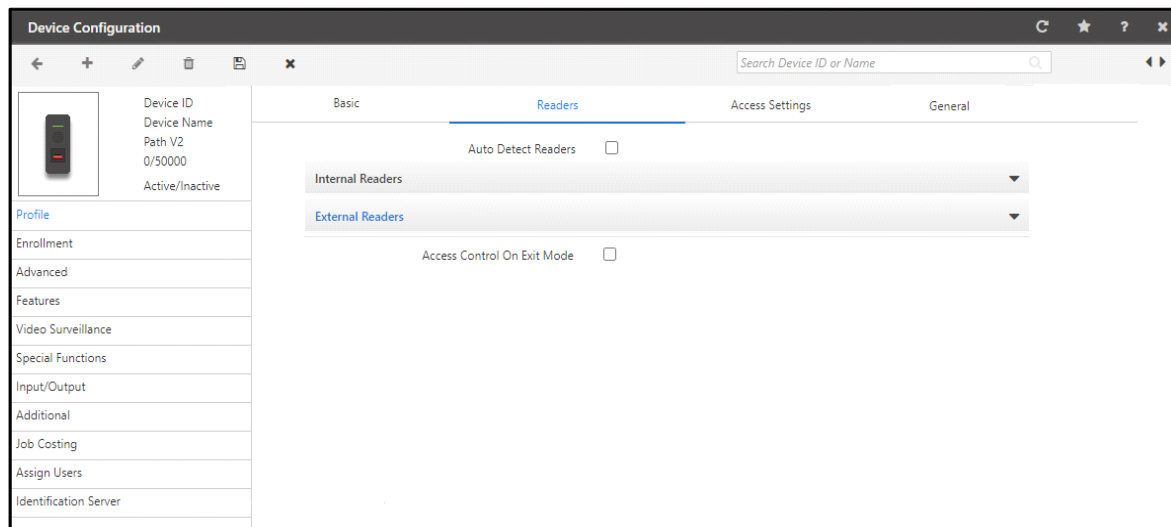
- **Access Zone** (only for panel doors) - Assign an access zone to the door by selecting from the drop down menu.
- **Access Cluster** (only for panel doors) - Assign an access cluster to the door by selecting from the drop down menu.
- **Door Group:** Door Group drop down includes list of all configured Door groups on corresponding panel. An additional option as 'None' is available and selected by default.
- **Auto IP Assignment:** There is option where panel door can be assigned its IP from device webpage. To enable this check the Auto IP Assignment box.



Access Zone and Access Cluster are configured while configuring Panel200.

Readers

Readers are important hardware components in a biometric door device. They may be internal or external. This section enables the administrator to configure both internal and external readers for a door as shown.



The following parameters are available for configuration:

- **Auto Detect Readers** (for direct doors only) - Select this checkbox to enable auto detection of Readers on a door controller connected to the server.

Internal Readers

This option allows the configuration of the Internal Reader for the selected door.


- **Mode:** Select the Mode as **Entry** or **Exit** from the drop down list.
- **Card Reader Type;** Select the Card Reader Type from the following options:
 - EM Prox Reader
 - HID Prox Reader
 - MiFare Reader
 - HID iClass-U Reader
 - HID iClass-W Reader
- **Card Format:** Only Single card format is applicable to PATH as direct door. The default card format is applied to PATH as direct door. To assign another card format for internal readers of the device; delete the default format and select another format from the picklist. To know more about Card Formatting, refer ["Card Formats"](#).

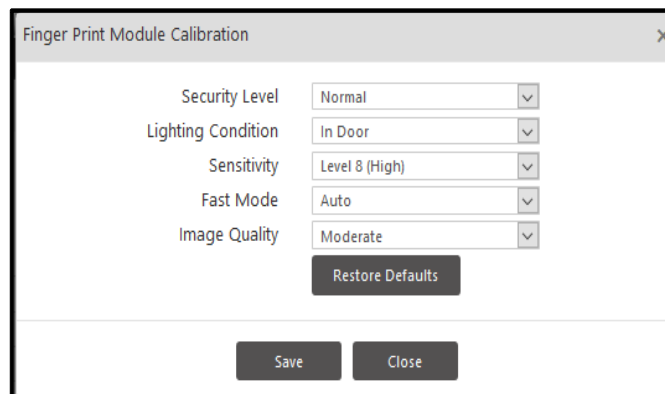
Multiple Card Format

For PATH as panel door; you can assign multiple card format. To assign multiple card formats to device click on **Add** button. Then click the picklist to select the card format. And click **OK** to save the format.

Similarly you can add maximum 5 card formats. When the card format is saved, the Configurable bits of that format as configured from Masters> Card format will be displayed here. Multiple Card format configurations will be dispatched to door separated by '**Format ID**' that is 'Member No.' along with all other format related parameters.

- Select the **Finger Reader Type** as **Finger Reader**.

Click the **FP Reader Configuration**  button to set the **Security Level**, **Lighting Condition**, **Sensitivity**, **Fast Mode**, **Image Quality** and **Restore Defaults** for the selected FP Reader as shown.



Finger Print Module Calibration

- **Security Level:** Security level specifies FAR (False Acceptance Ratio). Since FAR and FRR (False Rejection Ratio) is in inverse proportion to each other, FRR will increase with higher security levels.

For regular Time-Attendance system “**Normal**” level can be selected. For high security areas requiring complete or maximum matching of template, “**Highly Secure**” level must be selected. For approximate matching of template, “**Secure**” level can be selected.

- **Lighting Condition:** Optical sensors are sensitive to lighting condition. With this parameter, users can tune optical sensors to be adapted for their lighting environment. Select the In Door or Out Door option based on the device location.
- **Sensitivity:** Specifies sensor sensitivity to detect a finger. On high sensitivity, the module will accept the finger input more easily. Level 8 has the highest sensitivity.
- **Fast Mode:** Fast Mode parameter can be used to shorten the matching time with a little degradation of authentication performance. In typical cases, Fast Mode 1 is 2 to 3 times faster than Normal mode while Fast Mode 5 is 6 to 7 times faster than Normal mode. There is also an Auto mode.
- **Image Quality:** When a fingerprint is scanned, the module will check if the quality of the image is adequate for further processing. Image quality parameter specifies the strictness of this quality check. Strongest option might lead to higher number of finger rejections during the enrollment process.



Good quality of enrollment (around 70-75% quality) is recommended for proper identification of enrolled templates.

- Click on the **Restore Defaults** button to return the field values for this page to default values if needed.
- **Advertise Bluetooth-** Select this checkbox to enable Bluetooth of the device by which the device will be visible to others. Then configure the following parameters.
- **Bluetooth Name-** By default, if the Device Name is configured then it will be displayed here along with the Mode. The prefix will be the Device Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the bluetooth name as per your requirement. The Bluetooth Name can be a maximum of 10 characters.

- **Bluetooth Range-** The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m-2m), Medium (5m-7m) or Long (>8m).

Click **Save** to save all the configurations.

External Readers

This option allows the configuration of the External Reader for the selected door.

Member No	Card Format	Configurable Bits
1	Default Format	0

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop down list.
- **External Reader Type:** Select the desired type of External Reader from the drop-down list.
- **Card Format** - Select a card format to be applicable for external readers of the device. See Internal Readers section for details.
- **Exit Switch** - Select this checkbox to enable the use of **Exit Switch**.
- **User/ Visitor Access Mode** (not for Panel Doors) - Select the desired user/ visitor access mode applicable for external readers.
- **Configure Bluetooth from Server:** When you select **External Reader Type** as — CB U Reader, ATOM RD300, ATOM RD200 or ATOM RD100, select **Configure Bluetooth from Server** checkbox to enable Bluetooth feature for the mentioned external readers.

Once you enable **Configure Bluetooth from Server**, configure the following Bluetooth parameters:

- **Advertise Bluetooth**- Select this checkbox to enable Bluetooth of the PATH device by which the device will be visible to others. Then configure the following parameters
- **Bluetooth Name**- By default, if the Device Name is configured then it will be displayed here along with the Mode. The prefix will be the Device Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the bluetooth name as per your requirement.

The Bluetooth Name can be a maximum of 20 characters.

- **Bluetooth Range**- The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m-2m), Medium (5m-7m) or Long (>8m).



If Auto Detect Reader is enabled, then External Reader Bluetooth parameters will not be visible.

- **Access Control On Exit Mode** - Select this check box to enable the checking of the following access control policies on door when the external reader is in the 'exit' mode.
 - User enabled
 - User validity
 - Blocked user
 - Time Based Access Check
 - ASC
 - User Access Group

When this parameter is unchecked, all the following access control features will be checked on door (which are applicable and configured).

- User enabled
- Blocked user
- Time Based Access Check
- ASC
- User Access Group
- Deadman
- Door application mode
- Use count
- Mantrap
- Anti-pass back
- Panel Route access
- Smart card based route access
- 2-person
- Access mode
- Occupancy control
- Visitor escort rule

Click **Save** to save all the configurations.

Access Settings

This section is available for direct doors. The **Access Settings** page appears as shown below.

The screenshot shows the 'Device Configuration' window with the 'Access Settings' tab selected. The left sidebar lists various configuration categories, and the main area displays the following settings:

- Universal Time Zone:** A dropdown menu showing '(GMT+05:30)Chennai, Kolkata, New Delhi, Mumbai'.
- Time Format:** A dropdown menu showing '24 Hours'.
- Auto Synchronize with NTP:** A checkbox that is checked.
- Preferred NTP Server:** An empty text input field.
- Working Days:** A grid of checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, Sat, and Holiday, all of which are checked.
- Working Hours(HH:MM):** Two text input fields showing '00:00' and '23:59'.
- Holiday Schedules:** A table with four rows, each containing a 'Holiday Schedule' number (1-4) and a 'Schedule' dropdown menu.

- **Universal Time Zone** - Select the geographic time zone in which the DOOR will operate.
- **Time Format** - Specifies the time format to be displayed on Door Controller LCD display. The formats available are:
 - 24 Hours
 - 12 Hours

Select the relevant option from the drop down list as per the site requirements.

Auto Synchronize with NTP

If Date and time is to be automatically synchronized as per the **Preferred NTP Server** (predefined or user-defined NTP server address) selected by user, then you must enable **Auto Synchronize With NTP** checkbox.

Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from device webpage, which will be reflected on device display.

- When Auto Synchronization with NTP is disabled Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 1. You can specify the Preferred NTP server of your choice. In this case device will first try to get Date and Time from that server address.
If it does not get Date and Time in three tries; device will check from pre-defined NTP servers.
If you have entered one of the three pre-defined NTP servers(ntp1.cs.wisc.edu , time.windows.com , time.nist.gov); then device will first check that server first.
If it receives updated Date and Time then Updated Date and Time will be reflected on device webpage and display screen.
 2. You can keep the Preferred NTP server as blank. In this case device will check for Date and Time from the first NTP server.
 3. If user has manually entered Date and Time from webpage or Device Menu then those values of Date and Time will be reflected on device webpage and display screen.

In the case of the **Manual** option the administrator can manually update the time on the Door with that of the system time as and when required. This can be accomplished from the control application.

- **Working Days** - Specify the days on which the default working hours should be applicable. Check the relevant boxes to specify the active days.
- **Working Hours (HH:MM)** - Define the default working hours in HH:MM format.
- **Holiday Schedule** - This section allows the administrator to assign up to four holiday schedules to the device by using the Holiday Schedule pick-list.



If the same holiday schedule is configured for a user and for the door controller on which the user is assigned, then the user's attendance marking on this device, on any of the scheduled holidays will always be marked as a holiday.

General

The **General** page appears as follows.

Device Configuration

Search Device ID or Name

Device ID
Device Name
Path V2
0/50000
Active/Inactive

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Basic Readers Access Settings General

Mute Buzzer ☐

Allowed Acknowledgement

Display Duration (ms) 3000

LED - Buzzer Duration Long ⓘ

Denied Acknowledgement

Display Duration (ms) 3000

LED - Buzzer Duration Long ⓘ

- **Mute Buzzer** - User can mute or unmute the door buzzer by checking or clearing the box respectively. This is applicable for both Direct and Panel door.
- **Allowed Acknowledgment**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgment Allowed' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.
- **Denied Acknowledgment**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgment Denied' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.

Enrollment



The Enrollment section is not available for panel doors.

The Enrollment page appears as shown below.

- **Enrollment through Special Function** - Select this check-box to enable the feature. This allows the user to specify the user credential that can be enrolled by using the enrollment special function from the DOOR Controllers.
- **Enrollment Mode** - Select the Credential from the drop-down list that can be enrolled using the special function at the DOOR. The options are **ReadOnlyCard**, **SmartCard**, **Biometric** and **BiometricthenCard**, and **DuressFinger**. Refer [“Enroll Credentials”](#) or [“Enrolling Users”](#) to enroll User/Worker. Refer [“Enrollment”](#) or [“Enroll Credentials”](#) to enroll Worker. Refer [“Enroll Credentials”](#) to enroll a Visitor.



DuressFinger is only applicable for User and Worker.

- **Template Per Finger** - This parameter displays the values as configured at the global level. It shows the number of templates per finger getting enrolled.
- **Max Number of Fingers** - This parameter displays the values of the maximum number of fingers configured at the global level.
- **Number of Fingers/Cards** - Select the number of cards or fingerprints to be enrolled based on the credential option selected in the Enrollment Mode parameter.

Advanced

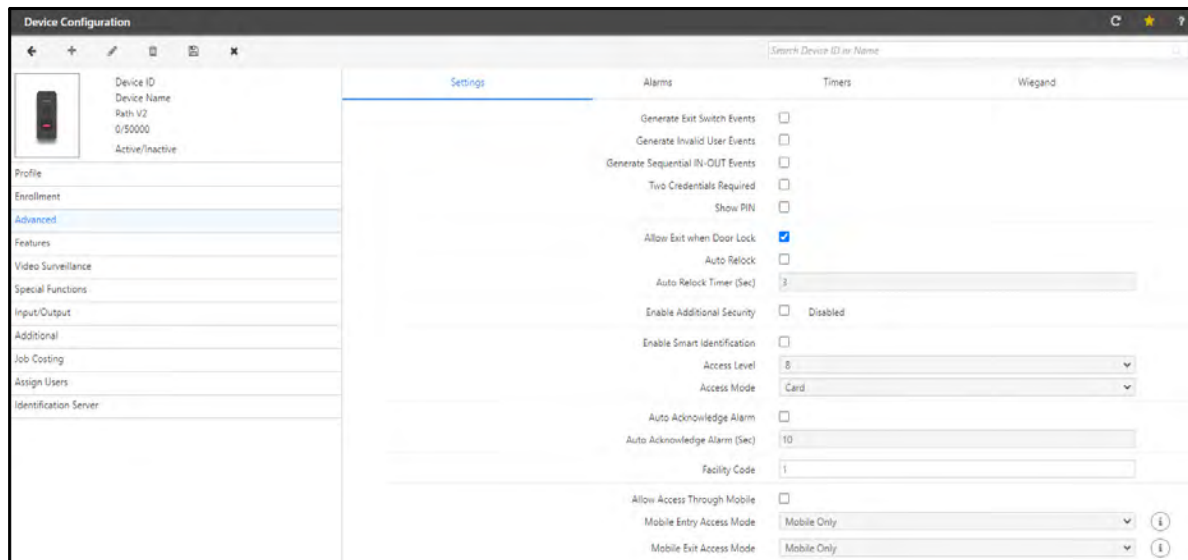
The Advanced tab allows the user to configure some advanced parameters such as access control settings, alarms and device timers.

To access this, After selecting the device, Select the **Advanced** tab from **Device Configuration** page. The advanced settings can be configured from following sections:

- “Settings”
- “Alarms”
- “Timers”
- “Wiegand”

Settings

The **Advanced Settings** page for PATH Door as a **Direct Door** appears on your screen as shown below:



The following parameters are available for configuration:

- **Generate Exit Switch Events** - Select this checkbox to enable the door to generate events every time the exit switch is used.
- **Generate Invalid User Events** - Select this checkbox to enable the door to generate events for invalid user inputs.
- **Generate Sequential IN-OUT Events** - Select this checkbox to generate user punches on device as the sequential IN-OUT events irrespective of whichever mode in which device is functioning.
- **Two Credentials Required**- Select this checkbox to enable the feature of verifying 2 credentials mandatory for users allowed to By-pass finger/palm.
- **Show PIN** - Select this checkbox to display the characters of PIN when the PIN is entered on device.
- **Allow Exit when Door Lock** - Select this checkbox if users are to be allowed to exit even when the Door relay is in locked condition.

- **Auto Relock** - Select this checkbox to allow the door to relock immediately when the door status changes to close after normal open irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Relock Timer** - Specify the time in seconds for the Auto Relock operation.
- **Enable Additional Security**- Select this checkbox to enable additional security at the selected Door Controller.



Changing this value can affect the SI function. Click on the **Default Code** button to reset the **Additional Security Code** to the value set in the **Global Additional Security Code** field on the Global System Policy page.

- **Enable Smart Identification** - Select this checkbox to enable this functionality at the selected Door Controller and select the **Access Level** and the **Access Mode** from the drop down list.
- **Auto Acknowledge Alarm** - Select this checkbox to enable the auto-acknowledgment of all alarms for this device.
- **Auto Acknowledge Alarm (sec)** - Set the time in seconds for the Auto Acknowledge Timer. The wait timer will start and on expiry of the timer, the alarm buzzer will stop automatically.
- **Facility Code** - Set a value for Facility Code to be set for access modes other than “Card”, if Facility Code is expected in Wiegand Output. This will be applicable to all direct doors except Door V1 and V2.
- **Allow Access Through Mobile**- Check the box to allow the access to device using COSEC ACS App.
- **Mobile Entry/Exit Access Mode**- Select the entry and exit door access mode from the options of **Mobile Only**, **Mobile then Biometrics**, **Mobile then Card** and **Mobile then PIN**.



If User Access Mode is selected as “None” in Zone Configuration and Mobile Access Mode is selected as “Mobile Then Biometrics” then door can be accessed through Mobile and then Biometric credential.

The **Advanced Settings** page for **PATH** as a **Panel door** will appear on screen as shown below:

1. **Tail-Gating** - Tail-gating refers to an access violation which occurs when more than one person tries to enter a secured area using a single person's access credentials. If this option is enabled on the panel door, the occupancy count of a zone should be incremented or decremented considering both the punch as well as the auxiliary input port of the panel door (say, input from a beam-counter). Set the wait timer for resetting the tailgating count (**Reset Wait Timer**) based on the door lock status or the door pulse wait timer (as configured).
2. **Man Trap Entry Timer (Sec)** - This check-box enables an alarm wait timer on the panel door to ensure that the user enters the next sequential door of a man-trap within a specific time-frame.
3. **Man Trap Exit Timer (Sec)** - This check-box enables an alarm wait timer on the panel door to ensure that the user exits the panel door to enter the next sequential door of a man-trap within a specific time-frame.
4. **Enable Man Trap Door Interlocking:** Select this check-box to activate the Door Interlock for the selected door (say Door1). This means if the Door1 is open then other doors will remain close.
 - **Door:** Click the pick list and select the doors to be assigned for the Interlock to the selected door (Door1). Suppose Door2 and Door3 are selected for Interlock with Door1. So When Door1 opens; Door2 and Door3 will remain close.



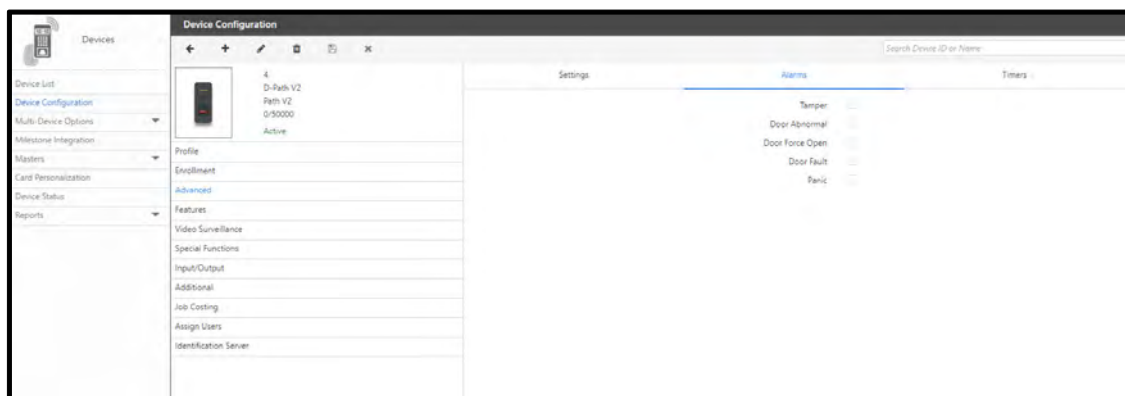
For Degrade mode Door Interlocking feature will not work.

Whenever a door is in abnormal state and for that door interlocking is enabled then user access in other doors of the interlocking group is allowed.

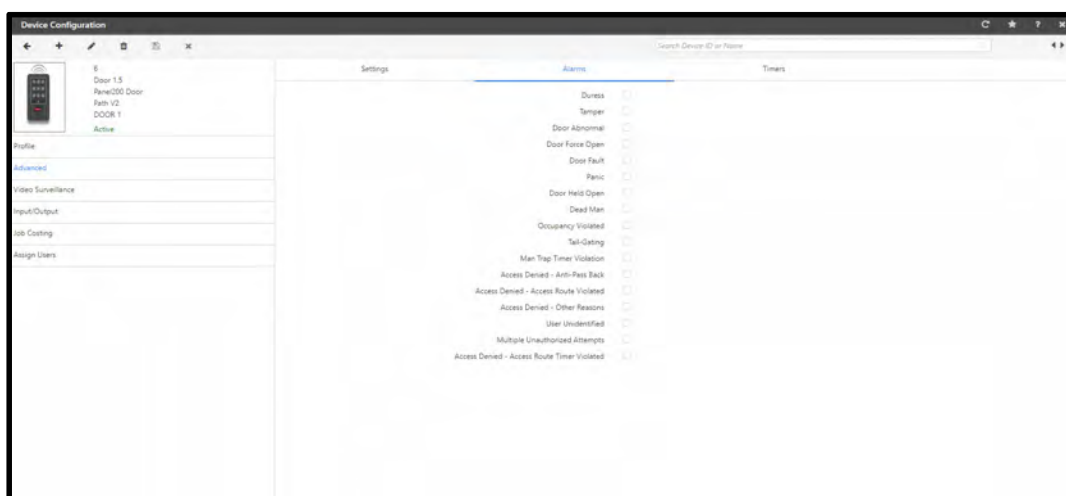
Alarms

In Alarm tab, you can assign below list of alarms to the door.

For Direct Door



For Panel Door



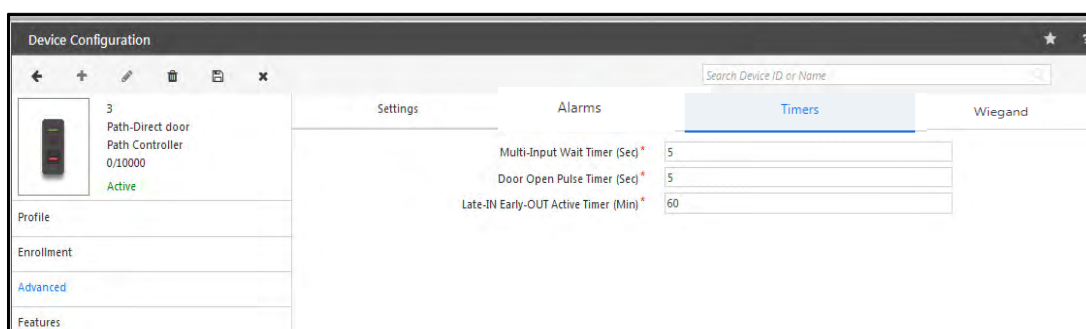
Select the respective checkbox of alarms which you want to enable.



Duress Alarm is only configurable for **Panel200 Path V2 Door**.

Timers

This section allows the configuration of various types of pre-defined device timers which can trigger off specific responses. In COSEC, timers are often used to control door behaviour and for triggering alarms. The Timers page for PATH V1 appears on your screen as shown below:



For PATH V2 and additional 'Inter-Digit Wait Timer' option is also available as shown below.

Inter-Digit Wait Timer (Sec) *	<input type="text" value="3"/>
Multi-Input Wait Timer (Sec) *	<input type="text" value="5"/>
Door Open Pulse Timer (Sec) *	<input type="text" value="5"/>
Late-IN Early-OUT Active Timer (Min) *	<input type="text" value="60"/>

- **Inter-Digit Wait Timer (sec)** - Specify the time period in seconds between two key inputs on the device keypad. On expiry of this timer, the system considers the user input to be complete and is ready for the next input.

- **Multi-Input Wait Timer (sec)** - Specify the time in seconds for which system needs to wait for the second credential input from the user when more than one credential is to be used to grant access.



We recommend you to set the timer value as greater than or equal to 10 seconds to avoid access denial issues to users. This is applicable when the system reads the credentials (biometric) from the user's Smart Cards.

- **Door Open Pulse Timer (sec)** - Specify the time in seconds (3 to 99) for the door to be energized for a valid credential. If the opened door does not return to a closed state before the expiry of this timer, the door will generate a "Door Abnormal" alarm.
- **Late-IN Early-OUT Active Timer (min)** - Specify the time in minutes for which the Late-IN and Early-OUT special functions will remain active after being enabled at the Door Controller.



The above features are available only for direct doors.

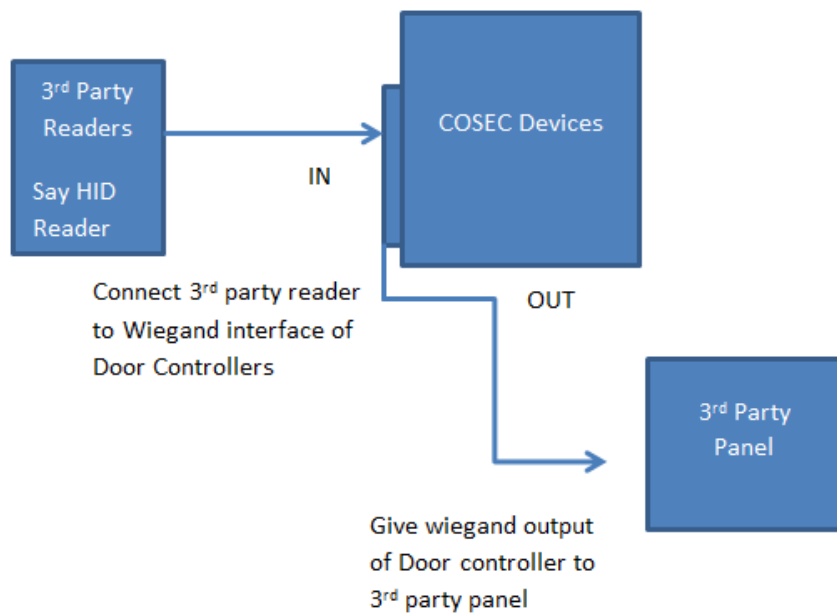
- **Pulse Time (sec)** - Specify the time in seconds for the panel door to be energized for a valid credential.



This feature is available only for panel doors.

Wiegand

The screenshot shows the 'Device Configuration' window with the 'Wiegand' tab selected. The left sidebar lists various configuration options, with 'Advanced' highlighted. The main area displays the 'Wiegand Interface' settings, including 'Reader Input' (dropdown), 'Output Mode Parameters' (checkbox), 'Wait For Panel Signal' (checkbox), 'Signal Wait Timer (Sec)' (input field with value 2), 'Wait For User Verification' (checkbox), 'Wiegand Output Format' (dropdown with value 26 Bit), and 'Send From' (dropdown with value MSB Bit).



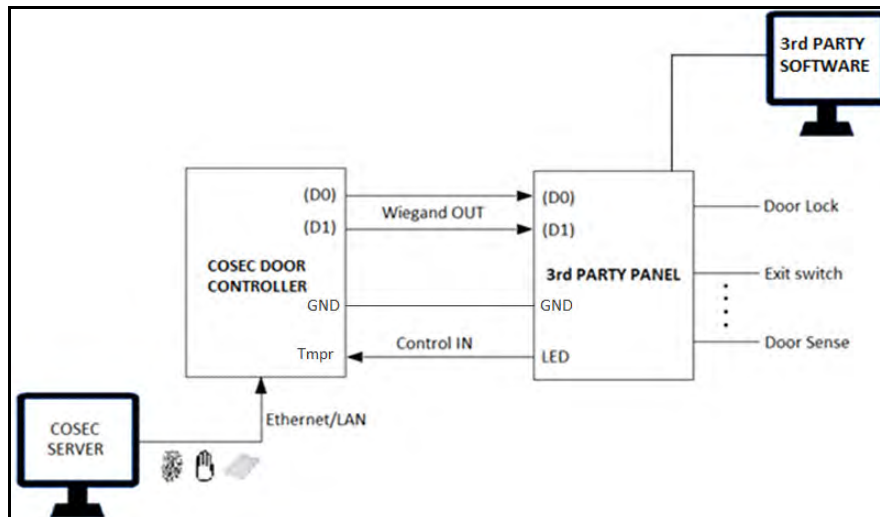
- **Wiegand Interface** -The PATH Controllers can be connected both as input devices (e.g. to receive data from a Wiegand Reader) or output devices (e.g. to support output to third party panel) via the Wiegand interface as shown above.

So select the interface of Door controller as **Output Mode** to work as weigand output to panel or **Reader Input** to take data from third party reader. If Reader Input option is selected, all the output mode parameters will be disabled.

If you select Output mode then configure the **Output Mode Parameters**.

- **Wait For Panel Signal** - If this option is enabled the door will wait for reply from the connected third party device before triggering any output, as per the defined **Signal Wait Timer (Sec)**.
- **Wait For User Verification** - If this option is enabled, user verification will be requested on the third party device before triggering any output.
- Specify the **Wiegand Output Format** and sending order for reader data as MSB or LSB Bit in the **Send From** field.

Wiegand Out Interface



- Also for the **Custom** format, user can configure details of fields to be sent as output from the Wiegand reader that has been added.

For each of the listed events, a custom Wiegand Output Format can be selected using the picklist button. Also an access code can be assigned for each communication (e.g. Invalid PIN Code). This will depend on the number of output bits configured for Access Code in the selected Wiegand Output Format. Also, See Devices> Masters> Wiegand Output Format.

Features

The Features tab allows the user to enable certain Access Control features for a device



The Features tab is available only with the Access Control Module license and is applicable only for direct doors.

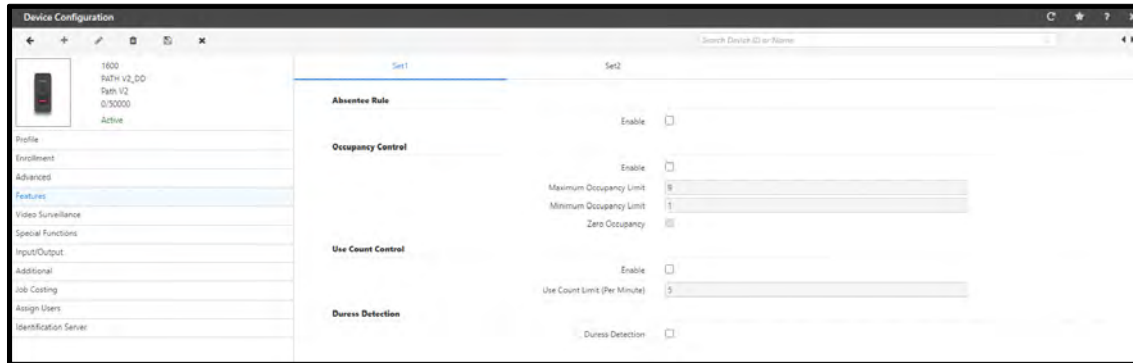
To access this, After selecting the device, Select **Device Configuration> Features**. The access control features for the device can be set from the following two sections:

- "Set1"
- "Set2"

Set1

This page allows the configuration of three rules - **Absentee Rule**, **Occupancy Control** and **Use Count Control**.

The page appears as shown below.



- **Absentee Rule** - Select this checkbox to enable this feature at the door. This rule sets the maximum number of days for non-use of a credential. On expiration of days limit, the user will be automatically blocked.
For configuring the rule *See Access Control> Absentee Rule*.
- **Occupancy Control** - Select this checkbox to enable the feature at the door and specify maximum number of users to be allowed within the controlled area after which a user exit is required to enable access to another user. Also specify the **Minimum Occupancy Limit** i.e. the minimum number of occupants the designated zone should have, and enable/disable the **Zero Occupancy** option to determine whether the designated zone should be allowed to be empty or not.
For configuring the rule *See Access Control> Occupancy Control*.
- **Use Count Control** - Select this checkbox to enable the feature at the door and specify the maximum number of uses per minute.
For configuring the rule *See Access Control> Use Count Control*.
- **Duress Detection** - Select the checkbox to enable the feature. Duress Detection is used to generate the duress alarm which informs that the user is forced to open the door under threat.

Set2

This page allows the configuration of three rules - **First-IN User Rule**, **Anti-Pass-Back (APB)** and **2-Person Rule**. The page appears as shown below.

The screenshot shows the 'Device Configuration' window for 'Set2'. On the left is a sidebar with a device icon and a list of configuration categories: Profile, Enrollment, Advanced, Features (highlighted), Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, and Assign Users. The main area is divided into three sections for rule configuration:

- First-IN User Rule:** Includes checkboxes for 'Enable' (checked), 'Reset On' (Day Change selected, Timer Expiry unselected), 'Access Timer (Sec)' (set to 3), and 'First-IN User Group' (set to 1). A 'List 1' button is also present.
- Anti-Pass-Back (APB):** Includes checkboxes for 'On Entry' (checked), 'On Exit' (checked), and 'Forgiveness' (checked). The 'Hard/Soft' option is set to 'Soft'.
- 2-Person Rule:** Includes checkboxes for 'Enable' (checked), a 'Mode' dropdown (set to Primary Must), 'Primary Group' (set to Select), 'Secondary Group' (set to None), and a '2nd Person Wait Timer (Sec)' (set to 5).

- **First-IN User Rule** -Select this checkbox to enable the feature at the direct door and select the First-In User group which would be valid at the door.
For configuring the rule *See Access Control> First- In User Rule> Assignment*
- **Anti-Pass Back (APB)** - Select this checkbox to enable the feature at the direct door.
For configuring the rule *See Access Control> Anti-Pass Back*
- **2-Person Rule** - Select this checkbox to enable the feature at the door and set the **wait time** in seconds after which the second person is allowed to punch on the door.
For configuring the rule *See Access Control> 2- Person Rule*

Video Surveillance

The Video Surveillance tab allows the user to configure parameters for video surveillance integration with the COSEC device.

It is available in Basic License.

To access this, Go to **Device Configuration> Video Surveillance**.

- “Visual Tagging”
- “Satatya”

Visual Tagging

The COSEC application can interface with some supported hybrid and network video recording systems and grab images triggered by user events at the Doors. The **Visual Tagging** option enables the administrator to define the video recorder parameters. The **Visual Tagging** page appears as shown below.



To view the user events and related images, go to **Admin > Views/Logs > Event View**. To know more about viewing events, refer to “Event View”.

The following parameters are available for configuration:

- **Capturing Device** - Select the video recording device type from the dropdown menu as shown. The compatible device types are:

- Matrix HVR/NVR
- Milestone

Matrix HVR/NVR

- **MAC Address** - In the event of selecting the Matrix HVR/NVR, the administrator needs to specify the MAC address of the video recorder device using “_” (underscore) as the separator.
- **Camera ID** - Specify the camera number or camera ID for IP cameras. For analog cameras specify the camera number.

- **Storage Root Folder** - Specify the Root folder PATH or FTP PATH where the uploaded images will be saved.
- **FTP Login Credentials** - Check this box to activate FTP login credentials for authentication.
- **Username** - Specify the FTP server username.
- **Password** -Specify the FTP server password.



Some COSEC devices do not support all the network connection options.

Milestone



*For more information on integration with **Milestone** devices, refer to [“Milestone Integration”](#).*

Satatya

This functionality is available for configuration only when the Matrix HVR/NVR device type is selected as the **Capturing Device** (from *Visual Tagging*). It enables the configured COSEC devices to directly send commands to the SATATYA HVR/NVR devices as per the configuration on this page. The Satatya configuration page appears as shown below:

Device Configuration

3 Path-Direct door Path Controller 0/10000 Active

Profile

Enrollment

Advanced

Features

Video Surveillance

Special Functions

Input/Output

Additional

Assign Users

Visual Tagging

Satatya Integration

Integration Type: Network

Active: ☒

Network Connection: Ethernet

IP Address: 192 . 168 . 104 . 30

Port Number: 8000

Name: Path HVR Intergration

Active: ☒

Schedule: 09:00 12:00

Days: ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat ☐ Holiday

Event: Access Allowed

Mode: Both

Action: Recording

Duration Min.: 10

Camera:

<input type="checkbox"/> 1	<input checked="" type="checkbox"/> 2	<input checked="" type="checkbox"/> 3	<input checked="" type="checkbox"/> 4	<input type="checkbox"/> 5
<input type="checkbox"/> 6	<input type="checkbox"/> 7	<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10
<input type="checkbox"/> 11	<input type="checkbox"/> 12	<input type="checkbox"/> 13	<input type="checkbox"/> 14	<input type="checkbox"/> 15
<input type="checkbox"/> 16	<input type="checkbox"/> 17	<input type="checkbox"/> 18	<input type="checkbox"/> 19	<input type="checkbox"/> 20
<input type="checkbox"/> 21	<input type="checkbox"/> 22	<input type="checkbox"/> 23	<input type="checkbox"/> 24	

- **Integration type**- Select the integration type from the options of Wired and Network. In wired integration, door is physically connected with Satatya Device. In Network integration, connection can be by ethernet, wireless or broadband depending upon the COSEC device support.
- **Active**- Check the box to activate the connection.
- **Network Connection**- Select the Network connection from the options of Ethernet, Broadband, Wireless.
- **IP Address**- Specify the IP address of HVR/NVR if device is connected with Ethernet.
- **Port Number**- Specify the port number of HVR/NVR
- **Name**-Specify a user friendly name for the integration function.
- **Active**- Check the Active box to enable the SATATYA integration functionality.
- **Schedule** - Specify a schedule for the function by specifying the start and the end time (*24 Hours format*) as well as checking the boxes against the applicable **days** of the week.
- **Event**- Select a COSEC event from the drop down list for which the resultant action is to be configured.
- **Mode**- Select the event mode from the options of Entry, Exit and Both from the drop down list wherever applicable.
- **Action**-Select the action for the Satatya device from the drop down list. The options available are:
 - Recording - Specify the duration in minutes.
 - Upload Image - This will be uploaded as per the ftp settings.
 - Video Pop-up - Specify the duration in seconds. The video pop up will be generated on the local client of Satatya device on the selected camera.
 - PTZ Preset - Specify the PTZ position number as defined on the SATATYA device.
 - Mail Image - Specify the email-ID.

- **Camera-** Select the relevant camera channels depending on the action selected.

Example1: For action as Video Pop up, the pop up of Camera 24 will be shown for 10 seconds.

Example2: For Access allowed event on COSEC Device, recording of camera channel 4,6,8 and 10 will be done for 10 seconds.

The first screenshot shows the configuration for 'Video Pop-Up' action. The 'Event' is 'Access Allowed', 'Mode' is 'Both', and 'Duration Sec.' is 10. Under 'Camera', camera 24 is selected.

The second screenshot shows the configuration for 'Recording' action. The 'Event' is 'Access Allowed', 'Mode' is 'Both', and 'Duration Min.' is 10. Under 'Camera', cameras 4, 6, 8, and 10 are selected. 'Add' and 'Cancel' buttons are at the bottom.

- Click the **Add** button to finish the process of linking the event to the action. The user may now configure another event-action linkage if required.

Name	Event	Action	Start Time	End Time	Active	
Path HVR Intergration	Access Allowed	Recording	09:00	12:00	Yes	

Special Functions

To configure *Special Functions* for COSEC doors, refer to [“Special Functions”](#).




‘Special Function’ section is available only for PATH V1 variants.

Input/Output

The Input/Output (I/O) configuration of a system determines how the output or response of a system is influenced by the input applied on it. In case of the COSEC Access Control System, the I/O configuration should enable the system to monitor and trigger a specific response to any changes in door state or event occurrences at the door device. This change of door state or occurrence of events may be considered as an input while the response or action that is generated by the system on detection of this input, may be defined as the output.



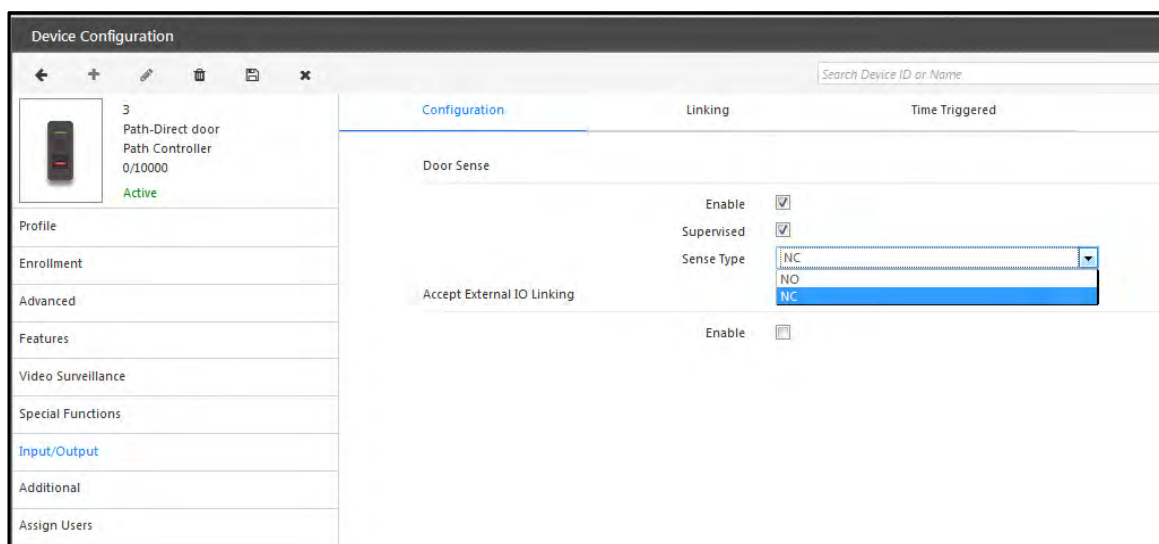
1. This functionality cannot be fully accessed in the Edit  mode for a selected device.
2. This functionality is available only with the Access Control add-on module license.

To access this, After selecting the device, Select **Device Configuration> Input Output**. The Input Output parameters can be set from the following sections:

- “Configuration”
- “Linking”
- “Time Triggered”

Configuration

The **Configuration** section appears as shown below.



The following parameters are available for configuration:

- **Door Sense** - The system by default can sense two states of a door - *Normally Open (NO)* and *Normally Closed (NC)* depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a *Door Abnormal* alarm.

Select the **Enable** checkbox to enable the system for such two-state monitoring.

Select the **Supervised** checkbox to enable the door for four-state monitoring where the door is also monitored for *door fault* and *door disconnection*. Specify the **Sense Type** as **NC** or **NO** (Default: NC).



The following feature is available in direct door only.

- **Accept External IO Linking** - Select the Enable checkbox to enable device-to-device IO Linking i.e. input from one Direct Door can trigger output in another Direct Door.
- **Network Interface**- Select the interface option for IO linking with external devices. The options are

- Ethernet
- Wireless
- Mobile Broadband



The Network Interface feature is available in PATH V2 variants only.



The following features are available in Panel door only.

- **Auxiliary Input** - Select the **Enable** checkbox option for Auxiliary Input (e.g. Smoke Detectors) depending on normal or supervised door state monitoring as described above.

Debounce Time (Sec) - Specify the Debounce time in seconds. Default value is 3 sec and range should be 0-99 sec. It defines the minimum time for which an input interface must be maintained in a given state before the system reports it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.

- **Auxiliary Output** - Select the **Enable** checkbox to enable Auxiliary Output (e.g. Fire Alarm) for the selected device. To set an additional waiting period before the Aux Output signal is sent, enter an **Output Wait Time (Sec)**.

- **Relay Output**

Output Group Number (Door Unlock)- Select the Output Group Number to which the device output for Door Unlock is to be assigned from the picklist.

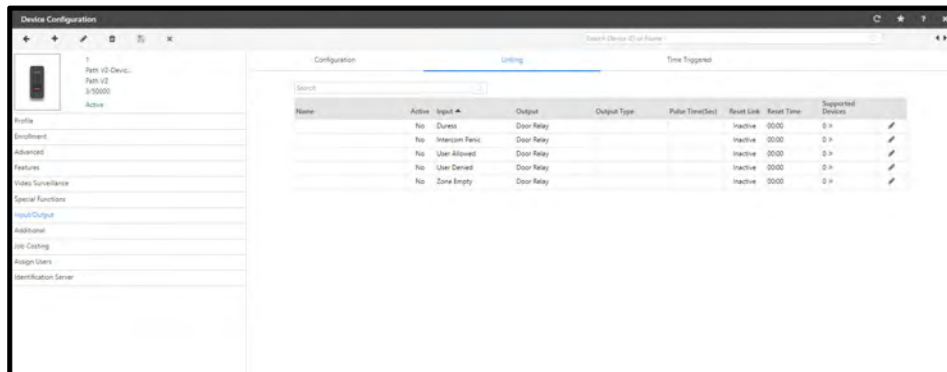
Output Group Number (Door Lock)- Select the Output Group Number to which the device output for Door Lock is to be assigned from the picklist.

Linking



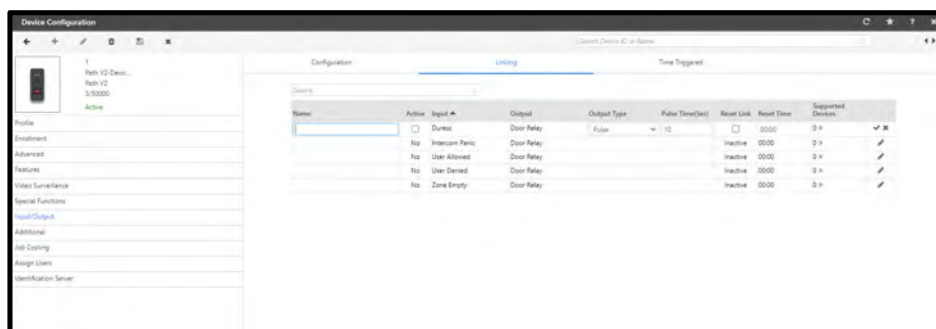
This section is not available for Panel doors.

The **Linking** section appears as shown below.



The COSEC application supports the Input/Output Linking feature to activate an output port based on a trigger received from an input port on the same Direct Door. This option enables the administrator to define how an event or events (input port) will trigger an output on the selected door.

Select a Input-Output linking row or click edit button.



- **Name** - Specify a name for the new I/O linking program to be defined.
- **Active** - Select this checkbox to activate this linking program.
- **Output Type** - Specify the appropriate type of output from the following four options available in the drop down list:
 - **Pulse**: With this type of output, the user needs to define the Pulse time in seconds.
 - **Interlock**: With this option, the output follows the input. The relay output is triggered as long as the input is activated after which it returns to normal state.
 - **Latch**: With this option, it is denoted that the relay output will be in an energized condition for infinite period and needs to be reset manually.
 - **Toggle**: With this option, the output group toggles its state whenever an input group is activated.
- **Pulse Duration (sec)** - For a *Pulse* output type, specify the pulse duration in seconds.

- Click the **OK** button and **Save** the configuration.

Time Triggered

On the **Input Output** page, select the **Time Triggered** section as shown.

The screenshot shows the 'Time Triggered' configuration window. It has three tabs: 'Configuration', 'Linking', and 'Time Triggered'. The 'Time Triggered' tab is active. Below the tabs is a search bar and a table. The table has columns: 'Function Name', 'Active', 'Time', 'Duration(Sec)', 'Days', and 'Output'. The first row shows 'Siren Activate' with 'Active' checked, 'Time' as '00:00', 'Duration(Sec)' as '10', 'Days' as 'Select', and 'Output' as 'Aux O/P'. A dropdown menu is open for the 'Days' column, showing options: 'Check All', 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', and 'Holiday', all with green checkmarks.

This functionality enables the user to control the activity of an Output without manual intervention. The time triggered functions are used for activating events like door unlock and siren activation that are set as per the start time and for the configured time duration. This functionality is designed to energize outputs for predefined periods at the configured time. The COSEC access control system supports up to 20 Time Triggered functions on a Direct Door.

The screenshot shows the 'Time Triggered' configuration window with the 'Time Triggered' tab active. The table now shows the configuration for 'Siren Activate' with 'Active' set to 'Yes', 'Time' as '00:00', 'Duration(Sec)' as '10', 'Days' as 'Su Mo Tu We Th Fr Sa Ph', and 'Output' as 'Aux O/P'. There are edit and delete icons next to the 'Output' column.

Additional

This section lists some additional configurations that can be enabled for door controllers.

To access these configurations, Go to **Device Configuration > Additional > Daylight Saving**



This section is available only for Direct Doors.

Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. COSEC doors can be configured to be compatible with this procedure keeping the RTC of the system updated with such changes.

The **Daylight Saving** configuration can be done in 2 ways i.e. Day-Month wise or Date-Month wise.

- Select the **DST Type** as Day-Month wise or Date-Month wise. The **Disable** option when selected, disables the application of DST on the system time.
- On selection of the **Day-Month wise** option, the DST is set by the day of the month on which clock needs to be forwarded and reverted back to normal. Set the month, week number, day of the week, and time for both the **Forward Clock** and **Backward Clock** as shown.

- On selection of the **Date-Month wise** option, the DST is set by date of the month on which clock needs to be forwarded and reverted back to normal. Define the **Time Period** for the date-month wise DST settings in **24-hours** format, and specify the day of the week, date and time for the **Forward Clock** and the **Backward Clock** as shown.

This DST Setting implies that on 1st sunday of November at 09:00 hours, the clock will be forwarded by 08:00 hours. And on 1st sunday of January at 10:00 hours, the clock will be reversed or backwarded by 08:00 hours.

- Click the **Save** button

Job Costing



Job Costing is applicable for PATH V2 and PATH Controller Direct Door only.

Job Costing enables the admin to assign default jobs on the PATH Controller.

Job Code	Name	Assignment Start	Assignment End
INV	Inventory	01/06/2017	30/06/2017

Show Job Menu: It is disabled for PATH controller.

Default Jobs: Click Add button to add the default job on the door. Then click on the Job picklist button and select the job to be assigned to the device. The Job costing user can directly punch on this door for starting the default job.

Finally click on **Save** button to save the configuration.

When the assignment date of the default job gets elapsed, then the respective job will be listed in **Previous Default Jobs** section.

Assign Users

To the configured device, you can select and assign the users.
Click the picklist button and select the users.

Device Configuration

3 Path-Direct door
Path Controller
0/10000
Active

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Assign Users

Assigned Users

Users ID Name

Search

ID	Name	
11	Vinutha	
12	Anila	
13	Purwang	

Save

Click the **Save** button to assign all the added users to the selected door.

Identification Server

This tab enables the selected device to be assigned to a pre-defined Identification Server.
Device has a limited memory capacity for storage of templates so we need Identification Server which will store the more number of templates and respond to device when asked for identification.

For more information on Identification Servers, See *Admin> System Configuration> Identification Server Configuration*.

To access these configurations, select the **Identification Server** tab.

Device Configuration

Device ID
Device Name
Path V2
0/50000
Active/Inactive

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Settings

Other Biometric Credentials

Enable Identification On Server ☒

Identification Server ID Name

Configure Alternate Server Address ☐

Server Address

Server Port 11005

Enable Finger Smart Identification ☐

Identification Time-Out Duration (Sec) 4

Auto Send Enrolled Templates ☒

Default Biometric Group No. 0

Other Biometric Credentials

- **Enable Identification On Server:** Select the checkbox to enable the identification of palm/finger templates on this device.
- **Identification Server:** Select an Identification Server using the picklist button to which the device is to be assigned. The configuration of server is done from **Admin module > System Configuration > Identification Server Configuration** and the Identification Service must be started from the service tray.
- **Server Address:** It displays the IP Address of the selected Identification Server.

Enable Identification On Server	<input checked="" type="checkbox"/>
Identification Server	<input type="text" value="ID"/> <input type="text" value="Name"/> <input type="button" value="Menu"/>
Configure Alternate Server Address	<input type="checkbox"/>
Server Address	<input type="text"/>
Server Port	<input type="text" value="11005"/>
Enable Finger Smart Identification	<input type="checkbox"/>
Identification Time-Out Duration (Sec)	<input type="text" value="4"/>
Auto Send Enrolled Templates	<input checked="" type="checkbox"/>
Default Biometric Group No.	<input type="text" value="0"/>

- **Configure Alternate Server Address:** Enable this check-box to configure external IP address of Identification Server.
 - **Server Address:** Enter the external network IP address which will be used for accessing identification server.
- **Server Port:** Enter the server port number. The default port number is 11005.
- **Enable Finger Smart Identification:** For all other supported doors, select the checkbox to enable fingerprint templates identification through Identification Server.
- **Identification Time-Out Duration (Sec):** Specify the duration in seconds after which the fingerprint template identification will get time out.
Example: If 5 seconds is specified, then the identification server will try to identify the template till 5 seconds and if not found then it will show time-out to the user.
- **Auto Send Enrolled Templates:** Select the checkbox to enable any enrolled templates to be saved both on the COSEC database as well as saved locally on the configured Identification Server. This enables prompt identification of user on enrollment.
- **Default Biometric Group No.:** Specify the default biometric group number to be assigned to the device. It is a number allotted to a device to be assigned to the Identification Server. This enables the Identification Server to match the template against only those devices that belong to the corresponding biometric group. This reduces the false detection as well time to search template.

Door Controllers

DOOR series controllers are versatile devices designed for reliability, modularity, and performance. These doors come in multiple variants specifically targeted at Time-Attendance and Access Control applications. The **DOOR V3** and **Door V4** can be connected as **Direct Door** as well as **Panel Door**.



The Configuration of Door V1 and Door V2 is similar to Door V3/Door V4. In this manual; configuration of Door V3 is explained for reference.

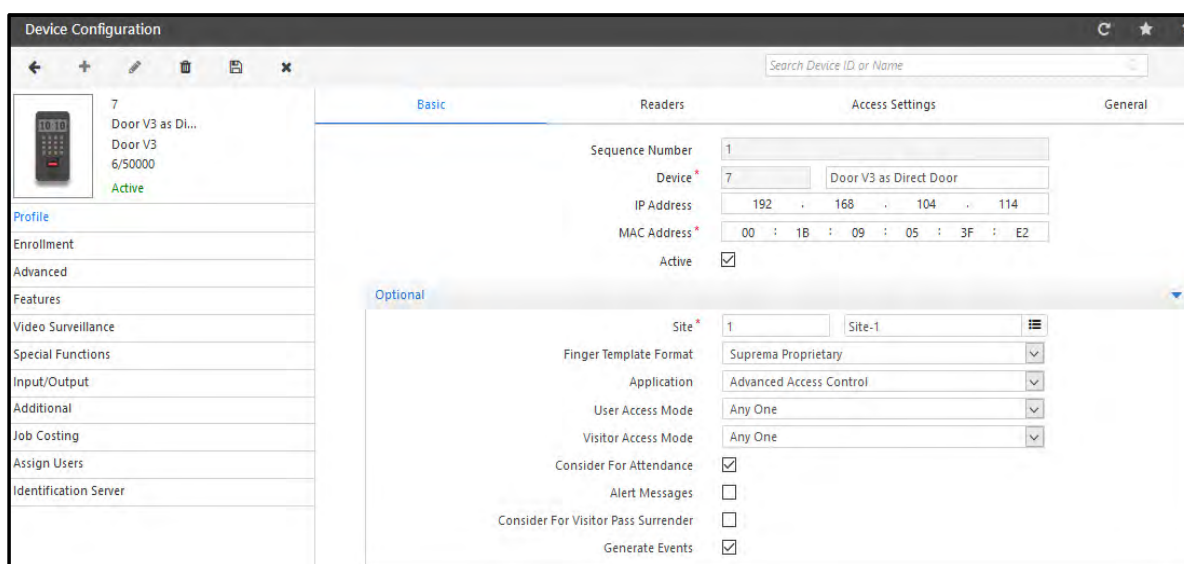


The basic difference between Door V1, Door V2, Door V3 and Door V4 is the support of user capacity and event buffer. Also Door V4 supports Wiegand Out feature.



The Door V3 uses 400 MHz ARM 9 based processors (ATMEL 9G45) while Door V4 uses 800MHz ARM CORTEX A8 based processors(AM3352).

The Device Configuration page for Door V3 appears as shown below.



Enter the MAC address of the door. The IP address will be displayed automatically once the device comes online in Monitor.

To add Devices automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the “Auto Add New Devices” checkbox. Once the device is connected in network, it will come online in COSEC Monitor.



The Monitor Service must be running while adding the device to COSEC.

Once the device is configured, click the **Save** button to save the configuration.

To know more about configuring devices, click on the links for different tabs of Device configuration.

- [“Profile”](#)
- [“Enrollment”](#)
- [“Advanced”](#)
- [“Features”](#)
- [“Video Surveillance”](#)
- [“Special Functions”](#)
- [“Input/Output”](#)
- [“Additional”](#)
- [“Job Costing”](#)
- [“Assign Users”](#)
- [“Cafeteria”](#)
- [“Identification Server”](#)

Profile

This section enables the user to set up the basic profile for any new device. Setting up a door profile involves defining basic parameters to set up any door controller device.

To do this, On the **Device Configuration** page, select the **Profile** tab. The Profile can be configured in the following sections:

- *“Basic”*
- *“Readers”*
- *“Access Settings”*
- *“General”*

Basic

The **Basic** section for “Door V3 as Direct door” is shown below:

The screenshot displays the 'Device Configuration' window with the 'Basic' tab selected. On the left, a sidebar lists various configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main area shows the configuration for device '56', identified as 'M_DOOR V3' with ID '1/50000' and status 'Active'. The 'Basic' tab contains the following fields: 'Sequence Number' (66), 'Device' (56, with a dropdown showing 'M_DOOR V3'), 'IP Address' (empty), 'MAC Address' (87 : 98 : 45 : 11 : 19 : 13), and 'Active' (checked). Below these is an 'Optional' section with a dropdown menu set to '1' (Site-1). This section includes: 'Finger Template Format' (Suprema Proprietary), 'Application' (Advanced Access Control), 'User Access Mode' (Any One), 'Visitor Access Mode' (Any One), 'Alert Messages' (unchecked), 'Consider For Visitor Pass Surrender' (unchecked), 'Consider For Attendance' (checked), and 'Generate Events' (checked).

The **Basic** section for “Door V3 as Panel door” is shown below:

Configure the following options as required:

- **Sequence Number** - This is a system generated sequence number for each new device.
- **Device**- Specify a name that can be assigned to the door. The Door ID is auto-generated by the system.
- **Connection Type** - Applicable only for Panel Doors. Specify the connection type as **Ethernet** or **RS485**.
- **IP Address** - This is the IP address assigned to the door. Once the device connection is established, this field will automatically display the door IP address.
- **MAC Address** - Specify the MAC Address of the door.



MAC address of door is required while manually adding the door to the COSEC Monitor. Note the MAC address from the device when it is powered on.

- **Active** - Check the box to activate the device on the network.



To add the Device automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the “**Auto Add New Devices**” checkbox.

The device will be added automatically but make sure you enable the **Active** checkbox in order to connect the device to the network. Once the device is connected to the network, it will come online in COSEC Monitor.

For Door V3 as Direct Door, the **Option** tab is as shown below:

- **Site** - Select the site to which this door is to be assigned from the site picklist window. Site is created from Devices> Masters> Site.
- **Finger Template Format** - Select the format as Suprema Proprietary or Suprema ISO according to which the templates will be enrolled. For globally setting the template format, you can set from Global policy.
- **Application** - Select the application type for which the device is to be used. The options are **Basic Access Control**, **Advanced Access Control** and **Cafeteria**. All devices set to **Cafeteria** will subsequently be available for Cafeteria configuration.



For Door V2 : The available license is ACS and Application is set to Basic Access Control. If this ACS voucher exhausts, then while dispatching Basic Configuration of device, application type will be sent as 'Advance Access Control'.

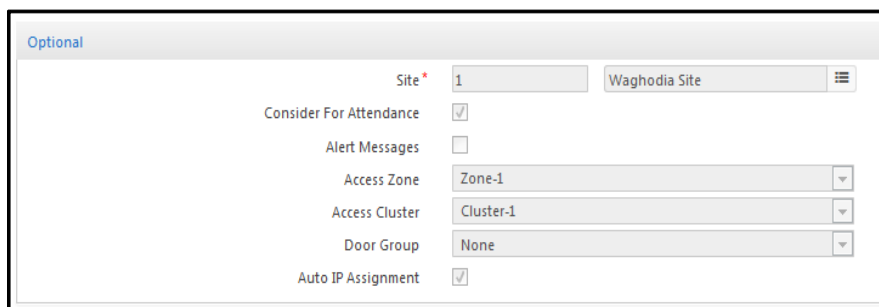
- **User/Visitor Access Mode** - Defines the type and combination of credentials required to identify and validate a user at the Door Controller. Select the appropriate credential combination from the drop down list.

The options available are:

- Any one
- Card
- Card + Biometrics
- Card + Biometrics + PIN
- Card + PIN
- Biometrics
- Biometrics + PIN
- Biometrics then Card
- Card then Biometric
- None
- **Consider for Attendance** - Select this checkbox if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as access control events.
- **Alert Messages** - Select this checkbox to enable the application to send alerts based on events from this door.
- **Consider for Visitor Pass Surrender:** Check the box to consider the selected device for visitor pass surrender. The Visitor can show his credential on this device to surrender the pass.

- **Generate Events:** This check-box is enabled by default. You can disable the check-box if the server is not required to receive any events from the respective devices.

For Door V3 as Panel door, the **Optional** tab shows the following configuration



The 'Optional' configuration tab for Door V3 displays the following settings:

- Site: 1
- Waghodia Site
- Consider For Attendance: ☒
- Alert Messages: ☐
- Access Zone: Zone-1
- Access Cluster: Cluster-1
- Door Group: None
- Auto IP Assignment: ☒

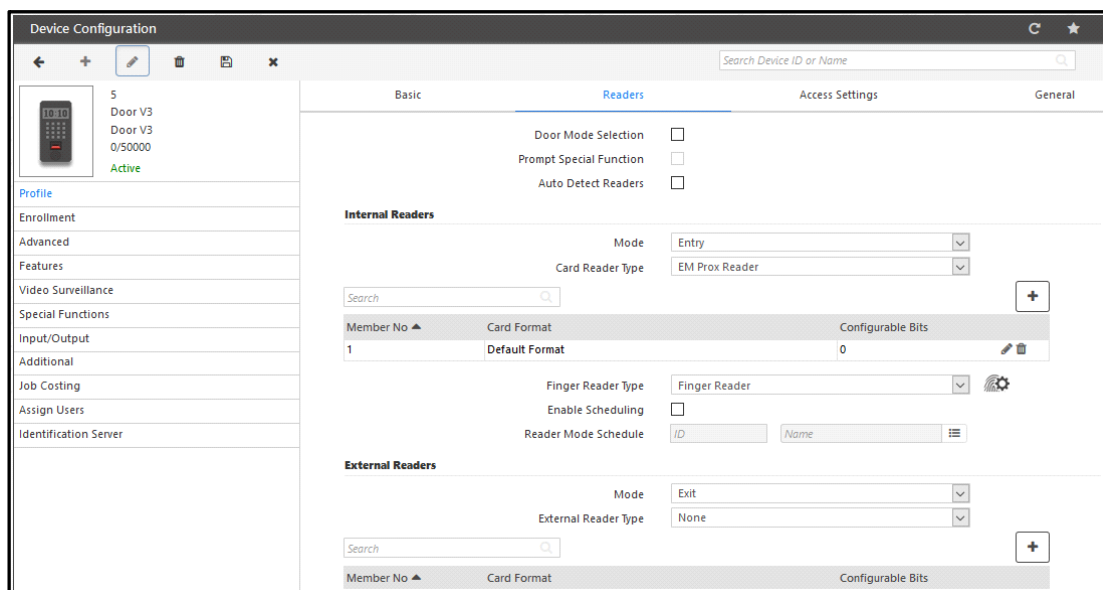
- **Access Zone** (only for panel doors) - Assign an access zone to the door by selecting from the drop down menu.
- **Access Cluster** (only for panel doors) - Assign an access cluster to the door by selecting from the drop down menu.
- **Door Group:** Door Group drop down includes list of all configured Door groups on corresponding panel. An additional option as 'None' is available and selected by default.
- **Auto IP Assignment:** There is option where panel door can be assigned its IP from device webpage. To enable this check the Auto IP Assignment box.



Access Zone is configured while configuring Panel200.

Readers

Readers are important hardware components in a biometric door device. They may be internal or external. This section enables the administrator to configure both internal and external readers for a door as shown.



The 'Device Configuration' window shows the 'Readers' tab for Door V3. The configuration includes:

- Basic Settings:**
 - Door Mode Selection: ☐
 - Prompt Special Function: ☐
 - Auto Detect Readers: ☐
- Internal Readers:**
 - Mode: Entry
 - Card Reader Type: EM Prox Reader
 - Search: [Search bar]
 - Member No: 1
 - Card Format: Default Format
 - Configurable Bits: 0
 - Finger Reader Type: Finger Reader
 - Enable Scheduling: ☐
 - Reader Mode Schedule: ID
- External Readers:**
 - Mode: Exit
 - External Reader Type: None
 - Search: [Search bar]
 - Member No: [Blank]
 - Card Format: [Blank]
 - Configurable Bits: [Blank]

The following parameters are available for configuration:

Door Mode Selection - If this option is enabled, then user will be prompted to select punch type as IN or OUT while punching on the device.

Eg: When a door is in Entry mode, your punches will always be in Entry side. But if you want to mark the punch in ext mode then you can select the door mode if “Door Mode Selection” is enabled.

If not selected, user will need to enable Scheduling to set reader mode of door as entry or exit as per user-defined schedules. For information on creating Reader Mode Schedules, **see Devices > Masters > Reader Mode Scheduler**.

Prompt Special Function- This will provide selection of special function on device screen and based on the selection of particular type of special function, job codes for JPC user will be prompted. This can be enabled only when “Door Mode Selection” is enabled.

Auto Detect Readers (for direct doors only) - Select this checkbox to enable auto detection of Readers on a door controller connected to the server.

Internal Readers

This option allows the configuration of the Internal Reader for the selected door.

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop down list.
- **Card Reader Type;** Select the Card Reader Type from the following options:
 - EM Prox Reader
 - HID Prox Reader
 - MiFare Reader
 - HID iClass-U Reader
 - HID iClass-W Reader
- **Card Format:** The single or multiple card formats can be assigned to the readers of both direct and panel doors. The default card format is assigned to device as shown in the grid. If no other card format is assigned to device; then this default format will be applied.



The formatting of card is described in Devices> Master> Card Format

Multiple Card Format

To assign multiple card formats to device click on **Add** button. Then click the picklist to select the card format. And click **OK** to save the format.

Member No ▲	Card Format	Configurable Bits
1	Default Format	0


Member No ▲	Card Format	Configurable Bits
1	Default Format	0
2	Format1	0

Similarly you can add maximum 5 card formats. When the card format is saved, the Configurable bits of that format as configured from Masters> Card format will be displayed here. Multiple Card format configurations will be dispatched to door separated by 'Format ID' that is 'Member No.' along with all other format related parameters.

Mode: Entry
Card Reader Type: EM Prox Reader

Member No ▲	Card Format	Configurable Bits
1	Default Format	0
2	Format1	26
3	Format2	32

- Select the **Finger Reader Type** as **Finger Reader**.

Click the **FP Reader Configuration**  button to set the **Security Level**, **Lighting Condition**, **Sensitivity**, **Fast Mode**, **Image Quality** and **Restore Defaults** for the selected FP Reader as shown.

Finger Print Module Calibration

Security Level: Normal
Lighting Condition: In Door
Sensitivity: Level 8 (High)
Fast Mode: Auto
Image Quality: Moderate

Restore Defaults

Save Close

Finger Print Module Calibration

- **Security Level:** Security level specifies FAR (False Acceptance Ratio). Since FAR and FRR (False Rejection Ratio) is in inverse proportion to each other, FRR will increase with higher security levels.

For regular Time-Attendance system “**Normal**” level can be selected. For high security areas requiring complete or maximum matching of template, “**Highly Secure**” level must be selected. For approximate matching of template, “**Secure**” level can be selected.

- **Lighting Condition:** Optical sensors are sensitive to lighting condition. With this parameter, users can tune optical sensors to be adapted for their lighting environment. Select the In Door or Out Door option based on the device location.
- **Sensitivity:** Specifies sensor sensitivity to detect a finger. On high sensitivity, the module will accept the finger input more easily. Level 8 has the highest sensitivity.
- **Fast Mode:** Fast Mode parameter can be used to shorten the matching time with a little degradation of authentication performance. In typical cases, Fast Mode 1 is 2 to 3 times faster than Normal mode while Fast Mode 5 is 6 to 7 times faster than Normal mode. There is also an Auto mode.
- **Image Quality:** When a fingerprint is scanned, the module will check if the quality of the image is adequate for further processing. Image quality parameter specifies the strictness of this quality check. Strongest option might lead to higher number of finger rejections during the enrollment process.



Good quality of enrollment(around 70-75% quality) is recommended for proper identification of enrolled templates.

- Click on the **Restore Defaults** button to return the field values for this page to default values if needed.
- Click on the **Save** button.
- **Enable Scheduling:** Select this checkbox to **Enable Scheduling** to set reader mode of door as entry or exit as per user-defined schedules. For information on creating Reader Mode Schedules, **see *Devices > Masters > Reader Mode Scheduler***.

External Readers

This option allows the configuration of the External Reader for the selected door.

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop down list.
- **External Reader Type:** Select the desired type of External Reader from the drop-down list.



Using PIN-W Reader; user can change their PIN number through devices.

- **Card Format** - Select a card format to be applicable for external readers of the device. This is applicable for all direct doors and all Panel doors. For multiple format description [See “Multiple Card Format” on page 768.](#)
- **Exit Switch** - Select this checkbox to enable the use of **Exit Switch**.
- **User/Visitor Access Mode** - Select the access mode from the options shown below:
 - Any One
 - Card
 - Biometrics
 - Card + Biometrics

- Biometrics then Card
- None
- **Access Control On Exit Mode** - Select this check box to enable the checking of the following access control policies on door when the external reader is in the 'exit' mode.
 - User enabled
 - User validity
 - Blocked user
 - Time Based Access Check
 - ASC
 - User Access Group

Access Settings

This section is available for direct doors. The **Access Settings** page appears as shown below:

The screenshot shows the 'Device Configuration' window with the 'Access Settings' tab selected. On the left, a sidebar lists various configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main area displays settings for a device with ID '6', model 'Door V3', and serial '0/50000'. The settings include: Universal Time Zone set to '(GMT+05:30)Chennai, Kolkata, New Delhi, Mumbai'; Time Format set to '12 Hours'; Auto Synchronize with NTP checked; Preferred NTP Server field empty; Working Days checked for Sun, Mon, Tue, Wed, Thu, Fri, Sat, and Holiday; Working Hours (HH:MM) set to '00:00' to '23:59'; and four Holiday Schedules, each with a number (1-4) and a schedule name.

- **Universal Time Zone** - Select the geographic time zone in which the DOOR will operate.
- **Time Format** - Specifies the time format to be displayed on Door Controller LCD display. The formats available are:
 - 24 Hours
 - 12 Hours

Select the relevant option from the drop down list as per the site requirements.

Auto Synchronize with NTP

If Date and time is to be automatically synchronized as per the **Preferred NTP Server** (predefined or user-defined NTP server address) selected by user, then you must enable **Auto Synchronize With NTP** checkbox.

Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from device webpage, which will be reflected on device display.

- When Auto Synchronization with NTP is disabled Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 1. You can specify the Preferred NTP server of your choice. In this case device will first try to get Date and Time from that server address.
If it does not get Date and Time in three tries; device will check from pre-defined NTP servers.
If you have entered one of the three pre-defined NTP servers(ntp1.cs.wisc.edu , time.windows.com , time.nist.gov); then device will first check that server first.
If it receives updated Date and Time then Updated Date and Time will be reflected on device webpage and display screen.
 2. You can keep the Preferred NTP server as blank. In this case device will check for Date and Time from the first NTP server.

3. If user has manually entered Date and Time from webpage or Device Menu then those values of Date and Time will be reflected on device webpage and display screen.

In the case of the **Manual** option the administrator can manually update the time on the Door with that of the system time as and when required. This can be accomplished from the COSEC Monitor and control application.

- **Working Days** - Specify the days on which the default working hours should be applicable. Check the relevant boxes to specify the active days.
- **Working Hours (HH:MM)** - Define the default working hours in HH:MM format.
- **Holiday Schedule** - This section allows the administrator to assign up to four holiday schedules to the device by using the Holiday Schedule picklist.



If the same holiday schedule is configured for a user and for the door controller on which the user is assigned, then the user's attendance marking on this device, on any of the scheduled holidays will always be marked as a holiday.

General

The **General** page appears as follows. Enter all general details applicable to the device in this section.

The screenshot shows the 'Device Configuration' window with the 'General' tab selected. The left sidebar lists various configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main area is divided into sections: 'Basic' (containing 'Mute Buzzer'), 'Readers', 'Access Settings', and 'General'. The 'General' section includes 'Allowed Acknowledgement' and 'Denied Acknowledgement' settings, each with 'Display Duration (ms)' and 'LED - Buzzer Duration' options. Below these are 'Enable Display Messages', 'Custom Birthday Message', and three 'Display Message' entries, each with a 'Schedule' and a 'Message' field. At the bottom, there is a 'Message' field with 'Good Night' and a 'Multi-Language Support' checkbox.

- **Mute Buzzer** - User can mute or unmute the door buzzer by checking or clearing the box respectively.
- **Allowed Acknowledgment**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgment Allowed' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.
- **Denied Acknowledgment**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgment Denied' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.



The below mentioned features are available in direct door only.

- **Enable Display Messages** - This feature allows the user to enable custom birthday message and display messages to be displayed on the door device. Upto 4 display messages can be configured for a door.
- **Custom Birthday Message**- Enter the birthday message which would appear on the door when the user punches on the door on his birth date.
The valid values are

A-Z

a-z

0-9

`~!@#\$%^&*()_+-{}\\|:;?<>.,'\"

- **Display Message** - Enable each display message individually by selecting this checkbox.
- **Schedule** - For each message, the user needs to define the time period between which this message is to be displayed.
- **Message** - Enter the message to be displayed in this field. Maximum 21 characters allowed.
- **Multi-Language Support** - Select this checkbox to enable multi-language support for the selected device.

The **Display From** field shall display the reading order for the selected language.



However Door V3 will support languages with english fonts (A-Z,a-z) only.

Enrollment



The Enrollment section is not available for panel doors.

The Enrollment page appears as shown below.

The screenshot shows the 'Device Configuration' window for a device named '55 Door V3-Devic...'. The 'Enrollment' tab is selected in the left sidebar. The main area displays the following settings:

- Enroll From Device:** ☒ (checked)
- Enrollment Mode:** Biometrics (dropdown)
- Enrollment Using:** User ID (dropdown)
- Template Per Finger:** Single Template/Finger (dropdown)
- Max Number Of Fingers:** Ten (dropdown)
- Number of Fingers:** One (dropdown)
- Number Of Cards:** One (dropdown)
- Enable Self-Enrollment:** ☐ (unchecked)

- **Enroll from Device** - Select this check-box to enable the enrollment of user from the door controller. When this check-box is enabled, 'Enroll User' special function on that device will get active as shown below.

If 'Enroll User' special function & 'Enroll From Device' check-box both are inactive in device configuration, then on activating 'Enroll User' special function, 'Enroll From Device' check-box will be enabled.

The screenshot shows the 'Device Configuration' window for the same device, with the 'Special Functions' tab selected. It displays a table of functions and their status.

No.	Function Name	Active	JOB Selection	User Group	Card-1
1	Official Work - IN	Yes	Yes	All	
2	Official Work - OUT	Yes	Yes	All	
3	Short Leave - IN	Yes	Yes	All	
4	Short Leave - OUT	Yes	Yes	All	
5	Regular - IN	Yes	Yes	All	
6	Regular - OUT	Yes	Yes	All	
7	Break End	Yes	Yes	All	
8	Break Start	Yes	Yes	All	
9	Overtime - IN	Yes	Yes	All	
10	Overtime - OUT	No	No	All	89789797876787897880
11	Enroll User	Yes	No	All	
12	Enroll Special Card	Yes	No	All	

- **Enrollment Mode** - Select the Credential from the drop-down list that can be enrolled using the special function at the DOOR. The options are **ReadOnlyCard**, **SmartCard**, **Biometric** and **BiometricthenCard**, and

DuressFinger. Refer [“Enroll Credentials”](#) or [“Enrolling Users”](#) to enroll User/Worker. Refer [“Enrollment”](#) or [“Enroll Credentials”](#) to enroll Worker. Refer [“Enroll Credentials”](#) to enroll a Visitor.



DuressFinger is only applicable for User and Worker.

- **Enrollment Using** - Select the option **User ID** or **Reference No.** using which enrollment will be done.
- **Template Per Finger** - This parameter displays the values as configured at the global level. This field is not user editable from this page.
- **Max Number of Fingers** - This parameter displays the values of the maximum number of fingers configured at the global level. This field is not user editable from this page.
- **Number of Fingers/Cards** - Select the number of cards or fingerprints to be enrolled based on the credential option selected in the Enrollment Mode parameter.
- **Enable Self-Enrollment** - Select this check-box to enable the self-enrollment feature on this door.

Advanced

The Advanced tab allows the user to configure some advanced parameters such as access control settings, alarms and device timers.

To access this, After selecting the device, Select the **Advanced** tab from **Device Configuration** page. The advanced settings can be configured from following sections:

- [“Settings”](#)
- [“Alarms”](#)
- [“Timers”](#)
- [“Wiegand”](#)

Settings

The **Advanced Settings** page for Door V3 as Direct Door appears on your screen as shown below:

The screenshot displays the 'Advanced Settings' page for a device named 'Door V3 as DI...'. The left sidebar contains a list of settings categories: Profile, Enrollment, Advanced (selected), Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main content area is divided into four tabs: Settings, Alarms, Timers, and Wiegand. The 'Settings' tab is active, showing various configuration options. The 'Temperature Logging' section is expanded, revealing a list of parameters for configuration.

Parameter	Value
Generate Exit Switch Events	<input type="checkbox"/>
Generate Invalid User Events	<input type="checkbox"/>
Generate Sequential IN-OUT Events	<input type="checkbox"/>
Two Credentials Required	<input type="checkbox"/>
Show Pin	<input type="checkbox"/>
Allow Exit When Door Lock	<input type="checkbox"/>
Auto Relock	<input type="checkbox"/>
Auto Relock Timer (Sec)	3
Enable Additional Security	<input type="checkbox"/> Disabled
Enable Smart Identification	<input type="checkbox"/>
Access Level	8
Access Mode	Card
Auto Acknowledge Alarm	<input type="checkbox"/>
Auto Acknowledge Alarm (Sec)	10
Facility Code	1

Temperature Logging	
Enable	<input type="checkbox"/>
Sensor Type	AST
Sensor Interface	USB
Emissivity	0.95
Calibration Parameter	+ 0.0
Approach to Sensor Wait-Timer (Sec)	3.0
Temperature Detection Time Out (Sec)	10
Tolerance between Consecutive Readings	0.5
Consecutive Readings Count within Tolerance	5
Temperature Threshold (°F)	99.5
Minimum Temperature for Access (°F)	95.0
Restriction Type	Soft
Bypass If Sensor Disconnected	<input type="checkbox"/>

The following parameters are available for configuration:

- **Generate Exit Switch Events** - Select this check-box to enable the door to generate events every time the exit switch is used.
- **Generate Invalid User Events** - Select this check-box to enable the door to generate events for invalid user inputs.
- **Generate Sequential IN-OUT Events** - Select this check-box to generate user punches on device as the sequential IN-OUT events irrespective of whichever mode in which device is functioning.
- **Two Credentials Required**- Select this check-box to enable the feature of verifying 2 credentials mandatorily for users allowed to By-pass finger/palm.
- **Show Pin**- Select this check-box to display the characters of PIN when the PIN is entered on device.
- **Allow Exit when Door Lock** - Select this check-box if users are to be allowed to exit even when the Door relay is in locked condition.

- **Auto Relock** - Select this checkbox to allow the door to relock immediately when the door status changes to close after normal open irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Relock Timer** - Specify the time in seconds for the Auto Relock operation.
- **Enable Additional Security** (for direct door) - Select this checkbox to enable additional security at the selected Door Controller.
- **Additional Security Code** - Enter a code (ranging from 1 to 65535) in the field provided. Re-enter the code to confirm.



Changing this value can affect the SI function. Click on the **Default Code** button to reset the **Additional Security Code** to the value set in the **Global Additional Security Code** field on the Global System Policy page.

- **Enable Smart Identification** - Select this checkbox to enable this functionality at the selected Door Controller and select the **Access Level** and the **Access Mode** from the drop down list.
- **Auto Acknowledge Alarm** - Select this check-box to enable the auto-acknowledgment of all alarms for this device.
- **Auto Acknowledge Alarm (sec)** - Set the time in seconds for the Auto Acknowledge Timer. The wait timer will start and on expiry of the timer, the alarm buzzer will stop automatically.
- **Facility Code** - Set a value for Facility Code to be set for access modes other than “Card”, if Facility Code is expected in Wiegand Output. This will be applicable to all direct doors except Door V1 and V2.
- **Allow Access Through Mobile**- Check the box to allow the access to device using COSEC ACS App.
- **Mobile Entry/Exit Access Mode**- Select the entry and exit door access mode from the options of **Mobile Only**, **Mobile then Biometrics** and **Mobile then Card**.



If User Access Mode is selected as “None” in Zone Configuration and Mobile Access Mode is selected as “Mobile Then Biometrics” then door can be accessed through Mobile and then Biometric credential.

Temperature Logging

- **Enable:** Enable the temperature logging feature on the zone.
- **Sensor Type:** Select the type of thermal sensor integrated in the device. There are three sensors: *AST*, *Web-Based* and *FEVOBOT*. Default sensor set is *FEVOBOT*.
- **Sensor Interface:** Select the interface on which device will communicate with the sensor.
For Sensor Type-AST
Sensor Interface options will be: RS-232 and USB
For Sensor Type- Web-based
Sensor Interface options will be: HTTP/S
For Sensor Type-FEVOBOT
Sensor Interface options will be: USB

- **Emissivity:** Set the emissivity parameter for Sensor. This parameter should only be visible when Sensor Type is AST. Default value is 0.95.
It is used to define accuracy in sensor to detect temperature of different skin or objects.
Not applicable for FEVOBOT.
- **Calibration Parameter:** Set the calibration parameter for the thermal sensor.
On click of + the value should increase by 0.1 and on click of – it should decrease by 0.1.
Not applicable for FEVOBOT.
- **Approach to Sensor Wait-Timer:** Time for which the device will wait for user to approach the device before starting Temperature Detection.
- **Temperature Detection Time-Out:** The timer till which temperature detection will be done for the user and if valid temperatures are not found till the expiry of timer then timeout will be declared.
- **Tolerance between consecutive readings:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature doesn't fall in tolerance range the reference temperature is updated with the current temperature and the process continues.
Not applicable for FEVOBOT.
- **Consecutive readings count within tolerance:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature doesn't fall in tolerance range the reference temperature is updated with the current temperature and the process continues.
Not applicable for FEVOBOT.
- **Minimum Temperature for Access:** The minimum temperature value that should be detected is to be considered as valid temperature.
It should be less than threshold temperature. If user tries to enter a value equal to or greater than threshold temperature validation should be shown.
The default value, unit and range should be updated based on the Temperature unit set on Panel.
- **Temperature Threshold:** To set the threshold value of the temperature. The default value, unit and range can be updated based on the Temperature unit set on Panel.
- **Restriction Type:** To set restriction type as soft/hard.
- **Bypass if Sensor Disconnected:** Enable this check-box to give provision of bypassing the feature if sensor connectivity is lost.

The **Advanced Settings** for **Door V3** as **Panel Door** is shown below:

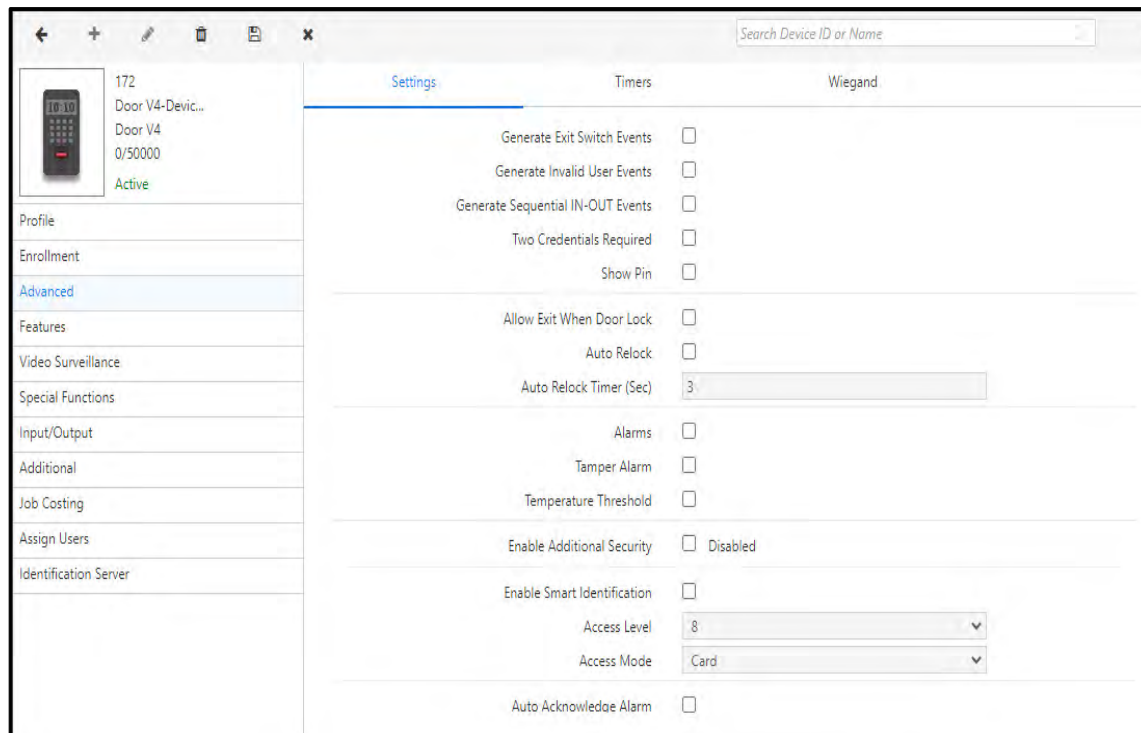
- **Auto Relock** - Select this checkbox to allow the door to relock immediately when the door status changes to close after normal open irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Relock Timer** - Specify the time in seconds for the Auto Relock operation.
- **Tail-Gating** - Tail-gating refers to an access violation which occurs when more than one person tries to enter a secured area using a single person's access credentials. If this option is enabled on the panel door, the occupancy count of a zone should be incremented or decremented considering both the punch as well as the auxiliary input port of the panel door (say, input from a beam-counter). Set the wait timer for resetting the tailgating count (**Reset Wait Timer**) based on the door lock status or the door pulse wait timer (as configured).
- **Man Trap Entry Timer(Sec)** - This checkbox enables an alarm wait timer on the panel door to ensure that the user enters the next sequential door of a man-trap within a specific time-frame.
- **Man Trap Exit Timer(Sec)** - This checkbox enables an alarm wait timer on the panel door to ensure that the user exits the panel door to enter the next sequential door of a man-trap within a specific time-frame.
- **Enable Man Trap Door Interlocking:** Select this check-box to activate the Door Interlock for the selected door (say Door1). This means if the Door1 is open then other doors will remain close.
- **Door:** Click the picklist and select the doors to be assigned for the Interlock to the selected door (Door1). Suppose Door2 and Door3 are selected for Interlock with Door1. So When Door1 opens; Door2 and Door3 will remain close.



For Degraded mode Door Interlocking feature will not work.

Whenever a door is in abnormal state and for that door interlocking is enabled then user access in other doors of the interlocking group is allowed.

The **Advanced** Setting page for **Door V4** as **Direct Door** appears on screen as shown below:



172 Door V4-Devic...
Door V4
0/50000
Active

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Settings Timers Wiegand

Generate Exit Switch Events ☐
Generate Invalid User Events ☐
Generate Sequential IN-OUT Events ☐
Two Credentials Required ☐
Show Pin ☐

Allow Exit When Door Lock ☐
Auto Relock ☐
Auto Relock Timer (Sec) 3

Alarms ☐
Tamper Alarm ☐
Temperature Threshold ☐

Enable Additional Security ☐ Disabled

Enable Smart Identification ☐
Access Level 8
Access Mode Card

Auto Acknowledge Alarm ☐

Auto Acknowledge Alarm (Sec) 10

Facility Code 1

Allow Access Through Mobile ☐
Mobile Entry Access Mode Mobile Only
Mobile Exit Access Mode Mobile Only

Advertise Bluetooth ☐
Bluetooth Name MATRIX
Bluetooth Range Medium (5m - 7m)

Temperature Logging

Enable ☐
Sensor Type AST
Sensor Interface USB
Emissivity 0.95
Calibration Parameter + 0.0
Approach to Sensor Wait-Time (Sec) 3.0
Temperature Detection Time Out (Sec) 10
Tolerance between Consecutive Readings 0.5
Consecutive Readings Count within Tolerance 5
Temperature Threshold (°F) 99.5
Minimum Temperature for Access (°F) 95.0
Restriction Type Soft
Bypass if Sensor Disconnected ☐

In addition to the features same as Door V3, there are 3 more features. They are:

- **Mobile Entry/Exit Access Mode-** Select the entry and exit door access mode from the options of **Mobile Only**, **Mobile then Biometrics**, **Mobile then Card** and **Mobile then PIN**.
- **Advertise Bluetooth-** Check the box to enable Bluetooth of the device by which the device will be visible to others.
- **Bluetooth Name-** When “Advertise Bluetooth” checkbox is enabled, you can enter the bluetooth name. The default name is Matrix.
- **Bluetooth Range-** You can select the bluetooth range as Short, Medium or Long based on which user can mark the attendance. Suppose if you select “Short” range; then user can mark the punch via bluetooth from near by office premises only.
 - Short(1m-2m)
 - Medium(5m-7m)
 - Long (>8m)

By default, the range will be set to “Medium”. If you want to allow punch marking from long distance, then you can select “Long” range.

Temperature Logging

- **Enable:** Enable the temperature logging feature on the zone.
- **Sensor Type:** Select the type of thermal sensor integrated in the device. There are three sensors: *AST*, *Web-Based* and *FEVOBOT*. Default sensor set is *FEVOBOT*.
- **Sensor Interface:** Select the interface on which device will communicate with the sensor.
For Sensor Type-AST
Sensor Interface options will be: RS-232 and USB
For Sensor Type- Web-based
Sensor Interface options will be: HTTP/S
For Sensor Type-FEVOBOT
Sensor Interface options will be: USB
- **Emissivity:** Set the emissivity parameter for Sensor. This parameter should only be visible when Sensor Type is AST. Default value is 0.95.
It is used to define accuracy in sensor to detect temperature of different skin or objects.
Not applicable for FEVOBOT.
- **Calibration Parameter:** Set the calibration parameter for the thermal sensor.
On click of + the value should increase by 0.1 and on click of – it should decrease by 0.1.
Not applicable for FEVOBOT.
- **Approach to Sensor Wait-Timer:** Time for which the device will wait for user to approach the device before starting Temperature Detection.
- **Temperature Detection Time-Out:** The timer till which temperature detection will be done for the user and if valid temperatures are not found till the expiry of timer then timeout will be declared.
- **Tolerance between consecutive readings:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature

doesn't fall in tolerance range the reference temperature is updated with the current temperature and the process continues.

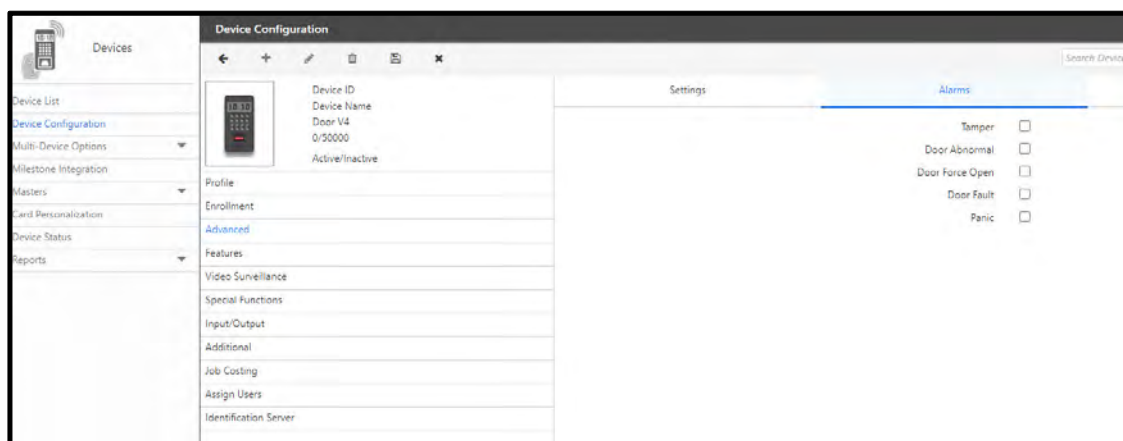
Not applicable for FEVOBOT.

- **Consecutive readings count within tolerance:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature doesn't fall in tolerance range the reference temperature is updated with the current temperature and the process continues.
Not applicable for FEVOBOT.
- **Minimum Temperature for Access:** The minimum temperature value that should be detected is to be considered as valid temperature.
It should be less than threshold temperature. If user tries to enter a value equal to or greater than threshold temperature validation should be shown.
The default value, unit and range should be updated based on the Temperature unit set on Panel.
- **Temperature Threshold:** To set the threshold value of the temperature. The default value, unit and range can be updated based on the Temperature unit set on Panel.
- **Restriction Type:** To set restriction type as soft/hard.
- **Bypass if Sensor Disconnected:** Enable this check-box to give provision of bypassing the feature if sensor connectivity is lost.

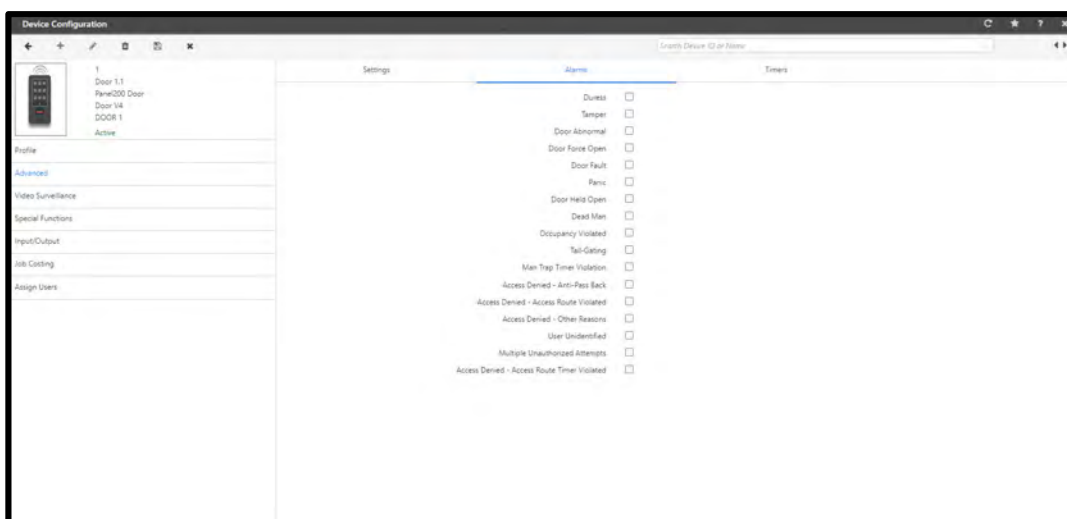
Alarms

In Alarm tab, you can assign below list of alarms to the door.

For Direct Door



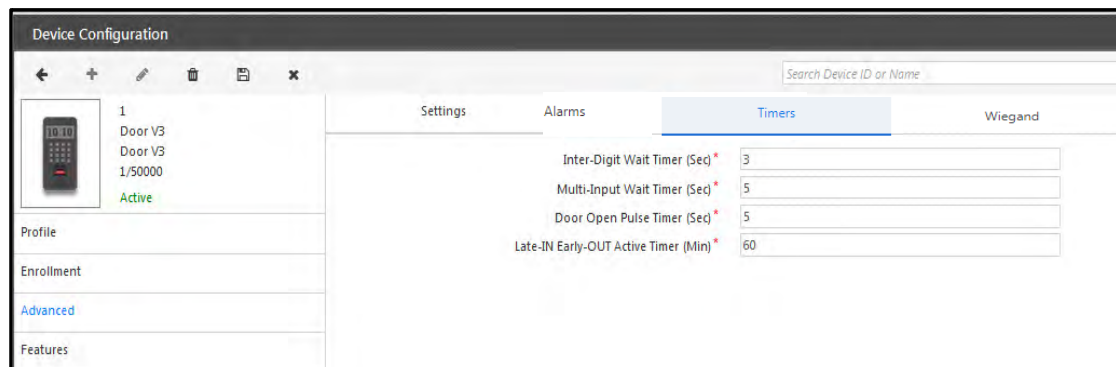
For Panel Door



Select the respective check-box of alarms which you want to enable.

Timers

This section allows the configuration of various types of pre-defined device timers which can trigger off specific responses. In COSEC, timers are often used to control door behaviour and for triggering alarms. The **Timers** page appears on your screen as shown below:



- **Inter-Digit Wait Timer (sec)** - Specify the time period in seconds between two key inputs on the device keypad. On expiry of this timer, the system considers the user input to be complete and is ready for the next input.
- **Multi-Input Wait Timer (sec)** - Specify the time in seconds for which system needs to wait for the second credential input from the user when more than one credential is to be used to grant access.



We recommend you to set the timer value as greater than or equal to 10 seconds to avoid access denial issues to users. This is applicable when the system reads the credentials (biometric) from the user's Smart Cards.

- **Door Open Pulse Timer (sec)** - Specify the time in seconds (3 to 99) for the door to be energized for a valid credential. If the opened door does not return to a closed state before the expiry of this timer, the door will generate a "Door Abnormal" alarm.
- **Late-IN Early-OUT Active Timer (min)** - Specify the time in minutes for which the Late-IN and Early-OUT special functions will remain active after being enabled at the Door Controller.



The above features are available only for direct doors.

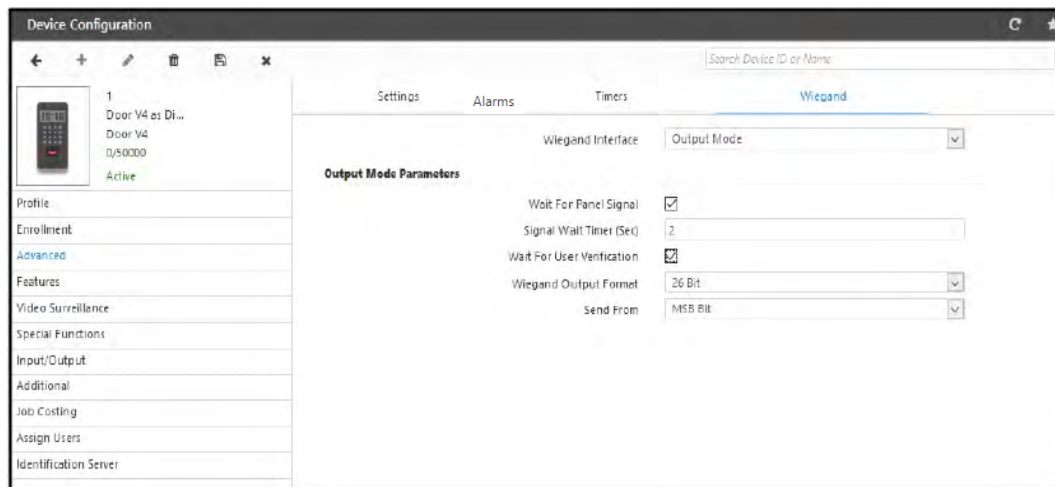
- **Pulse Time (sec)** - Specify the time in seconds for the panel door to be energized for a valid credential.



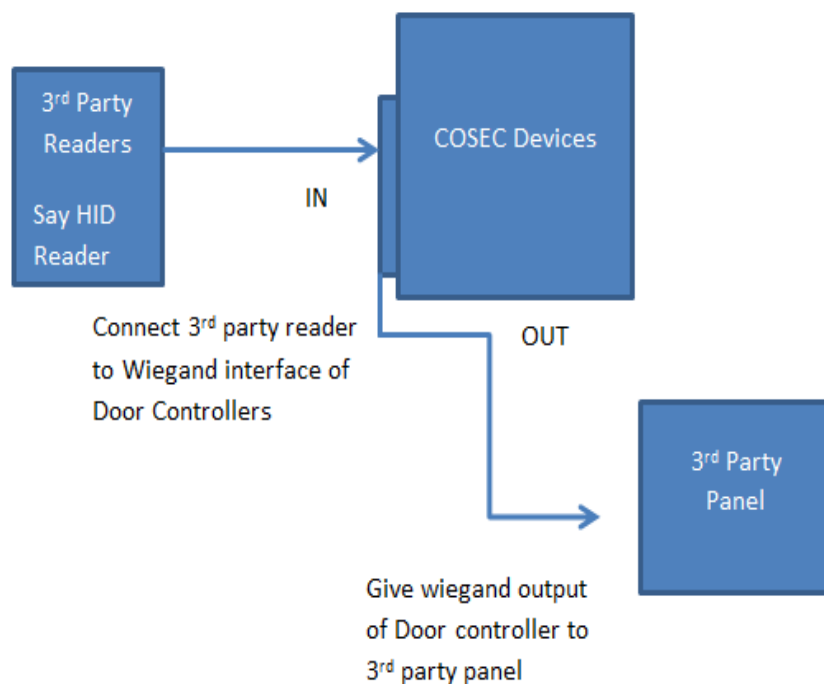
This feature is available only for panel doors.

Wiegand

Wiegand Interface is available in Door V4 only.



- **Wiegand Interface** - The COSEC device can be connected both as input devices (e.g. to receive data from a Wiegand Reader) or output devices (e.g. to support output to third party panel) via the Wiegand interface as shown below.

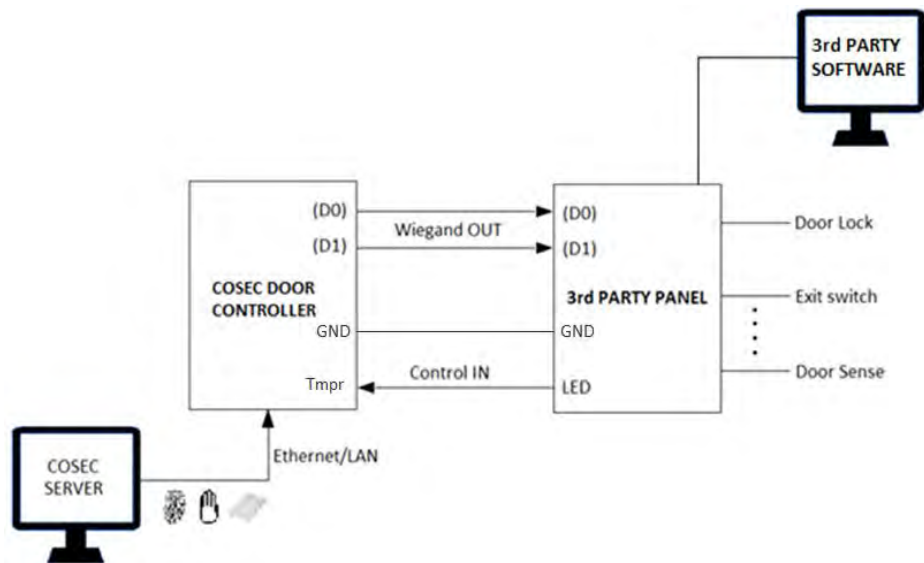


So select the interface of Door controller as **Output Mode** to work as Wiegand output to panel or **Reader Input** to take data from third party reader. If Reader Input option is selected, all the output mode parameters will be disabled.

If you select Output mode then configure the **Output Mode Parameters**.

- **Wait For Panel Signal** - If this option is enabled the door will wait for reply from the connected third party device before triggering any output, as per the defined Signal Wait Timer (Sec).
- **Wait For User Verification** - If this option is enabled, user verification will be requested on the third party device before triggering any output.
- Specify the **Wiegand Output Format** and sending order for reader data as MSB or LSB Bit in the **Send From** field.

Wiegand Out Interface



Also for the **Custom** format, user can configure details of fields to be sent as output from the Wiegand reader that has been added.

Door Access using QR code

The user can access the COSEC device using COSEC APTA installed in the mobile device. If the user has rights for COSEC APTA and the access to the device is allowed for the user, then he can use his mobile device to scan the QR code which constitute the details of the COSEC door.

There is icon for QR code on COSEC APTA application. Clicking that icon will open the camera in your mobile. Now you can show the mobile camera to scan the QR code. The COSEC door will get opened after verifying the security key and access policies of the user.

Steps to create a QR code

Step 1: Enter details in JSON format

```
{"version":"x","ip":"x.x.x.x","port":"x","pdid":"x","mode":"x"}
```

Valid values:

Field	Field range	Default Value	Remark
version	1-255	1	

Field	Field range	Default Value	Remark
ip	0.0.0.0-255.255.255.255	0.0.0.0	
port	0-65535	0	
pdid	0-255	0	If door is in direct door mode then, then PDID will be 0 If door is in panel door mode then, PDID will have values from 1-255
mode	0,1	0	0= for entry mode 1=for exit mode



Note:

Step1a. If door is in direct door mode enter IP & port of the direct door

b. If door is a panel door, then enter IP & port of the panel door and in the pdid specify the door id which is to be accessed.

Step 2: Encrypt the JSON string using key "matrix12" with simple DES/ECB mode.

Step 3: Encode the encrypted string using Base 64.

Step 4: Use this string to generate QR code through any third party software.

Features

The Features tab allows the user to enable certain Access Control features for a device



The Features tab is available only with the Access Control Module license and is applicable only for direct doors.

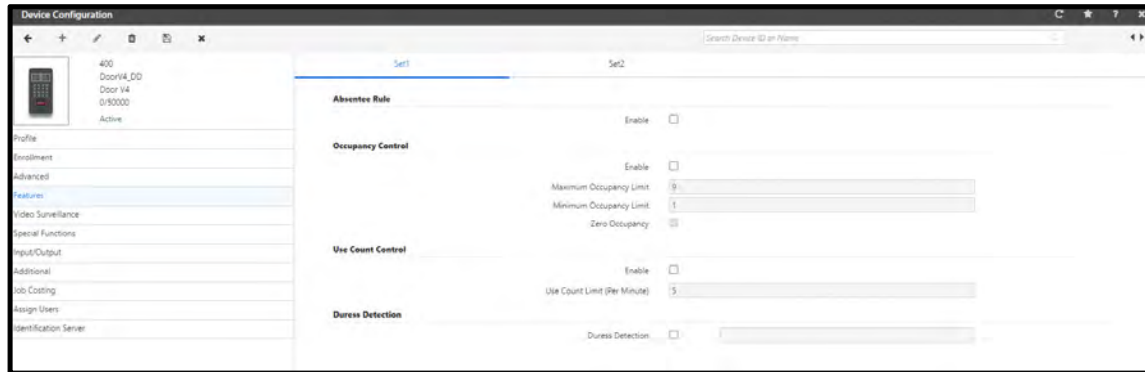
To access this, After selecting the device, Select **Device Configuration> Features**. The access control features for the device can be set from the following two sections:

- "Set1"
- "Set2"

Set1

This page allows the configuration of three rules - **Absentee Rule**, **Occupancy Control** and **Use Count Control**.

The page appears as shown below.



- **Absentee Rule** - Select this checkbox to enable this feature at the door. This rule sets the maximum number of days for non-use of a credential. On expiration of days limit, the user will be automatically blocked.
For configuring the rule See *Access Control > Absentee Rule*.
- **Occupancy Control** - Select this checkbox to enable the feature at the door and specify maximum number of users to be allowed within the controlled area after which a user exit is required to enable access to another user. Also specify the **Minimum Occupancy Limit** i.e. the minimum number of occupants the designated zone should have, and enable/disable the **Zero Occupancy** option to determine whether the designated zone should be allowed to be empty or not.
For configuring the rule See *Access Control > Occupancy Control*.
- **Use Count Control** - Select this checkbox to enable the feature at the door and specify the maximum number of uses per minute.
For configuring the rule See *Access Control > Use Count Control*.
- **Duress Detection** - Select this checkbox to enable the feature. The default duress detection code is displayed which is used to generate the duress alarm which informs that the user is forced to open the door under threat.



Duress Detection (PIN+ Finger) is supported only in Door V4.

Duress Detection (PIN only) is supported only in Door V3.

Duress Detection is not supported in Door V1 and Door V2.

Set2

This page allows the configuration of three rules - **First-IN User Rule**, **Anti-Pass-Back (APB)** and **2-Person Rule**. The page appears as shown below.

- **First-IN User Rule** - Select this checkbox to enable the feature at the direct door and select the First-In User group which would be valid at the door.
For configuring the rule See *Access Control> First- In User Rule> Assignment*
- **Anti-Pass Back (APB)** - Select this checkbox to enable the feature at the direct door.
 - **On Entry:** Check this box so that the system monitors the entry reader for APB violation.
 - **On Exit:** Check this box also so that the system monitors the entry as well as the exit readers for APB violations.
 - **Hard/Soft:** Select the restriction type as Hard or Soft option from the drop down options.
 - **Hard APB:** The access will be denied if the exit is not registered first. It does not allow a second entry using the same card without an exit.
 - **Soft APB:** The access will be granted even if the exit is not registered. It allows a second entry of the same user without an exit; however, an event and a warning are generated that indicates the second entry.

Forgiveness: Check this box to enable the system to reset the APB status. When forgiveness is enabled, then there will be following options to reset the pass.

1. **Reset After Day Change:** This will reset the APB status of all the users to NULL at midnight. This enables a user, who left the building in the evening without exit punch, to use his card for entry in the next morning.
2. **Reset After Timer Expiry:** This will reset the APB status of all the users after the expiry of user defined time.

Forgiveness Timer (Mins): Enter the time duration in minutes after which Anti-pass back status will get reset and the pass will be in original state.

- **2-Person Rule** - Select this checkbox to enable the feature at the door and set the **wait time** in seconds after which the second person is allowed to punch on the door.
For configuring the rule See *Access Control> 2- Person Rule*

Video Surveillance

The Video Surveillance tab allows the user to configure parameters for video surveillance integration with the COSEC device.

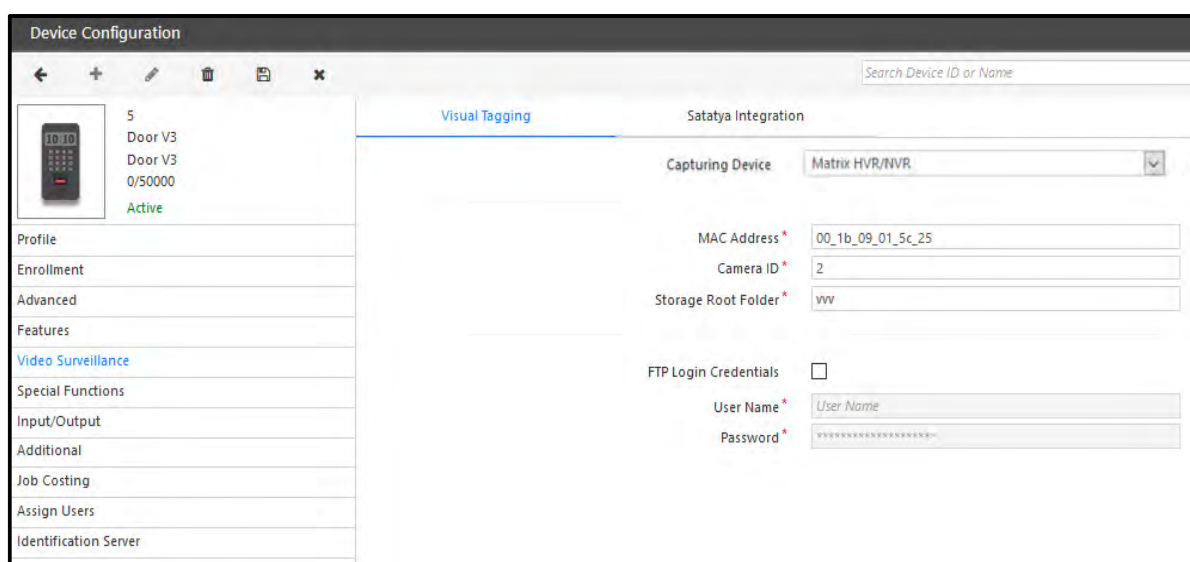
It is available in Basic License.

To access this, Go to **Device Configuration > Video Surveillance**.

- “Visual Tagging”
- “Satatya”

Visual Tagging

The COSEC application can interface with some supported hybrid and network video recording systems and grab images triggered by user events at the Doors. The **Visual Tagging** option enables the administrator to define the video recorder parameters. The **Visual Tagging** page appears as shown below.



The screenshot displays the 'Device Configuration' window. On the left, a sidebar shows a device icon and a list of configuration tabs: Profile, Enrollment, Advanced, Features, Video Surveillance (highlighted), Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main area is split into two panels. The left panel, titled 'Visual Tagging', is currently active. The right panel, titled 'Satatya Integration', contains the following fields: 'Capturing Device' (a dropdown menu showing 'Matrix HVR/NVR'), 'MAC Address' (a text field with '00_1b_09_01_5c_25'), 'Camera ID' (a text field with '2'), 'Storage Root Folder' (a text field with 'vv'), and 'FTP Login Credentials' (a checkbox). Below the checkbox are 'User Name' and 'Password' text fields.



To view the user events and related images, go to **Admin > Views/Logs > Event View**. To know more about viewing events, refer to “Event View”.

The following parameters are available for configuration:

- **Capturing Device** - Select the video recording device type from the dropdown menu as shown. The compatible device types are:
 - Matrix HVR/NVR
 - Milestone

Matrix HVR/NVR

- **MAC Address** - In the event of selecting the Matrix HVR/NVR, the administrator needs to specify the MAC address of the video recorder device using “_” (underscore) as the separator.
- **Camera ID** - Specify the camera number or camera ID for IP cameras. For analog cameras specify the camera number.

- **Storage Root Folder** - Specify the Root folder path or FTP Path where the uploaded images will be saved.
- **FTP Login Credentials** - Check this box to activate FTP login credentials for authentication.
- **User name** - Specify the FTP server user name.
- **Password** -Specify the FTP server password.



Some COSEC devices do not support all the network connection options.

Milestone

The screenshot shows the 'Device Configuration' window with the 'Visual Tagging' tab selected. On the left, a device list shows '1 Door V3-Devic...' with status 'Active'. The main area is titled 'Satatya Integration' and has 'Capturing Device' set to 'Milestone'. Below this is a search bar and a table with columns: Event ID, Name, User-Defined Event ID, and User-Defined Event Name. The table is currently empty with a 'No Data' message. Below the table is a 'Camera' section with input fields for 'ID' and 'Name'. At the bottom, there is a table with columns: Camera Name, GUID, Host Name, and Port. The table contains one entry: 'MATRIX COMSEC CIDR20VL12CW-P (192.168.112.193) - Camera 1' with GUID 'ac6c0e92-9acd-410d-b21f-f593c2b9d33f', Host Name 'ketanpipaliya', and Port '7563'.

Event ID	Name	User-Defined Event ID	User-Defined Event Name
No Data			

Camera Name	GUID	Host Name	Port
MATRIX COMSEC CIDR20VL12CW-P (192.168.112.193) - Camera 1	ac6c0e92-9acd-410d-b21f-f593c2b9d33f	ketanpipaliya	7563



*For more information on integration with **Milestone** devices, refer to "[Milestone Integration](#)".*

Satatya

This functionality is available for configuration only when the Matrix HVR/NVR device type is selected as the **Capturing Device** (from *Visual Tagging*). It enables the configured COSEC devices to directly send commands to the SATATYA HVR/NVR devices as per the configuration on this page. The Satatya configuration page appears as shown below:

- **Integration type**- Select the integration type from the options of Wired and Network.
In wired integration, door is physically connected with Satatya Device. In Network integration, connection can be by Ethernet, wireless or broadband depending upon the COSEC device support.
- **Active**- Check the box to activate the connection.
- **IP Address**- Specify the IP address of HVR/NVR.
- **Port Number**- Specify the port number of HVR/NVR
- **Name**-Specify a user friendly name for the integration function.
- **Active**- Check the Active box to enable the SATATYA integration functionality.
- **Schedule** - Specify a schedule for the function by specifying the start and the end time (*24 Hours format*) as well as checking the boxes against the applicable **days** of the week.
- **Event**- Select a COSEC event from the drop down list for which the resultant action is to be configured.
- **Mode**- Select the event mode from the options of Entry, Exit and Both from the drop down list wherever applicable.
- **Action**-Select the action for the Satatya device from the drop down list. The options available are:
 - Recording - Specify the duration in minutes.
 - Upload Image - This will be uploaded as per the ftp settings.

- Video Pop-up - Specify the duration in seconds. The video pop up will be generated on the local client of Satatya device on the selected camera.
 - PTZ Preset - Specify the PTZ position number as defined on the SATATYA device.
 - Mail Image - Specify the email-ID.
- **Camera-** Select the relevant camera channels depending on the action selected.

Example1: For action as Video Pop up, the pop up of Camera 24 will be shown for 10 seconds as configured below.

Example2: For Access allowed event on COSEC Device, recording of camera channel 4,6,8 and 10 will be done for 10 seconds.

The first screenshot shows the configuration for a 'Video Pop-Up' action. The 'Event' is 'Access Allowed', 'Mode' is 'Both', and 'Duration Sec.' is 10. Under 'Camera', camera 24 is selected.

The second screenshot shows the configuration for a 'Recording' action. The 'Event' is 'Access Allowed', 'Mode' is 'Both', and 'Duration Min.' is 10. Under 'Camera', cameras 4, 6, 8, and 10 are selected. 'Add' and 'Cancel' buttons are at the bottom.

- Click the **Add** button to finish the process of linking the event to the action. The user may now configure another event-action linkage if required.

Search						
Name	Event	Action	Start Time	End Time	Active	
NR16S integration	Access Allowed	Video Pop-Up	00:00	23:59	Yes	


Special Functions

To configure *Special Functions* for COSEC doors, refer to [“Special Functions”](#).

Input/Output

The Input/Output (I/O) configuration of a system determines how the output or response of a system is influenced by the input applied on it. In case of the COSEC Access Control System, the I/O configuration should enable the system to monitor and trigger a specific response to any changes in door state or event occurrences at the door device. This change of door state or occurrence of events may be considered as an input while the response or action that is generated by the system on detection of this input, may be defined as the output.



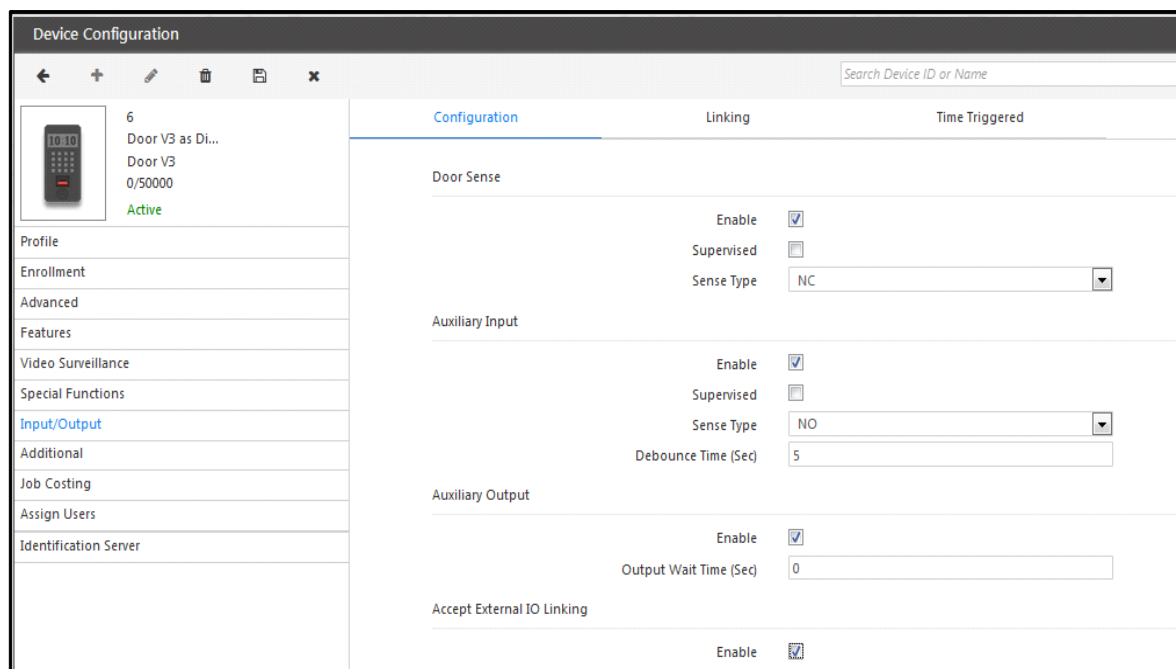
1. This functionality cannot be fully accessed in the Edit  mode for a selected device.
2. This functionality is available only with the Access Control add-on module license.

To access this, After selecting the device, Select **Device Configuration> Input Output**. The Input Output parameters can be set from the following sections:

- “Configuration”
- “Linking”
- “Time Triggered”

Configuration

The **Configuration** section for a Direct Door V3 appears as shown below.



The following parameters are available for configuration in both Direct door and Panel door:

- **Door Sense** - The system by default can sense two states of a door - *Normally Open (NO)* and *Normally Closed (NC)* depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a *Door Abnormal* alarm.

Select the **Enable** checkbox to enable the system for such two-state monitoring.

Select the **Supervised** checkbox to enable the door for four-state monitoring where the door is also monitored for *door fault* and *door disconnection*. Specify the **Sense Type** as **NC** or **NO** (Default: NC).

- **Auxiliary Input** - Select the **Enable** checkbox option for Auxiliary Input (e.g. Smoke Detectors) depending on normal or supervised door state monitoring as described above.

Debounce Time (Sec) - Specify the Debounce time in seconds. Default value is 3 sec and range should be 0-99 sec. It defines the minimum time for which an input interface must be maintained in a given state before the system reports it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.

- **Auxiliary Output** - Select the **Enable** checkbox to enable Auxiliary Output (e.g. Fire Alarm) for the selected device. To set an additional waiting period before the Aux Output signal is sent, enter an **Output Wait Time (Sec)**.

- **Relay Output**

Output Group Number (Door Unlock)- Select the Output Group Number to which the device output for Door Unlock is to be assigned from the picklist.

Output Group Number (Door Lock)- Select the Output Group Number to which the device output for Door Lock is to be assigned from the picklist.



The above feature is available in panel door only.



The following feature is available in direct door only.

- **Accept External IO Linking** - Select the Enable checkbox to enable device-to-device IO Linking i.e. input from one Direct Door can trigger output in another Direct Door.
- **Network Interface**- Select the interface option for IO linking with external devices. The options are
 - Ethernet
 - Wireless
 - Mobile Broadband

Linking



This section is not available for Panel doors.

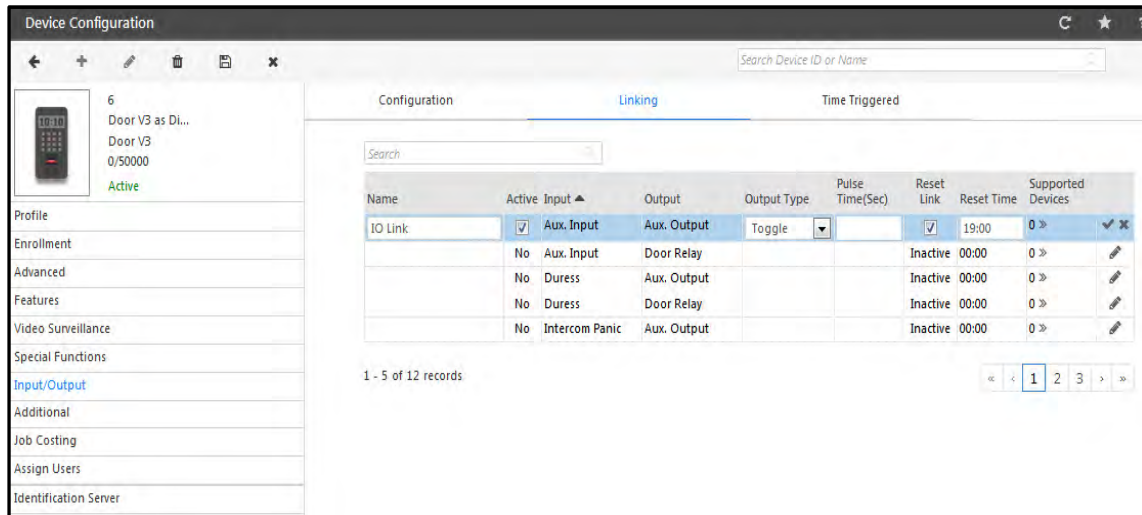
The **Linking** section appears as shown below.

The screenshot shows the 'Device Configuration' window with the 'Linking' tab selected. The sidebar on the left displays device details for 'Door V3 as Di...' (ID: 6, Status: Active). The main area contains a table with 8 columns: Name, Active, Input, Output, Output Type, Pulse Time(Sec), Reset Link, Reset Time, and Supported Devices. There are 5 rows of data in the table. At the bottom of the table, it shows '1 - 5 of 12 records' and a pagination control with buttons for navigating between pages (1, 2, 3, etc.).

Name	Active	Input	Output	Output Type	Pulse Time(Sec)	Reset Link	Reset Time	Supported Devices
	No	Aux. Input	Aux. Output			Inactive	00:00	0 »
	No	Aux. Input	Door Relay			Inactive	00:00	0 »
	No	Duress	Aux. Output			Inactive	00:00	0 »
	No	Duress	Door Relay			Inactive	00:00	0 »
	No	Intercom Panic	Aux. Output			Inactive	00:00	0 »

The COSEC application supports the Input/Output Linking feature to activate an output port based on a trigger received from an input port on the same Direct Door. This option enables the administrator to define how an event or events (input port) will trigger an output on the selected door.

Select a Input-Output linking row or click edit button.



- **Name** - Specify a name for the new I/O linking program to be defined.
- **Output Type** - Specify the appropriate type of output from the following four options available in the drop down list:
 - **Pulse**: With this type of output, the user needs to define the Pulse time in seconds.
 - **Interlock**: With this option, the output follows the input. The relay output is triggered as long as the input is activated after which it returns to normal state.
 - **Latch**: With this option, it is denoted that the relay output will be in an energized condition for infinite period and needs to be reset manually.
 - **Toggle**: With this option, the output group toggles its state whenever an input group is activated.
- **Pulse Duration (sec)** - For a *Pulse* output type, specify the pulse duration in seconds.
- **Active** - Select this checkbox to activate this linking program.
- **Reset Link**- Select this checkbox to reset the link automatically after a defined time period.
- **Reset Time**- Enter the time period in hh:mm format at which the link will get reset automatically. Suppose, an IO Link gets activated on 21/04/2017 at 15:00. And Reset Time is set as 18:00. When Device Time is 18:00 then that IO link will get reset.
- **Supported Devices** - All devices supported for external IO Linking will appear in this picklist for selection. Upto 255 external devices can be added by the administrator.
- Click the **OK** button and **Save** the configuration.

Time Triggered

On the **Input Output** page, select the **Time Triggered** section as shown.

The screenshot shows the 'Time Triggered' configuration window. It has tabs for 'Configuration', 'Linking', and 'Time Triggered'. The 'Time Triggered' tab is active. Below the tabs is a search bar and a table. The table has columns: 'Function Name', 'Active', 'Time', 'Duration(Sec)', 'Days', and 'Output'. The first row shows 'Siren Activate' with 'Active' checked, 'Time' as '00:00', 'Duration(Sec)' as '10', 'Days' as 'Select', and 'Output' as 'Aux O/P'. A dropdown menu is open for the 'Days' column, showing options: 'Check All', 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', and 'Holiday', all with green checkmarks.

This functionality enables the user to control the activity of an Output without manual intervention. The time triggered functions are used for activating events like door unlock and siren activation that are set as per the start time and for the configured time duration. This functionality is designed to energize outputs for predefined periods at the configured time. The COSEC access control system supports up to 20 Time Triggered functions on a Direct Door.

The screenshot shows the 'Time Triggered' configuration window. It has tabs for 'Configuration', 'Linking', and 'Time Triggered'. The 'Time Triggered' tab is active. Below the tabs is a search bar and a table. The table has columns: 'Function Name', 'Active', 'Time', 'Duration(Sec)', 'Days', and 'Output'. The first row shows 'Siren Activate' with 'Active' as 'Yes', 'Time' as '00:00', 'Duration(Sec)' as '10', 'Days' as 'Su Mo Tu We Th Fr Sa Ph', and 'Output' as 'Aux O/P'. There are edit and delete icons next to the 'Days' column.

Additional

This section lists some additional configurations that can be enabled for door controllers.

To access these configurations, Go to **Device Configuration > Additional > Daylight Saving**



This section is available only for Direct Doors.

Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. COSEC doors can be configured to be compatible with this procedure keeping the RTC of the system updated with such changes.

The **Daylight Saving** configuration can be done in 2 ways i.e. Day-Month wise or Date-Month wise.

- Select the **DST Type** as Day-Month wise or Date-Month wise. The **Disable** option when selected, disables the application of DST on the system time.
- On selection of the **Day-Month wise** option, the DST is set by the day of the month on which clock needs to be forwarded and reverted back to normal. Set the month, week number, day of the week, and time for both the **Forward Clock** and **Backward Clock** as shown.

The screenshot shows the 'Device Configuration' window with the 'Daylight Saving' tab selected. On the left, a sidebar lists various configuration options: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional (highlighted), and Assign Users. The main area displays settings for 'Daylight Saving'. The 'DST Type' is set to 'Day-Month wise'. The 'Time Period' is set to '08:00'. Under 'Forward Clock', the 'Month' is 'November', 'Week No.' is '1st', 'Day of Week' is 'Sunday', and 'Time' is '09:00'. Under 'Backward Clock', the 'Month' is 'January', 'Week No.' is '1st', 'Day of Week' is 'Sunday', and 'Time' is '10:00'. A 'Save' button is at the bottom right.

- On selection of the **Date-Month wise** option, the DST is set by date of the month on which clock needs to be forwarded and reverted back to normal. Define the **Time Period** for the date-month wise DST settings in 24-hours format, and specify the day of the week, date and time for the **Forward Clock** and the **Backward Clock** as shown.

This DST Setting implies that on 1st Sunday of November at 09:00 hours, the clock will be forwarded by 08:00 hours. And on 1st Sunday of January at 10:00 hours, the clock will be reversed by 08:00 hours.

The screenshot shows the 'Device Configuration' window with the 'Daylight Saving' tab selected. The 'DST Type' is now set to 'Date-Month wise'. The 'Time Period' remains '08:00'. Under 'Forward Clock', the 'Month' is 'November', 'Date' is '1', and 'Time' is '09:00'. Under 'Backward Clock', the 'Month' is 'January', 'Date' is '1', and 'Time' is '10:00'. A 'Save' button is at the bottom right.

- Click the **Save** button.

Job Costing



Job Costing is applicable for Door V3 and Door V4 Direct Door only.

When user punches on any device, there will be an option to select the Job Code on which the user is working. Job Costing enables the admin to show or hide Job Code selection on device. It also enables the admin to assign default jobs on device.

Device Configuration

6
Door V3 as Di...
Door V3
0/50000
Active

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Settings

Show Job Menu: Show List
Retain Job Selection: ☐

Assign Jobs

Job Group: 1
Job: ID

Search

Job Code	Name	Assignment Start	Assignment End	
PSD-R	PSD Review	22/05/2017	17/06/2017	
PSD-W	PSD study	08/05/2017	10/06/2017	
SAD	SAD study	08/05/2017	30/06/2017	
SWD	Development	22/05/2017	31/07/2017	

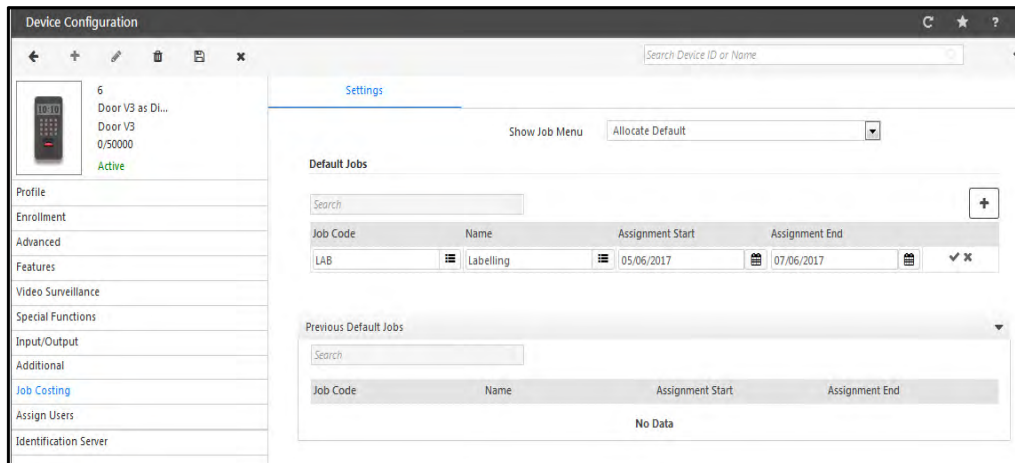
Show Job Menu: Select the option as **Show List** or **Allocate Default**.

When **Show List** is selected; then multiple jobs can be assigned to the device. The user can select the relevant job code while punching on the device. His job hours will be recorded for that job code.

- **Retain Job Selection:** Select this checkbox to retain the job code selected by a user which would be applicable for all the subsequent users until another job selection is done on device.
- **Assign Jobs:** Select the Job group or individual job from the picklist. Then click on Save button. The jobs will be listed to the grid.

When **Allocate Default** is selected; then default jobs for the device can be selected.

- **Default Jobs:** Click Add button to add the default job on the door. Then click on the Job picklist button and select the job to be assigned to the device. The Job costing user can directly punch on this door for starting the default job.



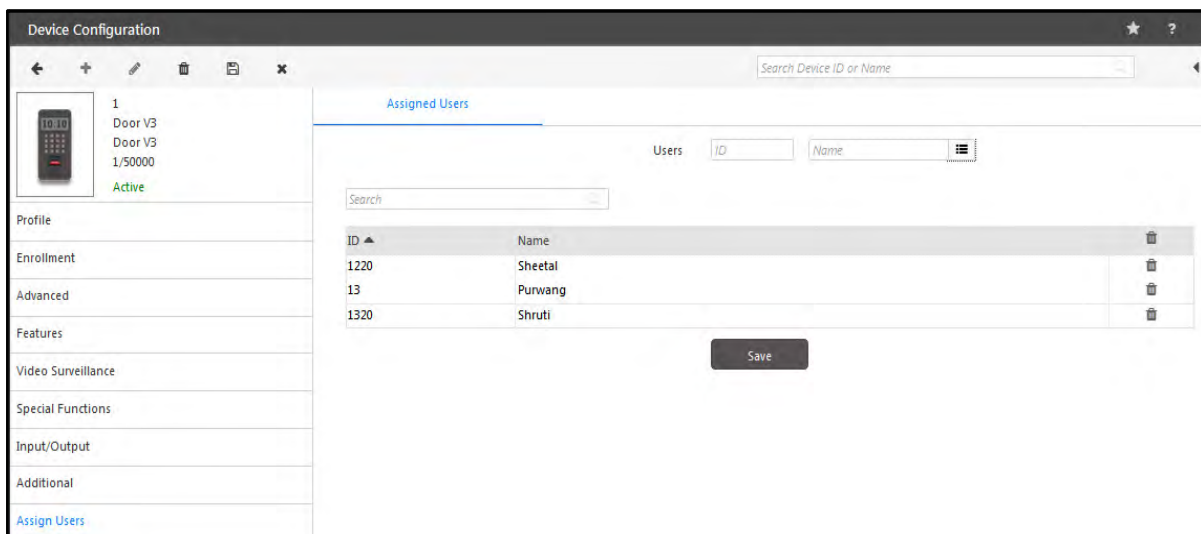
Finally click on **Save** button to save the configuration.

When the assignment date of the default job gets elapsed, then the respective job will be listed in **Previous Default Jobs** section.

Assign Users

To the configured device, you can select and assign the users.

Click the picklist button and select the users.

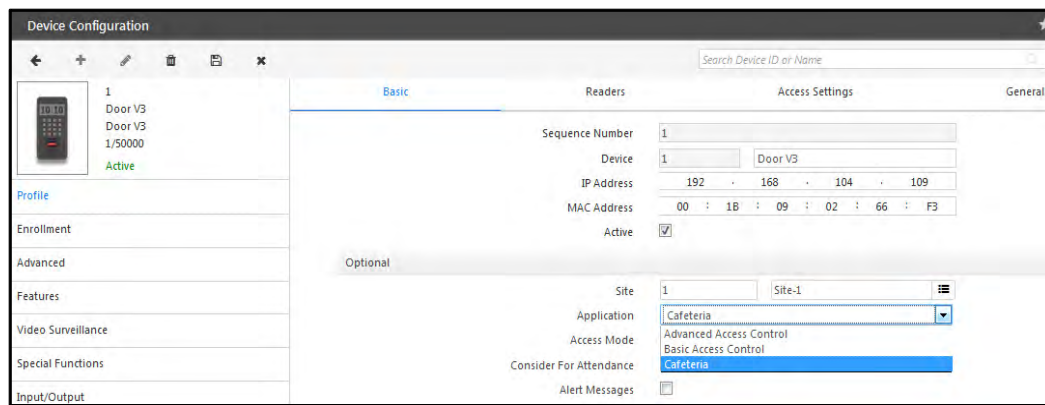


- Click the **Save** button to assign all the added users to the selected door.

Cafeteria

The COSEC system enables the user to configure devices which will be used by the Cafeteria management module.

To configure a door for Cafeteria application, select **Cafeteria** option in Device Profile> Basic> Application as shown below.



The Cafeteria tab will appear in Device Configuration page.
 Select **Device Configuration> Cafeteria> Settings**

Settings

The Cafeteria configuration for Door V3 is shown as below.

The screenshot shows a web application window titled "Device Configuration". On the left is a sidebar with a list of menu items: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, Cafeteria (highlighted in blue), and Identification Server. The main area is divided into two tabs: "Settings" and "Menu". The "Settings" tab is active and contains a "Printer Settings" section. This section includes a "Consecutive Transaction Delay (Sec)" input field with the value "0". Below this is a "Printer" dropdown menu set to "None", a "Connection Type" dropdown menu set to "RS232", and a "Baud Rate" dropdown menu set to "115200". There are also text input fields for "Company Name", "Company Address", and "Punch Line". At the bottom of the section is a checkbox labeled "Exclude Price-Cost From Coupon" which is currently unchecked. A search bar at the top right of the main area is labeled "Search Device ID or Name".

- **Consecutive Transaction Delay (Sec):** Enter the time interval between two transactions, wherein any user transaction would be restricted.

Printer Settings

- **Printer:** Select the printer from the dropdown list based on the site requirements.
- **Connection Type:** Select the printer connection type from the drop down list. The options available are:
 - RS232 (serial)
 - USB
- **Baud Rate:** In the event of a serial printer, select the appropriate baud rate from the drop down list.
- Specify the **Company Name**, **Company Address** and the **Punch Line** as per the site requirements. These details will be printed on the receipt dispensed from the selected printer.
- Select the **Exclude Price-Cost From Coupon** check box if you want to exclude the price from the coupon.

Menu

COSEC allows the administrator to assign one or more cafeteria menus (Menu 1, Menu 2, Menu 3... upto 99.) to a device. These can be configured by selecting pre-defined menus from the Menu picklist.



The Menu is created from Cafeteria module.

Device Configuration

Settings Menu

Assign Menu

Menu ID Name

Search

Menu No	ID	Menu Name	
1	1	Menu 1	

Save

Schedule Menu

Search

Menu No	ID	Menu Name	Start Time	End Time	Schedule Days	
1	1	Menu 1	12:00	15:00	_ Mo Tu We Th Fr Sa	

The Menu can be scheduled from Cafeteria module and is displayed in “Schedule Menus” as shown above.

If you have to assign another menu and schedule it on the door then select the Menu from the picklist. The Menu will be shown in the grid as shown below.

Assign Menu

Menu ID Name

Search

Menu No	ID	Menu Name	
1	1	Menu 1	
2	2	Menu 2	

Save

Schedule Menu

Search

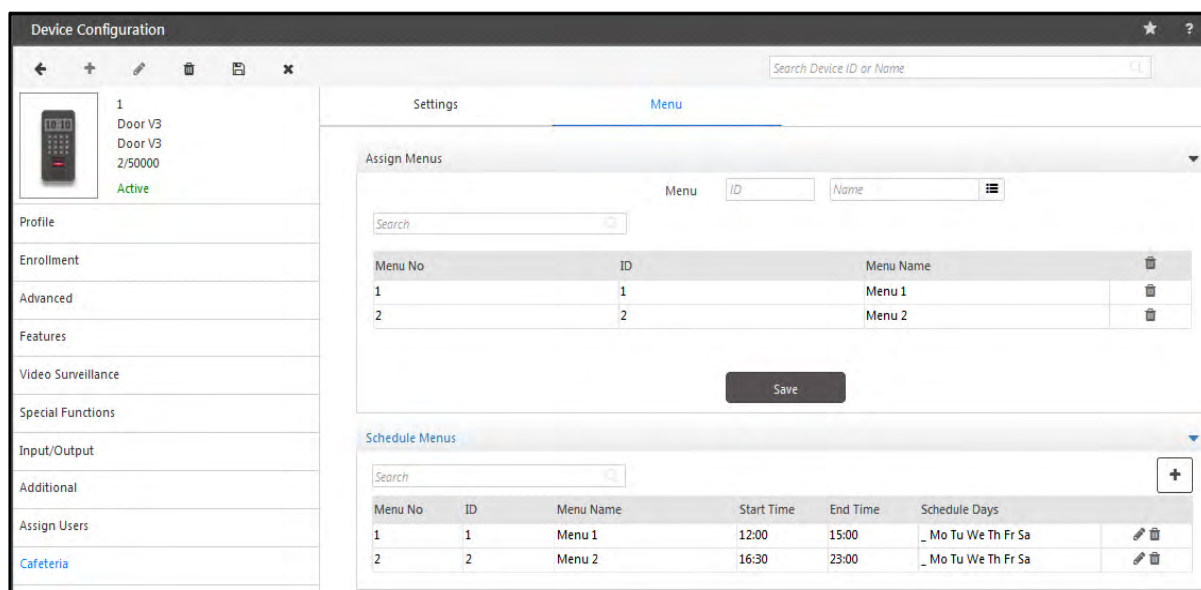
Menu No	ID	Menu Name	Start Time	End Time	Schedule Days	
1	1	Menu 1	12:00	15:00	_ Mo Tu We Th Fr Sa	

Add

Now to schedule the menu click **Add** button as shown above.

Then select the menu to be scheduled from the **ID** picklist. Specify the **Start** and **End time** for which the Menu will be active and is available to users on the selected door. Select the **days** for which this menu will be available i.e. scheduled on the door.

Then click **OK** and **Save** the Menu schedule on the door.



Two Menus cannot be scheduled for same timing.

Identification Server

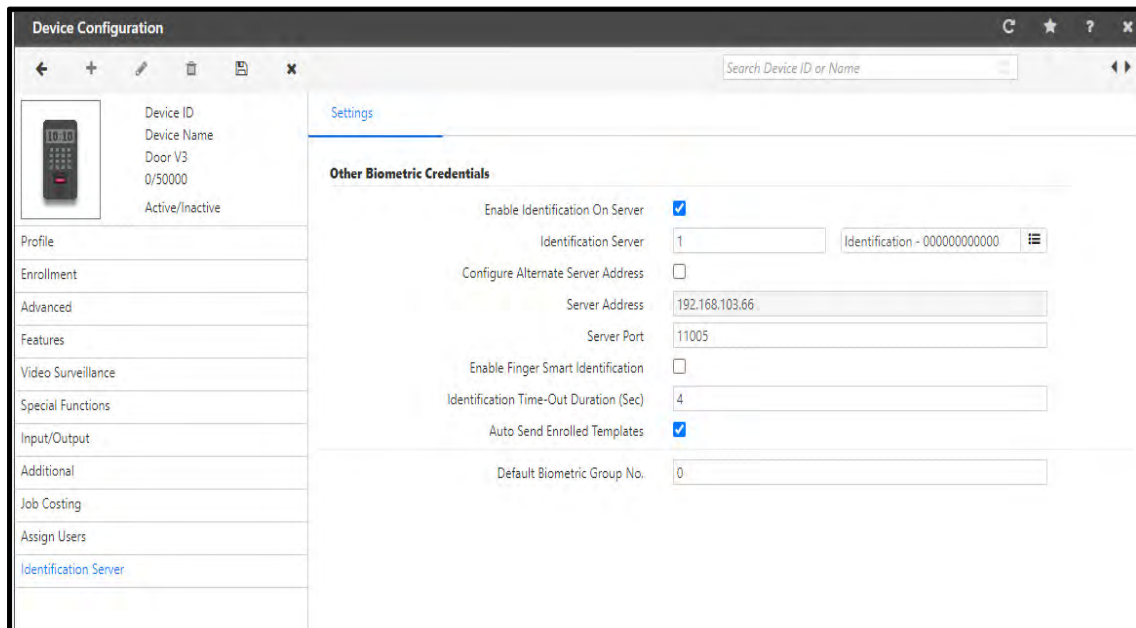
This tab enables the selected device to be assigned to a pre-defined Identification Server.

Device has a limited memory capacity for storage of templates so we need Identification Server which will store the more number of templates and respond to device when asked for identification.

For more information on Identification Servers, See *Admin> System Configuration> Identification Server Configuration*.

To access these configurations,

- On the **Device Configuration** page, select the **Identification Server** tab.



Other Biometric Credentials

- **Enable Identification On Server:** Select the checkbox to enable the identification of palm/finger templates on this device.
- **Identification Server:** Select an Identification Server using the picklist button to which the device is to be assigned. The configuration of server is done from **Admin module > System Configuration > Identification Server Configuration** and the Identification Service must be started from the service tray.
- **Configure Alternate Server Address:** Enable this check-box to configure external IP address of Identification Server.
- **Server Address:** It displays the IP Address of the selected Identification Server.
- **Server Port:** Enter the server port number. The default port number is 11005.
- **Enable Finger Smart Identification:** For all other supported doors, select the checkbox to enable fingerprint templates identification through Identification Server.
- **Identification Time-Out Duration (Sec):** Specify the duration in seconds after which the fingerprint template identification will get time out.
Example: If 5 seconds is specified, then the identification server will try to identify the template till 5 seconds and if not found then it will show time-out to the user.
- **Auto Send Enrolled Templates:** Select the checkbox to enable any enrolled templates to be saved both on the COSEC database as well as saved locally on the configured Identification Server. This enables prompt identification of user on enrollment.
- **Default Biometric Group No.:** Specify the default biometric group number to be assigned to the device. It is a number allotted to a device to be assigned to the Identification Server. This enables the Identification Server to match the template against only those devices that belong to the corresponding biometric group. This reduces the false detection as well time to search template.

Door FMX

COSEC DOOR FMX makes use of advance multispectral fingerprint sensor. It reads surface and subsurface of a finger and gives very clear and strong image. Door FMX can be connected as **Direct Door** only.



The Device Configuration page for Door FMX appears as shown below:

A screenshot of the Device Configuration page for Door FMX. The page is divided into a left sidebar and a main configuration area. The sidebar contains a list of tabs: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main configuration area is titled "Device Configuration" and has a search bar at the top. Below the search bar, there are four tabs: Basic, Readers, Access Settings, and General. The "Basic" tab is selected. Under the "Basic" tab, there are fields for Sequence Number (6), Device (4), IP Address, and MAC Address (DE : 46 : ED : B6 : 86 : 78). There is also a checkbox for "Active" which is checked. Below these fields, there is an "Optional" section with a dropdown for Site (1) and a list of settings: Finger Template Format (Lumidigm ISO), Application (Advanced Access Control), User Access Mode (Any One), Visitor Access Mode (Any One), Consider For Attendance (checked), Alert Messages (unchecked), Consider For Visitor Pass Surrender (unchecked), and Generate Events (checked).

Enter the MAC address of the door. The IP address will be displayed automatically once the device comes online in Monitor.

To add Devices automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the "Auto Add New Devices" checkbox. Once the device is connected in network, it will come online in COSEC Monitor.



The Monitor Service must be running while adding the device to COSEC.

Once the device is configured, click the **Save** button to save the configuration.

To know more about configuring devices, click on the links for different tabs of Device configuration.

- [“Profile”](#)
- [“Enrollment”](#)
- [“Advanced”](#)
- [“Features”](#)
- [“Video Surveillance”](#)
- [“Special Functions”](#)
- [“Input/Output”](#)
- [“Additional”](#)
- [“Job Costing”](#)
- [“Assign Users”](#)
- [“Cafeteria”](#)
- [“Identification Server”](#)

Profile

This section enables the user to set up the basic profile for any new device. Setting up a door profile involves defining basic parameters to set up any door controller device.

To do this, On the **Device Configuration** page, select the **Profile** tab. The Profile can be configured in the following sections:

- [“Basic”](#)
- [“Readers”](#)
- [“Access Settings”](#)
- [“General”](#)

Basic

The **Basic** section for “Door FMX” is shown below:

The screenshot shows the 'Device Configuration' window with the 'Basic' tab selected. The left sidebar lists various configuration options: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main area displays the following fields:

- Sequence Number: 6
- Device: 5 (with a dropdown menu showing 'FMX Direct')
- IP Address: (empty field)
- MAC Address: FD : ED : 46 : 31 : 12 : 12
- Active: ☒

Below these fields is an 'Optional' section with a dropdown arrow.

Configure the following options as required:

- **Sequence Number** - This is a system generated sequence number for each new device.
- **Device**- Specify a name that can be assigned to the door. The Door ID is auto-generated by the system.
- **IP Address** - This is the IP address assigned to the door. Once the device connection is established, this field will automatically display the door IP address.
- **MAC Address** - Specify the MAC Address of the door.



MAC address of door is required while manually adding the door to the COSEC Monitor. Note the MAC address from the device when it is powered on.

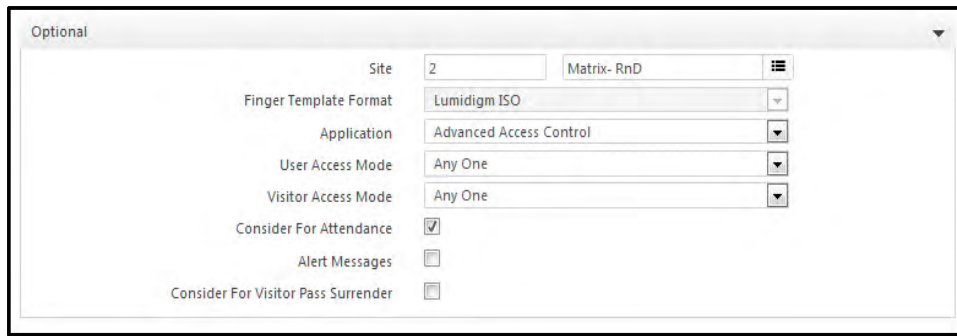
- **Active** - Check the box to activate the device on the network.



*To add the Device automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the “**Auto Add New Devices**” checkbox.*

*The device will be added automatically but make sure you enable the **Active** checkbox in order to connect the device to the network. Once the device is connected to the network, it will come online in COSEC Monitor.*

The **Basic** page also offers an **Optional** tab which provides optional configurations as shown below:



The screenshot shows a configuration window titled 'Optional'. It contains several settings:

- Site: 2
- Matrix- RnD: Matrix- RnD
- Finger Template Format: Lumidigm ISO
- Application: Advanced Access Control
- User Access Mode: Any One
- Visitor Access Mode: Any One
- Consider For Attendance: ☒
- Alert Messages: ☐
- Consider For Visitor Pass Surrender: ☐

- **Site** - Select the site to which this door is to be assigned from the site picklist window. Site is created from Devices> Masters> Site.
- **Finger Template Format** - For FMX door, the finger templates will be enrolled in Lumidigm ISO format. For globally setting the template format, you can set from Global policy.
- **Application** - Select the application type for which the device is to be used. The options are **Basic Access Control**, **Advanced Access Control** and **Cafeteria**. All devices set to **Cafeteria** will subsequently be available for Cafeteria configuration.
- **User/Visitor Access Mode** - Defines the type and combination of credentials required to identify and validate a user at the Door Controller. Select the appropriate credential combination from the drop down list.

The options available are:

- Any one
 - Card
 - Card + Biometrics
 - Card + Biometrics + PIN
 - Card + PIN
 - Biometrics
 - Biometrics + PIN
 - Biometrics then Card
 - None
 - Face
 - Card+ Face
 - PIN + Face
 - Biometrics+ Face
 - Card then Biometric
-
- **Cafeteria Face Access Mode** - When Application is set as '**Cafeteria**', only then this configuration is available to the Admin and to add provision of using face as a credential to make transactions on cafeteria devices.
 - Select the mode type from the drop down to allow a user to choose multiple menu items and upon checkout do transaction using face as credential.
 - The options available are **None**, **Default Item** and **Item Selection**.

Optional

Site * 1 Site-1

Finger Template Format Suprema Proprietary

Application Cafeteria

User Access Mode Any One

Visitor Access Mode Any One

Cafeteria Face Access Mode

Consider For Attendance

Alert Messages

Consider For Visitor Pass Surrender

Generate Events

None

None

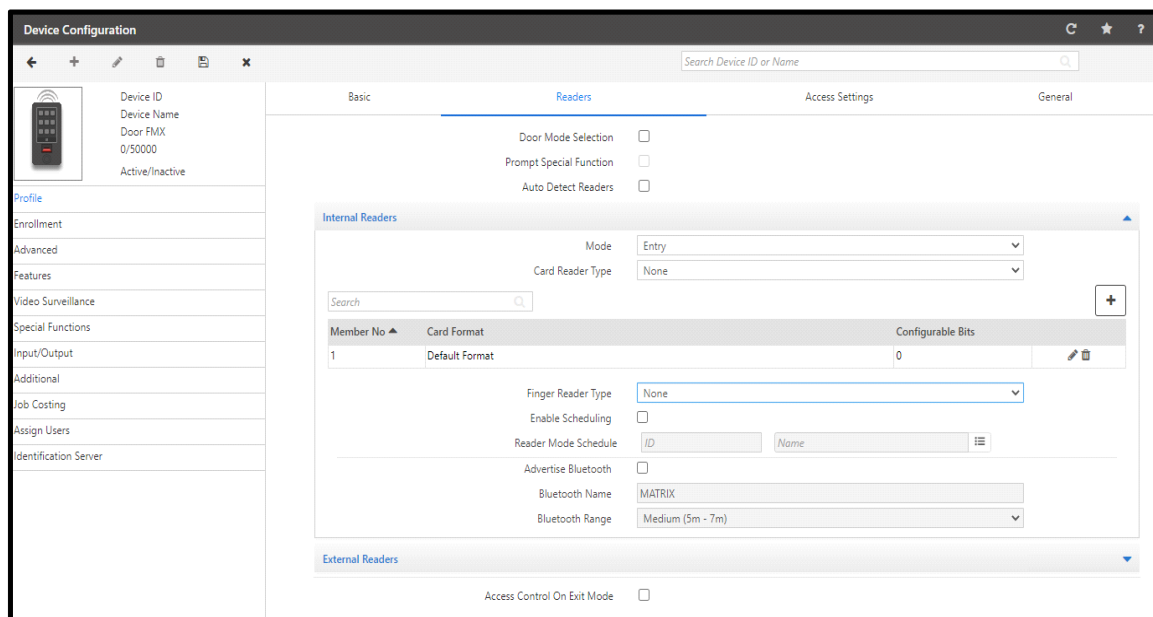
Default Item

Item Selection

- Default Item mode in cafeteria will allow users a touch less cafeteria experience. In Default Item mode only the transaction for default item is allowed. A default item is assigned in each scheduled menu.
- Item Selection mode in cafeteria will allow users to select the desired menu items and make a transaction using Face as a credential.
- **Consider for Attendance** - Select this check box if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as access control events.
- **Alert Messages** - Select this check box to enable the application to send alerts based on events from this door.
- **Consider for Visitor Pass Surrender:** Check the box to consider the selected device for visitor pass surrender. The Visitor can show his credential on this device to surrender the pass.
- **Generate Events:** This check-box is enabled by default. You can disable the check-box if the server is not required to receive any events from the respective devices.

Readers

Readers are important hardware components in a biometric door device. They may be internal or external. This section enables the administrator to configure both internal and external readers for a door as shown.



The following parameters are available for configuration:

- **Door Mode Selection** - If this option is enabled, then user will be prompted to select punch type as IN or OUT while punching on the device.

E.g.: When a door is in Entry mode, your punches will always be in Entry side. But if you want to mark the punch in exit mode then you can select the door mode if “Door Mode Selection” is enabled.
- **Prompt Special Function**- This will provide selection of special function on device screen and based on the selection of particular type of special function, job codes for JPC user will be prompted. This can be enabled only when “Door Mode Selection” is enabled.
- **Auto Detect Readers** - Select this checkbox to enable auto detection of Readers on a door controller connected to the server.

Internal Readers

This option allows the configuration of the Internal Reader for the selected door.

- **Mode**: Select the Mode as **Entry** or **Exit** from the drop down list.
- **Card Reader Type**; Select the Card Reader Type from the following options:
 - EM Prox Reader
 - HID Prox Reader
 - MiFare Reader
 - HID iClass-U Reader
 - HID iClass-W Reader
- **Card Format**: The single or multiple card formats can be assigned to the readers. The default card format is assigned to device as shown in the grid. If no other card format is assigned to device; then this default format will be applied.



The formatting of card is described in *Devices> Master> Card Format*

Multiple Card Format

To assign multiple card formats to device click on **Add** button. Then click the picklist to select the card format. And click **OK** to save the format.

Member No ▲	Card Format	Configurable Bits
1	Default Format	0

Member No ▲	Card Format	Configurable Bits
1	Default Format	0
2	Format1	0


Similarly you can add maximum 5 card formats. When the card format is saved, the Configurable bits of that format as configured from Masters> Card format will be displayed here. Multiple Card format configurations will be dispatched to door separated by '**Format ID**' that is 'Member No.' along with all other format related parameters.

Internal Readers

Mode: Entry
Card Reader Type: EM Prox Reader

Member No ▲	Card Format	Configurable Bits
1	Default Format	0
2	Format1	26
3	Format2	32

- Select the **Finger Reader Type** as **Finger Reader**.

Click the **FP Reader Configuration**  button to set the **Security Level** and **Sensitivity** and **Restore Defaults** for the selected FP Reader as shown.

Finger Print Module Calibration

Security Level: High
Sensitivity: Level 2

Restore Defaults

Save Close

Finger Print Module Calibration

- **Security Level:** Security level specifies FAR (False Acceptance Ratio). Since FAR and FRR (False Rejection Ratio) is in inverse proportion to each other, FRR will increase with higher security levels.

For regular Time-Attendance system “Normal” level can be selected. For high security areas requiring complete or maximum matching of template, “High/Highest” level must be selected. For approximate matching of template, “Low” level can be selected.

- **Sensitivity:** Specifies sensor sensitivity to detect a finger. On high sensitivity, the module will accept the finger input more easily. Level 3 has the highest sensitivity.
- Click on the **Restore Defaults** button to return the field values for this page to default values if needed.
- Click on the **Save** button.
- **Enable Scheduling:** Select this checkbox to **Enable Scheduling** to set reader mode of door as entry or exit as per user-defined schedules.
- **Reader Mode Schedule:** Select the schedule from the picklist which is to be assigned to the internal reader of Door FMX. With this the same reader can be configured to function both in Entry as well as Exit mode based on scheduled timings.
- **Advertise Bluetooth-** Select this checkbox to enable Bluetooth of the device by which the device will be visible to others. Then configure the following parameters
 - **Bluetooth Name-** By default, if the Device Name is configured then it will be displayed here along with the Mode. The prefix will be the Device Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the bluetooth name as per your requirement. The Bluetooth Name can be a maximum of 10 characters.
 - **Bluetooth Range-** The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m-2m), Medium (5m-7m) or Long (>8m).

External Readers

This option allows the configuration of the External Reader for the selected door.

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop down list.
- **External Reader Type:** Select the desired type of External Reader from the drop-down list.
- **Card Format** - Select a card format to be applicable for external readers of the device. For multiple format description [See “Multiple Card Format” on page 814.](#)
- **Exit Switch** - Select this checkbox to enable the use of **Exit Switch**.
- **User/Visitor Access Mode** - Select the access mode from the options shown below:
 - Any One
 - Card

- Biometrics
 - Card + Biometrics
 - Biometrics then Card
 - None
- **Access Control On Exit Mode** (only for direct door) - Select this checkbox to enable access control on the exit mode.

Access Settings

This section is available for direct doors. The **Access Settings** page appears as shown below:

The screenshot shows the 'Device Configuration' window with the 'Access Settings' tab selected. The left sidebar lists various configuration sections: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main area is divided into four tabs: Basic, Readers, Access Settings (active), and General. Under the 'Access Settings' tab, the following settings are visible:

- Universal Time Zone:** A dropdown menu showing '(GMT+05:30)Chennai, Kolkata, New Delhi, Mumbai'.
- Time Format:** A dropdown menu showing '24 Hours'.
- Auto Synchronize with NTP:** A checked checkbox.
- Preferred NTP Server:** An empty text input field.
- Working Days:** A grid of checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, Sat, and Holiday, all of which are checked.
- Working Hours(HH:MM):** Two text input fields showing '00:00' and '23:59'.
- Holiday Schedule:** A table with four rows, each containing a number (1-4) in a dropdown, a text input field for the schedule name, and a menu icon.

- **Universal Time Zone** - Select the geographic time zone in which the DOOR will operate.
- **Time Format** - Specifies the time format to be displayed on Door Controller LCD display. The formats available are:
 - 24 Hours
 - 12 Hours

Select the relevant option from the drop down list as per the site requirements.

Auto Synchronize with NTP

If Date and time is to be automatically synchronized as per the **Preferred NTP Server** (predefined or user-defined NTP server address) selected by user, then you must enable **Auto Synchronize With NTP** checkbox.

Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from device webpage, which will be reflected on device display.

- When Auto Synchronization with NTP is disabled Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 1. You can specify the Preferred NTP server of your choice. In this case device will first try to get Date and Time from that server address.
If it does not get Date and Time in three tries; device will check from pre-defined NTP servers.
If you have entered one of the three pre-defined NTP servers(ntp1.cs.wisc.edu , time.windows.com , time.nist.gov); then device will first check that server first.
If it receives updated Date and Time then Updated Date and Time will be reflected on device webpage and display screen.
 2. You can keep the Preferred NTP server as blank. In this case device will check for Date and Time from the first NTP server.
 3. If user has manually entered Date and Time from webpage or Device Menu then those values of Date and Time will be reflected on device webpage and display screen.

In the case of the **Manual** option the administrator can manually update the time on the Door with that of the system time as and when required. This can be accomplished from the COSEC Monitor and control application.

- **Working Days** - Specify the days on which the default working hours should be applicable. Check the relevant boxes to specify the active days.
- **Working Hours (HH:MM)** - Define the default working hours in HH:MM format.
- **Holiday Schedule** - This section allows the administrator to assign up to four holiday schedules to the device by using the Holiday Schedule picklist.



If the same holiday schedule is configured for a user and for the door controller on which the user is assigned, then the user's attendance marking on this device, on any of the scheduled holidays will always be marked as a holiday.

General

The **General** page appears as follows. Enter all general details applicable to the device in this section.

Device Configuration

30 Door FMX-Dev...
Door FMX
0/50000
Active

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Basic Readers Access Settings **General**

Mute Buzzer ☐

Allowed Acknowledgement

Display Duration (ms) 3000
LED - Buzzer Duration Long

Denied Acknowledgement

Display Duration (ms) 3000
LED - Buzzer Duration Long

Enable Display Messages ☐
Custom Birthday Message Happy Birthday
Display Message 1 ☒
Schedule 00:00 11:59
Message Good Morning
Display Message 2 ☒
Schedule 12:00 15:59
Message Good Afternoon
Display Message 3 ☒
Schedule 16:00 20:59
Message Good Evening
Display Message 4 ☒
Schedule 21:00 23:59
Message Good Night
Multi-Language Support ☐
Auto Hide Menu Bar ☐

- **Mute Buzzer** - User can mute or unmute the door buzzer by checking or clearing the box respectively.
- **Allowed Acknowledgment**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgment Allowed' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.
- **Denied Acknowledgment**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgment Denied' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.
- **Enable Display Messages** - This feature allows the user to enable custom birthday message and display messages to be displayed on the door device. Upto 4 display messages can be configured for a door.

- **Custom Birthday Message**- Enter the birthday message which would appear on the door when the user punches on the door on his birth date.

The valid values are

A-Z

a-z

0-9

`~!@#\$%^&*()_+-{}|;:?'<>.,\''"

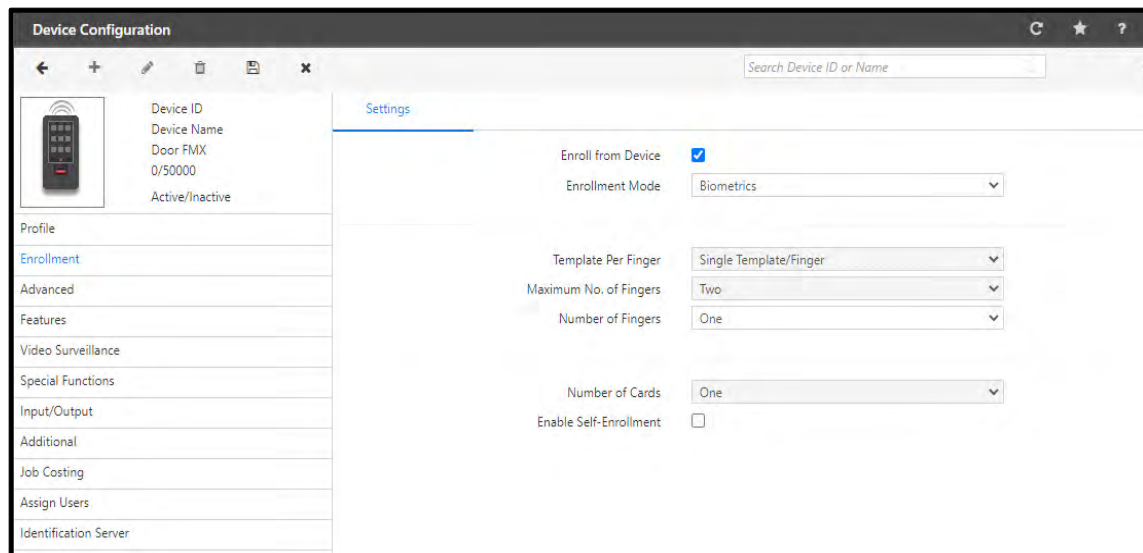
- **Display Message** - Enable each display message individually by selecting this checkbox.
- **Schedule** - For each message, the user needs to define the time period between which this message is to be displayed.
- **Message** - Enter the message to be displayed in this field. Maximum 21 characters allowed.
- **Multi-Language Support** - Select this checkbox to enable multi-language support for the selected device.

The **Display From** field shall display the reading order for the selected language.

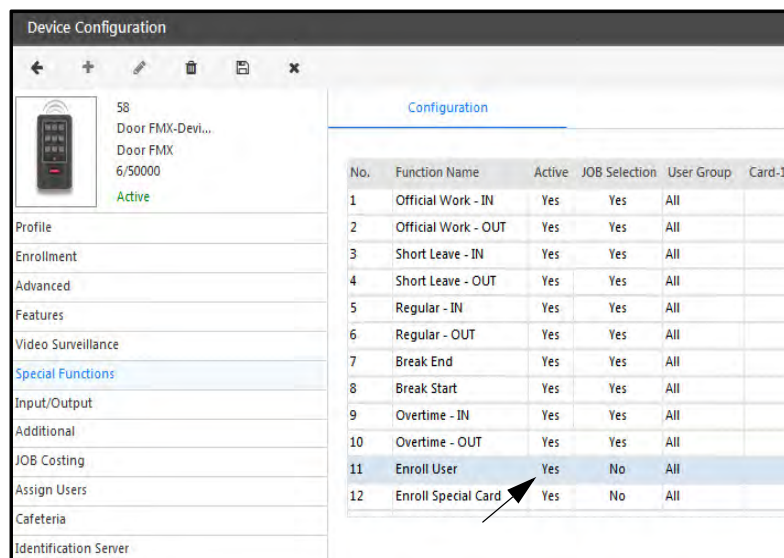
- **Auto Hide Menu Bar**- If a person touches the device screen by mistake and enter into Menu; then the finger sensor will not take the punch when he punches on device till the menu is closed or time out occurs. So in this case; enabling the **Auto hide Menu Bar** check-box will hide the menu and the user will be able to punch on the door. If you want to access the Menu then swipe upwards on the screen which will show the menu.

Enrollment

The Enrollment page appears as shown below.



- **Enroll from Device** - Select this check-box to enable the enrollment of user from the door controller. When this check-box is enabled, 'Enroll User' special function on that device will get active as shown below.



If 'Enroll User' special function & 'Enroll From Device' check-box both are inactive in device configuration, then on activating 'Enroll User' special function, 'Enroll From Device' check-box will be enabled.

- **Enrollment Mode** - Select the desired type of credential from the dropdown list that can be enrolled using the special function at the DOOR.

The options are — ReadOnlyCard, SmartCard, Biometrics, and BiometricsThenCard

- **Enrollment Using** - Select the option **User ID** or **Reference No.** using which enrollment will be done.
- **Template Per Finger** - This parameter displays the values as configured at the global level. This field is not user editable from this page.
- **Max Number of Fingers** - This parameter displays the values of the maximum number of fingers configured at the global level. This field is not user editable from this page.
- **Number of Fingers/Cards** - Select the number of cards or fingerprints to be enrolled based on the credential option selected in the Enrollment Mode parameter.
- **Enable Self-Enrollment** - Select this checkbox to enable the self-enrollment feature on this door.

Advanced

The Advanced tab allows the user to configure some advanced parameters such as access control settings, alarms and device timers.

To access this, After selecting the device, Select the **Advanced** tab from **Device Configuration** page. The advanced settings can be configured from following sections:

- *“Settings”*
- *“Alarms”*
- *“Timers”*
- *“Wiegand”*

Settings

The **Advanced Settings** page for Door FMX as **Direct Door** appears on your screen as shown below:

The screenshot shows the 'Device Configuration' window with the 'Advanced' tab selected. The left sidebar lists various configuration categories, and the main area displays settings for the 'Door FMX' device. The 'Advanced' tab is active, showing a list of settings including checkboxes for event generation, PIN display, and door lock exit, as well as numeric and dropdown settings for access levels, timers, and sensor parameters.

Settings	Alarms	Timers	Wiegand
Generate Exit Switch Events	<input type="checkbox"/>		
Generate Invalid User Events	<input type="checkbox"/>		
Generate Sequential IN-OUT Events	<input type="checkbox"/>		
Two Credentials Required	<input type="checkbox"/>		
Show PIN	<input type="checkbox"/>		
Allow Exit when Door Lock	<input checked="" type="checkbox"/>		
Auto Relock	<input type="checkbox"/>		
Auto Relock Timer (Sec)	3		
Enable Additional Security	<input type="checkbox"/> Disabled		
Enable Smart Identification	<input type="checkbox"/>		
Access Level	8		
Access Mode	Card		
Auto Acknowledge Alarm	<input type="checkbox"/>		
Auto Acknowledge Alarm (Sec)	10		
Facility Code	1		
Allow Access Through Mobile	<input type="checkbox"/>		
Mobile Entry Access Mode	Mobile Only		
Mobile Exit Access Mode	Mobile Only		
Show Attendance Details	<input type="checkbox"/>		
Sensor Type	FEVOTBOT		
Sensor Interface	USB		
Emissivity	0.95		
Calibration Parameter	+ 0.0		
Approach to Sensor Wait-Timer (Sec)	3.0		
Temperature Detection Time Out (Sec)	10		
Tolerance between Consecutive Readings	0.5		
Consecutive Readings Count within Tolerance	5		
Temperature Threshold (°F)	99.5		
Minimum Temperature for Access (°F)	95.0		
Restriction Type	Soft		
Bypass If Sensor Disconnected	<input type="checkbox"/>		

The following parameters are available for configuration:

- **Generate Exit Switch Events** - Select this checkbox to enable the door to generate events everytime the exit switch is used.
- **Generate Invalid User Events** - Select this checkbox to enable the door to generate events for invalid user inputs.
- **Generate Sequential IN-OUT Events** - Select this checkbox to generate user punches on device as the sequential IN-OUT events irrespective of whichever mode in which device is functioning.
- **Two Credentials Required**- Select this checkbox to enable the feature of verifying 2 credentials mandatorily for users allowed to By-pass finger/palm.
- **Show PIN**- Select this checkbox to display the characters of PIN when the PIN is entered on device.
- **Allow Exit when Door Lock** - Select this checkbox if users are to be allowed to exit even when the Door relay is in locked condition.

- **Auto Relock** - Select this checkbox to allow the door to relock immediately when the door status changes to close after normal open irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Relock Timer** - Specify the time in seconds for the Auto Relock operation.
- **Enable Additional Security** - Select this checkbox to enable additional security at the selected Door Controller.
- **Additional Security Code** - Enter a code (ranging from 1 to 65535) in the field provided. Re-enter the code to confirm.



*Changing this value can affect the SI function. Click on the **Default Code** button to reset the **Additional Security Code** to the value set in the **Global Additional Security Code** field on the Global System Policy page.*

- **Enable Smart Identification** - Select this checkbox to enable this functionality at the selected Door Controller and select the **Access Level** and the **Access Mode** from the drop down list.
- **Auto Acknowledge Alarm** - Select this checkbox to enable the auto-acknowledgement of all alarms for this device.
- **Auto Acknowledge Alarm (sec)** - Set the time in seconds for the Auto Acknowledge Timer. The wait timer will start and on expiry of the timer, the alarm buzzer will stop automatically.
- **Facility Code** - Set a value for Facility Code to be set for access modes other than “Card”, if Facility Code is expected in Wiegand Output. This will be applicable to all direct doors except Door V1 and V2.
- **Allow Access Through Mobile**- Check the box to allow the access to device using COSEC ACS App.
- **Mobile Entry/Exit Access Mode**- Select the entry and exit door access mode from the options of **Mobile Only**, **Mobile then Biometrics**, **Mobile then Card** and **Mobile then PIN**.



If User Access Mode is selected as “None” in Zone Configuration and Mobile Access Mode is selected as “Mobile Then Biometrics” then door can be accessed through Mobile and then Biometric credential.

- **Show Attendance Details** - Select this check-box for displaying the Attendance Details of the user on FMX door. This allows user to view his attendance details on FMX door itself and there is no need to login to ESS application to view attendance details.

The attendance details of user will be displayed for default Menu Time-Out period (30 sec) after Access Allowed screen.



*1. The user whose Attendance details are to be displayed on FMX door must be enabled for this feature. Enable the check-box **Show Attendance details on Device** from User Configuration> T&A> Attendance.*

2. While an attendance detail of one user is being displayed on device and second user tries to access the device; new user will be processed.

3. Whenever both users of 2-person rule are allowed to get access on device then attendance details screen of second user will be loaded on device.

- **Sensor Type:** Select the type of thermal sensor integrated in the device. There are three sensors: *AST*, *Web-Based* and *FEVOBOT*. Default sensor set is *FEVOBOT*.
- **Sensor Interface:** Select the interface on which device will communicate with the sensor.
For Sensor Type: *AST*
Sensor Interface options will be: RS-232 and USB
For Sensor Type- *Web-based*
Sensor Interface options will be: HTTP/S
For Sensor Type-*FEVOBOT*
Sensor Interface options will be: USB
- **Emissivity:** Set the emissivity parameter for Sensor. This parameter should only be visible when Sensor Type is *AST*. Default value is 0.95.
It is used to define accuracy in sensor to detect temperature of different skin or objects.
Not applicable for *FEVOBOT*.
- **Calibration Parameter:** Set the calibration parameter for the thermal sensor.
On click of + the value should increase by 0.1 and on click of – it should decrease by 0.1.
Not applicable for *FEVOBOT*.
- **Approach to Sensor Wait-Timer:** Time for which the device will wait for user to approach the device before starting Temperature Detection.
- **Temperature Detection Time-Out:** The timer till which temperature detection will be done for the user and if valid temperatures are not found till the expiry of timer then timeout will be declared.
- **Tolerance between consecutive readings:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature doesn't fall in tolerance range the reference temperature is updated with the current temperature and the process continues.
Not applicable for *FEVOBOT*.
- **Consecutive readings count within tolerance:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature doesn't fall in tolerance range the reference temperature is updated with the current temperature and the process continues.
Not applicable for *FEVOBOT*.
- **Minimum Temperature for Access:** The minimum temperature value that should be detected is to be considered as valid temperature.
It should be less than threshold temperature. If user tries to enter a value equal to or greater than threshold temperature validation should be shown.
The default value, unit and range should be updated based on the Temperature unit set on Panel.
- **Temperature Threshold:** To set the threshold value of the temperature. The default value, unit and range can be updated based on the Temperature unit set on Panel.
- **Restriction Type:** To set restriction type as soft/hard.
- **Bypass if Sensor Disconnected:** Enable this check-box to give provision of bypassing the feature if sensor connectivity is lost.

Alarms

In Alarm tab, you can assign below list of alarms to the door.

For Direct Door

Settings	Alarms	Timers
	Tamper	<input type="checkbox"/>
	Door Abnormal	<input type="checkbox"/>
	Door Force Open	<input type="checkbox"/>
	Door Fault	<input type="checkbox"/>
	Panic	<input type="checkbox"/>
	Temperature Threshold	<input type="checkbox"/>

Enable the respective check-box of alarms which is to be selected.

Timers

This section allows the configuration of various types of pre-defined device timers which can trigger off specific responses. In COSEC, timers are often used to control door behavior and for triggering alarms. The **Timers** page appears on your screen as shown below:

The screenshot shows the 'Device Configuration' window with the 'Timers' tab selected. On the left, a sidebar lists 'Profile', 'Enrollment', 'Advanced' (highlighted), 'Features', and 'Video Surveillance'. The main area shows four timer settings: 'Inter-Digit Wait Timer (Sec)' set to 3, 'Multi-Input Wait Timer (Sec)' set to 5, 'Door Open Pulse Timer (Sec)' set to 5, and 'Late-IN Early-OUT Active Timer (Min)' set to 60. A search bar at the top right says 'Search Device ID or Name'.

- **Inter-Digit Wait Timer (sec)** - Specify the time period in seconds between two key inputs on the device keypad. On expiry of this timer, the system considers the user input to be complete and is ready for the next input.
- **Multi-Input Wait Timer (sec)** - Specify the time in seconds for which system needs to wait for the second credential input from the user when more than one credential is to be used to grant access.



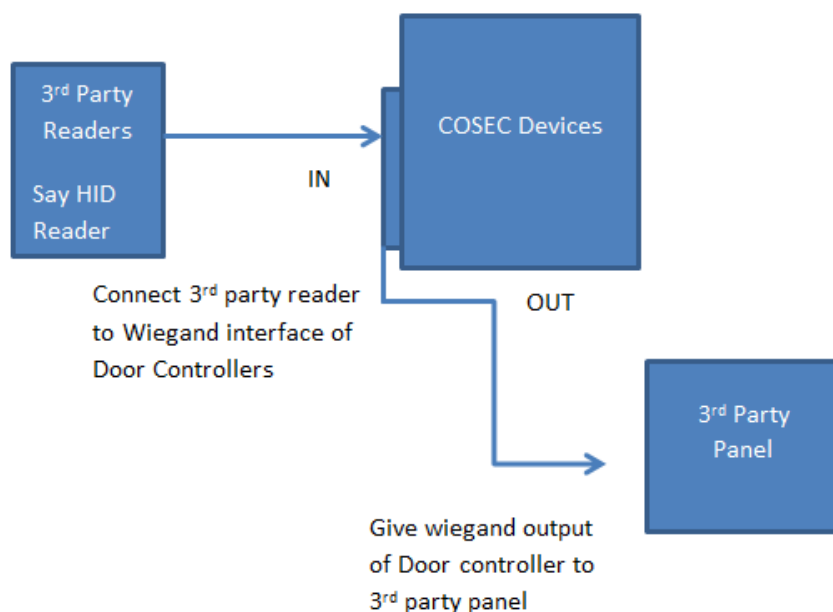
We recommend you to set the timer value as greater than or equal to 10 seconds to avoid access denial issues to users. This is applicable when the system reads the credentials (biometric) from the user's Smart Cards.

- **Door Open Pulse Timer (sec)** - Specify the time in seconds (3 to 99) for the door to be energized for a valid credential. If the opened door does not return to a closed state before the expiry of this timer, the door will generate a "Door Abnormal" alarm.
- **Late-IN Early-OUT Active Timer (min)** - Specify the time in minutes for which the Late-IN and Early-OUT special functions will remain active after being enabled at the Door Controller.

Wiegand

The screenshot shows the 'Device Configuration' window with the 'Wiegand' tab selected. The sidebar on the left is the same as in the Timers page. The main area shows 'Wiegand Interface' settings. Under 'Output Mode Parameters', there are four settings: 'Wait For Panel Signal' (checked), 'Signal Wait Timer (Sec)' set to 2, 'Wait For User Verification' (checked), and 'Wiegand Output Format' set to '26 Bit'. Below these, 'Send From' is set to 'MSB Bit'. A search bar at the top right says 'Search Device ID or Name'.

- **Wiegand Interface** - The COSEC device can be connected both as input devices (e.g. to receive data from a Wiegand Reader) or output devices (e.g. to support output to third party panel) via the Wiegand interface as shown below.

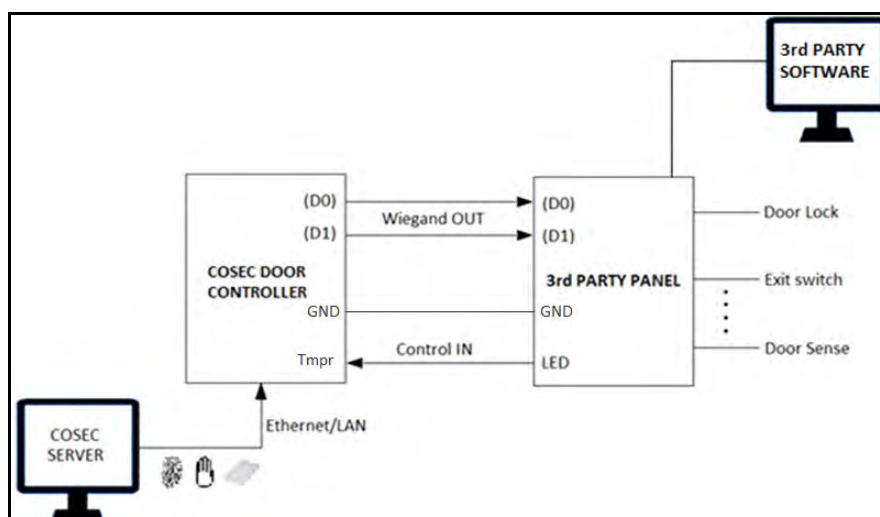


So select the interface of Door controller as **Output Mode** to work as weigand output to panel or **Reader Input** to take data from third party reader. If Reader Input option is selected, all the output mode parameters will be disabled.

If you select Output mode then configure the **Output Mode Parameters**.

- **Wait For Panel Signal** - If this option is enabled the door will wait for reply from the connected third party device before triggering any output, as per the defined **Signal Wait Timer (Sec)**.
- **Wait For User Verification** - If this option is enabled, user verification will be requested on the third party device before triggering any output.
- Specify the **Wiegand Output Format** and sending order for reader data as MSB or LSB Bit in the **Send From** field.

Wiegand Out Interface



Also for the **Custom** format, user can configure details of fields to be sent as output from the Wiegand reader that has been added.

Door Access using QR code

The user can access the COSEC device using COSEC APTA installed in the mobile device. If the user has rights for COSEC APTA and the access to the device is allowed for the user, then he can use his mobile device to scan the QR code which constitute the details of the COSEC door.

There is icon for QR code on COSEC APTA application. Clicking that icon will open the camera in your mobile. Now you can show the mobile camera to scan the QR code. The COSEC door will get opened after verifying the security key and access policies of the user.

Steps to create a QR code

Step 1: Enter details in JSON format

```
{"version":"x","ip": "x.x.x.x","port":"x","pdid":"x","mode":"x"}
```

Valid values:

Field	Field range	Default Value	Remark
version	1-255	1	
ip	0.0.0.0-255.255.255.255	0.0.0.0	
port	0-65535	0	
pdid	0-255	0	If door is in direct door mode then, then PDID will be 0 If door is in panel door mode then, PDID will have values from 1-255
mode	0,1	0	0= for entry mode 1=for exit mode



Note:

Step1a. If door is in direct door mode enter IP & port of the direct door

b. If door is a panel door, then enter IP & port of the panel door and in the pdid specify the door id which is to be accessed.

Step 2: Encrypt the JSON string using key "matrix12" with simple DES/ECB mode.

Step 3: Encode the encrypted string using Base 64.

Step 4: Use this string to generate QR code through any third party software.

Features

The Features tab allows the user to enable certain Access Control features for a device



The Features tab is available only with the Access Control Module license .

To access this, After selecting the device, Select **Device Configuration> Features**. The access control features for the device can be set from the following two sections:

- "Set1"
- "Set2"

Set1

This page allows the configuration of three rules - **Absentee Rule**, **Occupancy Control** and **Use Count Control**. The page appears as shown below.

The screenshot shows the 'Device Configuration' window for 'Set1'. On the left is a sidebar with a list of configuration categories: Profile, Enrollment, Advanced, Features (highlighted in blue), Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main panel displays the configuration for 'Set1' under the 'Features' tab. It contains three rule sections: 'Absentee Rule' with an 'Enable' checkbox checked and a 'Use Count Limit (Per minute)' of 9; 'Occupancy Control' with an 'Enable' checkbox checked, 'Maximum Occupancy Limit' of 9, 'Minimum Occupancy Limit' of 1, and 'Zero Occupancy' checked; and 'Use Count Control' with an 'Enable' checkbox checked and a 'Use Count Limit (Per minute)' of 5. A search bar at the top right says 'Search Device ID or Name'.

- **Absentee Rule** - Select this checkbox to enable this feature at the door. This rule sets the maximum number of days for non-use of a credential. On expiration of days limit, the user will be automatically blocked.
For configuring the rule *See Access Control> Absentee Rule*.
- **Occupancy Control** - Select this checkbox to enable the feature at the door and specify maximum number of users to be allowed within the controlled area after which a user exit is required to enable access to another user. Also specify the **Minimum Occupancy Limit** i.e. the minimum number of occupants the designated zone should have, and enable/disable the **Zero Occupancy** option to determine whether the designated zone should be allowed to be empty or not.
For configuring the rule *See Access Control> Occupancy Control*.
- **Use Count Control** - Select this checkbox to enable the feature at the door and specify the maximum number of uses per minute.
For configuring the rule *See Access Control> Use Count Control*.
You can enable **Duress Detection** on the door. The default duress detection code is displayed which is used to generate the duress alarm which informs that the user is forced to open the door under threat.
For details *See Device Configuration (Panel200)> Features> Set3> Duress Detection*.

Set2

This page allows the configuration of three rules - **First-IN User Rule**, **Anti-Pass-Back (APB)** and **2-Person Rule**. The page appears as shown below.

The screenshot shows the 'Device Configuration' window for 'Set2'. On the left is a sidebar with a device icon and a list of configuration categories: Profile, Enrollment, Advanced, Features (highlighted), Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main panel displays three rule configurations:

- First-IN User Rule:** Includes an 'Enable' checkbox (unchecked), 'Reset On' options (Day Change/Timer Expiry), 'Access Timer (Sec)' (3), and 'First-IN User Group' (1).
- Anti-Pass-Back (APB):** Includes 'On Entry' and 'On Exit' checkboxes (both checked), 'Hard/Soft' dropdown (Soft), 'Forgiveness' checkbox (checked), 'Reset After' radio buttons (Day Change/Timer Expiry, with Timer Expiry selected), and 'Forgiveness Timer (Mins)' (34).
- 2-Person Rule:** Includes an 'Enable' checkbox (unchecked), 'Mode' dropdown (Primary Must), 'Primary Group' (aaa), and 'Secondary Group' (None).

- **First-IN User Rule** -Select this checkbox to enable the feature at the direct door and select the First-In User group which would be valid at the door.
For configuring the rule See *Access Control> First- In User Rule> Assignment*

- **Anti-Pass Back (APB)** - Select this checkbox to enable the feature at the direct door.

On Entry: Check this box so that the system monitors the entry reader for APB violation.

On Exit: Check this box also so that the system monitors the entry as well as the exit readers for APB violations.

Hard/Soft: Select the restriction type as Hard or Soft option from the drop down options.

- **Hard APB:** The access will be denied if the exit is not registered first. It does not allow a second entry using the same card without an exit.
- **Soft APB:** The access will be granted even if the exit is not registered. It allows a second entry of the same user without an exit; however, an event and a warning are generated that indicates the second entry.

Forgiveness: Check this box to enable the system to reset the APB status. When forgiveness is enabled, then there will be following options to reset the pass.

1. **Reset After Day Change:** This will reset the APB status of all the users to NULL at midnight. This enables a user, who left the building in the evening without exit punch, to use his card for entry in the next morning.
 2. **Reset After Timer Expiry:** This will reset the APB status of all the users after the expiry of user defined time.
 - **Forgiveness Timer (Mins):** Enter the time duration in minutes after which Anti-pass back status will get reset and the pass will be in original state.
- **2-Person Rule** - Select this checkbox to enable the feature at the door and set the **wait time** in seconds after which the second person is allowed to punch on the door.
For configuring the rule See *Access Control> 2- Person Rule*

Video Surveillance

The Video Surveillance tab allows the user to configure parameters for video surveillance integration with the COSEC device.

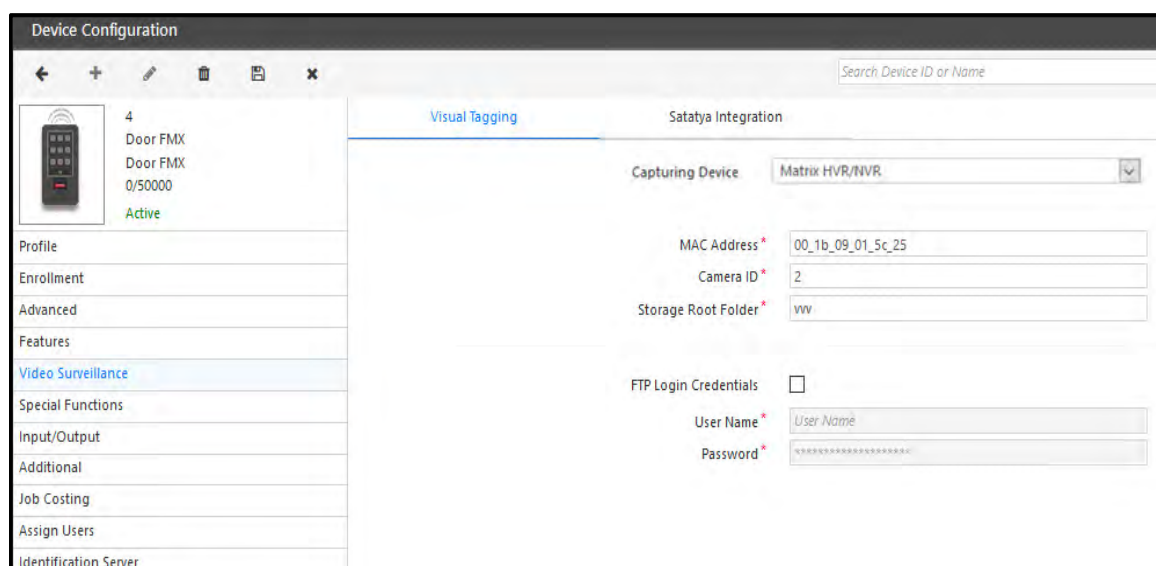
It is available in Basic License.

To access this, Go to **Device Configuration> Video Surveillance**.

- “Visual Tagging”
- “Satatya/IP Camera Integration”

Visual Tagging

The COSEC application can interface with some supported hybrid and network video recording systems as well as IP Cameras and grab images triggered by user events at the Doors. The **Visual Tagging** option enables the administrator to define the video recorder and IP Camera parameters. The **Visual Tagging** page appears as shown below.



To view the user events and related images, go to **Admin > Views/Logs > Event View**. To know more about viewing events, refer to “Event View”.

The following parameters are available for configuration:

- **Capturing Device** - Select the video recording device type from the dropdown menu as shown.

The compatible device types are:

- Matrix HVR/NVR
- Milestone
- IP Camera

Matrix HVR/NVR

- **MAC Address** - In the event of selecting the Matrix HVR/NVR, the administrator needs to specify the MAC address of the video recorder device using “_” (underscore) as the separator.

- **Camera ID** - Specify the camera number or camera ID for IP cameras. For analog cameras specify the camera number.
- **Storage Root Folder** - Specify the Root folder path or FTP Path where the uploaded images will be saved.

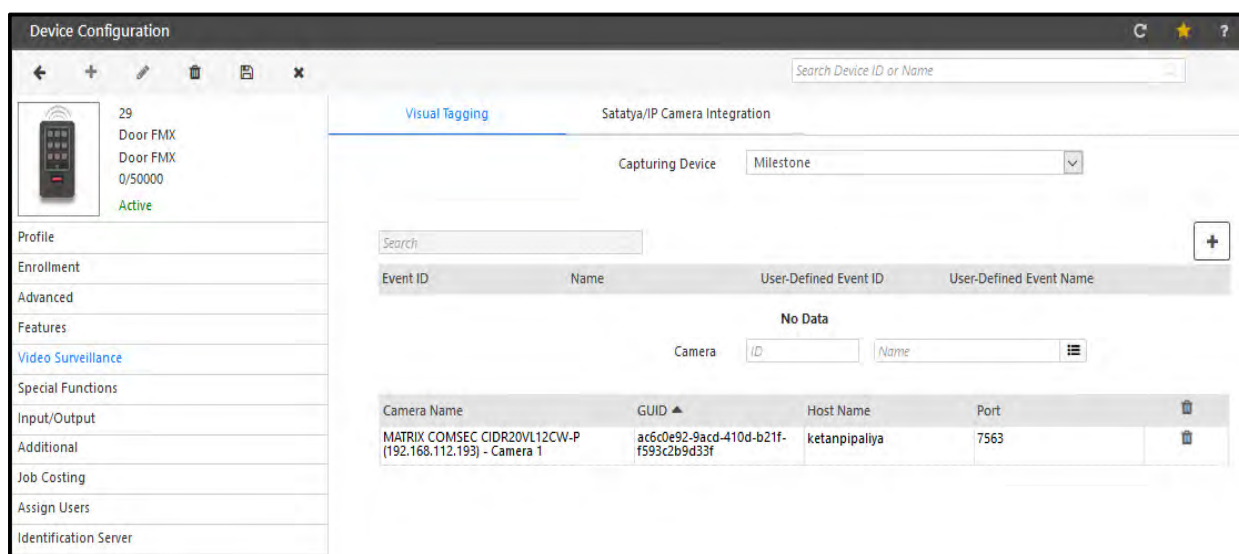


- **FTP Login Credentials** - Check this box to activate FTP login credentials for authentication.
- **Username** - Specify the FTP server username.
- **Password** - Specify the FTP server password.



Some COSEC devices do not support all the network connection options.

Milestone



*For more information on integration with **Milestone** devices, refer to [“Milestone Integration”](#).*

IP Camera

The screenshot shows the 'Device Configuration' window. On the left is a sidebar with a list of configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance (highlighted in blue), Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main area is titled 'Visual Tagging' and 'Satatya/IP Camera Integration'. It contains a 'Capturing Device' dropdown menu set to 'IP Camera'. Below this is a 'Snapshot URL' field with the value 'http://192.168.102.191/matrix-cgi/snapshot' and a note: 'Note: Mention the protocol http or https in URL.'. Under the 'API Login Credentials' section, there are fields for 'User Name' (set to 'admin') and 'Password' (masked with dots).

- **Snapshot URL:** If Capturing device is selected as IP Camera; then enter the API URL for taking the Snapshot through IP camera. You can use any camera for taking the snapshot/photo. The API for capturing snapshot will be available in the API document of camera.
- **User Name:** Enter the Username for accessing API for taking the Snapshot through IP Camera.
- **Password:** Enter the Password for accessing API for taking the Snapshot through IP Camera.



It is the same username and password using which IP camera login is done. Eg: username admin and password admin



The allowed values for snapshot URL, User Name and Password are **A-Z, a-z, 0-9 !"#%&'()*+,- . / : ; < = > ? @ [\] ^ _ ` { | } ~**

Satatya/IP Camera Integration

This functionality is available for configuration only when the Matrix HVR/NVR device type or IP Camera is selected as the **Capturing Device** (from *Visual Tagging*).

It enables the configured COSEC devices to directly send commands to the SATATYA HVR/NVR devices/ IP Camera as per the configuration on this page. The Satatya/IP Camera Integration page appears as shown below:



SATATYA Integration

Device Configuration

Search Device ID or Name

Visual Tagging | **Satatya/IP Camera Integration**

Integration type: **Network**

Active: ☒

IP Address: 192 . 168 . 104 . 37

Port Number: 8000

Name: FMXNVR integration

Active: ☒

Schedule: 14:00 to 19:00

Days: ☐ Sun ☒ Mon ☒ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Holiday

Event: Access Allowed

Mode: Entry

Action: Recording

Duration Min: 10

Camera: ☐ 1 ☒ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 22 ☐ 23 ☐ 24

Add Cancel

- **Integration type**- Select the integration type from the options of Wired and Network.
In wired integration, door is physically connected with Satatya Device. In Network integration, connection can be by ethernet, wireless or broadband depending upon the COSEC device support.
- **Active**- Check the box to activate the connection.
- **IP Address**- Specify the IP address of HVR/NVR.
- **Port Number**- Specify the port number of HVR/NVR.
- **Name**-Specify a user friendly name for the integration function.
- **Active**- Check the Active box to enable the SATATYA integration functionality.
- **Schedule** - Specify a schedule for the function by specifying the start and the end time (24 Hours format) as well as checking the boxes against the applicable **days** of the week.

- **Event-** Select a COSEC event from the drop down list for which the resultant action is to be configured.
- **Mode-** Select the event mode from the options of Entry, Exit and Both from the drop down list wherever applicable.
- **Action-** Select the action for the Satatya device from the drop down list. The options available are:
 - Recording - Specify the duration in minutes.
 - Upload Image - This will be uploaded as per the ftp settings.
 - Video Pop-up - Specify the duration in seconds. The video pop up will be generated on the local client of Satatya device on the selected camera.
 - PTZ Preset - Specify the PTZ position number as defined on the SATATYA device.
 - Mail Image - Specify the email-ID.
- **Camera-** Select the relevant camera channels depending on the action selected.
- Click the **Add** button to finish the process of linking the event to the action.

Name	Event	Action	Start Time	End Time	Active	
FMXNVR integration	Access Allowed	Recording	14:00	19:00	Yes	

- The user may now configure another event-action linkage if required.

Example1: For action as Video Pop up, the pop up of Camera 24 will be shown for 10 seconds.

Example2: For Access allowed event on COSEC Device, recording of camera channel 4,6,8 and 10 will be done for 10 seconds.

Event: Access Allowed

Mode: Both

Action: Video Pop-Up

Duration Sec. *: 10

Camera *: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10
☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15
☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20
☐ 21 ☐ 22 ☐ 23 ☒ 24

Event: Access Allowed

Mode: Both

Action: Recording

Duration Min. *: 10

Camera *: ☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5
☒ 6 ☐ 7 ☒ 8 ☐ 9 ☒ 10
☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15
☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20
☐ 21 ☐ 22 ☐ 23 ☐ 24

Add Cancel

IP Camera Integration

- **Schedule Name**-Specify a user friendly name for the schedule of Device-IP Camera integration.
- **Active**- Check the Active box to activate the schedule for IP Camera.
- **Event**- Select a COSEC event from the drop down list for which the resultant action is to be configured. The Events will appear in the list based on the availability of the license.



At max. 20 Events or schedules are allowed for configuration for a single device.

- **Mode**- Select the event mode from the options of Entry, Exit and Both from the drop down list.
- **Schedule Range**- Specify a schedule for the function by specifying the **start** and the **end time (24 Hours format)** as well as checking the boxes against the applicable **days** of the week.

Click **Add** button to add the configured schedule. The schedule will be listed in the grid. Then click **Save** button to save the schedule integration.

Name	Event	Mode	Start Time	End Time	
Denied User Schedule	User Denied	Both	00:00	23:59	

When user event is generated, then snapshot is taken by the configured camera. The events can be viewed in User Events (User module) page and Event view (Admin module) page.

The capturing of Snapshot is shown in Door FMX section.


Special Functions

To configure *Special Functions* for COSEC doors, refer to [“Special Functions”](#).

Input/Output

The Input/Output (I/O) configuration of a system determines how the output or response of a system is influenced by the input applied on it. In case of the COSEC Access Control System, the I/O configuration should enable the system to monitor and trigger a specific response to any changes in door state or event occurrences at the door device. This change of door state or occurrence of events may be considered as an input while the response or action that is generated by the system on detection of this input, may be defined as the output.



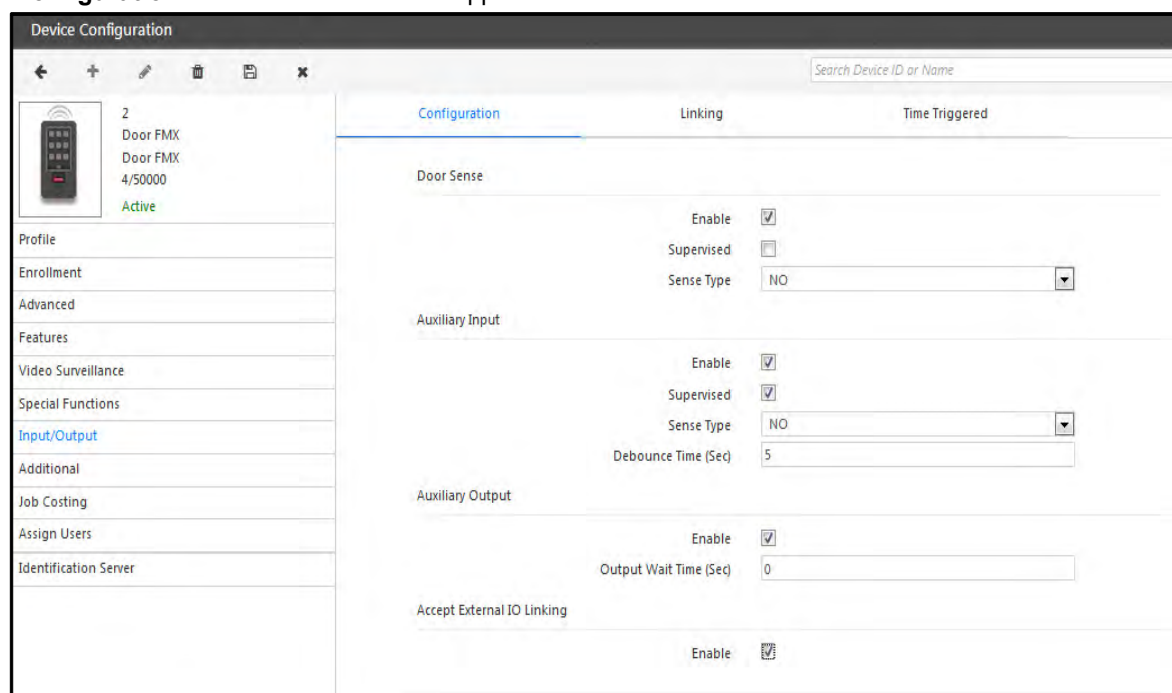
1. This functionality cannot be fully accessed in the Edit  mode for a selected device.
2. This functionality is available only with the Access Control add-on module license.

To access this, After selecting the device, Select **Device Configuration> Input Output**. The Input Output parameters can be set from the following sections:

- [“Configuration”](#)
- [“Linking”](#)
- [“Time Triggered”](#)

Configuration

The **Configuration** section for a Door FMX appears as shown below.



Section	Enable	Supervised	Sense Type	Debounce Time (Sec)	Output Wait Time (Sec)
Door Sense	<input checked="" type="checkbox"/>	<input type="checkbox"/>	NO		
Auxiliary Input	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	NO	5	
Auxiliary Output	<input checked="" type="checkbox"/>				0

Accept External IO Linking

Enable ☒

The following parameters are available for configuration:

- **Door Sense** - The system by default can sense two states of a door - *Normally Open (NO)* and *Normally Closed (NC)* depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a *Door Abnormal* alarm.

Select the **Enable** checkbox to enable the system for such two-state monitoring.

Select the **Supervised** checkbox to enable the door for four-state monitoring where the door is also monitored for *door fault* and *door disconnection*. Specify the **Sense Type** as **NC** or **NO** (Default: NC).

- **Auxiliary Input** - Select the **Enable** checkbox option for Auxiliary Input (e.g. Smoke Detectors) depending on normal or supervised door state monitoring as described above.

Debounce Time (Sec) - Specify the Debounce time in seconds. Default value is 3 sec and range should be 0-99 sec. It defines the minimum time for which an input interface must be maintained in a given state before the system reports it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.

- **Auxiliary Output** - Select the **Enable** checkbox to enable Auxiliary Output (e.g. Fire Alarm) for the selected device. To set an additional waiting period before the Aux Output signal is sent, enter an **Output Wait Time (Sec)**.

- **Relay Output**

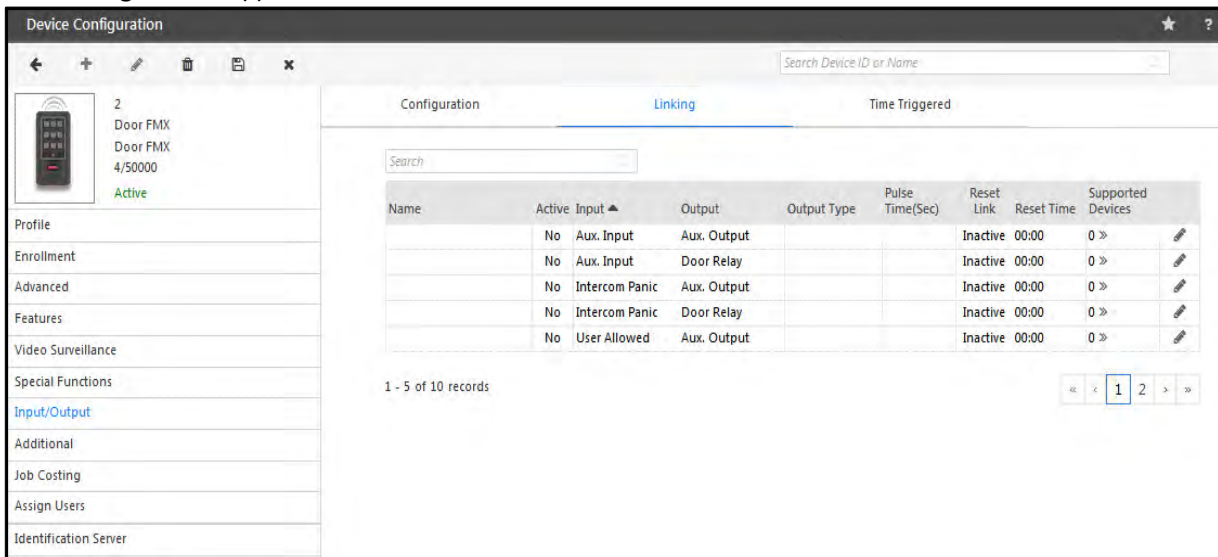
Output Group Number (Door Unlock)- Select the Output Group Number to which the device output for Door Unlock is to be assigned from the picklist.

Output Group Number (Door Lock)- Select the Output Group Number to which the device output for Door Lock is to be assigned from the picklist.

- **Accept External IO Linking** - Select the Enable checkbox to enable device-to-device IO Linking i.e. input from one Direct Door can trigger output in another Direct Door.

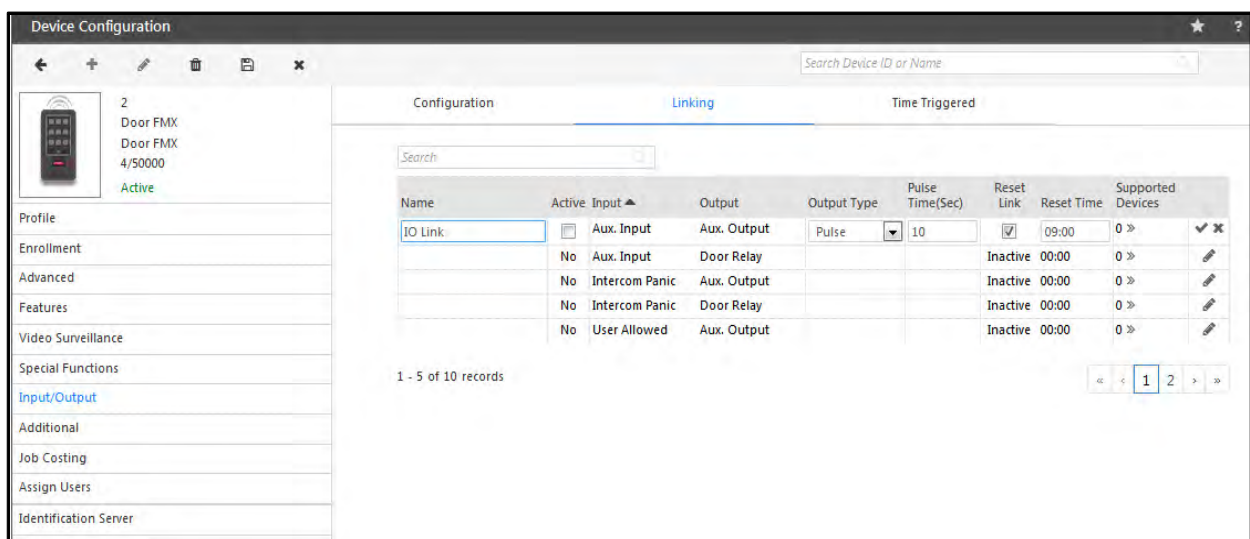
Linking

The **Linking** section appears as shown below.



The COSEC application supports the Input/Output Linking feature to activate an output port based on a trigger received from an input port on the same Direct Door. This option enables the administrator to define how an event or events (input port) will trigger an output on the selected door.

Select a Input-Output linking row or click edit button.



- **Name** - Specify a name for the new I/O linking program to be defined.
- **Active** - Select this checkbox to activate this linking program.
- **Output Type** - Specify the appropriate type of output from the following four options available in the drop down list:
 - **Pulse**: With this type of output, the user needs to define the Pulse time in seconds.
 - **Interlock**: With this option, the output follows the input. The relay output is triggered as long as the input is activated after which it returns to normal state.

- **Latch:** With this option, it is denoted that the relay output will be in an energized condition for infinite period and needs to be reset manually.
- **Toggle:** With this option, the output group toggles its state whenever an input group is activated.
- **Pulse Time (sec)** - For a *Pulse* output type, specify the pulse duration in seconds.
- **Reset Link-** Enable the Reset link and enter the time at which the IO link will get reset automatically.
- **Supported Devices** - All devices supported for external IO Linking will appear in this picklist for selection. Upto 255 external devices can be added by the administrator.
- Click the **OK** button and **Save** the configuration.

Time Triggered

On the **Input Output** page, select the **Time Triggered** section as shown.

Function Name	Active	Time	Duration(Sec)	Days	Output
Siren Activate	<input checked="" type="checkbox"/>	00:00	10	Select	Aux O/P

This functionality enables the user to control the activity of an Output without manual intervention. The time triggered functions are used for activating events like door unlock and siren activation that are set as per the start time and for the configured time duration. This functionality is designed to energize outputs for predefined periods at the configured time. The COSEC access control system supports up to 20 Time Triggered functions on a Direct Door.

Function Name	Active	Time	Duration(Sec)	Days	Output
Siren Activate	Yes	00:00	10	Su Mo Tu We Th Fr Sa Ph	Aux O/P

Additional

This section lists some additional configurations that can be enabled for door controllers.

To access these configurations, Go to **Device Configuration > Additional > Daylight Saving**



This section is available only for Direct Doors.

Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. COSEC doors can be configured to be compatible with this procedure keeping the RTC of the system updated with such changes.

The **Daylight Saving** configuration can be done in 2 ways i.e. Day-Month wise or Date-Month wise.

- Select the **DST Type** as Day-Month wise or Date-Month wise. The **Disable** option when selected, disables the application of DST on the system time.
- On selection of the **Day-Month wise** option, the DST is set by the day of the month on which clock needs to be forwarded and reverted back to normal. Set the month, week number, day of the week, and time for both the **Forward Clock** and **Backward Clock** as shown.

The screenshot shows the 'Device Configuration' window with the 'Additional' tab selected. Under 'Daylight Saving', the 'DST Type' is set to 'Day-Month wise'. The 'Time Period' is set to '08:00'. The 'Forward Clock' section is configured with Month: November, Week No.: 1st, Day of Week: Sunday, and Time: 09:00. The 'Backward Clock' section is configured with Month: January, Week No.: 1st, Day of Week: Sunday, and Time: 10:00. A 'Save' button is located at the bottom right of the configuration area.

- On selection of the **Date-Month wise** option, the DST is set by date of the month on which clock needs to be forwarded and reverted back to normal. Define the **Time Period** for the date-month wise DST settings in **24-hours** format, and specify the day of the week, date and time for the **Forward Clock** and the **Backward Clock** as shown.

This DST Setting implies that on 1st Sunday of November at 09:00 hours, the clock will be forwarded by 08:00 hours. And on 1st Sunday of January at 10:00 hours, the clock will be reversed by 08:00 hours.

The screenshot shows the 'Device Configuration' window for a device named '2 Door FMX 4/50000'. The 'Daylight Saving' tab is selected. The 'DST Type' is set to 'Date-Month wise' and the 'Time Period' is '08:00'. Under 'Forward Clock', the 'Month' is 'November', 'Date' is '1', and 'Time' is '09:00'. Under 'Backward Clock', the 'Month' is 'January', 'Date' is '1', and 'Time' is '10:00'. A 'Save' button is at the bottom right.

- Click the **Save** button.

Job Costing

When user punches on any device, there will be an option to select the Job Code on which the user is working. Job Costing enables the admin to show or hide Job Code selection on device.

To access these configurations, select the **Job Costing** tab.

The screenshot shows the 'Device Configuration' window for the same device, with the 'Job Costing' tab selected. The 'Show Job Menu' is set to 'Show List'. The 'Assign Jobs' section has a 'Retain Job Selection' checkbox. Below this, there are fields for 'Job Group' (set to '1') and 'RnD Job'. A table lists assigned jobs:

Job Code	Name	Assignment Start	Assignment End
PSD-W	PSD Writing	08/05/2017	30/06/2017

Show Job Menu: Select **Show List** so that multiple jobs can be assigned to the device. Select **Allocate Default** so that only default jobs can be assigned on the device.

The user can select the relevant job code while punching on the device. His job hours will be recorded for that job code.

- **Retain Job Selection:** Select this checkbox to retain the job code selected by a user which would be applicable for all the subsequent users until another job selection is done on device.

Assign Jobs: Select the Job group and multiple jobs from the picklist.
Then click on **Save** button. The jobs will be listed to the grid.



The maximum limit for job assignment is 1000 on each device



Job codes will be available for selection on the door when the user punches on the door.

Assign Users

To the configured device, you can select and assign the users.

Click the picklist button and select the users.

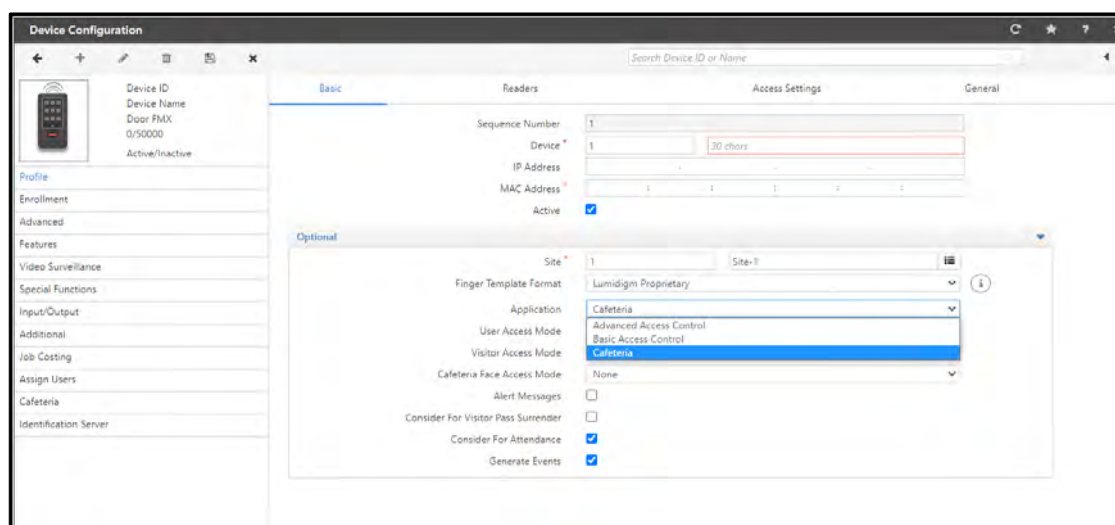
ID	Name	
1	Shalini	
101	Khushbu	
2	Chirag	
3	Isha	

Click the **Save** button to assign all the added users to the selected door.

Cafeteria

The COSEC system enables the you to configure devices which will be used by the Cafeteria management module.

To configure a door for Cafeteria application, make sure you have selected **Cafeteria** option in **Application** (Device Profile > Basic > Application) as shown below.



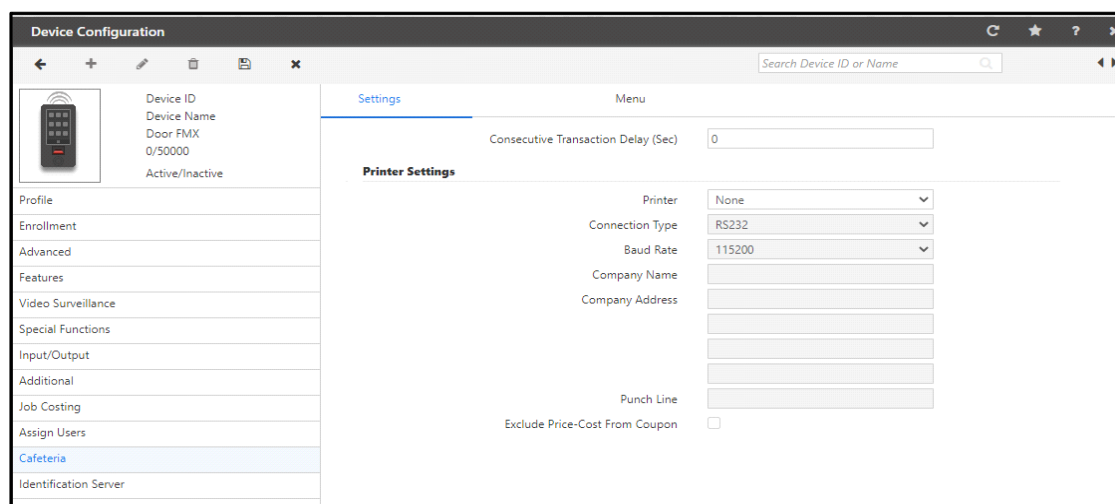
On the **Device Configuration** page, click **Cafeteria** on the left pane.

For the Cafeteria configurations, click the following links

- [“Settings”](#)
- [“Menu”](#)

Settings

The Cafeteria configuration for Door FMX is shown as below



- **Consecutive Transaction Delay (Sec):** Enter the time interval between two transactions, wherein any user transaction would be restricted.

Printer Settings

- **Printer:** Select the printer from the dropdown list based on the site requirements.
- **Connection Type:** Select the printer connection type from the drop down list. The options available are:
 - RS232 (serial)
 - USB
- **Baud Rate:** In the event of a serial printer, select the appropriate baud rate from the drop down list.
- Specify the **Company Name**, **Company Address** and the **Punch Line** as per the site requirements. These details will be printed on the receipt dispensed from the selected printer.
- Select the **Exclude Price-Cost From Coupon** check box if you want to exclude the price from the coupon.

Menu

COSEC allows the administrator to assign one or more cafeteria menus (Menu 1, Menu 2, Menu 3... upto 99.) to a device. These can be configured by selecting pre-defined menus from the Menu picklist.



The Menu is created from Cafeteria module.

The Menu can be scheduled from Cafeteria module and is displayed in “Schedule Menus” as shown above.

If you have to assign another menu and schedule it on the door then select the Menu from the picklist. The Menu will be shown in the grid as shown below.

Menu No	ID	Menu Name
1	1	Menu 1
2	2	Menu 2

Menu No	ID	Menu Name	Start Time	End Time	Schedule Days
1	1	Menu 1	12:00	15:00	Mo Tu We Th Fr Sa

Now to schedule the menu click **Add** button as shown above.

Then select the menu to be scheduled from the **ID** picklist. Specify the **Start** and **End time** for which the Menu will be active and is available to users on the selected door. Select the **days** for which this menu will be available i.e. scheduled on the door.

Then click **OK** and **Save** the Menu schedule on the door.



Two Menus cannot be scheduled for same timing.

Identification Server

This tab enables the selected device to be assigned to a pre-defined Identification Server.

Device has a limited memory capacity for storage of templates so we need Identification Server which will store the more number of templates and respond to device when asked for identification.

For more information on Identification Servers, See *Admin> System Configuration> Identification Server Configuration*.

To access these configurations,

- On the **Device Configuration** page, select the **Identification Server** tab.

Face Recognition

The screenshot displays the 'Device Configuration' web application. On the left is a sidebar with a list of configuration tabs: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server (which is highlighted in blue). The main area shows the 'Settings' for the selected device, with the 'Face Recognition' sub-tab active. The settings include: 'Enable FR' (checked), 'Face Capturing' (set to 'Tap & Go'), 'Enable Time Out' (unchecked), 'Free Scan Time Out (Sec)' (set to 30), 'IP Camera MJPEG URL' (http://192.168.1.126/matrix-cgi/mjpeg?profile-no=4), 'User Name' (Username), 'Password' (masked), 'FR Mode' (set to Local), 'Server Address' (192.168.50.2), 'Server Port' (12000), and 'Identification Time-Out Duration (Sec)' (4). A note below the URL field states: 'Note: Mention the protocol in URL.'

- **Enable FR:** Select the checkbox to enable the Face Recognition feature on the device.
- **Face Capturing:** Select the desired Face Capturing option — Tap & Go or Free Scan.
 - **Tap and Go:** If you select this option, user needs to tap on the device screen once. The MJPEG, that is motion recording screen appears. The device will capture and then identify the users face. If during working hours device is idle, then user needs to tap device to scan the face and gain access.
 - **Free Scan:** If you select this option, device will display the MJPEG, that is motion recording screen till the expiry of the Free Scan Time Out timer.

- **Enable Time Out:** Select this checkbox to enable the time out.
- **Free Scan Time Out (Sec):** Enter the free scan time out duration. The valid range is 1 to 999 sec.

In Free Scan method, multiple users can mark their attendance easily during peak entry hours.

For example, if the Free Scan Time Out is set as 30sec and if the user is identified in 10S then the system reloads the Free Scan Time Out timer again. Hence, device remains in the scanning mode.

- **IP Camera MJPEG URL:** Enter the URL for accessing the IP camera to receive the motion stream. For example: `http://192.168.104.48:80/matrix-cgi/mjpeg?profile-no=3`
 - **User Name:** Enter the user name for accessing the IP camera. For eg: admin
 - **Password:** Enter the password for accessing the camera. For eg: admin123

This will fetch the motion stream from camera to device screen. Then the users can show their face on camera. The face will be captured and after identification, the user will be allowed to access the door and punch will be marked.

- **FR Mode:** Select the FR mode as **Local** or **Server Assisted**.
 - **Local:** In this Local mode face templates will be stored in FR hardware module which can store 1 Lakh face templates. The captured face template will be verified with the templates already stored in FR module.
 - **Server Assisted:** In Server Assisted mode, the face templates will be stored directly in the server. You must first configure the Identification Server from where the face templates will be identified.
 - **Free Scan Time Out (Sec):** Enter the Free scan time out duration. The valid range is 1 to 999 sec.

When **FR Mode** is set as Local Mode, configure the following parameters:

- **Server Address/Port:** Enter the IP Address and Port number of the FR Server.
- **Identification Time-Out Duration (Sec):** Enter the identification time-out in seconds, after which the face template identification process will be timed out.

Example: If **Identification Time-Out Duration (Sec)** is 5 seconds, then the identification server will try to identify the face template until 5 seconds and if not found then it will show time-out to the user.

If you select FR Mode as **Server Assisted**, you must configure the following parameters

Settings

Face Recognition

Enable FR	<input checked="" type="checkbox"/>
Face Capturing	Free Scan
Enable Time Out	<input checked="" type="checkbox"/>
Free Scan Time Out (Sec) *	30
IP Camera MJPEG URL *	http://192.168.1.126/matrix-cgi/mjpeg?profile-no=4
	Note: Mention the protocol in URL.
User Name *	Username
Password *	*****
FR Mode	Server Assisted
Identification Server	1 Identification - 000000000000
Configure Alternate Server Address	<input type="checkbox"/>
Server Address	192.168.103.66
Server Port	11005
Identification Time-Out Duration (Sec)	4
Default Biometric Group No.	0

- **Identification Server:** Select an Identification Server using the picklist button to which the device is to be assigned. The configuration of server is done from **Admin module > System Configuration > Identification Server Configuration** and the Identification Service must be started from the service tray.
 - **Server Address:** It displays the IP Address of the selected Identification Server.
 - **Configure Alternate Server Address:** Select this checkbox to configure external IP address of Identification Server.
 - **Server Address:** Enter the external network IP address which will be used for accessing identification server.
 - **Server Port:** Enter the TCP port number. The default port number is 11005.
 - **Identification Time-Out Duration (Sec):** Enter the duration in seconds after which the fingerprint template identification will get time out.
- Example:** If 5 seconds is specified, then the identification server will try to identify the template till 5 seconds and if not found then it will show time-out to the user.
- **Default Biometric Group No.:** Enter the default biometric group number to be assigned to the device. It is a number allotted to a device to be assigned to the Identification Server. This enables the Identification Server to match the template against only those devices that belong to the corresponding biometric group. This reduces the false detection as well time to search template.

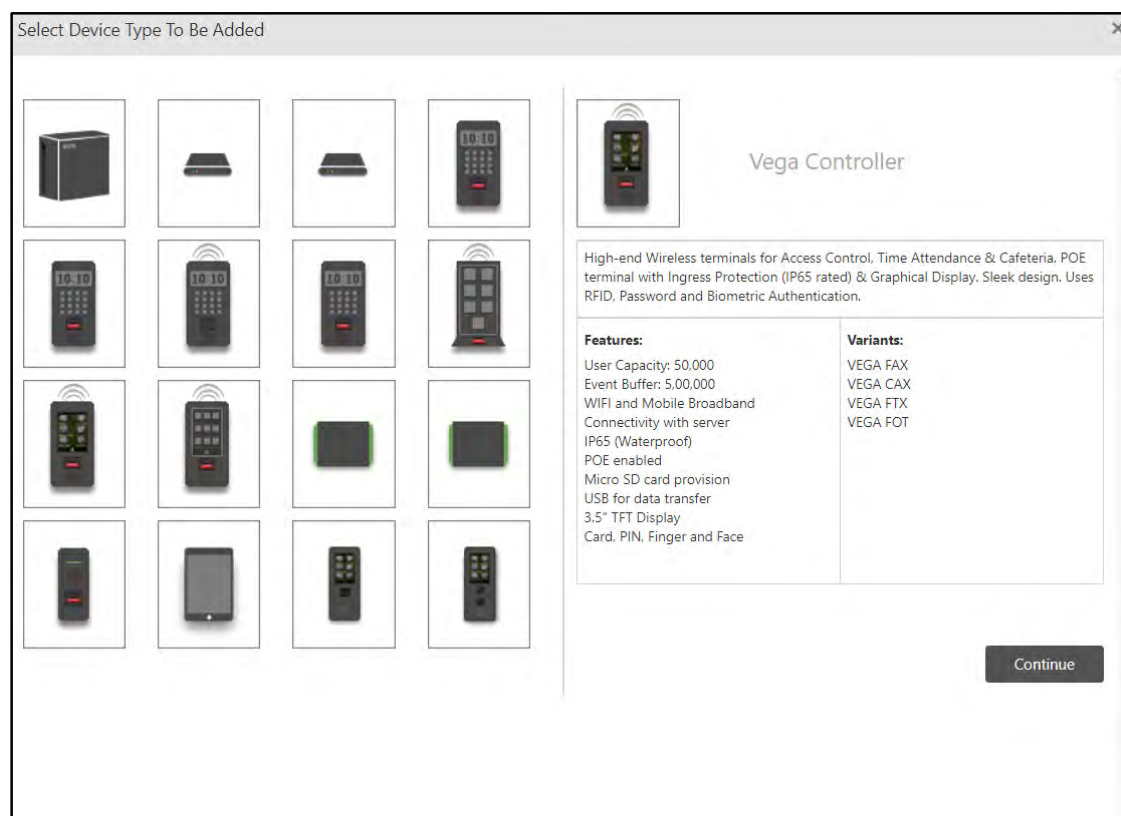
VEGA Door

VEGA series door controllers are engineered with careful blend of aesthetics, size, connectivity, reliability, and ease of use for modern enterprises. The VEGA devices are a perfect fit for Access Control and Time-Attendance solution required by modern organizations.

VEGA Door can be connected as **Direct Door** as well as **Panel Door**.



Click the Vaga Controller device from the Device List to add it as a **Direct Door**.



OR

Click Panel Door to add VEGA Controller device as a **Panel Door**.

Select Device Type To Be Added

Panel Door

Various Controllers can be configured as Panel doors with the defined panels (Master Controllers).

Features:	Variants:
Door V1 Door V2 Path Controller Vega Controller PVR Door ARC DC 100 Door V3 ARC IO 800 ARC DC 200 ARGO Door V4 Path V2 ARGO FACE	All supported door variants can be configured as Panel Doors

Panel: B_Panel200-Device-3

Door Type: Vega Controller

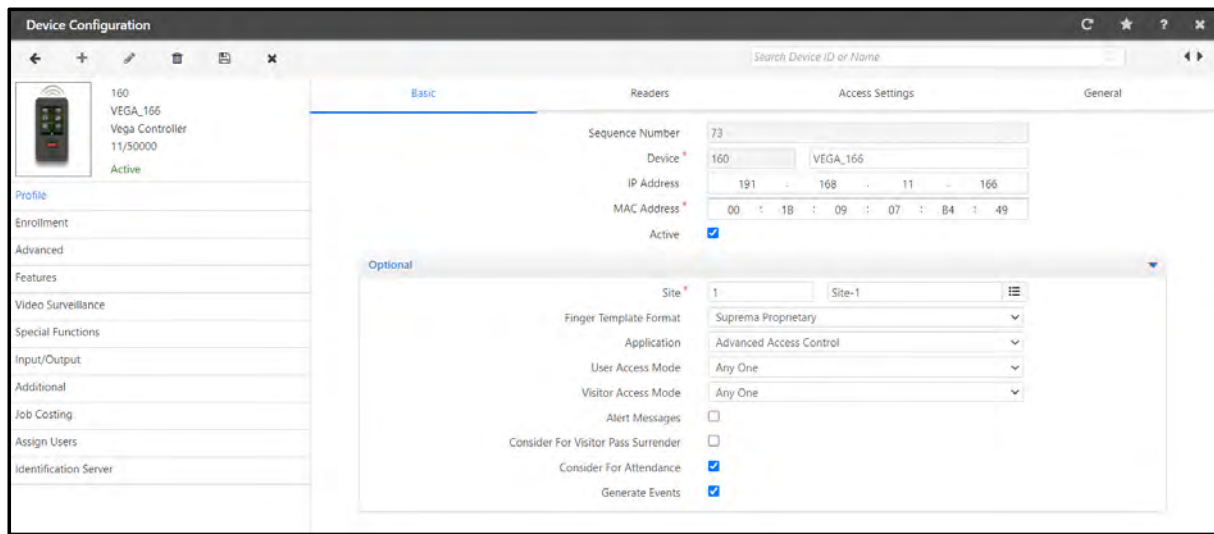
Continue

Panel: Select the desired Panel from the drop-down list with which you wish to connect the Door.

Door Type: Select **Vega Controller** from the drop-down list.

Click **Continue**.

The **Device Configuration** page for VEGA Controller appears.



If you wish to add devices automatically, click **Admin Module > System Configuration > Global Policy > Device**. Select the **Auto Add New Devices** check box. Once the device is connected in the network, it comes online in the COSEC Monitor.

The IP Address of the device will be displayed automatically in **Profile > Basic**.



While adding devices to the COSEC Server, makes sure the Monitor Service is running.

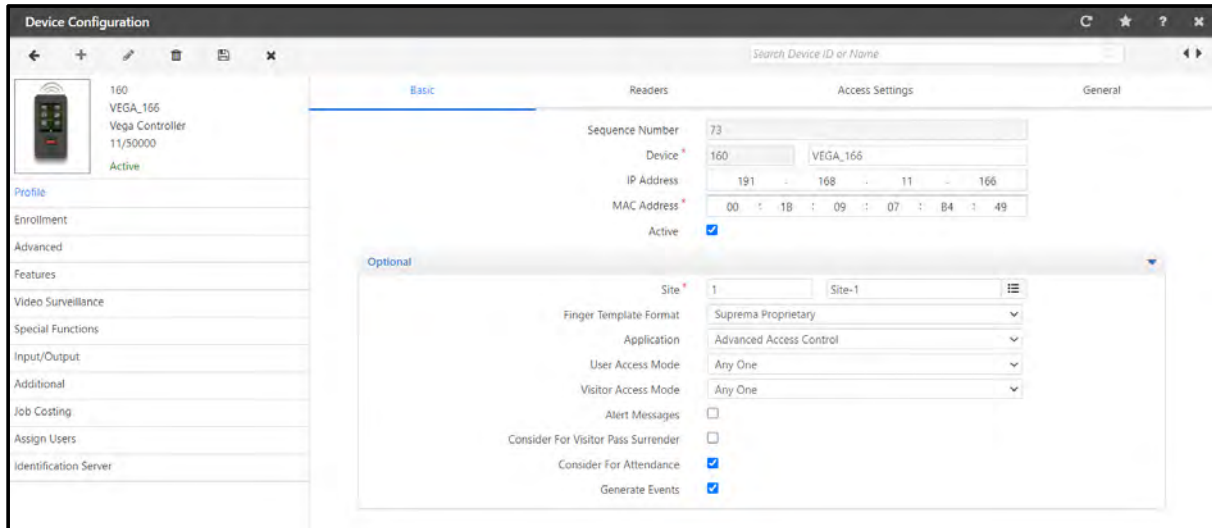
To configure the device parameters, click the following links:

- [“Profile”](#)
- [“Enrollment”](#)
- [“Advanced”](#)
- [“Features”](#)
- [“Video Surveillance”](#)
- [“Special Functions”](#)
- [“Input/Output”](#)
- [“Additional”](#)
- [“Job Costing”](#)
- [“Assign Users”](#)
- [“Cafeteria”](#)
- [“Identification Server”](#)

Profile

Setting up a door profile involves configuring basic parameters to set up any door controller device. This section enables the user to set up the basic profile for any new device.

To do so, on the **Device Configuration** page, click the **Profile** tab in the left pane.



To configure the Profile parameters click the following links:

- [“Basic”](#)
- [“Readers”](#)
- [“Access Settings”](#)
- [“General”](#)

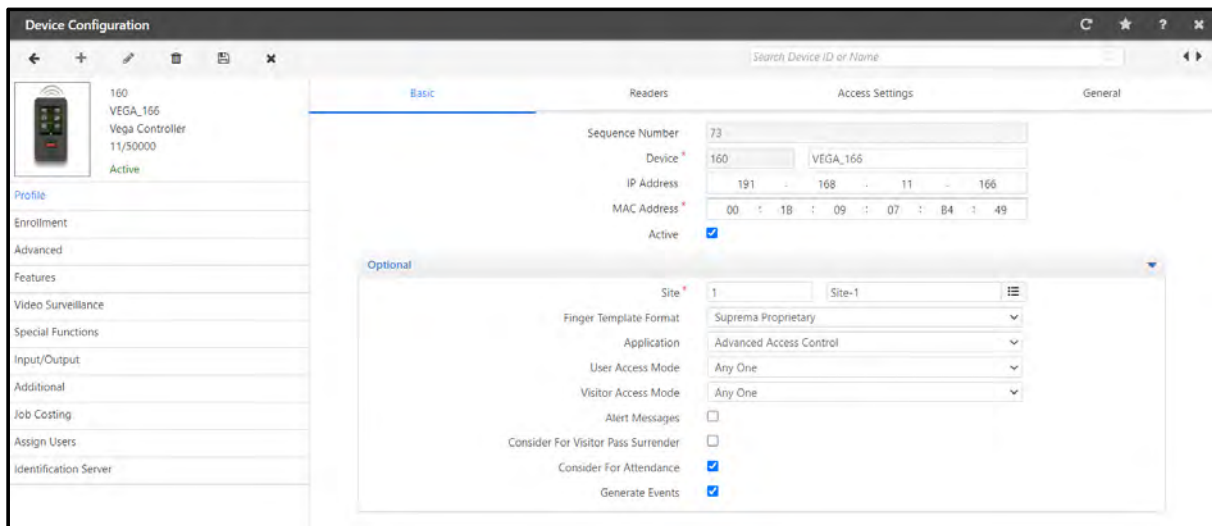
Basic

Click **Basic** tab. The **Basic** page appears.



Sequence Number, Device, IP Address, MAC Address and Active are applicable for both Direct Door and Panel Door.

For VEGA Door as a Direct Door,



Configure the following parameters:

- **Sequence Number:** This is a system generated sequence number for each new device.
- **Device:** Specify a name that can be assigned to the door. The Door ID is auto-generated by the system.
- **IP Address:** This is the IP Address assigned to the door. Once the device connection is established with the Server, this field will automatically displays the door IP address.
- **MAC Address:** Specify the MAC Address of the door.



MAC address of door is required while manually adding the door to the COSEC Monitor. You can note-down the MAC address from the device when it is powered on.

- **Active:** Select this check box to activate the device in the network.



*To add the Device automatically, click **Admin Module > System Configuration > Global Policy> Device**. Select the **Auto Add New Devices** check box.*

*The device will be added automatically but make sure you enable the **Active** check box in order to connect the device to the network. Once the device is connected to the network, it will come online in COSEC Monitor.*

Click the **Optional** collapsible tab, to configure the following parameters:

- **Site:** Click the picklist and select the site to which this door is to be assigned. Site is created from **Devices > Masters > Site**.
- **Finger Template Format:** Select the format according to which Finger Templates will be enrolled from the drop-down list— **Suprema Proprietary, Suprema ISO**. You can set the Finger Template Format globally from **System Configuration > Global Policy > Device > Suprema Finger Template Format**.
- **Application:** Select the type of application for which the device is to be used from the drop-down list— **Basic Access Control, Advanced Access Control or Cafeteria**. All devices set to **Cafeteria** will subsequently be available for Cafeteria configuration. Make sure you configure **Cafeteria Face Access Mode**.

- **User/ Visitor Access Mode:** This defines the type and combination of credentials required to identify and validate a user at the Door Controller. Select the appropriate credential combination from the drop-down list:
 - Any one
 - Card
 - Card + PIN
 - Card + Biometrics
 - Card + Biometrics + PIN
 - Biometrics
 - Biometrics + PIN
 - Biometrics + Group
 - Biometrics then Card
 - Card then Biometrics
 - None
 - Face
 - Card + Face
 - PIN + Face
 - Biometrics + Face
- **Cafeteria Face Access Mode:** If you have selected **Cafeteria** as the **Application**, select the desired **Cafeteria Face Access Mode** type from the drop-down list— **None**, **Default Item**, **Item Selection**.

Default Item mode in Cafeteria will allow users a touchless cafeteria experience. In Default Item mode only the transaction for default item is allowed. A default item is assigned in each scheduled menu.

Item Selection mode in Cafeteria will allow users to select the desired menu items and allow a transaction using Face as a credential.
- **Alert Messages:** Select this check box to enable the application to send alerts based on events from this door.
- **Consider for Visitor Pass Surrender:** Select this check box to consider the this door for Visitor Pass Surrender. The Visitors can show their credentials on this device to surrender their passes.
- **Consider for Attendance:** Select this check box if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as Access Control events.
- **Generate Events:** This check box is selected by default. Click to disable, if the server is not required to receive any events from this device.

For VEGA Door as a **Panel Door**.

The screenshot shows the 'Device Configuration' window for a 'dummy vega panel'. The 'Basic' tab is selected, displaying fields for 'Sequence Number' (77), 'Device' (11), 'IP Address' (111.111.10.111), and 'MAC Address' (AA:BB:AA:AA:EE:BA). An 'Optional' section is visible but collapsed. The left sidebar shows a list of devices, with '11 dummy vega pa...' selected. The bottom of the sidebar has links for 'Profile', 'Advanced', 'Video Surveillance', 'Input/Output', and 'Assign Users'.

Click the **Optional** collapsible panel, to configure the parameters:

- **Site:** Click the picklist and select the site to which this door is to be assigned. Site is created from **Devices > Masters > Site**.
- **Consider for Attendance:** Select this check box if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as Access Control events.
- **Alert Messages:** Select this check box to enable the application to send alerts based on events from this door.
- **Access Zone:** Select the desired Access Zone to be assigned to the door from the drop-down list.
- **Access Cluster:** Select the desired Access Cluster to be assigned to the door from the drop-down list.
- **Door Group:** The Door Group drop-down includes the list of all configured Door Groups on the corresponding Panel. By Default, None is selected.
- **Auto IP Assignment:** There is an option where the panel door can be assigned its IP from the device webpage. To enable this option, select the Auto IP Assignment check box.

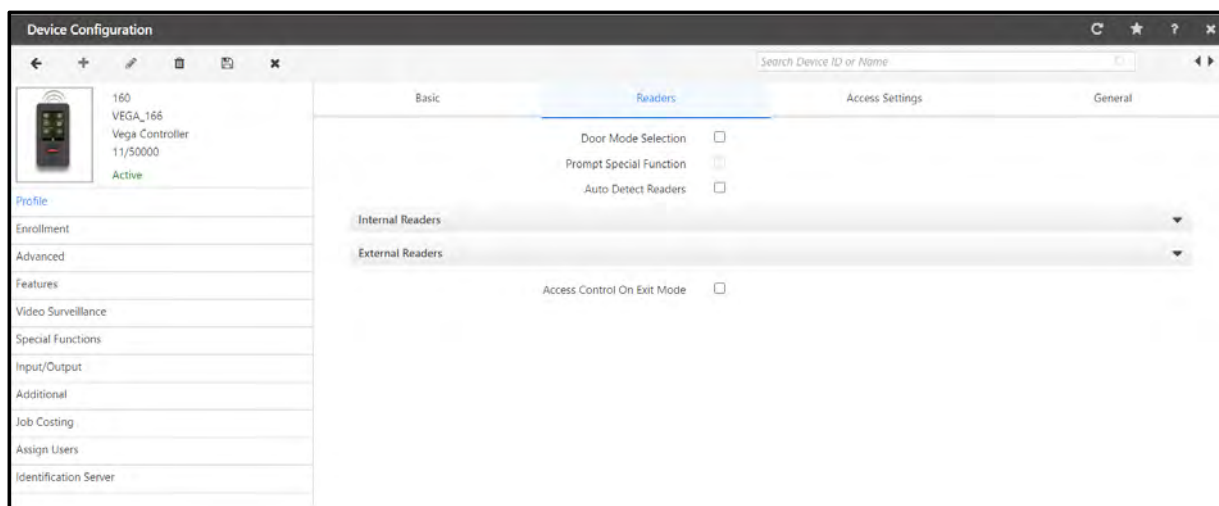


Access Zone is configured while configuring Panel200.

Readers

Readers are important hardware components in a biometric door device. They may be internal or external. This section enables you to configure both internal and external readers for a door.

Click the **Readers** tab. The Readers page appears.



Configure the following parameters:



Door Mode Selection, Prompt Special Function and Auto Detect Readers are applicable for Direct Door only.

- **Door Mode Selection:** Select the check box, if you wish to allow the user to select the punch type — IN or OUT while punching on the device.

For example, when a door is in the Entry mode, the punches will always be in Entry side. But if you wish to mark the punch in Exit mode then you can do so if Door Mode Selection is enabled.

If Door Mode Selection is not enabled, you need to enable Scheduling to set reader mode of door as entry or exit as per user-defined schedules. For more information on creating Reader Mode Schedules, refer **Devices > Masters > Reader Mode Scheduler**.

- **Prompt Special Function:** This will provide selection of special function on device screen and based on the selection of particular type of special function. Make sure you have enabled **Door Mode Selection**.
- **Auto Detect Readers:** Select this check box to enable auto detection of Readers on a Door connected with the Server.

Internal Readers

This option allows the configuration of the Internal Reader for the door.

Click **Internal Readers** collapsible panel.

Internal Readers

Mode: Entry

Card Reader Type: None

Search

Member No ▲	Card Format	Configurable Bits
1	Default Format	0

Finger Reader Type: None

Enable Scheduling: ☐

Reader Mode Schedule: ID Name

Advertise Bluetooth: ☐

Bluetooth Name:

Bluetooth Range: Medium (5m - 7m)

Configure the following parameters.

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop-down list.
- **Card Reader Type:** Select the desired Card Reader Type from the drop-down list — EM Prox Reader, HID Prox Reader, MiFare Reader, HID iClass-U Reader, HID iClass-W Reader.
- **Card Format:** Single or multiple card formats can be assigned to the readers of the door. A Default Format is assigned to the device. If no other card format is assigned to device; then this default format will be applied. For creating Card Formats, click **Devices > Master > Card Format**. For details refer to “[Card Formats](#)”.

Assigning Multiple Card Format

- Click **Add**, to assign multiple card formats to the device. Then click the picklist to select the card format and click **OK** to save the format.

Search

Member No ▲ Card Format Configurable Bits

1 Default Format 0

Add

Search

Member No ▲ Card Format Configurable Bits


2 Format1 0

1 Default Format 0

OK

Similarly, you can add maximum 5 card formats. When the card format is saved, the Configured bits of that format as configured from **Masters > Card** format are displayed here. Multiple Card format configurations will be sent to the door separated by **Format ID** that is Member No. along with all other format related parameters.

- **Finger Reader Type:** Select the **Finger Reader Type** as **Finger Reader**.

Click **FP Reader Configuration**  to set the Finger Print Module Calibration.

The **Finger Print Module Calibration** pop-up appears.

Configure the following parameters:

- **Security Level:** Select the desired Security Level to be set for the Finger Print Module Calibration from the drop-down list—Normal, Secure, Highly Secure. Security level specifies False Acceptance Ratio (FAR). Since False Acceptance Ratio (FAR) and False Rejection Ratio (FRR) is in inverse proportion to each other, FRR will increase with higher security levels. You can select **Normal** level for regular Time and Attendance system. You must select **Highly Secure** level for high security areas that require complete or maximum matching of template. You can select **Secure** level for approximate matching of template.
- **Lighting Condition:** Select the Lighting Condition to be set for the Finger Print Module Calibration from the drop-down list— **In Door**, **Out Door**. Optical sensors are sensitive to lighting condition. With this parameter, users can tune optical sensors to be adapted for their lighting environment.
- **Sensitivity:** Select the desired level of Sensor Sensitivity from the drop-down list — Level 1 to 8. This specifies sensor sensitivity to detect a finger. On high sensitivity, the module will accept the finger input more easily. Level 8 has the highest sensitivity.

- **Fast Mode:** Select the desired Fast Mode to reduce the matching time with a little degradation of authentication performance from the drop-down list — Auto, Mode 1 to 6. Fast Mode parameter can be used to reduce the matching time with a little degradation of authentication performance. In typical cases, Fast Mode 1 is 2 to 3 times faster than Normal mode while Fast Mode 5 is 6 to 7 times faster than Normal mode. You can also select the Auto mode.
- **Image Quality:** Select the Image Quality to be set for the fingerprint from the drop-down list—Weak, Moderate, Strong, Strongest. When a fingerprint is scanned, the module will check if the quality of the image is adequate for further processing. Image quality parameter specifies the strictness of this quality check. Strongest might lead to higher number of finger rejections during the enrollment process.



Good quality of enrollment (around 70-75% quality) is recommended for proper identification of enrolled templates.

- Click **Restore Defaults**, to set the values of the all the fields to default, if required.
- Click **Save**, to save the changes or **Close**, if you wish to discard the changes.
- **Enable Scheduling:** Select the check box to enable automated control of an Internal Reader. This will set Reader Mode of door as Entry or Exit as per user-defined schedules.
- **Reader Mode Schedule:** Click the picklist and select the schedule which is to be assigned to the internal reader of VEGA Door. With this the same reader can be configured to function both in Entry as well as Exit mode based on the scheduled timings.



For configuring Reader Mode Schedule, refer Devices> Masters> Reader Mode Scheduler.

- **Advertise Bluetooth:** Select this check box to enable Bluetooth of the device by which the device will be visible to others. Then configure the following parameters:
 - **Bluetooth Name:** By default, if the Device Name is configured then it will be displayed here along with the Mode. The prefix will be the Device Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the bluetooth name as per your requirement. The Bluetooth Name can be a maximum of 10 characters.
 - **Bluetooth Range:** The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — **Short (1m-2m), Medium (5m-7m) or Long (>8m).**
- Click **Save** to save all the configurations.

External Readers

This option allows you to configure the External Reader for the door.



Mode, External Reader Type, Card Format and Exit Switch are applicable for both Panel Door and Direct Door.

- Click **External Readers** collapsible panel and configure the following parameters:

External Readers

Mode: Exit

External Reader Type: None

Search

Member No ▲	Card Format	Configurable Bits
1	Default Format	0

Exit Switch: ☐

User Access Mode: Any One

Visitor Access Mode: Any One

- Mode:** Select the **Mode** from the drop-down list—**Entry, Exit**.
- External Reader Type:** Select the desired type of External Reader from the drop-down list.



If you are using PIN-W Reader; user's will be able to change their PIN number from the devices.

- Card Format:** Select a Card format to be applicable for external readers of the device. This is applicable for all Direct Doors and Panel Doors. For details, refer to [“Card Formats”](#).
- Exit Switch:** Select this check box to enable the use of **Exit Switch**.



User Access Mode, Visitor Access Mode and Access Control on Exit Mode is applicable for Direct Door only.

- User/Visitor Access Mode:** Select the Access Mode from the drop-down list — Any One, Card, Biometrics, Card + Biometrics, Biometrics then Card, Card then Biometrics, None, BLE, Card + PIN, Biometrics + PIN, Card + Biometrics + PIN.
- Configure Bluetooth from Server:** When you select **External Reader Type** as — CB U Reader, ATOM RD300, ATOM RD200 or ATOM RD100, select **Configure Bluetooth from Server** check box to enable Bluetooth feature for the mentioned external readers.

External Readers

Mode: Exit

External Reader Type: CB U Reader

Search

Member No ▲	Card Format	Configurable Bits
1	Default Format	0

Exit Switch: ☐

User Access Mode: Any One

Visitor Access Mode: Any One

Configure Bluetooth From Server: ☒

Advertise Bluetooth: ☒

Bluetooth Name:

Bluetooth Range: Short (1m - 2m)

Once you enable **Configure Bluetooth from Server**, configure the following Bluetooth parameters:

- **Advertise Bluetooth:** Select this check box to enable Bluetooth of the VEGA device by which the device will be visible to others. Then configure the following parameters.
- **Bluetooth Name:** By default, if the Device Name is configured then it will be displayed here along with the Mode. The prefix will be the Device Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the bluetooth name as per your requirement.

The Bluetooth Name can be a maximum of 20 characters.

- **Bluetooth Range-** The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — **Short (1m-2m), Medium (5m-7m) or Long (>8m).**



If Auto Detect Reader is enabled, then External Reader Bluetooth parameters will not be visible.

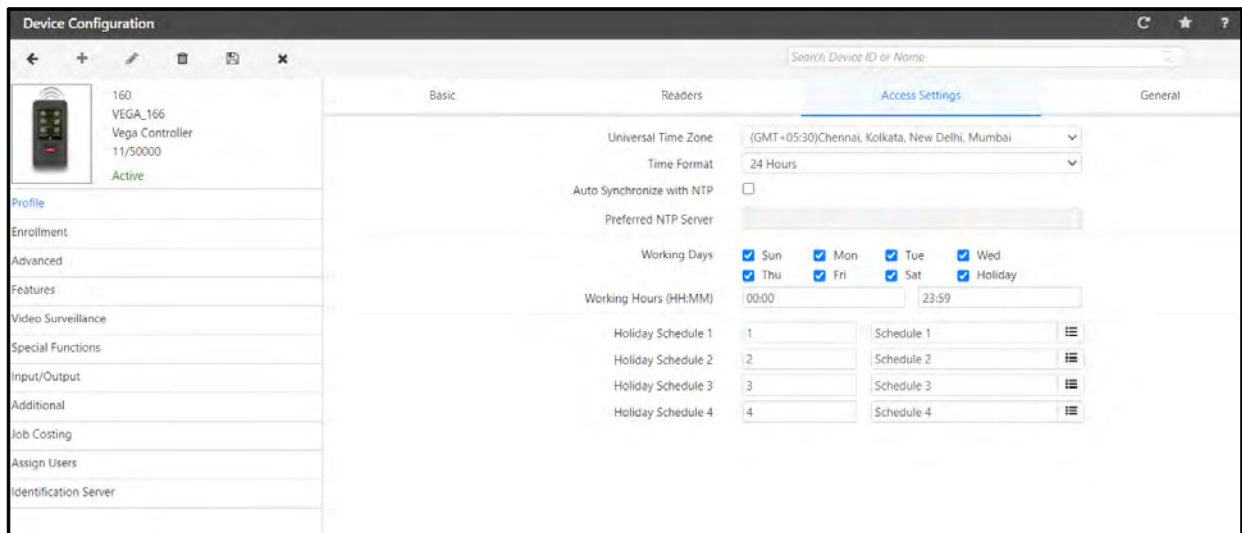
- **Access Control On Exit Mode:** Select this check box to enable the checking of the following access control policies on the door when the External Reader is in the Exit mode.
 - User enabled
 - User validity
 - Blocked user
 - Time Based Access Check
 - ASC
 - User Access Group
- Click **Save** to save all the configurations.

Access Settings



Access Settings are applicable for Direct Door only.

- Click the **Access Settings** tab. The **Access Settings** page appears.



Configure the following parameters:

- **Universal Time Zone:** Select the desired geographic time zone in which the door will operate from the drop-down list.
- **Time Format:** Select the time format to be displayed on door's LCD display from the drop-down list — 24 Hours or 12 Hours.

Auto Synchronize with NTP: If Date and time is to be automatically synchronized as per the **Preferred NTP Server** (predefined or user-defined NTP server address) selected by user, then you must select the **Auto Synchronize With NTP** check box to enable.

Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from device web page, which will be reflected on device display.

- When Auto Synchronization with NTP is disabled Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 - You can specify the **Preferred NTP Server** of your choice. In this case device will first try to get Date and Time from that server address.

If it does not get Date and Time in three tries; device will check from pre-defined NTP servers.

If you have entered one of the three pre-defined NTP servers(ntp1.cs.wisc.edu , time.windows.com, time.nist.gov); then device will first check that server first.

If it receives updated Date and Time then Updated Date and Time will be reflected on device web page and display screen.

- You can keep the Preferred NTP Server as blank. In this case device will check for Date and Time from the first NTP server.



If user has manually entered Date and Time from the web page or Device Menu then these values of Date and Time will be reflected on device web page and display screen.

If you select the **Manual** option, you can manually update the time on the door with that of the system time as and when required. This can be accomplished from the COSEC Monitor.

- **Working Days:** Specify the days on which the default working hours are applicable. To do so, select the respective check boxes of the relevant days.
- **Working Hours (HH:MM):** Specify the default working hours in HH:MM format.
- **Holiday Schedule:** Click the picklist and select the desired Holiday Schedule. You can assign upto four Holiday Schedules to the device.



If the same Holiday Schedule is configured for a user and on door which is assigned to the user, then the user's attendance marking on this device, on any of the scheduled holidays will always be marked as a holiday.

General

- Click the **General** tab. The General page appears.

The screenshot shows the 'Device Configuration' window with the 'General' tab selected. The left sidebar lists various configuration categories. The main content area is divided into several sections:

- Basic:** Includes fields for 'Display Duration (ms)' (set to 3000) and 'LED - Buzzer Duration' (set to Long).
- Denied Acknowledgement:** Similar to the Basic section, with 'Display Duration (ms)' (3000) and 'LED - Buzzer Duration' (Long).
- Enable Display Messages:** A checkbox that is currently unchecked.
- Custom Birthday Message:** A text field containing 'Happy Birthday'.
- Display Message 1:** Includes a 'Schedule' field (00:00 to 11:59) and a 'Message' field (Good Morning).
- Display Message 2:** Includes a 'Schedule' field (12:00 to 15:59) and a 'Message' field (Good Afternoon).
- Display Message 3:** Includes a 'Schedule' field (16:00 to 20:59) and a 'Message' field (Good Evening).
- Display Message 4:** Includes a 'Schedule' field (21:00 to 23:59) and a 'Message' field (Good Night).
- Multi-Language Support:** A checkbox that is currently unchecked.
- Auto Hide Menu Bar:** A checkbox that is currently unchecked.

Configure the following parameters:



Mute Buzzer, Allowed Acknowledgment and Denied Acknowledgment are applicable for both Direct Door and Panel Door.

- **Mute Buzzer:** You can mute or unmute the door buzzer. Select the check box to enable or clear the check box to disable.

- **Allowed Acknowledgment**

- **Display Duration (ms):** Specify the time duration for which the *Acknowledgment Allowed* message should be displayed. Valid Range: 500 to 3000ms.
- **LED - Buzzer Duration:** Select the time duration for the LED Buzzer from the drop-down list— **Long, Medium, Short.**

- **Denied Acknowledgment**

- **Display Duration (ms):** Specify the time duration for which the *Acknowledgment Denied* message should be displayed. Valid Range: 500 to 3000ms.
- **LED - Buzzer Duration:** Select the time duration for the LED Buzzer from the drop-down list — **Long, Medium, Short.**



Enable Display Messages, Custom Birthday Message, Display Message 1 to 4, Schedule, Message and Multi-Language Support are applicable for Direct Door only.

- **Enable Display Messages:** Select this check box to enable the Custom Birthday Message and the Display Messages. Upto 4 Display Messages can be configured.
- **Custom Birthday Message:** Configure the birthday message which you wish to display on the door when the user punches on the door on his/her birth date.

The valid values are

A-Z

a-z

0-9

`~!@#\$%^&*()_+-={}|\|:;?<>,.\'"

- **Display Message 1 to Display Message 4:** Select the respective check box of the desired Display Messages from 1 to 4, to enable.
 - **Schedule:** For each **Display Message**, define the time period for which the message is to be displayed.
 - **Message:** For each **Display Message**, configure the message you wish to display on the Panel Door as per the time set in the Schedule. Maximum 21 characters allowed.
- **Multi-Language Support:** Select this check box to enable multi-language support for this door.
- **Auto Hide Menu Bar:** If any user touches the device screen by mistake and enters into the Menu, then users punch will not be accepted by the device till the Menu is closed or till time out occurs. To avoid such a scenario, select this check box. This will hide the Menu, hence users will be able to punch on the door. To access the Menu, swipe upwards on the device screen. The Menu appears.

Enrollment



Enrollment is applicable for Direct Door only.

On the **Device Configuration** page, click the **Enrollment** tab in the left pane.

Settings

Configure the following parameters:

- **Enroll from Device:** Select this check box to enable the enrollment of user from the door. When this check box is enabled, *Enroll User* special function on that device will be activated.



If both Enroll User special function & Enroll From Device check box are inactive in Device Configuration, then if you enable Enroll User special function, Enroll From Device check box will also be enabled.

- **Enrollment Mode:** Select the Credential from the drop-down list that can be enrolled using the special function at the door— **ReadOnlyCard**, **SmartCard**, **Biometric**, **BiometricthenCard**, **DuressFinger**, **Face**. Refer “[Enroll Credentials](#)” or “[Enrolling Users](#)” to enroll User/Worker. Refer “[Enrollment](#)” or “[Enroll Credentials](#)” to enroll Worker. Refer “[Enroll Credentials](#)” to enroll a Visitor.



DuressFinger is applicable for User and Worker only.

- **Template Per Finger:** This displays the values as configured in the Global Policy. This field is not editable. For details refer to “[User Policy](#)”.
- **Max Number of Fingers:** This displays the values of the Maximum Number of Fingers configured in the Global Policy. This field is not editable. For details refer to “[User Policy](#)”.
- **Number of Fingers/Cards:** Select the Number of Cards or Fingerprints to be enrolled based on the credential option selected in Enrollment Mode.
- **Enable Self-Enrollment:** Select this check box to enable the Self-Enrollment feature on this door.

Advanced

The Advanced tab allows the user to configure some advanced parameters such as Access Control Settings, Alarms, Device Timers as well as Wiegand.

To do so, on the **Device Configuration** page, click the **Advanced** tab in the left pane.

To configure the Advanced parameters click the following links:

- [“Settings”](#)
- [“Alarms”](#)
- [“Timers”](#)
- [“Wiegand”](#)

Settings

The **Settings** tab differs for both Direct Door and Panel Door.

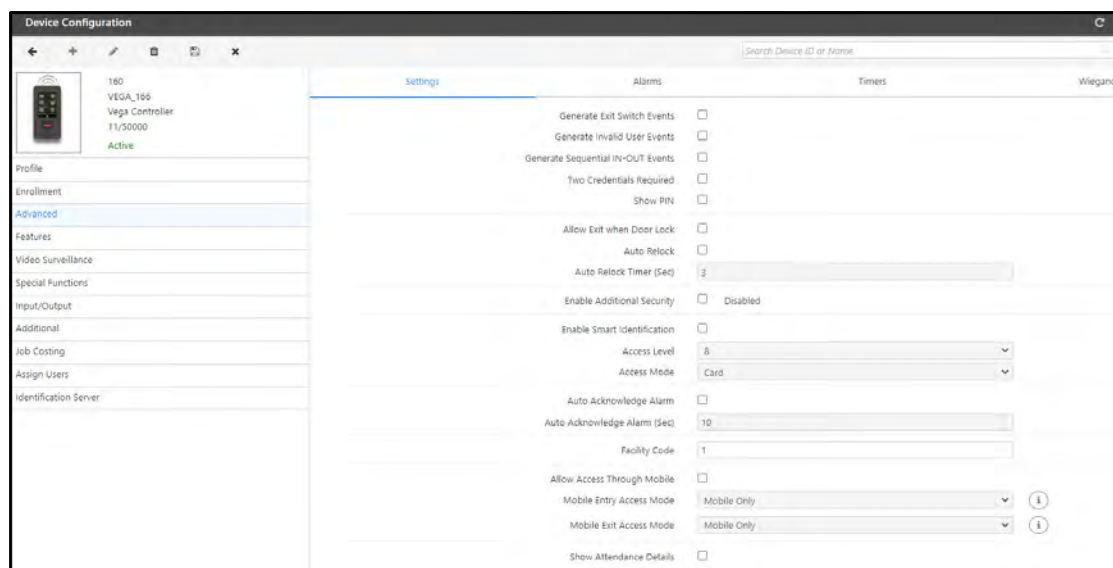
- Click **Settings** tab.

For configuring the Settings for **VEGA Controller** as a **Direct Door**, refer [“Settings - VEGA as Direct Door”](#).

For configuring the Settings for **VEGA Controller** as a **Panel Door**, refer [“Settings - VEGA as Panel Door”](#).

Settings - VEGA as Direct Door

The **Settings** page for **VEGA Controller** as a **Direct Door** appears.



Configure the following parameters:

- **Generate Exit Switch Events:** Select this check box to enable the door to generate Events every-time the Exit Switch is used.
- **Generate Invalid User Events:** Select this check box to enable the door to generate Events for Invalid User inputs.
- **Generate Sequential IN-OUT Events:** Select this check box to generate user punches on device as IN-OUT sequential events irrespective of the mode in which the device is functioning.
- **Two Credentials Required:** Select this check box to enable the feature. If both, **Bypass Finger/Palm/Face For Attendance** (User Configuration > T&A > Attendance) and **Two Credentials Required** check boxes are enabled, then two credentials will be mandatory for the users and the door will verify both these credentials.
- **Show Pin:** Select this check box to display the characters of PIN when the PIN is entered on device.
- **Allow Exit when Door Lock:** Select this check box if you wish to allow the users to Exit even when the Door Relay is in locked condition.
- **Auto Re-lock:** Select this check box to allow the door to re-lock immediately when the Door Status changes to close from normal open irrespective of the defined Pulse Time. This will be supported only if a door sense is installed and enabled.
- **Auto Re-lock Timer:** Specify the time in seconds after which the door should re-lock automatically.
- **Enable Additional Security:** Select this check box to enable additional security at the door.
 - **Additional Security Code:** Enter a code (ranging from 1 to 65535) you wish to set as the security code.
 - **Re-enter Code:** Re-enter the security code to confirm.



*Changing this value can affect the Smart Identification (SI) function. Click **Default Code** to reset the **Additional Security Code** values as set in the **System Configuration > Global Policy > Device > Smart Identification > General Additional Security Code**.*

- **Enable Smart Identification:** Smart Identification enables the identification of a user using the Smart Card even though the user is not registered on a device. Select this check box to enable Smart Identification at the door and select the **Access Level** and the **Access Mode** from the drop-down list.
- **Auto Acknowledge Alarm:** Select this check box to enable the acknowledgment of all alarms for this device automatically.
- **Auto Acknowledge Alarm (sec):** Specify the time in seconds. When the alarm buzzer rings the timer will start and on expiry of this timer, the alarm buzzer will stop automatically.
- **Facility Code:** Specify a value for **Facility Code** to be set for access modes other than Card, if Facility Code is expected in Wiegand Output.
- **Allow Access Through Mobile:** Select this check box to allow the Access to device using COSEC ACS Application.

- **Mobile Entry/Exit Access Mode:** Select the **Entry and Exit** door **Access Mode** from the drop-down list — Mobile Only, Mobile then Biometrics, Mobile then Card, Mobile then PIN.



*If User Access Mode is selected as **None** in Zone Configuration and Mobile Access Mode is selected as **Mobile Then Biometrics** then the door can be accessed through Mobile and then Biometric credential.*

- **Show Attendance Details:** Select this check box to display the Attendance Details of the user on the door. This allows the user to view his/her Attendance Details on the door itself and there is no need to login into the ESS application to view the Attendance Details.

The Attendance Details of the user will be displayed for default Menu Time-Out period, that is 30 sec after the Access Allowed screen.



*The user whose Attendance Details are to be displayed on the door must be enabled for this feature. Enable the check-box **Show Attendance details on Device** from User Configuration > T&A > Attendance.*

While an attendance detail of one user is being displayed on device and second user tries to access the device; new user will be processed.

Whenever both users of 2-person rule are allowed access on device then attendance details screen of second user will be displayed on the device.

Temperature Logging

Temperature Logging	
Enable	<input type="checkbox"/>
Sensor Type	FEVOBOT
Sensor Interface	USB
Emissivity	0.95
Calibration Parameter	+ 0.0
Approach to Sensor Wait-Timer (Sec)	3.0
Temperature Detection Time Out (Sec)	10
Tolerance between Consecutive Readings	0.5
Consecutive Readings Count within Tolerance	5
Temperature Threshold (°F)	99.5
Minimum Temperature for Access (°F)	95.0
Restriction Type	Soft
Bypass If Sensor Disconnected	<input type="checkbox"/>

- **Enable:** Select this check box to enable the temperature logging feature.
- **Sensor Type:** Select the type of thermal sensor integrated in the device from the drop-down list— **ASR**, **Web-Based** or **FEVOBOT**.
- **Sensor Interface:** Select the interface on which device will communicate with the sensor from the drop-down list.
 - For Sensor Type-AST, the Sensor Interface options are: RS-232 and USB
 - For Sensor Type-Web-based, the Sensor Interface options are: HTTP/S
 - For Sensor Type-FEVOBOT, the Sensor Interface option is USB
- **Emissivity:** Specify the Emissivity for the Sensor. This parameter will be applicable when Sensor Type is AST. Default value is 0.95.

- **Calibration Parameter:** Specify the Calibration Parameter for the thermal sensor. Select +, if you wish the value should increase by 0.1 and select – if you wish that the value should decrease by 0.1. This parameter is applicable when Sensor Type is AST or Web-Based.
- **Approach to Sensor Wait-Timer:** Specify the time for which the device should wait for user to approach the device before starting Temperature Detection.
- **Temperature Detection Time-Out:** Specify the time till which temperature detection should be done for the user and if valid temperatures are not found till the expiry of timer, then timeout will be declared.
- **Tolerance between Consecutive Readings:** Specify the time within which the consecutive readings are considered to be valid user temperature readings. This parameter is applicable when Sensor Type is AST or Web-Based.
- **Consecutive Readings Count within Tolerance:** Specify the number of readings within the Tolerance time for which the consecutive readings are considered to be valid user temperature readings. This parameter is applicable when Sensor Type is AST or Web-Based. For example: if the count is set as 5, then 5 readings are taken and the reading with the highest temperature is considered.
- **Temperature Threshold:** Specify the Maximum Temperature value for user that should be detected and will be considered as valid temperature.
- **Minimum Temperature for Access:** Specify the Minimum Temperature value for Access that should be detected and will be considered as valid temperature.
- **Restriction Type:** Specify the Restriction Type from the drop-down list—**Soft, Hard**.

If **Soft** is selected the user will be allowed access but the Alert for the same will be sent if configured.

If **Hard** is selected the user will be denied access as well as the Alert for the same will be sent if configured.

- **Bypass if Sensor Disconnected:** Select this check box to allow provision of by-passing the temperature detecting feature if sensor connectivity is lost.

Face Mask Compulsion


Face Mask Compulsion feature is used to enforce users to wear masks while they are within the premises.

After identifying the user, the Device will prompt the user to show Face with Mask when Face Mask Compulsion is enabled.

Based on identification of the Mask, the user will be allowed or denied access.

Face Mask Compulsion

Enable

☐


Approach to Camera Wait-Timer (Sec)

3.0

Mask Detection Time Out (Sec)

4

Restriction Type

Soft

▼

Make sure you have enabled **Enable FR** check box in **Devices> Device Configuration> Identification Server> Face Recognition> Enable FR** and configure the below mentioned parameters to avail this feature.

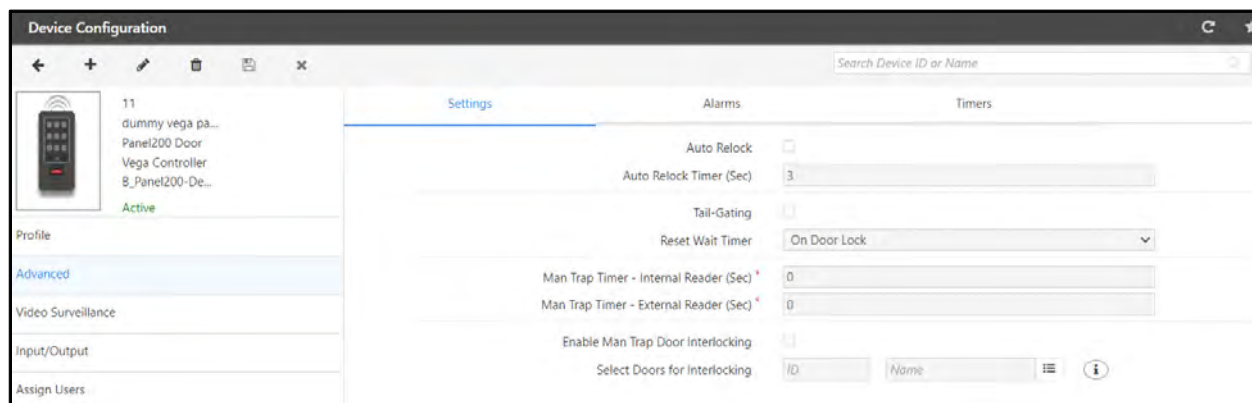
- **Enable:** Select this check box to enable Face Mask Compulsion feature for IDS.
- **Approach to Camera Wait-Timer (Sec):** This defines the time within which the user must approach the camera for face mask detection. Wait-Time Range: 0.0-15.0 seconds. Default: 3.0 seconds.
- **Mask Detection Time Out (Sec):** This defines the maximum time duration for which the system will try to detect the user's face mask. Detection Time out range: 0.0-15.0 seconds. Default: 4.0 seconds.
- **Restriction Type:** Select the type of restriction to be imposed when the face mask is not detected — **Soft or Hard**. Default: **Soft Restriction**.
 - **Soft Restriction:** The access will be granted even if the user is identified without wearing a mask; however, an event and a warning are generated that indicates the user has been identified without wearing a mask.
 - **Hard Restriction:** The access will be denied if the user is identified without wearing a mask.



Users face enrollments are dependent on the Visible Face parameter value set by you. For more details, refer to [“Face Recognition”](#).

Settings - VEGA as Panel Door

The **Settings** page for **VEGA Controller** as a **Panel Door** appears.



Configure the following parameters:

- **Auto Re-lock:** Select this check box to enable the door to re-lock automatically when the door status changes to close from normal open, irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Re-lock Timer:** Specify the time in seconds after which the door should re-lock automatically.
- **Tail-Gating:** Tailgating refers to an access violation which occurs when more than one person tries to enter a secured area using a single person's access credentials. If this option is enabled on the Panel Door, the occupancy count of a zone should be increased or decreased considering both the punch as well as the auxiliary input of the Panel Door. Select the check box if you wish to enable this feature.

- **Reset Wait Timer:** Select when the Wait Timer should be reset for Tailgating from the drop-down list — On Door Lock or Pulse Wait Timer.
- **Man Trap Timer- Internal Reader (Sec):** Specify the Man Trap Entry Timer within which the user should enter the next sequential door of a man-trap.
- **Man Trap Timer- External Reader (Sec):** Specify the Man Trap Exit Timer within which the user should exit the panel door to enter the next sequential door of a man-trap.
- **Enable Man Trap Door Interlocking:** Select this check box to enable the Door Interlock for the door (for example: Door1). This means if the Door1 is open, other doors will remain closed.
- **Select Doors for Interlocking:** Select the doors to be assigned for Interlocking from the picklist. For example, if Door 2 and Door 3 are selected for interlocking with Door 1, Door 2 and Door 3 will remain locked when Door 1 is open.

Door Interlocking feature will not work for Degraded mode.



For example, when a door is in abnormal state and for that door interlocking is enabled, then user access to other doors of the interlocking group is allowed.

Alarms

In **Alarms** tab, you can assign below list of alarms to the door.

Alarms tab differs for Direct Door and Panel Door.

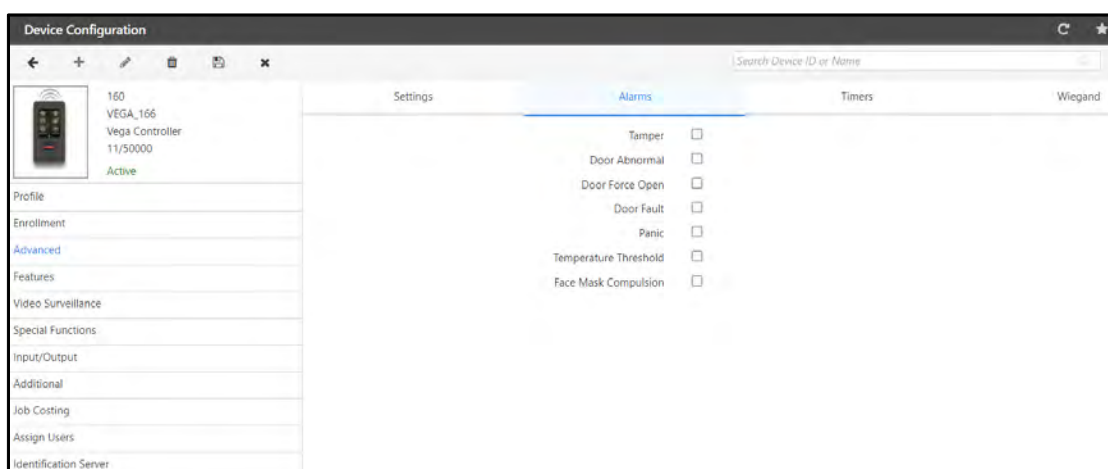
- Click **Alarms** tab.

For configuring the Alarms for **VEGA Controller** as a **Direct Door**, refer [“Alarms - VEGA as Direct Door”](#)

For configuring the Settings for **VEGA Controller** as a **Panel Door**, refer [“Alarms - VEGA as Panel Door”](#)

Alarms - VEGA as Direct Door

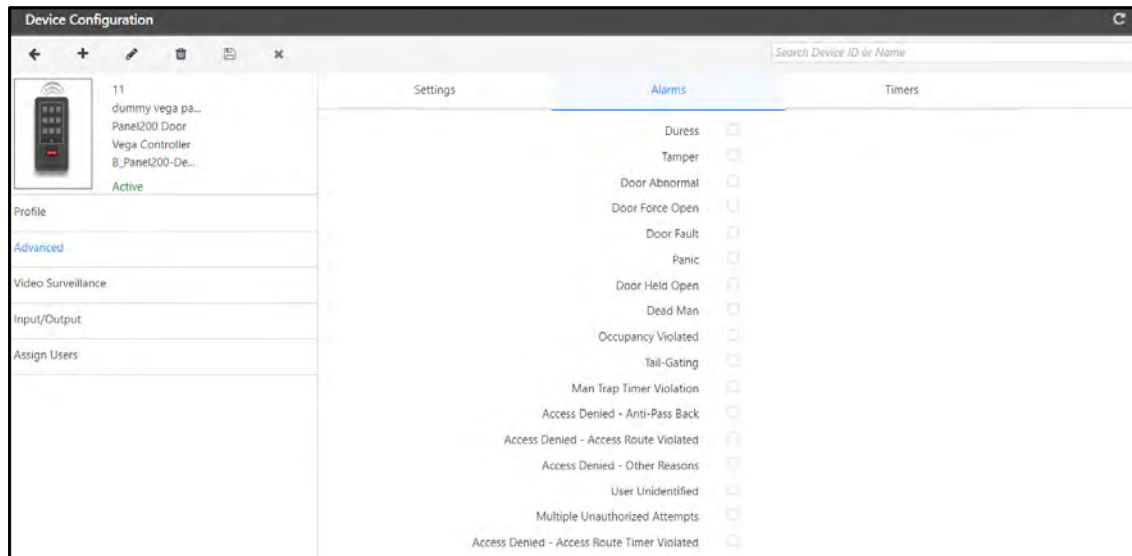
The **Alarms** page for VEGA as a Direct Door appears.



Select the check boxes of the desired alarms you wish to enable.

Alarms - VEGA as Panel Door

The **Alarms** page for VEGA as a Panel Door appears.



Select the check boxes of the desired alarms you wish to enable.

Timers

This section allows the configuration of various types of predefined device timers which can trigger off specific responses. In the Server, Timers are often used to control the door behaviour and for triggering alarms.

The **Timers** tab differs for Direct Door and Panel Door.

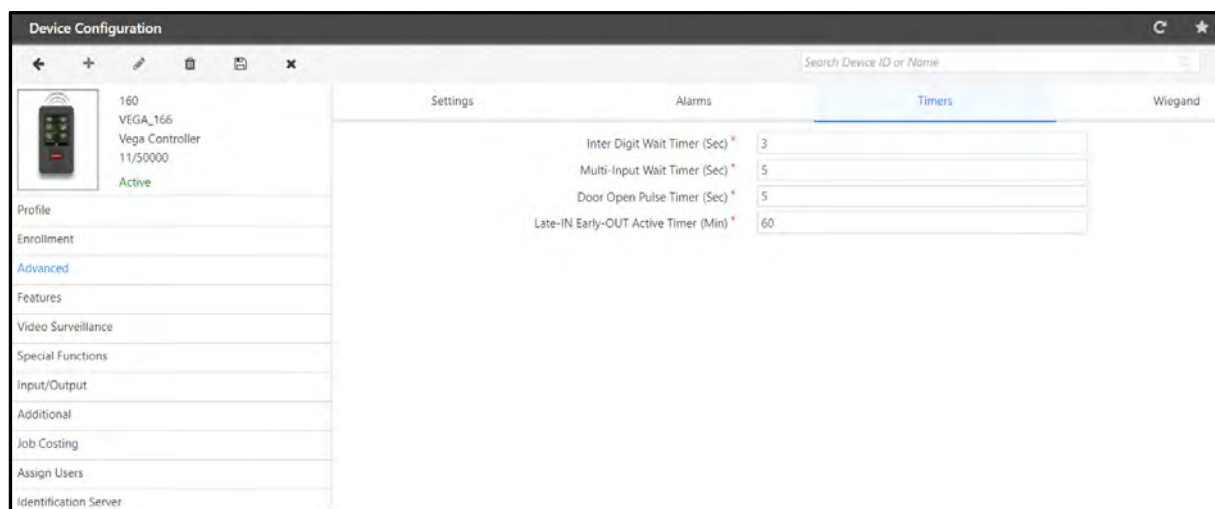
- Click **Timers** tab.

For configuring the Settings for **VEGA Controller** as a **Direct Door**, refer [“Timers - VEGA as Direct Door”](#).

For configuring the Settings for **VEGA Controller** as a **Panel Door**, refer [“Timers - VEGA as Panel Door”](#)

Timers - VEGA as Direct Door

The Timers page for VEGA as a Direct Door appears.



Configure the following parameters:

- **Inter-Digit Wait Timer (sec):** Specify the time period in seconds between two key inputs on the device keypad. On expiry of this timer, the system considers the user input to be complete and is ready for the next input.
- **Multi-Input Wait Timer (sec):** Specify the time in seconds for which system needs to wait for the second credential input from the user when more than one credential is to be used for granting access.

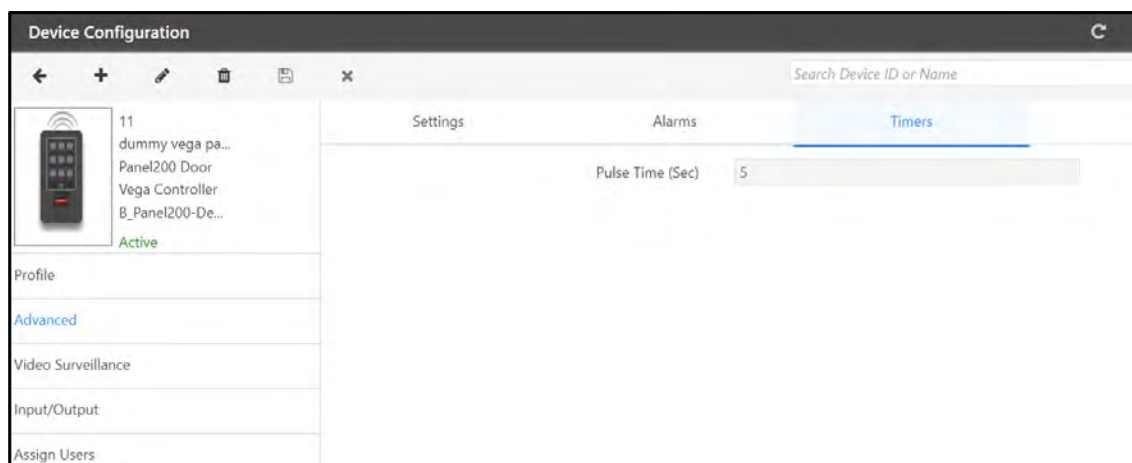


We recommend you to set the timer value as greater than or equal to 10 seconds to avoid access denial issues to users. This is applicable when the system reads the credentials (biometric) from the user's Smart Cards.

- **Door Open Pulse Timer (sec):** Specify the time in seconds (3 to 99) for the door to remain open for a valid credential. If the opened door does not return to a closed state before the expiry of this timer, the door will generate a **Door Abnormal** alarm.
- **Late-IN Early-OUT Active Timer (min):** Specify the time in minutes for which the Late-IN and Early-OUT special functions will remain active after being enabled on the door.

Timers - VEGA as Panel Door

The **Timers** page for **VEGA** as a **Panel Door** appears.



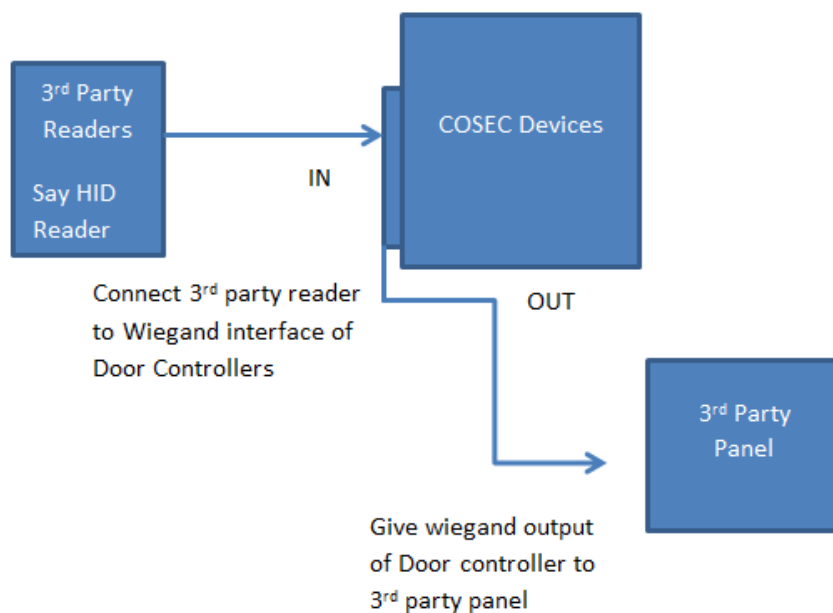
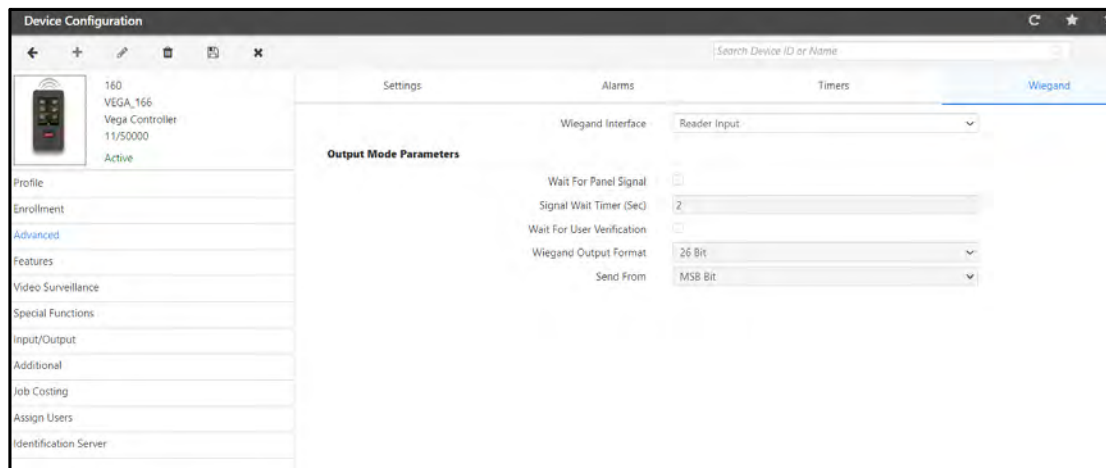
- **Pulse Time (sec):** Specify the time in seconds for the panel door to remain open for a valid credential.

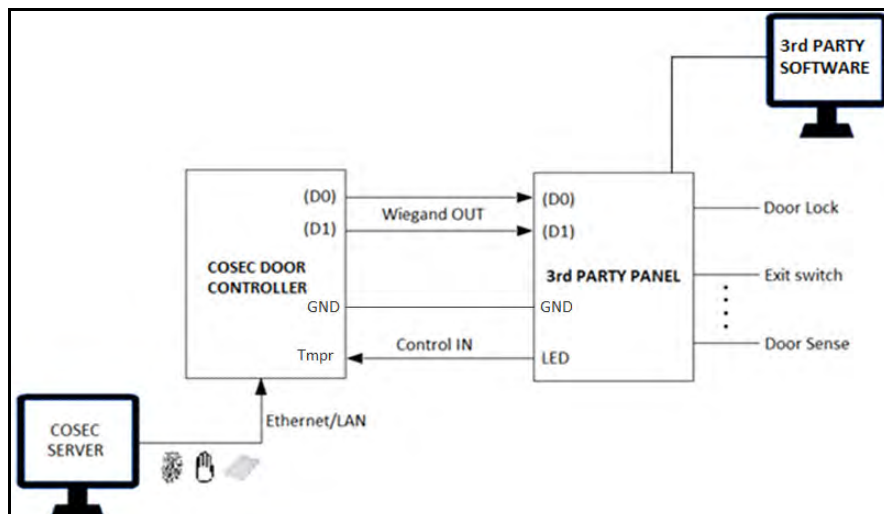
Wiegand



Wiegand is applicable for Direct Door only.

- Click the **Wiegand** tab. The Wiegand page appears.



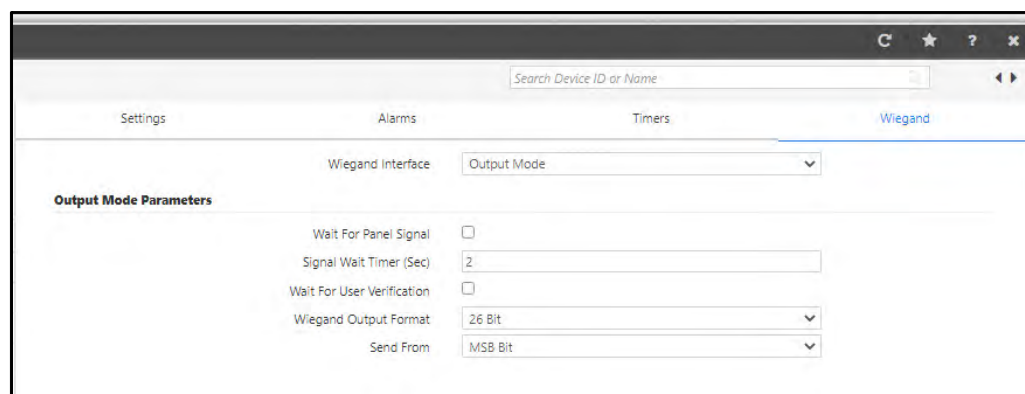


- **Wiegand Interface:** The devices can be connected both as input devices (that is, to receive data from a Wiegand Reader) or output devices (that is, to support output to third party panel) via the Wiegand interface as shown below.

So select the interface of Door controller as **Output Mode** to work as Wiegand Output to Panel or **Reader Input** to take data from third party reader. If Reader Input option is selected, all the Output Mode parameters will be disabled.

If you select Output mode then configure the **Output Mode Parameters**.

Output Mode Parameters



- **Wait For Panel Signal:** Select the check box to enable. If this option is enabled the Panel Door will wait for reply from the connected third party device before triggering any output. You need to configure the **Signal Wait Timer (Sec)**.
- **Signal Wait Timer:** Specify the time for which the Panel Door should wait for reply from the connected third party device before triggering any output.
- **Wait For User Verification:** Select the check box to enable. If this option is enabled, user verification will be requested on the third party device before triggering any output.

- **Wiegand Output Format:** Select the desired format — 26 Bit, 37 Bit, Actual or Custom.

The screenshot shows a web interface with tabs for Settings, Alarms, Timers, and Wiegand. The Wiegand tab is active, showing a 'Wiegand Interface' section with an 'Output Mode' dropdown menu. The dropdown is open, showing options: 26 Bit, 26 Bit (highlighted), Actual, 37 Bit, and Custom. Below the dropdown, there are checkboxes for 'Wait For Panel Signal' and 'Wait For User Verification', a 'Signal Wait Timer (Sec)' field set to 2, and a 'Send From' dropdown menu.

If you select **Custom**, you can configure details of fields to be sent as output from the Wiegand reader that has been added.

The screenshot shows the 'Wiegand Format' configuration screen. It lists various events with corresponding 'ID' and 'Name' picklist fields and a 'Code' input field. The events are: For Allowed Events, Allowed Code, For Identified Events, Identified Code, For Denied With Invalid Biometric Events, Invalid Biometric Code, For Denied With Invalid Card Events, Invalid Card Code, For Denied With Invalid PIN Events, Invalid PIN Code, For Denied With Credential Time-Out Events, and Credential Time-Out Code.

- For each of the listed events, click the picklist to select the desired **Wiegand Output Format**.
- Assign an Access **Code** for each communication (for example Invalid PIN Code). This will depend on the number of output bits configured for Access Code in the selected Wiegand Output Format.
- **Send From:** Select the desired sending order for reader data — MSB or LSB Bit.

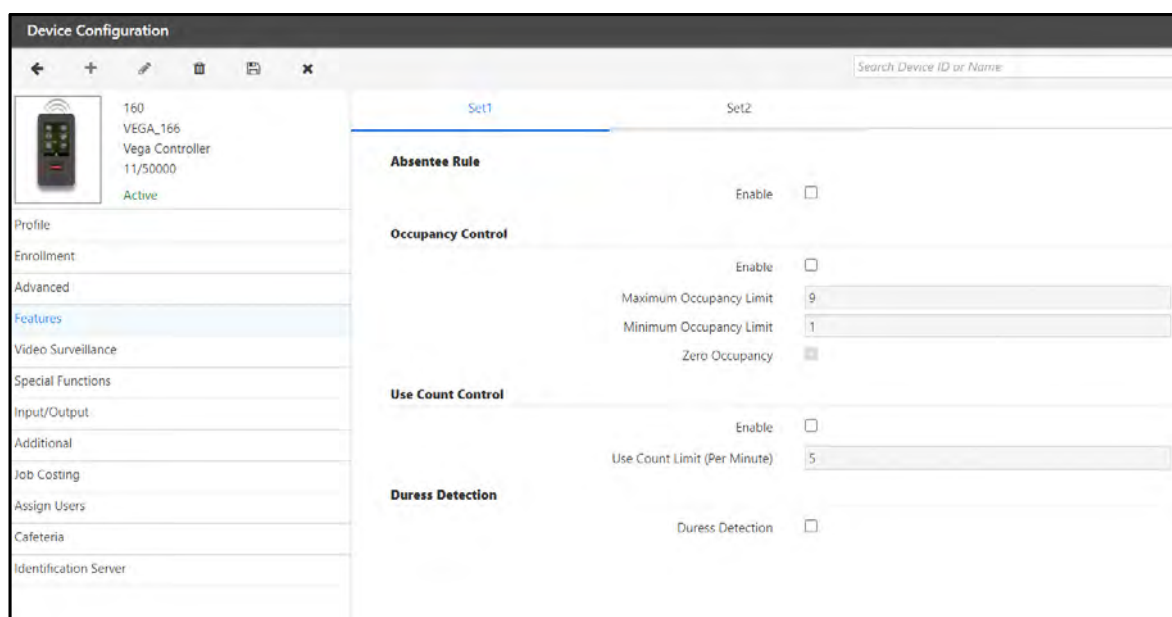
Features



The Features are available only with the Access Control Module license and are applicable for Direct Door only.

The Features tab enables the user to enable certain Access Control features for the device.

To do this, on the **Device Configuration** page, click the **Features** tab in the left pane.

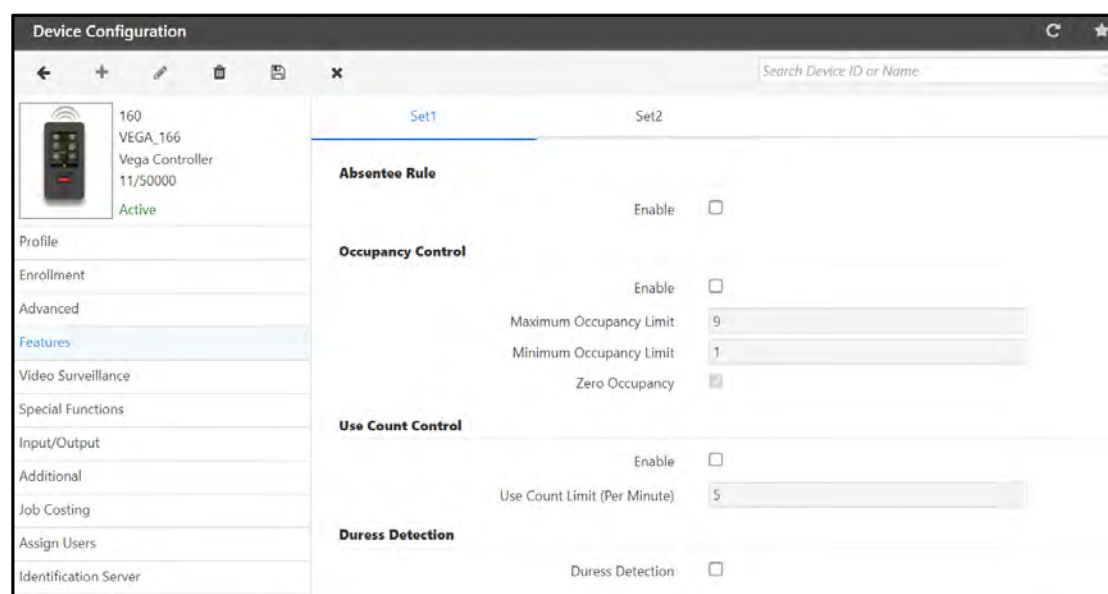


To configure the Features parameters, click the following links:

- [“Set1”](#)
- [“Set2”](#)

Set1

- Click **Set1** tab. The **Set1** page appears.



Configure the following parameters:

Absentee Rule

- **Enable:** Select this check box to enable the feature on the door. This rule sets the maximum number of days for non-use of a credential. On expiration of days limit, the user will be automatically blocked.

For configuring the rule, refer to [“Absentee Rule”](#).

Occupancy Control

- **Enable:** Select this check box to enable the feature on the door.
- **Maximum Occupancy Limit:** Specify the maximum number of users to be allowed within the controlled area, after which a user exit is required to enable access to another user.
- **Minimum Occupancy Limit:** Specify the minimum number of occupants to be present within the controlled area.
- **Zero Occupancy:** Select the check box to enable the controlled area to be empty.

For configuring the rule, refer to [“Occupancy Control”](#).

Use Count Control

- **Enable:** Select this check box to enable the feature on the door.
- **Use Count Limit (Per Minute):** Specify the maximum number of times a user is allowed to access an area with valid credentials per minute.

For configuring the rule, refer to [“Use Count Control”](#).

Duress Detection

- **Duress Detection:** Select this check box to enable Duress Detection on the door. The default duress detection code is displayed which is used to generate the duress alarm. Specify the desired duress code. This code informs that a user is forced to open the door under threat. Once this feature is enabled the system waits for the duress code after the User PIN and the right arrow key input before enabling the duress alarm. The keys have to be pressed in the following order: (User Pin Code) → (Right Arrow Key) → (2 digit Duress Code).

Set2

Click **Set2** tab. The **Set2** page appears.

Set1	Set2
First IN User Rule	
Enable	<input type="checkbox"/>
Reset On	<input checked="" type="radio"/> Day Change <input type="radio"/> Timer Expiry
Access Timer (Sec)	3
First IN User Group	1 List 1
Anti-Pass Back (APB)	
On Entry	<input type="checkbox"/>
On Exit	<input type="checkbox"/>
Hard/Soft	Soft
Forgiveness	<input checked="" type="checkbox"/>
Reset After	<input checked="" type="radio"/> Day Change <input type="radio"/> Timer Expiry
Forgiveness Timer (Min)	1
2-Person Rule	
Enable	<input type="checkbox"/>
Mode	Primary Must
Primary Group	g1
Secondary Group	None
2nd Person Wait Timer (Sec)	5

Configure the following parameters:

First-IN User Rule

- **Enable:** Select this check box to enable the feature on the door.
- **Reset On:** Select when the First-IN User rule should be reset from the options — **Day Change** or **Time Expiry**.

If you select **Time Expiry**, configure the **Access Timer (Sec)**.

- **Access Timer (sec):** Specify the duration for which the rule should be applied. After the expiry of this timer, the rule will be reset for all the users.
- **First-In User Group:** Select the desired group which should be valid at the door from the picklist.

For configuring the rule, refer to [“First In User Assignment”](#).

Anti-Pass Back (APB)

- **On Entry:** Select this check box to enable the system to monitor the entry reader for APB violation.
- **On Exit:** Select this check box to enable the system to monitor the entry as well as the exit readers for APB violations.
- **Hard/Soft:** Select the restriction type from the drop-down list options—Soft or Hard.

Hard APB: If you select Hard APB, access will be denied if the exit is not registered first. It does not allow a second entry using the same card without an exit.

Soft APB: The access will be granted even if the exit is not registered. It allows a second entry of the same user without an exit; however, an event and a warning are generated that indicates the second entry.

- **Forgiveness:** Select this check box to enable the system to reset the APB status.

If **Forgiveness** is enabled, configure the following parameters.

- **Reset After Day Change:** This will reset the APB status of all the users to NULL at midnight. This enables a user, who left the building in the evening without exit punch, to use his/her card for entry in the next morning.
- **Reset After Timer Expiry:** This will reset the APB status of all the users after the expiry of defined time.

If **Reset After Timer Expiry** is selected, configure the following parameter.

- **Forgiveness Timer (Mins):** Specify the time duration in minutes after which Anti-Pass Back status will get reset and the pass will be in original state.

2-Person Rule

- **Enable:** Select this check box to enable the feature on the door.
- **Mode:** Select the Mode from the drop-down list options— Primary Must or Primary & Secondary Must.
- **Primary Group:** Select the desired group from the drop-down list.
- **Secondary Group:** Select the desired group from the drop-down list.
- **2nd Person Wait Timer (sec):** Specify the wait time in seconds after which the second person is allowed to punch on the door.

For configuring the rule, refer to [“2 Person Rule Assignment”](#).

Video Surveillance



Video Surveillance is applicable for both Direct Door and Panel Door.

The **Video Surveillance** tab enables the user to configure parameters for video surveillance integration with the COSEC device. It is available in Basic License.

To do this, on the **Device Configuration** page, click the **Video Surveillance** tab in the left pane.

Device Configuration

160
VEGA_166
Vega Controller
11/50000
Active

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Cafeteria
Identification Server

Visual Tagging

Satatya/IP Camera Integration

Capturing Device: None

MAC Address:

Camera ID:

Storage Root Folder:

FTP Login Credentials: ☐

User Name:

Password:

To configure the Video Surveillance parameters, click the following links:

- [“Visual Tagging”](#)
- [“Satatya/IP Camera Integration”](#)

Visual Tagging

The COSEC application can interface with some supported Hybrid and Network Video Recorders and grab images triggered by user events at the Doors. The **Visual Tagging** tab enables the administrator to define the video recorder parameters.

Click the **Visual Tagging** tab. The **Visual Tagging** page appears.

Visual Tagging

Satatya Integration

Capturing Device: Matrix HVR/NVR

MAC Address:

Camera ID:

Storage Root Folder:

FTP Login Credentials: ☐

User Name:

Password:



To view the user events and related images, click **Admin > Views/Logs > Event View**. To know more about viewing events, refer to [“Event View”](#).

Configure the following parameters:

- **Capturing Device:** Select the video recording device type from the drop-down list options — Matrix HVR/NVR, Milestone or IP Camera.

If you select **Matrix HVR/NVR**, refer to [“Configuring Matrix HVR/NVR Parameters”](#).

If you select **Milestone**, refer to [“Milestone Integration”](#).

If you select **IP Camera**, refer to [“Configuring IP Camera Parameters”](#).

Configuring Matrix HVR/NVR Parameters

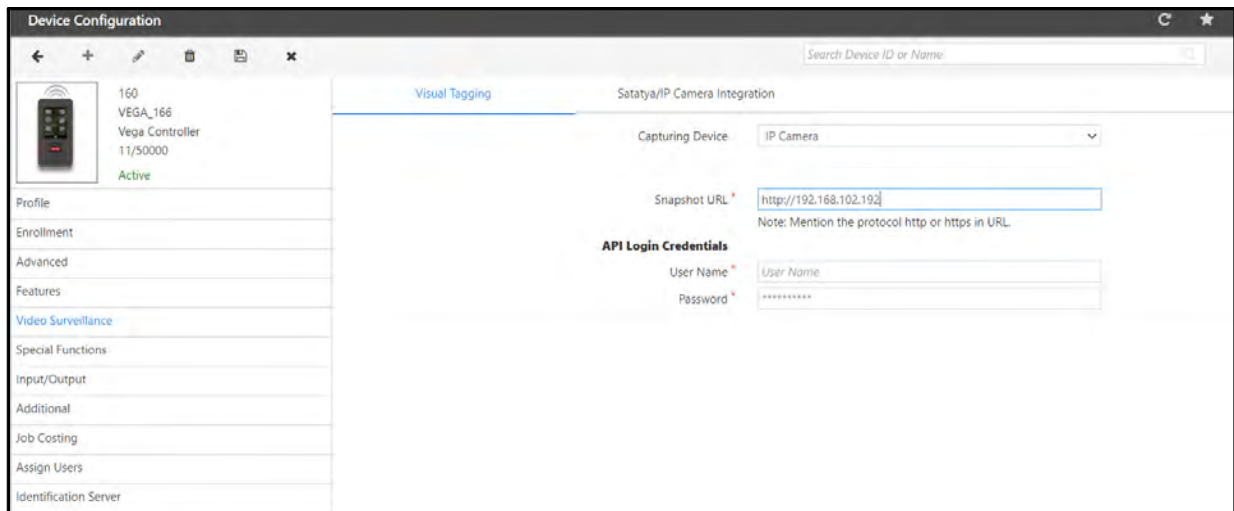
If you select Matrix HVR/NVR, then configure the following parameters:

The screenshot shows a web-based configuration interface for 'Satatya Integration'. At the top, there are two tabs: 'Visual Tagging' (which is active and highlighted with a blue underline) and 'Satatya Integration'. Below the tabs, the 'Capturing Device' is set to 'Matrix HVR/NVR' in a dropdown menu. The interface is divided into two main sections. The first section contains three input fields: 'MAC Address' (with a red asterisk), 'Camera ID' (with a red asterisk), and 'Storage Root Folder' (with a red asterisk). The second section is titled 'FTP Login Credentials' and includes a checkbox that is currently unchecked. Below the checkbox are two input fields: 'User Name' (with a red asterisk) and 'Password' (with a red asterisk). The 'User Name' field contains the placeholder text 'User Name', and the 'Password' field contains a series of asterisks.

- **MAC Address:** Specify the MAC address of the video recorder device using “_” (underscore) as the separator.
- **Camera ID:** Specify the Camera number or Camera ID for IP cameras. For analog cameras, specify the camera number.
- **Storage Root Folder:** Specify the Root Folder path or FTP Path where the uploaded images are to be saved.
- **FTP Login Credentials:** Select this check box to activate the FTP login credentials for authentication.
- **User name:** Specify the FTP Server User Name.
- **Password:** Specify the FTP Server Password.

Configuring IP Camera Parameters

If you select IP Camera, then configure the following parameters:



- **Snapshot URL:** If Capturing device is selected as IP Camera; then enter the API URL for taking the Snapshot through IP camera. You can use any camera for taking the snapshot/photo. The API for capturing snapshot will be available in the API document of camera.
- **User Name:** Enter the Username for accessing API for taking the Snapshot through IP Camera.
- **Password:** Enter the Password for accessing API for taking the Snapshot through IP Camera.



It is the same username and password using which IP camera login is done. For example, username admin and password admin



*The allowed values for snapshot URL, User Name and Password are **A-Z, a-z, 0-9 !"#%&'()*+,-./ :;<=>?@[\\]^_`{|}~***

Satatya/IP Camera Integration

This functionality is available for configuration only when the Matrix HVR/NVR device type or IP Camera is selected as the **Capturing Device** (from *Visual Tagging*).

It enables the configured COSEC devices to directly send commands to the SATATYA HVR/NVR devices/ IP Camera as per the configuration on this page. The Satatya/IP Camera Integration page appears as shown below:



Click **Satatya/IP Camera Integration** tab. The **Satatya/IP Camera Integration** page appears.

Device Configuration

160 VEGA_166 Vega Controller 11/50000 Active

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Visual Tagging **Satatya/IP Camera Integration**

Integration Type: Network
Active: ☒
IP Address:
Port Number: 7024-65535
Schedule Name:
Active: ☐
Schedule Range: 00:00 to 23:59
Days: ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Holiday
Event: Access Allowed
Mode: Both
Action: Recording
Duration Min.:
Camera: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 22 ☐ 23 ☐ 24
Add Cancel

Configure the following parameters:

- **Integration Type:** Select the **Integration Type** from the drop-down list options—Wired or Network.

If you select **Wired Integration**, door will be physically connected with the Satatya Device.

If you select **Network Integration**, connection can be by Ethernet, Wireless or Broadband depending upon the COSEC device support.

If you select **Matrix HVR/DVR** as the **Capturing Device** in **Visual Tagging** and selected **Network** as the **Integration Type** in **Satatya/IP Camera Integration**, refer to [“Configuring Network Integration Parameters”](#).

If you select **IP Camera** as the **Capturing Device** in **Visual Tagging**, for configuring the **Satatya/IP Camera Integration** parameters refer to [“Configuring IP Integration Parameters”](#).

Configuring Network Integration Parameters

- **Active:** Select this check box to enable the SATATYA Integration functionality.
- **IP Address:** Specify the IP Address of HVR/NVR.
- **Port Number:** Specify the Port Number of HVR/NVR.
- **Schedule Name:** Specify a user friendly Name for the Integration function.
- **Active:** Select this check box to enable the schedule.
- **Schedule:** Specify the Start Time and End Time of the Schedule in HH:MM format.
- **Days:** Select the check boxes for the desired Days on which you wish to apply the Schedule.
- **Event:** Select a COSEC Event for which the action is to be configured from the drop-down list.
- **Mode:** Select the event Mode from the drop-down list options—Entry, Exit, Both if you select the Event as Access Allowed, Access Denied or Invalid User.
- **Action:** Select the Action for the Satatya device from the drop-down list options—Recording, Image Upload, Video Pop-up, PTZ Preset, Mail Image.

If you select **Recording**, specify the **Duration Min..**

If you select **Upload Image**, Images will be uploaded as per the FTP settings.

If you select **Video Pop-up**, specify the **Duration Sec.** The video pop up will be generated on the local client of Satatya device.

If you select **PTZ Preset**, specify the desired **Position No.**

If you select **Mail Image**, specify the **Email ID.**

- **Camera:** Select the check boxes of the desired camera channels depending on the Action selected.

Example 1: For Action as Video Pop up and the camera channel selected is 24, then the pop-up of Camera 24 will be shown for 10 seconds.

Example 2: For Access Allowed event on COSEC Device and the camera channel selected are 4,6,8 and 10, then recording of these cameras will be done for 10 seconds.

- Click **Add**. All the Events and Actions configured for them appear in a list.

Visual Tagging
Satatya Integration

Integration Type
Network

Active
☒

IP Address *
192 . 168 . 111 . 164

Port Number *
8711

Schedule Name

Active
☐

Schedule Range *
00:00
23:59

Days *
☒ Sun
☒ Mon
☒ Tue
☒ Wed
☒ Thu
☒ Fri
☒ Sat
☒ Holiday

Event
Access Allowed

Mode
Both

Action
Recording

Duration Min. *

Camera *

☐ 1
☐ 2
☐ 3
☐ 4
☐ 5

☐ 6
☐ 7
☐ 8
☐ 9
☐ 10

☐ 11
☐ 12
☐ 13
☐ 14
☐ 15

☐ 16
☐ 17
☐ 18
☐ 19
☐ 20

☐ 21
☐ 22
☐ 23
☐ 24

Add
Cancel

Search

Name	Event	Action	Start Time	End Time	Active	
New Schedule	Access Allowed	Recording	00:00	23:59	Yes	

- **Active:** Select this check box to enable the SATATYA Integration functionality.
- **IP Address:** Specify the IP Address of HVR/NVR.
- **Port Number:** Specify the Port Number of HVR/NVR.
- **Schedule Name:** Specify a user friendly Name for the Integration function.
- **Active:** Select this check box to enable the schedule.
- **Schedule:** Specify the Start Time and End Time of the Schedule in HH:MM format.
- **Days:** Select the check boxes for the desired Days on which you wish to apply the Schedule.
- **Event:** Select a COSEC Event for which the action is to be configured from the drop-down list.
- **Mode:** Select the event Mode from the drop-down list options—Entry, Exit, Both if you select the Event as Access Allowed, Access Denied or Invalid User.
- **Action:** Select the Action for the Satatya device from the drop-down list options—Recording, Image Upload, Video Pop-up, PTZ Preset, Mail Image.

If you select **Recording**, specify the **Duration Min..**

If you select **Upload Image**, Images will be uploaded as per the FTP settings.

If you select **Video Pop-up**, specify the **Duration Sec.** The video pop up will be generated on the local client of Satatya device.

If you select **PTZ Preset**, specify the desired **Position No.**

If you select **Mail Image**, specify the **Email ID.**

- **Camera:** Select the check boxes of the desired camera channels depending on the Action selected.

Example 1: For Action as Video Pop up and the camera channel selected is 24, then the pop-up of Camera 24 will be shown for 10 seconds.

Example 2: For Access Allowed event on COSEC Device and the camera channel selected are 4,6,8 and 10, then recording of these cameras will be done for 10 seconds.

- Click **Add**. All the Events and Actions configured for them appear in a list.

Visual Tagging

Satatya Integration

Integration Type

Network

Active

☒

IP Address *

192 . 168 . 111 . 164

Port Number *

8711

Schedule Name

Active

☐

Schedule Range *

00:00

23:59

Days *

☒ Sun
 ☒ Mon
 ☒ Tue
 ☒ Wed
 ☒ Thu
 ☒ Fri
 ☒ Sat
 ☒ Holiday

Event

Access Allowed

Mode

Both

Action

Recording

Duration Min. *

Camera *

☐ 1
 ☐ 2
 ☐ 3
 ☐ 4
 ☐ 5
 ☐ 6
 ☐ 7
 ☐ 8
 ☐ 9
 ☐ 10
 ☐ 11
 ☐ 12
 ☐ 13
 ☐ 14
 ☐ 15
 ☐ 16
 ☐ 17
 ☐ 18
 ☐ 19
 ☐ 20
 ☐ 21
 ☐ 22
 ☐ 23
 ☐ 24

Add

Cancel

Search

Configuring IP Integration Parameters

If you select IP Camera in Capturing Device under Visual Tagging, then configure the following parameters under IP Camera Integration.

Device Configuration

160
VEGA_166
Vega Controller
11/50000
Active

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Visual Tagging

Satatya/IP Camera Integration

Schedule Name *

Active ☒

Event User Allowed

Mode Both

Schedule Range * 00:00 23:59

Days * ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Holiday

Add Cancel

- **Schedule Name:** Specify a user friendly Name for the Schedule for the Device-IP Camera Integration.
- **Active:** Select this check box to activate the schedule for the IP Camera.
- **Event:** Select the desired Event for which the action is to be configured from the drop-down list. The Events will appear in the list based on the availability of the license.



You can configure a maximum 20 Events or Schedules for a single device.

- **Mode:** Select the desired Mode from the drop-down list—Entry, Exit, Both.
- **Schedule Range:** Specify the **Start** and **End Time** for the schedule.
- **Days:** Select the check boxes of the desired days on which you wish run the schedule.

Click **Add** to add the configured schedule. The schedule will be listed in the grid. Then click **Save** to save the schedule integration.

Visual Tagging

Satatya/IP Camera Integration

Schedule Name *

Active ☐

Event User Allowed

Mode Both

Schedule Range * 00:00 23:59

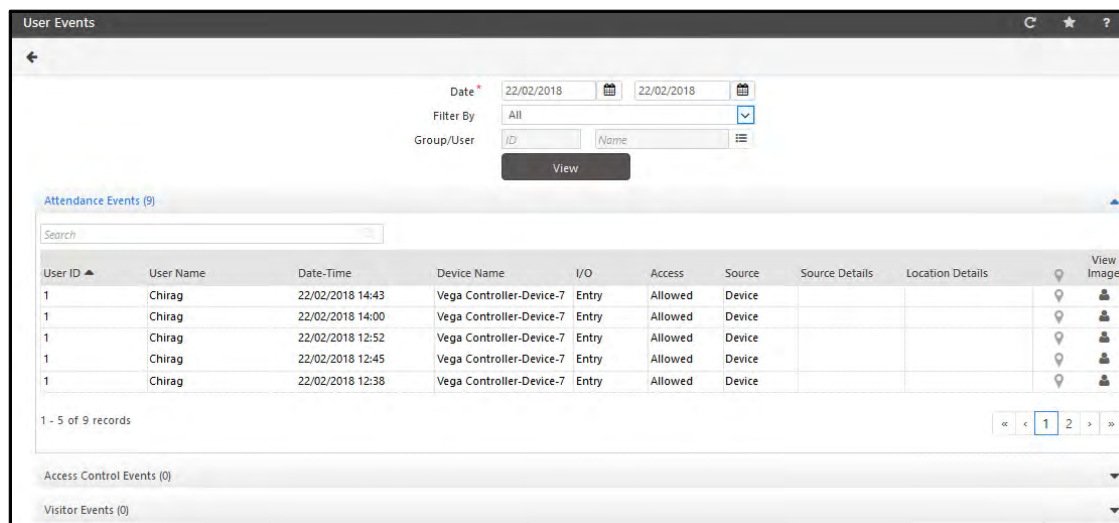
Days * ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Holiday

Add Cancel

Search

Name	Event	Mode	Start Time	End Time	
User Allowed Schedule	User Allowed	Both	09:00	19:00	

When User Event is generated, then snapshot will be taken by the configured camera. The Events can be viewed in User Events (User Module) page and Event View (Admin Module) page. The User Events page displays the details as shown below:

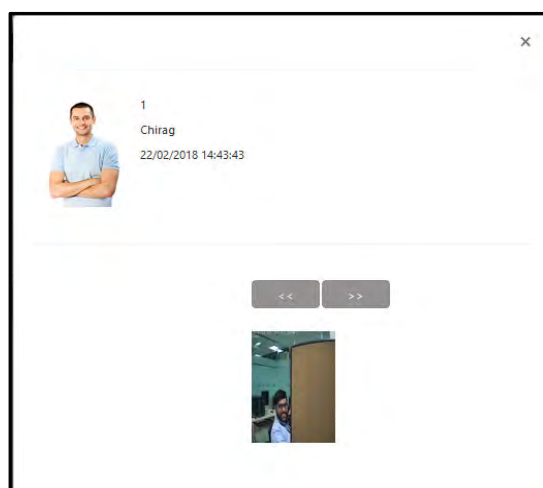


The screenshot shows the 'User Events' interface. At the top, there are filters for Date (22/02/2018), Filter By (All), and Group/User (ID/Name). Below the filters is a 'View' button. The main section is titled 'Attendance Events (9)' and contains a table with the following data:

User ID	User Name	Date-Time	Device Name	I/O	Access	Source	Source Details	Location Details	View Image
1	Chirag	22/02/2018 14:43	Vega Controller-Device-7	Entry	Allowed	Device			
1	Chirag	22/02/2018 14:00	Vega Controller-Device-7	Entry	Allowed	Device			
1	Chirag	22/02/2018 12:52	Vega Controller-Device-7	Entry	Allowed	Device			
1	Chirag	22/02/2018 12:45	Vega Controller-Device-7	Entry	Allowed	Device			
1	Chirag	22/02/2018 12:38	Vega Controller-Device-7	Entry	Allowed	Device			

Below the table, it says '1 - 5 of 9 records' and has pagination controls. At the bottom, there are sections for 'Access Control Events (0)' and 'Visitor Events (0)'.

Click **View Image**, to view the snapshot.



Special Functions



Special Functions is applicable for both Direct Door and Panel Door.

On the **Device Configuration** page, click the **Special Functions** tab in the left pane.

No.	Function Name	Active	Job Selection	User Group	Card 1	Card 2	Card 3	Card 4
1	Official Work - IN	Yes	Yes	All				
2	Official Work - OUT	Yes	Yes	All				
3	Short Leave - IN	Yes	Yes	All				
4	Short Leave - OUT	Yes	Yes	All				
5	Regular - IN	Yes	Yes	All				
6	Regular - OUT	Yes	Yes	All				
7	Break End	Yes	Yes	All				
8	Break Start	Yes	Yes	All				
9	Overtime - IN	Yes	Yes	All				
10	Overtime - OUT	Yes	Yes	All				
11	Enroll User	No	No	All				

To configure *Special Functions* for COSEC doors, refer to [“Special Functions”](#).

Input/Output



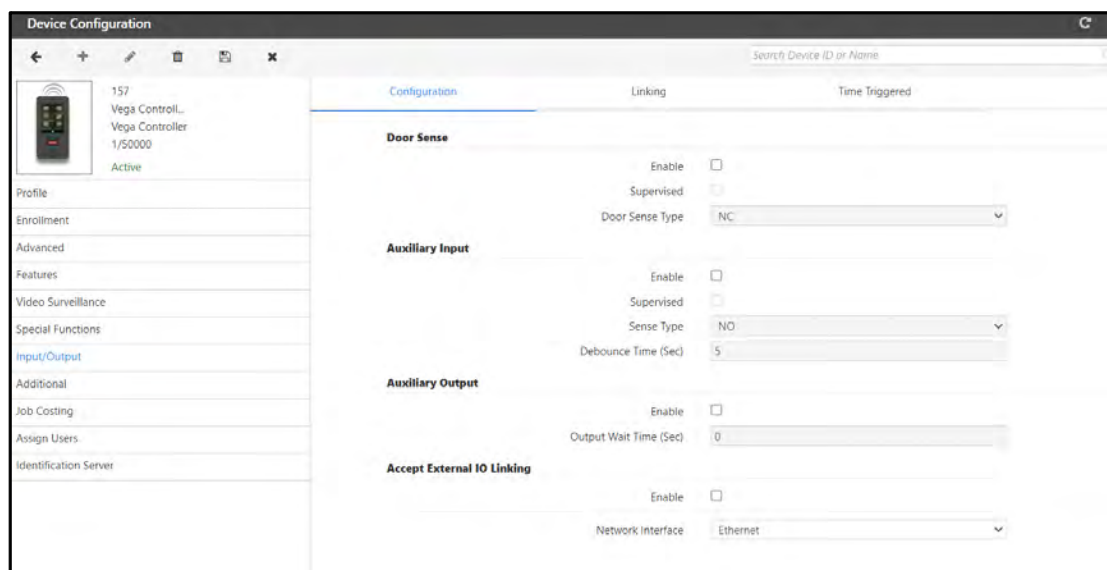
Input/Output is applicable for both Direct Door and Panel Door.

The Configuration Tab is applicable for both Direct Door and Panel Door, whereas Linking and Time Triggered tab is applicable for Direct Door only.

This functionality is available only with the Access Control add-on module license.

The Input/Output (I/O) configuration of a door determines how the output or response of a system is influenced by the input applied on it. In case of the COSEC Access Control System, the I/O configuration should enable the system to monitor and trigger a specific response to any changes in door state or event occurrences at the door device. This change of door state or occurrence of events may be considered as an input while the response or action that is generated by the system on detection of this input, may be defined as the output.

On the **Device Configuration** page, click the **Input/Output** tab in the left pane.



To configure the Input/Output parameters, click the following links:

- [“Configuration”](#)
- [“Linking”](#)
- [“Time Triggered”](#)

Configuration

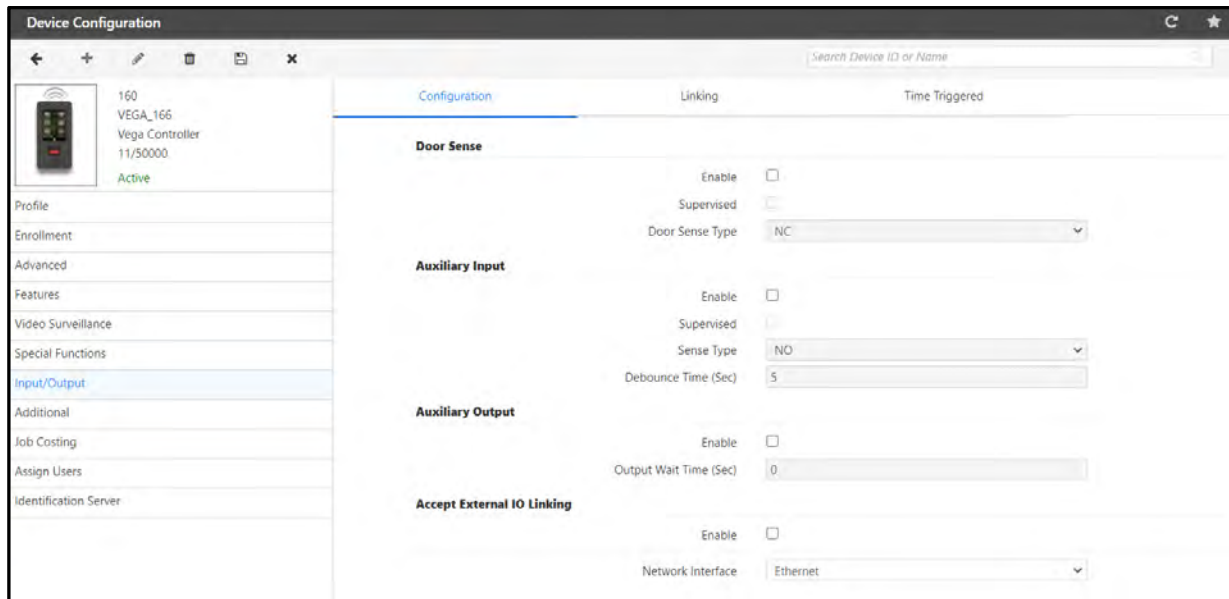


Configuration is applicable for both Direct Door and Panel Door.

Configuration tab differs for Direct Door and Panel Door.

Click **Configuration** tab. The **Configuration** page appears.

For VEGA as **Direct Door**.



Configure the following parameters:

Door Sense

The system by default can sense two states of a door - Normally Open (NO) and Normally Closed (NC) depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a **Door Abnormal** alarm.

- **Enable:** Select the check box to enable the feature.
- **Supervised:** Select the check box to enable the door for four-state monitoring, where the door is also monitored for Door Fault and Door Disconnection.
- **Door Sense Type:** Select the Door Sense Type from the drop-down list options — NO or NC.

Auxiliary Input

- **Enable:** Select the check box to enable the feature.
- **Supervised:** Select the check box to enable the door for four-state monitoring, where the door is also monitored for Door Fault and Door Disconnection.
- **Sense Type:** Select the Sense Type from the drop-down list options — NO or NC.
- **Debounce Time (Sec):** Specify the Debounce Time in seconds. It defines the minimum time for which the door should remain in a given state to enable the system to take action on it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.

Auxiliary Output

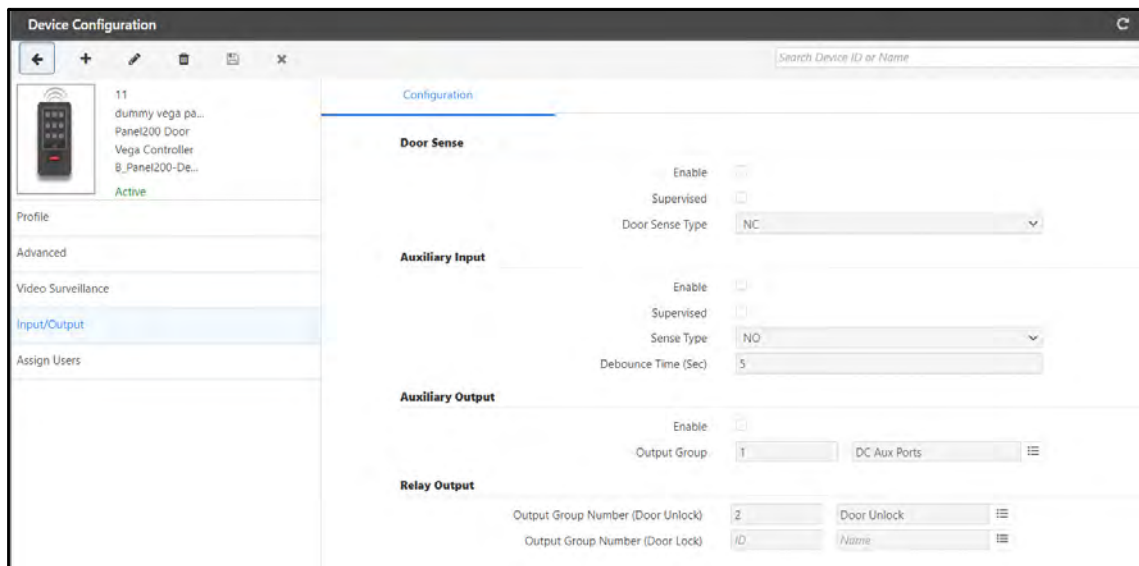
- **Enable:** Select the check box to enable the feature.

- **Output Wait Time (Sec):** Specify the time in seconds that will be set as an additional waiting period before the Aux Output signal is sent.

Accept External IO Linking

- **Enable:** Select the check box to enable device-to-device IO Linking, i.e. input from one Direct Door can trigger output in another Direct Door.
- **Network Interface:** Select the interface option for IO linking with external devices from the drop-down list options—Ethernet, Wireless or Mobile Broadband.

For VEGA as a **Panel Door**.



Configure the following parameters:

Door Sense

The system by default can sense two states of a door - Normally Open (NO) and Normally Closed (NC) depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a **Door Abnormal** alarm.

- **Enable:** Select the check box to enable the feature.
- **Supervised:** Select the check box to enable the door for four-state monitoring, where the door is also monitored for Door Fault and Door Disconnection.
- **Door Sense Type:** Select the Door Sense Type from the drop-down list options — NO or NC.

Auxiliary Input

- **Enable:** Select the check box to enable the feature.
- **Supervised:** Select the check box to enable the door for four-state monitoring, where the door is also monitored for Door Fault and Door Disconnection.

- **Sense Type:** Select the Sense Type from the drop-down list options — NO or NC.
- **Debounce Time (Sec):** Specify the Debounce Time in seconds. It defines the minimum time for which the door should remain in a given state to enable the system to take action on it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.

Auxiliary Output

- **Enable:** Select the check box to enable the feature.
- **Output Wait Time (Sec):** Specify the time in seconds that will be set as an additional waiting period before the Aux Output signal is sent.

Relay Output

- **Output Group Number (Door Unlock):** Select the Output Group Number to which the device output for Door Unlock is to be assigned from the picklist.
- **Output Group Number (Door Lock):** Select the Output Group Number to which the device output for Door Lock is to be assigned from the picklist.

Linking



Linking is applicable for Direct Door only.

The COSEC application supports the Input/Output Linking feature to activate an output port based on a trigger received from an input port on the same Direct Door. This option enables the administrator to define how an event or events (input port) will trigger an output on the door.

Click **Linking** tab. The **Linking** page appears.

The screenshot shows the 'Device Configuration' window for device 160 VEGA_166. The 'Linking' tab is selected, showing a table of linking rules. The table has columns for Name, Active Input, Output, Output Type, Pulse Time(Sec), Reset Link, Reset Time, and Supported Devices. There are 5 records displayed, showing various input events like Aux. Input, Duress, and Intercom Panic triggering different outputs like Aux. Output and Door Relay.

Name	Active Input	Output	Output Type	Pulse Time(Sec)	Reset Link	Reset Time	Supported Devices
	No Aux. Input	Aux. Output			Inactive	00:00	0 »
	No Aux. Input	Door Relay			Inactive	00:00	0 »
	No Duress	Aux. Output			Inactive	00:00	0 »
	No Duress	Door Relay			Inactive	00:00	0 »
	No Intercom Panic	Aux. Output			Inactive	00:00	0 »

1 - 5 of 12 records

Select a Input-Output linking row or click edit button.

- **Name:** Specify a Name for the new I/O linking program to be defined.
- **Active:** Select this check box to enable the IO Linking.
- **Output Type:** Specify the required type of Output from the drop-down list options—Pulse, Interlock, Latch, Toggle.

If you select **Pulse**, the output will be active for the defined pulse time, for example, 5 sec.

If you select **Interlock**, the output follows the input. The output will be active till the input is active, after which it returns to normal state.

If you select **Latch**, the relay output will be in energized condition for infinite period and needs to be reset manually. It means once the input is active, output will be active. It has to be reset manually. For example, during a Fire alarm, door should be unlocked permanently so Latch output can be used.

If you select **Toggle**, the output group toggles its state whenever an input group is activated.

- **Pulse Time (sec):** If you select the Output Type as **Pulse**, specify the time until which the output should be active.
- **Reset Link:** Select this check box to enable the system to reset the IO link.
- **Reset Time:** Specify the time after which the IO link should be reset in HH:MM format.
- **Supported Devices:** All devices supported for external IO Linking will appear in this picklist for selection. Select the required devices from the picklist. Upto 255 external devices can be added.

Click **OK** and then **Save** to save the configuration.

Time Triggered

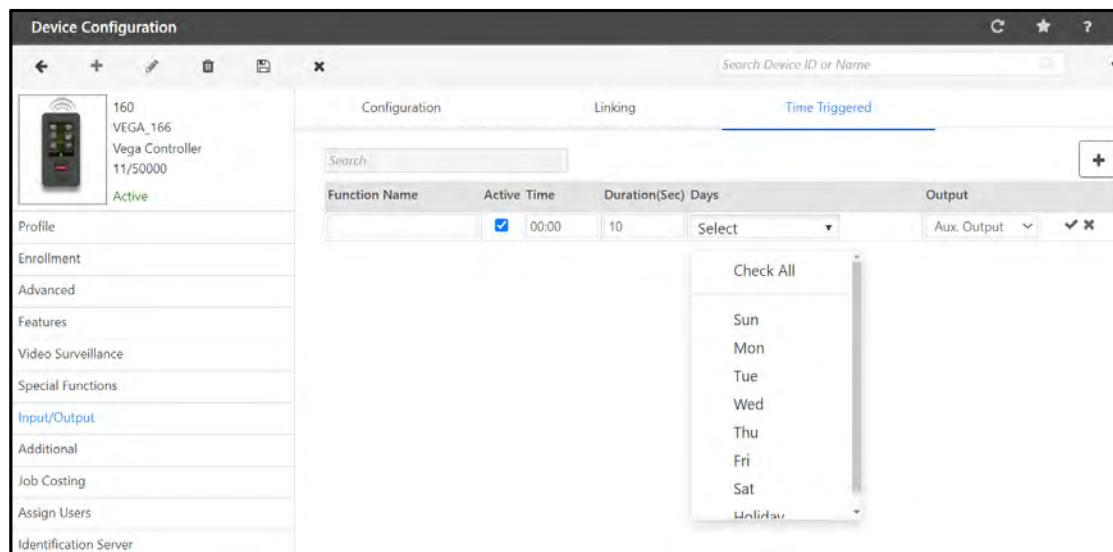


Time Triggered is applicable for Direct Door only.

This functionality enables the user to control the activity of an Output without manual intervention. The output gets active without the status of input, i.e. the selected output is triggered based on the configured time and not the IO link.

The time triggered functions are used for activating events like door unlock and siren activation that are set as per the start time and for the configured time duration. This functionality is designed to trigger outputs for predefined periods at the configured time. The COSEC access control system supports up to 20 Time Triggered functions on a Direct Door.

Click **Time Triggered** tab. The **Time Triggered** page appears.



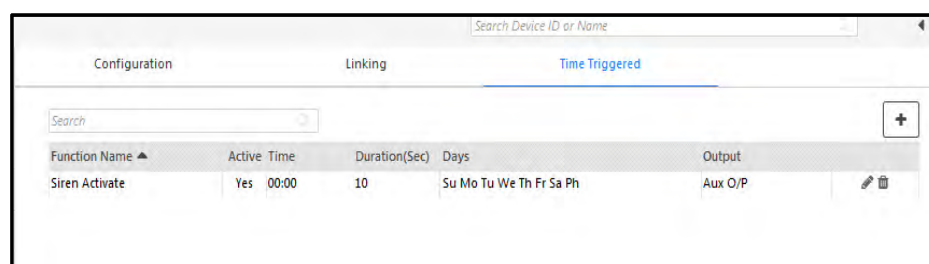
This functionality enables the user to control the activity of an Output without manual intervention. The time triggered functions are used for activating events like door unlock and siren activation that are set as per the start time and for the configured time duration. This functionality is designed to energize outputs for predefined periods at the configured time. The COSEC access control system supports up to 20 Time Triggered functions on a Direct Door.

Click **Add**.

Configure the following parameters:

- **Function Name:** Specify a user friendly Function Name.
- **Active:** Select this check box to enable the Time Triggered function.
- **Time:** Specify the time when the Time Triggered function should be activated.
- **Duration:** Specify the time duration for which the Time Triggered function should be active.
- **Days:** Select the check boxes for the desired days on which you wish to apply the Time Triggered function from the drop-down list. Click **Check All**, if you wish to select all the days.
- **Output:** Select the Output on which the Time Triggered function should be applied from the drop-down list options—Aux Output or Door Relay.

Click **OK** and then **Save** to save the settings.



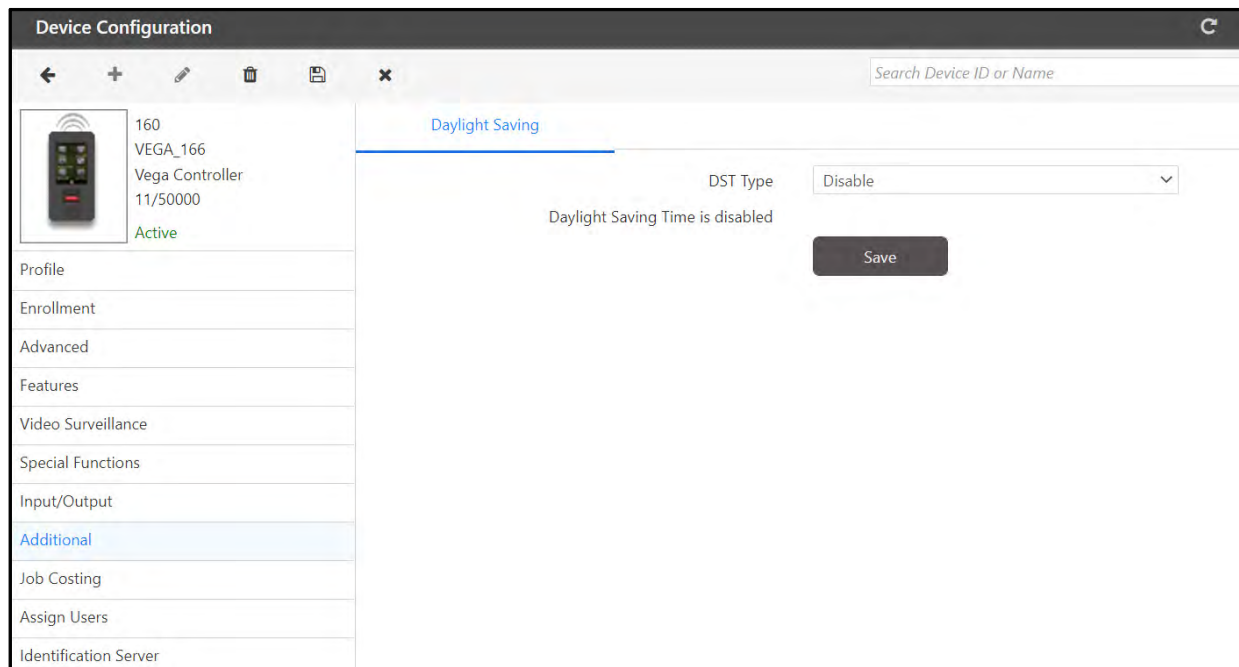
Additional



Additional is applicable for Direct Door only.

Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. COSEC doors can be configured to be compatible with this procedure keeping the RTC of the system updated with such changes

On the **Device Configuration** page, click the **Additional** tab in the left pane.



The **Daylight Saving** configuration can be done in 2 ways — Day-Month wise or Date-Month wise.

- **DST Type:** Select the **DST Type** as Day-Month wise or Date-Month wise. Select Disable, if you wish to disable the application of DST on the system time.

If you select the **Day-Month wise** option, configure the following parameters.

Daylight Saving

DST Type
Day-Month wise
Time Period
00:00

Forward Clock
Month
January
Week No.
1st
Day of Week
Sunday
Time
00:00

Backward Clock
Month
January
Week No.
1st
Day of Week
Sunday
Time
00:00

Save

- **Time Period:** Specify the time period by which the time period will be set forward or backward to achieve Daylight Saving.

Forward Clock

- **Month:** Select the month when the DST starts for the Forward Clock from the drop-down list.
- **Week No.:** Select the week of the month when the DST starts for the Forward Clock from the drop-down list. For example, if DST starts from 4th week of March, select 4th.
- **Day of Week:** Select the day of the week when the DST starts for the Forward Clock from the drop-down list.
- **Time:** Specify the time when the DST starts for the Forward Clock in HH:MM format.

Backward Clock

- **Month:** Select the month when the DST ends for the Backward Clock from the drop-down list.
- **Week No.:** Select the week of the month when the DST ends for the Backward Clock from the drop-down list. For example, if DST starts from 4th week of March, select 4th.
- **Day of Week:** Select the day of the week when the DST ends for the Backward Clock from the drop-down list.
- **Time:** Specify the time when the DST ends for the Backward Clock in HH:MM format.

Click **Save** to save the configurations.

If you select the **Date-Month wise** option, configure the following parameters.

Daylight Saving

DST Type
Date-Month wise
Time Period
00:00

Forward Clock
Month
January
Date
1
Time
00:00

Backward Clock
Month
January
Date
1
Time
00:00

Save

- **Time Period:** Specify the time period by which the time period will be set forward or backward to achieve Daylight Saving.

Forward Clock

- **Month:** Select the month when the DST starts for the Forward Clock from the drop-down list.
- **Date:** Select the date of the month when the DST starts for the Forward Clock from the drop-down list.
- **Time:** Specify the time when the DST starts for the Forward Clock in HH:MM format.

Backward Clock

- **Month:** Select the month when the DST ends for the Backward Clock from the drop-down list.
- **Date:** Select the date of the month when the DST ends for the Backward Clock from the drop-down list.
- **Time:** Specify the time when the DST ends for the Backward Clock in HH:MM format.

Click **Save** to save the configurations.

Suppose, the DST period in a region is from Sunday, 27 March at 02:00:00 hours till Sunday, 30 October at 03:00:00. If DST is configured according to this period and the **Time Period** is specified as 1 hour, the clock will be forwarded by 01:00 hours on 27 March at 02:00:00 hours. The clock will be set back by 01:00 hours on 30 October at 03:00:00.

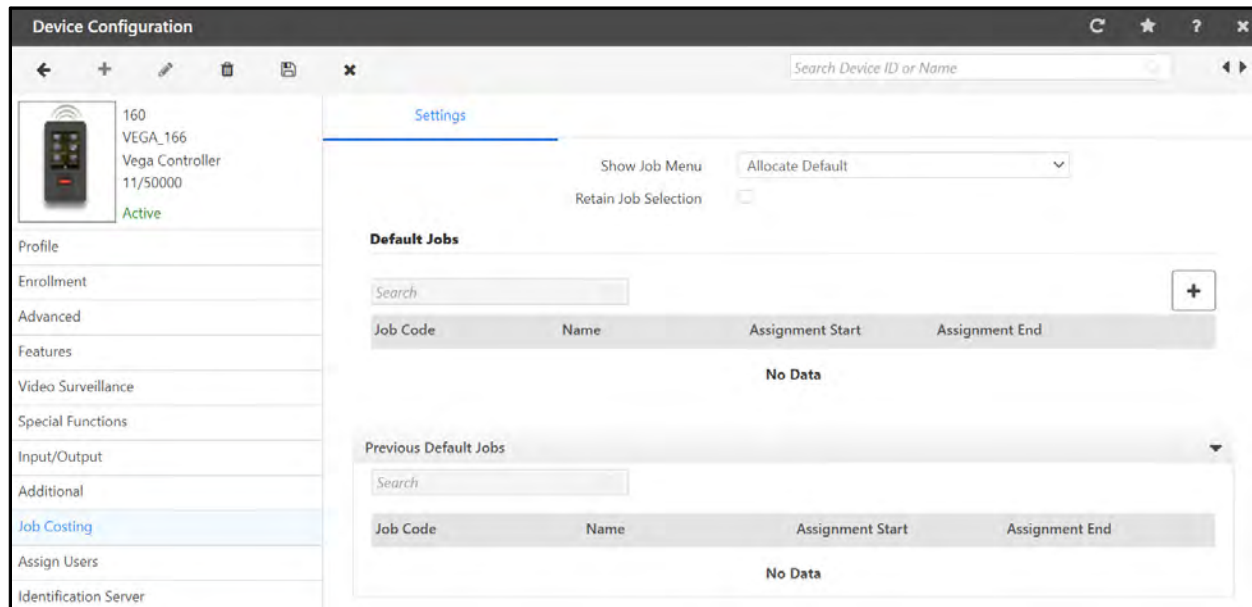
Job Costing



Job Costing is applicable for Direct Door only.

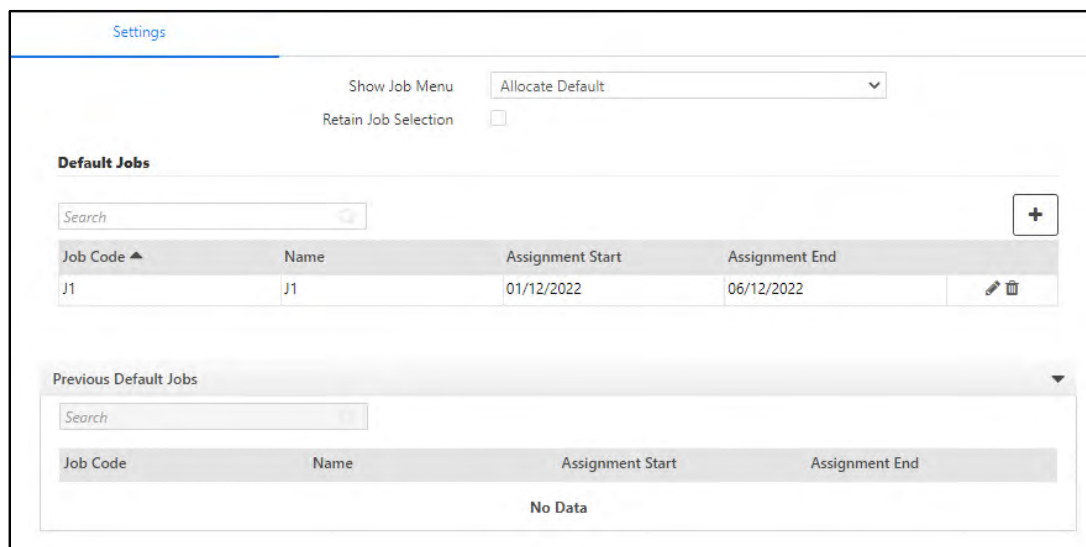
When user punches on any device, there will be an option to select the Job Code on which the user is working. Job Costing enables the Administrator to show or hide Job Code selection on device. It also enables the Administrator to assign default jobs on device.

On the **Device Configuration** page, click **Job Costing** tab in the left pane.



Settings

Click **Settings** tab. The **Settings** page appears.



- **Show Job Menu:** Select the Job Menu to be displayed from the drop-down list options— **Show List** or **Allocate Default**.

If you select **Show List**, configure the following parameters.

Settings

Show Job Menu: Show List

Retain Job Selection: ☒

Assign Jobs

Job Group: ID [] Name []

Job: ID [] Name []

Search []

Job Code	Name	Assignment Start	Assignment End	
J1	J1	01/12/2022	06/12/2022	

- **Retain Job Selection:** Select this check box to retain the Job Code selected by a user which would be applicable for all the subsequent users until another job selection is done on the device.

Assign Jobs

- **Job Group:** Select the desired Job Group from the picklist.
- **Job:** Select the desired Job from the picklist.

Click **Save**. The jobs will be listed to the grid.

If you select **Allocate Default**, configure the following parameters.

Settings

Show Job Menu: Allocate Default

Retain Job Selection: ☐

Default Jobs

Search []

Job Code	Name	Assignment Start	Assignment End	
J1	J1	01/12/2022	06/12/2022	

Previous Default Jobs

Search []

Job Code	Name	Assignment Start	Assignment End
No Data			

Default Jobs

Click **Add**, to add the default job for the door.

- **Job Code:** Select the desired Job Code from the picklist. The Job Name appears once you select the Job Code.
- **Name:** Select the desired Name from the picklist. The Job Code appears once you select the Name.

- **Assignment Start:** The Assignment Start date appears once you select the Job Code or Name. You can also specify the Assignment Start date, if required.
- **Assignment End:** The Assignment End date appears once you select the Job Code or Name. You can also specify the Assignment End date, if required.

Click **OK** and then click **Save**.

When the assignment date of the default job gets elapsed, then the particular job will be listed in **Previous Default Jobs** section.

Assign Users



Assign Users is applicable for both Direct Door and Panel Door.

You can select and assign users to the door.


On the **Device configuration** page, click **Assign Users**. The Assign Users page appears.

ID	Name	Delete
1	ar3	
1000	test_15	
101	JK_101	
102	JK_102	
103	JK_103	
105	Test_105	
1111	Test_08	
1212	test_16	
123	123	
5003	test5003	

- **Users:** Click the picklist. The Picklist For All Users window appears.

Select the check boxes of the desired Users and click **OK**.

The grid displays the list of selected users.

If you wish to remove any assigned user, click the respective **Delete**  icon.

- Click **Save**.

Cafeteria



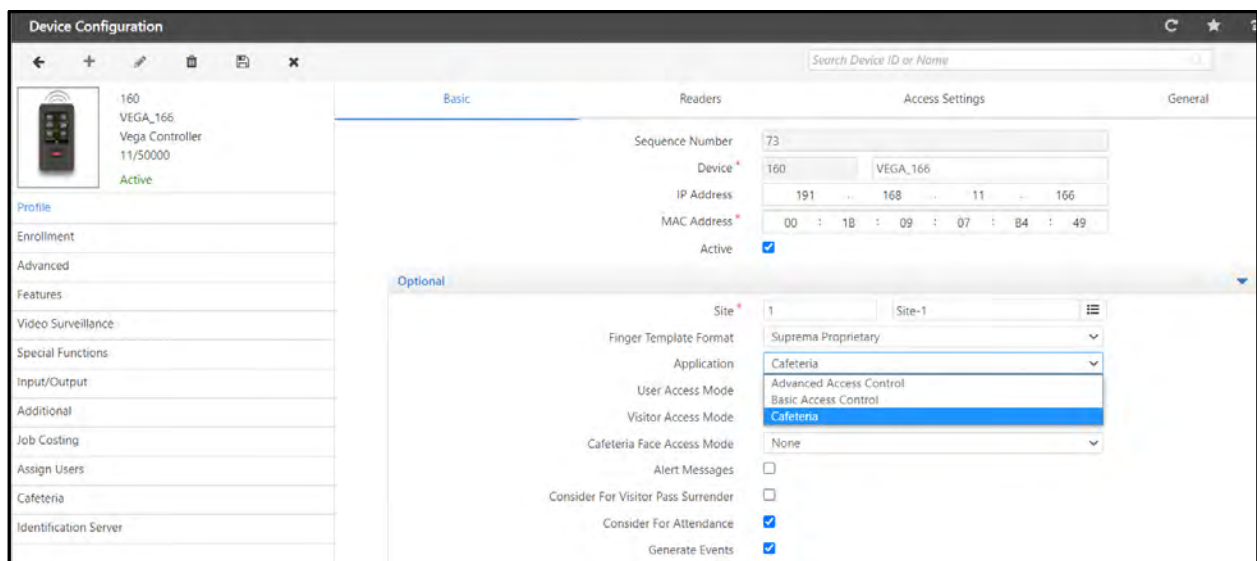
Cafeteria is applicable for Direct Door only.

*The Cafeteria tab will be available only if you have selected the **Application** option as **Cafeteria**. For details, refer to [“Profile”](#).*

The system enables you to configure devices which will be used for Cafeteria Management. To configure a door for Cafeteria application,

On the Device Configuration page, click **Profile**. Click **Optional** collapsible panel.

Select **Cafeteria** in **Application**.



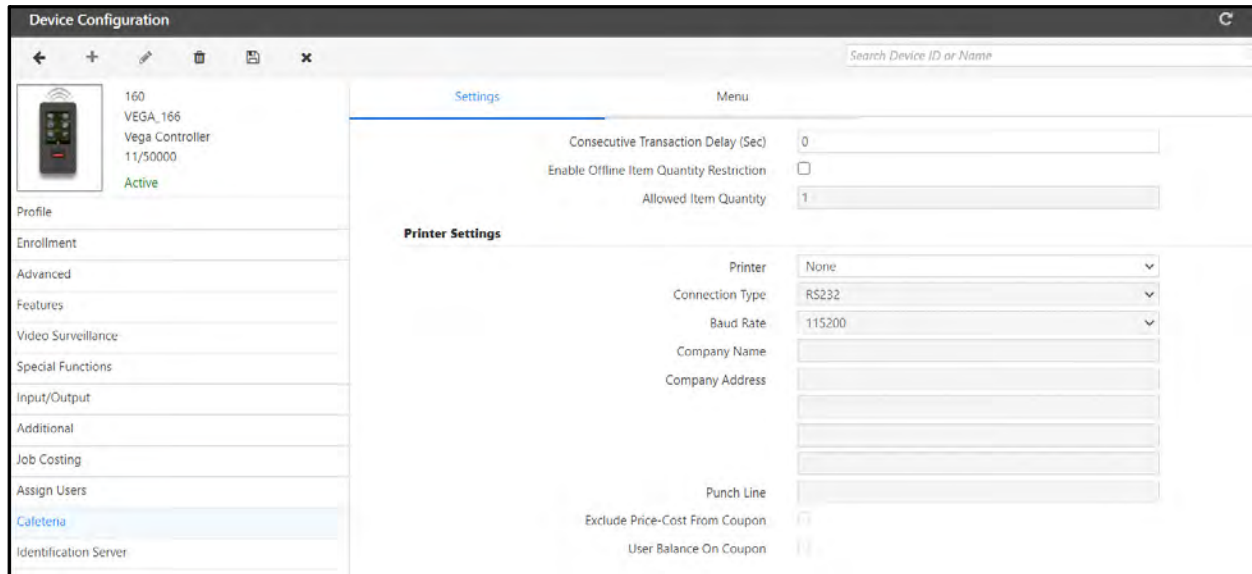
On the Device Configuration page, click the **Cafeteria** tab on the left pane.

To configure the Cafeteria parameters, click the following links:

- [“Settings”](#)
- [“Menu”](#)

Settings

Click **Settings** tab. The **Settings** page appears.



Configure the following parameters:

- **Consecutive Transaction Delay (Sec):** Enter the time interval after which you wish to allow the second transaction from the same user.
- **Enable Offline Item Quantity Restriction:** Select the check box if you wish to restrict the transaction on exceeding the item quantity while the device is in offline mode.
- **Allowed Item Quantity:** Specify the quantity to be allowed for each item when the device is in offline mode. This will be applicable for each item present in the Menu.

For example, if the Menu has two items Tea and Poha and you have configured the **Allowed Item Quantity** as 2, and if the device is offline, the user/worker will be allowed to consume Tea twice as well as Poha twice.

Printer Settings

- **Printer:** Select the desired **Printer** as per your site requirements from the drop-down list—EpsonTM88IV, EpsonTM88V, EpsonTMT90, WEPTM400.
- **Connection Type:** Select the Printer **Connection Type** from the drop down list—RS232 (serial), USB.
- **Baud Rate:** Select the appropriate **Baud Rate** from the drop-down list—9600, 1 9200, 38400, 57600, 115200.
- **Company Name:** Specify the **Company Name** as per your site requirement.
- **Company Address:** Specify the **Company Address** as per your site requirement.
- **Punch Line:** Specify the **Punch Line** as per the site requirements.

The Company Name, Company Address as well as Punch Line will be printed on the Cafeteria receipt dispensed from the selected printer.

- **Exclude Price-Cost From Coupon:** Select this check box, if you wish to exclude the price from the coupon.
- **User Balance On Coupon:** Select this check box, if you wish to print the Current Balance/Current Month Usage and Weekly Remaining Limit on the Cafeteria receipt.

For pre-paid account users, Current Balance and Weekly Remaining Limit will be printed.

For post-paid account users, Current Month Usage and Weekly Remaining Limit will be printed.

For details refer to [“Cafeteria Usage Policy”](#).

Menu

COSEC allows the you to assign one or more Cafeteria Menus (Menu 1, Menu 2, Menu 3... upto 99.) to a device. These can be configured by selecting pre-defined menus from the Menu picklist.



To create Menu's, refer to [“Menus”](#) in the Cafeteria Module.

Click **Menu** tab. The **Menu** page appears.

Configure the following parameters:

- **Assign Menu:** Click the **Assign Menu** collapsible panel.
 - **Menu:** Click the picklist and select the desired Menu or you can also enter the Menu **ID** or **Name** manually.

Click **Save**.

- **Schedule Menus:** Click the **Schedule Menus** collapsible panel.

Click Add and configure the following:

- **Menu No:** This displays the **Menu No.** after you have saved the Scheduled Menu.

- **ID:** Click the picklist and select the Menu **ID**.
- **Menu Name:** The **Menu Name** is auto-generated.
- **Start Time:** Specify the **Start Time** for which the Menu will be active and is available to users on this door.
- **End Time:** Specify the **End Time** after which the Menu will be not be active and will not be available to users on this door.



Two Menus cannot be scheduled for the same timing.

- **Schedule Days:** Select the desired **Days** for which this Menu will be applicable on the door or select **All**, if you wish to apply this Menu for all the days.
- Click **OK** and then click **Save**.

Identification Server

This tab enables the device to be assigned to a pre-defined Identification Server.

The door has a limited memory capacity for storage of templates so, we can assign an Identification Server which will store the templates for the door and will respond to the door when asked for identification.

For more information on Identification Servers, refer to [“Identification Server”](#).

On the **Device Configuration** page, click the **Identification Server** tab in the left pane.

160
VEGA_166
Vega Controller
11/50000
Active

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Settings

Face Recognition

Enable FR

☐

Face Capturing

Tap & Go

Enable Time Out

☐

Free Scan Time Out (Sec)

30

IP Camera MJPEG URL

User Name

Username

Password

FR Mode

Local

Server Address *

192.168.50.2

Server Port *

12000

Identification Time-Out Duration (Sec)

4

Group FR

☐

Exceptional Face Enrollment

☒

Face Enrollment

Conflict Check

☒

Conflict Matching Threshold (Face) *

93.00

Face Enrollment

Conflict Check

☒

Conflict Matching Threshold (Face) *

93.00

Adaptive Face Enrollment

Adaptive Face Enrollment

☐

Threshold Deviation (Face)

02.0

Multi-User Matching Score Deviation (Face)

02.0

Confirm Before Adaptive Face Enrollment

☐

Face Antispoofing

Face Anti-Spoofing

☐

Camera Mount

Wall Mount

Face Anti-Spoofing Mode

Advance

Face Anti-Spoofing Threshold

62.00

Other Biometric Credentials

Enable Identification On Server

☐

Identification Server

ID
Name

Configure Alternate Server Address

☐

Server Address

Server Port

11005

Enable Finger Smart Identification

☐

Identification Time-Out Duration (Sec)

4

Auto Send Enrolled Templates

☒

Default Biometric Group No.

0

Face Recognition



Make sure **“Enable FR”** check box is selected and **Basic Access Control** application is selected in **Devices > Device Configuration > Profile > Basic > Optional > Application** in order to edit the parameters in **Identification Server Settings**.

- **Enable FR:** Select this check box to enable the Face Recognition feature on the device.
- **Face Capturing:** Select the desired Face Capturing option — **Tap & Go**, **Free Scan**.
 - **Tap and Go:** If you select this option, user needs to tap on the device screen once. The MJPEG, that is motion recording screen appears. Device will capture and then identify the users face. If during working hours device is idle, then user needs to tap device to scan the face and gain access.
 - **Free Scan:** If you select this option, device will display the MJPEG, that is motion recording screen till the expiry of the Free Scan Time Out timer.
- **Enable Time Out:** Select this check box to enable the time out for the Free Scan Mode and set the time in Free Scan Timer Out (Sec).
- **Free Scan Time Out (Sec):** Specify the **Free Scan Time Out** duration. The valid range is 1 to 999 sec.

In Free Scan method, multiple users can mark their attendance easily during peak entry hours.

For example, if the Free Scan Time Out is set as 30 sec and if the user is identified in 10 sec then the system reloads the Free Scan Time Out timer again. Hence, device remains in the scanning mode.

- **IP Camera MJPEG URL:** Specify the URL for accessing the IP camera to receive the motion stream on the door. For example, <http://192.168.104.48:80/matrix-cgi/mjpeg?profile-no=3>.

If the device is auto-added then the default value will be <http://192.168.1.126/matrix-cgi/mjpeg?profile-no=4>.

- **User Name:** Specify the User Name for accessing the IP camera. For example, admin.
- **Password:** Specify the Password for accessing the IP camera. For example, admin123.

This will fetch the motion stream from camera to device screen. When the users show their face on camera, the face will be captured and after identification, the user will be allowed access and the punch will be marked.

- **FR Mode:** Select the desired **FR Mode** from the drop-down list—Local, Server Assisted.
 - **Local:** In this mode the face templates will be stored in the FR hardware module which can store 1 lakh face templates. The captured face template will be verified with the templates already stored in FR module.
 - **Server Assisted:** In this mode, the face templates will be stored directly in the Server. You must first configure the Identification Server from where the face templates will be matched and identified.

When FR Mode is selected as **Local** configure the following parameters:

- **Server Address/Port:** Specify the **IP Address** and **Port** of the FR Server.
- **Identification Time-Out Duration (Sec):** Specify the **Identification Time-Out** in seconds, after which the face template identification process will stop.

For example, if **Identification Time-Out Duration (Sec)** is 5 seconds, then the Identification Server will try to identify the face template until 5 seconds and if not found then it will stop and display time-out to the user.

When FR Mode is selected as **Server Assisted**, configure the below fields:

User can either assign a separate or a common Identification Server which is shared by other biometric credentials.

Face Recognition

Enable FR ☒

Face Capturing Tap & Go

Enable Time Out ☐

Free Scan Time Out (Sec) 30

IP Camera MJPEG URL * http://192.168.1.126/matrix-cgi/mjpeg?profile-no=4
Note: Mention the protocol in URL.

User Name *

Password * *****

FR Mode Server Assisted

Identification Server ID Name

Configure Alternate Server Address ☐

Server Address

Server Port 11005

Identification Time-Out Duration (Sec) 4

Group FR ☐

Exceptional Face Enrollment ☐

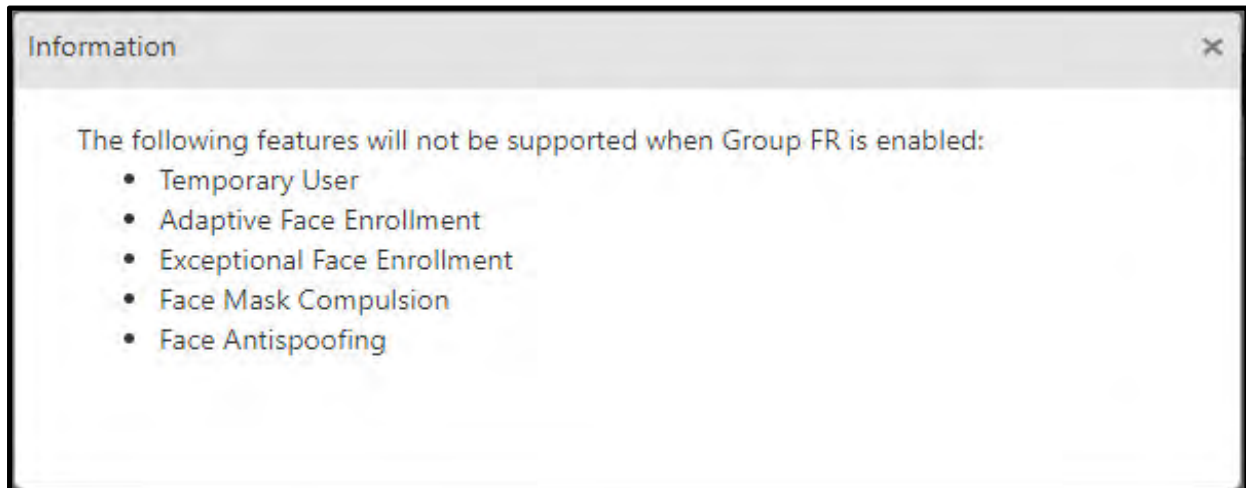
- **Identification Server:** Select an Identification Server using the picklist button to which the device is to be assigned. The configuration of Identification Server is done from **Admin module > System Configuration > Identification Server Configuration** and make sure you start the Identification Service from the service tray. This IP Address of this Identification Server is displayed in **Server Address**.
- **Configure Alternate Server Address:** Select this check box to configure an external IP Address of the FR Identification Server and configure the Server Address.
 - **Server Address:** By default it displays the IP Address of the selected Identification Server. Enter the external network IP address which will be used for accessing Identification Server.
- **Server Port:** Enter the TCP Port number. Default: 11005.

- **Identification Time-Out Duration (Sec):** Specify the duration in seconds after which the face template identification should stop.

For example, if 5 seconds is specified, then the Identification Server will try to identify the template till 5 seconds and if not found then it will stop the identification process and display time-out to the user.

- **Group FR:** Select this check box to enable face recognition feature for multiple users and mark their attendance at the same time via this door.

Once you enable Group FR, a pop-up appears.



The features listed in the pop-up will not be functional.

- **Exceptional Face Enrollment:** Select this check box to enroll exceptional faces of users via this door.



For Group FR (“[Mark Group Attendance](#)”) and Exceptional Face Enrollment feature to work, ensure that the desired Identification Service is selected in COSEC Admin > License and Service. For more details refer, Admin Management Portal User Manual.

If you have enabled the **Exceptional Face Enrollment** feature then make sure that you schedule a task of **Delete Exceptional Face** in Admin > System Utilities> Task Scheduler to avoid storage of excess data in the database.

Face Enrollment



If the **FR Mode** is **Server-Assisted** and you wish to enroll faces from the device, make sure **Enable Face Recognition** is selected in Users > User Configuration > Face Recognition and/or Visitor Management > Visitor Profile > Face Recognition and/or Contract Worker Management > Worker Profile > Face Recognition.

- **Conflict Check:** Select this check box for the system to check the conflict between the new face of a user and the already (existing) enrolled faces of all the users (available in the database) during the face enrollment process.
- **Conflict Matching Threshold:** Enter the desired Conflict Matching Threshold value in percentage.

The system will consider this value while comparing the face with the face templates already present in the database.

If a conflict is found, that is, if the system detects a face template in the database similar to the new face, then a conflict error will be displayed.

Make sure a higher value is set for this parameter, as it will result in less equivalent matches with the face templates available in the database.



Make sure the **Conflict Matching Threshold** is set lower than **Matching Threshold** in **Admin module > System Configuration > Identification Server Configuration**.

For example: Face Enrollment of Suresh

- **Conflict Check** check box is selected.
- **Conflict Matching Threshold** is set as 93%.

Now during the face enrollment of Suresh, the system will check in its database if his face matches with faces of other users available in the database.

- **Case 1:** If Suresh's face matches 92% with Ram, then the system will allow to enroll Suresh's face.
- **Case 2:** If Suresh's face matches 94% with Shyam, then the system will display the conflict error while enrolling Suresh's face.

Adaptive Face Enrollment

- **Adaptive Face Enrollment:** Adaptive Face Enrollment provides automatic real time face enrollment whenever change is experienced in facial features. By enabling Adaptive Enrollment process parameter, an additional slot will be provided internally to store 10 more face templates of a user. IDS will learn from face recognized, adapt and would take decision of storing new template of a user database.

Select this check box to enable Adaptive Face Enrollment for Identification Server.

If you enable Adaptive Face Enrollment, configure the following parameters:

- **Threshold Deviation (Face):** Specify the value of deviation from Matching Threshold in percentage. Based on the value entered for deviation, template for Adaptive Face Enrollment will be decided. Value can be set in decimal.

For example, if Deviation entered is 3% and Matching Threshold is 98% then it will classify template which has matching score between 98 - 95.

- **Multi-user Matching Score Deviation (Face):** Enter the value of deviation from matching score between 2 different users while Adaptive Face Enrollment.

Difference between matching scores of templates will be considered, when we have templates of two or more users falling under the specified deviation. Value can be set in decimal.

For example, let's consider the following parameters:

- Threshold Value = 98%
- Threshold Deviation = 3%

So, the result will display all matching templates having matching score between range 98 to 95.

- Now if you have set Multi-user Matching score deviation = 0.5%.

If 5 best templates of 2 users fall between 98 -95% range as follows.

User	Matching Score
User 1	97.8
User 1	97.6
User 1	97.4
User 2	97.25
User 2	97

As we have obtained templates of 2 users in which user 1 is having template of highest matching score, so will make a difference between lowest score template of user 1 and highest matching score template of user 2.

$97.4 - 97.25 = 0.15$; this is less than 0.5.

As difference is less than 0.5, user 1's template having matching score 97.8 for adaptive enrollment will not be used.

Both, Threshold Deviation and Multi-user Matching score deviation will act as two filters to fetch appropriate template for Adaptive Enrollment.



We recommend to set the Multi-user Matching Score Deviation (Face) as a higher percentage.

For example, if Multi-user Matching Score Deviation (Face) is set as 2.0, it reduces the probability of enrolling a particular user's face template in some different user's enrolled faces.

- **Confirm before Adaptive Face Enrollment:** Select this check box, if face enrolled using Adaptive Face Enrollment requires a confirmation.



Faces enrolled under Adaptive Enrollment process will be synced automatically with the IDS, but when IDS is restarted due to any reason, the adaptive faces which are not synced will be removed by default.

Face Anti-Spoofing

- **Face Anti-Spoofing:** To use this feature, make sure **Enable FR** check box is selected in **Devices> Device Configuration> Identification Server > Face Recognition > Enable FR**.

Select the **Face Anti-Spoofing** check box to enable this feature and configure the following parameters:

- **Camera Mount:** Select the desired Camera Mounting option from the drop-down list — **Wall Mount** or **Ceiling Mount**.

There is an impact of Camera Mounting in face liveness detection. Default: Wall Mount.



For Wall Mount, make sure the distance between camera and user is less than 3 feet for proper detection of face.

- **Face Anti-Spoofing Mode:** Liveness Detection helps to limit the fierce risk of spoofing attacks by using several anti-spoofing approaches. Along with the configurations to be done for Face Anti-Spoofing, you also need to take care of the recommended settings for Liveness Verification and for Face Recognition as well as the Camera Settings, refer [“Recommendations for Liveness Verification”](#), [“Recommendations for Face Recognition”](#) and [“Recommended Camera Settings for Liveness Verification”](#).

Select the **Face Anti-Spoofing Mode** for liveness detection from the drop-down list—Basic, Moderate, Advance.



If Ceiling Mount. is selected as the Camera Mount option, only Basic option of Face Anti-Spoofing Mode is applicable

Basic: The Basic Mode detects face as well as photos from the mobile phones. Select this option, when the distance between Camera and Face is more than 3 feet

Moderate: The Moderate Mode analyzes the texture of face. Select this option, when the distance between Camera and Face is less than 2 feet.

Advance: The Advance Mode combines the features of **Basic Mode** and **Moderate Mode** of Face Anti-Spoofing. Select this option, when the distance between Camera and Face is more than 1 feet and less than 2 feet. Default: **Advance**.

- **Face Anti-Spoofing Threshold:** Enter the Face Anti-Spoofing Threshold value in percentage within the range from 1.00 to 99.99 to identify user's face liveness for considering him/her as genuine person. As per the Face Anti-Spoofing Mode that you have selected, the Threshold value will vary.

Other Biometric Credentials

- **Enable Identification On Server:** Select this check box to enable identification of palm/finger templates on this device.
- **Identification Server:** Select an Identification Server using the picklist to which the device is to be assigned. The configuration of Identification Server is done from **Admin module > System Configuration > Identification Server Configuration** and make sure the Identification Service is started from the service tray. The IP Address of this Identification Server is displayed in **Server Address**.
- **Configure Alternate Server Address:** Select this checkbox to configure external IP address of Identification Server.
- **Server Address:** By default it displays the IP Address of the selected Identification Server. Enter the external network IP address which will be used for accessing identification server.
- **Server Port:** Specify the Server Port number. Default:11005.
- **Enable Finger Smart Identification:** Select this check box to enable the identification of fingerprint templates through Identification Server.
- **Identification Time-Out Duration (Sec):** Enter the duration in seconds after which the fingerprint template identification will stop and time out will be displayed to the user. For example, if 5 seconds is specified,

then the identification server will try to identify the template till 5 seconds and if not found then it will stop the identification and display time out to the user.

- **Auto Send Enrolled Templates:** Select this check box to enable any enrolled templates to be saved both in the COSEC database as well as saved locally in the configured Identification Server. This enables prompt identification of user on enrollment.
- **Default Biometric Group No.:** Specify the default Biometric Group Number to be assigned to the device. It is a number allotted to a device to be assigned to the Identification Server. This enables the Identification Server to match the template against only those devices that belong to the corresponding biometric group. This reduces false detection as well time to search template.

Accessing the Door using QR code

The user can access the COSEC device using COSEC APTA installed in the mobile device. If the user has rights for COSEC APTA and access to this device is allowed to the user, then he can use his mobile device to scan the QR code which constitute the details of the door.

There is icon for QR code on COSEC APTA application. Clicking that icon will open the camera in your mobile. Now using the mobile camera you can scan the device QR code. The COSEC door will open after verifying the security key and access policies assigned to the user.

Steps to create a QR code

Step 1: Enter details in JSON format

```
{"version":"x","ip": "x.x.x.x","port":"x","pdid":"x","mode":"x"}
```

Valid values:

Field	Field range	Default Value	Remark
version	1-255	1	
ip	0.0.0.0-255.255.255.255	0.0.0.0	
port	0-65535	0	
pdid	0-255	0	If door is in direct door mode then, then PDID will be 0 If door is in panel door mode then, PDID will have values from 1-255
mode	0,1	0	0= for entry mode 1=for exit mode



Notes for Step1

- If door is in direct door mode enter IP and port of the direct door
- If door is a panel door, then enter IP and port of the panel door and in the pdid specify the door id which is to be accessed.

Step 2: Encrypt the JSON string using key "matrix12" with simple DES/ECB mode.

Step 3: Encode the encrypted string using Base 64.

Step 4: Use this string to generate QR code through any third party software.

Wireless Door

The Device Configuration page for Wireless Door appears as shown below.

Enter the MAC address of the door. The IP address will be displayed automatically once the device comes online in Monitor.

To add Devices automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the “Auto Add New Devices” checkbox. Once the device is connected in network, it will come online in COSEC Monitor.



The Monitor Service must be running while adding the device to COSEC.

Once the device is configured, click the **Save** button to save the configuration.

To know more about configuring devices, click on the links for different tabs of Device configuration.

- [“Profile”](#)
- [“Enrollment”](#)
- [“Advanced”](#)
- [“Features”](#)
- [“Video Surveillance”](#)
- [“Special Functions”](#)
- [“Input/Output”](#)
- [“Additional”](#)
- [“Job Costing”](#)
- [“Assign Users”](#)
- [“Cafeteria”](#)
- [“Identification Server”](#)

Profile

This section enables the user to set up the basic profile for any new device. Setting up a door profile involves defining basic parameters to set up any door controller device.

To do this, On the **Device Configuration** page, select the **Profile** tab. The Profile can be configured in the following sections:

- “Basic”
- “Readers”
- “Access Settings”
- “General”

Basic

The **Basic** section for “Wireless Door as Direct door” is shown below:

Configure the following options as required:

- **Sequence Number** - This is a system generated sequence number for each new device.
- **Device**- Specify a name that can be assigned to the door. The Door ID is auto-generated by the system.
- **IP Address** - This is the IP address assigned to the door. Once the device connection is established, this field will automatically display the door IP address.
- **MAC Address** - Specify the MAC Address of the door.



MAC address of door is required while manually adding the door to the COSEC Monitor. Note the MAC address from the device when it is powered on.

- **Active** - Check the box to activate the device on the network.



To add the Device automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the “**Auto Add New Devices**” checkbox.

The device will be added automatically but make sure you enable the **Active** checkbox in order to connect the device to the network. Once the device is connected to the network, it will come online in COSEC Monitor.

The **Basic** page also offers an **Optional** tab which provides optional configurations as shown below:

- **Site** - Select the site to which this door is to be assigned from the site picklist window. Site is created from Devices> Masters> Site.
- **Application** - Select the application type for which the device is to be used. The options are **Basic Access Control**, **Advanced Access Control** and **Cafeteria**. All devices set to **Cafeteria** will subsequently be available for Cafeteria configuration.
- **Access Mode** - Defines the type and combination of credentials required to identify and validate a user at the Door Controller. Select the appropriate credential combination from the drop down list.

The options available are:

- Any one
- Card
- Card + Biometrics
- Card + Biometrics + PIN
- Card + PIN
- Biometrics
- Biometrics + PIN
- Biometrics then Card
- Card then Biometric
- None
- **Consider for Attendance** - Select this checkbox if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as access control events.
- **Alert Messages** - Select this checkbox to enable the application to send alerts based on events from this door.

Readers

Readers are important hardware components in a biometric door device. They may be internal or external. This section enables the administrator to configure both internal and external readers for a door as shown.

The screenshot shows the 'Device Configuration' window with the 'Readers' tab selected. The sidebar on the left contains various configuration options. The main panel is divided into four tabs: Basic, Readers, Access Settings, and General. The 'Readers' tab is active, displaying settings for 'Door Mode Selection' (checked), 'Prompt Special Function' (unchecked), and 'Auto Detect Readers' (unchecked). Below these are sections for 'Internal Readers' and 'External Readers'. The 'Internal Readers' section includes a search bar, a table with columns 'Member No', 'Card Format', and 'Configurable Bits', and a list of readers with fields for 'Mode', 'Card Reader Type', 'Finger Reader Type', 'Enable Scheduling', and 'Reader Mode Schedule'. The 'External Readers' section has similar fields for 'Mode' and 'External Reader Type'.

The following parameters are available for configuration:

Door Mode Selection - If this option is enabled, then user will be prompted to select punch type as IN or OUT while punching on the device.

Eg: When a door is in Entry mode, your punches will always be in Entry side. But if you want to mark the punch in ext mode then you can select the door mode if “Door Mode Selection” is enabled.

If not selected, user will need to enable Scheduling to set reader mode of door as entry or exit as per user-defined schedules. For information on creating Reader Mode Schedules, **see Devices > Masters > Reader Mode Scheduler**.

Prompt Special Function- This can be enabled only when “Door Mode Selection” is enabled. It will provide selection of special function on device screen and based on the selection of particular type of special function, job codes for JPC user will be prompted.

Auto Detect Readers (for direct doors only) - Select this checkbox to enable auto detection of Readers on a door controller connected to the server.

Internal Readers

This option allows the configuration of the Internal Reader for the selected door.

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop down list.
- **Card Reader Type;** Select the Card Reader Type from the following options:
 - EM Prox Reader
 - HID Prox Reader
 - MiFare Reader
 - HID iClass-U Reader
 - HID iClass-W Reader

- **Card Format:** The single or multiple card formats can be assigned to the readers of direct door. The default card format is assigned to device as shown in the grid. If no other card format is assigned to device; then this default format will be applied.



The formatting of card is described in *Devices> Master> Card Format*

Multiple Card Format

To assign multiple card formats to device click on **Add** button. Then click the picklist to select the card format. And click **OK** to save the format.

Member No ▲	Card Format	Configurable Bits
1	Default Format	0

Member No ▲	Card Format	Configurable Bits
2	Format1	0
1	Default Format	0

Similarly you can add maximum 5 card formats. When the card format is saved, the Configurable bits of that format as configured from Masters> Card format will be displayed here. Multiple Card format configurations will be dispatched to door separated by 'Format ID' that is 'Member No.' along with all other format related parameters.


Internal Readers

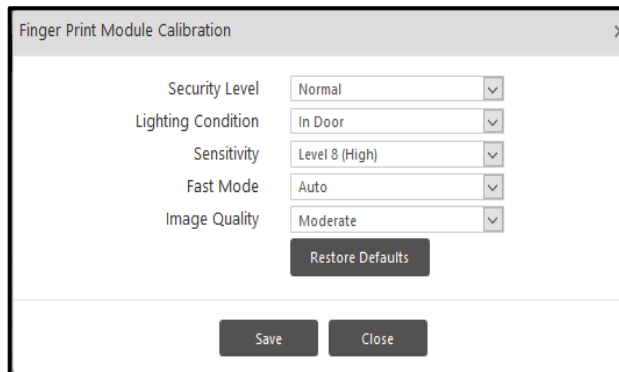
Mode: Entry

Card Reader Type: EM Prox Reader

Member No ▲	Card Format	Configurable Bits
1	Default Format	0
2	Format1	26
3	Format2	32

- Select the **Finger Reader Type** as **Finger Reader**.

Click the **FP Reader Configuration**  button to set the **Security Level**, **Lighting Condition**, **Sensitivity**, **Fast Mode**, **Image Quality** and **Restore Defaults** for the selected FP Reader as shown.



Finger Print Module Calibration

- **Security Level:** Security level specifies FAR (False Acceptance Ratio). Since FAR and FRR (False Rejection Ratio) is in inverse proportion to each other, FRR will increase with higher security levels.

For regular Time-Attendance system “**Normal**” level can be selected. For high security areas requiring complete or maximum matching of template, “**Highly Secure**” level must be selected. For approximate matching of template, “**Secure**” level can be selected.
- **Lighting Condition:** Optical sensors are sensitive to lighting condition. With this parameter, users can tune optical sensors to be adapted for their lighting environment. Select the In Door or Out Door option based on the device location.
- **Sensitivity:** Specifies sensor sensitivity to detect a finger. On high sensitivity, the module will accept the finger input more easily. Level 8 has the highest sensitivity.
- **Fast Mode:** Fast Mode parameter can be used to shorten the matching time with a little degradation of authentication performance. In typical cases, Fast Mode 1 is 2 to 3 times faster than Normal mode while Fast Mode 5 is 6 to 7 times faster than Normal mode. There is also an Auto mode.
- **Image Quality:** When a fingerprint is scanned, the module will check if the quality of the image is adequate for further processing. Image quality parameter specifies the strictness of this quality check. Strongest option might lead to higher number of finger rejections during the enrollment process.
- Click on the **Restore Defaults** button to return the field values for this page to default values if needed.
- Click on the **Save** button.
- **Enable Scheduling:** Select this checkbox to **Enable Scheduling** to set reader mode of door as entry or exit as per user-defined schedules.

External Readers

This option allows the configuration of the External Reader for the selected door.

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop down list.
- **External Reader Type:** Select the desired type of External Reader from the drop-down list.
- **Card Format** - Select a card format to be applicable for external readers of the device. This is applicable for all direct doors and all Panel doors. For multiple format description [See "Multiple Card Format" on page 920.](#)
- **Exit Switch** - Select this checkbox to enable the use of **Exit Switch**.
- **User/Visitor Access Mode** - Select the access mode from the options shown below:
 - Any One
 - Card
 - Biometrics
 - Card + Biometrics
 - Biometrics then Card
 - None
- **Access Control On Exit Mode** (only for direct door) - Select this checkbox to enable access control on the exit mode.

Access Settings

This section is available for direct doors. The **Access Settings** page appears as shown below:

The screenshot shows the 'Device Configuration' window with the 'Access Settings' tab selected. On the left, a sidebar lists various configuration options: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main area is divided into four tabs: Basic, Readers, Access Settings (active), and General. Under the 'Access Settings' tab, the following settings are visible:

- Universal Time Zone:** (GMT+05:30)Chennai, Kolkata, New Delhi, Mumbai
- Time Format:** 24 Hours
- Auto Synchronize with NTP:** ☒
- Preferred NTP Server:** (empty text field)
- Working Days:** ☒ Sun, ☒ Mon, ☒ Tue, ☒ Wed, ☒ Thu, ☒ Fri, ☒ Sat, ☒ Holiday
- Working Hours(HH:MM):** 00:00 to 23:59
- Holiday Schedule 1:** 1, Schedule 1
- Holiday Schedule 2:** 2, Schedule 2
- Holiday Schedule 3:** 3, Schedule 3
- Holiday Schedule 4:** 4, Schedule 4

- **Universal Time Zone** - Select the geographic time zone in which the DOOR will operate.
- **Time Format** - Specifies the time format to be displayed on Door Controller LCD display. The formats available are:
 - 24 Hours
 - 12 Hours

Select the relevant option from the drop down list as per the site requirements.

Auto Synchronize with NTP

If Date and time is to be automatically synchronized as per the **Preferred NTP Server** (predefined or user-defined NTP server address) selected by user, then you must enable **Auto Synchronize With NTP** checkbox.

Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from device webpage, which will be reflected on device display.

- When Auto Synchronization with NTP is disabled Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 1. You can specify the Preferred NTP server of your choice. In this case device will first try to get Date and Time from that server address.
If it does not get Date and Time in three tries; device will check from pre-defined NTP servers.
If you have entered one of the three pre-defined NTP servers(ntp1.cs.wisc.edu , time.windows.com , time.nist.gov); then device will first check that server first.
If it receives updated Date and Time then Updated Date and Time will be reflected on device webpage and display screen.
 2. You can keep the Preferred NTP server as blank. In this case device will check for Date and Time from the first NTP server.

If user has manually entered Date and Time from webpage or Device Menu then those values of Date and Time will be reflected on device webpage and display screen.

In the case of the **Manual** option the administrator can manually update the time on the Door with that of the system time as and when required. This can be accomplished from the COSEC Monitor and control application.

- **Working Days** - Specify the days on which the default working hours should be applicable. Check the relevant boxes to specify the active days.
- **Working Hours (HH:MM)** - Define the default working hours in HH:MM format.
- **Holiday Schedule** - This section allows the administrator to assign up to four holiday schedules to the device by using the Holiday Schedule picklist.



If the same holiday schedule is configured for a user and for the door controller on which the user is assigned, then the user's attendance marking on this device, on any of the scheduled holidays will always be marked as a holiday.

General

The **General** page appears as follows. Enter all general details applicable to the device in this section.

Device Configuration

Device ID: 0/50000
Device Name: Wireless Door
Active/Inactive

Basic Readers Access Settings **General**

Mute Buzzer ☐

Allowed Acknowledgement

Display Duration (ms): 3000
LED - Buzzer Duration: Long

Denied Acknowledgement

Display Duration (ms): 3000
LED - Buzzer Duration: Long

Enable Display Messages ☐

Custom Birthday Message: Happy Birthday

Display Message 1 ☒
Schedule: 00:00 - 11:59
Message: Good Morning

Display Message 2 ☒
Schedule: 12:00 - 15:59
Message: Good Afternoon

Display Message 3 ☒
Schedule: 16:00 - 20:59
Message: Good Evening

Display Message 4 ☒
Schedule: 21:00 - 23:59
Message: Good Night

Multi-Language Support ☐

- **Mute Buzzer** - User can mute or unmute the door buzzer by checking or clearing the box respectively. This is applicable for both Direct and Panel door.
- **Allowed Acknowledgment**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgment Allowed' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.
- **Denied Acknowledgment**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgment Denied' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.



The below mentioned features are available in direct door only.

- **Enable Display Messages** - This feature allows the user to enable custom birthday message and display messages to be displayed on the door device. Upto 4 display messages can be configured for a door.
- **Custom Birthday Message**- Enter the birthday message which would appear on the door when the user punches on the door on his birth date.
The valid values are

A-Z

a-z

0-9

~!@#\$%^&*()_+-{}|\\|:;?<>.,'""

- **Display Message** - Enable each display message individually by selecting this checkbox.
- **Schedule** - For each message, the user needs to define the time period between which this message is to be displayed.
- **Message** - Enter the message to be displayed in this field. Maximum 21 characters allowed.
- **Multi-Language Support** - Select this checkbox to enable multi-language support for the selected device.

The **Display From** field shall display the reading order for the selected language.



However Wireless Door will support languages with english fonts (A-Z,a-z) only.

Enrollment



The Enrollment section is not available for panel doors.

The Enrollment page appears as shown below.

The screenshot shows the 'Device Configuration' window with the 'Enrollment' tab selected. On the left, a sidebar lists various configuration categories, with 'Enrollment' highlighted. The main area displays settings for a device named '3 wireless Wireless Door 11/50000' which is 'Active'. The 'Enrollment' settings include: 'Enroll From Device' (checked), 'Enrollment Mode' (ReadOnlyCard), 'Template Per Finger' (Single Template/Finger), 'Max Number Of Fingers' (Ten), 'Number of Fingers' (One), 'Number Of Cards' (One), and 'Enable Self-Enrollment' (unchecked).

- **Enroll from Device** - Select this check-box to enable the enrollment of user from the door controller. When this check-box is enabled, 'Enroll User' special function on that device will get active as shown below.

If 'Enroll User' special function & 'Enroll From Device' check-box both are inactive in device configuration, then on activating 'Enroll User' special function, 'Enroll From Device' check-box will be enabled.

The screenshot shows the 'Device Configuration' window with the 'Special Functions' tab selected. It displays a table of functions with columns: No., Function Name, Active, JOB Selection, User Group, and Card-1. An arrow points to the 'Enroll User' function (row 11), which is active.

No.	Function Name	Active	JOB Selection	User Group	Card-1
1	Official Work - IN	No	No	All	
2	Official Work - OUT	No	No	All	
3	Short Leave - IN	No	No	All	
4	Short Leave - OUT	No	No	All	
5	Regular - IN	No	No	All	
6	Regular - OUT	No	No	All	
7	Break End	No	No	All	
8	Break Start	No	No	All	
9	Overtime - IN	No	No	All	
10	Overtime - OUT	No	No	All	
11	Enroll User	Yes	No	All	
12	Enroll Special Card	No	No	All	

- **Enrollment Mode** - Select the Credential from the dropdown list that can be enrolled using the special function at the DOOR. The options are **ReadOnlyCard**, **SmartCard**, **Biometrics** and **BiometricsThenCard**.
- **Enrollment Using** - Select the option **User ID** or **Reference No.** using which enrollment will be done.

- **Template Per Finger** - This parameter displays the values as configured at the global level. This field is not user editable from this page.
- **Max Number of Fingers** - This parameter displays the values of the maximum number of fingers configured at the global level. This field is not user editable from this page.
- **Number of Fingers/Cards** - Select the number of cards or fingerprints to be enrolled based on the credential option selected in the **Enrollment Mode** parameter.
- **Enable Self-Enrollment** - Select this checkbox to enable the self-enrollment feature on this door.

Advanced

The Advanced tab allows the user to configure some advanced parameters such as access control settings, alarms and device timers.

To access this, After selecting the device, Select the **Advanced** tab from **Device Configuration** page. The advanced settings can be configured from following sections:

- *“Settings”*
- *“Alarms”*
- *“Timers”*

Settings

The **Advanced Settings** page for Wireless Door as a Direct Door appears on your screen as shown below:

The screenshot displays the 'Advanced Settings' page for a 'Wireless Door' device. The left sidebar contains a list of settings categories: Profile, Enrollment, Advanced (selected), Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main content area is divided into tabs: Settings, Alarms, Timers, and Wiegand. The 'Settings' tab is active, showing a list of configuration options with checkboxes and input fields. A search bar at the top right allows searching by 'Device ID or Name'. Below the main settings, a separate section contains three options: 'Allow Access Through Mobile' (checked), 'Mobile Entry Access Mode' (set to 'Mobile Only'), and 'Mobile Exit Access Mode' (set to 'Mobile Only').

Settings	Alarms	Timers	Wiegand
<input type="checkbox"/> Generate Exit Switch Events	<input type="checkbox"/> Generate Invalid User Events		
<input type="checkbox"/> Generate Sequential IN-OUT Events	<input type="checkbox"/> Two Credentials Required		
<input type="checkbox"/> Show Pin			
<input type="checkbox"/> Allow Exit When Door Lock	<input type="checkbox"/> Auto Relock		
<input type="text" value="3"/> Auto Relock Timer (Sec)			
<input type="checkbox"/> Enable Additional Security	Disabled		
<input type="checkbox"/> Enable Smart Identification			
<input type="text" value="8"/> Access Level			
<input type="text" value="Card"/> Access Mode			
<input type="checkbox"/> Auto Acknowledge Alarm			
<input type="text" value="10"/> Auto Acknowledge Alarm (Sec)			
<input type="text" value="1"/> Facility Code			

☒ Allow Access Through Mobile
 Mobile Entry Access Mode
 Mobile Exit Access Mode

The following parameters are available for configuration:

- **Generate Exit Switch Events** - Select this checkbox to enable the door to generate events everytime the exit switch is used.
- **Generate Invalid User Events** - Select this checkbox to enable the door to generate events for invalid user inputs.
- **Generate Sequential IN-OUT Events** - Select this checkbox to generate user punches on device as the sequential IN-OUT events irrespective of whichever mode in which device is functioning.
- **Two Credentials Required**- Select this checkbox to enable the feature of verifying 2 credentials mandatorily for users allowed to By-pass finger/palm.
- **Show Pin**- Select this checkbox to display the characters of PIN when the PIN is entered on device.
- **Allow Exit when Door Lock** - Select this checkbox if users are to be allowed to exit even when the Door relay is in locked condition.
- **Auto Relock** - Select this checkbox to allow the door to relock immediately when the door status changes to close after normal open irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Relock Timer** - Specify the time in seconds for the Auto Relock operation.
- **Enable Additional Security** - Select this checkbox to enable additional security at the selected Door Controller.

- **Additional Security Code** - Enter a code (ranging from 1 to 65535) in the field provided. Re-enter the code to confirm.



Changing this value can affect the SI function. Click on the **Default Code** button to reset the **Additional Security Code** to the value set in the **Global Additional Security Code** field on the Global System Policy page.

- **Enable Smart Identification** - Select this checkbox to enable this functionality at the selected Door Controller and select the **Access Level** and the **Access Mode** from the drop down list.
- **Auto Acknowledge Alarm** - Select this checkbox to enable the auto-acknowledgment of all alarms for this device.
- **Auto Acknowledge Alarm (sec)** - Set the time in seconds for the Auto Acknowledge Timer. The wait timer will start and on expiry of the timer, the alarm buzzer will stop automatically.
- **Facility Code** - Set a value for Facility Code to be set for access modes other than “Card”, if Facility Code is expected in Wiegand Output. This will be applicable to all direct doors except Door V1 and V2.
- **Allow Access Through Mobile**- Check the box to allow the access to device using COSEC ACS App.
- **Mobile Entry/Exit Access Mode**- Select the entry and exit door access mode from the options of **Mobile Only**, **Mobile then Biometrics** and **Mobile then Card**.



If User Access Mode is selected as “None” in Zone Configuration and Mobile Access Mode is selected as “Mobile Then Biometrics” then door can be accessed through Mobile and then Biometric credential.

Temperature Logging

- **Enable:** Enable the temperature logging feature on the zone.
- **Sensor Type:** Select the type of thermal sensor integrated in the device. There are three sensors: *AST*, *Web-Based* and *FEVOBOT*. Default sensor set is *FEVOBOT*.
- **Sensor Interface:** Select the interface on which device will communicate with the sensor.
For Sensor Type-AST
Sensor Interface options will be: RS-232 and USB
For Sensor Type- Web-based
Sensor Interface options will be: HTTP/S
For Sensor Type-FEVOBOT
Sensor Interface options will be: USB
- **Emissivity:** Set the emissivity parameter for Sensor. This parameter should only be visible when Sensor Type is AST. Default value is 0.95.
It is used to define accuracy in sensor to detect temperature of different skin or objects.
Not applicable for FEVOBOT.
- **Calibration Parameter:** Set the calibration parameter for the thermal sensor.
On click of + the value should increase by 0.1 and on click of – it should decrease by 0.1.

Not applicable for FEVOBOT.

- **Approach to Sensor Wait-Timer:** Time for which the device will wait for user to approach the device before starting Temperature Detection.
- **Temperature Detection Time-Out:** The timer till which temperature detection will be done for the user and if valid temperatures are not found till the expiry of timer then timeout will be declared.
- **Tolerance between consecutive readings:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature doesn't fall in tolerance range the reference temperature is updated with the current temperature and the process continues.
Not applicable for FEVOBOT.
- **Consecutive readings count within tolerance:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature doesn't fall in tolerance range the reference temperature is updated with the current temperature and the process continues.
Not applicable for FEVOBOT.
- **Minimum Temperature for Access:** The minimum temperature value that should be detected is to be considered as valid temperature.
It should be less than threshold temperature. If user tries to enter a value equal to or greater than threshold temperature validation should be shown.
The default value, unit and range should be updated based on the Temperature unit set on Panel.
- **Temperature Threshold:** To set the threshold value of the temperature. The default value, unit and range can be updated based on the Temperature unit set on Panel.
- **Restriction Type:** To set restriction type as soft/hard.
- **Bypass if Sensor Disconnected:** Enable this check-box to give provision of bypassing the feature if sensor connectivity is lost.

Alarms

In Alarm tab, you can assign below list of alarms to the door.

For Direct Door

Settings	Alarms	Timers
	Tamper	<input type="checkbox"/>
	Door Abnormal	<input type="checkbox"/>
	Door Force Open	<input type="checkbox"/>
	Door Fault	<input type="checkbox"/>
	Panic	<input type="checkbox"/>
	Temperature Threshold	<input type="checkbox"/>

Enable the respective checkbox of alarms which is to be selected.

Timers

This section allows the configuration of various types of pre-defined device timers which can trigger off specific responses. In COSEC, timers are often used to control door behavior and for triggering alarms. The **Timers** page appears on your screen as shown below:

Timer Type	Value
Inter-Digit Wait Timer (Sec)	3
Multi-Input Wait Timer (Sec)	5
Door Open Pulse Timer (Sec)	5
Late-IN Early-OUT Active Timer (Min)	60

- **Inter-Digit Wait Timer (sec)** - Specify the time period in seconds between two key inputs on the device keypad. On expiry of this timer, the system considers the user input to be complete and is ready for the next input.
- **Multi-Input Wait Timer (sec)** - Specify the time in seconds for which system needs to wait for the second credential input from the user when more than one credential is to be used to grant access.



We recommend you to set the timer value as greater than or equal to 10 seconds to avoid access denial issues to users. This is applicable when the system reads the credentials (biometric) from the user's Smart Cards.

- **Door Open Pulse Timer (sec)** - Specify the time in seconds (3 to 99) for the door to be energized for a valid credential. If the opened door does not return to a closed state before the expiry of this timer, the door will generate a "Door Abnormal" alarm.
- **Late-IN Early-OUT Active Timer (min)** - Specify the time in minutes for which the Late-IN and Early-OUT special functions will remain active after being enabled at the Door Controller.

Door Access using QR code

The user can access the COSEC device using COSEC APTA installed in the mobile device. If the user has rights for COSEC APTA and the access to the device is allowed for the user, then he can use his mobile device to scan the QR code which constitute the details of the COSEC door.

There is icon for QR code on COSEC APTA application. Clicking that icon will open the camera in your mobile. Now you can show the mobile camera to scan the QR code. The COSEC door will get opened after verifying the security key and access policies of the user.

Steps to create a QR code

Step 1: Enter details in JSON format

```
{"version":"x","ip": "x.x.x.x","port":"x","pdid":"x","mode":"x"}
```


Valid values:

Field	Field range	Default Value	Remark
version	1-255	1	
ip	0.0.0.0-255.255.255.255	0.0.0.0	
port	0-65535	0	
pdid	0-255	0	If door is in direct door mode then, then PDID will be 0 If door is in panel door mode then, PDID will have values from 1-255
mode	0,1	0	0= for entry mode 1=for exit mode



Note:

Step1a. If door is in direct door mode enter IP & port of the direct door

b. If door is a panel door, then enter IP & port of the panel door and in the pdid specify the door id which is to be accessed.

Step 2: Encrypt the JSON string using key "matrix12" with simple DES/ECB mode.

Step 3: Encode the encrypted string using Base 64.

Step 4: Use this string to generate QR code through any third party software.

Features

The Features tab allows the user to enable certain Access Control features for a device



The Features tab is available only with the Access Control Module license.

To access this, After selecting the device, Select **Device Configuration> Features**. The access control features for the device can be set from the following two sections:

- "Set1"
- "Set2"

Set1

This page allows the configuration of three rules - **Absentee Rule**, **Occupancy Control** and **Use Count Control**. The page appears as shown below.

Set1	Set2
Absentee Rule	
Enable	<input checked="" type="checkbox"/>
Occupancy Control	
Enable	<input checked="" type="checkbox"/>
Maximum Occupancy Limit	9
Minimum Occupancy Limit	1
Zero Occupancy	<input checked="" type="checkbox"/>
Use Count Control	
Enable	<input checked="" type="checkbox"/>
Use Count Limit (Per minute)	
Duress Detection	<input checked="" type="checkbox"/> 10

- **Absentee Rule** - Select this checkbox to **enable** this feature at the door. This rule sets the maximum number of days for non-use of a credential. On expiration of days limit, the user will be automatically blocked.
For configuring the rule *See Access Control> Absentee Rule*.
- **Occupancy Control** - Select this checkbox to **enable** the feature at the door and specify maximum number of users to be allowed within the controlled area after which a user exit is required to enable access to another user. Also specify the **Minimum Occupancy Limit** i.e. the minimum number of occupants the designated zone should have, and enable/disable the **Zero Occupancy** option to determine whether the designated zone should be allowed to be empty or not.
For configuring the rule *See Access Control> Occupancy Control*.
- **Use Count Control** - Select this checkbox to **enable** the feature at the door and specify the maximum number of uses per minute.
For configuring the rule *See Access Control> Use Count Control*.
You can enable Duress Detection on the door. The default duress detection code is displayed which is used to generate the duress alarm which informs that the user is forced to open the door under threat.
For details *See Device Configuration (Panel200)> Features> Set3> Duress Detection*

Set2

This page allows the configuration of three rules - **First-IN User Rule**, **Anti-Pass-Back (APB)** and **2-Person Rule**. The page appears as shown below.

The screenshot shows the 'Device Configuration' window for 'Set2'. On the left is a sidebar with a list of configuration categories: Profile, Enrollment, Advanced, Features (highlighted), Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main panel displays three rule configurations:

- First-IN User Rule:** Includes an 'Enable' checkbox (checked), 'Reset On' options (Day Change selected, Timer Expiry unselected), 'Access Timer (Sec)' set to 3, and 'First-IN User Group' set to 1.
- Anti-Pass-Back (APB):** Includes an 'On Entry' checkbox (checked), 'On Exit' checkbox (unchecked), 'Hard/Soft' set to Soft, 'Forgiveness' checkbox (checked), 'Reset After' options (Day Change unselected, Timer Expiry selected), and 'Forgiveness Timer (Mins)' set to 1.
- 2-Person Rule:** Includes an 'Enable' checkbox (checked), 'Mode' set to Primary Must, 'Primary Group' set to aaa, and 'Secondary Group' set to None.

- **First-IN User Rule** - Select this checkbox to **enable** the feature at the direct door and select the First-In User group which would be valid at the door.
For configuring the rule See *Access Control > First- In User Rule > Assignment*
- **Anti-Pass Back (APB)** - Select this checkbox to enable the feature at the direct door.
 - **On Entry:** Check this box so that the system monitors the entry reader for APB violation.
 - **On Exit:** Check this box also so that the system monitors the entry as well as the exit readers for APB violations.
 - **Hard/Soft:** Select the restriction type as Hard or Soft option from the drop down options.
Hard APB: The access will be denied if the exit is not registered first. It does not allow a second entry using the same card without an exit.
Soft APB: The access will be granted even if the exit is not registered. It allows a second entry of the same user without an exit; however, an event and a warning are generated that indicates the second entry.
 - **Forgiveness:** Check this box to enable the system to reset the APB status. When forgiveness is enabled, then there will be following options to reset the pass.
 - **Reset After Day Change:** This will reset the APB status of all the users to NULL at midnight. This enables a user, who left the building in the evening without exit punch, to use his card for entry in the next morning.
 - **Reset After Timer Expiry:** This will reset the APB status of all the users after the expiry of user defined time.
 - **Forgiveness Timer (Mins):** Enter the time duration in minutes after which Anti-pass back status will get reset and the pass will be in original state.

- **2-Person Rule** - Select this checkbox to enable the feature at the door and set the **wait time** in seconds after which the second person is allowed to punch on the door.
For configuring the rule *See Access Control> 2- Person Rule*

Video Surveillance

The Video Surveillance tab allows the user to configure parameters for video surveillance integration with the COSEC device.

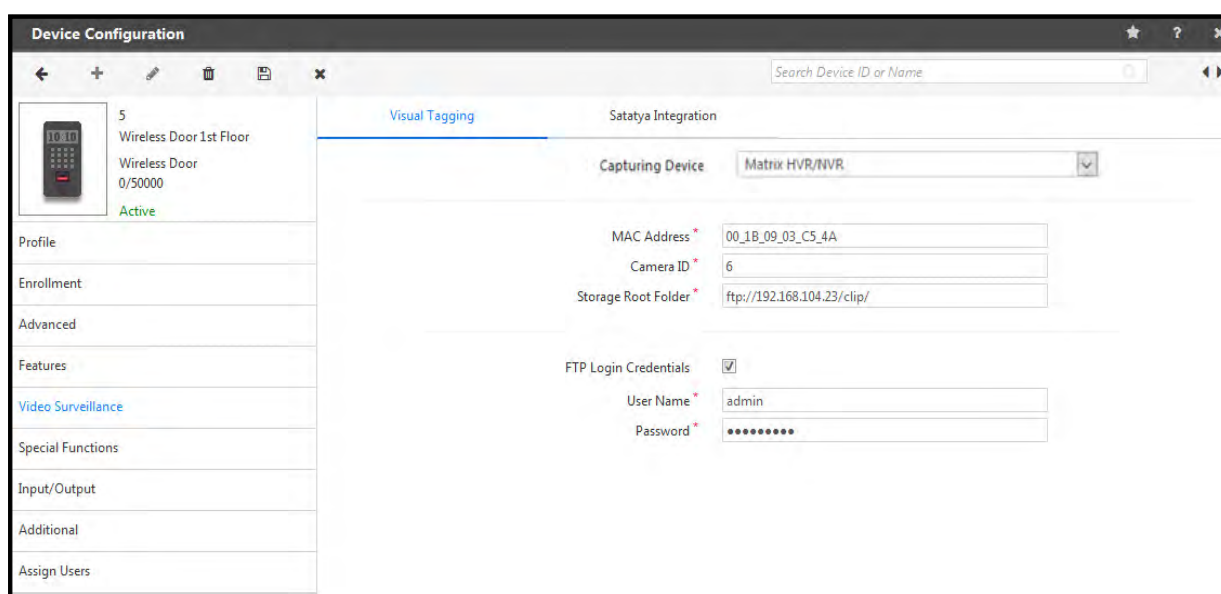
It is available in Basic License.

To access this, Go to **Device Configuration> Video Surveillance**.

- “Visual Tagging”
- “Satatya Integration”

Visual Tagging

The COSEC application can interface with some supported hybrid and network video recording systems and grab images triggered by user events at the Doors. The **Visual Tagging** option enables the administrator to define the video recorder parameters. The **Visual Tagging** page appears as shown below.



The screenshot displays the 'Device Configuration' window. On the left, a sidebar lists configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance (highlighted), Special Functions, Input/Output, Additional, and Assign Users. The main panel is titled 'Visual Tagging' and 'Satatya Integration'. It features a 'Capturing Device' dropdown menu set to 'Matrix HVR/NVR'. Below this, there are input fields for 'MAC Address' (00_1B_09_03_C5_4A), 'Camera ID' (6), and 'Storage Root Folder' (ftp://192.168.104.23/clip/). At the bottom, the 'FTP Login Credentials' checkbox is checked, with 'User Name' set to 'admin' and 'Password' masked with asterisks.



To view the user events and related images, go to **Admin > Views/Logs > Event View**. To know more about viewing events, refer to “Event View”.

The following parameters are available for configuration:

- **Capturing Device** - Select the video recording device type from the dropdown menu as shown.
The compatible device types are:
 - Matrix HVR/NVR
 - Milestone

Matrix HVR/NVR

- **MAC Address** - In the event of selecting the Matrix HVR/NVR, the administrator needs to specify the MAC address of the video recorder device using “_” (underscore) as the separator.
- **Camera ID** - Specify the camera number or camera ID for IP cameras. For analog cameras specify the camera number.
- **Storage Root Folder** - Specify the Root folder path or FTP Path where the uploaded images will be saved.
- **FTP Login Credentials** - Check this box to activate FTP login credentials for authentication.
- **Username** - Specify the FTP server Username.
- **Password** - Specify the FTP server password.



Some COSEC devices do not support all the network connection options.

Milestone

Event ID	Name	User-Defined Event ID	User-Defined Event Name
No Data			

Camera Name	GUID	Host Name	Port
MATRIX COMSEC CIDR20VL12CW-P (192.168.112.193) - Camera 1	ac6c0e92-8acd-410d-b21f-f593c2b9d33f	ketanpipaliya	7563



*For more information on integration with **Milestone** devices, refer to “[Milestone Integration](#)”.*

Satatya Integration

This functionality is available for configuration only when the Matrix HVR/NVR device type is selected as the **Capturing Device** (from *Visual Tagging*). It enables the configured COSEC devices to directly send commands to the SATATYA HVR/NVR devices as per the configuration on this page. The Satatya configuration page appears as shown below

The screenshot displays the 'Satatya Integration' configuration window. On the left is a sidebar with a list of configuration categories. The main panel is divided into two tabs: 'Visual Tagging' and 'Satatya Integration'. The 'Satatya Integration' tab is active, showing various configuration fields. At the top left of the main panel, there's a small device icon and a list of devices. The configuration fields include: 'Integration Type' set to 'Network'; 'Active' checkbox checked; 'IP Address' set to '192.168.104.37'; 'Port Number' set to '8000'; 'Name' set to 'WirelessNVR'; another 'Active' checkbox checked; 'Schedule' set from '09:00' to '14:00'; 'Days' with checkboxes for Mon, Tue, Wed, Thu, and Fri checked; 'Event' set to 'Access Allowed'; 'Mode' set to 'Both'; 'Action' set to 'Mail Image'; 'E-mail ID' set to 'sheetalraval@matrixrd.org'; and a grid of checkboxes for cameras 1 through 24, with camera 2 checked. 'Update' and 'Cancel' buttons are at the bottom right.

- **Integration type-** Select the integration type from the options of Wired and Network.
In wired integration, door is physically connected with Satatya Device. In Network integration, connection can be by Ethernet, wireless or broadband depending upon the COSEC device support.
- **Active-** Check the box to activate the connection.
- **IP Address-** Specify the IP address of HVR/NVR.
- **Port Number-** Specify the port number of HVR/NVR.
- **Name-**Specify a user friendly name for the integration function.
- **Active-** Check the Active box to enable the SATATYA integration functionality.
- **Schedule -** Specify a schedule for the function by specifying the start and the end time (*24 Hours format*) as well as checking the boxes against the applicable **days** of the week.
- **Event-** Select a COSEC event from the drop down list for which the resultant action is to be configured.
- **Mode-** Select the event mode from the options of Entry, Exit and Both from the drop down list wherever applicable.
- **Action-**Select the action for the Satatya device from the drop down list. The options available are:
 - Recording - Specify the duration in minutes.
 - Upload Image - This will be uploaded as per the ftp settings.

- Video Pop-up - Specify the duration in seconds. The video pop up will be generated on the local client of Satatya device on the selected camera.
- PTZ Preset - Specify the PTZ position number as defined on the SATATYA device.
- Mail Image - Specify the Email-ID.
- **Camera-** Select the relevant camera channels depending on the action selected.
- Click the **Add** button to finish the process of linking the event to the action.

Name	Event	Action	Start Time	End Time	Active	
WirelessNVR	Access Allowed	Mail Image	09:00	14:00	Yes	

- The user may now configure another event-action linkage if required.

Example1: For action as Video Pop up, the pop up of Camera 24 will be shown for 10 seconds.

Example2: For Access allowed event on COSEC Device, recording of camera channel 4,6,8 and 10 will be done for 10 seconds.

Event: Access Allowed
Mode: Both
Action: Video Pop-Up
Duration Sec.: 10
Camera: ☐1 ☐2 ☐3 ☐4 ☐5
☐6 ☐7 ☐8 ☐9 ☐10
☐11 ☐12 ☐13 ☐14 ☐15
☐16 ☐17 ☐18 ☐19 ☐20
☐21 ☐22 ☐23 ☒24

Event: Access Allowed
Mode: Both
Action: Recording
Duration Min.: 10
Camera: ☐1 ☐2 ☐3 ☒4 ☐5
☒6 ☐7 ☒8 ☐9 ☒10
☐11 ☐12 ☐13 ☐14 ☐15
☐16 ☐17 ☐18 ☐19 ☐20
☐21 ☐22 ☐23 ☐24
Add Cancel

Special Functions

To configure *Special Functions* for COSEC doors, refer to [“Special Functions”](#).

Input/Output

The Input/Output (I/O) configuration of a system determines how the output or response of a system is influenced by the input applied on it. In case of the COSEC Access Control System, the I/O configuration should enable the system to monitor and trigger a specific response to any changes in door state or event occurrences at the door device. This change of door state or occurrence of events may be considered as an input while the response or action that is generated by the system on detection of this input, may be defined as the output.



1. This functionality cannot be fully accessed in the Edit mode for a selected device.
2. This functionality is available only with the Access Control add-on module license.

To access this, After selecting the device, Select **Device Configuration> Input Output**. The Input Output parameters can be set from the following sections:

- “*Configuration*”
- “*Linking*”
- “*Time Triggered*”

Configuration

The **Configuration** section for a Direct Wireless Door appears as shown below.

The screenshot shows the 'Device Configuration' window for a device named '5 Wireless Door 1st Floor' with ID '0/50000' and status 'Active'. The left sidebar lists various configuration sections: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, **Input/Output** (selected), Additional, and Assign Users. The main area is divided into three tabs: Configuration, Linking, and Time Triggered. The 'Configuration' tab is active, showing the following settings:

- Door Sense:**
 - Enable: ☒
 - Supervised: ☐
 - Sense Type: NC (dropdown menu)
- Auxiliary Input:**
 - Enable: ☒
 - Supervised: ☒
 - Sense Type: NO (dropdown menu)
 - Debounce Time (Sec): 3 (text input)
- Auxiliary Output:**
 - Enable: ☒
 - Output Wait Time (Sec): 0 (text input)
- Accept External IO Linking:**
 - Enable: ☒

The following parameters are available for configuration:

- **Door Sense** - The system by default can sense two states of a door - *Normally Open (NO)* and *Normally Closed (NC)* depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a *Door Abnormal* alarm.

Select the **Enable** checkbox to enable the system for such two-state monitoring.

Select the **Supervised** checkbox to enable the door for four-state monitoring where the door is also monitored for *door fault* and *door disconnection*. Specify the **Sense Type** as **NC** or **NO** (Default: NC).

- **Auxiliary Input** - Select the **Enable** checkbox option for Auxiliary Input (e.g. Smoke Detectors) depending on normal or supervised door state monitoring as described above.

Debounce Time (Sec) - Specify the Debounce time in seconds. Default value is 3 sec and range should be 0-99 sec. It defines the minimum time for which an input interface must be maintained in

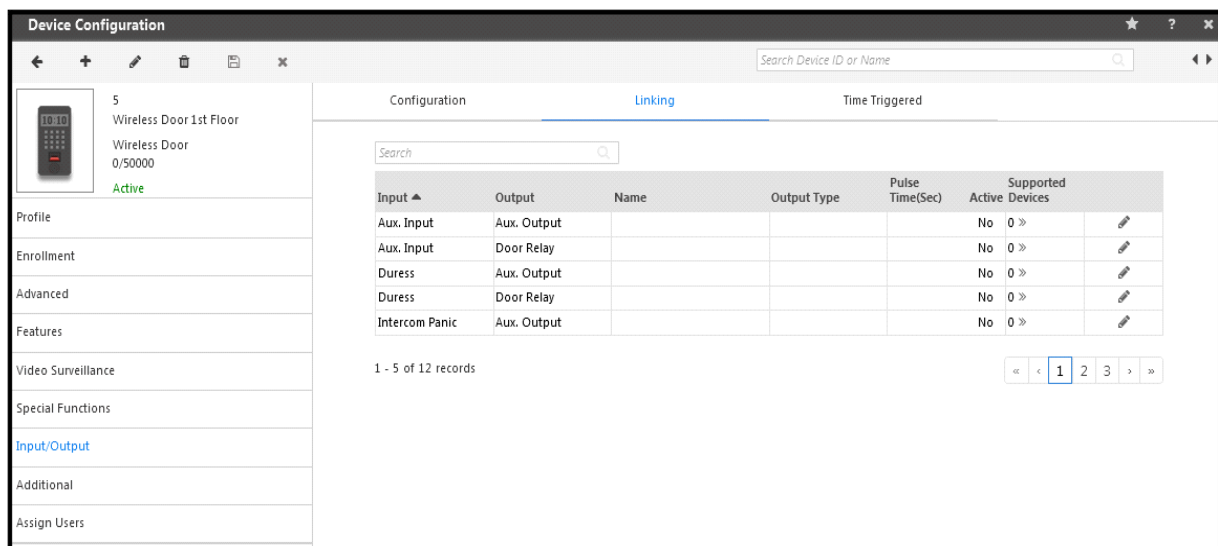
a given state before the system reports it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.

- **Auxiliary Output** - Select the **Enable** checkbox to enable Auxiliary Output (e.g. Fire Alarm) for the selected device. To set an additional waiting period before the Aux Output signal is sent, enter an **Output Wait Time (Sec)**.
- **Relay Output**
Output Group Number (Door Unlock)- Select the Output Group Number to which the device output for Door Unlock is to be assigned from the picklist.

Output Group Number (Door Lock)- Select the Output Group Number to which the device output for Door Lock is to be assigned from the picklist
- **Accept External IO Linking** - Select the Enable checkbox to enable device-to-device IO Linking i.e. input from one Direct Door can trigger output in another Direct Door.

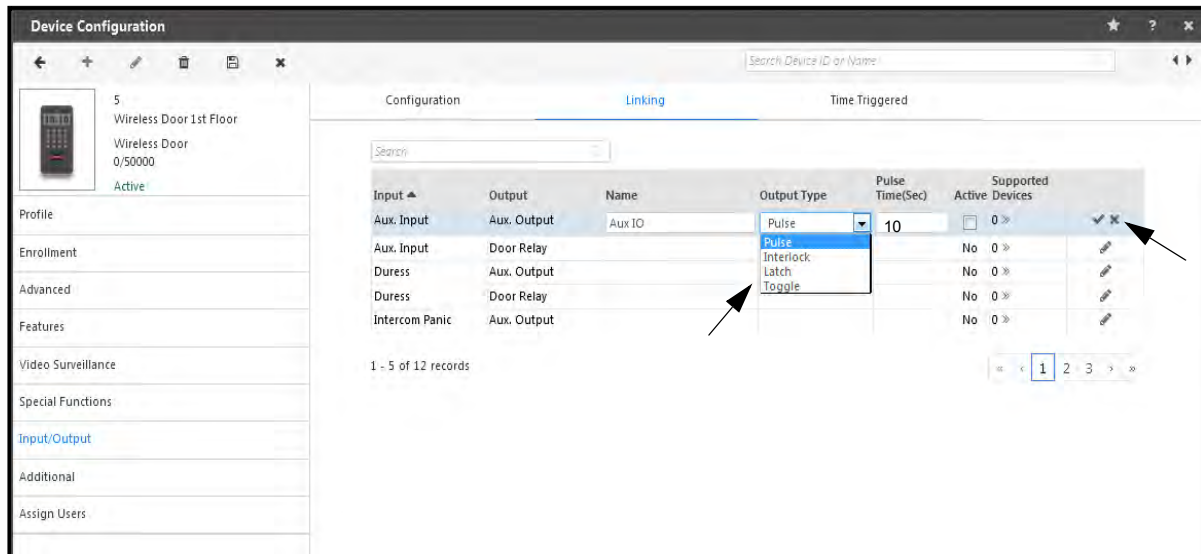
Linking

The **Linking** section appears as shown below.



The COSEC application supports the Input/Output Linking feature to activate an output port based on a trigger received from an input port on the same Direct Door. This option enables the administrator to define how an event or events (input port) will trigger an output on the selected door.

Select a Input-Output linking row or click edit button shown with arrow.



- **Name** - Specify a name for the new I/O linking program to be defined.
- **Output Type** - Specify the appropriate type of output from the following four options available in the drop down list shown with the arrow above:
 - **Pulse**: With this type of output, the user needs to define the Pulse time in seconds.
 - **Interlock**: With this option, the output follows the input. The relay output is triggered as long as the input is activated after which it returns to normal state.
 - **Latch**: With this option, it is denoted that the relay output will be in an energized condition for infinite period and needs to be reset manually.
 - **Toggle**: With this option, the output group toggles its state whenever an input group is activated.
- **Pulse Duration (sec)** - For a *Pulse* output type, specify the pulse duration in seconds.
- **Active** - Select this checkbox to activate this linking program.
- **Supported Devices** - All devices supported for external IO Linking will appear in this picklist for selection. Upto 255 external devices can be added by the administrator.
- Click the **OK** button and **Save** the configuration.

Time Triggered

On the **Input Output** page, select the **Time Triggered** section as shown.

The screenshot shows the 'Time Triggered' configuration window. It has tabs for 'Configuration', 'Linking', and 'Time Triggered'. Below the tabs is a search bar and a table. The table has columns: Function Name, Active, Time, Duration(Sec), Days, and Output. The first row shows 'Siren Activate' with 'Active' checked, 'Time' as '00:00', 'Duration(Sec)' as '10', 'Days' as 'Select', and 'Output' as 'Aux O/P'. A dropdown menu is open for the 'Days' column, showing options: 'Check All', 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', and 'Holiday', each with a green checkmark.

This functionality enables the user to control the activity of an Output without manual intervention. The time triggered functions are used for activating events like door unlock and siren activation that are set as per the start time and for the configured time duration. This functionality is designed to energize outputs for predefined periods at the configured time. The COSEC access control system supports up to 20 Time Triggered functions on a Direct Door.

The screenshot shows the 'Time Triggered' configuration window. It has tabs for 'Configuration', 'Linking', and 'Time Triggered'. Below the tabs is a search bar and a table. The table has columns: Function Name, Active, Time, Duration(Sec), Days, and Output. The first row shows 'Siren Activate' with 'Active' as 'Yes', 'Time' as '00:00', 'Duration(Sec)' as '10', 'Days' as 'Su Mo Tu We Th Fr Sa Ph', and 'Output' as 'Aux O/P'. There are edit and delete icons next to the 'Days' and 'Output' columns.

Additional

This section lists some additional configurations that can be enabled for door controllers.

To access these configurations, Go to **Device Configuration > Additional > Daylight Saving**

Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. COSEC doors can be configured to be compatible with this procedure keeping the RTC of the system updated with such changes.

The **Daylight Saving** configuration can be done in 2 ways i.e. Day-Month wise or Date-Month wise.

- Select the **DST Type** as Day-Month wise or Date-Month wise. The **Disable** option when selected, disables the application of DST on the system time.
- On selection of the **Day-Month wise** option, the DST is set by the day of the month on which clock needs to be forwarded and reverted back to normal. Set the **Month**, **Week No.**, **Day of Week**, and **Time** for both the **Forward Clock** and **Backward Clock** as shown.

The screenshot shows the 'Device Configuration' window for a device named '5 Wireless Door 1st Floor'. The 'Daylight Saving' tab is active. The 'DST Type' is set to 'Day-Month wise'. The 'Time Period' is set to '00:00'. Under 'Forward Clock', the 'Month' is 'January', 'Week No.' is '1st', 'Day of Week' is 'Sunday', and 'Time' is '00:00'. Under 'Backward Clock', the 'Month' is 'January', 'Week No.' is '1st', 'Day of Week' is 'Sunday', and 'Time' is '00:00'. A 'Save' button is at the bottom right.

- On selection of the **Date-Month wise** option, the DST is set by date of the month on which clock needs to be forwarded and reverted back to normal. Define the **Time Period** for the date-month wise DST settings in **24-hours** format, and specify **Month**, **Date** and **Time** for the **Forward Clock** and the **Backward Clock** as shown.

This DST Setting implies that on 1st Sunday of November at 09:00 hours, the clock will be forwarded by 08:00 hours. And on 1st Sunday of January at 10:00 hours, the clock will be reversed or backwarded by 08:00 hours.

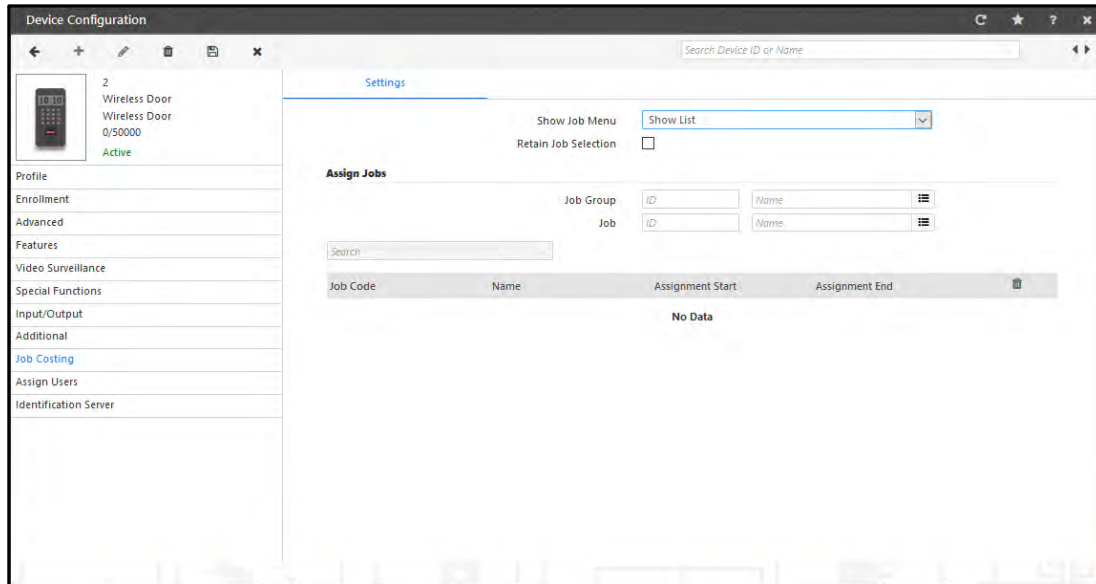
The screenshot shows the 'Device Configuration' window for the same device. The 'Daylight Saving' tab is active. The 'DST Type' is set to 'Date-Month wise'. The 'Time Period' is set to '00:00'. Under 'Forward Clock', the 'Month' is 'January', 'Date' is '1', and 'Time' is '00:00'. Under 'Backward Clock', the 'Month' is 'January', 'Date' is '1', and 'Time' is '00:00'. A 'Save' button is at the bottom right.

- Click the **Save** button.

Job Costing

When user punches on any device, there will be an option to select the Job Code on which the user is working. Job Costing enables the admin to show or hide Job Code selection on device.

To access these configurations, select the **Job Costing** tab.



Show Job Menu: Select **Show List** so that multiple jobs can be assigned to the device. Select **Allocate Default** so that only default jobs can be assigned on the device.

The user can select the relevant job code while punching on the device. His job hours will be recorded for that job code.

- **Retain Job Selection:** Select this checkbox to retain the job code selected by a user which would be applicable for all the subsequent users until another job selection is done on device.
- **Assign Jobs:** Select the Job group and multiple jobs from the picklist.

Then click on **Save** button. The jobs will be listed to the grid.



The maximum limit for job assignment is 1000 on each device

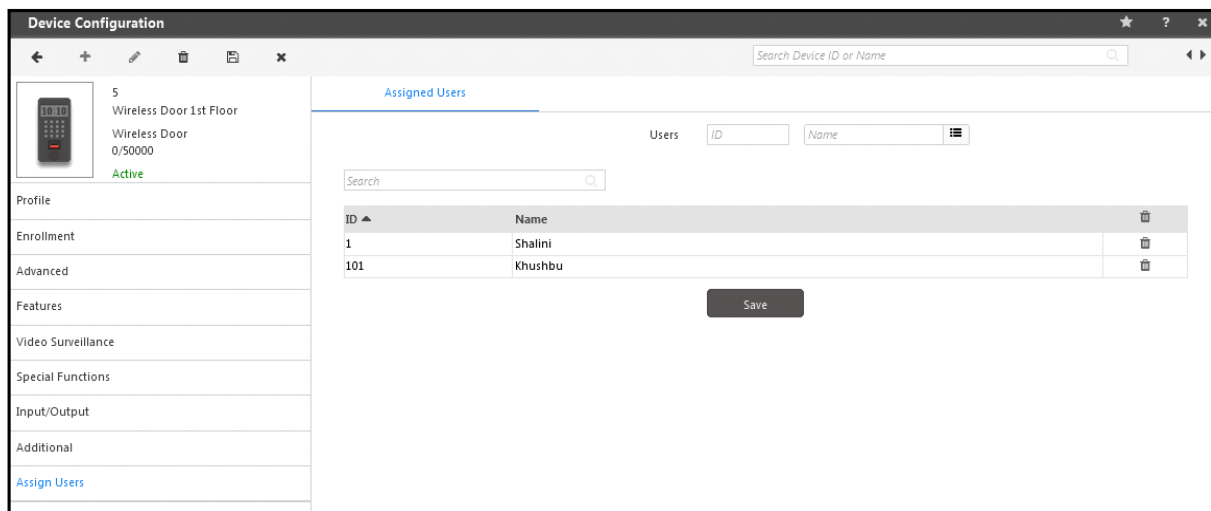


Job codes will be available for selection on the door when the user punches on the door.

Assign Users

To the configured device, you can select and assign the users.

Click the picklist button and select the users.

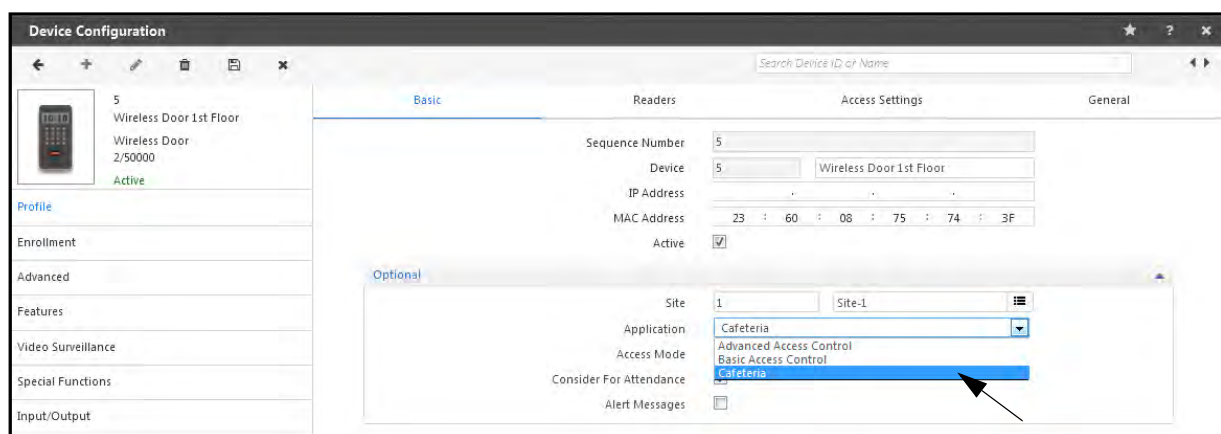


- Click the **Save** button to assign all the added users to the selected door.

Cafeteria

The COSEC system enables the user to configure devices which will be used by the Cafeteria management module.

To configure a door for Cafeteria application, select **Cafeteria** option in Device Profile> Basic> Application as shown below with arrow.



The Cafeteria tab will appear in Device Configuration page.

Select **Device Configuration> Cafeteria> Settings**

Settings

The Cafeteria configuration for Wireless Door is shown as below.

The screenshot shows the 'Device Configuration' window with the 'Cafeteria' tab selected. The left sidebar lists various configuration categories, with 'Cafeteria' highlighted. The main area displays the 'Printer Settings' section. At the top, there's a 'Consecutive Transaction Delay (Sec)' field set to 0. Below this, the 'Printer Settings' section includes a 'Printer' dropdown menu (set to 'None'), a 'Connection Type' dropdown menu (set to 'RS232'), and a 'Baud Rate' dropdown menu (set to '115200'). There are also text input fields for 'Company Name', 'Company Address', and 'Punch Line'. At the bottom, there is an 'Exclude Price-Cost From Coupon' checkbox, which is currently unchecked.

- **Consecutive Transaction Delay (Sec):** Enter the time interval between two transactions, wherein any user transaction would be restricted.

Printer Settings

- **Printer:** Select the printer from the dropdown list based on the site requirements.
- **Connection Type:** Select the printer connection type from the drop down list. The options available are:
 - RS232 (serial)
 - USB
- **Baud Rate:** In the event of a serial printer, select the appropriate baud rate from the drop down list.
- Specify the **Company Name**, **Company Address** and the **Punch Line** as per the site requirements. These details will be printed on the receipt dispensed from the selected printer.
- Select the **Exclude Price-Cost From Coupon** check box if you want to exclude the price from the coupon.

Menu

COSEC allows the administrator to assign one or more cafeteria menus (Menu 1, Menu 2, Menu 3... upto 99.) to a device. These can be configured by selecting pre-defined menus from the Menu picklist.



The Menu is created from Cafeteria module.

The Menu can be scheduled from Cafeteria module and is displayed in “Schedule Menus” as shown above.

If you have to assign another menu and schedule it on the door then select the Menu from the picklist. The Menu will be shown in the grid as shown below.

Now to schedule the menu click **Add** button as shown above.

Then select the menu to be scheduled from the **ID** picklist. Specify the **Start** and **End time** for which the Menu will be active and is available to users on the selected door. Select the **days** for which this menu will be available i.e. scheduled on the door.

Then click **OK** and **Save** the Menu schedule on the door.

Device Configuration

5 Wireless Door 1st Floor
Wireless Door
2/50000
Active

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Assign Users
Cafeteria

Menu

Assign Menu

Menu No	ID	Menu Name
1	2	Breakfast
2	1	Lunch

Schedule Menu

Menu No	ID	Menu Name	Start Time	End Time	Schedule Days
1	2	Breakfast	08:45	09:00	_ Mo Tu We Th Fr _
2	1	Lunch	12:30	14:00	_ Mo Tu We Th Fr _



Two Menus cannot be scheduled for same timing.

Identification Server

This tab enables the selected device to be assigned to a pre-defined Identification Server.

Device has a limited memory capacity for storage of templates so we need Identification Server which will store the more number of templates and respond to device when asked for identification.

For more information on Identification Servers, See *Admin> System Configuration> Identification Server Configuration*.

To access these configurations,

- On the **Device Configuration** page, select the **Identification Server** tab.

Device Configuration

Device ID
Device Name
Wireless Door
0/50000
Active/Inactive

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Identification Server

Other Biometric Credentials

Enable Identification On Server ☒

Identification Server 1 Identification - 000000000000

Configure Alternate Server Address ☐

Server Address 192.168.103.66

Server Port 11005

Enable Finger Smart Identification ☒

Identification Time-Out Duration (Sec) 4

Auto Send Enrolled Templates ☒

Default Biometric Group No. 0

Other Biometric Credentials

- **Enable Identification On Server:** Select the checkbox to enable the identification of palm/finger templates on this device.
- **Identification Server:** Select an Identification Server using the picklist button to which the device is to be assigned. The configuration of server is done from **Admin module > System Configuration > Identification Server Configuration** and the Identification Service must be started from the service tray.
 - **Server Address:** It displays the IP Address of the selected Identification Server.
- **Configure Alternate Server Address:** Enable this check-box to configure external IP address of Identification Server.
 - **Server Address:** Enter the external network IP address which will be used for accessing identification server.

Enable Identification On Server	<input checked="" type="checkbox"/>
Identification Server	1 Identification - 000000000000
Configure Alternate Server Address	<input type="checkbox"/>
Server Address	192.168.103.66
Server Port	11005
Enable Finger Smart Identification	<input checked="" type="checkbox"/>
Identification Time-Out Duration (Sec)	4
Auto Send Enrolled Templates	<input checked="" type="checkbox"/>
Default Biometric Group No.	0

- **Server Port:** Enter the server port number. The default port number is 11005.
- **Enable Finger Smart Identification:** For all other supported doors, select the checkbox to enable fingerprint templates identification through Identification Server.
- **Identification Time-Out Duration (Sec):** Specify the duration in seconds after which the fingerprint template identification will get time out.
Example: If 5 seconds is specified, then the identification server will try to identify the template till 5 seconds and if not found then it will show time-out to the user.
- **Auto Send Enrolled Templates:** Select the checkbox to enable any enrolled templates to be saved both on the COSEC database as well as saved locally on the configured Identification Server. This enables prompt identification of user on enrollment.
- **Default Biometric Group No.:** Specify the default biometric group number to be assigned to the device. It is a number allotted to a device to be assigned to the Identification Server. This enables the Identification Server to match the template against only those devices that belong to the corresponding biometric group. This reduces the false detection as well time to search template.

ARGO Door

COSEC ARGO series door controllers are performance and engineering wonders with emphasis on productivity and security for modern organizations. COSEC ARGO devices are the next generation door controllers for serious deployments of Access Control and Time and Attendance applications. The intelligent workhorse is designed to meet aesthetics, technology and harsh environmental requirements of the organization. It consists of POE terminal with Ingress Protection (IP65 rated) with Graphical Display.

There are in total 6 variants of ARGO door. They are:

Variants	Reader Supported
COSEC ARGO FOE212	EM Prox
COSEC ARGO FOM212	MiFare
COSEC ARGO FOI212	HID iClass
COSEC ARGO CAE200	EM Prox
COSEC ARGO CAM200	MiFare
COSEC ARGO CAI200	HID iClass







COSEC ARGO CAE200/CAM200/CAI200 do not support Fingerprint Module.





ARGO Door can be connected as **Direct Door** as well as **Panel Door**.











Click the ARGO device from the Device List to add it as a **Direct Door**.


Select Device Type To Be Added



ARGO

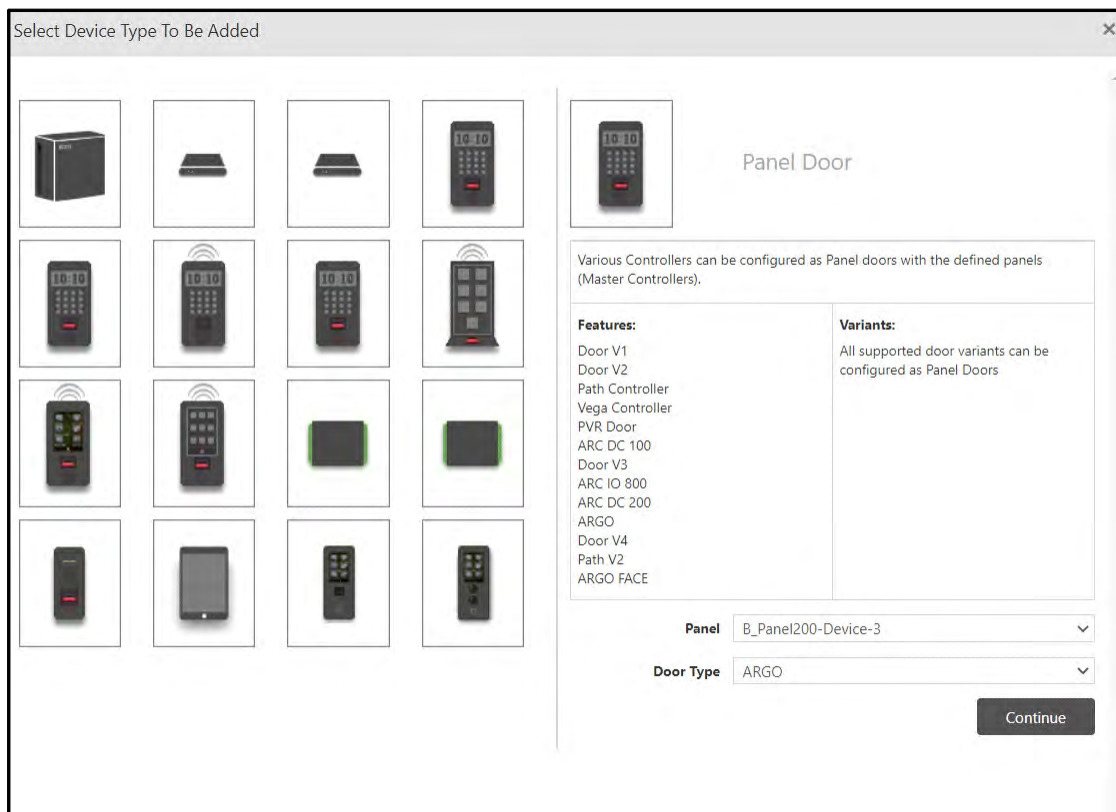
High-end Wireless terminals for Access Control, Time Attendance & Cafeteria. POE terminal with Ingress Protection (IP65 rated) & Graphical Display. Elegant design. Uses RFID, Password and Biometric Authentication.

Features:	Variants:
User Capacity: 50,000	FOE212
Event Buffer: 5,00,000	FOM212
3.5" TFT Display	FOI212
POE Enabled	CAE200
Wi-Fi and Mobile Broadband	CAM200
Connectivity with Server, Inbuilt Bluetooth	CAI200
Card, Pin, Finger and Face	

Continue

OR

Click Panel Door to add ARGO device as a **Panel Door**.

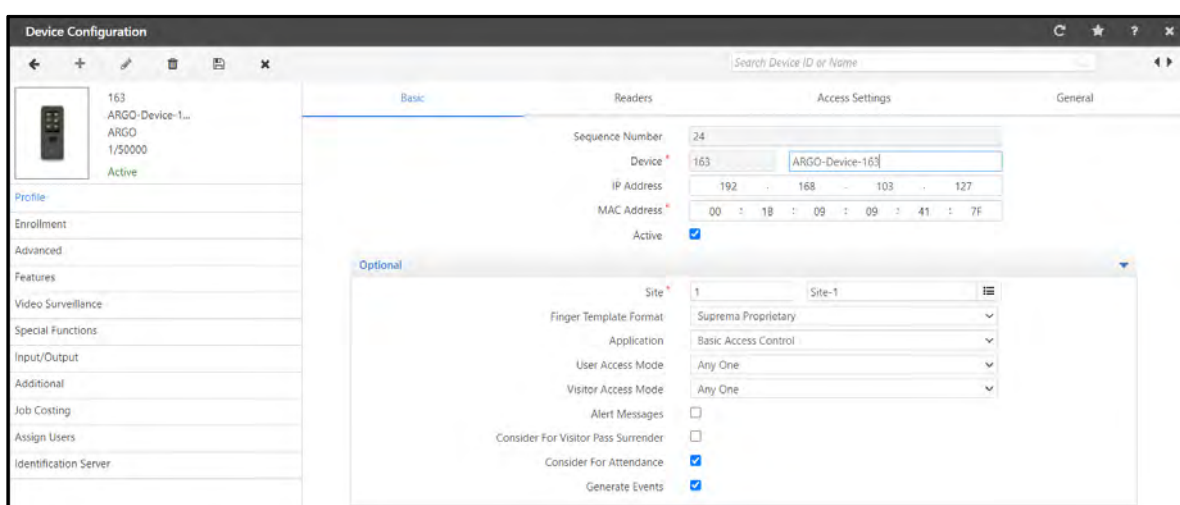


Panel: Select the desired Panel from the drop-down list with which you wish to connect the Door.

Door Type: Select **ARGO** from the drop-down list.

Click **Continue**.

The **Device Configuration** page for ARGO Door appears.



If you wish to add Devices automatically, click **Admin Module> System Configuration> Global Policy> Device**. Select the **Auto Add New Devices** check-box. Once the device is connected in network, it comes online in COSEC Monitor.

The IP Address of the device will be displayed automatically in **Profile > Basic**.



The Monitor Service must be running while adding the device to COSEC.

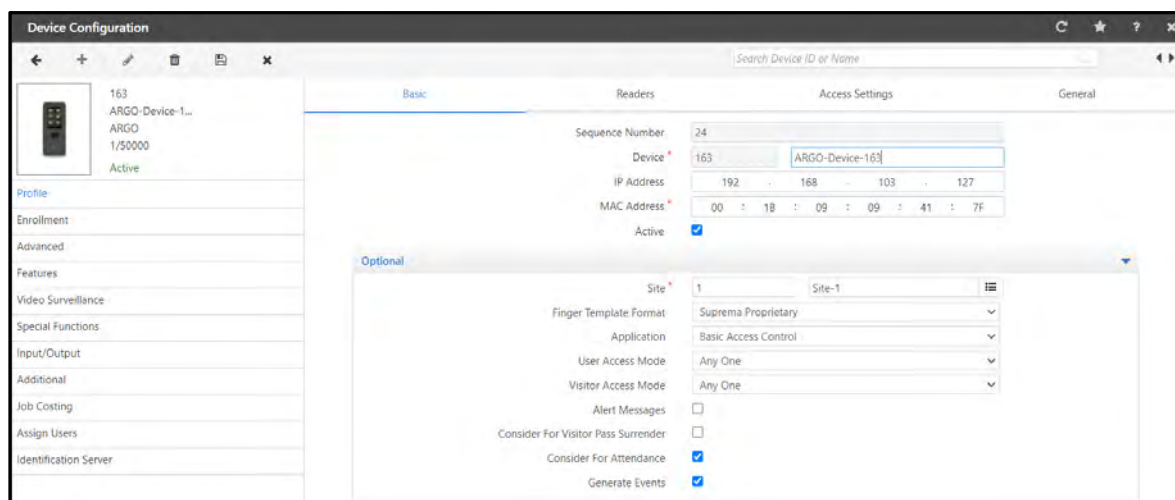
To configure the device parameters, click the following links:

- [“Profile”](#)
- [“Enrollment”](#)
- [“Advanced”](#)
- [“Features”](#)
- [“Video Surveillance”](#)
- [“Special Functions”](#)
- [“Input/Output”](#)
- [“Additional”](#)
- [“Job Costing”](#)
- [“Assign Users”](#)
- [“Cafeteria”](#)
- [“Identification Server”](#)

Profile

Setting up a door profile involves configuring basic parameters to set up any door controller device. This section enables the user to set up the basic profile for any new device.

To do so, on the **Device Configuration** page, click the **Profile** tab in the left pane.



To configure the Profile parameters click the following links:

- [“Basic”](#)
- [“Readers”](#)
- [“Access Settings”](#)
- [“General”](#)

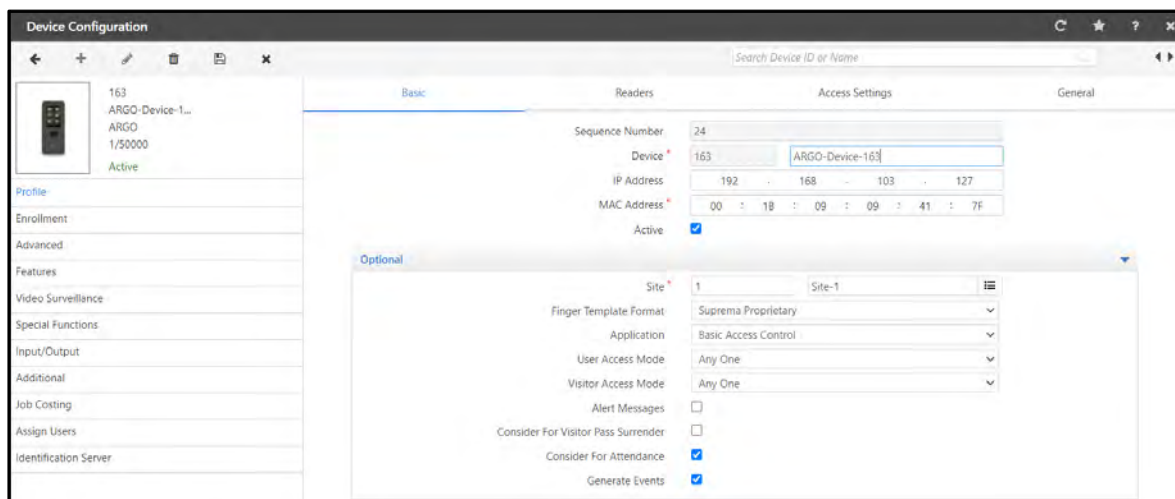
Basic

Click **Basic** tab. The **Basic** page appears.



Sequence Number, Device, IP Address, MAC Address and Active are applicable for both Direct Door and Panel Door.

For ARGO Door as a Direct Door,



Configure the following parameters:

- **Sequence Number:** This is a system generated sequence number for each new device.
- **Device:** Specify a name that can be assigned to the door. The Door ID is auto-generated by the system.
- **IP Address:** This is the IP address assigned to the door. Once the device connection is established, this field will automatically display the door IP address.
- **MAC Address:** Specify the MAC Address of the door.



MAC address of door is required while manually adding the door to the COSEC Monitor. Note the MAC address from the device when it is powered on.

- **Active:** Check the box to activate the device on the network.



To add the Device automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the “**Auto Add New Devices**” checkbox.

The device will be added automatically but make sure you enable the **Active** checkbox in order to connect the device to the network. Once the device is connected to the network, it will come online in COSEC Monitor.

Click the **Optional** collapsible tab, to configure the following parameters:

- **Site:** Select the site to which this door is to be assigned from the site pick list window. Site is created from Devices> Masters> Site.
- **Finger Template Format:** Select the format as Suprema Proprietary or Suprema ISO according to which the templates will be enrolled. For globally setting the template format, you can set from Global policy.
- **Application:** Select the application type for which the device is to be used. The options are **Basic Access Control**, **Advanced Access Control** and **Cafeteria**. All devices set to **Cafeteria** will subsequently be available for Cafeteria configuration.
- **User/Visitor Access Mode:** Defines the type and combination of credentials required to identify and validate a user at the Door Controller. Select the appropriate credential combination from the drop down list. The options available are:
 - Any one
 - Card

- Card + Biometrics
 - Card + Biometrics + PIN
 - Card + PIN
 - Biometrics
 - Biometrics + PIN
 - Biometrics then Card
 - None
 - Face
 - Card+ Face
 - PIN + Face
 - Biometrics+ Face
 - Card then Biometric
- **Cafeteria Face Access Mode** - When Application is set as '*Cafeteria*', only then this configuration is available to the Admin and to add provision of using face as a credential to make transactions on cafeteria devices.
 - Select the mode type from the drop down to allow a user to choose multiple menu items and upon checkout do transaction using face as credential.
 - The options available are **None**, **Default Item** and **Item Selection**.

The screenshot shows a configuration window titled 'Optional' for 'Site-1'. The 'Cafeteria Face Access Mode' dropdown is expanded, showing the following options:

- None
- Default Item
- Item Selection (highlighted)

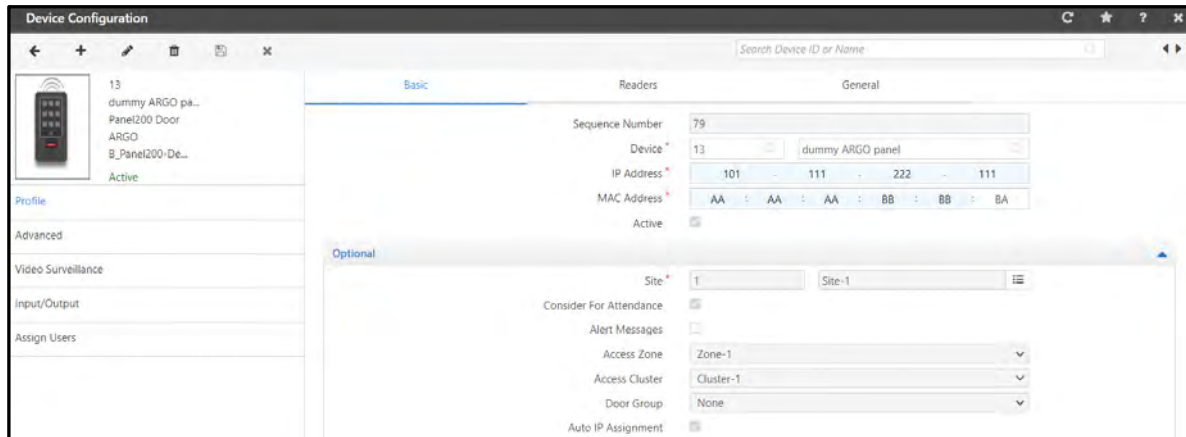
Other visible settings include:

- Site: 1
- Finger Template Format: Suprema Proprietary
- Application: Cafeteria
- User Access Mode: Any One
- Visitor Access Mode: Any One
- Consider For Attendance: ☐
- Alert Messages: ☐
- Consider For Visitor Pass Surrender: ☐
- Generate Events: ☒

- Default Item mode in cafeteria will allow users a touch less cafeteria experience. In Default Item mode only the transaction for default item is allowed. A default item is assigned in each scheduled menu.
 - Item Selection mode in cafeteria will allow users to select the desired menu items and make a transaction using Face as a credential.
- **Consider for Attendance** - Select this check box if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as access control events.
 - **Alert Messages** - Select this check box to enable the application to send alerts based on events from this door.
 - **Consider for Visitor Pass Surrender**: Check the box to consider the selected device for visitor pass surrender. The Visitor can show his credential on this device to surrender the pass.

- **Generate Events:** This check-box is enabled by default. You can disable the check-box if the server is not required to receive any events from the respective devices.

For ARGO Door as a **Panel Door**,



Click the **Optional** collapsible panel, to configure the parameters:

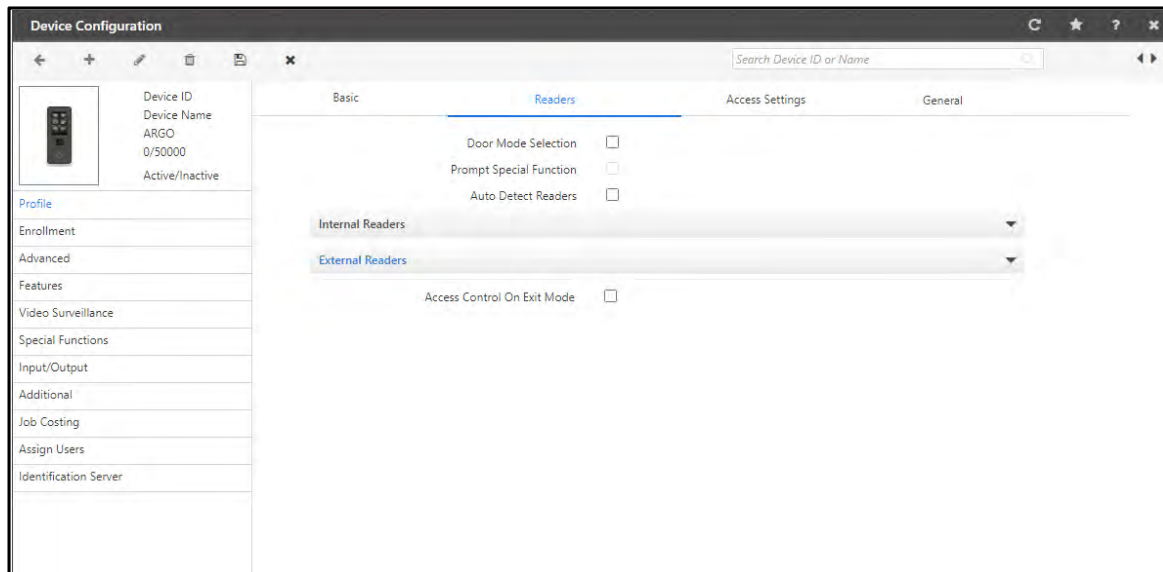
- **Site:** Click the picklist and select the site to which this door is to be assigned. Site is created from **Devices > Masters > Site**.
- **Consider for Attendance:** Select this check box if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as Access Control events.
- **Alert Messages:** Select this check box to enable the application to send alerts based on events from this door.
- **Access Zone** (only for panel doors) - Assign an access zone to the door by selecting from the drop down menu.
- **Access Cluster** (only for panel doors) - Assign an access cluster to the door by selecting from the drop down menu.
- **Door Group:** Door Group drop down includes list of all configured Door groups on corresponding panel. An additional option as 'None' is available and selected by default.
- **Auto IP Assignment:** There is option where panel door can be assigned its IP from device webpage. To enable this check the Auto IP Assignment box.



Access Zone is configured while configuring Panel200.

Readers

Readers are important hardware components in a biometric door device. They may be internal or external. This section enables the administrator to configure both internal and external readers for a door as shown.



The following parameters are available for configuration:

Door Mode Selection - If this option is enabled, then user will be prompted to select punch type as IN or OUT while punching on the device.

E.g: When a door is in Entry mode, your punches will always be in Entry side. But if you want to mark the punch in ext mode then you can select the door mode if “Door Mode Selection” is enabled.

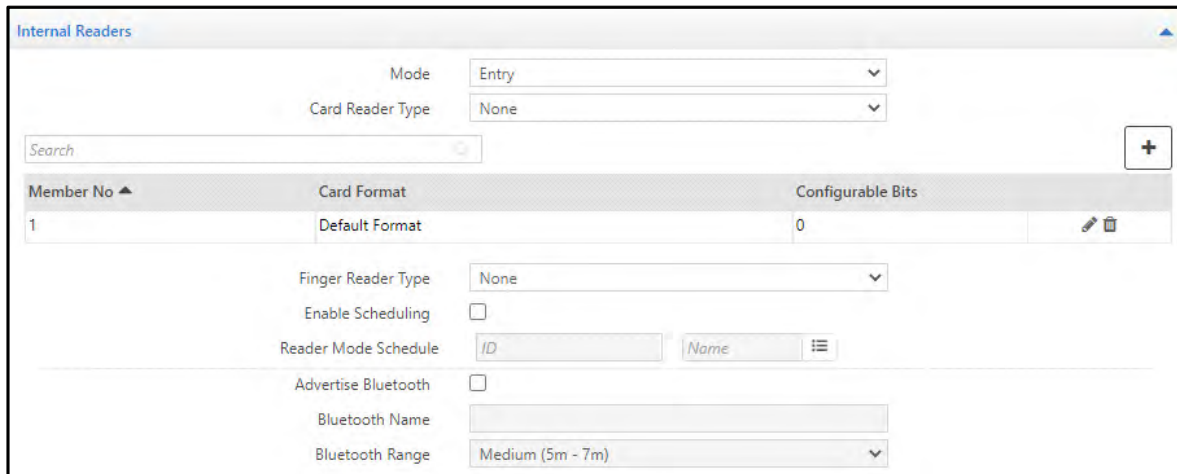
If not selected, user will need to enable Scheduling to set reader mode of door as entry or exit as per user-defined schedules. For information on creating Reader Mode Schedules, **see Devices > Masters > Reader Mode Scheduler**.

Prompt Special Function- This will provide selection of special function on device screen and based on the selection of particular type of special function, job codes for JPC user will be prompted. This can be enabled only when “Door Mode Selection” is enabled.

Auto Detect Readers (for direct doors only) - Select this checkbox to enable auto detection of Readers on a door controller connected to the server.

Internal Readers

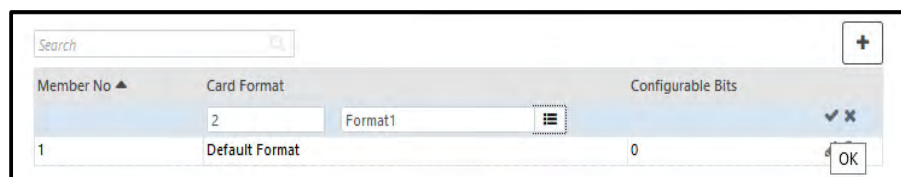
This option allows the configuration of the Internal Reader for the selected door.



- **Mode:** Select the Mode as **Entry** or **Exit** from the drop down list.
- **Card Reader Type;** Select the Card Reader Type from the following options:
 - EM Prox Reader
 - HID Prox Reader
 - MiFare Reader
 - HID iClass-U Reader
 - HID iClass-W Reader
- **Card Format:** The single or multiple card formats can be assigned to the readers of both direct and panel doors. The default card format is assigned to device as shown in the grid. If no other card format is assigned to device; then this default format will be applied. To know more about Card Formatting, refer ["Card Formats"](#).

Multiple Card Format

To assign multiple card formats to device click on **Add** button. Then click the picklist to select the card format. And click **OK** to save the format.



Similarly you can add maximum 5 card formats. When the card format is saved, the Configurable bits of that format as configured from Masters> Card format will be displayed here. Multiple Card format configurations will be dispatched to door separated by 'Format ID' that is 'Member No.' along with all other format related parameters.

Internal Readers

Mode: Entry

Card Reader Type: EM Prox Reader

Search:

Member No ▲	Card Format	Configurable Bits	
1	Default Format	0	
2	Format1	26	
3	Format2	32	

- Select the **Finger Reader Type** as **Finger Reader**.

Click the **FP Reader Configuration** button to set the **Security Level**, **Lighting Condition**, **Sensitivity**, **Fast Mode**, **Image Quality** and **Restore Defaults** for the selected FP Reader as shown.

Finger Print Module Calibration

Security Level: Normal

Lighting Condition: In Door

Sensitivity: Level 8 (High)

Fast Mode: Auto

Image Quality: Moderate

Restore Defaults

Save **Close**

Finger Print Module Calibration

- **Security Level:** Security level specifies FAR (False Acceptance Ratio). Since FAR and FRR (False Rejection Ratio) is in inverse proportion to each other, FRR will increase with higher security levels. For regular Time-Attendance system “**Normal**” level can be selected. For high security areas requiring complete or maximum matching of template, “**Highly Secure**” level must be selected. For approximate matching of template, “**Secure**” level can be selected.
- **Lighting Condition:** Optical sensors are sensitive to lighting condition. With this parameter, users can tune optical sensors to be adapted for their lighting environment. Select the In Door or Out Door option based on the device location.
- **Sensitivity:** Specifies sensor sensitivity to detect a finger. On high sensitivity, the module will accept the finger input more easily. Level 8 has the highest sensitivity.
- **Fast Mode:** Fast Mode parameter can be used to shorten the matching time with a little degradation of authentication performance. In typical cases, Fast Mode 1 is 2 to 3 times faster than Normal mode while Fast Mode 5 is 6 to 7 times faster than Normal mode. There is also an Auto mode.
- **Image Quality:** When a fingerprint is scanned, the module will check if the quality of the image is adequate for further processing. Image quality parameter specifies the strictness of this quality check. Strongest option might lead to higher number of finger rejections during the enrollment process.



Good quality of enrollment(around 70-75% quality) is recommended for proper identification of enrolled templates.

- Click on the **Restore Defaults** button to return the field values for this page to default values if needed.
- **Enable Scheduling:** Check the box to enable automated control for the mode of an Internal Reader. This will set reader mode of door as entry or exit as per user-defined schedules.
- **Reader Mode Schedule:** Select the schedule from the picklist which is to be assigned to the internal reader of ARGO door. With this the same reader can be configured to function both in Entry as well as Exit mode based on scheduled timings.



For configuring Reader Mode schedule See Devices> Masters> Reader Mode Scheduler.

- **Advertise Bluetooth-** Select this checkbox to enable Bluetooth of the device by which the device will be visible to others. Then configure the following parameters.
- **Bluetooth Name-** By default, if the Device Name is configured then it will be displayed here along with the Mode. The prefix will be the Device Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the bluetooth name as per your requirement. The Bluetooth Name can be a maximum of 10 characters.

- **Bluetooth Range-** The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m-2m), Medium (5m-7m) or Long (>8m).

Click on the **Save** button.

External Readers

This option allows the configuration of the External Reader for the selected door.

Member No	Card Format	Configurable Bits
1	Default Format	0

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop down list.
- **External Reader Type:** Select the desired type of External Reader from the drop-down list.



Using PIN-W Reader; user can change their PIN number through devices.

- **Card Format** - Select a card format to be applicable for external readers of the device. This is applicable for all direct doors and all Panel doors. For multiple format description [“Multiple Card Format”](#)
- **Exit Switch** - Select this checkbox to enable the use of **Exit Switch**.
- **User/ Visitor Access Mode** - Select the desired access mode for User/Visitor.
- **Configure Bluetooth from Server:** When you select **External Reader Type** as — CB U Reader, ATOM RD300, ATOM RD200 or ATOM RD100, select **Configure Bluetooth from Server** checkbox to enable Bluetooth feature for the mentioned external readers.

Member No	Card Format	Configurable Bits
1	Default Format	0

Configure Bluetooth From Server ☒

Advertise Bluetooth ☒

Bluetooth Name

Bluetooth Range

Once you enable **Configure Bluetooth from Server**, configure the following Bluetooth parameters:

- **Advertise Bluetooth-** Select this checkbox to enable Bluetooth of the ARGO device by which the device will be visible to others. Then configure the following parameters
- **Bluetooth Name-** By default, if the Device Name is configured then it will be displayed here along with the Mode. The prefix will be the Device Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the bluetooth name as per your requirement.

The Bluetooth Name can be a maximum of 20 characters.

- **Bluetooth Range-** The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m-2m), Medium (5m-7m) or Long (>8m).



If Auto Detect Reader is enabled, then External Reader Bluetooth parameters will not be visible.

- **Access Control On Exit Mode** (only for direct door) - Select this check box to enable the checking of the following access control policies on door when the external reader is in the 'exit' mode.
 - User enabled
 - User validity
 - Blocked user
 - Time Based Access Check
 - ASC
 - User Access Group

Click **Save** to save all the configurations.

Access Settings

This section is available for direct doors. The **Access Settings** page appears as shown below:

The screenshot displays the 'Device Configuration' window with the 'Access Settings' tab active. On the left, a sidebar lists various configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main area is divided into four tabs: Basic, Readers, Access Settings (selected), and General. Under the 'Access Settings' tab, the following settings are visible: 'Universal Time Zone' set to '(GMT+05:30)Chennai, Kolkata, New Delhi, Mumbai'; 'Time Format' set to '24 Hours'; 'Auto Synchronize with NTP' checked; 'Preferred NTP Server' as an empty text field; 'Working Days' with checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, Sat, and Holiday, all of which are checked; 'Working Hours(HH:MM)' set from '00:00' to '23:59'; and a section for 'Holiday Schedules' with four entries, each consisting of a number (1-4) and a schedule name (Schedule 1-4) with a menu icon.

- **Universal Time Zone** - Select the geographic time zone in which the DOOR will operate.
- **Time Format** - Specifies the time format to be displayed on Door Controller LCD display. The formats available are:
 - 24 Hours
 - 12 Hours

Select the relevant option from the drop down list as per the site requirements.

Auto Synchronize with NTP

If Date and time is to be automatically synchronized as per the **Preferred NTP Server** (predefined or user-defined NTP server address) selected by user, then you must enable **Auto Synchronize With NTP** checkbox.

Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from device webpage, which will be reflected on device display.

- When Auto Synchronization with NTP is disabled Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 1. You can specify the Preferred NTP server of your choice. In this case device will first try to get Date and Time from that server address.
If it does not get Date and Time in three tries; device will check from pre-defined NTP servers.
If you have entered one of the three pre-defined NTP servers(ntp1.cs.wisc.edu , time.windows.com , time.nist.gov); then device will first check that server first.
If it receives updated Date and Time then Updated Date and Time will be reflected on device webpage and display screen.
 2. You can keep the Preferred NTP server as blank. In this case device will check for Date and Time from the first NTP server.

3. If user has manually entered Date and Time from webpage or Device Menu then those values of Date and Time will be reflected on device webpage and display screen.

In the case of the **Manual** option the administrator can manually update the time on the Door with that of the system time as and when required. This can be accomplished from the COSEC Monitor and control application.

- **Working Days** - Specify the days on which the default working hours should be applicable. Check the relevant boxes to specify the active days.
- **Working Hours (HH:MM)** - Define the default working hours in HH:MM format.
- **Holiday Schedule** - This section allows the administrator to assign up to four holiday schedules to the device by using the Holiday Schedule picklist.



If the same holiday schedule is configured for a user and for the door controller on which the user is assigned, then the user's attendance marking on this device, on any of the scheduled holidays will always be marked as a holiday.

General

The **General** page appears as follows. Enter all general details applicable to the device in this section.

Device Configuration

26
KJ-ARGO
ARGO
0/50000
Active

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Basic Readers Access Settings **General**

Mute Buzzer ☐

Allowed Acknowledgement

Display Duration (ms) 500

LED - Buzzer Duration Short

Denied Acknowledgement

Display Duration (ms) 3000

LED - Buzzer Duration Long

Enable Display Messages ☐

Custom Birthday Message Happy Birthday

Display Message 1 ☒

Schedule 00:00 11:59

Message Good Morning

Display Message 2 ☒

Schedule 12:00 15:59

Message Good Afternoon

Display Message 3 ☒

Schedule 16:00 20:59

Message Good Evening

Display Message 4 ☒

Schedule 21:00 23:59

Message Good Night

Multi-Language Support ☐

Auto Hide Menu Bar ☐

- **Mute Buzzer** - User can mute or unmute the door buzzer by checking or clearing the box respectively. This is applicable for both Direct and Panel door.
- **Allowed Acknowledgement**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgement Allowed' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.
- **Denied Acknowledgement**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgement Denied' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.
- **Auto Hide Menu Bar**- If a person touches the device screen by mistake and enter into Menu; then the finger sensor will not take the punch when he punches on device till the menu is closed or time out occurs. So in this case; enabling the **Auto hide Menu Bar** check-box will hide the menu and the user will be able

to punch on the door. If you want to access the Menu then swipe upwards on the screen which will show the menu.

It is applicable for ARGO direct door and ARGO Panel200 door.



The below mentioned features are available in direct door only.

- **Enable Display Messages** - This feature allows the user to enable custom birthday message and display messages to be displayed on the door device. Upto 4 display messages can be configured for a door.
- **Custom Birthday Message**- Enter the birthday message which would appear on the door when the user punches on the door on his birth date.

The valid values are

A-Z

a-z

0-9

`~!@#\$%^&*()_+~{}|:;?<>,.\'"

- **Display Message** - Enable each display message individually by selecting this checkbox.
- **Schedule** - For each message, the user needs to define the time period between which this message is to be displayed.
- **Message** - Enter the message to be displayed in this field. Maximum 21 characters allowed.
- **Multi-Language Support** - Select this checkbox to enable multi-language support for the selected device.

The **Display From** field shall display the reading order for the selected language.



However for (Wireless Door/PVR Door/Door V3/Door V4) will support languages with english fonts (A-Z,a-z) only.

Enrollment



The Enrollment section is not available for panel doors.

The Enrollment page appears as shown below.

Device Configuration

29
ARGO-Device-2...
ARGO
4/50000
Active

Profile

Enrollment

Advanced

Features

Video Surveillance

Special Functions

Input/Output

Additional

Job Costing

Assign Users

Identification Server

Settings

Enroll From Device ☒

Enrollment Mode ReadOnlyCard

Template Per Finger Single Template/Finger

Max Number Of Fingers Two

Number of Fingers One

Number Of Cards One

Enable Self-Enrollment ☐

- **Enroll from Device** - Select this check-box to enable the enrollment of user from the door controller. When this check-box is enabled, 'Enroll User' special function on that device will get active as shown below.

Device Configuration

29
ARGO-Device-2...
ARGO
4/50000
Active

Profile

Enrollment

Advanced

Features

Video Surveillance

Special Functions

Input/Output

Additional

Job Costing

Assign Users

Identification Server

Configuration

No.	Function Name	Active	Job Selection	User Group	Card-1
1	Official Work - IN	Yes	Yes	All	
2	Official Work - OUT	Yes	Yes	All	
3	Short Leave - IN	Yes	Yes	All	
4	Short Leave - OUT	Yes	Yes	All	
5	Regular - IN	Yes	Yes	All	
6	Regular - OUT	Yes	Yes	All	
7	Break End	Yes	Yes	All	
8	Break Start	Yes	Yes	All	
9	Overtime - IN	Yes	Yes	All	
10	Overtime - OUT	Yes	Yes	All	
11	Enroll User	Yes	No	All	
	Enroll Special Card	Yes	No	All	

If 'Enroll User' special function & 'Enroll From Device' check-box both are inactive in device configuration, then on activating 'Enroll User' special function, 'Enroll From Device' check-box will be enabled.

- **Enrollment Mode** - Select the Credential from the drop-down list that can be enrolled using the special function at the DOOR. The options are **ReadOnlyCard**, **SmartCard**, **Biometric** and **BiometricthenCard**, and **DuressFinger**. Refer ["Enroll Credentials"](#) or ["Enrolling Users"](#) to enroll User/Worker. Refer ["Enrollment"](#) or ["Enroll Credentials"](#) to enroll Worker. Refer ["Enroll Credentials"](#) to enroll a Visitor.



DuressFinger is only applicable for User and Worker.

- **Template Per Finger** - This parameter displays the values as configured at the global level. This field is not user editable from this page.
- **Max Number of Fingers** - This parameter displays the values of the maximum number of fingers configured at the global level. This field is not user editable from this page.
- **Number of Fingers/Cards** - Select the number of cards or fingerprints to be enrolled based on the credential option selected in the Enrollment Mode parameter.
- **Enable Self-Enrollment** - Select this checkbox to enable the self-enrollment feature on this door.

Advanced

The Advanced tab allows the user to configure some advanced parameters such as access control settings, alarms and device timers.

To access this, After selecting the device, Select the **Advanced** tab from **Device Configuration** page. The advanced settings can be configured from following sections:

- *“Settings”*
- *“Alarms”*
- *“Timers”*
- *“Wiegand”*

Settings

The Advanced Settings page for ARGO as a Direct Door appears on your screen as shown below:

Device Configuration

Search Device ID or Name

Device ID: 0/50000
Device Name: ARGO
Active/Inactive

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Settings Alarms Timers Wiegand

Generate Exit Switch Events ☐
Generate Invalid User Events ☐
Generate Sequential IN-OUT Events ☐
Two Credentials Required ☐
Show PIN ☐
Allow Exit when Door Lock: ☒
Auto Relock: ☐
Auto Relock Timer (Sec): 3
Enable Additional Security: ☐ Disabled
Enable Smart Identification: ☐
Access Level: 8
Access Mode: Card
Auto Acknowledge Alarm: ☐
Auto Acknowledge Alarm (Sec): 10
Facility Code: 1
Allow Access Through Mobile: ☐
Mobile Entry Access Mode: Mobile Only
Mobile Exit Access Mode: Mobile Only
Show Attendance Details: ☐
Sensor Type: FEVOBOT
Sensor Interface: USB
Emissivity: 0.95
Calibration Parameter: + 0.0
Approach to Sensor Wait-Timer (Sec): 3.0
Temperature Detection Time Out (Sec): 10
Tolerance between Consecutive Readings: 0.5
Consecutive Readings Count within Tolerance: 5
Temperature Threshold (°F): 99.5
Minimum Temperature for Access (°F): 95.0
Restriction Type: Soft
Bypass If Sensor Disconnected: ☐

The following parameters are available for configuration:

- **Generate Exit Switch Events** - Select this checkbox to enable the door to generate events everytime the exit switch is used.
- **Generate Invalid User Events** - Select this checkbox to enable the door to generate events for invalid user inputs.
- **Generate Sequential IN-OUT Events** - Select this checkbox to generate user punches on device as the sequential IN-OUT events irrespective of whichever mode in which device is functioning.
- **Two Credentials Required**- Select this checkbox to enable the feature of verifying 2 credentials mandatorily for users allowed to By-pass finger/palm.
- **Show PIN**- Select this checkbox to display the characters of PIN when the PIN is entered on device.
- **Allow Exit when Door Lock** - Select this checkbox if users are to be allowed to exit even when the Door relay is in locked condition.

- **Auto Relock** - Select this checkbox to allow the door to relock immediately when the door status changes to close after normal open irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Relock Timer** - Specify the time in seconds for the Auto Relock operation.
- **Enable Additional Security**- Select this checkbox to enable additional security at the selected Door Controller.
- **Additional Security Code** - Enter a code (ranging from 1 to 65535) in the field provided. Re-enter the code to confirm.



*Changing this value can affect the SI function. Click on the **Default Code** button to reset the **Additional Security Code** to the value set in the **Global Additional Security Code** field on the Global System Policy page.*

- **Enable Smart Identification** - Select this checkbox to enable this functionality at the selected Door Controller and select the **Access Level** and the **Access Mode** from the drop down list.
- **Auto Acknowledge Alarm** - Select this checkbox to enable the auto-acknowledgement of all alarms for this device.
- **Auto Acknowledge Alarm (sec)** - Set the time in seconds for the Auto Acknowledge Timer. The wait timer will start and on expiry of the timer, the alarm buzzer will stop automatically.
- **Show Attendance Details** - Select this check-box for displaying the Attendance Details of the user on ARGO door. This allows user to view his attendance details on ARGO door itself and there is no need to login to ESS application to view attendance details.

The attendance details of user will be displayed for default Menu Time-Out period (30 sec) after Access Allowed screen.



*1. The user whose Attendance details are to be displayed on ARGO door must be enabled for this feature. Enable the check-box **Show Attendance details on Device** from User Configuration> T&A> Attendance.*

2. While an attendance detail of one user is being displayed on device and second user tries to access the device; new user will be processed.

3. Whenever both users of 2-person rule are allowed to get access on device then attendance details screen of second user will be loaded on device.

- **Facility Code** - Set a value for Facility Code to be set for access modes other than “Card”, if Facility Code is expected in Wiegand Output. This will be applicable to all direct doors except Door V1 and V2.
- **Allow Access Through Mobile**- Check the box to allow the access to device using COSEC ACS App.
- **Mobile Entry/Exit Access Mode**- Select the entry and exit door access mode from the options of **Mobile Only**, **Mobile then Biometrics**, **Mobile then Card** and **Mobile then PIN**.



If User Access Mode is selected as “None” in Zone Configuration and Mobile Access Mode is selected as “Mobile Then Biometrics” then door can be accessed through Mobile and then Biometric credential.

- **Sensor Type**: Select the type of thermal sensor integrated in the device. There are three sensors: *AST*, *Web-Based* and *FEVOBOT*. Default sensor set is *FEVOBOT*.

- **Sensor Interface:** Select the interface on which device will communicate with the sensor.
For Sensor Type-AST.
Sensor Interface options will be: RS-232 and USB
For Sensor Type- Web-based
Sensor Interface options will be: HTTP/S
For Sensor Type-FEVOBOT
Sensor Interface options will be: USB
- **Emissivity:** Set the emissivity parameter for Sensor. This parameter should only be visible when Sensor Type is AST.Default value is 0.95.
It is used to define accuracy in sensor to detect temperature of different skin or objects.
Not applicable for FEVOBOT.
- **Calibration Parameter:** Set the calibration parameter for the thermal sensor.
On click of + the value should increase by 0.1 and on click of – it should decrease by 0.1.
Not applicable for FEVOBOT.
- **Approach to Sensor Wait-Timer:** Time for which the device will wait for user to approach the device before starting Temperature Detection.
- **Temperature Detection Time-Out:** The timer till which temperature detection will be done for the user and if valid temperatures are not found till the expiry of timer then timeout will be declared.
- **Tolerance between consecutive readings:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature doesn't fall in tolerance range the reference temperature is updated with the current temperature and the process continues.
Not applicable for FEVOBOT.
- **Consecutive readings count within tolerance:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature doesn't fall in tolerance range the reference temperature is updated with the current temperature and the process continues.
Not applicable for FEVOBOT.
- **Minimum Temperature for Access:** The minimum temperature value that should be detected is to be considered as valid temperature.
It should be less than threshold temperature. If user tries to enter a value equal to or greater than threshold temperature validation should be shown.
The default value, unit and range should be updated based on the Temperature unit set on Panel.
- **Temperature Threshold:** To set the threshold value of the temperature. The default value, unit and range can be updated based on the Temperature unit set on Panel.
- **Restriction Type:** To set restriction type as soft/hard.
- **Bypass if Sensor Disconnected:** Enable this check-box to give provision of bypassing the feature if sensor connectivity is lost.

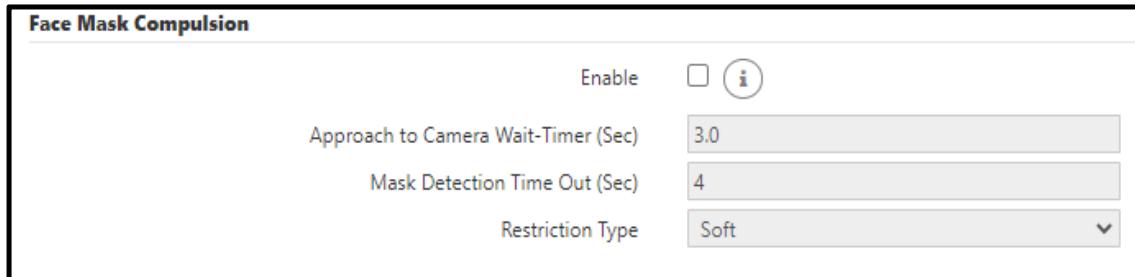
Face Mask Compulsion

Face Mask Compulsion feature is used to enforce users to wear masks while they are within the premises.

After identifying the user, Device will prompt the user to show Face with Mask when “Face Mask Compulsion” is enabled.

Based on identification of Mask, user will be allowed or denied access.

Make sure you have enabled **Enable FR** checkbox in **Devices> Device Configuration> Identification Server> Face Recognition> Enable FR** and configure the below mentioned parameters to avail this feature.



Face Mask Compulsion	
Enable	<input type="checkbox"/> ⓘ
Approach to Camera Wait-Timer (Sec)	3.0
Mask Detection Time Out (Sec)	4
Restriction Type	Soft ▼

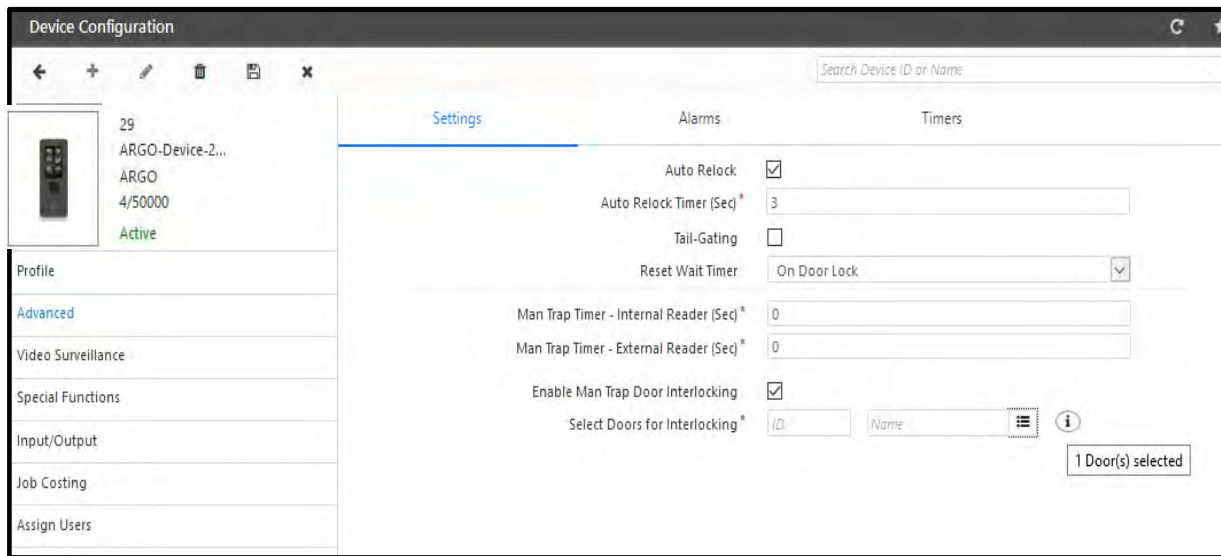
- **Enable:** Select this checkbox to enable Face Mask Compulsion feature for IDS.
- **Approach to Camera Wait-Timer (Sec):** This parameter defines the time within which the user must approach the camera for face mask detection.
 - You must enter the Wait-Time between 0.0-15.0 seconds.
 - By default, it is 3.0 seconds.
- **Mask Detection Time Out (Sec):** This parameter defines the maximum time duration for user's face mask detection.
 - You must enter the detection time out between 0.0-15.0 seconds.
 - By default, it is 4.0 seconds.
- **Restriction Type:** Select the type of restriction to be imposed when the configured policy is violated. Select the desired option - Soft or Hard.
 - **Soft Restriction:** The access will be granted even if the user is identified without wearing a mask; however, an event and a warning are generated that indicates the user has been identified without wearing a mask.
 - **Hard Restriction:** The access will be denied if the user is identified without wearing a mask.

By default it is **Soft Restriction**.



Users face enrollments are dependent on the Visible Face parameter value set by you. To know more, refer [“Face Recognition”](#).

The **Advanced Settings** for ARGO as **Panel door** is shown below:



1. **Tail-Gating** - Tail-gating refers to an access violation which occurs when more than one person tries to enter a secured area using a single person's access credentials. If this option is enabled on the panel door, the occupancy count of a zone should be incremented or decremented considering both the punch as well as the auxiliary input port of the panel door (say, input from a beam-counter). Set the wait timer for resetting the tailgating count (**Reset Wait Timer**) based on the door lock status or the door pulse wait timer (as configured).
2. **Man Trap Entry Timer (Sec)** - This check-box enables an alarm wait timer on the panel door to ensure that the user enters the next sequential door of a man-trap within a specific time-frame.
3. **Man Trap Exit Timer (Sec)** - This check-box enables an alarm wait timer on the panel door to ensure that the user exits the panel door to enter the next sequential door of a man-trap within a specific time-frame.
4. **Enable Man Trap Door Interlocking:** Select this check-box to activate the Door Interlock for the selected door (say Door1). This means if the Door1 is open then other doors will remain close.
 - **Door:** Click the pick-list and select the doors to be assigned for the Interlock to the selected door (Door1). Suppose Door2 and Door3 are selected for Interlock with Door1. So When Door1 opens; Door2 and Door3 will remain close.



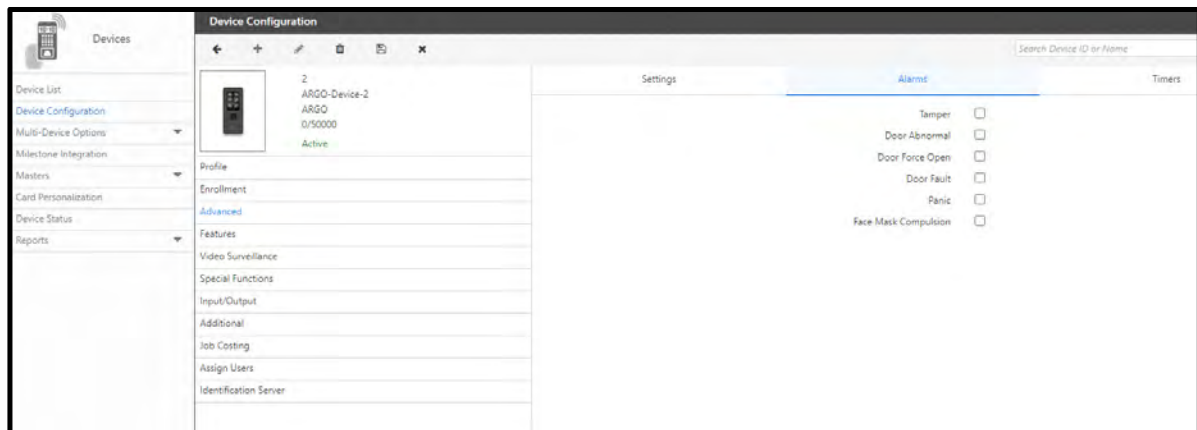
For Degrade mode Door Interlocking feature will not work.

Whenever a door is in abnormal state and for that door interlocking is enabled then user access in other doors of the interlocking group is allowed.

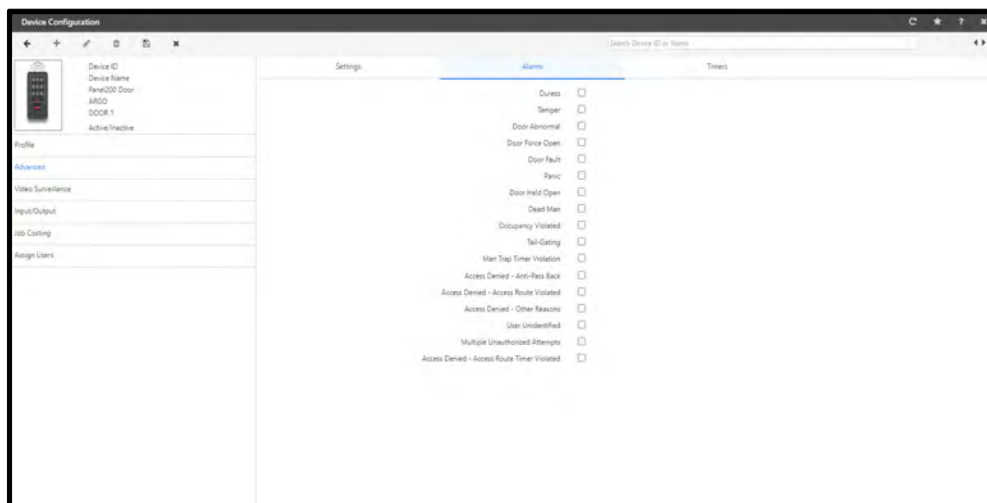
Alarms

In Alarm tab, you can assign below list of alarms to the door.

For Direct Door



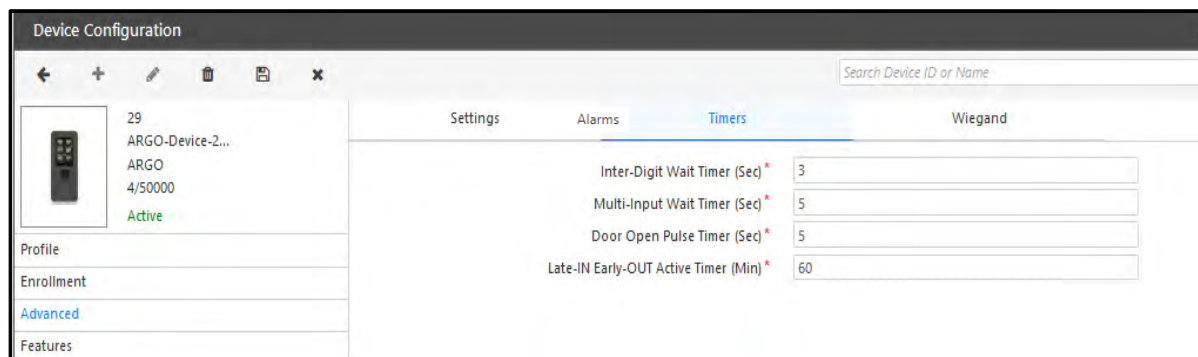
For Panel Door



Select the respective checkbox of alarms which you want to enable.

Timers

This section allows the configuration of various types of pre-defined device timers which can trigger off specific responses. In COSEC, timers are often used to control door behaviour and for triggering alarms. The **Timers** page appears on your screen as shown below:



- **Inter-Digit Wait Timer (sec)** - Specify the time period in seconds between two key inputs on the device keypad. On expiry of this timer, the system considers the user input to be complete and is ready for the next input.
- **Multi-Input Wait Timer (sec)** - Specify the time in seconds for which system needs to wait for the second credential input from the user when more than one credential is to be used to grant access.



We recommend you to set the timer value as greater than or equal to 10 seconds to avoid access denial issues to users. This is applicable when the system reads the credentials (biometric) from the user's Smart Cards.

- **Door Open Pulse Timer (sec)** - Specify the time in seconds (3 to 99) for the door to be energized for a valid credential. If the opened door does not return to a closed state before the expiry of this timer, the door will generate a "Door Abnormal" alarm.
- **Late-IN Early-OUT Active Timer (min)** - Specify the time in minutes for which the Late-IN and Early-OUT special functions will remain active after being enabled at the Door Controller.



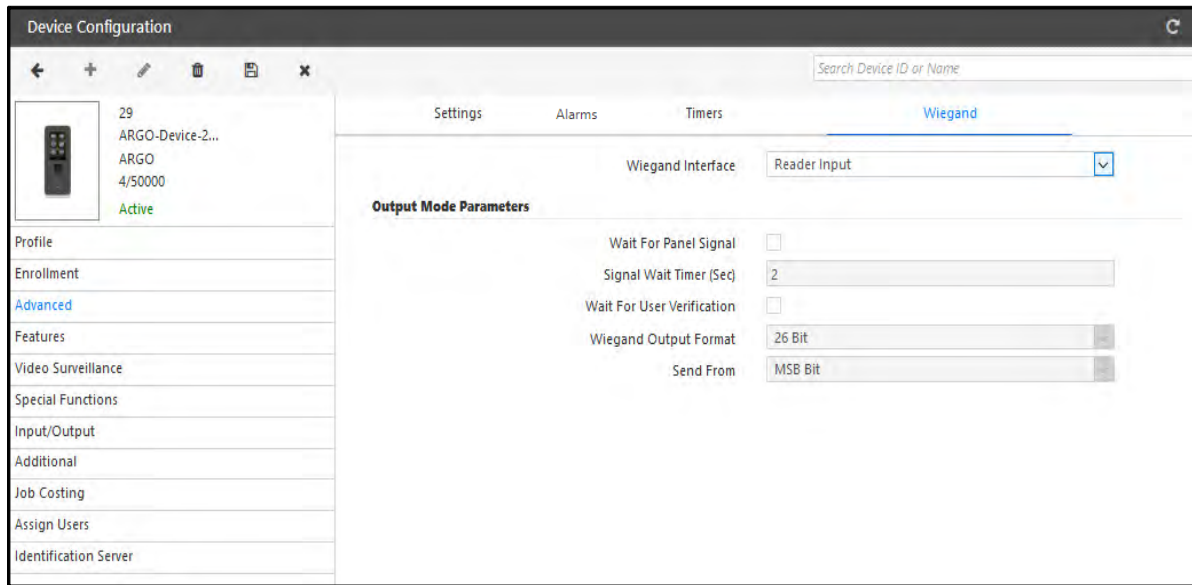
The above features are available only for direct doors.

- **Pulse Time (sec)** - Specify the time in seconds for the panel door to be energized for a valid credential.

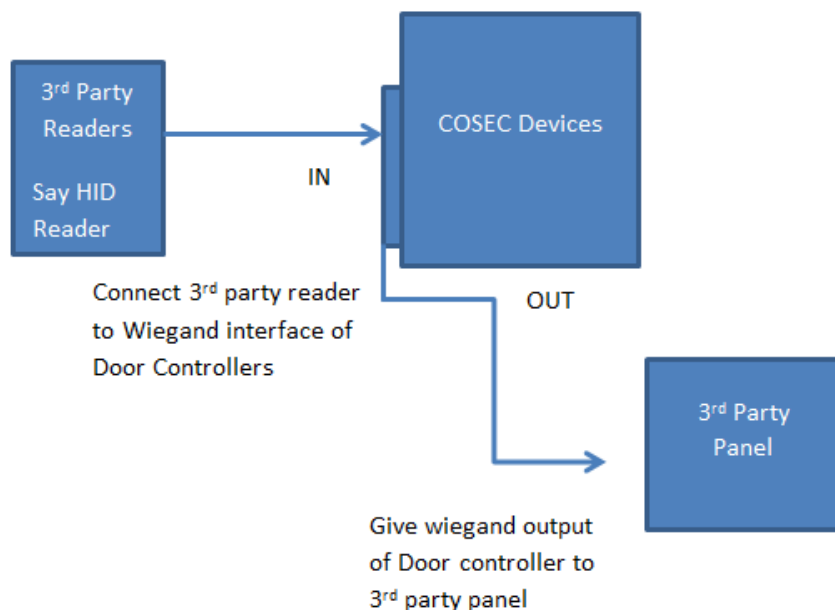


This feature is available only for panel doors.

Wiegand



- **Wiegand Interface** - The COSEC device can be connected both as input devices (e.g. to receive data from a Wiegand Reader) or output devices (e.g. to support output to third party panel) via the Wiegand interface as shown below.



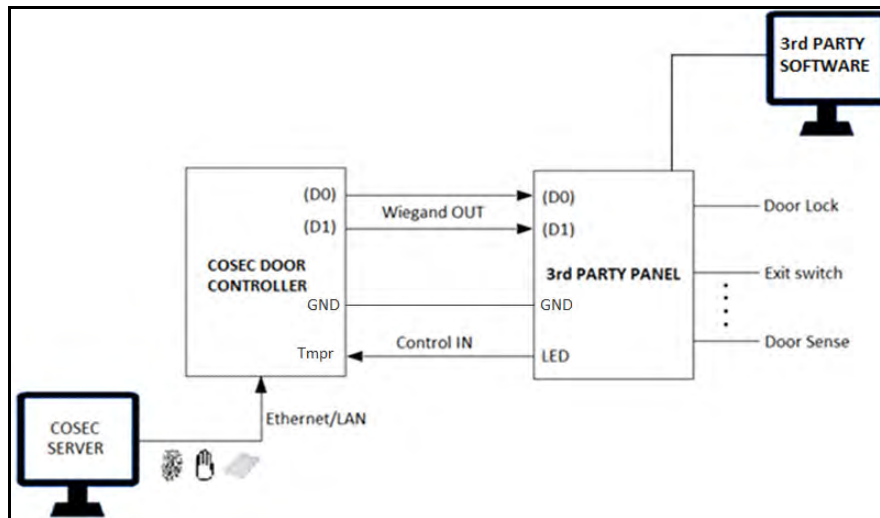
So select the interface of Door controller as **Output Mode** to work as Wiegand output to panel or **Reader Input** to take data from third party reader. If Reader Input option is selected, all the output mode parameters will be disabled.

If you select Output mode then configure the **Output Mode Parameters**.

- **Wait For Panel Signal** - If this option is enabled the door will wait for reply from the connected third party device before triggering any output, as per the defined **Signal Wait Timer (Sec)**.
- **Wait For User Verification** - If this option is enabled, user verification will be requested on the third party device before triggering any output.

- Specify the **Wiegand Output Format** and sending order for reader data as MSB or LSB Bit in the **Send From** field.

Wiegand Out Interface



Also for the **Custom** format, user can configure details of fields to be sent as output from the Wiegand reader that has been added.

Door Access using QR code

The user can access the COSEC device using COSEC APTA installed in the mobile device. If the user has rights for COSEC APTA and the access to the device is allowed for the user, then he can use his mobile device to scan the QR code which constitute the details of the COSEC door.

There is icon for QR code on COSEC APTA application. Clicking that icon will open the camera in your mobile. Now you can show the mobile camera to scan the QR code. The COSEC door will get opened after verifying the security key and access policies of the user.

Steps to create a QR code

Step 1: Enter details in JSON format

```
{"version":"x","ip": "x.x.x.x","port":"x","pdid":"x","mode":"x"}
```

Valid values:

Field	Field range	Default Value	Remark
version	1-255	1	
ip	0.0.0.0-255.255.255.255	0.0.0.0	
port	0-65535	0	
pdid	0-255	0	<p>If door is in direct door mode then, then PDID will be 0</p> <p>If door is in panel door mode then, PDID will have values from 1-255</p>

Field	Field range	Default Value	Remark
mode	0,1	0	0= for entry mode 1=for exit mode



Note:

Step1a. If door is in direct door mode enter IP & port of the direct door

b. If door is a panel door, then enter IP & port of the panel door and in the pdid specify the door id which is to be accessed.

Step 2: Encrypt the JSON string using key "matrix12" with simple DES/ECB mode.

Step 3: Encode the encrypted string using Base 64.

Step 4: Use this string to generate QR code through any third party software.

Features

The Features tab allows the user to enable certain Access Control features for a device



The Features tab is available only with the Access Control Module license and is applicable only for direct doors.

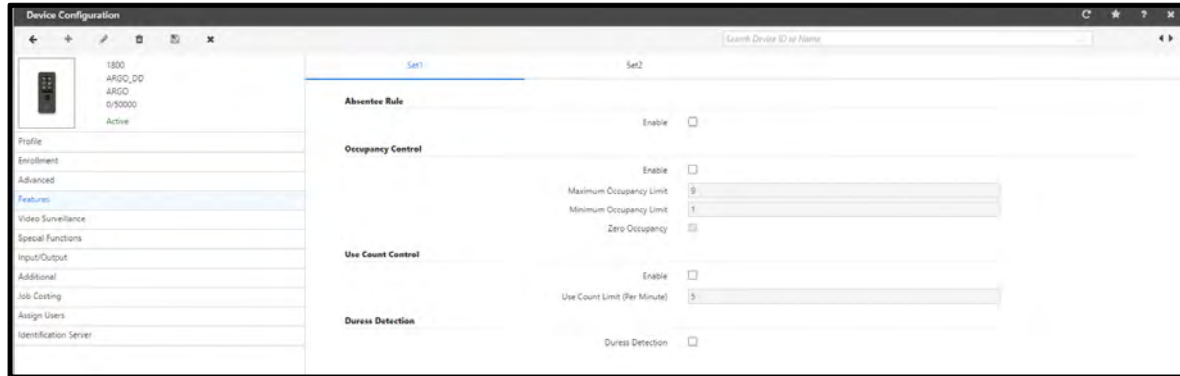
To access this, After selecting the device, Select **Device Configuration> Features**. The access control features for the device can be set from the following two sections:

- "Set1"
- "Set2"

Set1

This page allows the configuration of three rules - **Absentee Rule**, **Occupancy Control** and **Use Count Control**.

The page appears as shown below.



- **Absentee Rule** - Select this checkbox to enable this feature at the door. This rule sets the maximum number of days for non-use of a credential. On expiration of days limit, the user will be automatically blocked.
For configuring the rule *See Access Control> Absentee Rule*.
- **Occupancy Control** - Select this checkbox to enable the feature at the door and specify maximum number of users to be allowed within the controlled area after which a user exit is required to enable access to another user. Also specify the **Minimum Occupancy Limit** i.e. the minimum number of occupants the designated zone should have, and enable/disable the **Zero Occupancy** option to determine whether the designated zone should be allowed to be empty or not.
For configuring the rule *See Access Control> Occupancy Control*.
- **Use Count Control** - Select this checkbox to enable the feature at the door and specify the maximum number of uses per minute.
For configuring the rule *See Access Control> Use Count Control*.
- **Duress Detection** - Select the checkbox to enable the feature. Duress Detection is used to generate the duress alarm which informs that the user is forced to open the door under threat.

Set2

This page allows the configuration of three rules - **First-IN User Rule**, **Anti-Pass-Back (APB)** and **2-Person Rule**. The page appears as shown below.

The screenshot shows the 'Device Configuration' window for 'Set2'. On the left is a sidebar with a device icon and details: '29', 'ARGO-Device-2...', 'ARGO', '4/50000', and 'Active'. Below this are menu items: Profile, Enrollment, Advanced, Features (highlighted), Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main area is divided into three sections for rule configuration:

- First-IN User Rule:** Enable ☒. Reset On: ☒ Day Change ☐ Timer Expiry. Access Timer (Sec): 3. First-IN User Group: 1 (List 1).
- Anti-Pass-Back (APB):** On Entry ☒. On Exit ☐. Hard/Soft: Hard. Forgiveness ☒. Reset After: ☒ Day Change ☐ Timer Expiry. Forgiveness Timer (Mins): 1.
- 2-Person Rule:** Enable ☒. Mode: Primary Must. Primary Group: g1. Secondary Group: None.

- **First-IN User Rule** - Select this checkbox to enable the feature at the direct door and select the First-In User group which would be valid at the door.
For configuring the rule See *Access Control> First- In User Rule> Assignment*
- **Anti-Pass Back (APB)** - Select the checkbox to enable the feature at the direct door.

On Entry: Check this box so that the system monitors the entry reader for APB violation.

On Exit: Check this box also so that the system monitors the entry as well as the exit readers for APB violations.

Hard/Soft: Select the restriction type as Hard or Soft option from the drop down options.

- **Hard APB:** The access will be denied if the exit is not registered first. It does not allow a second entry using the same card without an exit.
- **Soft APB:** The access will be granted even if the exit is not registered. It allows a second entry of the same user without an exit; however, an event and a warning are generated that indicates the second entry.

Forgiveness: Check this box to enable the system to reset the APB status. When forgiveness is enabled, then there will be following options to reset the pass.

1. **Reset After Day Change:** This will reset the APB status of all the users to NULL at midnight. This enables a user, who left the building in the evening without exit punch, to use his card for entry in the next morning.
 2. **Reset After Timer Expiry:** This will reset the APB status of all the users after the expiry of user defined time.
 - **Forgiveness Timer (Mins):** Enter the time duration in minutes after which Anti-pass back status will get reset and the pass will be in original state.
- **2-Person Rule** - Select this checkbox to enable the feature at the door and set the **wait time** in seconds after which the second person is allowed to punch on the door.
For configuring the rule See *Access Control> 2- Person Rule*

Video Surveillance

The Video Surveillance tab allows the user to configure parameters for video surveillance integration with the COSEC device.

It is available in Basic License.

To access this, Go to **Device Configuration> Video Surveillance**.

- “Visual Tagging”
- “Satatya/IP Camera Integration”

Visual Tagging

The COSEC application can interface with some supported hybrid and network video recording systems as well as IP Cameras and grab images triggered by user events at the Doors. The **Visual Tagging** option enables the administrator to define the video recorder and IP Camera parameters. The **Visual Tagging** page appears as shown below.

The screenshot displays the 'Device Configuration' window with the 'Visual Tagging' tab selected. On the left, a sidebar lists various configuration categories, with 'Video Surveillance' highlighted. The main area is divided into two sections: 'Visual Tagging' and 'Satatya/IP Camera Integration'. Under 'Visual Tagging', there are fields for 'Capturing Device' (set to 'Matrix HVR/NVR'), 'MAC Address' (00_1b_09_01_5c_25), 'Camera ID' (2), and 'Storage Root Folder' (abc). The 'Satatya/IP Camera Integration' section includes a checkbox for 'FTP Login Credentials' and fields for 'User Name' and 'Password'.



To view the user events and related images, go to **Admin > Views/Logs > Event View**. To know more about viewing events, refer to “Event View”.

The following parameters are available for configuration:

- **Capturing Device** - Select the video recording type of device or IP Camera from the drop-down menu as shown.

The compatible device types are:

- Matrix HVR/NVR
- Milestone
- IP Camera

Matrix HVR/NVR

- **MAC Address** - In the event of selecting the Matrix HVR/NVR, the administrator needs to specify the MAC address of the video recorder device using “_” (underscore) as the separator.
- **Camera ID** - Specify the camera number or camera ID for IP cameras. For analog cameras specify the camera number.
- **Storage Root Folder** - Specify the Root folder path or FTP Path where the uploaded images will be saved.
- **FTP Login Credentials** - Check this box to activate FTP login credentials for authentication.
- **Username** - Specify the FTP server username.
- **Password** - Specify the FTP server password.



Some COSEC devices do not support all the network connection options.

Milestone

Event ID	Name	User-Defined Event ID	User-Defined Event Name
No Data			

Camera Name	GUID	Host Name	Port
MATRIX COMSEC CIDR20VL12CW-P (192.168.112.193) - Camera 1	ac6c0e92-9acd-410d-b21f-f593c2b9d33f	ketanpipaliya	7563



For more information on integration with **Milestone** devices, refer to [“Milestone Integration”](#).

IP Camera

- **Snapshot URL:** If Capturing device is selected as IP Camera; then enter the API URL for taking the Snapshot through IP camera. You can use any camera for taking the snapshot/photo. The API for capturing snapshot will be available in the API document of camera.
- **User Name:** Enter the Username for accessing API for taking the Snapshot through IP Camera.
- **Password:** Enter the Password for accessing API for taking the Snapshot through IP Camera. It is the same username and password using which IP camera login is done. Eg: username admin and password admin





The allowed values for snapshot URL, User Name and Password are **A-Z, a-z, 0-9 !\"#\$%&'()*+,- ./ :;<=>?@[\\]^_`{|}~**

The screenshot displays the 'Device Configuration' window. On the left, a sidebar lists various configuration options: Profile, Enrollment, Advanced, Features, Video Surveillance (highlighted in blue), Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main area is divided into two tabs: 'Visual Tagging' and 'Satatya/IP Camera Integration'. The 'Satatya/IP Camera Integration' tab is active, showing a 'Capturing Device' dropdown set to 'IP Camera'. Below this, the 'Snapshot URL' field contains 'http://192.168.102.191/matrix-cgi/snapshot', with a note stating 'Note: Mention the protocol http or https in URL.' Under the 'API Login Credentials' section, the 'User Name' field is set to 'admin' and the 'Password' field is masked with six dots.

Satatya/IP Camera Integration

This functionality is available for configuration only when the Matrix HVR/NVR device type or IP Camera is selected as the **Capturing Device** (from *Visual Tagging*).

It enables the configured COSEC devices to directly send commands to the SATATYA HVR/NVR devices/ IP Camera as per the configuration on this page. The Satatya/IP Camera Integration page appears as shown below:



SATATYA Integration

Device Configuration

Visual Tagging

Satatya/IP Camera Integration

Integration Type: Network

Active: ☒

IP Address: 192 . 168 . 104 . 37

Port Number: 8000

Name: VegaNVR Integration

Active: ☒

Schedule: 13:00 - 20:00

Days: ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat ☐ Holiday

Event: Invalid User

Mode: Entry

Action: Video Pop-Up

Duration Sec: 10

Camera: ☐ 1 ☒ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 22 ☐ 23 ☐ 24

Add Cancel

- **Integration type-** Select the integration type from the options of Wired and Network. In wired integration, door is physically connected with Satatya Device. In Network integration, connection can be by ethernet, wireless or broadband depending upon the COSEC device support.
- **Active-** Check the box to activate the connection.
- **IP Address-** Specify the IP address of HVR/NVR.
- **Port Number-** Specify the port number of HVR/NVR.

- **Name**-Specify a user friendly name for the integration function.
- **Active**- Check the Active box to enable the SATATYA integration functionality.
- **Schedule** - Specify a schedule for the function by specifying the start and the end time (*24 Hours format*) as well as checking the boxes against the applicable **days** of the week.
- **Event**- Select a COSEC event from the drop down list for which the resultant action is to be configured.
- **Mode**- Select the event mode from the options of Entry, Exit and Both from the drop down list wherever applicable.
- **Action**-Select the action for the Satatya device from the drop down list. The options available are:
 - Recording - Specify the duration in minutes.
 - Upload Image - This will be uploaded as per the ftp settings.
 - Video Pop-up - Specify the duration in seconds. The video pop up will be generated on the local client of Satatya device on the selected camera.
 - PTZ Preset - Specify the PTZ position number as defined on the SATATYA device.
 - Mail Image - Specify the email-ID.
- **Camera**- Select the relevant camera channels depending on the action selected.
- Click the **Add** button to finish the process of linking the event to the action.

Search						
Name	Event	Action	Start Time	End Time	Active	
VegaNVR Integration	Invalid User	Video Pop-Up	13:00	20:00	Yes	

The user may now configure another event-action linkage if required.

Example1: For action as Upload Image, the image of Camera 13 will be upload at path defined in Visual Tagging.

Event	Access Allowed
Mode	Both
Action	Upload Image
Camera *	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input checked="" type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	

IP Camera Integration

Device Configuration

29 ARGO-Device-2...
ARGO
4/S0000
Active

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Identification Server

Visual Tagging Satatya/IP Camera Integration

Schedule Name * User Allowed Schedule

Active ☒

Event User Allowed

Mode Both

Schedule Range * 09:00 19:00

Days * ☐ Sun ☒ Mon ☒ Tue ☒ Wed
☒ Thu ☒ Fri ☐ Sat ☐ Holiday

Add Cancel

- **Schedule Name**-Specify a user friendly name for the schedule of Device-IP Camera integration.
- **Active**- Check the Active box to activate the schedule for IP Camera.
- **Event**- Select a COSEC event from the drop down list for which the resultant action is to be configured. The Events will appear in the list based on the availability of the license.



At max. 20 Events or schedules are allowed for configuration for a single device.

- **Mode**- Select the event mode from the options of Entry, Exit and Both from the drop down list.
- **Schedule Range**- Specify a schedule for the function by specifying the start and the end time (24 Hours format) as well as checking the boxes against the applicable days of the week.

Click **Add** button to add the configured schedule. The schedule will be listed in the grid. Then click **Save** button to save the schedule integration.

Visual Tagging Satatya/IP Camera Integration

Schedule Name *

Active ☐

Event User Allowed

Mode Both

Schedule Range * 00:00 23:59

Days * ☒ Sun ☒ Mon ☒ Tue ☒ Wed
☒ Thu ☒ Fri ☒ Sat ☒ Holiday

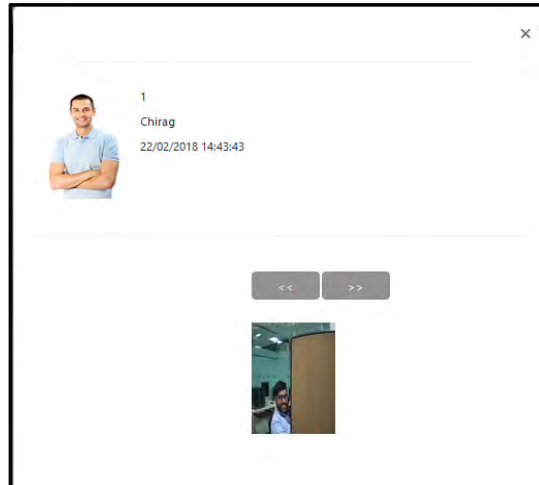
Add Cancel

Search

Name	Event	Mode	Start Time	End Time	
User Allowed Schedule	User Allowed	Both	09:00	19:00	

When user event is generated, then snapshot is taken by the configured camera. The events can be viewed in User Events (User module) page and Event view (Admin module) page.

The snapshot can be viewed by clicking on View Image button.




Special Functions

To configure *Special Functions* for COSEC doors, refer to [“Special Functions”](#).

Input/Output

The Input/Output (I/O) configuration of a system determines how the output or response of a system is influenced by the input applied on it. In case of the COSEC Access Control System, the I/O configuration should enable the system to monitor and trigger a specific response to any changes in door state or event occurrences at the door device. This change of door state or occurrence of events may be considered as an input while the response or action that is generated by the system on detection of this input, may be defined as the output.



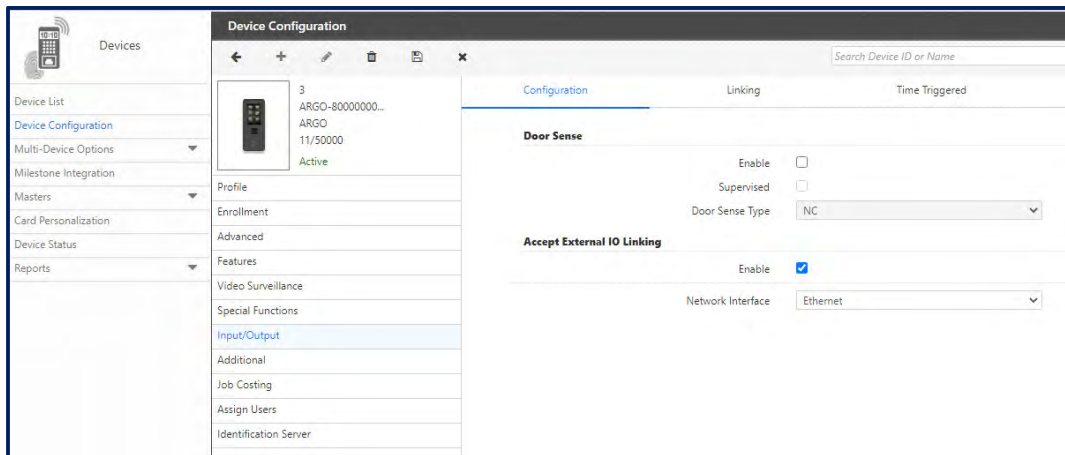
1. This functionality cannot be fully accessed in the Edit  mode for a selected device.
2. This functionality is available only with the Access Control add-on module license.

To access this, After selecting the device, Select **Device Configuration> Input Output**. The Input Output parameters can be set from the following sections:

- [“Configuration”](#)
- [“Linking”](#)
- [“Time Triggered”](#)

Configuration

The **Configuration** section for a ARGO Door appears as shown below.



The following parameters are available for configuration in both Direct door and Panel door:

- **Door Sense** - The system by default can sense two states of a door - *Normally Open (NO)* and *Normally Closed (NC)* depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a *Door Abnormal* alarm.

Select the **Enable** checkbox to enable the system for such two-state monitoring.

Select the **Supervised** checkbox to enable the door for four-state monitoring where the door is also monitored for *door fault* and *door disconnection*. Specify the **Sense Type** as **NC** or **NO** (Default: NC).

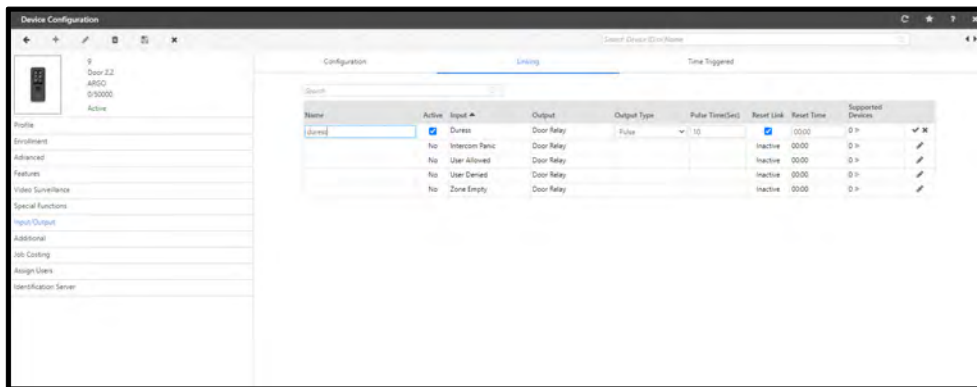
- **Accept External IO Linking** - Select the Enable checkbox to enable device-to-device IO Linking i.e. input from one Direct Door can trigger output in another Direct Door.
- **Network Interface**- Select the interface option for IO linking with external devices. The options are
 - Ethernet
 - Wireless
 - Mobile Broadband

Linking



This section is not available for Panel doors.

The **Linking** section appears as shown below.



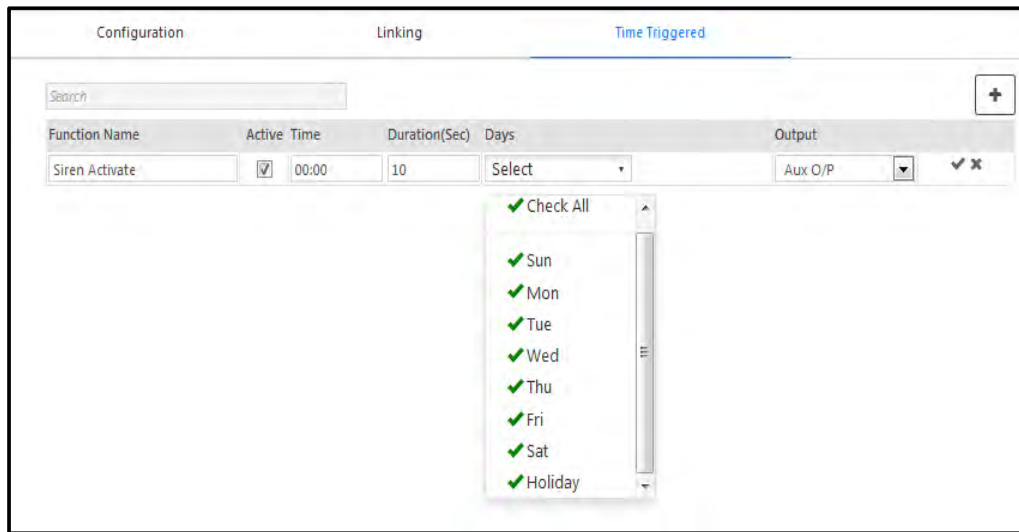
The COSEC application supports the Input/Output Linking feature to activate an output port based on a trigger received from an input port on the same Direct Door. This option enables the administrator to define how an event or events (input port) will trigger an output on the selected door.

Select a Input-Output linking row or click edit button.

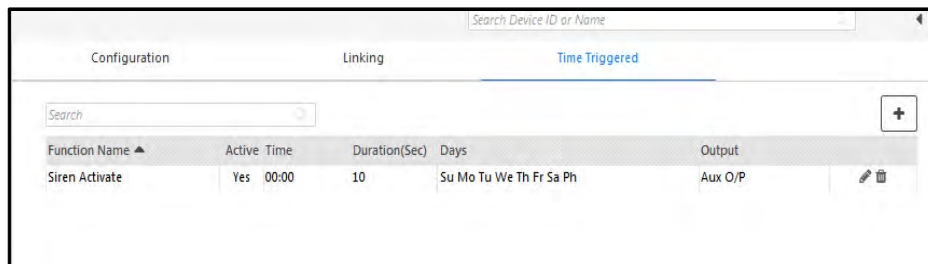
- **Name** - Specify a name for the new I/O linking program to be defined.
- **Output Type** - Specify the appropriate type of output from the following four options available in the drop down list:
 - **Pulse**: With this type of output, the user needs to define the Pulse time in seconds.
 - **Interlock**: With this option, the output follows the input. The relay output is triggered as long as the input is activated after which it returns to normal state.
 - **Latch**: With this option, it is denoted that the relay output will be in an energized condition for infinite period and needs to be reset manually.
 - **Toggle**: With this option, the output group toggles its state whenever an input group is activated.
- **Pulse Duration (sec)** - For a *Pulse* output type, specify the pulse duration in seconds.
- **Active** - Select this checkbox to activate this linking program.
- **Supported Devices** - All devices supported for external IO Linking will appear in this picklist for selection. Upto 255 external devices can be added by the administrator.
- Click the **OK** button and **Save** the configuration.

Time Triggered

On the **Input Output** page, select the **Time Triggered** section as shown.



This functionality enables the user to control the activity of an Output without manual intervention. The time triggered functions are used for activating events like door unlock and siren activation that are set as per the start time and for the configured time duration. This functionality is designed to energize outputs for predefined periods at the configured time. The COSEC access control system supports up to 20 Time Triggered functions on a Direct Door.



Additional

This section lists some additional configurations that can be enabled for door controllers.

To access these configurations, Go to **Device Configuration > Additional > Daylight Saving**



This section is available only for Direct Doors.

Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. COSEC doors can be configured to be compatible with this procedure keeping the RTC of the system updated with such changes.

The **Daylight Saving** configuration can be done in 2 ways i.e. Day-Month wise or Date-Month wise.

- Select the **DST Type** as Day-Month wise or Date-Month wise. The **Disable** option when selected, disables the application of DST on the system time.

- On selection of the **Day-Month wise** option, the DST is set by the day of the month on which clock needs to be forwarded and reverted back to normal. Set the month, week number, day of the week, and time for both the **Forward Clock** and **Backward Clock** as shown.

The screenshot shows the 'Device Configuration' window for a device named '29 ARGO-Device-2...'. The 'Daylight Saving' tab is active. The 'DST Type' is set to 'Day-Month wise'. The 'Time Period' is '08:00'. Under 'Forward Clock', the settings are: Month 'January', Week No. '1st', Day of Week 'Sunday', and Time '09:00'. Under 'Backward Clock', the settings are: Month 'January', Week No. '1st', Day of Week 'Sunday', and Time '10:00'. A 'Save' button is at the bottom right.

- On selection of the **Date-Month wise** option, the DST is set by date of the month on which clock needs to be forwarded and reverted back to normal. Define the **Time Period** for the date-month wise DST settings in 24-hours format, and specify the day of the week, date and time for the **Forward Clock** and the **Backward Clock** as shown.

This DST Setting implies that on 1st sunday of November at 09:00 hours, the clock will be forwarded by 08:00 hours. And on 1st sunday of January at 10:00 hours, the clock will be reversed or backwarded by 08:00 hours.

The screenshot shows the 'Device Configuration' window for the same device. The 'Daylight Saving' tab is active. The 'DST Type' is set to 'Date-Month wise'. The 'Time Period' is '08:00'. Under 'Forward Clock', the settings are: Month 'January', Date '1', and Time '09:00'. Under 'Backward Clock', the settings are: Month 'January', Date '1', and Time '10:00'. A 'Save' button is at the bottom right.

- Click the **Save** button.

Job Costing



Job Costing is applicable for Direct Door only.

When user punches on any device, there will be an option to select the Job Code on which the user is working. Job Costing enables the admin to show or hide Job Code selection on device. It also enables the admin to assign default jobs on device.

The screenshot shows the 'Device Configuration' window for a device named '29 ARGO-Device-2...'. The 'Settings' tab is active. Under 'Show Job Menu', 'Show List' is selected. The 'Assign Jobs' section has a 'Retain Job Selection' checkbox. Below it, there are input fields for 'Job Group' (set to 2) and 'Job' (with 'ID' and 'Name' picklists). A table lists assigned jobs:

Job Code	Name	Assignment Start	Assignment End
INV	Inventory	22/05/2017	30/06/2017
LAB	Labelling	22/05/2017	07/06/2017

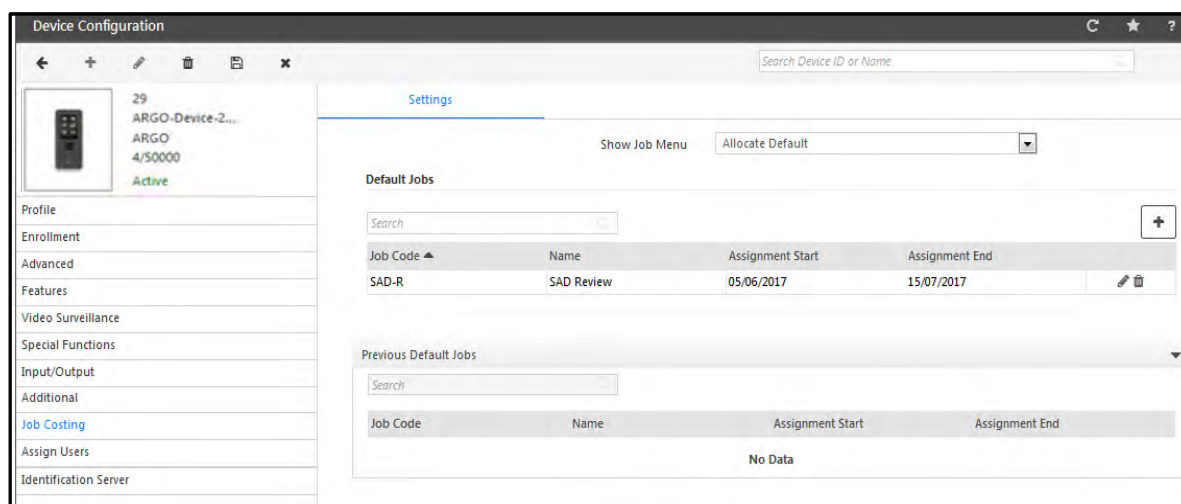
Show Job Menu: Select the option as **Show List** or **Allocate Default**.

When **Show List** is selected; then multiple jobs can be assigned to the device. The user can select the relevant job code while punching on the device. His job hours will be recorded for that job code.

- **Retain Job Selection:** Select this checkbox to retain the job code selected by a user which would be applicable for all the subsequent users until another job selection is done on device.
- **Assign Jobs:** Select the Job group or individual job from the picklist. Then click on Save button. The jobs will be listed to the grid.

When **Allocate Default** is selected; then default jobs for the device can be selected.

- **Default Jobs:** Click Add button to add the default job on the door. Then click on the Job picklist button and select the job to be assigned to the device. The Job costing user can directly punch on this door for starting the default job.



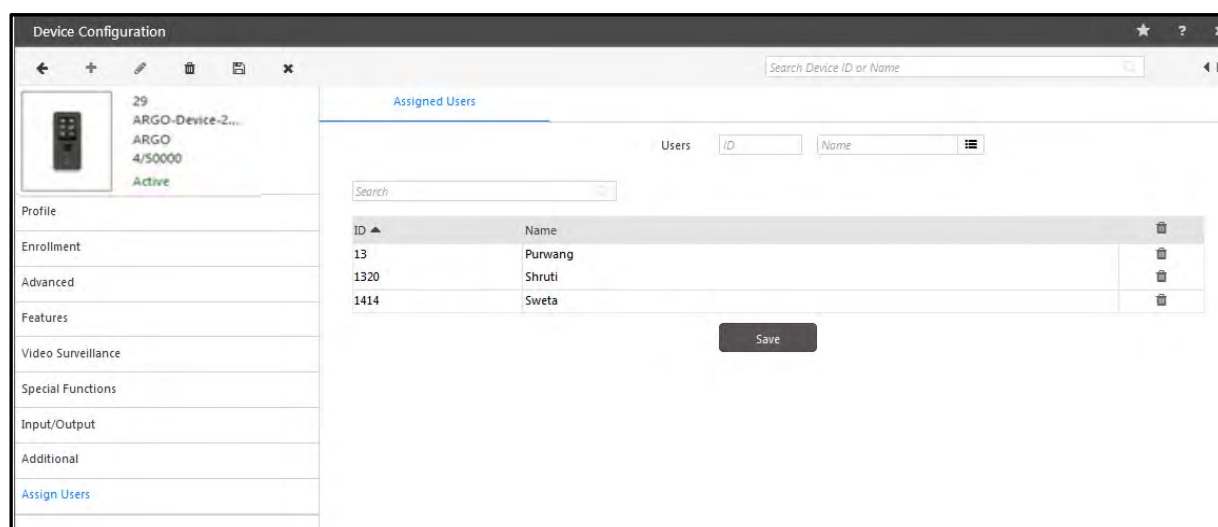
Finally click on **Save** button to save the configuration.

When the assignment date of the default job gets elapsed, then the respective job will be listed in **Previous Default Jobs** section.

Assign Users

To the configured device, you can select and assign the users.

Click the picklist button and select the users.

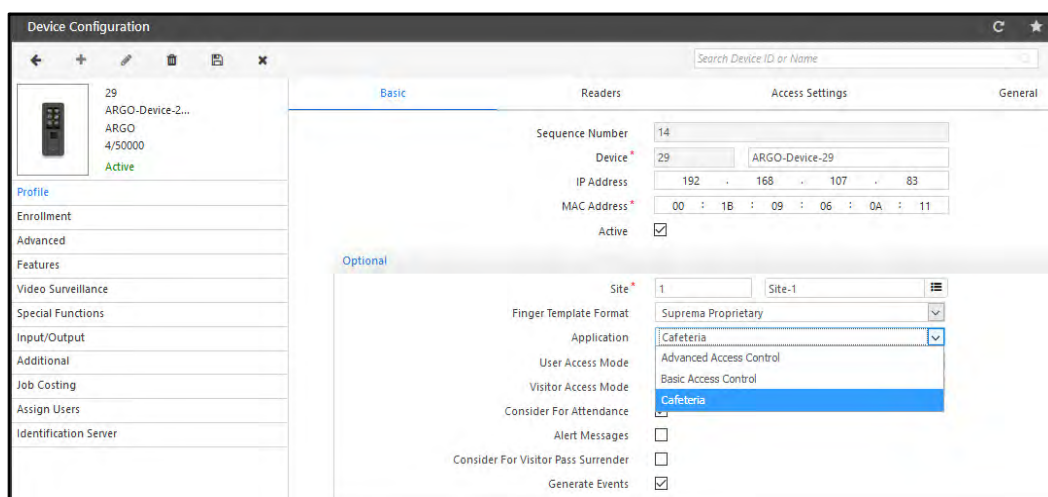


- Click the **Save** button to assign all the added users to the selected door.

Cafeteria

The COSEC system enables the user to configure devices which will be used by the Cafeteria management module.

To configure a door for Cafeteria application, select **Cafeteria** option in Device Profile> Basic> Application as shown below.

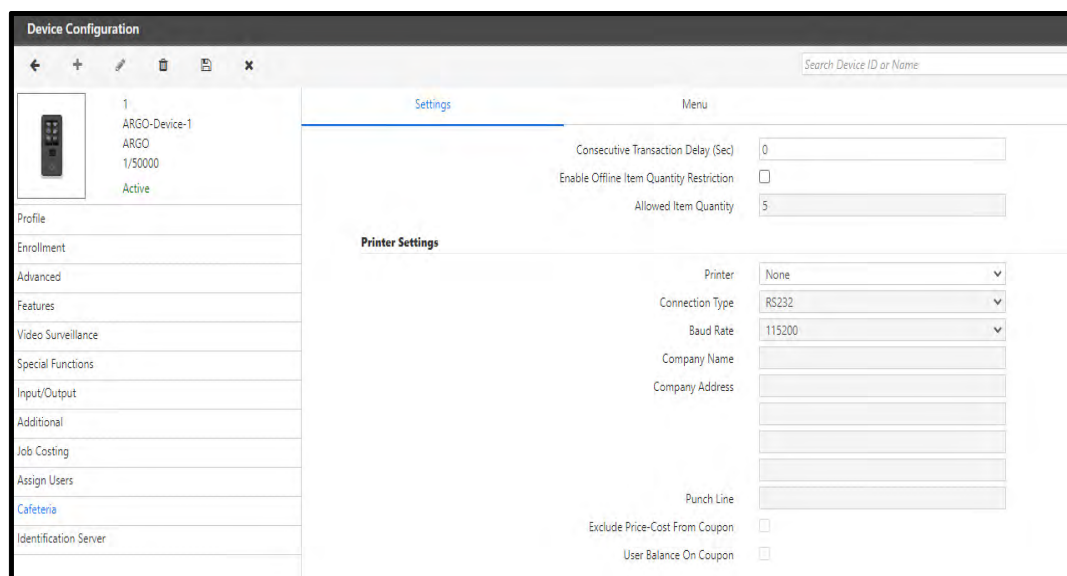


The Cafeteria tab will appear in Device Configuration page.

Select **Device Configuration> Cafeteria> Settings**

Settings

The Cafeteria configuration for ARGO Door is shown as below.



- **Consecutive Transaction Delay (Sec):** Enter the time interval after which you wish to allow the second transaction from the same user.
- **Enable Offline Item Quantity Restriction:** Select the checkbox if you desire restricting transaction on exceeding the item quantity while the device is in offline mode.
- **Allowed Item Quantity:** Specify the number of item quantity to be allowed when the device is in offline mode. This will be applicable for each item present in the Menu.

For example, if the Menu has two items Tea and Poha and you have configured the **Allowed Item Quantity** as 2, then when the device is offline, the user/worker will be allowed to consume Tea twice as well as Poha twice.

Printer Settings

- **Printer:** Select the printer from the dropdown list based on the site requirements.
- **Connection Type:** Select the printer connection type from the drop down list. The options available are:
 - RS232 (serial)
 - USB
- **Baud Rate:** In the event of a serial printer, select the appropriate baud rate from the drop down list.
- Specify the **Company Name**, **Company Address** and the **Punch Line** as per the site requirements. These details will be printed on the receipt dispensed from the selected printer.
- Select the **Exclude Price-Cost From Coupon** check box if you want to exclude the price from the coupon.
- Select the **User Balance On Coupon** check box, if you want Current Balance/ Current Month Usage and Weekly Remaining Limit to be printed on the Cafeteria receipt.

For pre-paid account users, Current Balance and Weekly Remaining Limit will be printed.

For post-paid account users, Current Month Usage and Weekly Remaining Limit will be printed.

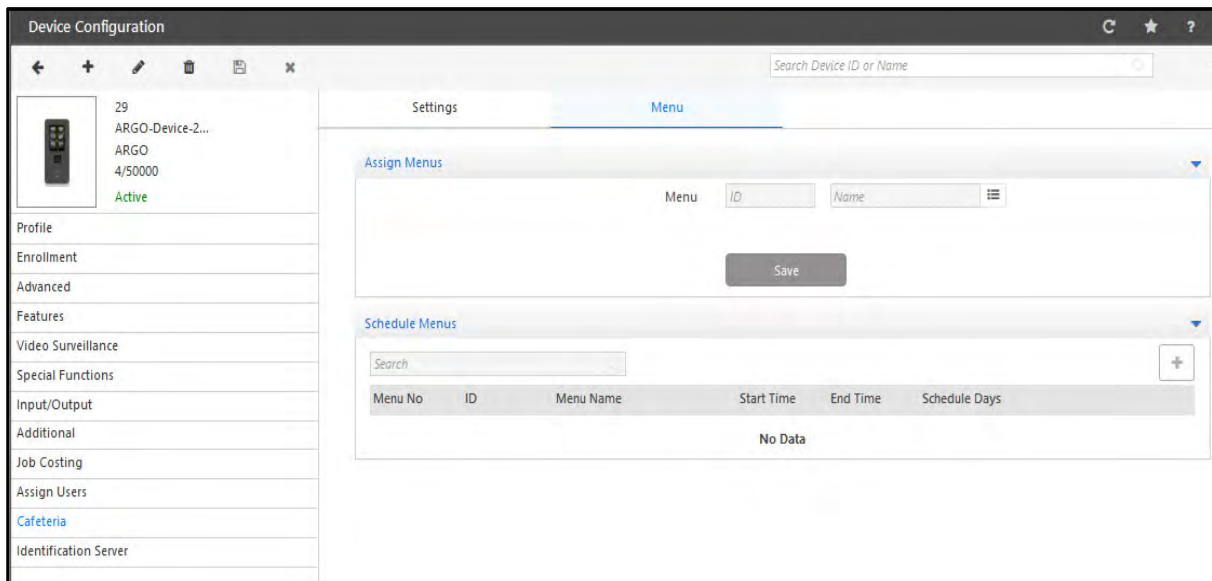
For details refer to "[Cafeteria Usage Policy](#)".

Menu

COSEC allows the administrator to assign one or more cafeteria menus (Menu 1, Menu 2, Menu 3... upto 99.) to a device. These can be configured by selecting pre-defined menus from the Menu picklist.

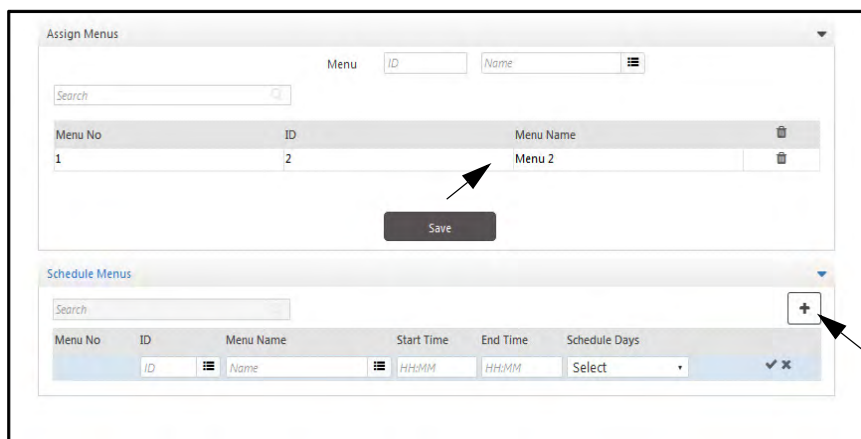


The Menu is created from Cafeteria module.



The Menu can also be scheduled from Cafeteria module which will be displayed in “Schedule Menus” in above screen.

If you have to assign menu and schedule it on the door from Device Configuration page, then select the Menu from the picklist. The Menu will be shown in the grid as shown below.



Now to schedule the menu click **Add** button as shown above.

Then select the menu to be scheduled from the **ID** picklist. Specify the **Start** and **End time** for which the Menu will be active and is available to users on the selected door. Select the **days** for which this menu will be available i.e. scheduled on the door.

Then click **OK** and **Save** the Menu schedule on the door.

Menu No	ID	Menu Name	Start Time	End Time	Schedule Days
2	2	Menu 2	09:00	11:00	Select

- ✓ Check All
- Sunday
- ✓ Monday
- ✓ Tuesday
- ✓ Wednesday
- ✓ Thursday
- ✓ Friday
- Saturday



Two Menus cannot be scheduled for same timing.

Identification Server

This tab enables the selected device to be assigned to a pre-defined Identification Server.

Device has a limited memory capacity for storage of templates so we need Identification Server which will store the more number of templates and respond to device when asked for identification.

For more information on Identification Servers, See *Admin> System Configuration> Identification Server Configuration*.

To access these configurations, select the **Identification Server** tab.

Settings

Face Recognition

Enable FR
☒

Face Capturing
Tap & Go

Enable Time Out
☐

Free Scan Time Out (Sec)
30

IP Camera MUEG URL *
http://192.168.1.126/matrix-cgi/mjpeg?profile-no=4

Note: Mention the protocol in URL.

User Name *
Username

Password *

FR Mode
Local

Server Address *
192.168.50.2

Server Port *
12000

Identification Time-Out Duration (Sec)
4

Group FR
☐

Exceptional Face Enrollment
☐

Face Enrollment

Conflict Check
☒

Conflict Matching Threshold (Face) *
93
%

Adaptive Face Enrollment

Adaptive Face Enrollment
☐

Threshold Deviation (Face)
02.0
%

Multi-User Matching Score Deviation (Face)
02.0
%

Confirm Before Adaptive Face Enrollment
☐

Face Anti-Spoofing

Face Anti-Spoofing
☒

Camera Mount
Wall Mount

Face Anti-Spoofing Mode
Advance

Face Anti-Spoofing Threshold *
62.00
%

Other Biometric Credentials

Enable Identification On Server
☐

Identification Server
ID
Name

Configure Alternate Server Address
☐

Server Address

Server Port
11005

Enable Finger Smart Identification
☐

Identification Time-Out Duration (Sec)
4

Auto Send Enrolled Templates
☒

Default Biometric Group No.
0

Face Recognition

- **Enable FR:** Select the checkbox to enable the Face Recognition feature on the device.



Make sure **“Enable FR”** flag is checked and **“Basic Access Control”** application is selected in Devices > Device Configuration > Profile > Basic > Optional > Application in order to edit the parameters in Identification Server Settings.

- **Face Capturing:** Select the desired Face Capturing option — Tap & Go or Free Scan.

- **Tap and Go:** If you select this option, user needs to tap on the device screen once. The MJPEG, that is motion recording screen appears. The device will capture and then identify the users face. If during working hours device is idle, then user needs to tap device to scan the face and gain access.
- **Free Scan:** If you select this option, device will display the MJPEG, that is motion recording screen till the expiry of the Free Scan Time Out timer.
 - **Enable Time Out:** Select this checkbox to enable the time out.
 - **Free Scan Time Out (Sec):** Enter the free scan time out duration. The valid range is 1 to 999 sec.

In Free Scan method, multiple users can mark their attendance easily during peak entry hours.

For example, if the Free Scan Time Out is set as 30sec and if the user is identified in 10S then the system reloads the Free Scan Time Out timer again. Hence, device remains in the scanning mode.

- **IP Camera MJPEG URL:** Enter the URL for accessing the IP camera to receive the motion stream. For example: <http://192.168.104.48:80/matrix-cgi/mjpeg?profile-no=3>.

If the device is auto-added then the default value will be <http://192.168.1.126/matrix-cgi/mjpeg?profile-no=4>.

- **User Name:** Enter the user name for accessing the IP camera. For eg: admin
- **Password:** Enter the password for accessing the camera. For eg: admin123

This will fetch the motion stream from camera to device screen. Then the users can show their face on camera. The face will be captured and after identification, the user will be allowed to access the door and punch will be marked.

- **FR Mode:** Select the FR mode as **Local** or **Server Assisted**.
 - **Local:** In this Local mode face templates will be stored in FR hardware module which can store 1 Lakh face templates. The captured face template will be verified with the templates already stored in FR module.
 - **Server Assisted:** In Server Assisted mode, the face templates will be stored directly in the server. You must first configure the Identification Server from where the face templates will be identified.

When FR Mode is selected as **Local** below mentioned parameters are to be configured:

Face Recognition	
Enable FR	<input checked="" type="checkbox"/>
Face Capturing	Tap & Go
Enable Time Out	<input type="checkbox"/>
Free Scan Time Out (Sec)	30
IP Camera MJPEG URL *	http://192.168.1.126/matrix-cgi/mjpeg?profile-no=4 Note: Mention the protocol in URL.
User Name *	
Password *	*****
FR Mode	Local
Server Address *	192.168.50.2
Server Port *	12000
Identification Time-Out Duration (Sec)	4
Group FR	<input type="checkbox"/>
Exceptional Face Enrollment	<input type="checkbox"/>

- **Server Address/Port:** Enter the IP Address and Port of the FR Server.
- **Identification Time-Out Duration (Sec):** Enter the identification time-out in seconds, after which the face template identification process will be timed out.

Example: If **Identification Time-Out Duration (Sec)** is 5 seconds, then the identification server will try to identify the face template until 5 seconds and if not found then it will show time-out to the user.

When FR Mode is selected as **Server Assisted**, configure the below fields:

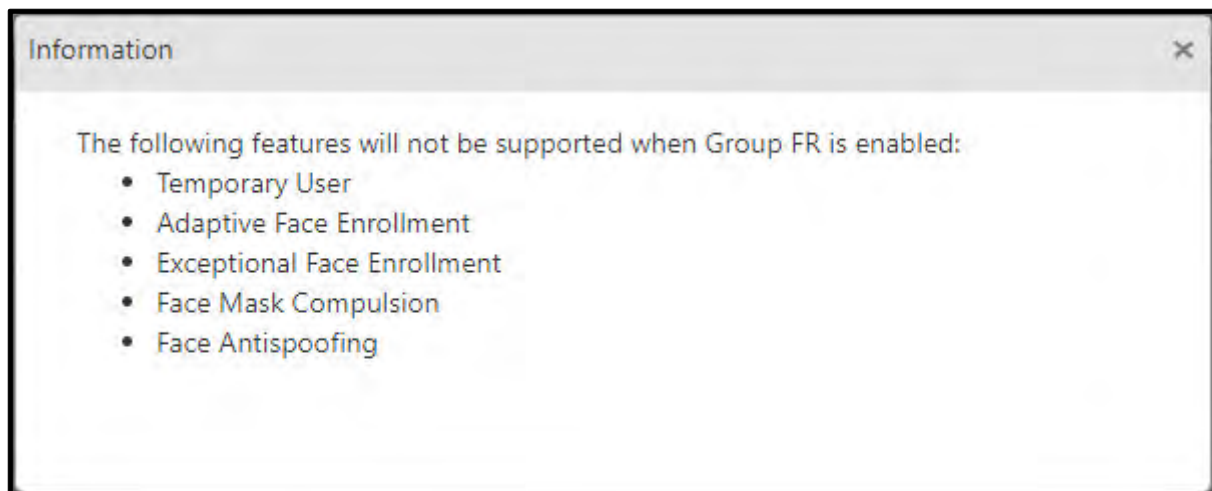
User can either assign a separate or a common Identification Server which is shared by other biometric credentials.

- **Identification Server:** Select the Identification Server from the picklist button to which the device is to be assigned to save the records.
- **Configure Alternate Server Address:** Select this checkbox to configure external IP address of FR Identification Server.
- **Server Address:** By default, this will display the configured Identification Server for FR. This field allows user to enter the Alternate IP Address for FR if **Configure Alternate Server Address** is enabled.
- **Server Port:** Enter the TCP port number. The default port number is 11005.
- **Identification Time-Out Duration (Sec):** Enter the duration in seconds after which the face template identification will get time out.

Example: If 5 seconds is specified, then the identification server will try to identify the template till 5 seconds and if not found then it will show time-out to the user.

- **Group FR:** Select this checkbox to enable face recognition feature for multiple users and mark their attendance at the same time via this door.

Once you enable Group FR, a pop-up will be displayed as shown below:



The features listed in the pop-up will not be functional.

- **Exceptional Face Enrollment:** Select this checkbox to enroll exceptional faces of users via this door



For Group FR (“[Mark Group Attendance](#)”) and Exceptional Face Enrollment feature to work, ensure that the desired Identification Service is selected in COSEC Admin > License and Service. For more details refer Admin Management Portal User Manual.



*If you have enabled the **Exceptional Face Enrollment** feature then make sure that you schedule a task of **Delete Exceptional Face** in Admin > System Utilities> Task Scheduler to avoid storage of excess data in the database.*

Face Enrollment



*If the **FR Mode** is **Server-Assisted** and you wish to enroll faces from the device, make sure **Enable Face Recognition** is selected in Users > User Configuration > Face Recognition and/or Visitor Management > Visitor Profile > Face Recognition and/or Contract Worker Management > Worker Profile > Face Recognition.*

- **Conflict Check:** Select the checkbox for the system to check the conflict between the new face of a user and the already (existing) enrolled faces of all the users (available in the database) during the face enrollment process.
- **Conflict Matching Threshold:** Enter the desired Conflict Matching Threshold value in percentage.

The system will consider this value while comparing the face with the face templates already present in the database.

If a conflict is found, that is, if the system detects a face template in the database similar to the new face, then a conflict error will be displayed.

Make sure a higher value is set for this parameter, as it will result in less equivalent matches with the face templates available in the database.



*Make sure the **Conflict Matching Threshold** is set lower than **Matching Threshold** in Admin module > System Configuration > Identification Server Configuration.*

Example: Face Enrollment of Suresh

- **Conflict Check** checkbox is selected.
- **Conflict Matching Threshold** is set as 93%.

Now during the face enrollment of Suresh, the system will check in its database if his face matches with faces of other users available in the database.

- **Case 1:** If Suresh's face matches 92% with Ram, then the system will allow to enroll Suresh's face.
- **Case 2:** If Suresh's face matches 94% with Shyam, then the system will display the conflict error while enrolling Suresh's face.

Adaptive Face Enrollment

- **Adaptive Face Enrollment:** Enable adaptive face enrollment for identification server.
 - Adaptive face enrollment provides automatic real time face enrollment whenever change is experienced in facial features.
 - Enabling adaptive enrollment process parameter, an additional slot will be provided internally to store 10 more face templates of a user.
 - IDS will learn from face recognized, adapt and would take decision of storing new template of a user database.

By enabling the adaptive face enrollment parameter will allow to specify following configurations:

- **Threshold Deviation (Face):** Enter the value of deviation from matching threshold in percentage. Based on the value entered for deviation, template for Adaptive Face Enrollment will be decided.

Example: If deviation entered is 3% and matching threshold is 98% then it will classify template which has matching score between 98 - 95 and one lower than this will be classified below margin.

- **Multi-user Matching Score Deviation (Face):** Enter the value of deviation from matching score between 2 different users while Adaptive Face Enrollment.
 - Difference between matching scores of templates will be done, when we have templates of two or more users falling under above specified deviation.

E.g. Assume the following parameters:

- *Threshold value = 98%*
- *Threshold Deviation= 3%*

So, Result will display all matching templates having matching score between range 98 to 95

- *Multi-user Matching score deviation = 0.5%*

Suppose, 5 best templates of 2 users fall between 98 -95% range

User	Matching Score
User 1	97.8
User 1	97.6
User 1	97.4

User 2	97.25
User 2	97

As we have obtained templates of 2 users in which user 1 is having template of highest matching score, so will make a difference between lowest score template of user 1 and highest matching score template of user 2.

$97.4 - 97.25 = 0.15$; this is less than 0.5

As difference is less than 0.5, user 1's template having matching score 97.8 for adaptive enrollment will not be used.

- Threshold Deviation and Multi-user Matching score deviation will act as two filters to fetch appropriate template for adaptive enrollment.
- Value can be added in decimal.



We recommend to set the multi-user matching score deviation higher always e.g.2.0 to reduce the probability of enrolling a particular user's face template in some different user's enrolled faces.

- **Confirm before Adaptive Face Enrollment:** Select this checkbox if face enrolled using Adaptive face enrollment requires confirmation from user.



Faces enrolled under Adaptive enrollment process will be synced automatically, but when IDS is restarted due to any reason, the adaptive faces which are not synced will be removed by default.

Face Anti-Spoofing

- **Face Anti-Spoofing:** To use this feature, make sure **Enable FR** checkbox is selected in **Devices> Device Configuration> Identification Server> Face Recognition> Enable FR**.

Then, select the **Face Anti-Spoofing** checkbox to enable this feature and configure the following parameters:

- **Camera Mount:** Select the desired Camera Mounting option - **Wall Mount** or **Ceiling Mount**.

There is an impact of Camera Mounting in face liveness detection.

By default, it is "Wall Mount".



For Wall Mount, make sure the distance between camera and user is less than 3 feet for proper detection of face.

- **Face Anti-Spoofing Mode:** Liveness Detection helps to limit the fierce risk of spoofing attacks by using several anti-spoofing approaches. Along with the configurations to be done for Face Anti-Spoofing you also need to take care of the recommended settings for liveness verification and for face recognition as well as the Camera Settings, refer ["Recommendations for Liveness Verification"](#), ["Recommendations for Face Recognition"](#) and ["Recommended Camera Settings for Liveness Verification"](#).

Select the Face Anti-Spoofing Mode for liveness detection from the following:

1. **Basic:** This mode detects face as well as photos from the mobile phones.
Select this option when the distance between Camera and Face is more than 3 feet

2. **Moderate:** This mode analyzes the texture of face.
Select this option when the distance between Camera and Face is less than 2 feet
3. **Advance:** This mode combines the features of **Basic Mode** and **Moderate Mode** of Face Anti-Spoofing.
Select this option when the distance between Camera and Face is more than 1 feet and less than 2 feet.
By default, Face Anti-Spoofing Mode will be **Advance**.



Only Basic option of Face Anti- Spoofing Mode will be applicable when the Camera Mount option is Ceiling Mount.

- **Face Anti-Spoofing Threshold:** Enter the Face Anti-Spoofing threshold value in percentage within the range from 1.00 to 99.99 to identify user's face liveness for considering him/her as genuine person. This Threshold value will vary as per **Face Anti-Spoofing Mode** selected by you.

Other Biometric Credentials

- **Enable Identification On Server:** Select the checkbox to enable the identification of palm/finger templates on this device.
- **Identification Server:** Select an Identification Server using the picklist button to which the device is to be assigned. The configuration of server is done from **Admin module > System Configuration > Identification Server Configuration** and the Identification Service must be started from the service tray. The IP Address of this server is displayed in **Server Address**.
- **Configure Alternate Server Address:** Select this checkbox to configure external IP address of Identification Server.
 - **Server Address:** By default it displays the IP Address of the selected Identification Server.
Enter the external network IP address which will be used for accessing identification server.
- **Server Port:** Enter the TCP port number. The default port number is 11005.
- **Enable Finger Smart Identification:** For all other supported doors, select the checkbox to enable fingerprint templates identification through Identification Server.
- **Identification Time-Out Duration (Sec):** Enter the duration in seconds after which the fingerprint template identification will get time out.
Example: If 5 seconds is specified, then the identification server will try to identify the template till 5 seconds and if not found then it will show time-out to the user.
- **Auto Send Enrolled Templates:** Select the checkbox to enable any enrolled templates to be saved both on the COSEC database as well as saved locally on the configured Identification Server. This enables prompt identification of user on enrollment.
- **Default Biometric Group No.:** Enter the default biometric group number to be assigned to the device. It is a number allotted to a device to be assigned to the Identification Server. This enables the Identification Server to match the template against only those devices that belong to the corresponding biometric group. This reduces the false detection as well time to search template.

Panel200

Panel200 functions in two modes — Standalone or Server.

For details of Panel200 as a Standalone Server, please refer to the **COSEC Panel200 System Manual**.

When Panel200 is set to function in the Server mode, then the Panel200 manages multiple controllers (Panel Doors) and acts as a bridge between the controllers and the central COSEC server. It is responsible for synchronizing all door controllers and implementing advanced access control features.



The Device Configuration option in COSEC enables the system administrator to add Panel200 in the COSEC network by setting the configurations through the COSEC application.

It is necessary to configure a Panel200 before starting the configuration of its slave controllers (Panel Doors).

You can connect the following devices as Panel Doors — Door V1, Door V2, Door V3, Door V4, Path Controller, Vega Controller, PVR Door, ARC DC 100, ARC IO 800, ARC DC 200, ARGO, Path V2, ARGO FACE.

The Panel200 configuration are explained for the Panel set in the Server Mode.




The Configuration of Panel and Panel Lite is similar to Panel200. In this manual, the configuration of Panel200 is explained for reference.

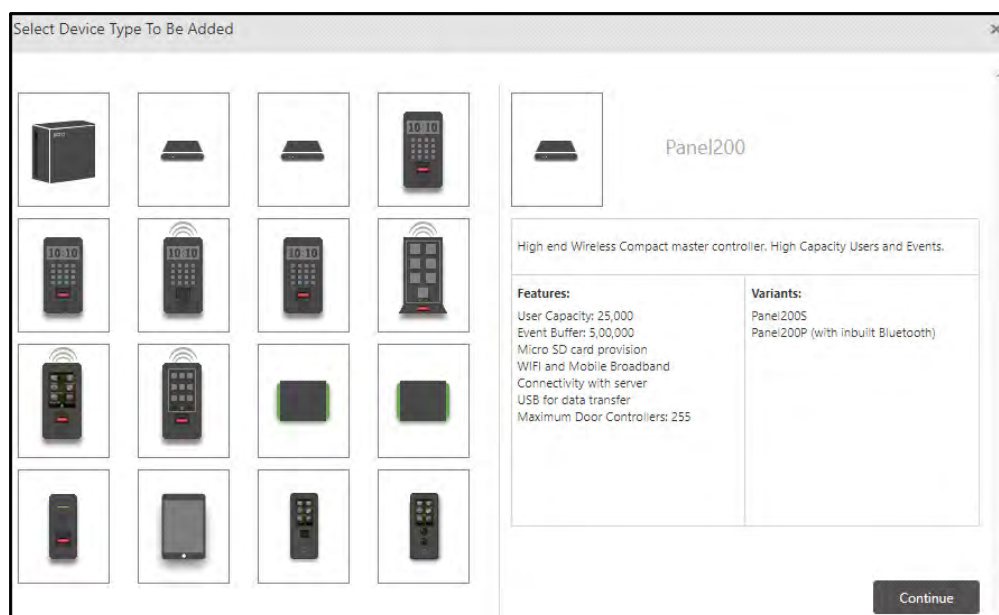
The basic difference between Panel, Panel lite and Panel200 is the support of user capacity and event buffer.

To configure a new Panel200 device, click **Devices Module > Device List** menu and the page appears as shown below.

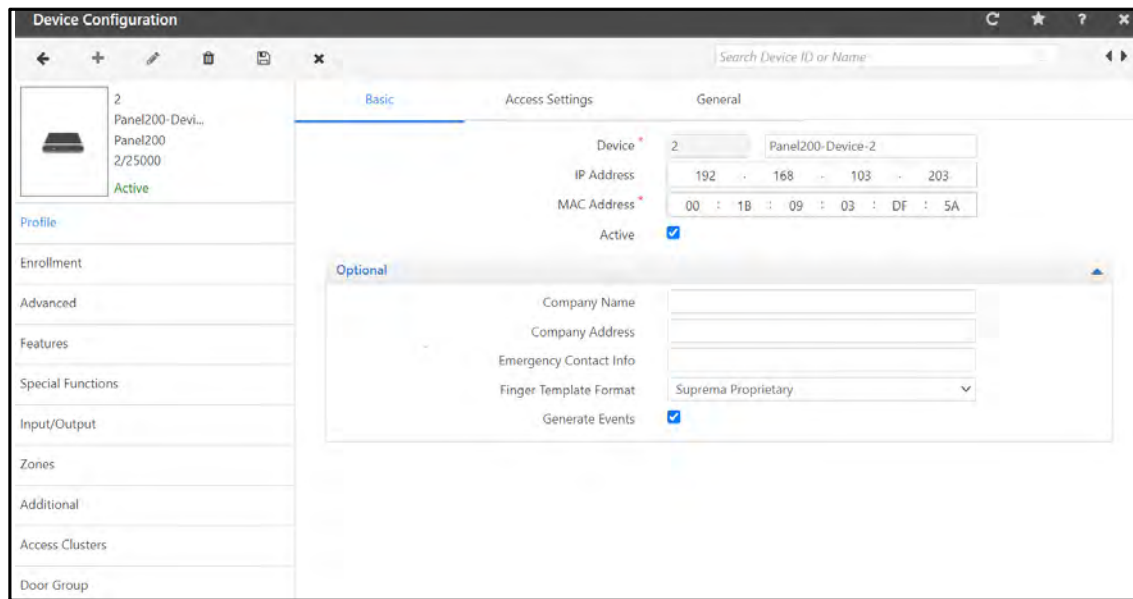
Device List				
<div> <div>Filter List</div> <div> <div>Device Type</div> <div>All</div> </div> <div> <div>Device Status</div> <div>All</div> </div> <div> <div>Site</div> <div>All</div> </div> <div>Search</div> </div>				
ID	Name	Device Type	Site	Status
21	PVR_Ground Floor	PVR Door	Site-1	Active
10	Vega as Direct Door	Vega Controller	Site-1	Active
10	PVR as Panel Door	Panel Lite V2 Door	Site-1	Active
9	Door V3 as Panel Door	Panel Lite V2 Door	Site-1	Active
9	Path as direct door	Path Controller	Site-1	Active
8	ARC as Direct Door	Arc Controller	Site-1	Active
8	ARC 2Door- Single Reader	Panel Lite V2 Door	Site-1	Inactive
7	Path as Panel door	Panel Lite V2 Door	Site-1	Active
6	Door FMX	Door FMX	Site-1	Active
6	ARC as Dual Door-Single Reader	Panel Lite V2 Door	Site-1	Active
5	Door V3	Door V3	Site-1	Active
5	ARC as Dual Door-Single Reader	Panel Lite V2 Door	Site-1	Active
4	ARC as Dual Door-Dual Reader	Panel Lite V2 Door	Site-1	Active
4	Wireless Door	Wireless Door	Site-1	Active

1 - 14 of 22 records

Click **New**  and select **Panel200** as device type and click **Continue**.



The **Device Configuration** page of Panel200 appears on your screen.



To add Devices automatically, click Admin Module> System Configuration> Global Policy> Device. Select the “Auto Add New Devices” check box to enable. Once the device is connected in network, it will come online in the COSEC Monitor.



Make sure the Monitor Service is running while adding the device to COSEC.

Once the device is configured, click the **Save** button to save the configuration.



The assignment of user on Panel Doors can be done from respective Panel Door Configuration > Assign Users.

To know more about configuring the Panel200, click on the links.

- [“Profile”](#)
- [“Enrollment”](#)
- [“Advanced”](#)
- [“Features”](#)
- [“Special Functions”](#)
- [“Input/Output”](#)
- [“Setting Up Access Zones”](#)
- [“Additional”](#)
- [“Access Clusters”](#)

- “Door Group”

Profile

This section enables the user to set up the basic profile for any new device. Setting up a profile involves defining basic parameters to set up the device.

Click each link to configure the Profile parameters:

- “Basic”
- “Access Settings”
- “General”

Basic

The **Profile > Basic** and the page appears as shown below:

The screenshot shows the 'Device Configuration' window with the 'Basic' tab selected. On the left, a list of devices includes '2 Panel200-Devi...', 'Panel200', and '2/25000', with the first one marked 'Active'. The main area contains fields for 'Device' (ID: 2, Name: Panel200-Device-2), 'IP Address' (192.168.103.203), and 'MAC Address' (00:1B:09:03:DF:5A). There is an 'Active' checkbox which is checked. Below this is an 'Optional' section with fields for 'Company Name', 'Company Address', 'Emergency Contact Info', 'Finger Template Format' (set to 'Suprema Proprietary'), and a 'Generate Events' checkbox which is also checked.

Configure the following options as required:

- **Device:** Enter a **Name** for the new Panel200 device. The **ID** will be assigned by the system.
- **IP Address and MAC Address:** Enter the MAC address of the Panel. The IP address will be displayed automatically once the device comes online in Monitor.



MAC address of Panel is required while manually adding the Panel to the COSEC Monitor. Take a note of the MAC address from the device when it is powered on.

Make sure the Panel200 is set in the Server Mode. To do so,

- Enter the IP Address of the Panel200 in the browser.
 - The Panel200 Web page appears.
 - Click Configuration > Basic Profile > Panel Mode
 - Select Server Mode
- **Active:** If the device is active on the network, select this check box to enable this option.



To add the Device automatically, click Admin Module> System Configuration> Global Policy> Device. Select the **Auto Add New Devices** check box to enable.

The device will be added automatically but make sure you enable the **Active** check box in order to connect the device to the network. Once the device is connected to the network, it will come online in the COSEC Monitor.

Optional

Click the **Optional** collapsible panel. It provides optional configurations as shown below:

The screenshot shows a web interface with a header labeled 'Optional'. Below the header are five configuration items: 'Company Name' with a text input field, 'Company Address' with a text input field, 'Emergency Contact Info' with a text input field, 'Finger Template Format' with a dropdown menu showing 'Suprema Proprietary', and 'Generate Events' with a checked checkbox.

- Configure the **Company Name**, **Company Address** and **Emergency Contact Info**.
- **Finger Template Format:** Select the Finger Template Format as **Suprema Proprietary** or **Suprema ISO**.



If you select either of the formats, then all the Existing Suprema Finger Templates will be deleted from the device and user will have to enroll with selected Fingerprint template format again.

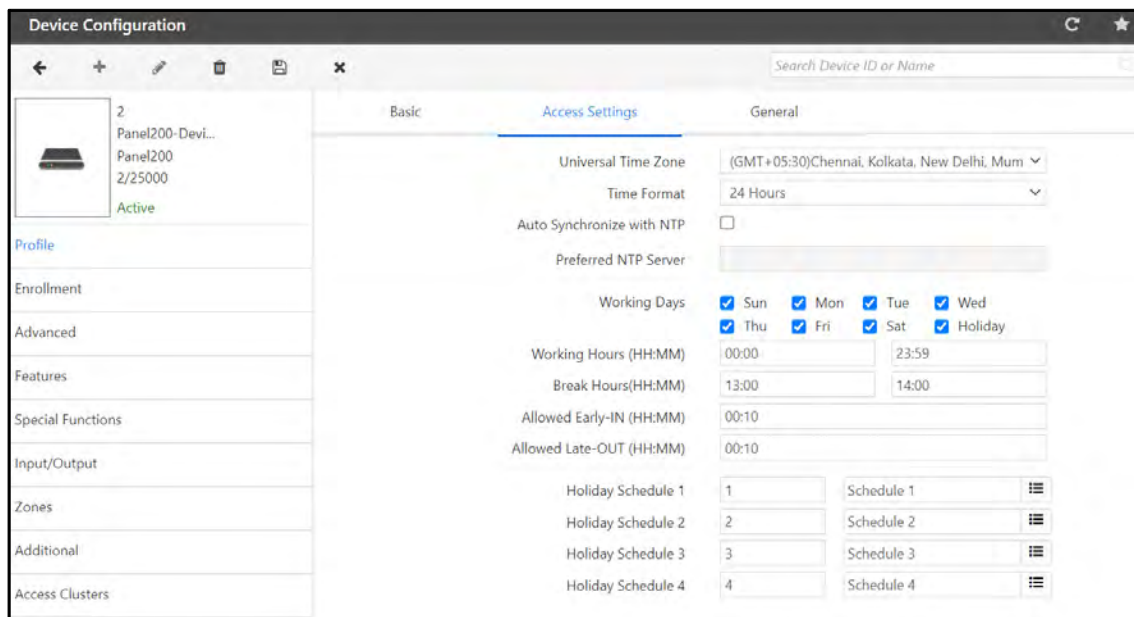
Suprema Proprietary is a local format of Suprema, while Suprema ISO is the standard format.

- **Generate Events:** By default, this option is enabled, that is the events generated in the Panel Doors will be displayed in the COSEC Monitor.

Clear the check box if you do not wish to view the Panel Door events in the COSEC Monitor.

Access Settings

Click **Profile > Access Settings** and the page appears as shown below:



- **Universal Time Zone:** Select the geographic time zone in which the Panel will operate.
- **Time Format:** Specifies the time format to be displayed on Panel Door LCD display connected with the Panel200. The formats available are:
 - 24 Hours
 - 12 Hours

Select the relevant option from the drop down list as per the site requirements.

- **Auto Synchronize with NTP:** If Date and time is to be automatically synchronized as per the Preferred NTP Server (predefined or user-defined NTP server address) selected by user, then you must enable Auto Synchronize With NTP check box.



Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from the Panel200 as well as the Panel Door device web-page, which will be reflected on the Panel Door device LCD display.

- When Auto Synchronization with NTP is disabled Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 - You can specify the Preferred NTP server of your choice. In this case Panel will first try to get Date and Time from that server address.

If it does not get Date and Time in three tries; Panel will check from pre-defined NTP servers.

If you have entered one of the three pre-defined NTP servers (ntp1.cs.wisc.edu, time.windows.com, time.nist.gov); then Panel will first check that server first.

- If it receives updated Date and Time then Updated Date and Time will be reflected on Panel webpage and Panel Door device display screen.

- You can keep the Preferred NTP server as blank. In this case Panel will check for Date and Time from the first NTP server.



If user has manually entered Date and Time from web-page of the Panel Door or Device Menu then those values of Date and Time will be reflected on device web-page and display screen.

In the case of the Manual option the administrator can manually update the time on the Door with that of the system time as and when required. This can be accomplished from the COSEC Monitor and control application.

- **Working Days:** While adding new devices, by default all the days including holidays for access are enabled. To change the default settings of working days, click on the relevant boxes which are not to be included in active working days.
- **Working Hours (HH:MM):** While adding new devices, the default working hours is set as 00:00 to 23:59. The user can change the default working hours in HH:MM format.
- **Allowed Early-IN (HH:MM):** Specifies the number of hours before official entry time, during which the user should be allowed entry.
- **Allowed Late-OUT (HH:MM):** Specifies the number of hours after official exit time, during which the user should be allowed to exit.
- **Holiday Schedule:** This section allows the administrator to assign up to four holiday schedules to the device by using the Holiday Schedule picklist

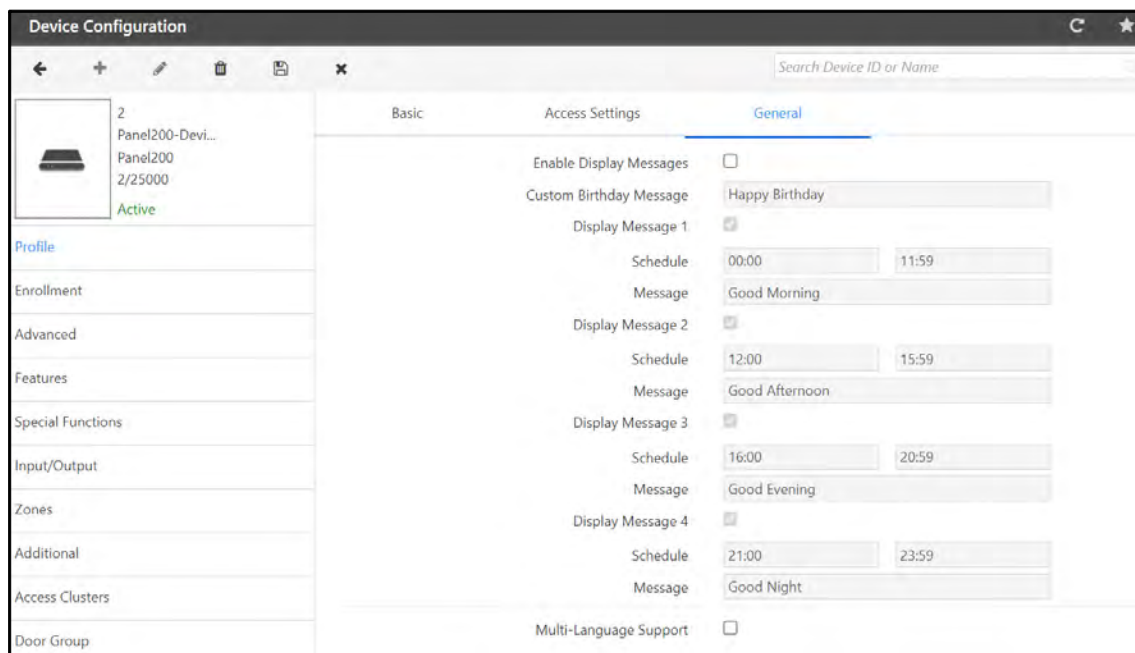


If the same holiday schedule is configured for a user and for the door controller on which the user is assigned, then the user's attendance marking on the device, on any of the scheduled holidays will always be marked as a holiday.

All these configurations will be applicable to the Panel Doors connected with the Panel.

General

Click **Profile > General** and the page appears as shown below.



- **Enable Display Messages:** Select this check box to enable the Custom Birthday Message and the Display Messages. Upto 4 Display Messages can be configured.
- **Custom Birthday Message:** Configure the birthday message which you wish to display on the Panel Door when the user punches on the door on his/her birth date.

The valid values are

A-Z

a-z

0-9

`~!@#\$%^&*()_+-{}|\\|:;?<>.,'\"

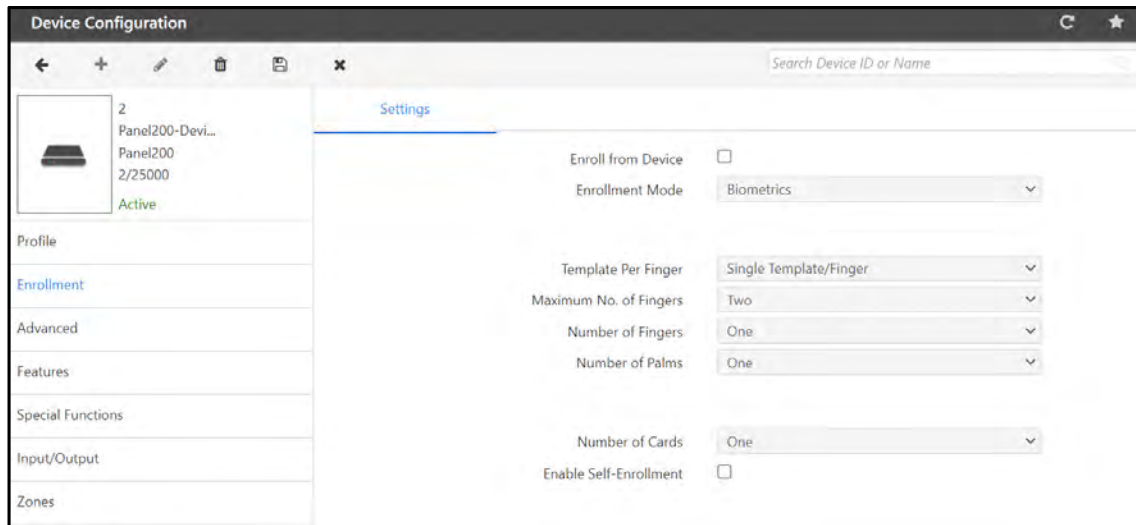
- **Display Message 1 to Display Message 4:** Select the respective check box of the desired Display Messages from 1 to 4, to enable.
 - **Schedule:** For each **Display Message**, define the time period for which the message is to be displayed.
 - **Message:** For each **Display Message**, configure the message you wish to display on the Panel Door as per the time set in the Schedule. Maximum 21 characters allowed.
- **Multi-Language Support:** Select this check box to enable multi-language support for the Panel Doors.



Wireless Door/PVR Door/Door V3 will support languages with English fonts (A-Z,a-z) only.

Enrollment

Click **Enrollment** and the page appears as shown below.



- **Enroll from Device:** Select this check box to enable the enrollment of user from the Panel Door.

When this check box is enabled, **Enroll User** under Special Function is enabled automatically.

Similarly, if Enroll User under Special Function and Enroll From Device check-box both are inactive in device configuration, then if you enable Enroll User under Special Function, Enroll From Device check box is enabled automatically.

- **Enrollment Mode:** Select the Credential — Biometrics, ReadOnlyCard, SmartCard, BiometricthenCard, Face and DuressFinger that you wish to enroll from the Panel Door. The selected option will work only if supported by the connected Panel Door.

Refer to [“Enroll Credentials”](#) or [“Enrolling Users”](#) to enroll User/Worker.

Refer [“Enrollment”](#) or [“Enroll Credentials”](#) to enroll Worker.

Refer [“Enroll Credentials”](#) to enroll a Visitor.



DuressFinger is only applicable for User and Worker.

- **Template Per Finger:** Displays the values as configured at the global level. This field is not editable.
- **Maximum No. of Fingers:** Displays the values of the maximum number of fingers configured at the global level. This field is not editable.
- **Number of Fingers and Palms/Cards:** Select the number of cards or fingerprints to be enrolled based on the credential option selected in the **Enrollment Mode**.
- **Enable Self-Enrollment:** Select this check box to enable the self-enrollment feature on the Panel Door.

Advanced

The Advanced tab allows the user to configure some advanced parameters such as access control Settings, Alarms, Timers and Wiegand.



The configurations done in Panel will be functional only if supported by the Device connected with it.

Click each link to configure the Advanced parameters:

- [“Settings”](#)
- [“Alarms”](#)
- [“Timers”](#)
- [“Wiegand”](#)

Settings

The **Advanced > Settings** and the page appears as shown below:

The screenshot shows the 'Device Configuration' window with the 'Settings' tab selected. The left sidebar lists various configuration categories, with 'Advanced' highlighted. The main panel displays settings for device 4 (Panel200-Devi..., Panel200, 4/25000, Active). The settings include:

- Generate Exit Switch Events: ☐
- Generate Invalid User Events: ☐
- Degraded Access: ☐
- Degrade Wait Timer (Sec): 5
- Access Mode: Any One
- Facility Code: 1
- Allow Facility Code Verification: ☐
- Enable Additional Security: ☐ Disabled
- Enable Smart Identification: ☐
- Access Level: 8
- Access Mode: Card
- Auto Acknowledge Alarm: ☐
- Alarm Auto Acknowledge Timer (Sec): 10
- Override IO Linking/Time Triggered during Disarm: ☐
- Allow Access Through Mobile: ☐
- Mobile Entry Access Mode: Mobile Only

The screenshot shows the 'Device Configuration' window with the 'Settings' tab selected. The left sidebar lists various configuration categories, with 'Advanced' highlighted. The main panel displays settings for device 1 (Panel200-Devi..., Panel200, 2/25000, Active). The settings include:

- Enable Smart Identification: ☐
- Access Level: 8
- Access Mode: Card
- Auto Acknowledge Alarm: ☐
- Alarm Auto Acknowledge Timer (Sec): 10
- Override IO Linking/Time Triggered during Disarm: ☐
- Allow Access Through Mobile: ☐
- Mobile Entry Access Mode: Mobile Only
- Mobile Exit Access Mode: Mobile Only
- Free Access: ☐
- Auto Assign New Panel Door to User/Device Group: ☒
- Advertise Bluetooth: ☐
- Bluetooth Name: MATRIX
- Bluetooth Range: Medium (5m - 7m)
- Panel Door Secured Communication: ☐

- **Generate Exit Switch Events:** Select this check box to enable the Panel Door to generate events every-time the exit switch is used.
- **Generate Invalid User Events:** Select this check box to enable the Panel Door to generate events for invalid user inputs.
- **Degraded Access:** Degraded mode allows a valid user to access the facility even if the Panel Door is not communicating with the Panel200. Select this check box to enable this feature at the Panel level. Make sure you also configure the Degraded Mode parameters in ["Configuration"](#) under ["Setting Up Access Zones"](#).
- **Degrade Wait Timer (sec):** Specifies the time period in seconds after the expiry of which the Panel Door switches from Network Fault to Degraded Mode. Default value is 5 sec.
- **Access Mode** - Defines the type and combination of credentials required to identify and validate a user at the Panel Door. Select the appropriate credential combination from the drop-down list. The options available are:
 - Any One
 - Card
 - Card + Biometrics
 - Card + Biometrics + PIN
 - Card + PIN
 - Biometrics
 - Biometrics + PIN
 - Biometrics then Card
 - Biometrics + Group
- **Facility Code:** Facility or site codes are encoded on cards, along with a card number, to ensure that cards belong to the facility where access is attempted. Facility Code is unique 8 or 16 bits of every HID Proximity card number specific to a site and is encoded into the card by the manufacturer.

COSEC also supports end user defined Facility Code (FC) to be written on to the card at the time of enrollment while using Smart Cards. Configure the Facility Code (ranging from 1 to 65535) as per your requirement.
- **Allow Facility Code Verification:** Select this check box to avail facility code verification on Panel Door.
- **Enable Additional Security:** In order to keep additional level of security check other than Facility Code and card number check, Smart Cards can be written with Additional Security Code that takes security to the next higher level. Select this check box to enable this functionality at the Panel level.
 - **Additional Security Code:** Configure the code (ranging from 1 to 65535).
 - **Re-enter Code:** Configure the code again to confirm.

Enable Additional Security
☒

Additional Security Code *

Re-enter Code *

Default Code

- **Default Code:** If you wish to use the default code, click the Default Code button, the Additional Security Code and Re-enter Code fields will be updated automatically.
- **Enable Smart Identification:** Select this check box to enable this functionality at the Panel.
- **Access Level:** Select the desired level from 1 to 15.
- **Access Mode:** Select the desired mode — Card, Card+PIN, Card+Biometrics, Card+Biometrics+PIN.

Enable Smart Identification
☐

Access Level

8

Access Mode

Card

- **Auto Acknowledge Alarm:** Select this check box to enable the auto-acknowledgment of all alarms.
- **Alarm Auto Acknowledge Timer (sec):** Set the time in seconds after the expiry of which the alarm buzzer will stop automatically.

Auto Acknowledge Alarm
☒

Alarm Auto Acknowledge Timer (Sec)

Override IO Linking/Time Triggered during Disarm
☒

Activate Windows
Go to Settings to activate

- **Override IO Linking/Time Triggered during Disarm:** Select this check box to enable Overriding of IO Linking/ Time Triggered configurations when the Disarm under Special Function is enabled.
- **Allow Access Through Mobile:** Select this check box to enable this functionality.

Allow Access Through Mobile
☐

Mobile Entry Access Mode

Mobile Only

i

Mobile Exit Access Mode

Mobile Only

i

- **Mobile Entry/Exit Access Mode:** Select the entry and exit door access mode from the options — Mobile Only, Mobile then Biometrics, Mobile then PIN and Mobile then Card.



If User Access Mode is selected as “None” in Zone Configuration and Mobile Access Mode is selected as “Mobile Then Biometrics” then Panel Door can be accessed through Mobile then Biometric credential.

- **Free Access:** Select this check box to allow the users to access all Panel Doors connected with the Panel200, irrespective of the Access Route assigned.

- **Auto Assign New Panel Door to User/Device Group:** Enabling this check box allows Panel to assign the new configured Panel Doors to the respective users and/or device groups automatically.

For example: Panel Door 1 and Panel Door 2 are assigned to the User 1 and Device Group 1. Now if the Panel Door 3 has been added in the same configured Panel and if this check box is enabled then, the newly added Panel Door 3 will be automatically assigned to the User 1 and Device Group 1.

- **Advertise Bluetooth:** Select this check box to enable bluetooth of the Panel by which the Panel will be visible to others. Then configure the following parameters.


- **Bluetooth Name:** Configure the name of the bluetooth by which it can be identified by other devices. Default: MATRIX.

If required, you can configure the bluetooth name as per your requirement. The **Bluetooth Name** can be a maximum of 10 characters.

- **Bluetooth Range:** Select the range for bluetooth as **Short**, **Medium** or **Long**. If Short range is selected then the Panel will be visible to the nearby devices which are in the range of 1m to 2m.

Select the Bluetooth Range as — **Short (1m-2m)**, **Medium (5m-7m)** or **Long (>8m)**.

- **Panel Door Secured Communication:** Select this check box to establish secure communication between Panel and Panel doors.

Click **Save**  to save all the configurations.

Alarms

Click **Advanced > Alarms** and the page appears as shown below.

The screenshot shows the 'Device Configuration' window with the 'Alarms' tab selected. On the left, a sidebar lists configuration categories: Profile, Enrollment, Advanced (selected), Features, Special Functions, Input/Output, Zones, Additional, Access Clusters, and Door Group. The main area displays a list of alarm types with checkboxes for activation: Duress, Dead Man, Panic, Door Offline, Door Fault, Occupancy Violated, Tail-Gating, Man Trap Timer Violation, Access Denied - Anti-Pass Back, Access Denied - Access Route Violated, Access Denied - Other Reasons, Multiple Unauthorized Attempts, User Unidentified, Access Denied - Access Route Timer Violated, and Face Mask Compulsion. Below this list are three input fields for 'Custom Alarm 1', 'Custom Alarm 2', and 'Custom Alarm 3'. At the bottom, there are two more settings: 'Alarm Reissue Wait Timer (Min)' set to 5 and 'Man Trap Alarm Wait Timer' with an unchecked checkbox.

Select the desired check boxes for the respective alarms to activate the same. You can configure upto 3 **Custom Alarms** also as per your requirement.

- **Duress Alarm:** Duress Alarm can be generated when a facility/premises has been accessed by a valid user but under some threat or force entry. In this situation; the user can alert the security by entering the duress code along with user code. This duress will be reported to the security at remote location without any local alarm.



Enable the Duress Detection feature and set the Duress Code from Duress Detection in “Set3” or/and Enroll Duress Finger from “Enrollment”.

- **Dead Man Alarm:** Dead Man Alarm is generated when the person working in restricted environment does not come out of the Dead Man Zone within a pre-defined Alert time.



Enable the Dead Man Zone feature at Panel level from Access Features > “Set3” and at Zone level from Zones> Configuration.

- **Panic Alarm:** You can enable the system to generate a Panic Alarm from the Panel Door by enabling the Panic Alarm check box. Also Door Alarm must be activated and the door must be in the normal condition (i.e. armed) then Panic Alarm will be generated.
- **Door Offline Alarm:** You can enable the system to generate a Door Offline Alarm by enabling the Door Offline check box. Also Door Alarm must be activated so when the door is offline then Door Offline alarm will be generated.
- **Door Fault Alarm:** You can enable the system to generate a Door Fault Alarm by enabling the Door Fault check box. Also door alarm must be active. So when the door is accessed and held opened for long time, then door fault alarm will be generated.

- **Occupancy Violated Alarm:** You can enable the system to generate the Occupancy Violated alarm, when the number of users permitted within a secured area or controlled zone exceed.



Enable the Occupancy Control feature at Panel level from Access Features > Set1 and at Zone level from Zones> Configuration.

- **Tail-Gating Alarm:** You can enable the system to generate the Tail-Gating alarm, when more than one person enters a secured area using a single person's access credentials.
- **Man Trap Timer Violation Alarm:** Whenever the Man Trap Timer is configured for a particular door, the user is expected to punch on the door present in the same zone within the specified Mantrap timer. If user fails to do so, Man Trap Timer Violation Alarm will be activated.



Enable Man Trap for the Zone level from Zones> Configuration.

- **Access Denied-Anti-Pass Back Alarm:** This alarm can be enabled to alert the fraudulent use of card when Anti-Pass back feature is applied in a zone. When the restriction is hard, the user has to follow entry and exit sequence before entering again; else access will be denied and alarm will be generated.



Enable the Anti-Pass back feature at Panel level from Access Features > "Set3" and at Zone level from Zones> Configuration.

- **Access Denied- Access Route Violated:** This alarm can be enabled to alert the violation of access route configured for the user. When the restriction is hard, the user has to follow the access route; only then he will be allowed to access the doors in the route.



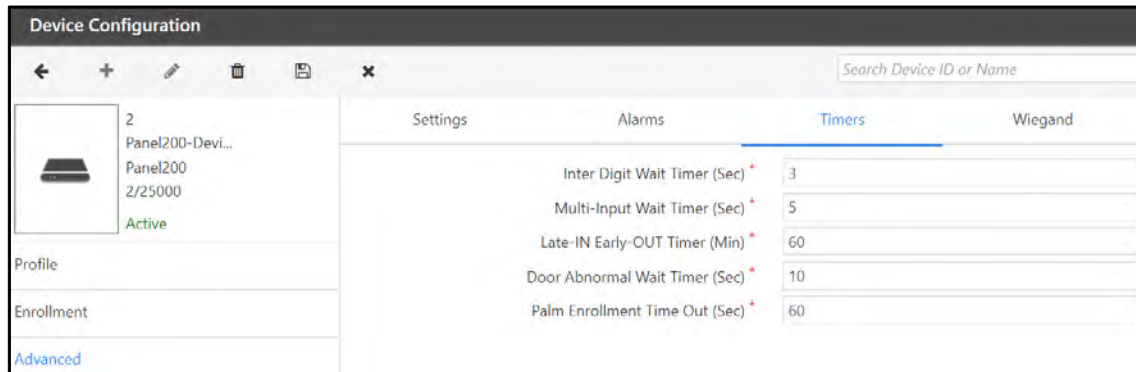
Enable the Access Route feature at Panel level from Access Features > Set1 and configure the Access Route feature from Access Control module> Access Route.

- **Access Denied-Other Reasons:** This alarm can be enabled to alert the violations of other Access control policies (other than APB violation & Access Route violation) while accessing the door.
- **Multiple Unauthorized Attempts:** This alarm can be enabled to provide an alert when an unauthorized user is trying to access the door multiple times.
- **User Unidentified:** This alarm can be enabled to provide an alert when the credential of user accessing the door are not identified.
- **Access Denied - Access Route Timer Violated:** This alarm is activated when the Access Route Timer is violated.
- **Custom Alarm 1/2/3:** You can configure custom alarm as per your requirements.
- **Alarm Reissue Wait Timer (min):** Define the time in minutes for which an acknowledged alarm should wait before being re-issued. Default value is 5 minutes.
- **Man Trap Alarm Wait Timer:** This check box enables an alarm wait timer on the panel to ensure that the user accesses sequential doors of a Man Trap within a specific time-frame.

Timers

This section allows the configuration of various types of pre-defined timers which can trigger off specific responses.

Click **Advanced > Timers** and the page appears as shown below:



Configure the following options as required:

- **Inter-Digit Wait Timer (sec):** Specifies the time period in seconds for which the Panel Door waits between two digits before considering the user input code as complete. Default value is 3 sec.
- **Multi-Input Wait Timer (sec):** Specifies the time for which system needs to wait for the second credential input from the user when more than one credential is to be used to grant access. Default value is 5 sec.

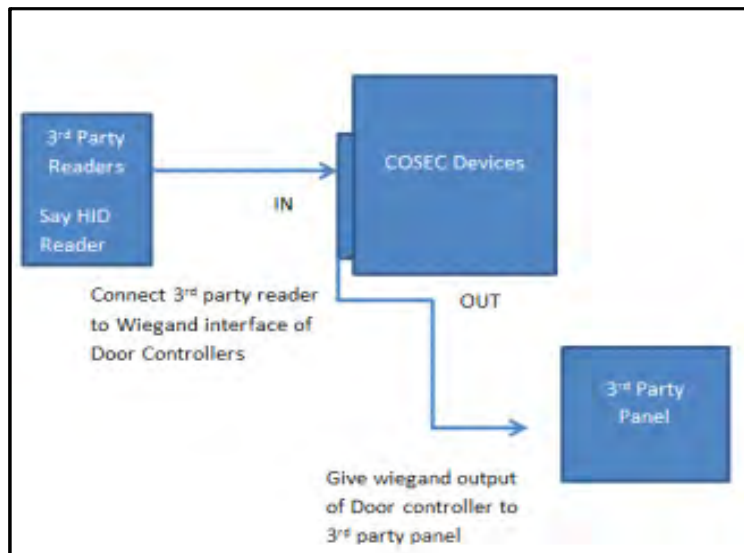
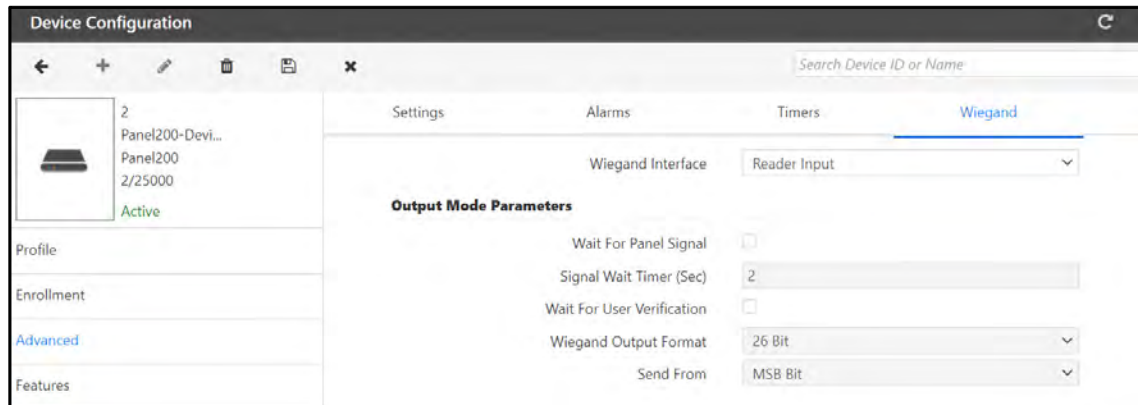


We recommend you to set the timer value as greater than or equal to 10 seconds to avoid access denial issues to users. This is applicable when the system reads the credentials (biometric) from the user's Smart Cards.

- **Late-IN Early-OUT Timer (min):** Specify the time in minutes for which the Late In and Early Out special functions will remain in effect after being enabled at the Panel.
- **Door Abnormal Wait Timer (sec):** Specify the time in seconds for which system needs to wait before generating an alarm for abnormal door status.
- **Palm Enrollment Time Out (sec):** Specify the time in seconds for which a Palm enrollment command will be valid for credential input on a PVR Panel Door. Once this timer runs out, a new enrollment command will have to be generated.

Wiegand

Click **Advanced > Wiegand** and the page appears as shown below:



- **Wiegand Interface:** Panel200 can be connected both as input devices (e.g. to receive data from a Wiegand Reader) or output devices (e.g. to support output to third party panel) via the Wiegand interface as shown above.

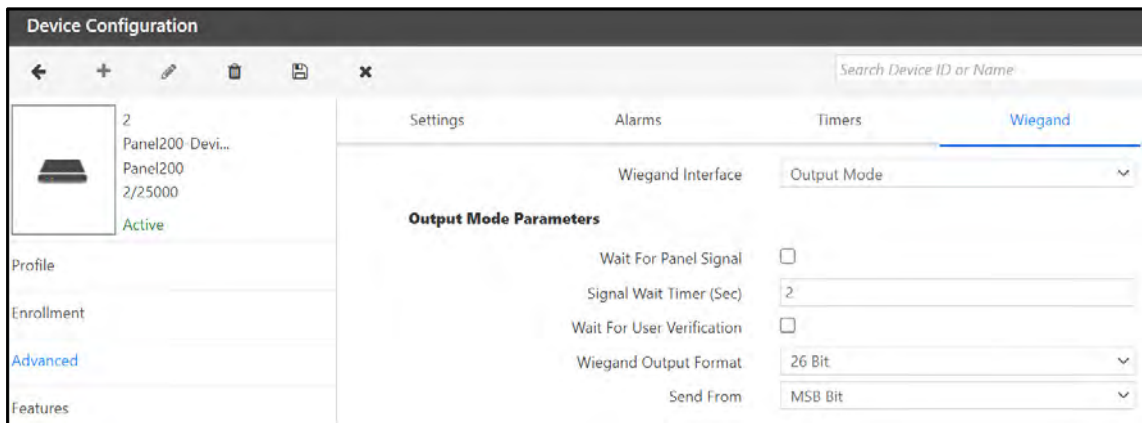
So select the interface of Panel Door as **Output Mode** to work as Wiegand Output to Panel or **Reader Input** to take data from third party reader. If Reader Input option is selected, all the output mode parameters will be disabled.

If you select Output Mode then configure the **Output Mode Parameters**.

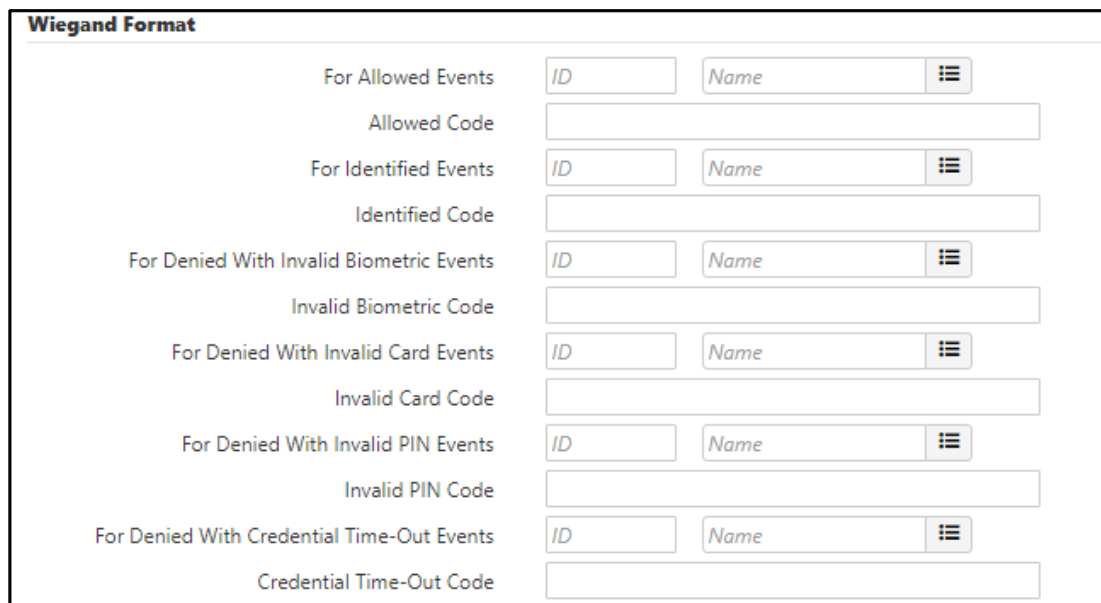
Output Mode Parameters

- **Wait For Panel Signal:** Select the check box to enable. If this option is enabled the Panel Door will wait for reply from the connected third party device before triggering any output. You need to configure the **Signal Wait Timer (Sec)**.
- **Signal Wait Timer:** Specify the time for which the Panel Door should wait for reply from the connected third party device before triggering any output.

- **Wait For User Verification:** Select the check box to enable. If this option is enabled, user verification will be requested on the third party device before triggering any output.
- **Wiegand Output Format:** Select the desired format — 26 Bit, 37 Bit, Actual or Custom.



If you select **Custom**, you can configure details of fields to be sent as output from the Wiegand reader that has been added.



- For each of the listed events, click the picklist to select the desired **Wiegand Output Format**.
- Assign an Access **Code** for each communication (for example Invalid PIN Code). This will depend on the number of output bits configured for Access Code in the selected Wiegand Output Format.
- **Send From:** Select the desired sending order for reader data — MSB or LSB Bit.

Features

The Features tab allows the you to enable certain Access Control features.



The Features tab is available only with the Access Control Module license.

The configurations done in Panel will be functional only if supported by the Device connected with it.

Click each link for details.

- [“Set1”](#)
- [“Set2”](#)
- [“Set3”](#)

Set1

This page allows the configuration of following rules - **Absentee Rule**, **Occupancy Control**, **Use Count Control**, **Soft Override**, **Access Route**, **Elevator Access Control** and **Block Users**.

Click **Features > Set1** and the page appears as shown below:

Set1	Set2	Set3
Absentee Rule		
Enable	<input type="checkbox"/>	
Occupancy Control		
Enable	<input type="checkbox"/>	
Default Occupancy Limit	<input type="text" value="9"/>	
Use Count Control		
Enable	<input type="checkbox"/>	
Default Use Count Limit (per minute)	<input type="text" value="5"/>	
Soft Override		
Enable	<input type="checkbox"/>	
Access Route		
Enable	<input type="checkbox"/>	
Elevator Access Control		
Enable	<input type="checkbox"/>	
Block Users		
Tail-Gating	<input type="checkbox"/>	
Man Trap Timer Violation	<input type="checkbox"/>	
Occupancy Violation	<input type="checkbox"/>	
Anti-Pass Back Violation	<input type="checkbox"/>	
Multiple Unauthorized Attempts	<input type="checkbox"/>	
Allowed Unauthorized Attempts	<input type="text" value="3"/>	

- **Absentee Rule:** This rule sets the maximum number of days for which the credential is not used (1 - 365 days). On expiry (that is, no usage of the credential for the maximum number of days set) the User will be blocked automatically. Select the **Enable** check box to enable this feature at the Panel level.
- **Occupancy Control:** Occupancy Control functionality enables the system to monitor and control the number of users permitted within a secured area or controlled zone. Occupancy control functionality requires entry and exit readers on the controlled area. Select the **Enable** check box to enable the feature at the Panel level and then enable the same at the Zone level.
- **Default Occupancy Limit:** Set the number of users to be considered as default Occupancy limit for Occupancy Control.

- **Use Count Control:** Use Count Control sets a maximum number of times an authorized user can use their credential in order to enter/exit a controlled area within a minute, after which the credential is blocked. Select the **Enable** check box to enable this feature at the Panel level.
- **Default Use Count Limit (per minute):** Specify the maximum number of times a user can use his/her credential per minute.
- **Soft Override:** The override function allows you to change the current status of a system temporarily, from the software application. Select the **Enable** box for enabling this functionality at the Panel level.



Once the **Soft Override** check box is enabled, you can temporarily Override the following Access Rule features — 2 Person Rule, ACS Policies, Alarm, Anti-Pass Back, First-IN User Rule, Mantrap, Occupancy Control and Visitor Escort Rule. Refer [“Soft Override”](#) for details.

- **Access Route:** This rule allows the you to enable defining an access path for users on a Panel by specifying the member Panel Doors using the *Access Control* module.
- **Elevator Access Control:** Enable this check box to enable Elevator Access Control at the Panel.
- **Block Users:** These check boxes can be used to enable conditions on the violation of which a user should be blocked on the Panel Door. For example, to block a user for multiple attempts at unauthorized access, select the **Multiple Unauthorized Attempts** check box. The maximum number of attempts allowed before the user is blocked can be specified using the **Allowed Unauthorized Attempts** option.

Set2

This page allows the configuration of following rules - **First-IN User Rule**, **Anti-Pass-Back (APB)** and **2-Person Rule**.

Click **Features > Set2** and the page appears as shown below.

The screenshot shows the configuration interface for Set2. It contains three main sections:

- First IN User Rule:** Includes an 'Enable' checkbox and four groups (Group 1 to Group 4). Each group has a text input field and a 'List' button.
- Anti-Pass Back (APB):** Includes an 'Enable' checkbox, 'On Entry' and 'On Exit' checkboxes with dropdown menus (currently set to 'Local'), a 'Hard/Soft' dropdown (set to 'Soft'), a 'Forgiveness' checkbox, a 'Reset After' section with radio buttons for 'Day Change' and 'Timer Expiry', and a 'Forgiveness Timer (Min)' input field set to '1'.
- 2-Person Rule:** Includes an 'Enable' checkbox, a 'Default Mode' dropdown (set to 'Primary Must'), a 'Default Primary Group' dropdown (set to 'Select'), a 'Default Secondary Group' dropdown (set to 'None'), and a '2nd Person Wait Timer (Sec)' input field set to '5'.

- **First-IN User Rule:** Select the **Enable** check box to enable the feature at the Panel Door.
 - Select the First-In User **Group 1 to 4** which would be valid at the door. For configuring the rule, refer to *Access Control> First- In User Rule> Assignment*.
- **Anti-Pass Back (APB):** Select the **Enable** check box to enable the feature at the Panel Door. For configuring refer to *Access Control> Anti-Pass Back*.
- **2-Person Rule:** Select the **Enable** check box to enable the feature at the Panel Door and set the **2nd Person Wait Timer** in seconds after which the second person is allowed to punch on the door. For configuring refer to *Access Control> 2- Person Rule*.

Set3

This page allows the configuration of following rules - **Visitor Escort Rule, Dead Man Zone, Duress Detection, Man Trap Door Interlock, DND Zone** and **Access Clusters**.

Click **Features > Set3** and the page appears as shown below.

Set1	Set2	Set3
Visitor Escort Rule		
	Enable	<input type="checkbox"/>
Dead Man Zone		
	Enable	<input type="checkbox"/>
	Default Warning Timer (Min)	3
	Default Alert Timer (Min)	10
Duress Detection		
	Enable	<input type="checkbox"/>
	Default Code	10
Man Trap Door Interlock		
	Enable	<input type="checkbox"/>
	Man Trap Wait Timer (Sec)	5
	Functioning	Zone Based
DND Zone		
	Enable	<input type="checkbox"/>
	Default Access Level	15
Access Clusters		
	Enable	<input type="checkbox"/>

- **Visitor Escort Rule:** This rule requires all Visitors to be accompanied by an escort and the display of the visitor's credential has to be followed by the credential of the Escort within the stipulated time period. Select the **Enable** check box to enable this feature.
- **Dead Man Zone:** This condition allows the system to track the safety and security of a user while a specific task is being performed. This requires the user to show his credential within the pre-defined dead man time period. Select the **Enable** check box to enable this feature.
- **Default Warning Timer (min):** Specify the minimum time in minutes, within which any user inside the dead man zone should show his/her card/finger to reset the timer and thus prevent the alarm.
- **Default Alert Timer (min):** Specify the maximum time in minutes, for which the user is allowed to remain inside the dead man zone.
- **Duress Detection:** Duress detection enables the card holder to trigger an alarm on output device in the event of threats or being forced to grant access to an unauthorized person.

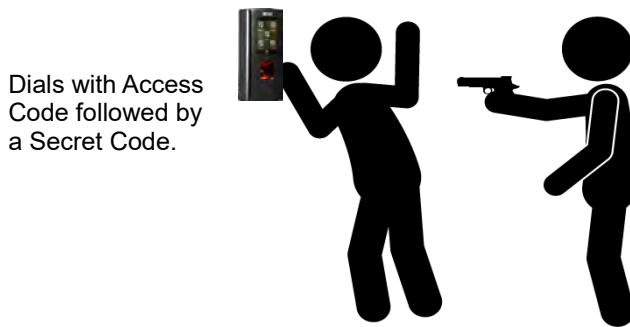
This feature can be activated by:

- finger credential, refer to ["Enrollment"](#) or/and
- when two digit duress code is keyed in, at the end of a User's allotted PIN Code.

To activate this feature using PIN,

- Select the **Enable** check box to enable this feature at the Panel level.
- Once this feature is enabled the system waits for the duress code after the User PIN and the right arrow key input before enabling the duress alarm. The keys have to be pressed in the following order:

(User Pin Code) → (Right Arrow Key) → (2 digit Duress Code)



- **Default Code:** Specify the default two digit duress code (ranging from 10 to 99).
- **Man Trap Door Interlock:** Mantrap interlock or airlock systems provide safety, security and environmental control between two or more rooms by ensuring that opening any door causes all other doors to lock until the opened door returns to the closed position. Select the **Enable** check box to enable the feature at the Panel level and then enable the same at the Zone level.



Door sense is must for this feature as the system will ignore the door status either in the absence of a door sense or its fault state.

This feature is not supported when the Panel Doors are in Degrade Mode.

- **Man Trap Wait Timer:** Specify the time in seconds for which the Panel Door needs to wait for the other door in the same zone where the mantrap feature is enabled to get closed. By default the value of the Man Trap Timer is 5 seconds and valid range is from 3 sec to 99 sec.
- **Functioning:** Select the desired option — Zone Based, Door Group Based.
- **DND Zone:** DND feature allows the user to declare that a particular zone is not to be accessed by other users for a specific period of time thereby ensuring that the users inside the zone are not disturbed by others. Select the **Enable** check box to enable this feature. The DND is activated using a special card or through the Menu of the Panel Doors.
- **Default Access Level:** Specify the default Access level for DND Zone within a range of 1-15.
- **Access Clusters:** Select the **Enable** check box to enable checking for access control restrictions when a user punches on any of the assigned Panel Doors.

Special Functions

COSEC provides its users the privilege to perform certain pre-defined operations directly from the Panel Doors. These operations are related to various time and attendance marking functions, administrative tasks, zone-related access and door-control functionality as well as alarms management.

A special function may be used in three different ways:

- Entering short codes on the device keypad.
- Navigating the device menu.
- Using Special Cards.



The configurations done in Panel will be functional only if supported by the Device connected with it.

Special Cards

A Special Card is especially useful when the user has to perform routine tasks, where repeated manual entry of codes can become tedious. It is also required when a Panel Door does not have keypad or LCD display for manual entry of special codes. In such a case, an RFID card can be encoded for a special function and the card-holder can perform a special function at the device just by showing this Special Card.

Example: In factories where workers avail shortleave; security guard can show the Special Card enrolled for Shortleave IN on the Entry door and can give the access to the worker. This same card can be used for multiple workers.

Configuring Special Functions

To access this,

Click **Special Functions** and the page appears as shown below:

The screenshot shows the 'Device Configuration' window. On the left is a sidebar with a tree view containing '2 Panel200-Devi...', 'Panel200', '2/25000', and 'Active'. Below this are menu items: 'Profile', 'Enrollment', 'Advanced', 'Features', 'Special Functions' (highlighted in blue), 'Input/Output', 'Zones', and 'Additional'. The main area has two tabs: 'Configuration' (selected) and 'Schedule'. Below the tabs is a table with 12 rows of special functions. Each row has columns for 'No.', 'Function Name', 'Active', 'User Group', and four card slots (Card 1, Card 2, Card 3, Card 4). Each card slot contains a small icon of a card. The functions listed are: 1. Official Work - IN, 2. Official Work - OUT, 3. Short Leave - IN, 4. Short Leave - OUT, 5. Regular - IN, 6. Regular - OUT, 7. Break End, 8. Break Start, 9. Overtime - IN, 10. Overtime - OUT, and 12. Set Panic Alarm. All functions are marked as 'Active' and 'All' for the user group.

No.	Function Name	Active	User Group	Card 1	Card 2	Card 3	Card 4
1	Official Work - IN	Yes	All				
2	Official Work - OUT	Yes	All				
3	Short Leave - IN	Yes	All				
4	Short Leave - OUT	Yes	All				
5	Regular - IN	Yes	All				
6	Regular - OUT	Yes	All				
7	Break End	Yes	All				
8	Break Start	Yes	All				
9	Overtime - IN	Yes	All				
10	Overtime - OUT	Yes	All				
12	Set Panic Alarm	Yes	All				

The COSEC system pre-defines 38 special functions for its users. For instance, all the special functions in the given list are supported on all COSEC Panels. The following list provides details of the special functions supported on Panel200.

Time and Attendance Functions *(Available only with the Time & Attendance add on module)*

Special Function	Description
Official Work-IN / Official Work-OUT	Late-IN as well as Early-OUT is marked as User's Official work in Time & Attendance.
Short Leave-IN / Short Leave-OUT	Late -IN as well as Early-OUT is marked as User's short leave in Time & Attendance.

Special Function	Description
Regular - IN / Regular - OUT	Normally used in Time & Attendance system in the absence of an exit reader. The punch in at start of shift and punch out at end of shift are sent with the appropriate flags.
Break End / Break Start	Clock-IN is marked as User post break entry and Clock-OUT is marked as User exit at start of break.
Late-IN Start / Late-IN Stop	System starts / stops inserting the special ID to T&A events of all users who clock-IN after this function.
Early-OUT Start / Early-OUT Stop	System starts / stops inserting the special ID to T&A events of all users who clock-OUT after this function.
Over Time - IN / Over Time - OUT	The IN punch is marked as User entering at start of over time while the OUT punch is marked as User exiting after completion of overtime.

Administrative Functions *(Available with the Basic platform license.)*

Special Function	Description
Enroll User	Application switches the door controller mode to Enrolment mode and User Credentials are enrolled against the defined user ID. Global Enrolment mode is selected by default for users.
Enroll Special Card	Application switches the door controller mode to Enrolment mode and special Cards are enrolled against special function ID
Delete Credentials	Enables user to delete the existing credential data from the PANEL User database against the selected user ID.
View User Profile	System reads the User's Smart Card and displays the stored user profile.

Zone Settings *(Highlighted options available only with the Access Control add on module)*

Special Function	Description
Activate DND / Deactivate DND	System switches the door zone from Normal to DND and vice versa.
Activate Dead-Man / Deactivate Dead-Man	System switches all Door Controllers of the zone from Normal mode to activated Dead Man Zone mode and vice versa.
Door Lock / Door Unlock	System locks/unlocks the selected Door. Entry is denied to all users. Exit request however, is enabled and the user can still provide T&A events.
Zone Lock / Zone Unlock	System locks/unlocks all Doors of the Zone. Entry is denied to all users. Exit request however, is enabled and the user can still provide T&A events.
Door Normal	System switches the mode of the door controller to the normal or controlled mode.
Zone Normal	System switches the mode of all Doors of the Zone to the normal or controlled mode.
Guard Tour	The security guard carries the guard tour card which is linked to the guard tour-ID.

Alarms *(Available only with the Access Control add on module)*

Special Function	Description
Set Panic Alarm	System enables the user to generate a Panic Alarm from the Door Controller.

Special Function	Description
Mute Door Buzzer	Enables the user to mute the Door Controller's existing Alarms.
Mute Panel Buzzer	Enables the user to mute the PANEL's existing Alarms.
Clear Door Aux O/P	Enables the user to Reset the Aux output of Door Controller and switch it back to Normal/Controlled state from its current state.
Clear Panel Aux O/P	Enables the user to Reset the Alarm output of PANEL and switch it back to Normal/Controlled state from its current state.
Door Arm/Door Disarm	To enable/disable door alarms using special function cards.
Zone Arm/Zone Disarm	To enable/disable zone alarms (for all doors in the zone) using special function cards.

To configure Special Functions, click **Edit** . For details, refer to [“Special Functions”](#).

Input/Output

The Input/Output (I/O) configuration of a system determines how the output or response of a system is influenced by the input applied on it. In case of the COSEC Access Control System, the I/O configuration should enable the system to monitor and trigger a specific response to any changes in door state or event occurrences at the door device. This change of door state or occurrence of events will be considered as an input while the response or action that is generated by the system on detection of this input, will be considered as the output.

The I/O configuration of Panels allows the user to enable Auxiliary Ports, create Input and Output groups, configure I/O Linking and set up Time Triggered Output functions.



This functionality is available only with the Access Control add-on module license.

The configurations done in Panel will be functional only if supported by the Device connected with it.

Click each link to configure the Input Output parameters:

- [“Configuration”](#)
- [“Input Groups”](#)
- [“Output Groups”](#)
- [“IO Linking”](#)
- [“Time Triggered”](#)

Configuration

Click **Input/Output > Configuration** and the page appears as shown below:

The screenshot shows the 'Device Configuration' window with the 'Configuration' tab selected. The left sidebar lists various configuration categories, with 'Input/Output' highlighted. The main panel displays settings for 'Auxiliary Input' and 'Auxiliary Output'. For 'Auxiliary Input', the 'Enable' checkbox is unchecked, 'Supervised' is unchecked, 'Sense Type' is set to 'NO', and 'Debounce Time (Sec)' is 5. For 'Auxiliary Output', 'Enable' is unchecked, 'Output Group' is set to 3, and 'Output Wait Time (Sec)' is 0. A 'Panel Output' button is located next to the 'Output Group' picklist.

Auxiliary Input

- **Enable:** Select the **Enable** check box option for Auxiliary Input (e.g. Smoke Detectors) depending on normal or supervised door state monitoring.
- **Supervised:** Select the **Supervised** check box to enable the door for four-state monitoring where the door is also monitored for Door Fault and Door Disconnection.
- **Sense Type:** The system by default can sense two states of a door — Normally Open (NO) and Normally Closed (NC) — depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a Door Abnormal alarm. Specify the **Sense Type** as **NC** or **NO** (Default: NC).
- **Debounce Time (Sec):** It defines the minimum time for which an input interface must be maintained in a given state before the system reports it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated. Specify the Debounce time in seconds. Range should be 0-99 sec.

Auxiliary Output

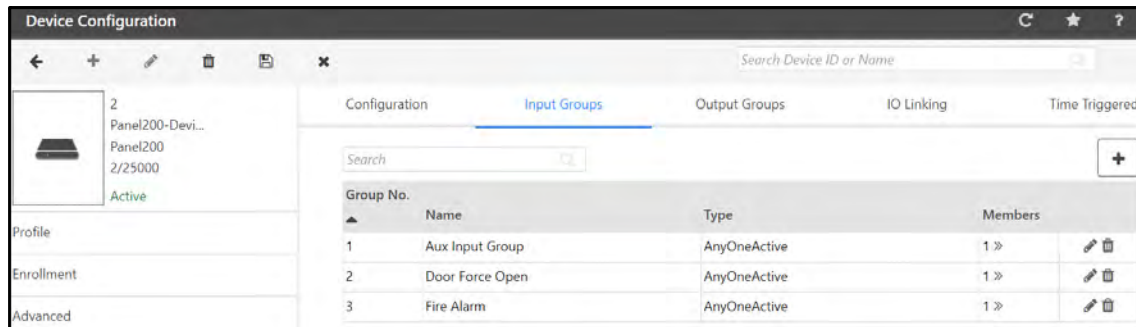
- **Enable:** Select the **Enable** check box to enable Auxiliary Output (e.g. Fire Alarm).
- **Output Group:** Click the picklist to select an Output Group to which the auxiliary output is to be assigned based on the output groups defined on the system.

To configure the output groups listed in the picklist, click **Device Configuration page > Input/Output > Output Groups**.

- **Output Wait Time (Sec):** Specify an Output Wait Time in Sec to set an additional waiting period before the Aux Output signal is sent.

Input Groups

Click **Input/Output > Input Groups** and the page appears as shown below:



Each Panel has one Input port while each of the slave Panel Doors have 4 inputs. The **Input Groups** option enables you to club these inputs into groups before they can be used in the Input/Output Linking.

Multiple input ports (logical ports) can be grouped together to form an input port group. This option allows you to assign user-friendly names to frequently used inputs and also setting the input parameters. You can club any of the inputs (not constrained to particular Panel Doors) and define them in a group.

Click **Add** to add a new Input Group.

- **Name:** Specify a user-friendly name to the Input group.
- **Type:** Select the Output **Type** from the options available in the drop down list (AllActive, AnyOneActive).
- **Members:** Click . The Member Configuration pop-up window appears.
- **Source:** Select the desired option — Panel, Door, Zone, Door Group.

- **Port:** The option in this will depend on the Source you select. Configure these as per your requirement.

Member No.	Source ID	Panel/Panel Door Name	Port
1	1	Panel200	MC_AlarmInput

If Man Trap feature with functioning as “Door Group based” is enabled, only then Door Group appears as Source in Member Configuration to configure the Input Group.

If you select **Source** as “*Door*” and **Port** as “DC_UserAllowed” or “DC_UserDenied” then a new parameter **User** will appear.

Member Configuration

Member No.

Source

Port

User Denied

Panel Door No.

Input Port Active Timer (Sec)

Member No. Source ID Par

DC_Offline
DC_Fault
DC_DoorForceOpen
DC_DoorAbnormal
DC_TamperFail
DC_AUX_1_IN_ACTIVE
DC_DuressAlarm
DC_PanicAlarm
DC_DeathMachAlarm
DC_UserAllowed
DC_UserDenied
Tail_Gating
Multiple_Unauthorized_Attempts
User_Unidentified
DC_AUX_1_IN_INACTIVE
DC_AUX_2_IN_ACTIVE
DC_AUX_2_IN_INACTIVE
DC_AUX_3_IN_ACTIVE
DC_AUX_3_IN_INACTIVE

Member Configuration

Member No.

Source

Port

User Denied

Panel Door No.

Input Port Active Timer (Sec)

User

Add Cancel

Member No. Source ID Panel/Panel Door Name Port

No Data

- **User:** You can select the desired option — All, Selected.

If you select the **Selected**, then in **Users Selected** click the picklist to select desired users.

The image shows two overlapping windows from a software application. The 'Member Configuration' window is in the background, and the 'Picklist For User' window is in the foreground. An arrow points from the 'User s Selected' picklist in the 'Member Configuration' window to the 'Picklist For User' window. Another arrow points from the 'OK' button in the 'Picklist For User' window to the text below.

Member Configuration

Member No.
Source
Port
User Denied
Panel Door No.
Input Port Active Timer (Sec)
User
User s Selected

Member No. Source ID Panel/Panel Door Name Port
No Data

Picklist For User

Total Selected : 3 Records

Search [Show Selected](#)

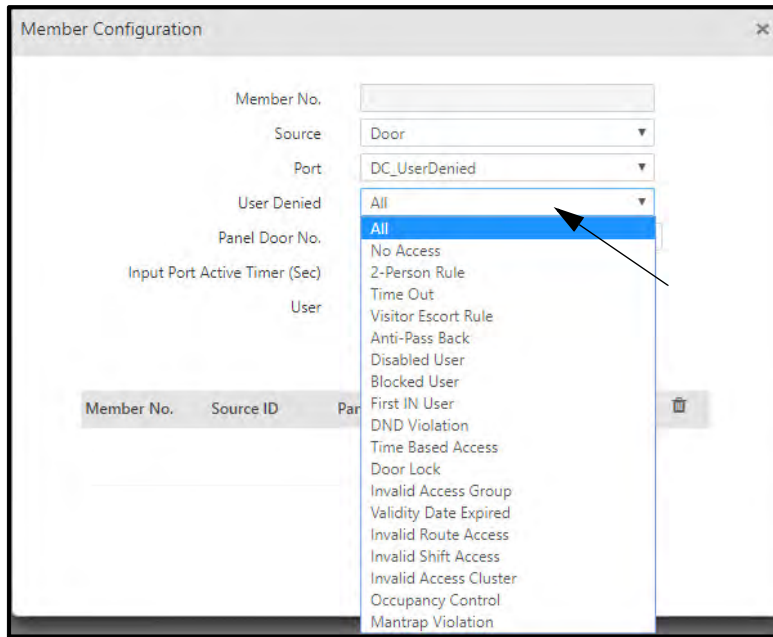
<input type="checkbox"/>	User ID ▲	Name
<input type="checkbox"/>	006	adfs1
<input checked="" type="checkbox"/>	011	UtsaviB
<input checked="" type="checkbox"/>	014	pathv2 priyanka
<input checked="" type="checkbox"/>	019	ninad_123
<input type="checkbox"/>	020	Podugu Uday Kiran
<input type="checkbox"/>	78	user-10

To do so,

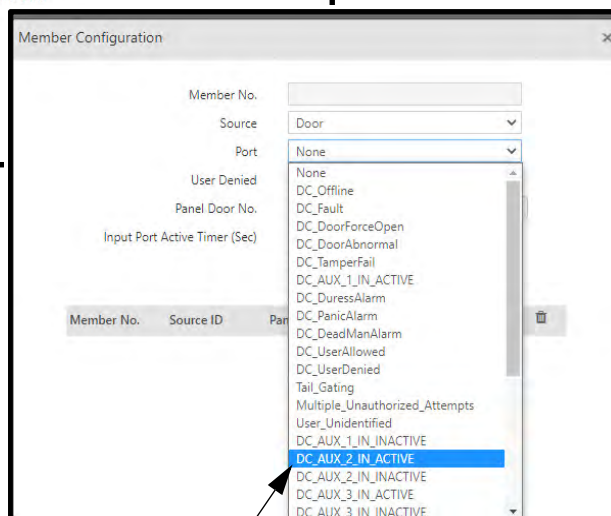
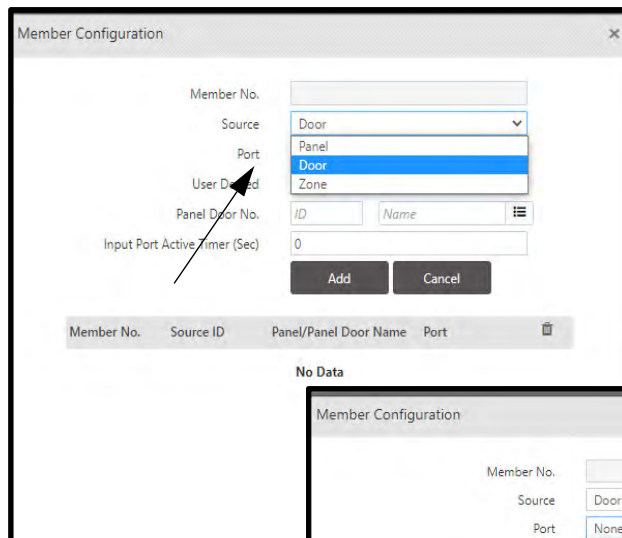
Select the check box of corresponding user that you want to add.

Click **OK**.

- **User Denied:** Will be editable when Source is selected as “DC_UserDenied”.



If you select **Source** as **Door** and **Port** as **DC_AUX-2_IN_ACTIVE** or **DC_AUX-2_IN_INACTIVE** then in the **Picklist For Panel Door Masters** for the parameter **Panel Door No.**, **ARC DC 200 Single Door Dual Reader** will be visible and can be selected.



Refer “ARC as Panel Door” to add a new **ARC DC 200 Single Door Dual Reader Panel door**.

Picklist For Panel Door Masters

Search

No	Name
1	Auxiliary ARC DC 200 Panel

Member Configuration

Member No.

Source

Port

User Denied

Panel Door No.

Input Port Active Timer (Sec)

Add **Cancel**

Member No.	Source ID	Panel/Panel Door Name	Port
No Data			

Member Configuration

Member No.

Source

Port

User Denied


Panel

Input Port Active Timer (Sec)

Add **Cancel**

Member No.	Source ID	Panel/Panel Door Name	Port
1	1	Auxiliary ARC DC 200 Panel	DC_AUX_2_IN_ACTIVE

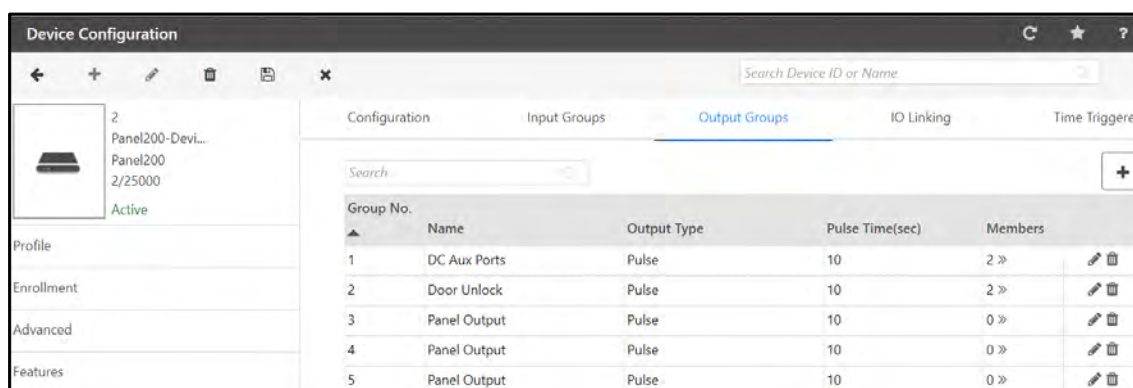
- **Panel Door No.:** Click the picklist to select the desired Panel Door.
- **Input Port Active Timer (Sec):** Specify the time in seconds for which the input port needs to remain active.

Click on **OK**  once done with the configuration.

You can now assign the individual relay outputs at the Panel and Panel Doors to this Input group as per the site requirements, prior to defining the IO Linking with this output group.

Output Groups


Click **Input/Output > Output Groups** and the page appears as shown below.



Each Panel has one Output port while each of the Panel Door has 2 Outputs one of which is used as a Door Relay. This option enables you to club these outputs into groups before they can be used in the Input/ Output Linking.

The output ports are physical ports and they can be assigned in to a group called Output Ports Group. The system supports up to 99 Output groups.

Click on **Add** button to add a new Output Group.

- **Name:** Specify a user-friendly name to the Output group.
- **Type:** Select the Output **Type** from the four options available in the drop down list (Pulse, Interlock, Latch, Toggle).
 - In the event of a **Pulse** type output, user needs to define the **Pulse time** in seconds.
 - In the **Interlock** option the Output group follows the input group. All member outputs are triggered as long as the input group is activated after which they return to normal state.
 - The **latch** option denotes the condition where all member outputs will be in an energized condition for infinite period and need to be reset manually.
 - In the **Toggle** option, the output group toggles its state whenever an input group is activated.
- **Members:** Click  . The Member Configuration pop-up window appears. Configure the members as per your requirement.

Click on **OK** once done with the configuration.

You can now go and assign the individual relay outputs at the Panel and Panel Doors to this Output group as per the site requirements, prior to defining the IO Linking with this output group.

IO Linking

Click **Input/Output > IO Linking** and the page appears as shown below:

No.	Name	Input Group	Output Group	Status
1	Aux Linking	Aux Input Group	DC Aux Ports	Inactive
2	Force Open link	Door Force Open	Panel Output	Inactive
3	Fire-Unlock	Fire Alarm	Door Unlock	Inactive

The COSEC application supports the Input Output Group linking feature to activate single or multiple output ports (output Group) based on a trigger received from single or multiple input ports (Input Group). This option enables the administrator to define how an event or events (input port group) will trigger outputs belonging to an output ports group.

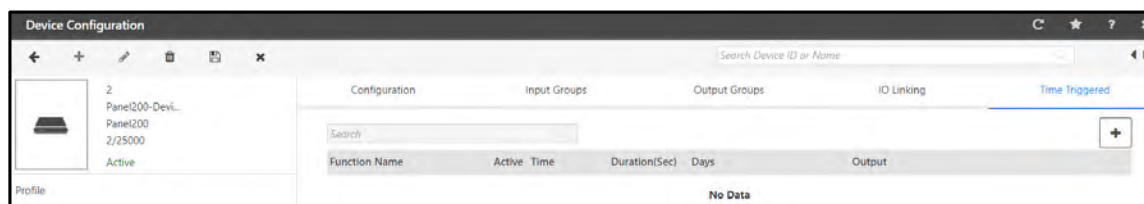
Input Output Group linking is a feature which enables the user to define programs which activate single or multiple output ports (output Group) based on a trigger received from single or multiple input ports (Input Group) on the Panels and Panel Doors.

- **Link Name** - Specify a user-friendly name to the linking program and
- **Active:** Select the check box to activate the linking program.
- **Input Group No.:** Click the picklist and select the desired input group.
- **Output Group No.** - Click the picklist and select the desired output group.
- **Raise Alarm:** Select a Custom Alarm (*See Advanced Configuration*) to be configured as output against an access violation event, if required.
- **Time Zone** - The Time Zones define the time slots in which the I/O linking Program must be activated.

Click **Add** once done with the configuration.

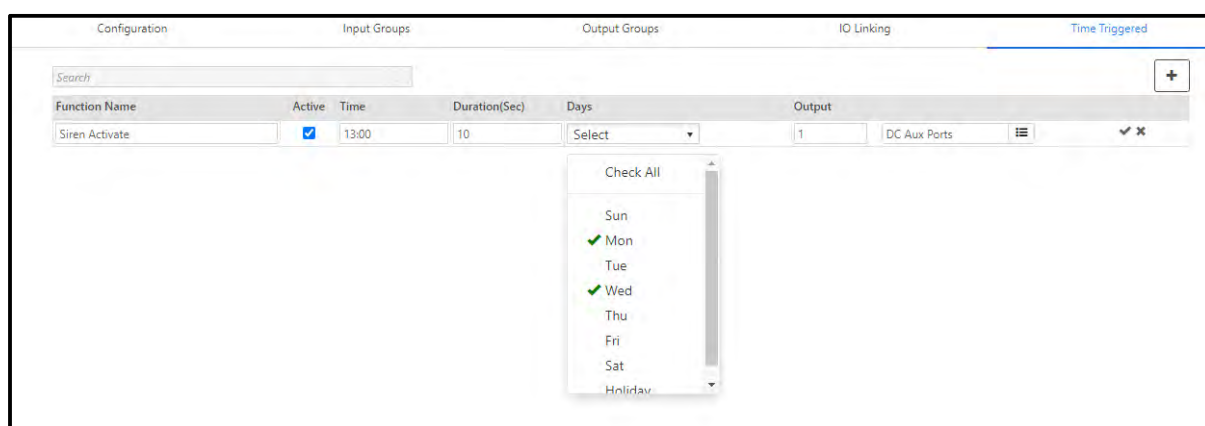
Time Triggered

Click **Input/Output > Time Triggering** and the page appears as shown below.



This functionality enables the user to control the activity of an Output without manual intervention. The time triggered functions are used for activating events like door unlock and siren activation that are set as per the start time and for the configured time duration. This functionality is designed to energize outputs for predefined periods at the configured time. The COSEC access control system supports up to 20 Time Triggered functions.

Click **Add** to add a new Profile for Time Trigger.



- **Function Name:** Configure a name to identify the function.
- **Active:** Select the check box to enable the function.
- **Time:** Configure the start time to trigger the function.
- **Duration (Sec):** Configure the duration for which this function should remain in the triggered state.
- **Days:** Select the days on which this functionality must be triggered.
- **Output:** Click the picklist to select the desired output.

Click **OK** once done with the configuration.

Setting Up Access Zones

Access Zones are areas with well defined boundaries, which are defined to effectively implement an Access Security System with Access Policies. A site can have multiple Access Zones, each Zone having multiple Panel Doors. You need to define the Access Zones before defining the Panel Doors and assigning the Access Zones. Any defined Access Zone can be directly assigned to users for free access during active working hours, without matching their Access Level with that of the zone's, by either defining the Zone as a **Home Zone** or a **Visit Zone**.

During the non-working hours, the non-working access level of the user's access group has to be higher than the Zone Access Level for allowing access to the user. All zones other than assigned Home Zone and Visit Zone are control zones to users and access to these zones are based on the result of the comparison between the user Access Level and the Zone's Access Level. The User Access Level has to be higher than the Zone Access Level to allow access. The system supports up to 99 Access Zones.



This section is available only with the Access Control add-on module license.

The configurations done in Panel will be functional only if supported by the Device connected with it.

Click each link to configure the Zone parameters:

- [“Setup”](#)
- [“Configuration”](#)
- [“Occupancy Control”](#)

Setup

Click **Zones > Setup** tab and the page appears as shown below.

By default **Zone-1** is created. You can either edit this zone or add a new zone as per your requirement.

To edit Zone-1,

- Click on Zone-1 in the grid. Edit the parameter as per your requirement.
- Click **Update**.

To add a new Zone,

- **Name:** Assign a name to the Zone you wish to add.
- **Access Level:** Select the access level you wish to assign to the zone. Valid Range:01 to 15.

- Select the mode of credentials required to identify and validate a **User** and **Visitor** both for internal and external readers. You can select the appropriate credential combination of Pin, Card, Face, BLE, Biometrics and Biometrics + Group or None in the following parameters.
 - **User Access Mode (Door):** Entry mode of user.
 - **Visitor Access Mode (Door):** Entry mode of visitor.
 - **User Access Mode (External Reader):** Exit mode of user.
 - **Visitor Access Mode (External Reader):** Exit mode of visitor.
- **Access Control on Exit Mode:** Select the check box to enable. The following Access Control Policies will be checked when the external reader is in the 'exit' mode.
 - User enabled
 - User validity
 - Blocked user
 - Time Based Access Check
 - ASC
 - User Access Group

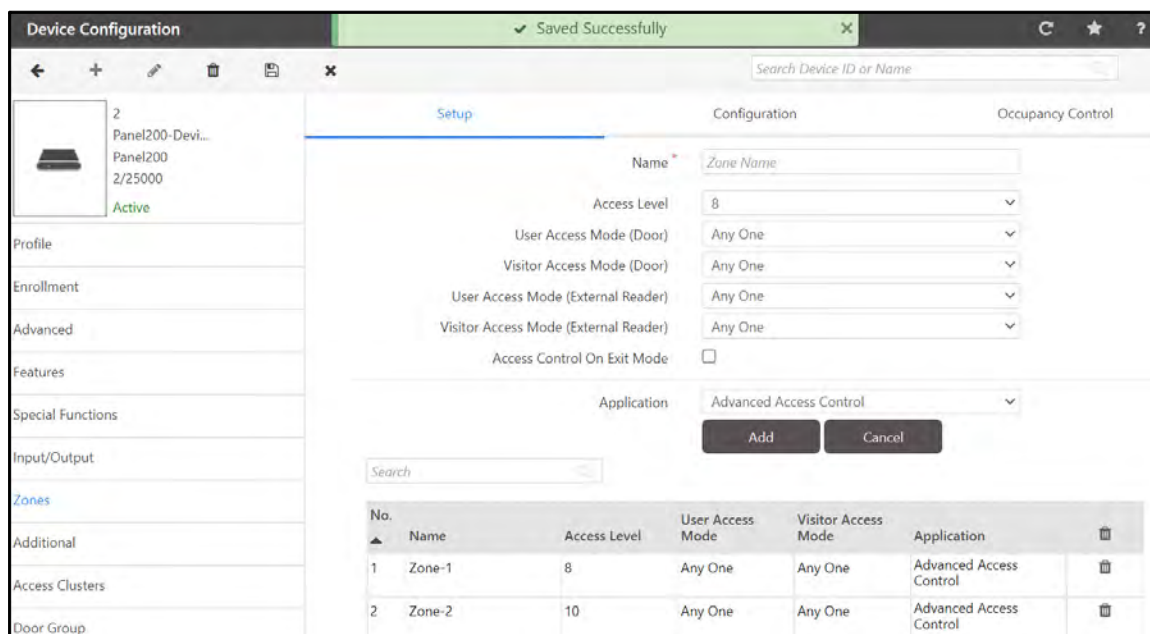
Clear the check box to disable. All the following access control features will be checked (which are applicable and configured).

- User enabled
 - Blocked user
 - Time Based Access Check
 - ASC
 - User Access Group
 - Deadman
 - Door application mode
 - Use count
 - Mantrap
 - Anti-pass back
 - Panel Route access
 - Smart card based route access
 - 2-person
 - Access mode
 - Occupancy control
 - Visitor escort rule
- **Application:** Select the desired Application — Advanced Access Control (inclusive of T&A) or Basic Access Control.



If you select Basic Access Control mode, Access Control functionalities mentioned above will not be applicable for the Zone. System will not check the same for the user access level for the Time and Attendance zone.

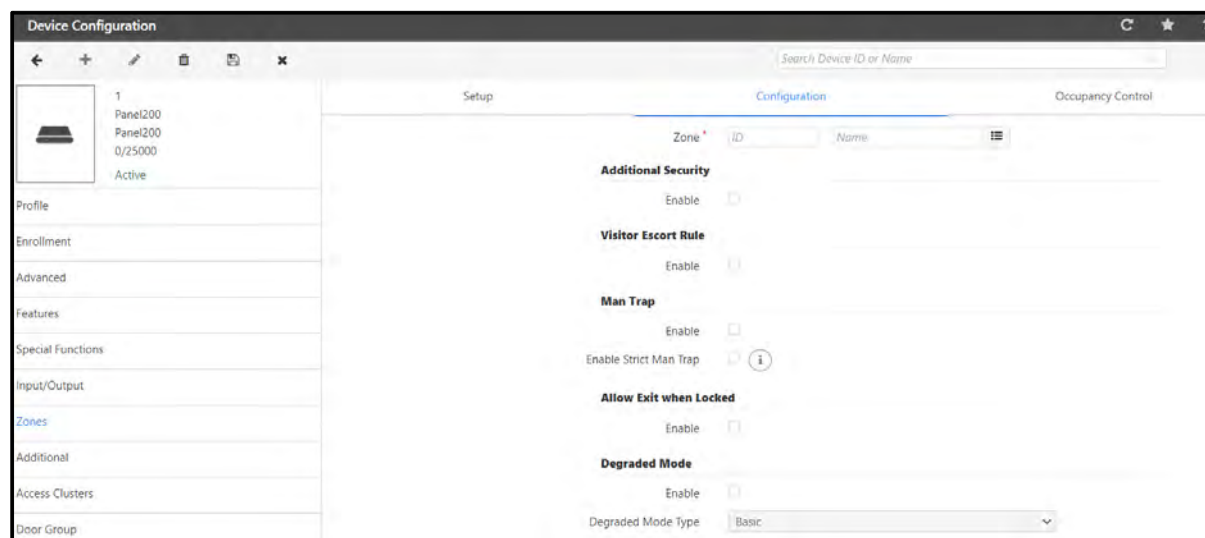
Click **Add** once done with the configuration. The newly added zone is displayed in the grid as shown below.

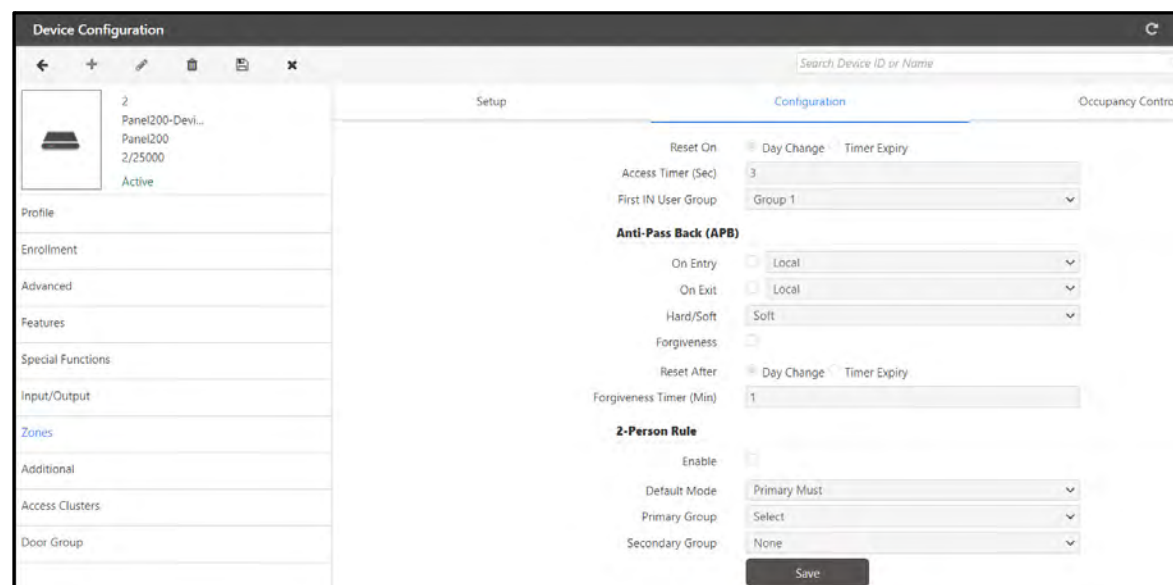
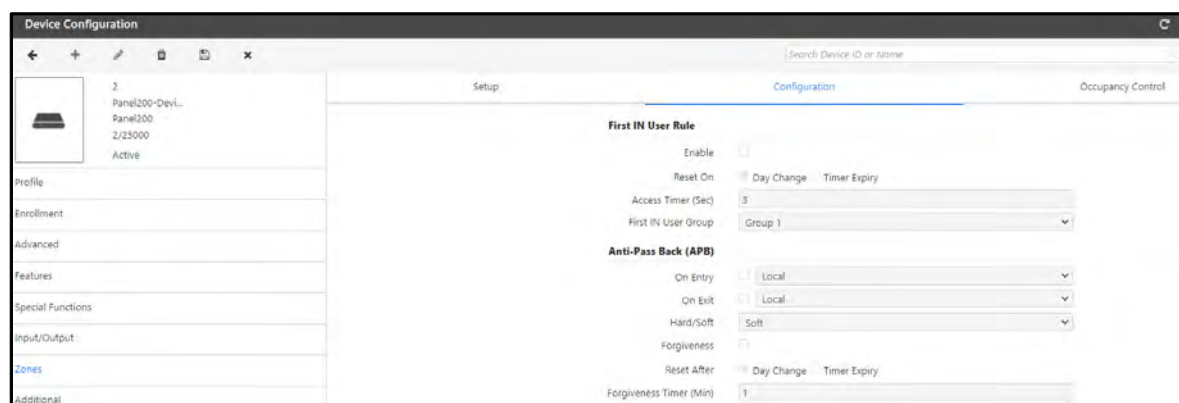
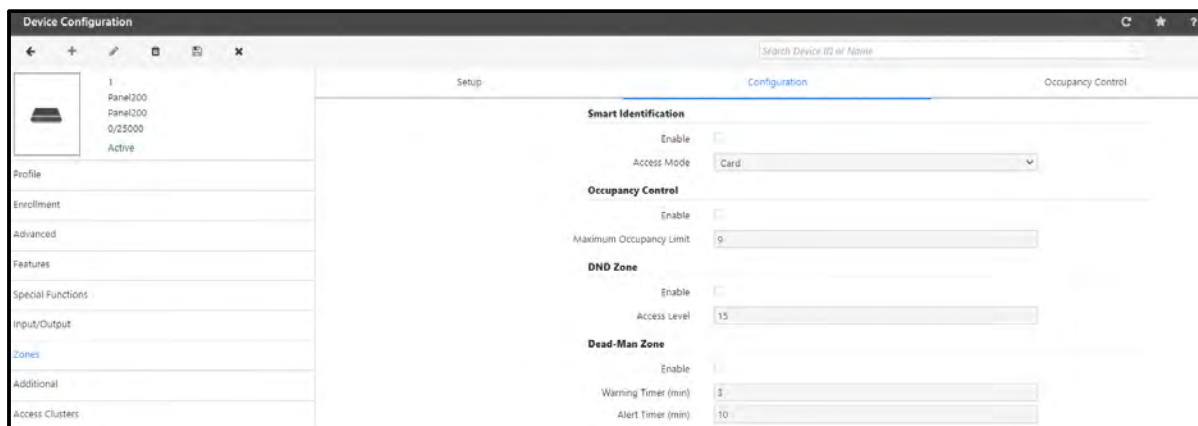


Configuration

Click **Zones > Configuration** and the page appears as shown below.

- **Zone:** Click the picklist to select the desired Zone.





Select and configure desired Access Control Policies you wish to apply to the selected zone and configure their respective parameters.

- **Additional Security:** Configure the following:
 - **Enable:** Select this check-box to enable the Additional Security feature for the Zone.

This Additional Security Check is possible only with Smart Cards which will prevent the duplicacy of card and restrict unauthorized access to the facility.

The user; who is assigned the zone enabled with ASC will be checked for ASC verification on the door.

- **Visitor Escort Rule:** For details, refer to [“Visitor Escort”](#).
- **Man Trap:** For details, refer to [“Man Trap”](#).
- **Allow Exit when Locked:** Select this check box to enable the user to exit when the Panel Door is locked.
- **Degraded Mode:** Configure the following:
 - **Enable:** Select this check box to allow a valid user to access the facility even if the Panel Door is not in communication with the Panel. Make sure you have enabled Degraded Mode and configured the Degraded Wait Timer under **Advanced > Settings**.
 - **Degraded Mode Type:** If you have enabled Degraded Mode, you can select the Degraded Mode Type — Basic, Advanced.

If you select **Basic**, the user will be allowed/denied entry on the basis of limited checking of credential (that is finger and card) verification, as well as Access Policies will not be checked if configured. For Exit, user will be allowed to exit only after credential are verified. No other checking/verification will be done during exit.

If you select **Advanced**, the user will be allowed/denied entry/exit on the basis of checking the credential (all credentials will be supported) as well as the user details will be verified and checked. However Access Policies will not be checked, if configured.

- **Smart Identification:** For details, refer to [“Smart Identification”](#).
- **Occupancy Control:** For details, refer to [“Occupancy Control”](#).
- **DND Zone:** For details, refer to [“Do Not Disturb”](#).
- **Dead-Man Zone:** For details, refer to [“Dead Man Zone”](#).
- **First IN User Rule:** For details, refer to [“First In User”](#) and [“First In User Assignment”](#).
- **Anti-Pass Back (APB):** For details, refer to [“Anti-Pass Back”](#).
- **2-Person Rule:** For details, refer to [“2 Person Group”](#) and [“2 Person Rule Assignment”](#).

Make sure the Access Control Policies are also enabled in [“Features”](#). The Configuration of the policies will be activated when these are configured from the Access Control module. For details refer to [“Access Control”](#).

Click **Save** once done with the configurations.

Occupancy Control

Click **Zones > Occupancy** and the page appears as shown below.

Setup Configuration **Occupancy Control**

Control Zone ID Name

Access Mode Entry

Action Alarm

Alarm Timer (Sec) 0

Monitor Zone-1 ID Name

Avoid Occupancy Equal To 0

Monitor Zone-2 ID Name

Avoid Occupancy Equal To 0 - 999

Check Conditions For Any One Zone

Add Cancel

Search

Control Zone	Action	Monitor Zone-1	Monitor Zone-2	
No Data				

- **Control Zone:** Click the picklist to select the desired zone, that is the zone whose occupancy is to be controlled.
- **Access Mode:** Select the desired access mode for the Control Zone — Entry, Exit or Both.
- **Action:** Select the desired action to be taken, that is raise an **Alarm** or to **Restrict** access to or from the control zone.
- **Alarm Timer (Sec):** If you have selected **Alarm** as the Action, set the alarm timer in seconds.
- **Monitor Zones:** Click the picklist to select upto 2 zones as **Monitor Zones** i.e. zones whose occupancy shall determine the occupancy of the control zone. These may be same or different from the one as configured in Control Zone.
- **Avoid Occupancy:** Set the occupancy condition for each Monitor Zone — Equal to, Greater than or Less than along with the number you wish to allow. This defines an occupancy condition that must be satisfied in the monitor zone, for an action to be triggered in the Control Zone, such as restricting entry/exit for a user, or generating an alarm (as specified earlier).

Monitor Zone-1 2 Zone-2

Avoid Occupancy Equal To 5

Monitor Zone-2

Avoid Occupancy Equal To Greater Than Less Than 10

Check Conditions For Both Zones

Add Cancel

- **Check Conditions For:** Select the desired option — Both Zones, Any One Zone. The Avoid Occupancy condition will be checked as per the option selected, that is for both monitor zones or for any one monitor zone in order to trigger the specified action in the control zone.

Click **Add** once done with the configuration. The newly added Control Zone is displayed in the grid as shown below.

The screenshot shows a web application window with a green header bar indicating 'Saved Successfully'. Below the header is a search bar labeled 'Search Device ID or Name'. The main content area has three tabs: 'Setup', 'Configuration', and 'Occupancy Control'. The 'Occupancy Control' tab is active, displaying a form for configuring occupancy control. The form includes fields for 'Control Zone' (ID and Name), 'Access Mode' (Entry), 'Action' (Alarm), 'Alarm Timer (Sec)' (0), 'Monitor Zone-1' (ID and Name), 'Avoid Occupancy' (Equal To, 0), 'Monitor Zone-2' (ID and Name), 'Avoid Occupancy' (Equal To, 0 - 999), and 'Check Conditions For' (Any One Zone). At the bottom of the form are 'Add' and 'Cancel' buttons. Below the form is a table with the following structure:

Control Zone ▲	Action	Monitor Zone-1	Monitor Zone-2	
Zone-1	Alarm	Zone-1		

Let us understand this with the help of the following example:.

A manufacturing facility is divided into three zone types - a *Security Cabin* which leads into a *High Security Area (HSA Zone)* within which there are several secure *Sub-Zones (Sub-HSA Zone)* such as storage areas, equipment rooms etc.

The facility has specific security requirements as follows:

Scenario 1

- Condition 1: There must be minimum two occupants in the Security Cabin always.
- Configuration: Here, exit from the Security Cabin has been restricted when occupancy of Security Cabin is less than 3.

The screenshot shows the 'Occupancy Control' configuration window with the following settings:

- Control Zone:** 1, Security Cabin
- Access Mode:** Exit
- Action:** Restrict
- Monitor Zone-1:** 1, Security Cabin
- Avoid Occupancy:** Less Than, 3
- Monitor Zone-2:** (empty)
- Avoid Occupancy:** Equal To, 0
- Check Conditions For:** Any One Zone

At the bottom of the form are 'Update' and 'Cancel' buttons.

Scenario 2

- Condition 2: The security cabin cannot be left unoccupied, when there are people present in the HSA Zone.
- Configuration :Here, exit from the Security Cabin has been restricted when occupancy of Security Cabin is 1 and occupancy of the HSA Zone is greater than 0.

The screenshot shows the 'Occupancy Control' configuration window. It has three tabs: 'Setup', 'Configuration', and 'Occupancy Control' (which is active). The configuration includes the following fields:

- Control Zone:** 1, Security Cabin
- Access Mode:** Exit
- Action:** Restrict
- Monitor Zone-1:** 1, Security Cabin
- Avoid Occupancy:** Equal To, 1
- Monitor Zone-2:** 2, HSA Zone
- Avoid Occupancy:** Greater Than, 0
- Check Conditions For:** Both Zones

At the bottom are 'Update' and 'Cancel' buttons.

Scenario 3

- Condition 3: At a time, any person entering the HSA Zone or any of the Sub-HSA Zones must always be accompanied by a security personnel.
- Configuration: Here, an alarm has been set to be triggered if occupancy of the HSA Zone is 1 for more than a time of 10 seconds. Hence, when the HSA Zone has zero occupancy, the entry of the first occupant should set off the alarm timer till entry of the second occupant. The same can also be configured for each of the Sub-HSA Zones.

The screenshot shows the 'Occupancy Control' configuration window. It has three tabs: 'Setup', 'Configuration', and 'Occupancy Control' (which is active). The configuration includes the following fields:

- Control Zone:** 2, HSA Zone
- Access Mode:** Both
- Action:** Alarm
- Alarm Timer (Sec):** 10
- Monitor Zone-1:** 2, HSA Zone
- Avoid Occupancy:** Equal To, 1
- Monitor Zone-2:** (empty), (empty)
- Avoid Occupancy:** Equal To, 0
- Check Conditions For:** Any One Zone

At the bottom are 'Update' and 'Cancel' buttons.

To know how Occupancy control parameters affect access control functionality, refer to [“Occupancy Control”](#).

Additional

This section lists some additional configurations that can be enabled for Panel Doors.

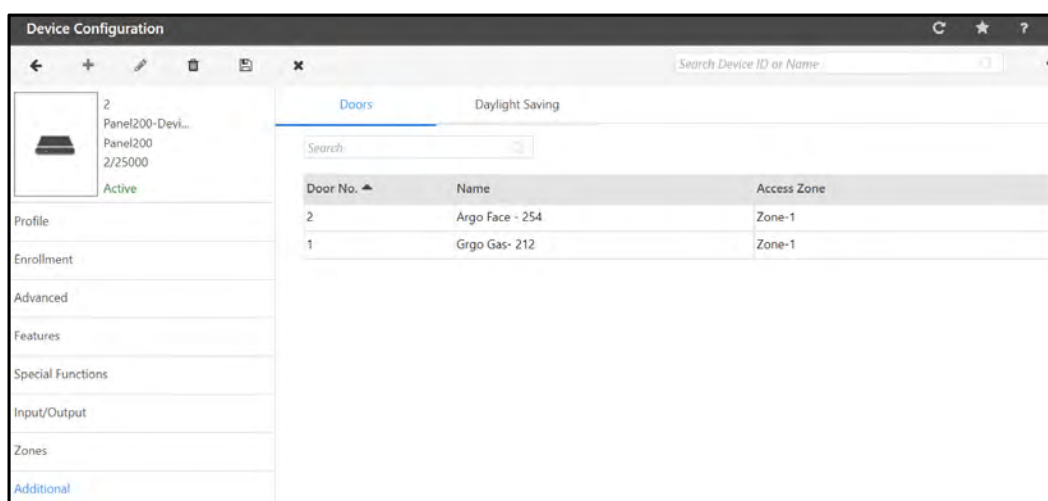
Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. COSEC doors can be configured to be compatible with this procedure keeping the RTC of the system updated with such changes.

Click each link to configure the Additional parameters:

- [“Doors”](#)
- [“Daylight Savings”](#)

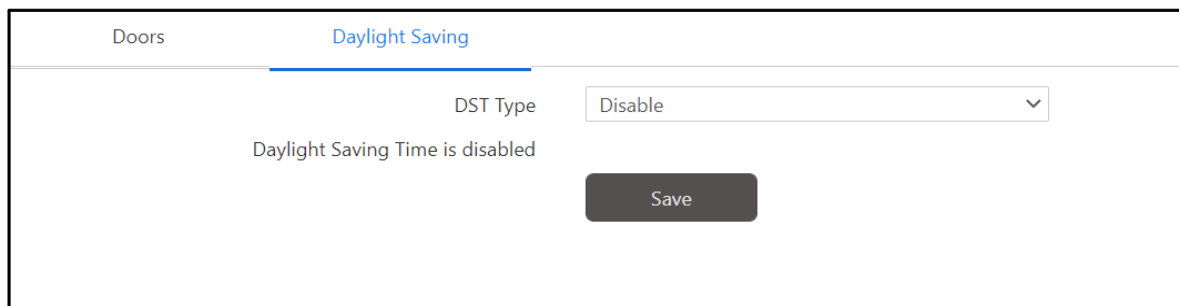
Doors

Click **Additional > Doors** and the page appears as shown below.



Daylight Savings

Click **Additional > Daylight Saving** and the page appears as shown below.



DST Type: Select the desired Daylight Saving configuration type — Disable, Day-Month wise or Date-Month wise.

The screenshot shows the 'Daylight Saving' configuration page. The 'DST Type' dropdown menu is open, displaying three options: 'Disable', 'Day-Month wise', and 'Date-Month wise'. The 'Disable' option is currently selected and highlighted in blue. The text 'Daylight Saving Time is disabled' is visible below the dropdown.

- If you select **Disable** option, DST will not be applicable.
- If you select **Day-Month wise** option, the DST is set by the day of the month on which clock needs to be forwarded and reverted back to normal.
 - Set the **Month**, **Week No.**, **Day of Week**, and **Time** for both the **Forward Clock** and **Backward Clock**.
- If you select **Date-Month wise** option, the DST is set by date of the month on which clock needs to be forwarded and reverted back to normal.
- Set the **Time Period** for the date-month wise DST settings in *24-hours* format, and specify **Month**, **Date** and **Time** for the **Forward Clock** and the **Backward Clock**.

The screenshot shows the 'Daylight Saving' configuration page with the following settings:

- DST Type:** Day-Month wise
- Time Period:** 08:00
- Forward Clock:**
 - Month:** November
 - Week No.:** 1st
 - Day of Week:** Sunday
 - Time:** 09:00
- Backward Clock:**
 - Month:** January
 - Week No.:** 1st
 - Day of Week:** Sunday
 - Time:** 10:00

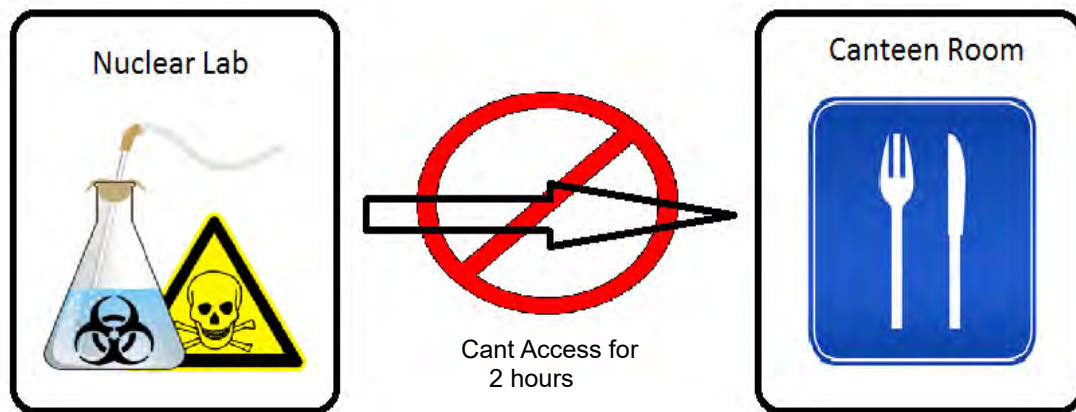
A 'Save' button is located at the bottom of the configuration area.

As per the above configuration, the DST Setting will be applicable on 1st Sunday of November at 09:00 hours, the clock will be forwarded by 08:00 hours. And on 1st Sunday of January at 10:00 hours, the clock will be reversed by 08:00 hours.

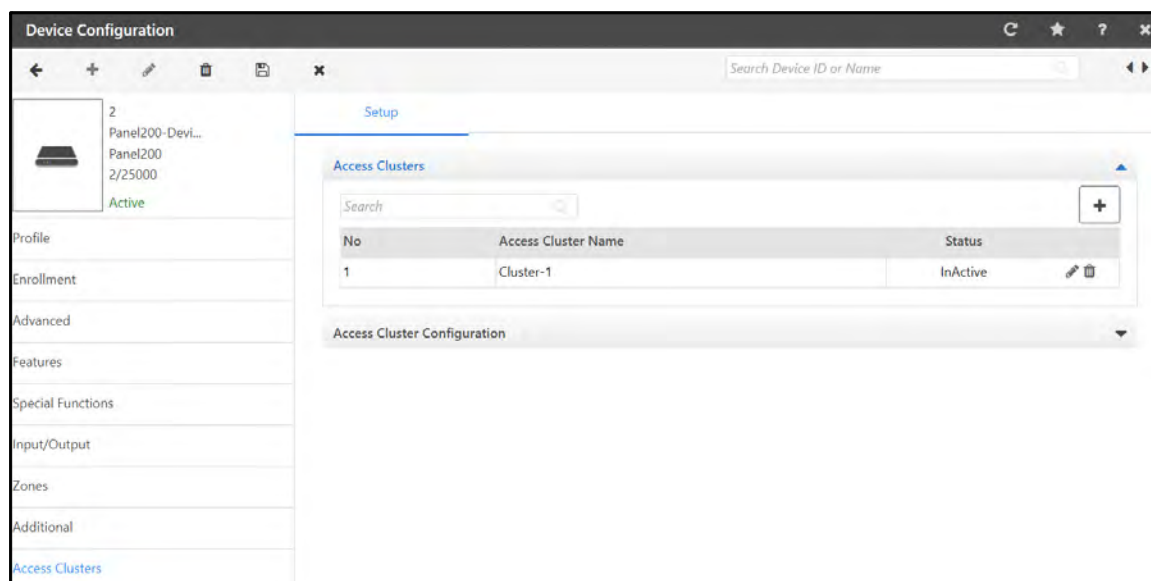
Click **Save** once done with the configurations.

Access Clusters

Access Clusters are door groups that can be created under each panel to restrict or limit access of users to some special regions. Once access clusters are defined under a panel, panel doors can be assigned to specific clusters. For e.g. In some workplaces, such as Chemical factories, once a user goes into a radiation exposed area, he/she must not be allowed in public areas such as the Admin department or the Cafeteria. However, this user will be allowed access to a specific quarantined zone. Such purpose can be served using the access cluster feature whereby, users going into one cluster can be allowed or denied access to other clusters based on configured policies.



Click **Access Clusters > Setup** and the page appears as shown below.



Access Clusters

Click the **Access Clusters** collapsible panel.

Click **Add** to add a new Cluster. You can Upto 75 clusters.

Setup

Access Clusters

Search

No	Access Cluster Name	Status	
	Cluster-2	<input type="checkbox"/>	✓ ✕
1	Cluster-1	InActive	✎ ✕

- **Access Cluster Name:** Assign a name for the new access cluster.
- **Active:** Select the **Active** check box to enable access cluster restrictions for this cluster.

Click **OK**. The cluster appears in the grid.

Access Cluster Configuration

Click the **Access Cluster Configuration** collapsible panel.

Access Cluster Configuration

Access Cluster ID Name

Cluster Mode Allow All

Restriction Duration HH:MM

Save

- **Access Cluster:** Click the picklist to select the desired Access Cluster.
- **Cluster Mode:** Select the desired mode for the selected cluster — **Allow All**, **Deny All**, **Selected**.

Access Cluster Configuration

Access Cluster ID Name

Cluster Mode Allow All

Restriction Duration HH:MM

Allow All
Selected
Deny All

- **Allow All:** Select this option to allow access for all clusters of the Panel.
- **Selected:** Select this option to allow access for selected clusters of the Panel.
 - **Allowed Cluster:** Click the picklist and select the desired clusters.
- **Deny All:** Select this option to deny access for all clusters of the Panel.
- **Restricted Duration:** Define the time period (HH:MM) for which the **Allow/Deny Mode** will be applicable to the cluster.

Click **Save** once done with the configurations.

Door Group

Door Group enables the grouping of Panel Doors belonging to different Zones of corresponding Panel.

Then Man Trap feature can be configured to operate on the basis of Zone OR Group.

Click each link to configure the Door Group parameters:

- [“Setup”](#)
- [“Configuration”](#)

Setup

Click **Door Group > Setup** and the page appears as shown below.

The screenshot shows the 'Device Configuration' window with the 'Setup' tab selected. On the left, a sidebar lists configuration options: Profile, Enrollment, Advanced, Features, Special Functions, and Input/Output. The main area displays the 'Setup' form for a Door Group. The 'Name' field is set to 'Matrix RnD'. Below it, a 'Door' picklist shows a selection of '2'. A table below the picklist shows the selected door: '2' with name 'Argo Face - 254'. At the bottom of the table are 'ADD' and 'Cancel' buttons. Below the table is another empty table with columns 'ID' and 'Name', and a 'No Data' message.

From the Setup, you can create Door Groups and assign multiple Panel Doors to it. Maximum 15 Door Groups can be configured for the selected Panel. Each Door Group can consist of maximum 9 Panel Doors.

- **Name:** Assign a user friendly name to the Door Group.
- **Door:** Click the picklist to select the desired Panel Doors to be added to the group.
- Click **Add** when done with the configurations. The Door Group will be displayed in the grid as shown.

The screenshot shows the 'Device Configuration' window with the 'Configuration' tab selected. A green banner at the top indicates 'Saved Successfully'. The 'Setup' tab is still visible in the sidebar. The main area displays the 'Configuration' form for a Door Group. The 'Name' field is set to 'Name'. Below it, a 'Door' picklist shows a selection of '1'. A table below the picklist shows the selected door: '1' with name 'Matrix RnD'. At the bottom of the table are 'ADD' and 'Cancel' buttons. Below the table is another empty table with columns 'ID' and 'Name', and a 'No Data' message.



At any instance of time a Panel Door can be assigned to only one Door Group.

Configuration

Click **Door Group > Configuration** and the page appears as shown below.

From Configuration, you can enable Man Trap for corresponding Door Group. Also you can enable Strict Man Trap from here. Doing so will allow opening a door only when all other doors of the respective group are closed irrespective of the Man Trap Wait Timer.

- **Door Group:** Click the picklist to select the desired door group for which Mantrap feature is to be enabled

Man Trap



To enable the feature of Man Trap on Door Groups:

- You must enable Man trap Door Interlock from **Features > Set3 > Man Trap Door Interlock** and select **Functioning as “Door Group Based”** as shown below:

The Door Group must be assigned in the Input Group. For details, refer to [“Input/Output”](#).

Enable: Select the **Enable** check box to activate the Man Trap feature.

Enable Strict Man Trap: If you wish to apply Strict Man trap, select this check box.

Click **Save** to save the settings.

MODE Door

The MODE (**M**obile **D**evice) devices are used for Time-Attendance solution in which user can mark the punch by using Face recognition method. MODE Door can be connected as **Direct Door** only.

The Device Configuration page for MODE Door appears as shown below.

Sequence Number - This is a system generated sequence number for each new device.

Device- Specify a name that can be assigned to the Mobile device. The Device ID is auto-generated by the system.

IP Address - This is the IP address assigned to the device. Once the device connection is established, this field will automatically display the door IP address.

UUID- Enter the UUID of the device which is the IMEI number of the Mobile device (Tablet device).

Active - Check the box to activate the device on the network.

To add Devices automatically, go to Admin Module> System Configuration> Global Policy> Device. Enable the "Auto Add New Devices" checkbox. Once the device is connected in network, it will come online in COSEC Monitor.



The Monitor Service must be running while adding the device to COSEC.

*The Auto added MODE device will be **Inactive** by default to avoid misuse of auto-add feature on mobile phones. Make sure you enable the **Active** checkbox in order to connect the device to the network. Once the device is connected to the network, it will come online in COSEC Monitor.*

Once the device is configured, click the **Save** button to save the configuration.

To know more about configuring devices, click on the links for different tabs of Device configuration.

- [*“Profile”*](#)
- [*“Enrollment”*](#)
- [*“Advanced”*](#)
- [*“Video Surveillance”*](#)
- [*“Special Functions”*](#)
- [*“Additional”*](#)
- [*“Assign Users”*](#)
- [*“Identification Server”*](#)

Profile

This section enables the user to set up the basic profile for any new device. Setting up a door profile involves defining basic parameters to set up any device.

Basic

The **Basic** section is shown below:

Optional

The **Basic** page has an **Optional** tab which provides optional configurations as shown below:

- **Site** - Select the site to which this Mobile device is to be assigned from the site pick-list window. Site is created from Devices> Masters> Site.
- **Application** - The application type for which the device is to be used is set as **Basic Access Control**.
- **User/Visitor Access Mode** - This defines the type and combination of credentials required to identify and validate a user at the Mobile device. Select the appropriate credential combination from the drop down list.

The options available are:

- Any one
- Face
- PIN + Face



If FR license is not available then User/Visitor Access Mode will have Any One option only.

- **Alert Messages** - Select this check-box to enable the application to send alerts based on events from this device.
- **Consider for Visitor Pass Surrender**- Check the box to consider the selected device for visitor pass surrender. The Visitor can show his credential on this device to surrender the pass.
- **Access Control through Device**- Enable this check-box if the events coming from the door are to be considered as access control events.



GPS Events generation is supported in the following devices only - Direct Doors (VEGA, ARGO, PATH Controller, ARC DC 200, ARGO FACE) and Panel Doors (ARGO, VEGA, PATH Controller and ARC DC 200).

- **Consider for Attendance**- Select the option as **Attendance** if the events sent by this door are to be considered for Time and Attendance data processing.
- **Alternate Address**: To access MODE from an external network (public network), enter an alternate address. It can be the Device IP Address or the Domain Name.

If MODE is selected for Location1. The IP address (Internal Address) of MODE is 192.168.104.114. The Alternate Address of Door V3 is 173.183.4.11:43.

When the door is accessed from external network then alternate address will be used for communication.

If you are using APTA in the external network at Location1 and tries to access MODE, then it will be accessed through 173.183.4.11:43. In Door API response to APTA, alternate IP address will be sent in response.

The communication between MODE and the external network takes place via device port configured in **Port No. (HTTPS)**.

- **Port No. (HTTPS)**: Enter the Device Port number for secure communication between the device and the external network.

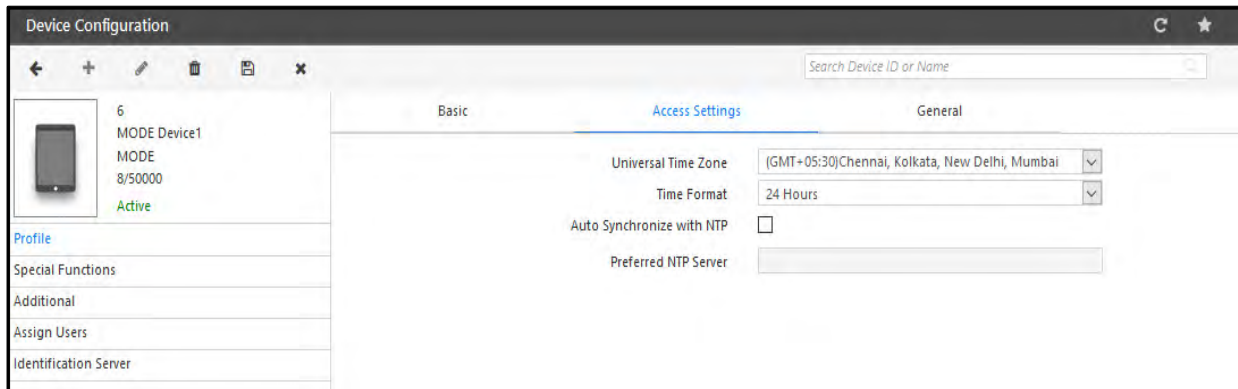


The Device picklist will show active Direct Doors and Panel200 doors (Except ARC IO 800 Panel Door and ARC IO 800 as direct door and MODE).

Consider For	Access Control	
Device *	1	Door V3-Device-1
Alternate Address	173.183.4.11:43	
Event Type	Entry	

Access Settings

The **Access Settings** page appears as shown below:



- **Universal Time Zone** - Select the geographic time zone in which the DOOR will operate.
- **Time Format** - Specifies the time format to be displayed on Door Controller LCD display. The formats available are:
 - 24 Hours
 - 12 Hours

Select the relevant option from the drop down list as per the site requirements.

Auto Synchronize with NTP

If Date and time is to be automatically synchronized as per the **Preferred NTP Server** (predefined or user-defined NTP server address) selected by user, then you must enable **Auto Synchronize With NTP** checkbox.

Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from device webpage, which will be reflected on device display.

- When Auto Synchronization with NTP is disabled Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 1. You can specify the Preferred NTP server of your choice. In this case device will first try to get Date and Time from that server address.
If it does not get Date and Time in three tries; device will check from pre-defined NTP servers.
If you have entered one of the three pre-defined NTP servers(ntp1.cs.wisc.edu , time.windows.com , time.nist.gov); then device will first check that server first.
If it receives updated Date and Time then Updated Date and Time will be reflected on device webpage and display screen.
 2. You can keep the Preferred NTP server as blank. In this case device will check for Date and Time from the first NTP server.
 3. If user has manually entered Date and Time from webpage or Device Menu then those values of Date and Time will be reflected on device webpage and display screen.

In the case of the **Manual** option the administrator can manually update the time on the Door with that of the system time as and when required. This can be accomplished from the COSEC Monitor and control application.

General

The **General** page appears as follows. Enter all general details applicable to the device in this section.

Device Configuration

Search Device ID or Name

28
MODE-Device-2...
MODE
0/50000
Active

Profile
Special Functions
Additional
Assign Users
Identification Server

Basic Access Settings General

Mute Buzzer ☐

Allowed Acknowledgement

Display Duration (ms) 3000
LED - Buzzer Duration Long ⓘ

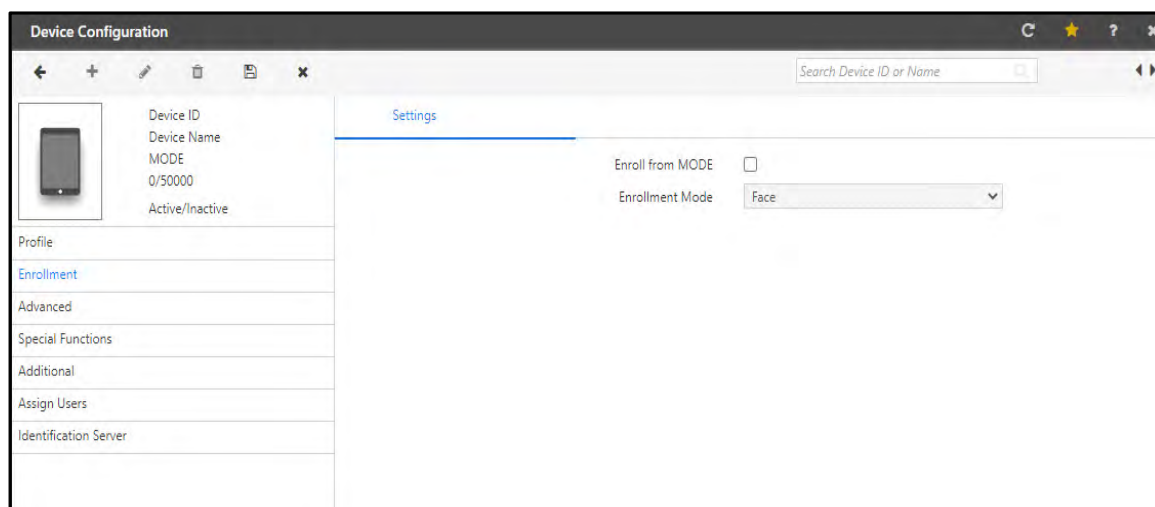
Denied Acknowledgement

Display Duration (ms) 3000
LED - Buzzer Duration Long ⓘ

- **Mute Buzzer** - User can mute or unmute the door buzzer by checking or clearing the box respectively.
- **Allowed Acknowledgement**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgement Allowed' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.
- **Denied Acknowledgement**
 - **Display Duration (ms)** - Define the time duration in between 500 to 3000ms till which the 'Acknowledgement Denied' message will be displayed.
 - **LED - Buzzer Duration** - Select the time duration as Long, Medium or short for the LED Buzzer.

Enrollment

The Enrollment page appears as shown below.



- **Enroll from MODE** - Select this checkbox to enable the enrollment of user from MODE.
- **Enrollment Mode** - The type of credential that can be enrolled using MODE is displayed i.e. Face.

Advanced

The Advanced tab allows the user to configure some advanced parameters such as access control settings.

To access this, After selecting the device, Select the **Advanced** tab from **Device Configuration** page. The advanced settings can be configured from following sections:

- *“Settings”*

Settings

The Advance Settings page for MODE appears on your screen as shown below:

The screenshot shows the 'Device Configuration' window with the 'Settings' tab selected. On the left, a sidebar lists various settings categories: Profile, Enrollment, Advanced (selected), Video Surveillance, Special Functions, Additional, Assign Users, and Identification Server. The main area is divided into two sections: 'Temperature Logging' and 'Face Mask Compulsion'. The 'Temperature Logging' section includes an 'Enable' checkbox, 'Sensor Type' (Web-Based), 'Sensor Interface' (HTTP/S), 'Calibration Parameter' (0.0), 'Approach to Sensor Wait-Timer (Sec)' (3.0), 'Temperature Detection Time Out (Sec)' (10), 'Tolerance between Consecutive Readings' (0.5), 'Consecutive Readings Count within Tolerance' (5), 'Temperature Threshold (°F)' (99.5), 'Minimum Temperature for Access (°F)' (95.0), 'Restriction Type' (Soft), and a 'Bypass If Sensor Disconnected' checkbox. The 'Face Mask Compulsion' section includes an 'Enable' checkbox, 'Approach to Camera Wait-Timer (Sec)' (3.0), 'Mask Detection Time Out (Sec)' (4), and 'Restriction Type' (Soft).

- **Enable GPS Location on IN-OUT Events:** Select the check box to enable GPS location to be received by the Server in Events generated from MODE.



Make sure this check box is selected and Location is turned on in the COSEC MODE App to send GPS coordinates in Events.

GPS Events generation is supported in the following devices only - Direct Doors (VEGA, ARGO, PATH Controller, ARC DC 200, ARGO FACE) and Panel Doors (ARGO, VEGA, PATH Controller and ARC DC 200).

Temperature Logging

- **Enable:** Enable the temperature logging feature on the zone.
- **Sensor Type:** Select the type of thermal sensor integrated in the device. There are three sensors: *Web-Based*.
- **Sensor Interface:** Select the interface on which device will communicate with the sensor.
For Sensor Type: Web-based
Sensor Interface options will be: HTTP/S
- **Emissivity:** Set the emissivity parameter for Sensor. This parameter should only be visible when Sensor Type is AST. Default value is 0.95.
It is used to define accuracy in sensor to detect temperature of different skin or objects.
- **Calibration Parameter:** Set the calibration parameter for the thermal sensor.
On click of + the value should increase by 0.1 and on click of – it should decrease by 0.1.
- **Approach to Sensor Wait-Timer:** Time for which the device will wait for user to approach the device before starting Temperature Detection.

- **Temperature Detection Time-Out:** The timer till which temperature detection will be done for the user and if valid temperatures are not found till the expiry of timer then timeout will be declared.
- **Tolerance between consecutive readings:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature doesn't fall in tolerance range the reference temperature is updated with the current temperature and the process continues.
- **Consecutive readings count within tolerance:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature doesn't fall in tolerance range the reference temperature is updated with the current temperature and the process continues.
- **Minimum Temperature for Access:** The minimum temperature value that should be detected is to be considered as valid temperature.
It should be less than threshold temperature. If user tries to enter a value equal to or greater than threshold temperature validation should be shown.
The default value, unit and range should be updated based on the Temperature unit set on Panel.
- **Temperature Threshold:** To set the threshold value of the temperature. The default value, unit and range can be updated based on the Temperature unit set on Panel.
- **Restriction Type:** To set restriction type as soft/hard.
- **Bypass if Sensor Disconnected:** Enable this check-box to give provision of bypassing the feature if sensor connectivity is lost.

Face Mask Compulsion

Face Mask Compulsion feature is used to enforce users to wear masks while they are within the premises.

After identifying the user, Device will prompt the user to show Face with Mask when "Face Mask Compulsion" is enabled.

Based on identification of Mask, user will be allowed or denied access.

Make sure you have enabled **Enable FR** checkbox in **Devices> Device Configuration> Identification Server> Face Recognition> Enable FR** and configure the below mentioned parameters to avail this feature.

- **Enable:** Select this checkbox to enable Face Mask Compulsion feature for IDS.
- **Approach to Camera Wait-Timer (Sec):** This parameter defines the time within which the user must approach the camera for face mask detection.
 - You must enter the Wait-Time between 0.0-15.0 seconds.
 - By default, it is 3.0 seconds.
- **Mask Detection Time Out (Sec):** This parameter defines the maximum time duration for user's face mask detection.
 - You must enter the detection time out between 0.0-15.0 seconds.
 - By default, it is 4.0 seconds.

- **Restriction Type:** Select the type of restriction to be imposed when the configured policy is violated. Select the desired option - Soft or Hard.
 - **Soft Restriction:** The access will be granted even if the user is identified without wearing a mask; however, an event and a warning are generated that indicates the user has been identified without wearing a mask.
 - **Hard Restriction:** The access will be denied if the user is identified without wearing a mask.

By default it is **Soft Restriction**.



Users face enrollments are dependent on the Visible Face parameter value set by you. To know more, refer "[Face Recognition](#)".

Video Surveillance

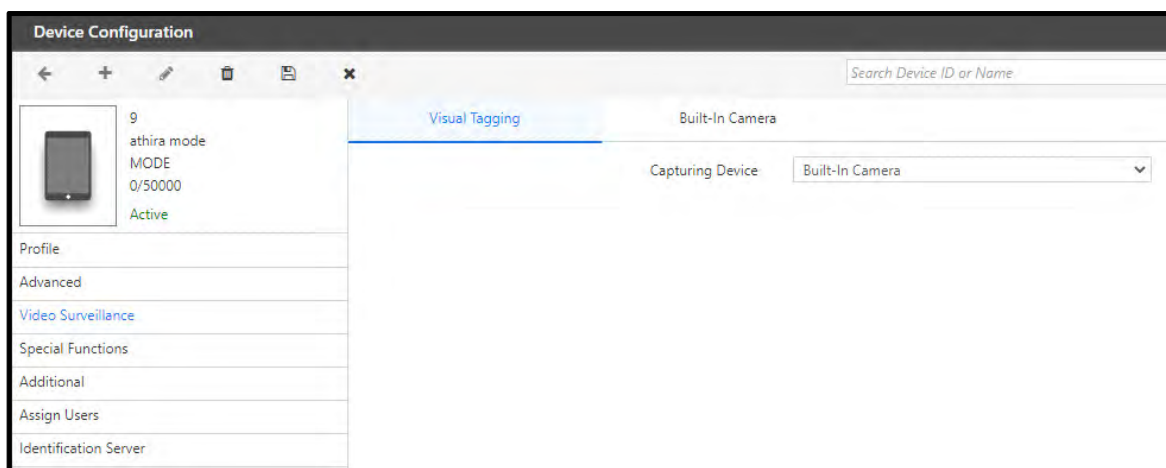
The Video Surveillance tab allows the user to configure parameters for video surveillance integration with the COSEC MODE.

This feature is useful to track if any user accesses using someone else's credentials.

Make sure you have enabled the **Consider for Attendance** checkbox in **Devices> Mode Device Configuration> Profile> Basic> Optional> Consider for Attendance**.

Visual Tagging

The COSEC application can interface with some supported hybrid and network video recording systems and grab images triggered by user events at the Doors. The **Visual Tagging** option enables the administrator to define the video recorder parameters. The **Visual Tagging** page appears as shown below.



Capturing Device: Select the video recording device type from the dropdown list.

- None
- Built-In Camera

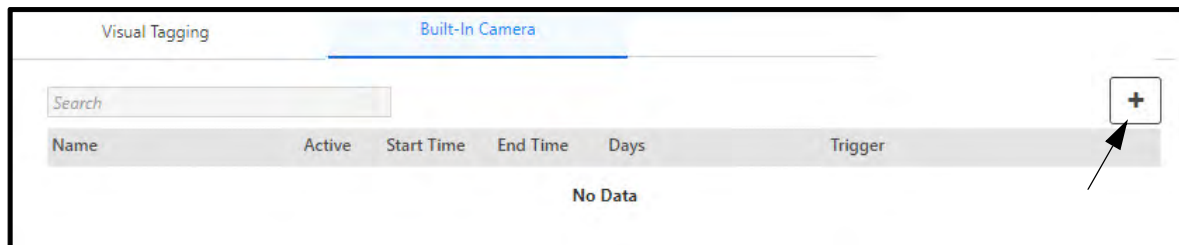
Select the **Built-In Camera** option to schedule the capture configuration.

Built-In Camera

This functionality enables configuration and scheduling of image capturing using the in-built camera of MODE device.

Click the **Built-In Camera** tab.

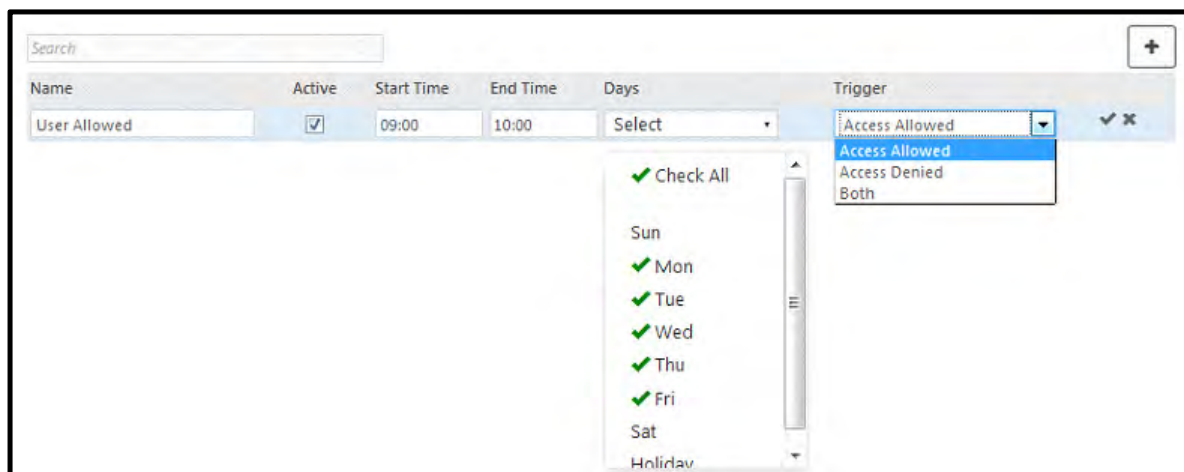
The **Built-In Camera** configuration page appears as shown below.



The Built-In Camera of MODE can be scheduled to capture images during specific periods which will be triggered by specific user events.

To configure the schedule, click **Add** button as shown above.

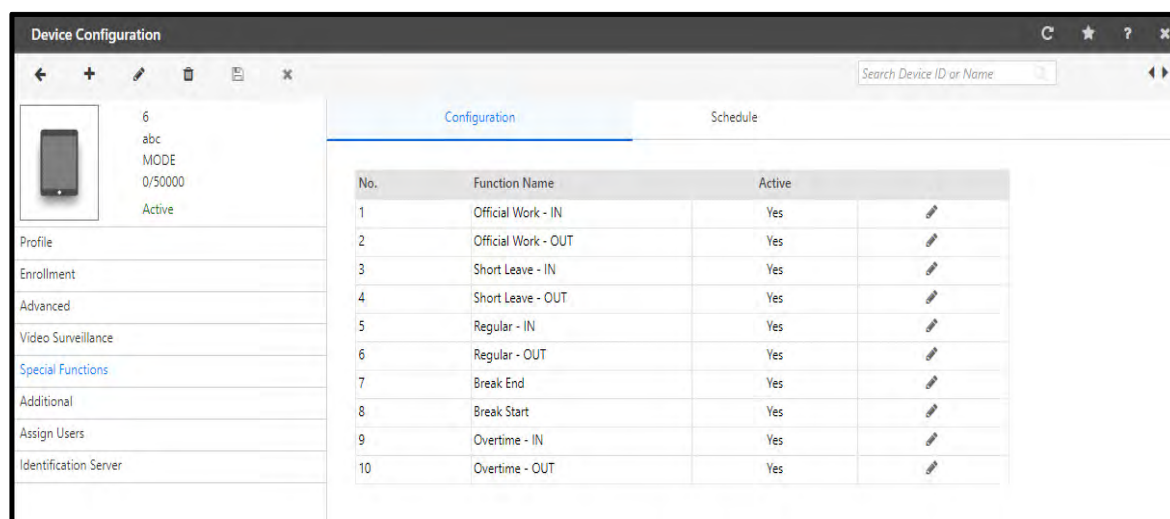
- Specify the function **Name** and select the **Active** check box to enable it.
- Specify the **Start** and **End Time** for the schedule.
- Select the Applicable **Days** for the schedule.
- Select the user events from the dropdown list by which you want image capturing to be **triggered**. The options are Access Allowed, Access Denied and Both.



- Click **OK** button and **Save** button to save the schedule.

Special Functions

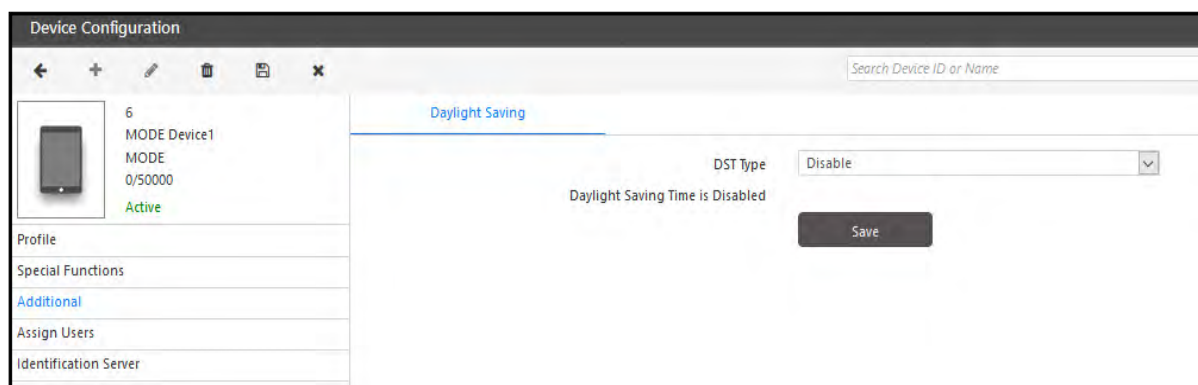
To configure *Special Functions* for COSEC doors, refer to “[Special Functions](#)”.



Additional

This section lists some additional configurations that can be enabled for door controllers.

To access these configurations, Go to **Device Configuration > Additional > Daylight Saving**



Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. COSEC devices can be configured to be compatible with this procedure keeping the RTC of the system updated with such changes.

The **Daylight Saving** configuration can be done in 2 ways i.e. **Day-Month wise** or **Date-Month wise**. The **Disable** option when selected, disables the application of DST on the system time.

On selection of DST type as **Day-Month wise** option, the DST is set by the day of the month on which clock needs to be forwarded and reverted back to normal. Set the month, week number, day of the week, and time for both the **Forward Clock** and **Backward Clock** as shown.

- This DST Setting implies that on 1st sunday of November at 09:00 hours, the clock will be forwarded by 08:00 hours. And on 1st sunday of January at 10:00 hours, the clock will be reversed or backwarded by 08:00 hours.

Device Configuration

Search Device ID or Name

6
MODE Device1
MODE
0/50000
Active

Profile

Special Functions

Additional

Assign Users

Identification Server

Daylight Saving

DST Type: Day-Month wise

Time Period: 08:00

Forward Clock

Month: November

Week No.: 1st

Day of Week: Sunday

Time: 09:00

Backward Clock

Month: January

Week No.: 1st

Day of Week: Sunday

Time: 10:00

Save

On selection of the **Date-Month wise** option, the DST is set by date of the month on which clock needs to be forwarded and reverted back to normal. Specify the **Time Period** for the date-month wise DST settings in **24-hours** format, and specify the day of the week, date and time for the **Forward Clock** and the **Backward Clock** as shown.

Device Configuration

Search Device ID or Name

6
MODE Device1
MODE
0/50000
Active

Profile

Special Functions

Additional

Assign Users

Identification Server

Daylight Saving

DST Type: Date-Month wise

Time Period: 08:00

Forward Clock

Month: November

Date: 1

Time: 09:00

Backward Clock

Month: January

Date: 1

Time: 10:00

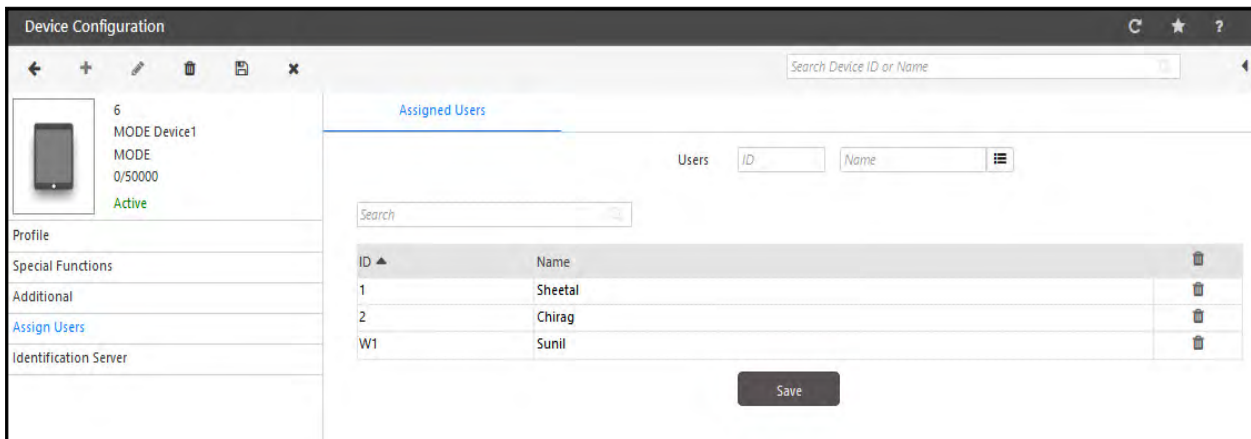
Save

- Click the **Save** button.

Assign Users

To the configured device, you can select and assign the users.

Click the picklist button and select the users.



The screenshot shows the 'Device Configuration' window. On the left, a sidebar lists various tabs: Profile, Special Functions, Additional, Assign Users (highlighted in blue), and Identification Server. The main area is titled 'Assigned Users' and contains a search bar, a 'Users' picklist, and a table of assigned users. The table has columns for ID, Name, and a delete icon. Below the table is a 'Save' button.

ID	Name	
1	Sheetal	
2	Chirag	
W1	Sunil	

- Click the **Save** button to assign all the added users to the selected device.\

Identification Server

This tab enables the selected device to assign the Identification mode as Local or Server Assisted.

Device has a limited memory capacity for storage of templates so we need Identification Server which will store more number of templates and respond to device when asked for identification.

For more information on Identification Servers, See *Admin> System Configuration> Identification Server Configuration*.



If FR license is not available then Identification Server tab will not be available.

To access these configurations, select the **Identification Server** tab.

The screenshot shows the 'Device Configuration' window with a sidebar on the left containing menu items: Profile, Enrollment, Advanced, Special Functions, Additional, Assign Users, and Identification Server. The main area is titled 'Settings' and contains three sections: 'Face Recognition', 'Face Enrollment', and 'Face Anti-Spoofing'. In the 'Face Recognition' section, 'Enable FR' is checked, 'Face Capturing' is set to 'Free Scan', 'Enable Time Out' is checked, 'Free Scan Time Out (Sec)' is 30, 'FR Mode' is 'Local', and 'Identification Time-Out Duration (Sec)' is 4. In the 'Face Enrollment' section, 'Conflict Check' is checked and 'Conflict Matching Threshold (Face)' is 93%. In the 'Face Anti-Spoofing' section, 'Face Anti-Spoofing' is checked, 'Face Anti-Spoofing Mode' is 'Advance', and 'Face Anti-Spoofing Threshold' is 62.00%.

Face Recognition

- **Enable FR:** By default, this check box is enabled, that is Face Recognition feature is enabled in the device. Clear the checkbox to disable.



Make sure “**Enable FR**” flag is checked and “**Consider For Attendance**” flag is enabled in Devices > Device Configuration > Profile > Basic > Optional in order to edit the parameters in Identification Server Settings.

- **Face Capturing:** Select the desired Face Capturing option.
 - **Tap and Go:** If you select this option, user needs to tap on the device screen once. The MJPEG, that is motion recording screen appears. Device will capture and then identify the users face. If during working hours device is idle, then user needs to tap the device to scan the face and gain access.
 - **Free Scan:** If you select this option, the device will display the MJPEG, that is motion recording screen till the expiry of the Free Scan Time Out timer
- **Enable Time Out:** Select this box to enable the time out.
- **Free Scan Time Out (Sec):** Enter the Free scan time out duration. The valid range is 1 to 999 sec. In Free Scan method, multiple users can mark their attendance easily during peak entry hours.

For example, if the Free Scan Time Out is set as 30sec and if the user is identified in 10S then the system reloads the Free Scan Time Out timer again. Hence, device remains in the scanning mode.

- **FR Mode:** Select the FR mode as **Local** or **Server Assisted**.
 - **Local:** In this Local mode Face templates will be stored in FR hardware module which can store 1 lakh face templates. The captured face template will be verified with the templates stored in the FR module.
 - **Server Assisted:** In Server Assisted mode, an identification server and the fields to configure an individual identification server will get enabled as shown below. You must select the Identification server from where the face templates will be identified.

When FR Mode is selected as **Local** below mentioned parameters are to be configured:

The screenshot shows a settings interface with three main sections: Face Recognition, Face Enrollment, and Face Anti-Spoofing. Each section contains several configuration options with checkboxes, dropdown menus, and text input fields.

Section	Parameter	Value
Face Recognition	Enable FR	<input checked="" type="checkbox"/>
	Face Capturing	Free Scan
	Enable Time Out	<input checked="" type="checkbox"/>
	Free Scan Time Out (Sec) *	30
	FR Mode	Local
	Identification Time-Out Duration (Sec)	4
Group FR	<input checked="" type="checkbox"/>	
	Exceptional Face Enrollment	<input checked="" type="checkbox"/>
Face Enrollment	Conflict Check	<input checked="" type="checkbox"/>
	Conflict Matching Threshold (Face) *	93 %
Face Anti-Spoofing	Face Anti-Spoofing	<input checked="" type="checkbox"/>
	Face Anti-Spoofing Mode	Advance
	Face Anti-Spoofing Threshold *	62.00 %

- **Identification Time-Out Duration (Sec):** Enter the duration in seconds after which the face identification will get timed out.
Example: If 5 seconds is specified, then the identification server will try to identify the face till 5 seconds and if not found then it will show time-out to the user.

If you select FR Mode as **Server Assisted**, you must configure the following parameters:

User can either assign a separate or a common Identification Server which is shared by other biometric credentials.

Settings

Face Recognition

Enable FR

☒

Face Capturing

Free Scan

Enable Time Out

☒

Free Scan Time Out (Sec) *

30

FR Mode

Server Assisted

Identification Server

ID

Name

Configure Alternate Server Address

☐

Server Address

Server Port

11005

Identification Time-Out Duration (Sec)

4

Group FR

☒

Exceptional Face Enrollment

☒

Adaptive Face Enrollment

Adaptive Face Enrollment

☒

Threshold Deviation (Face)

02.0

%

Multi-User Matching Score Deviation (Face)

02.0

%

Confirm Before Adaptive Face Enrollment

☒

Face Antispoofing

Face Anti-Spoofing

☒

Face Anti-Spoofing Mode

Advance

Face Anti-Spoofing Threshold *

58.50

%

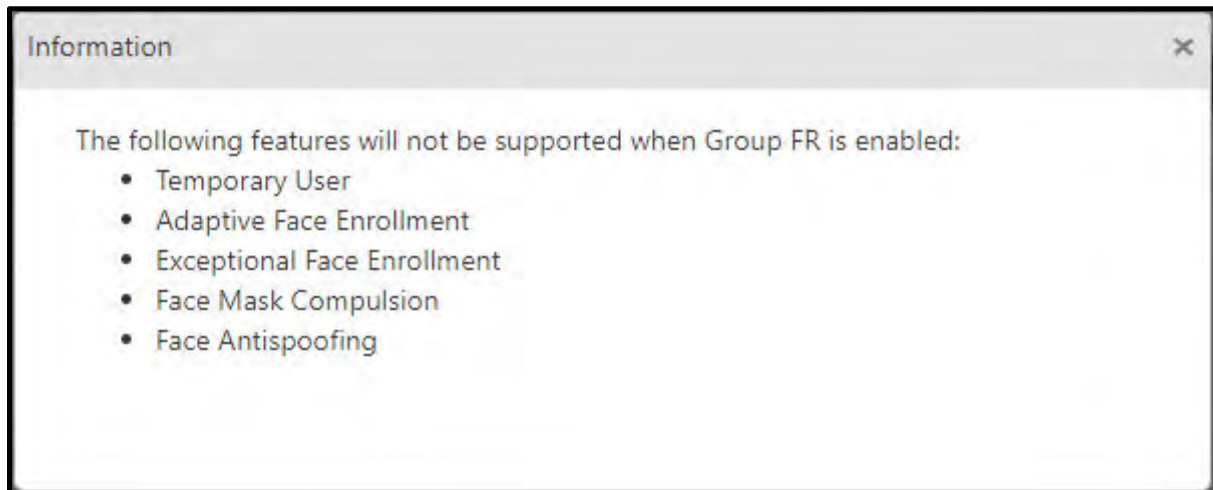
Default Biometric Group No.

0

- **Identification Server:** Select the Identification server from the picklist to which the device is to be assigned to save the records.
- **Configure Alternate Server Address:** Select this check box to configure external IP address of Identification Server.
- **Server Address:** By default, this is a non-editable field by which will display the configured Identification Server for FR. This field allows user to enter the Alternate IP Address for FR if **Configure Alternate Server Address** is enabled.
- **Server Port:** Enter the TCP port number. The default port number is 11005.

- **Identification Time-Out Duration (Sec):** Specify the duration in seconds after which the face identification will get timed out.
Example: If 5 seconds is specified, then the identification server will try to identify the face till 5 seconds and if not found then it will show time-out to the user.
- **Group FR:** Select this checkbox to enable face recognition feature for multiple users and mark their attendance at the same time via this door.

Once you enable Group FR, a pop-up will be displayed as shown below:



The features listed in the pop-up will not be functional.

- **Exceptional Face Enrollment:** Select this checkbox to enroll exceptional faces of users via this door.



For Group FR ("**Mark Group Attendance**") and **Exceptional Face Enrollment** feature to work, ensure that the desired **Identification Service** is selected in **COSEC Admin > License and Service**. For more details refer **Admin Management Portal User Manual**.



If you have enabled the **Exceptional Face Enrollment** feature then make sure that you schedule a task of **Delete Exceptional Face** in **Admin > System Utilities > Task Scheduler** to avoid storage of excess data in the database.

Face Enrollment



If the **FR Mode** is **Server-Assisted** and you wish to enroll faces from the device, make sure **Enable Face Recognition** is selected in **Users > User Configuration > Face Recognition** and/or **Visitor Management > Visitor Profile > Face Recognition** and/or **Contract Worker Management > Worker Profile > Face Recognition**.

- **Conflict Check:** Select the checkbox for the system to check the conflict between the new face of a user and the already (existing) enrolled faces of all the users (available in the database) during the face enrollment process.
- **Conflict Matching Threshold:** Enter the desired Conflict Matching Threshold value in percentage.

The system will consider this value while comparing the face with the face templates already present in the database.

If a conflict is found, that is, if the system detects a face template in the database similar to the new face, then a conflict error will be displayed.

Make sure a higher value is set for this parameter, as it will result in less equivalent matches with the face templates available in the database.



Make sure the *Conflict Matching Threshold* is set lower than *Matching Threshold* in *Admin module > System Configuration > Identification Server Configuration*.

Example: Face Enrollment of Suresh

- **Conflict Check** checkbox is selected.
- **Conflict Matching Threshold** is set as 93%.

Now during the face enrollment of Suresh, the system will check in its database if his face matches with faces of other users available in the database.

- **Case 1:** If Suresh's face matches 92% with Ram, then the system will allow to enroll Suresh's face.
- **Case 2:** If Suresh's face matches 94% with Shyam, then the system will display the conflict error while enrolling Suresh's face.

Adaptive Face Enrollment

When **FR Mode** is set as **Server Assisted Mode**, configure the following parameters:

- **Adaptive Face Enrollment:** Select this check box to Enable adaptive face enrollment for identification server.
 - Adaptive face enrollment provides automatic real time face enrollment whenever change is experienced in facial features.
 - Enabling adaptive enrollment process parameter, an additional slot will be provided internally to store 10 more face templates of a user.
 - IDS will learn from face recognized, adapt and would take decision of storing new template of a user database.

If you enable adaptive face enrollment, you must configure the following parameters.

- **Threshold Deviation (Face):** Enter the value of deviation from matching threshold in percentage. Based on the value entered for deviation, template for Adaptive Face Enrollment will be decided.

Example: If deviation entered is 3% and matching threshold is 98% then it will classify template which has matching score between 98 - 95 and one lower than this will be classified below margin.

- **Multi-User Matching Score Deviation (Face):** Enter the value of deviation from matching score between 2 different users while Adaptive Face Enrollment.

Difference between matching scores of templates will be done, when we have templates of two or more users falling under above specified deviation.

Let us understand this with the help of the following example:

- *Threshold value = 98%*
- *Threshold Deviation= 3%*

So, Result will display all matching templates having matching score between range 98 to 95

- *Multi-user Matching score deviation = 0.5%*

If, 5 best templates of 2 users fall between 98 -95% range

User	Matching Score
User 1	97.8
User 1	97.6
User 1	97.4
User 2	97.25
User 2	97

As we have obtained templates of 2 users in which user 1 is having template of highest matching score, so will make a difference between lowest score template of user 1 and highest matching score template of user 2.

97.4 - 97.25 = 0.15; this is less than 0.5

As difference is less than 0.5, user 1's template having matching score 97.8 for adaptive enrollment will not be used.

- Threshold Deviation and Multi-user Matching score deviation will act as two filters to fetch appropriate template for adaptive enrollment. Values can be added in decimal.



We recommend to set the multi-user matching score deviation higher always e.g.2.0 to reduce the probability of enrolling a particular user's face template in some different user's enrolled faces.

- **Confirm before Adaptive Face Enrollment:** Select this check box, if face enrolled using Adaptive face enrollment requires confirmation from User.



Faces enrolled under Adaptive enrollment process will be synced automatically, but when IDS is restarted due to any reason, the adaptive faces which are not synced will be removed by default.

Face Antispoofing

- **Face Anti-Spoofing:** To use this feature, make sure **Enable FR** checkbox is selected.

Then, select the **Face Anti-Spoofing** check box to enable this feature and configure the following parameters:

- **Face Anti-Spoofing Mode:** Liveness Detection helps to limit the fierce risk of spoofing attacks by using several anti-spoofing approaches. Along with the configurations to be done for Face Anti-Spoofing you also need to take care of the recommended settings for liveness verification and for face recognition, refer ["Recommendations for Liveness Verification"](#) and ["Recommendations for Face Recognition"](#).

Select the Face Anti-Spoofing Mode for liveness detection from the following:

1. **Basic:** This mode detects face as well as photos from the mobile phones.

Select this option when the distance between Camera and Face is more than 3 feet

2. **Moderate:** This mode analyzes the texture of face.

Select this option when the distance between Camera and Face is less than 2 feet

3. **Advance:** This mode combines the features of **Basic Mode** and **Moderate Mode** of Face Anti-Spoofing.

Select this option when the distance between Camera and Face is more than 1 feet and less than 2 feet.

By default, Face Anti-Spoofing Mode will be **Advance**.

If **FR Mode** is selected as Server Assisted, select the Face Anti-Spoofing Mode for detection from the following:

1. **Moderate:** This mode analyzes the texture of face. Select this option when the distance between Camera and Face is less than 2 feet

2. **Advance:** Select this option when the distance between Camera and Face is more than 1 feet and less than 2 feet. By default, Face Anti-Spoofing Mode will be **Advance**.

- **Face Anti-Spoofing Threshold:** Enter the Face Anti-Spoofing threshold value in percentage within the range from 1.00 to 99.99 to identify user's face liveness for considering him/her as genuine person.
- **Default Biometric Group No.:** When FR Mode is selected as Server Assisted, enter the default biometric group number to be assigned to the device. It is a number allotted to a device to be assigned to the Identification Server. This enables the Identification Server to match the template against only those devices that belong to the corresponding biometric group. This reduces the false detection as well time to search template.



When FR Mode is selected as Server assisted, then the Adaptive Enrollment feature can be configured in Admin> System Configuration> Identification Configuration.

In Local Mode Adaptive Enrollment feature is not supported.

ARGO FACE Door

Matrix COSEC ARGO FACE is a powerful Face Recognition Device powered by Matrix's advanced AI-based Deep Learning algorithms to offer superior Face Recognition performance. The COSEC ARGO FACE is an all-integrated, compact, elegant and robust Face Recognition Device specifically designed for enterprise-grade People Mobility applications. Loaded with versatile functions and a range of features, COSEC ARGO FACE is an ideal solution for organizations requiring accuracy, speed, ease of use and security.

ARGO FACE comes with built-in facial recognition and liveness detection support for Access Control, Time Attendance & Cafeteria. It consists of POE terminal with Ingress Protection (IP65 rated) and IK08 protection. It has an elegant design with graphical display. It supports Face, Card, PIN and BLE credentials.

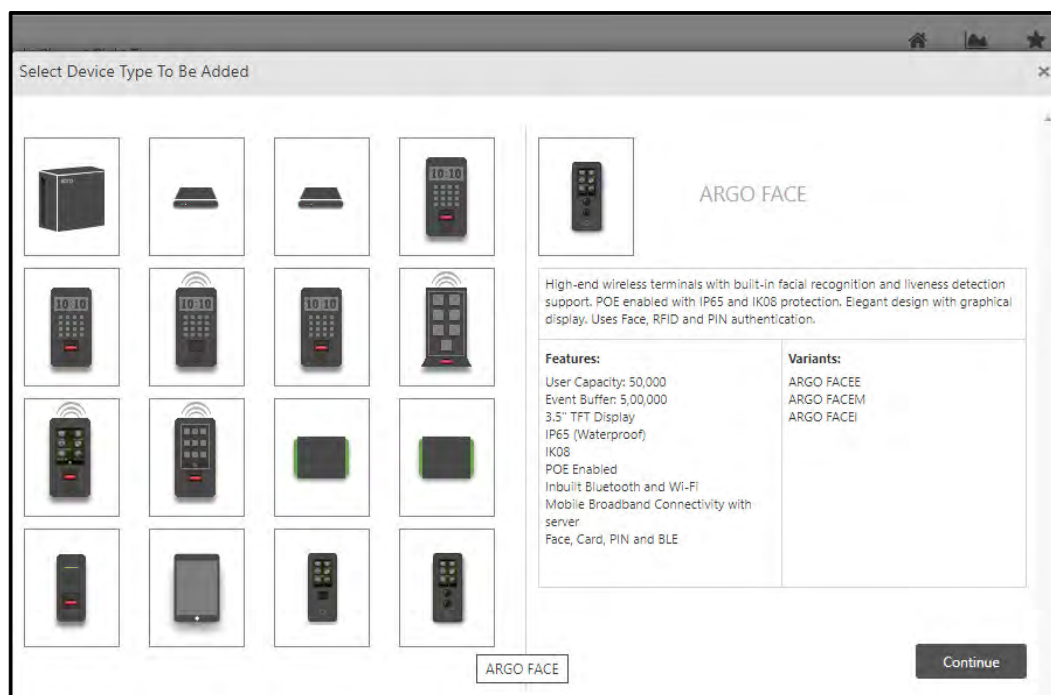
There are in total 3 variants of ARGO FACE door. They are:

Variants	Reader Supported
COSEC ARGO FACEE	EM Prox
COSEC ARGO FACEM	MiFare
COSEC ARGO FACEI	HID iClass

ARGO FACE can be connected as **Direct Door** as well as **Panel Door**.

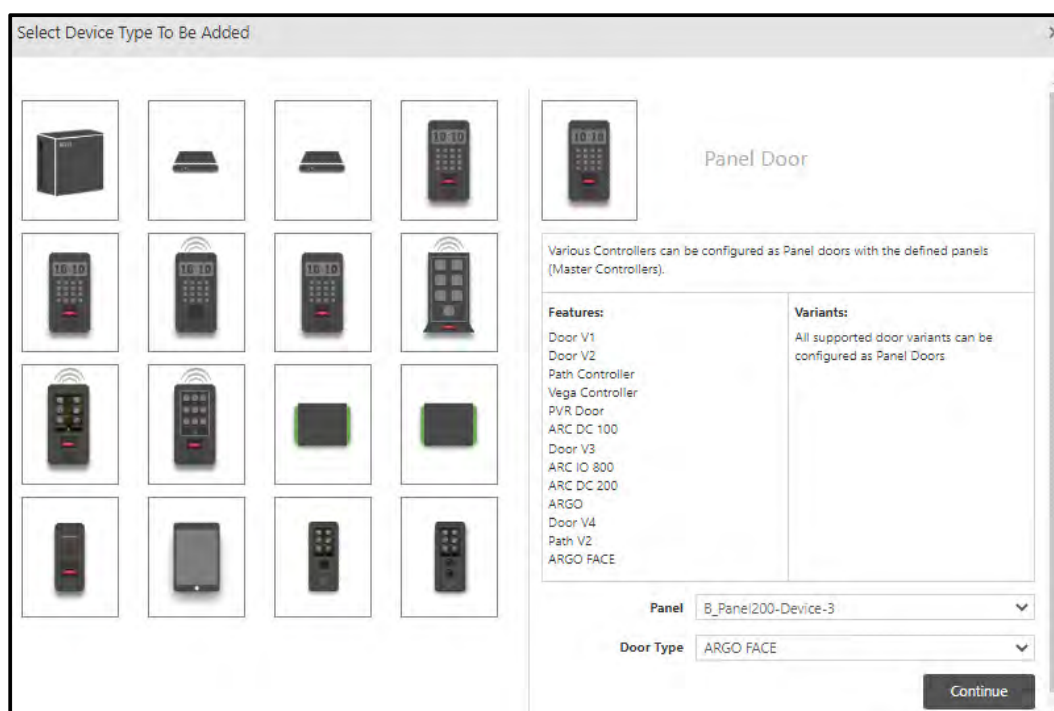


Click the ARGO FACE device from the Device List to add it as a **Direct Door**.



OR

Click Panel Door to add ARGO FACE device as a **Panel Door**.

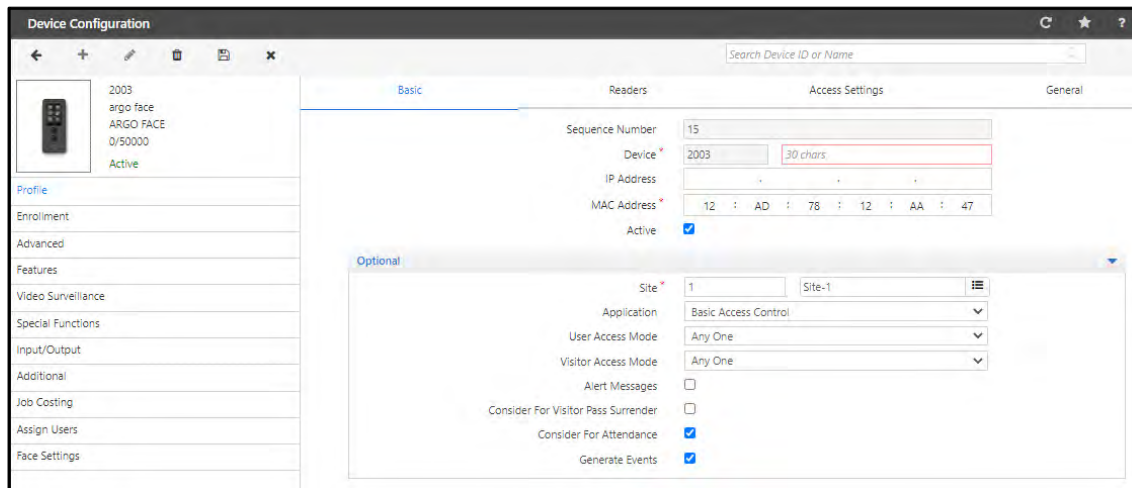


Panel: Select the desired Panel from the drop-down list with which you wish to connect the Door.

Door Type: Select **ARGO FACE** from the drop-down list.

Click **Continue**.

The **Device Configuration** page for ARGO FACE Door appears.



The screenshot displays the 'Device Configuration' window for an 'ARGO FACE' device. On the left, a sidebar lists various configuration tabs: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Face Settings. The 'Basic' tab is selected, showing fields for 'Sequence Number' (15), 'Device' (2003), 'IP Address', and 'MAC Address' (12 : AD : 78 : 12 : AA : 47). Below these, an 'Optional' section contains settings for 'Site' (1), 'Application' (Basic Access Control), 'User Access Mode' (Any One), 'Visitor Access Mode' (Any One), 'Alert Messages' (unchecked), 'Consider For Visitor Pass Surrender' (unchecked), 'Consider For Attendance' (checked), and 'Generate Events' (checked).

To add Devices automatically, click Admin Module> System Configuration> Global Policy> Device. Select the “Auto Add New Devices” check box. Once the device is connected in the network, it comes online in COSEC Monitor.



While adding the device to COSEC Server, make sure the COSEC Monitor Service is running.

To know more about configuring the device, click on the links for different tabs of Device configuration.

- [“Profile”](#)
- [“Enrollment”](#)
- [“Advanced”](#)
- [“Features”](#)
- [“Video Surveillance”](#)
- [“Special Functions”](#)
- [“Input/Output”](#)
- [“Additional”](#)
- [“Job Costing”](#)
- [“Assign Users”](#)
- [“Cafeteria”](#)
- [“Face Settings”](#)

Profile

The screenshot shows the 'Device Configuration' window with the 'Profile' tab selected. The left sidebar lists various configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Face Settings. The main area is divided into 'Basic' and 'Optional' sections. The 'Basic' section includes fields for Sequence Number (15), Device (2003), IP Address, MAC Address (12, AD, 78, 12, AA, 47), and an Active checkbox. The 'Optional' section includes Site (1), Application (Basic Access Control), User Access Mode (Any One), Visitor Access Mode (Any One), Alert Messages, Consider For Visitor Pass Surrender, Consider For Attendance, and Generate Events.

Section	Field	Value
Basic	Sequence Number	15
	Device	2003
	IP Address	
	MAC Address	12, AD, 78, 12, AA, 47
	Active	<input checked="" type="checkbox"/>
Optional	Site	1
	Application	Basic Access Control
	User Access Mode	Any One
	Visitor Access Mode	Any One
	Alert Messages	<input type="checkbox"/>
	Consider For Visitor Pass Surrender	<input type="checkbox"/>
	Consider For Attendance	<input checked="" type="checkbox"/>

This section enables the user to set up the basic profile for any new device. Setting up a door profile involves defining basic parameters to set up any door controller device.

To do this, on the **Device Configuration** page, click the **Profile** tab in the left pane. To configure the Profile parameters click the following links:

- [“Basic”](#)
- [“Readers”](#)
- [“Access Settings”](#)
- [“General”](#)

Basic

The **Basic** section appears on your screen as shown below.



Sequence Number, Device, IP Address, MAC Address and Active are applicable for both Direct Door and Panel Door.

For ARGO FACE as a **Direct Door**,

Configure the following options:

- **Sequence Number:** This is a system generated sequence number for each new device.
- **Device:** Specify a name that can be assigned to the door. The Door ID is auto-generated by the system.
- **IP Address:** This is the IP address assigned to the door. Once the device connection is established, this field will automatically display the door IP address.
- **MAC Address:** Enter the MAC Address of the door.



MAC address of door is required while manually adding the door to the COSEC Monitor. Note the MAC address from the device when it is powered on.

- **Active:** Select the check box to activate the device in the network.



*To add the Device automatically, click Admin Module> System Configuration> Global Policy> Device. Enable the **Auto Add New Devices** check box.*

*The device will be added automatically but make sure you enable the **Active** check box in order to connect the device to the network. Once the device is connected to the network, it will come online in COSEC Monitor.*

Click the **Optional** collapsible tab, to configure the parameters:

- **Site:** Click the picklist and select the site to which this door is to be assigned. Site is created from **Devices> Masters> Site**.

- **Application:** Select the type of application for which the device is to be used. Options are — **Basic Access Control, Advanced Access Control** and **Cafeteria**. All devices set to **Cafeteria** will subsequently be available for Cafeteria configuration.
- **User/Visitor Access Mode:** Defines the type and combination of credentials required to identify and validate a user at the Door Controller. Select the appropriate credential combination from the drop-down list. The options are
 - Any one
 - Card
 - Card + PIN
 - None
 - Face
 - Card+ Face
 - PIN + Face
- **Cafeteria Face Access Mode:** When Application option is set as '*Cafeteria*', only then this configuration is available to the Admin and to add provision of using face as a credential to make transactions on cafeteria devices.

Select the mode type from the drop-down list to allow a user to choose multiple menu items and upon checkout do transactions using face as credential.

The options available are **None, Default Item** and **Item Selection**.

Default Item: This mode in cafeteria will allow users a touch-less cafeteria experience. In Default Item mode only the transaction for default item is allowed. A default item is assigned in each scheduled menu.

- **Item Selection:** This mode in cafeteria will allow users to select the desired menu items and make a transaction using Face as a credential.
- **Alert Messages:** Select this check box to enable the application to send alerts based on events from this door.
- **Consider for Visitor Pass Surrender:** Select this check box to consider the selected device for visitor pass surrender. The Visitors can show their credentials on this device to surrender their passes.
- **Consider for Attendance:** Select this check box if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as Access Control events.
- **Generate Events:** By default, this check box is selected. Click to disable, if the server is not required to receive any events from the this device.

For ARGO FACE as a **Panel Door**.

The screenshot displays the configuration interface for an ARGO FACE device, specifically for a Panel Door. The interface is divided into three tabs: 'Basic', 'Readers', and 'General'. The 'Optional' section is expanded, showing various configuration parameters. The 'Basic' tab is currently selected, and the 'Optional' section is expanded. The 'Readers' tab is also visible, showing the 'Sequence Number' (4) and 'Device' (3). The 'General' tab is visible, showing the 'IP Address' (192.168.103.91) and 'MAC Address' (00:1B:09:09:D8:B0). The 'Optional' section includes the following parameters:

- Site:** A picklist showing '1' and 'Site-1'.
- Consider For Attendance:** A checked checkbox.
- Alert Messages:** An unchecked checkbox.
- Access Zone:** A dropdown menu showing 'Zone-1'.
- Access Cluster:** A dropdown menu showing 'Cluster-1'.
- Door Group:** A dropdown menu showing 'None'.
- Auto IP Assignment:** A checked checkbox.

Click the **Optional** collapsible panel, to configure the parameters:

- **Site:** Click the picklist and select the site to which this door is to be assigned. Site is created from Devices> Masters> Site.
- **Consider for Attendance:** Select this check box if the events sent by this door are to be considered for Time and Attendance data processing. If this option is disabled, then the system would consider all events coming from the door as Access Control events.
- **Alert Messages:** Select this check box to enable the application to send alerts based on events from this door.
- **Access Zone:** Assign an access zone to the door by selecting the desired zone from the drop-down list.
- **Access Cluster:** Assign an access cluster to the door by selecting the desired access cluster from the drop-down list
- **Door Group:** The Door Group drop-down includes the list of all configured Door Groups on the corresponding Panel. An additional option as 'None' is available and selected by default.
- **Auto IP Assignment:** There is an option where the panel door can be assigned its IP from the device webpage. To enable this option, select the Auto IP Assignment check box.



Access Zone is configured while configuring Panel200.

Readers

Readers are important hardware components in a biometric door device. They may be internal or external. This section enables the administrator to configure both internal and external readers for a door as shown below.

The screenshot shows the 'Device Configuration' window with the 'Readers' tab selected. The left sidebar contains a list of configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, and Face Settings. The main area is divided into sections for 'Internal Readers' and 'External Readers'. Under 'Internal Readers', there are settings for 'Door Mode Selection', 'Prompt Special Function', and 'Auto Detect Readers', each with a checkbox. Below these are dropdowns for 'Mode' (set to 'Entry') and 'Card Reader Type' (set to 'None'). A table lists internal readers with columns for 'Member No.', 'Card Format', and 'Configurable Bits'. The first entry is '1' with 'Default Format' and '0' bits. Below the table are settings for 'Enable Scheduling', 'Reader Mode Schedule' (with 'ID' and 'Name' dropdowns), 'Advertise Bluetooth', 'Bluetooth Name', and 'Bluetooth Range' (set to 'Medium (5m - 7m)'). The 'External Readers' section is currently empty. At the bottom, there is a checkbox for 'Access Control On Exit Mode'.

Click the **Reader** tab and configure the following parameters:



Door Mode Selection, Prompt Special Function and Auto Detect Readers are applicable for Direct Door only.

- **Door Mode Selection:** Select the check box, if you want the user to select the punch type as IN or OUT while punching on the device.

E.g: When a door is in Entry mode, your punches will always be in Entry side. But if you want to mark the punch in exit mode then you can select the door mode if “Door Mode Selection” is enabled.

If not selected, user will need to enable Scheduling to set reader mode of door as entry or exit as per user-defined schedules. For information on creating Reader Mode Schedules, refer **Devices > Masters > Reader Mode Scheduler**.

- **Prompt Special Function:** This will provide selection of special function on device screen and based on the selection of particular type of special function, job codes for JPC user will be prompted.

This can be enabled only when Door Mode Selection is enabled.

- **Auto Detect Readers:** Select this check box to enable auto detection of Readers on the door controller connected to the server.

Internal Readers

This option allows the configuration for the Internal Reader of the selected door.

Click **Internal Readers** collapsible panel and configure the following parameters.



Mode, Card Reader Type and Card Format are applicable for both Direct Door and Panel Door.

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop-down list.
- **Card Reader Type:** Select the desired Card Reader Type from the drop- down list.
- **Card Format:** Single or multiple card formats can be assigned to the readers of the door. The default card format is assigned to device as shown in the grid. If no other card format is assigned to device; then this default format will be applied.



The formatting of card is described in Devices> Master> Card Format.

Multiple Card Format

- To assign multiple card formats to device click **Add**. Then click the picklist to select the desired card format and click **OK** to save the format.

Member No ▲	Card Format	Configurable Bits
1	Default Format	0

Member No ▲	Card Format	Configurable Bits
1	Default Format	0
2	Format1	0

- Similarly, you can add maximum 5 card formats. When the card format is saved, the Configured bits of that format as configured from Masters> Card format will be displayed here. Multiple Card format configurations will be sent by the server to the door separated by '**Format ID**' that is 'Member No.' along with all other format related parameters.

Member No ▲	Card Format	Configurable Bits
1	Default Format	0
2	Format1	26
3	Format2	32



Enable Scheduling and Reader Mode Schedule are applicable for Direct Door only.

- **Enable Scheduling:** Select the check box to enable automated control of an Internal Reader. This will set reader mode of door as entry or exit as per user-defined schedules.
- **Reader Mode Schedule:** Click the picklist and select the schedule which is to be assigned to the internal reader of ARGO FACE Door. With this the same reader can be configured to function both in Entry as well as Exit mode based on scheduled timings.



For configuring Reader Mode Schedule refer Devices> Masters> Reader Mode Scheduler.



Advertise Bluetooth, Bluetooth Name and Bluetooth Range are applicable for both Direct Door and Panel Door.

- **Advertise Bluetooth:** Select this check box to enable Bluetooth of the device by which the device will be visible to others. Then configure the following parameters:

- **Bluetooth Name:** By default, if the Device Name is configured then it will be displayed here along with the Mode. The prefix will be the Device Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the bluetooth name as per your requirement. The Bluetooth Name can be a maximum of 10 characters.

- **Bluetooth Range:** The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the bluetooth range as — Short (1m-2m), Medium (5m-7m) or Long (>8m).

- Click **Save**.

External Readers

This option allows you to configure the External Reader for the selected door.



Mode, External Reader Type, Card Format and Exit Switch are applicable for both Panel Door and Direct Door.

Click **External Readers** collapsible panel and configure the following parameters.

Mode: Exit

External Reader Type: None

Search:

Member No	Card Format	Configurable Bits
1	Default Format	0

Exit Switch: ☐

User Access Mode: Any One

Visitor Access Mode: Any One

Access Control On Exit Mode: ☐

- **Mode:** Select the Mode as **Entry** or **Exit** from the drop-down list.
- **External Reader Type:** Select the desired type of External Reader from the drop-down list.



If you are using PIN-W Reader; user's will be able to change their PIN number from the devices.



User Access Mode, Visitor Access Mode and Access Control on Exit Mode is applicable for Direct Door only.

- **Exit Switch:** Select this check box to enable the use of **Exit Switch**.
- **User/ Visitor Access Mode:** Select the access mode from the options:
 - Any One
 - Card
 - None
 - BLE
 - Card + PIN
- **Card Format:** Select a card format to be applicable for external readers of the device. This is applicable for all Direct Doors and all Panel Doors. For multiple format description refer "[Multiple Card Format](#)".

Bluetooth parameters are configurable for both Direct Door as well as Panel Door.

The screenshot shows the 'External Readers' configuration interface. At the top, there are dropdown menus for 'Mode' (set to 'Exit') and 'External Reader Type' (set to 'CB U Reader'). Below these is a search bar and a table with the following data:

Member No	Card Format	Configurable Bits
1	Default Format	0

Below the table, there are several configuration options:

- Exit Switch:** Checked (blue square).
- Configure Bluetooth From Server:** Checked (blue square).
- Advertise Bluetooth:** Not checked (empty square).
- Bluetooth Name:** An empty text input field.
- Bluetooth Range:** A dropdown menu set to 'Medium (5m - 7m)'.

- **Configure Bluetooth from Server:** When you select External Reader Type as — CB U Reader, ATOM RD300, ATOM RD200 or ATOM RD100, select Configure Bluetooth from Server check box to enable Bluetooth feature of aforementioned readers.

Once you enable Configure Bluetooth from Server, configure the following Bluetooth parameters:

- **Advertise Bluetooth:** Select this check box to enable Bluetooth of the device by which the device will be visible to others. Then configure the following parameters:
 - **Bluetooth Name:** By default, if the Device Name is configured then it will be displayed here along with the Mode. The prefix will be the Device Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the bluetooth name as per your requirement. The Bluetooth Name can be a maximum of 10 characters.

- **Bluetooth Range:** The system supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

- **Access Control On Exit Mode:** Select this check box to enable the checking of the following access control policies on the door when the external reader is in the 'Exit' mode.
 - User enabled
 - User validity
 - Blocked user
 - Time Based Access Check
 - ASC
 - User Access Group

Access Settings



Access Settings are applicable for Direct Door only.

Click the **Access Settings** tab. The **Access Settings** page appears:

- **Universal Time Zone:** Select the geographic time zone in which the DOOR will operate. Select the relevant option from the drop-down list as per the site requirement.
- **Time Format:** Specifies the time format to be displayed on the Door Controller's LCD display. Select the relevant option from the drop-down list as per the site requirements.
 - 24 Hours
 - 12 Hours

Auto Synchronize with NTP: If Date and time is to be automatically synchronized as per the **Preferred NTP Server** (predefined or user-defined NTP server address) selected by user, then you must select the **Auto Synchronize With NTP** check box to enable.

Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from device webpage, which will be reflected on device display.

- When Auto Synchronization with NTP is disabled Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 - You can specify the **Preferred NTP Server** of your choice. In this case device will first try to get Date and Time from that server address.

If it does not get Date and Time in three tries; device will check from pre-defined NTP servers.

If you have entered one of the three pre-defined NTP servers(ntp1.cs.wisc.edu , time.windows.com, time.nist.gov); then device will first check that server first.

If it receives updated Date and Time then Updated Date and Time will be reflected on device webpage and display screen.

- You can keep the Preferred NTP Server as blank. In this case device will check for Date and Time from the first NTP server.



If user has manually entered Date and Time from device web page or Device Menu, then these values of Date and Time will be reflected on device webpage and display screen.

*In the case of the **Manual** option the administrator can manually update the time on the Door with that of the system time as and when required. This can be accomplished from the COSEC Monitor.*

- **Working Days:** Specify the days on which the default working hours should be applicable. Select the respective check boxes of the relevant days.
- **Working Hours (HH:MM):** Define the default working hours in HH:MM format.
- **Holiday Schedule:** Click the picklist and select the desired Holiday Schedule. The Administrator can assign upto four Holiday Schedules to the device.



If the same Holiday Schedule is configured for a user and for the door controller on which the user is assigned, then the user's attendance marking on this device, on any of the scheduled holidays will always be marked as a holiday.

General

Click the **General** tab.

Enter all general details applicable to the device in this section.

Basic Readers Access Settings **General**

Mute Buzzer ☐

Allowed Acknowledgement

Display Duration (ms) 3000

LED - Buzzer Duration Long ⓘ

Denied Acknowledgement

Display Duration (ms) 3000

LED - Buzzer Duration Long ⓘ

Enable Display Messages ☐

Custom Birthday Message Happy Birthday

Display Message 1 ⓘ

Schedule 00:00 11:59

Message Good Morning

Display Message 2 ⓘ

Schedule 12:00 15:59

Message Good Afternoon

Display Message 3 ⓘ

Schedule 16:00 20:59

Message Good Evening

Display Message 4 ⓘ

Schedule 21:00 23:59

Message Good Night

Multi-Language Support ☐

Auto Hide Menu Bar ☐



Mute Buzzer, Allowed Acknowledgment, Denied Acknowledgment and Auto Hide Menu Bar are applicable for both Direct Door and Panel Door.

- **Mute Buzzer:** Select the check box to enable door buzzer muting.
- **Allowed Acknowledgment**
 - **Display Duration (ms):** Specify the time duration for which the **Acknowledgment Allowed** message should be displayed. Valid Range is 500 to 3000 ms.
 - **LED - Buzzer Duration:** Select the time duration for the LED Buzzer from the drop-down list options—Long, Medium, Short.
- **Denied Acknowledgment**
 - **Display Duration (ms):** Specify the time duration for which the **Acknowledgment Denied** message should be displayed. Valid Range is 500 to 3000 ms.
 - **LED - Buzzer Duration:** Select the time duration for the LED Buzzer from the drop-down list options—Long, Medium, Short.



Enable Display Messages, Custom Birthday Message, Display Message 1 to 4, Schedule, Message and Multi-Language Support are applicable for Direct Door only.

- **Enable Display Messages:** Select this check box, if you wish to customize the messages as well as display them on the device. You can customize and display the Birthday Message and 4 other Messages.
- **Custom Birthday Message:** Enter the birthday message to be displayed on the door to the user, when the user punches on the door on her/his birth date.

The valid values are: A-Z a-z 0-9 `~!@#\$%^&*()_+-{}|\\|:;?<>.,'\"

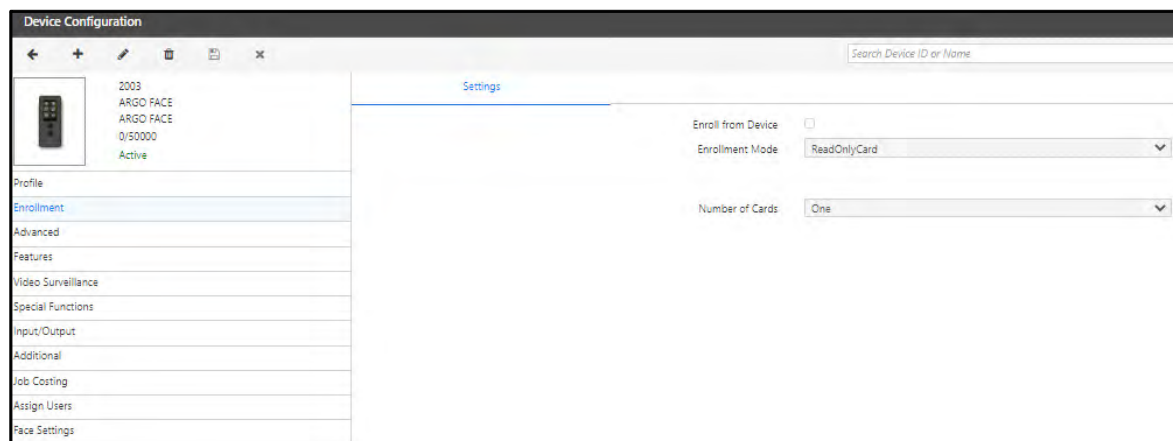
- **Display Message 1 to 4:** Select this check box to enable each display message. These check boxes are enabled automatically if you select the **Enable Display Message** check box.
- **Schedule:** Specify the time duration for which the display message should be displayed in HH:MM format.
- **Message:** Enter the message to be displayed. Maximum 21 characters are allowed.
- **Multi-Language Support:** Select this check box to enable multi-language support for the selected device.
- **Auto Hide Menu Bar:** If any user touches the device screen by mistake and enters into the Menu; then users punch will not be accepted by the device till the Menu is closed or till time out occurs. To avoid such a scenario, select this check box. This will hide the Menu, hence users will be able to punch on the door. To access the Menu, swipe upwards on the device screen. The Menu appears.

Enrollment



Enrollment is applicable for Direct Door only.

On the **Device Configuration** page, click the **Enrollment** tab in the left pane. The Enrollment page appears.



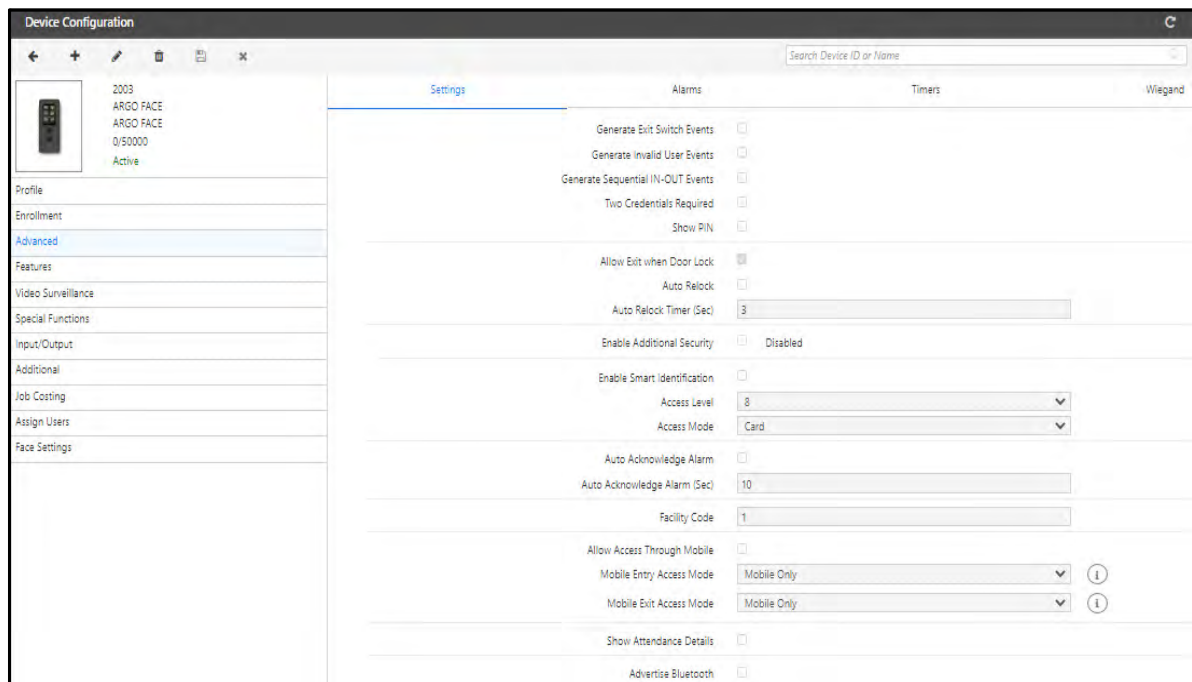
- **Enroll from Device:** Select this check box to enable the enrollment of user from the door controller. When this check box is enabled, 'Enroll User' special function on that device will get activated.



If 'Enroll User' Special Function & 'Enroll From Device' check box both are disabled in device configuration, then on activating 'Enroll User' special function, 'Enroll From Device' check box will be enabled.

- **Enrollment Mode:** Select the Credential from the drop-down list that can be enrolled using the special function at the DOOR. The options are — **ReadOnlyCard, SmartCard and Face**.
- **Number of Cards:** Select the number of cards to be enrolled based on the credential option (ReadOnlyCard or SmartCard) selected in the Enrollment Mode parameter.

Advanced



The Advanced tab allows you to configure some advanced parameters such as Access Control Settings, Alarms and Device Timers as well as Wiegand.

To access this, on the **Device Configuration** page, click the **Advanced** tab in the left pane. The advanced settings can be configured from following sections:

- “Settings”
- “Alarms”
- “Timers”
- “Wiegand”

Settings

Click the **Settings** tab.

The Settings parameters differ for ARGO Face as Direct Door and Panel Door.

Settings - Direct Door

The **Advanced> Settings** page for ARGO Face as **Direct Door** appears as shown below.

Device Configuration

Search Device ID or Name

Device ID: ARGO FACE
Device Name: 0/S0000
Active/Inactive

Profile
Enrollment
Advanced
Features
Video Surveillance
Special Functions
Input/Output
Additional
Job Costing
Assign Users
Face Settings

Settings Alarms Timers Wiegand

Generate Exit Switch Events ☐
Generate Invalid User Events ☐
Generate Sequential IN-OUT Events ☐
Two Credentials Required ☐
Show PIN ☐
Allow Exit when Door Lock ☒
Auto Relock ☐
Auto Relock Timer (Sec) 3
Enable Additional Security ☐ Disabled
Enable Smart Identification ☐
Access Level 8
Access Mode Card
Auto Acknowledge Alarm ☐
Auto Acknowledge Alarm (Sec) 10
Facility Code 1
Allow Access Through Mobile ☐
Mobile Entry Access Mode Mobile Only
Mobile Exit Access Mode Mobile Only
Show Attendance Details ☐
Sensor Type FEVOBOT
Sensor Interface USB
Calibration Parameter + 0.0
Approach to Sensor Wait-Time (Sec) 3.0
Temperature Detection Time Out (Sec) 10
Tolerance between Consecutive Readings 0.5
Consecutive Readings Count within Tolerance 5
Temperature Threshold (°F) 99.5
Minimum Temperature for Access (°F) 95.0
Restriction Type Soft
Bypass if Sensor Disconnected ☐

The following parameters are available for configuration:

- **Generate Exit Switch Events:** Select this check box to enable the door to generate events every-time the exit switch is used.
- **Generate Invalid User Events:** Select this check box to enable the door to generate events for invalid user inputs.
- **Generate Sequential IN-OUT Events:** Select this check box to generate user punches on device as the sequential IN-OUT events irrespective of the mode in which the device is functioning.
- **Two Credentials Required:** Select this check box to enable the feature of verifying 2 credentials compulsorily for users.
- **Show PIN:** Select this check box to display the characters of the PIN when the PIN is entered on the device.
- **Allow Exit when Door Lock:** Select this check box if users are to be allowed to exit even when the Door relay is in locked condition.
- **Auto Relock:** Select this check box to allow the door to relock immediately when the door status changes to close after normal open irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Relock Timer:** Specify the time in seconds after which the door should relock.

- **Enable Additional Security:** Select this check box to enable additional security at the selected Door Controller.
- **Enable Smart Identification:** Select this check box to enable this functionality on the selected Door Controller and select the **Access Level** and the **Access Mode** from the drop-down list.
- **Auto Acknowledge Alarm:** Select this check box to enable the auto-acknowledgment of all alarms for this device.
- **Auto Acknowledge Alarm (sec):** Set the time in seconds The wait timer will start and on expiry of the timer, the alarm buzzer will stop automatically.
- **Facility Code:** Set a value for Facility Code to be set for access modes other than “Card”, if Facility Code is expected in Wiegand Output. This will be applicable to all direct doors except Door V1 and V2.
- **Allow Access Through Mobile:** Check the box to allow the access to device using COSEC ACS Application.
- **Mobile Entry/Exit Access Mode:** Select the entry and exit door access mode from the options — **Mobile Only**, **Mobile then Card** and **Mobile then PIN**.
- **Show Attendance Details:** Select this check box for displaying the Attendance Details of the user on ARGO FACE door. This allows users to view their attendance details on ARGO FACE door and there is no need to login to ESS application to view attendance details.

The attendance details of user will be displayed for default Menu Time-Out period (30 sec) after the Access Allowed screen.



1. The user whose Attendance details are to be displayed on ARGO FACE door must be enabled for this feature. Enable the check-box **Show Attendance details on Device** from User Configuration> T&A> Attendance.

2. While an attendance detail of one user is being displayed on the device and second user tries to access the device; new user request will be processed.

3. Whenever both users of 2-person rule are allowed to get access on device then attendance details screen of second user will be loaded on device.

Temperature Logging

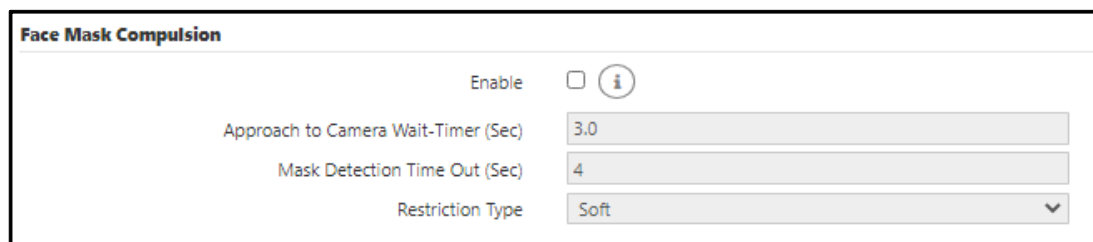
- **Sensor Type:** Select the type of thermal sensor integrated in the device. There are three sensors: *Web-Based* and *FEVOBOT*. Default: *FEVOBOT*.
- **Sensor Interface:** Select the interface on which device will communicate with the sensor.
For Sensor Type- Web-based, the Sensor Interface options will be: HTTP/S
For Sensor Type-FEVOBOT, the Sensor Interface options will be: USB
- **Calibration Parameter:** Set the calibration parameter for the thermal sensor. Not applicable for FEVOBOT. Click + the value increases by 0.1 and click – the value decreases by 0.1.
- **Approach to Sensor Wait-Timer:** This is the time for which the device will wait for user to approach the device before starting Temperature Detection.

- **Temperature Detection Time-Out:** The timer till which temperature detection will be done for the user and if valid temperatures are not found till the expiry of timer then timeout will be declared.
- **Tolerance between Consecutive Readings:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature doesn't fall in the tolerance range the reference temperature is updated with the current temperature and the process continues. Not applicable for FEVOBOT.
- **Consecutive Readings Count within Tolerance:** The Tolerance range of reference temperature within which the consecutive readings are considered to be valid user temperature readings. If current temperature doesn't fall in tolerance range the reference temperature is updated with the current temperature and the process continues. Not applicable for FEVOBOT.
- **Temperature Threshold:** To set the threshold value of the temperature. Default: 99.5
- **Minimum Temperature for Access:** The minimum temperature value detected that should be considered as valid temperature. Default: 95.0

It should be less than threshold temperature. If user tries to enter a value equal to or greater than threshold temperature validation should be displayed.

- **Restriction Type:** You can set the restriction type as soft/hard.
- **Bypass if Sensor Disconnected:** Enable this check box to give provision of bypassing the feature if sensor connectivity is lost.

Face Mask Compulsion



Face Mask Compulsion feature is used to enforce users to wear masks while they are within the premises.

After identifying the user, Device will prompt the user to show Face with Mask when “Face Mask Compulsion” is enabled.

Based on identification of Mask, user will be allowed or denied access.

Make sure you have enabled **Enable FR** check box in **Devices> Device Configuration> Identification Server> Face Recognition> Enable FR** and configure the below mentioned parameters to avail this feature.

- **Enable:** Select this check box to enable Face Mask Compulsion feature for IDS.
- **Approach to Camera Wait-Timer (Sec):** This parameter defines the time within which the user must approach the camera for face mask detection.
 - You must enter the Wait-Time between 0.0-15.0 seconds.
 - By default, it is 3.0 seconds.

- **Mask Detection Time Out (Sec):** This parameter defines the maximum time duration for user's face mask detection.
 - You must enter the detection time out between 0.0-15.0 seconds.
 - By default, it is 4.0 seconds.
- **Restriction Type:** Select the type of restriction to be imposed when the configured policy is violated. Select the desired option - Soft or Hard.
 - **Soft Restriction:** The access will be granted even if the user is identified without wearing a mask; however, an event and warning are generated that indicates the user has been identified without wearing a mask.
 - **Hard Restriction:** The access will be denied if the user is identified without wearing a mask.

By default it is **Soft Restriction**.



Users face enrollments are dependent on the Visible Face parameter value set by you. To know more, refer "[Face Recognition](#)".

Settings - Panel Door

The **Advanced > Settings** page for ARGO FACE as **Panel Door** appears as shown below.

The screenshot shows the 'Device Configuration' window for a device named '2 ARGO--PD--68'. The left sidebar lists various settings categories: Profile, Advanced, Video Surveillance, Input/Output, Assign Users, and Face Settings. The 'Advanced' tab is selected, showing three sub-tabs: Settings, Alarms, and Timers. The 'Settings' sub-tab is active, displaying the 'Face Mask Compulsion' section. This section includes a list of settings: 'Auto Relock' (checkbox), 'Auto Relock Timer (Sec)' (3), 'Man Trap Timer - Internal Reader (Sec)' (0), 'Man Trap Timer - External Reader (Sec)' (0), 'Enable Man Trap Door Interlocking' (checkbox), 'Select Doors for Interlocking' (ID and Name fields), 'Enable' (checkbox, checked), 'Approach to Camera Wait-Timer (Sec)' (3.0), 'Mask Detection Time Out (Sec)' (4), and 'Restriction Type' (Hard).

- **Auto Relock:** Select this check box to allow the door to relock immediately when the door status changes to close after normal open irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Relock Timer (Sec):** Specify the time in seconds after which the door should relock.
- **Man Trap Timer-Internal Reader (Sec):** This check-box enables an alarm wait timer on the panel door to ensure that the user enters the next sequential door of a man-trap within a specific time-frame.
- **Man Trap Timer-External Reader (Sec):** This check-box enables an alarm wait timer on the panel door to ensure that the user exits the panel door to enter the next sequential door of a man-trap within a specific time-frame.
- **Enable Man Trap Door Interlocking:** Select this check-box to activate the Door Interlock for the selected door (say Door1). This means if the Door1 is open then other doors will remain close.

- **Select Doors for Interlocking:** Click the picklist and select the doors to be assigned for the Interlock to the selected door (Door1). Suppose Door2 and Door3 are selected for Interlock with Door1. So When Door1 opens; Door2 and Door3 will remain close.



For Degrade mode Door Interlocking feature will not work.

Whenever a door is in abnormal state and for that door interlocking is enabled then user access in other doors of the interlocking group is allowed.

Face Mask Compulsion

Face Mask Compulsion feature is used to enforce users to wear masks while they are within the premises.

After identifying the user, Device will prompt the user to show Face with Mask when “Face Mask Compulsion” is enabled.

Based on identification of Mask, user will be allowed or denied access.

Make sure you have enabled **Enable FR** check box in **Devices> Device Configuration> Identification Server> Face Recognition> Enable FR** and configure the below mentioned parameters to avail this feature.

- **Enable:** Select this check box to enable Face Mask Compulsion feature for IDS.
- **Approach to Camera Wait-Timer (Sec):** This parameter defines the time within which the user must approach the camera for face mask detection.
 - You must enter the Wait-Time between 0.0-15.0 seconds.
 - By default, it is 3.0 seconds.
- **Mask Detection Time Out (Sec):** This parameter defines the maximum time duration for user’s face mask detection.
 - You must enter the detection time out between 0.0-15.0 seconds.
 - By default, it is 4.0 seconds.
- **Restriction Type:** Select the type of restriction to be imposed when the configured policy is violated. Select the desired option - Soft or Hard.
 - **Soft Restriction:** The access will be granted even if the user is identified without wearing a mask; however, an event and warning are generated that indicates the user has been identified without wearing a mask.
 - **Hard Restriction:** The access will be denied if the user is identified without wearing a mask.

By default it is **Soft Restriction**.



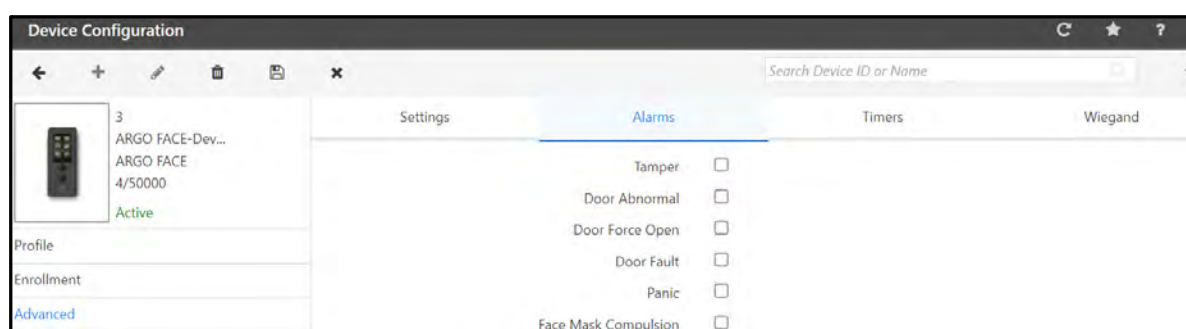
Users face enrollments are dependent on the Visible Face parameter value set by you. To know more, refer [“Face Recognition”](#).

Alarms

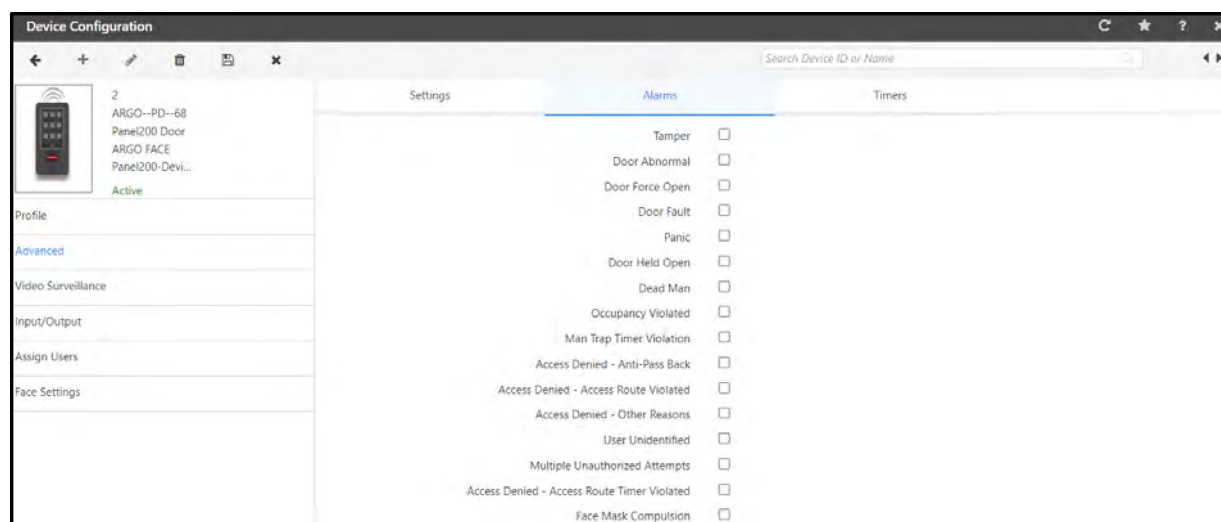
In the **Alarm** tab, you can assign below list of alarms to the door.

Click the **Alarms** tab. A different set of Alarms can be enabled/disabled for ARGO Face as Direct Door as well as Panel Door.

The **Alarms** page for ARGO FACE as **Direct Door** appears as shown below.



The **Alarms** page for ARGO FACE as **Panel Door** appears as shown below.



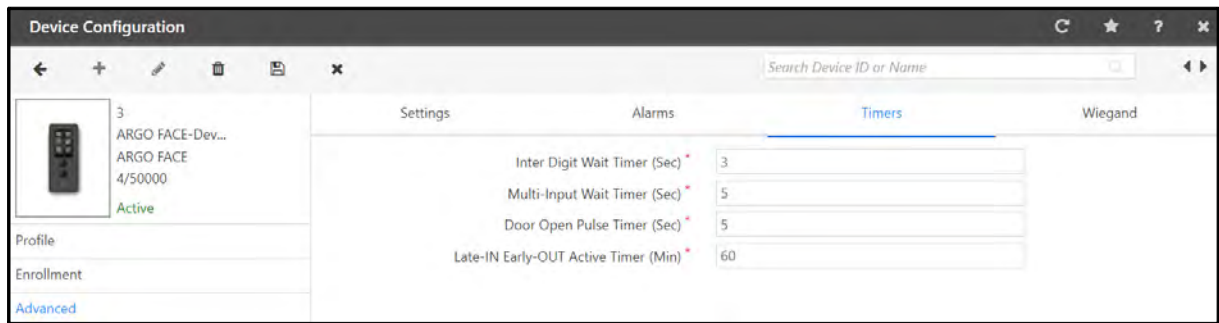
Select the check boxes of the desired Alarms you wish to enable.

Timers

This section allows the configuration of various types of pre-defined device timers which can trigger specific responses. In COSEC, timers are often used to control door behavior and for triggering alarms.

The Timers parameters differ for ARGO Face as Direct Door and Panel Door.

Click the **Timers** tab. The **Timers** page for ARGO FACE as **Direct Door** appears as shown below.



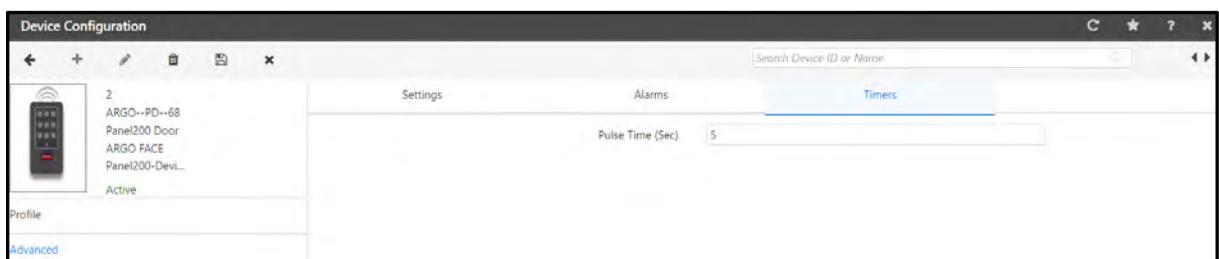
- **Inter-Digit Wait Timer (sec):** Specify the time period in seconds between two key inputs on the device keypad. On expiry of this timer, the system considers the user input to be complete and is ready for the next input.
- **Multi-Input Wait Timer (sec):** Specify the time in seconds for which system needs to wait for the second credential input from the user when more than one credential is to be used to grant access.



We recommend you to set the timer value as greater than or equal to 10 seconds to avoid access denial issues to users. This is applicable when the system reads the credentials (biometric) from the user's Smart Cards.

- **Door Open Pulse Timer (sec):** Specify the time in seconds (3 to 99) for the door to be energized for a valid credential. If the opened door does not return to a closed state before the expiry of this timer, the door will generate a "Door Abnormal" alarm.
- **Late-IN Early-OUT Active Timer (min):** Specify the time in minutes for which the Late-IN and Early-OUT special functions will remain active after being enabled for the Door Controller.

The **Timers** page for ARGO FACE as **Panel Door** appears as shown below.



- **Pulse Time (sec):** Specify the time in seconds for the panel door to be energized for a valid credential.

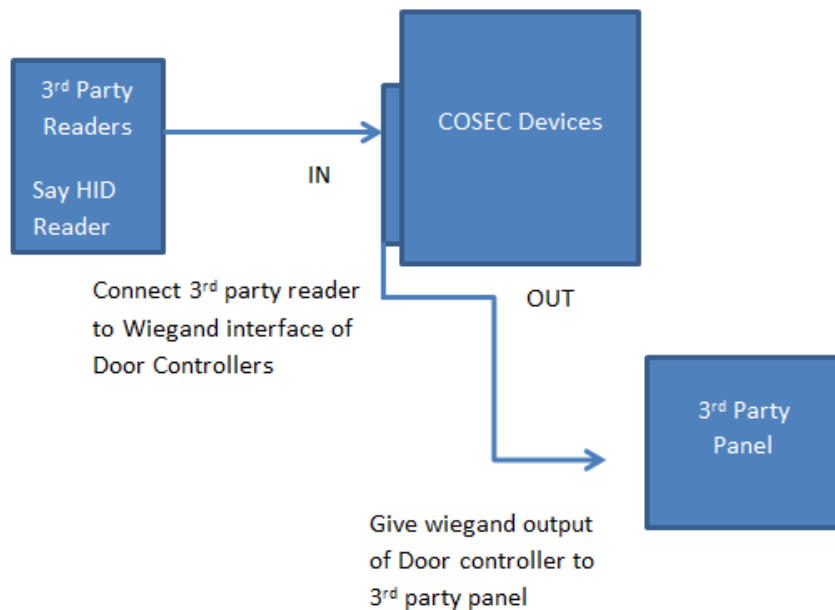
Wiegand



Wiegand is applicable for Direct Door only.

Click the **Wiegand** tab. The **Wiegand** page appears:

- **Wiegand Interface:** The COSEC device can be connected both as input devices (e.g. to receive data from a Wiegand Reader) or output devices (e.g. to support output to third party panel) via the Wiegand interface as shown below.



So select the interface of Door controller as **Output Mode** to work as Wiegand output to panel or **Reader Input** to take data from third party reader. If Reader Input option is selected, all the Output Mode parameters will be disabled.

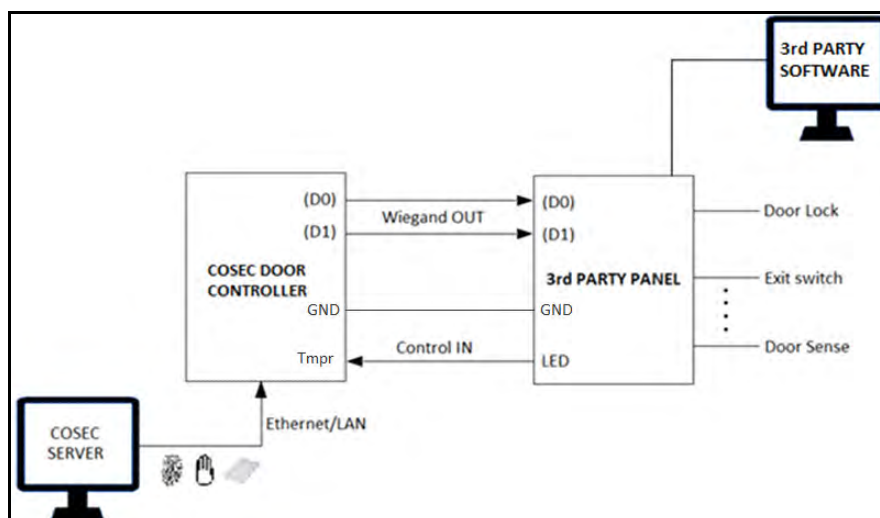
If you select Output Mode then configure the following **Output Mode Parameters**:

- **Wait For Panel Signal:** Select the check box to enable this option. The door will wait for reply from the connected third party device before triggering any output, as per the defined **Signal Wait Timer (Sec)**.
- **Signal Wait Timer (Sec):** The time for which the device will wait to receive the reply from the third party panel, before it triggers any output.
- **Wait For User Verification:** Select the check box to enable this option. The user verification will be requested to the third party device before triggering any output.
- **Wiegand Output Format:** Select the desired Wiegand Output Format from the options 26 Bit, 37 Bit, Actual or Custom.

If you select Custom, you need to configure the Wiegand Format. For details refer to Devices Module > Masters > Wiegand Output Format. (Give cross reference of Wiegand Format here)

- **Send From:** Specify the sending order for reader data as MSB or LSB Bit.

Wiegand Out Interface



Door Access using QR code

The user can access the COSEC device using COSEC APTA installed in the mobile device. If the user has rights for COSEC APTA and the access to the device is allowed for the user, then he can use his mobile device to scan the QR code which constitutes the details of the COSEC door.

There is icon for QR code in the COSEC APTA application. Click the icon, it will open the camera in your mobile. Now you can scan the QR Code using the mobile camera. The COSEC door will get opened after verifying the security key and access policies of the user.

Steps to create a QR code

Step 1: Enter details in JSON format

```
{"version":"x","ip": "x.x.x.x","port":"x","pdid":"x","mode":"x"}
```

Valid values:

Field	Field range	Default Value	Remark
version	1-255	1	
ip	0.0.0.0-255.255.255.255	0.0.0.0	
port	0-65535	0	
pdid	0-255	0	If door is in direct door mode then, then PDID will be 0 If door is in panel door mode then, PDID will have values from 1-255
mode	0,1	0	0= for entry mode 1=for exit mode



Note:

Step 1: If door is in direct door mode enter IP & port of the direct door.

Step 2: Encrypt the JSON string using key "matrix12" with simple DES/ECB mode.

Step 3: Encode the encrypted string using Base 64.

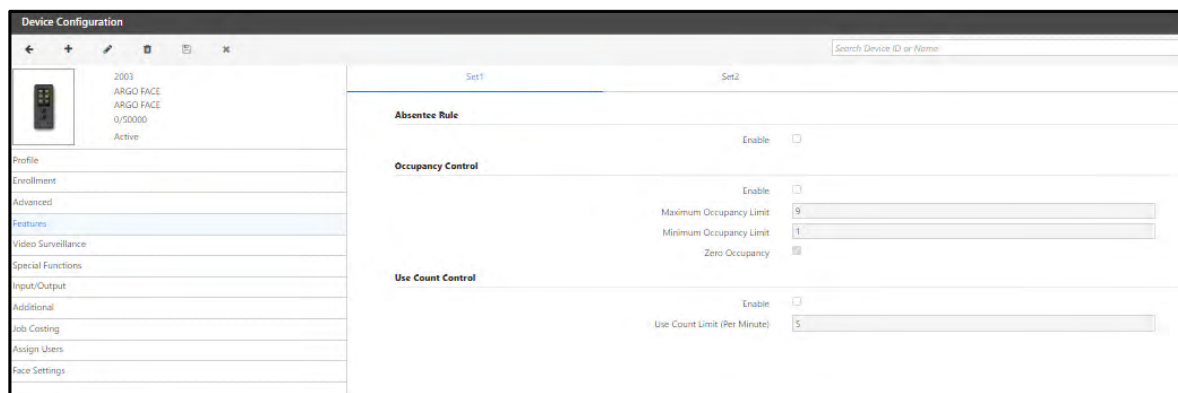
Step 4: Use this string to generate QR code through any third party software.

Features



The Features are available only with the Access Control Module license and are applicable for Direct Door only.

On the **Device Configuration** page, click **Features** on the left pane. This tab allows the user to enable certain Access Control features for the device.



To set the access control features for the device, click the following:

- "Set1"
- "Set2"

Set1

This page allows you to set the parameters for three rules - **Absentee Rule**, **Occupancy Control** and **Use Count Control**. Click the **Set1** tab, the page appears.

The screenshot shows a web interface with two tabs at the top: 'Set1' (selected) and 'Set2'. Below the tabs are three sections for configuring rules:

- Absentee Rule**: Contains an 'Enable' checkbox which is currently unchecked.
- Occupancy Control**: Contains an 'Enable' checkbox (unchecked), a 'Maximum Occupancy Limit' input field with the value '9', a 'Minimum Occupancy Limit' input field with the value '1', and a 'Zero Occupancy' checkbox (unchecked).
- Use Count Control**: Contains an 'Enable' checkbox (unchecked) and a 'Use Count Limit (Per Minute)' input field with the value '5'.

- **Absentee Rule:** Select the **Enable** check box to enable the feature on the door. This rule sets the maximum number of days for non-use of a credential. On expiration of days limit, the user will be automatically blocked. For configuring the rule, refer to *Access Control> Absentee Rule*.
- **Occupancy Control:** Select the **Enable** check box to enable this feature on the door.
 - **Maximum Occupancy Limit:** Specify the maximum number of users to be allowed within the controlled area after which a user exit is required to enable access to another user.
 - **Minimum Occupancy Limit:** Specify the minimum number of occupants the designated zone should have.
 - **Zero Occupancy:** Select the check box to enable, that is whether the designated zone should be allowed to be empty or not.

For configuring the rule, refer to *Access Control> Occupancy Control*.

- **Use Count Control:** Select the Enable check box to enable this feature on the door.
 - **User Count Limit (Per Minute):** Specify the maximum number of uses per minute allowed to the user.

For configuring the rule, refer to *Access Control> Use Count Control*.

Set2

This page allows you to set the parameter for the three rules - **First-IN User Rule**, **Anti-Pass-Back (APB)** and **2-Person Rule**. Click the **Set2** tab and the page appears.

The screenshot displays the configuration interface for the Matrix COSEC System, specifically the 'Set2' tab. It contains three main sections for configuring access rules:

- First IN User Rule:**
 - Enable:** A checkbox that is currently unchecked.
 - Reset On:** Radio buttons for 'Day Change' (selected) and 'Timer Expiry'.
 - Access Timer (Sec):** A text input field containing the value '3'.
 - First IN User Group:** A picklist showing '1' and a 'List 1' button.
- Anti-Pass Back (APB):**
 - On Entry:** An unchecked checkbox.
 - On Exit:** An unchecked checkbox.
 - Hard/Soft:** A dropdown menu set to 'Soft'.
 - Forgiveness:** A button with a plus icon.
 - Reset After:** Radio buttons for 'Day Change' (selected) and 'Timer Expiry'.
 - Forgiveness Timer (Min):** A text input field containing the value '1'.
- 2-Person Rule:**
 - Enable:** An unchecked checkbox.
 - Mode:** A dropdown menu set to 'Primary Must'.
 - Primary Group:** A dropdown menu set to 'Select'.
 - Secondary Group:** A dropdown menu set to 'None'.
 - 2nd Person Wait Timer (Sec):** A text input field containing the value '5'.

- **First-IN User Rule:** Select the Enable check box to enable the feature on the direct door and configure the parameters.
- **Reset On:** You can reset the rule as per your requirement. Select the desired option f — **Day Change** or **Time Expiry**.

If you select **Time Expiry**, configure the **Access Timer (Sec)**.

- **Access Timer (sec):** Configure the duration for which the rule should be applied. After the expiry of this timer the rule will be reset for all the users.

First-In User Group: Click the picklist to select the desired group which would be valid at the door. For configuring the rule, *refer to Access Control> First- In User Rule> Assignment*

- **Anti-Pass Back (APB):** Select the Enable check box to enable this feature on the direct door and configure the parameters.
- **On Entry:** Select the check box so that the system monitors the entry reader for APB violation.
- **On Exit:** Select the check box also so that the system monitors the entry as well as the exit readers for APB violations.
- **Hard/Soft:** Select the restriction type as Hard or Soft.
- **Hard APB:** The access will be denied if the exit is not registered first. It does not allow a second entry using the same card without an exit.
- **Soft APB:** The access will be granted even if the exit is not registered. It allows a second entry of the same user without an exit; however, an event and warning are generated that indicates the second entry.

- **Forgiveness:** Select this check box to enable the system to reset the APB status. When forgiveness is enabled, you can select one of the following options to reset the pass.
 - **Day Change:** This will reset the APB status of all the users to NULL at midnight. This enables a user, who left the building in the evening without exit punch, to use her/his card for entry in the next morning.
 - **Timer Expiry:** This will reset the APB status of all the users after the expiry of user defined time. If you select this option, configure the Forgiveness Timer (Mins).
 - **Forgiveness Timer (Mins):** Enter the time duration in minutes after which Anti-pass back status should be reset and the pass will be in original state.
- **2-Person Rule:** Select the Enable check box to enable the feature on the door and configure the parameters.
 - **Mode:** Set the Mode as **Primary Must** or **Primary & Secondary Must**.
 - **Primary Group:** Select the desired group from the drop-down list.
 - **Secondary Group:** Select the desired group from the drop-down list.
 - **2nd Person Wait Timer:** Set the wait time in seconds after which the second person is allowed to punch on the door.

For configuring the rule, refer to *Access Control > 2- Person Rule*

Video Surveillance



Video Surveillance is applicable for both Direct Door and Panel Door. On the **Device Configuration** page,

Click **Video Surveillance** on the left pane. The Video Surveillance tab allows you to configure parameters for video surveillance integration with the COSEC device. It is available in Basic License.

To set parameters, click the following links:

- [“Visual Tagging”](#)
- [“Satatya Integration”](#)

- [“Built-In Camera”](#)

Visual Tagging

The COSEC application acts as an interface between supported hybrid and network video recording systems as well as IP Cameras and grab images triggered by user events at the Doors. The **Visual Tagging** option enables the administrator to define the video recorder and IP Camera parameters.

Click **Visual Tagging** tab. The **Visual Tagging** page appears.



To view the user events and related images, click **Admin > Views/Logs > Event View**. To know more about viewing events, refer [“Event View”](#).

Configure the following parameters:

- **Capturing Device:** Select the video recording type of device or IP Camera from the drop-down list.
 - Matrix HVR/NVR
 - Built-In Camera
 - Milestone

If you select **Matrix HVR/NVR**, configure the following:

- **MAC Address:** Specify the MAC address of the video recorder device using “_” (underscore) as the separator.
- **Camera ID:** Specify the camera number or camera ID of the IP cameras. For analog cameras specify the camera number.
- **Storage Root Folder:** Specify the Root folder path or FTP Path where the uploaded images will be saved.
- **FTP Login Credentials:** Select this check box to enable FTP login credentials for authentication.
 - **Username:** Specify the FTP Server Username.
 - **Password:** Specify the FTP Server Password.



Some COSEC devices do not support all the network connection options.

If you select **Milestone**, refer to [“Milestone Integration”](#).

If you select **Built-In Camera**, refer to [“Built-In Camera”](#).

Satatya Integration

This functionality is available for configuration only when the **Matrix HVR/NVR** device type is selected as the **Capturing Device** under **Visual Tagging**. It enables the configured COSEC devices to directly send commands to the SATATYA HVR/NVR devices as per the configurations.



Click the **Satatya Integration** tab. The Satatya configuration page appears.

The screenshot shows the 'Satatya Integration' configuration page. It includes fields for Integration Type (Wired), Active checkbox, IP Address, Port Number (1024-65535), Schedule Name, Active checkbox, Schedule Range (00:00 to 23:59), Days (Sun, Mon, Tue, Wed, Thu, Fri, Sat, Holiday), Event (Access Allowed), Mode (Both), Action (Recording), Duration Min, and a grid of checkboxes for Camera selection (1-24). There are Add and Cancel buttons at the bottom.

- **Integration type:** Select the desired options — Wired, Network.

In **Wired**, the door is physically connected with Satatya Device. If you select this option then you do need to configure any other parameters.

In **Network**, connection can be though Ethernet, Wireless or Broadband depending upon the COSEC device support. If you select this option, configure the following parameters:

- **Active:** Select the check box to enable the connection.
- **IP Address:** Specify the IP Address of HVR/NVR.
- **Port Number:** Specify the Port Number of HVR/NVR.
- **Schedule Name:** Specify a user friendly name for the schedule function.**Active:** Select the check box to enable the SATATYA Integration functionality.
- **Schedule Range:** To run the schedule for the function, configure the start and the end time (*24 Hours format*).
- **Days:** To apply the configured schedule to the days of the week, select the check boxes of the desired days of the week.
- **Event:** Select the desired COSEC event from the drop-down list for which the action is to be configured.
- **Mode:** Select the desired event mode from the options — Entry, Exit and Both.
- **Action:** Select the action to be taken by the Satatya device from the drop-down list. The options are — Recording, Image Upload, Video Pop-up, PTZ Preset, Mail Image.

If you select **Recording**, configure the **Duration Min.** as well as select the desired **Camera** channels.

If you select **Upload Image**, select the desired **Camera** channels. Images will be uploaded as per the FTP settings.

If you select **Video Pop-up**, configure the **Duration Sec.** as well as select the desired **Camera** channels. The video pop up will be generated on the local client of Satatya device for the selected cameras.

If you select **PTZ Preset**, configure the desired **Position No.** as defined in the SATATYA device as well as select the desired **Camera** channels.

If you select **Mail Image**, configure the **Email ID** as well as select the desired **Camera** channels.

- **Camera:** Select the check boxes of the relevant camera channels depending on the action selected.

Example: For Access allowed event on COSEC Device, the video pop up of Camera 12 will be shown for 10 seconds.

Click **Add** to complete the process of linking the event with the action. You can also configure other event-action linkages as per your requirements.

The screenshot shows a configuration form with the following fields:

- Event:** Access Allowed (dropdown)
- Mode:** Both (dropdown)
- Action:** Video Pop-Up (dropdown)
- Duration Sec.:** 10 (text input)
- Camera:** A grid of checkboxes for cameras 1 through 24. Camera 12 is selected.

Built-In Camera

This functionality enables configuration and scheduling of image capturing using the in-built camera of the door.

Click the **Built-In Camera** tab. The **Built-In Camera** configuration page appears.

The screenshot shows the 'Built-In Camera' tab selected in the top navigation bar. Below the tabs is a search bar and a table with the following columns: Name, Active, Start Time, End Time, Days, and Trigger. The table is currently empty, displaying 'No Data'. An arrow points to a '+' button in the top right corner of the table area.

The ARGO FACE's built-in camera can be scheduled to capture images during scheduled periods and can be triggered by specific user events.

To configure a schedule click **Add** button as shown above.

- Specify the function **Name** and select the **Active** check box to enable it on the system.
- Specify a schedule by entering **Start** and **End Time**.
- Select the Applicable **Days**.
- Select the user events Trigger from the drop-down list on the occurrence of which the image capturing should be triggered. The options are Access Allowed, Access Denied and Both.

The screenshot shows the 'Built-In Camera' configuration page with a new entry added to the table:

Name	Active	Start Time	End Time	Days	Trigger
User Allowed	<input checked="" type="checkbox"/>	09:00	10:00	Select	Access Allowed

Below the table, there is a list of days with checkboxes: Sun, Mon, Tue, Wed, Thu, Fri, Sat, and Holiday. The 'Mon' through 'Fri' checkboxes are checked. A dropdown menu is open for the 'Trigger' column, showing the options: Access Allowed, Access Denied, and Both.

- Click **OK** and then click **Save** to save the schedule for the selected device.



If you delete ARGO FACE Panel Door from your device list, then the configurations stored for Built-In Camera will not be deleted. If you add the same ARGO FACE Panel Door again with the same Panel Door ID, then the configurations for Built-In Camera will be restored and displayed on the same page.

Special Functions



Special Functions are applicable for Direct Door only.

On the **Device Configuration** page, click the **Special Functions** tab on the left pane.

No.	Function Name	Active	Job Selection	User Group	Card 1	Card 2	Card 3	Card 4	
1	Official Work - IN	Yes	Yes	All					
2	Official Work - OUT	Yes	Yes	All					
3	Short Leave - IN	Yes	Yes	All					
4	Short Leave - OUT	Yes	Yes	All					
5	Regular - IN	Yes	Yes	All					
6	Regular - OUT	Yes	Yes	All					
7	Break End	Yes	Yes	All					
8	Break Start	Yes	Yes	All					
9	Overtime - IN	Yes	Yes	All					
10	Overtime - OUT	Yes	Yes	All					
11	Enroll User	No	No	All					
12	Enroll Special Card	Yes	No	All					

To configure *Special Functions* for COSEC doors, refer to [“Special Functions”](#).

Input/Output

The Input/Output (I/O) configuration of a system determines how the output or response of a system is influenced by the input applied on it. In case of the COSEC Access Control System, the I/O configuration should enable the system to monitor and trigger a specific response to any change in the door state or event occurrences at the door device. This change of door state or occurrence of events is considered as an input while the response or action that is generated by the system on detection of this input, is defined as the output.

Device Configuration

2003
ARGO FACE
ARGO FACE
Q/50000
Active

Input/Output

Door Sense

Enable ☐

Supervised ☐

Door Sense Type: **NC**

Accept External IO Linking

Enable ☐

Network Interface: **Ethernet**



- This functionality cannot be fully accessed in the Edit mode for a selected device.
- This functionality is available only with the Access Control add-on module license.

On the **Device Configuration** page, click the **Input Output** tab on the left pane. Click the following links to configure the parameters:

- [“Configuration”](#)
- [“Linking”](#)
- [“Time Triggered”](#)

Configuration



Configuration is applicable for both *Direct Door* and *Panel Door* but the parameters differ.

Click the **Configuration** tab. The **Configuration** page for ARGO FACE as **Direct Door** is shown below.

- **Door Sense:** The system by default can sense two states of a door - *Normally Open (NO)* and *Normally Closed (NC)* depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a *Door Abnormal* alarm.
 - Select the **Enable** check box to enable the system for two-state monitoring.
 - Select the **Supervised** check box to enable the door for four-state monitoring where the door is also monitored for *door fault* and *door disconnection*.
 - Specify the **Door Sense Type** as **NC** or **NO** (Default: NC).
- **Accept External IO Linking:** Select the **Enable** check box to enable device-to-device IO Linking i.e. input from one Direct Door can trigger output in another Direct Door.
- **Network Interface:** Select the interface option for IO linking with external devices. The options are:
 - Ethernet
 - Wireless
 - Mobile Broadband

The **Configuration** page for ARGO FACE as **Panel Door** is shown below.

The screenshot shows the 'Device Configuration' window for a device named '2 ARGO--PD--68 Panel200 Door ARGO FACE Panel200-Devi...'. The 'Configuration' tab is selected. Under 'Door Sense', the 'Enable' checkbox is checked, 'Supervised' is unchecked, and 'Door Sense Type' is set to 'NC'. Under 'Relay Output', 'Output Group Number (Door Unlock)' is set to '2' and 'Output Group Number (Door Lock)' is set to 'ID'. There are also buttons for 'Door Unlock' and 'Name'.

- **Door Sense:** The system by default can sense two states of a door - *Normally Open (NO)* and *Normally Closed (NC)* depending on which the output is determined. For example, any deviation of the door from its normal state may lead to the trigger of a *Door Abnormal* alarm.
- Select the **Enable** check box to enable the system for two-state monitoring.
- Select the **Supervised** check box to enable the door for four-state monitoring where the door is also monitored for *door fault* and *door disconnection*.
- Specify the **Door Sense Type** as **NC** or **NO** (Default: NC).
- **Relay Output:** This indicates the physical output which is received for opening and closing of the door.
- **Output Group Number (Door Unlock):** Select the Output Group Number to which the device output for Door Unlock is to be assigned from the picklist.
- **Output Group Number (Door Lock):** Select the Output Group Number to which the device output for Door Lock is to be assigned from the picklist.

Linking



Linking is applicable for Direct Door only.

Click the **Linking** tab. The **Linking** page appears.

Configuration

Linking

Time Triggered

Search

Name	Active	Input	Output	Output Type	Pulse Time(Sec)	Reset Link	Reset Time	Supported Devices	
	No	Intercom Panic	Door Relay			Inactive	00:00	0 >	
	No	User Allowed	Door Relay			Inactive	00:00	0 >	
	No	User Denied	Door Relay			Inactive	00:00	0 >	
	No	Zone Empty	Door Relay			Inactive	00:00	0 >	

The COSEC application supports the Input/Output Linking feature to activate an output port based on a trigger received from an input port on the same Direct Door. This option enables the administrator to define how an event or events (input port) will trigger an output on the selected door.

Select a Input-Output linking row or click **Edit** button.

- **Name:** Specify a name for the new I/O linking program.
 - **Active:** Select this check box to activate this linking program.
 - **Output Type:** Specify the appropriate type of output from the following four options available in the drop-down list:
 - **Pulse:** With this type of output, the user needs to define the Pulse time in seconds.
 - **Interlock:** With this option, the output follows the input. The relay output is triggered as long as the input is activated after which it returns to normal state.
 - **Latch:** With this option, it is denoted that the relay output will be in an energized condition for infinite period and needs to be reset manually.
 - **Toggle:** With this option, the output group toggles its state whenever an input group is activated.
 - **Pulse Time (sec):** For a *Pulse* output type, specify the pulse duration in seconds.
 - **Reset Link:** Select this check box to reset the link automatically after a defined time period.
 - **Reset Time:** Enter the time period in hh:mm format after which the link should be reset automatically.
- For example, an IO Link gets activated on 21/04/2017 at 15:00. And Reset Time is set as 18:00. When Device Time is 18:00 then that IO link will get reset.
- **Supported Devices:** Click the picklist, all devices supported for external IO Linking will appear in this . Select the desired devices. Upto 255 external devices can be added by the administrator.
 - Click the **OK** button and **Save** the configuration.

Time Triggered



Time Triggered is applicable for Direct Door only.

This functionality enables the user to control the activity of an Output without manual intervention.

The time triggered functions are used for activating events like door unlock and siren activation that are set as per the start time and for the configured time duration.

This functionality is designed to energize outputs for predefined periods at the configured time. The COSEC Access Control System supports up to 20 Time Triggered functions on a Direct Door

Click the **Time Triggered** tab and the page appears.

Function Name	Active	Time	Duration(Sec)	Days	Output
	<input checked="" type="checkbox"/>	00:00	10	Select	Door Relay

Click **Add**.

- Enter the **Function Name**.
- Select the **Active** check box.
- Enter the **Time** and **Duration** of the triggered function.
- Select the **Days** on which this function should be triggered.
- Click **OK** and then **Save** to save the settings.

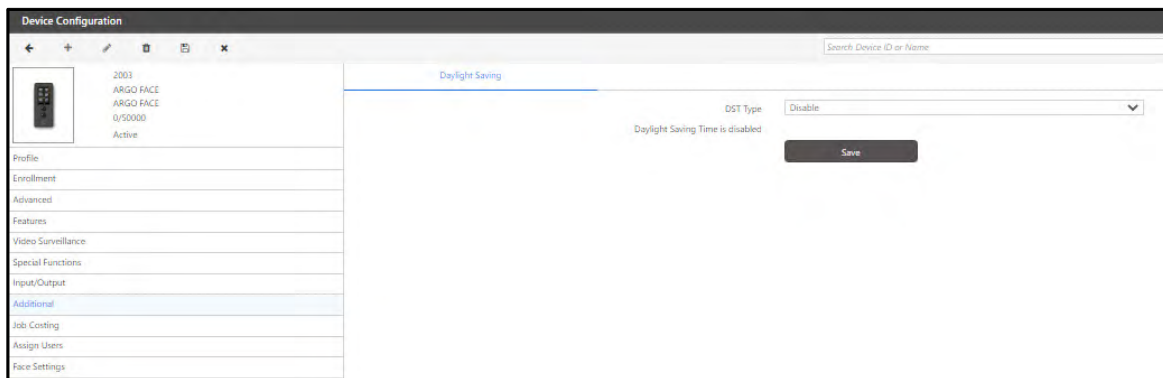
Additional



Additional is applicable for Direct Door only.

This section lists some additional configurations that can be enabled for door controllers.

On the **Device Configuration** page, click the **Additional** tab.



Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. COSEC doors can be configured and made compatible, keeping the RTC of the system updated with such changes.

The **Daylight Saving** configuration can be done in 2 ways. that is Day-Month wise or Date-Month wise.

- Select the **DST Type** as Day-Month wise or Date-Month wise.

Select **Disable** if you do not wish to apply DST.

- If you select the **Day-Month wise** option, the DST is set by the day of the month on which clock needs to be forwarded and reverted to normal. Set the month, week number, day of the week, and time for both the **Forward Clock** and **Backward Clock** as shown.

The screenshot shows the 'Daylight Saving' configuration window. At the top, 'Daylight Saving' is selected. Below it, 'DST Type' is set to 'Day-Month wise' and 'Time Period' is '00:00'. The 'Forward Clock' section has 'Month' as 'January', 'Week No.' as '1st', 'Day of Week' as 'Sunday', and 'Time' as '00:00'. The 'Backward Clock' section has 'Month' as 'January', 'Week No.' as '1st', 'Day of Week' as 'Sunday', and 'Time' as '00:00'. A 'Save' button is at the bottom.

- If you select the **Date-Month wise** option, the DST is set by date of the month on which clock needs to be forwarded and reverted to normal. Define the **Time Period** for the date-month wise DST settings in *24-hours* format, and specify the day of the week, date and time for the **Forward Clock** and the **Backward Clock** as shown.

The screenshot shows the 'Daylight Saving' configuration window. At the top, 'Daylight Saving' is selected. Below it, 'DST Type' is set to 'Date-Month wise' and 'Time Period' is '00:00'. The 'Forward Clock' section has 'Month' as 'January', 'Date' as '1', and 'Time' as '00:00'. The 'Backward Clock' section has 'Month' as 'January', 'Date' as '1', and 'Time' as '00:00'. A 'Save' button is at the bottom.

This DST Setting implies that on 1st Sunday of November at 09:00 hours, the clock will be forwarded by 08:00 hours. And on 1st Sunday of January at 10:00 hours, the clock will be reversed or set backward by 08:00 hours.

- Click the **Save** button.

Job Costing



Job Costing is applicable for Direct Door only.

When user punches on any device, there will be an option to select the Job Code on which the user is working. Job Costing enables the Administrator to display or hide Job Code selection on device. It also enables the Administrator to assign default jobs on device.

- **Show Job Menu:** Select the option as **Show List** or **Allocate Default**.

If you select **Show List**, multiple jobs can be assigned to the device. The user can select the relevant job code while punching on the device. His/her job hours will be recorded for that job code.

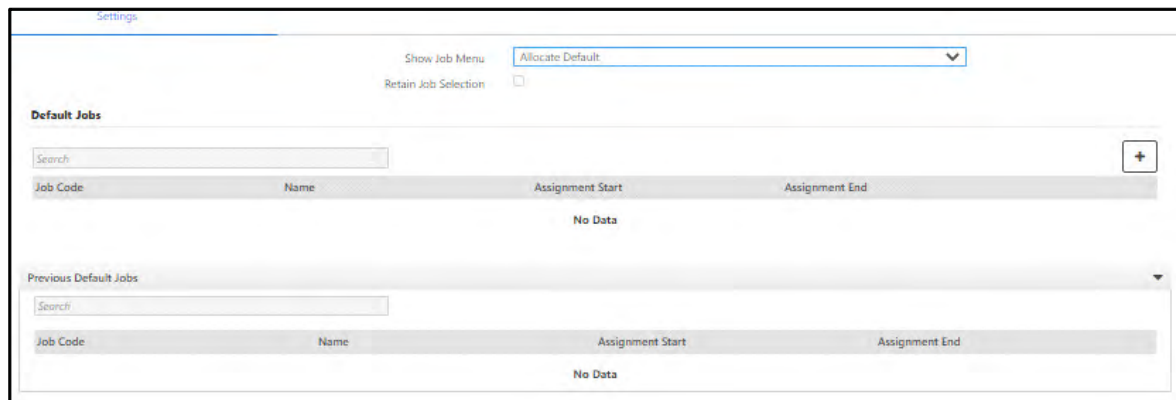
You need to configure Retain Job Selection and Assign Jobs.

- **Retain Job Selection:** Select this check box to retain the Job Code selected by a user which would be applicable for all the subsequent users until another job selection is done on the device.

Assign Jobs

- **Job Group:** Click the respective picklist to select the desired **Job Group**.
- **Job:** Click the respective picklist to select the individual **Job**.
- Then click **Save**. The jobs will be listed to the grid.

If you select **Allocate Default**, then default jobs for the device can be selected.



Default Jobs

- Click **Add**, to add the default job for the door.
- Click the picklist to select the desired **Job Code** .
- Click the picklist to select the desired **Job Name** .
- Enter the **Assignment Start** and **Assignment End** time.
- Click **OK** and then click **Save**.

The Job Costing user can directly punch on this door for starting the default job.

When the assignment date of the default job gets elapsed, then this job will be listed under **Previous Default Jobs** section.

Assign Users

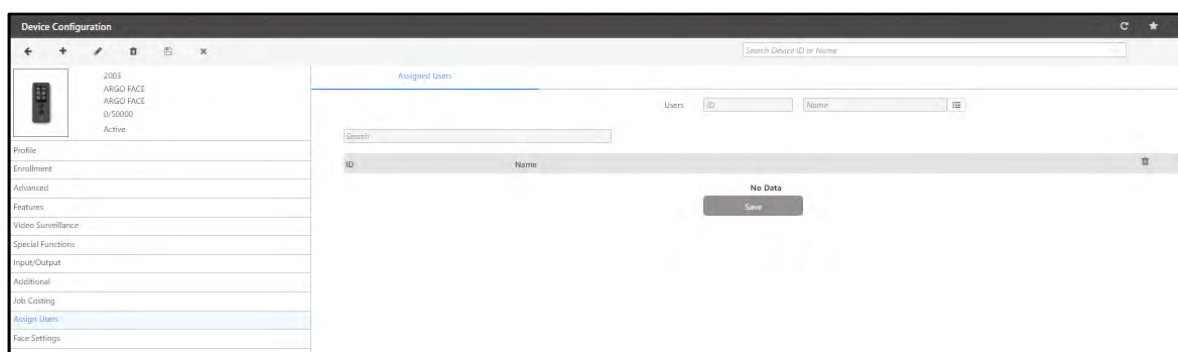


Assign Users is applicable for both Direct Door and Panel Door.

On the **Device configuration** page, click **Assign Users** on the left pane.

For the configured device, you can select and assign the users.

Click **Assigned Users** tab.



- **Users:** Click the picklist to select the desired Users ID/Name.
- Click **Save** to assign all the added users to the selected door.

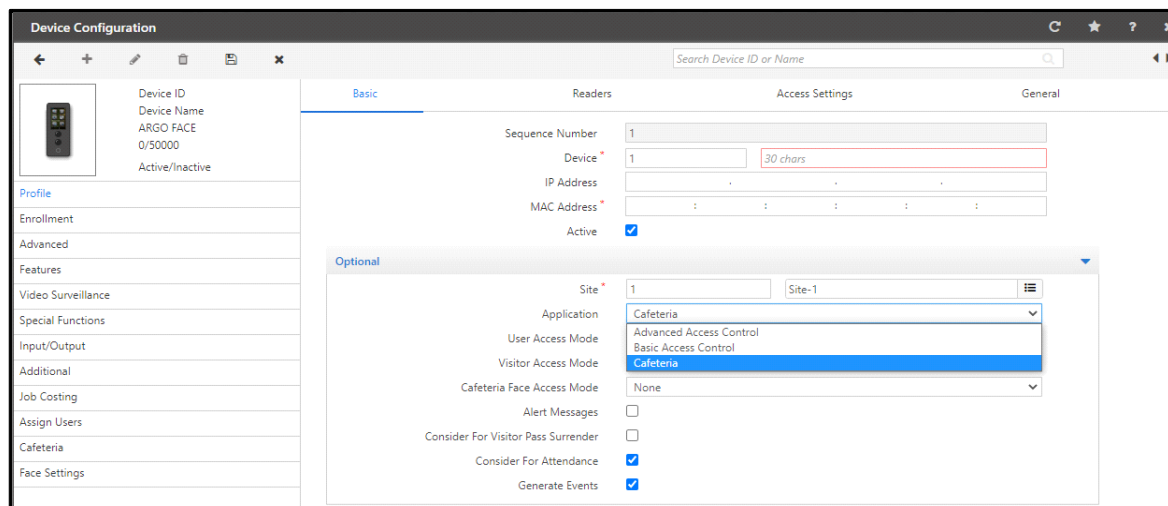
Cafeteria



Cafeteria is applicable for Direct Door only.

The COSEC system enables you to configure devices which will be used by the Cafeteria management module.

To configure a door for Cafeteria application, make sure you have selected **Cafeteria** option in **Application** (Device Profile > Basic > Application) as shown below.



On the **Device Configuration** page, click **Cafeteria** on the left pane.

For the Cafeteria configurations, click the following links.

- [“Settings”](#)
- [“Menu”](#)

Settings

Click **Settings** tab. The Cafeteria configuration for ARGO FACE Door appear.

The screenshot shows the 'Device Configuration' window for an 'ARGO FACE' device. The 'Settings' tab is active. On the left, a sidebar lists configuration categories: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions, Input/Output, Additional, Job Costing, Assign Users, Cafeteria (selected), and Face Settings. The main content area is split into two sections: 'Menu' and 'Printer Settings'. The 'Menu' section contains three settings: 'Consecutive Transaction Delay (Sec)' with a value of 0, 'Enable Offline Item Quantity Restriction' with an unchecked checkbox, and 'Allowed Item Quantity' with a value of 1. The 'Printer Settings' section contains eight settings: 'Printer' (set to None), 'Connection Type' (set to RS232), 'Baud Rate' (set to 115200), 'Company Name' (empty), 'Company Address' (empty), 'Punch Line' (empty), 'Exclude Price-Cost From Coupon' (unchecked), and 'User Balance On Coupon' (unchecked).

- **Consecutive Transaction Delay (Sec):** Enter the time interval after which you wish to allow the second transaction from the same user.
- **Enable Offline Item Quantity Restriction:** Select the check box if you desire restricting transaction on exceeding the item quantity while the device is in offline mode.
- **Allowed Item Quantity:** Specify the number of item quantity to be allowed when the device is in offline mode. This will be applicable for each item present in the Menu.

For example, if the Menu has two items Tea and Poha and you have configured the **Allowed Item Quantity** as 2, then when the device is offline, the user/worker will be allowed to consume Tea twice as well as Poha twice.

Printer Settings

- **Printer:** Select the printer from the drop-down list based on the site requirements.
- **Connection Type:** Select the printer connection type from the drop-down list. The options available are:
 - RS232 (serial)
 - USB
- **Baud Rate:** In the event of a serial printer, select the appropriate baud rate from the drop-down list.
- Specify the **Company Name**, **Company Address** and the **Punch Line** as per the site requirements. These details will be printed on the receipt dispensed from the selected printer.
- **Exclude Price-Cost From Coupon:** Select this check box if you want to exclude the price from the coupon.
- **User Balance On Coupon:** Select the check box, if you want Current Balance/ Current Month Usage and Weekly Remaining Limit to be printed on the Cafeteria receipt.

For pre-paid account users, Current Balance and Weekly Remaining Limit will be printed.

For post-paid account users, Current Month Usage and Weekly Remaining Limit will be printed.

For details refer to [“Cafeteria Usage Policy”](#).

Menu

Click the **Menu** tab.

COSEC allows the administrator to assign one or more Cafeteria Menus (Menu 1, Menu 2, Menu 3... upto 99.) to a device. These can be configured by selecting pre-defined menus from the Menu picklist.



The Menu is created from Cafeteria module.

The Menu can also be scheduled from Cafeteria module which will be displayed under “Schedule Menus” in above screen.

If you have to assign menu and schedule it on the door from Device Configuration page, then select the Menu from the picklist. The Menu will be displayed in the grid as shown below.

Now to schedule the Menu click **Add**.

Menu No	ID	Menu Name	Start Time	End Time	Schedule Days
	2	Menu 2	09:00	11:00	Select

- **ID:** Click the picklist to select the desired Menu ID
- **Name:** Click the picklist to select the desired Menu Name.
- **Start Time/End Time:** Specify the **Start Time** and **End Time** for which the Menu will be active and is available to users on the selected door.
- **Days:** Select the **days** for which this menu will be available, that is, scheduled on the door.
- Click **OK** and **Save** to save the Menu schedule on the door.



Two Menus cannot be scheduled for the same timing.

Face Settings



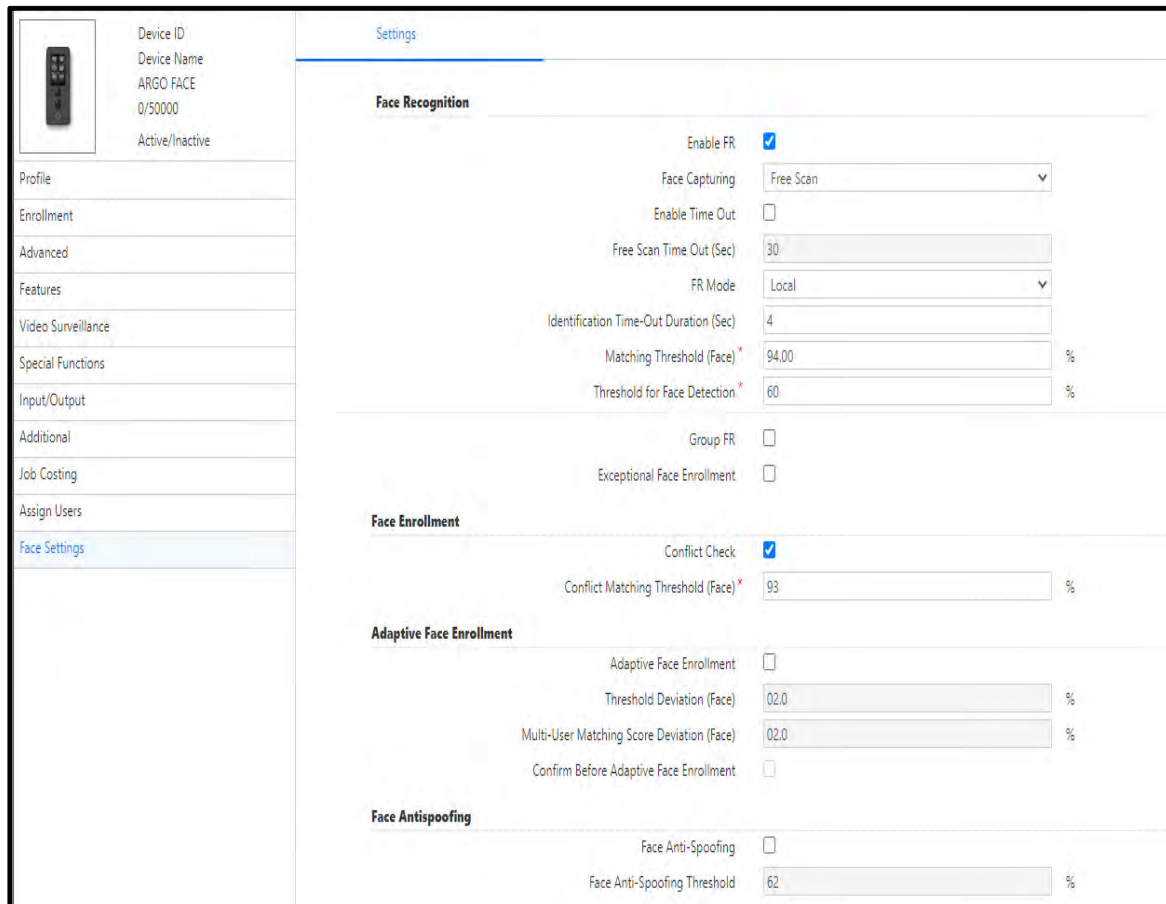
Face Settings (except Group FR which is applicable for Direct Door only) are applicable for both Direct Door and Panel Door.

ARGO Face as Panel Door supports FR Mode - Local only.

Device has a limited memory capacity for storage of templates so we need the Identification Server which will store more number of templates and respond to the device when asked for identification.

For more information on Identification Servers, see *Admin> System Configuration> Identification Server Configuration*.

On the Device Configuration page, click **Face Settings** on the left pane.



Settings	
Face Recognition	
Enable FR	<input checked="" type="checkbox"/>
Face Capturing	Free Scan
Enable Time Out	<input type="checkbox"/>
Free Scan Time Out (Sec)	30
FR Mode	Local
Identification Time-Out Duration (Sec)	4
Matching Threshold (Face) *	94.00 %
Threshold for Face Detection *	60 %
Face Enrollment	
Conflict Check	<input checked="" type="checkbox"/>
Conflict Matching Threshold (Face) *	93 %
Adaptive Face Enrollment	
Adaptive Face Enrollment	<input type="checkbox"/>
Threshold Deviation (Face)	02.0 %
Multi-User Matching Score Deviation (Face)	02.0 %
Confirm Before Adaptive Face Enrollment	<input type="checkbox"/>
Face Anti-Spoofing	
Face Anti-Spoofing	<input type="checkbox"/>
Face Anti-Spoofing Threshold	62 %

Face Recognition

- **Enable FR:** By default, this check box is enabled, that is Face Recognition feature is enabled in the device. Clear the check box to disable.



Make sure “**Enable FR**” flag is checked and “**Basic Access Control**” application is selected in Devices > Device Configuration > Profile > Basic > Optional > Application in order to edit the parameters in Face Settings.

- **Face Capturing:** Select the desired Face Capturing option.
 - **Tap and Go:** If you select this option, user needs to tap on the device screen once. The MJPEG, that is motion recording screen appears. Device will capture and then identify the users face. If during working hours device is idle, then user needs to tap the device to scan the face and gain access.
 - **Free Scan:** If you select this option, the device will display the MJPEG, that is motion recording screen till the expiry of the Free Scan Time Out timer.
 - **Enable Time Out:** Select this box to enable the time out.
 - **Free Scan Time Out (Sec):** Enter the Free scan time out duration. The valid range is 1 to 999 sec.

In Free Scan method, multiple users can mark their attendance easily during peak entry hours.

For example, if the Free Scan Time Out is set as 30sec and if the user is identified in 10S then the system reloads the Free Scan Time Out timer again. Hence, device remains in the scanning mode.

- **FR Mode:** Select the FR mode as **Local** or **Server Assisted**.



ARGO Face as Panel Door supports FR Mode - Local only.

- **Local:** In this Local mode Face templates will be stored in FR hardware module which can store 2 lakh face templates. The captured face template will be verified with the templates stored in the FR module.
- **Server Assisted:** In Server Assisted mode, an identification server and the fields to configure an individual identification server will get enabled as shown below. You must select the Identification server from where the face templates will be identified.

When FR Mode is selected as **Local** below mentioned parameters are to be configured:

Face Recognition		
Enable FR	<input checked="" type="checkbox"/>	
Face Capturing	Free Scan	▼
Enable Time Out	<input type="checkbox"/>	
Free Scan Time Out (Sec)	30	
FR Mode	Local	▼
Identification Time-Out Duration (Sec)	4	
Matching Threshold (Face) *	94.00	%
Threshold for Face Detection *	60	%
Group FR	<input checked="" type="checkbox"/>	
Exceptional Face Enrollment	<input type="checkbox"/>	
Face Enrollment		
Conflict Check	<input checked="" type="checkbox"/>	
Conflict Matching Threshold (Face) *	93	%
Adaptive Face Enrollment		
Adaptive Face Enrollment	<input type="checkbox"/>	
Threshold Deviation (Face)	02.0	%
Multi-User Matching Score Deviation (Face)	02.0	%
Confirm Before Adaptive Face Enrollment	<input type="checkbox"/>	
Face Antispoofing		
Face Anti-Spoofing	<input type="checkbox"/>	
Face Anti-Spoofing Threshold	62.00	%

- **Identification Time-Out Duration (Sec):** Specify the duration in seconds after which the face identification will get timed out.

Example: If 5 seconds is specified, then the identification server will try to identify the face till 5 seconds and if not found then it will show time-out to the user.

- **Matching Threshold (Face):** Enter the Matching Threshold in percentage for Face Recognition. This will be considered while face identification of the user. This value can be configured upto two decimal points. *Example:* If you set Matching threshold as low (e.g.: 20%) then false matching may be found. i. e. your Face may match with other person.

But if you set matching at high percentage (e.g.: 70%) then more accurate matching of your template will be done and accordingly access will be granted or denied.

- **Threshold for Face Detection:** Set the value in percentage. The system will consider this percentage as confidence of face presence in the received image. When the user image received is above this threshold it will be considered for further processing.

If you select FR Mode as **Server Assisted**, you must configure the following parameters:

User can either assign a separate or a common Identification Server which is shared by other biometric credentials.

The screenshot shows the 'Settings' page with a 'Face Recognition' section. The 'Enable FR' checkbox is checked. 'Face Capturing' is set to 'Free Scan'. 'Enable Time Out' is unchecked. 'Free Scan Time Out (Sec)' is set to 30. 'FR Mode' is set to 'Server Assisted'. 'Identification Server' has fields for 'ID' and 'Name'. 'Configure Alternate Server Address' is unchecked. 'Server Address' is empty. 'Server Port' is set to 11005. 'Identification Time-Out Duration (Sec)' is set to 4. 'Threshold for Face Detection' is set to 60%. Below this, 'Group FR' and 'Exceptional Face Enrollment' are unchecked. The 'Face Enrollment' section has 'Conflict Check' checked and 'Conflict Matching Threshold (Face)' set to 93%. The 'Adaptive Face Enrollment' section has 'Adaptive Face Enrollment' unchecked, 'Threshold Deviation (Face)' set to 02.0%, and 'Multi-User Matching Score Deviation (Face)' set to 02.0%. 'Confirm Before Adaptive Face Enrollment' is unchecked. The 'Face Antispoofing' section has 'Face Anti-Spoofing' unchecked, 'Face Anti-Spoofing Mode' set to 'Advance', 'Face Anti-Spoofing Threshold' set to 62.00%, and 'Default Biometric Group No.' set to 0.

- **Identification Server:** Select the Identification server from the picklist to which the device is to be assigned to save the records.
- **Configure Alternate Server Address:** Select this check box to configure external IP address of Identification Server.
- **Server Address:** By default, this will display the configured Identification Server for FR. This field allows user to enter the Alternate IP Address for FR if **Configure Alternate Server Address** is enabled.

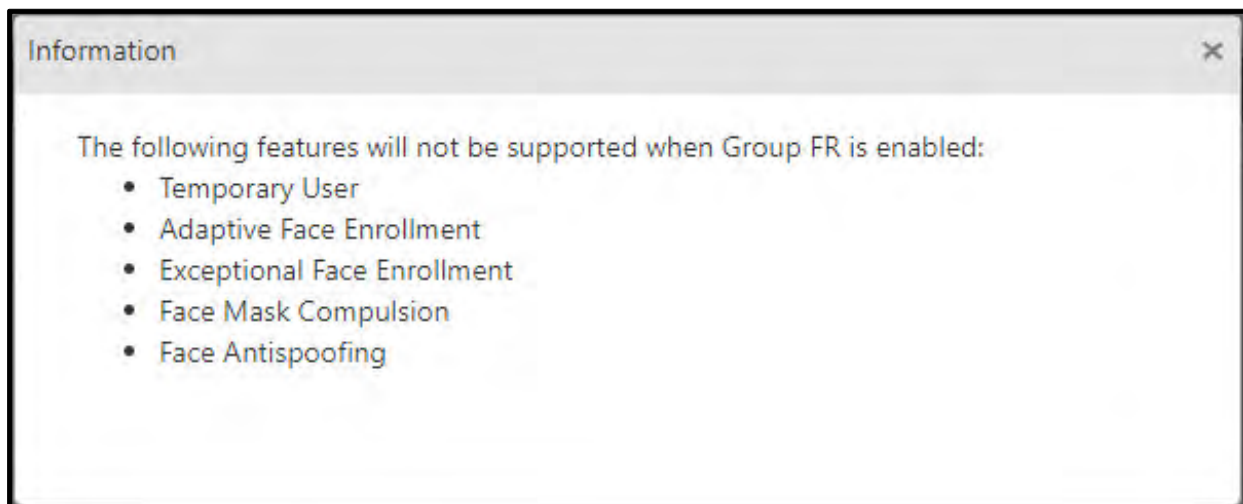
- **Server Port:** Enter the TCP port number. The default port number is 11005.
- **Identification Time-Out Duration (Sec):** Specify the duration in seconds after which the face identification will get timed out.
Example: If 5 seconds is specified, then the identification server will try to identify the face till 5 seconds and if not found then it will show time-out to the user.
- **Threshold for Face Detection:** Set the value in percentage. The system will consider this percentage as confidence of face presence in the received image. When the user image received is above this threshold it will be considered for further processing.



Group FR is applicable for Direct Door only.

- **Group FR:** Select this check box to enable face recognition feature for multiple users and marking their attendance at the same time via this door.

Once you enable Group FR, a pop-up will be displayed as shown below:



The features listed in the pop-up will not be functional.

- **Exceptional Face Enrollment:** Select this check box to enroll exceptional faces of users via this door.



For Group FR ("[Mark Group Attendance](#)") and Exceptional Face Enrollment feature to work, ensure that the desired Identification Service is selected in COSEC Admin > License and Service. For more details refer Admin Management Portal User Manual.



*If you have enabled the **Exceptional Face Enrollment** feature then make sure that you schedule a task of **Delete Exceptional Face** in Admin > System Utilities> Task Scheduler to avoid storage of excess data in the database.*

Face Enrollment



*If the **FR Mode** is **Server-Assisted** and you wish to enroll faces from the device, make sure **Enable Face Recognition** is selected in Users > User Configuration > Face Recognition and/or Visitor Management > Visitor Profile > Face Recognition and/or Contract Worker Management > Worker Profile > Face Recognition.*

- **Conflict Check:** Select the check box for the system to check the conflict between the new face of a user and the already (existing) enrolled faces of all the users (available in the database) during the face enrollment process.
- **Conflict Matching Threshold (Face):** Enter the desired Conflict Matching Threshold (Face) value in percentage.

The system will consider this value while comparing the face with the face templates already present in the database.

If a conflict is found, that is, if the system detects a face template in the database similar to the new face, then a conflict error will be displayed.

Make sure a higher value is set for this parameter, as it will result in less equivalent matches with the face templates available in the database.



*Make sure the **Conflict Matching Threshold (Face)** is set lower than **Matching Threshold** in **Admin module > System Configuration > Identification Server Configuration**.*

Example: Face Enrollment of Suresh

- **Conflict Check** check box is selected.
- **Conflict Matching Threshold (Face)** is set as 93%.

Now during the face enrollment of Suresh, the system will check in its database if his face matches with faces of other users available in the database.

- **Case 1:** If Suresh's face matches 92% with Ram, then the system will allow to enroll Suresh's face.
- **Case 2:** If Suresh's face matches 94% with Shyam, then the system will display the conflict error while enrolling Suresh's face.

Adaptive Face Enrollment

- **Adaptive Face Enrollment:** Select this check box to Enable Adaptive Face Enrollment for identification server.
 - Adaptive face enrollment provides automatic real time face enrollment whenever change is experienced in facial features.
 - Enabling adaptive enrollment process parameter, an additional slot will be provided internally to store 10 more face templates of a user.
 - IDS will learn from face recognized, adapt and would take decision of storing new template of a user database.

If you enable Adaptive Face Enrollment, you must configure the following parameters.

- **Threshold Deviation (Face):** Enter the value of deviation from matching threshold in percentage. Based on the value entered for deviation, template for Adaptive Face Enrollment will be decided.

Example: If deviation entered is 3% and matching threshold is 98% then it will classify template which has matching score between 98 - 95 and one lower than this will be classified below margin.

- **Multi-user Matching Score Deviation (Face):** Enter the value of deviation from matching score between 2 different users while Adaptive Face Enrollment.

Difference between matching scores of templates will be done, when we have templates of two or more users falling under above specified deviation.

Let us understand this with the help of the following example:

- *Threshold value = 98%*
- *Threshold Deviation= 3%*

So, Result will display all matching templates having matching score between range 98 to 95

- *Multi-user Matching score deviation = 0.5%*

If, 5 best templates of 2 users fall between 98 -95% range

User	Matching Score
User 1	97.8
User 1	97.6
User 1	97.4
User 2	97.25
User 2	97

As we have obtained templates of 2 users in which user 1 is having template of highest matching score, so will make a difference between lowest score template of user 1 and highest matching score template of user 2.

$97.4 - 97.25 = 0.15$; this is less than 0.5

As difference is less than 0.5, user 1's template having matching score 97.8 for adaptive enrollment will not be used.

- Threshold Deviation and Multi-user Matching score deviation will act as two filters to fetch appropriate template for adaptive enrollment. Values can be added in decimal.



We recommend to set the multi-user matching score deviation higher always e.g.2.0 to reduce the probability of enrolling a particular user's face template in some different user's enrolled faces.

- **Confirm before Adaptive Face Enrollment:** Select this check box, if face enrolled using Adaptive face enrollment requires confirmation from User.



Faces enrolled under Adaptive enrollment process will be synced automatically, but when IDS is restarted due to any reason, the adaptive faces which are not synced will be removed by default.

Face Antispoofing

- **Face Anti-Spoofing:** To use this feature, make sure **Enable FR** check box is selected.

Select the Face Anti-Spoofing check box to enable this feature.

- **Face Anti-Spoofing Threshold:** Enter the Face Anti-Spoofing threshold value in percentage within the range from 1.00 to 99.99 to identify user's face liveness for considering him/her as genuine person.

Click **Save**.

Special Functions

COSEC provides its users the privilege to perform certain pre-defined operations directly from the COSEC device. These operations are related to various time and attendance marking functions, administrative tasks, zone-related access and door-control functionality as well as alarms management. It also provides privilege to schedule these special functions. A special function may be used in three different ways by a user -

- Entering short codes on the device keypad.
- Navigating the device menu.
- Using Special Cards.

To access this functionality, select **Devices> Multi-Device Options> Special Functions**.

“Single Device Special function”

“Multiple Device Special functions”

Special Cards

A *Special Card* is especially useful when the user has to perform routine tasks, where repeated manual entry of codes can become tedious. It is also required when a door controller device does not have keypad or LCD display for manual entry of special codes. In such a case, an RFID card can be encoded for a special function and the card-holder can perform a special function at the device just by showing this special card.

Example: In factories where workers avail shortleave; security guard can show the Special card enrolled for Shortleave IN on the Entry door and can give the access to the worker. This same card can be used for multiple workers.

Configuring Special Functions

The COSEC system pre-defines 38 special functions for its users. These functions are supported differently by different COSEC devices. For instance, all the special functions in the given list are supported on all COSEC Panel200. The following list provides details of some of the available special functions and the devices they are supported on:

Time and Attendance Functions: *(Available only with the Time & Attendance add on module)*

Special Function	Available on	Description
Official Work-IN / Official Work-OUT	Panel200 and DIRECT DOORS.	Late-IN as well as Early-OUT is marked as User's Official work in Time & Attendance.
Short Leave-IN / Short Leave-OUT	Panel200 and DIRECT DOORS.	Late-IN as well as Early-OUT is marked as User's short leave in Time & Attendance.
Regular - IN / Regular - OUT	Panel200 and DIRECT DOORS.	Normally used in Time & Attendance system in the absence of an exit reader. The punch in at start of shift and punch out at end of shift are sent with the appropriate flags.
Break End / Break Start	Panel200 and DIRECT DOORS.	Clock-IN is marked as User post break entry and Clock-OUT is marked as User exit at start of break.
Late-IN Start / Late-IN Stop	Panel200 and DIRECT DOORS.	System starts / stops inserting the special ID to T&A events of all users who clock-IN after this function.
Early-OUT Start / Early-OUT Stop	Panel200 and DIRECT DOORS.	System starts / stops inserting the special ID to T&A events of all users who clock-OUT after this function.

Special Function	Available on	Description
Over Time - IN / Over Time - OUT	Panel200 and DIRECT DOORS.	The IN punch is marked as User entering at start of over time while the OUT punch is marked as User exiting after completion of overtime.

Administrative Functions: *(Available with the Basic platform license.)*

Special Function	Available on	Description
Enroll User	Panel200 and DIRECT DOORS	Application switches the door controller mode to Enrollment mode and User Credentials are enrolled against the defined user ID. Global Enrollment mode is selected by default for users.
Enroll Special Card	Panel200 and DIRECT DOORS	Application switches the door controller mode to Enrollment mode and special Cards are enrolled against special function ID
Delete Credentials	Panel200 and DIRECT DOORS	Enables user to delete the existing credential data from the PANEL User database against the selected user ID.
View User Profile	Panel200 only.	System reads the User's Smart Card and displays the stored user profile.

Zone Settings: *(Highlighted options available only with the Access Control add on module)*

Special Function	Available on	Description
Activate DND / Deactivate DND	Panel200 only.	System switches the door zone from Normal to DND and vice versa.
Activate Dead-Man / Deactivate Dead-Man	Panel200 only.	System switches all Door Controllers of the zone from Normal mode to activated Dead Man Zone mode and vice versa.
Door Lock / Door Unlock	Panel200 and DIRECT DOORS.	System locks/unlocks the selected Door. Entry is denied to all users. Exit request however, is enabled and the user can still provide T&A events.
Zone Lock / Zone Unlock	Panel200 only.	System locks/unlocks all Doors of the Zone. Entry is denied to all users. Exit request however, is enabled and the user can still provide T&A events.
Door Normal	Panel200 and DIRECT DOORS.	System switches the mode of the door controller to the normal or controlled mode.
Zone Normal	Panel200 only.	System switches the mode of all Doors of the Zone to the normal or controlled mode.
Guard Tour	Panel200 only.	The security guard carries the guard tour card which is linked to the guard tour-ID.

Alarms: *(Available only with the Access Control add on module)*

Special Function	Available on	Description
Set Panic Alarm	Panel200 only	System enables the user to generate a Panic Alarm from the Door Controller.
Mute Door Buzzer	Panel200 only	Enables the user to mute the Door Controller's existing Alarms.
Mute Panel Buzzer	Panel200 only	Enables the user to mute the PANEL's existing Alarms.

Special Function	Available on	Description
Clear Door Aux O/P	Panel200 only	Enables the user to Reset the Aux output of Door Controller and switch it back to Normal/Controlled state from its current state.
Clear Panel Aux O/P	Panel200 only	Enables the user to Reset the Alarm output of PANEL and switch it back to Normal/Controlled state from its current state.
Door Arm/Door Disarm	Panel200 only	To enable/disable door alarms using special function cards.
Zone Arm/Zone Disarm	Panel200 only	To enable/disable zone alarms (for all doors in the zone) using special function cards.
Clear Alarm	DIRECT DOORS only.	Enables the user to clear all the alarms at the DIRECT DOOR.

Cafeteria: (Available only with the Cafeteria add on module)

Special Function	Available on	Description
Sold Out	Cafeteria devices	System enables the user to mark an item as Sold Out.
Available	Cafeteria devices	Enables the user to mark an item as available.

Single Device Special function

To configure special functions for a single device,

- Select the **Devices module > Device Configuration > Special Functions**

The **Special Functions** page opens as follows, for a Door V3:

Device Configuration									
Search Device ID or Name									
Configuration Shortcuts Schedule									
No.	Function Name	Active	Job Selection	User Group	Card-1	Card-2	Card-3	Card-4	
1	Official Work - IN	Yes	Yes	All					
2	Official Work - OUT	Yes	Yes	All					
3	Short Leave - IN	Yes	Yes	All					
4	Short Leave - OUT	Yes	Yes	All					
5	Regular - IN	Yes	Yes	All					
6	Regular - OUT	Yes	Yes	All					
7	Break End	Yes	Yes	All					
8	Break Start	Yes	Yes	All					
9	Overtime - IN	Yes	Yes	All					
10	Overtime - OUT	Yes	Yes	All					
11	Enroll User	Yes	No	All					
12	Enroll Special Card	Yes	No	All					

1. Select a **Function Name** from the list on the Special Functions page.

No.	Function Name	Active	Job Selection	User Group	Card-1	Card-2	Card-3	Card-4
1	Official Work - IN	Yes	Yes	All				
2	Official Work - OUT	Yes	Yes	All				
3	Short Leave - IN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	All	1453			
4	Short Leave - OUT	Yes	Yes	All				
5	Regular - IN	Yes	Yes	All				
6	Regular - OUT	Yes	Yes	All				
7	Break End	Yes	Yes	All				
8	Break Start	Yes	Yes	All				
9	Overtime - IN	Yes	Yes	All				
10	Overtime - OUT	Yes	Yes	All				
11	Enroll User	Yes	No	All				
12	Enroll Special Card	Yes	No	All				

2. Check the **Active** box to enable the function.
3. Click the **User Group** drop down list and select the *Functional Group* for which this special function will be activated.
4. Specify the Card Serial Number (CSN) or a Comma separated CSN in the **Card** fields which would be registered to activate the special function at the devices. To know about the format of entering the Card details, refer **Access Card 1** in "*Credentials*" under *Users> User Configuration> Credentials> Access Card 1*.
5. Click **OK** after all the member cards have been added to save the defined parameters. Administrator can define up to 4 member cards per function. User can also assign cards to the special functions using the *Enrollment* option as explained in the "*Enrolling Special Cards*" section.

Multiple Device Special functions

To configure Special Functions for multiple devices, Select the **Devices module > Multi-Device Options > Special Functions**.

The **Multi-Device Special Function** page opens as follows:

Update	Function Name	Active	User Group	Card-1	Card-2	Card-3	Card-4
<input type="checkbox"/>	Official Work - IN	<input type="checkbox"/>	No Change				
<input type="checkbox"/>	Official Work - OUT	<input type="checkbox"/>	No Change				
<input checked="" type="checkbox"/>	Short Leave - IN	<input checked="" type="checkbox"/>	No Change	9876	6543		
<input type="checkbox"/>	Short Leave - OUT	<input type="checkbox"/>	No Change				
<input type="checkbox"/>	Regular - IN	<input type="checkbox"/>	No Change				

Device Type: Select the device type from the dropdown list.

Function: Select the special function which needs to be activated on the devices by checking the corresponding **Update** checkbox.

Active: Select the Active checkboxes for activating the special function on the selected devices.

User group: Some special functions can be assigned to specific user groups. For eg: “Enroll User” special function can be assigned to the desired User group from the drop down list as shown below.

Device Type		Panel Lite V2	
<input type="checkbox"/>	Overtime - IN	<input type="checkbox"/>	No Change
<input type="checkbox"/>	Overtime - OUT	<input type="checkbox"/>	No Change
<input type="checkbox"/>	Set Panic Alarm	<input type="checkbox"/>	No Change
<input checked="" type="checkbox"/>	Enroll User	<input checked="" type="checkbox"/>	RnD
<input type="checkbox"/>	Enroll Special Card	<input type="checkbox"/>	No Change
<input type="checkbox"/>	Delete Credentials	<input type="checkbox"/>	Staff
<input type="checkbox"/>	Late IN - Start	<input type="checkbox"/>	Visitor
<input type="checkbox"/>	Late IN - Stop	<input type="checkbox"/>	RnD
<input type="checkbox"/>	Late IN - Stop	<input type="checkbox"/>	No Change

Card: Specify the Card Serial Number (CSN) or a Comma separated CSN in the **Card** fields which would be registered to activate the special function at the devices. To know about the format of entering the Card details, refer **Access Card 1** in “[Credentials](#)” under *Users> User Configuration> Credentials> Access Card 1*.

Update	Function Name	Active	Job Selection	User Group	Card-1	Card-2	Card-3
<input checked="" type="checkbox"/>	Official Work - IN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Change	5698		
<input type="checkbox"/>	Official Work - OUT	<input type="checkbox"/>	<input type="checkbox"/>	No Change			
<input checked="" type="checkbox"/>	Short Leave - IN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Change	1256		
<input type="checkbox"/>	Short Leave - OUT	<input type="checkbox"/>	<input type="checkbox"/>	No Change			
<input type="checkbox"/>	Regular - IN	<input type="checkbox"/>	<input type="checkbox"/>	No Change			
<input type="checkbox"/>	Regular - OUT	<input type="checkbox"/>	<input type="checkbox"/>	No Change			

Filter

Device Filter: All

Update

Device Filter: Select the device randomly or all on which the special functions are to be activated.

Example: If 3 doors of type Door V3 are selected; then Official IN function can be accessed on these doors using the card with number 5698.


The screenshot shows a web interface titled "Filter". At the top, there is a "Device Filter" dropdown menu set to "Randomly". Below it, there are input fields for "Device" (containing "ID") and "Name". A search bar is also present. The main area contains a table with two columns: "ID" and "Name". The table has one row with the value "1" in the "ID" column and "Door v3" in the "Name" column. To the right of the table is a trash icon. Below the table is an "Update" button.

ID	Name
1	Door v3

Click on **Update** button to save the changes. This will enable the users to punch for “Official IN” function using card (5698) along with their respective credential on the Door V3.

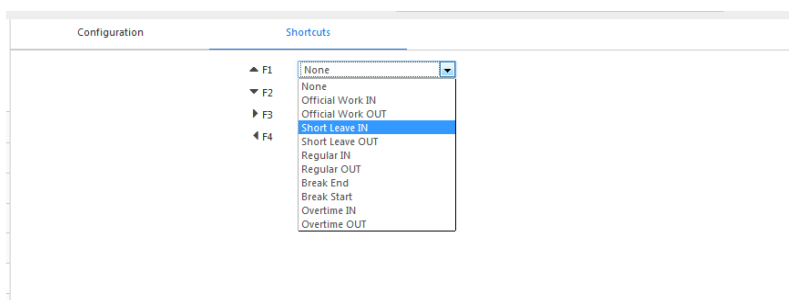
Special Functions Shortcuts

The COSEC application enables the user to map up to 4 special functions to the arrow keys on a Direct Door/Panel Door keypad. To do this,

1. Select a device on which the shortcuts are to be configured.
2. On the **Device Configuration** page, select the **Special Functions** tab.
3. Click **Edit** .
4. Under the **Special Functions** tab, select the **Shortcuts** section as shown below:

The screenshot shows the "Device Configuration" window. On the left, there is a sidebar with a list of configuration options: Profile, Enrollment, Advanced, Features, Video Surveillance, Special Functions (highlighted), Input/Output, Additional, Job Costing, Assign Users, and Identification Server. The main area is divided into three tabs: Configuration, Shortcuts (selected), and Schedule. Under the Shortcuts tab, there are four rows, each with a key (F1, F2, F3, F4) and a dropdown menu. All dropdown menus are currently set to "None".

5. Use the drop down lists for the appropriate arrow keys to assign a special function to each key, as per the site requirements.




6. Click **Save**  .



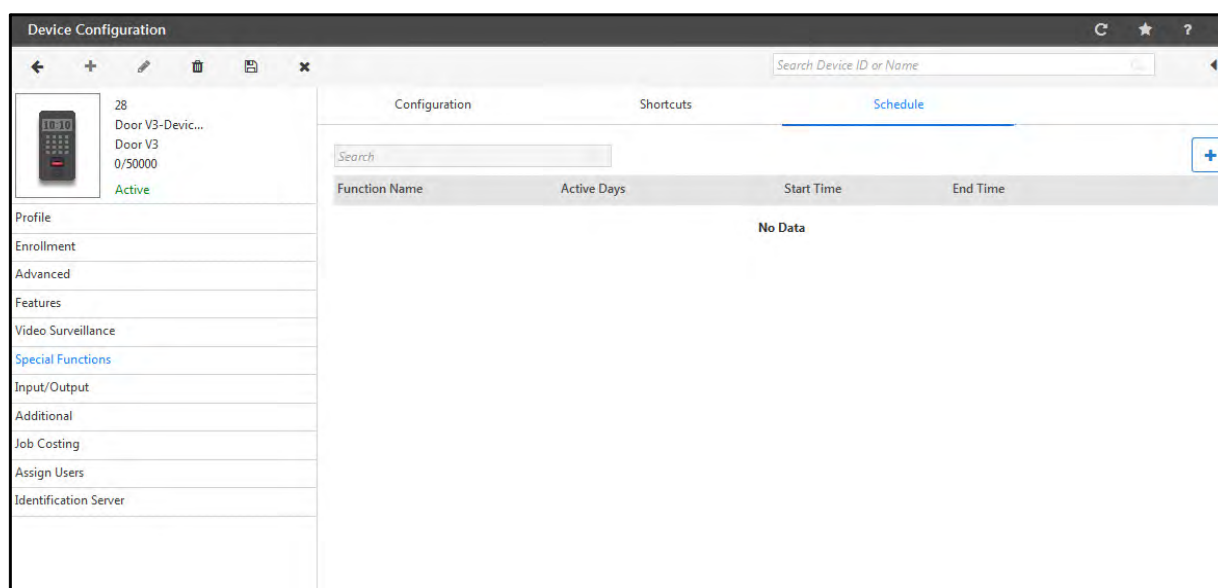
This option is not available for the NGT DOOR.

Special Functions Schedule

The COSEC application enables the user to schedule special functions for specified time range on a Direct Door/ Panel Door keypad. To do this,

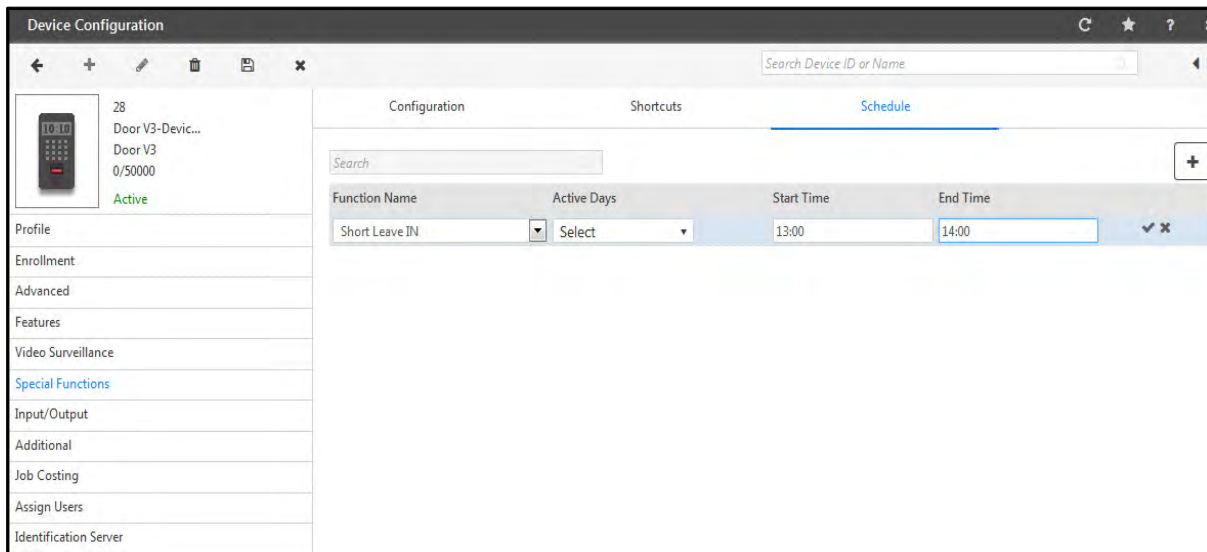
1. Select a device on which the scheduling is to be done.
2. On the **Device Configuration** page, select the **Special Functions** tab.
3. Click **Edit**  .

Under the **Special Functions** tab, select the **Schedule** section as shown below:



4. Click **Add**  .

5. Specify the **Function Name**, **Active Days**, **Start Time** and **End Time** as shown below:



6. Click on the **Tick**  to save the schedule.

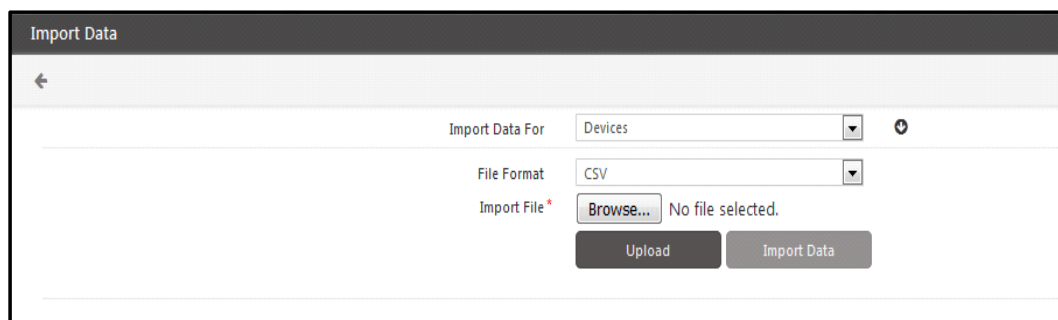
7. Click **Save**  .

Import Devices

The COSEC application has an inbuilt utility for enabling users to import data from excel files with predefined format. This would thus save the end user a lot of time and effort in having to make individual data entries at the application level.

To import device data from a file, select the **Devices module > Multi-Device Options > Import Devices**.

The **Import Data** page appears as shown.



The following options appear for configuration on the **Import Data** page.

- **Import Data For** - The Data is to be imported for Devices by default. You can download the sample import file and enter the data for devices. Then the updated file can be imported here.
- **File Format** - Select the file format to be imported. The options available are XLS or CSV.
- **Import File** - Browse the path of the file from which the data is to be imported.

Click **Upload** button to save the file. The **Preview Data** button enables the administrator to view the data in the respective worksheets to confirm that the data is in order prior to giving the import command.

Click on **Import** to start the import of data.

While importing the data from the User Worksheet, the system enables the administrator to directly assign controllers to the users while importing the user data.

Select the controllers to be assigned to the imported users by checking the boxes against the relevant controllers and click on **Import**. The system will import all the relevant valid entries from the sheet and will display the status in the bottom grid.



Administrator needs to ensure that the ASP.NET user has full rights on the folder containing the Excel or .csv file for the import data operation.

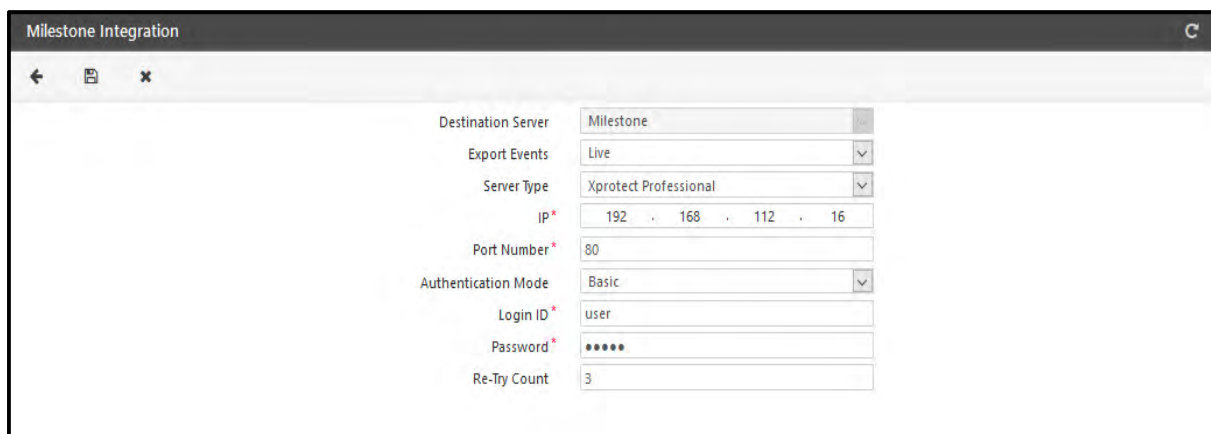
Milestone Integration

This feature enables the *COSEC Access Control Monitoring System* to be integrated with the *Milestone XProtect Video Management Software*. The integration provides a common platform and supports the following functions:

- Triggering Milestone User-Defined Events based on COSEC Events.
- Retrieving images captured by Milestone Devices.

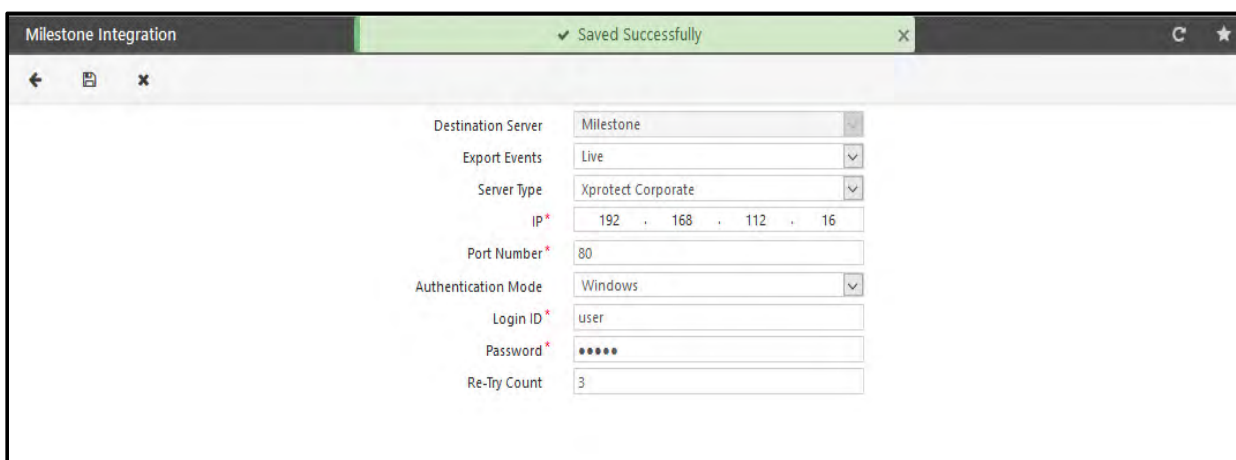
To set up Milestone Integration, Select the **Devices module > Milestone Integration**

The page will appear as shown:



The screenshot shows the 'Milestone Integration' configuration window. It contains the following fields and values:

Field	Value
Destination Server	Milestone
Export Events	Live
Server Type	Xprotect Professional
IP *	192 . 168 . 112 . 16
Port Number *	80
Authentication Mode	Basic
Login ID *	user
Password *	*****
Re-Try Count	3



The screenshot shows the 'Milestone Integration' configuration window after a successful save. A green message bar at the top indicates 'Saved Successfully'. The field values are updated as follows:

Field	Value
Destination Server	Milestone
Export Events	Live
Server Type	Xprotect Corporate
IP *	192 . 168 . 112 . 16
Port Number *	80
Authentication Mode	Windows
Login ID *	user
Password *	*****
Re-Try Count	3

Export Events: Select the type of COSEC Events to be exported from the drop-down list. You can select All or Live events.

Server Type: Select the Milestone Server Type for integration and enter the Server **IP** address and **Port** Number as configured for the selected Milestone server.

Authentication Mode: Select the Authentication mode as **Basic** or **Windows**.

- Enter the Milestone server login credentials (Login ID and Password) for Authentication.



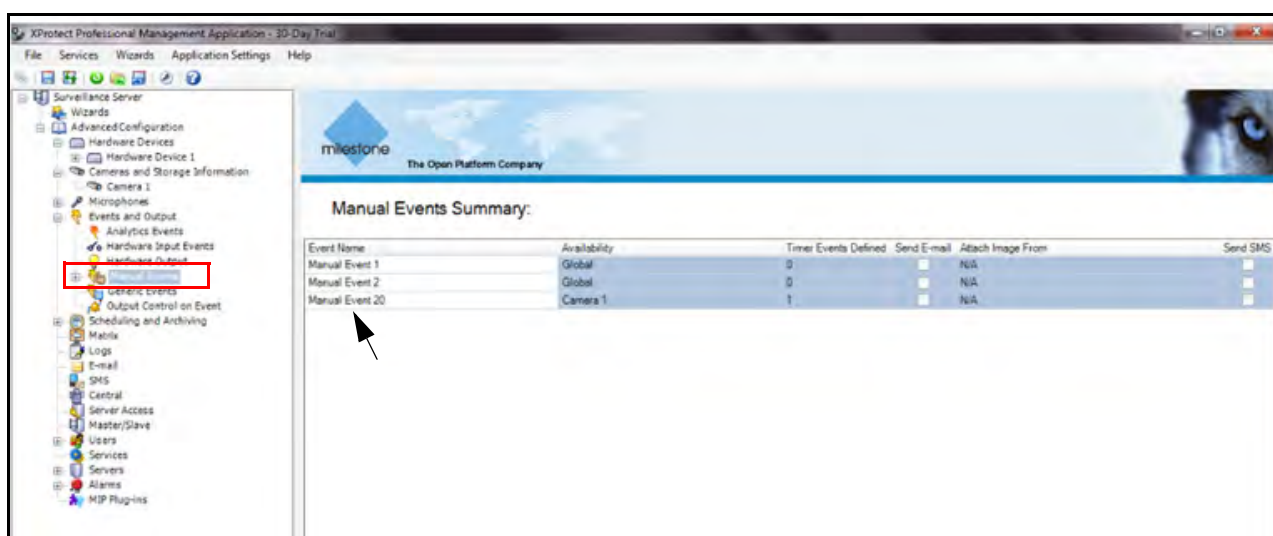
Windows Authentication Mode has been implemented & verified for Milestone - Corporate edition only.

Re-Try Count: The count must be numeric and will determine the number of times connection request will be renewed in case of failure to establish connection with Milestone server.

Then click **Save** to save the configuration.

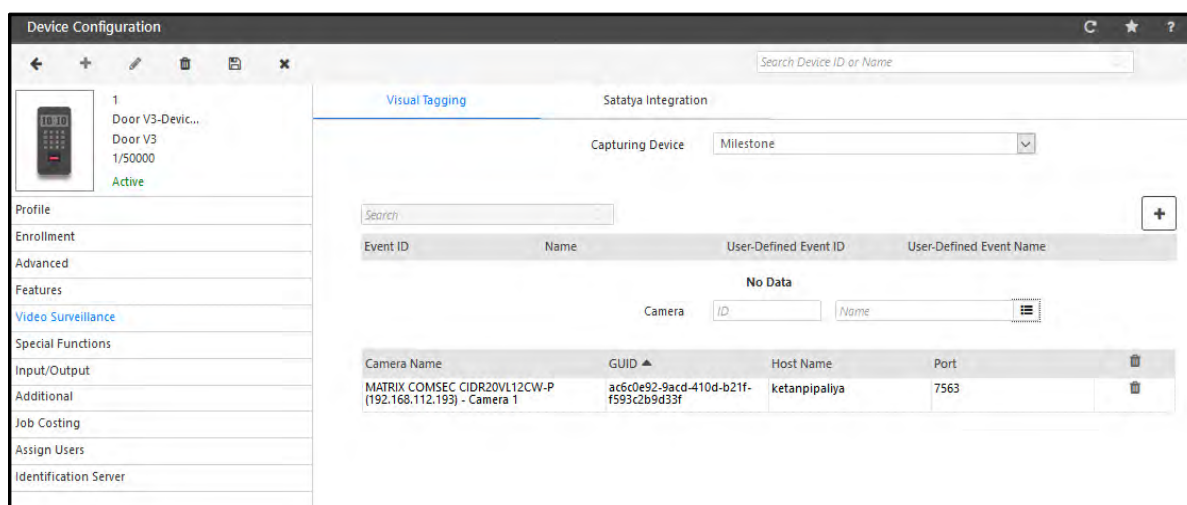
Mapping Milestone and COSEC events

Using this feature, the administrator can map Milestone user-defined events to be triggered based on COSEC Events. For this, *Manual Events* must first be defined on the *Milestone XProtect Management Application* as shown.



Now, to map these User defined events against COSEC events, go to **Devices > Device Configuration** (Select a Device) > **Video Surveillance > Visual Tagging**.

Select the **Capturing Device** as Milestone.



Select a COSEC Event using the corresponding picklist.

Click on **Add** button. Select the COSEC event and User defined Milestone event which is to be mapped with the selected COSEC Event. Then click OK to save the mapping.

The mapped events will appear in the grid as shown.

Event ID	Name	User-Defined Event	
101	Allowed	Manual Event 1	
104	Allowed - Dead Man Zone	Manual Event 1	

Camera Name	GUID	Host Name	Port	
Camera 1	1D17801D-7810-4958-B3EF-8C335BADE69F	192.168.153.144	800	

Camera: For each door, COSEC can also request images from the Milestone server against the mapped events. To do this, select a camera from a list of Milestone cameras using the **Camera** pick-list.

Picklist For Milestone Device

Total Selected : 0 Records

Search

Show Selected

<input type="checkbox"/>	Camera Name	GUID	Host Name	Port
<input type="checkbox"/>	MATRIX COMSEC CIDR20VL12CW-P (192.168.112.193) - Camera 1	ac6c0e92-9acd-410d-b21f-f593c2b9d33f	ketanpipaliya	7563
<input type="checkbox"/>	MATRIX COMSEC MIDR20FL60CWP (192.168.112.61) - Camera 1	d40ca39c-809c-4ce0-9e11-72d471a7abbd	ketanpipaliya	7563

OK Cancel

Click on OK and Save the configuration to complete the integration.

Device Configuration

1

Door V3-Devic...

Door V3

1/50000

Active

Profile

Enrollment

Advanced

Features

Video Surveillance

Special Functions

Input/Output

Additional

Job Costing

Assign Users

Identification Server

Visual Tagging

Sataty Integration

Capturing Device

Milestone

Search

+

Event ID	Name	User-Defined Event ID	User-Defined Event Name
No Data			

Camera

ID

Name

+

Camera Name	GUID	Host Name	Port	
MATRIX COMSEC CIDR20VL12CW-P (192.168.112.193) - Camera 1	ac6c0e92-9acd-410d-b21f-f593c2b9d33f	ketanpipaliya	7563	

When user punches on door say Access Allowed event is generated; then image captured by camera will be displayed in User Events as shown below:

User Events

Date *

12/09/2018

12/09/2018

Filter By

Individual

User *

1320

Shruti Patki

View

Attendance Events (2)

Search

User ID ▲	User Name	Date-Time	Device Name	I/O	Access	Source	Source Details	Location Details		View Image
1320	Shruti Patki	12/09/2018 10:56	Vega Controller-Device-8y	Entry	Allowed	Device				
1320	Shruti Patki	12/09/2018 10:55	Vega Controller-Device-8y	Entry	Denied	Device				



Access Control Events (0)

Visitor Events (0)

1320

Shruti Patki

12/09/2018 10:56:20

Managing Sites

A site is a distinct work area or unit within an enterprise with its specific access control and/or attendance marking needs. For instance, in a retail enterprise (say “ABC”), the access system for customers at retail outlets must be different than the access system implemented for warehouse employees. In this case, the administrator can define two separate sites, one for the store (say “ABC-Store”) and one for the warehouse (say “ABC-Warehouse”).

To create a Site, Go to **Devices Module > Masters > Site**.

The following page will appear:

The screenshot shows the 'Site' management window. On the left, there is a form with fields for 'Site ID' (containing '1'), 'Name' (containing 'Site-1'), 'Default' (unchecked), 'Consider As Assembly Point' (unchecked), and 'Default Biometric Group No.' (empty). Below these is a 'Devices On This Site' dropdown. On the right, a table lists existing sites:

ID	Name
1	Site-1

Click **New** button to add a Site.

Site: Enter a unique site name (Eg: “ABC-Store”) in the **Name** field. The ID will be genrated by the system automatically.

Default: Select this checkbox to make this site as a default site.

Consider As Assembly Point: Enable the checkbox to consider the configured site as assembly point. During an emergency situation, all the users are expected to assemble at this assembly point.

Default Biometric Group No.: Specify the Default Biometric Group No. to be assigned to the site. It is a number allotted to the site to be assigned to the devices belonging to that particular site. This enables the Identification Server to match the template against only those devices that belong to the corresponding biometric group site.

Click **Save** button to save the site as shown below.

The screenshot shows the 'Site' management window after saving a new site. The form fields are now: 'Site ID' (containing '2'), 'Name' (containing 'Matrix- RnD'), 'Default' (checked), 'Consider As Assembly Point' (unchecked), and 'Default Biometric Group No.' (containing '0'). The 'Devices On This Site' dropdown is still present. On the right, the table now lists two sites:

ID	Name
1	Site-1
2	Matrix- RnD

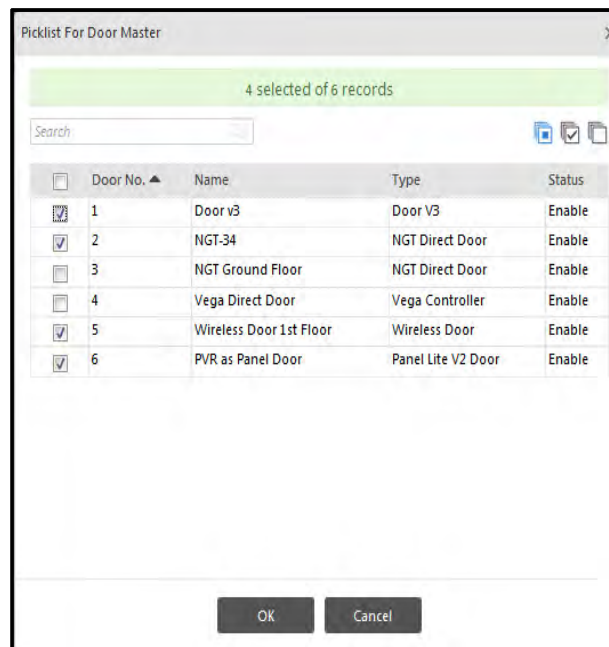
An arrow points to the newly added site 'Matrix- RnD' in the table.

Adding Devices to a Site

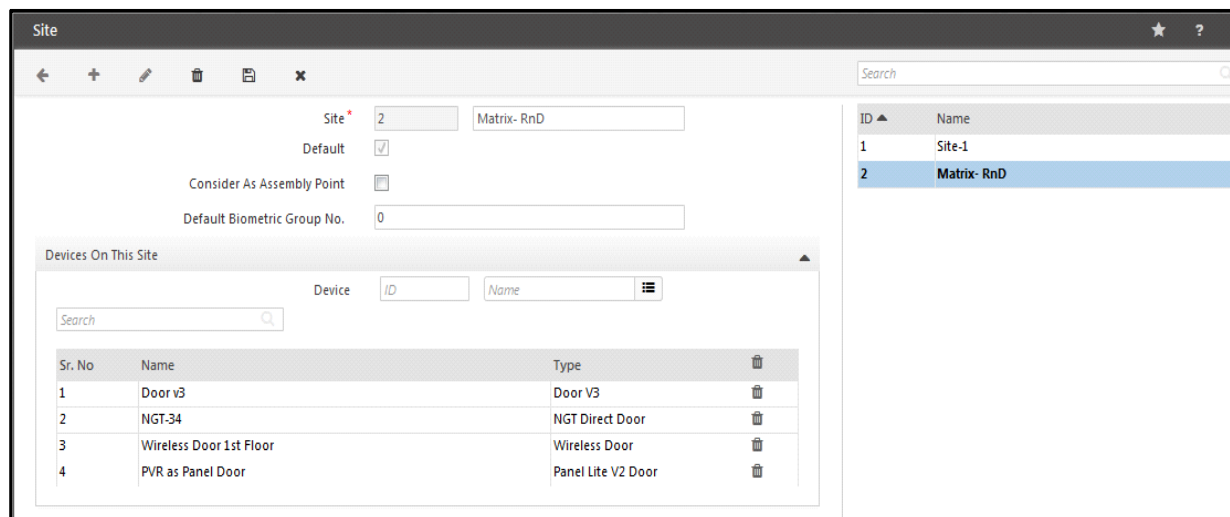
Each COSEC device can be assigned to a site. To do this, select **Devices On This Site** section.

Click **Edit** button.

Devices: Click the picklist and select the device to be assigned to the Site. Click **OK** button.



All devices assigned to this site will be listed in the grid as shown below.



On deletion of any device from the device list, the status of the respective site will be automatically changed to “default”. For a “default” site, devices can not be deleted from the device list.

Device Group

This option enables the administrator to assign multiple devices to a group. This functionality facilitates assignment of users to a group of devices.

To define a device group, select **Devices Module > Masters > Device Group**.

The **Device Group** page appears as shown below.

ID	Name
No Data	

Click **New** to configure a new device group.

- **ID:** This is a system-generated ID automatically assigned to each new device group.
- **Name:** Enter a unique device group name in this field.
- **Type:** Select the type of device group to be assigned. The options are **device group** and **super group**.



A **super group** is a group or collection of multiple device groups.

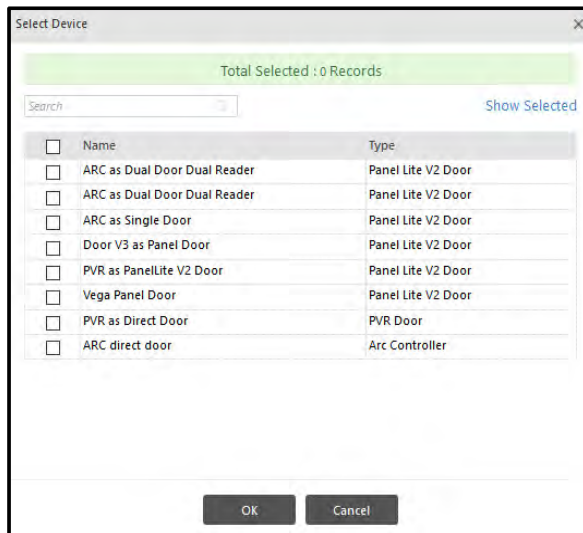
Click the **Save** button to save the device group.

A new device group is created successfully. All defined device groups can be viewed in the grid list view on the right-hand side of the page as follows:

ID	Name
1	Device Group-RnD

Assigning Devices to Device Group

Select **Assign Devices** section. You can add devices to the device group by selecting the device from the picklist as shown below.

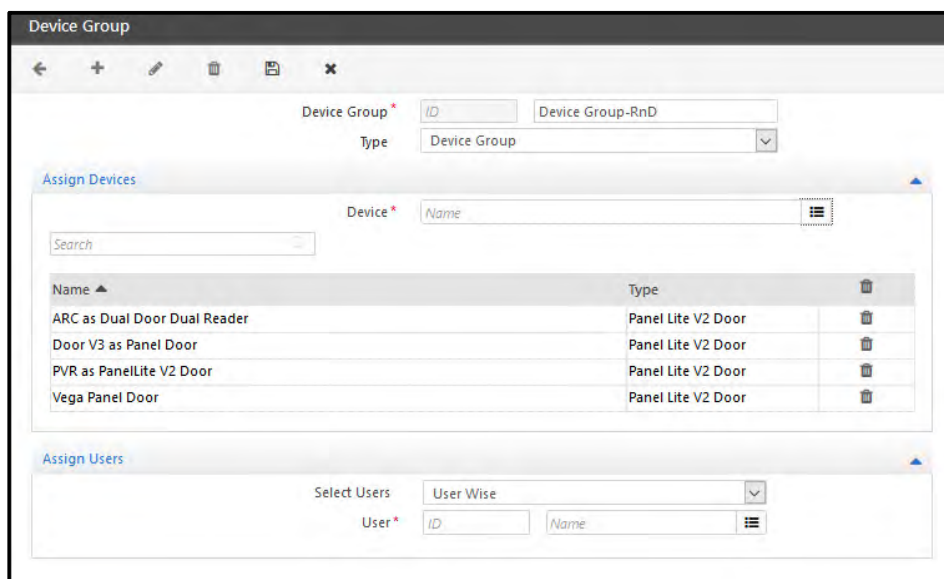


The 'Select Device' dialog box shows a table of available devices. The 'Total Selected' is 0 Records. The table lists various device names and their types.

Name	Type
ARC as Dual Door Dual Reader	Panel Lite V2 Door
ARC as Dual Door Dual Reader	Panel Lite V2 Door
ARC as Single Door	Panel Lite V2 Door
Door V3 as Panel Door	Panel Lite V2 Door
PVR as PanelLite V2 Door	Panel Lite V2 Door
Vega Panel Door	Panel Lite V2 Door
PVR as Direct Door	PVR Door
ARC direct door	Arc Controller



The device appearing in the device picklist will be Panel, Panel Lite, Panel200 Doors & Direct Doors only.



The 'Device Group' configuration window shows the 'Assign Devices' section. It includes a search bar and a table of assigned devices.

Name	Type
ARC as Dual Door Dual Reader	Panel Lite V2 Door
Door V3 as Panel Door	Panel Lite V2 Door
PVR as PanelLite V2 Door	Panel Lite V2 Door
Vega Panel Door	Panel Lite V2 Door

Click **Save** button to save the device group.

The device/devices are assigned to the specified device group successfully.

Device Group

✓ Saved Successfully

Device Group* 1 Device Group-RnD

Type Device Group

Assign Devices

Device* Name

Search

Name	Type
ARC as Dual Door Dual Reader	Panel Lite V2 Door
Door V3 as Panel Door	Panel Lite V2 Door
PVR as PanelLite V2 Door	Panel Lite V2 Door
Vega Panel Door	Panel Lite V2 Door

Assign Users

Select Users User Wise

User* ID Name

Search

ID	Name
1	Device Group-RnD

Assigning Users to Device Group

To assign users to a device group, select a device group from the right grid.

Select **Assign Users** section. You can assign the users based on filter options of Userwise, Groupwise or All.

Assign Users

Select Users User Wise

User* ID Name

Search

User ID	Name
1687	Aditi Gupta
103	Kruti Boghani
1688	Anu Bhatt

Click **Save** to save the assignment of users to all devices in the device group.

 The maximum number of device group allowed against a user is 99.

Any user/s exceeding the value of maximum allowed device group will not be assigned any device group.

Such user/s shall be displayed under the Exceptions tab.

Card Formats

All proximity cards store a sequence of numbers which can be read by card reader devices, when a card is swiped. This unique card number sequence is then verified against a user enrolled on the COSEC access control system to allow access to the card-holder. Hence, the pattern or structure of this card number must be compatible with the corresponding card reader format to support identification. This programmable data pattern of a proximity card is known as its *card format*.

Different card manufacturers across the industry provide some standard as well as proprietary card formats. However, organizations may require a format flexibility to match their site requirements. COSEC provides a unique option for users to write their own card formats to be compatible with their access control system.

Users can define upto 99 card profiles in COSEC. Custom Formats allow the user to enhance security by:

- Setting formats of up to 128 bits.
- Providing the option to add Facility Code to the Card Serial Number.
- Adding Parity bits for added accuracy of sent data.

To create a new card format, Select the **Devices Module > Masters > Card Format**.

The page will appear as shown below.

The screenshot shows the 'Card Format' configuration window. It has a top toolbar with icons for back, add, edit, delete, save, and close. A search bar is in the top right. The main form contains the following fields:

- Card Format***: A dropdown menu with 'ID' selected.
- Name**: A text input field.
- Max. No. Of Bits***: A text input field with '1-128'.
- Read Order**: A dropdown menu with 'Forward'.
- Include FC in Card No.**: A checkbox.
- Configurable Bits***: A text input field with '0-128'.
- Sequence of Operation**: A dropdown menu with 'Reading Order then Bit Configuration'.

Below the form is the **Bit Configuration** section. It has a title 'Select a color and click on Bits to define Card Reading Pattern' with a refresh icon. On the left is a legend with four items: 'Even Parity' (blue), 'Odd Parity' (orange), 'Facility Code' (grey), and 'Card Serial Number' (dark grey). To the right is a 16x8 grid of bits, numbered 1 to 128. The 'Card Serial Number' option is currently selected, highlighting all bits in dark grey.

Click **New** button to configure a card format.

Card Format: Enter a suitable name for the card format. The ID will be autogenerated by the system when the format is saved.

Max No. of bits: Specify the maximum number of bits that will be allowed for the format. Only the number of bits mentioned here will be considered for further processing. Remaining bits will be truncated. Maximum value can be 128 bits.

Read Order: It indicates the sequence in which the card serial number should be read by the card reader. The user should be aware of the reading order of the card reader before configuring this option.

Specify the Read Order as one of the following:

- **Forward** - This implies that the bits should be processed in the order of their arrival.
- **Reverse bitwise** - This implies that all incoming bits will be received and then reversed before processing them further.
- **Reverse byte-wise** - This implies that each incoming byte will be reversed separately and then used for further processing.

Include FC in Card No.: Enable this checkbox to ensure that the Card Number or Card ID includes Facility Code as well as Card Serial Number.

Configurable Bits: Specify the number of bits that will be configured in the card structure.

Eg: If 32 bits are set as configurable bits; then Bit Configuration grid will display 1 to 32 bits for configuration.



If the number of bits received at the card reader is greater than the number of configured bits, then default card format applicable for the reader will be used.

Sequence of Operation: Select the sequence of operation based on which operation is to be performed first and then second between Reading Order and Card Format Configuration.

In the **Bit Configuration** section, all configurable bits of the card data will appear numerically in a serial order, from left to right, as boxes. Here, each box represents a bit.

In the **Color Selection** area, click to select a colour that represents the bit type to be added to the card number. Then drag the cursor across boxes where the selected bit type is to be placed and select the box.

Click **Save** button to save the card format. The new format will now appear in the grid list on the right hand side of the page.



If you have configured Comma separated CSN as Access Card Value for Users, Visitor Profile and/or Worker Profile, make sure in the Card Format you configure Max. No. of bits and Configurable bits as 26 bits. Do not change any other settings. Save and assign this Card Format to the desired device. To know more about Comma separated CSN, refer Access Card 1 under "Credentials" in Users> User Configuration> Credentials> Access Card1.

The Card format can be assigned to the device from Device Configuration> Profile> Readers.

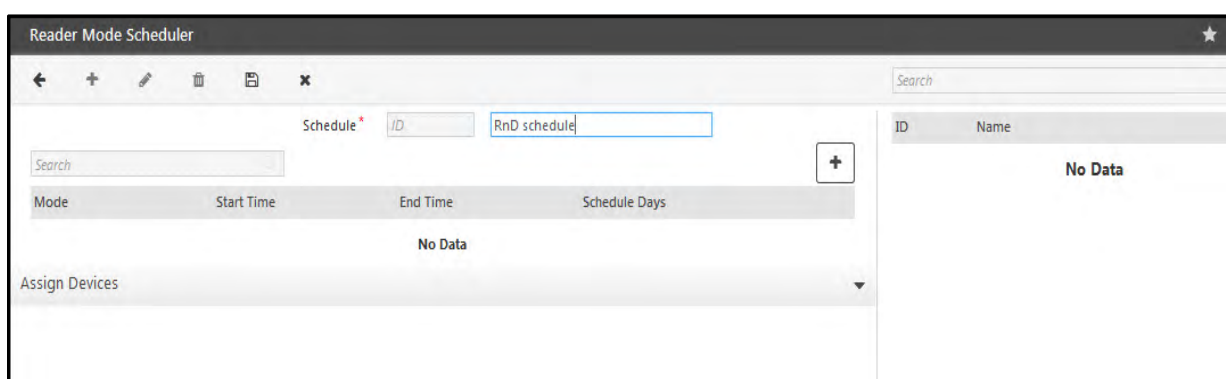
Reader Mode Scheduler

A device has Internal and External Readers, wherein the Internal Reader is mandatory and in Entry mode by default. The Exit mode is optional and can be replaced with an exit switch also. The **Reader Mode Scheduler** feature enables automated control for the mode of an Internal Reader. Using this feature, the same reader can be configured to function both in Entry as well as Exit mode based on scheduled timings.

User can create maximum 15 schedules in COSEC. To create a new Reader Mode Schedule,

Select the **Devices Module > Masters > Reader Mode Scheduler**.

The page will appear as shown below.

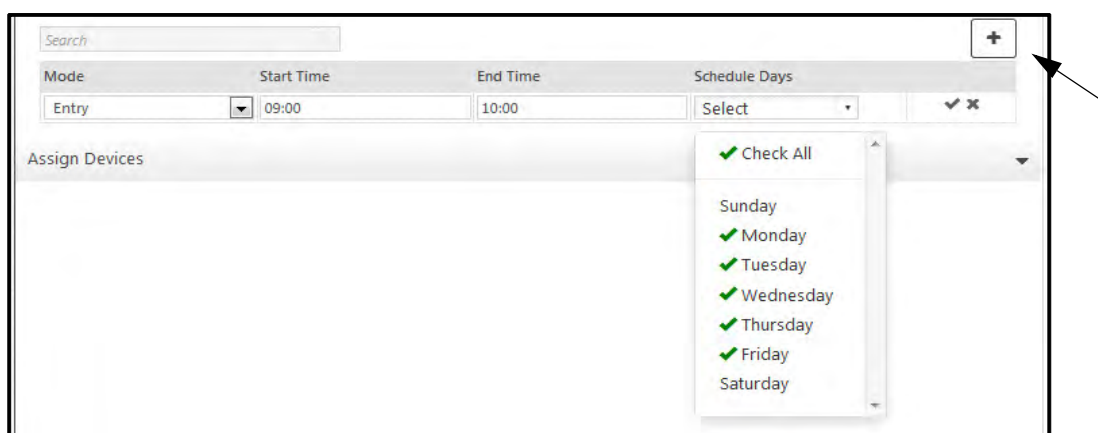


The screenshot shows the 'Reader Mode Scheduler' window. It has a search bar at the top right. Below it, there's a 'Schedule' section with an 'ID' field containing 'RnD schedule' and a '+ Add' button. The main table has columns: Mode, Start Time, End Time, and Schedule Days. The table is empty with 'No Data' displayed. At the bottom, there's an 'Assign Devices' section.

Click **New** button to define new reader mode scheduler.

Schedule: Enter a user-friendly name for the new schedule. The ID will be generated by the system automatically.

Click **Add** button to define the timing for entry and exit mode as shown below.



This screenshot shows the 'Add' button being clicked, which opens a dropdown menu for selecting days of the week. The menu options are: Check All, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. The 'Add' button is highlighted with a red arrow.

Select the **Mode** for the schedule as *Entry* or *Exit*.

Enter the **Start** and **End** time for the schedule in HH:MM format.

Select the **days** of the week for which the new schedule would be applicable.

Click the **OK** button to create the new schedule as shown below.

The screenshot shows the 'Reader Mode Scheduler' window. At the top, there's a toolbar with icons for back, add, edit, delete, save, and close. Below the toolbar, there's a search bar and a 'Schedule' dropdown menu with 'ID' and 'RnD schedule' options. A table lists the schedule details:

Mode	Start Time	End Time	Schedule Days
Entry	09:00	10:00	_ Mo Tu We Th Fr _
Exit	13:00	14:30	_ Mo Tu We Th Fr _

Below the table is an 'Assign Devices' section. On the right, there's a sidebar with a search bar and a list of schedules. The list is currently empty, showing 'No Data'.

Click **Save** to save the new schedule. The schedule now appears in the grid list on the right hand side of the page.

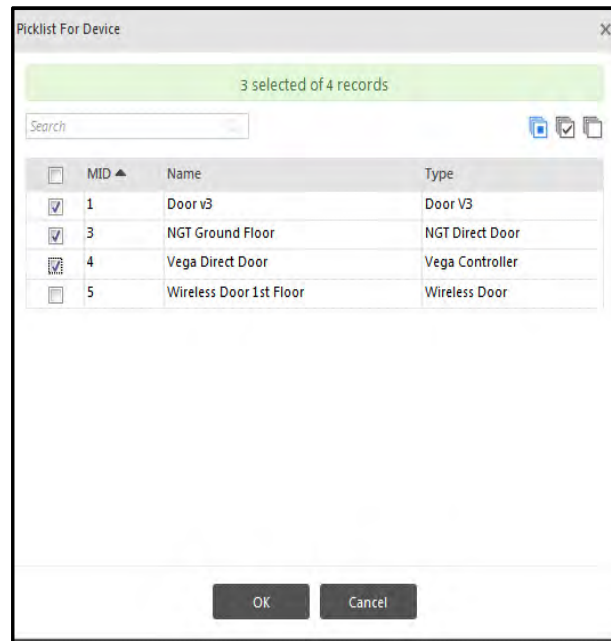
The screenshot shows the 'Reader Mode Scheduler' window after saving. A green notification bar at the top says 'Saved Successfully'. The 'Schedule' dropdown menu now shows '1'. The table of schedule details remains the same. In the sidebar on the right, the schedule list now contains one item: '1 RnD schedule', which is highlighted by a mouse cursor.

In the above example, a scheduler is set between 13:00 PM and 14:30 PM (break) on all week days (Mon-Fri), during which configured readers would register all punches in Exit Mode only. This will be especially useful when more doors are required in Exit mode at shift end time. Similarly, doors can also be scheduled to turn to Entry mode during shift start hours.

The user can assign a Reader Mode Schedule to selected devices configured in COSEC. Select a schedule and select the **Assign Devices** section.

The screenshot shows the 'Assign Devices' section. It has a search bar and a table with columns 'MID', 'Name', and 'Type'. The table is currently empty, showing 'No Data'. Below the table is an 'Assign' button.

Devices: Select one or more devices from the picklist.



Click **OK** after selecting devices. Then click **Assign** to save the settings.



*This feature is applicable on the following door controllers (direct doors only) - **Wireless Door, PVR Door, NGT Controller, Vega Controller, Door V3.***

Wiegand Output Format

In COSEC, Wiegand readers can send outputs not only in the standard formats or the actual information, but also in a custom data format whose structure can be defined. The COSEC administrator can use this page to create and save multiple profiles for different Wiegand Output Formats. Based on the output required, Wiegand output format in the Device Configuration module should be selected for allowed and denied events.

The admin can create maximum 9 Wiegand Output Formats.

To create a new format, Select the **Devices Module > Masters >Wiegand Output Format**.

The page will appear as shown below.

Click **New** button to add a new Weigand format.

Format: Enter a suitable **name** for the format. The ID will be autogenerated when the format is saved.

Output Bits: Enter the number of bits to be configured in Wiegand Output Format. For eg: If 32 is entered, then the configurable bits will become 32 as shown below.

The following fields can be defined in the Wiegand output format by using different **color** for each of the below mentioned fields:

- Even Parity
- Odd Parity
- Facility Code
- Card No.
- Access Code (indicates to the 3rd party panel whether the user has been allowed or not by the device)

In the **Color Selection** area, click to select a colour that represents the bit type to be added to the new format. Now, click to select the boxes where the selected bit type is to be placed. For e.g. In the above figure, Facility Code is placed across the bits 2-4.

Facility Code: If Facility Code is marked in the output bits, you must specify the source from where it must be read i.e. from Card No., from Card Personalization data or as per Device Configuration as shown below.

Replace with Card No. If FC not found: When FC is not obtained then you can select the alternate option of card number to send for FC by enabling this check box.

Read FC from Device: If access mode is kept as "Biometrics"/"Biometrics + PIN" and if FC is set to be read from card no. then FC will never be obtained, so in such cases which does not have card as any form of access mode, then FC stored in device can be sent by checking this box.

- The applicable devices are PVR, Vega Controller, Panel200

Click to **Save** the output format. The new format will now appear in the grid list on the right side of the page.



- *If a Wiegand Output format is edited and saved, it will be automatically sent to all the devices to which this format is assigned.*
- *The maximum bits of Facility Code and Card No. should be as defined in “**Card Personalization**” page of the Devices module. They should be selected one at a time.*
- *At a time, “Access Code” should be of 1 bit only but user can select it to be of more than 1 bit and till maximum 20 bits.*

Card Personalization

Card Personalization is used when you want to configure all the fields of the card with your choice.

This page allows users to program the memory mapping of smart cards as per their requirement. Users can configure their own card format by adding user-defined fields as well as modifying length, type and location of pre-defined fields on the different available memory sectors in specific **HID iClass** and **MiFare** cards. A total of maximum **99** fields can be configured for each personalized format.

This feature enables to:

- Add or modify fields such as name, ID, department, shift, fingerprint templates etc. to be written on the Smart Card.
- Add new fields starting from index 1 having pre-defined field as "Facility Code and define upto 99 fields.
- To configure location of pre-defined and the newly added fields.
- To change field type and length of pre-defined fields.
- To configure a field profile based on card type and card mode.

To use this feature, Select the **Devices Module > Card Personalization**.

The page will appear as shown below.

The screenshot shows the 'Card Personalization' window. On the left is a sidebar with 'Field List' and 'Configuration'. The main area contains a form to add a new field with fields for 'Field Name' (with a hint '30 chars'), 'Field Type' (a dropdown menu), and 'Max Field Length (Bytes)'. Below the form is a search bar and a table of existing fields. The table has columns for Index, Field Name, Field Type, Length (Bytes), and a delete icon. The table contains 5 rows of data. Below the table is a pagination bar showing '1 - 5 of 22 records' and a set of navigation buttons. At the bottom are 'Save' and 'Cancel' buttons.

Index	Field Name	Field Type	Length (Bytes)	
1	Facility Code	Numeric	2	
2	Additional Security Code	Numeric	2	
3	User ID	Numeric	4	
4	Value	Numeric	4	
5	User Name	Text	15	

Field List

On the Card Personalization page, select the **Field List** tab.

The screenshot shows the 'Card Personalization' window with the 'Field List' tab selected. On the left is a sidebar with 'Field List' and 'Configuration' tabs. The main area contains a form for adding a new field with the following fields: 'Field Name' (Date of Birth), 'Field Type' (Date), 'Date Type' (ASCII), 'Date Format' (ddmmyy), 'Separator' (/), and 'Max Field Length (Bytes)' (8). Below the form are 'Add' and 'Cancel' buttons. A search bar is located above a table of predefined fields. An arrow points to the 'Add' button.

Index	Field Name	Field Type	Length (Bytes)	
1	Facility Code	Numeric	2	
2	Additional Security Code	Numeric	2	
3	User ID	Numeric	4	
4	Value	Numeric	4	
5	User Name	Text	15	

1 - 5 of 22 records

Navigation: << 1 2 3 4 5 >>

Buttons: Save, Cancel

The index no. **1 - 50** is reserved for predefined fields. By default predefined fields are available from **1 to 24**. The user defined fields can be added from index no. **51 till 99**. You can add new field as per your requirement.

Field Name: Enter a field name for the new field.

Field Type: Specify the field type as Text, Numeric or Date.

- For Text and Numeric fields, specify the Max Field Length in bytes.
- For a Date field, specify a date type, format and separator. Based on your selection the maximum field length will be automatically determined.

The maximum length allowed for PIN on card is 3 bytes for numeric format and 6 bytes for text format.

Click the **Add** button. The new field will be added to the grid list as shown below:

The screenshot shows the 'Card Personalization' window with the 'Field List' tab selected. The form fields are: 'Field Name' (30 chars), 'Field Type' (Text), and 'Max Field Length (Bytes)' (empty). Below the form are 'Add' and 'Cancel' buttons. A search bar is located above a table of predefined fields. An arrow points to the 'Date of Birth' field in the table.

Index	Field Name	Field Type	Length (Bytes)	
21	User Finger Template 2	Raw	384	
22	Card No.	Numeric	8	
23	Smart Access Route ID	Numeric	1	
24	Max Route Level	Numeric	1	
	Date of Birth	Date	8	

21 - 25 of 25 records

Navigation: << 1 2 3 4 5 >>

Buttons: Save, Cancel

Click the **Save** button to save the new field.



If some pre-defined field's type is changed from text to numeric, the admin should make sure to have only numeric value in such fields. If any mismatch occurs, then while writing or reading information from card, conversion will not be performed and the field shall remain <Blank>.

Configuration

On the Card Personalization page, select the **Configuration** tab.

Card Type: Select a Card Type from the drop-down list. Hover your mouse on the icon to view information on each card type.

Card Mode: Select the Card Mode as **Default** to use the default card format where location of each field is fixed as per card type selected. If **Custom** mode is selected then location of all pre-defined fields will be allowed to be changed as per available memory sectors on the card.

1. **Default:** Select the Card Mode as Default to use the default card format where location of each field is fixed as per card type selected.
 - **Card No.:** If Default Card Mode is selected, you can specify if the Card No. to be used is the original **CSN**, or **UID** (Universal Identifier number).
2. **Custom Mode:** If Custom mode is selected then location of all pre-defined fields will be allowed to be changed as per available memory sectors on the card. Maximum 99 newly created fields will be accepted for such card types.
 - **Card No.:** If Custom Card Mode is selected, you can specify if the Card No. to be used is the original **CSN**, **UID** or **Custom** card no. as is defined at the time of enrollment. While location of CSN is fixed, it is mandatory to define a Field Profile for Custom Card Nos.



UID is supported in HID iClass cards only.

Card Type: iClass 2K2
 Card Mode: Default
 Card No.: CSN

Card Type: iClass 2K2
 Card Mode: Custom
 Card No.: CSN
 Read CSN: ☐



When you have selected Custom card no., you must specify the Card no. from User Configuration> Credentials during enrollment of card. The number specified in Access Card field will get write over the card. See [““Credentials””](#) on page 382.

Read CSN: If Card No. is selected as Custom, then “Read CSN” check-box is activated. Checking this box allows to read CSN number in case custom number is failed to read.

Valid Values	iClass 2K2	iClass 16K2	iClass 16K16	MiFare 1K	MiFare 4K
Available Page	Page0 (Total=1)	Page0 (Total=1)	Page0-Page6	NA	NA
Available Sector	NA	NA	NA	Sector0-Sector15 (Total=16)	Sector0-Sector39 (Total=40)
Available Block	19-31 (for all pages)	19-255 (for all pages)	19-31 (Page0), 6-31 (Page1-Page6)	1-2 (Sector0), 0-2 (Sector1-Sector15)	1-2 (Sector0), 0-2 (Sector1-Sector31), 0-14 (Sector32-Sector39)
Available Byte	0-7	0-7	0-7	0-15	0-15

Field Profile

For the Custom Card Mode, location on the card memory can be defined for each selected field. For this click the **Add** button and select a **Field** using the picklist button as shown below.

Card Type: iClass 2K2
 Card Mode: Custom
 Card No.: Custom
 Read CSN: ☐

Field Profile

Search:

Field	Start Position(Page-Block-Byte)	End Position(Page-Block-Byte)	Length(Bytes)
1 Facility Code	0 20	1	2

Save Cancel



If card number is selected as Custom, then it is must to add the field 22: Card No. in the field profile. If card number is set as CSN, then selecting field 22 is not mandatory.



When Card Mode is selected as "Custom" and Card No. is selected as "UID" then Card No. cannot be configured in field profile grid.

Specify the **Page** and **Block** on the card and number of **Bytes** to be used depending on the field type and the available memory for the selected field. Click the **OK** button. Similarly, add other required fields to card. Then click the **Save** button.

The configured field will appear on the grid list showing the Start and End position as shown below.

Field	Start Position(Page-Block-Byte)	End Position(Page-Block-Byte)	Length(Bytes)	
Facility Code	0-19-1	0-19-2	2	
Card No.	0-20-0	0-20-7	8	

Save Cancel



If the Custom Card mode is selected, all fields, their length, location and types should be reflected as per Card Personalization across COSEC applications such as COSEC Enroll at the time of card enrollment.

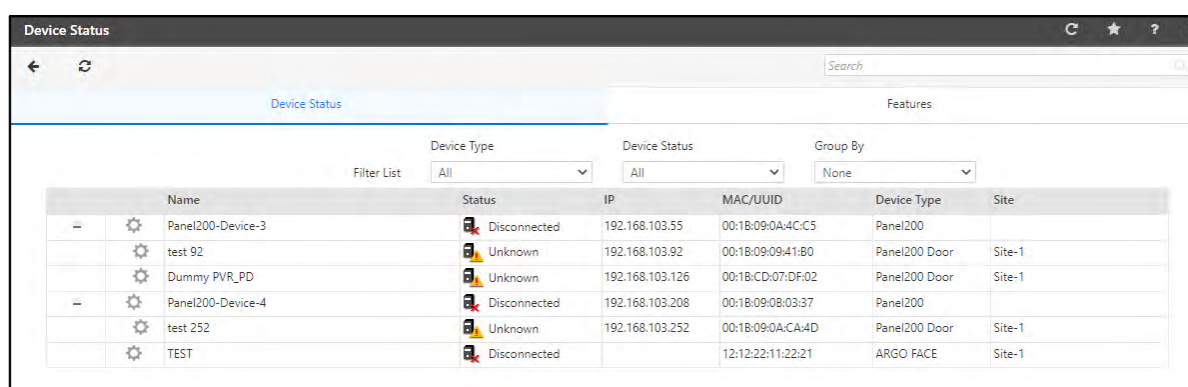
Device Status

The COSEC Web application enables the administrator to view the online or offline status of all configured devices as well as to send some basic control commands to the connected devices. This makes it easier for the administrator to keep track of disconnected devices and their respective sites and also to filter out lists of specific devices.

The administrator can view and reset the I/O linked events. It also provides the administrator the authority to Soft Override certain Access Control Features.

To view device status, select the **Device module > Device Status**.

The **Device Status** page will appear as follows.



Name	Status	IP	MAC/UUID	Device Type	Site
Panel200-Device-3	Disconnected	192.168.103.55	00:1B:09:0A:4C:C5	Panel200	
test 92	Unknown	192.168.103.92	00:1B:09:09:41:80	Panel200 Door	Site-1
Dummy PVR_PD	Unknown	192.168.103.126	00:1B:CD:07:DF:02	Panel200 Door	Site-1
Panel200-Device-4	Disconnected	192.168.103.208	00:1B:09:0B:03:37	Panel200	
test 252	Unknown	192.168.103.252	00:1B:09:0A:CA:4D	Panel200 Door	Site-1
TEST	Disconnected		12:12:22:11:22:21	ARGO FACE	Site-1

There are two tabs displayed namely:

- “Device Status”
- “Features”

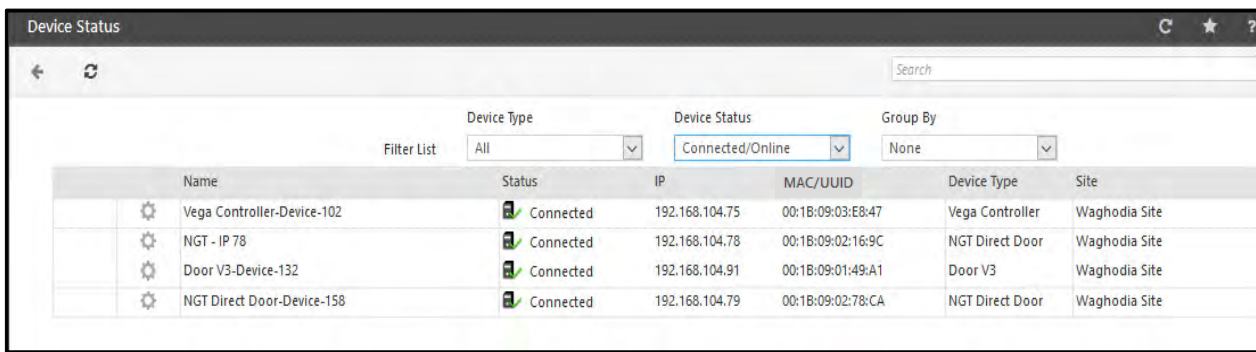
Device Status

Select **Device Status** tab to view the status of all the devices added to the Server. The **Device Status** page lists the devices and shows their **Name**, **Status**, **IP**, **MAC Address/ UUID**, **Device Type** and **Site**.

You can view the devices based on filters of:

- **Device Type**
- **Device Status** (All/Connected/Disconnected)
- **Group By** (None/Site/Device Type)


Once filters are applied, the filtered devices with their current status will appear in the list as shown below.



The screenshot shows the 'Device Status' window with a search bar and filters. The table below lists the devices currently connected.

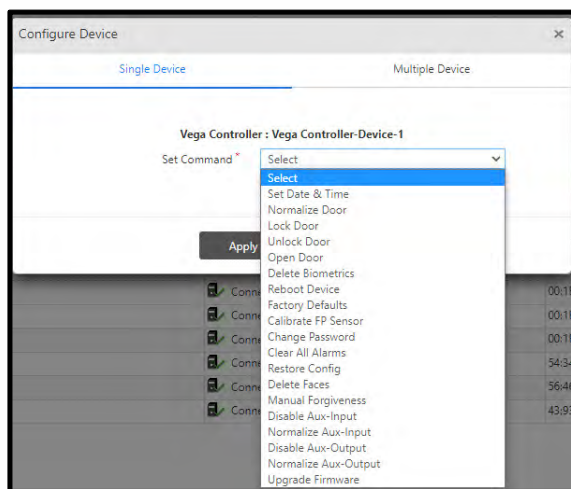
Name	Status	IP	MAC/UUID	Device Type	Site
Vega Controller-Device-102	Connected	192.168.104.75	00:18:09:03:E8:47	Vega Controller	Waghodia Site
NGT - IP 78	Connected	192.168.104.78	00:18:09:02:16:9C	NGT Direct Door	Waghodia Site
Door V3-Device-132	Connected	192.168.104.91	00:18:09:01:49:A1	Door V3	Waghodia Site
NGT Direct Door-Device-158	Connected	192.168.104.79	00:18:09:02:78:CA	NGT Direct Door	Waghodia Site

Sending Commands to Devices

The administrator can send direct commands to the selected device by clicking on  from the **Device Status** page.

The **Configure Device** window appears as shown below.

For a **Single Device**, select the Command from the **Set Command** drop down list and click **Apply** to set the command to the device.



These commands include:

- **Set Date & Time** - Sends the current system date and time to the device.
- **Normalize/Lock/Unlock/Open Door**- Sends the appropriate commands to the DOOR to reset the door lock status and open the door.
- **Delete Biometrics** - Sends command to delete the biometrics from the selected device.
- **Reboot Device** - Sends the reboot command to the device.
- **Factory Defaults** - Sends the command to default the device settings to the default factory settings.

- **Calibrate FP Sensor**- Sends the command to calibrate the finger print sensor.
- **Change Password** - Sends command to change the password of selected user on the COSEC device.
- **Clear All Alarms** - Sends the command to clear all alarms configured on the system.



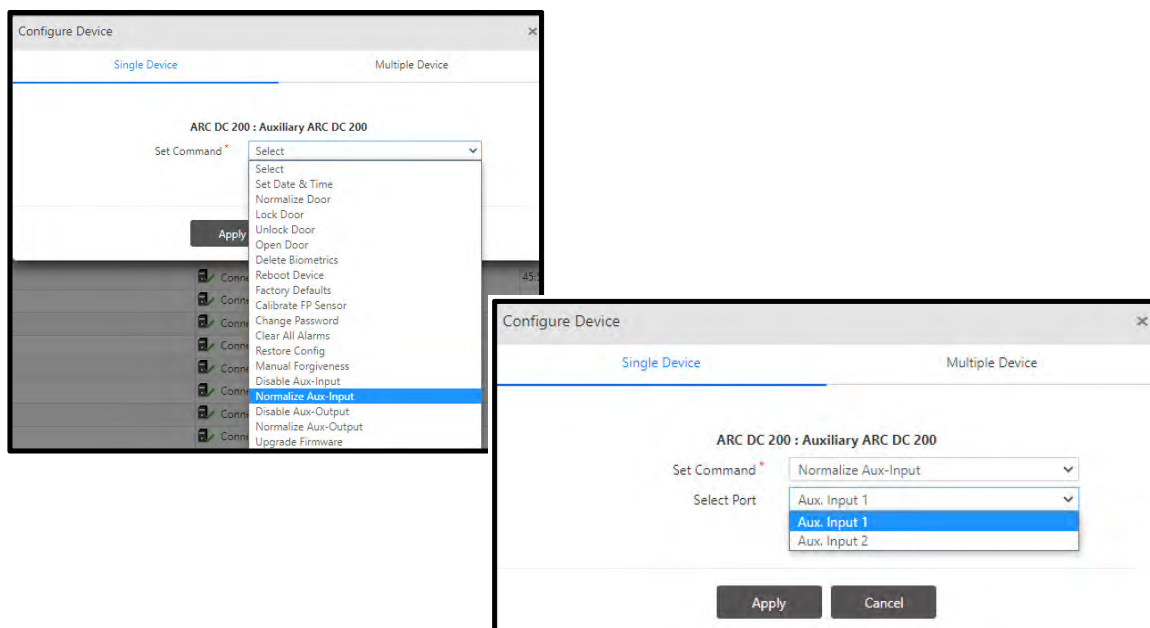
For changing the alarm status, the user will be prompted to provide the login password. Also, he may provide an optional remark to justify his action.

- **Restore Configuration** - For Panel200 door and direct doors, the user configuration /credentials can be restored on the device from the database.
- **Delete Faces (only for Vega/FMX, MODE, ARGO, and ARGO FACE Direct doors)**- Sends command to delete the faces from the selected device.
- **Manual Forgiveness (only for Panel200 and Direct doors PVR, V3, Wireless, Vega, FMX, ARC DC200, ARGO, ARGO FACE, and PATH V2)**- The user who is denied access due to Anti-pass back violation can be reset by giving **Manual Forgiveness** command. With this the user wont have to wait for the timer to expire and he can access the doors again.
- **Forgiveness For**- Select the option as **Local** or **Global** for which manual forgiveness is to be given.

For **Global**; forgiveness is sent to all the access zones of Panel200.

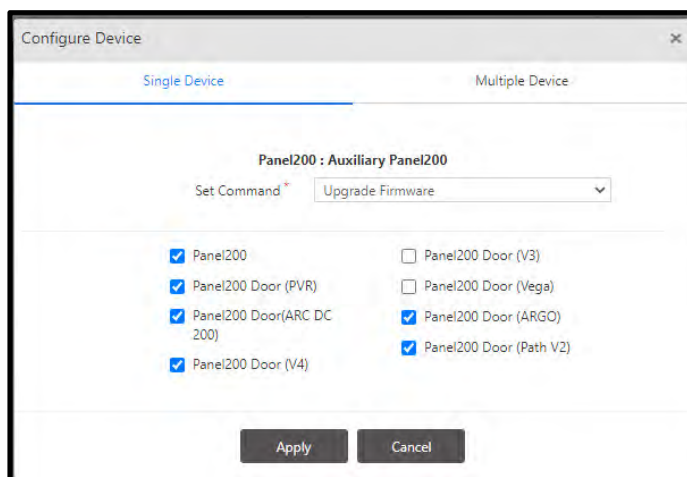
For **Local**; select the Access Zone from the picklist. In this forgiveness is sent to selected access zone only.

- **User**- Select the user for whom manual forgiveness is to be given.
- **Normalize/Disable Aux-Input (only for VEGA, V4, ARC DC200 Direct doors and ARC DC200 Single Door Dual Reader Panel door)**- Sends the appropriate commands to the DOOR to reset the Aux-Input status.



When **ARC DC200 Direct door/ARC DC200 Single Door Dual Reader Panel** door is selected in the **Device Status** list and **Set Command** is selected as **Disable Aux- Input/Normalize Aux-Input** then only **Select Port** parameter will be visible. You can select the desired port from the **Select Port** dropdown list.

- **Normalize/Disable Aux-Output (only for VEGA, V4, ARC DC200 Direct doors and ARC DC200 Single Door Dual Reader Panel doors)**- Sends the appropriate commands to the DOOR to reset the Aux-Output status.
- **Upgrade Firmware**- Sends the command to upgrade the firmware. When you upgrade the firmware of Panel200; then you can select the checkbox of Panel200 Door (V3), Panel200 Door (PVR) and Panel200 Door (Vega) to upgrade the firmware of selected type of doors of the Panel200.



When **Panel200** device is selected and if few of the components are checked and when you click **Apply** then the **Upgrade Firmware** command will be sent to the **Panel200** for selected components only.

If all the components are selected; then **Upgrade Firmware** command will be sent to the **Panel200** for **Panel door (PVR, ARC DC200, V4, V3, Vega, ARGO, and PATH V2)**.

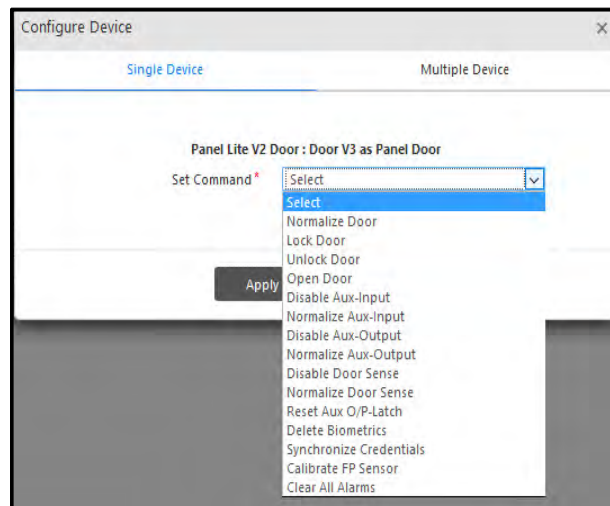
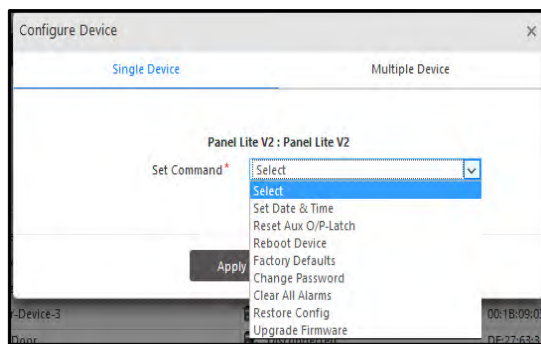
When **Upgrade Firmware** command is sent to direct door; then firmware of selected direct door will be upgraded.

- **Delete Fingerprints/Palms** - Sends command to delete the fingerprints/palm templates from the fingerprint/palm reader module of the selected device.
- **Synchronize Credentials (only for Panel200 Doors)** - Sends command to synchronize the fingerprints/palm templates from the Pane lite V2 to the Panel Doors. It is recommended to first send the delete fingerprints/palms command to the door before starting the synchronizing process.



*For different doors, there are different sets of **Set Command**.*

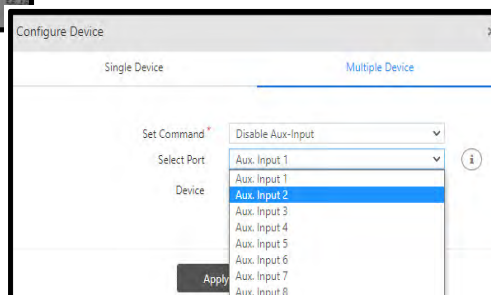
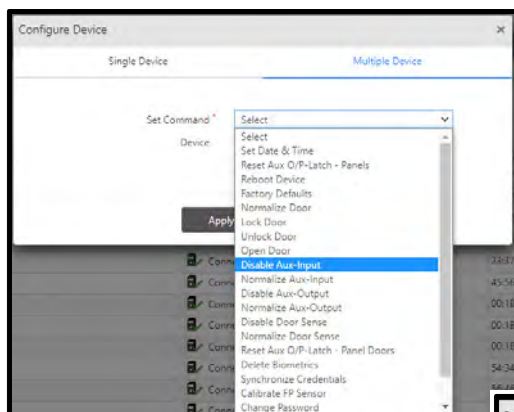
The following commands can be sent to the **Panel200** and **Panel200 Door**.

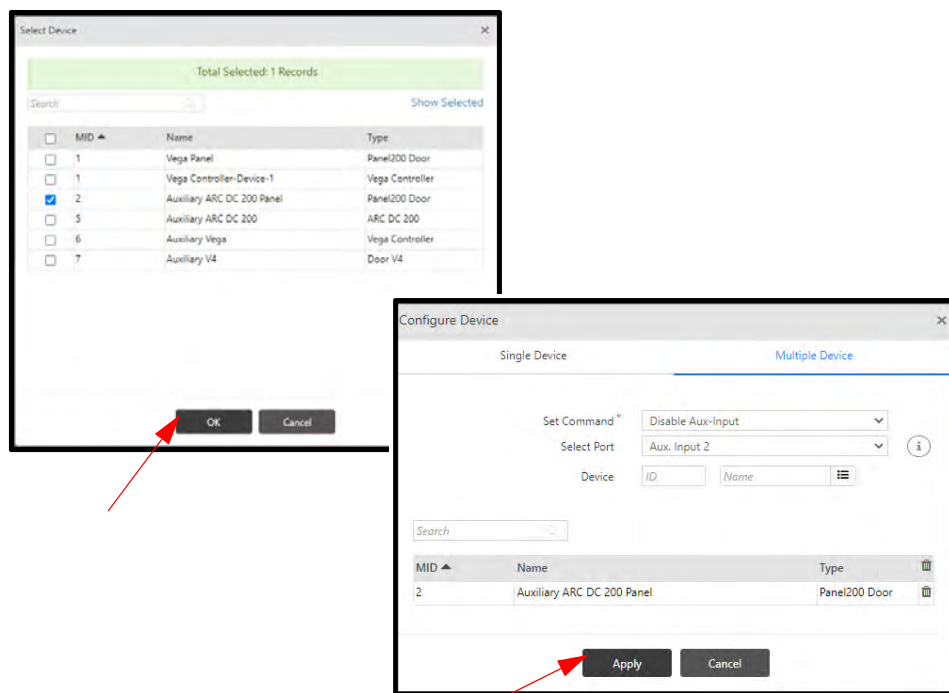


Click the  icon adjacent to a **Panel200** on the **Device Status** list to view the status of all Panel200 Doors assigned under it.

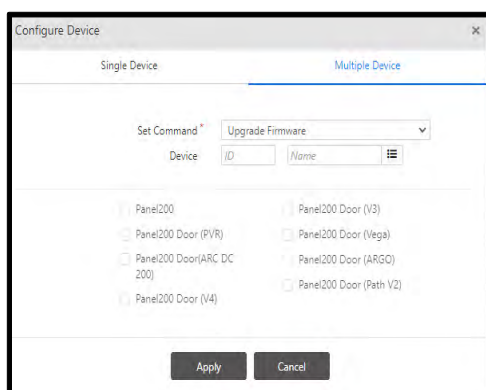
For **Multiple Device**, select the desired command from the **Set Command** drop down list; select the devices to which the command is to be sent from the **Device** picklist and click **Apply** to send the command to the selected devices.

To send command as **Disable Aux- Input/Normalize Aux- Input/ Disable Aux- Output/ Normalize Aux- Output** select the desired Command from the **Set Command** dropdown list. Select the desired Port from the **Select Port** dropdown list. Select the desired Device from the **Device** picklist and click **OK**. The selected device(s) appear in the **Configure Device** pop-up. Click **Apply** to send the desired command to the selected Multiple devices.





Multiple Device Command



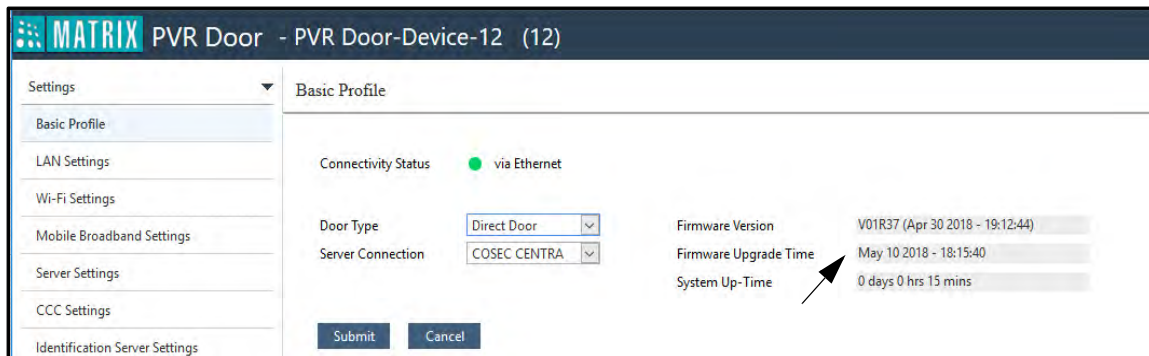
When **Panel200** device is selected in the list of **Multiple Device** selection and command is selected as **Upgrade Firmware** in the **Set Command** picklist, if few firmware components checkbox are selected and when you click **Apply** then the configuration for selected components only will be sent to the **Panel200**.



It is possible that the Firmware Location may have Firmware Update file of lower version then the current version of device firmware and still if the Firmware Update command is triggered then device firmware will get degraded to lower version.

Example: Firmware upgrade from FTP

Suppose the current firmware in PVR direct door is V1R37 which was upgraded on 10th May 2018.

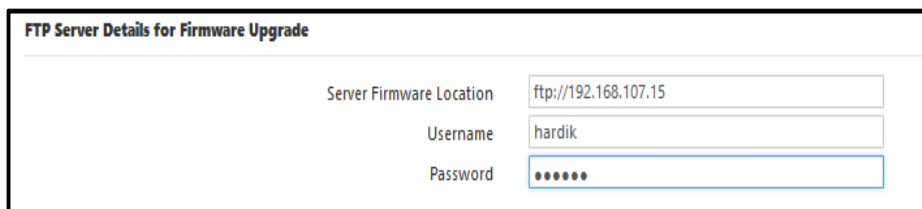


The screenshot shows the 'MATRIX PVR Door - PVR Door-Device-12 (12)' settings window. The 'Basic Profile' tab is selected. It displays the following information:

- Connectivity Status: ● via Ethernet
- Door Type: Direct Door (dropdown menu)
- Server Connection: COSEC CENTRA (dropdown menu)
- Firmware Version: V01R37 (Apr 30 2018 - 19:12:44)
- Firmware Upgrade Time: May 10 2018 - 18:15:40
- System Up-Time: 0 days 0 hrs 15 mins

Buttons for 'Submit' and 'Cancel' are at the bottom.

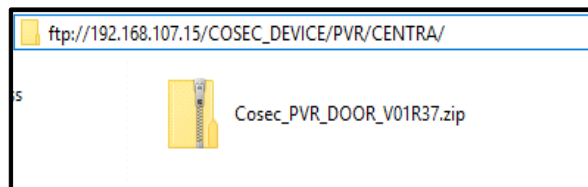
Now the FTP path for COSEC CENTRA is configured as shown below:



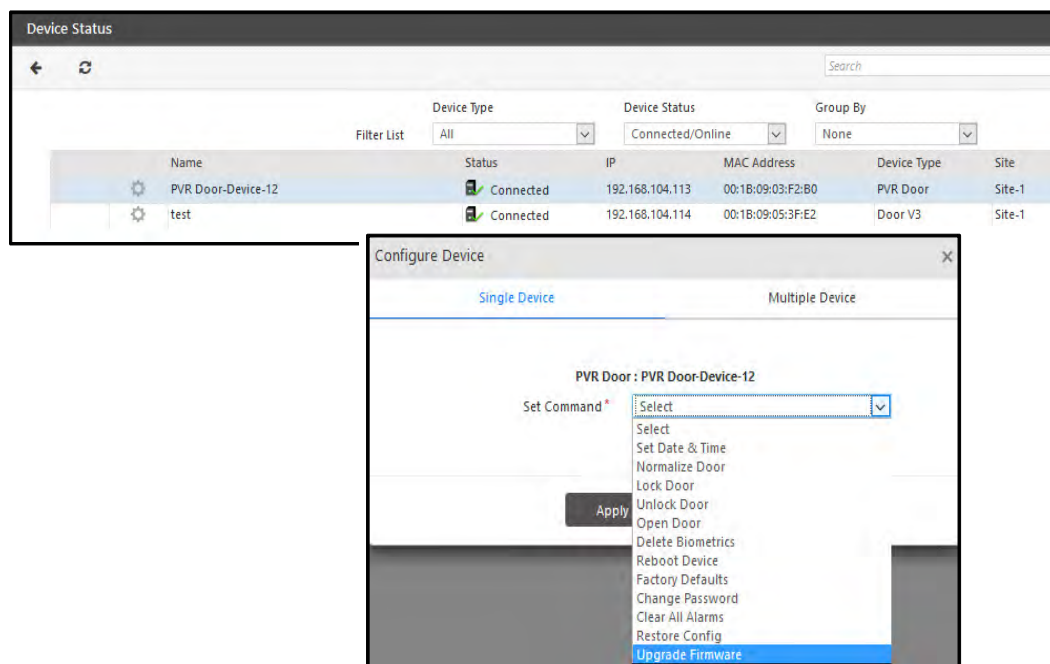
The screenshot shows the 'FTP Server Details for Firmware Upgrade' window with the following fields:

- Server Firmware Location: ftp://192.168.107.15
- Username: hardik
- Password: (masked with dots)

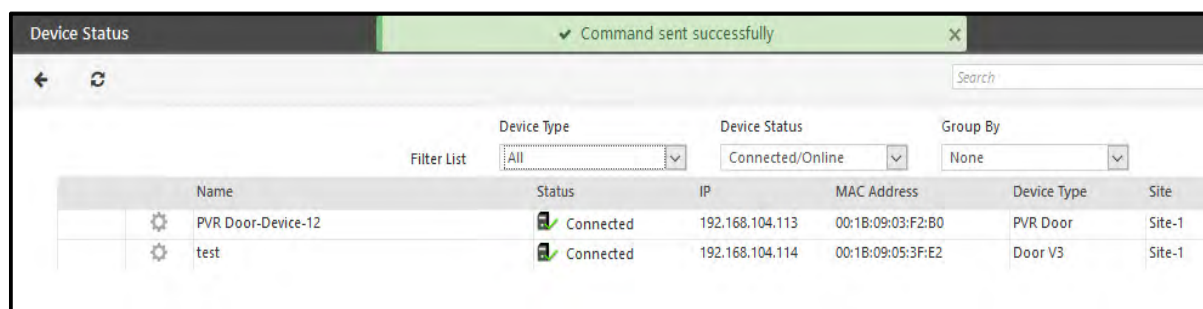
The new firmware of PVR door is available at FTP path as shown below:



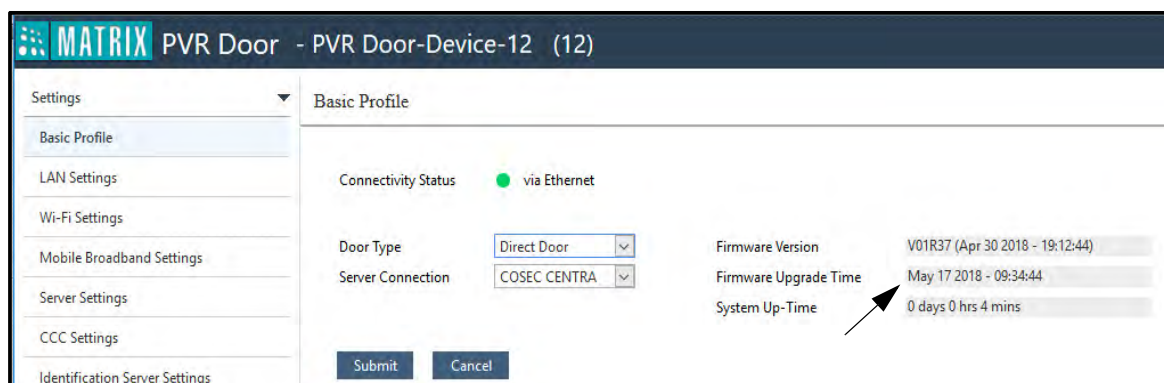
Now the firmware of PVR can be upgraded from Device Status page by selecting the Upgrade Firmware command as shown below.



The Command will be sent to the PVR door.



The door will reboot and firmware will be upgraded with the upgrade date-time as shown below.



Features

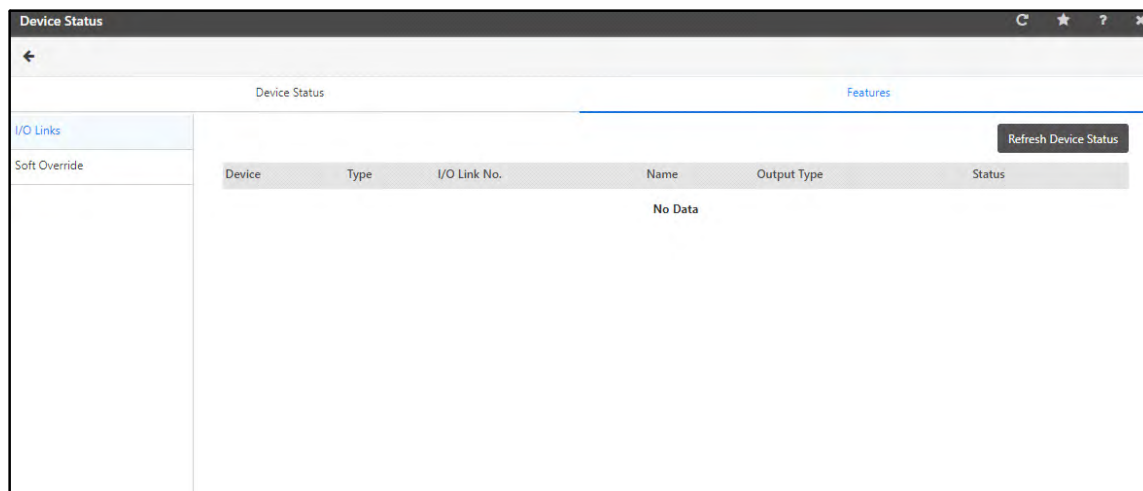
The Features tab consists of two pages — I/O Links and Soft Override.

I/O Links

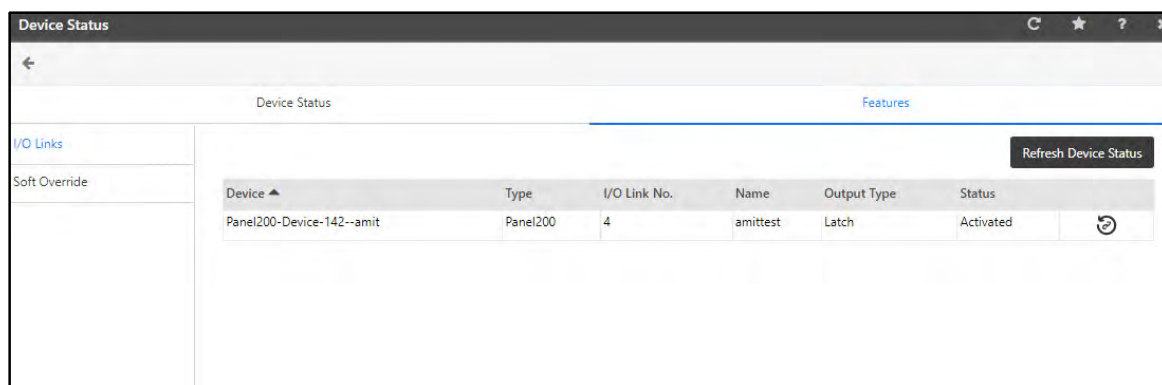
The I/O Links page allows you to view the Events related to I/O links of devices for the connected Panels/Direct Doors.

To view I/O linked events,

- Click **Device module > Device Status > I/O Links**.



- When an I/O Link related event occurs, it appears in a grid.
- Click **Refresh Device Status** to fetch the new events.



The details displayed are — Device Name, Type, I/O Link No., Name, Output Type and Status. If the Output Type is **Latch**, then **Reset** option appears.



*The **Reset** option is applicable only when the Output Type is **Latch**.*

- Click **Reset** to reset the output.

Soft Override

The Soft Override page allows you to override certain Access Control features for the connected Panel200 on a temporary basis.



Make sure you have selected the **Soft Override** check box from **Device Configuration > Features > Set 1** for Panel200 to enable the Soft Overriding of Access Control features.

To configure Soft Override,

- Click **Device module > Device Status > Soft Override**.

Device	Feature	Status	DateTime	Duration(Minutes)
No Data				

Configure the following parameters:

- Device:** Select the desired device on which you wish to override Access Control features from the drop-down list.
- Override:** Select the desired Access Control feature which you wish to override from the drop-down list and specify the time in minutes.

If you select ACS Policies, the time based access will be overridden if set. This includes Shift Based Access as well as Time Zone Based Access.


To know about the respective feature — 2 Person Rule, First User In, Alarm, Anti-Pass Back, Mantrap, Occupancy Control, Visitor Escort Rule — refer to [“Access Control”](#).

- Click **Submit**. Click **Refresh Device Status**. The overridden Access Control feature appears in the grid.

Device	Feature	Status	DateTime	Duration(Minutes)
Panel200-Device-142--amit	2 Person Rule	Overridden	12/12/2022 05:29:28 PM	10

The details displayed are — Device Name, Feature, Status, Date Time and Duration (Minutes).

You can stop the Soft Overriding of the Access Control feature, if required. To do so,

- Click **Resume**  to stop the overriding of the Access Control feature.

Device Reports

There are four categories of *Device Reports* which can be generated using the *Reports* option under the *Devices* module. These are as follows:

"Panel"

"Door"

"Invalid Events"

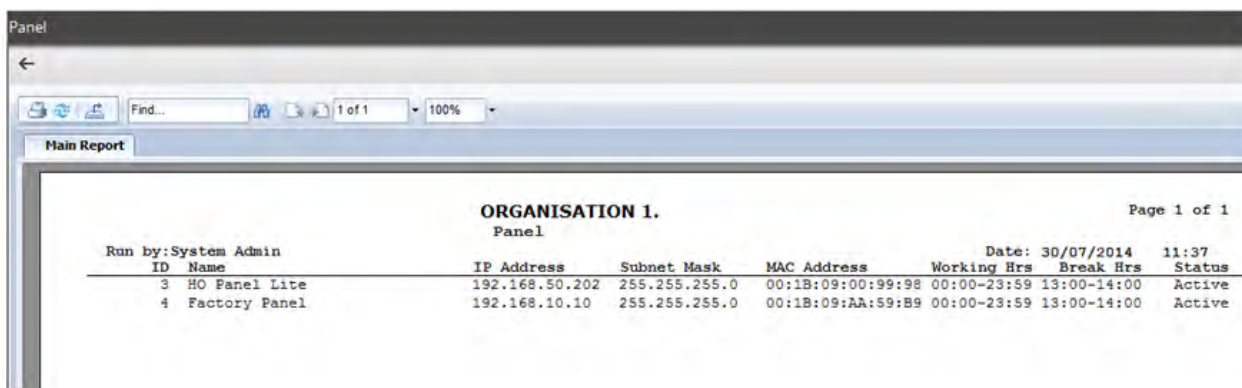
"Device wise events"

"Door Offline"

"Intercom Events"

Panel

Generates a detailed list of all panel devices on the system.

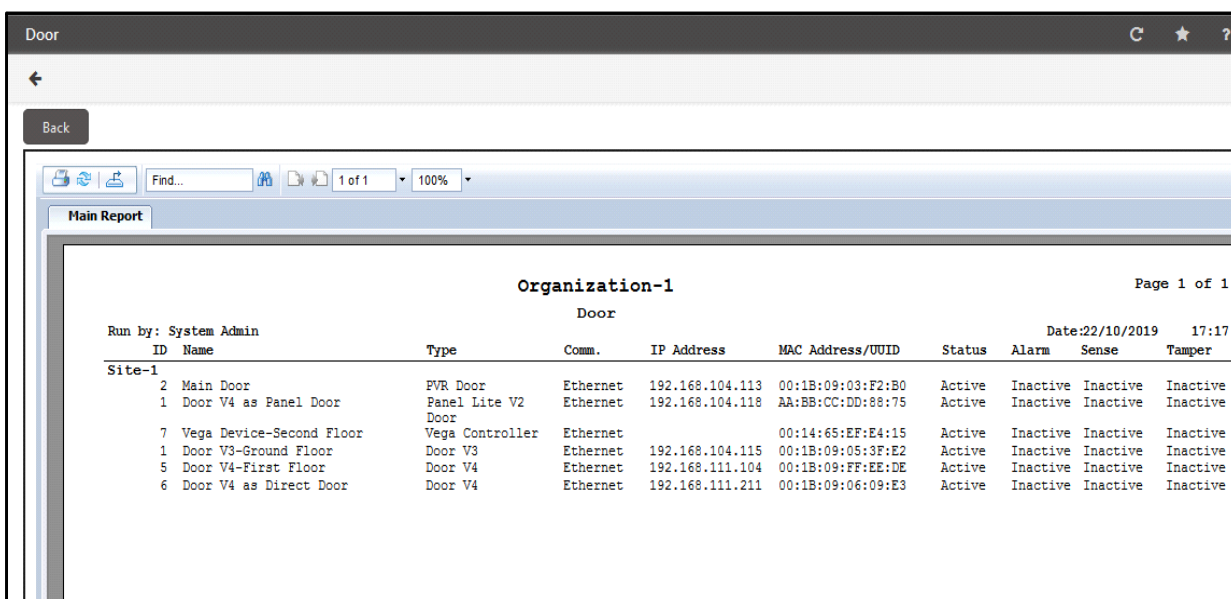


The screenshot shows a web application window titled "Panel". It contains a "Main Report" section with a table of panel devices for "ORGANISATION 1.". The table has columns for ID, Name, IP Address, Subnet Mask, MAC Address, Working Hrs, Break Hrs, and Status. The data is as follows:

ID	Name	IP Address	Subnet Mask	MAC Address	Working Hrs	Break Hrs	Status
3	HO Panel Lite	192.168.50.202	255.255.255.0	00:1B:09:00:99:98	00:00-23:59	13:00-14:00	Active
4	Factory Panel	192.168.10.10	255.255.255.0	00:1B:09:AA:59:B9	00:00-23:59	13:00-14:00	Active

Door

Generates a detailed site-wise list of all or specific door controller types on the system.



The screenshot shows a web application window titled "Door". It contains a "Main Report" section with a table of door controllers for "Organization-1". The table has columns for ID, Name, Type, Comm., IP Address, MAC Address/UUID, Status, Alarm, Sense, and Tamper. The data is as follows:

ID	Name	Type	Comm.	IP Address	MAC Address/UUID	Status	Alarm	Sense	Tamper
2	Main Door	FVR Door	Ethernet	192.168.104.113	00:1B:09:03:F2:B0	Active	Inactive	Inactive	Inactive
1	Door V4 as Panel Door	Panel Lite V2	Ethernet	192.168.104.118	AA:BB:CC:DD:88:75	Active	Inactive	Inactive	Inactive
7	Vega Device-Second Floor	Vega Controller	Ethernet		00:14:65:EF:E4:15	Active	Inactive	Inactive	Inactive
1	Door V3-Ground Floor	Door V3	Ethernet	192.168.104.115	00:1B:09:05:3F:E2	Active	Inactive	Inactive	Inactive
5	Door V4-First Floor	Door V4	Ethernet	192.168.111.104	00:1B:09:FF:EE:DE	Active	Inactive	Inactive	Inactive
6	Door V4 as Direct Door	Door V4	Ethernet	192.168.111.211	00:1B:09:06:09:E3	Active	Inactive	Inactive	Inactive

Invalid Events

Generates a list of invalid events on doors for a specified period. The **Invalid Events** page appears as shown in the figure below.

Invalid Events

←

Date * 01/05/2018 12/06/2018

Optional Parameters

Enterprise Group In Report Organization

Door Selection

Select Doors All

Generate Report

To generate this report,

- Specify the Start and End dates for the report.
- **Optional Parameters** section allows to select Enterprise Group for whom invalid events are to be generated.
- **Door Selection** section allows the selection of doors using the **Select Doors** drop down list. The options are:
 - **Door Wise:** Allows selection of door using the picklist button.
 - **ALL:** Allows selection of all the doors active on the system.
- Click the **Generate** button. The report appears as shown below.

Invalid Events

Back

Find... 1 of 5 100%

Main Report

Organization-1 Page 1 of 5

Invalid Events From 01/05/2018 To 12/06/2018

Run by: System Admin Date: 12/06/2018 14:26

Sr No	Time	IN/OUT	Reason
08/05/2018			
Door V3-Device-111			
1	16:33	IN	Denied - Invalid Input
2	16:33	IN	Denied - Time Out
3	16:35	IN	Denied - Invalid Input
4	16:35	IN	Denied - Time Out
5	16:35	IN	Denied - Time Out
6	16:36	IN	Denied - Time Out
7	16:36	IN	Denied - Time Out
8	16:37	IN	Denied - Time Out
9	16:37	IN	Denied - Time Out
10	16:38	IN	Denied - Time Out
11	16:38	IN	Denied - Time Out
12	16:38	IN	Denied - Time Out
13	16:39	IN	Denied - Time Out
14	16:39	IN	Denied - Invalid Input
15	16:39	IN	Denied - Time Out
16	16:42	IN	Denied - Time Out
17	16:42	IN	Denied - Time Out
18	17:45	IN	Denied - Invalid Input
19	18:17	IN	Denied - Time Out
20	18:17	IN	Denied - Time Out
21	18:18	IN	Denied - Time Out

Device wise events

Generates a record of device-wise events over a specified period. The **Device-Wise Events** page appears as shown in the figure below.

The screenshot shows a web application window titled "Device-Wise Event". At the top, there are date and time selection fields. The "Date" field has two input boxes, both showing "01/06/2018". The "Time" field has two input boxes, showing "09:00" and "11:00". Below these is a section titled "Optional Parameters". Inside this section, there is an "Event Type" dropdown menu with a list of options: "User Events" (checked), "Door Events" (checked), "Alarm Events" (unchecked), "System Events" (unchecked), and "Cafeteria Events" (unchecked). There is also a "Filter Devices" dropdown menu set to "All". Below the "Optional Parameters" section is a "User Selection" section. It contains a "Select Users" dropdown menu set to "User Wise". Below this, there are two input fields for "User": "ID" and "Name". At the bottom of the form is a "Generate Report" button.

To generate this report,

- Specify the Start and End dates for the report in the **Date** fields.
- Specify the Start and End time for the device-wise events to be listed in the **Time** field.
- In the **Optional Parameters** section, specify the **Event Type**.
- Use the **Filter Devices** drop down list to select devices based on the following filters:
 - ALL - All devices active on the system.
 - Device Group - Select a device group from the device group list.
 - Randomly - Select a random device.
- In the **User Selection** section, select users from the drop down list based on the following filters:
 - User Wise - Select a user randomly by clicking the **Select User** button.
 - Group Wise - Select all users belonging to an enterprise group. Specify the group from the **Select Group** drop down list.
 - ALL - Select all users active on the system.

Click the **Generate Report** button. The report appears as follows:

Device-Wise Event						
Back						
Find... 1 of 1 100%						
Main Report						
Organization-1						
Device-Wise Events From 01/06/2018 To 01/06/2018						
Run by: System Admin				Date: 12/06/2018 14:15		
Sr No	Event Date-Time	Event Type	Event Name	User ID	Name	
Device : Door V3 as Panel Door						Site : Site-1
1	01/06/2018-10:43:42	User	Allowed	1	Chirag	
2	01/06/2018-10:43:50	Door	Door Open/Close	1	Chirag	
3	01/06/2018-10:43:50	Door	Door Open/Close	1	Chirag	
4	01/06/2018-10:43:54	Door	Door Open/Close	1	Chirag	
5	01/06/2018-10:43:54	Door	Door Open/Close	1	Chirag	
6	01/06/2018-10:43:57	Door	Door Open/Close	1	Chirag	
7	01/06/2018-10:43:57	Door	Door Open/Close	1	Chirag	
8	01/06/2018-10:43:58	Door	Door Open/Close	1	Chirag	
9	01/06/2018-10:47:53	User	Allowed	1	Chirag	
10	01/06/2018-10:48:00	Door	Door Open/Close	1	Chirag	
11	01/06/2018-10:48:03	Door	Door Open/Close	1	Chirag	
Device : PVR as Panel Door						Site : Site-1
1	01/06/2018-10:38:52	User	Allowed	1687	Aditi Ajay Gupta Ahmedabad	
2	01/06/2018-10:38:54	User	Allowed	1687	Aditi Ajay Gupta Ahmedabad	
3	01/06/2018-10:38:58	User	Allowed	1687	Aditi Ajay Gupta Ahmedabad	
4	01/06/2018-10:39:03	Door	Door Open/Close	1687	Aditi Ajay Gupta Ahmedabad	
5	01/06/2018-10:39:04	User	Allowed	1687	Aditi Ajay Gupta Ahmedabad	
6	01/06/2018-10:39:09	Door	Door Open/Close	1687	Aditi Ajay Gupta Ahmedabad	
7	01/06/2018-10:40:02	User	Allowed	1687	Aditi Ajay Gupta Ahmedabad	
8	01/06/2018-10:40:07	Door	Door Open/Close	1687	Aditi Ajay Gupta Ahmedabad	
9	01/06/2018-10:40:25	User	Allowed	1687	Aditi Ajay Gupta Ahmedabad	

The Door Events are shown in below report.

Device-Wise Event						
Back						
Find... 1 of 1 100%						
Main Report						
Organization-1						
Device-Wise Events From 09/01/2018 To 25/01/2018						
Run by: System Admin				Date: 25/01/2018 15:08		
Sr No	Event Date-Time	Event Type	Event Name	User ID	Name	
Device : PVR Door-Device-10						Site : Site-1
1	25/01/2018-11:10:42	Door	Door Open/Close			
2	25/01/2018-11:27:25	Door	Door Open/Close	9888	User 1234	
3	25/01/2018-11:27:30	Door	Door Open/Close	9888	User 1234	
Device : PVR Panel Door IP-85						Site : Site-1
1	19/01/2018-11:22:48	Door	Door Controller Communication status			
2	19/01/2018-11:56:28	Door	Door Controller Communication status			
3	19/01/2018-11:56:34	Door	Door Controller Communication status			
						Site : Site-1
1	19/01/2018-11:23:22	Door	Door Controller Communication status			
2	19/01/2018-12:03:49	Door	Door Controller Communication status			
3	19/01/2018-12:03:53	Door	Door Controller Communication status			
4	19/01/2018-13:51:17	Door	Door Controller Communication status			
						Site : Site-1
1	19/01/2018-11:24:02	Door	Door Controller Communication status			
2	19/01/2018-11:36:56	Door	Door Controller Communication status			
Device : Vega Controller-Device-6						Site : Site-1
1	19/01/2018-18:39:03	Door	Door Controller Communication status			

Device-Wise Event

Back

1 of 1

Whole Page

Organization-1

Page 1 of 1

Device-Wise Events From 21/01/2022 To 21/01/2022

Run by: System Admin

Date: 21/01/2022 16:36

Sr No	Event Date-Time	Event Type	Event Name	User ID	Name
nk vega					
1	21/01/2022-14:00:23	User	Allowed	U1	Site-1
2	21/01/2022-14:01:02	User	Allowed	U1	User1
3	21/01/2022-14:03:05	User	Allowed	U1	User1
4	21/01/2022-14:03:51	User	Allowed	U1	User1
5	21/01/2022-14:09:22	User	Allowed	U1	User1
6	21/01/2022-14:09:45	User	Allowed	U1	User1
7	21/01/2022-14:11:02	User	Allowed - with Duress	U1	User1
8	21/01/2022-14:11:53	User	Allowed - with Duress	U1	User1

For more details on the Event “Door Controller Communication Status” for Direct Door as Panel door; see *Admin> Alert Message Configuration*.

Door Offline

Generates a list of all Panel lite and Direct Doors which have gone offline for a specific duration within a defined date range, as shown below:

Door Offline

Date *

04/07/2020

04/07/2020

Time

00:00

23:59

Optional Parameters

Offline Duration (Seconds)

0

Device Selection

Filter Devices

Group Wise

Select Group

Panel

Panel *

ID

Name

Generate Report

Specify a date & time range and the door offline duration (in seconds) i.e. the duration for which doors were offline in the specified date range. In this example, the **Offline Duration (Seconds)** is set as 10 second.

ID	Name	Offline Date-Time	Online Date-Time	Down Time
2	NGT Direct Door-Device-2	02/04/2018-16:14:48	08/05/2018-15:48:48	863:34:00
2	NGT Direct Door-Device-2	09/05/2018-13:57:28	11/05/2018-09:35:18	43:37:50
2	NGT Direct Door-Device-2	11/05/2018-18:27:53	11/05/2018-18:53:59	00:26:06
2	NGT Direct Door-Device-2	14/05/2018-16:09:29	14/05/2018-16:16:43	00:06:14
2	NGT Direct Door-Device-2	16/05/2018-17:36:58	16/05/2018-17:37:33	00:00:35
2	NGT Direct Door-Device-2	17/05/2018-22:52:30	17/05/2018-22:52:59	00:00:29
2	NGT Direct Door-Device-2	17/05/2018-22:53:33	17/05/2018-22:53:44	00:00:11
2	NGT Direct Door-Device-2	18/05/2018-10:05:02	18/05/2018-10:06:37	00:00:35
2	NGT Direct Door-Device-2	23/05/2018-19:09:28	23/05/2018-19:10:02	00:00:34
2	NGT Direct Door-Device-2	24/05/2018-19:26:43	24/05/2018-19:27:18	00:00:35
2	NGT Direct Door-Device-2	28/05/2018-18:01:33	28/05/2018-18:02:08	00:00:35
3	Panel Lite V2	04/05/2018-16:55:57	04/05/2018-16:57:04	00:01:07
3	Panel Lite V2	04/05/2018-17:19:17	22/05/2018-10:36:34	425:17:17
3	Panel Lite V2	22/05/2018-10:45:27	22/05/2018-10:46:40	00:01:13

In device selection, filter the devices by selecting either of them: **Group-wise or All**.

For Group-wise, if Panel is chosen then, select a **Panel** from Panel drop-down list.

If **Direct Door** option is chosen, then select a **Direct Door** from direct door drop down list.

For **Device Group**, select the desired group from the picklist.

Intercom Events

Generates a comprehensive report containing the event details as well as the resident's details, showing which apartment/user gave the command to the device and caused the visitor allowed/denied event or both events.

Sr. No.	Event Date-Time	Intercom No.	User ID	Name	Device Name
1	2015/05/08 11:35	1234jb			Vega Controller-Device-86
2	2015/05/08 11:35	234jb			Vega Controller-Device-86
3	2015/05/08 11:36		002	user002	Vega Controller-Device-86
4	2015/05/08 11:37		002	user002	Vega Controller-Device-86
5	2015/05/08 11:38	234			Vega Controller-Device-86
6	2015/05/08 12:43	234			Vega Controller-Device-86
7	2015/05/08 12:52		002	user002	FVR Door-Device-94
8	2015/05/08 12:55		002	user002	FVR Door-Device-94
9	2015/05/08 12:56		002	user002	FVR Door-Device-94
10	2015/05/08 12:56	1234b			FVR Door-Device-94
11	2015/05/08 12:57	1234b			FVR Door-Device-94
12	2015/05/08 12:50	234			FVR Door-Device-94
13	2015/05/08 15:13	1234jb			Door V3-Device-76


Shift Schedules are detailed chart indicating the working hours for group employees based on the organization's requirement. These display details like no. of days, timing, shift rotation, rotation count etc for each shift schedule.

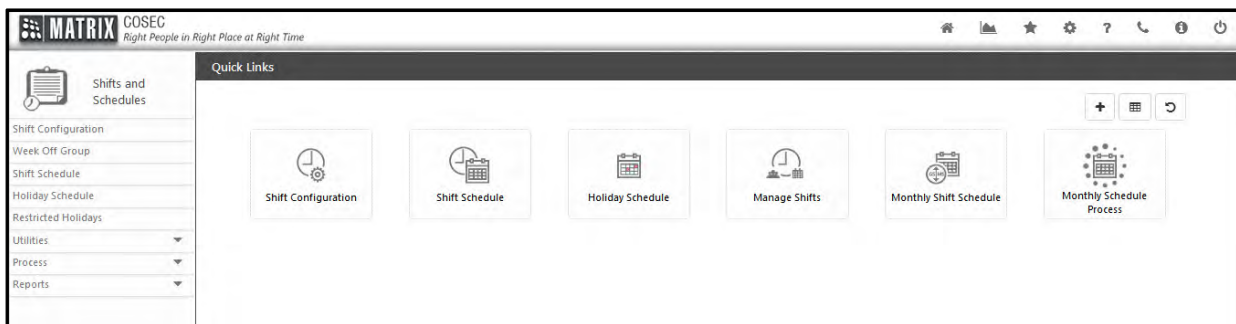


This functionality will not be available with the COSEC Application basic platform license.






*In order to start the configuration of the system the user needs to first define the devices from the **Basic** module and then proceed with the configuration of the Shifts from the **Shifts and Schedules** module.*

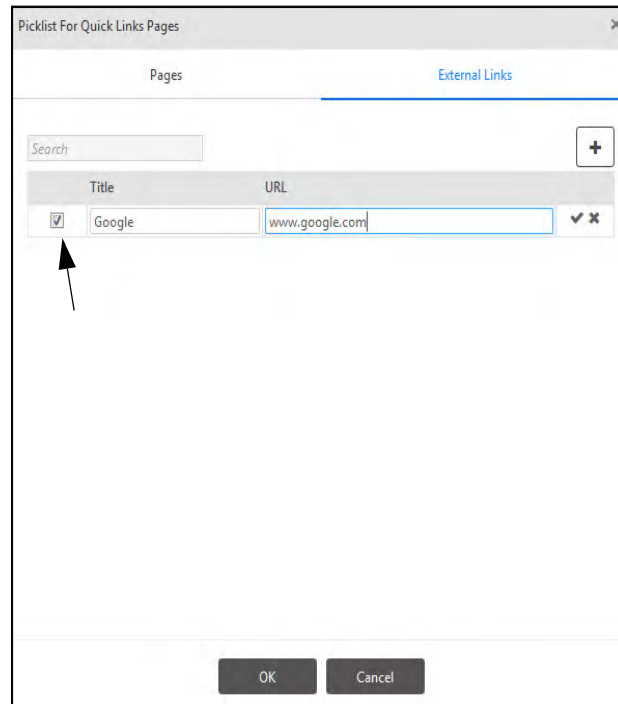
To use the Shift and Schedules functionality, Click on **Shifts and Schedules**  Module. The Shifts and Schedules page will appear on your screen.




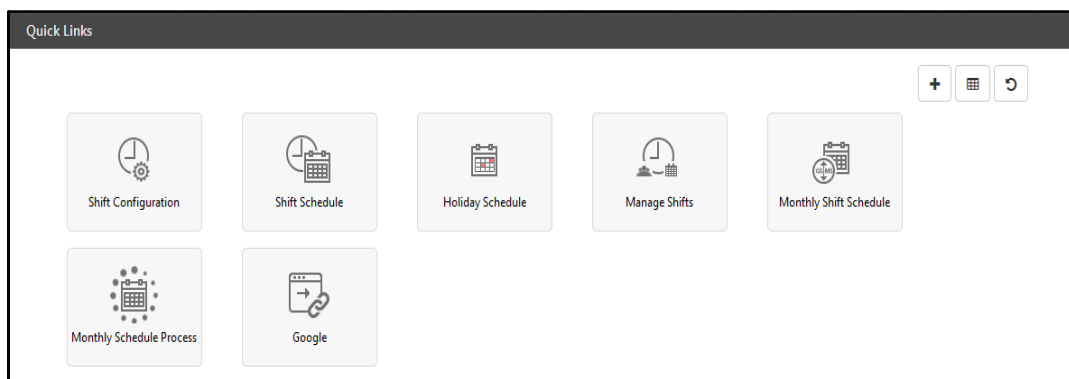
The page displays a menu and **Quick Links** to go to the required page in just one click. Quick Links are shortcuts to reach to a specific page easily. It also contains following three buttons:



- **Add Quick Link:** Click  button to add a quick link. A picklist for Quick Link pages appears for selecting the page or External Link for which the quick link is to be created. Maximum **20** quick links can be added.
- For Adding **Pages** in Quick Link, Select the Pages and click on OK
- For Adding **External Links**, Select External Link tab, click on  button to add new external link.

- Configure the **Title** and **URL** of the external link under the respective fields. click on checkbox to get the configured link on quick link screen as shown below. To save the configuration click on .



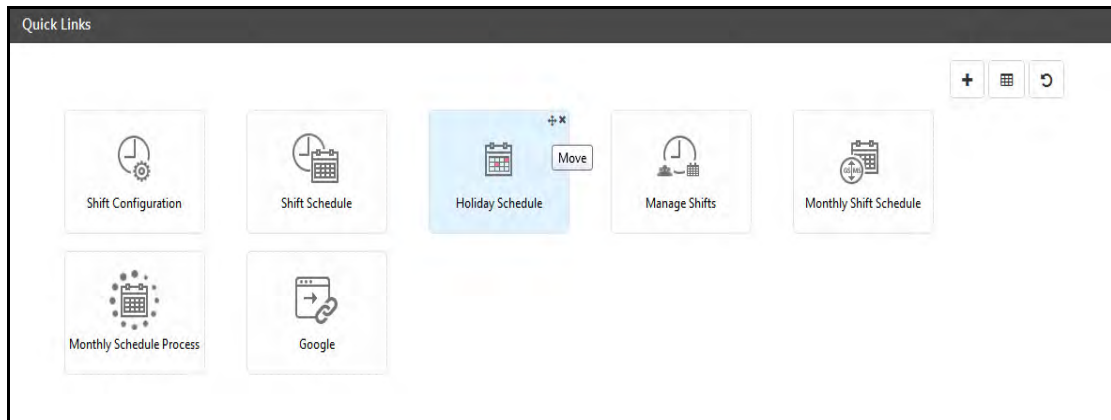
- To edit the saved configuration, click on .
- Click on OK to save the link configuration on Quick Link screen. The external link will be displayed as shown below:



- **Select Layout:** Click  button to select a layout for the quick links. You can select 5x4 or 4x5 layout to manage the quick links.
- **Reset Quick Links:** Click  button to reset the quick links to the default quick links.

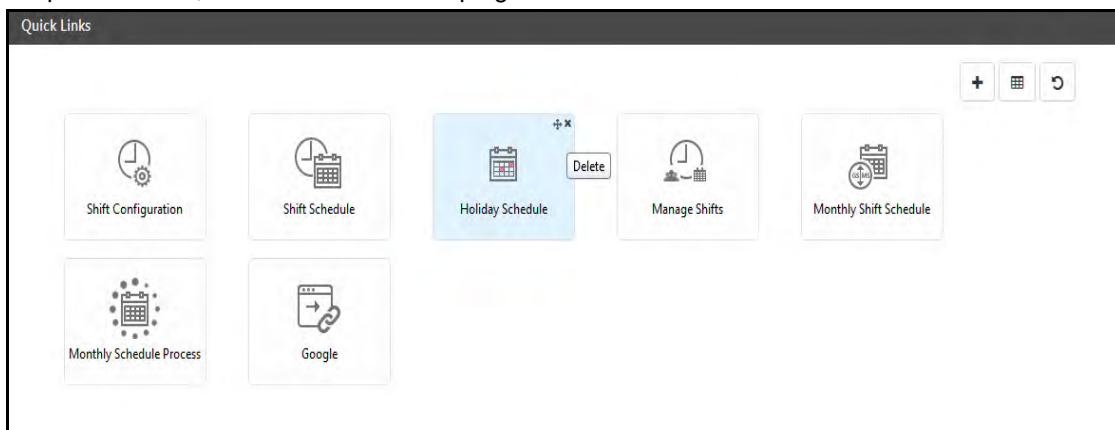
Move the Link

To move the link from one place to another, hover on the link on top right corner and click on “Move” icon as shown below. Then drag the quick link to the desired place. It will be placed at the desired location on the quick links page.




Delete the Link

To delete a particular link, hover on the link on top right corner and click on “Delete” icon as shown below.



Quick links are displayed as per rights given to System Account and ESS users.

Shifts and Schedules Dashboard

To view the Dashboard, click the Dashboard button  on the **Shifts and Schedules** page.

It displays the basic information on shifts and schedules relating to the COSEC Software under the four groups:

Dashboard

4

On Going Shifts

Shifts and Schedules	
Unused Shifts	0
Normal Shifts	11
Field Break Shifts	3
Rest Day Shifts	2
Un-assigned Schedules	17

16

Configured Shifts

Upcoming Holidays	
Holi	03/13/2017
Financial closing	03/31/2017
Labours Day	05/01/2017

19

Configured Schedules

Holiday Schedule	
Configured	5
Restricted Holidays	13

On Going Shifts- Total number of shifts assigned to user.

Configured Shifts- Total no. of shifts configured in COSEC.

Configured Schedules- Total no. of shift schedules configured in COSEC.

Shifts and Schedules

- Unused Shifts- Total no. of shifts, currently not configured in any Schedule.
- Normal Shifts- Total no. of shifts configured as Normal Type Shift.
- Field Break Shifts- Total no. of shifts configured as Field Break Type Shift.
- Rest Day Shifts- Total no. of shifts configured as Rest Day Type Shift.
- Un-assigned Schedules- Total no. of schedules, currently not configured to any user.

Upcoming Holidays

- The upcoming 5 holidays will be listed in ascending order.

Holiday Schedule

- Configured- Total no. of holiday schedules configured in COSEC.
- Restricted Holidays- Total no. of restricted holidays configured in Cosec.

For more information on the above Dashboard options, click the respective information links on the Dashboard. The

Latest values on Dashboard are updated on clicking the Refresh  button.

Shift Configuration

Shift Configuration enables to define the Shift, shift timing details, break details and Grace Time details. The total number of shifts that can be created in COSEC is 999.

To access the Shift Configuration, Click on **Shift Configuration** option from the Shift and Schedule page. The page appears as shown below:

The screenshot shows the 'Shift Configuration' window. On the left, there are input fields for 'Shift' (ID and Name), 'Shift Type' (a dropdown), 'Shift Timings' (three HHMM format boxes), 'Minimum Required Hours' (For Half Day and For Full Day), 'Min. Hours Required Within Shift Duration' (checkbox), 'Deviation From Shift Start (Mins)' (0-999), 'Deviation From Shift End (Mins)' (0-999), and 'Shift Allowance' (checkbox). At the bottom are expandable sections for 'Break Details' and 'Grace Time Details'. On the right, a search bar is at the top, and a table lists existing shifts.

ID	Name	Timings
12	Early Out Shift	09:00 - 18:00
GS	General Shift	09:00 - 18:00

Shift: Specify a User friendly Shift ID and Shift Name.

Shift Type: Select the Shift Type from the drop down options:

- **Normal-** This is a normal shift with one weekoff within a week.
- **Field Break-** This is a shift where a break of around 20 days can be given after working period of 2 months.
- **Rest Day-** This is a like a normal shift with one weekoff given for rest after 10-12 working days.

This screenshot shows the same 'Shift Configuration' window but with data entered. 'Shift' ID is 'NS' and Name is 'Night Shift'. 'Shift Type' is 'Normal'. 'Shift Timings' are '21:00', '05:00', and '08:00'. Under 'Minimum Required Hours', 'For Half Day' is '02:00' and 'For Full Day' is '04:00'. 'Min. Hours Required Within Shift Duration' is checked. 'Deviation From Shift Start (Mins)' and 'Deviation From Shift End (Mins)' are both '60'. 'Shift Allowance' is unchecked. The table on the right remains the same.

ID	Name	Timings
12	Early Out Shift	09:00 - 18:00
GS	General Shift	09:00 - 18:00

Shift Timings: Specify the start time and end time of the shift in hh:mm format.

The Shift duration or the total working hours of the shift is automatically calculated based on the start and end time

Minimum Required Working Hours

- **For Half Day:** Specify the minimum working hours required for marking half day. The format is in HH:MM.
- **For Full Day:** Specify the minimum working hours required for marking full day. The format is in HH:MM.

Min. Hours Required within Shift Duration: Check the box to enable this option. This functionality allows the minimum working hours for full day and half day to fall within the shift working time allotted to the employee.

This means if the shift duration is from 9:00 to 18:00, then your working hours must be within this shift duration to mark the employee present. If you have worked from 17:00 to 23:00, then your 6 hours of work is not in the shift duration. Out of 6 hours only 1 hour fall in the shift duration which is not enough to mark half day present (depends on minimum required working hours for half day= 2 hrs)

If 'Min Hours Required Within Shift' is enabled then system will consider 'EligibleHrs' for marking user absent due to less work hours.

- **Deviation from Shift Start (Mins):** If "Min hrs required within shift duration" is enabled, then you can specify the deviation to be allowed from the shift starting time.
- **Deviation from Shift End (Mins):** If "Min hrs required within shift duration" is enabled, then you can specify the deviation to be allowed from the shift ending time.



Minimum hours fulfillment is checked before the "Normal" type user is marked Absent due to Less work hours.

Eligible hours calculation

Example1: Shift: 09:00 to 18:00 hrs. Deviation allowed for shift start=1hr, Deviation allowed for shift end=1 hr.

IN Punch	Deviated Shift Start	ShiftStart	Shift End	Deviated Shift End	OUT Punch
6:00 hrs	8:00 hrs	9:00hrs	18:00 hrs	19:00 hrs	21:00 hrs
Actual work done= 15 hrs					
Early IN=3hrs				Overstay = 3hrs	
DEI=2hrs					DO=2hrs

- Work hours = 15:00 hrs (6:00 to 21:00 hrs)
- Work hours within Shift= Work hours- Early IN- Overstay
= 15 -3- 3 = 9:00 hrs
- Eligible Work hours= Work hours- Deviated Early IN(DEI)- Deviated Overstay(DO)
= 15- 2- 2 = 11 hrs

Example2:

IN Punch	Deviated Shift Start	Shift Start	Shift End	Deviated Shift End	OUT Punch
	13:00 hrs	15:00hrs	23:00 hrs	01:00 hrs	
15:00 hrs (5/7/16)					05:00 hrs (16/7/16)
		Actual work done= 14 hrs			
		Work hours within shift= 8 hrs			
Early IN=0hrs				Overstay = 6hrs	
DEI=0hrs					DO=4hrs

- Eligible Work hours= Work hours- Deviated Early IN(DEI)- Deviated Overstay(DO)
= 14- 0- 4 = 10hrs

Shift Allowance: Check the box to include the shift allowance in the salary calculation.

Break Details

Click on the drop down arrow to open the collapsible menu to set the Basic duration as shown below:

Start Time: Specify the start time of the break in hh:mm format.

End Time: Specify the end time of the break in hh:mm format.

Break Duration: The break duration is automatically calculated based on the start and end time.

Suppose If Break Start time is 23:00 hrs and Break End time is 23:30 hrs, then break duration will be 00:30 hr.

According to the break duration hours, shift duration will also be updated from 08:00 to 07:30 hrs as shown below.

Break Deviation Allowed: Check the box to allow the break deviation. By enabling this option, the employee is allowed to take the break at any time in the day.

Shift Timings * 21:00 05:00 07:30

Minimum Required Hours

For Half Day * 02:00

For Full Day * 04:00

Min. Hours Required Within Shift Duration ☒

Deviation From Shift Start (Mins) 60

Deviation From Shift End (Mins) 60

Shift Allowance ☐

Break Details

Break Timings 23:00 23:30 00:30

Break Deviation Allowed ☒

Advanced Details

Add Break Late-IN In Total Late-IN ☐

Add Break Early-OUT In Total Early-OUT ☐

Deduct Break From Working Hours

Deduction Type For 2 Punch ☒ Configured Break Duration

Deduction Type For 2+ Punch ☒ Actual Break Duration

Advanced Details

You can configure the Advanced Break details if “Break Deviation Allowed” is disabled.

Add Break Late-IN In Total Late-IN: Check the box to add the break late-in to the total late-in of the shift.

Eg: Suppose In GS (09:00 to 18:00 hrs), your break is from 13:00 to 14:00hrs. After availing break, you are entering office at 14:15 hrs, which is 15 minutes late. So Break Late-IN of 15 minutes will be added in the total Late-IN hours.

Add Break Early-OUT In Total Early-OUT: Check the box to add the break early-out time to the total early-out time of the shift.

Eg: Suppose In GS (09:00 to 18:00 hrs), your break is from 13:00 to 14:00hrs. You are going early for availing break at 12:45. Then 15 minutes of break early out will be considered. If your shift ends at 18:00 hrs. And you leave at 17:30 hrs. So it is 30 minutes Early-out. If this option is enabled then 15min (break early-out) will be added to the total early out (30 minutes) making it 45 minutes.

Deduct Break from Working Hours

The COSEC administrator can determine the basis for break deduction for employees for a particular shift.

Deduction Types can be specified in the event of a user marking 2 or 2+ punches by enabling the following options:

- Deduction Type For 2 Punch
- Deduction Type For 2+ Punch

Deduct Break From Working Hours

Deduction Type For 2 Punch ☒ Configured Break Duration

Deduction Type For 2+ Punch ☒ Actual Break Duration

For both 2 punches and 2+ punches, the following deduction types can be selected from the corresponding dropdown lists:

- **Configured Break Duration:** Deduction based on break duration as configured from Break Details..
- **Actual Break Duration:** Deduction based on user punches i.e. actual break taken.
- **Time Exceeding Break Duration:** Deduction based on the time exceeding configured break duration.
- **Configured Break If less, Else Actual Break Duration:** In this if the break availed by the employee is less than the configured break duration, then the configured duration is deducted from the working hours whereas if the break availed by the employee is greater than the configured break, then the actual break duration availed is deducted from the working hours.

For eg. if the configured break duration is 60mins and the user takes a break of 30mins, then the process will set the day's availed break as 60 mins. If the user takes a break of 70 mins, then the process will set the day's availed break as 70 mins.

- **Custom Break Deduction:** This field enables defining a customized break schedule by defining the range and allowing the actual or fixed value for rounding.

Break Range (From)	Break Range (To)	Consider Value As	Replace Value
1	15	Fixed	15
16	30	Fixed	30
31	60	Actual	

Break Range (From-To): Specify the range in minutes.

Replace Value: Select the options from the drop down list.

- **Fixed:** With fixed value, the defined value will replace the result if the parameter falls in the range.
- **Actual:** With actual value, the parameter value will be the result/output of the rounding function if the parameter value falls in its range.

Example: If break taken is within 1min to 15min then fixed 15 minutes will be deducted. If break is between 16 min to 30min, then fixed 30 mins will be deducted. If break is between 31min to 60min then actual break availed will be deducted.

Grace Time Details

Include Grace Time in Working Hours: Check the box to include the Grace time in the allotted working hours.

Grace Time for Shift Late-IN: Specify the grace time in minutes as the allowed deviation of timing while punching IN at start of the shift. [See “Late-IN Policy” on page 1491.](#)

Example: Consider shift is from 9:00 to 18:00 hrs, and “Include Grace Time in Working Hours” is enabled.

On 1/7/16: If Grace (checkbox is disabled) and Late-IN both are not applicable for user

On 4/7/16: If Grace is allowed (this checkbox is enabled), Late-IN not applicable. Then Late-IN column will show nothing.

On 5/7/16: If Late-IN allowed is 10 minutes, Grace time included in working hrs, Grace time for shift late-IN is 30 mins. IN-punch is 9:20, so due to grace timings, late-in will not be shown.

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/07/2016	GS	09:05	18:30	PR	PR			08:25	00:30		01:00			
02/07/2016	GS - WO			WO	WO									
03/07/2016	GS - WO			WO	WO									
04/07/2016	GS	09:10	18:30	PR	PR			08:20	00:30		01:00			
05/07/2016	GS	09:20	19:00	PR	PR			08:40	01:00		01:00			
06/07/2016	GS													

Overlap Grace Time With Shift Late-IN: Check the box to include the Grace Time with the Shift Late-IN time.

Example: Consider Grace time for Shift late-IN is 10 mins, Late-IN allowed is 20 mins, Overlap is disabled.

On 1st: IN punch 9:05, within Grace period of 10mins

On 4th: IN punch 9:11, beyond Grace period of 10 mins but within late-in allowed of 20mins so late-in by 1min

On 5th: IN Punch 9:21, Upto 9:10 is grace, after that late-in, so from 9:11 to 9:21 is 11 min of late-IN

On 6th: IN Punch 9:15, Upto 9:10 is grace, after that late-in, so from 9:11 to 9:15 is 5 min of late-IN

On 7th: IN Punch 9:31, Beyond grace and late-IN period so he will be marked Absent: Late-IN

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/07/2016	GS	09:05	18:30	PR	PR			08:25	00:30		01:00			
02/07/2016	GS - WO			WO	WO									
03/07/2016	GS - WO			WO	WO									
04/07/2016	GS	09:11	18:30	PR	PR	00:01		08:19	00:30		01:00			
05/07/2016	GS	09:21	19:00	PR	PR	00:11		08:39	01:00		01:00			
06/07/2016	GS	09:15	18:30	PR	PR	00:05		08:15	00:30		01:00			
07/07/2016	GS	09:31	18:30	AB	PR			07:59	00:30		01:00			AB:Late-IN
08/07/2016	ES			AB	AB									No Punches Available

When Overlap is allowed: Grace time will overlap with Late-IN

Example:

On 6th: IN punch 9:15 am, The employee will be marked as 15 min late. The Grace time will not be considered and it will overlap with Late-IN so total 15 mins will be considered as Late-IN. Similarly will be on 4th.

On 5th: IN Punch 9:21am, The employee will be marked as Absent due to Late-IN as the Late-IN allowed is only 20 mins. Similarly will be on 7th.

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/07/2016	GS	09:05	18:30	PR	PR			08:25	00:30		01:00			
02/07/2016	GS - WO			WO	WO									
03/07/2016	GS - WO			WO	WO									
04/07/2016	GS	09:11	18:30	PR	PR	00:11		08:19	00:30		01:00			
05/07/2016	GS	09:21	19:00	AB	PR			08:39	01:00		01:00			AB:Late-IN
06/07/2016	GS	09:15	18:30	PR	PR	00:15		08:15	00:30		01:00			
07/07/2016	GS	09:31	18:30	AB	PR			07:59	00:30		01:00			AB:Late-IN

Grace Time for Shift Early Out: Specify the grace time in minutes for going out early from the Office.

Overlap Grace Time With Shift Early-OUT: Check the box to include the Grace Time with the shift Early-Out time.



Grace for Early-OUT, Break Late-IN and Break Early-OUT will work similarly as Late-IN.

Grace Time for Break Late-IN: Specify the grace time in minutes.

Overlap Grace Time With Break Late-IN: Check the box to include the Grace Time too with the break Late-In time.

Grace Time for Break Early-OUT: Specify the grace time in minutes.

Overlap Grace Time With Break Early-OUT: Check the box to include the Grace Time too with the break Early-Out time.

Click on **Save** to save the changes. Once the user has completed the definition of all the shifts they can then be grouped into various schedule groups before being assigned to the users.

Example :Break Duration Calculation For Flexible User

To Configure Flexible Type of user, [See "Flexible Working Settings" on page 1432.](#)

Consider Break Hours Configuration for Flexible User Attendance Calculation are as follows:

- Shift Start Time: 8:00
- Shift End Time: 19:00
- Shift Duration: 10:30
- Minimum Required Working Hours: Half Day - **4:30** and Full Day - **06:00**
- Break Start Time: **13:00**
- Break End Time: **13:30**
- Break Deviation Allowed: **Checked**
- Advance Detail > Deduct Break From Working Hours: For 2 Punch, For 2+ Punch = **Checked**
 - For 2 Punch = Configured Break Duration
 - For 2+ Punch = Configured Break if less, else Actual Break Duration



Work hours may vary depending upon 'Flexible Work Setting > Consider Work Hours' configuration for flexible user.

Cases:

Case 1:

Punches [I/P]			Expected [O/P]			
			Flexible for 24 Hours	From Shift Start	Till Shift End	From Shift Start To Shift End
Punch 1	13:30 - IN	Work Hours	07:00	07:00	05:00	05:00
Punch 2	21:00 - OUT	Break Duration	00:30	00:30	00:30	00:30
		<i>Break Start Time</i>	-	-	-	-
		<i>Break End Time</i>	-	-	-	-

Case 2:

Punches [I/P]			Expected [O/P]			
			Flexible for 24 Hours	From Shift Start	Till Shift End	From Shift Start To Shift End
Punch 1	08:00 - IN	Work Hours	04:30	04:30	04:30	04:30
Punch 2	13:00 - OUT	Break Duration	00:30	00:30	00:30	00:30
		<i>Break Start Time</i>	-	-	-	-
		<i>Break End Time</i>	-	-	-	-

Case 3:

Punches [I/P]			Expected [O/P]			
			Flexible for 24 Hours	From Shift Start	Till Shift End	From Shift Start To Shift End
Punch 1	08:00 - IN	Work Hours	04:45	04:45	04:45	04:45
Punch 2	12:45 - OUT	Break Duration	00:00	00:00	00:00	00:00
		<i>Break Start Time</i>	-	-	-	-
		<i>Break End Time</i>	-	-	-	-

Case 4:

Punches [I/P]			Expected [O/P]			
			Flexible for 24 Hours	From Shift Start	Till Shift End	From Shift Start To Shift End
Punch 1	08:00 - IN	Work Hours	04:49	04:49	04:49	04:49
Punch 2	12:49 - OUT	Break Duration	00:00	00:00	00:00	00:00
		<i>Break Start Time</i>	-	-	-	-
		<i>Break End Time</i>	-	-	-	-

Case 5:

Punches [I/P]			Expected [O/P]			
			Flexible for 24 Hours	From Shift Start	Till Shift End	From Shift Start To Shift End
Punch 1	07:00 - IN	Work Hours	05:30	04:30	05:30	04:30
Punch 2	13:00 - OUT	Break Duration	00:30	00:00	00:30	00:30
		<i>Break Start Time</i>	-	-	-	-
		<i>Break End Time</i>	-	-	-	-

Case 6:

Punches [I/P]			Expected [O/P]			
			Flexible for 24 Hours	From Shift Start	Till Shift End	From Shift Start To Shift End
Punch 1	02:00 - IN	Work Hours	04:30	00:00	04:30	00:00
Punch 2	07:00 - OUT	Break Duration	00:30	00:00	00:30	00:00
		<i>Break Start Time</i>	-	-	-	-
		<i>Break End Time</i>	-	-	-	-

Case 7:

Punches [I/P]			Expected [O/P]			
			Flexible for 24 Hours	From Shift Start	Till Shift End	From Shift Start To Shift End
Punch 1	18:01 - IN	Work Hours	05:28	05:28	00:59	00:59
Punch 2	23:59 - OUT	Break Duration	00:30	00:30	00:00	00:00
		<i>Break Start Time</i>	-	-	-	-
		<i>Break End Time</i>	-	-	-	-

Week Off Group

Week Off Group enables to define the Week Off group which can be assigned to the user. The maximum 99 week off groups can be created.

To create WO group, select **Shift and Schedule module > Week Off Group**. The page appears as shown below:

The screenshot shows the 'Week Off Group' form with the following fields and values:

- Week Off Group ***: ID (empty), Name (empty)
- Auto Week Off Assignment**: ☐ Weekly Basis (dropdown)
- Off Day 1**: Sunday (dropdown)
- Off Day 2**: None (dropdown)
- Off Day 2 On Weeks**: ☐ W1 ☐ W2 ☐ W3 ☐ W4 ☐ W5 ☐ Last
- Week Off Rotation**: ☐ Enable ☐ Rotation Count * 7-99

The right sidebar shows a table with columns 'ID' and 'Name', and a message 'No Data'.

To create a new Week Off Group, click on **New** button.

Week Off Group: Specify a user friendly Name for the Week Off Group. The ID will be auto generated by the system while saving the group.

Auto Week Off Assignment: You can assign WOs on days on which user was found absent but eventually the number of WOs in a month will be as per schedule only. So enable Auto week off assignment on weekly or monthly basis.

For details See Shift Schedule> Auto Week Off Assignment

The screenshot shows the 'Week Off Group' form with the following fields and values:

- Week Off Group ***: ID (empty), RnD WO Group (empty)
- Auto Week Off Assignment**: ☒ Monthly Basis (dropdown)
- Off Day 1**: Sunday (dropdown)
- Off Day 2**: None (dropdown)
- Off Day 2 On Weeks**: ☐ W1 ☐ W2 ☐ W3 ☐ W4 ☐ W5 ☐ Last
- Week Off Rotation**: ☐ Enable ☐ Rotation Count * 7-99

Off Day 1: Select the Off Day 1 from the drop down list of Weekdays.

Off Day 2: If 2 week-offs are to be assigned in the week off group, then select the Off Day 2 from drop down list of Weekdays, else you can select None.

Off Day2 on Weeks: The second week-off can be assigned for the selected week by checking the boxes against the respective weeks as shown below. Eg: Off day2: Tuesday is assigned for 2nd and 4th week.

Auto Week Off Assignment ☐ Monthly Basis

Off Day 1 Sunday

Off Day 2 Tuesday

Off Day 2 On Weeks ☐ W1 ☒ W2 ☐ W3
☒ W4 ☐ W5 ☐ Last

Week Off Rotation

Enable ☐

Rotation Count * 7-99

Week Off Rotation

Enable: Week Off rotation can be enabled by checking the box.

Rotation Count: Specify the Rotation Count of up to 99 for the rotation of week-off days. However, **Rotation Count** can not be less than 7.

Example: If Off Day 1 and Off Day 2 are assigned on Sunday and Tuesday respectively as shown below. And week off rotation is enabled for count 8 days, then both the week offs will be rotated after 8 days.

Week Off Group * ID RnD WO Group

Auto Week Off Assignment ☐ Monthly Basis

Off Day 1 Sunday

Off Day 2 Tuesday


Off Day 2 On Weeks ☒ W1 ☒ W2 ☒ W3
☒ W4 ☒ W5 ☒ Last

Week Off Rotation

Enable ☒

Rotation Count * 8

As shown below, the Week off on 2nd, tuesday will be rotated after 8 days and shifted to wednesday. After 8 days it will be shifted to thursday and will continue to repeat. Similarly the week off sunday will rotate to monday after 8 days and will continue.

User Resham 

Attendance Period

Mon	Tue	Wed	Thu	Fri	Sat	Sun
1 GS	2 GS WO	3 GS	4 GS	5 GS	6 GS	7 GS WO
8 1R	9 GS	10 GS WO	11 GS	12 GS	13 GS	14 GS
15 GS WO	16 GS	17 GS	18 GS WO	19 1F	20 1F	21 1F
22 GS	23 GS WO	24 GS	25 GS	26 GS WO	27 GS	28 GS
29 1R	30 GS					

PH - Public Holiday
WO - Week Off
WO - Week Off & Public Holiday On Same Day



If some week off group is assigned to user, then it will override the off days configured in shift schedule assigned to that user, though it is not mandatory to assign some week off group to user.

Holiday Schedule

Holiday Schedule is a list of non-working days in a calendar year which are user defined. The user can define up to 9999 holiday schedules. In each schedule you can configure holidays and maximum 32 holidays can be synced to the device.

To access the Holiday Schedule, Click on **Holiday Schedule** option from the Shift and Schedule page. The page appears as shown below:

The screenshot shows the 'Holiday Schedule' window. On the left, the 'Configure Holidays' section includes fields for 'ID' (with a dropdown), 'Name' (with a dropdown), 'Default' (with a dropdown), 'Holiday List' (with a dropdown), and 'Total No. Of Days'. On the right, there is a table of 30 pre-defined schedules. The table has two columns: 'ID' and 'Name'. The first 10 rows are visible, showing IDs 1 through 10 and names 'Schedule 1' through 'Schedule 10'. Below the table, it says '1 - 10 of 30 records' and there are pagination controls.

ID	Name
1	Schedule 1
2	Schedule 2
3	Schedule 3
4	Schedule 4
5	Schedule 5
6	Schedule 6
7	Schedule 7
8	Schedule 8
9	Schedule 9
10	Schedule 10

There are pre-defined 30 schedules. You can create a new schedule by clicking New button.

To define holidays in your holiday schedule, select a schedule from the right grid. Click Edit button and configure the holidays in it.

The screenshot shows the 'Holiday Schedule' window with a selected schedule. The 'ID' field is set to '1' and the 'Name' field is set to 'Schedule 1'. The 'Default' dropdown is set to 'Default 1'. The 'Holiday List' dropdown is set to 'All'. The 'Total No. Of Days' is 0. Below the 'Configure Holidays' section, there is a table for defining holidays. The table has five columns: 'No.', 'From', 'To', 'Holiday', and 'Days'. The table is currently empty, and a 'No Data' message is displayed. On the right, the table of 30 pre-defined schedules is shown, with 'Schedule 1' selected. Below the table, it says '1 - 10 of 30 records' and there are pagination controls.

No.	From	To	Holiday	Days
-----	------	----	---------	------

ID/Name: For new schedule specify the name for the schedule. The ID will be auto-generated by the system. For existing schedule you can edit and specify the name to your schedule as shown below.

The screenshot shows the 'Holiday Schedule' window with a new schedule name. The 'ID' field is set to '1' and the 'Name' field is set to 'RnD Schedule'. The 'Default' dropdown is set to 'Default 1'. The 'Holiday List' dropdown is set to 'All'. The 'Total No. Of Days' is 0. On the right, the table of 30 pre-defined schedules is shown, with 'Schedule 1' selected. Below the table, it says '1 - 10 of 30 records' and there are pagination controls.

ID	Name
1	Schedule 1
2	Schedule 2

Default: The schedules 1 to 4 are default holiday schedules. To make other holiday schedule as default you can select the Default option.



When new user is added in COSEC; the holiday schedule which is Default1 will get assigned to the user.



The 4 default holiday schedules can be assigned to the device from Device Configuration> Access Settings.

Configure Holidays

Holiday List: It is the filter which will allow to view the configured holidays for **Previous year, Current year, Next year**. The **Device synced** filter will show those holidays for which Device Synced checkbox is enabled i.e. holidays are synced to device. The **Inactive holidays** filter will show those holidays for which Device Synced checkbox is disabled.

To configure the holidays into holiday schedule; click **Add** button.

Then select the **From** and **To** date by clicking the Calendar button on which holiday is to be given.



The date for which holiday is declared; will not be allowed to declare as Restricted holiday. The Restricted holiday for the same schedule can be configured from "Shift and Schedule> Restricted Holidays."

Specify the name of the **holiday** as shown below.

Enable the **Device Synced** checkbox for the holiday which is to be synced to the device. You can sync maximum 32 holidays in a schedule to the device. Then click **OK** to save the holiday.

Similarly you can add other holidays in the schedule.

Days shows the number of days for which a holiday is configured. For eg: Holi-Dhuleti is configured as one holiday. But it includes 2days so 2 separate days will be counted.

Configure Holidays

Holiday List

All

Total No. Of Days4

No.	From	To	Holiday	Days				
1	15/01/2018	15/01/2018	Makar Sakranti	1	Yes			
2	13/02/2018	13/02/2018	Basant Panchmi	1	No			
3	01/03/2018	02/03/2018	Holi-Dhuleti	2	Yes			

Total No. of days: It shows the sum of all the days configured as holidays in the selected schedule.

After configuring all holidays; click **Save** button to save the holiday schedule.

Holiday Schedule

✓ Saved Successfully

←

+

×

ID *

1

RnD Schedule

Default

Default 1

Configure Holidays

Holiday List

All

Total No. Of Days

4

No. ▲

From

To

Holiday

Days

1

15/01/2018

15/01/2018

Makar Sakranti

1

Yes

2

13/02/2018

13/02/2018

Basant Panchmi

1

No

3

01/03/2018

02/03/2018

Holi-Dhuleti

2

Yes

Search

ID ▲

Name

1

RnD Schedule

2

Schedule 2

3

Schedule 3

4

Schedule 4

5

Schedule 5

6

Schedule 6

7

Schedule 7

8

Schedule 8

9

Schedule 9

10

Schedule 10

1 - 10 of 30 records

«

<

1

2

3

>

»

Copy Holiday

You can create a copy of existing holiday by clicking **Copy Holiday** button of that holiday row. A new row will appear with the same holiday for next year.

No. ▲	From	To	Holiday	Days		
1	15/01/2018	15/01/2018	Makar Sakranti	1	Yes	
2	13/02/2018	13/02/2018	Basant Panchmi	1	No	
3	01/03/2018	02/03/2018	Holi-Dhuleti	2	Yes	

No. ▲	From	To	Holiday	Days		
	15/01/2019	15/01/2019	Makar Sakranti			
1	15/01/2018	15/01/2018	Makar Sakranti	1	Yes	
2	13/02/2018	13/02/2018	Basant Panchmi	1	No	
3	01/03/2018	02/03/2018	Holi-Dhuleti	2	Yes	

You can also change the date for holiday from calendar button.

Then click **OK** to save the new holiday.

No. ▲	From	To	Holiday	Days				
1	15/01/2018	15/01/2018	Makar Sakranti	1	Yes			
2	13/02/2018	13/02/2018	Basant Panchmi	1	No			
3	01/03/2018	02/03/2018	Holi-Dhuleti	2	Yes			
4	15/01/2019	15/01/2019	Makar Sakranti	1	No			

Now this holiday will appear in **Next Year** holiday list as shown below.

Configure Holidays

Holiday List

Next Year ▼

Total No. Of Days

1

No. ▲	From	To	Holiday	Days				
4	15/01/2019	15/01/2019	Makar Sakranti	1	No			

Click on **Save** to save the holidays to the schedule.

Similarly, when you want to configure holiday list for current year. You can take the already configured list of previous year. And edit the changes with new date or new name of holiday.

Eg: If Rakshabandhan in year 2017 was on 26 August. And for current year 2018, it is on 22 August. Then You can edit the date from 26 Aug 2017 to 22 Aug 2018. The holiday 26 Aug 2017 can be viewed from the **Previous holidays** list.

Once defined, the Holiday schedules can then be assigned to the users.

Read Restricted Holidays > Assigning Holiday schedule to user.

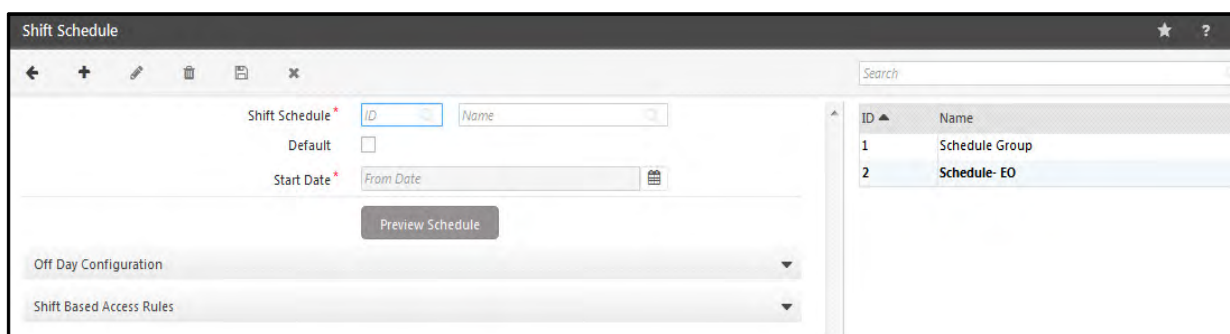
Shift Schedule

Shift Schedules are detailed chart indicating the working hours for group employees based on the organisation's requirement. It defines the details like timing, no. of days, shift rotation, rotation count etc for each shift configured.

The Shift Schedule enables the user to group multiple shifts into a single entity which can then be assigned to the employees. This option enables the administrator to assign different working hours and off days for each user by defining different schedules. For Assigning Shift Schedule to user *See User Configuration> Access Control*.

A maximum of **999** shift schedules can be configured and each Shift Schedule can have up to 32 different shifts as members.

To configure Shift Schedule, Select **Shift and Schedule module > Shift Schedule**. The page appears as shown below:

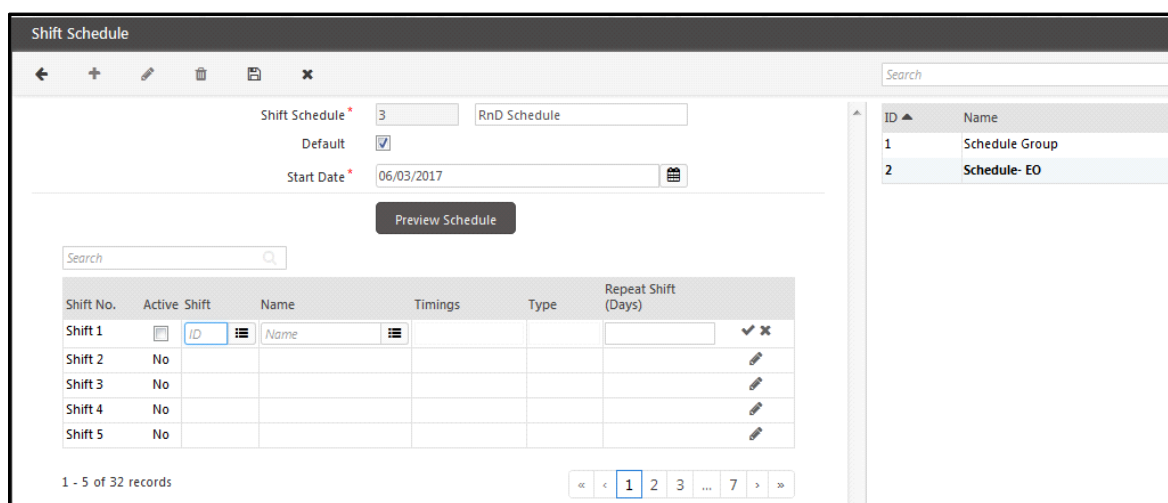


To create a new Shift Schedule click on **New** button. The Schedule ID will be generated by the system and cannot be edited by the user.

Name: Specify a user friendly Name for Shift schedule.

Default: Check the box to set the shift schedule to default.

Start Date: Select the Start Date from the calendar from which the Shift Schedule will be started.



To add the shifts to the schedule, click on Shift No. The grid will be enabled as shown above.

Active: Check the Active box to enable the shift.

Shift: Then select the Shift from the picklist to be added to the schedule. The Name of the shift, Timings and Type of the shift will be displayed.

Repeat Days: Enter the number of days for which shift will be continued. Suppose GS is repeated for 7 days and NS is repeated for 10 days so GS will continue for 7 days and then NS will continue for 10 days.

The first shift of the schedule is to be selected from the User configuration> Access Control> Basic> Start Shift.

Then click OK to save the shifts.

Shift No.	Active	Shift	Name	Timings	Type	Repeat Shift (Days)
Shift 1	Yes	GS	General Shift	09:00 - 18:00	Normal	7
Shift 2	Yes	NS	Night Shift	21:00 - 05:00	Normal	10
Shift 3	No					
Shift 4	No					
Shift 5	No					

Click **Save** button to save the Shift Schedule.

You can edit or delete the shift from the schedule by clicking on Edit button. In edit mode the preview of schedule can be viewed by clicking **Preview Schedule** button.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	1	2	3	4
5	6 GS	7 GS	8 GS	9 GS	10 GS	11 GS
12 GS WO	13 NS	14 NS	15 NS	16 NS	17 NS	18 NS
19 NS WO	20 NS	21 NS	22 NS	23 GS	24 GS	25 GS
26 GS WO	27 GS	28 GS	29 GS	30 NS	31 NS	1
2	3	4	5	6	7	8

PH - Public Holiday WO - Week Off WO - Week Off & Public Holiday On Same Day

Off Day Configuration

Click on the Off Day Configuration section to set the Off Days and Week Off Rotation as shown below:

The screenshot shows the 'Off Day Configuration' window. It includes the following fields and options:

- Auto Week Off Assignment:** A checked checkbox and a dropdown menu set to 'Weekly Basis'.
- Off Day 1:** A dropdown menu set to 'Sunday'.
- Off Day 2:** A dropdown menu set to 'Saturday'.
- Off Day 2 On Weeks:** A grid of checkboxes for weeks W1 through W6. W2 and W4 are checked.
- Week Off Rotation:** An 'Enable' checkbox (unchecked) and a 'Rotation Count' text box containing '7-99'.
- Shift Based Access Rules:** A dropdown menu at the bottom.

Auto Week Off Assignment:

You can assign WOs on days on which user was found absent but eventually the number of WOs in a month should be as per schedule only. So enable Auto week off assignment on weekly or monthly basis.



Only the Week-Offs assigned via Shift Schedule Process will be considered for movement or auto assignment; not the manually assigned Week-Offs.

For eg: WO on 7th is shifted on 4th as shown below. As the user is present on 7th so it is considered as working day and the same week off is given on the absent day marking as Week Off.

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/08/2016	GS	09:05	17:45	PR	AB			07:40			01:00			AB:Early-OUT
02/08/2016	GS	09:15	18:16	PR	PR			08:01	00:16		01:00			
03/08/2016	GS	09:30	18:30	PR	PR			08:00	00:30		01:00			
04/08/2016	GS	14:00	17:45	PR	AB			07:00			01:00			AB:Early-OUT
05/08/2016	GS	11:30	17:30	PR	AB			05:00			01:00			AB:Early-OUT
06/08/2016	GS	08:45	18:00	PR	PR			08:15	00:15		01:00			
07/08/2016	GS - WO	09:00	18:15	WO	WO			08:15	00:15		01:00			

After Monthly Attendance Process of the user, the Punches and WO will become as shown below:

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/08/2016	GS	09:05	17:45	PR	AB			07:40			01:00			AB:Early-OUT
02/08/2016	GS	09:15	18:16	PR	PR			08:01	00:16		01:00			
03/08/2016	GS	09:30	18:30	PR	PR			08:00	00:30		01:00			
04/08/2016	GS - WO	14:00	17:45	WO	WO			03:45						
05/08/2016	GS	11:30	17:30	PR	AB			05:00			01:00			AB:Early-OUT
06/08/2016	GS	08:45	18:00	PR	PR			08:15	00:15		01:00			
07/08/2016	GS	09:00	18:15	PR	PR			08:15	00:15		01:00			

If you have assigned two week offs in the schedule with Auto week off enabled, then WO will be shifted on 2 absent days.

Off Day1 & Off Day2: Select the Off Day 1 from the drop down list of Weekdays (eg: Sunday). For configuring second week off, select the Off Day 2 from the drop down list(eg: Saturday). If only one week off is to be given, then select "None" for Off Day2.

Off Day2 on Weeks: You can select the Late week for which Off Day2 is to be assigned. For eg: Saturday is assigned as week off on 2nd and 4th saturday.

Week Off Rotation

Enable: Off Day rotation can be enabled by checking the box. If Auto Week Off Assignment is enabled, Week Off Rotation will be disabled.

Rotation Count: Specify the Rotation Count for rotating single or both week offs as configured. The Rotation Count can not be less than 7.

Here as specied in below figure, The off day on sunday will rotate to monday after the count of 15 days. Similarly it will continue to rotate further to Tuesday and so on.

Off Day Configuration

Auto Week Off Assignment ☐ Weekly Basis

Off Day 1 Sunday

Off Day 2 None

Off Day 2 On Weeks ☐ W1 ☐ W2 ☐ W3 ☐ W4 ☐ W5 ☐ W6

Week Off Rotation

Enable ☒

Rotation Count 15

If both the off days are assigned for rotation, then both will rotate similarly.

Eg: Sunday will rotate to Monday and Tuesday will rotate to Wednesday after 15 days.

Off Day Configuration

Auto Week Off Assignment ☐ Weekly Basis

Off Day 1 Sunday

Off Day 2 Tuesday

Off Day 2 On Weeks ☒ W1 ☒ W2 ☒ W3 ☒ W4 ☒ W5 ☒ W6

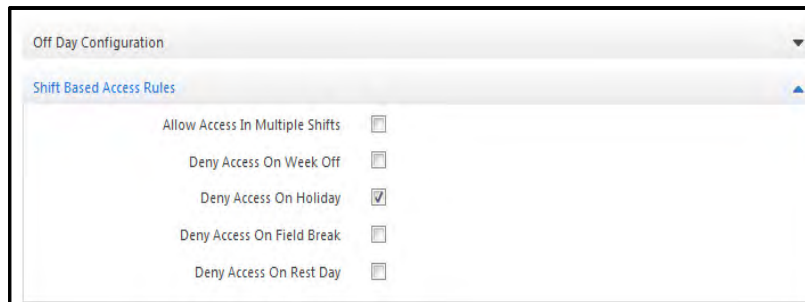
Week Off Rotation

Enable ☒

Rotation Count 15

Shift Based Access Rules

Click on the Shift Based Access Rules section to configure access based on shifts/ WO/ holidays as shown below:



The screenshot shows a configuration window titled "Off Day Configuration" with a dropdown arrow. Below the title bar, the "Shift Based Access Rules" section is selected and highlighted in blue. This section contains five settings, each with a label and a checkbox:

Setting	Checkbox
Allow Access In Multiple Shifts	<input type="checkbox"/>
Deny Access On Week Off	<input type="checkbox"/>
Deny Access On Holiday	<input checked="" type="checkbox"/>
Deny Access On Field Break	<input type="checkbox"/>
Deny Access On Rest Day	<input type="checkbox"/>

Allow Access in Multiple Shifts: Check this box to allow the User to work in multiple or any of the shifts from the schedule.

Deny Access on Week Off: Check the box to deny access on week off days.

Deny Access on Holiday: Check the box to deny access on holidays.

Deny Access on Field Break: Check the box to deny access on field break days.

Deny Access on Rest Day: Check the box to deny access on Rest day.

Click on **Save** button to save the changes to the shift schedule.

Restricted Holidays

The COSEC application allows the administrator to define restricted holidays which can be availed by the users in addition to the regular holidays as defined in the system. However, these are optional for the users and the individuals may choose a limited number of holidays from this category as per the organizational policies.

To access the Restricted Holidays, select **Shift and Schedule module > Restricted Holidays**. The page appears as shown below:

Restricted Holidays

Search

Schedule Name

Configure Holidays

Search

Date Restricted Holiday

No Data

ID	Name	No. Of Restricted Holidays
1	Schedule 1	0
2	Schedule 2	0
3	Schedule 3	0
4	Schedule 4	0
5	Schedule 5	0
6	Schedule 6	0
7	Schedule 7	0
8	Schedule 8	0
9	Schedule 9	0
10	Schedule 10	0
11	Schedule 11	0
12	Schedule 12	0
13	Schedule 13	0
14	Schedule 14	0
15	Schedule 15	0

1 - 15 of 31 records

<< < 1 2 3 > >>

The schedules in the right grid are those defined in ["Holiday Schedule"](#).

Select the Schedule from the grid wherein the restricted holidays are to be added.

Schedule: The Schedule ID and Name will be displayed as defined in Holiday Schedule.

Configure Holidays: To configure the Restricted holidays, click Add button as shown below.

Configure Holidays

Search

Date Restricted Holiday

03/03/2017

+

Date: Select the date from the Calendar on which the restricted holiday is to be configured. The system ensures that the date of the Restricted Holiday does not coincide with a holiday date as defined in the Holiday schedules.

Holiday Name: Specify the name for the restricted holiday.

Click on **OK** to add the list of holidays. Then click **Save** button to save the Restricted Holidays to the holiday schedule.

ID	Name	No. Of Restricted Holidays
1	Schedule 1	2
2	Schedule 2	0
3	Schedule 3	0
4	Schedule 4	0
5	Schedule 5	0
6	Schedule 6	0
7	Schedule 7	0
8	Schedule 8	0

Assigning holiday schedule to user

Now this holiday schedule with 15 holidays and 3 restricted holidays will be assigned to the user from the Access Control tab of **User configuration** as shown below:

After the schedule has been assigned to the user, the user must have the leave balance before applying for the leave(If the balance check is enabled for the leave).

Crediting RH leave

Then administrator must credit the leave to the employee from Leave Management module as shown below:

Leave Management

Credit/Debit/Encashment

Period: Monthly
 Entry Type: Credit
 Month-Year: July 2016
 Leave: RH Restricted Leave
 Credit Mode: Fixed
 Credit Value: 2
 Apply Pro-rata: ☐
 Remark:
 User Filter: Randomly
 User: NR Naman
 Apply

Here 2 Restricted leave is credit to the employee for the month July 2016.

Applying RH leave

Now the user can apply for the restricted holiday from his ESS account which will be then approved by the reporting incharge. Also the leave can be applied for the user through Leave Application module by system account user.

The user is applying the second half leave on 8 July as restricted holiday through ESS. As there is available balance so he can apply.

Leave Application

Application Date: 2016/07/08
 Half Day Consideration: Both
 From Date: 2016/07/08 Second Half
 To Date: 2016/07/08 Second Half
 Applied Days: 0.5
 Posted Days:
 Leave: RH - Restricted Leave
 Current Balance: 2.00
 Reason And Contact Info
 Reason: 50 Char
 Address: 30 Char
 Contact Number: 20 Char
 Apply For Cancellation
 Apply For Modification

✎ If he applies RH leave on some other day which is not declared as restricted holiday then he will not be allowed to apply for the leave.

Leave Application Leave Approval is pending

Application Date: 2016/07/08
 Half Day Consideration: Both
 From Date: 2016/07/08 Second Half
 To Date: 2016/07/08 Second Half
 Applied Days: 0.5
 Posted Days: 0.5
 Leave: RH - Restricted Leave
 Current Balance: 1.50
 Reason And Contact Info
 Reason: 50 Char

From	To	Leave	Application Date	Application Type	Status
2016/07/08	2016/07/08	RH	2016/07/08	New	Pending

Approving RH leave

1220
SHEETAL RAVAL

Time Attendance
Leave Management
Group Details
Approval/Authorization
Short Leave/Official In-Out Authorization
Attendance Correction Authorization
Leave Application Approval
Tour Application Approval
Award/Penalty Authorization
Field Visit Correction Authorization
Cafeteria
Job Costing
FVM
Reports

Leave Approval

Show All Pending Applications ☐

Leave Date 2016/06/08 2016/07/08

Authorization For Leave Application

Filter Users All

Group/User ID Name

View

Pending (1)

User ID	Name	From Date	To Date	Leave	Application Date	Posted Days	Approve	Reject	Details
NR	Naman	2016/07/08	2016/07/08	RH-Restricted Leave	2016/07/08	0.5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Approved (0)									
Rejected (0)									

The Reporting Incharge of the user can view the pending leave applications and approve or reject the leave by checking the respective box. Also the administrator can authorize the leave from Leave Approval section of Leave module.

There can be 1 or 2 reporting incharges depending on the configuration [See "Reporting In-Charge" on page 482](#).

The **Daily Attendance View** for User Naman shows RH in second half of 8th july.

2016/07/07	GS	08:45	19:45	PR	PR	
2016/07/08	GS	09:00		IN	RH	
2016/07/09	GS - WO					

Manage Shift

This page allows admin to change shifts of a single user/enterprise group, to change/view a user's view schedule or to check the shift-wise user count.

Go to **Shift Schedule module> Utilities> Manage Shift**. The Manage Shifts page is shown as below.

The screenshot shows the 'Manage Shifts' form. It has a title bar 'Manage Shifts' with navigation icons. Below the title bar, there are two date pickers: 'Date *' with '04/01/2017' and '04/26/2017'. Below the date pickers, there is a 'User *' field with '2' and a dropdown menu showing 'Chirag'. There are 'View' and 'Export' buttons at the bottom.

Date: Select the From and To Date to view the shift details for the selected date range.

User: Select the user from the picklist for whom the shift details is to be viewed and managed.

Click the **View** button to view the details of the users' everyday shifts in the defined date range. The selected user's summary is displayed on the right side as shown below.

The screenshot shows the 'Manage Shifts' page. It has a title bar 'Manage Shifts' with navigation icons. Below the title bar, there are two date pickers: 'Date *' with '04/01/2017' and '04/26/2017'. Below the date pickers, there is a 'User *' field with '2' and a dropdown menu showing 'Chirag'. There are 'View' and 'Export' buttons at the bottom. Below the buttons, there is a table showing shifts for the date range '04/01/2017 - 04/07/2017'. The table has columns for 'User ID', 'Name', and dates from '01 Apr Sat' to '07 Apr Fri'. The data row shows '2', 'Chirag', and 'GS' for all days. To the right of the table, there is a user summary for '2 Chirag'. It includes a profile picture, 'Shift Schedule' and 'Schedule Group' links, 'Starting Shift' 'GS - General Shift', and a table of shifts for the date range '04/01/2017 - 04/26/2017'. The table has columns for 'Shifts' and 'Days'. The data row shows 'GS' and '26'. Below this, there is a table of shift counts: 'WO' 4, 'PH' 0, 'Leave' 0, and 'Tour' 2.

User ID	Name	01 Apr Sat	02 Apr Sun	03 Apr Mon	04 Apr Tue	05 Apr Wed	06 Apr Thu	07 Apr Fri
2	Chirag	GS	GS	GS	GS	GS	GS	GS

04/01/2017 - 04/26/2017

Shifts	Days
GS	26

WO	4
PH	0
Leave	0
Tour	2

Click on Filter  to select the multiple users based on Enterprise groups.

User Selection

For multiple user selection, the options are:

- **User wise:** Individual user can be selected from the picklist.
- **Group wise:** user can be selected based on the selection of enterprise group.
- **All:** all the active users can be selected.

More Filters

Select Users

User Wise

User *

ID

Name

Search

User ID	Name
101	Khushbu
1567	Sheetal
2	Chirag

Apply

If multiple users are selected, clicking on **View** button shows the grid with list of shifts assigned (fetched as per the "T&A> Utilities> Shift-Wise Management" page). The right side of the page displays a filtered users' count Summary as shown below.

Manage Shifts

Date *

04/01/2017

04/26/2017

User *

ID

Name

View

Export

Shifts		04/01/2017					
Shift ID	Name	Scheduled	Reported	Not Reported	On Leave/Tour	On Week-Off	On Holiday
GS	General Shift	3	1	2	0	0	0

Not Scheduled 0

04/01/2017

Scheduled	3
Reported	1
Not Reported	2
On Leave/Tour	0
On Week-Off	0
On Holiday	0

To view the details of user who are **Scheduled, Reported, Not Reported** etc on the shift; click on the respective number. For eg: The Scheduled users will be displayed as below.

Manage Shifts

Date *

04/01/2017

04/26/2017

User *

ID

Name

View

Export

Scheduled		04/01/2017 - 04/07/2017						
User ID	Name	01 Apr Sat	02 Apr Sun	03 Apr Mon	04 Apr Tue	05 Apr Wed	06 Apr Thu	07 Apr Fri
101	Khushbu	GS	GS WO	GS	GS	GS	GS	GS
2	Chirag	GS	GS WO	GS	GS	GS	GS	GS
1567	Sheetal	GS	GS WO	GS	GS	GS	GS	GS

04/01/2017

Scheduled	3
Reported	1
Not Reported	2
On Leave/Tour	0
On Week-Off	0
On Holiday	0

Export & Import

The user can export the shifts of multiple user in XLS format to the local drive of a computer. This data can then be manually corrected and updated on the system by importing the excel sheet.

The date range for which the shift details is required must be selected. Then select a single user from the picklist or multiple users from the filter before exporting the shift details. [See “User Selection” on page 1212.](#)


User Selection

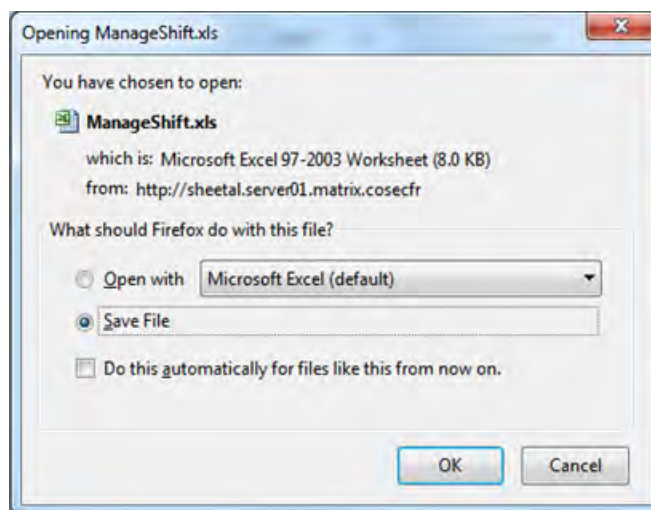
Click the filter  to select the users based on Enterprise groups. For multiple user selection, the options are:

- **User wise:** Individual user can be selected from the picklist
- **Group wise:** user can be selected based on the selection of enterprise group.
- **All:** all the active users can be selected.

Then click **Apply** to save the selection.

Export

Now click Export  button. The following pop up window will appear prompting to save the file on a local drive.



After saving the file, click the download folder and open the file.

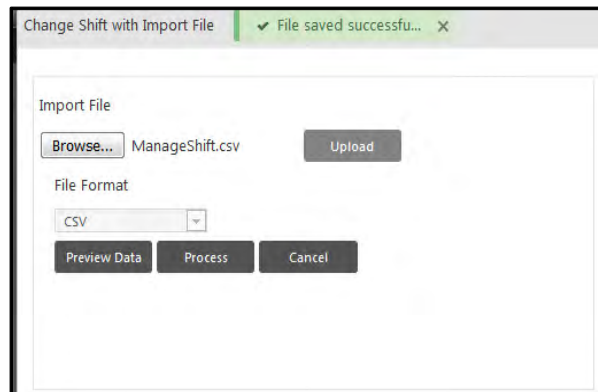
The exported shift file is shown as below.

Userid	User Name	01-Apr-2017	02-Apr-2017	03-Apr-2017	04-Apr-2017	05-Apr-2017	06-Apr-2017	07-Apr-2017	08-Apr-2017	09-Apr-2017	10-Apr-2017	11-Apr-2017	12-Apr-2017	13-Apr-2017	14-Apr-2017
101	Khushbu	GS	WO	GS	GS	GS	GS	GS	GS	WO	GS	GS	GS	GS	GS
1567	Sheetal	GS	WO	GS	GS	GS	GS	GS	GS	WO	GS	GS	GS	GS	GS
2	Chirag	GS	WO	GS	GS	GS	GS	GS	GS	WO	GS	GS	GS	GS	GS

Import

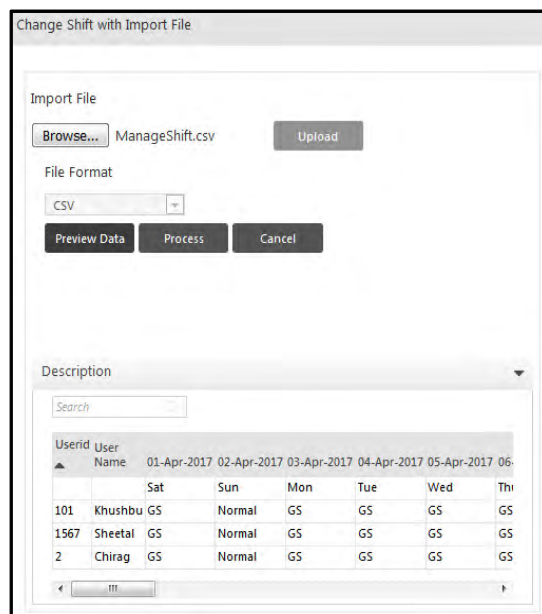
You can make the necessary manual corrections to the exported file. Save the file and note down the file location.

Click the **Import**  icon to import the file with changes in shift.



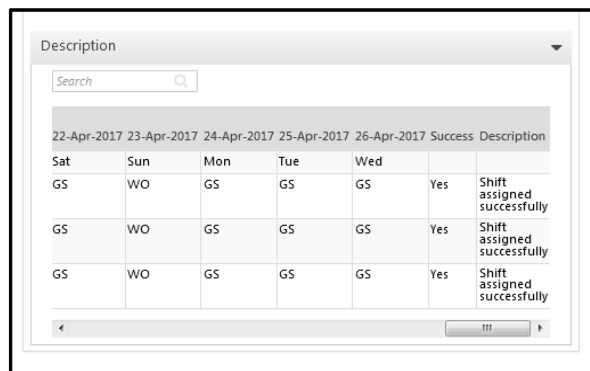
Browse the file and click **Upload** button to upload the modified shift file.

Select a **File Format** (XLS or CSV) for uploading. Click **Preview Data** to view the preview of updated data.



Userid	User Name	01-Apr-2017	02-Apr-2017	03-Apr-2017	04-Apr-2017	05-Apr-2017	06-Apr-2017
		Sat	Sun	Mon	Tue	Wed	Thu
101	Khushbu	GS	Normal	GS	GS	GS	GS
1567	Sheetal	GS	Normal	GS	GS	GS	GS
2	Chirag	GS	Normal	GS	GS	GS	GS

Click **Process** button to import the file and update the shift change. The Description section shows the success of import as shown below.



22-Apr-2017	23-Apr-2017	24-Apr-2017	25-Apr-2017	26-Apr-2017	Success	Description
Sat	Sun	Mon	Tue	Wed	Yes	Shift assigned successfully
GS	WO	GS	GS	GS	Yes	Shift assigned successfully
GS	WO	GS	GS	GS	Yes	Shift assigned successfully
GS	WO	GS	GS	GS	Yes	Shift assigned successfully



If WO is to be changed to other shift, then Normal must be typed in place of WO in excel sheet, then is imported. Once the WO is changed to Normal, then you can assign other shift to it.

For eg: The GS WO shift on 2nd April is changed to GS shift as shown below. Now this shift can be changed as per requirement.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1 GS
2 GS	3 GS	4 GS	5 GS	6 GS	7 GS	8 GS
9 GS WO	10 GS	11 GS	12 GS	13 GS	14 GS	15 GS
16 GS WO	17 GS	18 GS	19 GS	20 GS	21 GS	22 GS
23 GS WO	24 GS	25 GS	26 GS	27 GS	28 GS	29 GS
30 GS WO	1	2	3	4	5	6

PH - Public Holiday WO - Week Off WO - Week Off & Public Holiday On Same Day

To change the Shift

Click on the shift of user which is to be changed.

User ID	Name	01 Apr Sat	02 Apr Sun	03 Apr Mon	04 Apr Tue	05 Apr Wed	06 Apr Thu	07 Apr Fri
1567	Sheetal	GS	GS WO	GS	GS	GS	GS	GS

The Change Shift window appears as shown below.

Change Shift

Current Shift: GS General Shift: [dropdown]

Replace With*: NS Night Shift: [dropdown]

Week Off (WO): ☐

Holiday (PH): ☐

Change Shift For*: 04/03/2017 04/03/2017

[Update] [Cancel]

Replace with: Select the other shift from the picklist to replace the existing shift.

WO/PH: You can check the box for week-off or Holiday to be assigned to the selected day.

Change Shift for: The change in shift can be done for single day or multiple days by selecting the from and to dates.

Finally click on **Update** to change the shift.

So shift will be changed from GS to NS as shown below.

04/01/2017 - 04/07/2017								
User ID	Name	01 Apr Sat	02 Apr Sun	03 Apr Mon	04 Apr Tue	05 Apr Wed	06 Apr Thu	07 Apr Fri
1567	Sheetal	GS	GS WO	NS	GS	GS	GS	GS

To view the Schedule

The shift schedule of the user can be viewed by clicking on Schedule Group of the user and selecting **View Schedule** as shown below.

Manage Shifts

Date *

04/01/2017

04/26/2017

User *

2

Chirag

View

Export

04/01/2017 - 04/07/2017

User ID	Name	01 Apr Sat	02 Apr Sun	03 Apr Mon	04 Apr Tue	05 Apr Wed	06 Apr Thu	07 Apr Fri
2	Chirag	GS	GS	GS	GS	GS	GS	GS

2

Chirag

Shift Schedule

Schedule Group

View Schedule

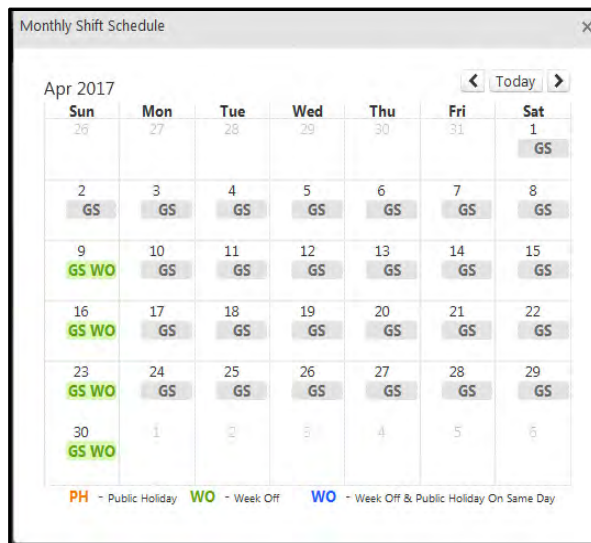
Starting Shift

GS - General S

Change Schedule

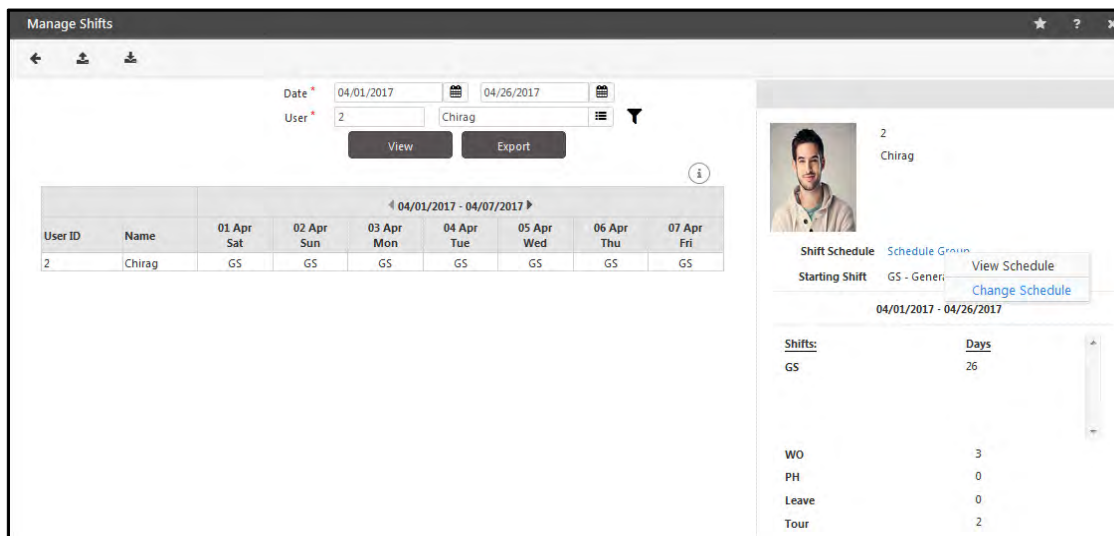
04/01/2017 - 04/26/2017

Shifts:	Days
GS	26
WO	3
PH	0
Leave	0
Tour	2



To Change the Schedule

The shift schedule of the user can be changed by clicking on Schedule Group of the user and selecting **Change Schedule** as shown below.



Change Type: You can select the schedule change as Temporary or Permanent.

New Schedule: Select the shift schedule from the picklist which is to be updated.

Start Shift: Select the shift as the starting shift of the schedule.

Attendance Period: Select the From and To date for which the schedule is to be changed temporary. For permanent change, only from date is to be selected.

Click on **Update** to change the schedule.

Change Schedule

User

2

Chirag

Change Type

Temporary

Change From

Existing Schedule

1

Schedule Group

Start Shift

GS

General Shift

Change To

New Schedule

3

RnD Schedule

Start Shift

GS

General Shift

Attendance Period

04/01/2017

04/28/2017

Update

Cancel

Change Schedule

This option enables the HR user to change the currently effective Schedule Group for a user or multiple users to another Schedule Group. This becomes essential in cases where the employee needs to be temporarily or permanently moved to a new shift based on certain considerations. The system maintains a record of the previous Schedule Groups which had been assigned to the users.

To use the Change Schedule feature, select **Shift and Schedule module > Utilities > Change Schedule**. The page appears as shown below:

The screenshot shows the 'Change Schedule' form. At the top, there is a 'Change Type' dropdown menu set to 'Temporary'. Below this, there are two rows of input fields. The first row is for 'Date', with 'From Date' and 'To Date' fields, each accompanied by a calendar icon. The second row is for 'Schedule', with 'ID' and 'Name' fields, each accompanied by a list icon. Below these is a 'Start Shift' row with 'ID' and 'Name' fields, also with list icons. A 'Preview' button is located below the 'Start Shift' fields. Below the 'Preview' button is a 'Select Users' dropdown menu set to 'User Wise'. Below this is a 'User' row with 'ID' and 'Name' fields, each with a list icon. An 'Apply' button is located at the bottom of the form.

Change Type: Select the Change Type which needs to be changed for the user from the drop down list. The options available are

- **Temporary:** For the Temporary change, click on the **Date** selection button and select the date range from the pop up calendar.
- **Permanent:** For the Permanent Change, only administrator can select the **Start Date**.

Schedule: Click on the Schedule Group Master Picklist button and select the **New Schedule Group** to which the user is to be assigned for this period.

Start Shift: Click on the Shift selection button and Select the Start Shift from which the new schedule is to be started.

The screenshot shows the 'Change Schedule' form with example data. The 'Change Type' dropdown is still 'Temporary'. The 'Date' row now has '02/01/2017' in the 'From Date' field and '02/25/2017' in the 'To Date' field. The 'Schedule' row has '2' in the 'ID' field and 'Schedule- EO' in the 'Name' field. The 'Start Shift' row has '12' in the 'ID' field and 'Early Out Shift' in the 'Name' field. The 'Preview' button is still present. The 'Select Users' dropdown is still 'User Wise'. The 'User' row has empty 'ID' and 'Name' fields. The 'Apply' button is still at the bottom.

Select Users: Select the User from the drop down list. The options to filter the user are:

- **User Wise:** It enables the administrator to randomly select users from the user Picklist.
- **Group Wise:** It enables the administrator to select all users belonging to a particular group.
- **All:** It enables the administrator to select all active users in the database.

Select the user by clicking on the box and Click on **Apply** to save the changes.

←

Change Schedule

Change Type

Temporary

▼

Date *

02/01/2017

📅

02/25/2017

📅

Schedule *

2

Schedule- EO

☰

Start Shift

12

Early Out Shift

☰

Preview

Select Users

Group Wise

▼

Select Group

Organization

▼

Organization *

ID

Name

☰

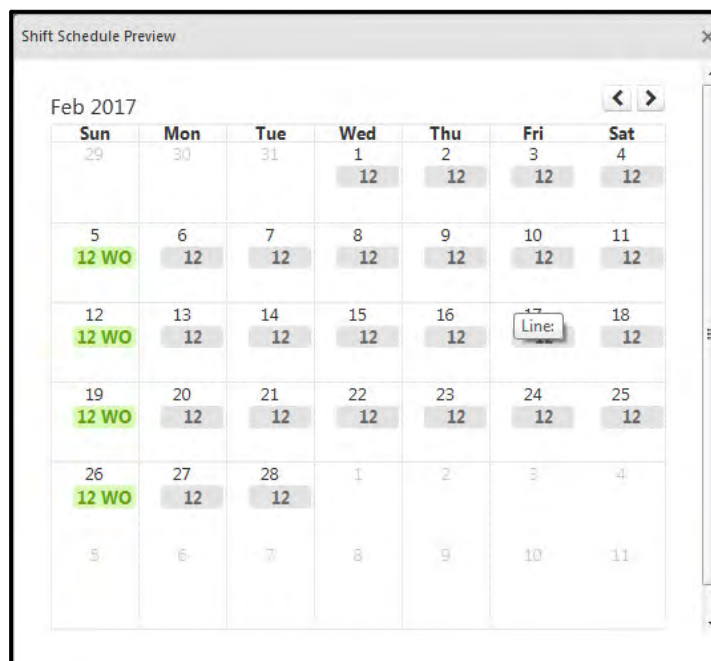
Search

🔍

ID	Name	Group ▲	🗑
1	Organization-1	Organization	🗑

Apply

The user can also view a graphical representation of the schedule in the case of a single user by clicking on the **Preview** button.



Thus, for the selected users, the shift schedule will be changed either temporary or permanent for the defined time period.

Change Week-Off

This functionality enables the administrator to swap a week off day as and when required. This is normally used when an employee or group of employees work on a week off and have to be given an off day on another day of the week.

To use the Change Week-off feature, select **Shifts and Schedule > Utilities > Change Week-off**. The page appears as shown below:

The screenshot shows the 'Change Week-Off' form. It has a title bar with a back arrow and a star icon. The form contains two date selection fields: 'Current Week-Off Date' with the value '16/04/2017' and 'New Week-Off Date' with the value '17/04/2017'. Below these is a 'Select Users' dropdown menu set to 'User Wise'. Underneath is a 'User' section with 'ID' and 'Name' input fields. At the bottom is an 'Apply' button.

Current Week-Off Date: Select the current weekoff date from the date selection button which is required to be changed.

New Week-Off Date: Select the new weekoff date from the date selection button to replace the current weekoff date.

User Filter: Select the user from the filter options of User Wise, Group Wise or All. The options to filter the user are:

- **User Wise:** Enables administrator to randomly select users from the user Picklist window.
- **Select Group:** Enables the administrator to select all users belonging to a particular group.
- **All:** Enables administrator to select all active users in the database.

This screenshot shows the 'Change Week-Off' form with a user list. The 'Current Week-Off Date' is '16/04/2017' and the 'New Week-Off Date' is '17/04/2017'. The 'Select Users' dropdown is set to 'User Wise'. Below it, the 'User' section shows 'ID' and 'Name' fields. A search bar is present. A table displays a list of users:

User ID	Name	
03	Arushi	

At the bottom is an 'Apply' button.

Click on **Apply** to change the week-off.

The Week-off on 16th will be changed to 17th as shown below.

User*03Arushi

Attendance PeriodApril2017

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1 GS
2 GS WO	3 GS PH	4 GS	5 GS	6 GS	7 GS	8 D2
9 GS WO	10 PP WO	11 GS	12 GS	13 GS	14 GS	15 GS
16 GS	17 GS WO	18 GS	19 GS	20 GS	21 GS	22 GS
23 GS WO	24 GS	25 GS	26 GS	27 GS	28 GS	29 GS
30 GS WO	1	2	3	4	5	6

PH - Public Holiday

WO - Week Off

WO - Week Off & Public Holiday On Same Day

Sync Change to Device

Sync Change to Device is a feature which is used to manually send and update the shift schedule(Exceptions list) on the devices with shift based access control feature.

To use the Sync Schedule change to Device feature, Click on **Shift and Schedule > Utilities > Sync Change to Device**. The page appears as shown below:

The screenshot shows a web application window titled "Sync Schedule Change To Device". It features a back arrow in the top left. The main form contains the following elements:

- Schedule Date ***: A date picker showing "04/14/2017".
- Device Filter**: A dropdown menu currently set to "Randomly".
- Device ***: Two input fields, "ID" and "Name", each with a list icon to its right.
- Sync Type**: A dropdown menu currently set to "Only Exceptions".
- User Filter**: A blue link-like label.
- Select Users**: A dropdown menu currently set to "User Wise".
- User ***: Two input fields, "ID" and "Name", each with a list icon to its right.
- Sync**: A dark button at the bottom center.

Schedule Date: Select the current or future date from the calendar whose updated schedule is to be synchronized to the device.

Device Filter: Select the device filter as **Randomly** or **All** on which the changed schedule is to be synchronized.

Device: For Randomly option click the picklist and select the Panel200 to sync the change to the respective Panel doors. For All option, all the Panel200 will be selected.

Sync Type: Select the Sync type options to synchronize the change to device.

- **Only Exceptions:** An exception record for the particular changed schedule i.e. the shift schedule change for a particular day will be generated and sent to the device.
- **All Shifts:** An exception record for all the selected user will be generated and sent to the device irrespective of any particular shift change.

The exception record will be generated only if the corresponding user has shift based access enabled and at least one Panel200 assigned to the user

Schedule Date * 04/14/2017

Device Filter Randomly

Device * ID Name

Sync Type Only Exceptions

User Filter

Select Users User Wise

User * ID Name

Search

User ID ▲	Name	
07	Aditi	
101	Khushbu	

Sync

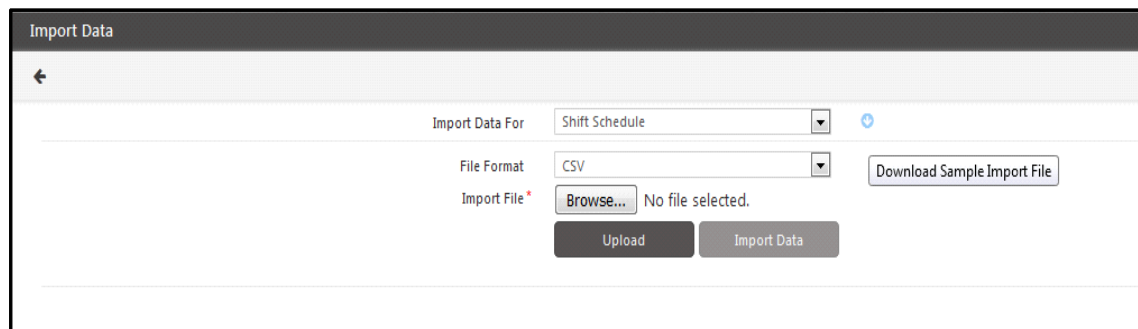
User Filter: Select the User from the drop down list for whom the shift schedule exceptions are to be synced to the device. The options to filter the user are:

- **Use Wise:** Enables administrator to randomly select users from the user Picklist window.
- **Group Wise:** Enables the administrator to select all users belonging to a particular group.
- **All:** Enables administrator to select all active users in the database.

Select the user and Click on **Sync** to send the changes to the device.

Manual Schedule Import

To Import the Manual Schedule, select **Shifts and Schedules> Utilities > Manual Schedule Import**. The page appears as shown below:



Import Data For: The Data is to be imported for Shift Schedule by default

You can download the sample import file and enter the data for Shift and Schedules. Then the updated file can be imported here.

File Format - Select the format for the file to be imported. The options available are XLS or CSV.

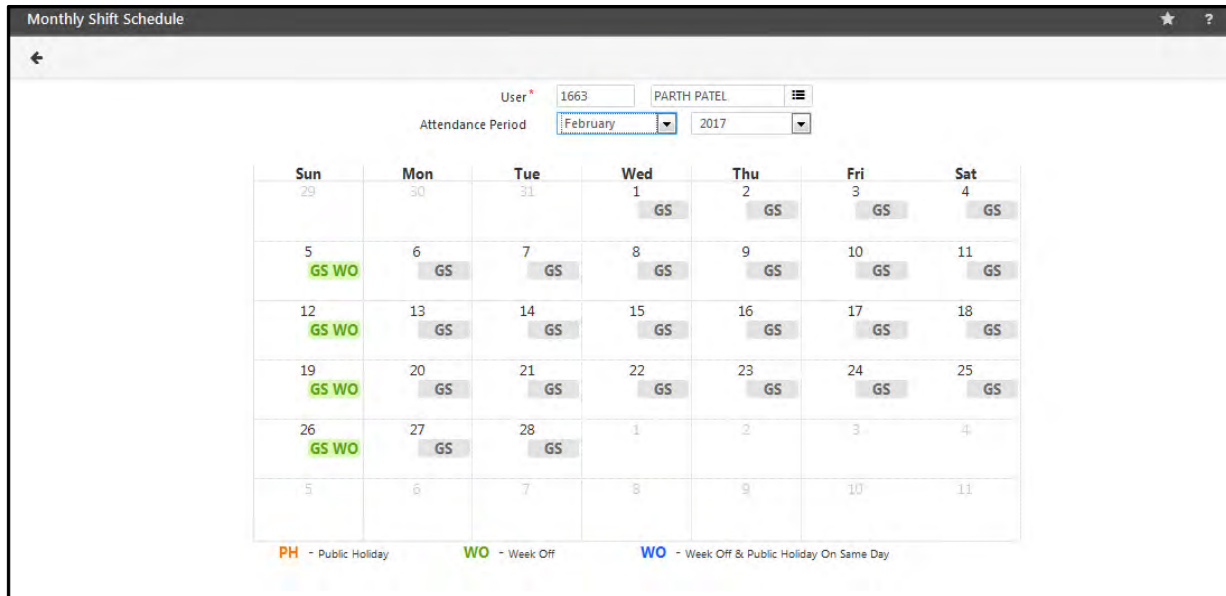
Import File - Browse the path of the file and select the file from which the data is to be imported.

Click **Upload** button to save the file. The **Preview Data** button enables the administrator to view the data in the respective worksheets to confirm that the data is in order prior to giving the import command.

Click on **Import Data** to start the import of data.

Monthly Shift Schedule

To view the monthly shift schedule assigned to the user, Click on **Monthly Shift Schedule** option under **Utilities** from the Shifts and Schedule page. The page appears as shown below:



Monthly Shift Schedule

User * 1663 PARTH PATEL

Attendance Period February 2017

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1 GS	2 GS	3 GS	4 GS
5 GS WO	6 GS	7 GS	8 GS	9 GS	10 GS	11 GS
12 GS WO	13 GS	14 GS	15 GS	16 GS	17 GS	18 GS
19 GS WO	20 GS	21 GS	22 GS	23 GS	24 GS	25 GS
26 GS WO	27 GS	28 GS	1	2	3	4
5	6	7	8	9	10	11

PH - Public Holiday WO - Week Off WO - Week Off & Public Holiday On Same Day

User: Select the user from the picklist whose shift schedule is to be viewed.

Attendance Period - Select the month and year for which the schedule is to be viewed.

The shift details for the selected user is shown in the grid as shown above. The week-off is shown by green colour. The other colour codes are mentioned below the grid.



The Shift Schedule is assigned to the user from **Shift and Schedules> Process> Monthly Schedule**.

Monthly Schedule

Shift Schedule generation for the month will create data for each day of the month for all users. Apart from the shift it will also mark weekly offs and holidays applicable to the users during the month. This process assigns shift for each day of the month as per the schedule group allotted to user. This process needs to be run at the end of the previous calendar month.

To use the Monthly Schedule Process, Select **Shifts and Schedule > Process > Monthly Schedule**. The page appears as shown below:

The screenshot shows the 'Monthly Schedule' process interface. At the top, there's a title bar 'Monthly Schedule' with a back arrow. Below it, the 'Month-Year' is set to 'May' and '2017'. There's a checkbox for 'Overwrite Existing Schedule'. Under 'Select Users', a dropdown menu is set to 'User Wise'. Below this, there are input fields for 'User ID' and 'Name', with a search icon. A table lists users with columns 'User ID' and 'Name'. The first row shows '1320' and 'SHRUTI SAGAR PATKI'. A 'Process' button is at the bottom.

User ID	Name
1320	SHRUTI SAGAR PATKI

Month-Year: Select the month and the year for which the process is to be run.

Overwrite Existing Schedule: Check the box to overwrite the shift schedule data already generated by an earlier process.

User Filter: Select the User from the drop down list. The options to filter the user are:

- **User Wise:** Enables administrator to randomly select users from the user Picklist window.
- **Select Group:** Enables the administrator to select all users belonging to a particular group.
- **All:** Enables administrator to select all active users in the database.

Select the user and Click on the **Process** button to start the process of Schedule Generation. The system starts processing the data and displays the process completion status.

Example: Suppose the current shift schedule for the user Aditi has GS shift as shown below.

Monthly Shift Schedule

User * 1687 Aditi Gupta

Attendance Period May 2017

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	1 GS	2 GS	3 GS	4 GS	5 GS	6 GS
7 GS WO	8 RS	9 GS	10 GS	11 GS	12 GS	13 GS
14 GS WO	15 GS	16 GS	17 GS	18 GS	19 GS	20 GS
21 GS WO	22 GS	23 GS	24 GS	25 GS	26 GS	27 GS
28 GS WO	29 GS	30 GS	31 GS	1	2	3
4	5	6	7	8	9	10

PH - Public Holiday WO - Week Off WO - Week Off & Public Holiday On Same Day

Now the new schedule with NS shift is assigned to the user. So it must be processed again with “Overtime Existing Schedule” enabled.

Monthly Schedule

✓ Process Completed.

Month-Year May 2017

Overwrite Existing Schedule ☒

Select Users User Wise

User * ID Name

Search

User ID	Name
1687	Aditi Gupta

Process

After the successful process, the schedule will be updated as shown below:

Monthly Shift Schedule

User * 1687 Aditi Gupta

Attendance Period May 2017

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	1 NS PH	2 NS PH	3 NS	4 NS	5 NS	6 NS
7 NS WO	8 NS	9 NS	10 NS	11 NS	12 NS	13 NS
14 NS WO	15 NS	16 NS	17 NS	18 NS	19 NS	20 NS
21 NS WO	22 NS	23 NS	24 NS	25 NS	26 NS	27 NS
28 NS WO	29 NS	30 NS	31 NS	1	2	3
4	5	6	7	8	9	10

PH - Public Holiday WO - Week Off WO - Week Off & Public Holiday On Same Day

Shifts & Schedule Reports

These reports are available only with the Access Control or the Time and Attendance modules. Reports available under this option are as follows.

“Shifts”

“Schedule Groups”

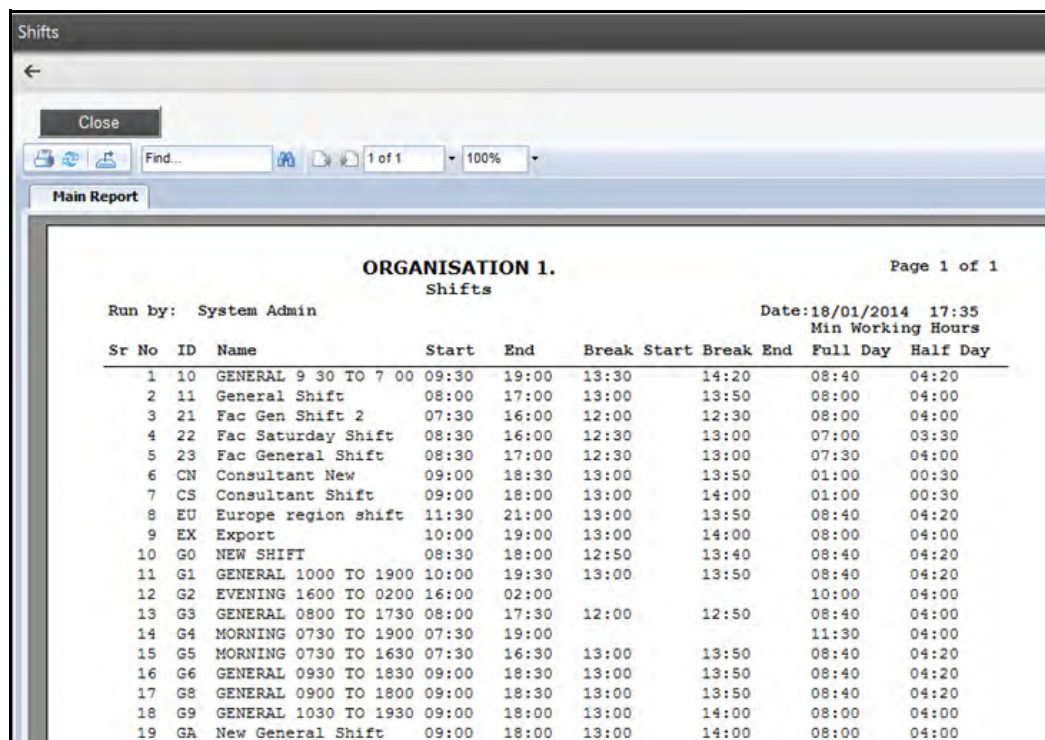
“Holiday Schedules”

“Shift Schedules”

“Week-Off Change”

Shifts

Generates a list of the shifts as defined in the system along with their configuration parameters as shown.

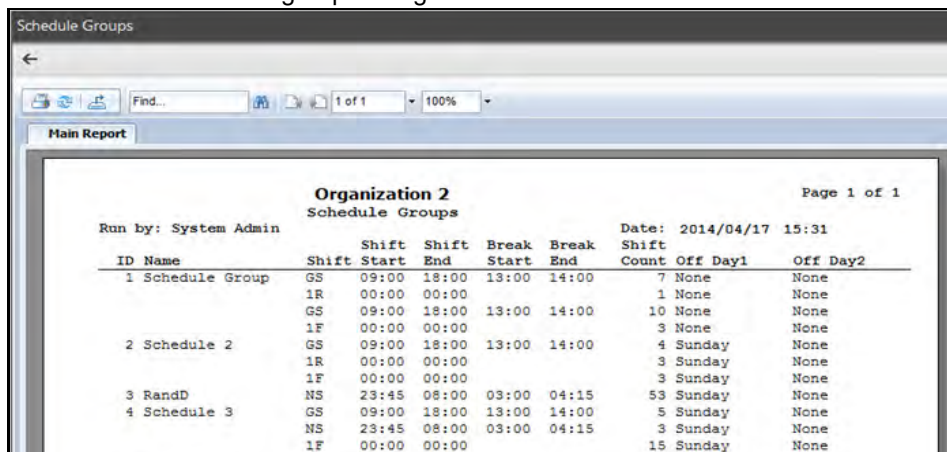


The screenshot shows a software window titled "Shifts" with a "Main Report" tab. The report is for "ORGANISATION 1. Shifts" and is "Page 1 of 1". It was run by "System Admin" on "Date: 18/01/2014 17:35". The table lists 19 shifts with columns for Sr No, ID, Name, Start, End, Break Start, Break End, Full Day, and Half Day.

Sr No	ID	Name	Start	End	Break Start	Break End	Full Day	Half Day
1	10	GENERAL 9 30 TO 7 00	09:30	19:00	13:30	14:20	08:40	04:20
2	11	General Shift	08:00	17:00	13:00	13:50	08:00	04:00
3	21	Fac Gen Shift 2	07:30	16:00	12:00	12:30	08:00	04:00
4	22	Fac Saturday Shift	08:30	16:00	12:30	13:00	07:00	03:30
5	23	Fac General Shift	08:30	17:00	12:30	13:00	07:30	04:00
6	CN	Consultant New	09:00	18:30	13:00	13:50	01:00	00:30
7	CS	Consultant Shift	09:00	18:00	13:00	14:00	01:00	00:30
8	EU	Europe region shift	11:30	21:00	13:00	13:50	08:40	04:20
9	EX	Export	10:00	19:00	13:00	14:00	08:00	04:00
10	G0	NEW SHIFT	08:30	18:00	12:50	13:40	08:40	04:20
11	G1	GENERAL 1000 TO 1900	10:00	19:30	13:00	13:50	08:40	04:20
12	G2	EVENING 1600 TO 0200	16:00	02:00			10:00	04:00
13	G3	GENERAL 0800 TO 1730	08:00	17:30	12:00	12:50	08:40	04:00
14	G4	MORNING 0730 TO 1900	07:30	19:00			11:30	04:00
15	G5	MORNING 0730 TO 1630	07:30	16:30	13:00	13:50	08:40	04:20
16	G6	GENERAL 0930 TO 1830	09:00	18:30	13:00	13:50	08:40	04:20
17	G8	GENERAL 0900 TO 1800	09:00	18:30	13:00	13:50	08:40	04:20
18	G9	GENERAL 1030 TO 1930	09:00	18:00	13:00	14:00	08:00	04:00
19	GA	New General Shift	09:00	18:00	13:00	14:00	08:00	04:00

Schedule Groups

Generates a list of the defined schedule groups along with the details of the member shifts as shown.



The screenshot shows a software window titled "Schedule Groups" with a "Main Report" tab. The report is for "Organization 2 Schedule Groups" and is "Page 1 of 1". It was run by "System Admin" on "Date: 2014/04/17 15:31". The table lists 4 schedule groups with columns for ID, Name, Shift, Shift Start, Shift End, Break Start, Break End, Shift Count, Off Day1, and Off Day2.

ID	Name	Shift	Shift Start	Shift End	Break Start	Break End	Shift Count	Off Day1	Off Day2
1	Schedule Group	GS	09:00	18:00	13:00	14:00	7	None	None
		1R	00:00	00:00			1	None	None
		GS	09:00	18:00	13:00	14:00	10	None	None
		1F	00:00	00:00			3	None	None
2	Schedule 2	GS	09:00	18:00	13:00	14:00	4	Sunday	None
		1R	00:00	00:00			3	Sunday	None
		1F	00:00	00:00			3	Sunday	None
3	RandD	NS	23:45	08:00	03:00	04:15	53	Sunday	None
4	Schedule 3	GS	09:00	18:00	13:00	14:00	5	Sunday	None
		1F	23:45	08:00	03:00	04:15	3	Sunday	None
		1F	00:00	00:00			15	Sunday	None

Holiday Schedules

Select Schedule as: **Holiday Schedule wise / All** and generates a listing of holidays as defined in the selected schedule as shown.

Sr No	Start Date	End Date	Holiday
1	14/01/2013	15/01/2013	MAKAR SANKRANTI
2	27/03/2013	27/03/2013	Dhulati
3	15/08/2013	15/08/2013	Independence Day
4	19/08/2013	19/08/2013	24TH 2ND SAT WORKING
5	20/08/2013	20/08/2013	Raksha Bandhan
6	28/08/2013	28/08/2013	Janmashtami
7	18/09/2013	18/09/2013	Ganesha Visarjan
8	06/11/2013	06/11/2013	Diwali (New Year)
9	04/11/2013	04/11/2013	Diwali (Bhaiduj)
10	05/11/2013	05/11/2013	Diwali (Bhaiduj)
11	13/08/2011	13/08/2011	Rakshabandhan
12	15/08/2011	15/08/2011	Independence Day
13	06/10/2011	06/10/2011	Dasera
14	26/10/2011	28/10/2011	Diwali
15	14/01/2010	14/01/2010	Makarsankranti
16	26/01/2010	26/01/2010	Republic Day
17	01/03/2010	01/03/2010	Holi
18	14/01/2012	15/01/2012	Makarsankranti
19	08/03/2012	08/03/2012	Holi
20	26/01/2012	26/01/2012	Republic Day
21	02/08/2012	02/08/2012	Raksha Bandhan
22	15/08/2012	15/08/2012	Independence Day

Shift Schedules

Select Month and Year from **For Month-Year**. **Select Users** either User-wise/Group-wise/All and Generate Report for either **All/Active/Inactive** users.

Shift Schedule

For Month-Year: October 2019

User Selection

Select Users: User Wise

User: ID Name

Generate Report For: All Users

Generate Report





Generates a listing of shift schedule for the selected user for the selected month-year as shown.

Shift Schedule

★ ? ×

←

Back

  Find...   1 of 60 100%

Main Report

ORGANISATION 1.

Shift Schedule For JANUARY-2013

Run by: System Admin

Date: 18/01/2014 17:41

Page 1 of 60

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
1 - SALIM ANSARI	23	23	23	23	22	22	23	23	23	23	23	22	22	23	23	23	23	23	22	22	23	23	23	23	23	23	22	22	23	23	23	23
	WO					WO							WO	PH	WO					WO						PH						

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
10 - RAJENDRA GOSWAMI	23	23	23	23	22	22	23	23	23	23	23	22	22	23	23	23	23	23	22	22	23	23	23	23	23	23	22	22	23	23	23	23
	WO					WO							WO	PH	WO					WO						PH						

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1001 - ANKITKUMAR SOHLIYA	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS
						WO							WO	PH	WO					WO						WO	WO				

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1002 - MEGHA H SHUKLA	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS
						WO							WO	PH	WO					WO						WO	WO				

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1003 - UMESH M TALANFURI	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS
						WO							WO	PH	WO					WO						WO	WO				

Week-Off Change

Generates the report with week-off change details of the selected or all users, group by Organization, Branch, Department, Section, etc. as shown.

Week-Off Change																				
←																				
Back																				
Find... 1 of 1 100%																				
Main Report																				
<div> <div>ORGANISATION 1.</div> <div>Organization-Wise Week-Off Change from 28/07/2014 To 28/07/2014</div> <div>Run by: System Admin</div> <div>Date: 28/07/2014 09:25</div> <div>Page 1 of 1</div> </div> <table> <tr> <th>User ID</th><th>Name</th><th>Department</th><th>Old Date</th><th>New Date</th><th>Changed By</th><th>Change Date</th></tr> <tr> <td>92</td><td>SMITA BARIA</td><td>HR & ADMIN</td><td>28/07/2014</td><td>29/07/2014</td><td>System Admin</td><td>28/07/2014</td></tr> </table>							User ID	Name	Department	Old Date	New Date	Changed By	Change Date	92	SMITA BARIA	HR & ADMIN	28/07/2014	29/07/2014	System Admin	28/07/2014
User ID	Name	Department	Old Date	New Date	Changed By	Change Date														
92	SMITA BARIA	HR & ADMIN	28/07/2014	29/07/2014	System Admin	28/07/2014														

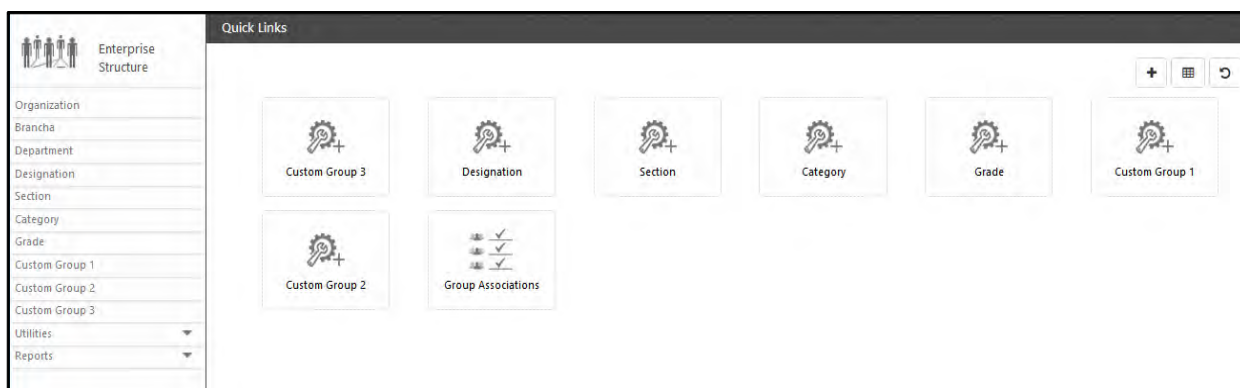
Every business, irrespective of size, needs to be structurally organized for smooth and efficient operability. This structural organization is effective at two levels, at functional level and personnel level. COSEC allows an enterprise to identify distinct functional and personnel units as groups which can be configured independently by system administrators.

To access the **Enterprise Structure** module with COSEC Web Application, click on **Enterprise Structure**






on the Module selection page.

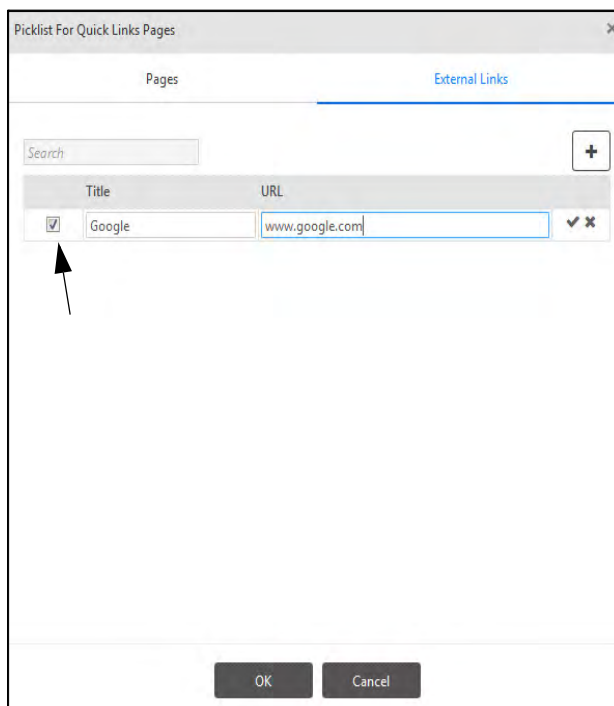
The **Enterprise Structure** page appears on the screen as shown below.



The page displays a menu and **Quick Links** to go to the required page in just one click. Quick Links are shortcuts to reach to a specific page easily. It also contains following three buttons:

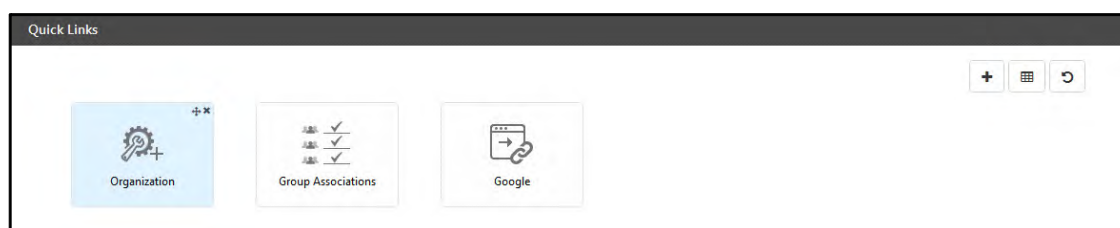
- **Add Quick Link:** Click  button to add a quick link. A picklist for Quick Link pages appears for selecting the page or External Link for which the quick link is to be created. Maximum **20** quick links can be added.
- For Adding **Pages** in Quick Link, Select the Pages and click on OK
- For Adding **External Links**, Select External Link tab, click on  button to add new external link.



- Configure the **Title** and **URL** of the external link under the respective fields. click on checkbox to get the configured link on quick link screen as shown below. To save the configuration click on .



	Title	URL	
<input checked="" type="checkbox"/>	Google	www.google.com	<input checked="" type="checkbox"/>

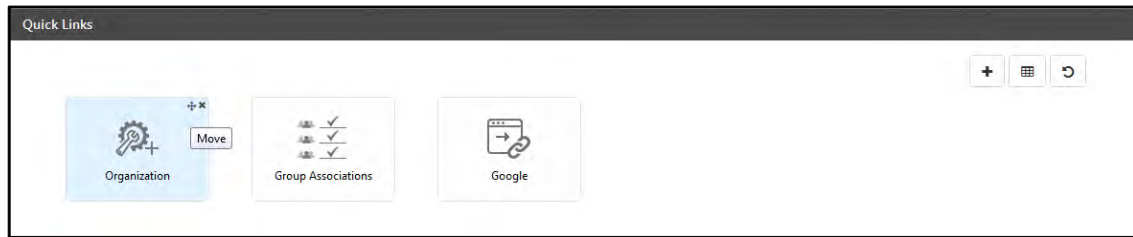
- To edit the saved configuration, click on .
- Click on OK to save the link configuration on Quick Link screen. The external link will be displayed as shown below:



- **Select Layout:** Click  button to select a layout for the quick links. You can select 5x4 or 4x5 layout to manage the quick links.
- **Reset Quick Links:** Click  button to reset the quick links to the default quick links.

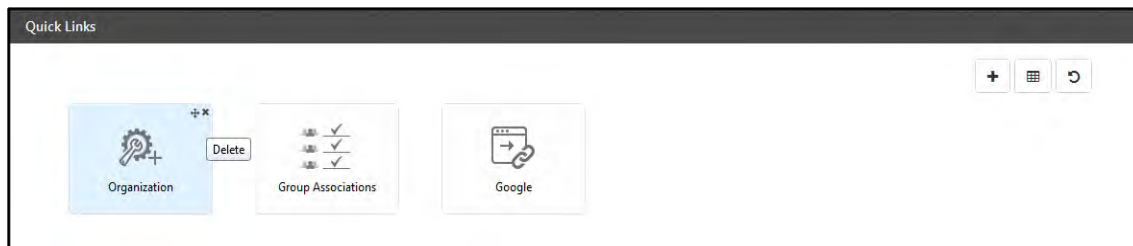
Move the Link

To move the link from one place to another, hover on the link on top right corner and click on “Move” icon as shown below. Then drag the quick link to the desired place. It will be placed at the desired location on the quick links page.



Delete the Link

To delete a particular link, hover on the link on top right corner and click on “Delete” icon as shown below.



Enterprise Groups

The following groups are defined under the *Enterprise Structure* module in COSEC:

- **Organization**
- **Branch**
- **Department**
- **Designation**
- **Section**
- **Category**
- **Grade**
- **Custom Group1**
- **Custom Group2**
- **Custom Group3**



All enterprise groups in COSEC are predefined and the user cannot define any new group types. The user can however, rename group labels as per business requirement. To know more, refer to [“Renaming Groups”](#).

An **organization** is a business unit that comprises of an individual or a collaborating group of people working towards a common commercial goal. Therefore, a business enterprise may have the need to identify multiple organizations. COSEC allows the creation of upto 9,99,999 organizations in its database. COSEC identifies organization as the broadest structural unit in a business environment.

An organization that operates across different geographical locations may be sub-divided structurally into branches. A **branch** may be further categorized into smaller functional units called **departments** which handle a specific aspect of the business, such as development, research, quality control, logistics and so on. Departments may have further sub-divisions in the form of **sections** which handle specific responsibilities or activities under the scope of their respective departments.

Hence, in terms of structure and function, an enterprise may be identified into the following hierarchical groups:

- Organization
- Branch
- Department
- Section

In terms of personnel structure, an enterprise may be classified into the following groups based on criteria such as function, responsibility, skill-sets, expertise, position, benefits, organizational rights and so on. These groups are:


- Category
- Grade
- Designation

Let us consider an example of how an Enterprise Structure can be classified into Enterprise Groups:

- Say, an enterprise operates two business organizations, namely *Company-1* and *Company-2*.
- *Company-1* operates across five branches world-wide, *Company-1- New York*, *Company-1- London*, *Company-1- Beijing*, *Company-1-Tokyo* and *Company-1- New Delhi*.
- The New Delhi branch runs two departments - *Sales* and *Customer-Support*.
- The Sales department for Company-1 further operates two sections or divisions, each for a product, say, *Product-1* and *Product-2*.
- For every product, employees are hired under two categories - *Contract-based* and *Permanent*.
- All the customer-support staff are classified either into *technical-support* or *commercial-support* teams, each team comprising *team managers*, *team leaders*, *engineers* and *executives*.

To know how to configure the structure of an enterprise, read the next section [“Configuring Groups”](#).

Enterprise Structure Dashboard

To view the **Enterprise Structure** Dashboard, select the Dashboard button  on the **Enterprise Structure** page. The Dashboard displays the basic information on *Enterprise Structure* under the following categories:

Dashboard																																													
<table><tr><th colspan="2">Structure Summary</th></tr><tr><td>Organization</td><td>75</td></tr><tr><td>Brancha</td><td>77</td></tr><tr><td>Department</td><td>58</td></tr><tr><td>Designation</td><td>58</td></tr><tr><td>Section</td><td>62</td></tr><tr><td>Category</td><td>52</td></tr><tr><td>Grade</td><td>47</td></tr><tr><td>Custom Group 1</td><td>12</td></tr><tr><td>Custom Group 2</td><td>11</td></tr><tr><td>Custom Group 3</td><td>7</td></tr></table>	Structure Summary		Organization	75	Brancha	77	Department	58	Designation	58	Section	62	Category	52	Grade	47	Custom Group 1	12	Custom Group 2	11	Custom Group 3	7	<table><tr><th colspan="2">Default Group Summary</th></tr><tr><td>Default Organization</td><td>1</td></tr><tr><td>Default Brancha</td><td>1</td></tr><tr><td>Default Department</td><td>1</td></tr><tr><td>Default Designation</td><td>1</td></tr><tr><td>Default Section</td><td>1</td></tr><tr><td>Default Category</td><td>1</td></tr><tr><td>Default Grade</td><td>1</td></tr><tr><td>Default Custom Group 1</td><td>1</td></tr><tr><td>Default Custom Group 2</td><td>1</td></tr><tr><td>Default Custom Group 3</td><td>1</td></tr></table>	Default Group Summary		Default Organization	1	Default Brancha	1	Default Department	1	Default Designation	1	Default Section	1	Default Category	1	Default Grade	1	Default Custom Group 1	1	Default Custom Group 2	1	Default Custom Group 3	1
Structure Summary																																													
Organization	75																																												
Brancha	77																																												
Department	58																																												
Designation	58																																												
Section	62																																												
Category	52																																												
Grade	47																																												
Custom Group 1	12																																												
Custom Group 2	11																																												
Custom Group 3	7																																												
Default Group Summary																																													
Default Organization	1																																												
Default Brancha	1																																												
Default Department	1																																												
Default Designation	1																																												
Default Section	1																																												
Default Category	1																																												
Default Grade	1																																												
Default Custom Group 1	1																																												
Default Custom Group 2	1																																												
Default Custom Group 3	1																																												
<table><tr><th colspan="2">Group Associations</th></tr><tr><td>Total Parameters</td><td>41</td></tr><tr><td>Associated Parameters</td><td>34</td></tr></table>		Group Associations		Total Parameters	41	Associated Parameters	34																																						
Group Associations																																													
Total Parameters	41																																												
Associated Parameters	34																																												

Structure Summary


- This section displays the total number for each enterprise group configured on the system.

Default Group Summary

- This section displays the group ID for default groups configured for each enterprise group type.

Group Associations

- Total Parameters - Total number of parameters available for group association.
- Associated Parameters - Total number of parameters actually associated with groups.

For more information on the above Dashboard options, click the respective information links on the Dashboard. The Latest values on Dashboard are updated on clicking the Refresh  button.

Configuring Groups

The COSEC **Enterprise Structure** module has been specially designed to allow flexibility for policy-makers in operating COSEC across all business units based on operational convenience. COSEC enables the HR administrator to configure each Enterprise group individually and assign users to them.

Users added to a particular enterprise group will inherit the configuration of this group automatically. Hence, it becomes easier to associate specific group properties with selected users.

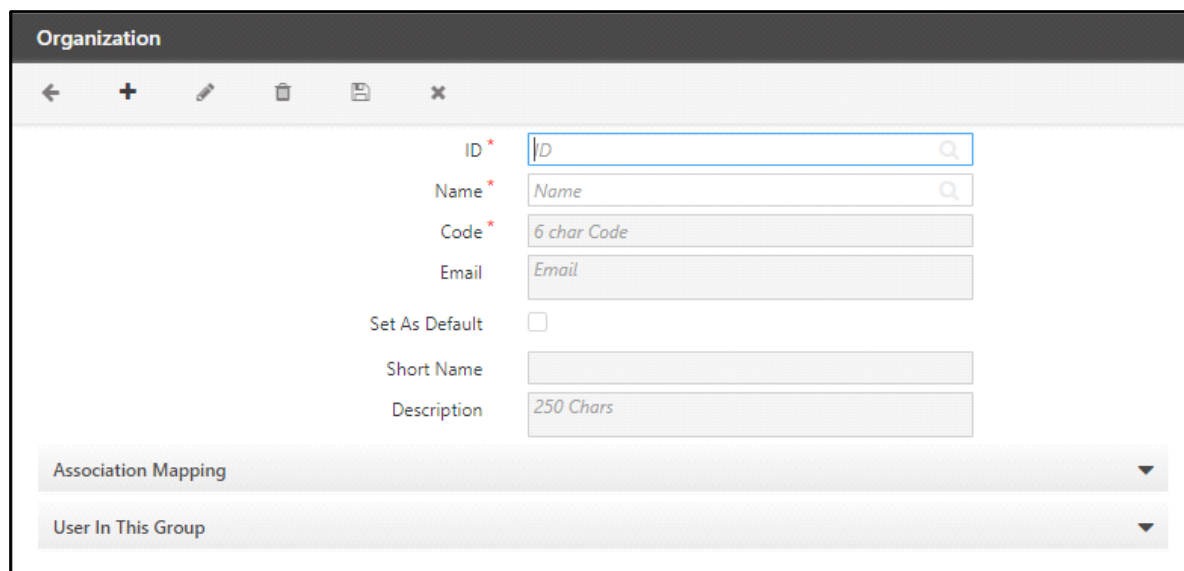
Following are the enterprise groups:

- *“Organization”*
- *“Branch”*
- *“Department”*
- *“Designation”*
- *“Section”*
- *“Category”*
- *“Grade”*

Organization

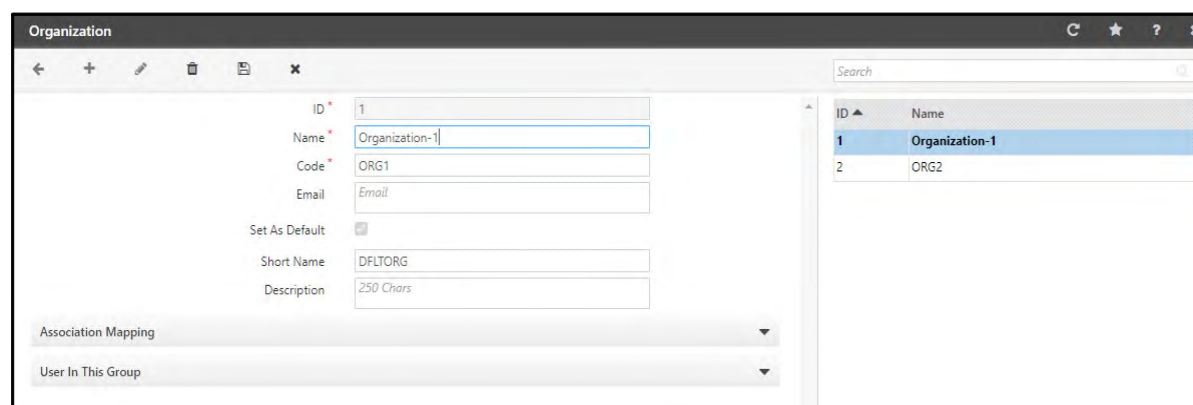
Organization tab enables to create and manage organizations. It helps to group users in a particular organization and assign policies accordingly. You can add 999999 organizations.

To view organization tab, click **Enterprise Structure > Organization** and the following screen appears.



The page displays configurations on the left side and to the right is the grid containing created organizations.

To configure an organization click the **New** button and the following screen appears.



ID	Name
1	Organization-1
2	ORG2

Enter the following details:

- **ID:** The ID field auto-generates a new ID for every new group defined on the system.
- **Name:** Specify the group name to be created. The supported values are: **A-Z, a-z, 0-9, () , [], _ (underscore), - (Hyphen), . (full Stop), /, &, , (comma), @, ' (single quote), [space]**. The invalid characters for Multi-language character set are Set3 which includes ` ~ # % ^ * = + { } | \ : ; " < > ?
- **Email:** Enter the Email address of the group.

- **Code:** Enter a max 6 character code for the new group. For example, the code for “Research and Development” can be “RND” or for “Vice President” can be “VP”.
- **Set As Default:** Enable to set the organization to be created as the default group.



Both default groups and groups that are already in use cannot be deleted from the system. In case all groups configured on the system are deleted, the system will automatically apply the settings of the default group on the concerned users.

- **Short Name:** Provide short name for the organization to be created.
- **Description:** Enter description for the organization. It can be maximum of 250 characters.

Association Mapping

The parameters under Association Mapping panel are known as Associated parameters as they are linked with the organization from the “[Group Associations](#)” page of **Utilities** tab. Only the enabled parameters become available for configuration in the **Association Mapping** panel of Organization page as shown below.



A single associated parameter can be linked with only one group, i.e. if a parameter is enabled for one group from the Group Associations page, then it becomes disabled for other enterprise groups.

PIN Authentication For Door Access will be only displayed here, when Allow Door Access through API is enabled in Group Association> ESS> Allow Door Access Through API.

Reason For Punch From Unassigned Location will only be displayed when Location Mandatory For Punch is enabled from Group Association> ESS> Location Mandatory For Punch as well as Location Mandatory For Punch = None/Any Location.

If you have enabled Job Costing, you need to add the new Job, refer “[Job Costing](#)” for details.

If you have enabled Capture Photo, refer “[ESS](#)” for details.

Select the organization from the grid to be edited and click **Edit**.

- In the **Association Mapping** panel, configure the associated parameters as required.

- Click **Save**  .

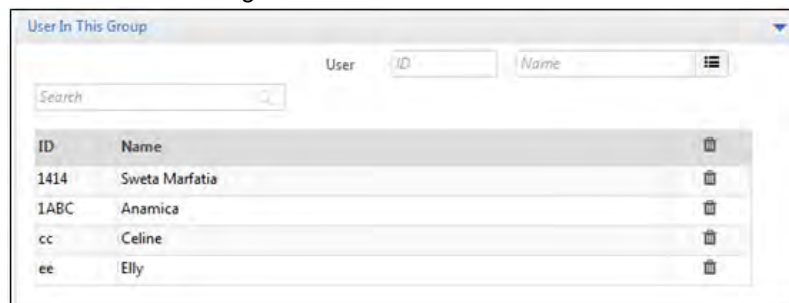






If Association Mapping is changed from one Enterprise Group Type to other (eg. From Organization to Branch), all current default jobs records (Assignment End Date \geq Current Date) will be deleted. Previous default job records (Assignment End Date $<$ Current Date) will still be retained.

If Enterprise Group is deleted then all job assignment records current as well as previous will be deleted.

User In This Group

This section enables to add users to the organization to be created.



ID	Name	
1414	Sweta Marfatia	
IABC	Anamica	
cc	Celine	
ee	Elly	

- Select users to be added using the picklist button. The selected users get displayed in the grid as shown above. One can also delete the selected users from the list or search a particular user using the **Search** field.





The picklist options that appear will be as per the rights assigned to the SA. For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#).

Once a user is deleted from a group, it gets restored to the default group and inherits all configurations assigned to the default group.

Click **Save** button and the created organization gets displayed in the grid on the right hand side.

You can edit or delete the organization if required. To do so,

- Click on the desired organization from the grind on the right hand side.
- To edit, click **Edit**  .
- To delete, click **Delete**  .



Only those organizations can be deleted that are not assigned to any user/worker/visitor.

Branch

Branch tab enables to create and manage branches. It helps to group users in a particular branch and assign policies accordingly. You can add 999999 branches.

To view branch tab, go to **Enterprise Structure > Branch** and the following screen appears.

The screenshot shows the 'Branch' configuration window. On the left, there are input fields for 'ID', 'Name', 'Code', 'Set As Default' (checkbox), 'Short Name', and 'Description'. Below these is a 'User In This Group' dropdown menu. On the right, there is a table with columns 'ID' and 'Name'. The table contains one entry: '1' with 'Branch-1'.

The page displays configurations on the left side and to the right is the grid containing created branches.

To configure a branch click the **New** button and the following screen appears.

The screenshot shows the 'Branch' configuration window with the following fields filled out: 'ID' is '10', 'Name' is 'Research And Development', 'Code' is 'RND', 'Set As Default' is checked, 'Short Name' is 'Research And De', and 'Description' is '250 chairs'. The 'User In This Group' dropdown menu is open, showing a table with columns 'User', 'ID', and 'Name'. The table contains two entries: '1414' with 'Sweta Marfatia' and 'rutu' with 'rutu'.

Provide the following details:

- **ID:** The ID field auto-generates a new ID for every new group defined on the system.
- **Name:** Specify the branch name to be created. The supported values are: **A-Z, a-z, 0-9, () , [], _ (underscore), - (Hyphen), . (full Stop), /, &, , (comma), @, ' (single quote), [space]**. The invalid characters for Multi-language character set are Set3 which includes ` ~ # % ^ * = + { } | \ : ; " < > ?
- **Code:** Enter a 6 character code for the new branch. For example, the code for "Research and Development" can be "RND" or for "Vice President" can be "VP".
- **Set As Default:** Enable to set the branch to be created as the default branch.



Both default branch and branches that are already in use cannot be deleted from the system. In case all groups configured on the system are deleted, the system will automatically apply the settings of the default group on the concerned users.

- **Short Name:** Provide short name for the branch to be created.
- **Description:** Enter description for the branch. It can be maximum of 250 characters.

User In This Group

This section enables to add users to the branch to be created.

- Select users to be added using the picklist button. The selected users get displayed in the grid as shown above. One can also delete the selected users from the list or search a particular user using the **Search** field.





The picklist options that appear will be as per the rights assigned to the SA. For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#).

Once a user is deleted from a branch, it gets restored to the default group and inherits all configurations assigned to the default group.

- Click **Save** button and the created branch gets displayed in the grid on the right hand side.

You can edit or delete the branch if required. To do so,

- Click on the desired branch from the grid on the right hand side.
- To edit, click **Edit** .
- To delete, click **Delete** .



Only those branches can be deleted that are not assigned to any user/worker/visitor.

Now, one can also associate parameters to the created branch. To do so [See “Association Mapping” on page 1241.](#)

Association Mapping

The parameters under Association Mapping panel are known as Associated parameters as they are linked with the branch from the **Group Associations** page of **Utilities** tab. Only the enabled parameters become available for configuration in the **Association Mapping** panel of Branch page as shown below.



A single associated parameter can be linked with only one group, i.e. if a parameter is enabled for one group from the Group Associations page, then it becomes disabled for other enterprise groups.

- Select the branch from the grid to be edited and click **Edit**.
- In the **Association Mapping panel**, configure the associated parameters as required. E.g. in the above screen, Enable Account has been enabled for all employees of the “Research And Development” branch.
- Click **Save**.



If Association Mapping is changed from one Enterprise Group Type to other (eg. From Organization to Branch), all current default jobs records (Assignment End Date \geq Current Date) will be deleted. Previous default job records (Assignment End Date $<$ Current Date) will still be retained.



If Enterprise Group is deleted then all job assignment records current as well as previous will be deleted.

Department

Department tab enables to create and manage department. It helps to group users in a particular department and assign policies accordingly. You can add 999999 departments.

To view Department tab, go to **Enterprise Structure > Department** and the following screen appears.

ID	Name
1	Marketing
2	Sales
3	Quality Control

The page displays configurations on the left side and to the right is the grid containing created departments.

To configure a department click the **New** button and the following screen appears.

ID	Name
1	Marketing
2	Sales
3	Quality Control

Provide the following details:

- **ID:** The ID field auto-generates a new ID for every new group defined on the system.
- **Name:** Specify the department name to be created. The supported values are: **A-Z, a-z, 0-9, () , [] , _ (underscore), - (Hyphen), . (full Stop), /, &, , (comma), @, ' (single quote), [space]**. The invalid characters for Multi-language character set are Set3 which includes ` ~ # % ^ * = + { } | \ : ; " < > ?
- **Code:** Enter a 6 character code for the new department. For example, the code for “Marketing” can be “MKT”.

- **Set As Default:** Enable to set the department to be created as the default department.



Both default department and departments that are already in use cannot be deleted from the system. In case all groups configured on the system are deleted, the system will automatically apply the settings of the default group on the concerned users.

- **Short Name:** Provide short name for the department to be created.
- **Description:** Enter description for the department. It can be maximum of 250 characters.
- **Color Code** - One can assign a color code to each department using color picklist as shown above.

User In This Group

This section enables to add users to the department to be created.

- Select users to be added using the picklist button. The selected users get displayed in the grid as shown above. One can also delete the selected users from the list or search a particular user using the **Search** field.





The picklist options that appear will be as per the rights assigned to the SA. For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#).

Once a user is deleted from a department, it gets restored to the default group and inherits all configurations assigned to the default group.

- Click **Save** button and the created department gets displayed in the grid on the right hand side.

You can edit or delete the department if required. To do so,

- Click on the desired department from the grid on the right hand side.
- To edit, click **Edit** .
- To delete, click **Delete** .



Only those departments can be deleted that are not assigned to any user/worker/visitor.

Now, one can also associate parameters to the created department. To do so [See “Association Mapping” on page 1245.](#)

Association Mapping

The parameters under Association Mapping panel are known as Associated parameters as they are linked with the department from the **Group Associations** page of **Utilities** tab. Only the enabled parameters become available for configuration in the **Association Mapping** panel of department page as shown below.

The screenshot displays the 'Department' configuration window. The 'Association Mapping' panel is active, showing various fields for configuration. The 'Access Details' section includes 'Access Validity' (checked) and 'Access Validity Date'. A list on the right shows the following departments:

ID	Name
1	Marketing
2	Sales
3	Quality Control



A single associated parameter can be linked with only one group, i.e. if a parameter is enabled for one group from the Group Associations page, then it becomes disabled for other enterprise groups.

- Select the department from the grid to be edited and click **Edit**.
- In the **Association Mapping panel**, configure the associated parameters as required. E.g. in the above screen, Access Validity has been enabled for all employees of the “Marketing” department.
- Click **Save**.



If Association Mapping is changed from one Enterprise Group Type to other (eg. From Organization to Branch), all current default jobs records (Assignment End Date \geq Current Date) will be deleted. Previous default job records (Assignment End Date $<$ Current Date) will still be retained.



If Enterprise Group is deleted then all job assignment records current as well as previous will be deleted.

Designation

Designation tab enables to create and manage designations. It helps to group users in a particular designation and assign policies accordingly. You can add 999999 designations.

To view designation tab, go to **Enterprise Structure > Designation** and the following screen appears.

ID	Name
1	Engineer
2	Team Leader
3	Business Manager

The page displays configurations on the left side and to the right is the grid containing created designations.

To configure a designation click the **New** button and the following screen appears.

ID	Name
1	Engineer
2	Team Leader
3	Business Manager

ID	Name
rutu	rutu
V@ishmi	vaishmi thakor

Provide the following details:

- **ID:** The ID field auto-generates a new ID for every new group defined on the system.
- **Name:** Specify the designation name to be created. The supported values are: **A-Z, a-z, 0-9, () , [] , _ (underscore), - (Hyphen), . (full Stop), /, &, , (comma), @, ' (single quote), [space]**. The invalid characters for Multi-language character set are Set3 which includes ` ~ # % ^ * = + { } | \ : ; " < > ?
- **Code:** Enter a 6 character code for the new designation. For example, the code for “Engineer” can be “EG”.
- **Set As Default:** Enable to set the designation to be created as the default designation.



Both default designation and designations that are already in use cannot be deleted from the system. In case all groups configured on the system are deleted, the system will automatically apply the settings of the default group on the concerned users.

- **Short Name:** Provide short name for the designation to be created.
- **Description:** Enter description for the designation. It can be maximum of 250 characters.

User In This Group

This section enables to add users to the designation to be created.

- Select users to be added using the picklist button. The selected users get displayed in the grid as shown above. One can also delete the selected users from the list or search a particular user using the **Search** field.





The picklist options that appear will be as per the rights assigned to the SA. For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#).

Once a user is deleted from a designation, it gets restored to the default group and inherits all configurations assigned to the default group.

- Click **Save** and the created designation gets displayed in the grid on the right hand side.

You can edit or delete the designation if required. To do so,

- Click on the desired designation from the grid on the right hand side.
- To edit, click **Edit** .
- To delete, click **Delete** .



Only those designations can be deleted that are not assigned to any user/worker/visitor.

Now, one can also associate parameters to the created designation. To do so [See “Association Mapping” on page 1247.](#)

Association Mapping

The parameters under Association Mapping panel are known as Associated parameters as they are linked with the designation from the **Group Associations** page of **Utilities** tab. Only the enabled parameters become available for configuration in the **Association Mapping** panel of designation page as shown below.

The screenshot displays the 'Designation' form. The main form fields are: ID (1), Name (Engineer), Code (EG), Set As Default (checked), Short Name (Engineer), Description (250 chars), Wage Level (LVL1), and Wage Level-1 (Wage Level-1). Below these is the 'Association Mapping' section, which includes 'Attendance' and 'Enable Attendance Calculation' (checked). On the right side, there is a list of designations with columns 'ID' and 'Name':

ID	Name
1	Engineer
2	Team Leader
3	Business Manager



A single associated parameter can be linked with only one group, i.e. if a parameter is enabled for one group from the Group Associations page, then it becomes disabled for other enterprise groups.

- Select the designation from the grid to be edited and click **Edit**.
- In the **Association Mapping panel**, configure the associated parameters as required. E.g. in the above screen, Enable Attendance Calculation has been enabled for all employees of the “Engineer” designation.
- Click **Save**.



If Association Mapping is changed from one Enterprise Group Type to other (eg. From Organization to Branch), all current default jobs records (Assignment End Date \geq Current Date) will be deleted. Previous default job records (Assignment End Date $<$ Current Date) will still be retained.



If Enterprise Group is deleted then all job assignment records current as well as previous will be deleted.

Section

Section tab enables to create and manage sections. It helps to group users in a particular section and assign policies accordingly. You can add 999999 sections.

To view Section tab, go to **Enterprise Structure > Section** and the following screen appears.

ID	Name
1	SAMAS Writers
2	COSEC Writers

The page displays configurations on the left side and to the right is the grid containing a list of created sections.

To configure a section, click the **New** button and the following screen appears.

ID	Name
1414	Sweta Marfatia
Rosy	Rosy

Provide the following details:

- **ID:** The ID field auto-generates a new ID for every new group defined on the system.
- **Name:** Specify the section name to be created. The supported values are: **A-Z, a-z, 0-9, () , [] , _ (underscore), - (Hyphen), . (full Stop), /, &, , (comma), @, ' (single quote), [space]**. The invalid characters for Multi-language character set are Set3 which includes ` ~ # % ^ * = + { } | \ : ; " ' < > ?
- **Code:** Enter a 6 character code for the new section. For example, the code for “Engineer” can be “EG”.
- **Set As Default:** Enable to set the section to be created as the default section.



Both default section and sections that are already in use cannot be deleted from the system. In case all groups configured on the system are deleted, the system will automatically apply the settings of the default group on the concerned users.

- **Short Name:** Provide short name for the section to be created.
- **Description:** Enter description for the section. It can be maximum of 250 characters.

User In This Group

This panel enables to add users to the section to be created.

- Select users to be added using the picklist button. The selected users get displayed in the grid as shown above. One can also delete the selected users from the list or search a particular user using the **Search** field.





The picklist options that appear will be as per the rights assigned to the SA. For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#).

Once a user is deleted from a section, it gets restored to the default group and inherits all configurations assigned to the default group.

- Click **Save** and the created section gets displayed in the grid on the right hand side.

You can edit or delete the section if required. To do so,

- Click on the desired section from the grid on the right hand side.
- To edit, click **Edit** .
- To delete, click **Delete** .



Only those sections can be deleted that are not assigned to any user/worker/visitor.

Now, one can also associate parameters to the created section. To do so [See “Association Mapping” on page 1250.](#)

Association Mapping

The parameters under Association Mapping panel are known as Associated parameters as they are linked with the section from the **Group Associations** page of **Utilities** tab. Only the enabled parameters become available for configuration in the **Association Mapping** panel of section page as shown below.



A single associated parameter can be linked with only one group, i.e. if a parameter is enabled for one group from the Group Associations page, then it becomes disabled for other enterprise groups.

- Select the section from the grid to be edited and click **Edit**.
- In the **Association Mapping** panel, configure the associated parameters as required. E.g. in the above screen, Enable Attendance Calculation has been enabled for all employees of the “Engineer” section.
- Click **Save**.



If Association Mapping is changed from one Enterprise Group Type to other (eg. From Organization to Branch), all current default jobs records (Assignment End Date \geq Current Date) will be deleted. Previous default job records (Assignment End Date $<$ Current Date) will still be retained.

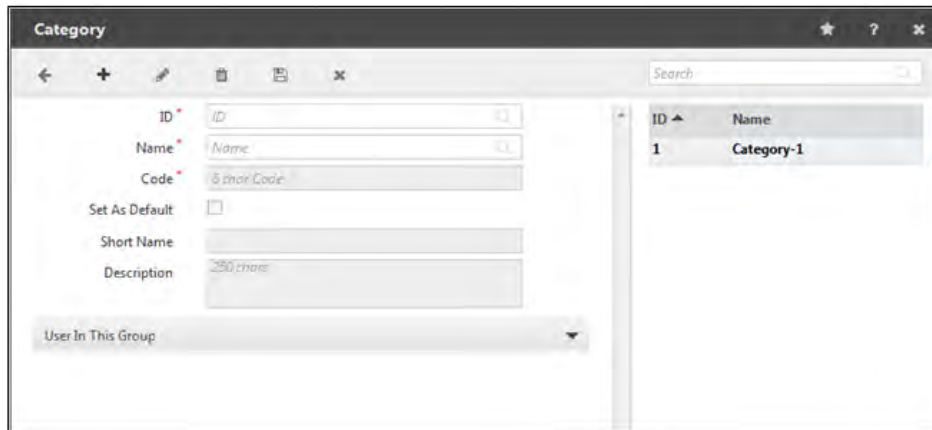


If Enterprise Group is deleted then all job assignment records current as well as previous will be deleted.

Category

Category tab enables to create and manage categories. It helps to group users in a particular category and assign policies accordingly. You can add 999999 categories.

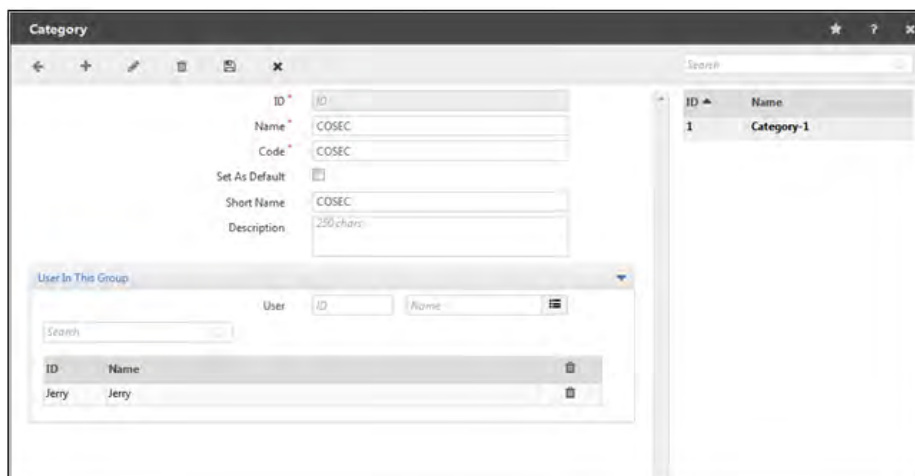
To view Category tab, go to **Enterprise Structure > Category** and the following screen appears.



ID	Name
1	Category-1

The page displays configurations on the left side and to the right is the grid containing a list of created categories.

To configure a new category, click the **New** button and the following screen appears.



ID	Name
1	Category-1

ID	Name
Jerry	Jerry

Provide the following details:

- **ID:** The ID field auto-generates a new ID for every new group defined on the system.
- **Name:** Specify the category name to be created. The supported values are: **A-Z, a-z, 0-9, () , [], _ (underscore), - (Hyphen), . (full Stop), /, &, , (comma), @, ' (single quote), [space]**. The invalid characters for Multi-language character set are Set3 which includes ` ~ # % ^ * = + { } | \ : ; " < > ?
- **Code:** Enter a 6 character code for the new category.
- **Set As Default:** Enable to set the category to be created as the default category.



Both default category and categories that are already in use cannot be deleted from the system. In case all categories configured on the system are deleted, the system will automatically apply the settings of the default category on the concerned users.

- **Short Name:** Provide short name for the category to be created.
- **Description:** Enter description for the category. It can be maximum of 250 characters.

User In This Group

This panel enables to add users to the category to be created.

- Select users to be added using the picklist button. The selected users get displayed in the grid as shown above. One can also delete the selected users from the list or search a particular user using the **Search** field.





The picklist options that appear will be as per the rights assigned to the SA. For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#).

Once a user is deleted from a category, it gets restored to the default category and inherits all configurations assigned to the default category.

- Click **Save** and the created category gets displayed in the grid on the right hand side.

You can edit or delete the category if required. To do so,

- Click on the desired category from the grid on the right hand side.
- To edit, click **Edit** .
- To delete, click **Delete** .



Only those categories can be deleted that are not assigned to any user/worker/visitor.

Now, one can also associate parameters to the created category. To do so [See “Association Mapping” on page 1253.](#)

Association Mapping

The parameters under Association Mapping panel are known as Associated parameters as they are linked with the category from the **Group Associations** page of **Utilities** tab. Only the enabled parameters become available for configuration in the **Association Mapping** panel of category page as shown below.



A single associated parameter can be linked with only one group, i.e. if a parameter is enabled for one group from the Group Associations page, then it becomes disabled for other enterprise groups.

- Select the category from the grid to be edited and click **Edit**.
- In the **Association Mapping panel**, configure the associated parameters as required. E.g. in the above screen, Enable Account has been enabled for all employees of the “COSEC” category.
- Click **Save**.



If Association Mapping is changed from one Enterprise Group Type to other (eg. From Organization to Branch), all current default jobs records (Assignment End Date \geq Current Date) will be deleted. Previous default job records (Assignment End Date $<$ Current Date) will still be retained.



If Enterprise Group is deleted then all job assignment records current as well as previous will be deleted.

Grade

Grade tab enables to create and manage grades. It helps to group users in a particular grade and assign policies accordingly. You can add 999999 grades.

To view Grade tab, go to **Enterprise Structure > Grade** and the following screen appears.

The screenshot shows the 'Grade' configuration window. On the left, there are input fields for 'ID', 'Name', 'Code', 'Set As Default' (checkbox), 'Short Name', and 'Description'. Below these is a 'User In This Group' dropdown. On the right, a table displays the existing grades. The table has two columns: 'ID' and 'Name'. It contains one entry with ID '1' and Name 'Grade-1'.

The page displays configurations on the left side and to the right is the grid containing a list of created grades.

To configure a new grade, click the **New** button and the following screen appears.

This screenshot shows the 'Grade' configuration window with the 'User In This Group' dropdown menu expanded. The dropdown shows a search bar and a list of users with columns for 'ID' and 'Name'. The users listed are 'Jerry' and 'V@ishmi'. The main configuration fields on the left are filled with 'Grade 1' for Name and Short Name, and 'G1' for Code. The table on the right still shows the existing 'Grade-1' entry.

Provide the following details:

- **ID:** The ID field auto-generates a new ID for every new grade defined on the system.
- **Name:** Specify the grade name to be created. The supported values are: **A -Z, a-z, 0 - 9, () , [] , _ (underscore), - (Hyphen), . (full Stop), / , & , , (comma), @ , ' (single quote), [space]**. The invalid characters for Multi-language character set are Set3 which includes ` ~ # % ^ * = + { } | \ : ; " ' < > ?
- **Code:** Enter a 6 character code for the new grade.
- **Set As Default:** Enable to set the grade to be created as the default grade.



Both default grade and grades that are already in use cannot be deleted from the system. In case all grades configured on the system are deleted, the system will automatically apply the settings of the default grade on the concerned users.

- **Short Name:** Provide short name for the grade to be created.
- **Description:** Enter description for the grade. It can be maximum of 250 characters.

User In This Group

This panel enables to add users to the grade to be created.

- Select users to be added using the picklist button. The selected users get displayed in the grid as shown above. One can also delete the selected users from the list or search a particular user using the **Search** field.





The picklist options that appear will be as per the rights assigned to the SA. For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#).

Once a user is deleted from a grade, it gets restored to the default grade and inherits all configurations assigned to the default grade.

- Click **Save** and the created grade gets displayed in the grid on the right hand side.

You can edit or delete the grade if required. To do so,

- Click on the desired grade from the grid on the right hand side.
- To edit, click **Edit** .
- To delete, click **Delete** .



Only those grades can be deleted that are not assigned to any user/worker/visitor.

Now, one can also associate parameters to the created grade. To do so [See “Association Mapping” on page 1256](#).

Association Mapping

The parameters under Association Mapping panel are known as Associated parameters as they are linked with the grade from the **Group Associations** page of **Utilities** tab. Only the enabled parameters become available for configuration in the **Association Mapping** panel of grade page as shown below.

Grade

ID: 1
 Name: Grade 1
 Code: G1
 Set As Default: ☒
 Short Name: Grade 1
 Description: 250 chars


Association Mapping

Attendance


Enable Attendance Calculation: ☒

ID	Name
1	Grade 1

User In This Group

 A single associated parameter can be linked with only one group, i.e. if a parameter is enabled for one group from the Group Associations page, then it becomes disabled for other enterprise groups.

- Select the grade from the grid to be edited and click **Edit**.
- In the **Association Mapping panel**, configure the associated parameters as required. E.g. in the above screen, Enable Attendance Calculation has been enabled for all employees of the “Grade 1”.
- Click **Save**.

 If Association Mapping is changed from one Enterprise Group Type to other (eg. From Organization to Branch), all current default jobs records (Assignment End Date \geq Current Date) will be deleted. Previous default job records (Assignment End Date $<$ Current Date) will still be retained.

 If Enterprise Group is deleted then all job assignment records current as well as previous will be deleted.

Custom Group1

Custom Group1 tab enables to create and manage custom group. It helps to group users in a particular custom group and assign policies accordingly. You can add 999999 custom group1.

To view Custom Group tab, go to **Enterprise Structure > Custom Group1** and the following screen appears.

ID	Name
1	Custom Group 1
2	Cadre

The page displays configurations on the left side and to the right is the grid containing a list of created custom groups.

To configure a new custom group, click the **New** button and enter the following details:

- **ID:** The ID is auto generated by the system.
- **Name:** Specify the name of the custom group. The supported values are: **A-Z, a-z, 0-9, () , [], _ (underscore), - (Hyphen), . (full Stop), /, &, , (comma), @, ' (single quote), [space]**. The invalid characters for Multi-language character set are Set3 which includes ` ~ # % ^ * = + { } | \ : ; " < > ?
- **Code:** Enter a code of maximum 6 characters for the new custom group.
- **Set As Default:** Enable to set the created custom group as the default group.



Both default custom group and custom group that are already in use cannot be deleted from the system. In case all custom group configured on the system are deleted, the system will automatically apply the settings of the default custom group on the concerned users.

- **Short Name:** Enter short name for the custom group to be created.
- **Description:** Enter description for the custom group. It can be maximum of 250 characters.

User In This Group

This section enables to add users to the custom group.

- Select users to be added using the picklist button. The selected users get displayed in the grid. You can also delete the selected users from the list or search a particular user using the **Search** field.

Custom Group 1

ID * 1

Name * Custom Group 1

Code * CG1

Set As Default ☒

Short Name DFLTCG1

Description 250 chars

User In This Group

Search

ID	Name	
12	12	
1551	Shalini Fefar	
1690	admin	
555	555	
apta	apta user	
cafe	cafeteria	

Grid on the right:

ID	Name
1	Custom Group 1
2	Cadre



The picklist options that appear will be as per the rights assigned to the SA. For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#).

Once a user is deleted from a custom group, it gets restored to the default custom group and inherits all configurations assigned to the default custom group.

- Click **Save** and the created custom group gets displayed in the grid on the right hand side.

You can edit or delete the custom group if required. To do so,

- Click on the desired custom group from the grid on the right hand side.
- To edit, click **Edit** .
- To delete, click **Delete** .



Only those custom groups can be deleted that are not assigned to any user/worker/visitor.

Now, you can also associate parameters to the created custom group. To do so See [“Association Mapping”](#) on page 1260.

Association Mapping

The parameters under Association Mapping section are known as Associated parameters as they are linked with the custom group from the **Utilities > Group Associations**. Once the parameters are enabled, they will be available for configuration in the **Association Mapping** section of Custom Group page as shown below.

The screenshot displays the 'Custom Group 1' configuration page. The top section contains fields for ID (1), Name (Custom Group 1), Code (CG1), Set As Default (checked), Short Name (DFLTCG1), and Description (250 chars). Below this is the 'Association Mapping' section, which is divided into three categories: ESS, Attendance, and Policy. Under ESS, there are three checkboxes: 'Enable Account' (unchecked), 'Edit Basic Details' (unchecked), and 'Punch Marking Via ESS' (unchecked). Under Attendance, there is one checkbox: 'Enable Attendance Calculation' (unchecked). Under Policy, there is a field for 'Attendance Policy' with a dropdown menu showing 'ID' and 'Name' options. At the bottom, there is a 'User In This Group' section.



A single associated parameter can be linked with only one group, i.e. if a parameter is enabled for one enterprise group from the Group Associations page, then it becomes disabled for other enterprise groups.

Eg: IF ESS> Enable Account is selected for Custom Group1 from Group Association page, then Enable Account will be disabled for other enterprise groups.

- Select the custom group from the grid to be edited and click **Edit**.
- In the **Association Mapping** panel, configure the associated parameters as required. E.g. In the below screen, Enable Attendance Calculation has been enabled for all users of the “Custom Group 1”.

Custom Group 1

ID * 1

Name * Custom Group 1

Code * CG1

Set As Default ☒

Short Name DFLTCG1

Description 250 chars

Association Mapping

ESS

Enable Account ☐

Edit Basic Details ☐

Punch Marking Via ESS ☐

Attendance

Enable Attendance Calculation ☒

Policy

Attendance Policy 1 Attendance Policy-1

- Click **Save** to save the settings.



If Association Mapping is changed from one Enterprise Group Type to other (eg. From Organization to Branch), all current default jobs records (Assignment End Date \geq Current Date) will be deleted. Previous default job records (Assignment End Date $<$ Current Date) will still be retained.



If Enterprise Group is deleted then all job assignment records current as well as previous will be deleted.

Custom Group2

Custom Group2 tab enables to create and manage custom group. It helps to group users in a particular custom group and assign policies accordingly. You can add 999999 custom group2.

To view Custom Group tab, go to **Enterprise Structure > Custom Group2** and the following screen appears.

ID	Name
1	Custom Group 2

The page displays configurations on the left side and to the right is the grid containing a list of created custom groups.

To configure a new custom group, click the **New** button and enter the following details:

- **ID:** The ID is auto generated by the system.
- **Name:** Specify the name of the custom group. The supported values are: **A-Z, a-z, 0-9, () , [], _ (underscore), - (Hyphen), . (full Stop), /, &, , (comma), @, ' (single quote), [space]**. The invalid characters for Multi-language character set are Set3 which includes ` ~ # % ^ * = + { } | \ : ; " < > ?
- **Code:** Enter a code of maximum 6 characters for the new custom group.
- **Set As Default:** Enable to set the created custom group as the default group.



Both default custom group and custom group that are already in use cannot be deleted from the system. In case all custom group configured on the system are deleted, the system will automatically apply the settings of the default custom group on the concerned users.

- **Short Name:** Enter short name for the custom group to be created.
- **Description:** Enter description for the custom group. It can be maximum of 250 characters.

User In This Group

This section enables to add users to the custom group.

- Select users to be added using the picklist button. The selected users get displayed in the grid. You can also delete the selected users from the list or search a particular user using the **Search** field.





The picklist options that appear will be as per the rights assigned to the SA. For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#).

Once a user is deleted from a custom group, it gets restored to the default custom group and inherits all configurations assigned to the default custom group.

- Click **Save** and the created custom group gets displayed in the grid on the right hand side.

You can edit or delete the custom group if required. To do so,

- Click on the desired custom group from the grid on the right hand side.
- To edit, click **Edit** .
- To delete, click **Delete** .



Only those custom groups can be deleted that are not assigned to any user/worker/visitor.

Now, you can also associate parameters to the created custom group. To do so See [“Association Mapping”](#) on [page 1264](#).

Association Mapping

The parameters under Association Mapping section are known as Associated parameters as they are linked with the custom group from the **Utilities > Group Associations**. Once the parameters are enabled, they will be available for configuration in the **Association Mapping** section of Custom Group page as shown below.

The screenshot displays the 'Custom Group 2' configuration interface. At the top, there are fields for ID (1), Name (Custom Group 2), and Code (CG2). Below these are checkboxes for 'Set As Default' (checked) and 'Short Name' (DFLTCG2), followed by a 'Description' field (250 chars). The 'Association Mapping' section is expanded, showing three sub-sections: 'Attendance' with a dropdown for 'OT/C-OFF Eligibility' (None) and checkboxes for 'Authorize C-OFF On' (WO, PH, WO/PH, FB, RD, Normal Day); 'Policy' with an 'Overtime Policy' dropdown (ID) and a 'Name' field; and 'Access Details' with a 'Shift Based Access' checkbox (unchecked).



A single associated parameter can be linked with only one group, i.e. if a parameter is enabled for one enterprise group from the Group Associations page, then it becomes disabled for other enterprise groups.

Eg: IF Policy> Overtime Policy is selected for Custom Group2 from Group Association page, then Overtime Policy will be disabled for other enterprise groups.

- Select the custom group from the grid to be edited and click **Edit**.
- In the **Association Mapping panel**, configure the associated parameters as required. E.g. In the below screen, Shift Based Access has been enabled for all users of the “Custom Group 2”.

Custom Group 2

ID * 1

Name * Custom Group 2

Code * CG2

Set As Default ☒

Short Name DFLTCG2

Description 250 chars

Association Mapping

Attendance

OT/C-OFF Eligibility None

Authorize C-OFF On ☐ WO ☐ PH ☐ WO/PH ☐ FB ☐ RD ☐ Normal Day

Policy

Overtime Policy ID Name

Access Details

Shift Based Access ☒

- Click **Save** to save the settings.



If Association Mapping is changed from one Enterprise Group Type to other (eg. From Organization to Branch), all current default jobs records (Assignment End Date \geq Current Date) will be deleted. Previous default job records (Assignment End Date $<$ Current Date) will still be retained.

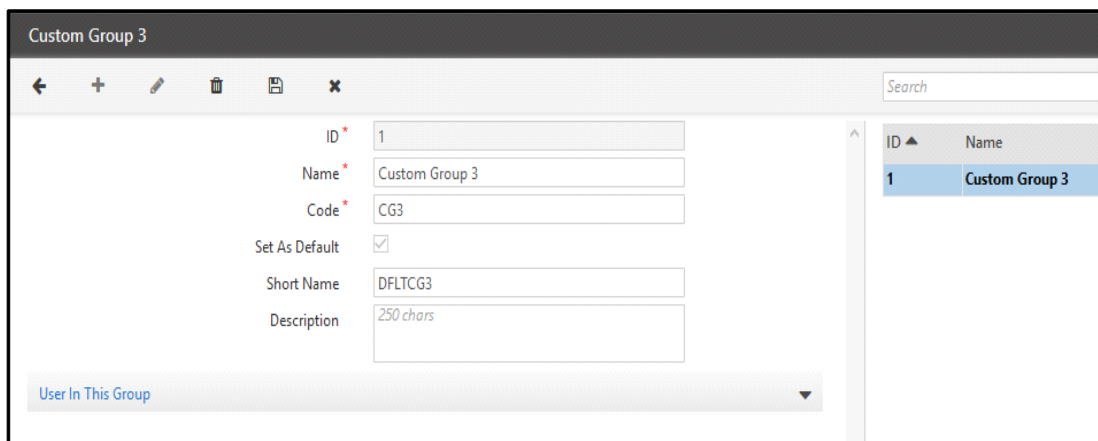


If Enterprise Group is deleted then all job assignment records current as well as previous will be deleted.

Custom Group3

Custom Group3 tab enables to create and manage custom group. It helps to group users in a particular custom group and assign policies accordingly. You can add 999999 custom group3.

To view Custom Group tab, go to **Enterprise Structure > Custom Group3** and the following screen appears.



ID	Name
1	Custom Group 3

The page displays configurations on the left side and to the right is the grid containing a list of created custom groups.

To configure a new custom group, click the **New** button and enter the following details:

- **ID:** The ID is auto generated by the system.
- **Name:** Specify the name of the custom group. The supported values are: **A-Z, a-z, 0-9, () , [], _ (underscore), - (Hyphen), . (full Stop), /, &, , (comma), @, ' (single quote), [space]**. The invalid characters for Multi-language character set are Set3 which includes ` ~ # % ^ * = + { } | \ : ; " < > ?
- **Code:** Enter a code of maximum 6 characters for the new custom group.
- **Set As Default:** Enable to set the created custom group as the default group.



Both default custom group and custom group that are already in use cannot be deleted from the system. In case all custom group configured on the system are deleted, the system will automatically apply the settings of the default custom group on the concerned users.

- **Short Name:** Enter short name for the custom group to be created.
- **Description:** Enter description for the custom group. It can be maximum of 250 characters.

User In This Group

This section enables to add users to the custom group.

- Select users to be added using the picklist button. The selected users get displayed in the grid. You can also delete the selected users from the list or search a particular user using the **Search** field.





The picklist options that appear will be as per the rights assigned to the SA. For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#).

Once a user is deleted from a custom group, it gets restored to the default custom group and inherits all configurations assigned to the default custom group.

- Click **Save** and the created custom group gets displayed in the grid on the right hand side.

You can edit or delete the custom group if required. To do so,

- Click on the desired custom group from the grid on the right hand side.
- To edit, click **Edit** .
- To delete, click **Delete** .



Only those custom groups can be deleted that are not assigned to any user/worker/visitor.

Now, you can also associate parameters to the created custom group. To do so See [“Association Mapping”](#) on page 1268.

Association Mapping

The parameters under Association Mapping section are known as Associated parameters as they are linked with the custom group from the **Utilities > Group Associations**. Once the parameters are enabled, they will be available for configuration in the **Association Mapping** section of Custom Group page as shown below.

The screenshot displays the 'Custom Group 3' configuration window. The top section contains fields for ID (1), Name (Custom Group 3), Code (CG3), Set As Default (checked), Short Name (DFLT CG3), and Description (250 chars). Below this is the 'Association Mapping' section, which is expanded to show three sub-sections: 'Access Details' with fields for Access Validity (unchecked), Access Validity Date (calendar icon), and Access Level For Smart Identification (8); 'Cafeteria' with a Discount Level dropdown set to 'None'; and 'Prepaid Account' with a Balance Management dropdown set to 'Device Based'.



A single associated parameter can be linked with only one group, i.e. if a parameter is enabled for one enterprise group from the Group Associations page, then it becomes disabled for other enterprise groups.

Eg: IF ESS> Enable Account is selected for Custom Group1 from Group Association page, then Enable Account will be disabled for other enterprise groups.

- Select the custom group from the grid to be edited and click **Edit**.
- In the **Association Mapping panel**, configure the associated parameters as required. E.g. In the below screen, Cafeteria- Discount Level1 has been set for all users of the “Custom Group 3”.

- Click **Save** to save the settings.



If Association Mapping is changed from one Enterprise Group Type to other (eg. From Organization to Branch), all current default jobs records (Assignment End Date \geq Current Date) will be deleted. Previous default job records (Assignment End Date $<$ Current Date) will still be retained.



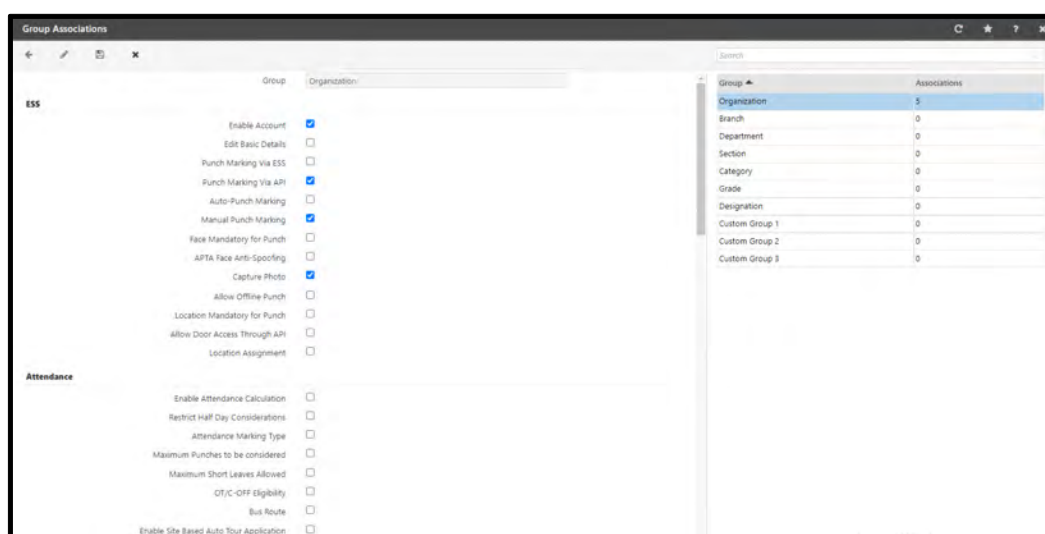
If Enterprise Group is deleted then all job assignment records current as well as previous will be deleted.

Group Associations

Group Association refers to the process of associating certain system parameters with an enterprise group, such that the configurations of these parameters will apply uniformly to all users within the group. For example, this function may be used to associate the *Attendance Policy* parameter with the *Designation* group so that different Attendance Policies can be applied to different designations within an organization.

The *Group Associations* feature in COSEC enables the system administrator to determine which parameters should be available for *Association Mapping* for an enterprise group.

To define *Group Associations* for each enterprise group, go to **Enterprise Structure module > Utilities > Group Associations** and the following screen appears.



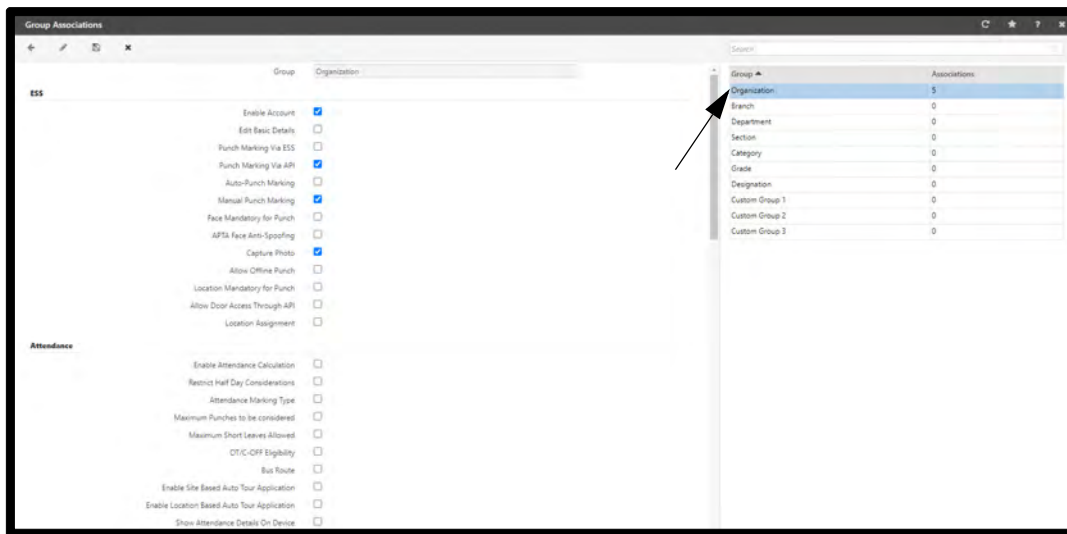
Group	Associations
Organization	5
Branch	0
Department	0
Section	0
Category	0
Grade	0
Designation	0
Custom Group 1	0
Custom Group 2	0
Custom Group 3	0

The Group Association can be done for the parameters of **ESS, Attendance, Policy, Access Details, Cafeteria, Prepaid Account, Postpaid Account, Job Costing, Field Visit Management, Face Recognition and Visitor Management**.

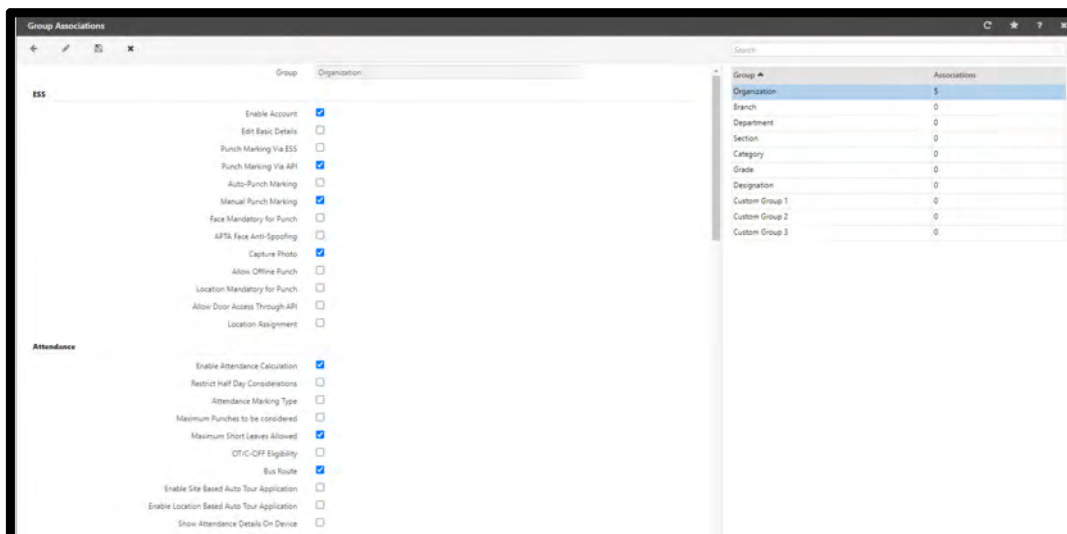


*The ESS Assignment check box under Job Costing will not be displayed if the **Show All Jobs while Punching** check box is enabled. For details, refer to [“Job Costing”](#) in [“Defining Global Policies”](#).*

1. Select a **Group** from the grid on the right hand side of the page as shown below.



2. Select the appropriate parameter check-boxes which are to be associated with the selected group as shown above.



3. Click **Save** to apply the associations to the selected group. The number of the association will be updated accordingly. These parameters will now appear on the particular group page for **Association Mapping**.

Example:

Suppose **Group** is selected as **Organization**.

Select **Enable Account**, **Punch Marking via API**, **Manual Punch Marking**, **Capture Photo**, and **Max Short Leaves Allowed** options as shown below:

The screenshot shows the 'Group Associations' window with the 'Organization' tab selected. The 'ESS' section has the following settings: 'Enable Account' (checked), 'Punch Marking via API' (checked), 'Manual Punch Marking' (checked), and 'Capture Photo' (checked). The 'Attendance' section has 'Maximum Short Leaves Allowed' (checked). The 'Associations' table on the right shows the following data:

Group	Associations
Organization	5
Branch	0
Department	0
Section	0
Category	0
Grade	0
Designation	0
Custom Group 1	0
Custom Group 2	0
Custom Group 3	0

Then the Organization tab on Enterprise Structure page will appear as shown below.

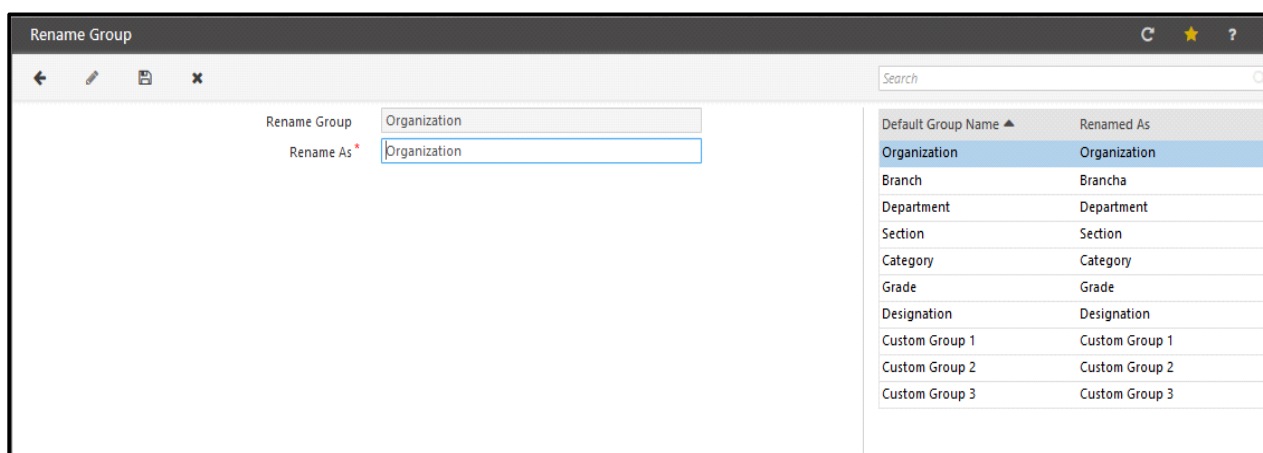
Enable Account, **Punch Marking via API**, **Manual Punch Marking**, **Capture Photo**, and **Max Short Leaves Allowed** will get associated with "Organization". You can enable the options for the particular organization by selecting it from the list and enabling the options for it.

The screenshot shows the 'Organization' window with the details of an organization. The 'Association Mapping' section shows the following settings: 'Enable Account' (checked), 'Punch Marking via API' (checked), 'Manual Punch Marking' (checked), and 'Capture Photo' (checked). The 'Attendance' section has 'Maximum Short Leaves Allowed' (checked). The 'Users In This Group' section shows a list of users.

Renaming Groups

COSEC enables the system administrator to decide how *Enterprise Groups* can be labelled to best represent a business structure. This can be done by renaming the existing groups predefined on the system.

To rename a group, Go to **Enterprise Structure > Utilities > Rename Groups** and the following screen appears.



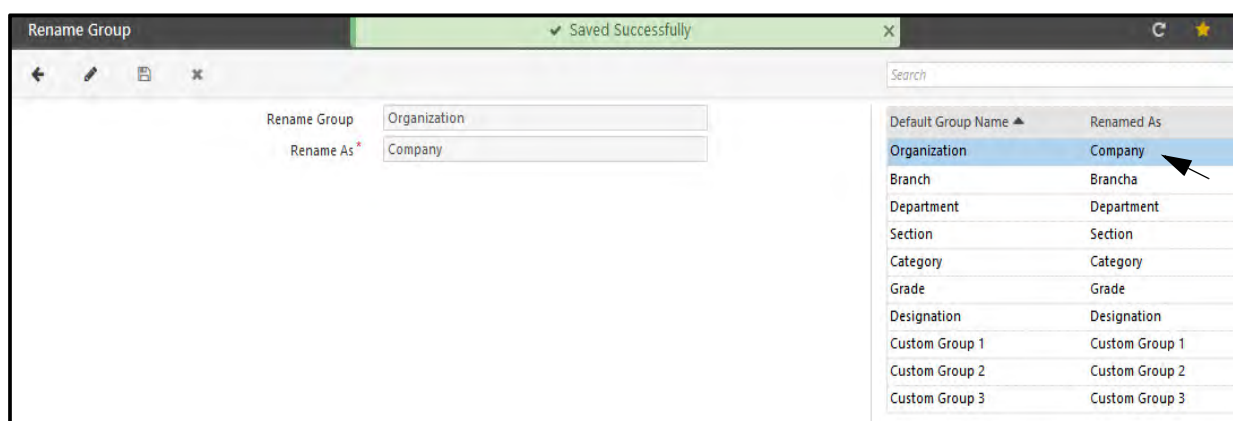
Default Group Name	Renamed As
Organization	Organization
Branch	Brancha
Department	Department
Section	Section
Category	Category
Grade	Grade
Designation	Designation
Custom Group 1	Custom Group 1
Custom Group 2	Custom Group 2
Custom Group 3	Custom Group 3

Select a Group from the list view that is to be renamed. The selected *Default Group Name* appears in the **Group Name** field.

Enter the new Group Name/label in the **Rename As** field.

Click the **Save** button.

The new Group name/label will appear in the list view under the **Renamed As** column as shown below.



Default Group Name	Renamed As
Organization	Company
Branch	Brancha
Department	Department
Section	Section
Category	Category
Grade	Grade
Designation	Designation
Custom Group 1	Custom Group 1
Custom Group 2	Custom Group 2
Custom Group 3	Custom Group 3



The user can also perform the **Rename Groups** function using the **Admin** module. To know more see [Renaming Group in Admin Module](#).

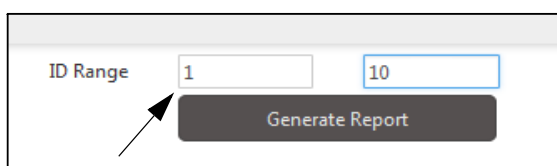
Enterprise Group Reports

The COSEC user can easily access and generate individual and detailed reports on enterprise groups related to a business. Enterprise Structure reports can be generated using the **Reports** section under the **Enterprise Structure** module. The following reports can be viewed under this section:

- Organization Report
- Branch Report
- Department Report
- Designation Report
- Section Report
- Category Report
- Grade Report
- Custom Group 1
- Custom Group 2
- Custom Group 3

To generate an *Enterprise Group* report,

1. On the respective group page, enter a **Number Range** in the given fields to specify the range of IDs to be retrieved for the particular group as shown in the figure below.



The screenshot shows a form with two input fields for 'ID Range'. The first field contains the number '1' and the second field contains the number '10'. An arrow points to the first field. Below the fields is a button labeled 'Generate Report'.

2. Click the **Generate Report** button.

The following figure displays a sample *Department Report* generated to retrieve the list of all existing departments with IDs between 1 to 10.

Organization-1 Organization						Page 1 of 1	
Run by: System Admin						Date: 14/02/2020	15:40
Sr No	ID Code	Name	Description	Email	Short Name	Default	
1	3 ORG_A1	Organization_Anmol1		parth.kapadia@matrixrd.org	Organization_An	No	
2	4 ORG_A2	Organization_Anmol2		vishvjeet.gohil@matrixrd.org	Organization_An	No	
3	5 VISH	5		vishvjeet.gohil@matrixrd.org	5	No	

The figure below illustrates another sample for a *Designation Report* for the same organisation.


Organization-1						Page 1 of 1	
Designation6							
Run by: System Admin						Date: 13/02/2020	12:50
Sr No	ID Code	Name	Description	Email	Short Name	Default	
1	1 DSG1	Designation-1			DFLTDSG	Yes	
2	2 DESA1	Designation_Anmol_1			Designation_Anm	No	
3	3 DESA2	Designation_Anmol_2			Designation_Anm	No	

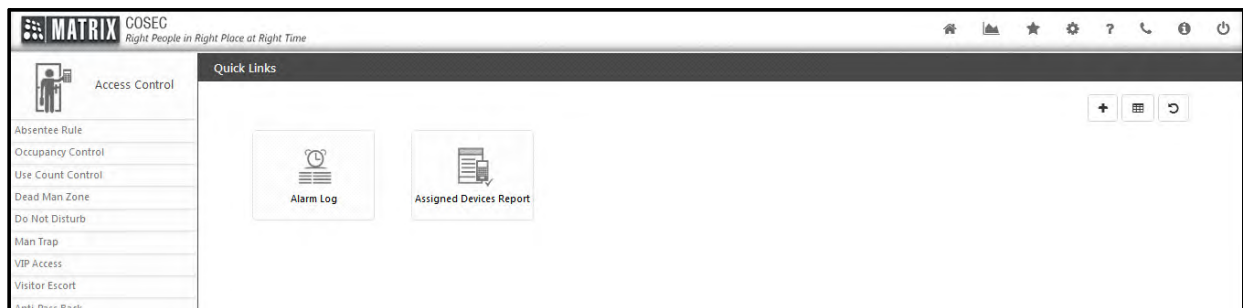
Access Control System can detect and report intrusion, access to sensitive places like warehouse, cash rooms in banks, R&D departments in corporate offices, troubled conditions, any other place, where unauthorized access needs to be monitored.

Access control systems can grant, record, deny, detect and report access to facilities, services, information and other assets that need to be protected from mass access.



In order to start the configuration of the system, the user needs to first define the devices from the **Device** module and then proceed with the configuration of the access control policies from the **Access Control** module.

To use the Access Control functionality,

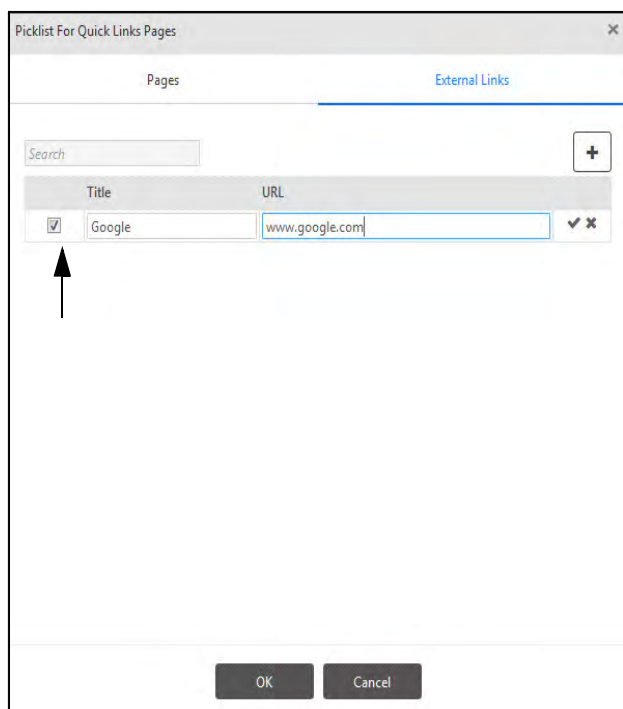
- Click on **Access Control**  module. The **Access Control** page appears.




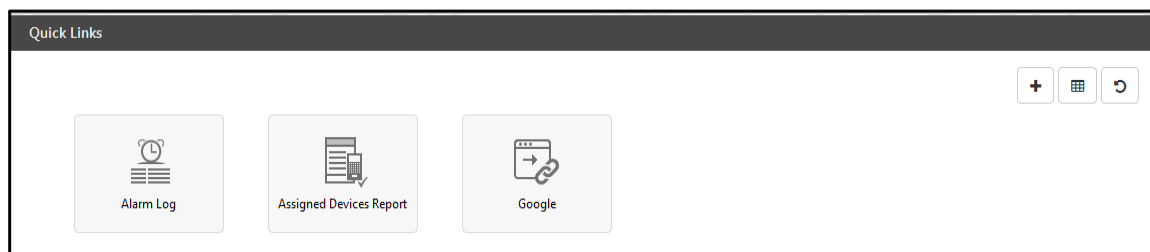
The page displays a menu and **Quick Links** to go to the required page in just one click. Quick Links are shortcuts to reach to a specific page easily. It also contains following three buttons:



- Add Quick Link:** Click **Add**  to add a quick link. A picklist for Quick Link pages appears for selecting the page or External Link for which the quick link is to be created. Maximum **20** quick links can be added.
- For Adding **Pages** in Quick Link, Select the Pages and click on OK.
- For Adding **External Links**, Select External Link tab, click **Add**  to add new external link.
- Configure the **Title** and **URL** of the external link under the respective fields. click on check box to get

the configured link on quick link screen as shown below. To save the configuration click **Save**  .



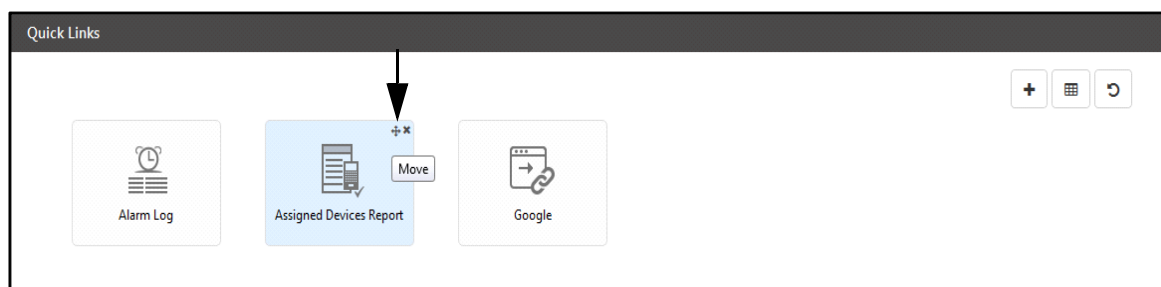
- To edit the saved configuration, click **Edit** .
- Click on OK to save the link configuration on Quick Link screen. The external link will be displayed as shown below:



- **Select Layout:** Click **Select Layout**  to select a layout for the quick links. You can select 5x4 or 4x5 layout to manage the quick links.
- **Reset Quick Links:** Click **Reset to Default**  to reset the quick links to the default quick links.

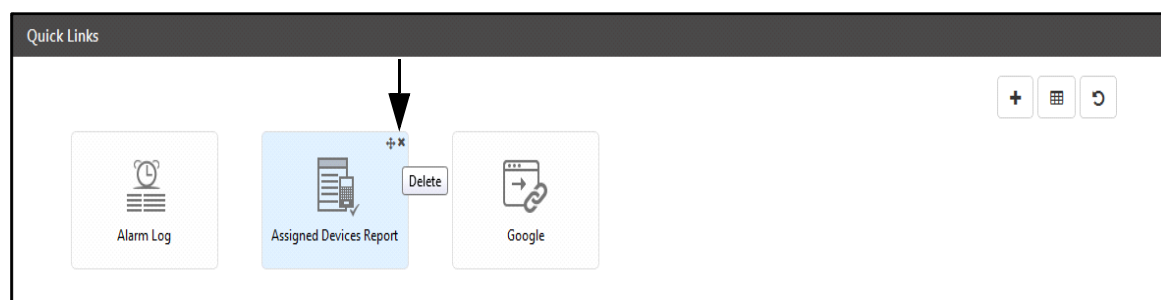
Move the Link

To move the link from one place to another, hover on the link on top right corner and click on **Move** as shown below. Then drag the quick link to the desired place. It will be placed at the desired location on the quick links page.




Delete the Link

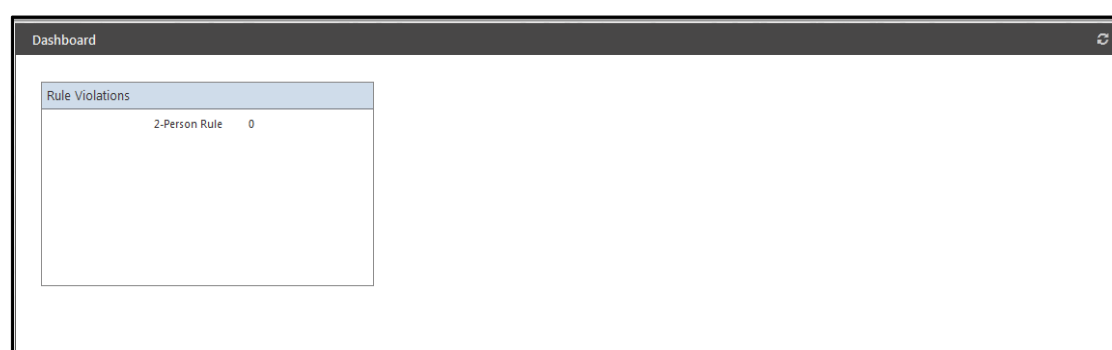
To delete a particular link, hover on the link on top right corner and click on **Delete** as shown below.



Quick links are displayed as per rights given to System Account and ESS users.

Access Control Dashboard

To view the Dashboard, click **Dashboard**  on the **Access Control** page. It displays the total number of violations on the current day for the 2-Person Rule:



For more information on the above Dashboard option, click the respective information link on the Dashboard. The

Latest values on Dashboard are updated on clicking **Refresh**



Absentee Rule

Absentee Rule feature enables the system to set the maximum number of days for non-usage of a credential (**1-99Days**). On expiration (no credential usage - for the maximum number of days set) the User will be automatically blocked.



*This functionality can also be enabled from the **Device Module > Device Configuration > Features** option.*

To set the Absentee Rule,

- Click **Access Control > Absentee Rule**. The **Absentee Rule** page appears.

The screenshot shows the 'Absentee Rule' configuration window. On the left, there is a sidebar with two tabs: 'Device - Wise' (selected) and 'User - Wise'. The main content area for 'Device - Wise' includes a 'Device' section with input fields for 'ID' and 'Name', and an 'Enable Rule' checkbox. Below these is an 'Update Device' button.

The Absentee Rule can be configured in two forms:

- Device-Wise
- User-Wise

Device-Wise

In Device-Wise Absentee Rule, the rule will be applicable to the door as well as the users assigned to it.


To configure Device-Wise Absentee Rule,

- Click the **Device-Wise** tab.


The screenshot shows the 'Absentee Rule' configuration window with the 'Device - Wise' tab selected. The 'Device' field is set to '2' and 'PVR Direct Door'. The 'Enable Rule' checkbox is checked. Below the configuration fields is a table with the following data:





User ID	Name	Rule Enabled	Days Count	
07	Aditi	No	60	
1	Shalini	No	60	
101	Khushbu	No	60	
2	Chirag	No	60	

Configure the following parameters:

- **Device:** Select the required device using the **Device**  picklist. A list of all users on the selected device appear in the grid.
- **Enable Rule:** Select the check box to enable the rule on the selected device.
- Click **Update Device** to save the device selection.

The grid displays all the users assigned to the selected device. The following details appear — User ID, Name, Rule Enabled and Days Count. You can edit the rule for a particular user.

- Click **Edit**  corresponding to the user you wish to edit the rule.

Search 				
User ID ▲	Name	Rule Enabled	Days Count	
07	Aditi	No	60	
1	Shalini	<input checked="" type="checkbox"/>	60	 
101	Khushbu	No	60	
2	Chirag	No	60	









- **Rule Enabled:** Select the check box to enable the rule for the selected user.
- **Days Count:** Specify the absent days count after which the selected user should be blocked.
- Click **OK** to update the details or click **Cancel** to discard.

User Wise

In User-Wise Absentee Rule, the rule will be applicable to the user as well as the doors assigned to the user.

To configure User-Wise Absentee Rule,


- Click the **User-Wise** tab.









Absentee Rule ★ ? ✕					
Device - Wise		User * 07 Aditi 			
User - Wise		Search 			
Device ID ▲	Name	Rule Active	Rule Applicable	Days Count	
1	Door v3	No	No	60	
2	PVR Direct Door	Yes	No	60	
3	NGT Ground Floor	No	No	60	
4	Vega Direct Door	No	No	60	
5	Wireless Door 1st Floor	Yes	No	60	
6	PVR Door-Device-6	No	No	60	

Configure the following parameters:

- **User:** Select the required user using the **User**  picklist. A list of all devices on the selected user appear in the grid.

The grid displays all the devices assigned to the selected user. The following details appear — Device ID, Name, Rule Active, Rule Applicable and Days Count. You can edit the rule for a particular device.

- Click **Edit**  corresponding to the device you wish to edit the rule.

<input type="text" value="Search"/>						
Device ID ▲	Name	Rule Active	Rule Applicable	Days Count		
1	Door v3	No	No	60		
2	PVR Direct Door	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	60		
3	NGT Ground Floor	No	No	60		
4	Vega Direct Door	No	No	60		
5	Wireless Door 1st Floor	Yes	No	60		
6	PVR Door-Device-6	No	No	60		

- **Rule Active:** Select the check box to activate the rule for the selected device.
- **Rule Applicable:** Select the check box to enable the rule for the selected device.
- **Days Count:** Specify the absent days count after which the user will be blocked for the selected device.
- Click **OK** to update the details or click **Cancel** to discard.

Occupancy Control

Occupancy Control feature enables the system to monitor and control the number of users permitted within a secured area or controlled zone. This feature can be useful for high security bank vaults, research organizations where a single person cannot be trusted.

The access to secured zone can be restricted by specifying Maximum and Minimum Occupancy limit for direct door as well as for Panel200 and Zones.

Occupancy Control functionality requires **Entry** and **Exit** readers on the controlled area.



This functionality can also be enabled from the **Device Module > Device Configuration > Features** option.

- 1.If Dead Man and Occupancy Control feature both are enabled then Occupancy Control feature will not work.
- 2.If Duress feature is enabled then user will be allowed directly. Occupancy Control feature will not be checked.
3. SI user will be restricted to enter the Occupancy Control enabled Zone.

To set the Occupancy Control,

- Click **Access Control > Occupancy Control**. The **Occupancy Control** page appears.

Occupancy Control

Device * Name

Enable Rule ☐

Zone *


Enable Rule On Zone ☐

Occupants Limit *

ID	Name
2	NGT Direct Door-Device-2
3	Panel Lite V2
4	Panel Lite
4	Wireless Door
5	Door V3
6	Door FMX
8	ARC as Direct Door
9	Path as direct door
10	Vega as Direct Door

The grid on the right hand side of the page shows the list of the devices configured with Advance Access Control System.

Configure the following parameters:

- **Device:** Select the required device using the **Device**  picklist.
- **Enable Rule:** Select the check box to enable the rule on the selected device.
- Click **Update Device** to enable the rule on the device.

Once you update the device, you can configure the following parameters:

- **Zone:** Select the Zone on which you want to enable the rule.



This parameter is applicable only when the selected device is Panel/Panel Lite/Panel200.

- **Enable Rule on Zone:** Select the check box to enable the rule on the Zone.



This parameter is applicable only when the selected device is Panel/Panel Lite/Panel200.

- **Occupants Limit:** Specify the value for Occupants Limit to control the number of persons in a secured area. Maximum Occupancy Limit can vary from **0 to 999** users for any direct door. If the user count exceeds the maximum limit and a VIP user accesses the door then access will be granted.
- Click on **Update Zone** to save the changes.

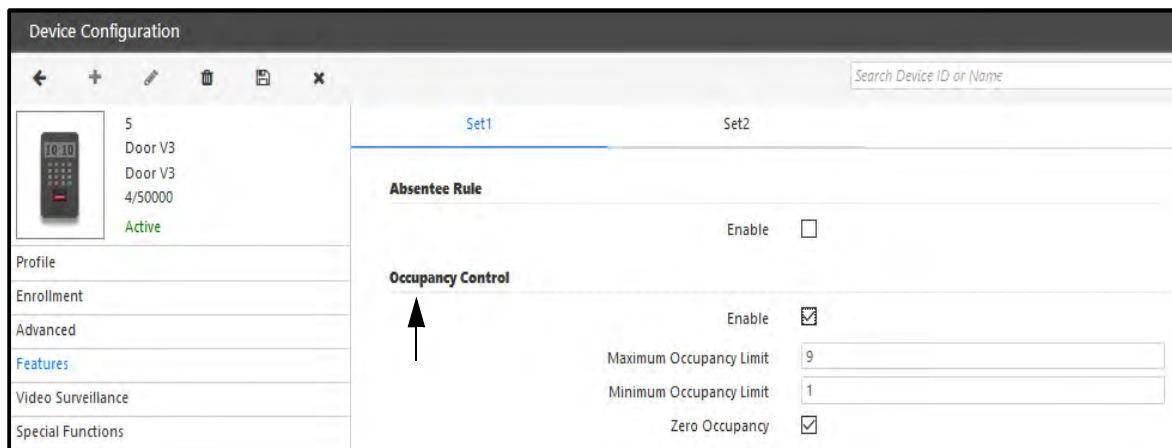
For Direct Doors

The occupancy count should be affected on each entry (made through entry reader) and on each exit (made through exit reader). Occupancy control is verified even if the First-in-User or 2-Person Rule is enabled.



Occupancy count shall be stored in RAM and on reboot, this value will be reset to zero.

You can configure **Minimum Occupancy Limit** and **Zero Occupancy** in Direct doors from **Device Configuration > Features**.



- **Maximum Occupancy Limit:** It is the maximum number of users that can be present in the zone/area at a time. For example: If Maximum Occupancy Limit is set as 9, 10th individual will not be allowed to enter the zone. Users are allowed to enter until the Maximum Occupancy Limit is reached.
- **Minimum Occupancy Limit:** It is the minimum number of users that need to be present in the zone/area at a time. For example: If Minimum Occupancy Limit is set as 2, a single user is not allowed to enter. At least 2 users must enter together. After that, individual users can enter till the Maximum Occupancy Limit is reached.

When 1st user punches on the door, the device will wait for the 2nd user to punch. If second user does not come before the time out duration, the first user will not be allowed to enter.

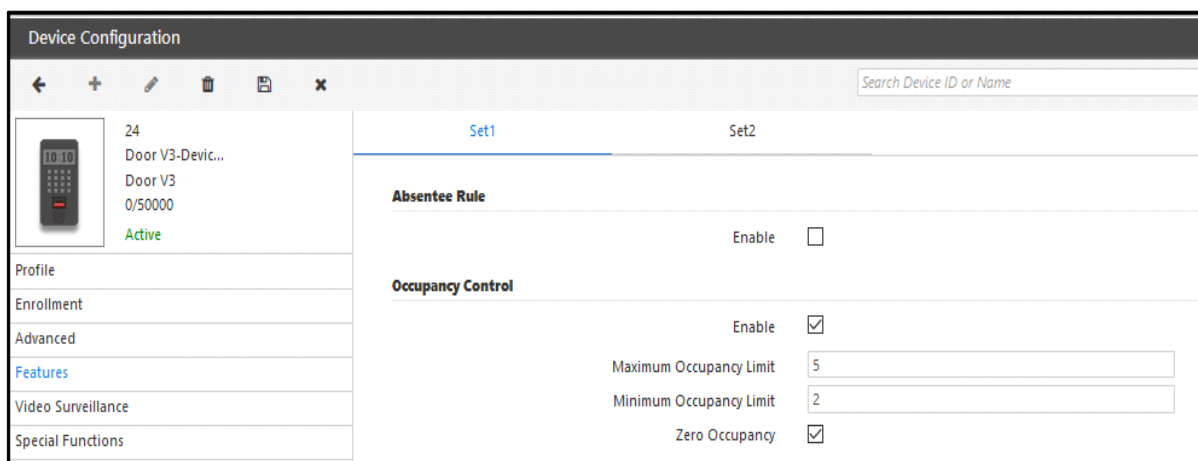
- **Zero Occupancy:** Enable this check box if the zone is allowed to be empty or have zero occupancy which will be checked when user exists from the zone.

Case1: If Minimum Occupancy Limit is set as 2 and Zero Occupancy is enabled;

- If there are only 2 users left in the zone, so both users can exit the zone together leaving the zone vacant. But, users cannot exit one after another.


Case2: If Minimum Occupancy Limit is set as 2 and Zero Occupancy is disabled;

- If there are only 2 users left in the zone and as the zone cannot be empty; so the 2 users cannot exit from the zone maintaining the minimum limit.




Example: Consider a scenario where the Minimum Occupancy Limit is configured as 2 and the Maximum Occupancy Limit is 4. The following possibilities can occur.

- If User 1 punches and User 2 does not punch; the minimum occupancy condition will be violated and User 1 will be denied access as shown below.


User Details		Events					
 <p>User ID: 1 Chirag</p> <p>Device: Door V3-Device-24</p> <p>Event Date & Time: 19/06/2018 06:07:00 PM</p> <p>Department: DFLDPT</p> <p>Designation: DFLTDSG</p>		Sr No.	Date Time	Type	Device	Category	Detail
		576	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ External Reader Configuration Sent. TID: 1806190040000729
		577	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	ACK	← External Reader Configuration Successful.
		578	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ External Reader Configuration Sent. TID: 1806190040000730
		579	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	ACK	← External Reader Configuration Successful.
		580	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ External Reader Configuration Sent. TID: 1806190040000731
		581	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	ACK	← External Reader Configuration Successful.
		582	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ External Reader Configuration Sent. TID: 1806190040000732
		583	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	ACK	← External Reader Configuration Successful.
		584	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ MultiLanguage Configuration Sent. TID: 1806190040000733
		585	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	ACK	← MultiLanguage Configuration Successful.
		586	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ Identification Server Configuration Sent. TID: 1806190040000734
		587	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	ACK	← Identification Server Configuration Successful.
		588	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ Special Function Configuration Sent. Special Function No: 11 TID: 1806190040000735
		589	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	ACK	← Special Function Configuration Successful. Special Function No: 11
		590	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ End Of Message
		591	19/06/2018 06:07:01 PM	Door V3	Door V3-Device-24	User	→ Denied - Minimum Occupancy with Finger. User ID: 1 Event Date Time: 19/06/2018 06:07:00 PM
		592	19/06/2018 06:07:01 PM	Door V3	Door V3-Device-24	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 42

- 2 users will be allowed when they enter together, that is, they punch one after another which maintains Minimum Occupancy Limit as shown below.

User Details		Events					
 <p>User ID: 101 Khushbu</p> <p>Device: Door V3-Device-24</p> <p>Event Date & Time: 19/06/2018 06:09:46 PM</p> <p>Department: DFLDPT</p> <p>Designation: DFLTDSG</p>		Sr No.	Date Time	Type	Device	Category	Detail
		580	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ External Reader Configuration Sent. TID: 1806190040000731
		581	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	ACK	← External Reader Configuration Successful.
		582	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ External Reader Configuration Sent. TID: 1806190040000732
		583	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	ACK	← External Reader Configuration Successful.
		584	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ MultiLanguage Configuration Sent. TID: 1806190040000733
		585	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	ACK	← MultiLanguage Configuration Successful.
		586	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ Identification Server Configuration Sent. TID: 1806190040000734
		587	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	ACK	← Identification Server Configuration Successful.
		588	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ Special Function Configuration Sent. Special Function No: 11 TID: 1806190040000735
		589	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	ACK	← Special Function Configuration Successful. Special Function No: 11
		590	19/06/2018 06:06:16 PM	Door V3	Door V3-Device-24	Other	→ End Of Message
		591	19/06/2018 06:07:01 PM	Door V3	Door V3-Device-24	User	→ Denied - Minimum Occupancy with Finger. User ID: 1 Event Date Time: 19/06/2018 06:07:00 PM
		592	19/06/2018 06:07:01 PM	Door V3	Door V3-Device-24	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 42
		593	19/06/2018 06:09:47 PM	Door V3	Door V3-Device-24	User	→ Allowed with Finger. User ID: 1 Event Date Time: 19/06/2018 06:09:46 PM
		594	19/06/2018 06:09:47 PM	Door V3	Door V3-Device-24	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 43
		595	19/06/2018 06:09:47 PM	Door V3	Door V3-Device-24	User	→ Allowed with Finger. User ID: 101 Event Date Time: 19/06/2018 06:09:46 PM
		596	19/06/2018 06:09:47 PM	Door V3	Door V3-Device-24	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 44

- When a single user tries to exit from the door, he/she will not be allowed as occupancy of 1 is not allowed. So, both users must punch to exit which will satisfy zero occupancy.
- The Maximum Occupancy Limit will be violated if more than 5 occupants try to access the door. Even VIP user will be denied to access the area.

User Details



User ID: HR1

Ronald

Denied - Occupancy Control

Device:

Door V3-Device-24

Event Date & Time:

19/06/2018 06:22:14 PM

Department:

DFLTDPT

Designation:

DFLTDSG

Events

Sr No.	Date Time	Type	Device	Category	Detail
994	19/06/2018 06:21:45 PM	Door V3	Door V3-Device-24	Other	→ Identification Server Configuration Sent. TID: 1806190040000904
995	19/06/2018 06:21:45 PM	Door V3	Door V3-Device-24	ACK	← Identification Server Configuration Successful.
996	19/06/2018 06:21:45 PM	Door V3	Door V3-Device-24	Other	→ Special Function Configuration Sent. Special Function No: 11 TID: 1806190040000905
997	19/06/2018 06:21:45 PM	Door V3	Door V3-Device-24	ACK	← Special Function Configuration Successful. Special Function No: 11
998	19/06/2018 06:21:45 PM	Door V3	Door V3-Device-24	Other	→ End Of Message
999	19/06/2018 06:21:54 PM	Door V3	Door V3-Device-24	User	→ Allowed with Finger. User ID: 1 Event Date Time: 19/06/2018 06:21:53 PM
1000	19/06/2018 06:21:54 PM	Door V3	Door V3-Device-24	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 66
1001	19/06/2018 06:21:54 PM	Door V3	Door V3-Device-24	User	→ Allowed with Finger. User ID: 101 Event Date Time: 19/06/2018 06:21:53 PM
1002	19/06/2018 06:21:54 PM	Door V3	Door V3-Device-24	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 67
1003	19/06/2018 06:21:59 PM	Door V3	Door V3-Device-24	User	→ Allowed with Finger. User ID: 4 Event Date Time: 19/06/2018 06:21:58 PM
1004	19/06/2018 06:21:59 PM	Door V3	Door V3-Device-24	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 68
1005	19/06/2018 06:22:05 PM	Door V3	Door V3-Device-24	User	→ Allowed with Finger. User ID: 102 [1689] Event Date Time: 19/06/2018 06:22:04 PM
1006	19/06/2018 06:22:05 PM	Door V3	Door V3-Device-24	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 69
1007	19/06/2018 06:22:10 PM	Door V3	Door V3-Device-24	User	→ Allowed with Finger. User ID: 1687 Event Date Time: 19/06/2018 06:22:09 PM
1008	19/06/2018 06:22:10 PM	Door V3	Door V3-Device-24	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 70
1009	19/06/2018 06:22:15 PM	Door V3	Door V3-Device-24	User	→ Denied - Occupancy Control with Finger. User ID: HR1 [1693] Event Date Time: 19/06/2018 06:22:14...
1010	19/06/2018 06:22:15 PM	Door V3	Door V3-Device-24	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 71

For Panel Doors

The Occupancy Control rule for Panel Doors can be configured by enabling the rule for Panel200 and the specific Zones. Once the rule is updated on Zone, it is applicable to all the doors of the respective zones.

In Panel200, the **Maximum Occupancy Limit** is the Default Occupancy Limit.

When you create new zones of Panel200, the Maximum Occupancy Limit for that zone will be set to the default value as set in the Panel200. If the Default Occupancy Limit for Panel200 is 9, so all the newly created zones will have the default value as 9.

Device Configuration

3

Panel Lite V2

Panel Lite V2

4/25000

Active

Profile

Enrollment

Advanced

Features

Special Functions

Input/Output

Set1

Set2

Set3

Absentee Rule

Enable

☐

Occupancy Control

Enable

☒

Default Occupancy Limit

9

Use Count Control

Enable

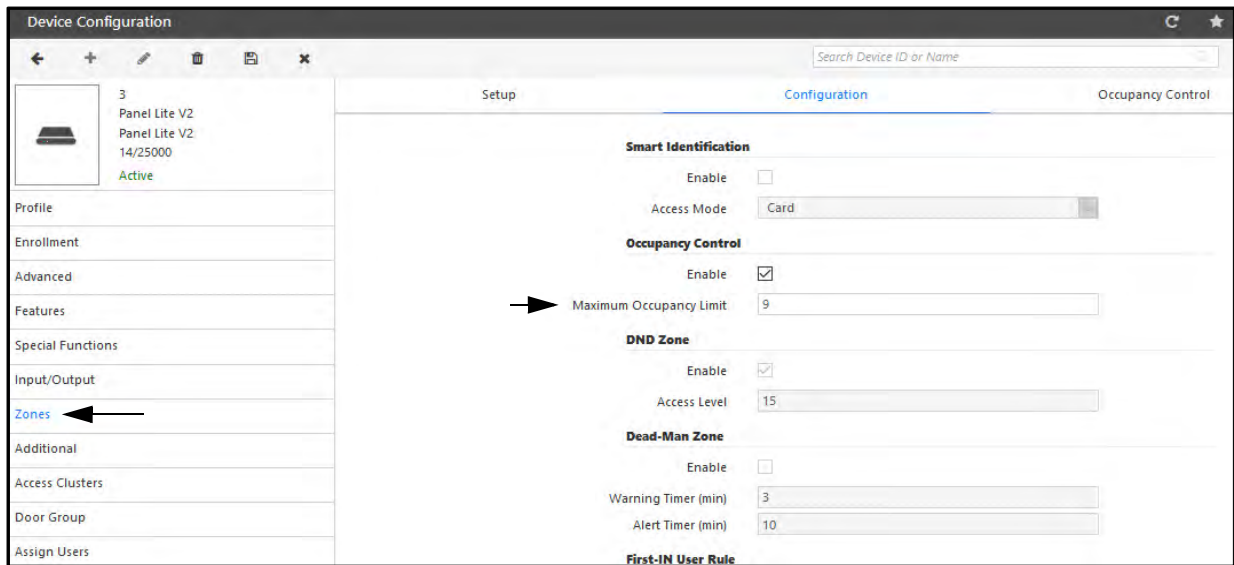
☐

Default Use Count Limit (per minute)

5

You can change the Maximum Occupancy Limit for the specific zone from

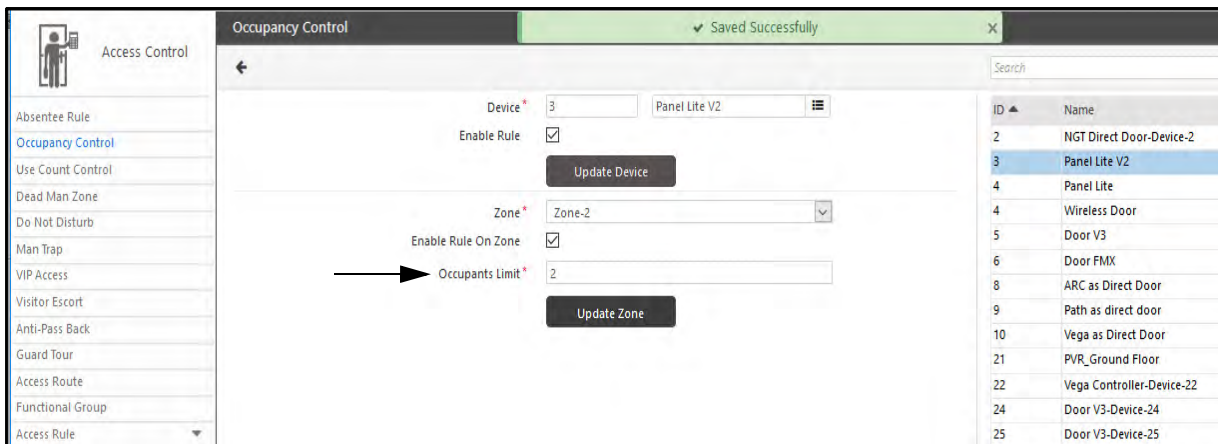
- **Panel200 > Zones> Configuration> Occupancy Control**
- OR
- **Access Control > Occupancy Control**



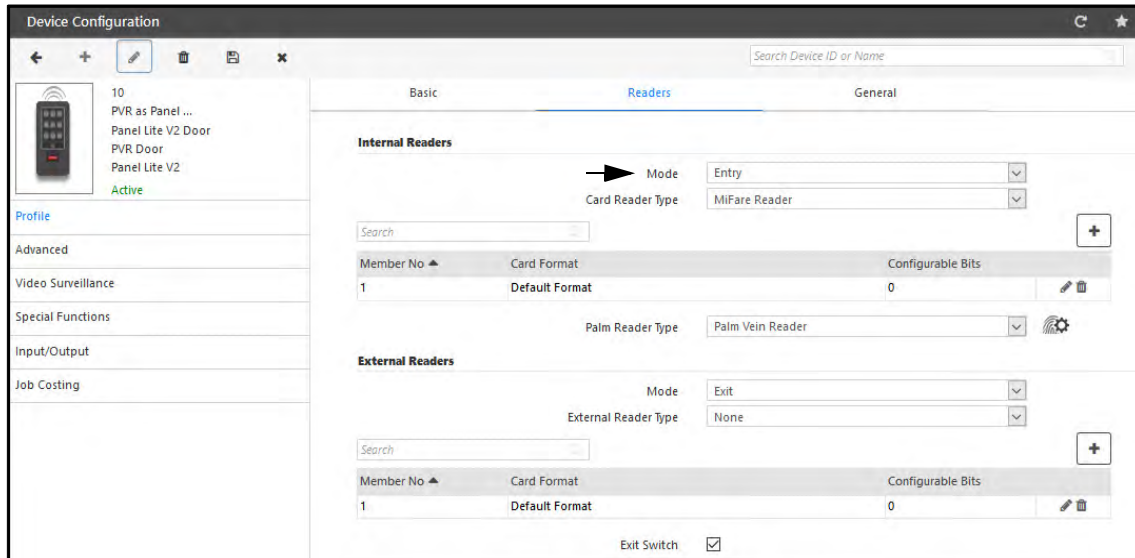
For Single Zone

Consider the following example to understand the functioning of Occupancy Control feature for a single zone.


- The Occupancy Control is enabled on Zone-2 of Panel200 and the Maximum Occupants is configured as 2.



- Now, the PVR door of Zone2 is set with Mode as Entry.



- When User1 and User2 punch on the PVR door, they will be allowed access.
- When User3 punches on PVR door, he/she will be denied access due to occupancy violation as shown below.

User Details		Events					
		Sr No.	Date Time	Type	Device	Category	Detail
 <p>User ID: 101 Khushbu Denied - Occupancy Control</p> <p>Device: Panel Lite V2 -> PVR as Pane</p> <p>Event Date & Time: 19/06/2018 05:32:46 PM</p> <p>Department: DFLTDPF</p> <p>Designation: DFLTDSG</p>		574	19/06/2018 05:32:10 PM	Panel Lite V2	Panel Lite V2	Other	→ Access Zone Configuration Sent. Access Zone No: 2 TID: 1806190040000522
		575	19/06/2018 05:32:10 PM	Panel Lite V2	Panel Lite V2	ACK	← Access Zone Configuration Successful. Access Zone No: 2
		576	19/06/2018 05:32:10 PM	Panel Lite V2	Panel Lite V2	Other	→ Access Zone Configuration Sent. Access Zone No: 3 TID: 1806190040000523
		577	19/06/2018 05:32:10 PM	Panel Lite V2	Panel Lite V2	ACK	← Access Zone Configuration Successful. Access Zone No: 3
		578	19/06/2018 05:32:10 PM	Panel Lite V2	Panel Lite V2	Other	→ Access Cluster Configuration Sent. TID: 1806190040000524
		579	19/06/2018 05:32:10 PM	Panel Lite V2	Panel Lite V2	ACK	← Access Cluster Configuration Successful.
		580	19/06/2018 05:32:10 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
		581	19/06/2018 05:32:21 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	Allowed with Palm. User ID: 1 Event Date Time: 19/06/2018 05:32:20 PM
		582	19/06/2018 05:32:21 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1675
		583	19/06/2018 05:32:26 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	Door	← Door Open/Close - NotOperated. User ID: 1 Event Date Time: 19/06/2018 05:32:25 PM
		584	19/06/2018 05:32:26 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1676
		585	19/06/2018 05:32:42 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	Allowed with Card. User ID: 1687 Event Date Time: 19/06/2018 05:32:41 PM
		586	19/06/2018 05:32:42 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1677
		587	19/06/2018 05:32:47 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	Door	← Door Open/Close - NotOperated. User ID: 1687 Event Date Time: 19/06/2018 05:32:46 PM
		588	19/06/2018 05:32:47 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1678
		589	19/06/2018 05:32:49 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	Denied - Occupancy Control with Palm. User ID: 101 Event Date Time: 19/06/2018 05:32:46 PM
		590	19/06/2018 05:32:49 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1679

For Multiple Zones

Occupancy Control can be applied on each zone separately or occupancy of one zone (**Monitor zone**) can be monitored to control access into another zone (**Control zone**). To know about the detailed configuration, refer to ["Occupancy Control"](#).

Consider the following examples to understand the functioning of Occupancy Control for multiple zones.

Example1:

Let there be two zones,

- Zone 1 - Control Zone - Door V3
- Zone 2 - Monitor Zone - PVR door

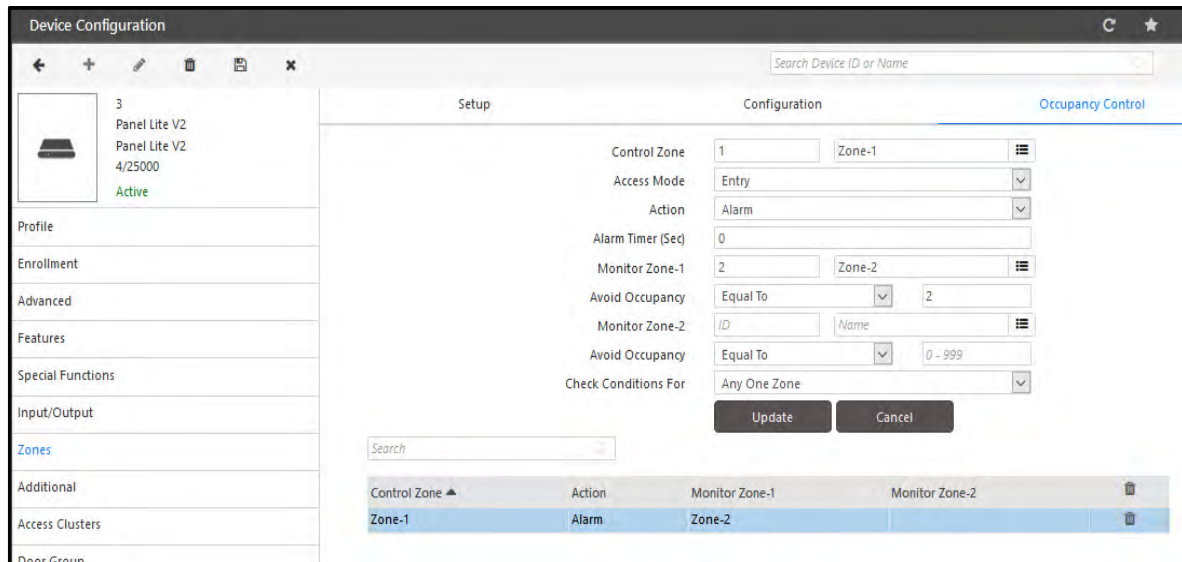
Initially occupancy of both the zones is empty.

Access Mode of both zones is **Entry**.

Action is selected as **Alarm** and Alarm Timer is 0 seconds.

Condition is avoid occupancy equal to 2

In this case, the first user will be allowed to access the monitor zone. When the second user tries to access the monitor zone, he/she will be allowed access but the occupancy rule will be violated. The occupancy violated Alarm will be generated when a user tries to access the control zone.



Example2:

Let there be two zones,

- Zone 1 - Control Zone - Door V3
- Zone 2 - Monitor Zone - PVR door

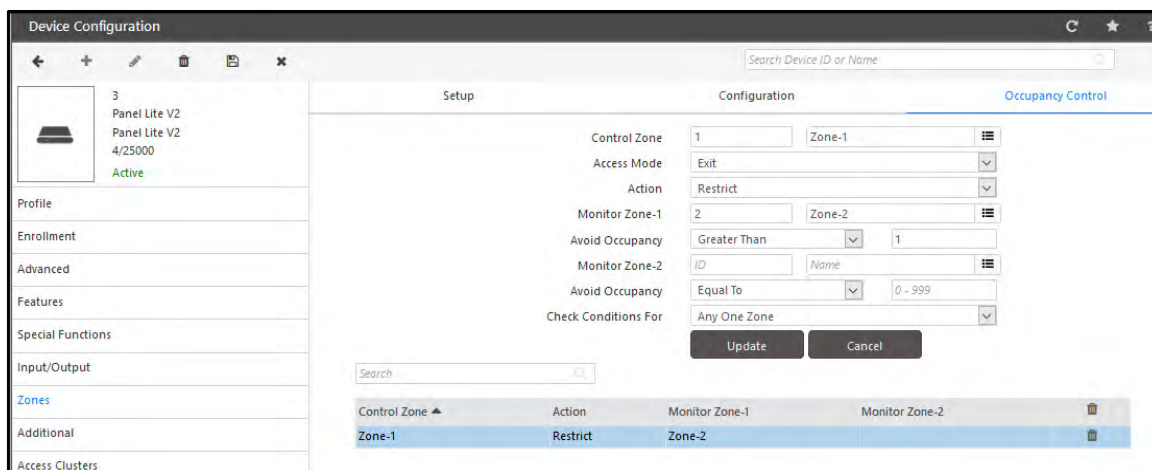
Initially occupancy of both the zones is **zero**.

Access Mode of both zones is **Exit**.

Action is selected as **Restrict**.

Condition is avoid occupancy greater than 1

In this case, the first user will be allowed to access the monitor zone. When the second user tries to access the monitor zone, he/she will be allowed access but the occupancy rule will be violated. When a user tries to access the control zone, he/she will be restricted access due to the violation of occupancy in monitor zone.



Example 3:

Let there be two zones,

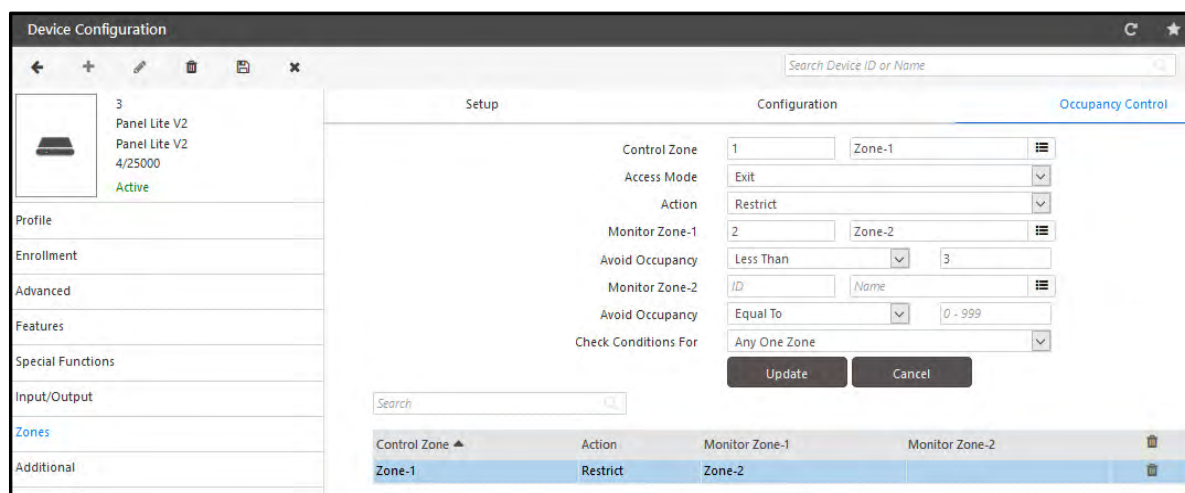
- Zone 1 - Control Zone - Door V3
- Zone 2 - Monitor Zone - PVR door

Occupancy of both zones is 4. User 1 to User 4 are in Monitor Zone while User 5 to User 8 are in Control Zone. Out of all the users, User 4 and User 8 are VIP Users.


Access Mode of both zones is **Exit**. The **Access Control on Exit Mode** check box is enabled for both the zones.


Action is selected as **Restrict**.

Condition is avoid occupancy less than 3.



- In this case, Exit of User 1 from monitor zone is allowed. Exit of User 2 (Normal User) or User 4 (VIP User) from monitor zone will be allowed but it will violate the occupancy.
- When the User 5 tries to exit the control zone, access will be denied to him/her. But at the same time, if User 8 (VIP User) tries to exit from the control zone, access will be allowed to him/her as shown below.

User Details		Events					
 User ID: 101 Khushbu Denied - Occupancy Control Device: Panel Lite V2 -> Door V3 as Par Event Date & Time: 19/06/2018 12:12:15 PM		Sr No.	Date Time	Type	Device	Category	Detail
		106	19/06/2018 12:12:00 PM	Panel Lite V2	Panel Lite V2	ACK	← Set Date & Time Command Successful
		107	19/06/2018 12:12:00 PM	Panel Lite V2	Panel Lite V2	Other	→ Get Information from Device
		108	19/06/2018 12:12:00 PM	Panel Lite V2	Panel Lite V2	Other	← Reply Information from Device
		109	19/06/2018 12:12:00 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
		110	19/06/2018 12:12:06 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Finger. User ID: 1 Event Date Time: 19/06/2018 12:12:05 PM
		111	19/06/2018 12:12:06 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1643
		112	19/06/2018 12:12:11 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Finger. User ID: HR1 [1693] Event Date Time: 19/06/2018 12:12:10 PM
		113	19/06/2018 12:12:11 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1644
		114	19/06/2018 12:12:15 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Door Open/Close - NotOperated. User ID: HR1 [1693] Event Date Time: 19/06/2018 12:12:15 PM
		115	19/06/2018 12:12:16 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1645
		116	19/06/2018 12:12:18 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Denied - Occupancy Control with Finger. User ID: 101 Event Date Time: 19/06/2018 12:12:15 PM
		117	19/06/2018 12:12:18 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1646

User Details		Events					
 User ID: HR1 Ronald Allowed Device: Panel Lite V2 -> Door V3 as Par Event Date & Time: 19/06/2018 12:24:16 PM Department: DLTDPT Designation: DLTDSG		Sr No.	Date Time	Type	Device	Category	Detail
		106	19/06/2018 12:12:00 PM	Panel Lite V2	Panel Lite V2	ACK	← Set Date & Time Command Successful
		107	19/06/2018 12:12:00 PM	Panel Lite V2	Panel Lite V2	Other	→ Get Information from Device
		108	19/06/2018 12:12:00 PM	Panel Lite V2	Panel Lite V2	Other	← Reply Information from Device
		109	19/06/2018 12:12:00 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
		110	19/06/2018 12:12:06 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Finger. User ID: 1 Event Date Time: 19/06/2018 12:12:05 PM
		111	19/06/2018 12:12:06 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1643
		112	19/06/2018 12:12:11 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Finger. User ID: HR1 [1693] Event Date Time: 19/06/2018 12:12:10 PM
		113	19/06/2018 12:12:11 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1644
		114	19/06/2018 12:12:15 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Door Open/Close - NotOperated. User ID: HR1 [1693] Event Date Time: 19/06/2018 12:12:15 PM
		115	19/06/2018 12:12:16 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1645
		116	19/06/2018 12:12:18 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Denied - Occupancy Control with Finger. User ID: 101 Event Date Time: 19/06/2018 12:12:15 PM
		117	19/06/2018 12:12:18 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1646
		118	19/06/2018 12:24:17 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Finger. User ID: HR1 [1693] Event Date Time: 19/06/2018 12:24:16 PM
		119	19/06/2018 12:24:17 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1647
		120	19/06/2018 12:24:22 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Door Open/Close - NotOperated. User ID: HR1 [1693] Event Date Time: 19/06/2018 12:24:21 PM
		121	19/06/2018 12:24:22 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1648

Example 4:

Let there be two zones,

- Zone 1 - Control Zone - Door V3
- Zone 2 - Monitor Zone - PVR door

Initially occupancy of both the zones is **zero**.

Access Mode of both zones is **Entry**.

Action is selected as **Restrict**.

Condition is Avoid occupancy equal to 2 in monitor zone-1 (Zone-2).

Device Configuration

3

Panel Lite V2

Panel Lite V2

14/25000

Active

Profile

Enrollment

Advanced

Features

Special Functions

Input/Output

Zones

Additional

Access Clusters

Door Group

Assign Users

Setup

Configuration

Occupancy Control

Control Zone

1

Zone-1

Access Mode

Entry

Action

Restrict

Monitor Zone-1

2

Zone-2

Avoid Occupancy

Equal To

2

Monitor Zone-2

ID

Name

Avoid Occupancy

Equal To

0 - 999

Check Conditions For

Any One Zone

Update

Cancel

Search

Control Zone

Action

Monitor Zone-1

Monitor Zone-2


Zone-1

Restrict

Zone-2

- In this case, when the User 1 punches on PVR (Zone-2), he/she is allowed access.

- When User 2 punches on PVR (Zone-2), he/she will also be allowed access.
- But, when User 3 punches on Door V3 in control zone (Zone-1), he/she will be restricted access due to the violation of occupancy =2 in monitor zone (Zone-2) as shown below.

User Details		Events					
 User ID: 4 Shinjini Ghosh Denied - Occupancy Control Device: Panel Lite V2 -> Door V3 as P Event Date & Time: 14/06/2018 05:49:04 PM Department: DFLTDPT Designation: DFLTDG		Sr No.	Date Time	Type	Device	Category	Detail
		406	14/06/2018 05:48:28 PM	Panel Lite V2	Panel Lite V2	Other	→ Advance Configuration Sent. TID: 1806140040000146
		407	14/06/2018 05:48:28 PM	Panel Lite V2	Panel Lite V2	ACK	← Advance Configuration Successful.
		408	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	Other	→ Access Zone Configuration Sent. Access Zone No: 1 TID: 1806140040000147
		409	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	ACK	← Access Zone Configuration Successful. Access Zone No: 1
		410	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	Other	→ Access Zone Configuration Sent. Access Zone No: 2 TID: 1806140040000148
		411	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	ACK	← Access Zone Configuration Successful. Access Zone No: 2
		412	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	Other	→ Access Cluster Configuration Sent. TID: 1806140040000149
		413	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	ACK	← Access Cluster Configuration Successful.
		414	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
		415	14/06/2018 05:48:53 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	→ Allowed with Palm. User ID: 1 Event Date Time: 14/06/2018 05:48:51 PM
		416	14/06/2018 05:48:53 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1126
		417	14/06/2018 05:48:58 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	→ Allowed with Palm. User ID: 101 Event Date Time: 14/06/2018 05:48:56 PM
		418	14/06/2018 05:48:58 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1127
		419	14/06/2018 05:49:03 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	Door	← Door Open/Close - NotOperated. User ID: 101 Event Date Time: 14/06/2018 05:49:01 PM
		420	14/06/2018 05:49:03 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1128
		421	14/06/2018 05:49:06 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Denied - Occupancy Control with Finger. User ID: 4 Event Date Time: 14/06/2018 05:49:04 PM
		422	14/06/2018 05:49:06 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1129

- Now, when User 4 punches on PVR Door in Zone-2, he/she will be restricted access as the maximum occupancy limit for Zone-2 is configured as 2 as shown below and User 1 and User 2 are already occupied in Zone-2.

Occupancy Control

Device *

3

Panel Lite V2

Enable Rule

☒

Update Device

Zone *

Zone-2

Enable Rule On Zone

☒


Occupants Limit *

2

Update Zone

Search

ID	Name
2	NGT Direct Door-Device-2
3	Panel Lite V2
4	Panel Lite
4	Wireless Door
5	Door V3
6	Door FMX
8	ARC as Direct Door
9	Path as direct door
10	Vega as Direct Door

User Details		Events					
 User ID: 1687 Aditi Ajay Gupta Denied - Occupancy Control Device: Panel Lite V2 -> PVR as Pane Event Date & Time: 14/06/2018 06:18:49 PM Department: DFLTDPT Designation: DFLTDG		Sr No.	Date Time	Type	Device	Category	Detail
		408	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	Other	→ Access Zone Configuration Sent. Access Zone No: 1 TID: 1806140040000147
		409	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	ACK	← Access Zone Configuration Successful. Access Zone No: 1
		410	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	Other	→ Access Zone Configuration Sent. Access Zone No: 2 TID: 1806140040000148
		411	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	ACK	← Access Zone Configuration Successful. Access Zone No: 2
		412	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	Other	→ Access Cluster Configuration Sent. TID: 1806140040000149
		413	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	ACK	← Access Cluster Configuration Successful.
		414	14/06/2018 05:48:29 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
		415	14/06/2018 05:48:53 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	→ Allowed with Palm. User ID: 1 Event Date Time: 14/06/2018 05:48:51 PM
		416	14/06/2018 05:48:53 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1126
		417	14/06/2018 05:48:58 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	→ Allowed with Palm. User ID: 101 Event Date Time: 14/06/2018 05:48:56 PM
		418	14/06/2018 05:48:58 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1127
		419	14/06/2018 05:49:03 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	Door	← Door Open/Close - NotOperated. User ID: 101 Event Date Time: 14/06/2018 05:49:01 PM
		420	14/06/2018 05:49:03 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1128
		421	14/06/2018 05:49:06 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Denied - Occupancy Control with Finger. User ID: 4 Event Date Time: 14/06/2018 05:49:04 PM
		422	14/06/2018 05:49:06 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1129
		423	14/06/2018 06:18:50 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	→ Denied - Occupancy Control with Card. User ID: 1687 Event Date Time: 14/06/2018 06:18:49 PM
		424	14/06/2018 06:18:50 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1130



The IN- OUT punches are stored in memory of Panel200. Re-booting the Panel/Panel Doors will not reset the Occupancy Count to zero.

If there are entry punches in a zone so zone will be occupied. There must be exit punch from the reader or from door in Exit mode to decrease the occupancy from the zone.

Example5:

Consider the above example 4 with change in Action as Alarm.

Action is selected as **Alarm** with Alarm Timer as 2 seconds. This will activate the alarm after 2 seconds of user access in control zone when the occupancy is violated in monitor zone.

The screenshot shows the 'Device Configuration' window for a 'Panel Lite V2' device. The 'Occupancy Control' tab is active. The configuration includes:

- Control Zone:** 1, Zone-1
- Access Mode:** Entry
- Action:** Alarm (indicated by an arrow)
- Alarm Timer (Sec):** 2 (indicated by an arrow)
- Monitor Zone-1:** 2, Zone-2
- Avoid Occupancy:** Equal To, 2
- Monitor Zone-2:** ID, Name
- Avoid Occupancy:** Equal To, 0 - 999
- Check Conditions For:** Any One Zone

Buttons for 'Update' and 'Cancel' are at the bottom right. A table at the bottom shows the configuration for 'Zone-1' and 'Zone-2'.

Control Zone	Action	Monitor Zone-1	Monitor Zone-2
Zone-1	Restrict	Zone-2	

- In this case, when User 1 and User 2 punch on PVR door, they will be allowed access.
- But, when User 3 punches on Door V3 then he/she will be allowed access. But after 2 seconds, alarm will be generated as shown below.

Matrix COSEC MONITOR

File Device Tools Help

Features

- Alarms
- I/O Link
- Soft Override
- Events
- Exceptions
- Time Triggered Functions
- EMAP

Devices - All 1 10

Name	Site	IP/RS485 Address	MAC Address	Type	Status
Panel Lite V2		192.168.104.111	00:1B:09:04:65:D1	Panel Lite V2	Connected
ARC as Single Door	Site-2	192.168.105.3	DF:E3:65:54:34:44	Panel Lite V2 Door	OFF-Line
Dummy Door	Site-1	192.111.111.111	11:11:11:11:11:11	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-2	192.168.105.5	DF:E6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-2	192.168.105.5	DF:E6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-2	192.168.105.6	FE:47:48:46:74:69	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.6	FE:47:48:46:74:69	Panel Lite V2 Door	OFF-Line
Both as Dual door	Site-1	192.168.105.7	EE:66:7A:6A:00:9C	Panel Lite V2 Door	OFF-Line

User Details

User ID: 1
Chirag
Allowed

Device: Panel Lite V2 -> Door V3 as P
Event Date & Time: 14/06/2018 06:51:49 PM
Department: DFLTDPT
Designation: DFLTDG

Events

Sr No.	Date Time	Type	Device	Category	Detail
571	14/06/2018 06:50:03 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
572	14/06/2018 06:50:12 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	→ Allowed with Palm. User ID: 1 Event Date Time: 14/06/2018 06:50:11 PM
573	14/06/2018 06:50:12 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1139
574	14/06/2018 06:50:17 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	Door	← Door Open/Close - NotOperated. User ID: 1 Event Date Time: 14/06/2018 06:50:16 PM
575	14/06/2018 06:50:17 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1140
576	14/06/2018 06:50:19 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	→ Allowed with Palm. User ID: 101 Event Date Time: 14/06/2018 06:50:17 PM
577	14/06/2018 06:50:19 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1141
578	14/06/2018 06:50:22 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	Door	← Door Open/Close - NotOperated. User ID: 101 Event Date Time: 14/06/2018 06:50:22 PM
579	14/06/2018 06:50:22 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1142
580	14/06/2018 06:51:50 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed with Finger. User ID: 1 Event Date Time: 14/06/2018 06:51:49 PM
581	14/06/2018 06:51:50 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1143
582	14/06/2018 06:51:52 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Alarm	← Occupancy Violated - User ID: 1 Event Date Time: 14/06/2018 06:51:51 PM
583	14/06/2018 06:51:52 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1144
584	14/06/2018 06:51:52 PM	Panel Lite V2	Panel Lite V2	System	← User Blocked - Occupancy Violated User ID: 1 Event Date Time: 14/06/2018 06:51:51 PM
585	14/06/2018 06:51:52 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1145
586	14/06/2018 06:51:55 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Door Open/Close - NotOperated. User ID: 1 Event Date Time: 14/06/2018 06:51:54 PM
587	14/06/2018 06:51:55 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1146

Matrix COSEC MONITOR

File Device Tools Help

Features

- Alarms
- I/O Link
- Soft Override
- Events
- Exceptions
- Time Triggered Functions
- EMAP

Devices - All 1 10

Name	Site	IP/RS485 Address	MAC Address	Type	Status
Panel Lite V2		192.168.104.111	00:1B:09:04:65:D1	Panel Lite V2	Connected
ARC as Single Door	Site-2	192.168.105.3	DF:E3:65:54:34:44	Panel Lite V2 Door	OFF-Line
Dummy Door	Site-1	192.111.111.111	11:11:11:11:11:11	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-2	192.168.105.5	DF:E6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-2	192.168.105.5	DF:E6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-2	192.168.105.6	FE:47:48:46:74:69	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.6	FE:47:48:46:74:69	Panel Lite V2 Door	OFF-Line
Both as Dual door	Site-1	192.168.105.7	EE:66:7A:6A:00:9C	Panel Lite V2 Door	OFF-Line

User Details

User ID: 1
Chirag
Allowed

Alarms

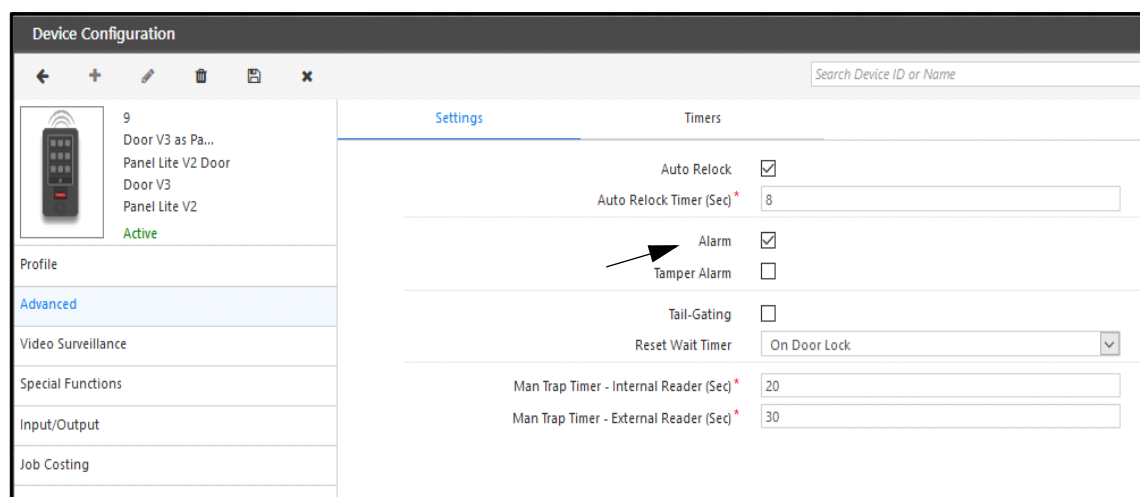
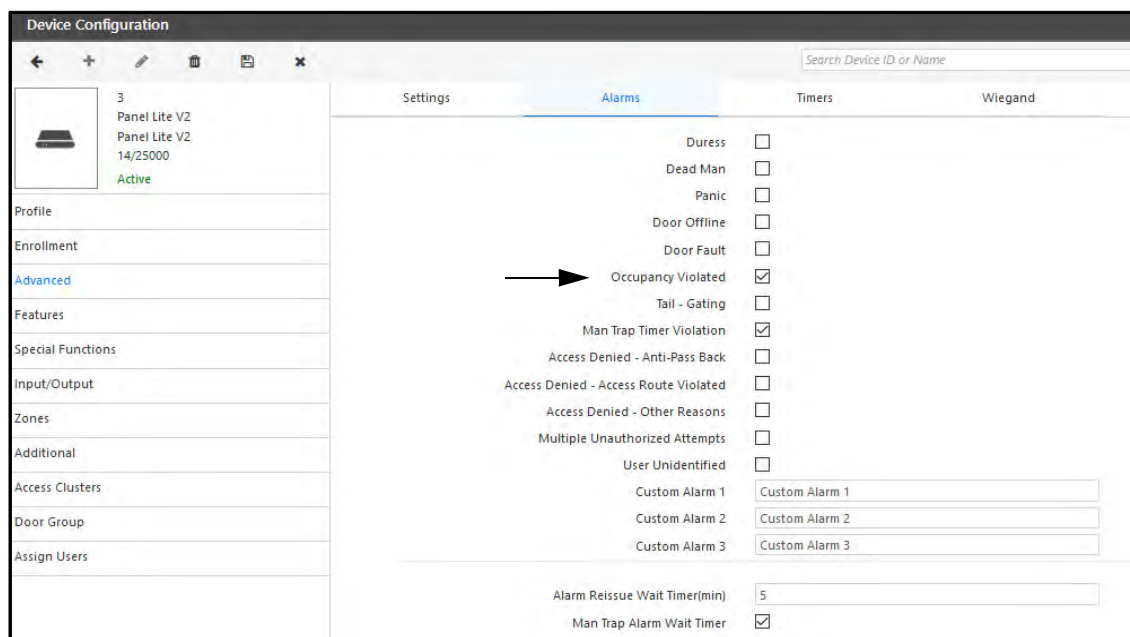
Device	Type	Description	Level	Status	Alarm Date Time
Panel Lite V2 -> Door V3...	Panel Lite V2 ...	Occupancy Violated	Major	New	14/06/2018 06:51:51 PM

Context Menu:

- Acknowledge
- Acknowledge All
- Clear
- Clear All
- Cancel

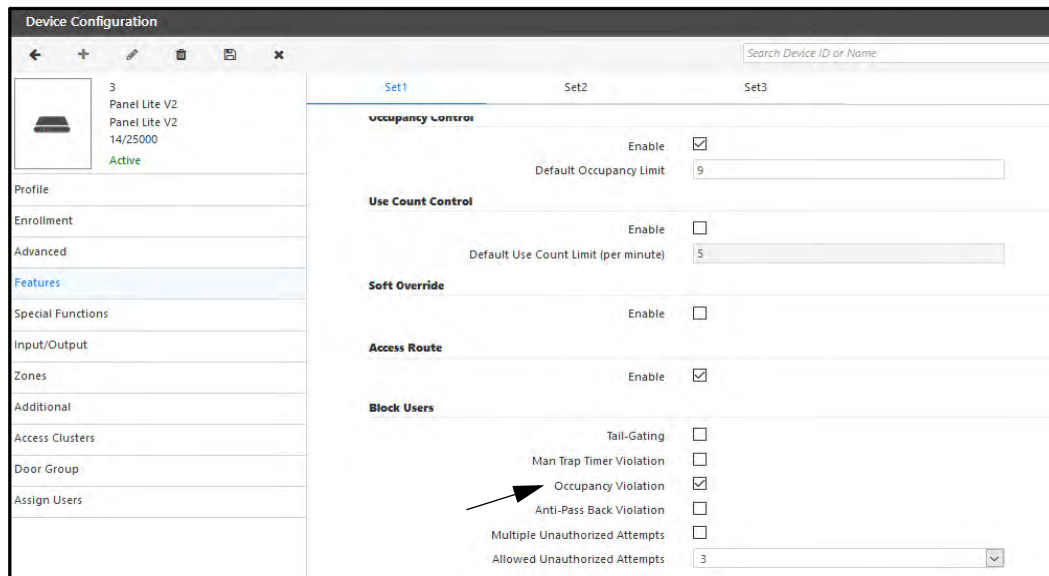
For occupancy violation Alarm to generate, you must enable Alarms from both Panel200 and Panel door.

- Panel200> Advanced> Alarms> Occupancy Violated
- Panel door (in Control zone i.e. Door V3 here) > Advanced > Settings> Alarm



If you want to block the user who is violating occupancy rule, then enable the Occupancy Violation check-box for Block Users in Panel200> Features> Set1 as shown below.

This will block the user and you will have to restore back the user from Block Users page.



Example6:

Let there be 3 zones of Panel200:

- Zone 1 - Control Zone - Door V3
- Zone 2 - Monitor Zone1- PVR Door
- Zone-3- Monitor Zone 2- Door V3-115

Initially occupancy of all the zones is empty. Access Mode of all zones is Entry. (Configure Access Mode from Panel doors> Reader section.)

Access mode is selected as Entry. This is the access mode of user in control zone (Zone-1) for which the Action (Alarm/ Restrict) is to be taken.

Action is selected as Alarm and Alarm Timer is set as 2 seconds. This will activate the alarm after 2 seconds of user access in control zone when the occupancy is violated in monitor zone.

Condition for Monitor Zone 1 condition is Avoid Occupancy equal to 2. For Monitor Zone 2 condition is Avoid occupancy greater than 1.

If **Check Conditions For** is selected as

- **Any One Zone** then occupancy Condition will be checked for any one zone. If occupancy is violated in either of the monitor zone then Alarm will be generated after the duration of Alarm Timer when the user punches in Control zone.
- If **Both Zones** is selected then occupancy Condition will be checked for both the zones. The alarm will be generated in control zone if occupancy is violated in both the monitor zones.

Control Zone	Action	Monitor Zone-1	Monitor Zone-2
Zone-1	Alarm	Zone-2	Zone-3

- When User 1 punches on Door V3-115 (Zone-3), he/she will be allowed access. When User 2 punches on Door V3-115 (Zone-3), he/she will be also be access allowed. But this is violating Occupancy >1.
- Now when User 3 punches on Door V3 (Zone-1) then he/she will be allowed access but after 2 seconds alarm will be generated as shown below.

Sr No.	Date Time	Type	Device	Category	Detail
1708	18/06/2018 12:50:41 PM	Panel Lite V2	Panel Lite V2	Other	→ Access Cluster Configuration Sent. TID: 1806180040000625
1709	18/06/2018 12:50:41 PM	Panel Lite V2	Panel Lite V2	ACK	← Access Cluster Configuration Successful.
1710	18/06/2018 12:50:41 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
1711	18/06/2018 12:50:49 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed with Finger. User ID: 101 Event Date Time: 18/06/2018 12:50:48 PM
1712	18/06/2018 12:50:49 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1283
1713	18/06/2018 12:50:54 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed with Finger. User ID: 1 Event Date Time: 18/06/2018 12:50:52 PM
1714	18/06/2018 12:50:54 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1284
1715	18/06/2018 12:50:59 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	→ Door Open/Close - NotOperated. User ID: 1 Event Date Time: 18/06/2018 12:50:57 PM
1716	18/06/2018 12:50:59 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1285
1717	18/06/2018 12:51:16 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed with Finger. User ID: 1 Event Date Time: 18/06/2018 12:51:15 PM
1718	18/06/2018 12:51:16 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1286
1719	18/06/2018 12:51:18 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1287
1720	18/06/2018 12:51:18 PM	Panel Lite V2	Panel Lite V2	System	← User Blocked - Occupancy Violated User ID: 1 Event Date Time: 18/06/2018 12:51:17 PM
1721	18/06/2018 12:51:18 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Alarm	← Occupancy Violated - User ID: 1 Event Date Time: 18/06/2018 12:51:17 PM
1722	18/06/2018 12:51:18 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1288
1723	18/06/2018 12:51:21 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	→ Door Open/Close - NotOperated. User ID: 1 Event Date Time: 18/06/2018 12:51:20 PM
1724	18/06/2018 12:51:21 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 1289



Similarly if Action is Restrict; then User 3 will be denied access on Door V3.

If Check Conditions For is Both Zones, then occupancy in PVR door will also be monitored.

Use Count Control

Use Count Control feature enables the system to set the maximum number of times an authorized user can use his/her credential in order to enter/exit a controlled area within a minute, after which the credentials are blocked.

For example: If the use count per minute is set as 5, a valid user can access the door, that is, can mark the punch for entry/exit only 5 times in a minute. If the user punches for 6th time in a minute, his/her credentials will be blocked. The user will need to restore the credentials before using them again.



*This functionality can also be enabled from the **Device Module > Device Configuration > Features** option.*


To set the Use Count Control,

- Click **Access Control > Use Count Control**. The **Use Count Control** page appears.

ID	Name
2	NGT Direct Door-Device-2
3	Panel Lite V2
4	Panel Lite
4	Wireless Door
5	Door V3
6	Door FMX
8	ARC as Direct Door
9	Path as direct door
10	Vega as Direct Door
12	PVR Door-Device-12

The grid on the right hand side of the page displays the list of the devices configured with Advance Access Control System.

Configure the following parameters:

- **Device:** Select the required device using the **Device**  picklist.
- **Enable Rule:** Select the check box to enable the rule on the selected device.
- **Use Count per Minute:** Specify the number of counts (entry /exit) allowed per minute.
- Click **Update Device** to enable the rule on the device.

Example of Use Count Control for Direct Door

Consider the following scenario where a NGT Direct Door is enabled for Use Count Control with Use Count per minute as 3.

Use Count Control ✔ Saved Successfully

Device * NGT Direct Door-Device-2

Enable Rule ☒

Use Count Per Minute *

Update Device

Search

ID	Name
2	NGT Direct Door-Device-2
3	Panel Lite V2
4	Panel Lite
4	Wireless Door
5	Door V3
6	Door FMX
8	ARC as Direct Door
9	Path as direct door
10	Vega as Direct Door
12	PVR Door-Device-12

- The User 1 is assigned the NGT direct door on which Use Count Control rule is enabled.

User Configuration

1 Chirag
Active

Profile

Devices

Credentials

Group

T&A

Access Control

ESS

Assign Configure

Device Group

ID Name

Device


ID Name

Search

Device Name	Type	Restrict Access	Restrict Attendance	
NGT Direct Door-Device-2	NGT Direct Door	<input type="checkbox"/>	<input type="checkbox"/>	
Panel Lite V2	Panel Lite V2	<input type="checkbox"/>	<input type="checkbox"/>	
PVR Door-Device-12	PVR Door	<input type="checkbox"/>	<input type="checkbox"/>	

- When User 1 punches on the door, he/she will be allowed access for 3 times including entry and exit punches. But when he/she punches for the 4th time in 1 minute, he/she will be denied access and user will be blocked.

User Details



User ID: 1
Chirag

Denied - Blocked User

Device:
NGT Direct Door-Device-2

Event Date & Time:
24/05/2018 12:51:57 PM

Department:
DFLTDP

Designation:
DFLTDSG

Events

Sr No.	Date Time	Type	Device	Category	Detail
38	24/05/2018 12:50:46 PM	NGT Direct Door	NGT Direct Door-Device-2	Other	→ End Of Message
39	24/05/2018 12:50:56 PM	PVR Door	PVR Door-Device-12	User	Allowed with Palm. User ID: 102 [1689] Event Date Time: 24/05/2018 12:50:55 PM
40	24/05/2018 12:50:56 PM	PVR Door	PVR Door-Device-12	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 92
41	24/05/2018 12:51:37 PM	NGT Direct Door	NGT Direct Door-Device-2	Request	← Message Request Received
42	24/05/2018 12:51:37 PM	NGT Direct Door	NGT Direct Door-Device-2	Other	→ Advance Configuration Sent. TID: 1805240040000003
43	24/05/2018 12:51:37 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	← Advance Configuration Successful.
44	24/05/2018 12:51:37 PM	NGT Direct Door	NGT Direct Door-Device-2	Other	→ End Of Message
45	24/05/2018 12:51:42 PM	NGT Direct Door	NGT Direct Door-Device-2	User	Allowed with Finger. User ID: 1 Event Date Time: 24/05/2018 12:51:42 PM
46	24/05/2018 12:51:42 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 220
47	24/05/2018 12:51:47 PM	NGT Direct Door	NGT Direct Door-Device-2	User	Allowed with Finger. User ID: 1 Event Date Time: 24/05/2018 12:51:47 PM
48	24/05/2018 12:51:47 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 221
49	24/05/2018 12:51:52 PM	NGT Direct Door	NGT Direct Door-Device-2	User	Allowed with Finger. User ID: 1 Event Date Time: 24/05/2018 12:51:52 PM
50	24/05/2018 12:51:52 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 222
51	24/05/2018 12:51:57 PM	NGT Direct Door	NGT Direct Door-Device-2	System	← User Blocked - Usage Count User ID: 1 Event Date Time: 24/05/2018 12:51:57 PM
52	24/05/2018 12:51:57 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 223
53	24/05/2018 12:51:57 PM	NGT Direct Door	NGT Direct Door-Device-2	User	Denied - Blocked User with Finger. User ID: 1 Event Date Time: 24/05/2018 12:51:57 PM
54	24/05/2018 12:51:57 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 224

- The user will be blocked and listed in Blocked User list. The user must be restored to be allowed to punch on the NGT Direct Door.

Blocked User						
Blocked User (1)						
Search						
ID	Name	Panel/Direct Door	Block DateTime	Reason for Block	Remark	Restore
1	Chirag	NGT Direct Door-Device-2	24/05/2018 12:51:57	Usage Count		
Restored User (0)						

Example of Use Count Control for Panel Door

Consider the following scenario where a Panel200 is enabled for Use Count Control with Use Count per minute as 3. When Use Count Control is enabled on Panel200, the use count on each of its doors will be monitored.

Use Count Control

✓ Saved Successfully

Device *

3

Panel Lite V2

Enable Rule

☒

Use Count Per Minute *

3


Update Device

ID	Name
2	NGT Direct Door-Device-2
3	Panel Lite V2
4	Panel Lite
4	Wireless Door
5	Door V3
6	Door FMX
8	ARC as Direct Door
9	Path as direct door
10	Vega as Direct Door

- If Door V3 and PVR are connected to Panel200. The maximum use count on each door will be set as 3.

Device Status							
Search							
Filter List		Device Type	Device Status		Group By		
		All	Connected/Online		None		
Name	Status	IP	MAC Address	Device Type	Site		
Panel Lite V2	Connected	192.168.104.111	00:1B:09:04:65:D1	Panel Lite V2			
Door V3 as Panel Door	Online	192.168.104.114	00:1B:09:05:3F:E2	Panel Lite V2 Door			
PVR as Panel Door	Online	192.168.104.113	00:1B:09:03:F2:B0	Panel Lite V2 Door			

- When a user who is assigned with the Panel punches on any of the connected doors for the 4th time in 1 minute, he will be blocked and denied access on all doors of Panel200.



User ID: 1

Chirag

Denied - Blocked User

Device:
Panel Lite V2 -> PVR as Pane

Event Date & Time:
24/05/2018 05:08:38 PM

Department:
DFLDPT

Designation:
DFLTDSG

Events

Sr No.	Date Time	Type	Device	Category	Detail
280	24/05/2018 05:07:45 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 193
281	24/05/2018 05:07:45 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
282	24/05/2018 05:07:52 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	→ Allowed with Palm. User ID: 1 Event Date Time: 24/05/2018 05:07:51 PM
283	24/05/2018 05:07:52 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 194
284	24/05/2018 05:07:54 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	→ Allowed with Palm. User ID: 1 Event Date Time: 24/05/2018 05:07:53 PM
285	24/05/2018 05:07:54 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 195
286	24/05/2018 05:08:02 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed with Finger. User ID: 1 Event Date Time: 24/05/2018 05:08:00 PM
287	24/05/2018 05:08:02 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 196
288	24/05/2018 05:08:08 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed with Finger. User ID: 1 Event Date Time: 24/05/2018 05:08:06 PM
289	24/05/2018 05:08:08 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 197
290	24/05/2018 05:08:12 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed with Finger. User ID: 1 Event Date Time: 24/05/2018 05:08:10 PM
291	24/05/2018 05:08:12 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 198
292	24/05/2018 05:08:17 PM	Panel Lite V2	Panel Lite V2	System	← User Blocked - Usage Count User ID: 1 Event Date Time: 24/05/2018 05:08:15 PM
293	24/05/2018 05:08:17 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 199
294	24/05/2018 05:08:17 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Denied - Blocked User with Finger. User ID: 1 Event Date Time: 24/05/2018 05:08:15 PM
295	24/05/2018 05:08:17 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 200
296	24/05/2018 05:08:37 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	→ Denied - Blocked User with Palm. User ID: 1 Event Date Time: 24/05/2018 05:08:36 PM
297	24/05/2018 05:08:38 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 201

- The user will be blocked and listed in Blocked User list. The user must be restored from the Blocked List to be able to punch on the NGT Direct Door again.

Blocked User						
Blocked User (2)						
Search						
ID ▲	Name	Panel/Direct Door	Block DateTime	Reason for Block	Remark	Restore
1	Chirag	NGT Direct Door-Device-2	24/05/2018 12:51:57	Usage Count		↺
1	Chirag	Panel Lite V2	24/05/2018 15:58:56	Usage Count		↺
Restored User (0)						

Blocked User (1)					
Restored User (1)					
Search					
ID ▲	Name	Panel/Direct Door	Application Restore DateTime	Controller Restore DateTime	Remark
1	Chirag	Panel Lite V2	24/05/2018 16:01:15		

Dead Man Zone

Dead Man Zone feature enables the system to track the safety and security of a user while performing a task in a risky environment. The user is expected to come out of the zone at predefined intervals (Dead Man time period) to show his/her card/credential.



*This functionality can also be enabled from the **Device Module > Device Configuration > Features** option.*


To set the Dead Man Zone,

- Click **Access Control > Dead Man Zone**. The **Dead Man Zone** page appears.

ID	Name
3	Panel Lite V2
4	Panel Lite

The grid on the right hand side of the page displays the list of the Panel devices configured with Advance Access Control System.

Configure the following parameters:

- **Device:** Select the required device using the **Device**  picklist.
- **Enable Rule:** Select the check box to enable the rule on the selected device.
- Click **Update Device** to enable the rule on the device.

Once you update the device, you can configure the following parameters:

- **Zone:** Select the Zone on which you want to enable the rule.
- **Enable Rule on Zone:** Select the check box to enable the rule on the zone.
- **Warning Timer (Min):** Specify the Dead Man Time/Warning Time within which any user inside the zone must show the credentials.
- **Alert Timer (Min):** Specify the time for which a user is allowed to stay in the Dead Man Zone.



Dead Man Alarm is generated when the person working in restricted environment does not come out of the Dead Man Zone within a pre-defined Warning time i.e. when the presence of user is not marked.

- Click on **Update Zone** to save the changes.

When any user enters into the zone, the Warning timer and the Alert timer start. If the user comes out of the zone within the Alert time, the Alarm will reset. If the user fails to exit the Dead Man Zone within the Alert time, the Alarm will be generated.

For a Panel device, the Dead Man Zone can be activated when you select **Activate Dead-Man** from **Device module > Device Configuration (Panel200/Panel/Panel Lite) > Special Functions**.

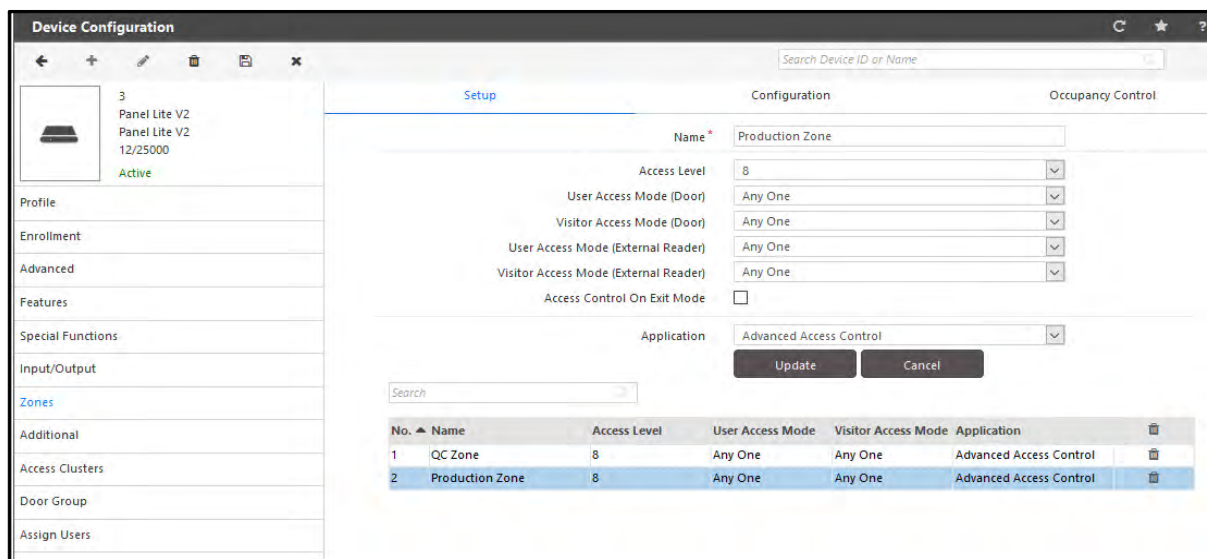
Create a users group (For example: Admin). Users belonging to Admin functional group can activate this feature using the card enrolled for this feature. You can enroll special function card from Users> Credential Management> Enrollment> Special Card.

No.	Function Name	Active	User Group	Card-1	Card-2	Card-3	Card-4	
16	Late IN - Start	Yes	Staff					
17	Late IN - Stop	Yes	Staff					
18	Early OUT - Start	Yes	Staff					
19	Early OUT - Stop	Yes	Staff					
20	View User Profile	Yes	Staff					
21	Activate DND	Yes	Staff					
22	Deactivate DND	Yes	Staff					
23	Activate Dead-Man	<input checked="" type="checkbox"/>	Admin					<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
24	Deactivate Dead-Man	Yes	Staff					
25	Door Lock	Yes	Staff					
26	Door Unlock	Yes	Staff					
27	Door Normal	Yes	Staff					
28	Zone Lock	Yes	Staff					

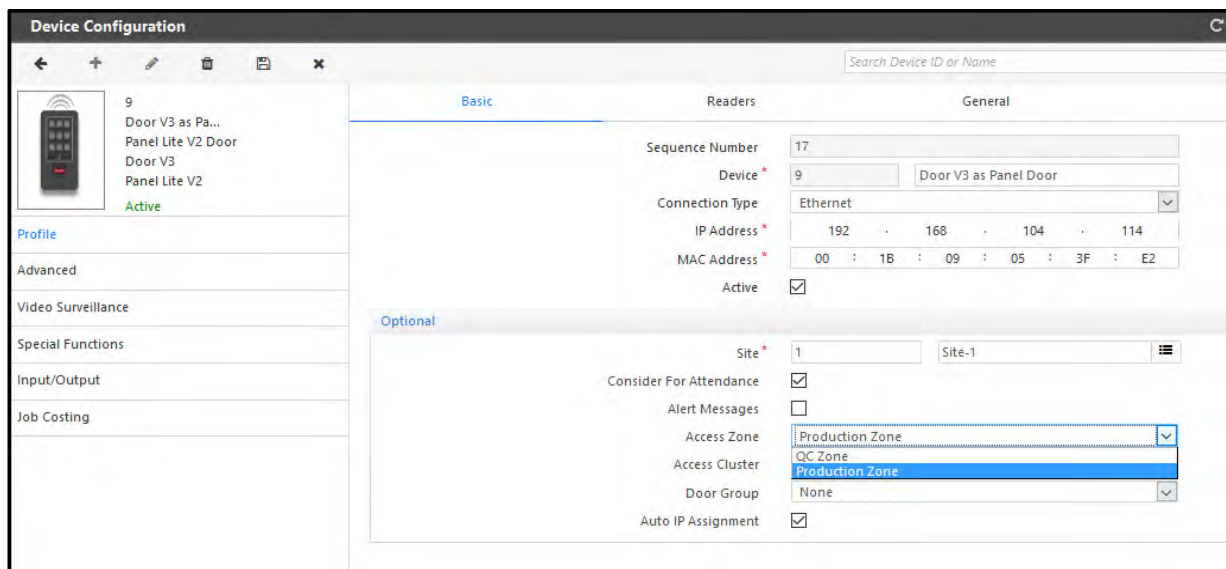
Example of Dead Man Zone - Panel device.

Consider the following scenario where a Panel200 has a Door V3 connected to it. Dead Man Zone is enabled for the Panel200.

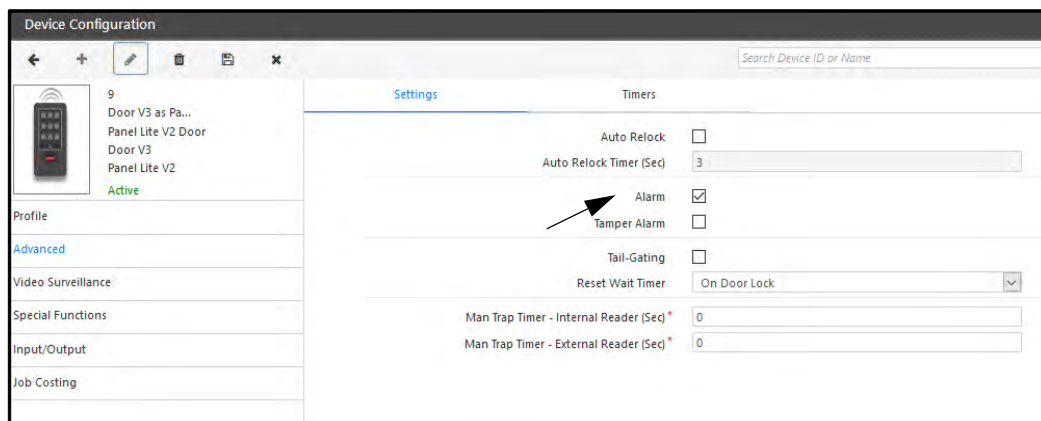
The Dead Man Zone is activated for Production Zone on the Panel.



Now the Access Zone for Panel Door, that is Door V3 must be set as Production zone as shown below.



You must activate the Alarm for the Door V3.



9

Door V3 as Pa...

Panel Lite V2 Door

Door V3

Panel Lite V2

Active

Profile

Advanced

Video Surveillance

Special Functions

Input/Output

Job Costing

Basic

Readers

General

Internal Readers

Mode

Entry

Card Reader Type

EM Prox Reader

Search

Member No

Card Format

Configurable Bits

1

Default Format

0

Finger Reader Type

Finger Reader

External Readers

Mode

Exit

External Reader Type

Combo Exit Reader

Search

Member No

Card Format

Configurable Bits

1

Default Format

0


Exit Switch

☒



The events will be displayed in the Monitor as below.

User Details



User ID: 1

Chirag

Allowed - Dead Man Zone

Device:

Panel Lite V2 -> Door V3 as F

Event Date & Time:

22/05/2018 01:54:16 PM

Department:

DFLTDTPT

Designation:

DFLTDSG

Sr No.	Date Time	Type	Device	Category	Detail
130	22/05/2018 01:01:24 PM	Panel Lite V2	Panel Lite V2	Other	→ External Reader Configuration Sent. TID: 1805220040000217
131	22/05/2018 01:01:24 PM	Panel Lite V2	Panel Lite V2	ACK	← External Reader Configuration Successful.
132	22/05/2018 01:01:24 PM	Panel Lite V2	Panel Lite V2	Other	→ External Reader Configuration Sent. TID: 1805220040000218
133	22/05/2018 01:01:24 PM	Panel Lite V2	Panel Lite V2	ACK	← External Reader Configuration Successful.
134	22/05/2018 01:01:24 PM	Panel Lite V2	Panel Lite V2	Other	→ External Reader Configuration Sent. TID: 1805220040000219
135	22/05/2018 01:01:24 PM	Panel Lite V2	Panel Lite V2	ACK	← External Reader Configuration Successful.
136	22/05/2018 01:01:24 PM	Panel Lite V2	Panel Lite V2	Other	→ External Reader Configuration Sent. TID: 1805220040000220
137	22/05/2018 01:01:24 PM	Panel Lite V2	Panel Lite V2	ACK	← External Reader Configuration Successful.
138	22/05/2018 01:01:24 PM	Panel Lite V2	Panel Lite V2	Other	→ External Reader Configuration Sent. TID: 1805220040000221
139	22/05/2018 01:01:24 PM	Panel Lite V2	Panel Lite V2	ACK	← External Reader Configuration Successful.
140	22/05/2018 01:01:24 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
141	22/05/2018 01:54:17 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 51
142	22/05/2018 01:54:16 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Dead man timer changed - Activated Event Date Time: 22/05/2018 01:54:16 PM
143	22/05/2018 01:54:17 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed - Dead Man Zone with Finger. User ID: 1 Event Date Time: 22/05/2018 01:54:16 PM
144	22/05/2018 01:54:17 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 52
145	22/05/2018 01:54:30 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Dead man timer changed - Deactivated Event Date Time: 22/05/2018 01:54:29 PM
146	22/05/2018 01:54:30 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 53

1305

Matrix COSEC MONITOR

File Device Tools Help

Features

- Alarms
- I/O Link
- Soft Override
- Events
- Exceptions
- Time Triggered Functions
- EMAP

Devices - All 3 7

Name	Site	IP/RS485 Address	MAC Address	Type	Status
Panel Lite V2		192.168.104.111	00:1B:09:04:65:D1	Panel Lite V2	Connected
ARC as Single Door	Site-1	192.168.105.3	DF:E3:65:54:3A:44	Panel Lite V2 Door	OFF-Line
Dummy Door	Site-1	192.111.111.111	11:11:11:11:11:11	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-1	192.168.105.5	DF:E6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-1	192.168.105.5	DF:E6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.6	FE:47:48:46:74:69	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.6	FE:47:48:46:74:69	Panel Lite V2 Door	OFF-Line
Both as Dual door	Site-1	192.168.105.7	EE:E6:7A:8A:0A:8E	Panel Lite V2 Door	OFF-Line

User Details

User ID: 1
Chirag

Allowed - Dead Man Zone

Device: Panel Lite V2 -> Door V3 as F

Event Date & Time: 22/05/2018 02:05:18 PM

Department: DFLTDPT

Designation: DFLTDG

Events

Sr No.	Date Time	Type	Device	Category	Detail
170	22/05/2018 02:03:55 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
171	22/05/2018 02:04:23 PM	NGT Direct Door	NGT Direct Door-Device-2	Request	← Login Request Received.
172	22/05/2018 02:04:23 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	→ Login Success Poll Duration: 3 Poll Interval: 2
173	22/05/2018 02:04:23 PM	NGT Direct Door	NGT Direct Door-Device-2	Request	← Message Request Received
174	22/05/2018 02:04:23 PM	NGT Direct Door	NGT Direct Door-Device-2	Command	→ Event Request for RollOver: 0 Event Seq. No.: 212
175	22/05/2018 02:04:23 PM	NGT Direct Door	NGT Direct Door-Device-2	Other	← Start Of Event
176	22/05/2018 02:04:23 PM	NGT Direct Door	NGT Direct Door-Device-2	Command	→ Set Date & Time
177	22/05/2018 02:04:23 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	← Set Date & Time Command Successful
178	22/05/2018 02:04:23 PM	NGT Direct Door	NGT Direct Door-Device-2	Other	→ End Of Message
179	22/05/2018 02:05:19 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Dead man timer changed - Activated Event Date Time: 22/05/2018 02:05:18 PM
180	22/05/2018 02:05:19 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 57
181	22/05/2018 02:05:19 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed - Dead Man Zone with Finger: User ID: 1 Event Date Time: 22/05/2018 02:05:18 PM
182	22/05/2018 02:05:19 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 58
183	22/05/2018 02:06:19 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 59
184	22/05/2018 02:06:19 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Alarm	← Dead man timer expired Alarm - User IN - User ID: 1 Event Date Time: 22/05/2018 02:06:18 PM
185	22/05/2018 02:06:19 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Dead man timer changed - Deactivated Event Date Time: 22/05/2018 02:06:18 PM
186	22/05/2018 02:06:19 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 60

The description of Alarm is shown below. You can acknowledge the Alarm by right clicking on the Alarm. The Alarm will be re-issued after the Alarm Re-issue Wait Timer (default 5 mins). You can also clear the Alarm.

User Details

User ID: 1
Chirag

Allowed - Dead Man Zone

Device: Panel Lite V2 -> Door V3 as F

Event Date & Time: 22/05/2018 02:05:18 PM

Department: DFLTDPT

Designation: DFLTDG

Alarms

Device	Type	Description	Level	Status	Alarm Date Time
Panel Lite V2 -> Door V3...	Panel Lite V2...	Dead man timer expired Alarm - User IN	Critical	New	22/05/2018 02:06:18 PM

After the expiry of Alert Timer duration; the Dead Man Zone violation alert will be sent as SMS and Email to the configured user if the Alert Message Configuration is done for Dead Man Zone Violation. For details, refer to ["Configuring Alert Messages"](#).

Send Alert To: You can select the user to whom SMS and Email alert is to be sent. The contact details of the user must be available in the user profile for sending the alert.

Send Alert Of: You can select the users whose Dead Man Violation alert is to be sent.

Alert Message Configuration

Alert Filter

Access Control

Event

Dead Man Zone Violation

Header Message

Dear User,

Footer Message

From COSEC Software

Additional Message Parameters

Message Selection

☒ SMS
☒ Email

Message Preview

Assign Alert

Assign Alert

Send Alert To

User *

3

Sheetal Raval

User

ID

Name

Send Alerts Of

Select Users

Randomly

User

ID

Name

Search

User ID	Name	SMS	Email	
1	Chirag	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Do Not Disturb

DND feature allows the user to declare that a particular zone is not to be accessed by other users for a specific period of time thereby ensuring that the users inside the zone are not disturbed by others.



This functionality can also be enabled from the **Device Module > Device Configuration > Features** option.

A screenshot of the 'Do Not Disturb' configuration web interface. The interface includes a search bar at the top right. Below it, there are two main sections: 'Device' and 'Zone'. The 'Device' section has input fields for 'ID' and 'Name', an 'Enable Rule' checkbox, and an 'Update Device' button. The 'Zone' section has a 'Zone' dropdown menu, an 'Enable Rule On Zone' checkbox, an 'Access Level' dropdown menu, and an 'Update Zone' button. On the right side, there is a table listing configured devices.

ID	Name
1	Panel Lite V2-Device-1
21	panel lite v2 default

The grid on the page shows the list of the Panel200 configured with Access Control System.

The user can select any Panel200 from the list. Click on the Panel200 from the grid. The selection will be reflected in the **Device** field. Also the Device picklist is given to search and select the device from a list of devices.

Click on **Enable Rule**.

Then Click on **Update Device**. The DND rule will be updated on device.

Zone: Click on the Zone dropdown button and select the Zone of the Panel200 where the DND rule is to be configured.

Enable Rule on Zone: Check the box to enable this Rule on Zone. The Rule is enabled on the zone only after the device is updated for the rule.

Access Level: Select the Access level for DND Zone within a range of 1-15. DND access Level must be higher than the zone access level so that the unwanted users are restricted to access the DND zone.

Eg: If DND Zone access level - 5 and User access level - 4; then user is not allowed to enter in DND zone.

VIP users are not affected by the do not disturb zone i.e. they will be allowed to access the door even if DND is enabled.

Click on **Update Zone**. The Do Not Disturb Rule will be activated.

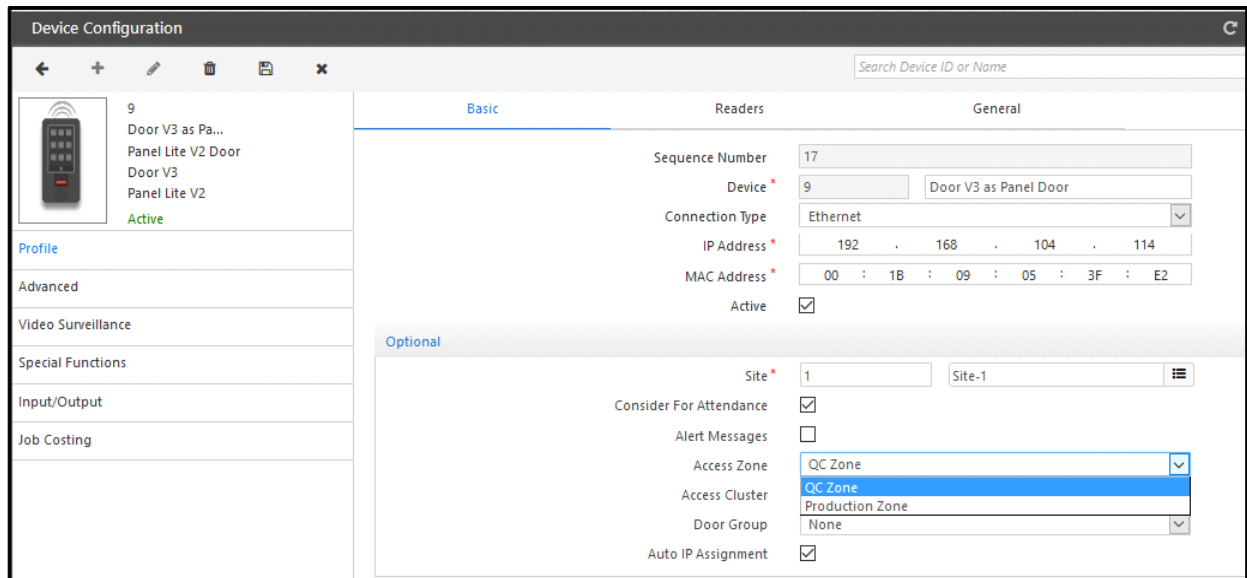


The DND can be activated using a special card i.e. Special function **21** on Panel lite or it can be activated on the door using Active DND special function.

Configuration of DND feature

Create a Zone of Pane Lite V2 where the DND rule is to be configured. Eg: QC Zone

Now the Panel door (say Door V3) where the DND rule is to be activated must be assigned the QC Zone.



Device Configuration

Search Device ID or Name

Basic

Sequence Number: 17

Device: 9

Connection Type: Ethernet

IP Address: 192 . 168 . 104 . 114

MAC Address: 00 : 1B : 09 : 05 : 3F : E2

Active: ☒

Optional

Site: 1

Consider For Attendance: ☒

Alert Messages: ☐

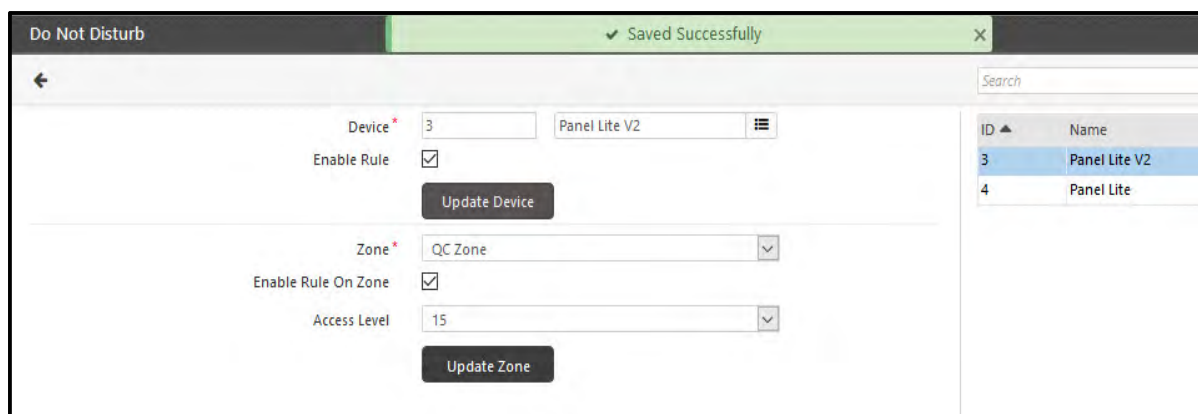
Access Zone: QC Zone

Access Cluster: QC Zone

Door Group: None

Auto IP Assignment: ☒

Now enable the DND rule from Access Control on Panel200 and QC Zone. Ensure that the access level of zone is higher than the access level of user.



Do Not Disturb

✓ Saved Successfully

Device: 3

Enable Rule: ☒

Update Device

Zone: QC Zone

Enable Rule On Zone: ☒

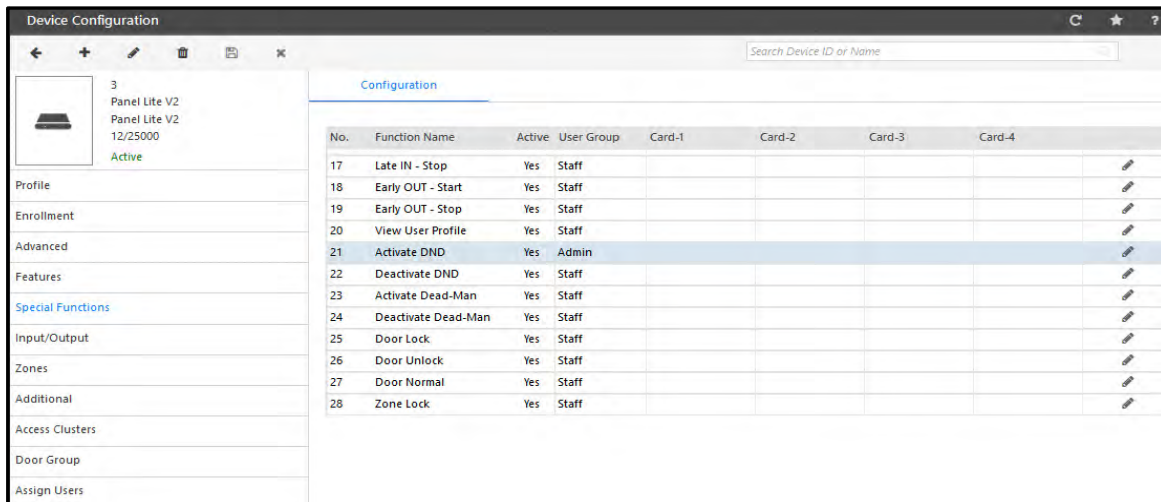
Access Level: 15

Update Zone

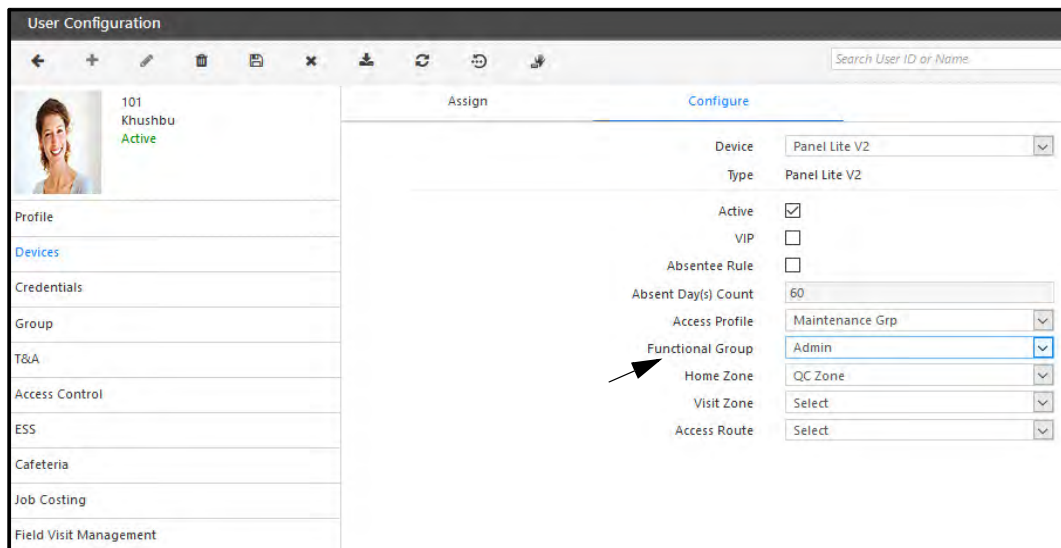
ID	Name
3	Panel Lite V2
4	Panel Lite

If you want to allow the special function to be activated by specific user group then select that user group for the particular special function.

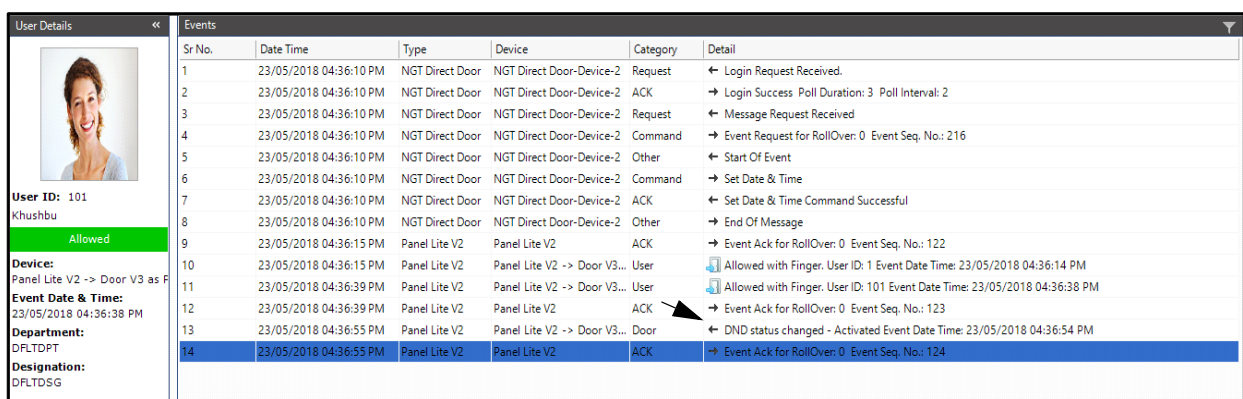
Eg: The Special function “Activate DND” can be activated by the “Admin” user group as configured below. Similarly “Deactivate DND” function can be set on the door by “Staff” user group.




Now the user 101 is assigned functional group “Admin” for Panel200 as shown below. So this user can activate DND on Door V3.



When the particular area is to be set as Do Not Disturb, then go to Menu> Zone Settings> Do Not Disturb> Activate from the display of door. Then show your ID on door i.e. punch on the door. This will activate Do Not Disturb feature. The DND activated event will be shown on Monitor as below.



Now when any user punches on door; then he/she will be denied access as it is DND enabled zone.



User ID: 102

Shruti Patki

Denied - DND Enabled

Device:

Panel Lite V2 -> Door V3 as F

Event Date & Time:

23/05/2018 04:38:12 PM

Department:

DFLTDPT

Designation:

DFLTDSG

Sr No.	Date Time	Type	Device	Category	Detail
2	23/05/2018 04:36:10 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	→ Login Success Poll Duration: 3 Poll Interval: 2
3	23/05/2018 04:36:10 PM	NGT Direct Door	NGT Direct Door-Device-2	Request	← Message Request Received
4	23/05/2018 04:36:10 PM	NGT Direct Door	NGT Direct Door-Device-2	Command	→ Event Request for RollOver: 0 Event Seq. No.: 216
5	23/05/2018 04:36:10 PM	NGT Direct Door	NGT Direct Door-Device-2	Other	← Start Of Event
6	23/05/2018 04:36:10 PM	NGT Direct Door	NGT Direct Door-Device-2	Command	→ Set Date & Time
7	23/05/2018 04:36:10 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	← Set Date & Time Command Successful
8	23/05/2018 04:36:10 PM	NGT Direct Door	NGT Direct Door-Device-2	Other	→ End Of Message
9	23/05/2018 04:36:15 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 122
10	23/05/2018 04:36:15 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed with Finger. User ID: 1 Event Date Time: 23/05/2018 04:36:14 PM
11	23/05/2018 04:36:39 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed with Finger. User ID: 101 Event Date Time: 23/05/2018 04:36:38 PM
12	23/05/2018 04:36:39 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 123
13	23/05/2018 04:36:55 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← DND status changed - Activated Event Date Time: 23/05/2018 04:36:54 PM
14	23/05/2018 04:36:55 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 124
15	23/05/2018 04:38:02 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Denied - DND Enabled with Finger. User ID: 4 Event Date Time: 23/05/2018 04:38:01 PM
16	23/05/2018 04:38:02 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 125
17	23/05/2018 04:38:13 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Denied - DND Enabled with Finger. User ID: 102 [1689] Event Date Time: 23/05/2018 04:38:12 PM
18	23/05/2018 04:38:13 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 126

The DND feature can be deactivated by the user belonging to the user group which is set for this special function. Here "Staff" group is set for Deactivate DND. So go to Menu> Zone Settings> Do Not Disturb> Deactivate from the display of door. Then show your ID on door i.e. punch on the door. This will deactivate Do Not Disturb feature.

Events					
Sr No.	Date Time	Type	Device	Category	Detail
4	23/05/2018 04:36:10 PM	NGT Direct Door	NGT Direct Door-Device-2	Command	→ Event Request for RollOver: 0 Event Seq. No.: 216
5	23/05/2018 04:36:10 PM	NGT Direct Door	NGT Direct Door-Device-2	Other	← Start Of Event
6	23/05/2018 04:36:10 PM	NGT Direct Door	NGT Direct Door-Device-2	Command	→ Set Date & Time
7	23/05/2018 04:36:10 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	← Set Date & Time Command Successful
8	23/05/2018 04:36:10 PM	NGT Direct Door	NGT Direct Door-Device-2	Other	→ End Of Message
9	23/05/2018 04:36:15 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 122
10	23/05/2018 04:36:15 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed with Finger. User ID: 1 Event Date Time: 23/05/2018 04:36:14 PM
11	23/05/2018 04:36:39 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed with Finger. User ID: 101 Event Date Time: 23/05/2018 04:36:38 PM
12	23/05/2018 04:36:39 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 123
13	23/05/2018 04:36:55 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← DND status changed - Activated Event Date Time: 23/05/2018 04:36:54 PM
14	23/05/2018 04:36:55 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 124
15	23/05/2018 04:38:02 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Denied - DND Enabled with Finger. User ID: 4 Event Date Time: 23/05/2018 04:38:01 PM
16	23/05/2018 04:38:02 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 125
17	23/05/2018 04:38:13 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Denied - DND Enabled with Finger. User ID: 102 [1689] Event Date Time: 23/05/2018 04:38:12 PM
18	23/05/2018 04:38:13 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 126
19	23/05/2018 04:40:04 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← DND status changed - Deactivated Event Date Time: 23/05/2018 04:40:03 PM
20	23/05/2018 04:40:04 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 127

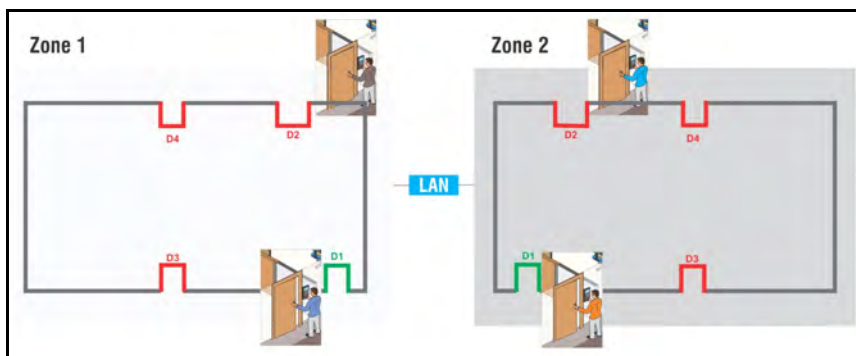
Man Trap

Mantrap, interlock or airlock systems provide safety, security and environmental control between two or more rooms by ensuring that opening any door causes all other doors to lock until the opened door returns to the closed position.

In this feature, Mantrap timer is provided which is the timer for which door needs to wait for the other door to get closed in the same zone where the mantrap feature is enabled. The system then waits for the defined timer period and then ignores the status of that door if it continues to be in the abnormal state.

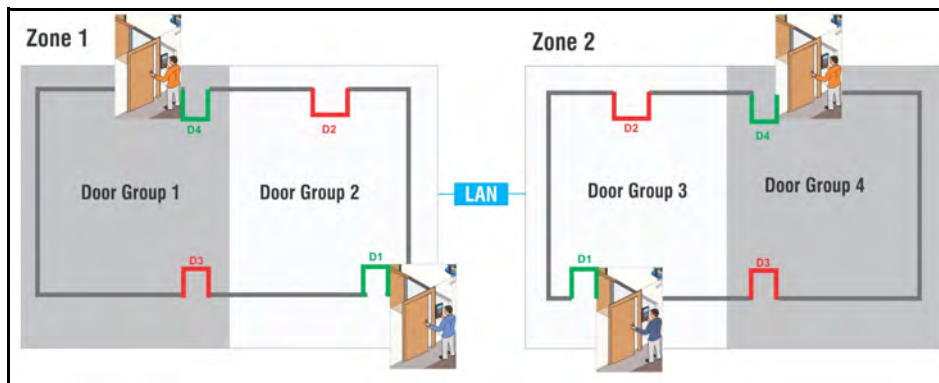
Man Trap-Zone Based

Second Door opens only after the first Door gets closed completely of that particular Zone.



Man Trap-Door Based

Second Door opens only after the first Door gets closed completely of that particular Door Group.



This functionality can also be enabled from the **Device Module > Device Configuration > Features** option.



1. Door sense is must for this feature as the system will ignore the door status either in the absence of a door sense or its fault state.
2. This feature is not supported when the Panel Doors are in degraded mode (standalone mode).

To use the Man Trap feature, select **Access Control module > Man Trap**. The page appears as shown below:

Man Trap

Device * 9 Panel Lite V2-Device-9

Enable Rule ☒

Man Trap Wait Timer (Sec) * 5

Functioning Zone Based

Update Device

Zone * Zone-1

Enable Rule On Zone ☐

Enable Strict Man Trap ☐

Update Zone

Search

ID	Name
1	RnD Panel lite V2
9	Panel Lite V2-Device-9

The grid on the page shows the list of the Panel lite configured with Access Control System.

The user can select any Panel lite from the list. The selection will be reflected in the **Device** field.

Enable Rule: Check the box to enable Man trap rule on the selected Panel lite.

Man Trap Wait Timer: Specify the Man Trap Wait Timer (sec) for which the door needs to wait for the other door to get closed in the same zone where the mantrap feature is enabled. By default the value of the Man-trap timer is 5 seconds and valid range is from **3 sec to 99 sec**.

Functioning: Select the Man Trap functioning from the option of **Zone based** and **Door Group based**.

Then Click on **Update Device**. The device will be updated as shown below:

Man Trap

Device * 9 Panel Lite V2-Device-9

Enable Rule ☒

Man Trap Wait Timer (Sec) * 5

Functioning Zone Based

Update Device

Zone * HO zone

Enable Rule On Zone ☒

Enable Strict Man Trap ☒

Update Zone

Search

ID	Name
1	RnD Panel lite V2
9	Panel Lite V2-Device-9

Zone: If Zone based functioning is selected then select the Zone from the configured Zones of panel lite to be monitored for security.

Enable Rule on Zone: Check the box to enable this rule on Zone.

Enable Strict Man Trap: Check the box to Enable Strict Man Trap. By this the man trap process will not use the wait timer to open the next door. Instead it will indefinitely wait for one door to close before the second door can open.

Click on **Update Zone**. The Man Trap Rule will be activated on Zone.

Door Group: If Door Group functioning is selected then select the Door Group on which Man Trap feature is to be implemented.

The screenshot shows the 'Man Trap' configuration window for a device. The 'Device' dropdown is set to '9' (Panel Lite V2-Device-9). The 'Enable Rule' checkbox is checked. The 'Man Trap Wait Timer (Sec)' is set to 5. The 'Functioning' dropdown is set to 'Door Group Based'. There is an 'Update Device' button. Below this, the 'Door Group' dropdown is set to 'RandD Group'. The 'Enable Rule On Door Group' checkbox is checked. The 'Enable Strict Man Trap' checkbox is unchecked. There is an 'Update Group' button. On the right, a table lists devices:

ID	Name
1	RnD Panel lite V2
9	Panel Lite V2-Device-9

Enable Rule on Door Group: Check the box to enable this Rule on Door Group.

Enable Strict Man Trap: Check the box to Enable Strict Man Trap. By this the man trap process will not use the wait timer to open the next door. Instead it will indefinitely wait for one door to close before the second door can open.

Click on **Update Group**. The Man Trap Rule will be activated on Door Group.

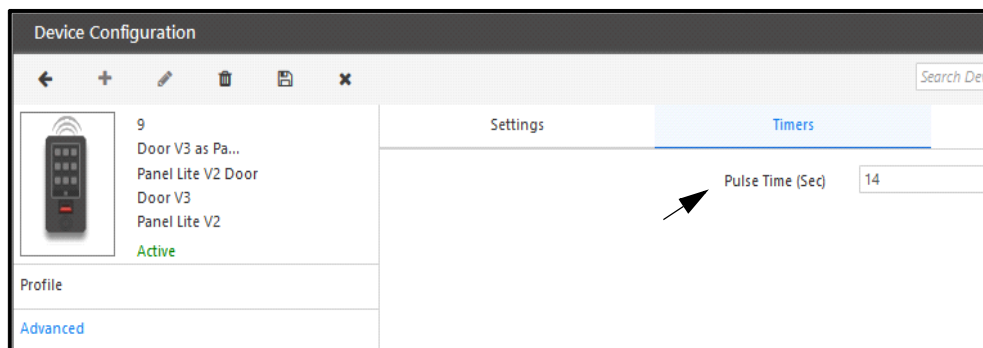
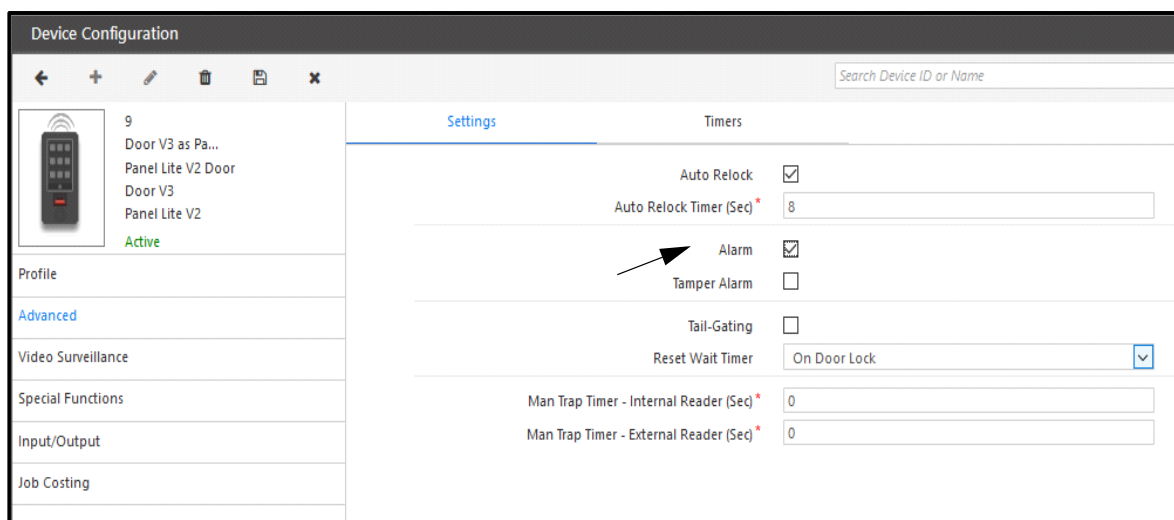
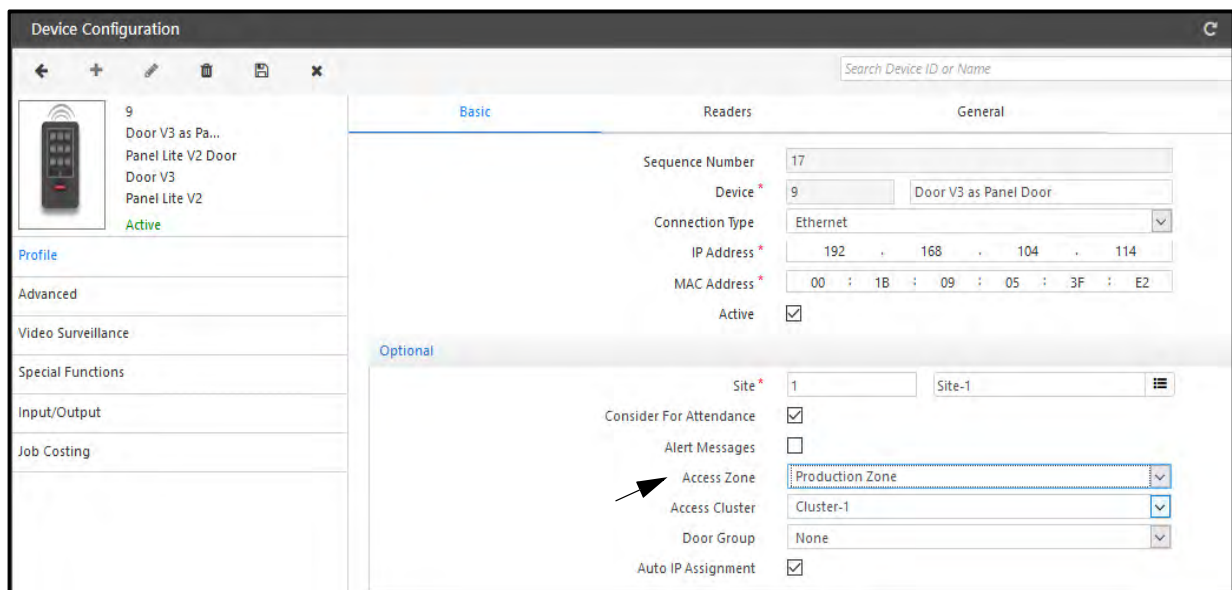
Configuration of Man Trap- Zone based

Let us configure Man Trap on Panel200 for Zone Based on Production Zone. So Enable the rule for Panel200 and for Production zone as shown below.

The screenshot shows the 'Man Trap' configuration window for a zone. A green banner at the top says 'Saved Successfully'. The 'Device' dropdown is set to '3' (Panel Lite V2). The 'Enable Rule' checkbox is checked. The 'Man Trap Wait Timer (Sec)' is set to 20. The 'Functioning' dropdown is set to 'Zone Based'. There is an 'Update Device' button. Below this, the 'Zone' dropdown is set to 'Production Zone'. The 'Enable Rule On Zone' checkbox is checked. The 'Enable Strict Man Trap' checkbox is unchecked. There is an 'Update Zone' button. On the right, a table lists zones:

ID	Name
3	Panel Lite V2
4	Panel Lite

Now the Production zone has 2 doors i.e. Door V3 and PVR door. Both doors are assigned Production Zone from door profile as shown below.



Settings	Alarms	Timers	Wiegand
<div> <div>3</div> <div>Panel Lite V2</div> <div>Panel Lite V2</div> <div>14/25000</div> <div>Active</div> </div> <div> <div>Profile</div> <div>Enrollment</div> <div>Advanced</div> </div>			
<div> <div>Inter-Digit Wait Timer (Sec)*</div> <div>3</div> </div> <div> <div>Multi-Input Wait Timer (Sec)*</div> <div>5</div> </div> <div> <div>Late-IN Early-OUT Timer (Min)*</div> <div>60</div> </div> <div> <div>Door Abnormal Wait Timer (Sec)*</div> <div>15</div> </div> <div> <div>Palm Enrollment Time Out (Sec)*</div> <div>60</div> </div>			

The Door Sense for the doors must be configured as shown below. You can select sense type as NO or NC.

Configuration
<div> <div>10</div> <div>PVR as Panel ...</div> <div>Panel Lite V2 Door</div> <div>PVR Door</div> <div>Panel Lite V2</div> <div>Active</div> </div> <div> <div>Profile</div> <div>Advanced</div> <div>Video Surveillance</div> <div>Special Functions</div> <div>Input/Output</div> <div>Job Costing</div> </div>
<div> <div>Door Sense</div> <div> <div>Enable</div> <div><input checked="" type="checkbox"/></div> </div> <div> <div>Supervised</div> <div><input type="checkbox"/></div> </div> <div> <div>Sense Type</div> <div>NO</div> </div> </div> <div> <div>Auxiliary Input</div> <div> <div>Enable</div> <div><input type="checkbox"/></div> </div> <div> <div>Supervised</div> <div><input type="checkbox"/></div> </div> <div> <div>Sense Type</div> <div>NO</div> </div> <div> <div>Debounce Time (Sec)</div> <div>5</div> </div> </div> <div> <div>Auxiliary Output</div> <div> <div>Enable</div> <div><input type="checkbox"/></div> </div> <div> <div>Output Group</div> <div>1</div> </div> <div> <div>DC Aux Ports</div> <div></div> </div> </div> <div> <div>Relay Output</div> <div> <div>Output Group Number(Door Unlock)</div> <div>2</div> </div> <div> <div>Door Unlock</div> <div></div> </div> <div> <div>Output Group Number(Door Lock)</div> <div>ID</div> </div> <div> <div>Name</div> <div></div> </div> </div>

Man Trap Only

When user1 punches on Door V3, door opens. If pulse time is elapsed before closing the door then "Door held open too long" alarm is generated. Now if door still remains open till abnormal wait timer elapse then "Door abnormal" alarm will be generated.



When Alarm is disabled for Door V3 then alarms "Door Held Open too long" and "Door abnormal" will not be generated and displayed in Monitor.


Now If **Man Trap Wait timer** is **20 sec**; then PVR door waits for 20 sec for Door V3 to close. If Strict Man Trap is enabled then PVR door wont check for the 20 sec time; it will only wait for Door V3 to close.

If Door V3 is open and user2 punches on PVR door then he will be asked to wait displaying the message on door as another door is open.

When 20 sec is over or Door V3 gets closed then user2 is access allowed on PVR door.


Suppose the Pulse time for Door V3 is set as 14sec. The Door Abnormal Wait Timer is set as 15sec. Suppose user1 access Door V3 at 11:50:41 hrs. Then after 14 seconds i.e. at 11:59:56 Door Held open too long alarm is generated. The door is still open so after 15 sec; Door Abnormal alarm is generated. Now after 20 sec i.e. at 12:00:31 user 2 will be allowed access on PVR door.

The events on Monitor is shown below.

User Details		Events					
		Sr No.	Date Time	Type	Device	Category	Detail
 User ID: 1 Chirag Allowed Device: Panel Lite V2 -> PVR as Pane Event Date & Time: 01/06/2018 12:00:41 PM Department: DRLTDPT Designation: DRLTDSG		125	01/06/2018 11:46:14 AM	NGT Direct Door	NGT Direct Door-Device-2	Other	← Start Of Event
		126	01/06/2018 11:46:14 AM	NGT Direct Door	NGT Direct Door-Device-2	Command	→ Set Date & Time
		127	01/06/2018 11:46:14 AM	NGT Direct Door	NGT Direct Door-Device-2	ACK	← Set Date & Time Command Successful
		128	01/06/2018 11:46:14 AM	NGT Direct Door	NGT Direct Door-Device-2	Other	→ End Of Message
		129	01/06/2018 11:59:41 AM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	← Allowed with Finger, User ID: 1 Event Date Time: 01/06/2018 11:59:41 AM
		130	01/06/2018 11:59:41 AM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 628
		131	01/06/2018 11:59:45 AM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Door Open/Close - Open, User ID: 1 Event Date Time: 01/06/2018 11:59:44 AM
		132	01/06/2018 11:59:45 AM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 629
		133	01/06/2018 11:59:56 AM	Panel Lite V2	Panel Lite V2 -> Door V3...	Alarm	← Door Held open too long, Event Date Time: 01/06/2018 11:59:56 AM
		134	01/06/2018 11:59:56 AM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 630
		135	01/06/2018 12:00:11 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Alarm	← Door Abnormal, Event Date Time: 01/06/2018 12:00:11 PM
		136	01/06/2018 12:00:11 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 631
		137	01/06/2018 12:00:31 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	← Allowed with Palm, User ID: 1 Event Date Time: 01/06/2018 12:00:31 PM
		138	01/06/2018 12:00:31 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 632
		139	01/06/2018 12:00:36 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	Door	← Door Open/Close - NotOperated, User ID: 1 Event Date Time: 01/06/2018 12:00:36 PM
		140	01/06/2018 12:00:36 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 633
		141	01/06/2018 12:00:40 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Door Open/Close - Close, User ID: 1 Event Date Time: 01/06/2018 12:00:39 PM
		142	01/06/2018 12:00:40 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 634

Advance Configuration with Readers duration

Enable Man Trap Timer Violation and Man Trap Alarm Wait Timer for Panel200 as shown below.



3
Panel Lite V2
Panel Lite V2
14/25000
Active

Profile
Enrollment
Advanced
Features
Special Functions
Input/Output
Zones
Additional
Access Clusters
Door Group
Assign Users

Settings

Alarms

Timers

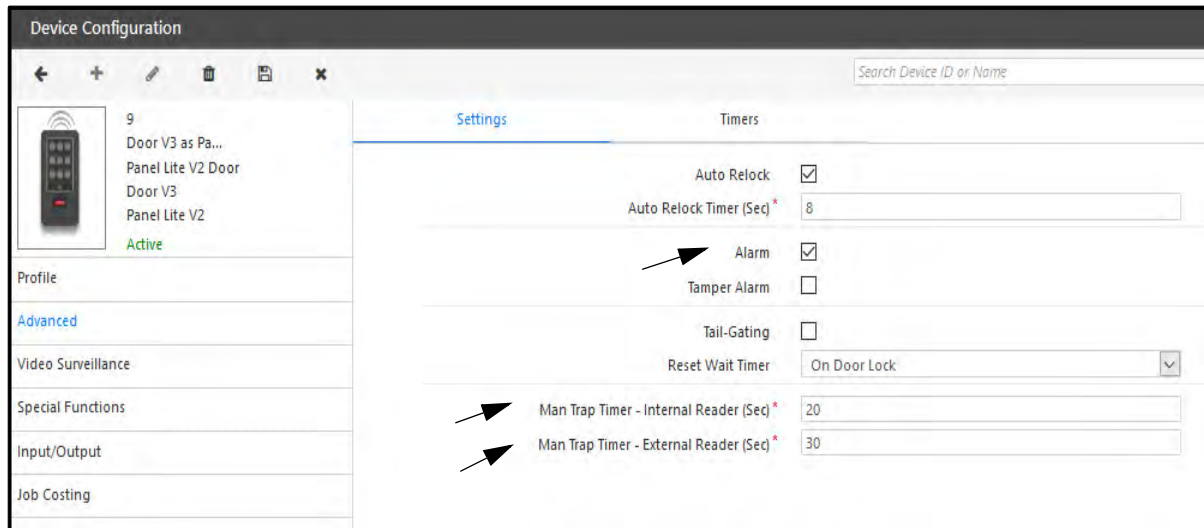
Wiegand

☐ Duress
☐ Dead Man
☐ Panic
☐ Door Offline
☐ Door Fault
☐ Occupancy Violated
☐ Tail - Gating
☒ Man Trap Timer Violation
☐ Access Denied - Anti-Pass Back
☐ Access Denied - Access Route Violated
☐ Access Denied - Other Reasons
☐ Multiple Unauthorized Attempts
☐ User Unidentified
 Custom Alarm 1
 Custom Alarm 2
 Custom Alarm 3

Alarm Reissue Wait Timer(min)
☒ Man Trap Alarm Wait Timer

The Panel doors must be enabled with Alarm. And enter the duration in seconds for Man Trap Timer- Internal Reader and Man Trap Timer- External Reader as shown below.

Door V3- 20 sec for Internal reader and **30 sec** for External reader
PVR Door - 25 sec for Internal reader and **35 sec** for External reader

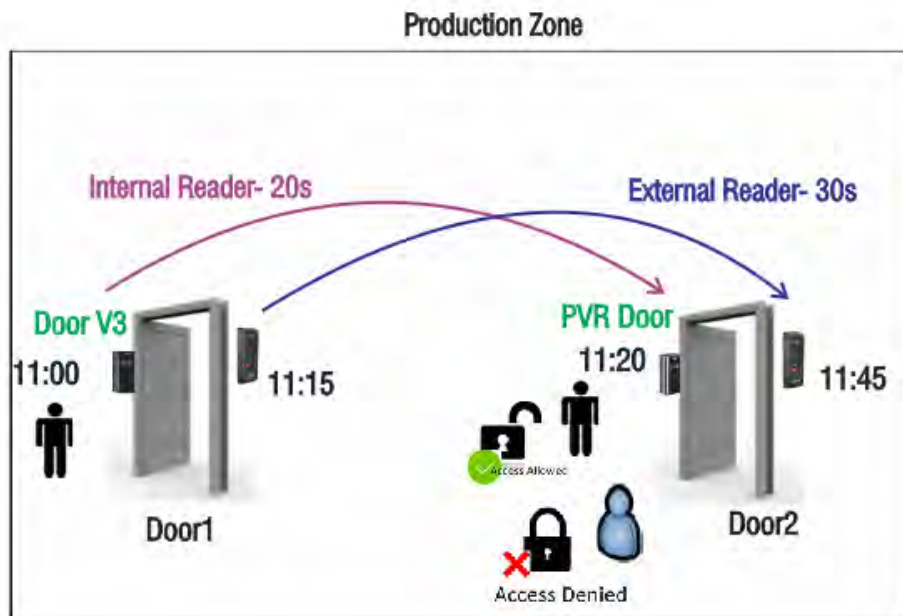


When user punches on internal reader of a door (say Door V3). Then he is expected to punch on internal reader of any other door (say here PVR door) of same zone within 20 seconds (Man Trap timer- Internal reader of Door V3).

- Until the same user punches on any internal reader in the same zone, no other user will be allowed to any other internal reader in the same zone.

When user punches on external reader of a door then he is expected to punch on external reader of any other door (say here PVR door) of same zone within 30 seconds (Man Trap timer- External reader of Door V3).

- Until the same user punches on any external reader in the same zone, no other user will be allowed to any other external reader in the same zone. This will work if Access Control on Exit mode is enabled for the zone. If this check-box is disabled then other user also can access the external reader of (say PVR door).



Matrix COSEC MONITOR

File Device Tools Help


Features <<

- Alarms
- I/O Link
- Soft Override
- Events
- Exceptions
- Time Triggered Functions
- EMAP

Devices - All 2 8

Name	Site	IP/RS485 Address	MAC Address	Type	Status
Panel Lite V2		192.168.104.111	00:18:09:04:65:D1	Panel Lite V2	Connected
ARC as Single Door	Site-1	192.168.105.3	DF:E3:65:54:34:44	Panel Lite V2 Door	OFF-Line
Dummy Door	Site-1	192.111.111.111	11:11:11:11:11:11	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-1	192.168.105.5	DF:E6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-1	192.168.105.5	DF:E6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.6	FE:47:48:46:74:69	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.6	FE:47:48:46:74:69	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.7	FE:66:74:84:00:9C	Panel Lite V2 Door	OFF-Line

User Details <<



User ID: 1687
Aditi Ajay Gupt

Device:
Panel Lite V2 -> PVR as Pane

Event Date & Time:
06/06/2018 05:57:26 PM

Department:
DRLTDPT

Designation:
DRLTDSG


Denied - Control zone

Events

Sr No.	Date Time	Type	Device	Category	Detail
9	06/06/2018 05:57:14 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Finger. User ID: 1 Event Date Time: 06/06/2018 05:57:13 PM
10	06/06/2018 05:57:14 PM	Panel Lite V2	Panel Lite V2	ACK	Event Ack for RollOver: 0 Event Seq. No.: 873
11	06/06/2018 05:57:19 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	Door Open/Close - Open. User ID: 1 Event Date Time: 06/06/2018 05:57:18 PM
12	06/06/2018 05:57:19 PM	Panel Lite V2	Panel Lite V2	ACK	Event Ack for RollOver: 0 Event Seq. No.: 874
13	06/06/2018 05:57:21 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	Door Open/Close - Close. User ID: 1 Event Date Time: 06/06/2018 05:57:20 PM
14	06/06/2018 05:57:21 PM	Panel Lite V2	Panel Lite V2	ACK	Event Ack for RollOver: 0 Event Seq. No.: 875
15	06/06/2018 05:57:27 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	Denied - Control zone with Palm. User ID: 1687 Event Date Time: 06/06/2018 05:57:26 PM
16	06/06/2018 05:57:27 PM	Panel Lite V2	Panel Lite V2	ACK	Event Ack for RollOver: 0 Event Seq. No.: 876

If user fails to punch within Man Trap Internal/External timer then Man Trap violation alarm will be generated.

User Details <<



User ID: 1687
Aditi Ajay Gupt

Device:
Panel Lite V2 -> PVR as Pane

Event Date & Time:
06/06/2018 05:57:26 PM

Department:
DRLTDPT

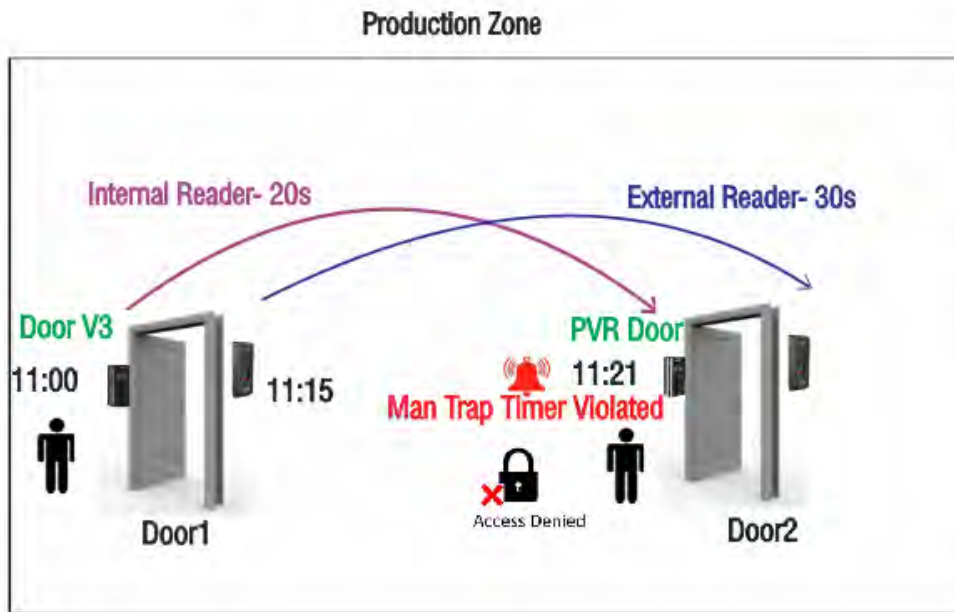
Designation:
DRLTDSG

Denied - Control zone

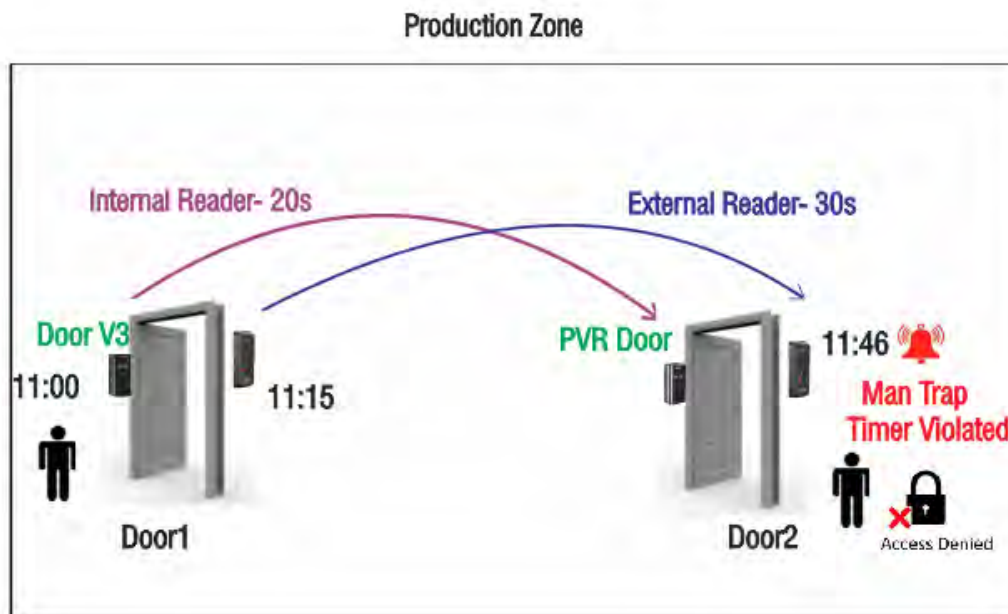
Events

Sr No.	Date Time	Type	Device	Category	Detail
9	06/06/2018 05:57:14 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Finger. User ID: 1 Event Date Time: 06/06/2018 05:57:13 PM
10	06/06/2018 05:57:14 PM	Panel Lite V2	Panel Lite V2	ACK	Event Ack for RollOver: 0 Event Seq. No.: 873
11	06/06/2018 05:57:19 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	Door Open/Close - Open. User ID: 1 Event Date Time: 06/06/2018 05:57:18 PM
12	06/06/2018 05:57:19 PM	Panel Lite V2	Panel Lite V2	ACK	Event Ack for RollOver: 0 Event Seq. No.: 874
13	06/06/2018 05:57:21 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	Door Open/Close - Close. User ID: 1 Event Date Time: 06/06/2018 05:57:20 PM
14	06/06/2018 05:57:21 PM	Panel Lite V2	Panel Lite V2	ACK	Event Ack for RollOver: 0 Event Seq. No.: 875
15	06/06/2018 05:57:27 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	User	Denied - Control zone with Palm. User ID: 1687 Event Date Time: 06/06/2018 05:57:26 PM
16	06/06/2018 05:57:27 PM	Panel Lite V2	Panel Lite V2	ACK	Event Ack for RollOver: 0 Event Seq. No.: 876
17	06/06/2018 05:57:34 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Alarm	Man Trap Timer Violation Alarm - User ID: 1 Event Date Time: 06/06/2018 05:57:33 PM
18	06/06/2018 05:57:34 PM	Panel Lite V2	Panel Lite V2	ACK	Event Ack for RollOver: 0 Event Seq. No.: 877

When user1 punches on Door V3 at 11:00 hours then he is expected to punch PVR door within 11:20 hours. When 20 second elapses and user does not punch then Man Trap violation alarm is generated.



Also if user1 punches on external reader of Door V3 at 11:15 hours then he is expected to punch on external reader of PVR door within 11:45 hours. When 30 second elapses and user does not punch then Man Trap violation alarm is generated.



Features

Alarms

I/O Link

Soft Override

Events

Exceptions

Time Triggered Functions

EMAP

Devices - All

28

Name	Site	IP/RS485 Address	MAC Address	Type	Status
Panel Lite V2		192.168.104.111	00:1B:09:04:65:D1	Panel Lite V2	Connected
ARC as Single Door	Site-1	192.168.105.3	DFE3:65:54:34:44	Panel Lite V2 Door	OFF-Line
Dummy Door	Site-1	192.111.111.111	11:11:11:11:11:11	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-1	192.168.105.5	DFE6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-1	192.168.105.5	DFE6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.6	FE47:48:46:74:69	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.6	FE47:48:46:74:69	Panel Lite V2 Door	OFF-Line
Both as Panel door	Site-1	192.168.105.7	FE66:7A:9A:00:9E	Panel Lite V2 Door	OFF-Line

User Details

User ID: 1

Chirag

Allowed

Device:

Panel Lite V2 -> Door V3 as P

Event Date & Time:

06/06/2018 06:16:47 PM

Department:

DPLTDPT

Designation:

DPLTDSG

Events

Sr.No.	Date Time	Type	Device	Category	Detail
16	06/06/2018 05:57:27 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 876
17	06/06/2018 05:57:34 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Alarm	← Man Trap Timer Violation Alarm - User ID: 1 Event Date Time: 06/06/2018 05:57:33 PM
18	06/06/2018 05:57:34 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 877
19	06/06/2018 06:16:27 PM	Panel Lite V2	Panel Lite V2	Request	← Message Request Received
20	06/06/2018 06:16:27 PM	Panel Lite V2	Panel Lite V2	Command	→ Clear alarm. Alarm Seq. No.: 67 TID: 1806060050000016
21	06/06/2018 06:16:27 PM	Panel Lite V2	Panel Lite V2	ACK	← Clear alarm Command Successful. Alarm Seq. No.: 67
22	06/06/2018 06:16:27 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Alarm	← Alarm cleared Event Date Time: 06/06/2018 06:16:26 PM
23	06/06/2018 06:16:27 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
24	06/06/2018 06:16:27 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 878
25	06/06/2018 06:16:43 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed with Finger. User ID: 1 Event Date Time: 06/06/2018 06:16:41 PM
26	06/06/2018 06:16:43 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 879
27	06/06/2018 06:16:48 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 880
28	06/06/2018 06:16:48 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	→ Allowed with Finger. User ID: 1 Event Date Time: 06/06/2018 06:16:47 PM
29	06/06/2018 06:16:56 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Door Open/Close - NotOperated. User ID: 1 Event Date Time: 06/06/2018 06:16:55 PM
30	06/06/2018 06:16:56 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 881
31	06/06/2018 06:17:18 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Alarm	← Man Trap Timer Violation Alarm - User ID: 1 Event Date Time: 06/06/2018 06:17:17 PM
32	06/06/2018 06:17:18 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 882

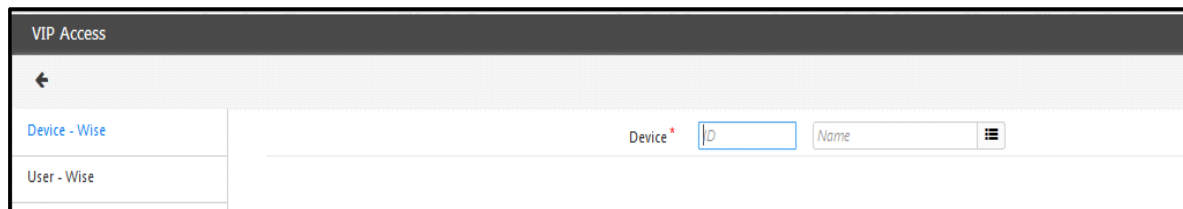


If user punches on PVR first; then Man Trap timer- Internal and External of PVR door will be considered.

VIP Access

VIP Access feature allows the admin to give VIP access to a specific user on the particular door for security purposes.

To use the VIP Access feature, Select **Access Control module> VIP Access**. The page appears as shown below:



There are two modes to configure this rule:

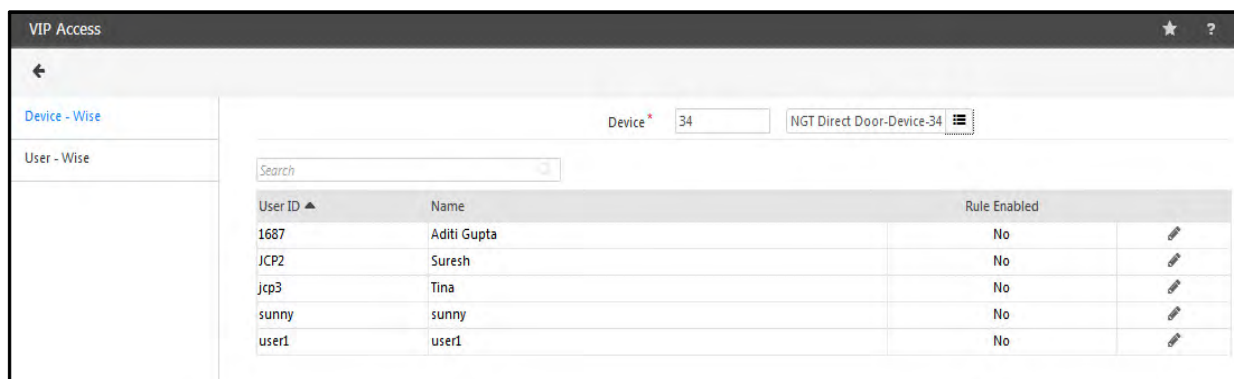
- Device-wise configuration
- User-wise configuration

Device- Wise

To Assign VIP Access Rule Device-wise, select Device-wise option. The following page appears.

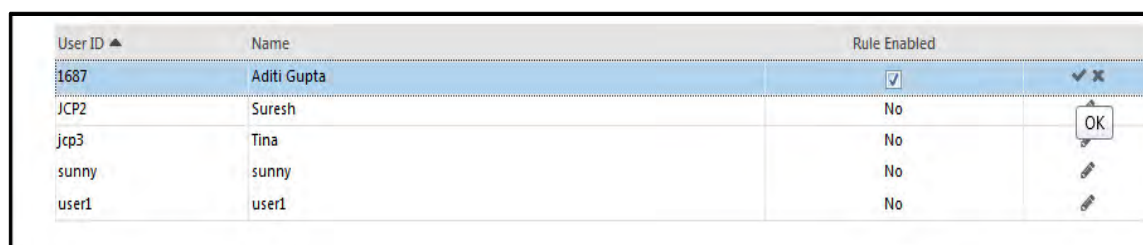
The user can select the **Device** from the picklist where the Rule is to be configured. Click on the button and select the Device from the Picklist.

The List of the assigned Users on the selected device will be listed in the grid as shown below.



User ID ▲	Name	Rule Enabled	
1687	Aditi Gupta	No	
JCP2	Suresh	No	
jcp3	Tina	No	
sunny	sunny	No	
user1	user1	No	

To assign the VIP access rule to one or more person on the selected device, click the edit button for that user. Now check the **Rule Enabled** box and click **OK** to save the changes as shown below.

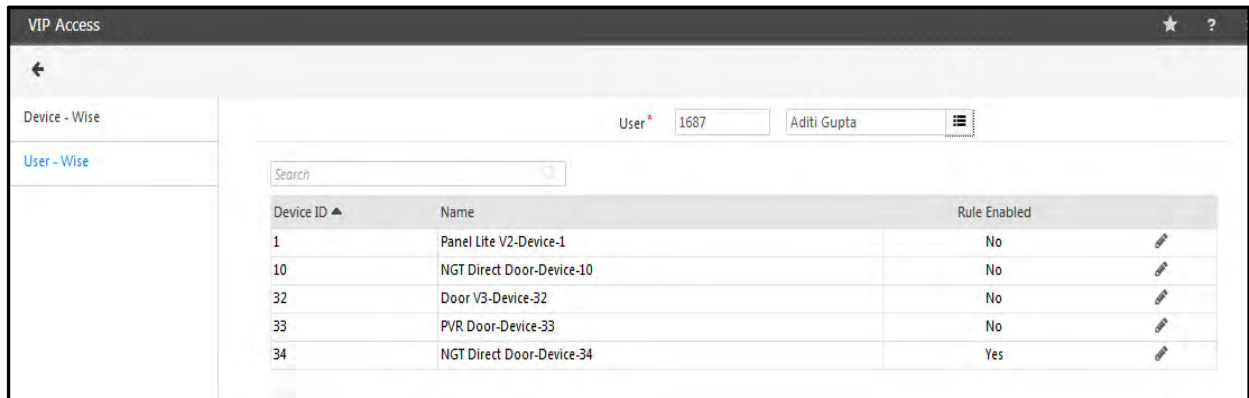


User ID ▲	Name	Rule Enabled	
1687	Aditi Gupta	<input checked="" type="checkbox"/>	
JCP2	Suresh	No	
jcp3	Tina	No	
sunny	sunny	No	
user1	user1	No	

User- Wise

To Assign VIP Access Rule User-wise, select User-wise option. The following page appears.


The admin can select the user for whom the Rule is to be configured. Click the picklist button and select the User.



Device ID	Name	Rule Enabled
1	Panel Lite V2-Device-1	No
10	NGT Direct Door-Device-10	No
32	Door V3-Device-32	No
33	PVR Door-Device-33	No
34	NGT Direct Door-Device-34	Yes

The List of all the devices assigned to the selected user will be listed in the grid.

To assign the VIP access rule on one or more devices for the selected user, click the edit button for the device. Now check the **Rule Enabled** box and click **OK** to save the changes as shown below.



Device ID	Name	Rule Enabled
1	Panel Lite V2-Device-1	No
10	NGT Direct Door-Device-10	No
32	Door V3-Device-32	<input checked="" type="checkbox"/>
33	PVR Door-Device-33	No
34	NGT Direct Door-Device-34	Yes

Visitor Escort

This rule requires all Visitors to be accompanied by an escort and the display of the visitor's credential has to be followed by the credential of the Escort within the stipulated time period. Check this box to enable this feature at the system level.



*This functionality can also be enabled from the **Device Module > Device Configuration > Features** option.*

To use the Visitor Escort Rule, Click on **Visitor Escort** option from the Access Control page. The page appears as shown below:

ID	Name
4	Panel Lite V2

The grid on the page shows the list of the Panel configured with Access Control System.

The user can select any Panel from the list. Click on the Panel from the grid. The selection will be reflected in the **Device** field.

Enable Rule: Check the box to enable the rule.

Then Click on **Update Device**. The device will be updated as shown below:

ID	Name
4	Panel Lite V2

Zone: Click on the Zone dropdown button and select the Zone to be monitored for security from the configured Zones of the selected panel.

Enable Rule on Zone: Check the box to enable this Rule on Zone.

Click on **Update Zone**. The Visitor Escort Rule will be activated.

Anti-Pass Back

The Anti Pass Back or APB feature is used to ensure that users pass through the entry reader followed by the exit reader before their ID will be accepted a second time at the designated entry reader. It prevents a card holder from passing back his/her card to other person to gain entry into an access controlled area.

Hard APB restricts the entry/exit of a person in case of an APB violation while **Soft APB** does not restrict the person from re-entering/ leaving on an APB Violation but reports the same and maintains a log.



In degraded mode, APB will not be verified.



The configuration of Anti-pass back feature as done from Access Control > Anti-Pass back will be updated on Device Configuration (Panel lite) > Zones (respective zones)

For Direct doors, Anti-pass back must be configured from **Device Module > Device Configuration > Features** option.



To use the Anti-Pass Back feature, Click on **Anti-Pass Back** option from the Access Control page. The page appears as shown below:

ID	Name
1	Panel lite V2

The grid on the right side shows the list of the Panel lite configured with Access Control System. The user can select any Panel lite from the grid on which Anti-pass back Rule is to be configured.

Enable Rule: Check the box to enable the rule for the selected Panel lite.

Then Click on **Update Device** to update the rule on the panel lite. The device will be updated as shown below and the Zone section will get enabled.

The screenshot shows the 'Anti-Pass Back' configuration window. At the top, a green banner indicates 'Saved Successfully'. The 'Device' section is active, showing 'Device *' as '1' and 'Panel lite V2'. The 'Enable Rule' checkbox is checked. The 'Update Device' button is visible. Below this, the 'Zone' section is partially visible, showing 'Zone *' as 'Zone-1'. The 'On Entry' and 'On Exit' checkboxes are unchecked, and 'Hard/Soft' is set to 'Soft'. The 'Forgiveness' checkbox is checked. The 'Reset After' section has 'Day Change' selected. The 'Forgiveness Timer (Mins)' is set to '1'. The 'Update Zone' button is at the bottom. On the right, a table lists the device:

ID	Name
1	Panel lite V2

Zone: Click on the Zone dropdown button and select the Zone to be monitored for security from the configured Zones of the selected panel.

The screenshot shows the 'Anti-Pass Back' configuration window with the 'Zone' section active. 'Device *' is '1' and 'Panel lite V2'. 'Enable Rule' is checked. The 'Update Device' button is visible. The 'Zone *' dropdown is set to 'RnD Zone'. The 'On Entry' and 'On Exit' checkboxes are checked, and both are set to 'Local'. 'Hard/Soft' is set to 'Soft'. 'Forgiveness' is checked. 'Reset After' has 'Timer Expiry' selected. 'Forgiveness Timer (Mins)' is set to '5'. The 'Update Zone' button is at the bottom. The right-hand table remains the same:

ID	Name
1	Panel lite V2

On Entry: Check this box so that the system monitors the entry reader for APB violation. Select the options from Local or Global from the drop down list.

- **Local:** In the event of the Local APB, the system applies the Anti-Pass back rule at the Zone level. [See "Local" on page 1332.](#)
- **Global:** In the event of the Global APB, the system applies the rule across all zones at the Panel Lite level. [See "Global" on page 1333.](#)

On Exit: Check this box also so that the system monitors the entry as well as the exit readers for APB violations.

Eg: If Anti Pass back in exit mode is configured for the internal port then the system shall display 'Access Allowed', 'Entry Was Not Registered' for Soft Anti Pass Back and for Hard Anti Pass back display 'Access Denied, Entry Not Recorded'.

Restriction Type: Select the restriction type as Hard or Soft option from the drop down options.

- **Hard APB:** The access will be denied if the exit is not registered first. It does not allow a second entry using the same card without an exit. [See “Configuration of APB- Hard” on page 1329.](#)
- **Soft APB:** The access will be granted even if the exit is not registered. It allows a second entry of the same user without an exit; however, an event and a warning are generated that indicates the second entry. [See “Configuration of APB- Soft” on page 1331.](#)

Forgiveness: Check this box to enable the system to reset the APB status. When forgiveness is enabled, then there will be following options to reset the pass.

1. **Reset After Day Change:** This will reset the APB status of all the users to NULL at midnight. This enables a user, who left the building in the evening without exit punch, to use his card for entry in the next morning.
2. **Reset After Timer Expiry:** This will reset the APB status of all the users after the expiry of user defined time.
 - **Forgiveness Timer (Mins):** Enter the time duration in minutes after which Anti-pass back status will get reset and the pass will be in original state.

Click on **Update Zone**. The Anti-Pass Back Rule will be updated.

ID	Name
1	Panel lite V2

Configuration of APB- Hard

Create the zone of Panel200. Then select that zone (say Production zone) where the APB feature is to be activated.

The screenshot shows the 'Anti-Pass Back' configuration window. It has a left sidebar with a back arrow and a search bar. The main area contains the following fields:

- Device: 3, Panel Lite V2
- Enable Rule: ☒
- Update Device button
- Zone: Production Zone (selected from a dropdown)
- On Entry: ☒ Local
- On Exit: ☒ Local
- Hard/Soft: Hard
- Forgiveness: ☒
- Reset After: ☐ Day Change ☒ Timer Expiry
- Forgiveness Timer (Mins): 60
- Update Zone button

On the right, there is a table with the following data:

ID	Name
3	Panel Lite V2
4	Panel Lite

Now the door in the zone where APB violation is to be monitored must be assigned the Access zone as Production Zone. The Door V3 is assigned Production zone as shown below.

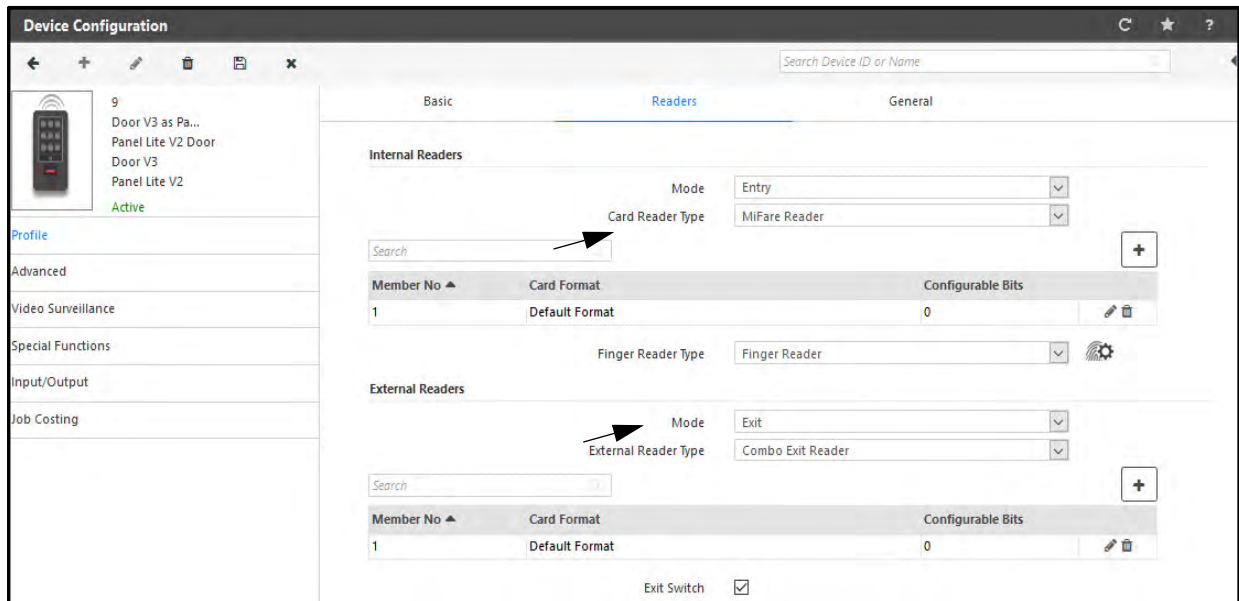
The screenshot shows the 'Device Configuration' window for 'Door V3 as Panel Door'. It has a left sidebar with a search bar and a list of devices. The main area is divided into 'Basic' and 'Optional' tabs. The 'Basic' tab contains the following fields:

- Sequence Number: 17
- Device: 9, Door V3 as Panel Door
- Connection Type: Ethernet
- IP Address: 192 . 168 . 104 . 114
- MAC Address: 00 : 1B : 09 : 05 : 3F : E2
- Active: ☒

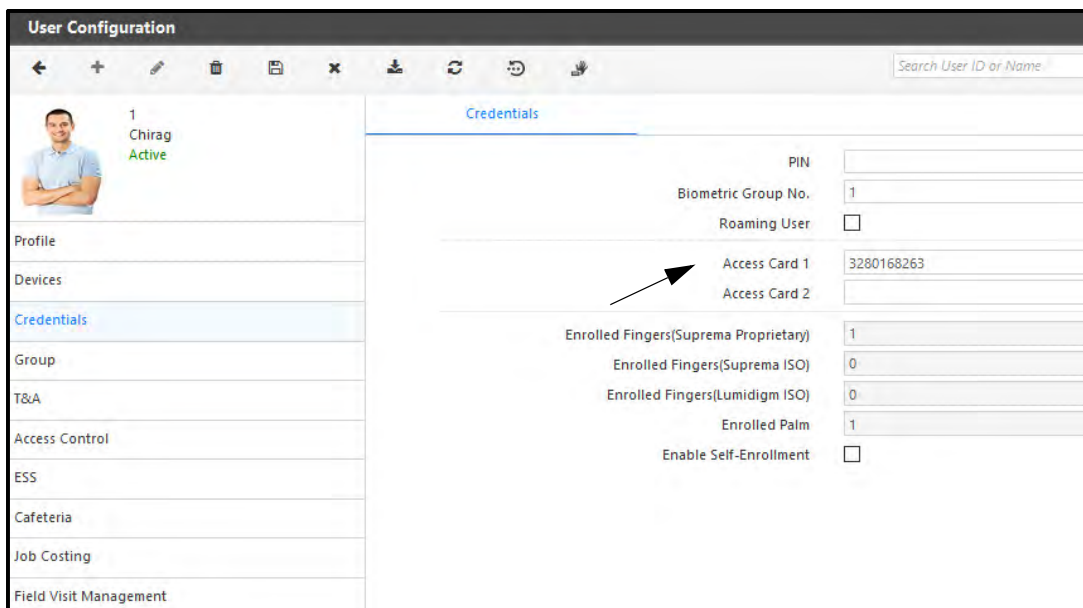
The 'Optional' tab contains the following fields:

- Site: 1, Site-1
- Consider For Attendance: ☒
- Alert Messages: ☐
- Access Zone: Production Zone (selected from a dropdown)
- Access Cluster: Cluster-1
- Door Group: None
- Auto IP Assignment: ☒


For APB feature, you must have Exit reader. So here PATH RDFE is connected to Door V3 as exit reader. And the Mode in External Reader is selected as Exit and Reader type is selected as Combo Exit Reader.



The Card must be enrolled for the user.



During Entry punch user is allowed. If there is second Entry punch using the same card then user will be denied access with Anti-Pass back violation.



User ID: 1

Chirag

Denied - Anti-Pass Back

Device:

Panel Lite V2 -> Door V3 as F

Event Date & Time:

24/05/2018 06:05:17 PM

Department:

DLTDPT

Designation:

DLTDG

Sr No.	Date Time	Type	Device	Category	Detail
1	24/05/2018 06:04:49 PM	NGT Direct Door	NGT Direct Door-Device-2	Request	← Login Request Received.
2	24/05/2018 06:04:49 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	→ Login Success Poll Duration: 3 Poll Interval: 2
3	24/05/2018 06:04:50 PM	NGT Direct Door	NGT Direct Door-Device-2	Request	← Message Request Received
4	24/05/2018 06:04:50 PM	NGT Direct Door	NGT Direct Door-Device-2	Command	→ Event Request for RollOver: 0 Event Seq. No.: 238
5	24/05/2018 06:04:50 PM	NGT Direct Door	NGT Direct Door-Device-2	Other	← Start Of Event
6	24/05/2018 06:04:50 PM	NGT Direct Door	NGT Direct Door-Device-2	Command	→ Set Date & Time
7	24/05/2018 06:04:50 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	← Set Date & Time Command Successful
8	24/05/2018 06:04:50 PM	NGT Direct Door	NGT Direct Door-Device-2	Other	→ End Of Message
9	24/05/2018 06:04:55 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 234
10	24/05/2018 06:04:54 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Card. User ID: 1 Event Date Time: 24/05/2018 06:04:54 PM
11	24/05/2018 06:05:02 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Finger. User ID: 1 Event Date Time: 24/05/2018 06:05:02 PM
12	24/05/2018 06:05:02 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 235
13	24/05/2018 06:05:12 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Card. User ID: 1 Event Date Time: 24/05/2018 06:05:12 PM
14	24/05/2018 06:05:12 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 236
15	24/05/2018 06:05:17 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Denied - Anti-Pass Back with Card. User ID: 1 Event Date Time: 24/05/2018 06:05:17 PM
16	24/05/2018 06:05:17 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 237

Configuration of APB- Soft

Anti-Pass Back

✓ Saved Successfully

Device *

3

Panel Lite V2

Enable Rule

☒

Update Device

Zone *

Production Zone

On Entry

☒ Local

On Exit

☒ Local

Hard/Soft

Soft

Forgiveness

☒

Reset After

☐ Day Change ☒ Timer Expiry

Forgiveness Timer (Mins)


60

Update Zone

ID	Name
3	Panel Lite V2
4	Panel Lite

In Soft APB, when APB is violated, it will give message on door as “Exit not Registered” but door can be accessed.

User Details



User ID: 1
Chirag

Allowed - Anti-Pass Back-soft

Device:
Panel Lite V2 -> Door V3 as F

Event Date & Time:
24/05/2018 06:14:45 PM

Department:
DFLTDPT

Designation:
DFLTDG

Events

Sr No.	Date Time	Type	Device	Category	Detail
57	24/05/2018 06:14:35 PM	Panel Lite V2	Panel Lite V2	Request	← Login Request Received.
58	24/05/2018 06:14:36 PM	Panel Lite V2	Panel Lite V2	ACK	→ Login Success Poll Duration: 3 Poll Interval: 2
59	24/05/2018 06:14:38 PM	Panel Lite V2	Panel Lite V2	Request	← Message Request Received
60	24/05/2018 06:14:38 PM	Panel Lite V2	Panel Lite V2	Command	→ Event Request for RollOver: 0 Event Seq. No.: 242
61	24/05/2018 06:14:38 PM	Panel Lite V2	Panel Lite V2	Other	← Start Of Event
62	24/05/2018 06:14:38 PM	Panel Lite V2	Panel Lite V2	Command	→ Set Date & Time
63	24/05/2018 06:14:38 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Finger. User ID: 1 Event Date Time: 24/05/2018 06:14:27 PM
64	24/05/2018 06:14:38 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 242
65	24/05/2018 06:14:38 PM	Panel Lite V2	Panel Lite V2	ACK	← Set Date & Time Command Successful
66	24/05/2018 06:14:38 PM	Panel Lite V2	Panel Lite V2	Other	→ Get Information from Device
67	24/05/2018 06:14:38 PM	Panel Lite V2	Panel Lite V2	Other	← Reply Information from Device
68	24/05/2018 06:14:38 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
69	24/05/2018 06:14:42 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Card. User ID: 1 Event Date Time: 24/05/2018 06:14:42 PM
70	24/05/2018 06:14:43 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 243
71	24/05/2018 06:14:46 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed - Anti-Pass Back-soft with Card. User ID: 1 Event Date Time: 24/05/2018 06:14:45 PM
72	24/05/2018 06:14:46 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 244

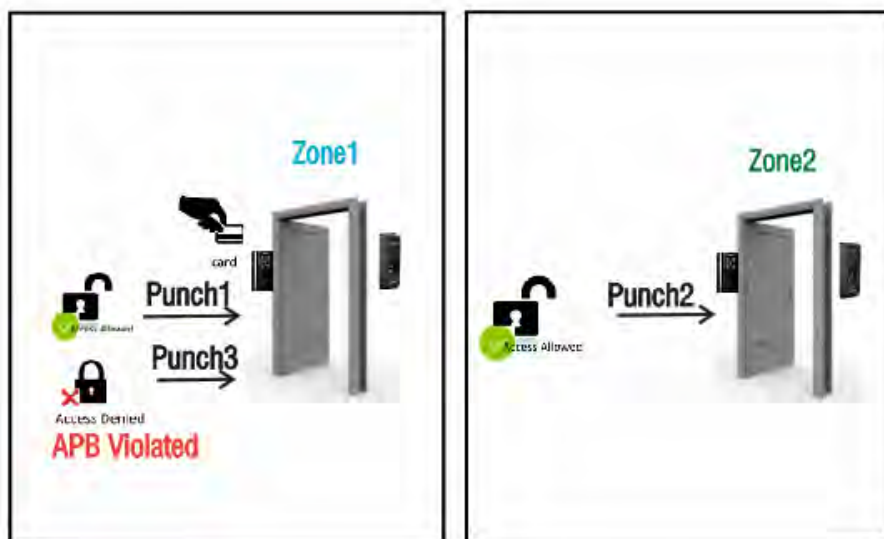
Local

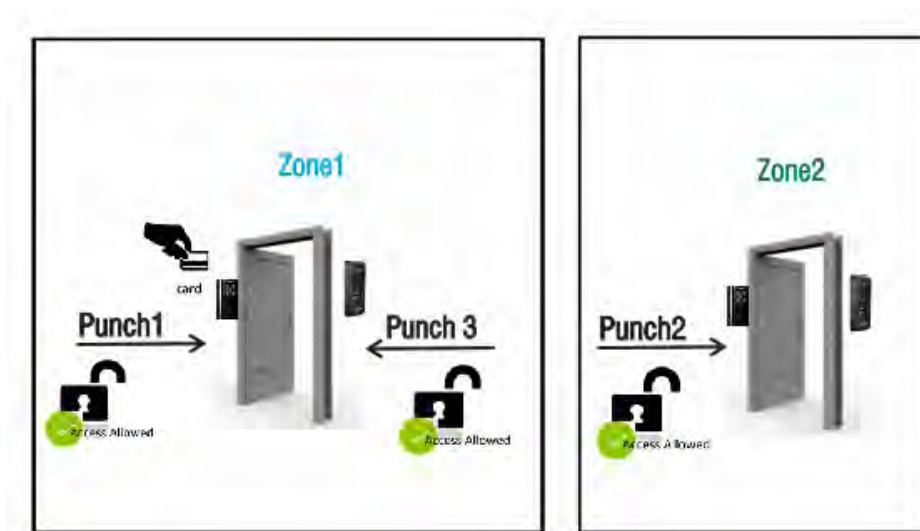
Local configuration can be used when specific zones of panel lite is to be restricted. When “Local” is selected “On Entry” then APB is monitored zone wise. So here both the zone (Production and QC zone) must be selected and configured for APB.

The image displays two side-by-side screenshots of the 'Panel Lite V2' configuration interface. Both screenshots show the 'Device' set to '3' and 'Panel Lite V2'. The 'Enable Rule' checkbox is checked. The 'Update Device' button is visible. In the left screenshot, the 'Zone' is set to 'Production Zone', 'On Entry' is 'Local', 'On Exit' is 'Local', 'Hard/Soft' is 'Soft', 'Forgiveness' is checked, 'Reset After' is 'Timer Expiry', and 'Forgiveness Timer (Mins)' is 60. In the right screenshot, the 'Zone' is set to 'QC Zone', 'On Entry' is 'Local', 'On Exit' is 'Local', 'Hard/Soft' is 'Soft', 'Forgiveness' is checked, 'Reset After' is 'Timer Expiry', and 'Forgiveness Timer (Mins)' is 60. Both screenshots have an 'Update Zone' button at the bottom.

Suppose **Door V3** is in- **Production zone** and **PVR Door** is in- **QC zone** of Panel200.

- When user1 enters Production zone through Door V3 then he will be access allowed. Then his exit punch is required from production zone i.e. exit reader of Door V3.
- Without exit punch from production zone; If the same card is used to punch on PVR door (entry punch) of QC zone then he will be allowed access because both the doors are in different zone and APB is monitored zone wise.
- But without exit punch from production zone; If the same card is used to punch on Door V3 i.e. production zone; then APB will be violated. And access will be allowed if Soft APB is configured else access will be denied if Hard APB is configured.





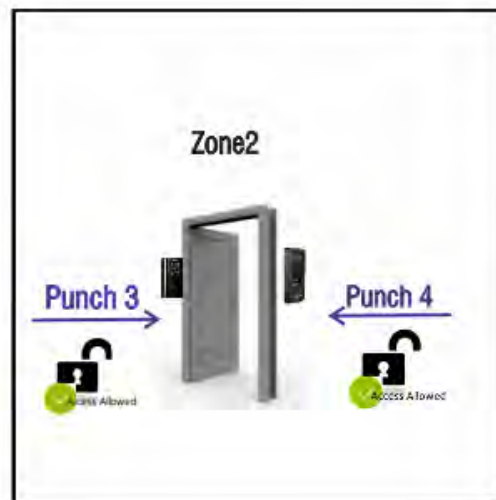
Global

Global configuration can be used when all zones of panel lite are to be restricted. When “Global” is configured “On Entry” then APB is monitored Panel Lite wise.

The image shows two side-by-side screenshots of a web-based configuration interface for an access control system. Both screenshots show the 'Device' dropdown set to '3' and 'Panel Lite V2'. The 'Enable Rule' checkbox is checked. In the left screenshot, the 'Zone' dropdown is set to 'Production Zone'. The 'On Entry' dropdown is set to 'Global' (indicated by an arrow), and 'On Exit' is set to 'Local'. The 'Hard/Soft' dropdown is set to 'Hard', 'Forgiveness' is checked, and 'Reset After' is set to 'Timer Expiry' with a '60' minute timer. The right screenshot shows the 'Zone' dropdown set to 'QC Zone'. The 'On Entry' dropdown is set to 'Global' (indicated by an arrow), and 'On Exit' is set to 'Local'. The 'Hard/Soft' dropdown is set to 'Hard', 'Forgiveness' is checked, and 'Reset After' is set to 'Timer Expiry' with a '60' minute timer. Both screenshots have an 'Update Device' button and an 'Update Zone' button.

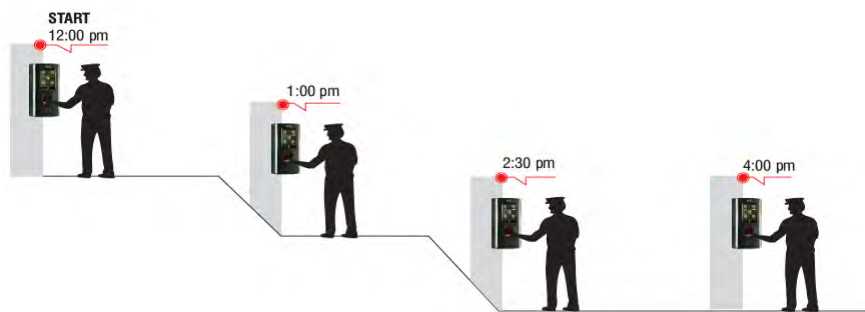
Suppose **Door V3** is in- **Production zone** and **PVR Door** is in- **QC zone** of Panel200.

- When user1 enters Production zone through Door V3 then he will be access allowed. Then his exit punch from production zone is must; only then he can access another zone of same panel lite.
- Without exit punch from production zone; If the same card is used to punch on PVR door (entry punch) of QC zone then he will be denied access.



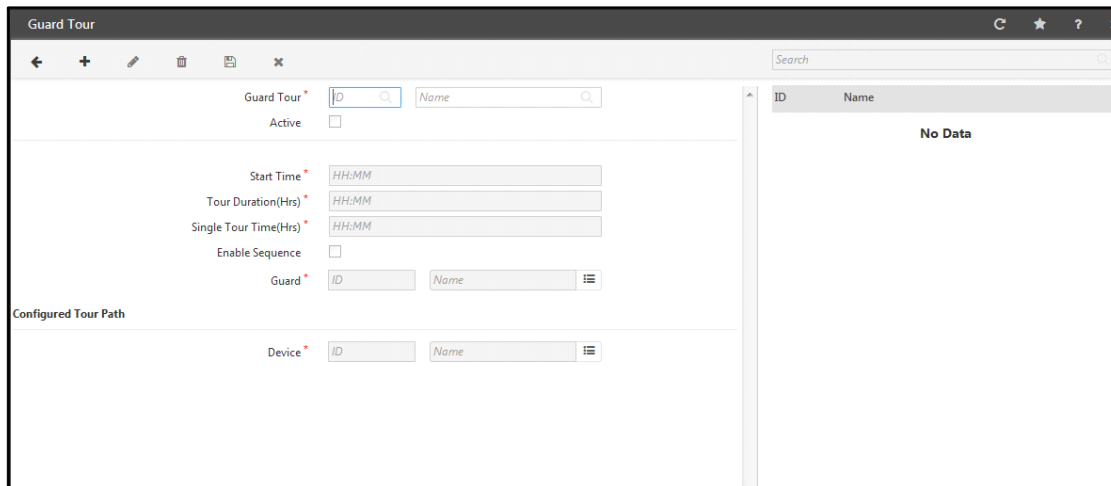
Guard Tour

Guard Tour functionality enables the system to monitor the movements of the security guards within the facility premises during the specified time periods. It is specially required to provide security during the non working hours. This is achieved by defining a series of check points or door controllers where the guard has to show the configured credential within a given amount of time. The check points can be sequenced (they must be activated in a specified order) or they can be unsequenced (they can be activated in any order).



A maximum of **99** Guard Tours and **99** member devices per Guard Tour can be configured in the system. Devices can also be repeated in the member list. The guard tour configuration is maintained at the system level and is not sent to the devices.

To use the Guard Tour feature, Click on **Guard Tour** option from the Access Control page. The page appears as shown below:



To Add a Guard Tour, Click on **Add** button.

Name: Specify a unique and descriptive Guard Tour Name.

Active: Check the box to activate the Guard tour.

Start Time: Specify the **Start Time** in **hh:mm** format for the Guard Tour when the guard will start the tour.

Tour Duration: Specify the **Tour Duration** in **hh:mm** format for the Guard Tour. It defines the time period within which a particular number of tour cycles should be completed.

Single Tour Time: Specify the time period within which the guard has to complete a single tour. Specify the single tour time in hh:mm format.

- **Example:** If Tour duration for a guard tour is 6:00 hours, start tour time is 00:00 and single tour time is 00:30 hours. And the devices defined for the tour are 4. Then the guard has to start the tour from 00:00 and have to cover all the four check points(4 devices) within 30 minutes. This tour cycle will continue for 6 hours i.e. the duration of the tour.

Enable Sequence: The guard tour can be defined as sequenced or un-sequenced by checking or unchecking the Enable Sequence box.

In case of the sequenced option the Guard has to go to the devices in the sequence as mentioned in the member list in the grid below.

Guard: Select the user whose credentials will be used for the guard tour from the User Master picklist window.

Now user needs to define the Member devices which would be part of the Guard tour being defined.

Click on the **Add device** button and select the devices from the **Device Selection** pop up window by checking the boxes against the devices which are to be added as members in the guard tour configuration.

Select Device

Total Selected : 0 Records

Search [Show Selected](#)

<input type="checkbox"/>	MID ▲	Name	Type
<input type="checkbox"/>	2	Main Door	PVR Door
<input type="checkbox"/>	7	Vega Device-Second Floor	Vega Controller
<input type="checkbox"/>	1	Door V3-Ground Floor	Door V3
<input type="checkbox"/>	5	Door V4-First Floor	Door V4

OK Cancel

Click on **OK** to add the devices into the list in the bottom grid.

Seq.	Device ID	Name	Up/Down	
1	2	Main Door	▼	🗑️
2	7	Vega Device-Second Floor	▲▼	🗑️
3	1	Door V3-Ground Floor	▲▼	🗑️
4	5	Door V4-First Floor	▲	🗑️

Click on **Save** button to add the Tour to the list in the right grid. The **ID** will be automatically generated.

ID	Name
1	Guard Tour 1
2	Gaurd Tour

The user can change the sequence of Devices by clicking on **Up/Down** arrow to move the devices up or down the list. The device not required in guard tour can be deleted by clicking on **Delete** button.



User needs to ensure that the door controllers are added in the sequence which the Guard needs to cover in the tour (required only if the **Sequence** box is checked).

Access Route

The Access Route functionality enables the administrator to define an access policy which allows the user to access only specified doors (applicable to Panel200 and Panel doors) with specified levels in predefined route, sequenced or unsequenced.

The COSEC system has the capability to define up to maximum **255** routes and **255** doors on a single route.



*This functionality can also be enabled from the **Device Module > Device Configuration > Features** and **User Module > User Configuration > Devices > Configure**.*

To use the Access Route feature, Click on **Access Route** option from the Access Control page. The page appears as shown below:

Panel: Select the Panel from the picklist on which the Access Route feature is to be configured.

Click **New** button from the toolbar to configure the route.

Access Route: Specify a unique and descriptive name for the route. The Access Route ID is auto-generated and cannot be edited by the user.

Active: Check the Active box to activate the Access Route.

Sequence Route: The Access Route can be sequenced or unsequenced. Check this box if you require the configured route to be Sequenced.

In sequenced route the system checks the route based on the levels defined. For e.g. the user has to swipe the credential on a Level 1 door and then go to Level 2, Level 3 and so on. In this case the order needs to be maintained for both the “IN” as well as the “OUT” punches. Therefore it is necessary to have exit readers installed on all the doors of the access route.

Restrictions: Select the Restriction option from the drop down list as per the site requirements.

This functionality can operate in two modes:

- **Hard:** Access will be allowed only if the access route is followed.
- **Soft:** Access will be allowed on any door on the access route with an access route violation message.

Reset On Start Level: Check the box to enable the system to reset the current level status to allow access on the lowest level.

This option is useful in the event of the user not following the proper order while exiting the premises. If this functionality is enabled then the user will be allowed access on the lowest level irrespective of his/her state but this will happen only on entry side.

Check on Last Exit Level: Select the checkbox, if you want the system to check the Lowest Route Level Door accessed by the User during exit.

If enabled, then the system will check whether any violation has occurred during Access Route Cycle (i.e. from Entry to Exit).

If any violation has not occurred during the Cycle, then the User will be allowed to access the Lowest Level door.

If any violation has occurred during the Cycle, then the system will allow/deny the access to the User as per the option configured in “Last Exit Level Restriction” option.

Last Exit Level Restriction: Select the Last Exit Level Restriction option from the drop down list as per the site requirements.

- **Hard:** The access will be denied if the Access Route is not followed by the User while he/she exits.
- **Soft:** The access will be granted even if the Access Route is not followed by the User while he/she exits, with an Access Route Violation Alert.

Configured Route

Click **Add** button to add the doors to the route.

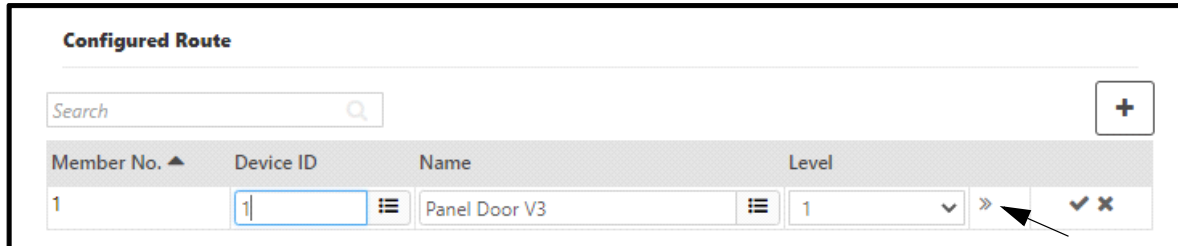
The screenshot shows a web interface titled "Configured Route". At the top, there is a search bar with the placeholder text "Search". To the right of the search bar is a button with a "+" sign. Below the search bar is a table with the following columns: "Member No.", "Device ID", "Name", and "Level". The first row of the table contains the values: "1", "1", "Panel Door V3", and "1". There are also some icons and a dropdown arrow in the "Level" column. An arrow points to the "+" button, and another arrow points to the "Device ID" field in the first row.

Device ID: Click on the Picklist button and select the Device ID of the Panel door to be added to the route.

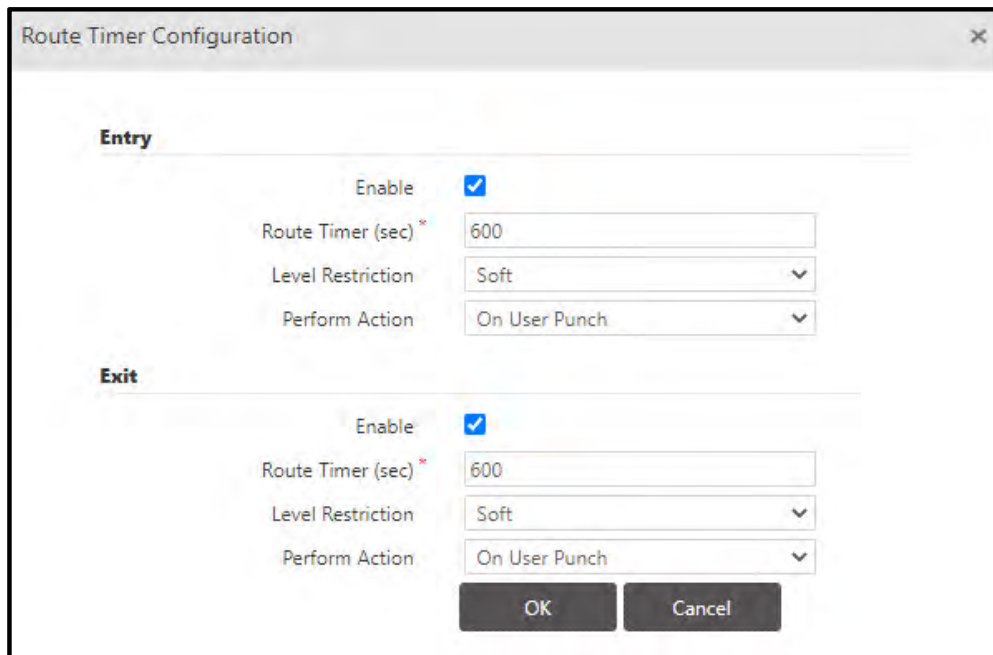
Name: Click on the Picklist button and select the Panel door to be added to the route.

Level: Select the Level number for the Door from the drop down list. Multiple Doors can be assigned to a single level. However, the same door cannot be assigned to multiple levels.

Now click on **Route Timer Configuration**  button.



A pop-up of **Route Timer Configuration** appears as shown below:



Entry

Enable: Select this checkbox to enable Access Route Timer and Restrictions while the User enters.

Route Timer (sec): This is the time within which the User needs to access the next configured door defined in the respective route.

Enter the value of Timer as per your requirement.

Level Restriction: Select the Level Restriction option from the drop down list as per the site requirements.

- **Hard:** The User will not be allowed to access the door. Additionally, an Alarm will be raised for the violation of Access Route Timer Policy.

- **Soft:** The User will be allowed to access the door, however an Alarm will be raised for the violation of Access Route Timer Policy.

Perform Action: Select the desired option from the drop down list.

- **On User Punch:** Access Route Timer Violation Alarm as well as an Alert (if configured) will be generated once the User punches on the next Route Level Door after the configured Route Timer, which violates the Access Route Timer Policy.
- **On Timer Elapsed:** Access Route Timer Violation Alarm as well as an Alert (if configured) will be generated automatically once the User fails to punch within the configured Route Timer, which violates the Access Route Timer Policy.

Exit

Enable: Select this checkbox to enable Access Route Timer and Restrictions while the User exits.

Route Timer (sec): This is the time within which the User needs to access the next configured door defined in the respective route.


Level Restriction: Select the Level Restriction option from the drop down list as per the site requirement.

This functionality can operate in two modes:

- **Hard:** The User will be denied to access the door. Additionally, an Alarm will be generated for the violation of Access Route Timer Policy.
- **Soft:** The User will be allowed to access the door, however an Alarm will be generated for the violation of Access Route Timer Policy.

Perform Action: Select the desired option from the drop down list.

- **On User Punch:** Access Route Timer Violation Alarm as well as an Alert (if configured) will be generated once the User punches on the next Route Level Door after the configured Route Timer, which violates the Access Route Timer Policy.
- **On Timer Elapsed:** Access Route Timer Violation Alarm as well as an Alert (if configured) will be generated automatically once the User fails to punch within the configured Route Timer, which violates the Access Route Timer Policy.

Click  button to save the added door.

Similarly add other panel doors to the route as shown below.

Configured Route				
<input type="text" value="Search"/>				+
Member No. ▲	Device ID	Name	Level	
1	1	PVR Paneldoor	1	
2	2	Path Paneldoor	1	
3	4	Vega Paneldoor	2	

The Door which is not required in the route can be deleted from the **Delete** button.

Finally click on Save button to save the configured Access Route. The route will be listed in grid on right side.

Access Route

←

+

✎

🗑

📄

✕

Search

Panel *

2

HO Panellite V2

Access Route *

2

Head Ofc Route

Active

☒

Sequenced Route

☒

Restrictions

Soft

Reset On Start Level

☒

Configured Route

Search

+

Member No. ▲	Device ID	Name	Level	
1	1	PVR Paneldoor	1	✎ 🗑
2	2	Path Paneldoor	1	✎ 🗑
3	4	Vega Paneldoor	2	✎ 🗑

ID ▲

Name

2

Head Ofc Route

Functional Group

The Functional Group feature is used to group users with similar profiles and access policies to help the System administrators in better managing the security and access control policies of a site.

This user grouping is used in assigning the activation rights of the Special Functions as explained in the “**Special Function**” section of this manual.

These groups are usually classified based on the roles they perform. A maximum of 99 functional groups can be created in the system.

To use the Functional Group feature, Select **Access Control module > Functional Group**. The page appears as shown below:

The screenshot shows the 'Functional Group' management window. It has a toolbar with icons for back, add, edit, delete, save, and close. Below the toolbar, there are two input fields: 'Functional Group *' with a value of '1' and a search icon, and 'Name' with a value of 'Staff' and a search icon. On the right, there is a table with two columns: 'ID' and 'Name'. The table contains two rows: ID 1 with Name 'Staff' and ID 2 with Name 'Visitor'.

ID	Name
1	Staff
2	Visitor

The system creates two default functional groups viz. **Staff** and **Visitor**.

To create a new Functional Group, Click on **New** button. The following window appears on your screen.

The screenshot shows the 'Functional Group' management window after clicking the 'New' button. The 'Functional Group *' field now has a value of '3' and the 'Name' field has a value of 'RnD'. The table on the right now has three rows: ID 1 with Name 'Staff', ID 2 with Name 'Visitor', and ID 3 with Name 'RnD'.

ID	Name
1	Staff
2	Visitor
3	RnD

Functional Group: Specify a user friendly name for the new Functional Group. The ID appears by default and cannot be edited by the user.

Click on **Save** button. The functional Group will be created as shown in the grid.

Administrator can now assign the users to the respective functional groups from the **User Module>User Configuration> Devices**. The users belonging to these functional groups can then be assigned to activate certain Special functions.

Time Schedule

Time Schedule allows the system to grant access to the users to certain Access Zone only in a specified time period. This time period can be set to a full 24-hours or any limited set of hours or minutes. You can create maximum **99** time schedules.

Each time zone represents a particular period of time and time zones may have overlapping time periods. The maximum time period which can be assigned to a time zone is **23:59** hours.

To use the Time Schedule feature, Click on **Access Control > Time Schedule**. The page appears as shown below:

The screenshot displays the 'Time Schedule' configuration window. It includes a toolbar with icons for back, add, edit, delete, save, and close. A search bar is located in the top right. The main form contains the following fields:

- Time Schedule***: A dropdown menu with the value '2'.
- Name**: A text input field containing 'Lunch Time'.
- Active**: A checkbox that is checked.
- Start Time**: A time input field set to '13:00'.
- End Time**: A time input field set to '15:00'.
- Active Days***: A set of checkboxes for days of the week: Sun (unchecked), Mon (checked), Tue (checked), Wed (checked), Thu (checked), Fri (checked), Sat (checked), and Holiday (unchecked).

On the right side, there is a table listing existing time zones:

ID	Name
1	Time Zone-1
2	Lunch Time
3	Maintenance Zon
4	Working Shift

To create a new Time Schedule, Click on **New** button.

Time Schedule: Specify a user friendly name for the new Time Schedule. The ID will be auto-generated when the time schedule is saved.

Active: Check the box to activate the Time Schedule.

Start Time-End Time: Specify the Start and End time period (in hh:mm) for particular Time Schedule for the below selected day/s.

Active Days: Check the days box for which the Time schedule is to be activated.

Click on **Save** to save the time schedule configurations.

This time schedule can be assigned to the user in Access Profile while configuring schedule based Access level override. See *Access Profile* for details.

Time Schedule Group

You can create maximum **99** time schedule groups.

To use the Time Schedule Group feature, Click on **Access Control > Time Schedule Group**. The page appears as shown below:

Sr. No.	ID	Time Schedule	Active	Start Time	End Time	Active Days	
No Data							

To create a new Time Schedule Group, Click on **New** button.

Time Schedule Group: Specify a user friendly name for the new Time Schedule Group. The ID will be auto-generated when the time schedule group is saved.

Time Schedule: Click the pick-list and select the time schedules as created from Time Schedule page. The time schedules will be listed in the grid showing the Start and End time on the Active days. You can add maximum **9** time schedules per time schedule group.

Sr. No.	ID	Time Schedule	Active	Start Time	End Time	Active Days	
1	1	Time Zone-1	Yes	09:00	18:00	Su Mo Tu We Th Fr Sa PH	
2	2	Time Zone-2	Yes	07:00	14:00	Mo Tu We Th Fr	

Click on **Save** to save the time schedule group.



Same Time Schedule can be added in multiple Time Schedule Groups.

Time Schedule Group

✓ Saved Successfully

← + ✎ 🗑️ 📄 ✕

Time Schedule Group * 1 Emp Group

Configure Time Schedule

Time Schedule * ID Name

Search

Sr. No. ▲	ID	Time Schedule	Active	Start Time	End Time	Active Days	🗑️
1	1	Time Zone-1	Yes	09:00	18:00	Su Mo Tu We Th Fr Sa PH	🗑️
2	2	Time Zone-2	Yes	07:00	14:00	Mo Tu We Th Fr	🗑️

Search

ID ▲	Name
1	Emp Group

Elevator Configuration

In high-rise corporate buildings; Elevators can be integrated with the Access Control Solution. This enables employees/users to access the specific areas or floors of buildings in-order to ensure company's security and employees' convenience.

Elevator configuration enables to create the elevators and assign floors to the elevators. You can add maximum **24** Elevators in a Panel200.

To configure the Elevator Configuration, Click on **Access Control > Elevator Access Control> Elevator Configuration**. The page appears as shown below:

The screenshot shows the 'Elevator Configuration' web application. It features a top navigation bar with a search field. Below the navigation bar, there are several configuration sections: 'Panel' with ID and Name fields, 'Elevator' with ID and Name fields, 'Authentication Device' with ID and Name fields, and 'Access Duration For Floor(s)' with a numeric input field (1-99) and a '(secs)' label. A 'Floor Configuration' section contains a search field and a table with columns: Floor No., Floor Name, Free Access Floor, Device ID, Name, and Output Port. The table currently shows 'No Data'. On the right side of the interface, there is a table with columns ID and Name, also showing 'No Data'.

Select the Panel200 from the pick-list. The Panel200 must be enabled for "Elevator Access Control" feature from Device Configuration> Features.

Now click on **New** button.

Elevator: Enter the name for the elevator. You can add maximum 24 elevators.

Authentication Device: Click the pick-list and select the Panel200 door which will act as authentication device to access the Elevator. The authentication device must be placed inside the Elevator so it is recommended to select another authentication device for another Elevator.

Once the user credential is verified on Authentication device; only then floor selection buttons will become active. The supported doors for Authentication device are: **Door V1,Door V2,Door V3,Door V4,Vega Controller, Path Controller, PVR Door, ARC DC100.**

Access Duration For Floors: Enter the Access duration in seconds (1 - 99). The default time is 10 seconds. It is the duration for which floor selection buttons in Elevator will remain active for the selection.

If the floor is not selected within this access duration then selection buttons will become disable. Then user has to punch on authentication device again for activating floor selection buttons.

Elevator Configuration

Panel * 1 Panel Lite V2

Elevator * 1 Elevator1

Authentication Device * 1 Vega Panel Door

Access Duration For Floor(s) * 10 (secs)

Floor Configuration

Search +

Floor No.	Floor Name	Free Access Floor	Device ID	Name	Output Port
No Data					

Floor Configuration

Click on **Add** button to add the floors to the Elevator. You can add maximum **64** floors to an Elevator.

Elevator Configuration

Panel * 1 Panel Lite V2

Elevator * 1 Elevator1

Authentication Device * 1 Vega Panel Door

Access Duration For Floor(s) * 10 (secs)

Floor Configuration

Search +

Floor No.	Floor Name	Free Access Floor	Device ID	Name	Output Port
1	Ground Floor	<input checked="" type="checkbox"/>	2	ARC IO800	None

None
Aux. Output 1
Aux. Output 2
Aux. Output 3
Aux. Output 4
Aux. Output 5
Aux. Output 6
Aux. Output 7
Aux. Output 8

Floor No.- It is auto generated by system. You can also change the floor number if required.

Floor Name: Specify the name of the floor.

Free Access Floor: Enable this check-box to allow the floor to be accessed freely by everyone.

Device ID/Name: Click the pick-list and select the ARC IO800 Panel200 door.

Output Port: Select the Aux output port from the drop down options which is to be connected to the respective floor of the Elevator.

You can also connect one Aux Output Port to multiple floors.

Example: If a user is to be given access to Floors 1, 3 and 5; then one Aux Port say Aux Output1 can be connected to floor1,3 and 5.

Click **OK**. Similarly configure other floors and click **Save** button to save the Elevator configuration.

Elevator Configuration
✔ Saved Successfully

Panel * 1

Elevator * 1

Authentication Device * 1

Access Duration For Floor(s) * 10 (secs)

Panel Lite V2

Elevator1

Vega Panel Door

Floor Configuration

+

Floor No. ▲	Floor Name	Free Access Floor	Device ID	Name	Output Port	
1	Ground Floor	Yes	2	ARC IO800	Aux. Output 1	
2	Canteen Floor	Yes	2	ARC IO800	Aux. Output 2	
3	Telecom Floor	No	2	ARC IO800	Aux. Output 3	

ID ▲	Name
1	Elevator1

Similarly you can add other Elevators to the Panel200 as shown below.

Elevator Configuration
✔ Saved Successfully

Panel * 1

Elevator * 2

Authentication Device * 3

Access Duration For Floor(s) * 10 (secs)

Panel Lite V2

Elevator2

Door V3 as Panel Door

Floor Configuration

+

Floor No. ▲	Floor Name	Free Access Floor	Device ID	Name	Output Port	
1	Ground Floor	Yes	2	ARC IO800	Aux. Output 4	
2	Surveillance Fl	No	2	ARC IO800	Aux. Output 5	
3	Hardware Floor	No	2	ARC IO800	Aux. Output 6	

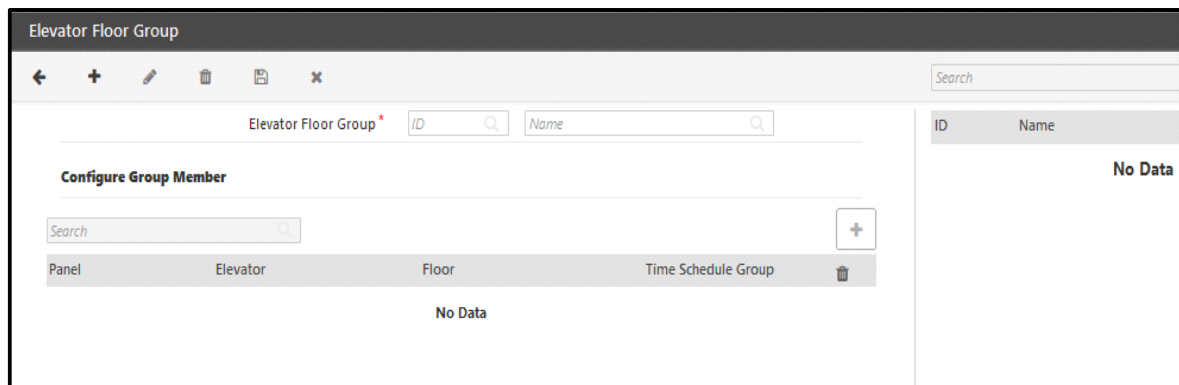
ID ▲	Name
1	Elevator1
2	Elevator2

Elevator Floor Group

Elevator Floor Group enables to create the group of floors. The floors can be of same Elevator or different Elevators. This Elevator floor group is then assigned to the user. The user can access the floors included in the group.

You can configure maximum **99** Elevator Floor Groups.

To configure the Elevator Floor Group, Click on **Access Control > Elevator Access Control> Elevator Floor Group**. The page appears as shown below:



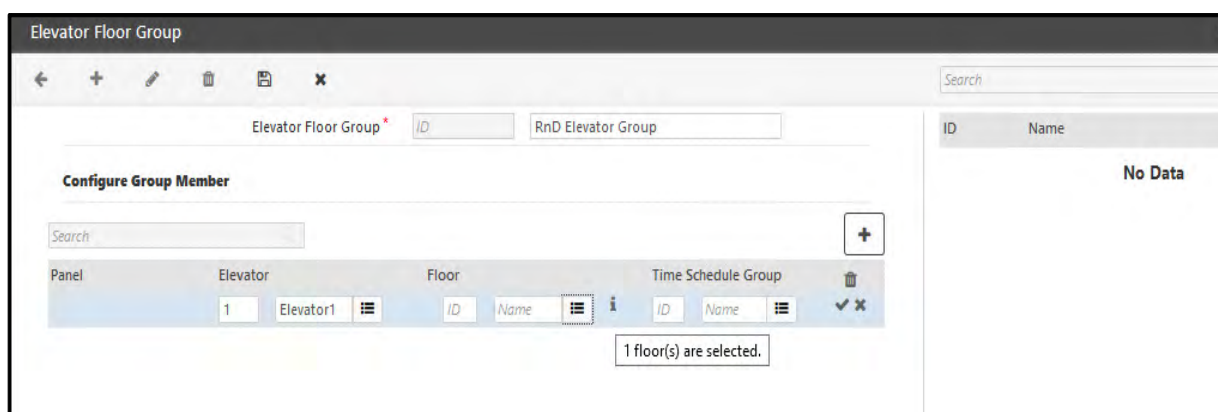
To create a new Elevator Floor Group, Click on **New** button.

Elevator Floor Group: Specify a user friendly name for the Elevator Floor Group. The ID will be auto-generated when the group is saved.

Configure Group Members

Click on **Add** button to add the floors of the Elevator to the Group. Max **999999** members can be added to the group.

Click the pick-list and select the **Elevator**. Then select the **Floor** of that Elevator from the floor pick-list.



Now click the picklist and select the **Time Schedule Group**.

Click on **OK** to save the group member.

Example: Telecom Floor of Elevator1 is selected and Emp Group is assigned as the Time Schedule group. So Telecom Floor can be accessed by Elevator1 in the time zones available in Emp Group.

Similarly you can add other group members.



Time Schedule Group is created from Access Control > Time Schedule Group.

Click on **Save** to save the Elevator Floor Group as shown below.



Same Elevator, Floor & Time Schedule Group combination can coexist in multiple Elevator Floor Groups but not in same group.



If no time zone group is assigned then that particular floor of the elevator will be accessible throughout the day.



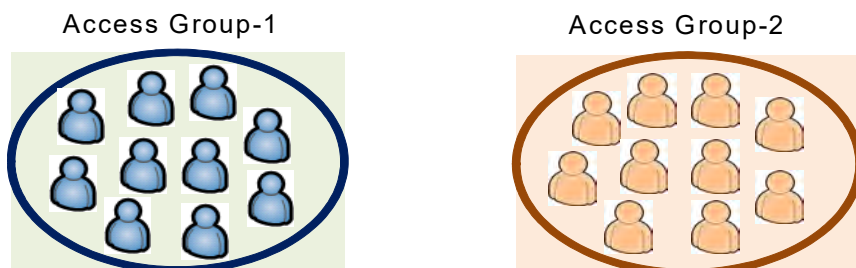
The Access to the Elevators can be viewed in Elevator Access Report and it can also be scheduled in Report Scheduler.

Access Profile

Access Profile defines the group of users having similar job functions and need equal privileges throughout the day.

Access Groups having Time Zone based Access Levels programmed, when assigned to any user, enables the system to determine user Access Level at any particular time.

System Access Policy compares User's Access Level with Zone's Access Level before the user is Allowed or Denied to access the restricted areas. A maximum of **99** Access Groups can be defined in the system.



Once the Access Groups are defined, the system administrator can define the Users from **User Module > User Configuration**.

To use the Access Profile feature, Select **Access Control module > Access Group > Access Profile**. The page appears as shown below:

The screenshot shows the 'Access Profile' configuration interface. At the top, there's a header bar with navigation icons and a search field. Below the header, the 'Access Profile' section includes a dropdown for 'Access Profile' (set to 'ID'), a 'Name' field, and an 'Active' checkbox. The 'User Access Levels' section contains three dropdown menus for 'Work Hours', 'Break Hours', and 'Non-Working Hours', all currently set to '8'. Below this is a 'Schedule Based Access Level Override' section. At the bottom, there's a table with columns: Member, ID, Time Schedule, Status, and Access Level. The table is currently empty, showing 'No Data'. On the right side of the window, there's a sidebar with a table listing the two default access groups:

ID	Name
1	Group-1
2	Group-2

The Group-1 and Group-2 are default Access Groups which are predefined and have an access level of 8.

To define a new **Access Group**, click on the **New** button. The following window appears on your screen.

Access Profile

Access Profile: 3 RnD Employees

Active: ☒

User Access Levels

Work Hours: 9

Break Hours: 8

Non-Working Hours: 8

Schedule Based Access Level Override

Member ID	ID	Time Schedule	Status	Access Level
1	1	Time Zone-1	InActive	8
2	1	Time Zone-1	InActive	8
3	1	Time Zone-1	InActive	8
4	1	Time Zone-1	InActive	8
5	1	Time Zone-1	InActive	8

1 - 5 of 8 records

« < 1 2 > »

Search

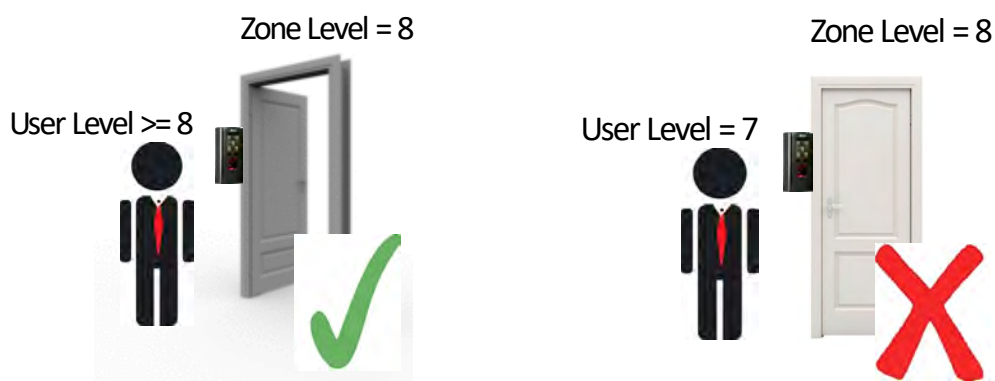
ID	Name
1	Group-1
2	Group-2

Access Profile: Enter a user friendly name for the new Access Profile in the Name field. The ID appears automatically.

Active: Check the box to activate the Access Profile.

User Access Levels

The access level of the user is compared to the access level of the zone and user is granted access only if user access level is greater than or equal to the access level of the zone. Either the User Access Levels or the Schedule Based Access Levels will work at a time.



Work Hours: Specify the Access Level for the Working hours ranging from **01 to 15** from the drop down list.

Break Hours: Specify the Access Level for the Break hours ranging from **01 to 15** from the drop down list.

Non- Working Hours: Specify the Access Level for the Non- Working hours ranging from **01 to 15** from the drop down list.

Example:

If shift is defined from 9am to 6pm and Access Level for Work Hours is set at **9**, Access Level for Break Hours is set at **8**, Access Level for Non-Working Hours is set at **8**, Access Level for the Panel Door is set at **9** in Zone3 (Not Home zone)

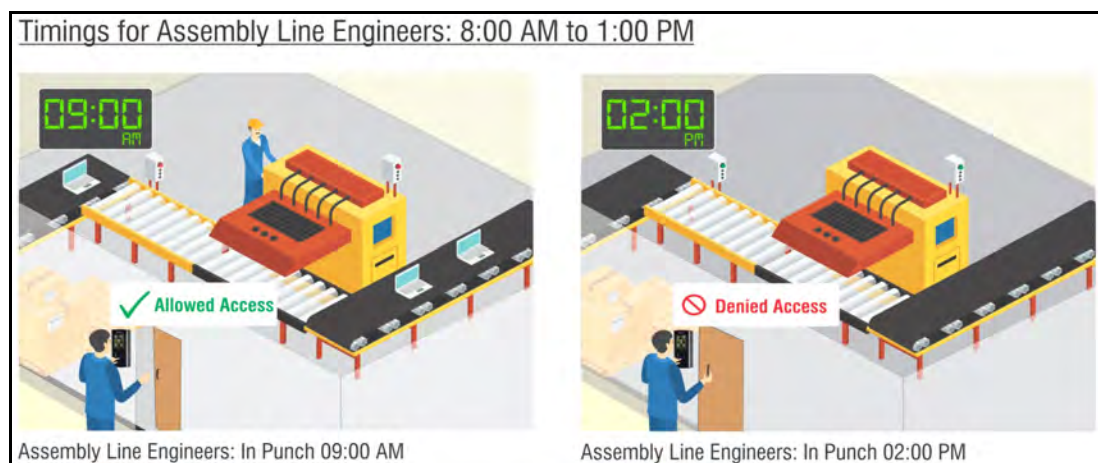
Case1: Then if employee punches between 9 to 6, he will be allowed access.

Case2: If employee punches before 9am, he will be denied access as access level for Non-working hours (8) is less than the access level of Door(9).

Case3: If employee punches during break hours, he will be denied access as access level for Break hours (8) is less than the access level of Door(9).

Schedule Based Access Level Override

Sometimes it is essential for certain groups to have access to a particular zone in Multiple Time Slots. The Time Zone based Access Levels allows user to configure such additional time slots for certain groups to have access to various zones during different time periods of the day.



Click on the Member to select the time schedule for which the group is to be activated based on the access level.

Time Schedule: Select the time zone from the picklist. To configure Time Schedule click Access Control > Time Schedule.

Status: Check the box to activate the Time Zone.

Access Level: Select the Access Level for the Time Zone ranging from 1 to 15 from the drop down list.

Schedule Based Access Level Override					
Member	ID	Time Schedule	Status	Access Level	
1	4	Working Shift	<input checked="" type="checkbox"/>	9	<input type="checkbox"/> <input type="checkbox"/>
2	1	Time Zone-1	InActive	8	<input type="checkbox"/>
3	1	Time Zone-1	InActive	8	<input type="checkbox"/>
4	1	Time Zone-1	InActive	8	<input type="checkbox"/>
5	1	Time Zone-1	InActive	8	<input type="checkbox"/>

1 - 5 of 8 records

<< < 1 2 > >>

Click on **OK** and **Save** the Changes. The Time schedule for “Working Shift” and “Lunch Time” zones is activated for the RnD Employees group as shown below.

Access Profile

←

+

✎

🗑

📄

✕

Search

ID

Name

1

Group-1

2

Group-2

3

RnD Employees

Access Profile *

3

RnD Employees

Active

☒

User Access Levels

Work Hours

9

Break Hours

8

Non-Working Hours

8

Schedule Based Access Level Override

Member	ID	Time Schedule	Status	Access Level	
1	4	Working Shift	Active	9	<input type="checkbox"/>
2	2	Lunch Time	Active	9	<input type="checkbox"/>
3	1	Time Zone-1	InActive	8	<input type="checkbox"/>
4	1	Time Zone-1	InActive	8	<input type="checkbox"/>
5	1	Time Zone-1	InActive	8	<input type="checkbox"/>

1 - 5 of 8 records

<< < 1 2 > >>

If the Access level of Panel Door at the configured zones is 9 then employees belonging to RnD Employees profile can access the Working Shift zone and Lunch Time zone as the access level for user is 9.

For assigning users to the Access Profile see *Access Group > Assignment*.



Either the User Access Levels or the Schedule Based Access Levels will work at a time. For example: If Access level of Break is 8; then employee will not be allowed to access in break hours. But the Lunch Time Zone has access level 9, so the employee will be allowed to access the lunch area.

Access Profile Assignment

Access Profile Assignment enables to assign Access Group to Users and Devices.

To use the Access Profile Assignment feature, Select **Access Control module > Access Group > Assignment**. There are two modes of Access Profile Assignment:

- Device-Wise
- User-Wise

Device -Wise Configuration

Device: Select the Device (*Panel200*) from the device selection picklist to which the rule is to be assigned. The assigned users on the selected device will appear in the grid as shown below:

The screenshot shows the 'Access Profile Assignment' window with the 'Device - Wise' tab selected. The 'Device' field is set to '3' and 'Panel Lite V2'. The 'User' and 'Access Profile' fields are empty. An 'Update' button is visible. Below the fields is a search bar and a table with the following data:

User ID	Name	Access Profile
1	Chirag	Group-1
101	Khushbu	Group-1
1687	Aditi Ajay Gupta_Ahmedabad	Group-1

User: The single or multiple users can be selected from the picklist to which Access Profile is to be assigned. The number of selected users will be displayed on hovering over INFO icon.

Access Profile: You can select the Access profile from the picklist which is to be assigned to the selected users on the selected Panel200. The profile is created from Access Group > Access Profile.

Example: The 2 users are selected as shown by INFO icon. The default Access Profile of users is Group-1 which is displayed in the grid. Now the Access Profile for the users to be assigned on Panel200 is selected as "Group- 2" as shown below.

This screenshot shows the same window as the previous one, but with changes. The 'Access Profile' field is now set to '2' and 'Group-2'. An arrow points to the 'Group-2' picklist. Another arrow points to the 'INFO' icon in the 'User' field, which now displays a tooltip: '2 User(s) are selected'. The table below remains the same:

User ID	Name	Access Profile
1	Chirag	Group-1
101	Khushbu	Group-1
1687	Aditi Ajay Gupta_Ahmedabad	Group-1



The Access Profile for a User on a device can be set from User Module > Devices > Configure.

Click on **Update** to save the assignment. The Access profile will be processed and updated as shown below.

User ID ▲	Name	Access Profile
1	Chirag	Group-2
101	Khushbu	Group-2
1687	Aditi Ajay Gupta_Ahmedabad	Group-1

User -Wise Configuration

User: Select the User from the picklist to whom the Access Profile is to be assigned.

The assigned devices on the selected user will appear in the grid as shown below:

Device ID ▲	Name	Access Profile
3	Panel Lite V2	Group-2
4	Panel Lite	Group-1

Device: The single or multiple devices (Panel200) can be selected from the picklist to which the Access Profile is to be assigned. The number of selected devices will be displayed on hovering over INFO icon.

Access Profile: You can select the Access Profile from the picklist to assign on the selected devices for the selected user. The profile is created from Access Group > Access Profile.

Access Profile Assignment

Device - Wise

User - Wise

User *

101

Khushbu

Device *

ID

Name

Access Profile *

3

RnD Group

Update

1 Device(s) are selected

Search

Device ID ▲	Name	Access Profile
3	Panel Lite V2	Group-2
4	Panel Lite	Group-1

Click on **Update** to save the assignment. The Access Profile will be processed and updated as shown below.

Access Profile Assignment

✓ Process Completed.

Device - Wise

User - Wise

User *

101

Khushbu

Device *

ID

Name

Access Profile *

ID

Name

Update

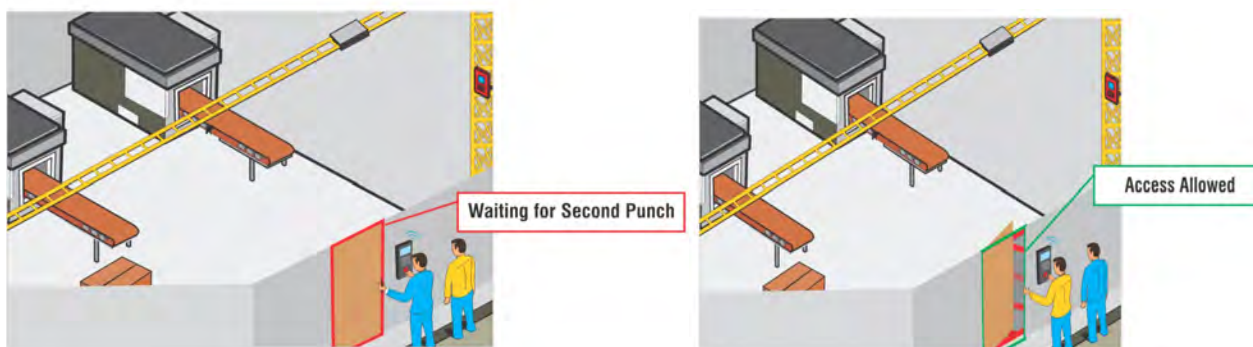
Search

Device ID ▲	Name	Access Profile
3	Panel Lite V2	RnD Group
4	Panel Lite	Group-1

2 Person Group

'2-Person' rule is a feature that enables the system to insist for two valid user entries within specified time to allow access to a secured zone.

This is a control mechanism, designed to achieve a high level of security, especially for critical areas like Cash rooms, R&D Labs, sensitive documents storage etc.



This functionality can also be enabled from the **Device Module > Device Configuration > Features** option.

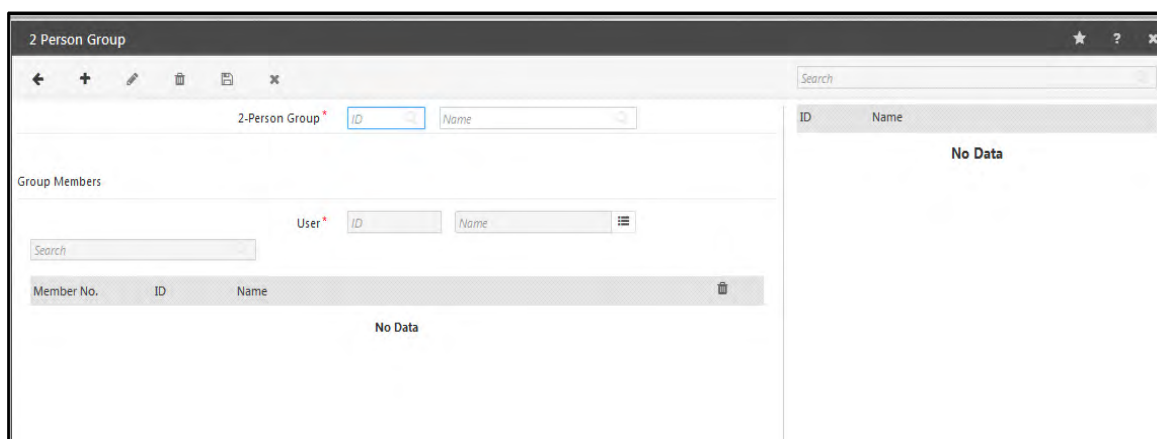


Visitors with or without Escort are not allowed into a zone where 2-person rule is enabled while a VIP user can always enter a 2-person rule enabled zone without the need for a second credential.



If the first person is an authorized user and the 2nd person is a VIP then, system considers the VIP as an authorized 2nd person to validate the 2 -person rule.

To use the '2-Person' rule, Click on **Access Control module > 2-Person Rule > Group**. The page appears as shown below:



To create a new Group, Click on **New** button. You can create upto 9999 Groups.

The following window appears.

The screenshot shows a window titled "2 Person Group" with a toolbar containing icons for back, add, edit, delete, save, and close. Below the toolbar, there are two input fields: "2-Person Group" with the value "1" and "QA Group". To the right is a search bar. The main area is divided into two sections. The left section, titled "Group Members", contains a "User" section with "ID" and "Name" input fields and a "Picklist" button. Below this is a search bar and a table with columns "Member No.", "ID", and "Name". The table is currently empty, showing "No Data". The right section is a table with columns "ID" and "Name", also showing "No Data".

2 person Group: Specify a user friendly name for the Group. The Group ID will be generated by the system and cannot be edited by the user.

Group Members

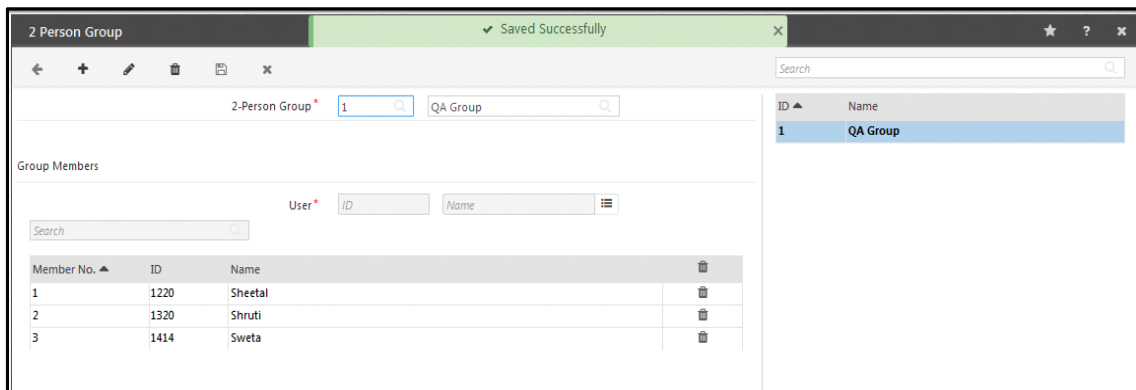
User: Click on the **Picklist** button and select the Users for the Group one by one. You can define upto 20 person per group.

The screenshot shows the same "2 Person Group" window, but now the "Group Members" table is populated with three rows of data. The table has columns "Member No.", "ID", and "Name". The data is as follows:

Member No.	ID	Name
1	1220	Sheetal
2	1320	Shruti
3	1414	Sweta

The "User" section and the right-hand table remain the same as in the previous screenshot.

Click on **Save** button from the toolbar. The Group with **2 person Rule** will be saved in the right grid as shown below:



Create the other groups same as above.



Zone Access Mode (ZAM) is applied on both users while verifying for 2-person group authorization. ZAM is not applied on VIP user under any condition.

To assign Groups to doors, refer [“2 Person Rule Assignment”](#).

2 Person Rule Assignment

2 Person Rule Assignment enables to assign 2 Person Rule to Users and Devices.

To use the 2 Person Rule Assignment feature, Select **Access Control module > 2 Person Rule > Assignment**. The page appears as shown below:

The screenshot shows the '2-Person Rule Assignment' window. On the left, there are input fields for 'Device' (containing 'ID'), 'Name' (empty), 'Enable Rule' (checkbox), 'Zone' (dropdown menu), 'Enable Rule On Zone' (checkbox), 'Primary Group' (dropdown menu), 'Secondary Group' (dropdown menu), and 'Mode' (dropdown menu). There are 'Update Device' and 'Update Zone' buttons. On the right, there is a search bar and a table of devices.

ID	Name
1	Door V3
1	R and D PanelliteV2
2	Vega Directdoor
3	Path-Direct door

The grid on the right shows all the devices including Panel200 and Direct Doors set to Advanced Access Control.

Click on the device from the grid, the related parameters will appear in the respective fields as shown below for Panel200:

The screenshot shows the '2-Person Rule Assignment' window with the configuration for the selected device 'R and D PanelliteV2'. The 'Device' field now contains '1' and the 'Name' field contains 'R and D PanelliteV2'. The 'Enable Rule' checkbox is checked. The 'Zone' dropdown menu is set to 'Zone-1'. The 'Enable Rule On Zone' checkbox is checked. The 'Primary Group' dropdown menu is set to 'QA Group'. The 'Secondary Group' dropdown menu is set to 'Testing Group'. The 'Mode' dropdown menu is set to 'Primary Must'. The 'Update Device' and 'Update Zone' buttons are still present. The device list on the right is the same as in the previous screenshot, but the row for 'R and D PanelliteV2' is highlighted.

Enable Rule: Select the check box to enable the 2 Person Rule on selected device.

Click on **Update Device** to update the rule on selected device.

Zone: For Panel200, Select the Zone from the drop down list.

Enable Rule on Zone: Select the check box to enable the 2 Person Rule on selected Zone.



Zone is applicable for Panel Door only.

Mode: Select the Mode from the options of Primary Must or Primary and Secondary Must.

- **Primary Must:** In this mode, the 2 Person Rule will grant access only when at least 1 user from the 2 Person Group is from the Primary Group. i.e. the access is granted if both users are from Primary Group or first from Primary and second from Secondary Group. The only situation when the access will be denied is when both the users are from Secondary Group.
- **Primary & Secondary Must:** In this mode, the 2 Person Rule will grant access only in one condition, one user from Primary Group and the other from Secondary Group. In all other situations the access will be denied.

Primary Group: Select the Group from the pick list to work as Primary Group. Members from the Primary Group are now valid users for the access and any two members of this group together can access a controlled area. If the Mode is selected as Primary Must, at least one person from the Primary Group is required for gaining access.

Secondary Group: Select the Group from the pick list to work as Secondary Group. If Secondary Group is selected, then the system verifies that any member of Secondary Group is always accompanied by a member from the Primary Group or a VIP user before allowing access to the zone. If the Mode is selected as Primary & Secondary Must, one person from both Primary and Secondary Group are required for the access.



For 2 Person Rule, maximum 16 Groups can be assigned to the Panel.

For Direct Doors, maximum 2 groups can be assigned at any point of time.



If you wish to use only one Group, make sure you select the Primary Group. This is required because a member from the Secondary Group needs to be accompanied by a member from the Primary Group always for a valid transaction. However, any two members from the Primary Group are treated as valid user for the access to the Door.

Click on **Update Zone** to save the changes.

First In User

First-IN User rule uses a card or fingerprint as credential of the user declared as First-IN User to unlock the Access locked to a particular zone.

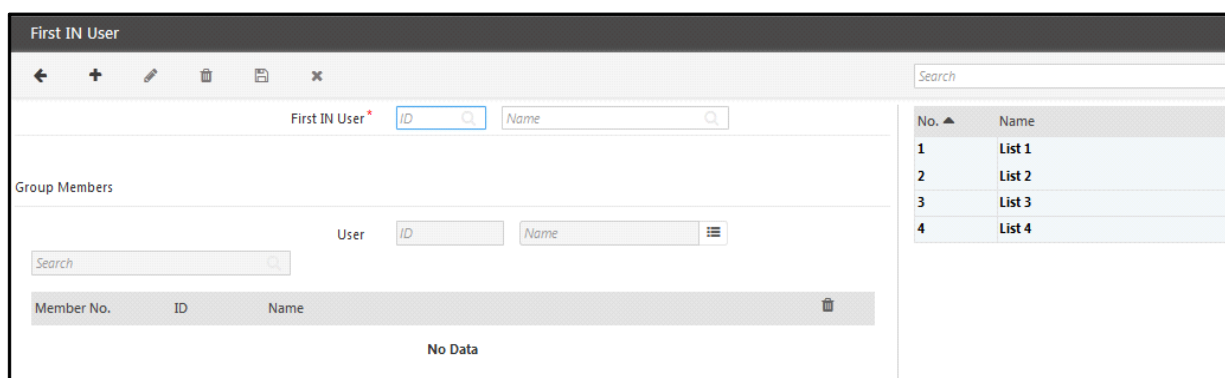
The access control system waits in lock mode till a valid First IN user is detected whose effective working hours overlaps with the current time. The working hours of the zone is linked to the first detected first IN user's effective working hours and system allows access to all authorized users till the working hours of the First In user is valid.

The system allows the administrator to define upto 99 groups with 25 entries in each group.



This functionality can also be enabled from the **Device Module > Device Configuration > Features** option.

To use the 'First IN User' rule, select **Access Control module > First IN User Rule > Group** .The page appears as shown below:



No.	Name
1	List 1
2	List 2
3	List 3
4	List 4

To create a new Group, Click on **New** button. You can also select the group from the right grid and add the users to it.

First IN User: Specify a user friendly name for the Group for First-In users. The ID No. appears by default and cannot be edited by the user.

Group Members:

User: Click on the **Picklist** button and select the Users for the Group one by one. You can define upto 25 person per group.

Click on **Save** button from the toolbar. The First IN Group will be saved in the right grid as shown below.



A VIP user is allowed to access the First-IN enabled zone even when the zone is not activated by a First-IN user. However, the VIP user cannot activate the zone to allow access to other users.

First In User Assignment

First-In User Rule Assignment enables to assign the Rule on Devices.

To use the First In User Assignment feature, select **Access Control module > First IN User Rule > Assignment**. The page appears as shown below:

ID	Name
1	Door v3
1	RnD Panel lite V2
3	NGT Ground Floor
4	Vega Direct Door
5	Wireless Door 1st Floor
7	NGT-34
8	Panel Lite V2-Device-8

The grid on the right shows all the devices including Panel200 and direct doors set to advanced access control.

Click on the device from the grid, the related parameters will appear in the respective fields.

Panel200

ID	Name
1	Door v3
1	RnD Panel lite V2
3	NGT Ground Floor
4	Vega Direct Door
5	Wireless Door 1st Floor
7	NGT-34
8	Panel Lite V2-Device-8

Enable Rule: Check the box to enable the First-In user rule on selected device.

Group1-4: You can select four First-IN groups which can then be assigned to different zones of Panel200. Select the First-IN group from the picklist button. It will list all the First-IN groups as created from First IN User Rule-Group.

Click on **Update Device** to update the First IN groups on Panel200.

Zone: Select the Zone from the drop down list. The zones are configured while adding Panel200 to the Devices.

Enable Rule on Zone: Check the box to enable the first-In user rule on selected Zone.

Reset On: If a user from “First-IN User” group punches then access to other users can be restricted to that day or defined time duration.

- **Day Change:** If Day Change is selected, other user will be allowed access in the selected zone on that day and will be restricted on next day.
- **Access Timer (Sec):** If Timer Expiry is selected, specify the Access Timer in seconds (say 5 seconds); after which the user will be restricted the access.

First-IN User Group: Select the “First-In User” group to be applicable for the selected zone.

Eg: For zone QC, Group1 is selected.

Click on **Update Zone** and **Save** the selection.

First IN Rule Assignment

Search

Device * 8 Panel Lite V2-Device-8

Enable Rule ☒

Group 1 * 5 HO First IN

Group 2 * 2 List 2

Group 3 * 3 List 3

Group 4 * 4 List 4

Update Device

Zone QC

Enable Rule On Zone ☒

Reset On ☐ Day Change ☒ Timer Expiry

Access Timer (Sec) 3

First-IN User Group Group 1

Update Zone

ID	Name
1	Door v3
1	RnD Panel lite V2
3	NGT Ground Floor
4	Vega Direct Door
5	Wireless Door 1st Floor
7	NGT-34
8	Panel Lite V2-Device-8

Direct Door

First IN Rule Assignment

←

Search

Device *

1

Door v3

⋮

Enable Rule

☒

Reset On

☒ Day Change ☐ Timer Expiry

Access Timer (Sec)

3

First-IN User Group

4

List 4

⋮

Update Device

ID ▲	Name
1	Door v3
1	RnD Panel lite V2
3	NGT Ground Floor
4	Vega Direct Door
5	Wireless Door 1st Floor
7	NGT-34
8	Panel Lite V2-Device-8

Enable Rule: Check the box to enable the First-In user rule on selected door.

Reset On and Access Timer(Sec) are disabled for direct door.

First-IN User Group: Select the “First-In User” group to be applicable for the selected door.

Click on **Update Device** to save the selection.

Smart Access Route

The Smart Access Route functionality using Mifare Cards/ HiD Cards enables the administrator to define an access policy which allows the user to access the COSEC Doors in the configured sequence. The COSEC system has the capability to define up to **75** doors on a single route.



*This functionality must be enabled from the **Admin Module > System Configuration> Global Policy> Access Control** option.*

Also Access Route type and Smart Card Key settings are to be done from Global Policy Page.

To use the Smart Card based Access Route, Click on **Access Route** option under **Smart Access** from the Access Control page. The page appears as shown below:

To create a new Access Route, Click on **New** button.

Name: Specify a user friendly name for the Access Route.

Active: Check the box to activate the feature.

Sequenced Route: When sequenced Route is checked then restrictions for the route can be configured. If the box is unchecked then the Restrictions option will be disabled. Then the non-sequenced route can be configured.

Restrictions: Select the Restriction mode from the drop down list.

This functionality can operate in two modes:

- **Hard:** Access will be allowed only if the access route is followed.
- **Soft:** Access will be allowed on any door on the access route with an access route violation message.

Reset on Start Level: Check the box to enable the system to reset the current level status to allow access on the lowest level.

This option is useful in the event of the user not following the proper order while exiting the premises. If this functionality is enabled then the user will be allowed access on the lowest level irrespective of his/her state but this will happen only on entry side.

Configured Route

The user needs to define the member doors as the part of defined Access Route. Click on **Add** button to add the doors to Access route.

Device: Click on the **Picklist** button and select the required direct door or panel door from the Picklist window.

Level: Select the Level number to be assigned to the Door from the drop down list.

Click on **OK** button. The Door will appear in the grid. Similarly you can add other doors in the route.

The screenshot shows the 'Smart Access Route' configuration window. It includes a toolbar with icons for back, add, edit, delete, save, and close. Below the toolbar, there are input fields for 'Smart Access Route' (with an ID dropdown) and 'Matrix Route'. Configuration options include 'Active' (checked), 'Sequenced Route' (checked), 'Restrictions' (set to 'Soft'), and 'Reset On Start Level' (unchecked). A 'Configured Route' section at the bottom features a search bar and a table with columns: Sr. No., Device ID, Name, and Level. The table contains one entry: Sr. No. 1, Device ID 1, Name Door V3-Device-7, and Level 1. A '+' button is located to the right of the table.

Sr. No.	Device ID	Name	Level
1	1	Door V3-Device-7	1

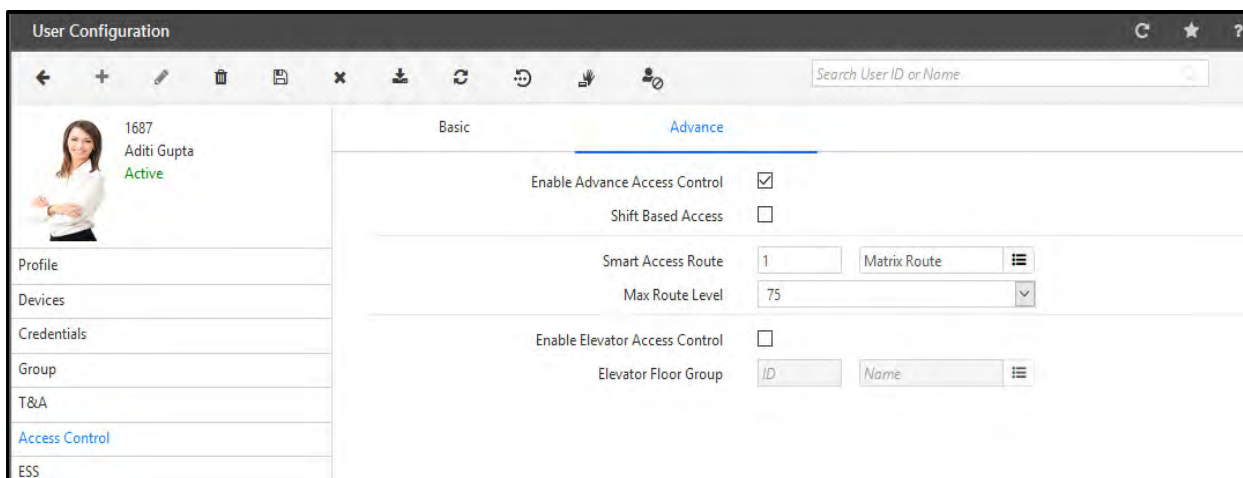
Click on **Save** to save the configured Smart Access Route. The **ID** will be system generated and Route will be shown in right grid.

The screenshot shows the 'Smart Access Route' configuration window after saving. A green banner at the top indicates 'Saved Successfully'. The configuration options remain the same. The 'Configured Route' table now contains three entries:

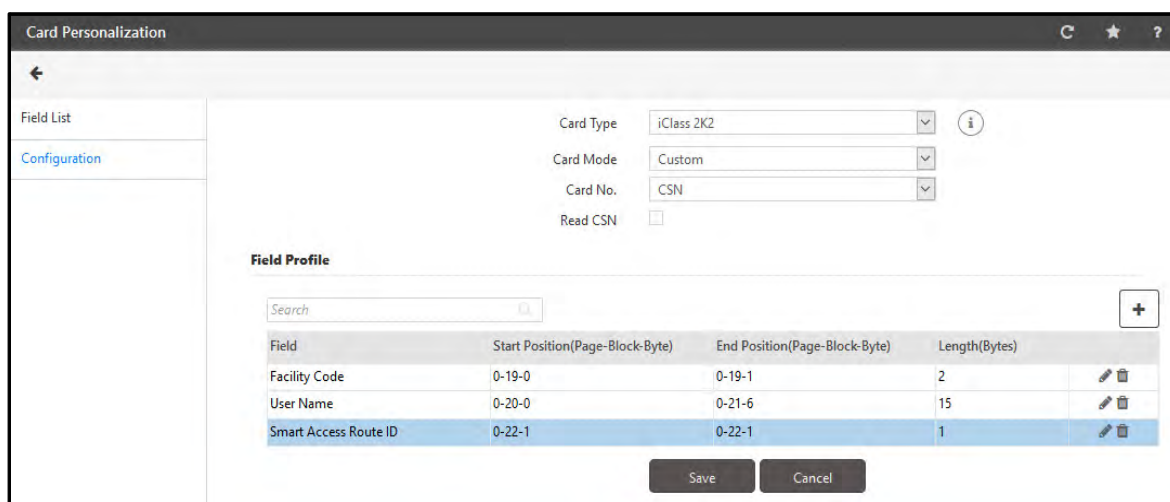
Sr. No.	Device ID	Name	Level
1	1	Door V3-Device-7	1
2	8	ARC as Dual Door Dual Reader	1
3	2	PVR as Panel Door	1

On the right side, a grid shows the saved route with columns 'ID' and 'Name', containing one entry: ID 1, Name Matrix Route.

After configuring the Smart Access Route; it can be assigned to the user from User Configuration> Access Control> Advance. The user can access the assigned route using the smart card enrolled with Smart Access Route. The card can be configured to include Smart Access Route from Card Personalization.



The 'User Configuration' window shows the 'Advance' tab for user 'Aditi Gupta' (ID: 1687, Active). The 'Smart Access Route' is set to '1' and 'Matrix Route'. The 'Max Route Level' is '75'. The 'Enable Advance Access Control' checkbox is checked. The 'Elevator Floor Group' is set to 'ID' and 'Name'.



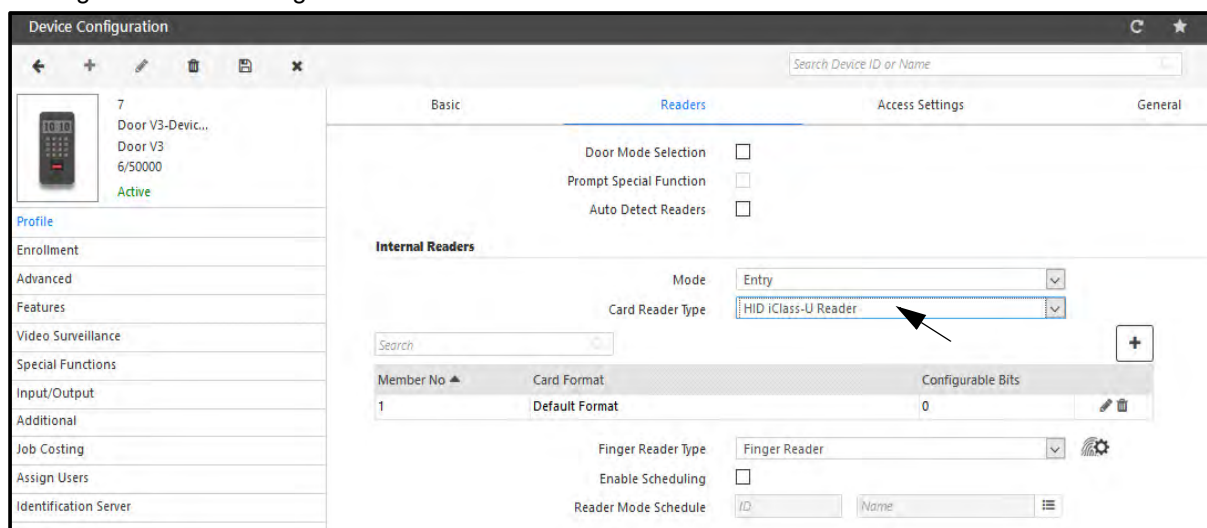
The 'Card Personalization' window shows the 'Field Profile' section. The 'Card Type' is 'iClass 2K2', 'Card Mode' is 'Custom', and 'Card No.' is 'CSN'. The 'Field Profile' table lists the following fields:

Field	Start Position(Page-Block-Byte)	End Position(Page-Block-Byte)	Length(Bytes)
Facility Code	0-19-0	0-19-1	2
User Name	0-20-0	0-21-6	15
Smart Access Route ID	0-22-1	0-22-1	1

The 'Save' and 'Cancel' buttons are at the bottom.

Enrolling Smart Card

The configuration for enrolling Smart Card is shown below.



The 'Device Configuration' window shows the 'Readers' tab for device 'Door V3-Devic...' (ID: 7, Active). The 'Internal Readers' section shows the 'Mode' set to 'Entry' and the 'Card Reader Type' set to 'HID iClass-U Reader'. The 'Member No.' is '1', 'Card Format' is 'Default Format', and 'Configurable Bits' is '0'. The 'Finger Reader Type' is 'Finger Reader'.

Enroll Credentials

Enrollment Command Sent

Door

7

Door V3-Devi

Device Readers

Enrollment Type

Smart Card

Number Of Cards

One

Details on Smart Card

User ID

☒

Facility Code (FC)

☒

Additional Security Code (ASC)

☐

Finger Templates

None

Additional Details On Smart Card

Short Name

☒ Aditi Gupta

Branch

☐ DFLTBR

Department

☐ DFLTDPT

Designation

☐ DFLTDSG

Emergency Contact

☐

Blood Group

☐ NA

Medical History

☐

Enroll

User Configuration

1687

Aditi Gupta

Active

Profile

Devices

Credentials

Group

T&A

Access Control

ESS

Cafeteria

Job Costing

Field Visit Management

Credentials

PIN

Biometric Group No.

8

Roaming User

☐

Access Card 1

11453921554

Access Card 2

Enrolled Fingers(Suprema Proprietary)

1

Enrolled Fingers(Suprema ISO)

0

Enrolled Fingers(Lumidigm ISO)

0

Enrolled Palm

1

Enrolled Face


0

Enable Self-Enrollment

☐

Sr No.	Date Time	Type	Device	Category	Detail
333	20/09/2018 12:35:48 PM	Door V3	Door V3-Device-7	Enrollment	→ TID: 1809200150000006
334	20/09/2018 12:35:48 PM	Door V3	Door V3-Device-7	ACK	← Enrollment Command Successful
335	20/09/2018 12:35:48 PM	Door V3	Door V3-Device-7	Other	→ End Of Message
336	20/09/2018 12:36:06 PM	Door V3	Door V3-Device-7	Request	← Message Request Received
337	20/09/2018 12:36:06 PM	Door V3	Door V3-Device-7	Enrollment	→ TID: 1809200150000007
338	20/09/2018 12:36:06 PM	Door V3	Door V3-Device-7	ACK	← Enrollment Command Successful
339	20/09/2018 12:36:06 PM	Door V3	Door V3-Device-7	Other	→ End Of Message
340	20/09/2018 12:36:14 PM	Door V3	Door V3-Device-7	System	← Enrollment Card - User ID: 1687 Event Date Time: 20/09/2018 12:36:12 PM
341	20/09/2018 12:36:14 PM	Door V3	Door V3-Device-7	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 35
342	20/09/2018 12:36:17 PM	Door V3	Door V3-Device-7	Request	← Message Request Received
343	20/09/2018 12:36:17 PM	Door V3	Door V3-Device-7	Request	→ Get Card for User ID: 1687. TID: 1809200320000001
344	20/09/2018 12:36:17 PM	Door V3	Door V3-Device-7	Reply Data	← User Card Received. User ID: 1687
345	20/09/2018 12:36:17 PM	Door V3	Door V3-Device-7	Other	→ End Of Message
346	20/09/2018 12:36:18 PM	Panel Lite V2	Panel Lite V2	Request	← Message Request Received
347	20/09/2018 12:36:18 PM	Panel Lite V2	Panel Lite V2	Other	→ User Configuration Sent. User ID: 1687 TID: 1809200040000441
348	20/09/2018 12:36:18 PM	Panel Lite V2	Panel Lite V2	ACK	← User Configuration Successful. User ID: 1687
349	20/09/2018 12:36:18 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message

User Details



User ID: 1687
Aditi Gupta

Allowed - Smart card based Route Access - Soft

Device:
Door V3-Device-7

Event Date & Time:
20/09/2018 12:56:51 PM

Department:
DPLDPT

Designation:
DPLTDSG

Events

Sr No.	Date Time	Type	Device	Category	Detail
435	20/09/2018 12:54:34 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
436	20/09/2018 12:54:40 PM	Panel Lite V2	Panel Lite V2	Request	← Message Request Received
437	20/09/2018 12:54:40 PM	Panel Lite V2	Panel Lite V2	Other	→ Access Zone Configuration Sent. Access Zone No: 1 TID: 1809200040000539
438	20/09/2018 12:54:40 PM	Panel Lite V2	Panel Lite V2	ACK	← Access Zone Configuration Successful. Access Zone No: 1
439	20/09/2018 12:54:40 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
440	20/09/2018 12:54:57 PM	Door V3	Door V3-Device-7	User	→ Allowed - Smart card based Route Access - Soft with Card. User ID: 1687 Event Date Time: 20/09/20...
441	20/09/2018 12:54:57 PM	Door V3	Door V3-Device-7	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 37
442	20/09/2018 12:56:52 PM	Door V3	Door V3-Device-7	User	→ Allowed - Smart card based Route Access - Soft with Card. User ID: 1687 Event Date Time: 20/09/20...
443	20/09/2018 12:56:52 PM	Door V3	Door V3-Device-7	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 38
444	20/09/2018 12:57:45 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	Door	← Door Communication Status Changed - Offline Event Date Time: 20/09/2018 12:57:38 PM
445	20/09/2018 12:57:45 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 13
446	20/09/2018 12:57:49 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	Door	← Door Communication Status Changed - Online Event Date Time: 20/09/2018 12:57:42 PM
447	20/09/2018 12:57:49 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 14
448	20/09/2018 12:58:32 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	Door	← Door Communication Status Changed - Offline Event Date Time: 20/09/2018 12:58:25 PM
449	20/09/2018 12:58:32 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 15
450	20/09/2018 01:01:04 PM	Panel Lite V2	Panel Lite V2 -> PVR as...	Door	← Door Communication Status Changed - Online Event Date Time: 20/09/2018 01:00:57 PM
451	20/09/2018 01:01:04 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 16

Smart Identification

Smart Identification enables to define the Access Mode on the selected device (Panel or direct door) through Smart Card, Finger or PIN combinations.

Under this functionality, users defined in the system will be assigned smart cards by enrolling at the COSEC Enrollment station. Access to these users is granted based on the information written on the smart cards.



*This functionality can also be enabled from the **Device Module > Device Configuration > Advanced** option.*



*This functionality has to be first enabled from the **Admin Module > System Configuration > Global Policy > Device** option.*

Also Set any General Additional Security Code which can be used as a passcode for this feature.



*Click on the Default button on Door to set the **Additional Security Code** to the value set in the **General Additional Security Code** field on the Global Policy page of Admin Module.*

Firstly, User Shows RFID Card in which Fingerprint Template is Stored



Device Temporarily Stores the Fingerprint Template



User Punches after Showing the RFID Card



Device Matches the Punch against the Temporarily Stored Fingerprint Template



To use the Smart identification feature, Select **Access Control module > Smart Access > Smart Identification**. The page appears as shown below:

ID	Name
23	wireless fake test
24	PVR door new
26	Pvr door2
28	Vega to testcount
29	fake pvr door
30	Door FMX-Device-30
31	Vega Controller-Device-31
32	Door V3-Device-32
33	PVR Door-Device-33
34	NGT Direct Door-Device-34

16 - 25 of 25 records

The grid on the right shows all the configured devices including direct doors and Panel200.

Click on the device from the grid, the related parameters will appear in the respective fields.

Device: 4, Panel Lite V2

Enable Rule: ☐

Update Device

Zone: Zone-1

Enable Rule On Zone: ☐

Zone Access Level: 8

SI Access Mode: Card

Update Zone

Enable Rule: Check the box to enable the smart Identification rule on selected device.

Click on **Update Device**.

Zone: Select the Zone from the drop down list.

Enable Rule on Zone: Check the box to enable the smart identification feature on selected Zone.

Zone Access Level: Select the Zone Access Level from the drop down list.

SI Access Mode: Select the Smart Identification(SI) mode from the drop down list. The options available are:

- Card
- Card + Finger
- Card + Finger+ PIN
- Card + PIN

For the PVR Door (Direct Door/Panel Door), the SI Access mode is as below:

- Card
- Card + PIN
- Card + Biometric
- Card + Biometric + PIN

Click on **Update Zone**.



However, the user needs to ensure that the functionality is enabled at the device level.

It is essential to install either a Mifare or an HID i-Class serial reader at the DOOR devices for this functionality to work.

SI users need not be assigned any devices and need to be enrolled from the COSEC ENROLL application only.

Access Rule Profile

The Access Rule option allows you to create the conditional rules for a particular time duration to access the doors. Access Rule can be configured for Panel200 (Server Mode) and Panel Doors.

To use this feature you must:

- create an Access Rule
- assign doors to the Access Rule
- assign/revoke users to the Access Rule

Access Rule Profile

To configure the Access Rule,

- Click **Access Control Module > Access Rule > Access Rule Profile**. The **Access Rule Profile** page appears.

The screenshot displays the 'Access Rule Profile' configuration interface. On the left is a sidebar with a tree view containing various access control settings. The main area is divided into two sections. The top section, 'Access Rule', contains fields for 'Access Rule' (with a dropdown), 'Active' (checkbox), 'Start Time' (calendar), 'End Time' (calendar), and 'Active Days' (checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, Sat). The bottom section, 'Assign Doors', has a 'Device' dropdown and a search bar. Below these is a table with columns 'Name' and 'Type'. The table is currently empty, showing 'No Data'. On the right side of the interface, there is a small table with one entry: '1' in the first column and 'Access Rule 1' in the second column.

- Click **New**  .



Maximum 999 Access Rules can be created.

Maximum 99 Access Rules can be assigned to each user.

Access Rule Profile

←

+

✎

✖

📄

✕

Access Rule *

2

Access Rule 2

Active

☒

Start Time *

09:00

End Time *

18:00

Active Days *

☐ Sun
☒ Mon
☒ Tue
☒ Wed
☒ Thu
☒ Fri
☐ Sat

Assign Doors

Device *

Name

⌵

Search


🔍

Name ▲	Type	✖
ARGOFACE_PanelDoor1	Panel200 Door	✖
ABhavin Argoface - 131	Panel200 Door	✖

Configure the following parameters:

- **Access Rule:** Specify a user friendly name for the new Access Rule. The ID is auto-generated by default.
- **Active:** Select the check box to activate the Access Rule.
- **Start Time:** Specify the Start Time for the Access Rule in HH:MM format.
- **End Time:** Specify the End Time for the Access Rule in HH:MM format.
- **Active Days:** Select the check boxes for the days on which you wish the Access Rule to be applied.

Assign Doors

- **Device:** Select the desired device to which you wish to assign the Access Rule using the **Device**  picklist. All the active Panel Doors appear in the list. All the selected devices appear in a grid.

Access Rule Profile

Access Rule: 2 Access Rule 2

Active: ☒

Start Time: 09:00

End Time: 18:00

Active Days: ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

Assign Doors

Device: Name

Search

Name	Type	
ARGOFACE_PanelDoor1	Panel200 Door	
ABhavin Argoface - 131	Panel200 Door	

The device details displayed are — Name and Type. You can delete a Panel Door from the grid if required.

- Click **Delete** corresponding to the required device to delete it from the Access Rule.

If any device or a device belonging to any device group is un-assigned against any user or is selected for deletion but is a part of the Access Rule which is assigned to that user, then those door(s) will be retained against that user.

- Click **Save** to save the Access Rule.

The new Access Rule Profile appears in the right pane.

Access Rule Profile

Access Rule: 2 Access Rule 2

Active: ☒

Start Time: 09:00

End Time: 18:00

Active Days: ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

Assign Doors

Device: Name

Search

Name	Type	
ARGOFACE_PanelDoor1	Panel200 Door	
ABhavin Argoface - 131	Panel200 Door	

Search

ID	Name
1	Access Rule 1
2	Access Rule 2

If you wish to edit any profile,

- Click the desired Access Rule from the right pane. Edit the Access Rule as per your requirement.
- Click **Save** to save the Access Rule.

Assign/Revoke

Assign/Revoke

To Assign/Revoke users to/from an Access Rule,

- Click **Access Control Module > Access Rule > Assign/Revoke**. The **Assign/Revoke** page appears.

The screenshot shows the 'Assign/Revoke' page. On the left is a sidebar with 'Access Control' and a list of access rules. The main area has two tabs: 'Assign Users' (selected) and 'Revoke Users'. The 'Assign Users' tab shows a table with columns 'Access Rule' and 'User'. The 'Access Rule' column has a dropdown menu with 'ID' and 'Name' options. The 'User' column has a dropdown menu with 'ID' and 'Name' options. An 'Add' button is at the bottom right.

Assign Users



To Assign a user to an Access Rule,

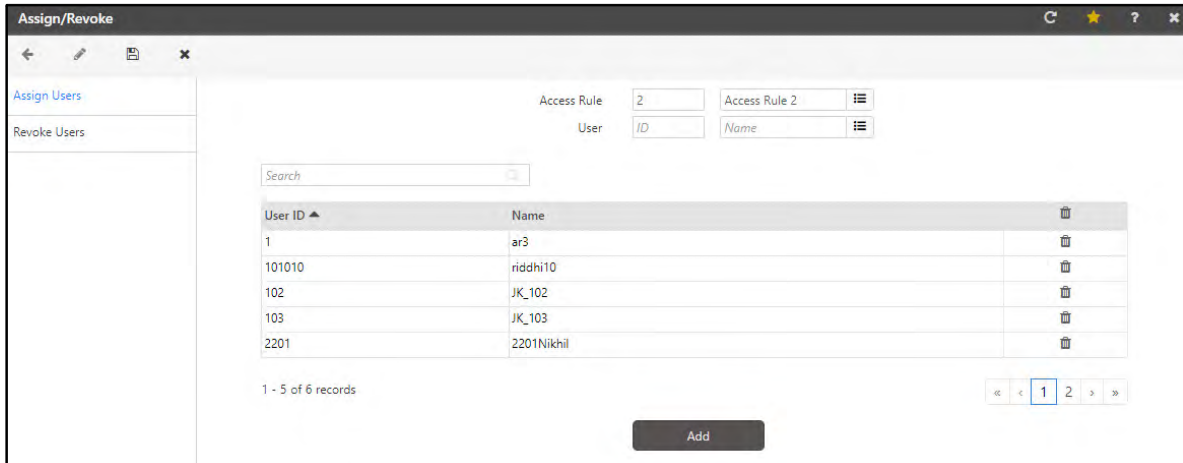
- Click **Access Control Module > Access Rule > Assign/Revoke > Assign Users**. The **Assign Users** page appears.

The screenshot shows the 'Assign Users' page. It has a sidebar with 'Assign Users' and 'Revoke Users' tabs. The 'Assign Users' tab is active, showing a table with columns 'User ID' and 'Name'. The table contains 6 records. A search bar is at the top left. The 'Add' button is at the bottom right.






User ID	Name
1	ar3
101010	riddhi10
102	JK_102
103	JK_103
2201	2201Nikhil

Configure the following parameters:

- **Access Rule:** Select the desired Access Rule to which you wish to assign users using the **Access Rule**  picklist.
- **User:** Select the desired users which you wish to assign the Access Rule using the **Users**  picklist. All the selected users appear in a grid.




The screenshot shows the 'Assign/Revoke' window with the 'Assign Users' tab selected. At the top, there are two picklists: 'Access Rule' (set to '2') and 'User' (set to 'ID'). Below these is a search bar. A table displays the following data:

User ID	Name	
1	ar3	
101010	riddhi10	
102	JK_102	
103	JK_103	
2201	2201Nikhil	


Below the table, it says '1 - 5 of 6 records'. At the bottom right, there are pagination controls showing '1' and '2'. An 'Add' button is located at the bottom center.

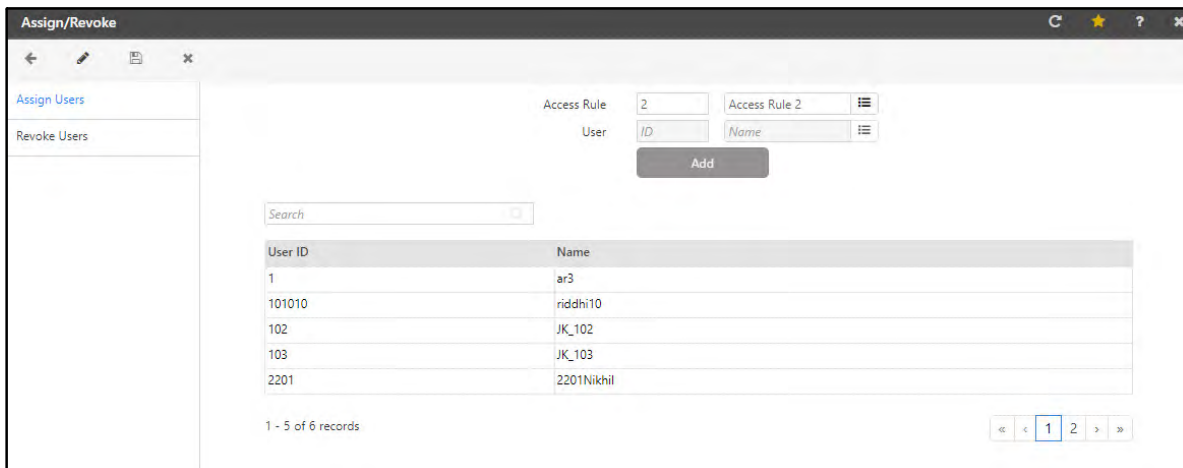
The user details displayed are — User ID and Name. You can delete a user from the grid if required.

- Click **Delete**  corresponding to the required user to delete it from the Access Rule.
- Click **Add** to add the users to the Access Rule. Once the users are added you cannot delete them from the grid.



The Panel - Server Mode supports 25000 users. If this is exhausted and you assign a new user to the desired Panel Door, then the same will not be possible.

- Click **Save**  to save the Access Rule.



This screenshot is identical to the one above, showing the 'Assign/Revoke' window with the 'Assign Users' tab. It displays the same search bar, picklists, table of users, and pagination controls.

Revoke Users

To Revoke a user from an Access Rule,

- Click **Access Control Module > Access Rule > Assign/Revoke > Revoke Users**. The **Revoke Users** page appears.

Assign/Revoke

Assign Users

Revoke Users

Access Rule: 2 Access Rule 2


Search

User ID	Name
1	ar3
101010	riddhi10
102	JK_102
103	JK_103
2201	2201Nikhil

1 - 5 of 6 records

« < 1 2 > »

Configure the following parameters:

- Access Rule:** Select the desired Access Rule from which you wish to revoke the users using the **Access Rule**  picklist. All the users assigned to the Access Rule appear in the grid.

Assign/Revoke


Assign Users

Revoke Users

Access Rule: 1 AR 1

Search

User ID	Name	Revoke
1003G	1003G	<input type="checkbox"/>
1003H	1003H	<input type="checkbox"/>
1003I	1003I	<input type="checkbox"/>

- Select the check box corresponding to the desired user to revoke them from the Access Rule.
- Click **Save**  to save the Access Rule.

View Alarm Log

View option enables the user to view logs of all alarms which have occurred in the time period as specified in the filtering option. Alarm Log Events can be filtered to show only events within a certain time period or based on the Alarm Type.

To access the Alarm Log view feature, Click on **Access Control module > View > Alarm Log**. The page appears as shown below:

The screenshot shows the 'Alarm Log' window with a search bar at the top. Below it, there are two date pickers labeled 'Date' with the value '21/03/2017'. Between the date pickers is a dropdown menu for 'Alarm Type' set to 'All'. A 'View' button is located below the dropdown menu.

Date: Select the Start and the End date to define the time period for which the alarm logs are to be viewed.

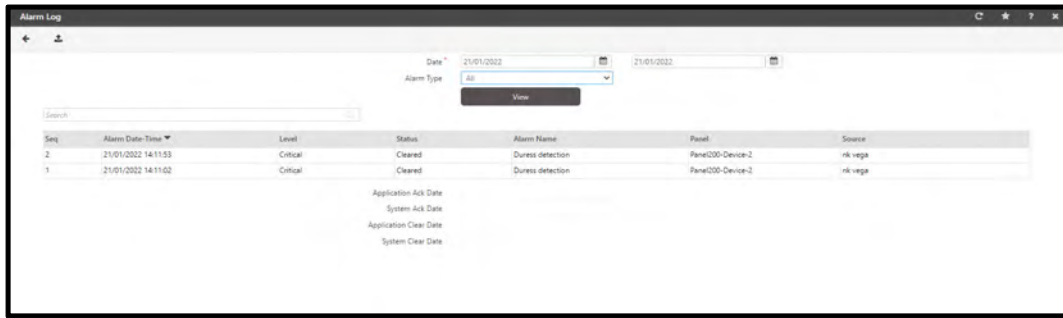
Alarm type: Select the Alarm type from the options of Critical, Major, Minor and All.

Click on the **View** button to view the alarm logs. The following page appears displaying the alarm logs for selected period.

The screenshot shows the 'Alarm Log' window with the same filters as before. Below the filters, there is a search bar and a table of alarm events. The table has columns for Seq, Alarm Date-Time, Level, Status, Alarm Name, Panel, and Source. Below the table, there are four labels: Application Ack Date, System Ack Date, Application Clear Date, and System Clear Date.

Seq	Alarm Date-Time	Level	Status	Alarm Name	Panel	Source
0	15/03/2017 11:46:09	Critical	Cleared	Tamper Alarm	WIRELESS DOOR DEVICE 8 SWETAAA	WIRELESS DOOR DEVICE 8 SWETAAA
0	15/03/2017 11:23:23	Critical	Cleared	Tamper Alarm	WIRELESS DOOR DEVICE 8 SWETAAA	WIRELESS DOOR DEVICE 8 SWETAAA
0	15/03/2017 10:29:31	Critical	Cleared	Tamper Alarm	WIRELESS DOOR DEVICE 8 SWETAAA	WIRELESS DOOR DEVICE 8 SWETAAA
0	10/03/2017 16:27:22	Critical	Cleared	Tamper Alarm	WIRELESS DOOR DEVICE 8 SWETAAA	WIRELESS DOOR DEVICE 8 SWETAAA
0	10/03/2017 16:06:55	Critical	Cleared	Tamper Alarm	WIRELESS DOOR DEVICE 8 SWETAAA	WIRELESS DOOR DEVICE 8 SWETAAA
0	10/03/2017 15:56:34	Critical	Cleared	Tamper Alarm	WIRELESS DOOR DEVICE 8 SWETAAA	WIRELESS DOOR DEVICE 8 SWETAAA
0	10/03/2017 15:55:05	Critical	New	Tamper Alarm	WIRELESS DOOR DEVICE 8 SWETAAA	WIRELESS DOOR DEVICE 8 SWETAAA

Application Ack Date
System Ack Date
Application Clear Date
System Clear Date



Application Ack Date: It shows the date on which alarm is acknowledged by the user.

System Ack Date: It shows the date on which alarm is acknowledged by the system.

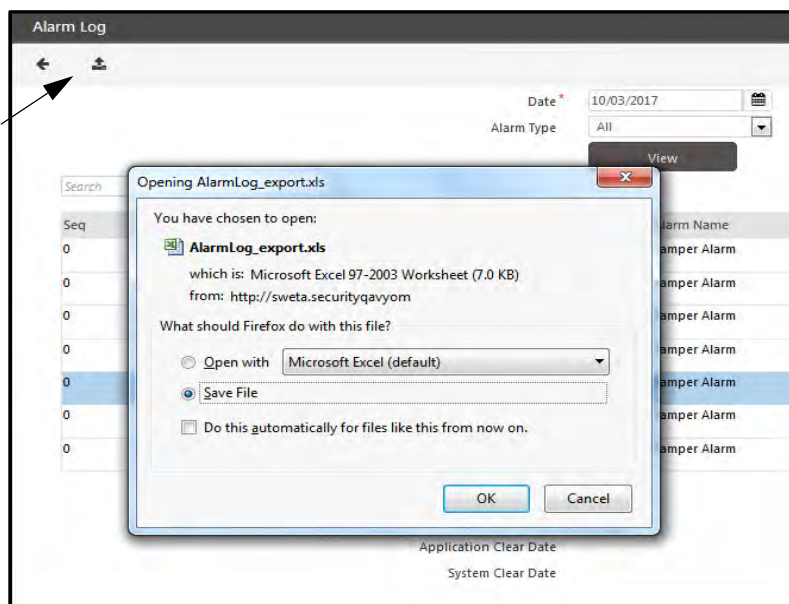
Application Clear Date: It shows the date on which alarm is cleared by the user.

System Clear Date: It shows the date on which alarm is cleared by the system.

Application Ack Date	<input type="text"/>
System Ack Date	<input type="text"/>
Application Clear Date	10/03/2017 16:07:11
System Clear Date	10/03/2017 16:07:13

Export

To export the log of alarm, click on Export button as shown below. You can open or save the Alarm log in excel file.



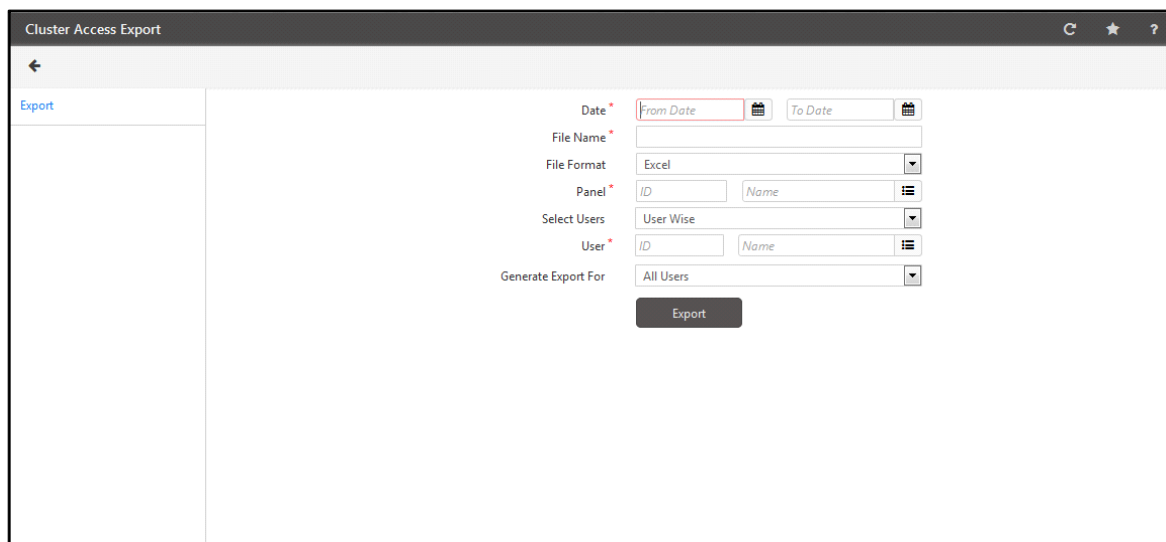
The exported file is shown as below:

Seq	Alarm Date-Time	Level	Status	Alarm Name	Panel	Source	Application Ack	System Ack	Application Clear Date	System Clear Date
1	15/03/2017 11:46:09	Critical	Cleared	Tamper Alarm	WIRELESS DOOR	WIRELESS DOOR				15/03/2017 11:46:15
2	15/03/2017 11:23:23	Critical	Cleared	Tamper Alarm	WIRELESS DOOR	WIRELESS DOOR				15/03/2017 11:23:33
3	15/03/2017 10:29:31	Critical	Cleared	Tamper Alarm	WIRELESS DOOR	WIRELESS DOOR				15/03/2017 10:29:45
4	10/03/2017 16:27:22	Critical	Cleared	Tamper Alarm	WIRELESS DOOR	WIRELESS DOOR			10/03/2017 16:27:42	10/03/2017 16:27:46
5	10/03/2017 16:06:55	Critical	Cleared	Tamper Alarm	WIRELESS DOOR	WIRELESS DOOR			10/03/2017 16:07:11	10/03/2017 16:07:13
6	10/03/2017 15:56:34	Critical	Cleared	Tamper Alarm	WIRELESS DOOR	WIRELESS DOOR				10/03/2017 15:56:43
7	10/03/2017 15:55:05	Critical	New	Tamper Alarm	WIRELESS DOOR	WIRELESS DOOR				
8										
9										
10										
11										

Cluster Access Details Export

This functionality enables the administrator to export access cluster data in a pre-defined Excel format. The exported file displays the information, which includes user-wise punches details.

To access this functionality, Select **Access Control** module > **Exports** > **Cluster Access Details** and the following page appears.

The screenshot shows a web application window titled "Cluster Access Export". On the left is a sidebar with a back arrow and an "Export" link. The main area contains a form with the following fields: "Date" with "From Date" and "To Date" date pickers; "File Name" as a text input; "File Format" as a dropdown menu currently set to "Excel"; "Panel" with "ID" and "Name" input fields and a list icon; "Select Users" as a dropdown menu currently set to "User Wise"; "User" with "ID" and "Name" input fields and a list icon; and "Generate Export For" as a dropdown menu currently set to "All Users". An "Export" button is located at the bottom of the form.

Date: Enter the date range for which data has to be exported.

File Name: Enter an appropriate **File Name** for the export file as shown.

File Format: Specify the export **File Format** as **Excel**.

Panel: Select the Panel for which cluster access details are to be fetched.

Select Users: Select one of the following filters from the **User Filter** drop down list:

- **User Wise** - To select users randomly using the **User** picklist.
- **Group Wise** - To select all users associated with a particular enterprise group.
- **All** - To select all users on the system.

Generate Export for: Select the users as **All**, **Active** or **Inactive** for which Cluster Access Detail is to be exported.

Click the **Export** button. On the **File Download** dialog box, click **Save**. Save the file at a desired location.

The Exported File will display the date-wise user's punches in the following format.

A		
1	User-wise Cluster Access Details From	
2	04/18/2017 To 04/26/2017	
3	1-Cluster-1	
4	Date: 18/04/2017	
5	07-Aditi	
6	08:30-IN	
7	19:30-IN	
8	Date: 19/04/2017	
9	07-Aditi	
10	09:00-IN	
11	19:00-IN	
12	Date: 20/04/2017	
13	07-Aditi	
14	09:01-IN	
15	10:02-IN	
16	19:01-IN	
17	20:02-IN	
18	Date: 21/04/2017	
19	07-Aditi	
20	07:00-IN	
21	09:00-IN	
22	09:01-IN	
23	09:02-IN	
24	09:42-IN	
25	19:01-IN	
26	Date: 22/04/2017	
27	07-Aditi	
28	10:02-IN	

Access Control Reports

Reports available within the COSEC Access Control option are categorized as under:

"Access Zone"

"Time Zone"

"Groups"

"I/O Linking"

"User Access"

"Guard"

"Access Route Master"

"Elevator Access Control"

"Door Held Open"

"Emergency Evacuation"

"Alarm Details"

Access Zone

Generates a Panel wise list of all the Access Zones defined in the system.

ID	Name	Group
3	Panel Lite V2	Panel
4	Panel Lite	Panel

It also displays the access level selected for the zone along with the access mode (credentials) for the zone. If the Visitor Escort rule and First-IN user rule are activated for the zone; then it will display Active for the respective zones.

Sr No	ID	Name	Level	Application Type	Visitor Escort	Zone Access Mode	First-In User	First-In User Group
Panel Lite V2								
1	1	QC Zone	8	Advanced Access Control	Inactive	ANYONE	Inactive	List 1
2	2	Production Zone	7	Advanced Access Control	Active	FINGER	Inactive	List 1
Panel Lite								
1	1	Zone-1	8	Advanced Access Control	Inactive	ANYONE	Inactive	List 1

Time Zone

Generates a report showing the Time Zones assigned from *Access Control > Access Group > Access Profile > Time Schedule*.

These time zones can be then assigned to the user Access Profile which will determine user access at any particular time.

Organization-1						Page 1 of 1
Time Zone						
Run by: System Admin						Date:03/05/2018 10:55
Sr No	ID Name	Start	End	Active Days	Status	
1	1 Time Zone-1	09:00	18:00	SUN,MON,TUE,WED,THU,FRI,SAT,Holiday	Active	
2	2 Maintenanc Zone	10:00	05:00	FRI,SAT	Active	
3	3 Lunch Time	13:00	14:30	MON,TUE,WED,THU,FRI	Active	

Groups

Access Group

Generates a list of all the Access Groups defined from *Access Control > Access Group > Access Profile*. It also displays the user access level for working hours, break hours and non-working hours for the respective groups.

Organization-1						Page 1 of 1
Access Group						
Run by: System Admin						Date: 04/05/2018 14:47
User Access Level						
Sr No	ID Name	Working	Break	Non Working	Status	
1	1 Group-1	8	8	8	Active	
2	2 Group-2	8	8	8	Active	
3	3 RnD Group	8	8	7	Active	

Functional Group

Generates a report displaying the Functional Groups created from *Access Control> Functional Group*.

Functional Group		
←		
Find... 1 of 1 100%		
Main Report		
<div> <div>Organization-1</div> <div>Functional Group</div> <div>Run by: System Admin</div> <div> <div>Sr No</div> <div>ID Name</div> <div>1 1 Staff</div> <div>2 2 Visitor</div> <div>3 3 Admin</div> </div> <div>Page 1 of 1</div> <div>Date:04/05/2018 15:04</div> </div>		

2-Person Groups
Generates a group-wise list of the members of all the 2- Person Groups.

2-Person Groups		
←		
Find... 1 of 1 100%		
Main Report		
<div> <div>Organization-1</div> <div>2-Person Groups</div> <div>Run by: System Admin</div> <div> <div>Sr No</div> <div>User ID</div> <div>Name</div> <div>Member Group</div> <div>1 1 Chirag</div> <div>2 4 Shinjini Ghosh</div> <div>TL Group</div> <div>1 101 Khushbu</div> <div>2 102 Shruti Patki</div> </div> <div>Page 1 of 1</div> <div>Date:04/05/2018 15:05</div> </div>		

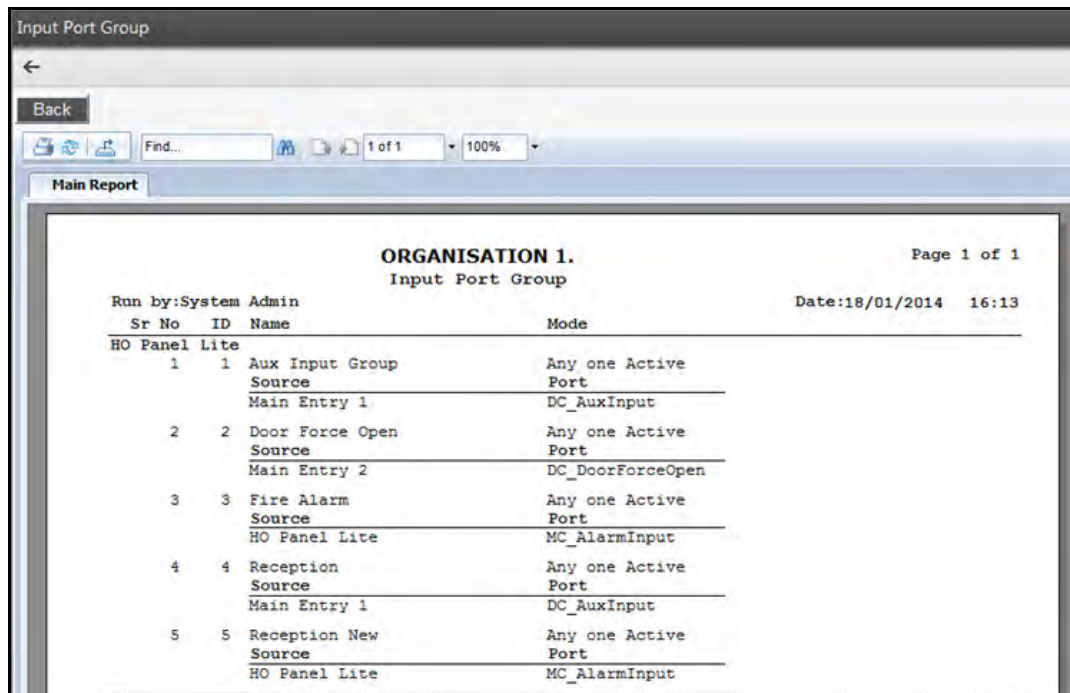
Access Group wise Time Zone
Generates an Access Group wise list of all the Time Zones as with their Access level defined in the system.

Access Group-Wise Time Zone				
←				
Back				
Find... 1 of 1 100%				
Main Report				
<div> <div>Organization-1</div> <div>Access Group-Wise Time Zone</div> <div>Run by: System Admin</div> <div> <div>Sr No</div> <div>ID Name</div> <div>Access Level</div> <div>Status</div> <div>Maintenance Grp</div> <div>1 2 Maintenanc Zone 9 Active</div> <div>HO Group</div> <div>1 4 Experience Zone 9 Active</div> <div>RnD Group</div> <div>1 3 Canteen Time 9 Active</div> <div>2 4 Experience Zone 8 Active</div> </div> <div>Page 1 of 1</div> <div>Date:04/05/2018 15:20</div> </div>				

I/O Linking

Input Port Group

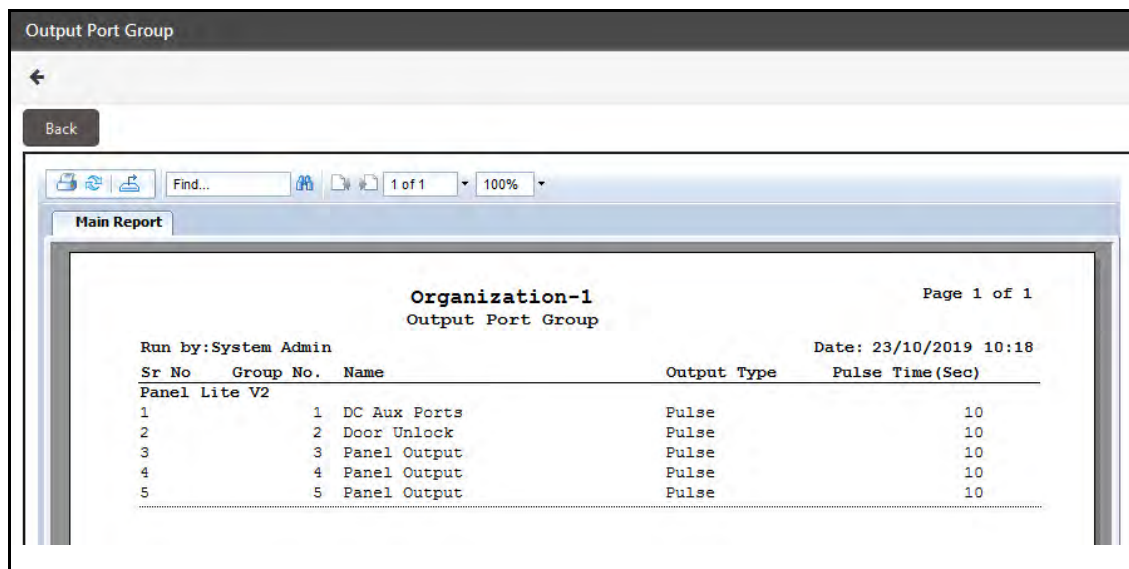
Generates a Panel wise list of the Input Port Groups defined in the system.



ORGANISATION 1.				Page 1 of 1
Input Port Group				
Run by: System Admin				Date: 18/01/2014 16:13
Sr No	ID	Name	Mode	
HO Panel Lite				
1	1	Aux Input Group Source	Any one Active Port	
		Main Entry 1	DC_AuxInput	
2	2	Door Force Open Source	Any one Active Port	
		Main Entry 2	DC_DoorForceOpen	
3	3	Fire Alarm Source	Any one Active Port	
		HO Panel Lite	MC_AlarmInput	
4	4	Reception Source	Any one Active Port	
		Main Entry 1	DC_AuxInput	
5	5	Reception New Source	Any one Active Port	
		HO Panel Lite	MC_AlarmInput	

Output Port Group

Generates a PANEL wise listing of the Output Port Groups defined in the system.



Organization-1				Page 1 of 1
Output Port Group				
Run by: System Admin				Date: 23/10/2019 10:18
Sr No	Group No.	Name	Output Type	Pulse Time (Sec)
Panel Lite V2				
1	1	DC Aux Ports	Pulse	10
2	2	Door Unlock	Pulse	10
3	3	Panel Output	Pulse	10
4	4	Panel Output	Pulse	10
5	5	Panel Output	Pulse	10

Panels

The options available under this node enables the user to generate a PANEL wise listing of the I/O linking programs defined in the system.

Panels							
Back							
Find... 1 of 1 100%							
Main Report							
Organization-1							
I/O Linking-Panels							
Run by: System Admin				Date: 23/10/2019 10:22			
Sr No	Link No.	Name	Input Group	Output Group	Time Zone1	Time Zone2	Status
Panel Lite V2							
1	1	Aux Linking	Aux Input Group	DC Aux Ports			Inactive
2	2	Force Open link	Door Force Open	Panel Output			Inactive
3	3	Fire-Unlock	Fire Alarm	Door Unlock			Inactive

Direct Doors

The options available under this node enables the user to generate a DIRECT DOOR wise listing of the I/O linking programs defined in the system.

Direct Doors						
Back						
Find... 1 of 2 100%						
Main Report						
Organization-1						
I/O Linking-Direct Doors						
Run by: System Admin				Date: 23/10/2019 10:24		
Sr No	ID Name	Input Group	Output Group	Output Type	Pulse Time(Sec)	Status
Door V3-Ground Floor						
1	1	User Allowed	Aux. Output			Inactive
2	2	User Allowed	Door Relay			Inactive
3	3	User Denied	Aux. Output			Inactive
4	4	User Denied	Door Relay			Inactive
5	5	Aux. Input	Aux. Output			Inactive
6	6	Aux. Input	Door Relay			Inactive
7	7	Duress	Aux. Output			Inactive
8	8	Duress	Door Relay			Inactive
9	9	Intercom Panic	Aux. Output			Inactive
10	10	Intercom Panic	Door Relay			Inactive
11	11	Zone Empty	Aux. Output			Inactive
12	12	Zone Empty	Door Relay			Inactive
Main Door						
1	1	User Allowed	Aux. Output			Inactive
2	2	User Allowed	Door Relay			Inactive
3	3	User Denied	Aux. Output			Inactive
4	4	User Denied	Door Relay			Inactive
5	5	Aux. Input	Aux. Output			Inactive
6	6	Aux. Input	Door Relay			Inactive
7	7	Duress	Aux. Output			Inactive
8	8	Duress	Door Relay			Inactive
9	9	Intercom Panic	Aux. Output			Inactive
10	10	Intercom Panic	Door Relay			Inactive

User Access

First In User

Generates a list wise report of the members of all the first in user lists created.

First-In User			
Back			
Find... 1 of 1 100%			
Main Report			
Organization-1			Page 1 of 1
First-In User			
Run by: System Admin		Date: 23/10/2019 10:29	
Sr No	User ID	Name	
List 1			
1	1	Yagnesh	
2	2	Yesha	
3	4	Dhwani	
List 2			
1	13	Sujal	
2	15	Rushi	
3	4462	Rushi	
List 3			
1	1	Yagnesh	
2	13	Sujal	
3	15	Rushi	
4	2	Yesha	
5	4	Dhwani	
6	4462	Rushi	
7	54	Hitesh	
List 4			
1	54	Hitesh	

Zones Accessed By User

Generates a zone wise list of users who have entered an Access Zone.

Zones Accessed by User							
Back							
Find... 1 of 2 100%							
Main Report							
ORGANISATION 1.							
Zones Accessed by User from 18/01/2013 to 20/02/2013							
Run by: System Admin				Date: 18/01/2014		16:22	
Sr No	User ID	Name	Date	In	Out	Duration	
HO Panel Lite							
Zone-1							
1	1001	ANKITKUMAR SOHLIYA	20/02/2013	10:57			
2	1002	MEGHA H SHUKLA	18/02/2013	16:32			
Factory Panel							
QC							
3	10	RAJENDRA GOSWAMI	18/01/2013	08:22			
4	10	RAJENDRA GOSWAMI	18/01/2013	17:03			
5	10	RAJENDRA GOSWAMI	19/01/2013	17:01			
6	10	RAJENDRA GOSWAMI	21/01/2013	08:19			
7	10	RAJENDRA GOSWAMI	21/01/2013	17:00			
8	10	RAJENDRA GOSWAMI	22/01/2013	08:21			

2-Person Access

Generates a list of 2 person access transaction records as shown.

2-Person Access

Back

Find... 1 of 2 100%

Main Report

2-Person Access Transaction from 04/01/2014 to 04/02/2014

Run by: System Admin Date: 04/02/2014

Sr No	DateTime	User ID	Name	Group	Department	Designation
Name		paneldoor9988				
1	22/01/2014 07:44:33	2prsonusr1	2prsnusr1	Primary	Department-1	Designation-1
2	22/01/2014 07:44:33	dinesh5	dinesh5	Secondary	Department-1	Designation-1
3	22/01/2014 07:44:36	2prsonusr1	2prsnusr1	Primary	Department-1	Designation-1
4	22/01/2014 07:44:36	dinesh5	dinesh5	Secondary	Department-1	Designation-1
5	22/01/2014 07:45:57	2prsonusr1	2prsnusr1	Primary	Department-1	Designation-1

Zone-Wise Who Is In

Generates a list showing count and details of users who are inside some particular zone.

Zone-Wise Who Is In

Back

Find... 1 of 1 100%

Main Report

Organization-1 Page 1 of 1

Who Is In On 05/28/2015 15:41

Run by: System Admin Date: 05/28/2015 15:41

Zone No.	Name	Panel Name	Who Is In Count
1	Zone-1	Panel Lite-Device-2	1
2	zone 2	Panel Lite-Device-2	1

Access Route- Wise Who Is In

Generates a list showing count and details of users who have entered the last access level in access route.

Access Route-Wise Who Is In

Back

Find... 1 of 1 100%

Main Report

Organization-1 Page 1 of 1

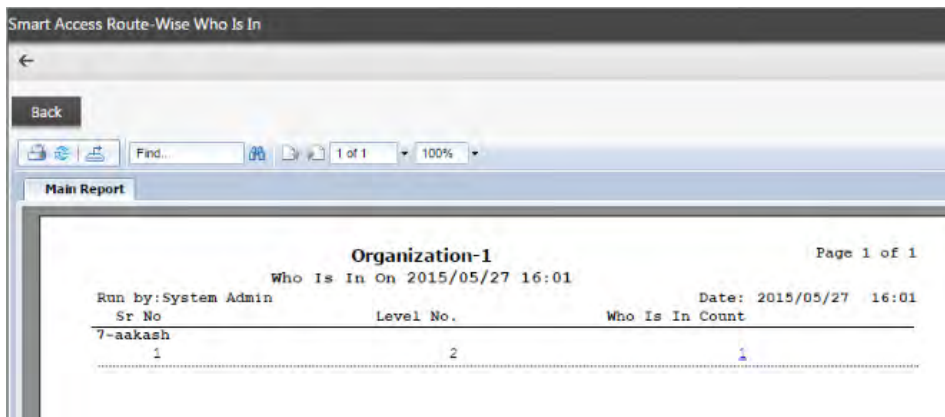
Who Is In On 2015/05/27 15:59

Run by: System Admin Date: 2015/05/27 15:59

Sr No	Level No.	Who Is In Count
13-Panel Lite V2-Device-13		
2-routel		
1	3	1

Smart Access Route- Wise Who Is In

Generates a list showing count and details of users who have entered the last access level in smart access route.



Assigned Device

Generates a list of devices that can be accessed by the selected user.

Assigned Devices

Back

Find... 1 of 2 100%

Main Report

Organization-1 Page 1 of 2

Run by: System Admin Organization-Wise Assigned Devices Date: 08/03/2018 09:30

Panel/Door Name	MID	DID	Device Type	Status	Assignment Type	Details
Organization-1						
1 - Chirag						
PVR Rnd Door	1		FVR Door	Active		
NGI Direct Door-Device-4	4		NGI Direct Door	Active		
Vega Direct Door	5		Vega Controller	Active		
FMX Door	6		Door FMX	Active		
Vega Controller-Device-7	7		Vega Controller	Inactive		
Panel Lite V2-Device-4	4		Panel Lite V2	Active		
PVR as Panel door	4	1	Panel Lite V2 Door	Active	Home Zone	1-Zone-1
Door V3 as Panel Door	4	2	Panel Lite V2 Door	Active	Home Zone	1-Zone-1
101 - Khushbu						
PVR Rnd Door	1		FVR Door	Active		
NGI Direct Door-Device-4	4		NGI Direct Door	Active		
Vega Controller-Device-7	7		Vega Controller	Inactive		
Panel Lite V2-Device-4	4		Panel Lite V2	Active		
PVR as Panel door	4	1	Panel Lite V2 Door	Active	Home Zone	1-Zone-1
Door V3 as Panel Door	4	2	Panel Lite V2 Door	Active	Home Zone	1-Zone-1
1687 - Aditi Ajay Gupta Ahmedabad						
PVR Rnd Door	1		FVR Door	Active		
NGI Direct Door-Device-4	4		NGI Direct Door	Active		
Vega Direct Door	5		Vega Controller	Active		
FMX Door	6		Door FMX	Active		
Vega Controller-Device-7	7		Vega Controller	Inactive		
Panel Lite V2-Device-4	4		Panel Lite V2	Active		
PVR as Panel door	4	1	Panel Lite V2 Door	Active	Home Zone	1-Zone-1

Guard

Guard Tour

Generates a PANEL wise listing of the Guard Tours defined in the system.

Guard Tour

←

Back

Find...

1 of 1

100%

Main Report

Organization-1

Page 1 of 1

Guard Tour

Run by: System Admin

Date: 23/10/2019 10:45

ID	Guard Tour Name	User ID	Name	Start Time	Tour Duration	Cycle Time	Sequenced
1	Guard Tour 1	13	Sujal	10:30	05:00	02:30	Yes
		Door Controller:					
		ID	Name	Device Type			
		2	Main Door	PVR Door			
		6	Door V4 as Direct Door	Door V4			
2	Gaurd Tour	54	Hitesh	23:59	01:30	00:10	No
		Door Controller:					
		ID	Name	Device Type			
		1	Door V3-Ground Floor	Door V3			
		2	Main Door	PVR Door			
		5	Door V4-First Floor	Door V4			
		7	Vega Device-Second Floor	Vega Controller			

Tour Details

Generates list of the Guard Tours details as defined in the system.

Configure the Optional Parameters and Tour Selection in Tour details as shown below.

- **Optional Parameter**

Select the required format of the report from the drop-down list. The options are Format 1 and Format 2

- **Tour Selection**

Select the desired tour as 'Tour Wise' or 'All' for which the report is to be generated.

1. Tour Wise: Creates a report of desired tour which is to be selected from the pick list.

2. All: Creates report of all tours.

Once the parameters are configured, click on the **Generate Report** button to generate the Tour Details' report as shown below.

Tour Details

Back

Find...

1 of 2

100%

Main Report

Organization-1

Page 1 of 2

Guard Tour Details Report From 23/10/2019 To 23/10/2019

Run by: System Admin

Date: 23/10/2019 10:48

Tour Details	Cycle No.	Start Time	End Time	Device1 Main Door	Device2 Door V4 as Direct Door	Device3	Device4	Device5	Device6	Device7	Device8	Verdict
Tour ID: 1	1	10:30	13:00									
Date: 23/10/2019	2	13:00	15:30									
Tour Period: 10:30-15:30												
No. of Devices: 2												
Guard ID: 13												
Name: Sujal												
Sequential: Yes												

Access Route Master

This report shows the details of Panel lite, Access Route assigned to the Panel lite along with Devices in the Access Route. Enable the check-box “New Page for Each Panel” if Access Routes for each panel is required on separate page.

Access Route Master

Optional Parameters

New Page For Each Panel

Access Route Selection

Select Panel

Panel Wise

Panel *

ID

Name

Search

ID	Name	
3	Panel Lite V2	
4	Panel Lite	

Select Access Route

All

Generate Report

Access Route Master

Back

Find... 1 of 1 100%

Main Report

Organization-1

Access Route Master

Page 1 of 1

Run by: System Admin Date:23/04/2018 12:01

Sr No	DID	Device Name	Type	Access Level
3 - Panel Lite V2 - Panel Lite V2				
1 - Route 1 - Non Sequence				
1	7	Path as Panel door	Path Controller	1
2	10	Door V3 as Panel Door	Door V3	1
2 - Route2 - Sequence				
1	6	ARC as Dual Door-Single Reader	Arc Controller	1
2	7	Path as Panel door	Path Controller	1
3	10	Door V3 as Panel Door	Door V3	2
4 - Panel Lite - Panel Lite				
1 - Access Route HO - Sequence				
1	1	Door V3 as Panel Door	Door V3	1
2	2	Path as Panel Door	Path Controller	2

Elevator Access Control

Elevator Access Report

This report shows the list of users accessing Elevators based on Date and Time filters. You can select the Format as "Elevator Wise User Access" or "User Wise Elevator Access".

Elevator Access Report	
Date *	31/07/2018 31/07/2018
Time	00:00 17:30
Optional Parameters	
Format Selection	Elevator Wise User Access
Filter	
Select Elevator	All
Generate Report For	All Users
Generate Report	

The user must be enabled for Elevator Access Control feature from User Configuration> Access Control> Advance and Elevator Floor group must be assigned to the user. The Elevator Floor Group in Access Control consist of Elevator-Floor- members based on which user can access the floors of Elevator.

PVR door is authentication device of Elevator1 and Door V3 is authentication device of Elevator2. The users accessing the authentication device of Elevators are listed in Elevator Access Report as shown below.

Elevator Access Report			
Back			
Find... 1 of 1 100%			
Main Report			
Organization-1			Page 1 of 1
Elevator Wise User Access Report From 31/07/2018 To 31/07/2018			
Run by: System Admin		Date: 31/07/2018 17:31	
Sr. No	User ID	User Name	Access Date Time
Elevator: 1 - Elevator1			
Door: 4 - PVR as Panellite V2 Door			
1	2	John	31/07/2018-10:21:03
Elevator: 2 - Elevator2			
Door: 3 - Door V3 as Panel Door			
1	1	Chirag	31/07/2018-09:21:25
2	1687	Aditi Gupta	31/07/2018-09:20:51

Elevator Floor Group Master

This report can be generated by selecting specific Elevator Floor Group or All groups.

Elevator Floor Group Master			
Elevator Floor Group Selection			
Select Elevator Floor Group		Elevator Floor Group Wise	
Elevator Floor Group *		ID	Name
Search			
ID	Name		
1	RnD Elevator Group		
Generate Report For		All Users	
Generate Report			

The report displays details of Elevator, Floor, Time Schedule Group & User Count Details configured on Elevator Floor Group.

Also it displays the count of users assigned the Elevator Floor Group. On clicking the User Count; a sub report will be generated which shows details of user for selected Elevator Floor Group.

Elevator Floor Group Master

Back

Find...

1 of 1

100%

Main Report

Organization-1

Page 1 of 1

Elevator Floor Group Master

Run by: System Admin

Date: 30/07/2018 12:36

Sr No	Elevator ID	Elevator Name	Floor ID	Floor Name	Time Schedule	Time Schedule	Group ID	Group Name
1	1	Elevator1	3	Telecom Floor			1	Emp Group
2	2	Elevator2	2	Surveillance Fl			1	Emp Group

Main Report

Assigned User:2

Organization-1

Page 1 of 1

Elevator Floor Group Master

Run by: System Admin

Date: 30/07/2018 12:38

Sr No	User ID	User Name	Department Name
1	1687	Aditi Gupta	Department-1
2	V3	Parshv	Department-1

Door Held Open

Generates a list of the occasions when the door has been held open for more than the permissible limits.

Door Held Open

Back

Find...

1 of 1

100%

Main Report

Organization-1

Page 1 of 1

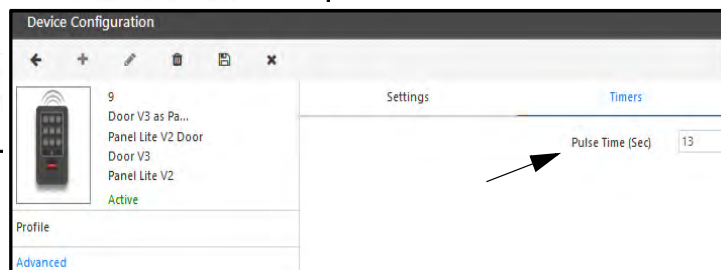
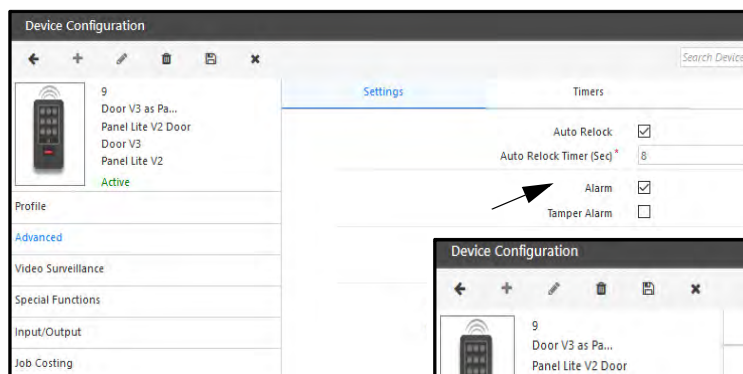
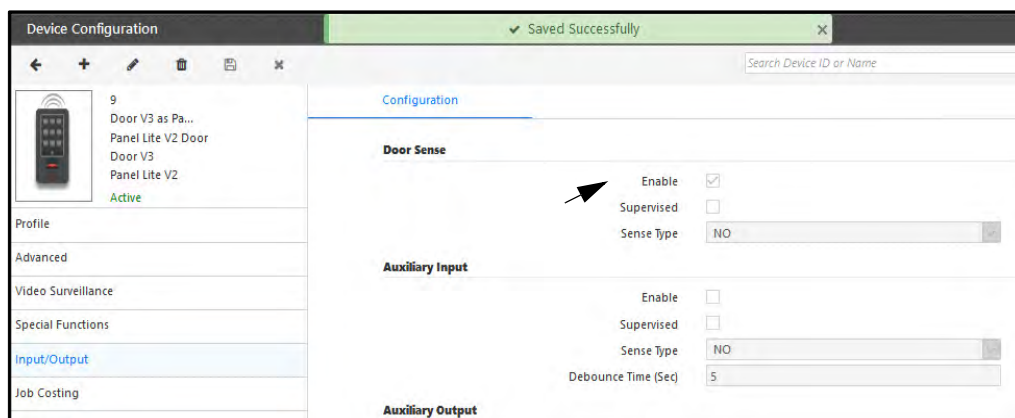
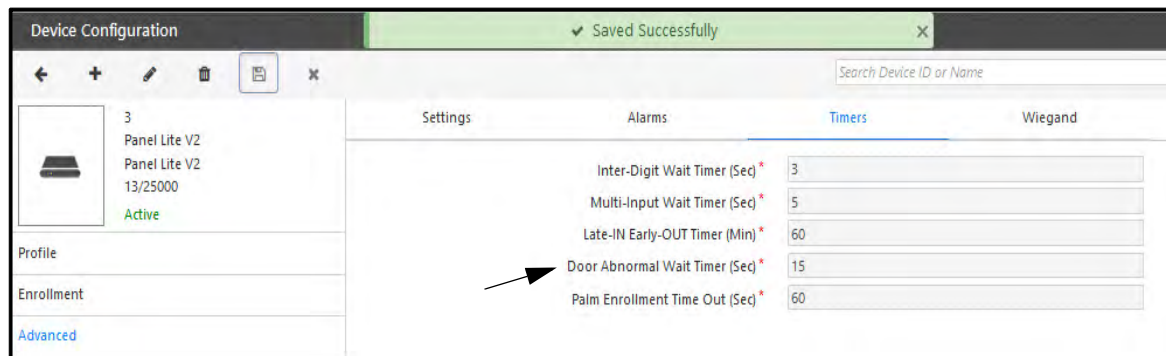
Door Held Open List From 28/05/2018 To 28/05/2018

Run by: System Admin


Date: 28/05/2018 16:51

Sr No	Date Time	Clear Date Time	Door controller	Duration
1	28/05/2018 16:20:38	28/05/2018 16:20:40	Door V3 as Panel Door 0	Days 00:00:02
2	28/05/2018 16:37:15	28/05/2018 16:37:16	Door V3 as Panel Door 0	Days 00:00:01
3	28/05/2018 16:43:28	28/05/2018 16:43:36	Door V3 as Panel Door 0	Days 00:00:08
4	28/05/2018 16:45:43	28/05/2018 16:46:03	Door V3 as Panel Door 0	Days 00:00:20

Following configurations for Door Abnormal Wait Timer, Door Sense, Enable Alarm, Pulse Timer must be done as shown below.



When Door Opens and closes within the Pulse timer duration; then no Alarm will be generated.

User Details		Events					
 User ID: 1 Chirag Device: Panel Lite V2 -> Door V3 as F Event Date & Time: 28/05/2018 04:40:20 PM Department: DFLTDP Designation: DFLTDSG		Sr No.	Date Time	Type	Device	Category	Detail
		210	28/05/2018 04:40:08 PM	Panel Lite V2	Panel Lite V2	Other	← Start Of Event
		211	28/05/2018 04:40:08 PM	Panel Lite V2	Panel Lite V2	Command	→ Event Request for RollOver: 0 Event Seq. No.: 447
		212	28/05/2018 04:40:08 PM	Panel Lite V2	Panel Lite V2	Command	→ Set Date & Time
		213	28/05/2018 04:40:08 PM	Panel Lite V2	Panel Lite V2	ACK	← Set Date & Time Command Successful
		214	28/05/2018 04:40:08 PM	Panel Lite V2	Panel Lite V2	Other	→ Get Information from Device
		215	28/05/2018 04:40:08 PM	Panel Lite V2	Panel Lite V2	Other	← Reply Information from Device
		216	28/05/2018 04:40:08 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
		217	28/05/2018 04:40:21 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Finger. User ID: 1 Event Date Time: 28/05/2018 04:40:20 PM
		218	28/05/2018 04:40:21 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 447
		219	28/05/2018 04:40:26 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Door Open/Close - Open. User ID: 1 Event Date Time: 28/05/2018 04:40:26 PM
		220	28/05/2018 04:40:27 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 448
		221	28/05/2018 04:40:29 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Door Open/Close - Close. User ID: 1 Event Date Time: 28/05/2018 04:40:28 PM
		222	28/05/2018 04:40:29 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 449
		223	28/05/2018 04:40:36 PM	NGT Direct Door	NGT Direct Door-Device-2	Request	← Login Request Received.
		224	28/05/2018 04:40:36 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	→ Login Success Poll Duration: 3 Poll Interval: 2
		225	28/05/2018 04:40:37 PM	NGT Direct Door	NGT Direct Door-Device-2	Request	← Message Request Received

The user punches on the door and the door opens with **Door Open/Close-Open** event.

When the door remains open for long time i.e. the till the expiry of pulse timer then **Door Held open too long** alarm is generated.

- Eg: User punches at 4:45:30 and Pulse timer duration= 13sec so Door Held Open too long alarm will be generated at 4:45:43

If the door is not closed even after the lapse of pulse timer and remains open till the expiry of Door Abnormal Wait timer then **Door Abnormal Event** alarm is generated.

- Now the Door Abnormal Wait timer= 15sec so after the 15 seconds of Door Held Open alarm i.e. (4:45:43 + 0:00:15= 4:45:58); Door Abnormal Event alarm will be generated at 4:45:58.

Features

Alarms

I/O Link

Soft Override

Events

Exceptions

Time Triggered Functions


EMAP

Devices - All

27

Name	Site	IP/RS485 Address	MAC Address	Type	Status
Panel Lite V2		192.168.104.111	00:18:09:04:65:D1	Panel Lite V2	Connected
ARC as Single Door	Site-1	192.168.105.3	DF:E3:65:54:34:44	Panel Lite V2 Door	OFF-Line
Dummy Door	Site-1	192.111.111.111	11:11:11:11:11:11	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-1	192.168.105.5	DF:E6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-1	192.168.105.5	DF:E6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.6	FE:47:48:46:74:69	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.6	FE:47:48:46:74:69	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.7	FE:E6:7A:8A:00:0E	Panel Lite V2 Door	OFF-Line

User Details



User ID: 101
Khushbu
Allowed
Device:
Panel Lite V2 -> Door V3 as F
Event Date & Time:
28/05/2018 04:45:30 PM
Department:
DLTDPT
Designation:
DLTDSDG

Sr No.	Date Time	Type	Device	Category	Detail
10	28/05/2018 04:43:58 PM	Panel Lite V2	Panel Lite V2	Other	→ End Of Message
11	28/05/2018 04:44:27 PM	NGT Direct Door	NGT Direct Door-Device-2	Request	← Login Request Received.
12	28/05/2018 04:44:27 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	→ Login Success Poll Duration: 3 Poll Interval: 2
13	28/05/2018 04:44:28 PM	NGT Direct Door	NGT Direct Door-Device-2	Request	← Message Request Received
14	28/05/2018 04:44:28 PM	NGT Direct Door	NGT Direct Door-Device-2	Command	→ Event Request for RollOver: 0 Event Seq. No.: 254
15	28/05/2018 04:44:28 PM	NGT Direct Door	NGT Direct Door-Device-2	Other	← Start Of Event
16	28/05/2018 04:44:28 PM	NGT Direct Door	NGT Direct Door-Device-2	Command	→ Set Date & Time
17	28/05/2018 04:44:28 PM	NGT Direct Door	NGT Direct Door-Device-2	ACK	← Set Date & Time Command Successful
18	28/05/2018 04:44:28 PM	NGT Direct Door	NGT Direct Door-Device-2	Other	→ End Of Message
19	28/05/2018 04:45:31 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 459
20	28/05/2018 04:45:31 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	User	Allowed with Finger. User ID: 101 Event Date Time: 28/05/2018 04:45:30 PM
21	28/05/2018 04:45:38 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Door	← Door Open/Close - Open. User ID: 101 Event Date Time: 28/05/2018 04:45:37 PM
22	28/05/2018 04:45:38 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 460
23	28/05/2018 04:45:44 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Alarm	← Door Held open too long Event Date Time: 28/05/2018 04:45:43 PM
24	28/05/2018 04:45:44 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 461
25	28/05/2018 04:45:59 PM	Panel Lite V2	Panel Lite V2 -> Door V3...	Alarm	← Door Abnormal Event Date Time: 28/05/2018 04:45:58 PM
26	28/05/2018 04:45:59 PM	Panel Lite V2	Panel Lite V2	ACK	→ Event Ack for RollOver: 0 Event Seq. No.: 462

Emergency Evacuation

Generates a list of people who are present and missing in/from a secured zone at the time of emergency.

The User type can be selected as Users, Visitors or Both. And the site can be selected from optional parameters. The users/visitors can be filtered from Active and Inactive users.

Emergency Evacuation

←

Date * 01/08/2018 28/08/2018

Time 00:00 12:22

Optional Parameters

User Type Both

Select Site All

User Selection

Select Users/Visitors All

Generate Report For All Users/Visitors

Generate Report

Emergency Evacuation

←

Back

Find... 1 of 1 100%

Main Report

Organization1 Page 1 of 1

Emergency Evacuation From 01/08/2018 00:00 To 28/08/2018 12:22

Run by: System Admin Date: 28/08/2018 12:24

Site ID	Name	Category	IN Count	OUT Count	Who Is IN	Assembly Count	Missing Count
Users							
1	Site-1	Category-1	1	0	1	0	1
2	Site2	Category-1	1	0	1	0	1
3	Site3	Category-1	1	0	1	0	1
4	Site4	Category-1	1	0	1	0	1
Total			4	0	4	0	4
Visitors							
1	Site-1		13	0	13	0	13
2	Site2		15	0	15	0	15
3	Site3		15	0	15	0	15
4	Site4		11	0	11	0	11
Total			54	0	54	0	54
Grand Total			58	0	58	0	58

IN Count: Number of users whose latest IN event within the duration specified is on this site. The events should not include events on Assembly points.

OUT Count: Number of users whose latest OUT and latest IN event within the duration specified both are on this site. The events should not include events on Assembly points.

Who Is IN: Number of users whose latest IN event within the duration specified is on this site and thereafter there is no OUT event within the specified duration. The events should not include events on Assembly points.

Assembly Count: Number of users contributing in Who Is IN Count whose at least one event is on assembly point within the specified duration. A site will be considered as an Assembly Point only if the check-box 'Consider As Assembly Point' is checked on Devices Module> Site page.

Missing Count: Difference between Who Is IN Count and Assembly Count. i.e. Who Is IN Count – Assembly Count.

You can click on the number of Missing count to view the details of user/visitor along with punch details. For example clicking on Total-4 generates the sub report as shown below.

Emergency Evacuation									
Back									
Find... 1 of 1 100%									
Main Report 4									
Organization1									
User Event Details From 01/08/2018 00:00 To 28/08/2018 12:22									
Run by:	System Admin					Date:	28/08/2018 12:34		
Date	User ID	Name	Category	Designation	Device Name	IN Punch	Official No.	Personal No.	
Branch-1									
Department-1									
24/08/2018	ds1	Dhruti Shah	Category-1	Designation-1	Kratika	23:59			
24/08/2018	ds1	Dhruti Shah	Category-1	Designation-1	Door V3_52822	23:59			
24/08/2018	ds1	Dhruti Shah	Category-1	Designation-1	Path	23:59			
24/08/2018	ds1	Dhruti Shah	Category-1	Designation-1	Controller_24611				
24/08/2018	ds1	Dhruti Shah	Category-1	Designation-1	Door V2_29708	23:59			

Alarm Details

Generates the data of all alarms and the remark which is entered while manually acknowledging and clearing the Alarms.

Alarm Details									
Back									
Find... 1 of 1 100%									
Main Report									
Organization-1									
Alarm Details From 21/05/2018 To 28/05/2018									
Run by:	System Admin					Date:	28/05/2018 15:29		
Sr No	Alarm Status	Alarm Type	Door Name	Panel Name	Date-Time	Ack/Cleared By	Remark	Remark By	
4 Dead man timer expired Alarm - User IN									
Acknowledged									
1	New	1		Panel Lite V2	22/05/2018 14:06:18				
2	Acknowledged	1		Panel Lite V2	22/05/2018 14:07:19	Server		SA	
4 Dead man timer expired Alarm - User IN Cleared									
1	New	1		Panel Lite V2	22/05/2018 14:12:19				
2	Acknowledged	1		Panel Lite V2	22/05/2018 14:12:58	Server		SA	
3	Cleared	1		Panel Lite V2	22/05/2018 14:17:01	Server		SA	
5 Dead man timer expired Alarm - User IN Cleared									
1	New	1		Panel Lite V2	22/05/2018 14:58:47				
2	Acknowledged	1		Panel Lite V2	22/05/2018 14:59:05	Server		SA	
3	Cleared	1		Panel Lite V2	22/05/2018 14:59:47	Server		SA	
6 Dead man timer expired Alarm - User IN									
Acknowledged									
1	New	1		Panel Lite V2	22/05/2018 15:43:52				
2	Acknowledged	1		Panel Lite V2	22/05/2018 15:44:14	Server		SA	

Alarm Details									
Back									
Find... 1 of 1 100%									
Main Report									
Organization-1 Page 1 of 1									
Run by: System Admin Alarm Details From 28/05/2018 To 28/05/2018 Date: 28/05/2018 16:49									
Sr No	Alarm Status	Alarm Type	Door Name	Panel Name	Date-Time	Ack/Cleared By	Remark	Remark By	
32	Door Held open too long	Cleared							
1	New	3		Panel Lite V2	28/05/2018 16:20:38				
2	Cleared	3		Panel Lite V2	28/05/2018 16:20:40	System Interlock			
33	Door force open	Cleared							
1	New	1		Panel Lite V2	28/05/2018 16:22:11				
2		1		Panel Lite V2	28/05/2018 16:22:26	Server		SA	
3	Acknowledged	1		Panel Lite V2	28/05/2018 16:23:16	Server		SA	
34	Door force open	Cleared							
1	New	1		Panel Lite V2	28/05/2018 16:25:38				
2	Cleared	1		Panel Lite V2	28/05/2018 16:25:44	Server		SA	
35	Door Held open too long	Cleared							
1	New	3		Panel Lite V2	28/05/2018 16:37:15				
2	Cleared	3		Panel Lite V2	28/05/2018 16:37:16	System Interlock			
36	Door Held open too long	Cleared							
1	New	3		Panel Lite V2	28/05/2018 16:43:28				
2	Cleared	3		Panel Lite V2	28/05/2018 16:43:36	System Interlock			

Alarm Details									
Back									
1 of 1 Whole Page									
Organization-1 Page 1 of 1									
Run by: System Admin Alarm Details From 21/01/2022 To 21/01/2022 Date: 21/01/2022 16:34									
Sr No	Alarm Status	Alarm Type	Door Name	Panel Name	Date-Time	Ack/Cleared By	Remark	Remark By	
1	Duress detection	Cleared							
1	New	1nk vega		Panel200-Device-	21/01/2022 14:11:02				
2	Cleared	1nk vega		Panel200-Device-	21/01/2022 14:11:07	Device Web Page		SA	
2	Duress detection	Cleared							
1	New	1nk vega		Panel200-Device-	21/01/2022 14:11:53				
2	Acknowledged	1nk vega		Panel200-Device-	21/01/2022 14:11:59	Server		SA	
3	Cleared	1nk vega		Panel200-Device-	21/01/2022 14:12:17	Server		SA	

Matrix COSEC MONITOR

FileDeviceToolsHelp

Features

Alarms

I/O Link

Soft Override

Events

Exceptions

Time Triggered Functions

EMAP

Devices - All

27

Name	Site	IP/RS485 Address	MAC Address	Type	Status
Panel Lite V2		192.168.104.111	00:1B:09:04:65:D1	Panel Lite V2	Connected
ARC as Single Door	Site-1	192.168.105.3	DF:E3:65:54:34:44	Panel Lite V2 Door	OFF-Line
Dummy Door	Site-1	192.111.111.111	11:11:11:11:11:11	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-1	192.168.105.5	DF:E6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Dual Reader	Site-1	192.168.105.5	DF:E6:37:56:35:56	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.6	FE:47:48:46:74:69	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.6	FE:47:48:46:74:69	Panel Lite V2 Door	OFF-Line
ARC as Dual Door-Single Reader	Site-1	192.168.105.7	EE:E6:74:04:00:0E	Panel Lite V2 Door	OFF-Line

User Details

User ID: 101

Khushbu

Allowed

Device:

Panel Lite V2 -> Door V3 as F

Event Date & Time:

28/05/2018 05:21:53 PM

Department:

DFLTDP

Designation:

DFLTDG

Alarms

Device	Type	Description	Level	Status	Alarm Date Time
Panel Lite V2 -> Door V3 ...	Panel Lite V2 ...	Door Abnormal	Major	New	28/05/2018 05:22:23 PM
Panel Lite V2 -> Door V3 ...	Panel Lite V2 ...	Door Held open too long	Minor	New	28/05/2018 05:22:08 PM

The COSEC Web based Time-Attendance Module enables organization to customize various time-attendance policies like Late-In, Overtime, C-OFF etc for the users and automate them. It allows an organization to have different time schedules and holidays for its different facilities. Elaborate reports and views are also available for people working at different levels.

The COSEC Time and Attendance system is a combination of hardware and software where


- Hardware is used to record time of an user from a credential and
- Software is used to process the time according to the Attendance Policy.

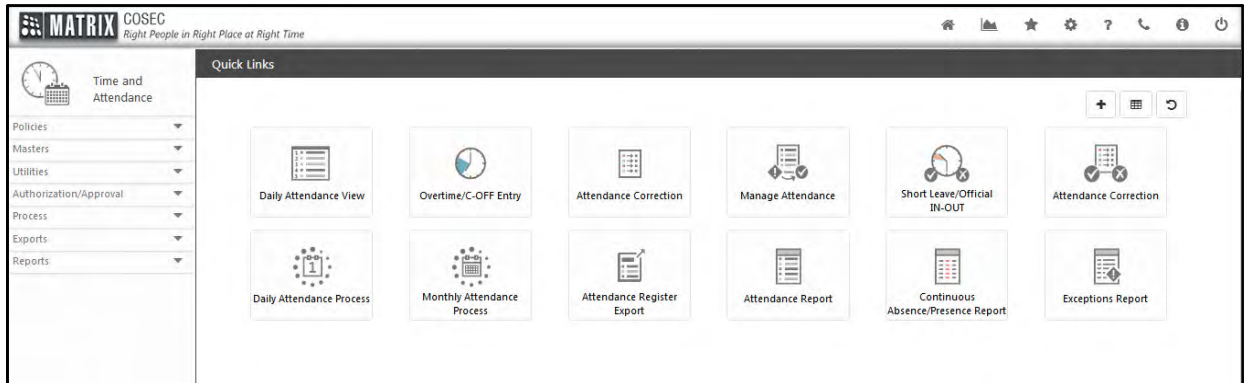
The **Benefits** of Time and Attendance system are mentioned as below:

- Eliminate human error in employee time records.
- Prevent buddy punching and fraudulent time keeping records.
- Significantly increase employee and manager satisfaction.
- Cut down on administrative time and cost.
- Monitor and analyze absence to reduce impact on productivity.
- Significantly cut down on payroll processing time.
- Adapt to existing HR policies.
- Eliminate payments for unapproved or fraudulent overtime.
- Give employees self-service access.




The **Features** of Time and Attendance system are mentioned as below:

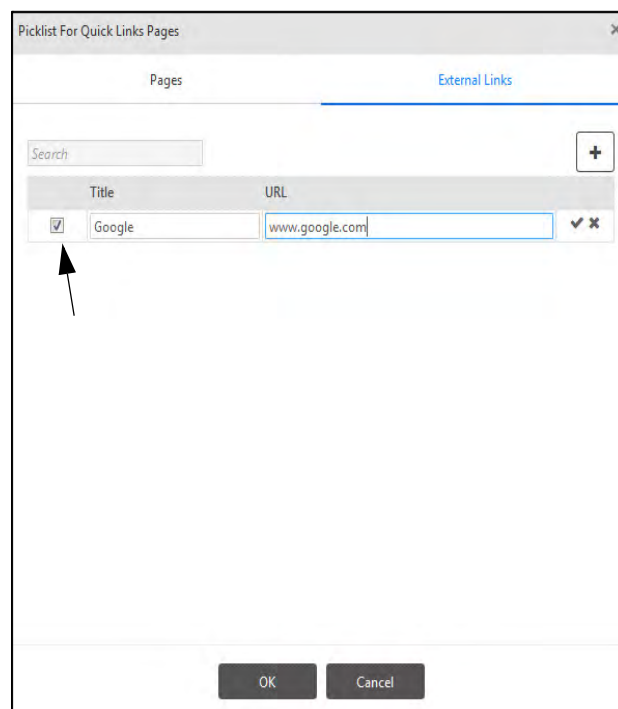
- Support for Multiple working shift time
- User wise Late In & Early Out Policy, Overtime Policy, Compensatory OFF Policy
- User wise Absentee Policy for Week off and Holiday
- Manual Entry and Correction
- Past Adjustment
- Authorization
- Integration with Payroll
- SMS and E-mail Alert Notification
- View Attendance Details

To use the Time and Attendance functionality, select the **Time and Attendance** module icon  on the module selection page. The **Time and Attendance** page appears on the screen as shown below.



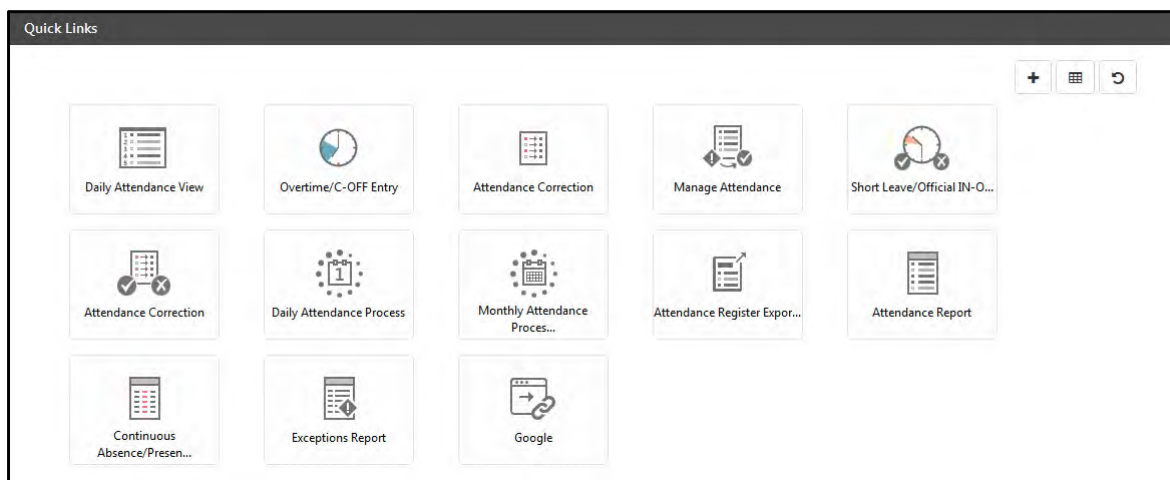
The page displays a menu and **Quick Links** to go to the required page in just one click. Quick Links are shortcuts to reach to a specific page easily. It also contains following three buttons:



- **Add Quick Link:** Click  button to add a quick link. A picklist for Quick Link pages appears for selecting the page or External Link for which the quick link is to be created. Maximum **20** quick links can be added.
- For Adding **Pages** in Quick Link, Select the Pages and click on OK
- For Adding **External Links**, Select External Link tab, click on  button to add new external link.
- Configure the **Title** and **URL** of the external link under the respective fields. click on checkbox to get the configured link on quick link screen as shown below. To save the configuration click on .



- To edit the saved configuration, click on .

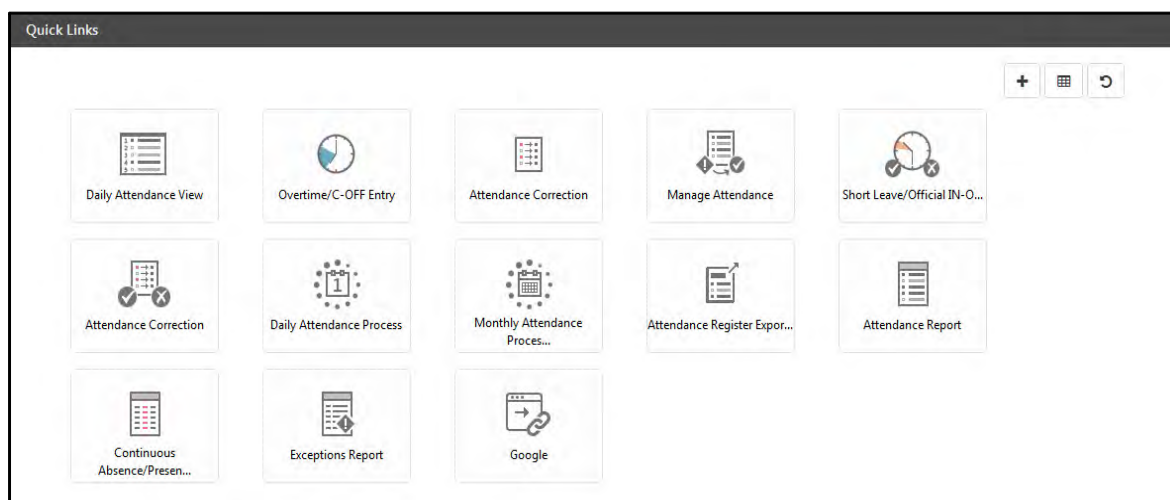
- Click on OK to save the link configuration on Quick Link screen. The external link will be displayed as shown below:



- **Select Layout:** Click  button to select a layout for the quick links. You can select 5x4 or 4x5 layout to manage the quick links.
- **Reset Quick Links:** Click  button to reset the quick links to the default quick links.

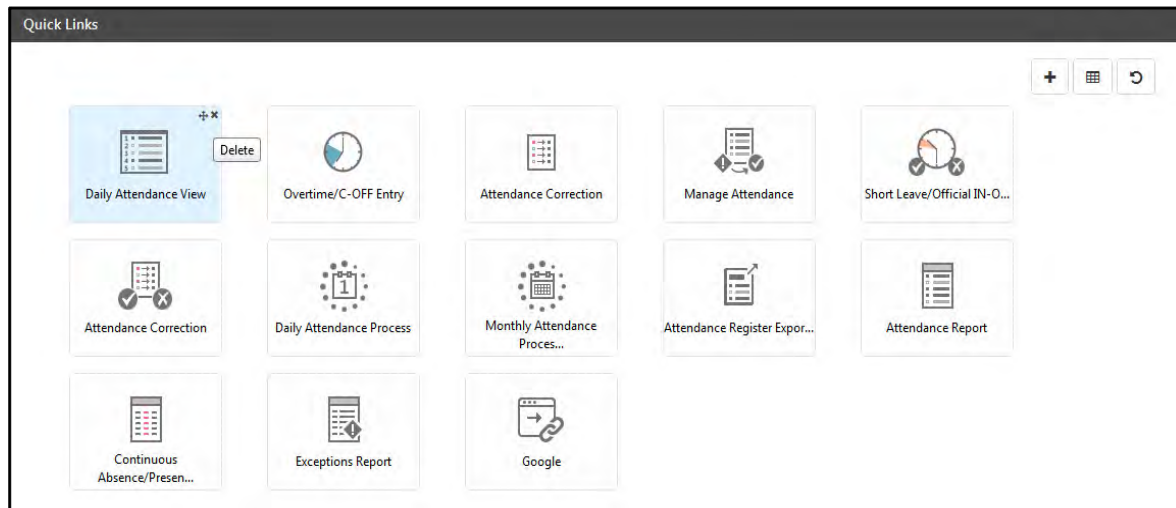
Move the Link

To move the link from one place to another, hover on the link on top right corner and click on “Move” icon as shown below. Then drag the quick link to the desired place. It will be placed at the desired location on the quick links page.




Delete the Link

To delete a particular link, hover on the link on top right corner and click on “Delete” icon as shown below.



Quick links are displayed as per rights given to System Account and ESS users.

Time and Attendance Dashboard

To view the Dashboard, click the Dashboard button  on the **Time and Attendance** page. It displays basic information of the module under the following categories:



Daily Attendance Summary

Total Users: Total No. of active T&A users.

- **Reported:** Total No. of users who have shifts scheduled on the current day and at least one punch as well.
- **Not Yet Reported:** Total no. of all unreported users whose punches are unavailable for current date, though their shift is scheduled and are not on Week-Off, Public Holiday, Leave or Tour.
- **On Leave:** Total No. of leaves on the current day.
- **On Tour:** Total No. of tours on the current day.

- **On Week Off:** Total No. of users on Week Off on the current day.
- **On Holiday:** Total No. of users on holiday on the current day.
- **On Field Break:** Total No. of users on field break on the current day.
- **On Rest Day:** Total No. of users on rest day on the current day.

Scheduled Users: Total no. of active users whose working shift is scheduled for the current day.

Scheduled Shifts: Total no. of scheduled shifts for the current day.




Exceptions

- **Present:** Total No. of users who have punched for current day.
- **No Punches Available:** Total No. of users whose punches are not available for current day.
- **Punches Not in Pair:** Total No. of users whose punches are not in pair for current day.
- **Less Work Hours:** Total No. of users whose working hours are less than the required hours to complete the shift for the current day.
- **Unauthorized:** Total No. of users whose punches are not authorized for current day.
- **Late-IN:** Total No. of users who have started their shift late on the current day.
- **Early-OUT:** Total No. of users who have left their work early on the current day.
- **Absent Club/Cover Rule:** Total No. of users who are Absent due to club/cover rule on current day.
- **Leave Club/Cover Rule:** Total No. of users who are Absent due to leave club/cover rule on current day.
- **Short Leave Balance:** Total No. of users who are Absent due to exceeding limit of short leave balance.
- **Target Shortfall:** Total No. of users who are Absent due to target shortfall.
- **Less Grace Count:** Total No. of users who are Absent due to exceeding limit of allowed less grace count in flexible shift.
- **Work Hours Limit:** Total No. of users who are Absent due to exceeding work hours limit.

Pending Authorization/Approval

- **Short Leave/ Official IN-OUT** - Total No. of pending applications for Short Leave and Official IN-OUT marking.
- **Overtime/C-OFF**: Total No. of pending applications for overtime/C-OFF approval.
- **Daily Attendance**: Total No. of all users who need to be authorized daily for attendance.
- **Attendance Correction**: Total No. of pending applications for attendance correction.
- **Event Authorization**: Total No. of events pending for authorization.

For more information on the above Dashboard options, click the respective information links on the Dashboard. The Latest values on Dashboard are updated on clicking the **Refresh**  button.

Attendance Policy

An attendance policy can be defined as a set of rules governing the attendance system that an organization follows for payroll calculation purposes. COSEC has a provision for administrators to configure such policies as per the company standards and regulations.

Different organizations follow different attendance policies, depending on which, resultant factors such as attendance period, attendance summary, attendance marking and previous attendance adjustments vary. The *Attendance Policy* option enables users to define policies as per site requirements. Later, each policy can be linked with a user or group of users.

[“General Parameters”](#)

[“Short Leave/Official Hours Restrictions Parameters”](#)

[“Absent Marking Rule”](#)

[“Auto Attendance Correction”](#)

[“Flexible Working Settings”](#)

[“Attendance Correction-Short Leave/Official Hours Application Restrictions”](#)

To define an Attendance Policy, Select the **Time & Attendance module > Policies> Attendance Policy**.

The **Attendance Policy** page appears on your screen as follows:

The screenshot displays the 'Attendance Policy' configuration interface. At the top, there are fields for 'Attendance Policy' (ID: 1) and 'Attendance Policy-1'. Below these is a 'Default' checkbox which is checked. The 'Attendance Period' is set to 'Calendar Month'. The 'Month Start-End Date' is set to '2' to '1'. The 'Yearly Period For Leave Balance' section shows 'Start-End Month' as 'January' to 'December'. At the bottom, there are several expandable sections: 'General', 'Short Leave/Official Hours Restrictions', 'Absent Marking Rule', 'Auto Attendance Correction', 'Flexible Working Settings', and 'Attendance Correction- Short Leave/Official Hours Application Restrictions'.

Click the **New** button to define a new Attendance Policy.

Attendance Policy: Enter a user-friendly name for the Attendance Policy. The ID will auto generated by the system.

Default: Select this checkbox if the new Attendance Policy is to be set as default. The new users will be linked with this Attendance Policy by default. You can change the attendance policy of user from User Configuration > T&A> Policy.

Attendance Period: Select the attendance period for the policy as Calendar Month or Customized.

- **Calendar Month:** This option allows the user to set the attendance period as per the calendar month.

- **Customized:** This option enables the user to define the customized start date of the month. In this case the system will automatically calculate the end date as follows:

Attendance Period	Customized
Month Start-End Date	25 24

Example1: 25th August 2016 to 24th September 2016 is considered as the attendance month of September 2016. The shift schedule for a user (who is joining on 1st sept) for the month of September is shown as below.

User

749

Vivek

Attendance Period

September

2016

Mon	Tue	Wed	Thu	Fri	Sat	Sun
			25	26	27	28
29	30	31	1	2	3	4
			GS	GS	GS	GS WO
5	6	7	8	9	10	11
GS	GS	GS	GS	GS	GS WO	GS WO
12	13	14	15	16	17	18
GS	GS	GS	GS	GS	GS	GS WO
19	20	21	22	23	24	
GS	GS	GS	GS	GS	GS WO	

Example2: If Month Start-End is 15 to 14. Then from 15th August 2016 to 14th September 2016 is considered for the September 2016. If user joins on 1st September; then only 14 days will be counted in his attendance period of September month.

Yearly Period For Leave Balance: Specify the starting month of the calendar year from which the system will start calculating the Leave Balance. The system automatically calculates the ending month as shown.

Yearly Period For Leave Balance	
Start-End Month	January December

Once the above parameters have been defined, you can configure the other parameters on this page as discussed in the following sections.

General Parameters

On the *Attendance Policy* page, expand the **General** panel. The **General** section enables the administrator to configure the following parameters.

The screenshot shows the 'General' configuration window. It includes the following settings:

- Max Punches To Consider***: 2
- Deduct Out Time**: Always (dropdown), 7:999 Mins
- Duplicate Punch Period (Mins)***: 0
- Out Punch From Exit Reader**: ☐
- Always Mark First Punch As IN Punch**: ☐
- Event Authorization**
 - Authorization Required**: ☒ (info icon)
 - Event Source**:
 - ☒ Device
 - ☒ ESS
 - ☒ User Assigned Locations
 - ☒ User Unassigned Locations
 - ☒ Others
 - Auth Required for at least one Event of the day**: ☐ (info icon)
- Daily Attendance Authorization Required**: ☒
- Biometric Credential Must For Attendance**: ☐
- Extra Hours Checked With Auth OT/C-OFF**: ☒
- Auto Shift Correction**: ☐

The screenshot shows the 'Attendance Process Calibration' configuration window. It includes the following settings:

- Auto Shift Correction**: ☐
- Attendance Correction In Closed Period**: ☒
- Adjustment Generated For Closed Period**: ☐
- Valid Period For Adjustment (Months)**: 0
- Attendance Process Calibration**
 - Enable**: ☐
 - Max Early-IN Allowed (Hrs)**: HH:MM
 - Max Late-OUT Allowed (Hrs)**: HH:MM
 - Priority**: Early-IN (Next Shift) (dropdown)
 - Max Working Hours Per Day (Hrs)**: HH:MM

Max Punches to Consider: This parameter enables the user to define the maximum number of punches per day which would be considered as a valid punch to be used in the Attendance calculation of the users. The values which can be assigned to this parameter are limited to **2, 4, 6, 8, 10 or 12, N**.

Example: 4 punch user

The first and last punch of the user is displayed in First IN and Last OUT columns of Daily Attendance view. The other punches (for example: 2nd and 3rd punch for **4 punch user**) can be viewed from Attendance Correction page as shown below:

Date	Shift	First IN	Last OUT	1st Half	2nd Half
01/09/2016	GS	08:00	19:00	PR	PR

Attendance Correction

1 IN Date: 01/09/2016 Time: 08:00 Special Function: IN Reason: 	2 OUT Date: 01/09/2016 Time: 10:00 Special Function: OUT Reason:
3 IN Date: 01/09/2016 Time: 11:00 Special Function: IN Reason: 	4 OUT Date: 01/09/2016 Time: 19:00 Special Function: OUT Reason:

- **Deduct Out Time:** For N-punch user, you can select the option to deduct the out timings from the total work hours.
 - **Always:** When Always is selected, then out timings will be deducted always.
 - **Beyond:** For “Beyond” option, specify the time in minutes, beyond which the out timings will be deducted from the working hours.
 - **If Greater than:** For “If Greater than” option, specify the time in minutes. If out time is greater than the specified time then the out timings will be deducted from the working hours.

Punches	Punch timings	Always	Beyond 15 minutes	Greater than 15 minutes
		OUT Time	OUT Time	OUT Time
IN Punch	09:00			
OUT Punch	10:00			
IN Punch	10:30	00:30	00:15 (30 mins -15 mins)	00:30 (actual 30 min outtime)
OUT Punch	12:00			
IN Punch	15:00	03:00	02:45 (3 hrs-15 mins)	03:00 (actual 3 hrs outtime)
OUT Punch	16:00			
IN Punch	16:05	00:05		
OUT Punch	21:00			
N-Punch Hours		08:25 hours	09:00 hours	08:30 hours
Total OUT Time		03:35 hours	03:00 hours	03:30 hours

Duplicate Punch Period (mins): This parameter enables the user to define the time period in minutes between punches, which would be considered by the system as a duplicate punch. If the system identifies a duplicate punch then the first punch of the day will be considered as the IN punch and the last punch of the day will be considered as the OUT punch.

Now you can click **Save** button to save the Attendance Policy as shown below.

Out Punch from Exit Reader: Select this checkbox to enable OUT punches to be allowed only on an Exit Reader. Hence an employee's exit event will be identified only when the OUT punch is made at an Exit Reader. To use this functionality it is essential to have either an external reader or another DOOR which is configured as an Exit reader or DOOR.



If this box is left unchecked, the system considers the first punch of the day as the IN punch and the last punch of the day as the OUT punch. Hence, to enable this functionality, the Administrator needs to ensure that all the out punches occur only at the readers whose mode is defined as Exit.

If this checkbox is enabled and device is not in exit mode, then out punch will not be shown.

For example: The N punch user is punching on the same device. His all the punches are shown as IN punch. And the Out time is not shown.

05/09/2016	GS	09:06		IN		
06/09/2016	GS	09:05		IN		
07/09/2016	GS					

After the Daily Attendance process, the user will be marked Absent on that day as shown below:



Shift correction is possible only among shifts in the same schedule group.

Allow Attendance Correction in Closed Period: If this parameter is enabled then the system will permit users to edit data of previously closed attendance period.

Adjustment Generated For Closed Period: This parameter enables the user to allow the system to calculate adjustments based on the corrections made for the previous paid attendance period.

Valid Period for Adjustment (Months): This parameter enables the user to specify the maximum number of attendance periods in months allowed for previous adjustment calculations.

Attendance Process Calibration: These Attendance processing parameters can be calibrated to determine how a user's punch is posted on COSEC. Select the Enable checkbox to enable the feature for all users on whom this policy is assigned.

- **Max Early-IN Allowed (Hrs):** Maximum number of hours before shift-start time during which a punch should be considered as an Early-IN punch. Default value is 02:00 hours.
- **Max Late-OUT Allowed (Hrs):** Maximum number of hours after shift-end time during which a punch should be considered as a Late-OUT punch. Default value is 02:00 hours.
- **Priority:** This parameter assigns posting priority to an intermediate punch between two shifts. The administrator can determine whether such a punch is to be posted as an Early-IN punch for the next shift or a Late-OUT punch for the previous shift.
- **Max Working Hours Per Day (Hrs):** The maximum number of working hours to be considered per day for punch posting. All punches falling within this duration will be posted for the same day as per shift-based priority (if any). Default value is 16:00 hours.

Attendance Process Calibration parameters can also be defined at the global system level. See [“Defining Global Policies” on page 121](#).

Short Leave/Official Hours Restrictions Parameters

The administrator can define certain restrictions on employees for reporting late or leaving earlier than the official shift timings. A Short Leave is a personal time concession on official work hours, that an employee is permitted to take in addition to official breaks. This option enables the administrator to configure the parameters related to short leaves and official hours restrictions as shown.

The user can use/apply short leave when he has used late-in or early-out more than the number of times allowed. So using short leave converts the absent punches to present. See [“Applying Short leave on Late-IN occurrences”](#)



Short leave hours availed are not required to be compensated by working extra hours.

Short Leave/Official Hours Restrictions

Short Leave Check In Attendance Period

Enable ☒

Maximum Minutes Allowed

Maximum Count Allowed

Duration Check Per Short Leave Entry

Enable ☒

Minimum Duration (In Minutes)

Maximum Duration (In Minutes)

Range Based Short Leave ☒

Search

+

Range (From) ▲	Range (To)	Deduction
30	60	1

Consider Grace In Short Leave

For Shift Late-IN ☐

For Shift Early-OUT ☐

For Break Late-IN ☐

For Break Early-OUT ☐

Short Leave Authorization Required ☐

Add Short Leave Hours In Work Hours ☐

Official IN/OUT Authorization Required ☐

Add Official Hours In Work Hours ☐

Club Short Leave / Official With Break ☒

Short Leave Check in Attendance Period: Select this checkbox to enable a check on the number of times a short leave can be taken over a defined period of time.

Maximum Minutes Allowed: Define the maximum number of minutes in a month that can be permitted for Short Leave.

Maximum Count Allowed: Define the maximum number of Short leaves to be allowed in an attendance period.

Duration Check Per Short Leave Entry: Select this checkbox if you want to enable a check on the duration of a Short Leave.

Minimum Duration (In Minutes): Specify the minimum duration (in minutes) allowed in a day for Short Leave.

Maximum Duration (In Minutes): Specify the maximum duration (in minutes) allowed in a day for Short Leave. This duration has to be greater than the minimum personal duration allowed.

Range Based Short Leave: Select this checkbox to enable short leave deduction on the basis of availed short leave duration when a short leave is applied.

- **Range (In Minutes):** Click Add and specify the range (in minutes) for Short Leave duration based on which deduction is to be calculated.

- **Deduction:** Specify the deduction to be made from user's available short leave count for the range defined. Click the OK button to save the range and the deduction. User can define multiple ranges and save them in the policy, as shown below.

Example: If range is from 30min to 60min and short leave count deduction is 1; Then if user takes short leave of duration in the specified range say 45min, then 1 short leave will be deducted.

Range Based Short Leave <input checked="" type="checkbox"/>			
<input type="text" value="Search"/>			<input data-bbox="1034 501 1074 539" type="button" value="+"/>
Range (From) ▲	Range (To)	Deduction	
30	60	1	<input type="button" value="edit"/> <input type="button" value="delete"/>
61	90	2	<input type="button" value="edit"/> <input type="button" value="delete"/>
91	180	3	<input type="button" value="edit"/> <input type="button" value="delete"/>

Consider Grace in Short Leave: This option enables a grace period to be considered in addition to Short Leave duration. Enable the following options for the type of grace period to be added to the short leave duration:

- For Shift Late-IN (Late entry)
- For Shift Early-OUT (Early exit)
- For Break Late-IN (Late entry after break)
- For Break Early-OUT (Early exit for break)

Say, the short leave duration is 30 minutes and the Shift Late-IN option is enabled (say, grace period is 30 minutes), then the short leave duration can be stretched upto a maximum of 120 minutes.

Consider Grace In Short Leave	
For Shift Late-IN	<input type="checkbox"/>
For Shift Early-OUT	<input type="checkbox"/>
For Break Late-IN	<input type="checkbox"/>
For Break Early-OUT	<input type="checkbox"/>
Short Leave Authorization Required	<input type="checkbox"/>
Add Short Leave Hours In Work Hours	<input type="checkbox"/>
Official IN/OUT Authorization Required	<input type="checkbox"/>
Add Official Hours In Work Hours	<input type="checkbox"/>
Club Short Leave / Official With Break	<input checked="" type="checkbox"/>

Authorization for Short leave/Official hours

Short Leave Authorization Required: Select this checkbox to enable a requirement for authorization in order to take a Short Leave.

Eg: If employee makes Entry for short leave from ESS, then his application goes for authorization to his reporting incharge.

Add Short Leave Hours in Work Hours: Select the checkbox to enable the inclusion of short leave hours in work hours.

Eg: If shift working hrs is 9 hours, and short leave allowed is 1hour. Employee takes short leave of 1hr on 6/7/16. Then total working hours on 6th will be considered as 9 hrs though he has worked only for 8 hours.

Official IN/OUT Authorization Required: Check this box if the Official hours occurrences have to be further authorized by a supervisor before regularization.

Eg: If employee makes Entry for Official In/OUT from ESS, then his application goes for authorization to his reporting in-charge

Add Official Hours In Work Hours: In the event of this parameter being enabled the system will include the official hours in the working hours calculation.

Eg: If shift working hrs is 9 hours. The employee goes for official work and spends 3 hours. So If this check box is enabled then 3 hrs will be counted in total work hours.

Club Short Leave/Official with Break: Select the checkbox to enable the inclusion of short leave or official hours with Break hours.

This checkbox will be enabled by default. So any 2nd and 3rd punch (official or short leave) will be considered as break punches.

If this checkbox is disabled then system will consider the punch pair as break punches when it is not accompanied with any special function or with break special function. For flexible users, Break-Duration will be calculated when 2 punches are made.

Absent Marking Rule

This option enables the administrator to configure the parameters relating to the Late In and Early Out rules of the organization as shown.

Late-IN/Early-OUT Check:

- **Mark Absent As per:** Select the absent marking type as **Monthly Count** or **Monthly Duration**. When “Monthly Count” option is selected, then maximum allowed Late-IN and Early-OUT will have to be specified in terms of count, whereas for option “Monthly Duration”, it must be specified in terms of duration (mins).
- **Mode:** The COSEC application has the capability to have a common count for the number of Late-IN and Early-OUT occurrences. In order to enable this functionality select the **Combined** option from the Mode drop down list.

- On selecting the **Independent** option, the user needs to configure the Late-IN and Early-OUT options independently.

Combined Mode

The screenshot shows the 'Absent Marking Rule' dialog box. Under the 'Late-IN/Early-OUT Check' section, the 'Mark Absent As Per' is set to 'Monthly Count', the 'Mode' is set to 'Combined', the 'Maximum Late-IN/Early-OUT Allowed Count' is set to '3', the 'Absent Marking Type' is set to 'Continuous', 'Mark Absent For Late-IN' is set to 'Half Day', and 'Mark Absent For Early-OUT' is set to 'Half Day'.

Maximum Late-IN/Early-OUT Allowed: Specify the maximum allowed count for Late-IN or Early-OUT occurrences after which a user will be marked absent.

Absent Marking Type: Select the absent marking type as or **Slab-wise**.

In type, every Late-IN occurrence has to be marked as absent after the max occurrence count has been reached.

In **Slab** wise option the system will mark an absent after every max occurrence count. Then the count will be reset.

See Example1 and Example2.

Mark Absent for Late-IN: Select the option as Half Day or Full Day to mark the user absent for coming in late after the Late-IN allowed count for the user is reached.

Mark Absent for Early-OUT: Select the option as Half Day or Full Day to mark the user absent for going out early after the Early-OUT allowed count for the user is reached.

Independent Mode

The screenshot shows the 'Absent Marking Rule' dialog box in 'Independent' mode. Under the 'Late-IN/Early-OUT Check' section, the 'Mark Absent As Per' is set to 'Monthly Count' and the 'Mode' is set to 'Independent'. Below this, there are two sections: 'Late-IN Occurrence Check' and 'Early-OUT Occurrence Check'. Both sections have an 'Enable' checkbox checked. For 'Late-IN Occurrence Check', the 'Maximum Allowed Count Per Month' is set to '3', the 'Absent Marking Type' is set to 'Continuous', and the 'Mark Absent' is set to 'Half Day'. For 'Early-OUT Occurrence Check', the 'Maximum Allowed Count Per Month' is set to '3', the 'Absent Marking Type' is set to 'Continuous', and the 'Mark Absent' is set to 'Half Day'.

On selecting the **Independent** option under **Mode**, the user needs to configure the Late-IN and Early-OUT options independently.

Late-IN Occurrence Check: Enable this option to keep a check upon the number of Late-IN occurrences within a defined attendance period.

- **Maximum Allowed Per Month:** Specify the maximum allowed count for Late-IN occurrences after which a user will be marked absent.
- **Absent Marking Type:** Select the absent marking type as or Slab-wise.
In type, every Late-IN occurrence has to be marked as absent after the max occurrence count has been reached.
In **Slab** wise option the system will mark an absent after every max occurrence count. Then the count will be reset.
- **Mark Absent:** Select the option as Half Day or Full day to mark the user absent after the max Late In count has been reached.

Early-OUT Occurrence Check: Enable this option to keep a check upon the number of Early-OUT occurrences within a defined attendance period.

- **Maximum Allowed Per Month:** Specify the maximum allowed count for Early-OUT occurrences after which a user will be marked absent.
- **Absent Marking Type:** Select the absent marking type as Continuous or Slab-wise.
In **Continuous** type, every Early-OUT occurrence has to be marked as absent after the max occurrence count has been reached.

In **Slab** wise option the system will mark an absent after every max occurrence count. Then the count will be reset.
- **Mark Absent:** Select the option as Half Day or Full day to mark the user absent after the max Early Out count has been reached.

Less Working Hours Check: Enable this option to configure less working hours (shift duration-work hours) for a day and monitor the less working hours availed by the user.

- **Daily Allowed Limit (mins):** Specify the minutes of less working hours allowed for a day.
- **Monthly Allowed Limit (mins):** Specify the minutes of less working hours allowed in a month.
- **Absent Marking Type:** Select the absent marking type as Continuous or Slab-wise.
 - **Continuous type:** The user will be ly marked absent till the month end after crossing the duration of “maximum allowed per month”.
 - **Slab wise:** One day will be marked as absent after crossing the maximum duration. After each slab, maximum allowed per month minutes will be reset and credited to the user after monthly processing.
- **Mark Absent:-** Select **half day** or **full day** to mark as absent when summation of user’s daily “less working hours” exceed the duration set in maximum allowed per month.

Marking

The Daily Attendance View shows the following punches of a user.

Initially the punches after 3rd late-in or early-out will be shown as present.

Daily Attendance View

User:

Attendance Period:

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/11/2016	GS	09:10	18:30	PR	PR			08:20	00:30		01:00			
02/11/2016	GS	09:00	17:45	PR	PR		00:15	07:45			01:00			
03/11/2016	GS	09:25	19:00	PR	PR	00:15		08:35	01:00		01:00			
04/11/2016	GS	09:00	17:55	PR	PR		00:05	07:55			01:00			
05/11/2016	GS	09:27	19:30	PR	PR	00:17		09:03	01:30		01:00			
06/11/2016	GS - WO			WO	WO									
07/11/2016	GS	09:00	17:50	PR	PR		00:10	07:50			01:00			

←

Daily Attendance View

User

1220

Sheetal

📄

Attendance Period

November

▼

2016

▼

View

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark	Details
01/11/2016	GS	09:10	18:30	PR	PR			08:20	00:30		01:00				📄
02/11/2016	GS	09:00	17:45	PR	PR		00:15	07:45			01:00				📄
03/11/2016	GS	09:25	19:00	PR	PR	00:15		08:35	01:00		01:00				📄
04/11/2016	GS	09:00	17:55	PR	PR		00:05	07:55			01:00				📄
05/11/2016	GS	09:27	19:30	AB	PR	00:17		09:03	01:30		01:00			1st Half AB:Late-IN Limit	📄
06/11/2016	GS - WO			WO	WO										📄
07/11/2016	GS	09:00	17:50	AB	AB		00:10	07:50			01:00			Full Day AB:Early-OUT Limit	📄
08/11/2016	GS	09:00	19:00	PR	PR			09:00	01:00		01:00				📄
09/11/2016	GS	09:00	17:40	AB	AB		00:20	07:40			01:00			Full Day AB:Early-OUT Limit	📄

If the user is coming late or going out early after the allowed count is over, then ly he will be marked absent.

Example2: Combined mode

Slab-Wise Marking

The user is allowed for combined count of Late-IN and Early-OUT 3 times a month. For Late-IN, half day slab-wise marking and for Early-OUT, full day slab-wise marking.

The Daily Attendance View shows the following punches of a user.

Initially the punches after 3rd late-in or early-out will be shown as present. But after the Monthly attendance process the user will be marked Absent due to Late-IN limit or Early-OUT limit as shown below:

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark	Details
01/11/2016	GS	09:10	18:30	PR	PR			08:20	00:30		01:00				
02/11/2016	GS	09:00	17:45	PR	PR		00:15	07:45			01:00				
03/11/2016	GS	09:25	19:00	PR	PR	00:15		08:35	01:00		01:00				
04/11/2016	GS	09:00	17:55	PR	PR		00:05	07:55			01:00				
05/11/2016	GS	09:27	19:30	AB	PR	00:17		09:03	01:30		01:00			1st Half AB:Late-IN Limit	
06/11/2016	GS - WO			WO	WO										
07/11/2016	GS	09:00	17:50	PR	PR		00:10	07:50			01:00				
08/11/2016	GS	09:00	19:00	PR	PR			09:00	01:00		01:00				
09/11/2016	GS	09:00	17:40	PR	PR		00:20	07:40			01:00				
10/11/2016	GS	09:20	19:00	PR	PR	00:10		08:40	01:00		01:00				
11/11/2016	GS	09:00	17:50	AB	AB		00:10	07:50			01:00			Full Day AB:Early-OUT Limit	
12/11/2016	GS			AB	AB									No Punches Available	

On 5/11/2016, user is marked half day Absent (for late-IN) due to the completion of combined count.

As the marking is Slab-wise, so the user will be marked absent and the slab will be reset. And the user can now again avail maximum 3 Late-IN and Early-OUT shown on 7th,9th and 10th.

On 11th the user is marked full day absent (for Early-OUT) and again the slab will be reset.

Example3: Independent mode

& Slab-Wise Marking

The user is allowed for 3 Late-IN and 3 Early-OUT independently. For Late-IN, half day marking and for Early-OUT, full day slab-wise marking.

The Daily Attendance View shows the following punches of a user.

Initially the punches after 3rd late-in or early-out will be shown as present. But after the Monthly attendance process the user will be marked Absent due to Late-IN limit or Early-OUT limit as shown below:

Daily Attendance View																
<div> <div>User 1220 Sheetal</div> <div>Attendance Period November 2016</div> <div>View</div> </div>																
Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark	Details	
01/11/2016	GS	09:10	18:30	PR	PR			08:20	00:30		01:00					
02/11/2016	GS	09:00	17:45	PR	PR		00:15	07:45			01:00					
03/11/2016	GS	09:25	19:00	PR	PR	00:15		08:35	01:00		01:00					
04/11/2016	GS	09:00	17:55	PR	PR		00:05	07:55			01:00					
05/11/2016	GS	09:27	19:30	PR	PR	00:17		09:03	01:30		01:00					
06/11/2016	GS - WO			WO	WO											
07/11/2016	GS	09:00	17:50	PR	PR		00:10	07:50			01:00					
08/11/2016	GS	09:00	19:00	PR	PR			09:00	01:00		01:00					
09/11/2016	GS	09:00	17:40	AB	AB		00:20	07:40			01:00			Full Day AB:Early-OUT Limit		
10/11/2016	GS	09:20	19:00	PR	PR	00:10		08:40	01:00		01:00					
11/11/2016	GS	09:00	17:50	PR	PR		00:10	07:50			01:00					
12/11/2016	GS	09:20	19:00	AB	PR	00:10		08:40	01:00		01:00			1st Half AB:Late-IN Limit		
13/11/2016	GS - WO			WO	WO											
14/11/2016	GS	09:20	17:50	AB	PR	00:10	00:10	07:30			01:00			1st Half AB:Late-IN Limit		
15/11/2016	GS	09:00	17:45	PR	PR		00:15	07:45			01:00					
16/11/2016	GS	09:00	17:55	AB	AB		00:05	07:55			01:00			Full Day AB:Early-OUT Limit		
17/11/2016	GS			AB	AB									No Punches Available		

The Late-IN and Early-OUT counts are checked independently. The user can avail 3 Early-Out and 3 Late-IN.

On 9/11/2016, fourth Early-OUT is used, so user is marked full day absent and slab is reset. So he can avail early-out again.

On 12/11/2016, fourth Late-IN is used, so user is marked half day absent. Then onwards if further any late-in is used, then user will be marked absent ly as marked on 14/11/2016.

Auto Attendance Correction

This option enables auto-adjustment of user's shortfalls in working duration due to *Late-IN* or *Early-OUT* by making use of available leaves, overtime, short leaves or official hours, based on their assigned priority. Auto Correction configurations performed using this option will be reflected when the attendance data is processed for an attendance period.

Auto Attendance Correction

Leaves

Enable ☐

Overtime

Enable ☐

Previous Months For Overtime Hours

Short Leave

Enable ☐

Official Hours

Enable ☐

Duration Check Per Official Hour Entry

Enable ☐

Minimum Duration (In Minutes)

Maximum Duration (In Minutes)

Official Hours Check In Attendance Period

Enable ☐

Maximum Minutes Allowed

Maximum Count Allowed

Priority	Name	Up/Down
1	Leaves	▼
2	OverTime	▲▼
3	Short Leave	▲▼
4	Official Hours	▲

- **Leaves:** Enable this option to adjust users' less working hours with available leaves in an attendance period. However, this may not work for certain leave application restrictions (for e.g. if the concerned date falls within a period when leave application is restricted).

Example:

Auto Adjustment with Leave

Consider PL :minimum application required= 2 and SL: minimum application required=0 is enabled for auto adjustment from Leave group as shown below. PL is at priority 1 and SL is at 2.

Auto Adjustment	Priority	Code	Name	Leave Type	Up/Down	
<input checked="" type="checkbox"/>	1	PL	Privelege leave	Paid Leave	▼	
<input checked="" type="checkbox"/>	2	SL	Sick Leave	Paid Leave	▲ ▼	
<input type="checkbox"/>	3	RH	Restricted leave	Restricted Holiday	▲	

The user attendance punches are shown below.

<div> <div>←</div> <div> <div>User</div> <div>SF</div> <div>Shalini Fefar</div> </div> <div> <div>Attendance Period</div> <div>September</div> <div>2016</div> </div> <div>View</div> </div>														
Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/09/2016	GS	09:00	17:00	PR	AB			07:00			01:00			AB:Early-OUT
02/09/2016	GS	09:15	18:00	PR	PR	00:05		07:45			01:00			
03/09/2016	GS	10:00	18:30	AB	PR			07:30	00:30		01:00			AB:Late-IN
04/09/2016	GS - WO			WO	WO									
05/09/2016	GS	09:30	16:00	PR	AB	00:20		05:30			01:00			AB:Early-OUT
06/09/2016	GS	10:00	17:00	AB	AB			06:00			01:00			AB:Early-OUT
07/09/2016	GS	11:00	18:00	AB	PR			06:00			01:00			AB:Late-IN
08/09/2016	GS	09:00	17:30	PR	AB			07:30			01:00			AB:Early-OUT
09/09/2016	GS	10:30	16:30	AB	AB			05:00			01:00			AB:Early-OUT
10/09/2016	GS - WO			WO	WO									
11/09/2016	GS - WO			WO	WO									

After processing the daily and monthly attendance of the user, the Absent days are automatically adjusted by the leave balance of the user.


On 1st AB is replaced by SL because PL has to minimum 2 as per configuration. On 5th to 7th PL is marked making Absent days as present. Similarly leaves are automatically adjusted to mark AB as PR.

<div> <div>←</div> <div> <div>User</div> <div>SF</div> <div>Shalini Fefar</div> </div> <div> <div>Attendance Period</div> <div>September</div> <div>2016</div> </div> <div>View</div> </div>														
Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/09/2016	GS	09:00	17:00	PR	SL			07:00			01:00			
02/09/2016	GS	09:15	18:00	PR	PR	00:05		07:45			01:00			
03/09/2016	GS	10:00	18:30	SL	PR			07:30	00:30		01:00			
04/09/2016	GS - WO			WO	WO									
05/09/2016	GS	09:30	16:00	PR	PL	00:20		05:30			01:00			
06/09/2016	GS	10:00	17:00	PL	PL			06:00			01:00			
07/09/2016	GS	11:00	18:00	PL	PR			06:00			01:00			
08/09/2016	GS	09:00	17:30	PR	SL			07:30			01:00			
09/09/2016	GS	10:30	16:30	SL	SL			05:00			01:00			
10/09/2016	GS - WO			WO	WO									


The number of availed leave and the closing balance can be viewed from Leave balance as shown below:



Leave Balance

←

User SF Shalini Fefar 

Leaves

Period Monthly 

Balance Month-Year September  2016 

Year	Month	Code	Name	Opening	Credit	Debit	Encashment	Availed	Closing
2016	Sep	PL	Privelege leave	0.00	20.00	0.00	0.00	4.0	16.00
2016	Sep	RH	Restricted leave	0.00					0.00
2016	Sep	SL	Sick Leave	0.00	10.00	0.00	0.00	2.5	7.50

C-OFF

Overtime: Enable this option to adjust users' less working hours with available overtime in an attendance period.

Previous Months For Overtime Hours: For attendance correction with overtime hours, specify the number of previous months here, for which the overtime should be considered. The value '1' in the field would indicate the overtime for the current month to be considered.

Short Leave: Enable this option to adjust users' less working hours with available short leaves in an attendance period.

Official Hours: Enable this option to adjust users' less working hours with available official hours in an attendance period.

Duration Check Per Official Hour Entry: Enable this option to keep a check on the duration of Official Hours allowed for auto-correction in a day.

Minimum Duration (In Minutes): Specify the minimum duration of Official Hours (in minutes) allowed in a day for auto-correction.

Maximum Duration (In Minutes): Specify the maximum duration of Official Hours (in minutes) allowed in a day for auto-correction.

Official Hours Check In Attendance Period: Enable this option to keep a check on the total duration of Official Hours allowed for auto-correction in an attendance period.

Maximum Minutes Allowed: Define the maximum number of minutes in a month that can be permitted for auto-correction using Official Hours.

Maximum Count Allowed: Define the maximum number of times in a month that Official Hours can be used auto-correction.

- Set a priority-wise order for Leaves, Overtime, Short Leave and Official Hours, based on which preference would be shown for auto-adjustment of less work hours. Use the **Up/Down** arrow buttons to change priority as shown below.

Priority	Name	Up/Down
1	Leaves	▼
2	OverTime	▲▼
3	Short Leave	▲▼
4	Official Hours	▲

Flexible Working Settings

This option enables attendance policy configuration for a Flexible type of user. A Flexible type user can be created from User Configuration (T&A) in *Users* module.

A Flexible category user's attendance is checked against his/her minimum working hours required and a "present" status is marked on the basis of fulfillment of daily, weekly or monthly targets.

Daily targets for a Flexible user may be set from the *User Configuration* page, while weekly or monthly targets can be defined using the *Attendance Policy* page.

On the **Attendance Policy** page, select the **Flexible Working Settings** tab.

Consider Daily Hours: Select one of the following options to determine how the daily work hours should be considered in case of a Flexible user -

- **Flexible For 24 Hrs:** If this option is selected, then user should be marked present depending on work done and irrespective of the time within which it was done.
- **From Shift Start:** If this option is selected, then work hours before shift start time should not be considered.
- **Till Shift End:** If this option is selected, then work hours after shift end time should not be considered.
- **From Shift Start To Shift End:** If this option is selected, then work hours before shift start time and after shift end time should not be considered.

Grace For Work Hours:

- **Daily Grace Limit (In Minutes) :** The value mentioned in Daily Grace Limit (In Minutes) indicates the duration for which grace should be allowed in the minimum working hours which are required in a day to mark a user half day or full day present. Hence, user should be marked present if these grace minutes are less than the required full day limit and compensating these minutes should not be required.

For e.g. say, Minimum Working Hours Required for Full Day is 5 hours and for Half Day is 3 hours, and Daily Grace Limit is 20 minutes. Now, the employee's work hours for a day is 4 hours 50 minutes. The user will be marked Full Day present.

- **Grace Count (Monthly):** It specifies the number of times in a month that grace will be allowed for the minimum required work hours of a user. For e.g. if Grace Count in the above case is 5, user can work 20 minutes less than the minimum required hours 5 days a month.

Flexible Hours Calculation: Specify if the Flexible hours calculation w.r.t. a user's target hours should be done on a **Weekly** or **Monthly** basis. If **None** is selected then the behavior of flexible user type should get affected only due to grace and shift boundary configuration.

Weekly Basis

- **First Day Of Week:** For Weekly calculation, specify the day which should be considered as the starting day of the week.
- **Apply Daily Work Limit:** If this option is enabled, then user should become present based on half day and full day hours mentioned in "**User Configuration**" page. If this checkbox is unchecked for "Weekly" target and user fulfills the target then user will be marked "present" irrespective of punches.
- **Weekly Target As Per:** Select the option based on which the flexible hours of a user is calculated. One can select from **Fixed Limit** or **Days In A Week** option.
- **Target Hours:** This text-box will be displayed when *Weekly Target As Per* is chosen as **Fixed Limit**. Specify the target hours to be completed in a week by a Flexible type user to mark him "present".
- **Daily Hours (In Full Day):** This text-box will be displayed when *Weekly Target As Per* is chosen as **Days In A Week**. Specify the number of hours to be considered as full day for Flexible type of user to mark him "present" for that week.
- **Grace Hours:** If this checkbox is checked, then the used grace hours should be considered while calculating total work hours in a week.

Monthly Basis

- **Apply Daily Work Limit:** If this option is enabled, then user should become present based on half day and full day hours mentioned in "**User Configuration**" page. If this checkbox is unchecked for "Monthly" target and user fulfills the target then user will be marked "present" irrespective of punches.
- **Monthly Target As Per:** Select the option based on which the flexible hours of a user is calculated. One can select from **Fixed Limit** or **Days In A Week** option.
- **Target Hours:** This text-box will be displayed when *Monthly Target As Per* is chosen as **Fixed Limit**. Specify the target hours to be completed in a month by a Flexible type user to mark him "present".
- **Daily Hours (In Full Day):** This text-box will be displayed when *Monthly Target As Per* is chosen as **Days In A Week**. Specify the number of hours to be considered as full day for Flexible type of user to mark him "present" for that week.
- **Grace Hours:** If this checkbox is checked, then the used grace hours should be considered while calculating total work hours in a month.

Deduct Hours From Target: This parameter ensures that fixed hours should get deducted from weekly/monthly target if any type of leave/tour/C-OFF, WO, PH or FB/RD occurs in a week/month. Also, it allows hours deduction from weekly/monthly target if days are prior to joining date or after leaving date occurs in a respected week or month. To avail this functionality, enable **Not Applicable Day**. Select the relevant check-boxes and enter the number of hours to be deducted against each selected option..

Deduct Hours From Target

Leave (Full Day Hrs)
☒
06:00

WO (Full Day Hrs)
☒
06:00

PH (Full Day Hrs)
☐
HH:MM

FB/RD (Full Day Hrs)
☐
HH:MM

Not Applicable Day (Full Day Hrs)
☐
HH:MM

Example 1: If Leave occurs in week/month, then 6 hrs will be deducted from target hours. If WO occurs then again 6 hrs will be deducted. So total 12 hrs will be reduced from the target hours if both leave and WO fall in the considering week/month

When full day hours are specified for the **leave**, which is on only for **Half Day**, then [Configured Leave (Full day hours)/2] hours get deducted from target hours. Consider “Example 8: Leave Hour deduction from target Hours for 24 Hrs Flexible User.”

For some cases in which one half is either WO or PH or WO/PH and other half is a leave, then hours deduction from target hours will be based on day status marked in 1st half of the particular day. Consider Following table for understanding the same:

Case No.	1st Half	2nd Half	Deduct Hours From Target Based on
1	WO	PL	Half of Configured WO (Full Day Hours) & Half of Configured Leave (Full Day Hours)
2	PL	WO	Half of Configured Leave (Full Day Hours) & Half of Configured WO (Full Day Hours)
3	PH	PL	Half of Configured PH (Full Day Hours) & Half of Configured Leave (Full Day Hours)
4	PL	PH	Half of Configured Leave (Full Day Hours) & Half of Half of Configured PH (Full Day Hours)
5	WO/PH	PL	Half of Configured WO (Full Day Hours) & Half of Configured Leave (Full Day Hours)
6	PL	WO/PH	Half of Configured Leave (Full Day Hours) & Half of Half of Configured WO (Full Day Hours)

Shortfall Hours Deduction: Specify the number of hours to be deducted as Full Day Hours from the weekly/ monthly target shortfall hours, if any.

It is deduction of full day hours and accordingly half will be the half day hours (HD hrs) when target hours are not met by the user.

The shortfall hours (SF hrs) will be target hours (TH)- actual hours (AH).

No. of half days to be marked as absent = SF hrs/ HD hrs

Let us consider an example:

Consider Weekly Target = 40:00

Consider Weekly Actual work hours done by user = 12:00

So Weekly Shortfall Hours (SF)= (TH)40- (AH)12 = 28 hours

Deduct (Full Day Hrs) = 08:00

Hence deduction of Half Day Hrs(HD) = 08:00/2 = 04:00

No. of Half Days to be deducted = (SF/HD)28:00/04:00 = 7

Hence, 7 half days will be deducted.

Consider Work Hours:

If this checkbox is checked then work hours done on AB/IN, any type of leave/tour/C-OFF, WO, PH or FB/RD in a week/month should be considered in total work hours of that week/month. You can specify the number of hours in the box to be considered.


Consider Work Hours		
On AB/IN	<input checked="" type="checkbox"/>	00:00
On Leave	<input checked="" type="checkbox"/>	00:00
On WO	<input checked="" type="checkbox"/>	00:00
On PH	<input checked="" type="checkbox"/>	00:00
On FB/RD	<input checked="" type="checkbox"/>	00:00

If work hours is enabled and value is 00:00, then the actual work done as per punches will be calculated.

If work hours is enabled and value is other than 00:00, say 08:00 hrs so 08:00 hrs is the minimum required hrs to be considered for work hours. If only 2 hrs of work is done, then it will not be considered.

Absent Marking Mode:

This parameter decides the conditions based on which a person is marked absent.

Absent Marking Mode		
Mark Absent For	Calculated Shortfall Hours	
Grace For Shortfall Hours	HHH : MM	
Mark Half Day Absent For Every	HH:MM	Hours 

- **Mark Absent For:** Select the mode as “Calculated Shortfall Hours” or “Custom Shortfall Hours” from the drop-down list based on which a person is marked absent.
- **Grace For Shortfall Hours:** Specify the grace hours to be considered in shortfall hours. This means the shortfall hours will be calculated after deducting grace from the actual work hours.
Shortfall hours = Target hours - Actual work hours - Grace hours
- **Mark Half Day Absent For Every:** Specify the hours after which the person will be marked as absent for half day.

Absent Marking Mode		
Mark Absent For	Custom Shortfall Hours ▼	
Grace For Shortfall Hours	005	: 00
Mark Half Day Absent For Every	04:00	Hours ⓘ

Flexible Process

Step1: Calculate Monthly/Weekly Target (Per day hours x No. of day)

Step2: Calculate actual work hours

Step3: Find shortfall (when work hours < target hours)

Step4: Mark AB on the basis of Shortfall

Example1: Calculated Shortfall

- Deduct (Full day hrs)= 8:00 hrs
- Target hours= 120
- Actual work hours= 110
- Mark Absent For- Calculated Shortfall

Shortfall hours = Target hours- Actual work hours
= 120- 110= 10 hours

Deduction for Half day hour= $8/2 = 4$ hours

Now $10/4 = 2.5 = 3$ halves

So in this case 3 halves will be marked Absent.

Example2: Custom Shortfall

Grace for Shortfall hours=4 hrs

Mark half day absent for every = 4 hrs

Target hours= 120

Actual work hours= 110

Shortfall hours= Target hrs- Actual work hrs- Grace for shortfall hrs
= 120- 110-4
= 6

Deduction for Half day hour= $8/2 = 4$ hours

Now $6/4 = 1.5 = 2$ halves

So in this case 2 halves will be marked Absent.



The Examples for Flexible Policy configuration for 24 hours flexibility is given below.

The flexible policy for options "From Shift Start", "Till Shift End" and "From Shift Start to Shift End" is same as "Flexible for 24 hrs"; only the calculation of daily work hours varies.

Example3: Flexible for 24 hrs- Target Completing

Min. working hrs for full day- **06:00**

Min. working hrs for half day- **03:00**

Daily Grace Limit= **30min**

Grace Count in month = **30**

Flexible hrs Calculation- **Weekly Basis**

First Day of week- **Tuesday**

Apply Daily Work limit- **disabled**

Weekly Target as Per- **Fixed Limit**

Target hours- **030:00**

Grace hours- **disabled**

Deduct hours from Target- **all disabled**

Shortfall hours deduction - **08:00**

Consider Work hours- **all enabled with 00:00**

The user has to complete atleast 2:30 hrs for half day and 5:30 hrs for full day utilizing grace of 30 mins.

If weekly work of 30 hrs is done then absent markings will be marked as Present after monthly attendance process.

The punches of the user are shown below:

Daily Attendance View														
←														
User 9 Nishu														
Attendance Period November 2016														
View														
Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/11/2016	GS	07:00	09:30	PR	AB			02:30						AB:Less Work Hrs
02/11/2016	GS	13:00	15:30	AB	AB			01:30			01:00			AB:Less Work Hrs
03/11/2016	GS	10:00	16:00	PR	AB			05:00			01:00			AB:Less Work Hrs
04/11/2016	GS	09:30	20:00	PR	PR			09:30	03:30		01:00			
05/11/2016	GS	10:30	19:00	PR	PR			07:30	01:30		01:00			
06/11/2016	GS - WO	10:00	19:00	WO	WO			08:00			01:00			
07/11/2016	GS	09:00	17:00	PR	PR			07:00			01:00			

41 hrs

By calculating hours from Work hours column, actual hours is 41 hrs

Target hours = 30

As the user completes the target hours i.e. 41 hrs > 30 hrs so any absent marking will be converted into Present after the Monthly Attendance process as shown below.

Daily Attendance View														
←														
<div> <div>User 9 Nishu</div> <div> <div>Attendance Period</div> <div>November</div> <div>2016</div> </div> <div>View</div> </div>														
Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/11/2016	GS	07:00	09:30	PR	PR			02:30						
02/11/2016	GS	13:00	15:30	PR	PR			01:30			01:00			
03/11/2016	GS	10:00	16:00	PR	PR			05:00			01:00			
04/11/2016	GS	09:30	20:00	PR	PR			09:30	03:30		01:00			
05/11/2016	GS	10:30	19:00	PR	PR			07:30	01:30		01:00			
06/11/2016	GS - WO	10:00	19:00	WO	WO			08:00			01:00			
07/11/2016	GS	09:00	17:00	PR	PR			07:00	01:00		01:00			

Example 4: Flexible for 24 hrs-Deduct WO hours;Target Completing



All configurations are same as Example3 except Deduct hours from Target

Min. working hrs for full day- **06:00**

Min. working hrs for half day- **03:00**

Daily Grace Limit= **30min**

Grace Count in month = **30**

Flexible hrs Calculation- **Weekly Basis**

First Day of week- **Tuesday**

Apply Daily Work limit- **disabled**

Weekly Target as Per- **Fixed Limit**

Target hours- **030:00**

Grace hours- **disabled**

Deduct hours from Target- **Leave- 06:00, WO-06:00**

Shortfall hours deduction - **08:00**

Consider Work hours- **all enabled with 00:00**

The punches of the user are shown below:

Daily Attendance View															
<div> <div>User 1 Roma</div> <div>Attendance Period November 2016</div> <div>View</div> </div>															
Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark	Details
01/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00				
02/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00				
03/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00				
04/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00				
05/11/2016	GS	09:00	11:30	PR	AB			02:30						AB:Less Work Hrs	
06/11/2016	GS - WO	16:00	18:00	WO	WO			02:00							
07/11/2016	GS	09:00	11:30	PR	AB			02:30						AB:Less Work Hrs	

31 hrs

WO is falling on 6th nov considering the week from 1nov Tuesday to 7th nov Monday. So WO hrs i.e. 6 hrs will be deducted from target hours.

Target hours configured = 30 hrs

Thus Actual Target hours = Target hrs - WO hrs

$$= 30 - 6 = 24 \text{ hrs}$$

Actual work hours = 31:00 hrs which is greater than 24 hours.

So after monthly process, absent marking will be converted into Present as shown below.

Daily Attendance View															
<div> <div>User 1 Roma</div> <div>Attendance Period November 2016</div> <div>View</div> </div>															
Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark	
01/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00				
02/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00				
03/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00				
04/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00				
05/11/2016	GS	09:00	11:30	PR	PR			02:30							
06/11/2016	GS - WO	16:00	18:00	WO	WO			02:00							
07/11/2016	GS	09:00	11:30	PR	PR			02:30							



In this if **Apply Daily Work Limit** is enabled, then punches on 5/11 & 7/11 will not become present.

As for full day present, minimum 6 hrs work should be done and for half day, minimum 3 hrs work should be done.

Example 5: Flexible for 24 hrs- Target shortfall



All configurations are same as Example4 except Target Hours

Min. working hrs for full day- **06:00**

Min. working hrs for half day- **03:00**

Daily Grace Limit= **30min**

Grace Count in month = **30**

Flexible hrs Calculation- **Weekly Basis**

First Day of week- **Tuesday**

Apply Daily Work limit- **disabled**

Weekly Target as Per- **Fixed Limit**

Target hours- **060:00**

Grace hours- **disabled**

Deduct hours from Target- **Leave- 06:00, WO-06:00**

Shortfall hours deduction - **08:00**

Consider Work hours- **all enabled with 00:00**

The punches of the user are shown below:

Daily Attendance View

User

1

Roma

Attendance Period

November

2016

View

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
02/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
03/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
04/11/2016	GS	09:00	15:00	PR	AB			05:00			01:00			AB:Less Work Hrs
05/11/2016	GS	09:00	11:30	PR	AB			02:30						AB:Less Work Hrs
06/11/2016	GS - WO	16:00	18:00	WO	WO			02:00						
07/11/2016	GS	09:00	11:30	PR	AB			02:30						AB:Less Work Hrs

Daily Attendance View														
<div> <div>User 1 Roma</div> <div>Attendance Period November 2016</div> <div>View</div> </div>														
Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
02/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
03/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
04/11/2016	GS	09:00	15:00	AB	AB			05:00			01:00			1st Half AB:Target Shortfall
05/11/2016	GS	09:00	11:30	AB	AB			02:30						1st Half AB:Target Shortfall
06/11/2016	GS - WO	16:00	18:00	WO	WO			02:00						
07/11/2016	GS	09:00	11:30	AB	AB			02:30						1st Half AB:Target Shortfall

Example 6: Flexible for 24 hrs- Including Work hours configuration; Actual Work hrs< Minimum required.



All configurations are same as Example5 except Consider Work hours

Min. working hrs for full day- **06:00**

Min. working hrs for half day- **03:00**

Daily Grace Limit= **30min**

Grace Count in month = **30**

Flexible hrs Calculation- **Weekly Basis**

First Day of week- **Tuesday**

Apply Daily Work limit- **disabled**

Weekly Target as Per- **Fixed Limit**

Target hours- **060:00**

Grace hours- **disabled**

Deduct hours from Target- **Leave- 06:00, WO-06:00**

Shortfall hours deduction - **08:00**

Consider Work hours- **all enabled with 00:00; On WO- 8:00 hrs ;On leave- 8:00 hrs**

The punches of the user are shown below:

Daily Attendance View														
<div> <div>User 1 Roma</div> <div>Attendance Period November 2016</div> <div>View</div> </div>														
Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
02/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
03/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
04/11/2016	GS	09:00	15:00	PR	AB			05:00			01:00			AB:Less Work Hrs
05/11/2016	GS	09:00	11:30	PR	AB			02:30						AB:Less Work Hrs
06/11/2016	GS - WO	16:00	18:00	WO	WO			02:00						
07/11/2016	GS	09:00	11:30	PR	AB			02:30						AB:Less Work Hrs

28 hrs

IF WO is enabled and work of 8 hrs is done, only then included in total work hrs.

In this case as work on WO is 2 hrs, so it is not considered. Hence actual work hours is 30- WO work hrs

= 30-2= **28 hrs.**

Target hrs= 54 hrs. (60-6= 54 hrs)

Shortfall hrs= 54- 28= **26 hrs.**

Absent marking = 26/4 = 6.5 i.e. 7 half days will be marked absent as shown below.

Daily Attendance View														
<div> <div>User 1 Roma</div> <div>Attendance Period November 2016</div> <div>View</div> </div>														
Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/11/2016	GS	09:00	16:00	PR	AB			06:00			01:00			2nd Half AB:Target Shortfall
02/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
03/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
04/11/2016	GS	09:00	15:00	AB	AB			05:00			01:00			1st Half AB:Target Shortfall
05/11/2016	GS	09:00	11:30	AB	AB			02:30						1st Half AB:Target Shortfall
06/11/2016	GS - WO	16:00	18:00	WO	WO			02:00						
07/11/2016	GS	09:00	11:30	AB	AB			02:30						1st Half AB:Target Shortfall

Example 7: Flexible for 24 hrs- Including Work hours configuration; Actual Work hrs>= Minimum required.

Min. working hrs for full day- **06:00**

Min. working hrs for half day- **03:00**

Daily Grace Limit= **30min**

Grace Count in month = **30**

Flexible hrs Calculation- **Weekly Basis**

First Day of week- **Tuesday**

Apply Daily Work limit- **disabled**

Weekly Target as Per- **Fixed Limit**

Target hours- **060:00**

Grace hours- **disabled**

Deduct hours from Target- **Leave- 06:00, WO-06:00**

Shortfall hours deduction - **08:00**

Consider Work hours- **all enabled with 00:00; On WO- 8:00 hrs ;On leave- 8:00 hrs**

The punches of the user are shown below:

Daily Attendance View

User Roma

Attendance Period

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark	Details
01/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00				
02/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00				
03/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00				
04/11/2016	GS	09:00	15:00	PR	AB			05:00			01:00			AB:Less Work Hrs	
05/11/2016	GS	09:00	11:30	PR	AB			02:30						AB:Less Work Hrs	
06/11/2016	GS - WO	12:00	21:00	WO	WO			08:00			01:00				
07/11/2016	GS	09:00	11:30	PR	AB			02:30						AB:Less Work Hrs	

36 hrs

User has worked 8 hrs on WO so 8 hrs will be considered. So Actual work hours= 36 hrs

Target hrs= 54 hrs

Shortfall hrs= 54-36= 18 hrs

Absent marking = $18/4 = 4.5$ i.e. 5 half day will be marked absent.

Daily Attendance View

User Roma

Attendance Period

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
02/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
03/11/2016	GS	09:00	16:00	PR	PR			06:00			01:00			
04/11/2016	GS	09:00	15:00	PR	AB			05:00			01:00			AB:Less Work Hrs
05/11/2016	GS	09:00	11:30	AB	AB			02:30						1st Half AB:Target Shortfall
06/11/2016	GS - WO	12:00	21:00	WO	WO			08:00			01:00			
07/11/2016	GS	09:00	11:30	AB	AB			02:30						1st Half AB:Target Shortfall

Example 8: Leave Hour deduction from target Hours for 24 Hrs Flexible User:

Consider,

Min Required Hours for Half day = **03:00**,

Min Required Hours for Full Day = **06:00**,

Apply Daily Work Limit = checked,

Weekly Target Hours = **50:00**,

For Deduct Hours From Target: WO,PH, Leave = Checked,

WO = 06:00,

PH = 06:00,

Leave = 06:00.

For Consider Work Hours: WO,PH, Leave = Checked.

Deduct (Full Day Hrs) = **06:00**.

Consider Daily View:

Day No.	First Punch	Last Punch	Work Hours	Actual Status		Updated Status		Status Summary
				1st Half	2nd Half	1st Half	2nd Half	
1	09:00	15:00	06:00	PR	PR	PR	AB	2nd half AB: Weekly hours shortfall
2	09:00	15:00	06:00	PR	PR	PR	PR	-
3	09:00	12:00	03:00	PR	PL	AB	PL	1st half AB: Weekly hours shortfall
4	09:00	17:00	08:00	PR	PR	PR	PR	No Punches Available
5	-	-	-	PH	PH	PH	PH	-
6	-	-	-	WO	WO	WO	WO	-
7	-	-	-	WO	WO	WO	WO	-

Consider following calculation:

Days considered = **3.5**

Actual Weekly Target = **29:00**

[= 50:00 - 3:00 (Day 3 2nd Half PL) - 6:00 (Day 5 PH) - 6:00 (Day 6 WO) - 6:00 (Day 7 WO)]

Weekly Work Hours = **23:00**

Weekly Shortfall Hours = **29:00 - 23:00 = 06:00**

No. of half days to be deducted = 06:00 / 3:00 = **2**

Attendance Correction-Short Leave/Official Hours Application Restrictions

The administrator can define certain restrictions on employees applications for Attendance Correction, Short Leave and/or Official Hours. This option enables the administrator to configure the parameters related to the restrictions that will be applicable to the above mentioned applications.



For restrictions to be applicable to Attendance Correction Application, make sure the application is applied by On Behalf System Account User from **Time and Attendance> Utilities> Attendance Correction**. For details, refer to [“On Behalf System Account User”](#).

For restrictions to be applicable to Short Leave/Official In-Out applications, make sure the Auto-Approve check box against Attendance Correction is disabled. For details, refer [“Roles and Rights Configuration”](#).

Click Attendance Correction-Short Leave/Official Hours Application Restrictions collapsible panel and configure the following parameters.

- **Apply To:** Select where you want to apply the restrictions from the drop down list—Attendance Correction, Short Leave/Official In-Out, Both.
- **Minimum Days After Attendance Date:** Specify the minimum number of days after the attendance date for which the application should be allowed.
- **Maximum Days After Attendance Date:** Specify the maximum number of days after the attendance date for which the application should be allowed.
- **Restrict Application Within Specified Period:** Select this check box to apply restrictions within a specified period.
- **Restriction Type:** Select the **Restriction Type** from the drop down list— Restrict w.r.t Joining Date, Restrict till Confirmation Date.
 - **Restrict w.r.t Joining Date:** If you select this option, you must configure the Restriction Period.

Restriction Period: Specify the number of days or months after joining date, for which application will not be allowed. Valid Value for Days: 1 to 999. Valid Value for Months:1 to 99.

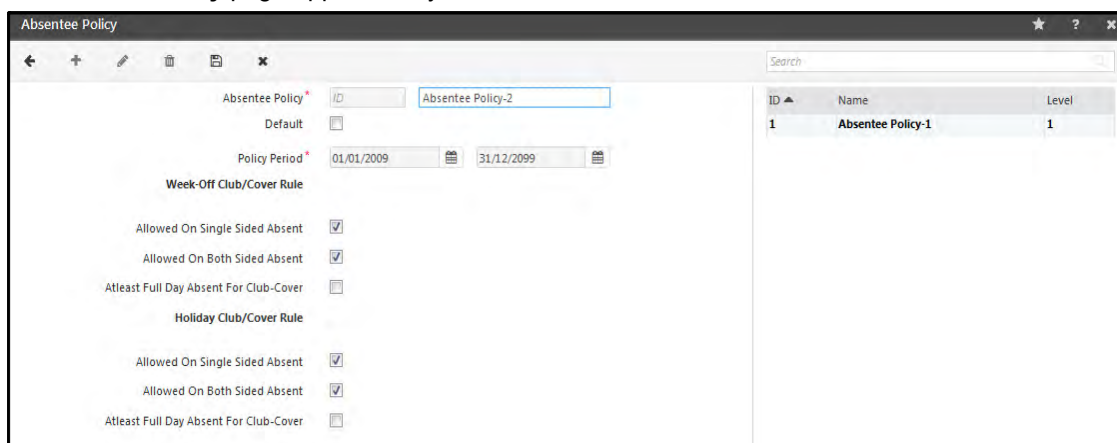
- **Restrict till Confirmation Date:** If you select this option, restriction will be applicable as per the confirmation date available in the database of the user.

Absentee Policy

The Absentee Policy option enables the user to set rules for marking the absence of an employee in the event of an employee remaining absent on either or both sides of a holiday or week-off. The user can configure a set of rules and group them together in policies.

To define Absentee Policy, Select the **Time and Attendance Module > Policies > Absentee Policy**.

The **Absentee Policy** page appears on your screen as shown below.



ID	Name	Level
1	Absentee Policy-1	1

Click the **New** icon to define a new Absentee Policy.

Each Absentee Policy will have a unique **ID** for identification and this is generated by the system automatically when the policy is saved.

Specify a user-friendly name for the Absentee Policy in the **Name** field. Specify the parameters for the other options as described hereunder:

Check the **Default** box if you want to set the current policy as the default. Users will be linked with this Absentee Policy by default in the event of a user not being linked to any Absentee Policy. Therefore, it is mandatory to define one default Absentee Policy.

Select a start date and the end date for the **Policy Period**.

Configure the absentee policy for **Week-Off** and **Holiday** cases where in the administrator can specify if the week-off or holiday is allowed in case of leaves on a single side or both sides.

Click the **Save** button to save the new policy to the COSEC database. The new *Absentee Policy* will now reflect in the Absentee Policy list as shown.



Each time the user edits the date fields in an existing policy (other than Attendance Policy) the system creates a new level for the policy as shown. The system thus maintains a record of the existing policy as well as the edited one.

ID	Name	Level
1	Absentee Policy-1	1
2	Absentee Policy-2	1
2	Absentee Policy-2	2

Example1: Consider

Allowed on Single Sided Absent is **enabled**. This means the user is allowed to be absent on only single side of week-off. The single side can be second half of previous day or first half of next day or either of the full day.



If "Atleast Full day absent for Club-cover" is enabled, then it is must to be absent for full day for absentee policy to be applicable. See Example:4

Allowed on Both Sided Absent is **disabled**. This means the user is not allowed to be absent on both sides of week-off. The both sides can be second half of previous day and first half of next day or full day on both sides.

In case1: The user is absent on only one side of week off i.e. on 2/9/16.

In case2: The user is absent on both sides of week off i.e. on 9/9/16 and 12/9/16.

User

1320

Shruti

Attendance Period

September

2016

View

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark	Details
01/09/2016	GS	08:40	19:00	PR	PR			09:20	01:20	00:20	01:00				
02/09/2016	GS			AB	AB									No Punches Available	
03/09/2016	GS - WO			WO	WO										
04/09/2016	GS - WO			WO	WO										
05/09/2016	GS	09:00	19:00	PR	PR			09:00	01:00		01:00				
06/09/2016	GS	09:00	19:00	PR	PR			09:00	01:00		01:00				
07/09/2016	GS	09:15	19:00	PR	PR	00:15		08:45	01:00		01:00				
08/09/2016	GS	09:00	20:00	PR	PR			10:00	02:00		01:00				
09/09/2016	GS			AB	AB									No Punches Available	
10/09/2016	GS - WO			WO	WO										
11/09/2016	GS - WO			WO	WO										
12/09/2016	GS	09:06	10:50	AB	AB	00:06		01:44						AB:Early-OUT	

After doing monthly attendance process, the week off on 3/9/16 and 4/9/16 remains as week-off because the user was absent on single side which is allowed. And the week-off on 10/9/16 and 11/9/16 will be marked as Absent because the user was absent on both sides of week-off which is not allowed.

The user punches and Remark is shown as below:

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark	Details
01/09/2016	GS	08:40	19:00	PR	PR			09:20	01:20	00:20	01:00				
02/09/2016	GS			AB	AB									No Punches Available	
03/09/2016	GS - WO			WO	WO										
04/09/2016	GS - WO			WO	WO										
05/09/2016	GS	09:00	19:00	PR	PR			09:00	01:00		01:00				
06/09/2016	GS	09:00	19:00	PR	PR			09:00	01:00		01:00				
07/09/2016	GS	09:15	19:00	PR	PR	00:15		08:45	01:00		01:00				
08/09/2016	GS	09:00	20:00	PR	PR			10:00	02:00		01:00				
09/09/2016	GS			AB	AB									No Punches Available	
10/09/2016	GS - WO			AB	AB									WO-AB:Absent Cover Rule	
11/09/2016	GS - WO			AB	AB									WO-AB:Absent Cover Rule	
12/09/2016	GS	09:06	10:50	AB	AB	00:06		01:44						AB:Early-OUT	

Example2:

In above example if Allowed on Both Sided Absent is also **enabled**; then week-off on 10/9/16 and 11/9/16 will remain as week-off.

Example3:

If Allowed on Single Sided Absent is **disabled** and Allowed on Both Sided Absent is **disabled**; then both the week-offs will be marked absent.

Example4: Consider

Allowed on Single Sided Absent is **enabled**.

Atleast Full day absent for Club-cover is **enabled**

This means the week-off will become absent if user is full day absent on both sides of weekoff.

- If second half of previous day(Case1) or first half of next day(Case2) is absent. Then after monthly attendance process, week-off will remain as week-off.
- If full day absent on one side(Case3 & Case4), Then after monthly attendance process, week-off will remain as week-off.
- If user is full day absent on both sides of week-off(Case5). Then after monthly attendance process, week-off will become absent.

S.NO	Saturday First half	Saturday Second half	Sunday WO	Monday First half	Monday Second half	WO after monthly process
Case1	PR	AB	WO	-	-	WO
Case2	-	-	WO	AB	PR	WO
Case3	AB	AB	WO	-	-	WO
Case4	-	-	WO	AB	AB	WO
Case5	AB	AB	WO	AB	AB	AB



The Holiday club/cover rule will work similar to the week-off club/cover rule.

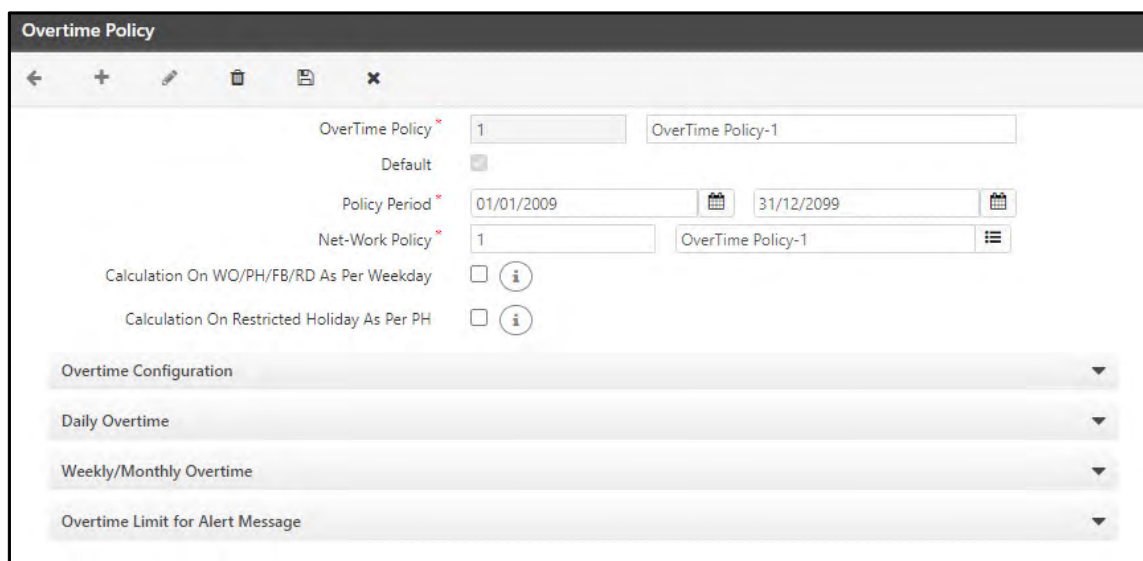
Overtime Policy

Overtime Policy is the Policy of a company which consists of rules for providing overtime compensation to the employees.

For example, a company may allow its employees to work overtime for a duration of maximum 2 hours per working day. Hence, this may be converted by the respective HR team into an overtime policy that is applicable to all employees across the organization.

COSEC simplifies and automates such implementations by enabling administrators to configure parameters related to overtime policies.

To configure an Overtime policy, select to **T&A> Policies> Overtime Policy**



Click the **New** button to define a new OT policy.

Enter a **OverTime Policy** name for the new policy in the field provided. The **ID** will be automatically generated by the system for every new policy defined.

Select the **Default** checkbox if the policy is to be stated as the default policy for the system.

Define the **Policy Period** by specifying the Start and End Dates for the span of policy.

Network Hour Policy: Select a network hours policy from the picklist.

Calculation On WO/PH/FB/RD As Aer Weekday: Select this checkbox to calculate Net-Work Hours and Overtime as per week day's configuration if nothing has been configured for WO/PH.

Calculation On Restricted Holiday As Per PH: Select this checkbox to calculate Net-Work Hours and Overtime as per configuration of PH if user has worked on day configured for full day RH leave. If RH is applied for half day, then it will work as per week day.

- Example: The user has worked on RH leave for 10 hours. But the Net-work hours and overtime will not be calculated when this checkbox is enabled.

Click **Save** to add the new policy to the database successfully.

Overtime Configuration

The Overtime Configuration allows you to configure Overtime parameters like **Daily/Weekly/Monthly** and **rounding** of overtime minutes. Refer "[Calculation of Overtime](#)".

For JPC user, refer "[OT for JPC User](#)".

- Select the **Overtime Configuration** tab as shown.

- **Enable Overtime Calculation** - Select this checkbox to enable overtime calculation for all users to whom this Net-work hours and OT policy would be applicable.
- **Daily Overtime** - Select the days of the week which are to be considered for *Daily Overtime* calculation. You can also select WO, PH or WO/PH to calculate daily overtime based on day status.
- **Weekly/Monthly Overtime** - Select the days of the week which are to be considered for *Weekly/Monthly Overtime* calculation. You can also select WO, PH or WO/PH to calculate weekly/monthly overtime based on day status.



The Days (Mon to Sun) selected for Daily OT will be disabled for Weekly/Monthly OT Selection and Vice versa.



WO, PH and WO/PH can be selected for both Daily as well as Weekly/Monthly Overtime.



For Overtime calculation, the Days will be prioritized and considered based on day status (like WO, PH, WO/PH).


For example:

Days selected in 'Daily Overtime > Days To Consider For Calculation' are:

- Monday
- Tuesday
- Friday

- PH

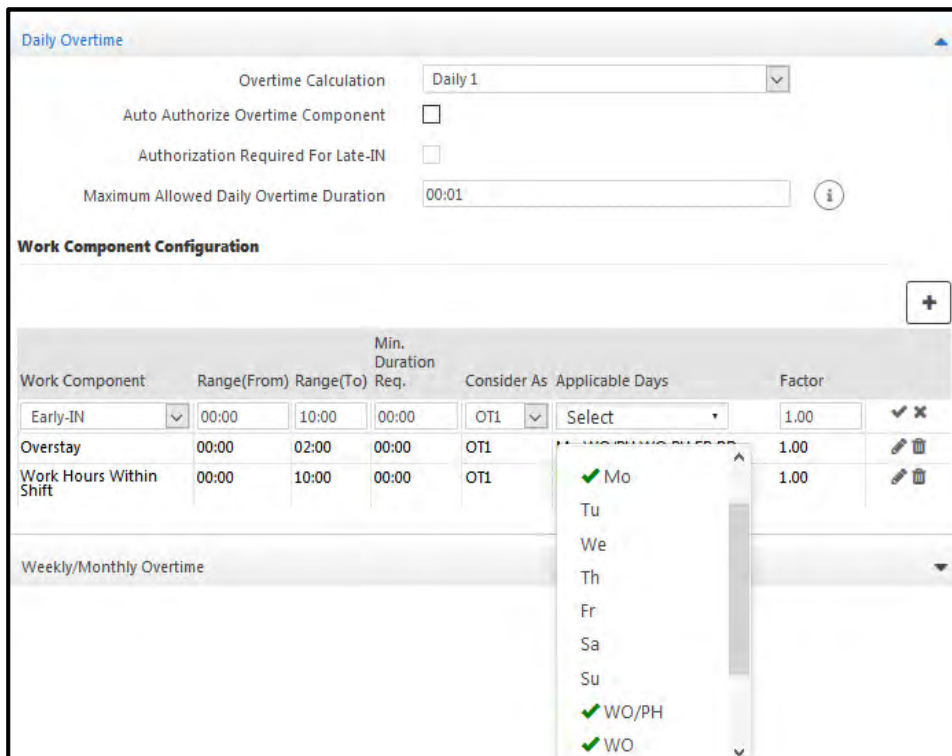
So irrespective of PH falls on any other day like Wednesday, Thursday, Saturday or Sunday, days with day status as PH should be considered in daily overtime calculation.

- **Overtime Rounding For Fraction of An Hour** - Enable this feature for users to obtain rounded values for the final calculated overtime. This allows the administrator to specify how a fractional part of an hour in the final overtime value should be considered for calculation.
 - Activate the Overtime Rounding by checking the **Enable** box.
 - Specify the **range** of overtime hours in minutes which is to be rounded off and select the **replace value** as actual or fixed value.
 - Here we have kept 1 to 10 minutes of range to be rounded off with the **actual value**.
 - If **fixed option** is selected, then mention a fixed value to replace. Suppose if a user has overtime of 8 minutes. And fixed rounding is set for range 1 to 20 minutes at value 10 minutes. Then he will get overtime of 10 minutes.
- Click **Save**  to save the overtime configuration.

Daily Overtime

This section allows the administrator to configure Daily Overtime calculation.

- Select the **Daily Overtime** tab as shown.



Work Component	Range(From)	Range(To)	Min. Duration Req.	Consider As	Applicable Days	Factor
Early-IN	00:00	10:00	00:00	OT1	Select	1.00
Overstay	00:00	02:00	00:00	OT1		1.00
Work Hours Within Shift	00:00	10:00	00:00	OT1		1.00

Weekly/Monthly Overtime

- **Overtime Calculation** - Select the type of daily overtime calculation to be performed from the options of Daily1 or Daily2. You can disable the OT as well.

- **Auto Authorize Overtime Component** - Select this checkbox to enable automatic authorization of daily overtime. In case it is not checked, the reporting in-charge or administrator can authorize the overtime.
- **Authorization Required for Late-IN** - Check this box in case the Late-IN is to be authorized.

Click the Add button to configure the Work Component. Select **Early-IN**, **Overstay** and **Work hours within Shift** and configure the related parameters as shown below.

The screenshot shows the 'Daily Overtime' configuration window for 'Daily 1'. It includes checkboxes for 'Auto Authorize Overtime Component' (checked) and 'Authorization Required For Late-IN' (unchecked). Below is the 'Work Component Configuration' table:

Work Component	Range (From)	Range (To)	Minimum Duration Required	Consider As	Applicable Days	Factor	
Early-IN	00:00	10:00	00:00	OT1	WO/PH WO PH FB RD	1.00	
Overstay	00:00	02:00	00:00	OT1	WO/PH WO PH FB RD	1.00	
Work Hours Within Shift	00:00	10:00	00:00	OT1	WO/PH WO PH FB RD	1.00	

For Daily2 OT

The screenshot shows the 'Daily Overtime' configuration window for 'Daily 2'. It includes checkboxes for 'Auto Authorize Overtime Component' (checked), 'Authorization Required For Late-IN' (checked), and 'Allow Overlapping Work Components' (checked). There are also input fields for 'Special OT Time Range' in HH:MM format. Below is the 'Work Component Configuration' table:

Net-Work Hours Range (From)	Net-Work Hours Range (To)	Minimum Duration Required	Consider As	Applicable Days	Factor	Overtime Assignment As Per	
00:00	100:00	00:00	OT1	WO/PH WO PH FB RD	1.00	Priority Work Component	

- **Allow Overlapping Work Components**- Check this box if the overlapping of work components ranges is to be allowed. It may be useful when some special OT is required to be granted if user works within some special time range along with the existing granted OT.
- **Special OT Time Range**- Specify the time range for eg: 21:00 hrs to 04:00 hrs for which special OT is to be given to the person who has worked in this time range. Refer "".

Click the Add button to configure the Network hours.

- **Net work hours Range** - Define a time range for the Net work hours in the HHH:MM format to be considered as daily overtime.
- **Min Duration Required Within Range** - Define a minimum duration within the range which must be covered to qualify as daily overtime.

- **Consider As-** This field contains 5 different OT components. These components are used to differentiate OT calculations. Like in one component say OT1, we can add calculated values of Early-in and in other component say OT2, we can add calculated values of Overstay. In this way these components can get used.
- **Applicable Days** - Select the days of the week for which this overtime configuration will be applicable.
- **Multiplication Factor** - Specify the multiplication factor which should be used against the total calculated overtime for a specified period for overtime pay calculation.
- **Overtime Assignment As Per-** Select the option as Priority Work Component or Special Time Range. According to this selection the OT will be assigned. For eg: OT1 is given the Priority work component and OT2 is given the Special Time range component as shown below.
- Click the **Save** button to save the overtime configuration.



For overlapping range of Priority OT and Special Time range OT; if x hr OT is given for time range OT; then priority OT cannot be given for same time hrs. Eg: From 9:00 to 10:00 hrs, special OT is given to user. Then priority OT cannot be given for 9:00 to 10:00 hrs.

If user is working for more than 1 shift, say for around 24 hours at a time, then he should mark OUT punch using special function OT OUT if configured. See Devices> Multi Device Options> Special Functions> Special function-Overtime Out.

Daily1 OT and Daily2 OT Examples

Daily 1 overtime calculation will be based on Shift timings as per components Early-IN, Overstay and Work Hours Within Shift.



If configuration for WO, PH and WO/PH is available and also its respective day, then priority to WO, PH and WO/PH should be given.

"Work Hours Within Shift" = Work Hours - Early-IN - Overstay - Short Leave Hours (if "Add Short Leave Hours In Work Hours" field is checked in "Attendance Policy" page) - Official Hours (If "Add Official Hours In Work Hours" field is checked in "Attendance Policy" page)

For flexible type user, only "Work Hours Within Shift" and "Overstay" value are calculated on normal day so similar behavior should be followed for WO, PH and WO/PH where these components should be calculated as per shift as done on normal day.

For FB/RD, only "Work Hours Within Shift" component gets calculated.

Example1

Shift: 09:00 to 18:30 hours

Punches: 18:00 - 20:00 hours

Work hours (on WO): 02:00

Net- work hours: 02:00 (NOTE: Consider all components for whole component range is configured)

Overtime (**Daily 1**): 00:30 (NOTE: Consider "Work Hours Within Shift" work component for whole component range is configured)

Overtime (**Daily 2**): 02:00

Example2

Shift: 15:00 - 23:00

Punches: 07:00 - 10:00 [i.e. not within shift]

Work Hours (on WO): 03:00

Net-Work Hours: 03:00 (Early-IN) (NOTE: Consider all components for whole component range is configured)

Overtime (**Daily 1**) = 03:00 (Early-IN) (NOTE: Consider all components for whole component range is configured)

Overtime (**Daily 2**)= 03:00 (Early-IN) (NOTE: Consider "Early-IN" and "Overstay" components for whole component range is configured)

Weekly/Monthly Overtime

This section allows the administrator to configure Weekly/Monthly Overtime calculation.

To configure Weekly/Monthly Overtime,

- Select the **Weekly/Monthly Overtime** tab as shown.

The screenshot shows the 'Weekly/Monthly Overtime' configuration window. It includes the following fields and sections:

- Overtime Calculation:** A dropdown menu set to 'Weekly'.
- Week Start Day:** A dropdown menu set to 'Monday'.
- Auto Authorize Overtime Component:** A checked checkbox.
- Authorization Required For Late-IN:** A checked checkbox.
- Maximum Allowed Weekly Overtime Duration:** A field with '999' and '59' separated by a colon, with an information icon.
- Consider In Net Work Hours:** A section with four rows: 'Week Offs', 'Holidays', 'Paid Leaves', and 'Not Applicable Day'. Each row has a checkbox and a 'Shift Based' dropdown with an 'HHMM' input field. The 'Week Offs' checkbox is checked. There is an information icon to the right of this section.
- Consider Work Done on WO/PH/Paid Leaves:** A checked checkbox.
- Work Component Configuration:** A table with a '+' button to add new components.

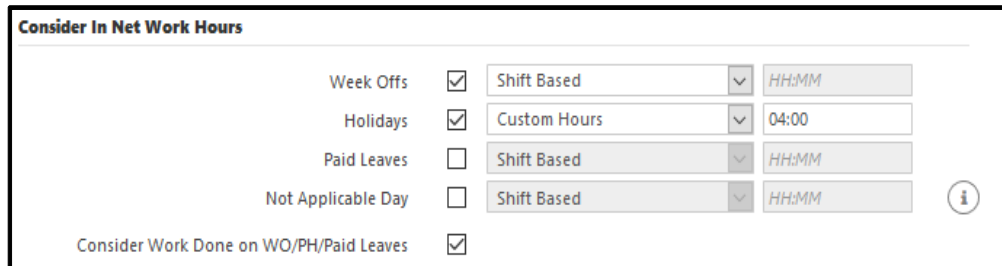
Net-Work Hours Range(From)	Net-Work Hours Range(To)	Min. Duration Req.	Consider As	Factor
00:00	100:00	00:00	OT1	1.00

- **Overtime Calculation** - Select the type of overtime calculation (**weekly or monthly**) to be performed from the dropdown list. Select Disabled to disable both weekly/monthly overtime calculation.
- For **Weekly** overtime calculation, the **Week Start Day** is to be specified from the drop-down list as shown to indicate the overtime calculation cycle. So, if Monday is selected as the **Week Start Day**, the weekly overtime will be calculated till the coming Sunday.
- **Auto Authorize Overtime Component** - Select this checkbox to enable automatic authorization of weekly/monthly overtime.
- **Authorization Required for Late-IN** - Select this checkbox in case the Late-IN is to be authorized.

Consider In Net Work Hours

Select the checkboxes to specify whether **Week Offs**, **Holidays**, **Paid Leaves** or **Not Applicable Day** are to be considered within Net Work Hours for the weekly/monthly overtime calculation.

- You can select **Shift Based** hours to consider complete shift hours in Network hours or
- You can select **Custom hours** and specify specific hours to be included in Net-work hours.



Consider Work Done on WO/PH/Paid Leaves: If this checkbox is enabled only then work done on WO/PH/Paid leaves will be considered in Net-work hours.

Example: If Week Offs is enabled for Shift Based and Holidays for Custom 4 hrs. And “Consider Work Done on WO/PH/Paid Leaves” is enabled;

- Then suppose user has worked for 5 hrs on WO then shift hours (say 8hrs) + work done (5 hrs) = 13 hrs will be added to the Net work hours.
- Suppose user has done work for 6 hrs on holiday then custom hrs (4 hrs) + work done (6 hrs) will be added to the Net-work hours.

If “Consider Work Done on WO/PH/Paid Leaves” is disabled;

- Then work done on WO/Holidays wont be considered in Net-work hours and only shift hours/custom hours will be considered.
- In case of paid leave with half day present status, then work done on half day hours will be added in the net work hours.
- In case of full day paid leave status, then work done on that day will not be added in the net work hours.



For work done on a Week Off/Public Holiday, the shift duration for a WO/PH day shall be counted in the week's total net work hours, if and only if, that day of the week is applicable for Weekly OT calculation.

Example: Daily overtime is to be calculated for WO and PH days. Weekly overtime should consider custom hours of 09:00 for Not Applicable Days falling in the week. Any work above 45:00 should be considered as Overtime. Consider Work Done on WO/PH/Paid Leaves” = Unchecked.

Date	Day Type	Work hours
15-4-2019 Monday	Not Applicable	
16-4-2019 Tuesday	Not Applicable	
17-4-2019 Wednesday Joining Date	Normal	9:30

Date	Day Type	Work hours
18-4-2019 Thursday	Normal	9:30
19-4-2019 Friday	Normal	9:15
20-4-2019 Saturday	Week Off	5:00
21-4-2019 Sunday	Week Off	00:00

In above example:

Daily OT generated on 20/04/2019 - **05:00**

Weekly OT - **01:15** (This will be achieved since Net-Work = 09:00 (15/04/2019) + 09:00 (16/14/2019) + 09:30 (17/04/2019) + 09:30 (18/04/2019) + 09:15 (19/11/2018) = 46:15

Work Component Configuration

- **Work Component** - Select the work component option as **Net-Work Hours**. This indicates that the weekly/monthly overtime will be calculated based on the Net-Work Hours Configuration as performed earlier.
- **Work Component Range** - Define a time range for a user's net work hours in the HHH:MM format to be considered as overtime.
- **Min Duration Required Within Range** - Define a minimum duration within the Work Component Range which must be covered, for the user's net work hours to qualify as overtime.
- **Consider Component As** - This is to designate the selected work component as an overtime type. COSEC allows the definition of up to 5 overtime types on the system - OT1, OT2, OT3, OT4 and OT5.
- **Multiplication Factor** - Specify the multiplication factor which should be used against the total calculated overtime for a specified period for overtime pay calculation.

Click the **Add** button to save the overtime configuration. The work component and its parameters are now reflected in a grid list as shown.

Work Component	Range	Consider AS	Min Duration Req.	Applicable Days	Factor	
Net-Work Hours	100:00 - 200:00	OT1	100:00		0.5	

Click **Save**  .



For users who are auto-authorized for Overtime and are assigned Net-Work Hours & Overtime Policy having Overtime as auto-authorized, an OT authorization request will still be generated if User is late to report for a shift (i.e. after Shift Start Time added with Grace Time for Shift Late-IN).

OT for JPC User

Daily1

Example1

Consider 2 punch system, Shift timings: 9:00- 18:00, No Break Configured.

Work Component	Range	Consider as	Minimum required	Applicable days	Multiplication Factor
Early-IN	0:00 to 23:59	OT1	00:00	All	1
Overstay	0:00 to 23:59	OT2	00:00	All	1
Work Within Shift	0:00 to 23:59	OT3	00:00	All	1

JPC Timesheet Transactions

Network and OT against transaction

Transaction start	Transaction end	Early IN	Late-OUT	Work within Shift	OT1	OT2	OT3
07:00	15:00	02:00	00:00	06:00	02:00		06:00
15:00	17:00	00:00	00:00	02:00			02:00
17:00	20:00	00:00	02:00	01:00		02:00	01:00

Example2

Consider 2 punch system, Shift timings: 9:00- 18:00, No Break Configured

OT	Work Component	Range	Minimum required	Applicable days	Multiplication Factor
OT1	Early-IN	00:00 to 01:00	00:00	All	1
OT2	Early-IN	01:00 to 23:59	00:00	All	1
OT1	Overstay	00:00 to 01:00	00:00	All	1
OT2	Overstay	01:00 to 23:59	00:00	All	1
OT1	Work within Shift	00:00 to 01:00	00:00	All	1
OT2	Work within Shift	01:00 to 23:59	00:00	All	1

T&A Transaction and Overtime

IN Punch	OUT Punch	Early IN	Late-OUT	Work within Shift	OT1	OT2
07:00	20:00	02:00	02:00	09:00	03:00	10:00

OT1= Early IN (1 hr) + Late-Out (1 hr) + Work within shift (1 hr) = 3 hours

OT2= Early IN (1 hr) + Late-Out (1 hr) + Work within shift (8 hr) = 10 hours

JPC Timesheet Transactions

Transaction start	Transaction end	Early IN	Late-OUT	Work within Shift	OT1	OT2
07:00	15:00	02:00	00:00	06:00	02:00	06:00
15:00	17:00	00:00	00:00	02:00	00:00	02:00
17:00	20:00	00:00	02:00	01:00	01:00	02:00

Daily2 OT

Consider 2 punch system, Shift timings: 9:00- 18:00, No Break Configured.

Net work hours include: Early-IN, Work Hours Within Shift and Overstay (00:00-23:59)

Range	Consider as	Minimum duration	Applicable days
6:00 to 8:00	OT1	00:00	All
8:00 to 12:00	OT2	00:00	All
12:00 to 23:59	OT3	00:00	All

No Change in JPC

T&A Punches	Network Hours	Standard Hours	OT1	OT2	OT3
09:00- IN 21:00 –OUT	12:00	06:00	2:00	4:00	-

Normal Hours: Hours considered in T&A's Network hours against corresponding JPC transaction i.e. the hours considered in Network hours which are distributed as per JPC's transaction.

Eg: If Network hours is 12 hours and total transactions are of 15 hours so normal hours will be 12 hours only.

Standard Hours: Hours not accountable for overtime calculation (Daily 2) i.e. if overtime is to be given after working hours of 9 hours, then standard hours are 9 hours. You can calculate from the Range if given. Suppose Range is 6:00 to 8:00, then OT will be given after 6 hours so the standard hours is 6 hours.

Network and OT against transaction

Transaction start	Transaction end	Normal Hours	Standard Hours	OT1	OT2	OT3
09:00	15:00	06:00	06:00			
15:00	17:00	02:00	00:00	02:00		
17:00	21:00	04:00	00:00		04:00	

Specified Award/Penalty against transaction

Transaction start	Transaction end	Award	Penalty
09:00	15:00	03:00	
15:00	17:00		
17:00	21:00		02:00

Network Hours= Network hours+ Award Duration-Penalty Duration
= 12+3-1 =13:00 hours
So, Standard hours= 6:00
OT1= 2:00, OT2=4:00, OT3=1:00

Network and OT against transaction after Award/Penalty Consideration

Transaction start	Transaction end	Award	Penalty	Normal Hours	Standard Hours	OT1	OT2	OT3
09:00	15:00	3:00		09:00	06:00	02:00	01:00	
15:00	17:00			02:00	00:00		02:00	
17:00	21:00		2:00	02:00	00:00		01:00	01:00

OT for Overlapping Time Range

Consider 2 punch system, Special Time Range=21:00 to 04:00

Net-Work Hours include: Early-IN, Work Hours Within Shift, Overstay, Award Duration and Penalty Duration (00:00 - 23:59)

Range	Consider as	Minimum duration	Applicable days	Consider Overtime as per
9:00 to 11:00	OT1	00:00	All	Priority
11:00 to 23:59	OT3	00:00	All	Priority
9:00 to 11:00	OT2	00:00	All	Special Time Range
11:00 to 23:59	OT4	00:00	All	Special Time Range

Example:1

T&A Punches	Network Hours	Standard Hours	Special OT	Priority OT	OT1	OT2	OT3	OT4
09:00- IN 21:00 –OUT	12:00	06:00	0:00	3:00	2:00		1:00	

Example:2

T&A Punches	Network Hours	Standard Hours	Special OT	Priority OT	OT1	OT2	OT3	OT4
18:00- IN 06:00 –OUT	12:00	09:00	1:00	2:00	2:00			1:00

Priority OT: Overtime calculated against Priority OT Component Range.

Special OT: Overtime calculated against Special OT Time Range.

Special OT calculation

When Daily 2 Overtime configuration is including Special OT components then first it decides the overall Special Overtime and Priority Overtime. Projected OT Start should be figured out considering Eligible Early IN that has actually contributed in the Net-Work Hours.

Net-Work Hours Calculation:

Maintain a variable as Eligible Early IN which should be calculated as sum of the early-in duration that is contributing to Net-Work Hours for the day

Daily 2 Overtime Calculation:

Steps for figuring out Projected OT Start have been updated to consider Eligible Early IN .

Example1: With Early IN

Shift Timings= 18:00 to 03:00

Graveyard shift time range: 21:00 to 05:00

Network hours Configuration

Component	Range	Minimum duration	Applicable days
Early IN	0:00 to 23:59	00:00	Week days
Work within shift	0:00 to 23:59	00:00	Week days
Overstay	0:00 to 23:59	00:00	Week days

Work Hours Duration

Range	Consider as	Minimum duration	Applicable days	Graveyard Shift
9:00 to 11:00	OT1	00:00	Week days	No
11:00 to 23:59	OT3	00:00	Week days	No
9:00 to 11:00	OT2	00:00	Week days	Yes
11:00 to 23:59	OT4	00:00	Week days	Yes

T&A Punches	Network Hours	Standard Hours	Eligible Early-IN	Projected OT start	OT time range	Special OT	Priority OT	OT 1	OT 2	OT 3	OT 4
15:00- IN 17:00 – OUT 18:00-IN 06:00- OUT	14:00	09:00	2:00	1:00	01:00 to 06:00	4:00	1:00	1: 00	2: 00		2: 00

Description:

Network hours: (Punch IN time:15:00 hrs to Punch OUT time:06:00 hrs) - (Out time from 17:00 to 18:00 hrs)
 = 15 hrs - 1 hr
 = 14:00 hrs

Eligible Early IN: (Punch time:15:00 hrs to Shift start time:18:00 hrs) - (Out time from 17:00 to 18:00 hrs)
 = 3 hrs - 1 hr
 = 2 hrs

Projected OT start= Shift start- Eligible Early IN + standard hours
 = 18:00- 2:00+ 9:00
 = 01:00 so OT is projected to start from 1am

Thus OT time range= Projected OT start time to OUT punch time
= 1 am to 6am

So Total OT is to be given for 1 am to 6am of work = 5 hrs

Special OT is to be given first. Now the special time range or Graveyard shift range is from 21:00 hrs to 05:00 hrs.
Hence from 1am to 5am will be given as **Special OT= 4 hrs**

Remaining 1 hr from 5am to 6am will be given as **Priority OT= 1 hr**

The Priority OT of 1 hr will be distributed among OT1 and OT3. As OT1 has range of 2 hours so OT1 will be given 1 hr.

The Special OT of 4 hrs will be distributed among OT2 and OT4. As OT2 has range of 2 hours so OT2 will be given 2 hrs and OT4 as 2 hrs.

Example2: WithOut Early IN

Consider only work within shift and overstay in Network hours. All other configurations being same.

T&A Punches	Network Hours	Standard Hours	Eligible Early-IN	Projected OT start	OT time range	Special OT	Priority OT	OT 1	OT 2	OT 3	OT 4
15:00- IN 17:00 – OUT 18:00-IN 06:00- OUT	12:00	09:00	Do not calculate as Early-IN is not configured	3:00	03:00 to 06:00	2:00	1:00	1:00	2:00		

Projected OT start= Shift start- Eligible Early IN + standard hours
= 18:00- 0:00+ 9:00
= 3:00 hrs

Example1: Daily2 OT Calculation with Priority OT and Special OT

Consider Network Hours configuration as:

Work Component	Range	Consider as	Minimum duration reqd.	Applicable days	factor	Remarks
Work hours within shift	00:00 to 10:00	work	00:00	M,T,W,Th,F Sa	1	Shift duration is counted in network hrs
Early-IN	00:00 to 02:00	work	00:10	M,T,W,Th,F Sa	1	Min 0 and Max 2 hrs of EI will be calculated for Net-work hours
Overstay	02:00 to 08:00	work	00:30	M,T,W,Th,F Sa	1	Min 2 and Max 8 hrs of Overstay will be calculated for Net-work hours

Consider Overtime Configuration as:

Daily Overtime is enabled for M, T ,W, Th

Consider Daily Overtime Configuration as:

Overtime Calculation is selected as Daily2
 Auto Authorize Overtime component is enabled
 Allow Overlapping work components is enabled
 Special OT time range is 21:00 to 04:00

Range	Consider as	Minimum duration reqd.	Applicable days	Multiplication factor	OT assignment
01:00 to 100:00	OT1	00:00	M,T,W,Th	1	Priority
02:00 to 100:00	OT2	00:10	M,T,W,Th	1	Time Range

Consider Weekly/Monthly Overtime as Disabled

Consider shift of the user is 09:00 to 18:00. Shift duration is 8 hrs with break from 13:00 to 14:00. Break deviation allowed.

To generate the overtime of the user, Daily and Monthly attendance process must be run.

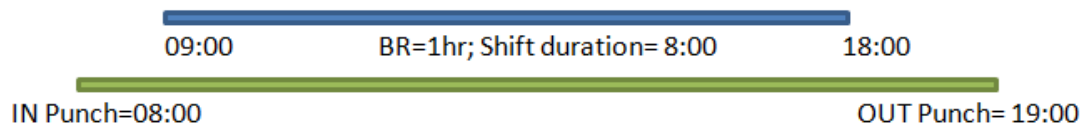
Now after the daily and monthly attendance process, the user punches in the Daily attendance view are shown below:

<div> User <input type="text" value="rf"/> Rosy </div> <div> Attendance Period <input type="text" value="September"/> 2016 </div> <div> View </div>														
Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/09/2016	GS	08:00	19:00	PR	PR			10:00	02:00	09:00	01:00	08:00		
02/09/2016	GS	09:00	21:00	PR	PR			11:00	03:00	09:00	01:00			
03/09/2016	GS	09:00	20:00	PR	PR			10:30	02:00	08:30	00:30			
04/09/2016	GS - WO	07:30	21:00	WO	WO			12:30	04:30		01:00			
05/09/2016	GS	08:15	19:00	PR	PR			10:30	01:45	09:30	00:15	08:30		
06/09/2016	GS	07:30	22:00	PR	PR			13:30	05:30	11:30	01:00	09:30		
07/09/2016	GS	09:15	23:30	PR	PR			14:05	05:30	12:05	00:10	10:05		
08/09/2016	GS	06:00	23:00	PR	PR			16:00	08:00	13:00	01:00	11:00		
09/09/2016	GS	09:00	23:45	PR	PR			13:45	05:45	11:45	01:00			
10/09/2016	GS - WO			WO	WO									
11/09/2016	GS - WO			WO	WO									

Calculation of Network hours

Network hours= Early IN component + Work hours within shift + Overstay component

On 1st



- Early IN=1hr
- Work hours within shift=(9hrs to 18 hr - break duration) =9-1 = 8 hrs
- Overstay= 1hr but overstay range should be minimum 2 hrs to consider for network hours so Overstay=0

So **Network hours=EI + WS+ OS = 1+ 8 +0 = 9hrs** which is shown by arrow on 1st

2nd

Network hours= Early IN component + Work hours within shift + Overstay component
=0 +(shift duration- break hrs) + (3-2)
= 0+ (9:00-1:00) +1 = 8+1= 9 hrs

3rd

Network hours= Early IN component + Work hours within shift + Overstay component
=0 +(shift duration- break hrs) + (2-2)
= 0 +(9:00- 00:30) +0
= 8:30 hrs

4th

Network hrs is not calculated on sunday as it is not configured for sunday.

5th

Network hours= Early IN component + Work hours within shift + Overstay component
=00:45 +(shift duration- break hrs) + (1hr < min reqd 2 hr)
= 00:45 +(9:00- 00:15) +0
= 00:45 + 8:45 = 9:30

6th

Network hours= Early IN component + Work hours within shift + Overstay component
=1:30 +(shift duration- break hrs) + (4-2)
=1:30 +(9:00- 01:00) +2
= 1:30 + 8:00+2 = 11:30

7th

Network hours= Early IN component + Work hours within shift + Overstay component
=0 +(shift duration- break hrs) + (5:30-2)
= 0 +[9:15 to 18:00]- 00:10) +3:30
= 08:35 +3:30 = 12:05

8th

Network hours= Early IN component + Work hours within shift + Overstay component
=(3:00 hrs, but max allowed is2:00) +(shift duration- break hrs) + (5-2)
=2:00 +(9:00- 01:00) +3
= 2:00 + 8:00+ 3 = 13:00

9th

Network hours= Early IN component + Work hours within shift + Overstay component
=0 +(shift duration- break hrs) + (5:45-2)

$$= 0 + (9:00 - 01:00) + 3:45$$

$$= 08:00 + 3:45 = 11:45$$

Calculation of Overtime

Overtime = Network hours- Standard hours

Standard hours is the minimum hours in the Range of network hours to consider for overtime.

From range 01:00 to 100:00, Priority OT1 is configured. So here standard hours is 1:00

From range 02:00 to 100:00, Special OT2 is configured. So here standard hours is 2:00

Date	Network hours	Work done	Overlapping hours with special time range (21:00 to 04:00)	Standard hours	Daily2 on M,T,W,Th	Overtime= Network hours- Standard hours	Special OT OT2	Priority OT OT1
1/9/16	9	8:00 to 19:00	0	1	Th	9-1= 8	-	8:00
2/9/16	9	9:00 to 21:00	0	1	F	NA on Friday	-	-
3/9/16	8:30	9:00 to 20:00	0	1	Sa	NA on Saturday	-	-
4/9/16	NA on Sunday	7:30 to 21:00	0	1	Su	NA on Sunday	-	-
5/9/16	9:30	8:15 to 19:00	0	1	M	8:30	-	8:30
6/9/16	11:30	7:30 to 22:00	1:00	2	T	9:30	1:00	8:30
7/9/16	12:05	9:15 to 23:30	2:30	2	W	10:05	2:30	7:35
8/9/16	13:00	6:00 to 23:00	2:00	2	Th	11:00	2:00	9:00
9/9/16	11:45	9:00 to 23:45	2:45	2	F	NA on Friday	-	-

Here Standard hours is 1:00 when work is not done in special time range of 21:00 to 04:00; other wise standard hours considered will be 2:00 hrs as configured in the range.

Now Daily2 OT is configured from Monday to Thursday. So OT on 1st= 8 hrs. This will be Priority OT which is OT1; so OT1 for 1st = 8:00 hrs

Similarly on 5th, OT1= 9:30 -1 = 8:30 hrs.

On 6th user has worked from 21:00 to 22:00 in special time range, so 1:00 hr will be given to special OT.

Total OT= Network hrs- Standard hrs

$$= 11:30 - 2 = 9:30 \text{ hrs}$$

Out of total overtime of 9:30 hrs, Special OT OT2= 1 hr

So Priority OT; OT1=8:30 hrs

Similarly OT1 and OT2 can be calculated for other days as shown in above table.

Example2: Weekly OT Calculation

Consider Network Hours configuration as:

Work Component	Range	Consider as	Minimum duration reqd.	Applicable days	factor	Remarks
----------------	-------	-------------	------------------------	-----------------	--------	---------

Work hours within shift	00:00 to 10:00	work	00:00	M,T,W,Th,F Sa	1	Shift duration is counted in network hrs
Early-IN	00:00 to 02:00	work	00:10	M,T,W,Th,F Sa	1	Min 0 and Max 2 hrs of EI will be calculated for Net-work hours
Overstay	02:00 to 08:00	work	00:30	M,T,W,Th,F Sa	1	Min 2 and Max 8 hrs of Overstay will be calculated for Net-work hours

Consider Overtime Configuration as:

Weekly Overtime is enabled for F, Sa, Sun

Consider Weekly/Monthly Overtime Configuration as:

Overtime Calculation is selected as Weekly

Week Start Date is selected as Monday

Auto Authorize Overtime component is enabled

Consider in Net work hours is enabled for Week-Offs

Work Component	Range	Consider as	Minimum duration reqd.	Multiplication factor
Net-work hours	00:00 to 100:00	OT3	01:00	1

Consider shift of the user is 09:00 to 18:00. Shift duration is 8 hrs with break from 13:00 to 14:00. Break deviation allowed.

To generate the overtime of the user, Daily and Monthly attendance process must be run.

Now after the daily and monthly attendance process, the user punches in the Daily attendance view are shown below:

User

rf

Rosy

Attendance Period

September

2016

View

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/09/2016	GS	08:00	19:00	PR	PR			10:00	02:00	09:00	01:00			
02/09/2016	GS	09:00	21:00	PR	PR			11:00	03:00	09:00	01:00	03:00		
03/09/2016	GS	09:00	20:00	PR	PR			10:30	02:00	08:30	00:30	02:00		
04/09/2016	GS - WO	07:30	21:00	WO	WO			12:30	04:30		01:00	20:30		
05/09/2016	GS	08:15	19:00	PR	PR			10:30	01:45	09:30	00:15			
06/09/2016	GS	07:30	22:00	PR	PR			13:30	05:30	11:30	01:00			
07/09/2016	GS	09:15	23:30	PR	PR			14:05	05:30	12:05	00:10			
08/09/2016	GS	06:00	23:00	PR	PR			16:00	08:00	13:00	01:00			
09/09/2016	GS	09:00	23:45	PR	PR			13:45	05:45	11:45	01:00	05:45		
10/09/2016	GS - WO			WO	WO									
11/09/2016	GS - WO			WO	WO							22:00		

For weekly OT, total Net work hours is to be calculated first.

The Network hours is calculated from the components Early IN, Work hours within shift and Overstay on Friday and Saturday.

The weekly OT will be allotted on F,Sa and Su as configured from Overtime configuration.

Now Week Offs check box is enabled in “Consider in Network hours” so shift work hours on the week-off will be considered in net-work hours.

Hence Total Network hours will be calculated from Friday, Saturday and Sunday.

Calculation of Network hours is same as done in previous Example1. See “Calculation of Network hours” on page 1464.

Total Network hours = Friday N/w hrs + Saturday N/w hrs + Sunday shift hours
= 9:00 + 8:30 + 8:00
= 25:30 hours

Calculation of Weekly OT

The total network hours of 25:30 hours will be distributed from Friday to Sunday as OT3 depending on the extra work done on the day. The left over OT will be given on the last day of the week.

On 2/9/16 Friday; Extra work hours = 03:00 so OT3 will be given as 03:00 hours.

On 3/9/16 Saturday; Extra work hours = 02:00 so OT3 will be given as 02:00 hours.

On 4/9/16 Sunday, Remaining hours = 25:30 - (OT allotted on friday and Saturday)
= 25:30- (05:00)
= 20:30 will be given as OT3; shown by arrow in above screenshot

Similarly for week 5/9/16 to 11/9/16, Total network hours = 11:45 + 8:00 + 8:00
= 27:45 hours

Overtime can be allotted on 9/9/16 as per the extra work hours as 5:45 hours. So OT3 on 9th is 5:45 hrs.

The Remaining OT will be given to the last day(11/9/16) of the week which is = 27:45- 05:45 hrs
= 22:00 hours; shown by arrow in above screenshot

Example3: Monthly OT Calculation

Consider Network hours configuration and Overtime configuration same as Weekly OT configuration

Consider Weekly/Monthly Overtime Configuration as:

Overtime Calculation is selected as Monthly

Auto Authorize Overtime component is enabled

Consider in Net work hours is enabled for Week-Offs

Work Component	Range	Consider as	Minimum duration reqd.	Multiplication factor
Net-work hours	00:00 to 100:00	OT4	01:00	1

Consider shift of the user is 09:00 to 18:00. Shift duration is 8 hrs with break from 13:00 to 14:00. Break deviation allowed.

To generate the overtime of the user, Daily and Monthly attendance process must be run.

Now after the daily and monthly attendance process, the user punches in the Daily attendance view are shown below:

User

rf

Rosy

Attendance Period

September

2016

View

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/09/2016	GS	08:00	19:00	PR	PR			10:00	02:00	09:00	01:00			
02/09/2016	GS	09:00	21:00	PR	PR			11:00	03:00	09:00	01:00	03:00		
03/09/2016	GS	09:00	20:00	PR	PR			10:30	02:00	08:30	00:30	02:00		
04/09/2016	GS - WO	07:30	21:00	WO	WO			12:30	04:30		01:00	04:30		
05/09/2016	GS	08:15	19:00	PR	PR			10:30	01:45	09:30	00:15			
06/09/2016	GS	07:30	22:00	PR	PR			13:30	05:30	11:30	01:00			
07/09/2016	GS	09:15	23:30	PR	PR			14:05	05:30	12:05	00:10			
08/09/2016	GS	06:00	23:00	PR	PR			16:00	08:00	13:00	01:00			
09/09/2016	GS	09:00	23:45	PR	PR			13:45	05:45	11:45	01:00	05:45		
10/09/2016	GS - WO			WO	WO									
11/09/2016	GS - WO			WO	WO									

Calculation of Network hours is same as done in Example1. See ["Calculation of Network hours" on page 1464](#).

Now Total Network hours for the month is calculated. As Monthly OT is applicable for F, Sa and Su so Network hours for all F, Sa and Su is added.

Date	Network hours	Remarks
2/9/16	9:00	
3/9/16	8:30	
4/9/16	8:00	As WO is enabled to consider for Network hours
9/9/16	11:45	
10/9/16	8	As WO is enabled to consider for Network hours
11/9/16	8	
16/9/16	-	AB
17/9/16	-	PH
18/9/16	8	As WO is enabled to consider for Network hours
23/9/16	8	
24/9/16	8	As WO is enabled to consider for Network hours
25/9/16	8	

Total Network hours= 84:75 hours

Calculation of Monthly OT

The total network hours of 84:75 hours will be distributed from Friday to Sunday as OT4; according to the extra work done on the day.

On 2/9/16 Friday; Extra work hours = 03:00 so OT4 will be given as 03:00 hours. Similarly OT4 will be given to other days (F, Sa, Su)

The left over OT will be given on the last day of the month. As monthly OT is allowed for Friday, Saturday and Sunday so left over OT will be given to last Sunday of the month.

Thus left over OT of 68:00 hours is given on 25/9/16 as shown below

22/09/2016	GS	08:00	19:00	PR	PR			10:00	02:00	09:00	01:00	
23/09/2016	GS	09:00	20:00	PR	PR			10:00	02:00	08:00	01:00	02:00
24/09/2016	GS - WO			WO	WO							
25/09/2016	GS - WO			WO	WO							68:00
26/09/2016	GS	09:00	18:30	PR	PR			08:30	00:30	08:00	01:00	
27/09/2016	GS	08:45	21:00	PR	PR			11:15	03:15	09:15	01:00	
28/09/2016	GS			AB	AB							
29/09/2016	GS			AB	AB							
30/09/2016	GS											

OT Calculation for user with Not Applicable Days configuration:

Example 1:

For Daily Overtime, Days to consider for Overtime= WO and PH.

For Weekly Overtime, Days to consider for Overtime= **Sun, Mon, Wed, Thu, Fri, Sat** and **PH**. Also, custom hours = 09:00 for Not Applicable Days falling in the week as well as any work done above **35:00** hours is considered as Overtime.

- "Consider Work Done on WO/PH/Paid Leaves" = **Unchecked**.
- Week-Start = **Monday (15/04/2019)**, Week-End = **Sunday (21/04/2019)**
- Joining Date = **Wednesday (17/04/2019)**
- Considering following daily view:

Date	Day Type	Work Hours	Consider for Weekly/ Monthly Overtime Calculation	Remark
15/04/2019 (Monday)	Normal	-	Yes	Not Applicable Day

Date	Day Type	Work Hours	Consider for Weekly/ Monthly Overtime Calculation	Remark
16/04/2019 (Tuesday)	Normal	-		Not Applicable Day This day will not be considered as it is not configured in "Overtime Calculation > Weekly/Monthly Overtime > Day to Consider for Calculation".
17/04/2019 (Wednesday)	Normal	9:30	Yes	Joining Date
18/04/2019 (Thursday)	Normal	9:30	Yes	
19/04/2019 (Friday)	Normal	9:15	Yes	
20/04/2019 (Saturday)	Week Off	05:00		
21/04/2019 (Sunday)	Week Off	00:00		

- In above mentioned scenario, OT should be generated as follows:
 - Daily OT on 20/04/2019 - **05:00**
 - Weekly OT – **02:15**
 - This should be achieved since Net-Work = **09:00** (15/04/2019) + 09:30 (17/04/2019) + 09:30 (18/04/2019) + 09:15 (19/11/2018) = **37:15**.

Example 2:

For Daily Overtime, Days to consider for Overtime= WO and PH.

For Weekly Overtime, Days to consider for Overtime= **Sun, Mon, Tue, Wed, Thu, Fri, Sat** and **PH**. Also, custom hours = 09:00 for **Not Applicable Days** falling in the week, as well as any work done above **45:00** hours is considered as Overtime.

- “Consider Work Done on WO/PH/Paid Leaves” = **Unchecked**.
- Week-Start = **Monday (15/04/2019)**, Week-End = **Sunday (21/04/2019)**
- Joining Date = **Wednesday (17/04/2019)**
- Considering following daily view:

Date	Day Type	Work Hours	Consider for Weekly/ Monthly Overtime Calculation	Remark
15/04/2019 (Monday)	Normal	-	Yes	Not Applicable
16/04/2019 (Tuesday)	Normal	-	Yes	Not Applicable

Date	Day Type	Work Hours	Consider for Weekly/ Monthly Overtime Calculation	Remark
17/04/2019 (Wednesday)	Normal	9:30	Yes	Joining Date
18/04/2019 (Thursday)	Normal	9:30	Yes	
19/04/2019 (Friday)	Normal	9:15	Yes	
20/04/2019 (Saturday)	Week Off	05:00		
21/04/2019 (Sunday)	Week Off	00:00		

- In above mentioned scenario, OT should be generated as follows:
 - Daily OT on 20/04/2019 - **05:00**
 - Weekly OT - **01:15**
 - This should be achieved since Net-Work = **09:00** (15/04/2019) + **09:00** (16/14/2019) + 09:30 (17/04/2019) + 09:30 (18/04/2019) + 09:15 (19/04/2018) = **46:15**

Example 3:

For Daily Overtime, Days to consider for Overtime= WO and PH.

For Monthly Overtime, Days to consider for Overtime= **Mon** and **Tue**. Also, custom hours = 09:00 for **Not Applicable Days** falling in the month, as well as any work done above **90:00** hours is considered as Overtime.

- “Consider Work Done on WO/PH/Paid Leaves” = **Unchecked**.
- Month-Start = **Monday (01/04/2019)**, Month-End = **Tuesday (30/04/2019)**
- Joining Date = **Monday (15/04/2019)**

- Considering following daily view:

Date	Day Type	Work Hours	Consider for Weekly/ Monthly Overtime Calculation	Remark
01/04/2019 (Monday)	Normal	-	Yes	Not Applicable Day
02/04/2019 (Tuesday)	Normal	-	Yes	Not Applicable Day
03/04/2019 (Wednesday).	Normal	-		Not Applicable Days These days will not be considered as it is not configured in "Overtime Calculation > Weekly/ Monthly Overtime > Day to Consider for Calculation"
04/04/2019 (Thursday)	Normal	-		
05/04/2019 (Friday)	Normal	-		
06/04/2019 (Saturday)	Week Off	-		
07/04/2019 (Sunday)	Week Off	-		
08/04/2019 (Monday)	Normal	-	Yes	Not Applicable Day
09/04/2019 (Tuesday)	Normal	-	Yes	Not Applicable Day
10/04/2019 (Wednesday)	Normal.	-		Not Applicable Days These days will not be considered as it is not configured in "Overtime Calculation > Weekly/ Monthly Overtime > Day to Consider for Calculation"
11/04/2019 (Thursday)	Normal	-		
12/04/2019 (Friday)	Normal	-		
13/04/2019 (Saturday)	Week Off	-		
14/04/2019 (Sunday)	Week Off	-		
15/04/2019 (Monday)	Normal	9:30	Yes	Joining Day
16/04/2019 (Tuesday)	Normal	9:30	Yes	

Date	Day Type	Work Hours	Consider for Weekly/ Monthly Overtime Calculation	Remark
17/04/2019 (Wednesday)	Normal	9:30		These days will not be considered as it is not configured in "Overtime Calculation > Weekly/ Monthly Overtime > Day to Consider for Calculation".
18/04/2019 (Thursday)	Normal	9:30		
19/04/2019 (Friday)	Normal	9:30		
20/04/2019 (Saturday)	Week OFF	05:00		
21/04/2019 (Sunday)	Week OFF	-		
22/04/2019 (Monday)	Normal	9:30	Yes	
23/04/2019 (Tuesday)	Normal	9:30	Yes	
24/04/2019 (Wednesday)	Normal	9:30		These days will not be considered as it is not configured in "Overtime Calculation > Weekly/ Monthly Overtime > Day to Consider for Calculation".
25/04/2019 (Thursday)	Normal	9:30		
26/04/2019 (Friday).	Normal	9:30		
27/04/2019 (Saturday)	Week OFF	-		
28/04/2019 (Sunday)	Week OFF	-		
29/04/2019 (Monday)	Normal	9:30	Yes	
30/04/2019 (Tuesday)	Normal	9:30	Yes	

- In above mentioned scenario, OT is generated as follows:
 - Daily OT on 20/04/2019 - **05:00**
 - Monthly OT - **03:00**
 - This is achieved since Net-Work = **09:00** (01/04/2019) + **09:00** (02/04/2019) + **09:00** (08/04/2019) + **09:00** (09/11/2018) + 09:30 (15/04/2019) + 09:30 (16/04/2019) + 09:30 (22/04/2019) + 09:30 (23/04/2018) + 09:30 (29/04/2019) + 09:30 (30/04/2018) = **93:00**.

Example 4:

For Daily Overtime, Days to consider for Overtime= WO and PH.

For Monthly Overtime, Days to consider for Overtime= **Mon, Tue, WO** and **PH**. Also, custom hours = 09:00 for **Not Applicable Days**, 09:30 for **WO** and **08:00** for **PH** falling in the month, as well as any work done above **150:00** hours is considered as Overtime.

- “Consider Work Done on WO/PH/Paid Leaves” = **Unchecked**.
- Month-Start = **Monday (01/04/2019)**, Month-End = **Tuesday (30/04/2019)**
- Joining Date = **Monday (15/04/2019)**

- Considering following daily view:

Date	Day Type	Work Hours	Consider for Weekly/ Monthly Overtime Calculation	Remark
01/04/2019 (Monday)	Normal	-	Yes	Not Applicable Day
02/04/2019 (Tuesday)	Normal	-	Yes	Not Applicable Day
03/04/2019 (Wednesday).	Normal	-		Not Applicable Days These days will not be considered as it is not configured in “Overtime Calculation > Weekly/ Monthly Overtime > Day to Consider for Calculation”
04/04/2019 (Thursday)	Normal	-		
05/04/2019 (Friday)	Normal	-		
06/04/2019 (Saturday)	Week Off	-	Yes	Not Applicable Day
07/04/2019 (Sunday)	Week Off	-	Yes	Not Applicable Day
08/04/2019 (Monday)	Normal	-	Yes	Not Applicable Day
09/04/2019 (Tuesday)	Normal	-	Yes	Not Applicable Day
10/04/2019 (Wednesday)	Normal.	-		Not Applicable Days These days will not be considered as it is not configured in “Overtime Calculation > Weekly/ Monthly Overtime > Day to Consider for Calculation”
11/04/2019 (Thursday)	Normal	-		
12/04/2019 (Friday)	PH	-	Yes	Not Applicable Day
13/04/2019 (Saturday)	Week Off	-	Yes	Not Applicable Day
14/04/2019 (Sunday)	Week Off	-	Yes	Not Applicable Day
15/04/2019 (Monday)	Normal	9:30	Yes	Joining Day
16/04/2019 (Tuesday)	Normal	9:30	Yes	

Date	Day Type	Work Hours	Consider for Weekly/ Monthly Overtime Calculation	Remark
17/04/2019 (Wednesday)	Normal	9:30		These days will not be considered as it is not configured in "Overtime Calculation > Weekly/ Monthly Overtime > Day to Consider for Calculation".
18/04/2019 (Thursday)	Normal	9:30		
19/04/2019 (Friday)	Normal	9:30		
20/04/2019 (Saturday)	Week OFF	05:00	Yes	
21/04/2019 (Sunday)	Week OFF	-	Yes	
22/04/2019 (Monday)	Normal	9:30	Yes	
23/04/2019 (Tuesday)	Normal	9:30	Yes	
24/04/2019 (Wednesday)	Normal	9:30		These days will not be considered as it is not configured in "Overtime Calculation > Weekly/ Monthly Overtime > Day to Consider for Calculation".
25/04/2019 (Thursday)	Normal	9:30		
26/04/2019 (Friday).	Normal	9:30		
27/04/2019 (Saturday)	Week OFF	-	Yes	
28/04/2019 (Sunday)	Week OFF	-	Yes	
29/04/2019 (Monday)	Normal	9:30	Yes	
30/04/2019 (Tuesday)	Normal	9:30	Yes	

- In above mentioned scenario, OT is generated as follows:
 - Daily OT on 20/04/2019 - **05:00**
 - Monthly OT - **27:00**
 - This is achieved since Net-Work = **09:00** (01/04/2019) + **09:00** (02/04/2019) + **09:30** (06/04/2019) + **09:30** (07/04/2018) + **09:00** (08/04/2019) + **09:00** (09/04/2018) + **08:00** (12/04/2019) + **09:30** (13/04/2018) + **09:30** (14/04/2019) + **09:30** (15/04/2019) + **09:30** (16/04/2019) + **09:30** (20/04/2018) + **09:30** (21/04/2019) + **09:30** (22/04/2019) + **09:30** (23/04/2018) + **09:30** (27/04/2018) + **09:30** (28/04/2019) + **09:30** (29/04/2019) + **09:30** (30/04/2018) = **177.00**

Example 5:

For Daily Overtime, Days to consider for Overtime= WO and PH.

For Weekly Overtime, Days to consider for Overtime= **Sun, Mon, Wed, Thu, Fri, Sat** and **PH**. Also, custom hours = 09:00 for **Not Applicable Days** falling in the week, as well as any work done above **40:00** hours is considered as Overtime.

- “Consider Work Done on WO/PH/Paid Leaves” = **Unchecked**.
 - Week-Start = **Monday (29/04/2019)**, Week-End = **Sunday (05/05/2019)**
 - Joining Date = **Wednesday (01/05/2019)**
- Considering following daily view:

Date	Day Type	Work Hours	Consider for Weekly/ Monthly Overtime Calculation	Remark
29/04/2019 (Monday)	Normal	-	Yes	Not Applicable Day
30/04/2019 (Tuesday)	Normal	-		Not Applicable Day This day will not be considered as it is not configured in “Overtime Calculation > Weekly/ Monthly Overtime > Day to Consider for Calculation”.
01/05/2019 (Wednesday)	Normal	10:30	Yes	Joining Date
02/05/2019 (Thursday)	Normal	11:00	Yes	
03/05/2019 (Friday)	Normal	10:30	Yes	
04/05/2019 (Saturday)	Week Off	06:30		
05/04/2019 (Sunday)	Week Off	00:00		

- In above mentioned scenario, OT should be generated as follows:
 - Daily OT on 04/05/2019 - **06:30**
 - Weekly OT - **01:00**
 - This is achieved since Net-Work = **09:00** (29/04/2019) + 10:30 (01/05/2019) + 11:00 (02/05/2019) + 10:30 (03/05/2018) = **41:00**.



For some cases when week or custom month period is overlapping in two months and leaving date falls in same week but in previous month, then monthly attendance process runs for current month & (current month +1) and updates attendance summary table.

Example 6:

For Daily Overtime, Days to consider for Overtime= WO and PH.

For Monthly Overtime, Days to consider for Overtime= **Mon, Tue, WO** and **PH**. Also, custom hours = 09:00 for **Not Applicable Days**, 09:30 for **WO** and 08:00 for **PH** falling in the month, as well as any work done above **150:00** hours is considered as Overtime.

- “Consider Work Done on WO/PH/Paid Leaves” = **Unchecked**.
- Month-Start = **Monday (01/04/2019)**, Week-End = **Tuesday (30/04/2019)**
- Joining Date = **Monday (15/04/2019)**
- Schedule start Date = **Wednesday (10/04/2019)**

- Considering following daily view:

Date	Day Type	Work Hours	Consider for Weekly/ Monthly Overtime Calculation	Remark
01/04/2019 (Monday)	Normal	-	Yes	Not Applicable Day
02/04/2019 (Tuesday)	Normal	-	Yes	Not Applicable Day
03/04/2019 (Wednesday).	Normal	-		Not Applicable Days These days will not be considered as it is not configured in “Overtime Calculation > Weekly/ Monthly Overtime > Day to Consider for Calculation”
04/04/2019 (Thursday)	Normal	-		
05/04/2019 (Friday)	Normal	-		
06/04/2019 (Saturday)	Week Off	-	Can't identify whether these days are week off or not as schedule start date is 10/04/2019. In such case these days will not be considered as Saturday and Sunday which are not configured in “Overtime Calculation > Weekly/Monthly Overtime > Day to Consider for Calculation”.	Not Applicable Day
07/04/2019 (Sunday)	Week Off	-		Not Applicable Day
08/04/2019 (Monday)	Normal	-	Yes	Not Applicable Day
09/04/2019 (Tuesday)	Normal	-	Yes	Not Applicable Day

Date	Day Type	Work Hours	Consider for Weekly/ Monthly Overtime Calculation	Remark
10/04/2019 (Wednesday)	Normal.	-		Schedule Start Day Not Applicable Days These days will not be considered as it is not configured in "Overtime Calculation > Weekly/ Monthly Overtime > Day to Consider for Calculation"
11/04/2019 (Thursday)	Normal	-		
12/04/2019 (Friday)	PH	-	Yes	Not Applicable Day
13/04/2019 (Saturday)	Week Off	-	Yes	Not Applicable Day
14/04/2019 (Sunday)	Week Off	-	Yes	Not Applicable Day
15/04/2019 (Monday)	Normal	9:30	Yes	Joining Day
16/04/2019 (Tuesday)	Normal	9:30	Yes	
17/04/2019 (Wednesday)	Normal	9:30		These days will not be considered as it is not configured in "Overtime Calculation > Weekly/ Monthly Overtime > Day to Consider for Calculation".
18/04/2019 (Thursday)	Normal	9:30		
19/04/2019 (Friday)	Normal	9:30		
20/04/2019 (Saturday)	Week OFF	05:00	Yes	
21/04/2019 (Sunday)	Week OFF	-	Yes	
22/04/2019 (Monday)	Normal	9:30	Yes	
23/04/2019 (Tuesday)	Normal	9:30	Yes	
24/04/2019 (Wednesday)	Normal	9:30		These days will not be considered as it is not configured in "Overtime Calculation > Weekly/ Monthly Overtime > Day to Consider for Calculation".
25/04/2019 (Thursday)	Normal	9:30		
26/04/2019 (Friday).	Normal	9:30		
27/04/2019 (Saturday)	Week OFF	-	Yes	

Date	Day Type	Work Hours	Consider for Weekly/ Monthly Overtime Calculation	Remark
28/04/2019 (Sunday)	Week OFF	-	Yes	
29/04/2019 (Monday)	Normal	9:30	Yes	
30/04/2019 (Tuesday)	Normal	9:30	Yes	

- In above mentioned scenario, OT is generated as follows:
 - Daily OT on 20/04/2019 - **05:00**
 - Monthly OT - **08:00**
 - This is achieved since Net-Work = **09:00** (01/04/2019) + **09:00** (02/04/2019) + **09:00** (08/04/2019) + **09:00** (09/04/2018) + **08:00** (12/04/2019) + **09:30** (13/04/2018) + **09:30** (14/04/2019) + 09:30 (15/04/2019) + 09:30 (16/04/2019) + **09:30** (20/04/2018) + 09:30 (21/04/2019) + 09:30 (22/04/2019) + 09:30 (23/04/2018) + **09:30** (27/04/2018) + **09:30** (28/04/2019) + 09:30 (29/04/2019) + 09:30(30/04/2018) = **158.00**

Overtime Limit for Alert Message

This feature enables you to send the Overtime Exceed Alert to the respective users and group in-charges based on — Daily, Weekly and Monthly Overtime.



If for Authorized Overtime, the Weekly/Monthly overtime option is enabled for WO, PH, WO/PH as well as Daily overtime is enabled for the same day, then in this case the Alert would be sent twice to the respective user.

You can also configure Push Notification for this feature.

Select *Time and Attendance* as the *Alert Filter* and in *Event* select *Overtime Limit Exceeded - Group-Incharge / Overtime Limit Exceeded - User*. Refer “[Configuring Alert Messages](#)” for details.

Overtime Limit for Alert Message

Overtime Alert Calculation
Generated Overtime

Daily Overtime Limit
HH:MM

Weekly Overtime Limit
HHH : MM

Week Start Day
Monday

Monthly Overtime Limit
HHH : MM

Configure the following parameters:

- Overtime Alert Calculation:** Select the desired method of overtime calculation for alert based on — **Generated Overtime** and **Authorized Overtime**.

Generated Overtime is the time generated by the system once the user exceeds the overtime limit.
Authorized Overtime is the overtime approved by the Admin.

- **Daily Overtime Limit:** Enter daily overtime limit time after which the Overtime Exceed Alert will be triggered.

- **Weekly Overtime Limit:** Enter time in 24 hours format to set it as Overtime exceed limit for Weekly Overtime Alert.

Make sure you have enabled **Weekly** in *Weekly/Monthly Overtime> Overtime Calculation*.

- **Week Start Day:** Select a day from the dropdown list to set it as a week start for Weekly Overtime Limit.

Make sure you have selected Weekly in *Weekly/Monthly Overtime> Overtime Calculation*.

If **Weekly** is configured under **Weekly/Monthly Overtime**, then display the selected **Week Start Day**.

- **Monthly Overtime Limit:** Enter time in 24 hours format to set it as Overtime exceed limit for Monthly Overtime Alert.

Make sure you have selected Monthly in *Weekly/Monthly Overtime> Overtime Calculation*.



The triggering of the **Overtime Limit Exceeded** Alert (Weekly/Monthly) will be dependent on the parameters set in the:

- Overtime Policy: **Weekly/Monthly Overtime Limit** set.
- Overtime Policy: **Auto Authorization of Overtime** check box enabled.
- Network Hours Policy: **Total Number of Overtime Hours** configured.

Examples

Below given examples demonstrate the Overtime limit exceed calculations and alert triggering:

1. Only Daily configurations:

- Daily is configured with days Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and Sunday.
- Weekly/Monthly is not configured.
- Daily Overtime Limit is 1 hour.
- Weekly Overtime Limit is 10 hours.
- Week Start Day is Monday.

Refer below given table for Overtime hours:

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
2 Hours	2 Hours	2 Hours	2 Hours	45 Minutes	2 Hours	1 Hour 30 Minutes

- In this case Daily overtime alert will be triggered for Monday, Tuesday, Wednesday and Thursday.
- In this case Daily + Weekly alert will be triggered for Saturday and Sunday (Here Weekly is calculated based on summation of Daily Overtime hours and 10 hours threshold is violated on Saturday and Sunday, hence the alerts are triggered on both the days).

2. Only Weekly/Monthly configurations:

- Daily is not configured.
- Weekly/Monthly is configured with WO and PH. Saturday and Sunday are marked as week-off days. Where Monday is first day of the week.
- Weekly Overtime Limit is 2 hours.

Refer below given table for Overtime hours

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
2 Hours	2 Hours	2 Hours	2 Hours	45 Minutes	3 Hours	1 Hour

- In this case Weekly/Monthly alert will be triggered for Saturday and Sunday (Because the limit is exceeded on Saturday it self and again it was violated on Sunday).

3. Both Daily and Weekly/Monthly configurations:

- Daily is configured with days Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, WO, PH and WO/PH.
- Weekly/Monthly is configured with WO, PH and WO/PH. Saturday and Sunday are marked as week-off days. Where Monday is first day of the week.
- Daily Overtime Limit is 1 hours.
- Weekly Overtime Limit is 4 hours.

Refer below given table for Overtime hours:

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
2 Hours	2 Hours	2 Hours	2 Hours	45 Minutes	3 Hours	2 Hours

- In case Daily overtime alert will be triggered for Monday, Tuesday, Wednesday and Thursday.
- Here Saturday and Sunday are considered under WO.
- Hence, Daily + Weekly overtime alert will be triggered for Saturday and Sunday (As per Daily configuration it's violated and also, for Weekly it's violated so a single common alert would be sent)



For calculation of a day falling under Daily and Weekly would be summation of both the Daily Overtime hours + Weekly / Monthly Overtime hours, as per existing logic. Hence user is advised to configure accordingly (In this case it would be Weekly overtime = 7 hours. As WO for Daily + total WO for Weekly).

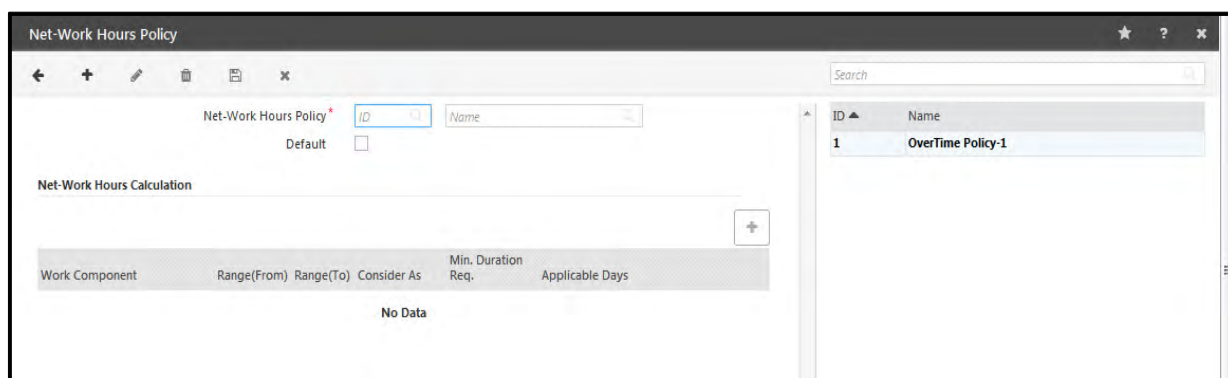
As per existing if Saturday and Sunday are assigned week-off of Shift and under Overtime Policy if WO is checked, WO would be given priority over the days for considering Overtime component.

Net-Work Hours Policy

Certain organizations allow employees to work for extra hours apart from their work hours and pay compensation for the extra work done. This concept of “Overtime” can be designed as per the requirements and work culture practiced in the organization.

Net-Work hours Policy enables to calculate the Net-work hours which is the payable hours of the employee; based on which overtime can be calculated for the user.

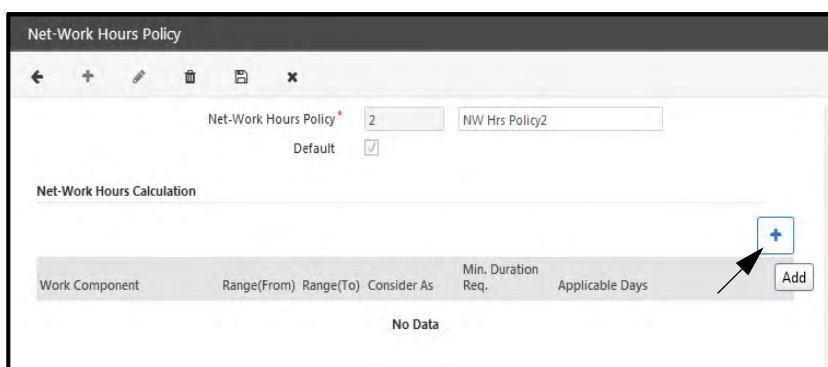
To configure a Net-work hours policy, Go to **T&A> Policies> Net-Work hours Policy**



Click on **New** button from the toolbar.

Enter a **Name** for the Net-work hours policy to be created. For eg: NW Hrs Policy2
The **ID** will be auto-generated on saving the policy.

You can enable the **Default** box to make the Net-work hours policy default. When the new user is created, the default policy will be assigned directly.



Net-Work Hours Components

Net-Work hours can comprise of various work components for which Employer wants to pay the employee.

To add and configure Net-Work hours components to the Net-Work hours policy; click on **Add** button as shown above.

The Work Component options are shown below.

Now select a **Work component**. Eg: Early-IN

Range

The “From” and “To” Range is the minimum and maximum hours for which the work component will be considered for calculation of Net-Work hours.

Example: For Early-IN component; Enter the Range as 00:30 hrs to 02:00 hrs.

This means the employee can avail Early-IN **minimum 30 minutes** before shift start and **maximum 2 hrs** before shift start.

Example:

Early IN Range=00:30 to 02:00 hours; Shift= 09:00 to 18:30 hours

Min Duration required within range=00:00 minutes

If shift start is at 09:00 hrs, then the timing before 08:30 hrs and after 07:00 hrs will be considered for Net-Work hours

- Case1: IN Punch at 06:30 hours -> Only 2 hrs will be considered for Net-Work hrs as Early IN range is defined for max 2 hrs.
- Case2: IN Punch at 08:00 hours-> Only 30min will be considered for Net-Work hrs. (from 08:00 to 08:30 hrs)
- Case3: IN Punch at 08:45 hours-> 15 minutes will not be considered for Net-Work hrs as minimum Early IN must be 30 mins.

Consider As

You can assign the work component to be counted as "Work" or "No work". If the component is considered for Work, then it will be considered in net-work hours and if No work then it will not be considered in net-work hours calculation.

Min. Duration Required

This is the minimum duration within Work Component range which is must to be fulfilled by the employee, only then the work component will be considered in Net-Work hours calculation.

Example:

Early IN Range=00:00 to 02:00 hours; Shift= 09:00 to 18:30 hours

Min Duration required within range=00:10 minutes

- Case1: IN Punch at 08:45 hours-> Early IN of 15 minutes> Minimum required 10 minutes so Early IN is valid to consider in Net work hours.
- Case2 : IN Punch at 08:52 hours-> Early in of 8 minutes< Minimum required 10 minutes so Early IN is not counted in Network hours.

Net-Work Hours Calculation

Work Component	Range(From)	Range(To)	Consider As	Min. Duration Req.	Applicable Days	Factor	
Early-IN	00:30	02:00	Work	00:10	Select	1.0	✓ ✕

Applicable Days

Click the drop down and select the days for which the work component will be applicable. Then click **OK** to save the configuration and **Save** button to save the Net-Work hours policy.

Net-Work Hours Calculation

Work Component	Range(From)	Range(To)	Consider As	Min. Duration Req.	Applicable Days	Factor
Early-IN	00:30	02:00	Work	00:10	Select	1.0

Applicable Days dropdown menu:

- ✓ Check All
- ✓ Mo
- ✓ Tu
- ✓ We
- ✓ Th
- ✓ Fr
- ✓ Sa
- ✓ Su
- W/O/PH

Net-Work Hours Policy

Net-Work Hours Policy: 2

Default: ☐

Net-Work Hours Calculation

Work Component	Range(From)	Range(To)	Consider As	Min. Duration Req.	Applicable Days	Factor
Work Hours Within Shift	00:30	02:00	Work	00:10	Su Mo Tu We Th Fr Sa PH FB RD	1.0

Right-hand list:

ID	Name
1	OverTime Policy-1
2	NetWork Hour Policy

The Configuration of **Overstay** and **Work hours Within Shift** is shown as below.

Net-Work Hours Policy

Net-Work Hours Policy: 2

Default: ☐

Net-Work Hours Calculation

Work Component	Range(From)	Range(To)	Consider As	Min. Duration Req.	Applicable Days	Factor
Work Hours Within Shift	00:30	02:00	Work	00:10	Mo Tu We Th Fr Sa	1.0
Early-IN	00:30	02:00	Work	00:10	Mo Tu We Th Fr Sa	1.0
Overstay	00:30	02:00	Work	00:10	Su Mo Tu We Th Fr Sa	1.0

Calculation of Net-Work hours with different components

Consider shift of employee be 09:00 to 18:00 hours. Total duration is 09:00 hours. Break duration is 01:00 hour with deviation allowed. Shift duration is 08:00 hours.

1. Work Hours within Shift

Range= 00:00 to 08:00

IN Punch	OUT Punch	Working Hours	Work hours within Shift	Net-Work hours
09:00	18:30	09:00 (from 09:00 to 18:00)	08:00 Working hrs - Lunch hrs = 9-1=8	08:00

2. Early-IN

Range= 00:00 to 02:00

Min. duration reqd = 00:10

IN Punch	OUT Punch	Working Hours	Early-IN	Net-Work hours
08:30	18:00	09:00	00:30 Shift start time- IN Punch =9:00- 8:30 = 00:30	00:30

3. Overstay

Range= 00:00 to 04:00

Min. duration reqd = 02:00

IN Punch	OUT Punch	Working Hours	Overstay	Net-Work hours
09:00	21:00	12:00	03:00 OUT Punch- Shift End time =21:00- 18:00 = 03:00	03:00

4. Break Hours

Range= 00:00 to 01:00

Min. duration reqd = 00:10

IN Punch	Break OUT	Break IN	OUT Punch	Working Hours	Break	Net-Work hours
09:00	13:00	13:40	18:00	09:00	00:40 Break IN- Break OUT =13:40-13:00= 00:40	00:40

See "Shift Configuration> Break details" for Break duration configuration.

5. Late-IN

Range= 00:00 to 00:45
Min. duration reqd = 00:10

IN Punch	OUT Punch	Working Hours	Late-IN	Net-Work hours
09:20	18:30	08:40	00:20 IN Punch- Shift start =09:20-09:00= 00:20	00:20

See "Late IN Policy" for Late-IN configuration.

6. Early-OUT

Range= 00:00 to 00:45
Min. duration reqd = 00:10

IN Punch	OUT Punch	Working Hours	Early-OUT	Net-Work hours
09:00	17:30	08:00	00:30 Shift End- OUT Punch =18:00-17:30= 00:30	00:30

See "Early OUT Policy" for Early-OUT configuration.

7. IN Grace

Range= 00:00 to 00:45
Min. duration reqd = 00:05

IN Punch	OUT Punch	Working Hours	IN Grace	Net-Work hours
09:07	18:00	08:23	00:07 IN Punch- Shift start =09:07-09:00= 00:07	00:07

Consider Grace time for Shift Late-IN= 10min
See "Shift Configuration> Grace time details" for Grace duration configuration.

8. OUT Grace

Range= 00:00 to 00:45
Min. duration reqd = 00:05

IN Punch	OUT Punch	Working Hours	OUT Grace	Net-Work hours
09:00	17:55	08:25	00:05 Shift End- OUT Punch =18:00-17:55= 00:05	00:05

Consider Grace time for Shift Early-OUT= 15min
See "Shift Configuration> Grace time details" for Grace duration configuration.

9. Short Leave Duration

Range= 00:00 to 01:00

Min. duration reqd = 00:30

IN Punch	OUT Punch	Working Hours	Short Leave Duration	Net-Work hours
09:00	17:00	07:30	01:00 Shift End- OUT Punch =18:00-17:00= 01:00	01:00

See "Attendance Policy" for Short leave hours configuration.

Considering the components "Working hours within shift" and "Short Leave duration" together in Net work hours calculation:

Net work hours= Working hours within shift (7:30 hours) + Official IN/OUT duration (01:00hours)
= 08:30 hours

10. Official IN/OUT Duration

Range= 00:00 to 08:00

Min. duration reqd = 02:00

Official IN/ OUT	IN Punch	OUT Punch	Working Hours	Official hours	Net-Work hours
Official OUT	09:00	15:00	05:30	03:00 Shift End- OUT Punch =18:00-15:00= 03:00	03:00
Official IN	12:30	18:00	05:00	03:30 IN Punch- Shift Start =12:30- 09:00= 03:30	03:30

See "Attendance Policy" for Official hours configuration.

Considering the components "Working hours within shift" and "Official OUT" together in Net work hours calculation:

Net work hours= Working hours within shift (5:30 hours) + Official IN/OUT duration (03:00hours)
= 08:30 hours

11. Adjusted Work Hours

Range= 00:00 to 10:00

Min. duration reqd = 00:10

IN Punch	OUT Punch	Working Hours	Adjusted Work Hours	Net-Work hours
09:00	16:00	06:30	01:30 Shift Duration- OUT Punch =08:00-06:30= 01:30	01:30

Considering the components "Working hours within shift" and "Adjusted Work hours" together in Net work hours calculation:

Net work hours= Working hours within shift + Adjusted Work Hours
=06:30 +01:30 =8:00 hours



To enable the Adjusted Work Hours feature, go to Attendance Policy> Auto Attendance Correction. check the Overtime Enable box. And select the number of months to consider as previous months for overtime hours.

Adjustment of Work hours from previous OT

Adjusting the work hours implies that available overtime from the previous selected months can be used to adjust the shortfall hours of the user to mark him present.

Suppose on 20/11/16 the employee punches out at 16:00 hours which is before the shift end time. The working hours is 06:30 hours which is less than the required 08:00 hours. So the employee is marked as Absent due to less working hours.

As the Overtime is available from previous days of the month so that OT is adjusted on 20th to make complete 8 hours and hence user is marked Present.

Hence 01:30 hours is given as adjusted work hours from the available OT hours and the employee is marked as Present.

Late-IN Policy

Late-IN in COSEC is an attendance feature that allows special configurations for users who report later than the expected reporting time. Late-IN policies assign different rules to late-coming users based on their roles and functions. This option allows a user to define the parameters for Late-In policies which can then be assigned to individual users or group of users.

To define Late-IN Policies, Select the **Time & Attendance Module > Policies > Late-IN Policy**.

The following **Late-IN Policy** settings page appears on your screen.

ID	Name	Level
1	Late In Policy-1	1

Click on **New** button to define a new Late-IN Policy.

Late-IN- Specify a user-friendly name for the Late-IN Policy. The ID will be generated by the system automatically when the policy is saved.

Default: Select this checkbox if you want to set the current policy as the default one. Users will be linked with this Late-In Policy by default in the event of a user not being linked to any Late-In Policy. Therefore, it is mandatory to define one default Late-In Policy.

Policy Period: Click on the calendar button and select the **From** and **To** dates. This would specify the period of validity for the Late-IN policy. This can be edited only after the policy is saved.

Late-IN Applicable: Check this box to activate the policy.

Max Late-IN Allowed (Min): Specify the maximum allowed time duration (in minutes) for which Late-IN is allowed.

Enable Rounding for fraction of an Hour: Check this box to enable the rounding off rule for the Late In time. Click **Add** button. Then specify the time range and select the actual or fixed value of late-in to be considered. For eg: From 1 to 10 minutes of Late In; Actual value will be considered. From 11 to 15mins, fixed 15 mins will be considered as Late In. From 16 to 30 mins, fixed 30 mins will be considered as Late In.

Then click **OK** to save the rounding configuration.

Enable Rounding For Fraction Of An Hour ☒

Search

Range (From) ▲	Range (To)	Consider Value As	Replace Value	
16	30	Fixed	30	✓ ✕
1	10	Actual		✎ ✕
11	15	Fixed	15	✎ ✕

Once the above parameters have been defined click **Save**  to save the changes on the system.



In case a particular policy is edited, the application creates a new level of the policy with the same ID and name as can be seen in the grid below. In the event of a conflict in dates or some rule then the parameters as defined in the policy with the highest level will be considered as the valid policy for that user.

Example1:

Late IN with Grace time

Shift is from 9:00 to 18:00 hours

If Late-in allowed is kept as 10 minutes, Grace time is included in working hours and Grace time for shift late-in as 30 minutes, then IN punch till 9:30 will be considered in grace period as shown on 1/7/16.

IN punch after completion of grace time(30 min) will be considered in late-in duration. The IN punch of 9:42 is Late-IN by 12 minutes.

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime
01/07/2016	GS	09:15	18:00	PR	PR			07:45			01:00	
02/07/2016	GS - WO	09:00	18:00	WO	WO			05:00			01:00	
03/07/2016	GS - WO			WO	WO							
04/07/2016	GS	09:42	18:30	PR	PR	00:12		07:48	00:30		01:00	
05/07/2016	GS											

If Grace time is not included in working hours and Grace time for shift late-in is 0, then punch after 9:00hrs will be marked as Late-IN as shown below: See Grace time configuration in Shift Configuration.

06/07/2016	GS	09:05	18:30	PR	PR	00:05		08:25	00:30		01:00	
07/07/2016	GS	09:25	18:30	PR	PR	00:25		08:05	00:30		01:00	

Applying Short leave on Late-IN occurrences

- 09:00 to 18:00 hours; Min required for half day- 2hrs, full day- 4 hrs

- Include Grace time in working hrs enabled
- Grace time for shift late-IN - 30min

- Maximum Late-IN allowed- 30 min

- Maximum minutes allowed- 180
- Maximum count allowed- 3

- minimum- 5 min,
- maximum-60 min

- Mark Absent as per- Monthly count
- Mode- Independent

- Maximum allowed per month- 3
- Absent marking type-
- Mark absent as- full day

Daily Attendance View

←

User

1220

Sheetal

Attendance Period

October

2016

View

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/10/2016	MS	09:25	20:00	PR	PR			10:35	02:00	10:35		05:00		
02/10/2016	MS - WO			WO	WO									
03/10/2016	MS	09:25	22:30	PR	PR			13:05	04:30	13:05		07:30		
04/10/2016	MS	09:20	21:00	PR	PR			11:40	03:00	11:40		06:00		
05/10/2016	MS	09:45	22:00	PR	PR	00:15		12:15	04:00	12:15		07:00		
06/10/2016	MS	09:50	19:00	PR	PR	00:20		09:10	01:00	09:10		04:00		
07/10/2016	MS	09:55	19:00	PR	PR	00:25		09:05	01:00	09:05		04:00		
08/10/2016	MS	09:56	19:00	AB	AB	00:26		09:04	01:00	09:04		04:00		Full Day AB:Late-IN Limit
09/10/2016	MS - WO			WO	WO									
10/10/2016	MS	09:46	19:30	AB	AB	00:16		09:44	01:30	09:44		04:30		Full Day AB:Late-IN Limit
11/10/2016	MS	09:59	19:45	AB	AB	00:29		09:46	01:45	09:46		04:45		Full Day AB:Late-IN Limit
12/10/2016	MS	09:37	20:00	AB	AB	00:07		10:23	02:00	10:23		05:00		Full Day AB:Late-IN Limit

The user is allowed to take grace period of 30 minutes i.e. he can come upto 9:30 without being marked as Late-in. When the user comes after 9:30, he will be marked present with Late-IN.

The user can take late-ins for 3 times in a month as configured. When he comes late for 4th time, his punch will be marked present. But after processing monthly attendance, he will be marked absent as full day or half day as per the absent marking rule.

So, on 4th late-IN on 8-10-16, the user will be marked as absent as shown above.

If you are allowed to avail short leave hours, then you can apply the short leave on 8-10-16 which will convert your absent to present.

To apply short leave, go to T&A>Utilities> Attendance correction as shown below.

Date	Shift	1st Half	2nd Half	Work Hours
20/10/2016	MS	AB	AB	
19/10/2016	MS	AB	AB	
18/10/2016	MS	AB	AB	
17/10/2016	MS	AB	AB	
16/10/2016	MS - WO	WO	WO	
15/10/2016	MS	AB	AB	
14/10/2016	MS	AB	AB	
13/10/2016	MS	AB	AB	
12/10/2016	MS	AB	AB	10:23
11/10/2016	MS	AB	AB	09:46
10/10/2016	MS	AB	AB	09:44
09/10/2016	MS - WO	WO	WO	
08/10/2016	MS	AB	AB	09:04
07/10/2016	MS	PR	PR	09:05
06/10/2016	MS	PR	PR	09:10
05/10/2016	MS	PR	PR	12:15

The short leave is allowed for only 3 days. After applying short leave, the absent days will be marked as present shown by rectangle in below screenshot.

If you apply short leave for 4th day, you will be able to apply it. But after the monthly attendance process, it will be marked as absent as shown below.

Daily Attendance View														
<div> <div>User1220Sheetal</div> <div> <div>Attendance Period</div> <div>October2016</div> <div>View</div> </div> </div>														
Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/10/2016	MS	09:25	20:00	PR	PR			10:35	02:00	10:35		05:00		
02/10/2016	MS - WO			WO	WO									
03/10/2016	MS	09:25	22:30	PR	PR			13:05	04:30	13:05		07:30		
04/10/2016	MS	09:20	21:00	PR	PR			11:40	03:00	11:40		06:00		
05/10/2016	MS	09:45	22:00	PR	PR	00:15		12:15	04:00	12:15		07:00		
06/10/2016	MS	09:50	19:00	PR	PR	00:20		09:10	01:00	09:10		04:00		
07/10/2016	MS	09:55	19:00	PR	PR	00:25		09:05	01:00	09:05		04:00		
08/10/2016	MS	09:56	19:00	PR	PR			09:04	01:00	09:04		04:00		SHORT LEAVE
09/10/2016	MS - WO			WO	WO									
10/10/2016	MS	09:46	19:30	PR	PR			09:44	01:30	09:44		04:30		SHORT LEAVE
11/10/2016	MS	09:59	19:45	PR	PR			09:46	01:45	09:46		04:45		SHORT LEAVE
12/10/2016	MS	09:37	20:00	AB	PR			09:46	02:00	10:23		05:00		SHORT LEAVE

Early-OUT Policy

Early-OUT in COSEC is an attendance feature that allows special configurations for users who exit the workplace earlier than the expected time. The application provides the functionality to assign different Early-OUT rules to users based on their roles and functions. This option allows user to define the parameters for the Early-OUT policies which can then be assigned to individual users or group of users.

An Early-OUT policy involves grouping of set of rules with varying parameters related to the early punching out of employees.

To configure an Early-OUT Policy, Select the **Time and Attendance Module > Policies > Early-OUT Policy**.

The **Early-OUT Policy** page appears on your screen as shown below.


ID	Name	Level
1	Early Out Policy-1	1

1. Click **New** to define a new Early-Out Policy.
2. Configure the following options as required:
 - **ID:** Each Early-OUT Policy will have a unique ID for identification and this is generated by the system automatically when the policy is saved.
 - **Name:** Specify a user-friendly name for the Early-Out Policy.
 - Check the **Default** box if you want to set the current policy as the default one. Users will be linked with this Early-Out Policy by default in the event of a user not being linked to any Early-Out Policy. Therefore, it is mandatory to define one default Early-Out Policy.
 - **Policy Period:** Click on the Calendar picker button to select the **From** and **To** dates. This would specify the period of validity for the Early-Out policy. This can be edited only after the policy is saved.
 - **Early Out Applicable:** Check this box to activate the policy.
 - **Max Early Out Allowed:** Specify the maximum time in minutes for which the early out is allowed.
 - **Enable Rounding for fraction of an Hour:** Check this box to enable the rounding off rule for the Early-Out time.
Click **Add** button. Then specify the time range and select the actual or fixed value of early out to be considered.

For eg: From 1 to 10 minutes of Early Out; Actual value will be considered. From 11 to 15mins, fixed 15 mins will be considered as Early Out. From 16 to 30 mins, fixed 30 mins will be considered as Early Out.

Then click **OK** to save the rounding configuration.

Range (From)	Range (To)	Consider Value As	Replace Value
1	10	Actual	
11	15	Fixed	15
16	30	Fixed	30

- Once the above parameters have been defined click **Save**  to save the changes on the system.

Example1:

Early Out with Grace time

Shift is from 9:00 to 18:00 hours

If Early Out allowed is kept as 10 minutes, Grace time is included in working hours and Grace time for shift Early Out as 30 minutes, then Out punch before 30 mins of shift end i.e. till 17:30 will be considered in grace period as shown on 1/2/17 and 2/2/17.

Shift Configuration

Shift * 12 Early Out Shift

Shift Type Normal

Shift Timings * 09:00 18:00 08:00

Minimum Required Hours

For Half Day * 02:00

For Full Day * 04:00

Min. Hours Required Within Shift Duration ☐

Shift Allowance ☐

Break Details

Grace Time Details

Include Grace Time In Working Hours ☒

Grace Time For Shift Late-IN 0

Overlap Grace Time With Shift Late-IN ☐

Grace Time For Shift Early-OUT 30

Overlap Grace Time With Shift Early-OUT ☐

Out punch after availing grace time(30 min) will be considered in Early Out duration.

The Out punch of 17:20 is Early-Out by 10 minutes which is within the max allowed limit of 10 mins. So the Out punch is marked PR on 3/2/17

The Out punch of 17:15 is Early-Out by 15 minutes which is beyond the max allowed limit of 10 mins. So the Out punch is marked AB on 4/2/17 with Remark of AB: Early -Out.

Daily Attendance View

User * 3 Isha

Attendance Period February 2017

Search

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/02/2017	12	09:00	17:30	PR	PR			08:30						
02/02/2017	12	09:15	17:45	PR	PR	00:15		08:30						
03/02/2017	12	09:05	17:20	PR	PR	00:05	00:10	08:15						
04/02/2017	12	09:00	17:15	PR	AB			08:15						AB:Early-OUT
05/02/2017	12 - WO			WO	WO									
06/02/2017	12	09:15	17:16	PR	AB	00:15		08:01						AB:Early-OUT

Example2:

Applying Short leave on Early-Out occurrences

The user punches are shown below:

Daily Attendance View

User*

3

Isha

Attendance Period

February

2017

Search

Date ▲	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/02/2017	12	09:00	17:30	PR	PR			08:30						
02/02/2017	12	09:15	17:45	PR	PR	00:15		08:30						
03/02/2017	12	09:05	17:20	PR	PR	00:05	00:10	08:15						
04/02/2017	12	09:00	17:15	PR	AB			08:15						AB:Early-OUT
05/02/2017	12 - WO			WO	WO									
06/02/2017	12	09:15	17:16	PR	AB	00:15		08:01						AB:Early-OUT

User *

3

Isha

Attendance Period

February

2017

Search

Date ▲	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark
01/02/2017	12	09:00	17:30	PR	PR			08:30						
02/02/2017	12	09:15	17:45	PR	PR	00:15		08:30						
03/02/2017	12	09:05	17:20	PR	PR	00:05	00:10	08:15						
04/02/2017	12	09:00	17:15	PR	AB			08:15						AB:Early-OUT
05/02/2017	12 - WO			WO	WO									
06/02/2017	12	09:15	17:16	PR	PR	00:15		09:00						SHORT LEAVE

C-OFF Policy

A Compensatory-Off (C-OFF) can be defined as paid time-off awarded to an eligible employee in return for working additional hours during an attendance period. Accrued compensatory leave may be used to provide time-off from work at a later date of the employee's choice, but within a valid time period.

To define a C-OFF Policy, Select the **Time and Attendance module > Policies > C-OFF Policy**.

The **C-OFF Policy** page opens as shown below.

ID	Name	Level
1	COFF Policy-1	1

Click on **New** button to define a new C-OFF Policy.

C-OFF Policy - Specify a user-friendly name for the C-OFF Policy. The ID will be generated by the system automatically when the policy is saved.

Default - Select this checkbox to mark the C-OFF Policy as default.

Policy Period - Click on the calendar button and select the **From** and **To** dates. This would specify the period of validity for the C-OFF policy. This can be edited only after the policy is saved.

Minimum Overtime Required for C-OFF - Specify the minimum number of overtime hours in HH:MM format which would be required for granting C-OFF to the user.

C-OFF Authorized in Multiples Of - Specify the multiples of timing as per which C-OFF will be authorized to the employee. Eg: If 01:00 is set here, then C-OFF can be authorized in multiples of 1h. This means you cannot give 2h 30 mins as C-OFF but 2h or 3 h is allowed.

C-OFF Validity Type - The C-OFF Validity Type can be either **Monthly**, **Yearly** or in terms of **Days**.

On selecting the **Monthly** (or **Days**) option, specify the maximum number of months (or days) in the **C-OFF Validity** field, before which the C-OFF has to be availed. For the **Yearly** option, select the day and month of the year when the available C-OFFs will lapse.

- **Minimum C-OFF For Half Day Off** - Specify the hours in HH:MM format which would be the minimum hours required for half day marking.

- **Minimum C-OFF For Full Day Off** - Specify the hours in HH:MM format which would be the minimum hours required for full day marking.
- **Auto Authorize C-OFF** - Select this checkbox for automatic authorization of C-OFF.

Click **Save** button to add the new policy.

Configuration to give OT and C-OFF to user

Example1: If Only Overtime is to be given to user

Select **OT/C-OFF Eligibility** for the user as **Only Overtime** from the drop down options as shown below.

The Overtime Policy configuration for user is:

Overtime Configuration: Daily Overtime is enabled for Monday to Saturday.

Daily Overtime: Daily1

Work Component	Range	Consider as	Minimum duration reqd.	Applicable days	Multiplication factor
Early-IN	00:00 to 04:00	OT1	00:00	M,T,W,Th,F,Sa	1
Overstay	00:00 to 04:00	OT2	00:00	M,T,W,Th,F,Sa	1

Auto Authorize Overtime Component must be disabled.

The **Daily Attendance View** shows the user punches and generated overtime as shown below.

Example2: If Only C-OFF is to be given to user

Select **OT/C-OFF Eligibility** for the user as **Only C-OFF** from the drop down options as shown below.

The screenshot shows the 'User Configuration' window for user 'NP Nisha'. The 'Policy' tab is selected, and the 'Attendance' section is active. The 'OT/C-OFF Eligibility' dropdown menu is open, showing options: 'None', 'Only Overtime', 'Only C-OFF' (selected), and 'Both'. Other settings include 'Enable Attendance Calculation' (checked), 'Attendance Marking Type' (Normal), 'Max Punches To Be Considered' (Select), 'Bypass Finger/Palm For Attendance' (unchecked), 'Max Short Leaves Allowed' (empty), 'Authorize C-OFF On' (WO/PH), 'Bus Route' (Normal Day), 'Enable Auto Tour Application' (unchecked), 'Tour' (empty), 'Base Site Selection' (ID/Name), and 'Auto Authorize Tour Application' (unchecked).

The C-OFF Policy configuration for user is:

Minimum Overtime required for C-OFF: 01:00 hr

C-OFF authorized in multiples of: 01:00 hr

Minimum C-OFF for half day off: 04:00 hr

Minimum C-OFF for full day off: 08:00 hr

The **Daily Attendance View** shows the user punches and actual overtime as shown below.

The screenshot shows the 'Daily Attendance View' for user 'NP Nisha' in May 2017. The table displays attendance data for the first five days of the month. The 'Actual Overtime' column is highlighted with an arrow.

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark	Details
01/05/2017	GS	08:45	21:00	PR	PR			11:15	02:45	02:45	01:00	02:45			
02/05/2017	GS	08:00	22:00	PR	PR			13:00	04:30	04:30	01:00	04:30			
03/05/2017	GS	07:56	21:00	PR	PR			12:04	03:34	03:34	01:00	03:34			
04/05/2017	GS	09:00	19:45	PR	PR			09:45	01:15	01:15	01:00	01:15			

Now to authorize overtime hours go to T&A> Authorization/Approval> OT/C-OFF. The Pending collapsible panel shows the Total overtime hours which can be authorized as **C-OFF**.

Overtime/C-OFF Authorization

Date * 10/04/2017 11/05/2017

Filter Users Individual

User NP Nisha

View

Pending (4)

User NP Nisha

Attendance Date 02/05/2017

Overtime Type OT2

OT2 Hours 03:30

Authorize As Overtime 000 : 00

Authorize As C-OFF 002 : 00

Remarks COFF for 2 hrs authorized

Authorize

Search

User ID	Name	Date	Shift	1st Half	2nd Half	Gross Work	Extra Work	Net Work	Total Overtime	Auth As Overtime	Auth As C-OFF	Details
NP	Nisha	01/05/2017	GS	PR	PR	11:15	02:45	02:45	02:45			
NP	Nisha	02/05/2017	GS	PR	PR	13:00	04:30	04:30	04:30			
NP	Nisha	03/05/2017	GS	PR	PR	12:04	03:34	03:34	03:34			
NP	Nisha	04/05/2017	GS	PR	PR	09:45	01:15	01:15	01:15			

After the C-Off is authorized, it will be shown in Authorized column.



If all the available overtime hours are authorized as C-OFF or OT, then the transaction will be shown in Authorized panel. If only few hours are authorized then it will be shown in Pending panel only.

Now this 4 hrs C-OFF will be shown in available C-OFF in Leave balance page as shown below. The user can apply for C-OFF leave from C-OFF application. For eg: user can avail half day with 4 hrs of C-OFF.

Leave Balance

User ID NP Nisha

Leaves

C-OFF

Validity Period 11/03/2017 11/05/2017

Total Hours 02:00

Available C-OFF Details

Search

Date	Authorized	Manual Credit	Manual Debit	Encashed	Availed	Available
02/05/2017	02:00					02:00

Example3: If Both OT & C-OFF are to be given to user.
(How to give OT on week days and C-OFF on WO automatically?)

Select **OT/C-OFF Eligibility** for the user as **Both** from the drop down options. Select **Authorize C-OFF on** as “WO” as shown below. So OT will be given from Monday to Saturday as configured from Overtime Configuration and C-OFF will be given on Sunday.

The screenshot shows the 'User Configuration' window for user 'Isha'. The 'Attendance' tab is active, displaying the 'Policy' section. The 'OT/C-OFF Eligibility' dropdown is set to 'Both'. The 'Authorize C-OFF On' section has 'WO' selected. The 'Bus Route' section is also visible.

Overtime Policy & Daily Overtime

Enable “Calculation on WO/PH/FB/RD as per Weekday”
Daily1 components are configured from Sunday to Saturday
For auto-authorizing overtime, enable “Auto Authorize Overtime component”.

The screenshot shows the 'Overtime Policy' configuration window. The 'OverTime Policy' is set to '2' and 'OT Policy-Daily1'. The 'Policy Period' is from '01/01/2009' to '31/12/2099'. The 'Net-Work Policy' is set to '1' and 'OverTime Policy-1'. The 'Calculation On WO/PH/FB/RD As Per Weekday' checkbox is checked. The 'Overtime Configuration' section is expanded, showing the 'Daily Overtime' tab. The 'Overtime Calculation' is set to 'Daily 1', and the 'Auto Authorize Overtime Component' checkbox is checked.

Daily Overtime

Overtime Calculation: Daily 1

Auto Authorize Overtime Component: ☒

Authorization Required For Late-IN: ☐

Work Component Configuration

Work Component	Range(From)	Range(To)	Min. Duration Req.	Consider As	Applicable Days	Factor	
Early-IN	00:00	04:00	00:00	OT1	Su Mo Tu We Th Fr Sa	1.0	
Overstay	00:00	04:00	00:00	OT2	Su Mo Tu We Th Fr Sa	1.0	

C-OFF Policy

Enable "Auto Authorize C-OFF"

C-OFF Policy

C-OFF Policy: 2 COFF Policy-2

Default: ☐

Policy Period: 01/01/2009 31/12/2099

Minimum Overtime Required For C-OFF: 01:00

C-OFF Authorized In Multiples Of: 01:00

C-OFF Validity Type: Monthly

C-OFF Validity (Months): 2

Minimum C-OFF For Half Day Off: 04:00

Minimum C-OFF For Full Day Off: 08:00

Auto Authorize C-OFF: ☒

ID	Name	Level
1	COFF Policy-1	1
2	COFF Policy-2	1

Daily Attendance View

The punch details of the user is shown below. The overtime of 3:30 hrs on 6-5-17 will be given as OT and 1:30 hrs on 7-5-17 (Week-off) will be given as C-OFF.

Daily Attendance View

User: 3 Isha

Attendance Period: May 2017

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work	Break Hours	Actual Overtime	Authorized Overtime	Remark	Details
01/05/2017	GS	08:15	19:00	PR	PR		09:45	01:15	01:15	01:00	01:15	01:15			
02/05/2017	GS	09:00	22:00	PR	PR		12:00	03:30	03:30	01:00	03:30	03:30			
03/05/2017	GS	08:00	21:00	PR	PR		12:00	03:30	03:30	01:00	03:30	03:30			
04/05/2017	GS	09:00	20:00	PR	PR		10:00	01:30	01:30	01:00	01:30	01:30			
05/05/2017	GS	08:00	21:00	PR	PR		12:00	03:30	03:30	01:00	03:30	03:30			
06/05/2017	GS	08:30	21:30	PR	PR		12:00	03:30	03:30	01:00	03:30	03:30			
07/05/2017	GS - WO	09:00	20:00	WO	WO		10:00	01:30	01:30	01:00	01:30	01:30			
08/05/2017	GS	09:00	20:00	PR	PR		10:00	01:30	01:30	01:00	01:30	01:30			

The authorized OT is shown by pink arrow which will be given from Monday to Saturday and authorized C-OFF is shown by green arrow which is given on Sunday.
The C-OFF authorized is of 1hrs as it has to be in multiples of 1 hr as configured from C-OFF Policy.

Overtime/C-OFF Authorization

Date *

10/04/2017

11/05/2017

Filter Users

Individual

User

3

Isha

View

Pending (0)

Authorized (8)

User

3

Isha

Attendance Date

06/05/2017

Overtime Type

OT1

OT1 Hours

000:30

Authorize As Overtime

000 : 30

Authorize As C-OFF

000 : 00

Remarks

Authorize

Search

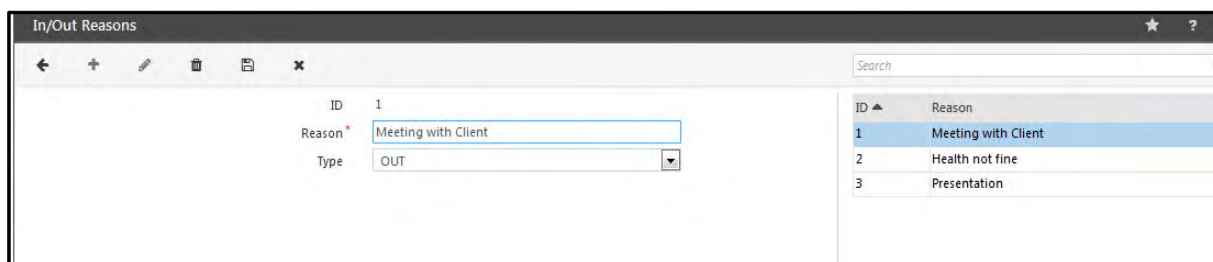
User ID	Name	Date	In	Out	In	Out	Shift	OT	Auth OT	Auth OT Date	Auth C-OFF	Auth C-OFF Date	Auth By	Details
3	Isha	06/05/2017	08:30	21:30			GS	03:30	03:30					
3	Isha	07/05/2017	09:00	20:00			GS	01:30			01:00			
3	Isha	08/05/2017	09:00	20:00			GS	01:30	01:30					

In/Out Reasons

In some organizations, employees may be required to offer valid reasons for In/Out punch events or to explain attendance exceptions. Such valid reasons can be pre-defined by the system administrator as per the organizational policies and requirement. These pre-defined In/Out reasons can be then used for manual attendance correction by HR users or for personal/official entry marking by employees using the **Employee Self Service** module.

To define a new In/Out Reason, Select the **Time and Attendance module > Masters > In/Out Reasons**.

The **In/Out Reasons** page will appear as shown.



ID	Reason
1	Meeting with Client
2	Health not fine
3	Presentation

Click **New** button to create new reason.

The In/Out Reason **ID** is automatically system-generated for every new reason created.

Enter a brief description of the In/Out Reason in the **Reason** field. This can be of a maximum length of 30 characters (For e.g. "Sickness" or "Meeting with Client").

In the **Type** field, select **IN** or **OUT** to specify the type of punch with which the reason is to be associated.

Click **Save** button to save the new In/Out reason.



Maximum number of In/Out Reasons that can be created on COSEC is 999.



While applying for the Attendance correction, you can select the In/OUT reason for the respective punches.

Bus Route

The COSEC application allows the administrator to define bus routes which in turn can then be assigned to users from the **User Configuration** option of the **Users** module.

To define a new Bus Route, Select the **Time and Attendance module > Masters > Bus Route**.

The **Bus Route** page appears on your screen as follows:

ID	Name
1	Makarpura Route

Click **New** to enter the details of a new Bus Route.

Each Bus Route will have a unique **ID** for identification and this is generated by system automatically when the bus route is saved.

Specify a name for the Bus Route in the **Name** field which can be a maximum of *30 characters*.

Select the **Active** checkbox to enable the Bus Route.

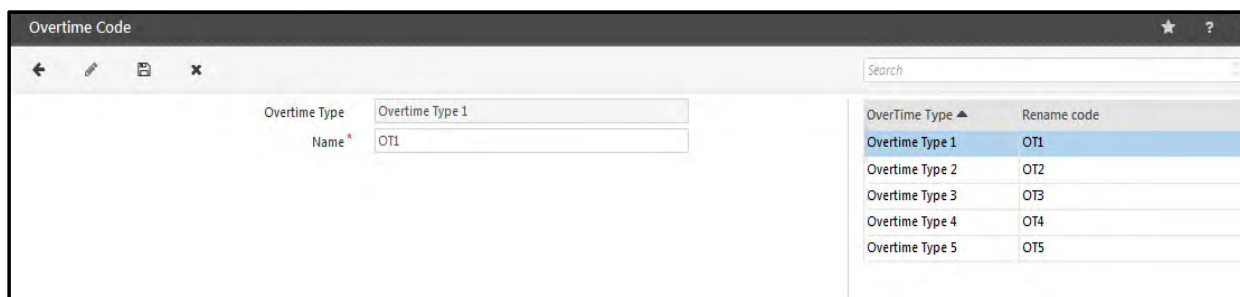
Click **Save** to save the configured bus route.

Overtime Code

Each Overtime type defined in COSEC can be re-labelled as per the site requirement using the *Overtime Code* functionality. For example, an organization may wish to rename the overtime type “OT1” as “OThlf” based on a “0.5” multiplication factor they implement for pay calculation. Such overtime codes can be up to 5 *characters* long.

To do this, Select the **Time and Attendance module > Masters > Overtime Code**.

The **Overtime Code** page appears as follows:

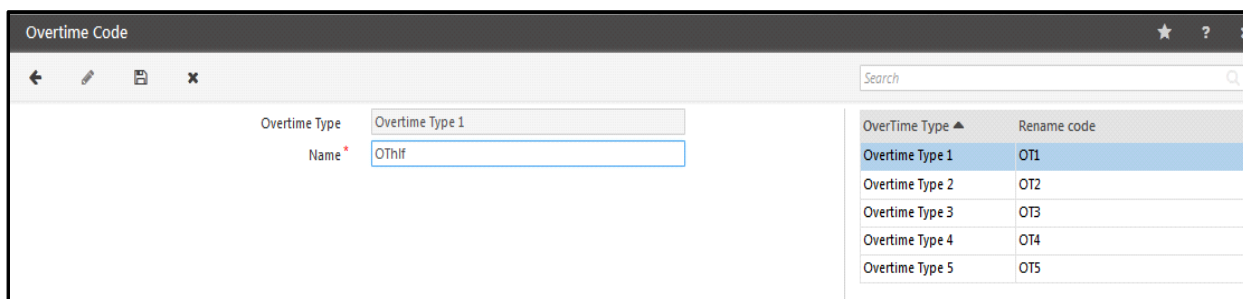


OverTime Type ▲	Rename code
Overtime Type 1	OT1
Overtime Type 2	OT2
Overtime Type 3	OT3
Overtime Type 4	OT4
Overtime Type 5	OT5

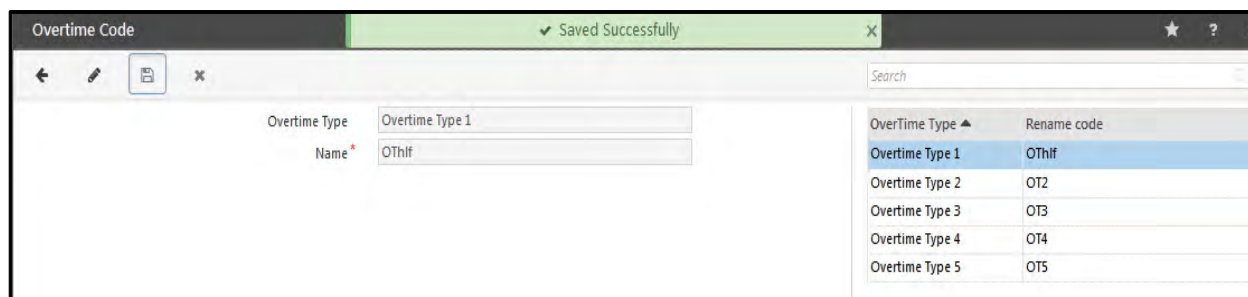
Select an **Overtime Type** from the list on the right-hand side of the page (say, “Overtime Type1”).

In the **Name** field, enter a new overtime code.

Click **Save** button. The new overtime code will appear on the overtime type list as follows:



OverTime Type ▲	Rename code
Overtime Type 1	OThlf
Overtime Type 2	OT2
Overtime Type 3	OT3
Overtime Type 4	OT4
Overtime Type 5	OT5



OverTime Type ▲	Rename code
Overtime Type 1	OThlf
Overtime Type 2	OT2
Overtime Type 3	OT3
Overtime Type 4	OT4
Overtime Type 5	OT5

Attendance Summary

The **Attendance Summary** summarizes and displays all attendance data of a user for the chosen attendance period. It provides easy viewing of attendance details to the HR administrator.

To access this functionality, Select the **Time and Attendance module > Utilities > Attendance Summary**.

The **Attendance Summary** page will appear as follows:

The screenshot shows the 'Attendance Summary' page with a header bar containing a star and a question mark icon. Below the header, there are navigation icons (back and refresh). The main content area has two filters: 'User' with a dropdown menu showing '1690' and 'Priyank Bora', and 'Attendance Period' with dropdowns for 'March' and '2017'. Below the filters, there are two tabs: 'Summary' (selected) and 'Details'.

User: Select a user from the picklist whose attendance summary is to be viewed.

Attendance Period: Select the month and year as the Attendance Period for which the summary is to be obtained.

Viewing Attendance Summary

To view the *Attendance Summary* for a user, click the **Summary** section as shown below.


The screenshot shows the 'Attendance Summary' page with the 'Summary' tab selected. The page displays various attendance metrics for the user 'Priyank Bora' for the month of 'March 2017'. The metrics are as follows:

Metric	Value
Presents	1.0
Absents	20.0
Paid Leaves	0.0
Unpaid Leaves	0.0
Tours	0.0
Week-Offs	8
Holidays	2
Work Hours	00:18
Extra Work	00:18
Net Work Hours	HH:MM
Break Hours	HH:MM
Authorized Overtime	HH:MM
Generated Overtime	00:18

Below the metrics, there is a calendar for March 2017 showing the days of the week (Mo, Tu, We, Th, Fr, Sa, Su) and the corresponding dates (1 to 31). The calendar is color-coded to show the user's attendance status for each day.

At the bottom of the page, there is a section for 'Available Short Leaves' and 'Available Short Leave Duration' with input fields for 'Late-IN', 'Early-OUT', and 'Availed/Allowed Less Work Duration (Mins)'.

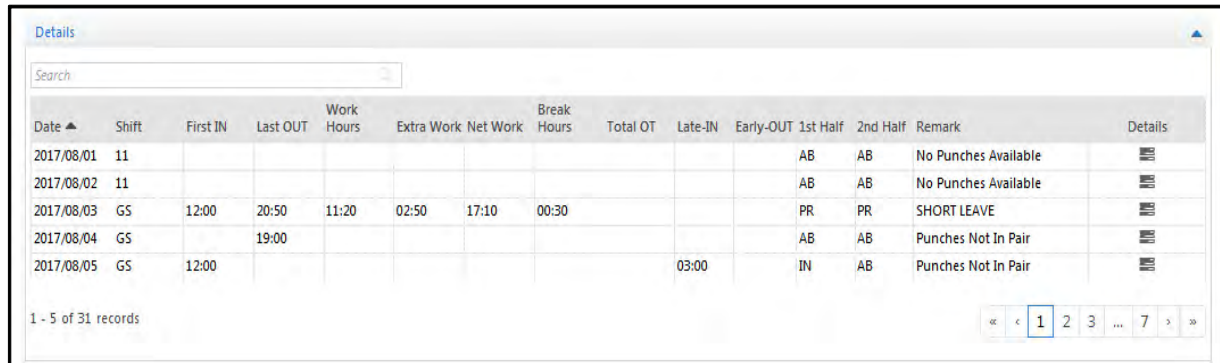
The attendance summary of the selected user appears with the corresponding number of days or hours for each field as shown above.






The administrator can also view a detailed overtime summary by clicking the overtime summary  button next to the **Generated Overtime** field.

The Overtime Summary presents the individual overtime hours for OT1, OT2, OT3, OT4 and OT5 and the respective Authorized overtime. It also displays other overtime details such as Total unauthorized and authorized overtime, total manual debit/credit, availed and available overtime for the selected user.

Viewing Attendance Details


To view attendance details for the selected user, click the **Details** section as shown below.

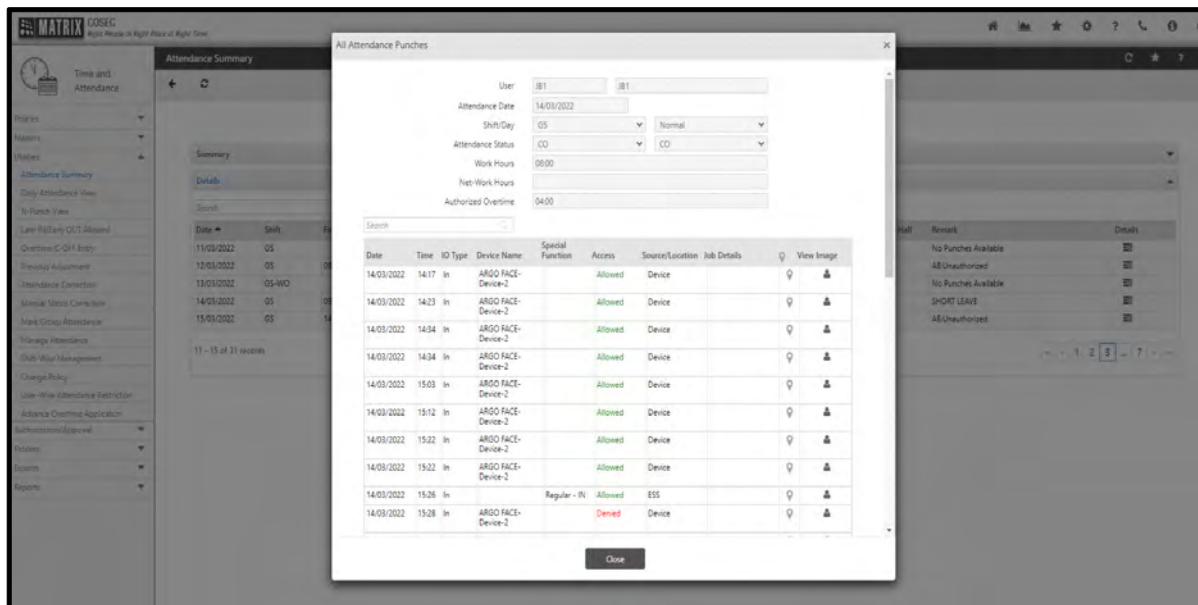












Date	Shift	First IN	Last OUT	Work Hours	Extra Work	Net Work	Break Hours	Total OT	Late-IN	Early-OUT	1st Half	2nd Half	Remark	Details
2017/08/01	11										AB	AB	No Punches Available	
2017/08/02	11										AB	AB	No Punches Available	
2017/08/03	GS	12:00	20:50	11:20	02:50	17:10	00:30				PR	PR	SHORT LEAVE	
2017/08/04	GS		19:00								AB	AB	Punches Not In Pair	
2017/08/05	GS	12:00							03:00		IN	AB	Punches Not In Pair	

1 - 5 of 31 records

The **Details** section displays the attendance details for individual days of the defined attendance period for the selected employee.

To view the details of attendance punches for a day, click the **Details**  icon corresponding to the respective **Date** row. The **All Attendance Punches** window appears as shown.



Date	Time	ID Type	Device Name	Special Function	Access	Source/Location	Job Details	View Image
14/03/2022	14:17	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	14:23	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	14:34	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	14:34	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:03	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:12	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:22	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:22	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:26	In	Regular - IN	Allowed	ESS			
14/03/2022	15:28	In	ARGO FACE-Device-2		Denied	Device		

Click **Close** to close the window.



If Map is not loaded; check the network connection of your PC or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

Daily Attendance View

The Daily Attendance View displays all attendance data of a user for a chosen Attendance Period. This feature in COSEC provides easy viewing of attendance details for the HR administrator.

To access this functionality, Select the **Time and Attendance module > Utilities > Daily Attendance View** and the following screen appears.

The screenshot shows the 'Daily Attendance View' window with the 'Template Configuration' tab selected. The interface includes a 'View' tab and a 'Template Configuration' tab. Under 'Template Configuration', there are fields for 'User' (Guest), 'Attendance Period' (October 2021), 'Display View as Per' (Default View), 'Display Summary' (Overall), and 'Starting Day of the Week' (Monday). Below these fields is a table with columns: Date, Shift, First IN, Last OUT, 1st Half, 2nd Half, Late-IN, Early-OUT, Work Hours, Extra Work, Net-Work, Break Hours, Generated Overtime, Authorized Overtime, Remark, and Details. The table currently displays 'No Data'.

There are two tabs displayed namely:

- View
- Template Configuration

Select **Template Configuration** tab to customize the view that you want to see in **Daily Attendance View** Page.

The screenshot shows the 'Daily Attendance View' window with the 'Template Configuration' tab selected. The interface includes a 'View' tab and a 'Template Configuration' tab. Under 'Template Configuration', there are fields for 'Template' (ID, Name), 'Field Configuration' (Field Type: Database, Field Value: 1st Half Status, Display Name), and a table with columns: Fields, Field Type, View/Export, Display Summary, Up/Down. The table currently displays 'No Data'. On the right side, there is a list of templates with columns 'ID' and 'Name', showing '1 Default View'.

In the right pane, the **Default View** template is displayed.

You can either edit the **Default View** Template or add a new template as per your requirement.

Editing the Default View Template

Click Default View Template in the right pane.

In Template, by default the name displayed is **Default View**. You can change it if required.

The template parameters are displayed under **Field Configuration**.

Field Type: Select the type from the options - **Database** and **Custom**.

Field Value: This will be displayed according to the Field Type you select:

- If you select **Database**, select the desired value from the drop down list.
- If you select **Custom**, configure the desired value. To do so, enter “~” and the list appears. Select the desired parameters from this list or you can also configure any sql expression here. If you want to enter parameters other than those from the selection list make sure you add these within the square bracket, for example [Day Type].



*Few fields have been removed from Template mapping in this release. If you get an error while accessing a **Default View** existing template, then you need to create a new template.*

Display Name: Configure the desired name you wish to assign to the selected Field Value.

According to the configuration you have set, the details will be displayed in the grid.

Fields	Field Type	View/Export	Display Summary	Up/Down
Date	Database	<input type="checkbox"/>	<input type="checkbox"/>	
Shift	Custom	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	▼
First IN	Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>	▲▼
Last OUT	Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>	▲▼
1st Half	Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>	▲▼
2nd Half	Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>	▲▼
Late-IN	Database	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	▲▼
Early-OUT	Database	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	▲▼
Minute Absence	Database	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	▲▼


The Parameters in the grid are:

- **View/Export:** Clear the check boxes of the respective parameters, if you do not wish to view or export it. By default, it is enabled (selected). The Date parameter cannot be edited. If you wish to disable the **View/Export** for all the parameter, clear the check box in the header row under **View/Export**.
- **Display Summary:** Clear the check boxes of the respective parameters, if you do not wish to display their summary. By default, it is enabled (selected). If you wish to disable the **Display Summary** for all the parameter, clear the check box in the header row under **Display Summary**.

- Click **Delete**, if you wish to delete the parameter.
- **UP/Down**: Click the Up or Down arrow to change the sequence of the desired parameter in the list.

Share View With: You can share this template with others. In **Default View**, by default it is applicable to all users.

Click **Save**.

In case you overwrote a Default View Template and you desire to restore it again, then select the **Reset** , in the top menu bar.

Adding a New Template

In the **Template Configuration** tab, click Add button to add a new template and configure the following parameters:

Template: Configure the desired name you wish to assign to the new template.

Default: Select the checkbox if **Default View** template parameters are to be restored as configuration in the new template.

The template parameters are displayed under **Field Configuration**

Field Type: Select the type from the option - **Database** and **Custom**.

Field Value: This will be displayed according to the Field Type you select:

- If you select **Database**, select the desired value from the drop down list.
- If you select **Custom**, configure the desired value. To do so, enter“~” and the list appears. Select the desired parameters from this list or you can also configure any sql expression here.



You can also create a **Custom Column Name** by creating formula with **Field Value** selection as per your choice.

For example if you have selected three **Field Values**: ~ First In~ ~ Last Out~ ~Punch Date~
You can provide the **Display Name** for above selected field values as 'Total Duration' which should be considered as **Custom Column Name**.

Few fields have been removed from Template mapping in this release. If you get an error while accessing an existing template, then you need to create a new template.

Display Name: Configure the desired name you wish to assign to the selected Field Value.

According to the configuration you have set, the details will be displayed in the grid.

The parameters in the grid are:

View/Export: Select the check boxes of the desired fields, if these should be displayed in the Daily Attendance View Page. The Date parameter cannot be edited.

Display Summary: Click the checkboxes of the desired parameters to view as summary. It will only display the summary for the parameters that have time calculations.

Click **Delete**, if you wish to delete the parameter.

UP/Down: Click the Up or Down arrow to change the sequence of the desired parameter in the list.

Fields	Field Type	View/Export	Display Summary	Up/Down
Date	Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Morning	Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>	▼
Afternoon	Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>	▲▼
Overtime	Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>	▲

Share View With: You can share this template with others. Select the desired option – **Group Wise**, **User Wise** or **All**.

If you select **Group Wise**, select the Group and Organization.

If you select **User Wise**, select the user.

Click **Save**.

This new template will appear in the right pane

Now Click the **View** tab to display the configured template.

User: Select the user from the picklist whose Attendance details are to be viewed.

Attendance Period: Attendance Period can be selected in two ways: Month-wise and Date-wise.

- **Month-wise:** Selecting this option will display the attendance of the particular month. Select the month and year from the drop down list for which the daily attendance is to be viewed.
- **From/To Date:** Selecting this option will display the attendance of the range selected in the Attendance Period. Select the starting and ending date using the date selection button for which the daily attendance is to be viewed. For a single day select the same date in both the fields.

Display View as Per: Select the type of view you desire from the drop down list. All the created templates will appear in the list.

Display Summary: Select the desired option — **Week-Wise, Overall, Both** or **None**.

- If you select **Week- Wise**, it will display the total weekly summary.
- If you select **Overall**, it will display the data summary as per the Attendance Period set.
- If you select **Both**, it will display both weekly as well as monthly summary.
- If you select **None**, it will display the users data without any details of total. According to the configuration you have set and the type of template selected, the details will be displayed in the grid.

Starting Day of the Week: Select the starting day of the week from the drop down list. Based on the day selected, weekly attendance view will be shown in the grid.

The attendance details with In time, Out time, Work hours, Extra work hours and other shift details appear in the grid.

Daily Attendance View

View

Template Configuration

User: 1575 PRIVILEGE

Attendance Period: January 2020

From Date: To Date:

Display View as Per: Default View

Display Summary: Overall

Starting Day of the Week: Monday

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net-Work	Break Hours	Generated Overtime	Authorized Overtime	Remark	Details
01/01/2020	GS-Normal	08:41	18:13	PR	PR		00:17	09:02	00:19	09:02	00:30				
02/01/2020	GS-Normal	08:06	12:40	PR	PL			04:34	00:54	04:34					
03/01/2020	GS-Normal			PL	PL										
04/01/2020	GS-WO			WO	WO										
05/01/2020	GS-WO			WO	WO										
06/01/2020	GS-Normal	08:49	18:43	PR	PR			09:24	00:24	09:24	00:30				
07/01/2020	GS-Normal	09:03	18:44	PR	PR			09:11	00:14	09:11	00:30				
08/01/2020	GS-Normal	08:29	13:05	PR	AB			04:36	00:31	04:36				AB Early-OUT	
09/01/2020	GS-Normal	08:52	13:24	PR	AB			04:32	00:08	04:32				AB Early-OUT	
10/01/2020	GS-Normal			AB	AB									No Punches Available	
11/01/2020	GS-WO			WO	WO										
Total							01:08	82:37	05:10	82:37	03:30				

The last row of the grid displays the total hours of all days for the respective columns.

You can apply for the attendance correction option by clicking on the AB punch marking as shown below.

Date	Shift	First IN	Last OUT	1st Half	2nd Half
01/01/2020	GS-Normal	08:41	18:13	PR	PR
02/01/2020	GS-Normal	08:06	12:40	PR	PL
03/01/2020	GS-Normal			PL	PL
04/01/2020	GS-WO			WO	WO
05/01/2020	GS-WO			WO	WO
06/01/2020	GS-Normal	08:49	18:43	PR	PR
07/01/2020	GS-Normal	09:03	18:44	PR	PR
08/01/2020	GS-Normal	08:29	13:05	PR	AB
09/01/2020	GS-Normal	08:52	13:24	PR	AB
10/01/2020	GS-Normal			AB	AB

Correction Options

- Apply Leave
- Apply C-OFF
- Apply Tour
- Short Leave/Official In-Out
- Attendance Correction

Click on the **Details** to view all the Attendance Punches as shown below.

All Attendance Punches

User

JB1

JB1

Attendance Date

15/03/2022

Shift/Day

GS

Normal

Attendance Status

AB

AB

Work Hours

00:19

Net-Work Hours

Authorized Overtime

Search

Date	Time	IO Type	Device Name	Special Function	Access	Source/Location	Job Details		View Image
15/03/2022	14:08	In	ARGO FACE-Device-2		Allowed	Device	J1 - Job1		
15/03/2022	14:09	In	ARGO FACE-Device-2		Denied	Device			
15/03/2022	14:14	In	ARGO FACE-Device-2		Allowed	Device	J1 - Job1		
15/03/2022	14:19	In	ARGO FACE-Device-2		Denied	Device			
15/03/2022	14:25	In	ARGO FACE-Device-2		Denied	Device			
15/03/2022	14:27	In	ARGO FACE-Device-2		Allowed	Device	J4 - Job4		
15/03/2022	14:27	In	ARGO FACE-Device-2		Allowed	Device	J4 - Job4		

Close



If Map is not loaded; check the network connection of your PC or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

N-Punch View

The term *N-Punch* stands for “n” number of punches and is a system for punch calculation on COSEC. This means that all the available attendance punches of a user on a particular day will be considered for his work hours calculation. The **N-Punch View** functionality enables you to view the details of punch timings and manually edit details if required for a selected date. This is applicable only to users for whom the N-Punch calculation is enabled in their respective Attendance Policies.



To enable the N-Punch system for a user, go to **Time and Attendance > Policies > Attendance Policy**. Select the applicable policy and set the **Max Punches to Consider** parameter. For details, refer to [“Attendance Policy”](#).

To access this functionality, Select the **Time and Attendance module > Utilities > N-Punch View**.

The page will be displayed on your screen as follows:

The screenshot shows the N-Punch View interface. At the top, there are filters for User (4, Priyank), Attendance Date (03/05/2017), and Shift (GS). Below these is a table with columns: Source, IO Type, Date, Time, Out Time, Special Function, Edit, and a trash icon. The table contains four rows of punch data. At the bottom, there are summary fields: Gross Work Hours (09:50), Total Out Time (01:00), N-Punch Work Hours (08:50), Extra Work Hours (00:30), Authorized Overtime (00:30), and Status (PR, AB).

Source	IO Type	Date	Time	Out Time	Special Function	Edit	
Device - NGT Direct Door-Device-1	IN	03/05/2017	09:10				
Device - NGT Direct Door-Device-1	OUT	03/05/2017	13:00				
Device - NGT Direct Door-Device-1	IN	03/05/2017	14:00	01:00			
Device - NGT Direct Door-Device-1	OUT	03/05/2017	19:00				

Gross Work Hours: 09:50 Total Out Time: 01:00 N-Punch Work Hours: 08:50 Extra Work Hours: 00:30 Authorized Overtime: 00:30 Status: PR AB

User: Select a user from the **User** picklist. This picklist will show only N punch users.

Attendance Date: Select the Attendance Date for which user punches are to be viewed. Click the button to specify a custom period for date selection. All punches for the selected date are displayed as shown in the grid.

To add a punch manually, Click the **ADD** button. The new row in the grid will appear.

The screenshot shows the N-Punch View interface with a new row being added to the punch table. The new row is highlighted in blue and contains the following data: Source: Device - NGT Direct Door-Device-1, IO Type: IN, Date: 03/05/2017, Time: 20:00. The table now has five rows. An arrow points to the ADD button (a plus sign in a circle) at the top right of the table.

Source	IO Type	Date	Time	Out Time	Special Function	Edit	
Device - NGT Direct Door-Device-1	IN	03/05/2017	20:00				
Device - NGT Direct Door-Device-1	IN	03/05/2017	09:10				
Device - NGT Direct Door-Device-1	OUT	03/05/2017	13:00				
Device - NGT Direct Door-Device-1	IN	03/05/2017	14:00	01:00			
Device - NGT Direct Door-Device-1	OUT	03/05/2017	19:00				

Enter the timing for the punch. Then click OK. The punch will be automatically saved as IN punch and it will be added to the grid list as a *Manual Entry*.

The screenshot shows the 'N-Punch View' window. At the top, there are fields for 'User' (4, Priyank), 'Attendance Date' (03/05/2017), and 'Shift' (GS). Below these is a table with columns: Source, IO Type, Date, Time, Out Time, Special Function, Edit, and a trash icon. The table contains five rows of device-based punches and one 'Manual Entry' row at the bottom, which is highlighted in blue. An arrow points to the 'Manual Entry' row.

Source	IO Type	Date	Time	Out Time	Special Function	Edit	
Device - NGT Direct Door-Device-1	IN	03/05/2017	09:10				
Device - NGT Direct Door-Device-1	OUT	03/05/2017	13:00				
Device - NGT Direct Door-Device-1	IN	03/05/2017	14:00	01:00			
Device - NGT Direct Door-Device-1	OUT	03/05/2017	19:00				
Manual Entry	IN	03/05/2017	20:00				



The **IO** dropdown list will appear (for punch type selection) only if the **Out Punch From Exit Reader** option is enabled during Attendance Policy configuration of the selected user. Else, the day's first punch will automatically be counted as an IN punch, the second as OUT punch, the third as IN punch and so on.

To edit a punch, click the button. Edit the punch data and add a special function if required. Click OK to save the changes.

This screenshot shows the 'N-Punch View' window with the 'Manual Entry' row selected. The 'Special Function' dropdown menu is open, showing options: Select, Select, Official Out, ShortLeave Out, Early-Out Allowed, Overtime Out, and Regular Out. Below the table, there are summary fields: Gross Work Hours (10:50), Total Out Time (01:00), N-Punch Work Hours (09:50), Extra Work Hours (01:30), Authorized Overtime (01:30), and Status (PR, PR).

Source	IO Type	Date	Time	Out Time	Special Function	Edit	
Device - NGT Direct Door-Device-1	IN	03/05/2017	09:10				
Device - NGT Direct Door-Device-1	OUT	03/05/2017	13:00				
Device - NGT Direct Door-Device-1	IN	03/05/2017	14:00	01:00			
Device - NGT Direct Door-Device-1	OUT	03/05/2017	19:00		Select		
Manual Entry	IN	03/05/2017	20:00				

Gross Work Hours: 10:50 Total Out Time: 01:00 N-Punch Work Hours: 09:50 Extra Work Hours: 01:30 Authorized Overtime: 01:30 Status: PR PR

Source	IO Type	Date	Time	Out Time	Special Function	Edit	
Device - NGT Direct Door-Device-1	IN	03/05/2017	09:10				
Device - NGT Direct Door-Device-1	OUT	03/05/2017	13:00				
Device - NGT Direct Door-Device-1	IN	03/05/2017	14:00	01:00			
Manual Entry	OUT	03/05/2017	19:00		Official OUT		
Manual Entry	IN	03/05/2017	20:00				

The N-Punch data can be exported in Excel format. Click the Export button. You can open or save the file at the desired location.

	A	B	C	D	E	F
1	Source	IO Type	Date	Time	Out Time	Special Function
2	Device - NGT Direct Door-Device-1	IN	03/05/2017	09:10		
3	Device - NGT Direct Door-Device-1	OUT	03/05/2017	13:00		
4	Device - NGT Direct Door-Device-1	IN	03/05/2017	14:00	01:00	
5	Manual Entry	OUT	03/05/2017	19:00		Official OUT
6	Manual Entry	IN	03/05/2017	20:00	01:00	
7	Manual Entry	OUT	03/05/2017	20:30		
8						
9	Summary					
10						
11	Gross Work Hours: 12:20					
12	Total Out Time: 02:00					
13	N-Punch Work Hours: 10:20					
14	Extra Work Hours: 02:00					
15	Overtime Hours: 02:00					
16	Status: PR PR					

Late-IN/Early-OUT Allowed

An HR administrator may, at times, be required to provide special allowance for employees to come in late or leave early on a particular day. Such a requirement may arise due to various reasons such as bus service failure, unnatural weather conditions, red alerts or festivities. On such an occasion, the administrator can use the **Late-IN/Early-OUT Allowed** functionality to allow all Late-IN or Early-OUT punches for the specified day.

To access this functionality,

Select the **Time and Attendance module > Utilities > Late-IN/Early-OUT Allowed**.

The **Late-IN/Early-OUT Allowed** page appears as shown below:

ID	Date	Type	Start Time	End Time
No Data				

Select a date from the date selection picklist in the **Override On** field, on which the Late-IN/Early-OUT Policy is to be overridden.



System will allow the application of this feature only on a day on or before the current date.

Select **LateIn** or **EarlyOut** as the **Override Policy** to be applied.

Enter the start and end time in the **Start Time - End Time** fields in the HH:MM format. This defines the duration for which the override policy will be allowed on the chosen date.

The **Reason** field is available only for the **LateIn** policy. Select the reason from the drop down list as **Other** or **BusLate** as shown.

Reason	Other
Bus Route	Other
Remark	BusLate

If the reason for Late-IN is due to the late arrival of bus, then the **BusLate** option should be selected. For all other reasons, **Other** can be selected.

For **BusLate**, select the particular bus route from the **Bus Route** detail picklist.

Add a remark on the Late-IN if required in the **Remark** field.

In the **Device Selection** section, select a **Panel/Direct Door** from the drop down list and select the door. This is the door on which user would be punching. The Late-In punch will be updated after monthly attendance process.

Click **Save** button to save the changes.

The screenshot shows a web application window titled "Late-IN/Early-OUT Allowed". At the top, a green status bar indicates "Saved Successfully". Below the title bar, there is a navigation menu with icons for back, forward, delete, save, and close. A search bar is located on the right side of the navigation menu.

The main form area is divided into two sections. The top section contains the following fields:

- Override On ***: A date picker showing "08/05/2017".
- Override Policy**: A dropdown menu showing "Late-IN".
- Start Time - End Time ***: Two time input fields showing "09:00" and "10:00".
- Reason**: A dropdown menu showing "BusLate".
- Bus Route**: A dropdown menu showing "1" and a button labeled "Makarpura Route".
- Remark**: A text input field containing "Bus Puncture".

The bottom section is titled "Device Selection" and contains the following fields:

- Panel/Direct Door**: A dropdown menu showing "NGT Direct Door-Device-1".
- Door**: A dropdown menu showing "All".

On the right side of the form, there is a table with the following columns: ID, Date, Type, Start Time, and End Time. The table contains one row of data:

ID	Date	Type	Start Time	End Time
1705090001	08/05/2017	Late-IN	09:00	10:00

Overtime/C-OFF Entry

This option enables the HR administrator to manually enter Overtime/C-OFF details for an employee as well as credit/debit OT/C-OFF in cases where an employee has not been able to mark the entry or exit times.



Authorized Overtime = Authorized OT + Manual Credit OT - Manual Debit OT

To access this functionality,

Select the **Time and Attendance module > Utilities > Overtime/C-OFF Entry**.

The **Overtime/C-OFF Entry** page appears as follows:

1. Select a **User** from the picklist for whom the manual Overtime/C-OFF entry is to be made.
2. Select the **Attendance Date** from the calendar button. Click the “Modification Allowed” button to specify the period within which overtime/C-OFF entry should be allowed.
3. On the selection of the **Custom Period** option, the system allows you to enter the number of months prior to the current date for which the attendance details can be viewed.

Once the attendance period is defined, the Overtime/C-OFF Entry page appears as follows.

4. Select the date from the right grid or by calendar button for which OT/ C-OFF entry is to be made.

Attendance Details

Manual Overtime/C-OFF Entry

Component	Processed	Authorized	Manual Credit	Manual Debit
OT1	-	-	-	-
OT2	-	-	-	-
OT3	-	-	-	-
OT4	-	-	-	-
OT5	-	-	-	-
C-OFF	-	-	-	-

Component: OT1
Entry Type: Credit
Value:
Process

Date	Total OT Credit	Total OT Debit	Total C-OFF Credit	Total C-OFF Debit
13/02/2017				
12/02/2017				
11/02/2017				
10/02/2017				
09/02/2017				
08/02/2017				
07/02/2017				
06/02/2017				
05/02/2017				
04/02/2017				
03/02/2017				
02/02/2017				
01/02/2017				

16 - 28 of 28 records

- To view attendance details for the selected date, select the **Attendance Details** section as shown. It shows the work hours details and Total Available Overtime of the user.

Attendance Details

Shift/Day: GS
Attendance Status: PR
Status Summary: Present
Work Hours: 11:00
Extra Work Hours: 02:00
Net Work Hours: 11:00
Adjusted Work Hours: 00:00
Total Available Overtime: 00:00

- In the **Manual Overtime/C-OFF Entry** section, select the **Component** for which manual entry is to be done. For e.g. to make an entry for "OT4", select component **OT4**.
- Specify the **Entry Type** as **Credit** or **Debit**.
- Enter a **Value** for the hours which are to be credited or debited to the selected component in the HH:MM format as shown.

Manual Overtime/C-OFF Entry

Search

Component	Processed	Authorized	Manual Credit	Manual Debit
OT1	-	-	-	-
OT2	-	-	-	-
OT3	-	-	-	-
OT4	-	-	-	-
OT5	-	-	-	-
C-OFF	-	-	-	-

Component:

Entry Type:

Value:

Process

9. Click the **Process** button to save the manual entry for the selected date.
The credited OT will be shown in Total Available Overtime and Manual credited value as shown below.

Overtime/C-OFF Entry

User: Sweta

Attendance Date:

Attendance Details

Shift/Day:

Attendance Status:

Status Summary: Present

Work Hours: 11:00

Extra Work Hours: 02:00

Net Work Hours: 11:00

Adjusted Work Hours: 00:00

Total Available Overtime: 02:00

Manual Overtime/C-OFF Entry

Search

Component	Processed	Authorized	Manual Credit	Manual Debit
OT1	-	-	-	-
OT2	-	-	-	-
OT3	-	-	-	-
OT4	-	-	02:00	-
OT5	-	-	-	-
C-OFF	-	-	-	-

Summary Table

Date	Total OT Credit	Total OT Debit	Total C-OFF Credit	Total C-OFF Debit
13/02/2017				
12/02/2017				
11/02/2017				
10/02/2017				
09/02/2017				
08/02/2017				
07/02/2017				
06/02/2017				
05/02/2017				
04/02/2017				
03/02/2017				
02/02/2017	02:00			
01/02/2017				

16 - 28 of 28 records

Navigation:

The manual entry will now reflect in the OT/C-OFF balance for the selected user and can be used for encashment, leave application etc.

Previous Adjustment

This option enables the HR user to update previous adjustment data of an employee (from a closed attendance period) in the current attendance records. This may include entry for adjustment in attendance days, OT hours, working hours and shifts allowance. Such adjustment is then reflected in the attendance data of the current attendance period. This feature can be useful to the HR user for effective payroll calculation.

Previous Adjustment entry can be of two types:

- System Generated - Previous adjustment entry is automatically generated by the system in the following cases:
 - After Leave Application and Approval
 - Tour Application and Approval
 - Manual Correction in Attendance Period
 - Shift Count (More than 1 shift attended by employee)
- Manual - Previous adjustment entry is manually done by the HR user for an employee.




A “closed” attendance period in COSEC, is a previous attendance period for which attendance data has already been processed and changes can no longer be made. This is based on the Monthly Process configuration for an attendance period. To enable attendance correction or attendance adjustment for a closed attendance period, go to **Time and Attendance > Attendance Policy > General**.

To manually enter previous adjustment data, Select the **Time and Attendance module > Utilities > Previous Adjustment**.

The **Previous Adjustment** page is displayed as shown.


The screenshot shows the 'Previous Adjustment Entry' form. At the top, there's a 'User' section with 'ID' and 'Name' fields. Below that is 'Previous Attendance Date For Adjustment' with a 'From Date' field and a calendar icon. The 'Attendance Details' section has a 'Current' dropdown. The 'First Half', 'Second Half', 'Work Hours', 'Extra Work Hours', and 'Shift Allowance' sections are currently empty. The 'Target Month For Adjustment Values' section shows 'October' and '2019'. The 'Adjustment Entry' section has 'Attendance Days', 'Work Hours', 'Overtime', and 'Shift Allowance' dropdowns, each with a corresponding input field. The 'Remark' field is a text area with a '50 chars' limit. At the bottom, there's a 'Previous Adjustment Records' section with a dropdown arrow.

1. Click **New** .
2. In the **User** field, enter a user ID or select a user by clicking the picklist button.
3. In the **Previous Attendance Date for Adjustment** field, enter a date by clicking the date selection button. This is the previous date for which the adjustment is to be done.

4. In the **Attendance Details** field, select **Current** or **Previous** to load the current or previous attendance details for system-generated adjustment. These details will include **First Half**, **Second Half**, **Working Hours**, **Extra Work Hours** and **Shift Allowance**.
5. In the **Target Month For Adjustment Values**, select the month and year in which the previous adjustment is to be reflected.
6. Under **Adjustment Entry**, there are four options for which adjustment entry can be made - Attendance Days, Work Hours, Overtime and Shift Allowance. Select “**Add(+)**” or “**Subtract(-)**” from the dropdown list against each entry to add or deduct the respective field value. This can be assigned in the adjoining fields as shown. Add a **Remark** if required.

The screenshot shows the 'Adjustment Entry' form. It has four rows: 'Attendance Days' with a 'Select' dropdown, 'Work Hours' with an 'Add(+)' dropdown and an 'HH:MM' input field, 'Overtime' with a 'Select' dropdown and an 'HH:MM' input field, and 'Shift Allowance' with a 'Select' dropdown. The 'Remark' field at the bottom contains the text '50 chars'.

The screenshot shows the 'Adjustment Entry' form with the same layout as the previous one, but with different values: 'Attendance Days' has 'Add(+)', 'Work Hours' has 'Subtract(-)' and '1' in the input field, 'Overtime' has 'Add(+)' and '05:00' in the input field, and 'Shift Allowance' has 'Select'. The 'Remark' field is empty.

7. Click **Save**  to save the adjustment. The saved record will appear under the **Previous Adjustment Records** collapsible panel.

Attendance Correction

Attendance corrections are required in the event of modifications being needed in the entry or exit times posted in the daily attendance data of users, or if new entry or exit data for a user is needed to be entered for a particular date manually. This feature is often useful for HR users in rectifying reported issues of missing or forgotten punches.

Attendance correction can be executed by — “[System Admin](#)” or an “[On Behalf Account User](#)”.

The System Admin can modify the attendance time as well as assign Special functions for the user in the same application.

The On Behalf Account User can modify the attendance time as well as the Short Leave IN/Out time. For this two separate applications need to be made. Refer “[Attendance Correction Application](#)” and “[Short Leave/Official IN-OUT Application](#)”.

To create and assign roles and rights to the System Admin User or On Behalf Account User, refer to “[Managing System Accounts](#)”.

System Admin

To correct employee attendance manually,

Select the **Time and Attendance module > Utilities > Attendance Correction**.

The **Attendance Correction** page will open as follows:

Date	Shift	1st Half	2nd Half	First IN	Last OUT	Work Hours
No Data						

User: Select a User from the user selection picklist whose attendance correction is to be done. The selected user's attendance data for the last attendance period will be loaded in the right side grid.

The Attendance Correction window displays the following fields and data:

- User:** 2, Chirag
- Attendance Date:** Date (calendar icon), Custom Months, 1
- Shift/Day:** GS, Normal
- Attendance Status:** (empty)
- Manual Status Marking:** None
- Status Summary:** (empty)
- Remark:** (empty)
- Events:** (button)
- Attendance Correction:** (button)
- Break Punches:** (button)
- Attendance Details:** (button)

Date	Shift	1st Half	2nd Half	First IN	Last OUT	Work Hours
08/02/2017	GS	PR	AB	08:45	17:00	07:15
06/02/2017	GS	AB	AB			
04/02/2017	GS	AB	AB	09:00	16:00	06:00
02/02/2017	GS	AB	PR	09:45	19:00	08:15
01/02/2017	GS	AB	AB			

Attendance Date: Select the date from the calendar button or select the date from the right grid for which manual correction is to be done.

By default, attendance correction for the selected user will be allowed for any date within the last attendance period. However, to change this, click the *Set Modification Allowed Selection* button to define a period within which attendance correction should be allowed. You can select custom period of week or months by selecting the required option.

The Set Modification Allowed Selection dropdown menu is open, showing the following options:

- 1 Week
- 2 Week
- Current Month
- Previous Month
- Custom Months

Click the **Events** button to view all attendance punches for the selected user on the selected date. The Attendance punches along with location is shown as below.

The All Attendance Punches window displays the following data:

Date	Time	ID Type	Device Name	Special Function	Access	Source/Location	Job Details	View Image
14/03/2022	14:17	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	14:23	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	14:34	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	14:34	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:03	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:12	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:22	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:22	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:26	In	Regular - IN		Allowed	ESS		
14/03/2022	15:26	In	ARGO FACE-Device-2		Denied	Device		
14/03/2022	15:26	In	ARGO FACE-Device-2		Allowed	Device	J1 - Job1	
14/03/2022	15:46	In	ARGO FACE-Device-2		Allowed	Device	J1 - Job1	
14/03/2022	15:50	In	ARGO FACE-Device-2		Allowed	Device	J1 - Job1	
14/03/2022	15:54	In	ARGO FACE-Device-2		Allowed	Device	J1 - Job1	



If Map is not loaded; check the network connection of your PC or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

In the following example, the user's attendance status for the selected date is "AB" (absent) for the second half, and is to be marked present.

Date	Shift	1st Half	2nd Half	First IN	Last OUT	Work Hours
08/02/2017	GS	PR	AB	08:45	17:00	07:15
06/02/2017	GS	AB	AB			
04/02/2017	GS	PR	AB	09:00	16:00	06:00
02/02/2017	GS	AB	PR	09:45	19:00	08:15
01/02/2017	GS	AB	AB			

Change the **Shift/Day** marking and **Manual Status Marking**, if required.

Manual Status Marking has following options:



For a particular user, if **Restrict Half Day Considerations** is enabled in the page User > User configuration > T&A, then in **Manual Status Marking** drop down list, only full day attendance options will be visible and all the other half day options will be restricted for that particular user as shown in the screen below.

You have to add a **Remark** to the application in the respective field.

Attendance Correction/Special Functions

Expand the Attendance Correction panel to manually enter/edit the IN and OUT punch timings as required in the **Time** field.

You can also specify a **Special Function** such as a *Short Leave IN*, *Early-OUT Allowed* etc. to mark the entry or exit. An IN/OUT Reason can be selected if required.

The screenshot shows the 'Attendance Correction' window. It has two main sections: '1 IN' and '2 OUT'.
Section 1 (IN):
- Date: 04/02/2017
- Time: 09:00
- Sp. Function: Select
- In Reason: Select
Section 2 (OUT):
- Date: 04/02/2017
- Time: 18:30
- Sp. Function: Select
- Out Reason: Select

The punch correction will be authorized automatically if it is done by system administrator.

Example:

Consider a user having following attendance correction for 03/08/2019(Week-Off) and 04/08/2019(Week-Off) on special function selected as Official Work Hour and Short Leave respectively. The punches are corrected as shown below:

For 03/08/2019:

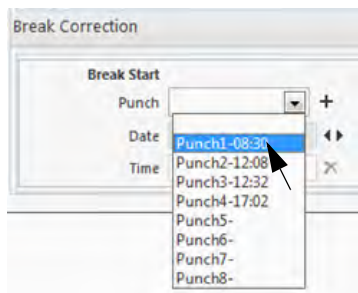
The screenshot shows the 'Attendance Correction' window for 03/08/2019.
Section 1 (IN):
- Date: 03/08/2019
- Time: 11:00
- Sp. Function: Official IN
- In Reason: Select
Section 2 (OUT):
- Date: 03/08/2019
- Time: 15:00
- Sp. Function: Official OUT
- Out Reason: Select

For 04/08/2019:

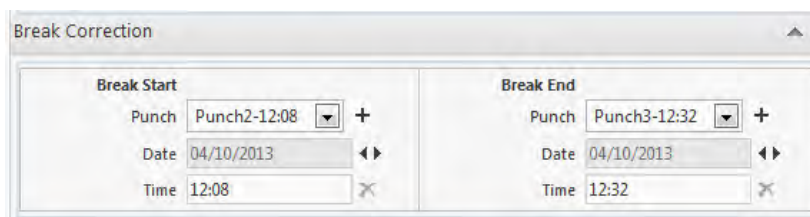
The screenshot shows the 'Attendance Correction' window for 04/08/2019.
Section 1 (IN):
- Date: 04/08/2019
- Time: 10:00
- Sp. Function: ShortLeave IN
- In Reason: Select
Section 2 (OUT):
- Date: 04/08/2019
- Time: 17:30
- Sp. Function: ShortLeave OUT
- Out Reason: Select

Break Punches

Expand the **Break Correction** panel to manually edit/enter punch timings for Break Start and Break End. To do this select an existing punch from the **Break Start** dropdown list as shown.

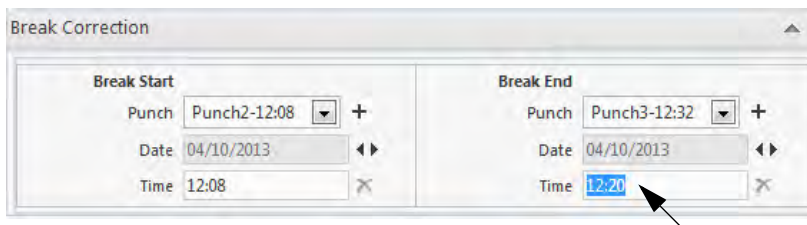


The next available punch will automatically be selected as the **Break End** punch (vice versa, when editing the Break End punch timing i.e. the previous available punch is selected for Break Start).



If no punch is available before or after the selected punch, a new punch can be created by manually entering the punch timing.


1. Enter/Edit the selected punch timing as shown.



For N punch user, break punch correction is done from All Punches window from Attendance Correction.

2. Click **Save**  to successfully update the manual corrections on the system.

Attendance Details

Expand the **Attendance Details** panel to view details such as the user's Work Hours, Break Hours, Authorized Overtime Hours etc. for the selected date. Select the  button to view additional details.



Authorized Overtime = Authorized OT + Manual Credit OT - Manual Debit OT

Now let us see an example to understand how punch posting works when Break and Short Leave/Official Hours are taken consecutively,

Consider Shift Start = 09:00, Shift End = 18:30, Break Start = 13:00 and Break End = 13:50 , Break Deduction Type is set as Actual Break Duration. Short Leave Authorization is required.

Punch1	Punch2	Punch3	Punch4
09:00	12:00 Short leave Out	14:00 Break End	19:00
	Application with 'Short Leave Start' as 12:00 and 'Short Leave End' as 13:00 (Configured Break Start) is created.	When punch of 14:00 arrives, a new application with Short Leave start as 12:00 and Short Leave end as 14:00 will be sent. Also the punch at 12:00 is copied at Break start field. Hence the break hours are calculated as per the configurations.	

Break Details	Punch1	Punch2	Punch3	Punch4	Break duration	Short leave duration
Break deviation is allowed	09:00	12:00 Short leave Out	13:50 Break End	19:00	00:50 (From 13:00 to 13:50)	01:00 (From 12:00 to 13:00)
Break deviation is not allowed	09:00	12:00 Short leave Out	13:30 Break End	19:00	00:30 (From 13:00 to 13:30)	01:00 (From 12:00 to 13:00)



If the Applied duration (End time of short leave - Start of short leave) is greater than the maximum limit of short leave or less than the Minimum limit of short leave then Posted duration will be 00:00 hours.

Suppose the range of short leave is 00:01 to 00:90 hours.

Punch1	Punch2	Punch3	Punch4	Applied Duration	Posted Duration
09:00	13:00	13:30	16:00 Short leave Out	02:30	00:00 (As 02:30 00:90)



If the Grace in Shift Late-IN is allowed then the grace duration will be added to the short leave duration provided the total short leave duration does not exceed the maximum range of short leave allowed.

Suppose the grace for Late-IN is 30 minutes. Short leave duration is of 90 minutes.

Punch1	Punch2	Punch3	Punch4	Short leave duration
09:30 (30 minutes from shift start)	13:00	13:30	17:30 Short leave Out (60 minutes before the shift ends)	00:90 (30 minutes + 60 minutes)

Case1: If the Punch1 is at 09:40 then it will not be added to the short leave duration.

Case2: If the Punch4 is at 17:00 then 90 minutes of short leave is utilized so no more addition of 30 minutes of grace.

On Behalf Account User

Attendance Correction Application

To correct the attendance manually for the desired user,

Select the **Time and Attendance module > Utilities > Attendance Correction**.



Attendance Corrections application restrictions will be applicable as configured in the Attendance Policy. To know more refer to. [“Attendance Correction-Short Leave/Official Hours Application Restrictions”](#)

The **Attendance Correction** page will open as follows:

Date	Shift	1st Half	2nd Half	First IN	Last OUT	Work Hours
08/10/2021		AB	AS			
07/10/2021		AB	AB			
06/10/2021		AB	AB			
05/10/2021		AB	AS			

User: Select a User from the user selection picklist whose attendance correction is to be done. The selected user's attendance data for the last attendance period will be loaded in the right side grid.

Attendance Date: Select the date from the calendar button or select the date from the right grid for which manual correction is to be done.

By default, attendance correction for the selected user will be allowed for any date within the last attendance period. However, to change this, click the *Set Modification Allowed Selection* button to define a period within which attendance correction should be allowed. You can select custom period of week or months by selecting the required option.

Change the **Shift/Day** marking, if required.

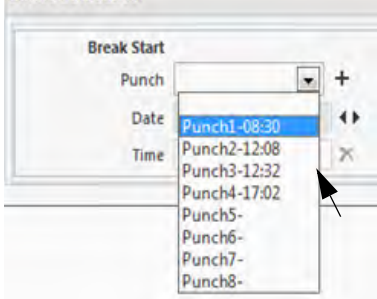
You have to add a **Remark** to the application in the respective field.

Click to expand the **Attendance Correction** collapsible panel to manually enter/edit the IN and OUT punch timings as required in the **Time** field.

The correction application will be sent to the RIC or will be authorized automatically, depending on the rights assigned to the On Behalf Account User. For more details refer [“On Behalf System Account User”](#)

Break Punches

Click to expand the **Break Correction** collapsible panel to manually edit/enter punch timings for Break Start and Break End. To do this select an existing punch from the **Break Start** dropdown list as shown.




The next available punch will automatically be selected as the **Break End** punch (vice versa, when editing the Break End punch timing i.e. the previous available punch is selected for Break Start).

A screenshot of a 'Break Patches' panel. It is divided into two columns: 'Break Start' and 'Break End'. Each column has a 'Punch' dropdown menu, a 'Date' field, and a 'Time' field. The 'Punch' dropdowns are set to 'New Punch'. The 'Date' fields are set to '08/10/2021'. The 'Time' fields are empty, with a placeholder 'HH:MM'.


If no punch is available before or after the selected punch, a new punch can be created by manually, by clicking **Add** or selecting the **New Punch** option and then entering the punch timing.

Enter/Edit the selected punch timing as shown.

A screenshot of the 'Break Patches' panel, similar to the previous one, but with the 'Time' fields filled in. The 'Break Start' 'Time' field contains '12:00' and the 'Break End' 'Time' field contains '12:30'. Both fields are highlighted with a blue border.

Click **Save**  to successfully update the manual corrections on the system.

Attendance Details

Expand the **Attendance Details** panel to view details such as the user's Work Hours, Break Hours, Authorized Overtime Hours etc. for the selected date. Select the  button to view additional details.

Attendance Details

Work Hours	06:00	
Break Hours	01:00	
Authorized Overtime	HHMM	
Net Work Hours	HHMM	
Adjusted Work Hours	0	
Early-IN Duration	HHMM	
Late-IN Duration	HHMM	
Early-OUT Duration	HHMM	
Overstay Duration	HHMM	
Extra Work Duration	HHMM	



Authorized Overtime = Authorized OT + Manual Credit OT - Manual Debit OT

To view the status of the application, click the **Application Details** tab in the right grid.

Attendance Correction

User: 3807 SR

Attendance Date: 01/10/2021

Application Date: 01/10/2021

Attendance Values: Actual

Status: Select

Shift/Day: Normal

Attendance Status:

Status Summary:

Remark:

Reason: 100 hours

Attendance Detail

Application Date	Attendance Date	1st Half	2nd Half	Status	Approval Details
20/10/2021	07/10/2021	AB	AB		

Short Leave/Official IN-OUT Application

To apply for Short Leave/Official IN-OUT Application manually for the desired user,

Select the **Time and Attendance module > Utilities > Short Leave/Official IN-OUT Entry**

The **Short Leave/Official IN-OUT Entry** page will open as follows:

Date	Shift	1st Half	2nd Half	First IN	Last OUT	Work Hours
08/10/2021	AB	AB		10:58	11:46	00:48
07/10/2021	AB	AB		14:47	18:25	03:38

User: Select a User from the user selection picklist whose Short Leave/Official IN-OUT Application is to be done. The selected user's data for the last attendance period will be loaded in the right side grid.

Attendance Date: Select the date from the calendar button or select the date from the right grid for which manual correction is to be done.

By default, Short Leave/Official IN-OUT for the selected user will be allowed for any date within the last attendance period. However, to change this, click the *Set Modification Allowed Selection* button to define a period within which correction should be allowed. You can select custom period of week or months by selecting the required option.

Click to expand the **Short Leave/Official Hours Entry** collapsible panel.

Under **IN/ OUT**, select the desired **Special Function** — *Short Leave IN, Official IN or Short Leave-OUT Official-OUT* to mark the entry or exit.

If required, you can enter the **Reason**. To do so, click **Edit** and enter the reason.

The correction application will be sent to the RIC or will be authorized automatically, depending on the rights assigned to the On Behalf Account User. For more details refer "[On Behalf System Account User](#)"

Attendance Details

Expand the **Attendance Details** panel to view details such as the user's Work Hours, Break Hours, Authorized Overtime Hours etc. for the selected date. Select the button to view additional details.

Attendance Details

Work Hours	06:00	
Break Hours	01:00	
Authorized Overtime	HHMM	
Net Work Hours	HHMM	
Adjusted Work Hours	0	
Early-IN Duration	HHMM	
Late-IN Duration	HHMM	
Early-OUT Duration	HHMM	
Overstay Duration	HHMM	
Extra Work Duration	HHMM	



Authorized Overtime = Authorized OT + Manual Credit OT - Manual Debit OT

Click **Save**  to successfully update the corrections on the system.

To view the status of the application, click the **Application Summary** collapsible panel.

Short Leave/Official IN-OUT Entry

User

2807

SR

Attendance Date

08/10/2021

Shift/Day

GS

Normal

Attendance Status

AB

AB

Status Summary

AB Early-OUT

Events

Short Leave/Official Hours Entry

Attendance Details

Application Summary

Search

Start	End	Applied Duration	Posted Duration	Special Function	Status	Details
09:00	10:58	01:58	00:00	Short Leave	Approved	

Available Short Leave (Oct)

Date	Shift	1st Half	2nd Half	First IN	Last OUT	Work Hours
08/10/2021	GS	AB	AB	10:58	11:46	00:48
07/10/2021	GS	AB	AB	14:47	19:25	03:38

Manual Status Correction

The *Manual Status Correction* functionality is applicable when the attendance status of multiple users is to be updated simultaneously for a selected date range. This allows the administrator to make uniform status changes (e.g. To mark all users “present”) for the same dates and apply it to all or selected users on COSEC.

To perform Manual Status Correction, Select the **Time and Attendance module >Utilities > Manual Status Correction**.

The page will open as follows:

The screenshot shows the 'Manual Status Correction' web application interface. At the top, there are date selection fields for 'Date' (13/09/2020 to 13/09/2020), a 'Manual Status Marking' dropdown menu set to 'Full Day Present', and a 'Remark' text field containing 'Marked Status Manually'. Below these is the 'User Selection' section, which includes a 'Select Users' dropdown menu set to 'User Wise', a 'User' search bar, and a table of users. The table has columns for 'User ID', 'Name', and a delete icon. The users listed are: 1 (Athira), 10 (Utsok), 11 (Raj), 2 (Rushi), and 3 (Vipul). At the bottom of the table, it says '1 - 5 of 10 records'. A 'Process' button is located at the bottom center of the interface.

User ID	Name
1	Athira
10	Utsok
11	Raj
2	Rushi
3	Vipul

Date: Select a date range for the Manual Status Correction of selected users.

Manual Status Marking: Select a Manual Status Marking option depending upon the new status to be applied for the users.

Remark: Add a **Remark** while marking the status correction.

Select Users: Select the user by filtering the option of **User Wise**, **Group Wise** or **All** for whom the status correction is to be applied.

Click the **Process** button. The status for all selected users will be updated once the processing is complete. In the figure below, all the selected users will be marked **Full Day Present**.

Manual Status Correction

Date: 13/09/2020 13/09/2020

Manual Status Marking: Full Day Present

Remark: Marked Status Manually

User Selection

Select Users: User Wise

User: ID Name

Processing User - 8 [100%]

Cancel

1 - 5 of 10 records

Process

Error List

The status for the user will be marked as PR as shown below:

Daily Attendance View

User: 1 Shalini

Attendance Period: May 2017

Date	Shift	First IN	Last OUT	1st Half	2nd Half	Late-IN	Early-OUT	Work Hours	Extra Work	Net Work Hours	Break Hours	Actual Overtime	Authorized Overtime	Remark	Details
01/05/2017	GS			PR	PR										
02/05/2017	GS			PR	PR										
03/05/2017	GS			PR	PR										
04/05/2017	GS			PR	PR										
05/05/2017	GS			PR	PR										
06/05/2017	GS			PR	PR										
07/05/2017	GS - WO			--	--										
08/05/2017	GS			PR	PR										
09/05/2017	GS			PR	PR										
10/05/2017	GS			PR	PR										
11/05/2017	GS			PR	PR										
12/05/2017	GS			--	--										
13/05/2017	GS			--	--										
14/05/2017	GS - WO														

Mark Group Attendance

The Mark Group Attendance page allows the SA to mark the attendance of group of people in a single go.

SA can upload group images of users and the system will recognize each user from the image and then it will mark their attendance automatically.

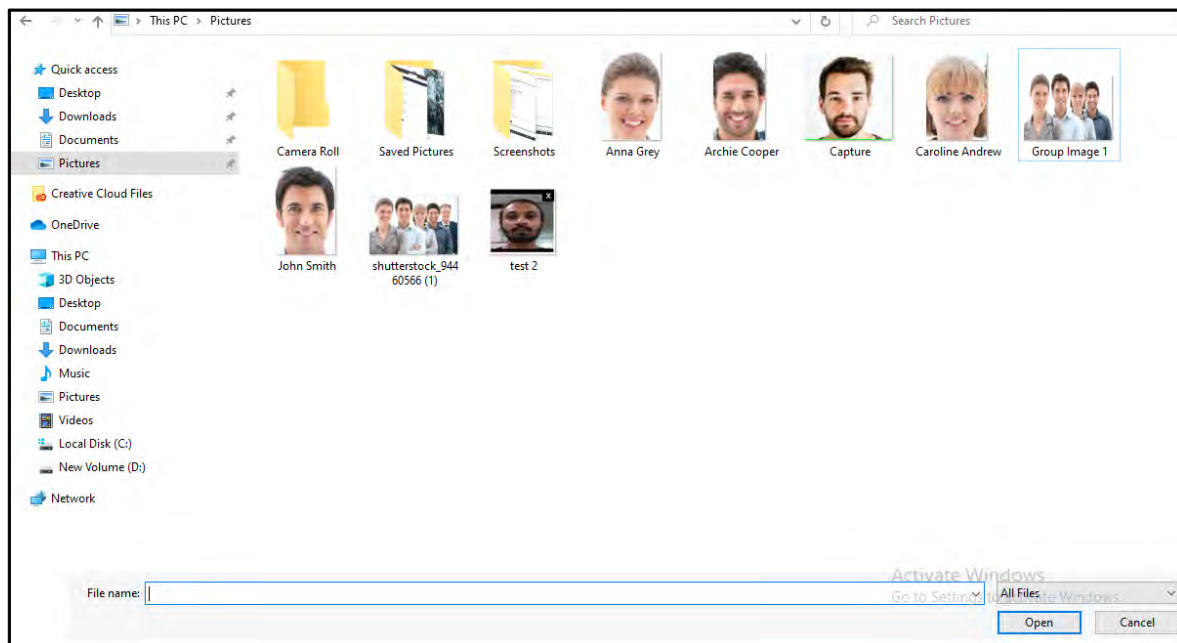


For Group FR ("[Mark Group Attendance](#)") and Exceptional Face Enrollment feature to work, ensure that the desired Identification Service is selected in COSEC Admin > License and Service. For more details refer Admin Management Portal User Manual.

To perform Mark Group Attendance, select the **Time and Attendance module > Utilities > Mark Group Attendance** and the following page appears:

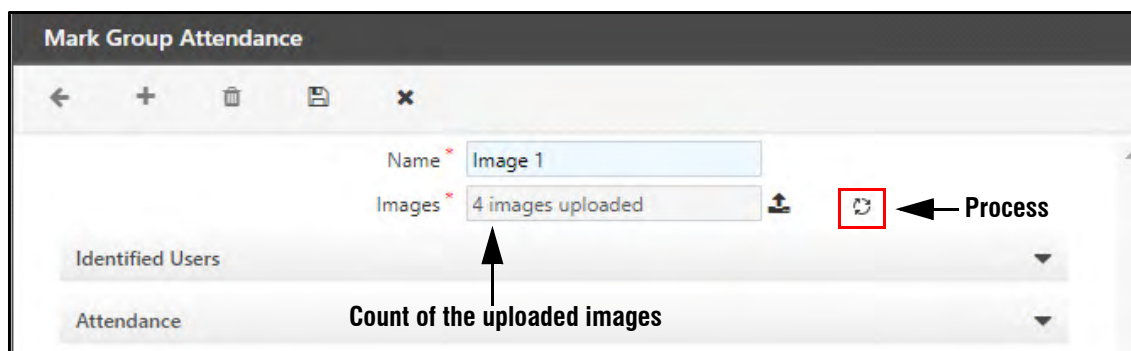
Click **Add** to upload a new group image and configure the following parameters:

- **Name:** Enter the desired **Name**.
- **Images:** To upload group image/s of users, click **Upload File**  and the dialog box appears as shown below.



Now select the desired image/s. Here, the image format supported are .jpg, and the size of a single image must be a maximum of 15 MB.


You can upload maximum of 20 photos at a time. The text box displays the count of the uploaded images.




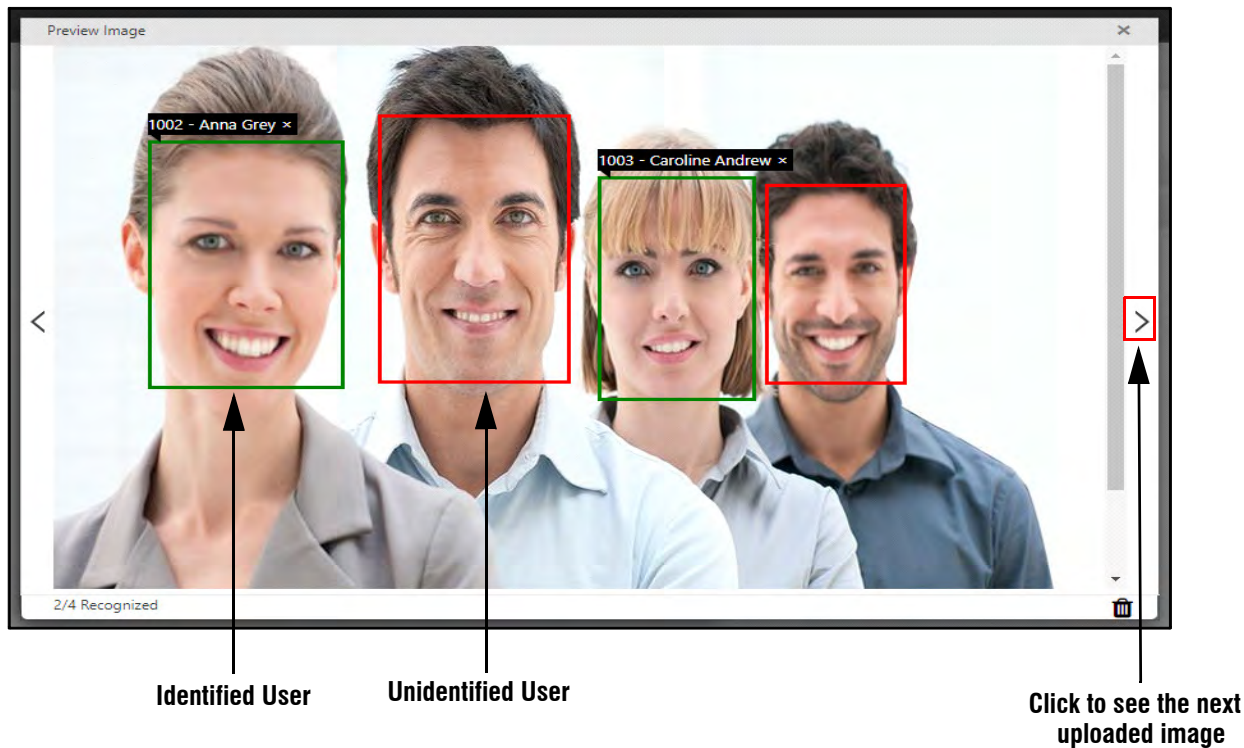
Once you upload the image/s, **Process**  icon will be visible.

Click **Process** to perform the Face Recognition (FR) process on the uploaded image/s.

Once the FR process is successfully performed on these images, the list of recognized users will be added and displayed in the **Identified Users** list. For more information, refer ["Identified Users"](#).

After the FR process, the **Preview**  icon will be visible which will allow you to preview the uploaded group image/s.

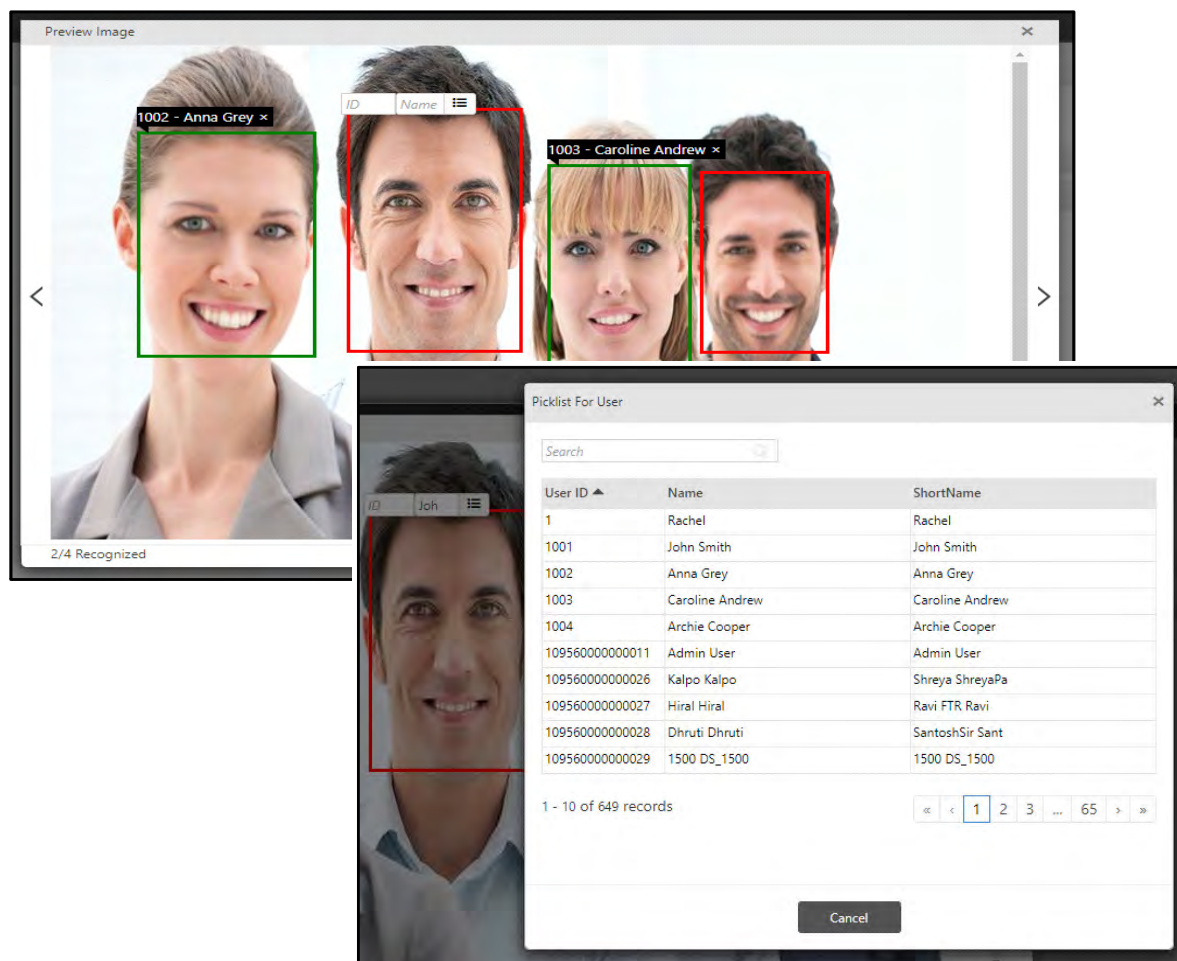
Click **Preview**  icon and the **Preview Image** window appears with the uploaded image/s as shown below.



The faces identified by the system will have a green frame with a name and ID tag mentioned.

Now, there can be few faces in the group image/s which are not identified by the system. Such faces will have a red frame. You can manually tag the name against such faces of the users from the **Preview Image** window.

To manually tag the names against the faces of the users, click on the red frame and a user picklist will be displayed as shown below.

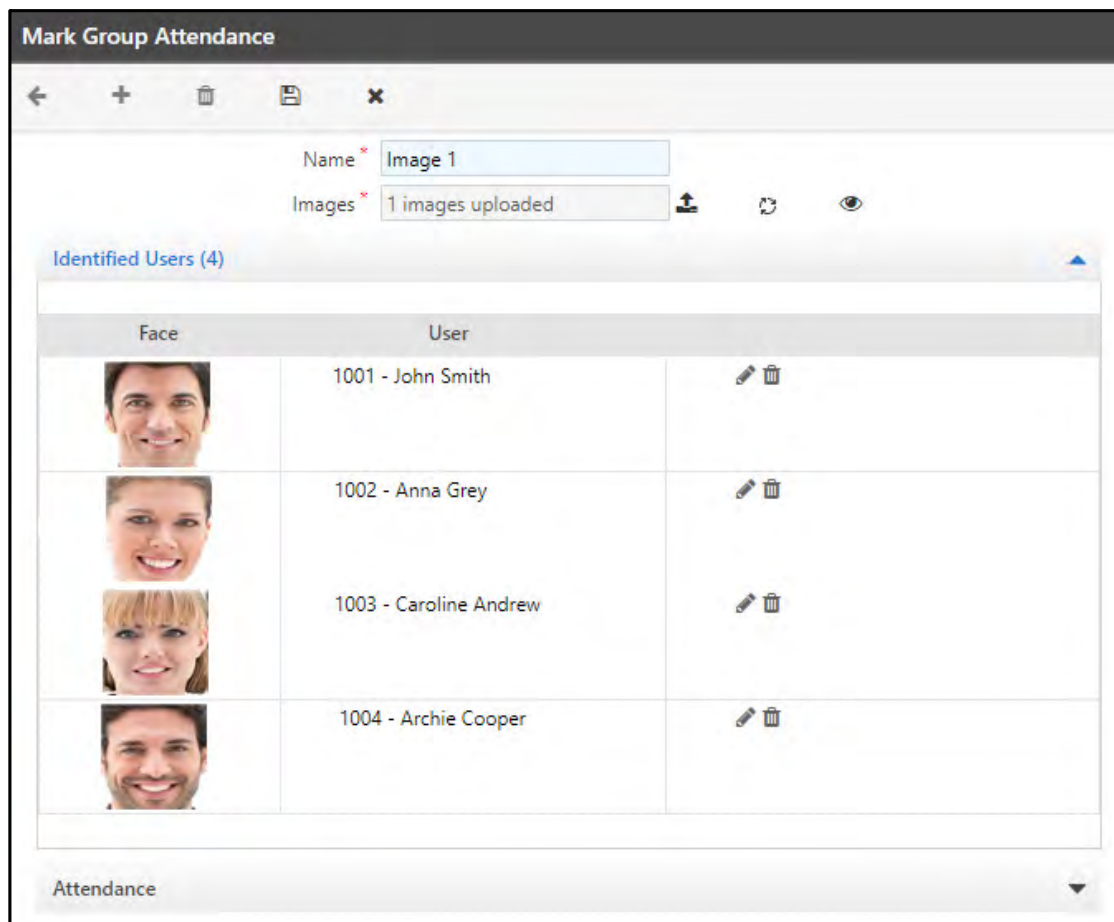



Select the respective user name from the picklist or manually enter the user name/ID.

Then these faces will be added to the **Identified Users** list along with the system identified users.

Identified Users

- It displays the list of the identified users after the FR Process. For SA, all recognized users will be displayed in this list.



- Identified Users include system recognized users as well as manually tagged users from the photos.
- Attendance will be marked for only those users that are displayed in this list.
- Single face of the user will be displayed in the grid along with the User's ID and Name for SA to authenticate the list.
- You can also edit the user name against the faces of users available in the image. To edit, click **Edit**  icon.





Mark Group Attendance

← + 🗑️ 📁 ✕

Name *

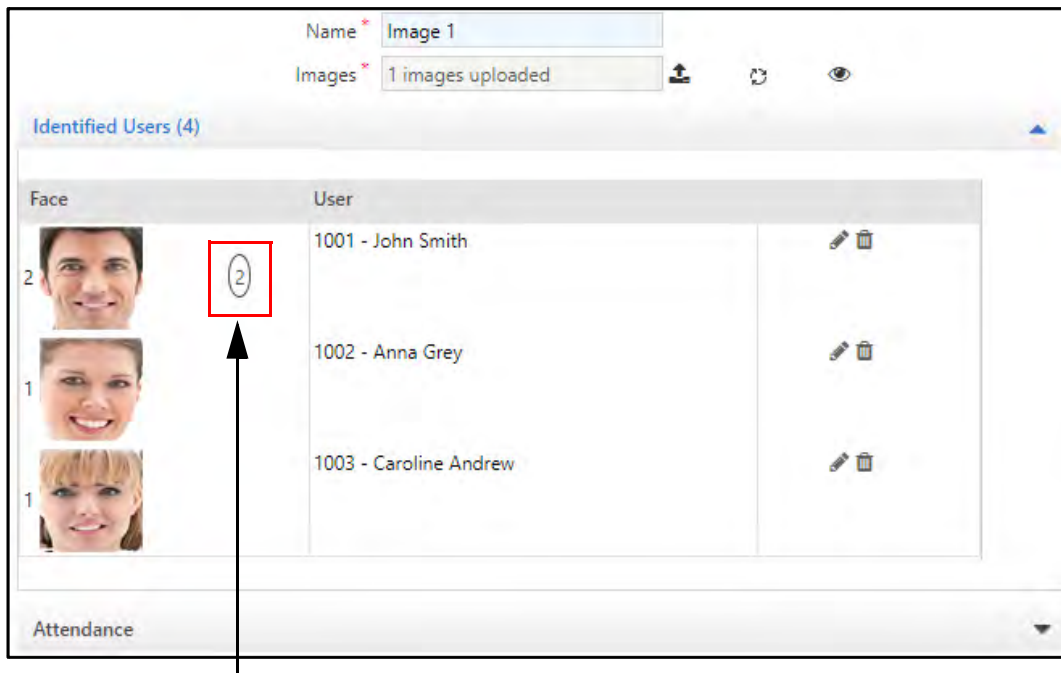
Images * 📁 ↺ 👁️

Identified Users (4) ▲

Face	User	
	<input type="text" value="1001"/> <input type="text" value="John Smith"/> 📄	✓ ✕
	1002 - Anna Grey	✎ 🗑️
	1003 - Caroline Andrew	✎ 🗑️
	1004 - Archie Cooper	✎ 🗑️

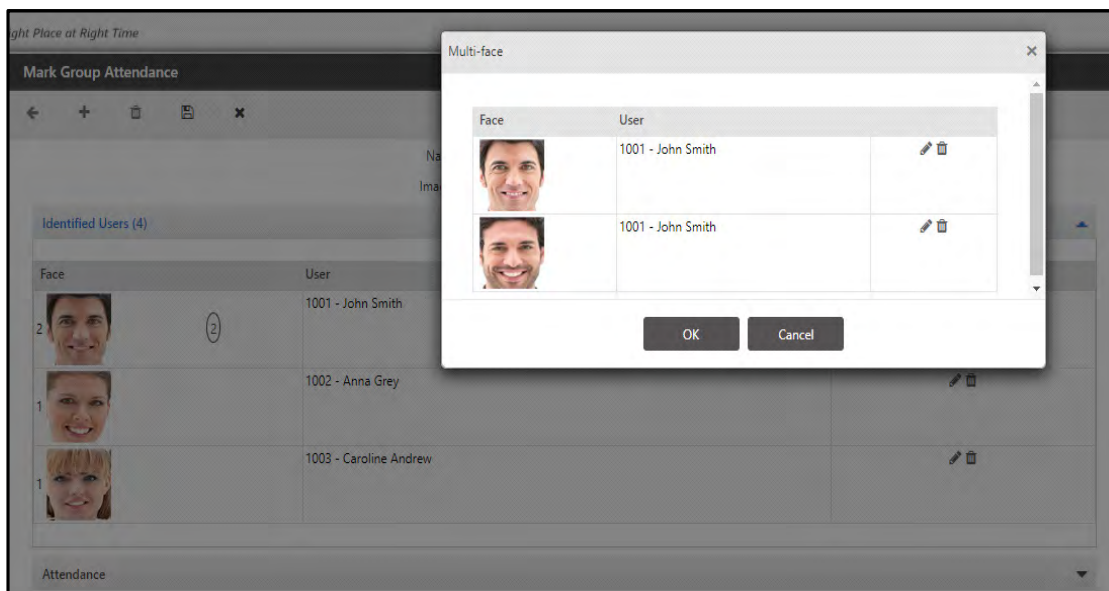
Attendance ▼




- Select the respective user name from the picklist again or manually enter the desired user name/ID. Then click **OK** ✓. To discard, click **Cancel** ✕.
- If multiple faces of the same user are identified, then only single face will be displayed in the grid and the number of faces identified will be displayed as shown below.




Number of faces identified of a single user

- To view other identified faces of the same user, click on the numeric value of the identified faces of the user.
- Multi-face** window appears where you will be able to view more images of that user.




- You can also edit the user name against the faces in case of false identification. To edit, click **Edit** .
- Select the respective user name from the picklist again or manually enter the desired user name/ID. Then click **OK** . To discard, click **Cancel** .

- If same user is tagged against multiple faces, then entry of those faces will be merged and displayed as a single entry in the grid.
- To delete any entry of the identified user from the list, click **Delete** .

When any entry is deleted from the list, then the user tagged against that face will be untagged and that face will be considered as detected but not recognized.

Attendance

To mark the attendance of the users in the group:

- Make sure there are one or more entries in the **Identified User** list to configure **Attendance**.
- Enter the desired **Date** and **Time** for which the attendance of the user is to be marked.
- Select the desired **Event** from the options — IN Punch or Out Punch.
- Select the desired **Special Function**.
- Select the desired **Location Selection** from the options — Configured Location or Custom.
 - If **Location Selection** is selected as Configured Location, then select the desired configured **Location** from the picklist.
 - If **Location Selection** is selected as Custom, then enter the Latitude/Longitude co-ordinates or click on the  icon and select the location manually.
- Enter the desired **Remark** for marking the attendance for the user.
- Click on the **Save** button. Once saved SA will be able to view the added entry but will not be allowed to edit the entry.
- SA can delete a group attendance entry by clicking on the **Delete**.
- On delete, images uploaded and Identified User list should be cleared for database.

Manage Attendance

This page allows admin to handle single as well as multiple users' attendance efficiently. It allows various provisions like changing shift, applying leave/ tour/ c-off, marking status manually and regularizing user's attendance automatically. Also you can do editing of Punches, viewing users' count based on filtering of exceptions and applying latest changes to other user's records.

Go to **T&A module> Utilities> Manage Attendance**. The Manage Attendance page is shown as below.

The screenshot shows the 'Manage Attendance' interface. It includes a title bar, navigation icons, and two input fields for 'Date' (01/10/2016 to 05/10/2016) and 'User' (3, Nilam). A 'View' button is located below the user selection.

Date: Select the From and To Date to view the attendance data for the selected date range.

User: Select the user from the picklist for whom the attendance data is to be viewed and managed.

Click the **View** button to view the attendance data in the grid. The user punches for the selected date are shown in the grid. When a single user is selected, the Attendance summary is displayed on the right side as shown below.

The screenshot shows the 'Manage Attendance' interface with the 'View' button clicked. It displays a table of attendance data for user Nilam from 01/10/2016 to 07/10/2016. The table shows User ID 3, User Name Nilam, and attendance status (PR, PR, PR, PR, AB, PR) for the respective days. To the right, an 'Attendance Summary For 01/10/2016 - 05/10/2016' is shown, including Present (3.5), Absent (0.5), Leave (0), Tour (0), Week-Off (0), Holiday (0), Field Break (0), Rest Day (0), Work Hours (00:00), Extra Work (00:00), Net Work Hours (00:00), Break Hours (00:00), Authorized Overtime (00:00), and Generated Overtime (07:30).

User ID	User Name	01-Oct Sat	02-Oct Sun	03-Oct Mon	04-Oct Tue	05-Oct Wed	06-Oct Thu	07-Oct Fri
3	Nilam	PR PR		PR PR	PR PR	AB PR		

Attendance Summary For 01/10/2016 - 05/10/2016

3 - Nilam

- Present: 3.5
- Absent: 0.5
- Leave: 0
- Tour: 0
- Week-Off: 0
- Holiday: 0
- Field Break: 0
- Rest Day: 0
- Work Hours: 00:00
- Extra Work: 00:00
- Net Work Hours: 00:00
- Break Hours: 00:00
- Authorized Overtime: 00:00
- Generated Overtime: 07:30

Click on Filter  to select the multiple users based on Exceptions or Enterprise groups.

[See "Exception Selection" on page 1555.](#)

User Selection

For multiple user selection, the options are:

- **User wise:** Individual user can be selected from the picklist
- **Group wise:** Users can be selected based on the selection of enterprise group.
- **All:** All the active users can be selected.

More Filter

Exception Selection User Selection

Select Users User Wise

User* User Wise
Group Wise
All

Apply Cancel

More Filter

Exception Selection User Selection

Select Users User Wise

User* ID Name

Search

User ID	Name
3	Nilam
4	Shalini
5	Chirag

Apply Cancel

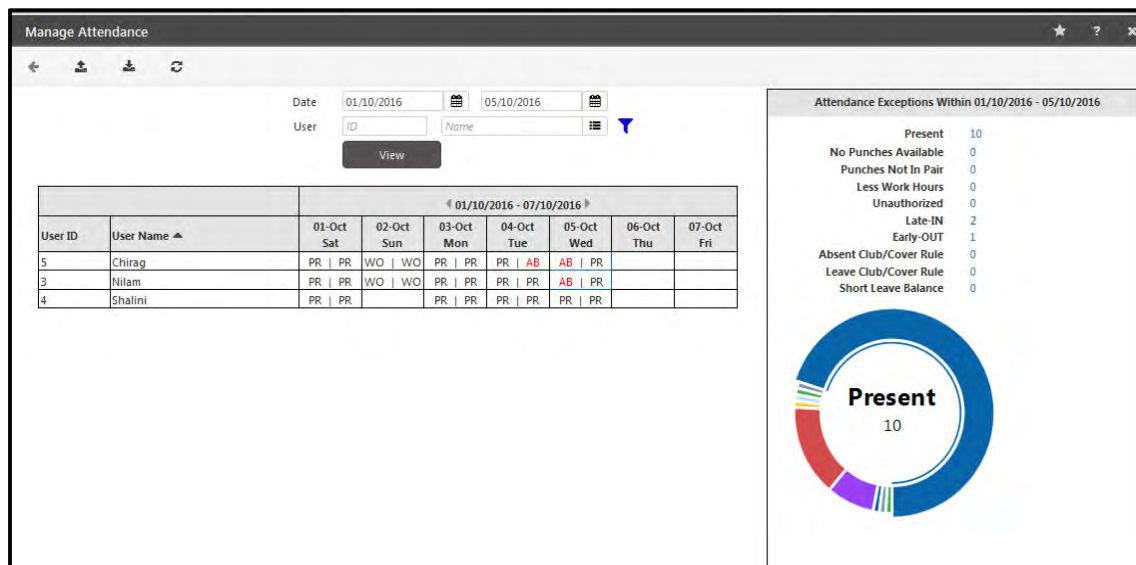
After **applying** the multiple user selection, click **View** button to view the attendance status of multiple user for selected date.

Date 01/10/2016 05/10/2016

User ID Name

View

When multiple users are selected, Count of users according to the configured exceptions and selected date-range is displayed on right side as shown below.



Exception Selection

Click the filter button to configure the exceptions to filter users based on those exceptions. Check the boxes from **Exception Selection** list as shown below as per which the users will be filtered. Now select the users from the **User Selection**. Then click **Apply** to save the selection. The users will be displayed based on configuration of exceptions.



The filter applied on Date and exceptions will appear on OR condition.

Eg: Suppose 5 users are selected from User selection but exceptions are available for only 3 users; then data for 3 users will be generated.

More Filter

Exception Selection | User Selection

Exception	Operator	Value (Min)	
<input type="checkbox"/> No Punches Available			
<input checked="" type="checkbox"/> Punches Not In Pair			
<input type="checkbox"/> Shift Not Available			
<input checked="" type="checkbox"/> AB:Late-IN	>	15	X
<input checked="" type="checkbox"/> AB:Early-OUT	>	5	X
<input type="checkbox"/> AB:Less Work Hrs			
<input type="checkbox"/> AB:Unauthorized			
<input type="checkbox"/> AB:Break Late-IN	>	0	X
<input type="checkbox"/> AB:Break Early-OUT	>	0	X
<input type="checkbox"/> WO-AB:Absent Club Rule			

1 - 10 of 27 records

1 2 3 >

Apply Cancel


Exceptions are those instances where the punch behavior of a user deviates from the expected organizational practice and requires a need for manual intervention by the HR administrator.

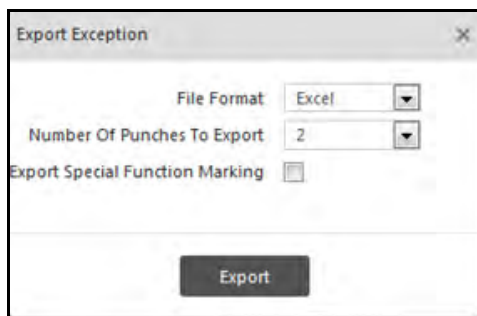
- For instance, absence of punches for a working day or a missing punch may be considered as an attendance exception. So if an employee forgets to punch IN/OUT on a particular working day and is marked absent for the whole day, the punches can be updated by the HR administrator by manual correction from “Manage Attendance”.
- For exceptions related to time eg: AB:Late-IN, the operator can be selected and minimum value can be specified; comparing which the exceptions will be generated. The exceptions can be exported in excel sheet which can be manually corrected and then the sheet can be imported.
 - Example: AB: Late-IN >15mins. The users who are marked Absent due to late-in of 15 mins or more within the selected date-range would be considered in exception.

Export & Import

The user can export the exception data in XLS format to the local drive of a computer. This data can then be manually corrected and updated on the system by importing the excel sheet.

Export

The data to be exported can be configured and selected from the “[Exception Selection](#)” filter. After selecting the exceptions, select the user from “[User Selection](#)” filter. Now click Export  button. The Export Exception page appears as shown below.



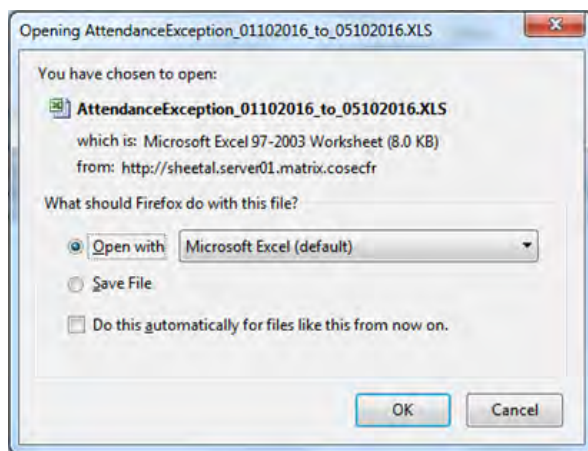
Select the file format as Excel, CSV or XLSX.

Select the **Number of Punches To Export** for each user using the drop-down list.

Select the **Export Special Function Marking** to export special Function IDs with Punches.

Click the **Export** button.

The following pop up window will appear prompting to open or save the file on a local drive.




After saving the file, click the download folder and open the file.

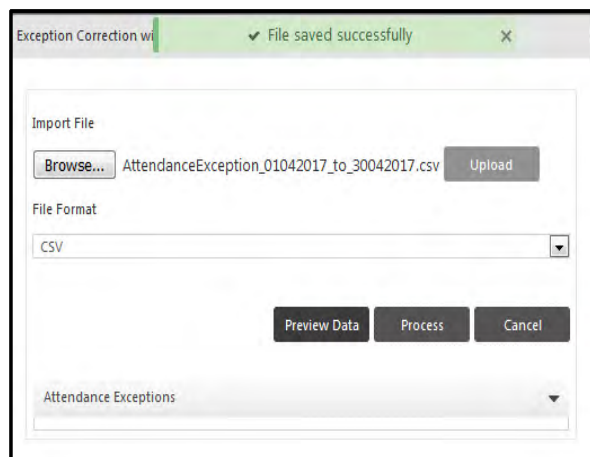
The exported exception file is shown as below.

A	B	C	D	E	F	G	H	I	J
Attendance Date	UserId	User Name	Shift	WO	PH	Punch1	Punch2	BreakStart	BreakEnd
04/10/2016	5	Chirag	GS	0	0	04/10/2016 09:00:00	04/10/2016 14:00:00		
05/10/2016	5	Chirag	GS	0	0	05/10/2016 14:00:00	05/10/2016 21:00:00		
05/10/2016	3	Nilam	GS	0	0	05/10/2016 13:45:00	05/10/2016 20:00:00		
01/10/2016	1	Rosy	GS	0	0	01/10/2016 09:45:00	01/10/2016 18:30:00		
05/10/2016	4	Shalini	GS	0	0	05/10/2016 09:30:00	05/10/2016 18:30:00		

Import

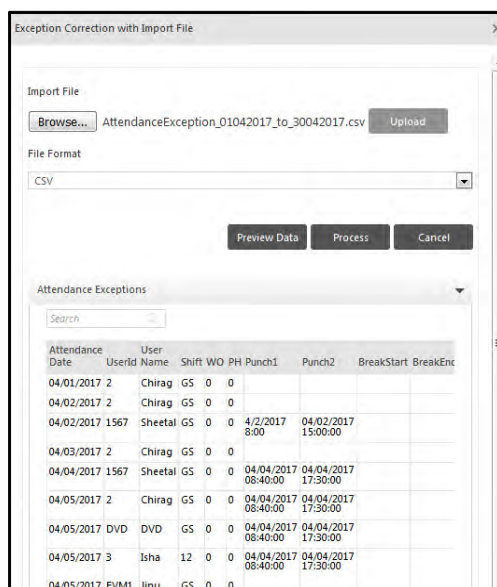
You can make the necessary manual corrections to the exported file. Save the file and note down the file location.

Click the **Import**  icon to import the exception file.



Browse the file and click **Upload** button to upload the manually corrected exception file.

Select a **File Format** (XLS or CSV) for uploading. You can preview the data by clicking **Preview Data** button. The changes made in data will be shown as below.



Attendance Date	User	UserId	Name	Shift	WO	PH	Punch1	Punch2	BreakStart	BreakEnd
04/01/2017	2	Chirag	GS	0	0					
04/02/2017	2	Chirag	GS	0	0					
04/02/2017	1567	Sheetal	GS	0	0	4/2/2017 8:00	04/02/2017 15:00:00			
04/03/2017	2	Chirag	GS	0	0					
04/04/2017	1567	Sheetal	GS	0	0	04/04/2017 08:40:00	04/04/2017 17:30:00			
04/05/2017	2	Chirag	GS	0	0	04/04/2017 08:40:00	04/04/2017 17:30:00			
04/05/2017	DVD	DVD	GS	0	0	04/04/2017 08:40:00	04/04/2017 17:30:00			
04/05/2017	3	Isha	12	0	0	04/04/2017 08:40:00	04/04/2017 17:30:00			
04/05/2017	FVM1	Jinu	GS	0	0					

Click **Process** button to process the imported data.

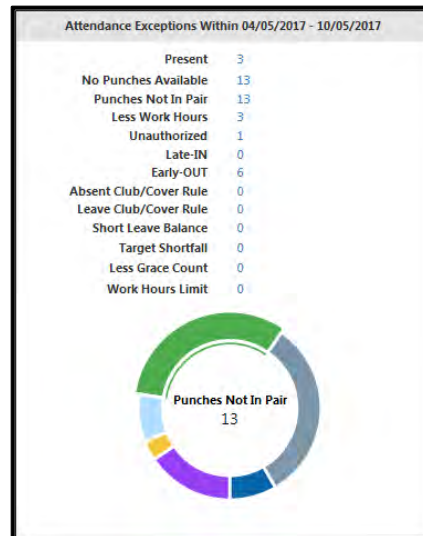
Managing Attendance and Exceptions

To view Attendance Exception count

Admin can filter out the selected users on the basis of applied exceptions.

Example: The exceptions for multiple users are selected as shown below. The updated Attendance Exception count will be displayed after clicking Refresh button as shown below.

Exception	Operator	Value (Min)
<input type="checkbox"/> No Punches Available		
<input type="checkbox"/> Punches Not In Pair		
<input type="checkbox"/> Shift Not Available		
<input checked="" type="checkbox"/> AB:Late-IN	=	0
<input checked="" type="checkbox"/> AB:Early-OUT	>	0
<input checked="" type="checkbox"/> AB:Less Work Hrs		
<input checked="" type="checkbox"/> AB:Unauthorized		
<input type="checkbox"/> AB:Break Late-IN	>	0
<input type="checkbox"/> AB:Break Early-OUT	>	0
<input type="checkbox"/> WO-AB:Absent Club Rule		




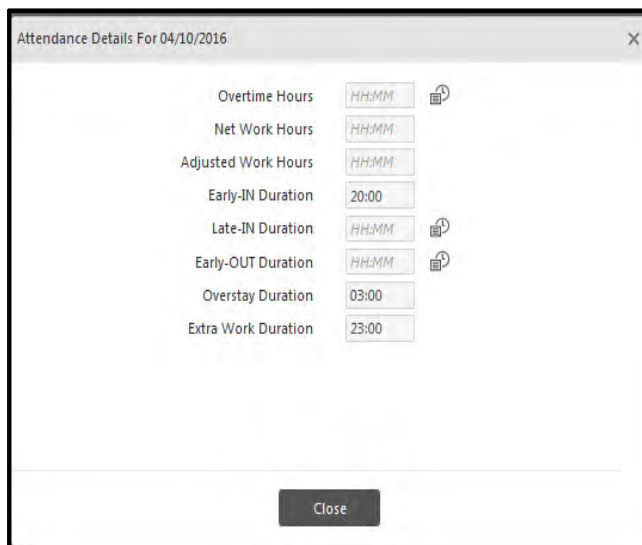
To view user's attendance summary

To view user's attendance summary for selected date-range by clicking on User ID.

The Attendance Details shows the Work hours, Break hours, Late duration, Early duration, Overtime details, Present, Absent, Leave, Tour, Week Off, Holiday, Field Break, Rest Day, Extra work, Net Work Hours.

Date	Time	Sp. Function	In Reason
03/10/2016	09:10	Select	Select

The **Attendance Details** can be viewed by clicking More Attendance Details icon 



Attendance Details For 04/10/2016

Overtime Hours

Net Work Hours

Adjusted Work Hours

Early-IN Duration

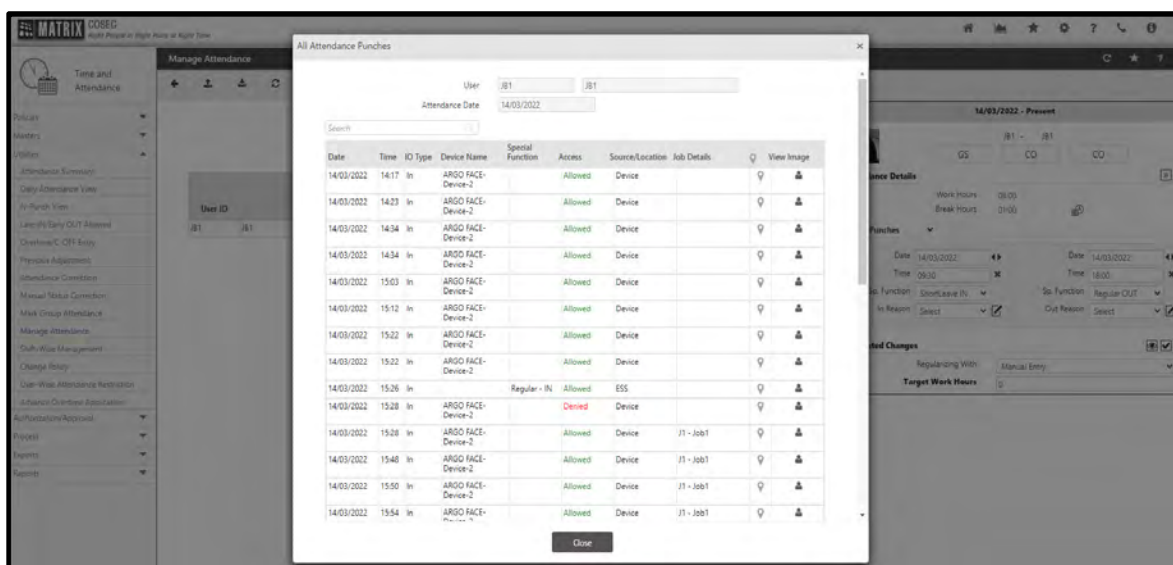
Late-IN Duration

Early-OUT Duration

Overstay Duration

Extra Work Duration

The **Attendance events** can be viewed by clicking 



The screenshot displays the Matrix COSEC System interface. On the left, the 'Manage Attendance' sidebar is visible. The main area shows the 'All Attendance Punches' window for user JB1 on 14/03/2022. The table lists attendance events with columns for Date, Time, ID Type, Device Name, Special Function, Access, Source/Location, Job Details, and View Image. The events are as follows:

Date	Time	ID Type	Device Name	Special Function	Access	Source/Location	Job Details	View Image
14/03/2022	14:17	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	14:23	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	14:34	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	14:34	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:03	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:12	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:22	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:22	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:26	In	ARGO FACE-Device-2	Regular - IN	Allowed	ESS		
14/03/2022	15:28	In	ARGO FACE-Device-2		Denied	Device		
14/03/2022	15:28	In	ARGO FACE-Device-2		Allowed	Device	J1 - Job1	
14/03/2022	15:48	In	ARGO FACE-Device-2		Allowed	Device	J1 - Job1	
14/03/2022	15:50	In	ARGO FACE-Device-2		Allowed	Device	J1 - Job1	
14/03/2022	15:54	In	ARGO FACE-Device-2		Allowed	Device	J1 - Job1	

On the right, the 'Attendance Details' window for 14/03/2022 - Present is shown, displaying Work Hours (08:05), Break Hours (01:00), and a list of punches with Start/End times and functions (Shift/Late IN, Shift/Late OUT, Regular IN, Regular OUT).



If Map is not loaded; check the network connection of your PC or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

The **Break hour** details can be viewed by clicking . The break start and break end is shown as below.

Break Hour Details Of 04/10/2016

Break Start: 13:00

Break End: 14:00

Break Hours: 01:00

Close

To do Attendance Correction

Selecting any date from user's daily attendance grid and correct it using available options.

- **Change Shift:**

If no shift has been assigned to the user then you can assign the shift. You can change and assign another shift. Also WO/Holiday can be assigned on the selected day.

Click on the shift to be changed as shown below. The **Change Shift** pop up appears. Click the picklist and select the shift to be replaced.

06/10/2016 - No Punches Available

4 - Shalini

NS AB AB

Change Shift

Shift: NS Night Shift

Week Off ☐

Holiday ☐

Apply Cancel

Picklist For Shift Masters

SFTID	SFTName	SFTSTTime	SFTEDTime	BRKSTTime	BRKEDTime
GS	General Shift	09:00	18:00	13:00	14:00
NS	Night Shift	21:00	05:00		

The GS shift is selected and Week Off is enabled as shown below. Click on Apply. The shift on 6/10/16 changes to GS-WO.

Change Shift

Shift: GS General Shift

Week Off ☒

Holiday ☐

Apply Cancel

06/10/2016 - No Punches Available

4 - Shalini

GS WO WO

Attendance Details

Work Hours

Break Hours

Actual Punches

- **Mark Manual Status:**

The user's attendance status for the selected date is "AB" (absent) for the first half, and is to be marked present.

01/10/2016 - 07/10/2016

03-Oct Mon	04-Oct Tue	05-Oct Wed	06-Oct Thu
PR PR	PR PR	AB PR	AB AB

AB:Late-IN

05/10/2016 - AB:Late-IN

3 - Nilam

GS AB PR

Attendance Details

Work Hours

Break Hours

Actual Punches

Manual Status Marking

None

Apply

Cancel

Click on AB and select the option **Mark Status Manually**. Now select the required option for **Manual Status Marking** from the drop down options. Here "First Half Present" is selected as shown below. Then click Apply.

05/10/2016 - AB:Late-IN

3 - Nilam

GS AB PR

Attendance Details

Manual Status Marking

None

Apply

None

First Half Absent

Second Half Absent

Full Day Absent

First Half Present

Second Half Present

Full Day Present

Absent-Present

Present-Absent

Actual Punches

Date 05/10/2016

Time 13:45

Sp. Function Select

In Reason Select

Out Reason Select

After the manual status is selected and applied, the punch status will be changed from AB to PR as shown below.

Manage Attendance

✓ Saved Successfully

Date 01/10/2016 07/10/2016

User 3 Nilam

View

User ID	User Name	01-Oct Sat	02-Oct Sun	03-Oct Mon	04-Oct Tue	05-Oct Wed	06-Oct Thu	07-Oct Fri
3	Nilam	PR PR	WO WO	PR PR	PR PR	PR PR	AB AB	AB AB

05/10/2016 - AB:Late-IN

3 - Nilam

GS PR PR

Attendance Details

Work Hours 06:15

Break Hours

Actual Punches

Date 05/10/2016

Time 13:45

Sp. Function Select

In Reason Select

Date 05/10/2016

Time 20:00

Sp. Function Select

Out Reason Select

Suggested Changes

Regularizing With Manual Entry

Target Work Hours 0



For a particular user, if **Restrict Half Day Considerations** is enabled in the page **User > User configuration > T&A**, then in **Manual Status Marking** drop down list, only full day attendance options will be visible and all the other half day options will be restricted for that particular user as shown in the screen below

07/08/2017 - No Punches Available

1687 - Aditi Gupta

DL AB AB

Manual Status Marking: None (selected), None, Full Day Absent, Full Day Present

Apply

Actual Punches

Date: 07/08/2017 Time: HH:MM Sp. Function: Select In Reason: Select

Date: 07/08/2017 Time: HH:MM Sp. Function: Select Out Reason: Select

- **Apply Leave/Tour/C-OFF**

The user's attendance status for the selected date is "AB" (absent), and is to be applied for full day leave. Click on AB and select the option **Apply Leave**.

		01/10/2016 - 07/10/2016						
User ID	User Name	01-Oct Sat	02-Oct Sun	03-Oct Mon	04-Oct Tue	05-Oct Wed	06-Oct Thu	07-Oct Fri
5	Chirag	PR PR	WO WO	PR PR	PR AB	AB PR	AB AB	AB AB

No Punches Available

Manage Attendance

Date: 01/10/2016 to 07/10/2016

User: 5 Chirag

View

User ID	User Name	01-Oct Sat	02-Oct Sun	03-Oct Mon	04-Oct Tue	05-Oct Wed	06-Oct Thu	07-Oct Fri
5	Chirag	PR PR	WO WO	PR PR	PR AB	AB PR	AB AB	AB AB

06/10/2016 - No Punches Available

5 - Chirag

NS AB AB

Attendance Details

Work Hours

Break Hours

Actual Punches

Mark Status: Manually, Apply Leave, Apply Tour, Apply C-OFF

Now select the leave to be applied from the drop down list. You can select the first half/second half /full day. The available leave balance for the selected leave is shown in **Current balance**. You can mention the reason for applying the leave.

06/10/2016 - No Punches Available

5 - Chirag

NS AB AB

Attendance Details

Work Hours

Break Hours

Actual Punches

Leave on 06/10/2016

Leave: SL - Sick Leave

Current Balance: 10.00

Reason: Fever

Apply Cancel

Date: 06/10/2016 Time: HH:MM Sp. Function: Select In Reason: Select

Date: 06/10/2016 Time: HH:MM Sp. Function: Select Out Reason: Select

Then click **Apply**. The leave will be applied on the selected date as shown below.

01/10/2016 - 07/10/2016				
03-Oct Mon	04-Oct Tue	05-Oct Wed	06-Oct Thu	07-Oct Fri
PR PR	PR AB	AB PR	AB SL	AB AB




The user must have leave balance to be applied for leave application.

Also the medical certificate is required for applying certain leave eg: Sick leave. The requirement of the certificate depends on the leave configuration of the company.




The application for Tour/ C-OFF can be done in same way as applying for Leave.

- **Edit Regular and Break Punches**

1. To add or Edit **Regular Punches**, Select "Actual Punches" by clicking .

Enter the **time** for Punch IN and Punch OUT as shown below. You can select any special function for eg: Official IN/ OUT, Short leave IN/OUT while adding or editing the punches.

06/10/2016 - No Punches Available


3 - Nilam

GS
AB
AB

Attendance Details

Work Hours
Break Hours


Actual Punches

Date: 06/10/2016
Time: 09:00
Sp. Function: Select
In Reason: Select

Date: 06/10/2016
Time: 18:30
Sp. Function: Select
Out Reason: Select

Suggested Changes

Regularizing With: Leave
Leave: CL
Full Day: Full Day
Current Balance: 0.00

Click **Apply Changes**  to save the regular punches. The user status will become Present as shown below.

06/10/2016 - Present

3 - Nilam

GS PR PR

Attendance Details

Work Hours 08:30

Break Hours 01:00

Actual Punches

Date 06/10/2016	Date 06/10/2016
Time 09:00	Time 18:30
Sp. Function Select	Sp. Function Select
In Reason Select	Out Reason Select

2. To add **Break Punches**, Select “Break Punches” by clicking .

03/10/2016 - Present

5 - Chirag

GS PR PR

Attendance Details

Work Hours 11:50

Break Hours 01:00

Actual Punches

Actual Punches

Break Punches

Regularized Punches

Date 03/10/2016	Date 03/10/2016
Time 09:10	Time 22:00
Sp. Function Select	Sp. Function Select
In Reason Select	Out Reason Select

03/10/2016 - Present

5 - Chirag

GS PR PR

Attendance Details

Work Hours 11:50

Break Hours 01:00

Break Punches

Punch Select	Punch Select
Date 03/10/2016	Date 03/10/2016
Time HHMM	Time HHMM

Enter the Break Start time and Break End time. Click **Apply Changes** to save the added break time.

Break Punches

Punch Select	Punch Select
Date 03/10/2016	Date 03/10/2016
Time 13:00	Time 14:00

Suggested Changes

The system shows the suggestions using which the exception can be eliminated and the selected user can be marked present.

Manage Attendance

Date: 01/10/2016 to 07/10/2016

User: ID / Name

View

User ID	User Name	01-Oct Sat	02-Oct Sun	03-Oct Mon	04-Oct Tue	05-Oct Wed	06-Oct Thu	07-Oct Fri
5	Chirag	PR	PR	WO	WO	PR	PR	AB
3	Nilam	PR	PR	WO	WO	PR	PR	AB
4	Shalini	PR	PR	WO	WO	PR	PR	AB

04/10/2016 - AB:Early-OUT

5 - Chirag

GS PR AB

Attendance Details

Work Hours: 04:00

Break Hours: 01:00

Actual Punches

Date: 04/10/2016

Time: 09:00

Sp. Function: Select

In Reason: Select

Date: 04/10/2016

Time: 14:00

Sp. Function: Select

Out Reason: Select

Suggested Changes

Regularizing With: Short Leave

Available Short Leave: 0

The suggestions available for regularizing are:

- **Shift** - To regularize a record by assigning the suggested shift. Any other suitable shift can also be selected and assigned.
- **Leave** - To regularize a record by using suggested leaves. A half day or full day leave will be suggested depending on the number of hours to be covered. If leave balance is available, the leave will be approved instantly.



This is applicable for only paid leaves and c-off. Other leave types where balance is not required can also be applied. Tour can also be applied.

However, this may not work for certain leave application restrictions (for e.g. if the date of regularization falls within a period when leave application is restricted.).

- **Late-IN** - To regularize a record using the *Late-IN Allowed* special function. Using this special function will not affect the user's available *Late-IN*.
- **Early-OUT** - To regularize a record using the *Early-OUT Allowed* special function. Using this special function will not affect the user's available *Early-OUT*.
- **Available Overtime** - To regularize a record using the *available overtime* of the user (sum total of user's *authorized overtime* and *manually credited overtime*). However, no partial adjustment will be done, i.e. if 3 hours are to be adjusted but available overtime is 2.5 hours, no adjustment will be allowed.



The total available overtime will be considered for the period specified for overtime adjustment in the **Attendance Correction with Overtime** option in the user's Attendance Policy. If this option is disabled, the available overtime will be considered for the previous month only.

- **Short Leave** - To regularize the user's attendance using available short leaves.
- **Manual Entry** - To regularize a record by manually adding or editing the available punches. Select the record from the grid. Enter the target work hours to be achieved in order to mark the user present. Click on Apply. The punches are adjusted automatically according to target work hours and attendance status gets updated.

If shift hours for full day is 8:00 hrs, then you must enter target work hours as 08:00 to make user full day present.

Manage Attendance

Date: 01/10/2016 07/10/2016

User: ID Name

View

		01/10/2016 - 07/10/2016						
User ID	User Name	01-Oct Sat	02-Oct Sun	03-Oct Mon	04-Oct Tue	05-Oct Wed	06-Oct Thu	07-Oct Fri
5	Chirag	PR	PR	WO	WO	PR	PR	AB
3	Nilam	PR	PR	WO	WO	PR	PR	PR
4	Shalini	PR	PR	WO	WO	PR	PR	PR

06/10/2016 - No Punches Available

5 - Chirag

NS AB SL

Attendance Details

Work Hours

Break Hours

Actual Punches

Date: 06/10/2016 Time: HHMM

Sp. Function: Select

In Reason: Select

Date: 06/10/2016 Time: HHMM

Sp. Function: Select

Out Reason: Select

Suggested Changes

Regularizing With: Manual Entry

Target Work Hours: 0

For half day to be present, minimum 2 hrs are required. So enter Target hours as 02:00 hrs. Then Click **Apply Changes**. This will make the user present on first half as shown below.

06/10/2016 - AB:Early-OUT

5 - Chirag

NS PR SL

Attendance Details

Work Hours: 02:00

Break Hours

Actual Punches

Date: 06/10/2016 Time: 21:00

Sp. Function: Select

In Reason: Select

Date: 06/10/2016 Time: 23:00

Sp. Function: Select

Out Reason: Select

Suggested Changes


Regularizing With: Manual Entry

Target Work Hours: 02:00

To apply latest change to multiple date

There is a provision to apply latest change to multiple date records. This will be useful in cases where similar change is to be done for various days.

Example: Shift is changed for one user on 1st oct.

Then **Apply Similar Change** symbol  appears as shown below.

Manage Attendance ✓ Saved Successfully

Date: 01/10/2016 12/10/2016

User: ID /Name

View

		01/10/2016 - 07/10/2016						
User ID	User Name	01-Oct Sat	02-Oct Sun	03-Oct Mon	04-Oct Tue	05-Oct Wed	06-Oct Thu	07-Oct Fri
5	Chirag	PR AB	WO WO	PR PR	PR PR	AB PR	PR SL	AB AB
3	Nilam	PR PR	WO WO	PR PR	PR PR	PR PR	PR PR	PR PR
4	Shalini	PR PR	WO WO	PR PR	PR PR	PR PR	WO WO	AB AB

Apply Similar Change: Shift Chan

01/10/2016 - Present

5 - Chirag

NS PR AB

Attendance Details

Work Hours 12:50

Break Hours

Actual Punches

Date: 01/10/2016 Time: 08:40

Sp. Function: Select In Reason: Select

Date: 01/10/2016 Time: 21:30

Sp. Function: Select Out Reason: Select

Suggested Changes

Regularizing With: Short Leave

Available Short Leave: 3

Click on this symbol and select the records in the grid for which the same change is to be applied. The selected records will be marked by yellow colour as shown below.

Manage Attendance 6 record(s) selected

Date: 01/10/2016 12/10/2016

User: ID /Name

View

		01/10/2016 - 07/10/2016						
User ID	User Name	01-Oct Sat	02-Oct Sun	03-Oct Mon	04-Oct Tue	05-Oct Wed	06-Oct Thu	07-Oct Fri
5	Chirag	PR AB	WO WO	PR PR	PR PR	AB PR	PR SL	AB AB
3	Nilam	PR PR	WO WO	PR PR	PR PR	PR PR	PR PR	PR PR
4	Shalini	PR PR	WO WO	PR PR	PR PR	PR PR	WO WO	AB AB

01/10/2016 - Present

5 - Chirag

NS PR AB

Attendance Details

Work Hours 12:50

Break Hours

Actual Punches

Date: 01/10/2016 Time: 08:40

Sp. Function: Select In Reason: Select

Date: 01/10/2016 Time: 21:30

Sp. Function: Select Out Reason: Select

Suggested Changes

Regularizing With: Short Leave

Available Short Leave: 3

After selecting the records, click Apply  button to apply the shift change to the selected records.

Shift-Wise Management

The **Shift-Wise Management** functionality allows the administrator to view and manage the shift-based attendance and reporting status of employees for a chosen date. To know more about shift-based attendance, refer to the **Shift and Schedule** module.

To access this functionality, select the **Time and Attendance module > Utilities > Shift-Wise Management**

The **Shift-Wise Management** page will open as shown:

The screenshot shows the 'Shift-Wise Management' interface. At the top, there's a title bar with a star and a question mark icon. Below it, a search bar is present. The main section contains filters: 'Attendance Date' (04/04/2017), 'Filter Users' (All), and 'Group/User' (ID and Name). A 'View' button is located below these filters. Below the filters is a table with the following data:

Shift ID ▲	Name	Assigned	Scheduled	On Leave/Tour	On Week-Off	On Holiday	Reported	Not Yet Reported
		5	4	1	0	0	1	3
FB	Field break	1	1	0	0	0	0	1
GS	General Shift	16	13	1	2	0	3	10
NE	newshift	1	1	0	0	0	0	1
NS	Night Shift	1	1	0	0	0	0	1

Attendance Date: Select a date from the date selection picklist for which you want to view the shift-wise details.

Filter Users: Select an individual user or multiple users associated with a specific enterprise group from the Filter Users drop down list.

Group/User: Specify an enterprise group or user using the given picklist.

Once the above fields are specified, click the **View** button.

The shift-based details for the specified date and users will be displayed as follows:

Shift ID ▲	Name	Assigned	Scheduled	On Leave/Tour	On Week-Off	On Holiday	Reported	Not Yet Reported
		5	4	1	0	0	1	3
FB	Field break	1	1	0	0	0	0	1
GS	General Shift	16	13	1	2	0	3	10
NE	newshift	1	1	0	0	0	0	1
NS	Night Shift	1	1	0	0	0	0	1

The above list displays the following columns:

- **Shift ID:** This column displays the IDs of all the shifts for the specified date.
- **Name:** This column displays the names of the shifts.

- **Assigned:** This column displays the number of users who are assigned the selected shift for the specific date.
- **Scheduled:** This column displays the number of users scheduled for the respective shifts for the specific date.
- **On Leave/Tour:** This column displays the number of users on a shift who are on leave/tour.
- **On Week-Off:** This column displays the number of users on a shift who are on week-off.
- **On Holiday:** This column displays the number of users on a shift who are on holiday.
- **Reported:** This column displays the total number of users on the shift who have reported on the selected date.
- **Not Yet Reported:** This column displays the total number of users on the shift who have not yet reported on the selected date.

To view a detailed list of users whose numbers are represented on the columns, click the respective number link. This will open a pop up window with the list of users.

The admin can use this pop up window to update the shift and day status of the users by selecting the user from the list and selecting the Shift/Day from the drop down list.

The screenshot shows a pop-up window titled "- Not Yet Reported (3)". It contains a form for updating user attendance. The form fields are:

- User: ID (text input), Name (text input)
- Attendance Date: Date (text input)
- Shift/Day: Select (dropdown menu), Normal (dropdown menu)
- Attendance Status: (text input)
- Work Hours: HHMM (text input)
- Extra Work Hours: HHMM (text input)
- Net-Work Hours: HHMM (text input)
- Total Overtime: HHMM (text input)

Below the form is a search bar labeled "Search". Below the search bar is a table with the following columns: User ID, Name, Shift, First Punch, Last Punch, First Half, and Second Half. The table contains three rows of data:

User ID	Name	Shift	First Punch	Last Punch	First Half	Second Half
1320	SHRUTI SAGAR PATKI					
NSuser	Night Shift user					
user1	user1					

At the bottom of the window are two buttons: "Update" and "Close".

Click the **Update** button to save the changes in shift.

Change Policy

The **Change Policy** function is used to change the current effective *Time and Attendance* policy for a user or multiple users to another policy configured in the system. Such changes can be made for the following *Time and Attendance* policies:

- Absentee Policy
- Overtime Policy
- Late-IN Policy
- Early-OUT Policy
- C-OFF Policy



An Attendance Policy cannot be changed using this feature. To change the Attendance Policy for a user, go to Users> User Configuration> T&A> Policy.



You can change the policies upto maximum 99 times.

To change the Policy, Select **Time and Attendance > Utilities > Change Policy**

The **Change Policy** page opens as follows:

The *Change Policy* function can be performed for single users as well as multiple users at a time.

Single User

To change the policy for a single user, select the **Single User** tab.

User: Select the user from the user selection picklist whose policy is to be changed.

The **User Attendance Details** section displays the current policies assigned to the selected user.

Change Policy: Select the policy type which is to be changed.

Date: Select the Start and End dates from the date selection button for which the policy change would apply.

New Policy: Select a new policy from the picklist to replace the old policy.
For eg: Late- IN Policy is to be changed from Late-IN Policy-2 to Late-IN Policy-1.

Remark: A remark related to the new policy change can be entered in the Remark field.

Click the **Apply** button to apply the policy change. The changed policy will be reflected in the User Attendance Details section only when the Date range includes the current date.

Else; New Policy will be reflected in the **User Attendance Change Records** section as shown.

User ID	Change Policy	From Date	To Date	New Policy
07	Late-IN	01/01/2009	31/12/2099	Late In Policy-2
07	Late-IN	01/03/2017	31/03/2017	Late In Policy-1

Multiple Users

To change policy for multiple users at a time, select the **Multiple User** tab.

Change Policy: Select the policy type which is to be changed for multiple users.

Date: Select the Start and End dates from the date selection button for which the policy change would apply.

New Policy: Select a new policy from the picklist to replace the old policy.

Remark: A remark related to the new policy change can be entered in the Remark field.

Select Users: Once Change Policy has been configured, select the users for whom the policy change is to be applied using the filter options of Userwise, Groupwise or All.:

- Userwise - To select random users from a user picklist.
- Groupwise - To select a group of users from the Select Group dropdown list.
- All - To select all users active on the system.

Once the users are specified, click the **Apply** button to apply the changed policy.

User-Wise Attendance Restriction

This option enables the application user to assign a User-wise Restriction on selected devices for Attendance Process. The attendance restriction can be assigned to a *single user* or *multiple users*.

To access this functionality, select the **Time and Attendance module > Utilities > User-Wise Attendance Restriction**.

Single User Restriction

The screenshot shows the 'User-Wise Attendance Restriction' window in 'Single User' mode. The 'User' field is set to '3' and 'Isha'. Below, the 'Assigned Devices' table lists five devices with checkboxes for restricting attendance.

Device Name	Type	Restrict Attendance
Door V3	Door V3	<input checked="" type="checkbox"/>
NGT Ground Floor	NGT Direct Door	<input checked="" type="checkbox"/>
Panel Lite V2-Device-9	Panel Lite V2	<input type="checkbox"/>
RnD Panel lite V2	Panel Lite V2	<input type="checkbox"/>
Vega Direct Door	Vega Controller	<input type="checkbox"/>

An 'Apply' button is located at the bottom right of the table.

User: Select a user from the user selection picklist for whom attendance is to be restricted. On selection of user, a list of the **Assigned Devices** is displayed.

Select the appropriate checkboxes under the **Restrict Attendance** column to restrict the user's attendance for the corresponding device as shown in the above figure.

So when the user punches on these devices, the attendance will not be calculated. The user will be allowed access through these devices.

Click the **Apply** button to apply the changes.

Multiple User Restriction

The screenshot shows the 'User-Wise Attendance Restriction' window in 'Multiple User' mode. It features a 'Select Devices' section with a 'Device Filter' dropdown set to 'Randomly', and a 'Select Users' section with a 'User Wise' dropdown. Both sections have input fields for 'ID' and 'Name'. An 'Apply' button is at the bottom.

Device Filter: Select a device based on filter options of All, Device Group and Randomly.

Device: Select the required devices/device group using the corresponding picklist.

Select a device and enable the **Allow Attendance** or **Restrict Attendance** checkbox as shown below.

Allow Attendance will enable the calculation of user attendance on the selected door. **Restrict Attendance** will restrict the calculation of user attendance of the selected door.

Select	Device Name	Type	Allow Attendance	Restrict Attendance
<input checked="" type="checkbox"/>	Door v3	Door V3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Panel Lite V2-Device-9	Panel Lite V2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Vega Direct Door	Vega Controller	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Select Users: Select the users based on one of the following filters from the dropdown list:

- **User Wise** - To select users randomly using the User picklist.
- **Select Group** - To select all users associated with a particular enterprise group using the **Select Group** dropdown list.
- **ALL** - To select all users active in the system.

User ID	Name	
1782	Nidhi	
2	Chirag	
4	Sweta	

Click the **Apply** button to save the changes.

Advance Overtime Application

Advance Overtime Application is a formal mode of requesting overtime approval before an employee has put in extra working hours as overtime. It enables an organization to keep a track of all the requested, approved/rejected /pending overtime applications.

The Overtime applications can be made by:

- System Account User
- On Behalf System Account User
- Using the ESS Self Service Module

COSEC Web enables all *System Account users* with appropriate page rights to make overtime applications using the *Time and Attendance* module. All applications made by the System Account user are *pre-approved* by default.

COSEC Web also enables all On Behalf System Account User with appropriate page rights to make overtime applications using the *Time and Attendance* module. All applications made by the On Behalf System Account User are *pre-approved* by default. For creating and assigning the roles and rights to the On Behalf System Account User. Refer to "[On Behalf System Account User](#)"

For overtime applications applied in advance using the *Employee Self Service* module, the advance overtime application approvals/rejections have to be done by the respective supervisors of the reporting group by logging into their ESS login. However, such applications can also be approved by the System Account user from the Time and Attendance module of the COSEC Web Application.



For SA users, make sure you have enabled Advance Overtime Application Rights from Admin> System Accounts> Role and Rights Configuration.

For ESS users, make sure you have enabled Advance Overtime Application ESS Rights from Users> Utilities> ESS Role Rights.



ESS users can apply for overtime application in advance only using the ESS module and such advance overtime applications require approval either from the Reporting Group In-Charge or the COSEC Web System Account user. Advance Overtime Application directly approved by the System Administrator do not require any further approval from respective supervisors.

The Advance Overtime Application applied from Time and Attendance module get approved automatically.

Advance Overtime Application for an employee can be applied by the System Account user from **Time Attendance> Utilities> Advance Overtime Application**.

The page appears as shown below:

The screenshot shows the 'Advance Overtime Application' form. On the left is a sidebar with navigation options like Policies, Masters, Utilities, and various attendance views. The main form area has a header with a clock icon and 'Time and Attendance'. Below this, there are fields for User (with a picklist), Application Date, Attendance Date, and OT Hours. A section titled 'Reason And Contact Info' contains fields for Reason, Address, and Contact Number. To the right, there's a summary section showing counts for Pending, Approved, and Rejected applications, and a table for application details. The table currently shows 'No Data'.

To generate a new Advance Overtime Application, click on the **Add** button and configure the following parameters.

This is a close-up of the 'Advance Overtime Application' form. It highlights the top navigation bar which contains a back arrow, a plus sign icon (labeled as the 'Add' button), and a trash icon. An arrow points to the plus sign icon. Below the navigation bar, the form fields for User, Application Date, Attendance Date, OT Hours, Reason, Address, and Contact Number are visible. The 'Reason' field is highlighted with a red border. At the bottom are 'Submit' and 'Cancel' buttons.

User: Select a user from the picklist for whom this overtime application is being generated.

Application Date: This field displays the current date (system generated) on which the application is being generated.

Attendance Date: Enter the desired date for which this Overtime Application is being generated. The SA will be allowed to select past dates (only for Night Shift Cases and provided the system has not generated OT hours automatically), current dates (before assigned shift hours) as well as future dates for overtime application.

OT Hours: Enter the total duration for which the User wants to work overtime in the format of hours and minutes.

←

+

🗑

User *

1

Athira

⋮

Application Date

08/01/2021

Attendance Date *

23/01/2021

📅

OT Hours *

09:00

Reason And Contact Info

Reason *

Overtime

Address

A-19 Shivashish Society

Contact Number

9658741230

Submit

Cancel

Reason And Contact Info

Reason: Enter the reason for overtime.

Address: Enter an address of the User.

Contact Number: Enter the contact number of the User.

Once all the details are filled, Click on the **Submit** button.

The application gets pre-approved after submitting and following parameters will be displayed.

Advance Overtime Application

✓ OT Application has been submitted successfully

⌵

←

+

🗑

User *

1

Athira

⋮

Application Date

08/01/2021

Attendance Date *

23/01/2021

📅

OT Hours *

09:00

Approved OT Hours

09:00

Reason And Contact Info

Reason *

Overtime

Address

A-19 Shivashish Society

Contact Number

9658741230

Application Status

Approved (08/01/2021 11:37)

Submit

Cancel

Jan 2021

📅

Mar 2021

📅

1 Pending

4 Approved

3 Rejected

Application Details

⌵

OT Date	Applied OT Hours	Approved OT Hours	Application Date	Status
23/01/2021	09:00	09:00	08/01/2021	✓
20/01/2021	02:00		07/01/2021	✗
13/01/2021	05:00		06/01/2021	✗
12/01/2021	05:00	05:00	07/01/2021	✓
09/01/2021	04:00		07/01/2021	✗
08/01/2021	03:00		06/01/2021	✗
07/01/2021	04:00	04:00	06/01/2021	✓

The grid on the right side of this page displays the details of all the applied Applications of the particular user like **OT Date**, **Applied OT Hours**, **Approved OT Hours**, **Application Date** and the **Status** of the Applications.

Jan 2021

Mar 2021

1 Pending

2 Approved

2 Rejected

Application Details

OT Date ▲	Applied OT Hours	Approved OT Hours	Application Date	Status
13/01/2021	05:00		06/01/2021	⊗
12/01/2021	05:00		07/01/2021	⌚
08/01/2021	03:00		06/01/2021	⊗
07/01/2021	04:00	04:00	06/01/2021	✓
05/01/2021	03:00	03:00	05/01/2021	✓

Rejected


Pending

Approved


You can even filter the Applications based on **All**, **Pending**, **Approved** and **Rejected** by clicking on the **Filter**  button.




System Administrator can delete pending/approved/rejected application.

Click **Approval Details**  icon from the grid available on the left side of the page to view the Approval Details of the already applied application.

Jun 2021



Aug 2021



0 Pending





1 Approved

1 Rejected

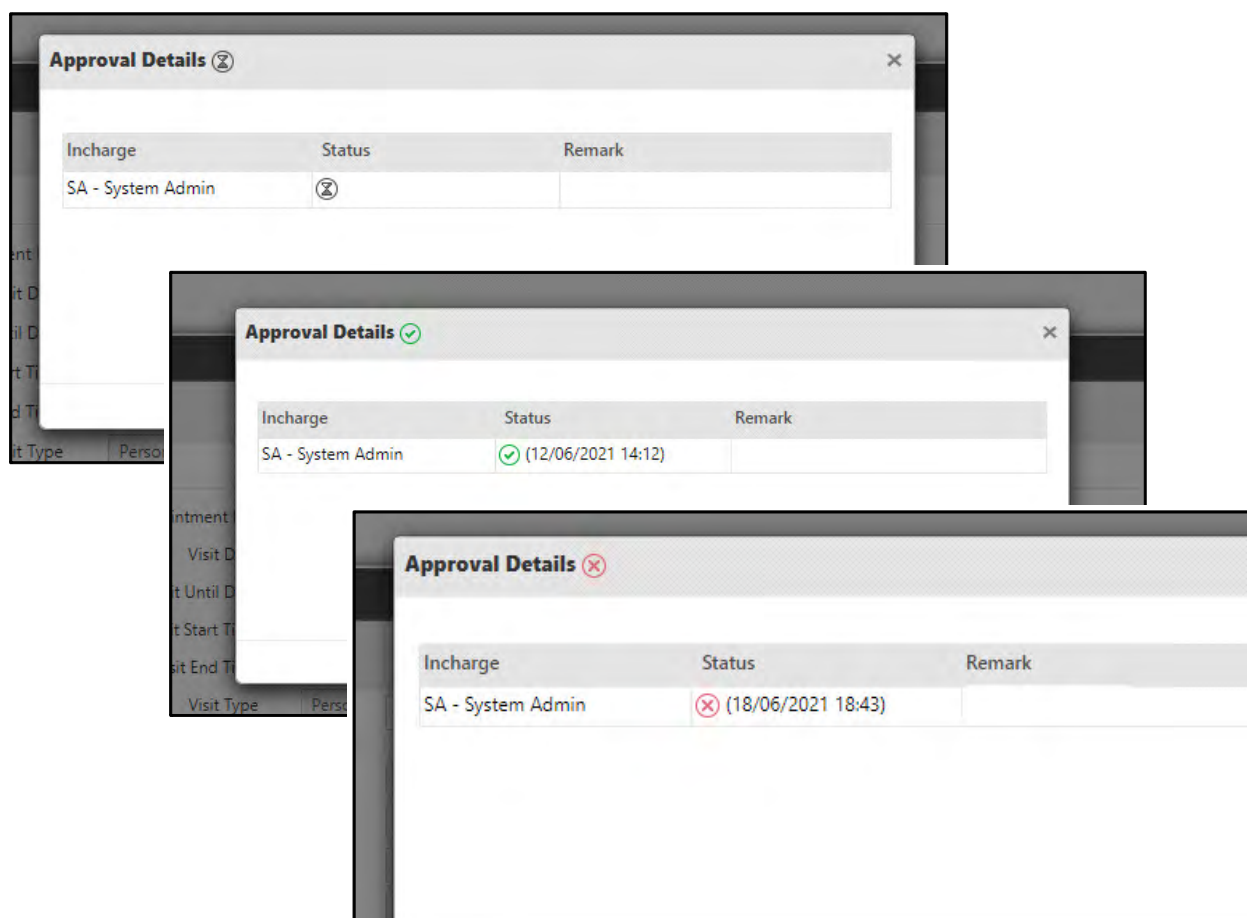
Application Details

▼

⌵

OT Date ▲	Applied OT Hours	Approved OT Hours	Application Date	Status	Approval Details
25/06/2021	02:00	02:00	23/06/2021		
24/06/2021	05:00		23/06/2021		

Approval Details window appears as shown below:



It displays the status of the user's application under **Approval Details**, that is, whether it is — pending, approved or rejected.

The application's status is displayed in the **Status** column as Pending ⌚ , Approved ✓ or Rejected ✗ .

Remark displays the comments provided by the Admin/ RIC/ System.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer [“Approval Policy”](#).

Authorization or Approval

Authorization refers to the act of sanctioning or approving an action, task, manual data entry or event performed on the COSEC Web Application. Authorization for any activity on the COSEC Web Application can be performed by a System Account user with appropriate page rights.

This functionality is useful when the HR administrator in an organization needs to supervise employee attendance and authorize certain data before it is officially recorded for an employee. The Time and Attendance module enables the administrator to perform the following authorizations/approvals for a user:

- “Short Leave/Official In-Out Approval”
- “Overtime/C-OFF Approval”
- “Daily Attendance Approval”
- “Attendance Correction Approval”
- “Event Authorization”
- “Advance Overtime Authorization”



The system requires some of the above authorizations to be enabled during the configuration of the corresponding T&A policy. Entries or applications will be forwarded for authorization/approval only if authorization/approval functionality has been enabled for them.

Short Leave/Official In-Out Approval

This option enables the HR user to authorize all Short Leave/Official IN-OUT requests from ESS users who have punched IN late or punched OUT early for a particular day as per the scheduled shift timings. The ESS users can request the Late-IN or Early-OUT events to be authorized as either a Short Leave, if allowed by HR policy, or as official entry or exit events.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to [“Reporting In-Charge”](#), [“Approval Policy”](#) and [“Configuring Users”](#).

To do this, select the *Time and Attendance module > Authorization/Approval > Short Leave/Official IN-OUT*.

The **Short Leave/Official IN-OUT Authorization** page opens as follows:

You can either:

- view all the pending applications for Short Leave/Official IN-OUT Authorization
- set the filters — Date, Filter Users — to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To know more, refer to [“Pending Authorization”](#).



The population on this page depends on the server's database. It might take time to load all pending applications.

Applications according to Set Filters

To Set the Filters,

- **Date:** Select this option to enable the date filter. Select the start and end date as the duration for which the application status of the Short Leave/Official IN-OUT Authorization is to be viewed.
- **Filter Users:** You can filter records according to the desired Enterprise Group, All or for an Individual.

Select **All**, to view authorization status of the applications of all the active users on the system.

Select **Individual**, to view authorization status of the applications of a single user. Click the picklist to select the desired User ID/Name.

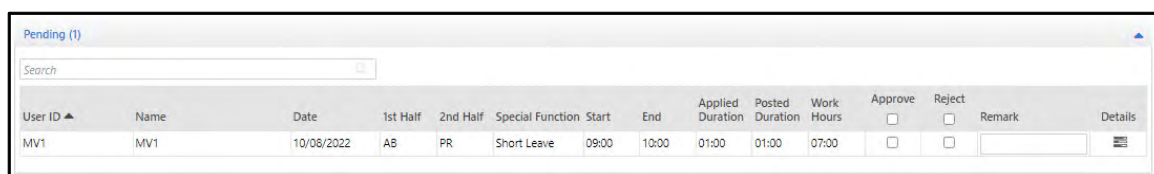
Select the desired Enterprise Group — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Group1/2/3 and then click the picklist to select the desired group's ID/Name, to view authorization status of these applications.

Click **View**. The Pending, Approved and Rejected collapsible panels appear.

Pending Authorization

Click the **Pending** collapsible panel.

The **Pending** section lists all employees for whom Short Leave/Official IN-OUT requests are pending for authorization.



The screenshot shows a window titled "Pending (1)" with a search bar and a table of pending applications. The table has columns for User ID, Name, Date, 1st Half, 2nd Half, Special Function, Start, End, Applied Duration, Posted Duration, Work Hours, Approve, Reject, Remark, and Details. A single row is visible for User ID MV1, Name MV1, Date 10/08/2022, 1st Half AB, 2nd Half PR, Special Function Short Leave, Start 09:00, End 10:00, Applied Duration 01:00, Posted Duration 01:00, Work Hours 07:00, and empty checkboxes for Approve and Reject.

User ID ▲	Name	Date	1st Half	2nd Half	Special Function	Start	End	Applied Duration	Posted Duration	Work Hours	Approve	Reject	Remark	Details
MV1	MV1	10/08/2022	AB	PR	Short Leave	09:00	10:00	01:00	01:00	07:00	<input type="checkbox"/>	<input type="checkbox"/>		

When any application is in the Pending state it can be authorized by the Admin or RIC.

- To approve/reject applications selectively, click the respective application check box against the user.
- To approve/reject all the applications simultaneously, click the Approve /Reject checkbox in the header column.

Once the Admin approves/ rejects the application, the record will be moved from the **Pending** section to the **Approved/ Rejected** section respectively.

The default **Remark** for the Approved and Rejected application will appear in the respective fields. You can enter any customized Remark while authorizing the application.

Click the **Details**  icon to view the attendance details of the corresponding user.

All Attendance Punches window appears as shown below:

All Attendance Punches

User: MV1 MV1

Attendance Date: 10/08/2022

Shift/Day: GS Normal

Attendance Status: AB PR

Work Hours: 07:00

Extra Work Hours:

Net-Work Hours:

Authorized Overtime:

Reason: 62 chars

Search


Date	Time	IO Type	Device Name	Special Function	Access	Source/Location	Job Details	View Image
14/03/2022	14:17	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	14:23	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	14:34	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	14:34	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:03	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:12	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:22	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:22	In	ARGO FACE-Device-2		Allowed	Device		
14/03/2022	15:26	In		Regular - IN	Allowed	ESS		

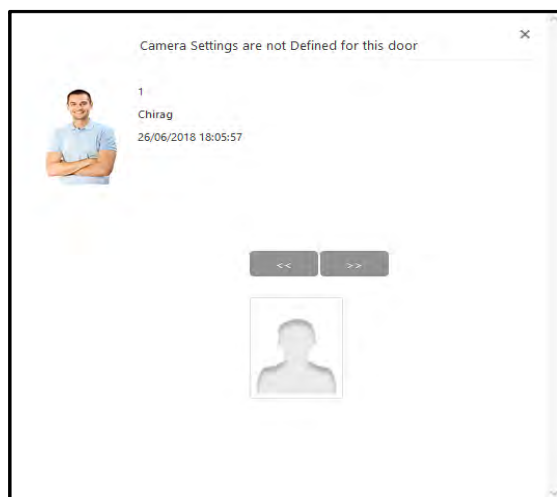
All Attendance Punches window displays the user's attendance and overtime details.

Click the  button to view source location co-ordinate details for an entry or exit event of the user.



If Map is not loaded; check the network connection or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

If there is a Built-In Camera to capture the image of the user while punching on the door; you can view that image by clicking on the **View Image**  icon.



If the event is generated by API then there will not be any image popup window on clicking View Image icon.

All Attendance Punches window also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer [“Approval Policy”](#).

Remark displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.



The pending applications can not be authorized if the attendance period is closed while doing monthly attendance process and “Attendance Correction in Closed Period” check-box is disabled from Time and Attendance> Policies> Attendance Policy> General> Event Authorization.

Even though; the period is closed but if “Attendance Correction in Closed Period” checkbox in Policy is enabled then authorization can be made.

Approved Short Leave/Official IN-OUT

Click the **Approved** collapsible panel.

This section lists all short leave/official IN-OUT requests that have been approved. The following screen is an example of an **Approved** list for Official IN-OUT requests for a specific date range:

Approved (8)														
<div>Search</div>														
User ID	Name	Date	1st Half	2nd Half	Special Function	Start	End	Applied Duration	Posted Duration	Work Hours	Approve	Reject	Remark	Details
5	dhruvi	03/08/2019	PR	PR	Official	09:00	11:00	02:00	02:00	12:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Official	
52	Dinesh	02/08/2019	WO	WO	Short Leave	09:00	10:00	01:00	01:00	10:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Short Lei	
52	Dinesh	03/08/2019	WO	WO	Short Leave	09:00	11:00	02:00	00:00	04:36	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Short Lei	

To change the authorization verdict of any application, select **Reject** checkbox against the corresponding user. Once you reject an approved application, the record will be moved to the **Rejected** section.

Click the **Details** icon to view the attendance details of the corresponding user.

All Attendance Punches window appears as shown below:

All Attendance Punches

User

MV1

MV1

Attendance Date

10/08/2022

Shift/Day

G5

Normal

Attendance Status

AB

PR

Work Hours

07:00

Extra Work Hours

Net-Work Hours

Authorized Overtime

Reason

62 chars

Search


Date	Time	IO Type	Device Name	Special Function	Access	Source/Location	Job Details		View Image
14/03/2022	14:17	In	ARGO FACE-Device 2		Allowed	Device			
14/03/2022	14:23	In	ARGO FACE-Device 2		Allowed	Device			
14/03/2022	14:34	In	ARGO FACE-Device 2		Allowed	Device			
14/03/2022	14:34	In	ARGO FACE-Device 2		Allowed	Device			
14/03/2022	15:03	In	ARGO FACE-Device 2		Allowed	Device			
14/03/2022	15:12	In	ARGO FACE-Device 2		Allowed	Device			
14/03/2022	15:22	In	ARGO FACE-Device 2		Allowed	Device			
14/03/2022	15:22	In	ARGO FACE-Device 2		Allowed	Device			
14/03/2022	15:26	In		Regular - IN	Allowed	ESS			
14/03/2022	15:28	In	ARGO FACE-Device 2		Denied	Device			
14/03/2022	15:28	In	ARGO FACE-Device 2		Allowed	Device	J1 - Job1		
14/03/2022	15:48	In	ARGO FACE-Device 2		Allowed	Device	J1 - Job1		
14/03/2022	15:50	In	ARGO FACE-Device 2		Allowed	Device	J1 - Job1		
14/03/2022	15:54	In	ARGO FACE-Device 2		Allowed	Device	J1 - Job1		
14/03/2022	16:05	In	ARGO FACE-Device 2		Allowed	Device	J2 - Job2		
14/03/2022	16:10	In	ARGO FACE-Device 2		Allowed	Device	J1 - Job1		
14/03/2022	16:10	In	ARGO FACE-Device 2		Denied	Device			

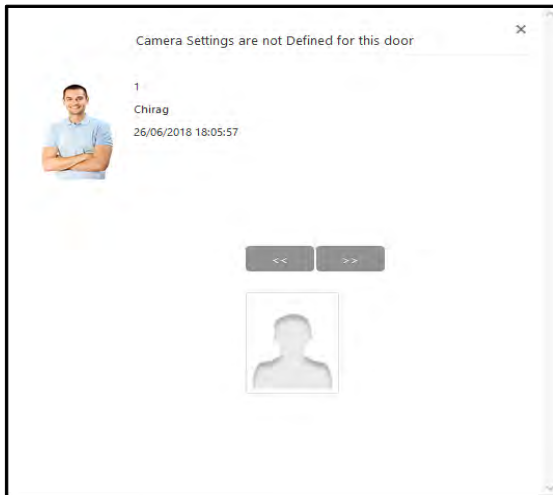
All Attendance Punches window displays the user's attendance and overtime details.

Click the  button to view source location co-ordinate details for an entry or exit event of the user.



If Map is not loaded; check the network connection or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

If there is a Built-In Camera to capture the image of the user while punching on the door; you can view that image by clicking on the **View Image**  icon.



If the event is generated by API then there will not be any image popup window on clicking View Image icon.

All Attendance Punches window also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

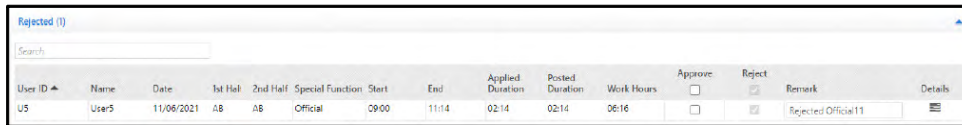
Remark displays the comments provided by the Admin / RIC / System.

Click **Save** to save the authorization.

Rejected Short Leave/Official IN-OUT

Click the **Rejected** collapsible panel.

This section lists all short leave/official IN-OUT requests that have been rejected. The following screen is an example of **Rejected** list for Official IN-OUT requests for a specific date range:

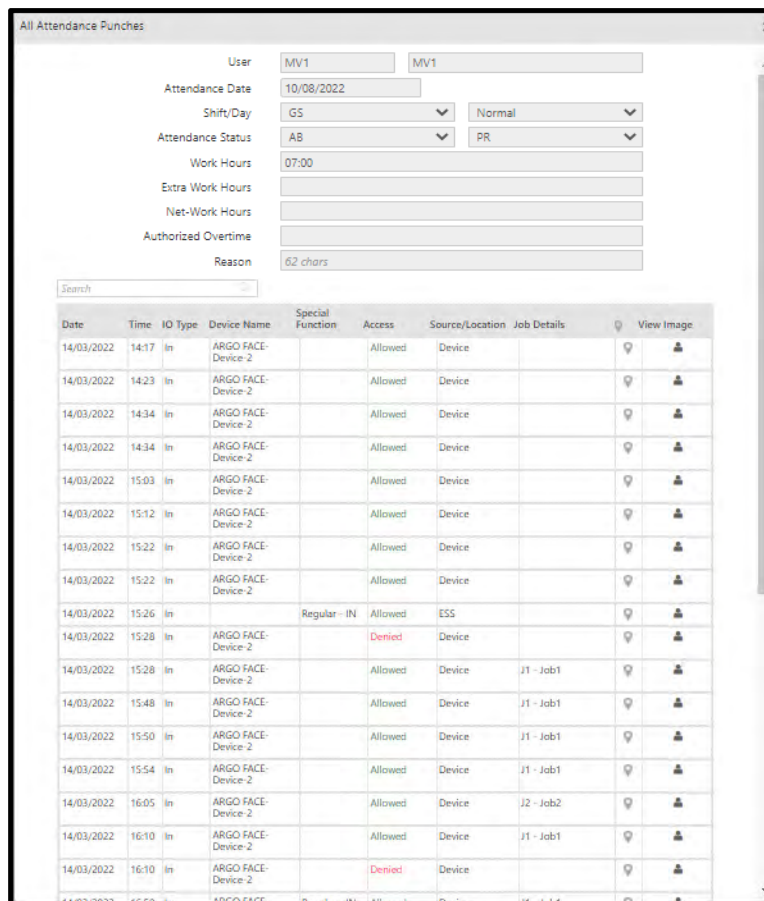


User ID	Name	Date	1st Half	2nd Half	Special Function	Start	End	Applied Duration	Posted Duration	Work Hours	Approve	Reject	Remark	Details
US	User5	11/08/2021	AB	AB	Official	09:00	11:14	02:14	02:14	06:16	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Rejected Official11	

To change the authorization verdict of any application, select **Approve** checkbox against the corresponding user. Once you approve a rejected application, the record will be moved to the **Approved** section.

Click the **Details**  icon to view the attendance details of the corresponding user.

All Attendance Punches window appears as shown below:



All Attendance Punches

User: MV1

Attendance Date: 10/08/2022

Shift/Day: GS Normal

Attendance Status: AB PR

Work Hours: 07:00

Extra Work Hours:

Net-Work Hours:

Authorized Overtime:

Reason: 62 chars


Date	Time	IO Type	Device Name	Special Function	Access	Source/Location	Job Details	View Image
14/03/2022	14:17	In	ARGO FACE-Device 2		Allowed	Device		
14/03/2022	14:23	In	ARGO FACE-Device 2		Allowed	Device		
14/03/2022	14:34	In	ARGO FACE-Device 2		Allowed	Device		
14/03/2022	14:34	In	ARGO FACE-Device 2		Allowed	Device		
14/03/2022	15:03	In	ARGO FACE-Device 2		Allowed	Device		
14/03/2022	15:12	In	ARGO FACE-Device 2		Allowed	Device		
14/03/2022	15:22	In	ARGO FACE-Device 2		Allowed	Device		
14/03/2022	15:22	In	ARGO FACE-Device 2		Allowed	Device		
14/03/2022	15:26	In		Regular - IN	Allowed	ESS		
14/03/2022	15:28	In	ARGO FACE-Device 2		Denied	Device		
14/03/2022	15:28	In	ARGO FACE-Device 2		Allowed	Device	J1 - Job1	
14/03/2022	15:48	In	ARGO FACE-Device 2		Allowed	Device	J1 - Job1	
14/03/2022	15:50	In	ARGO FACE-Device 2		Allowed	Device	J1 - Job1	
14/03/2022	15:54	In	ARGO FACE-Device 2		Allowed	Device	J1 - Job1	
14/03/2022	16:05	In	ARGO FACE-Device 2		Allowed	Device	J2 - Job2	
14/03/2022	16:10	In	ARGO FACE-Device 2		Allowed	Device	J1 - Job1	
14/03/2022	16:10	In	ARGO FACE-Device 2		Denied	Device		

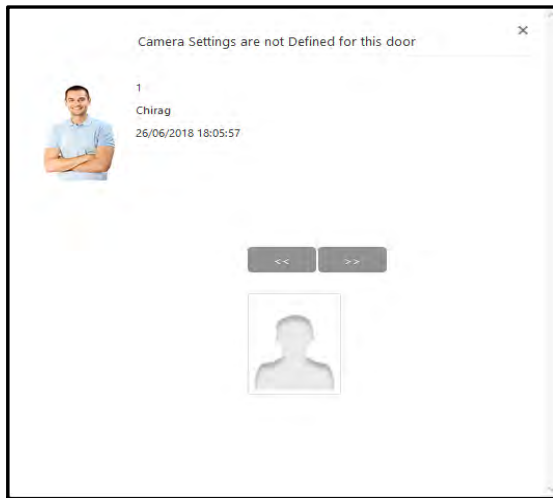
All Attendance Punches window displays the user's attendance and overtime details.

Click the  button to view source location co-ordinate details for an entry or exit event of the user.



If Map is not loaded; check the network connection of your PC or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

If there is a Built-In Camera to capture the image of the user while punching on the door; you can view that image by clicking on the **View Image**  icon.



If the event is generated by API then there will not be any image popup window on clicking View Image icon.

All Attendance Punches window also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer ["Approval Policy"](#).

Remarks displays the comments provided by the Admin / RIC / System.

Click **Save** button to save the changes.



System Administrator can delete pending/approved/rejected application.

Overtime/C-OFF Approval

This option enables the HR user to authorize the conversion of an employee's extra work hours into Overtime or C-OFF hours. Extra hours authorized using this option can only be considered for overtime payment or C-OFF hours compensation.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to [“Reporting In-Charge”](#), [“Approval Policy”](#) and [“Configuring Users”](#).



To enable Overtime/C-OFF Authorization, make sure that the “Auto Authorize” option is disabled during both Overtime and C-OFF Policy configuration.

To authorize OT/C-OFF for a user, select the *Time and Attendance module > Authorization/Approval > Overtime/C-OFF*.

The **Overtime/C-OFF Authorization** page opens as follows:

You can either:

- view all the pending applications for Overtime/C-Off Authorization
- set the filters — Date, Filter Users, Authorization For — to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To know more, refer to [“Pending Overtime/C-OFF”](#).



The population on this page depends on the server's database. It might take time to load all pending applications.

Applications according to Set Filters

- **Date/Attendance Period:** Select this option to enable the date filter.

If you select the Period as Daily, select the start and end dates by clicking the respective date selection buttons.

If you select the Period as Monthly, select the month and year for monthly period. This defines the period for which authorization status is to be viewed for extra work hours.

- **Filter Users:** You can filter records according to the desired Enterprise Group, All or for an Individual.

Select **All**, to view authorization status of the applications of all the active users on the system.

Select **Individual**, to view authorization status of the applications of a single user. Click the picklist to select the desired User ID/Name.

Select the desired Enterprise Group — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Group1/2/3 and then click the picklist to select the desired group's ID/Name, to view authorization status of these applications.

- **Authorization For:** Select the option as Single Record to authorize single/ individual transaction. Select the option as Multiple Records to authorize multiple transaction records.

Daily Period- Single Record

Authorization For

Single Record

View

Pending (4)

Search

<input type="checkbox"/>	User ID ▲	Name	Date	Shift	OT Type	OT Hours	Details
<input type="checkbox"/>	DN	Dinesh	2017/08/25	G5	OT1	00:20	
<input type="checkbox"/>	DN	Dinesh	2017/08/25	G5	OT5	08:30	
<input type="checkbox"/>	DN	Dinesh	2017/08/26	G5	OT1	01:00	
<input type="checkbox"/>	DN	Dinesh	2017/08/26	G5	OT5	08:30	

Define and Authorize

Daily Period- Multiple Record

Authorization For

Multiple Records

View

Pending (4)

Search

<input type="checkbox"/>	User ID ▲	Name	Date	Shift	OT Type	OT Hours	Details
<input type="checkbox"/>	DN	Dinesh	2017/08/25	G5	OT1	00:20	
<input type="checkbox"/>	DN	Dinesh	2017/08/25	G5	OT5	08:30	
<input type="checkbox"/>	DN	Dinesh	2017/08/26	G5	OT1	01:00	
<input type="checkbox"/>	DN	Dinesh	2017/08/26	G5	OT5	08:30	

Define and Authorize

Monthly Period- Single Record

Authorization For

Single Record

View

Pending (3)

Search

User ID ▲	Name	OT Type	OT Hours	Auth as OT	Auth as C-OFF	Remarks	Authorization Sequence	Details
DN	Dinesh	OT1	03:20	01:00	01:00			
DN	Dinesh	OT3	08:15	03:10	02:34			
DN	Dinesh	OT5	42:30	16:30	17:00			

Multiple Period- Multiple Record

Authorization For: Multiple Records

View

Pending (3)

Search

User ID	Name	OT Type	OT Hours	Auth as OT	Auth as C-OFF	Remarks	Details
DN	Dinesh	OT1	03:20	01:00	01:00		
DN	Dinesh	OT3	08:15	03:10	02:34		
DN	Dinesh	OT5	42:30	16:30	17:00		

Define and Authorize

Click the **View** button to view the pending and authorized application with their details.

Pending Overtime/C-OFF

Click the **Pending** collapsible panel.

The **Pending** section lists all users whose extra work hours are pending to be authorized as OT/C-OFF by an HR administrator or Reporting In-charge.

The following example displays a pending authorization requests generated for the user.

Single Record Authorization

Authorization For: Single Record

View

Pending (5)

Search

User ID	Name	Date	Shift	OT Type	OT Hours	Auth as OT	Auth as C-OFF	Remarks	Details
DN	Dinesh	2017/08/07	GS	OT1	01:00				
DN	Dinesh	2017/08/07	GS	OT3	02:00	HHH : MM	HHH : MM	Authorized Overtime/C-OFF	✓ X
DN	Dinesh	2017/08/07	GS	OT5	08:30				
DN	Dinesh	2017/08/08	GS	OT3	02:00				
DN	Dinesh	2017/08/08	GS	OT5	08:30				

Select a record of a user from the Pending list which is to be authorized as shown above.

You can authorize the requested hours as **Overtime hours**, **C-OFF hours** or both as required. Enter the number of hours to be authorized as shown below. Here 30 minutes is authorized for OT and 1 hour is authorized for C-OFF.

Pending (5)

Search

User ID	Name	Date	Shift	OT Type	OT Hours	Auth as OT	Auth as C-OFF	Remarks	Details
DN	Dinesh	2017/08/07	GS	OT1	01:00				
DN	Dinesh	2017/08/07	GS	OT3	02:00	00 : 30	1 : 00	Authorized Overtime/C-OFF	✓ X
DN	Dinesh	2017/08/07	GS	OT5	08:30				
DN	Dinesh	2017/08/08	GS	OT3	02:00				
DN	Dinesh	2017/08/08	GS	OT5	08:30				

Authorized (0)

You must add a **Remark** while authorization.

Then click **Save** to save the authorization.



The OT/C-OFF Eligibility is configured from User Configuration> T&A> Attendance. The C-OFF hours can be authorized in multiple of specified value in C-OFF Policy.

If the user is eligible for OT and C-OFF, authorization can be done for both.

Once you approve, the record will be moved from the **Pending** section to the **Authorized** section.

The authorized overtime hours will be displayed in the grid as shown below.

User ID	Name	Date	Shift	OT Type	OT Hours	Auth as OT	Auth OT Date	Auth as C-OFF	Auth C-OFF Date	Auth By	Remarks	Details
DN	Dinesh	2017/08/07	GS	OT3	02:00	00:30	2017/09/01	01:00	2017/09/01	SA		

Click the **Details** icon corresponding to the user, to view the detailed attendance record as well as the Advance Overtime Application and its status.

The **All Attendance Punches** window appears as shown below.

User: U2 U2
Attendance Date: 19/04/2022
Shift/Day: GS Normal
Attendance Status: PR PR
Work Hours: 08:00
Extra Work Hours:
Net-Work Hours:

Advance Overtime Application

Date	Time	IO Type	Device Name	Special Function	Access	Source/Location	Job Details	View Image
19/04/2022	11:52	In	ARGO-Device-2		Allowed	Device		
19/04/2022	11:52	In	ARGO-Device-2		Allowed	Device		
19/04/2022	11:55	In	ARGO-Device-2		Allowed	Device	Default Job	
19/04/2022	11:55	In	ARGO-Device-2		Allowed	Device	J1 - Job1	
19/04/2022	11:55	In	ARGO-Device-2		Allowed	Device	J1 - Job1	
20/04/2022	10:22	In	ARGO-Device-2		Allowed	Device	J1 - Job1	
20/04/2022	10:22	In	ARGO-Device-2		Allowed	Device	J2 - Job2	
20/04/2022	10:22	In	ARGO-Device-2		Allowed	Device	J1 - Job1	
20/04/2022	10:22	In	ARGO-Device-2		Allowed	Device	J2 - Job2	

Approval Details

Incharge	Status	Remark


Close

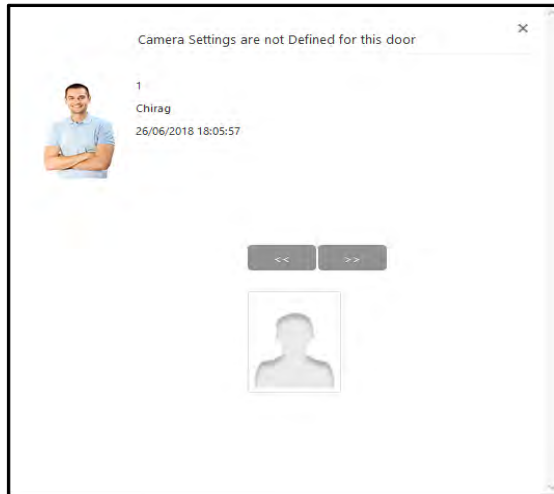
All Attendance Punches window displays the user's attendance and overtime details.

Click the  button to view source location co-ordinate details for an entry or exit event of the user.



If Map is not loaded; check the network connection of your PC or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

If there is a Built-In Camera to capture the image of the user while punching on the door; you can view that image by clicking on the **View Image**  icon.



If the event is generated by API then there will not be any image popup window on clicking View Image icon.

All Attendance Punches window also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remark displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.

Multiple Record Authorization

If you want to authorize multiple records at a time then select Multiple Records in "Authorization For" and click View. The page appears as shown below.

Authorization For: Multiple Records View

Pending (6)

Search:

<input type="checkbox"/>	User ID ▲	Name	Date	Shift	OT Type	OT Hours	Details
<input type="checkbox"/>	DN	Dinesh	2017/08/25	GS	OT1	00:20	
<input checked="" type="checkbox"/>	DN	Dinesh	2017/08/25	GS	OT3	01:15	
<input type="checkbox"/>	DN	Dinesh	2017/08/25	GS	OT5	08:30	
<input type="checkbox"/>	DN	Dinesh	2017/08/26	GS	OT1	01:00	
<input checked="" type="checkbox"/>	DN	Dinesh	2017/08/26	GS	OT3	01:30	

1 - 5 of 6 records

Define and authorize

Now select the checkboxes for the overtime record to be authorized. For example: Here OT3 on 25th and 26th August is to be authorized for 1 hour.

Click **Define and Authorize** button. The **Configure Authorization Parameters** window appears. You can authorize OT for multiple records in following ways:

- **Authorize:** You can select the option as Available OT or Defined OT hours for OT Type-Wise or Record Wise option.
- Select the option as **Available OT** to authorize the respective available overtime hours for the selected records.

Configure Authorization Parameters

Authorize: Available OT

Authorization Mode: OT Type-Wise

Authorize in Terms of: Percentage OT

OT Type	Define Hours for OT(%)	Define Hours for C-OFF(%)
OT1	50.00 %	50.00 %
OT2	60 %	40.00 %
OT3	30 %	70.00 %
OT4	100.00 %	0.00 %
OT5	100.00 %	0.00 %

Authorize Hours for Each Record(As Overtime): %

Authorize Hours for Each Record(As C-OFF): %

Remarks: Authorized Overtime/C-OFF

Authorize

Authorized (2)

Search:

<input type="checkbox"/>	User ID ▲	Name	Date	Shift	OT Type	OT Hours	Auth as OT	Auth OT Date	Auth as C-OFF	Auth C-OFF Date	Auth By	Remarks	Details
<input type="checkbox"/>	DN	Dinesh	2017/08/25	GS	OT3	01:15	00:22	2017/09/18	00:52	2017/09/18	SA		
<input type="checkbox"/>	DN	Dinesh	2017/08/26	GS	OT3	01:00	00:18	2017/09/18	00:42	2017/09/18	SA		

OT3 on 25th = 30% of OT = 30% of 1:15 hrs = 22 minutes; C-OFF = 70% of 1.15 hrs = 52 minutes

OT3 on 26th = 30% of OT = 30% of 1:00 hrs = 18 minutes; C-OFF = 70% of 1.00 hrs = 42 minutes

- Select the option as **Defined OT hours** to define a value of hours to be authorized for selected records.

Configure Authorization Parameters

Authorize: Defined OT Hours

Authorization Mode: Record-Wise

Authorize in Terms of: Hours

OT Type	Define Hours for OT	Define Hours for C-OFF
OT1		
OT2		
OT3		
OT4		
OT5		

Authorize Hours for Each Record(As Overtime): 001 : 00

Authorize Hours for Each Record(As C-OFF): HHH : MM

Remarks: 1 hour to be authorized as OT

Authorize

Authorization Mode: Select the mode as **OT-Type Wise** to authorize hours separately for each OT or **Record-Wise** to authorize hours for the selected records.

Available OT

In the option “**OT Type-Wise**” you can authorize hours based on the OT type (OT1, OT2,...OT5) for the selected records.

- **Authorize in Terms of:** Select the option as **Hours** or **Percentage** of OT/C-OFF based on which number of hours or percentage of hours is to be authorized as Overtime or C-OFF.
- **Hours:** Enter the number of hours to be assigned as overtime for OT1, OT2...OT5. The remaining hours from the available overtime will be assigned to the C-OFF hours.
- **Percentage:** Enter the percentage value to calculate OT1, OT2...OT5 as percentage of available overtime hours. Based on entered OT percentage, C-OFF percentage will appear. For example: If OT1 is set to 40% of OT then C-OFF will be calculated as 60% of OT.

In the option “Record-Wise” you can authorize hours for OT and C-OFF for each records.

- **Authorize in Terms of:** Select the option as **Hours** or **Percentage** of OT/C-OFF based on which number of hours or percentage of hours is to be authorized as Overtime or C-OFF.
- **Hours:** When Hours of OT or Hours of C-OFF is selected then enter the number of hours in the field **Authorize Hours for Each Record (As Overtime)** or **Authorize Hours for Each Record (As C-OFF)** depending on the selection. For example: If available OT hrs is 2 hrs and Authorize hours for each record (As Overtime) is entered as 1:00 hr then remaining 1 hr is given to C-OFF.
- **Percentage:** When Percentage of OT or Percentage of C-OFF is selected then enter the percentage in the field Authorize Hours for Each Record (As Overtime) or Authorize Hours for Each Record (As C-OFF) depending on the selection. For example: If Authorize hours for each record (As Overtime) is entered as 40% then remaining 60% is given to C-OFF.

Defined OT Hours

In the option “**OT Type-Wise**” you can authorize hours based on the OT type (OT1, OT2,...OT5) for the selected records.

- **Authorize in Terms of:** Select the option as **Hours** or **Percentage** based on which number of hours or percentage of hours is to be authorized as Overtime or C-OFF.
- **Hours:** Enter the number of hours to be assigned as overtime and or C-OFF for OT1, OT2...OT5.
- **Percentage:** Enter the percentage value for overtime and C-OFF to calculate OT1, OT2...OT5.

The left screenshot shows the 'Configure Authorization Parameters' dialog box with the 'Hours' authorization mode selected. It features a table for defining hours for OT types (OT1 to OT5) and C-OFF. The right screenshot shows the same dialog box with the 'Percentage' authorization mode selected, where the values are entered as percentages.

OT Type	Define Hours for OT	Define Hours for C-OFF
OT1	001 : 00	001 : 00
OT2	002 : 00	000 : 30
OT3	001 : 00	000 : 30
OT4	HHH : MM	HHH : MM
OT5	HHH : MM	HHH : MM

Below the table, there are fields for 'Authorize Hours for Each Record(As Overtime)' and 'Authorize Hours for Each Record(As C-OFF)', both set to 'HHH : MM'. A 'Remarks' field is also present.

In the option “**Record-Wise**” you can authorize hours for OT and C-OFF for each records.

- **Authorize in Terms of:** Select the option as **Hours** or **Percentage** based on which number of hours or percentage of hours is to be authorized as Overtime or C-OFF.
- **Hours:** When Hours is selected then enter the number of hours in the field **Authorize Hours for Each Record (As Overtime)** and or **Authorize Hours for Each Record (As C-OFF)**.
- **Percentage:** Enter the percentage value in the field **Authorize Hours for Each Record (As Overtime)** and or **Authorize Hours for Each Record (As C-OFF)**.

Authorizing Monthly Records

The screenshot shows the 'Authorization For Multiple Records' dialog box. It has a 'View' button and a 'Pending (3)' status. Below, there is a table with columns: UserID, Name, OT Type, OT Hours, Auth as OT, Auth as C-OFF, Remarks, and Details. Three records are listed, all for a user named 'Dinesh'.

UserID	Name	OT Type	OT Hours	Auth as OT	Auth as C-OFF	Remarks	Details
DN	Dinesh	OT1	03:30	01:00	01:00		
DN	Dinesh	OT3	08:15	03:10	02:34		
DN	Dinesh	OT5	42:30	16:30	17:00		

At the bottom, there is a 'Define and Authorize' button.

After selecting the records, click on **Define and Authorize**. The **Configure Authorization Parameters** page appears as shown below.

Configure the below parameters as described before.

You can select the Authorization Sequence from the options of **OT then C-OFF** and **C-OFF then OT**.

Configure Authorization Parameters

Authorize: Available OT

Authorization Mode: OT Type-Wise

Authorize in Terms of: Percentage

OT Type	Define Hours for OT(%)	Define Hours for C-OFF(%)
OT1	40	60.00
OT2	70	30.00
OT3	60	40.00
OT4	50	50.00
OT5	100.00	0.00

Authorize Hours for Each Record(As Overtime):

Authorize Hours for Each Record(As C-OFF):

Remarks: Authorize OT then C-OFF

Authorization Sequence: OT then C-OFF

Authorize

Configure Authorization Parameters

Authorize: Available OT

Authorization Mode: Record-Wise

Authorize in Terms of: Hours

OT Type	Define Hours for OT	Define Hours for C-OFF
OT1		
OT2		
OT3		
OT4		
OT5		

Authorize Hours for Each Record(As Overtime): 0003 : 00

Authorize Hours for Each Record(As C-OFF): Remaining OT Hours

Remarks:

Authorization Sequence: OT then C-OFF

Authorize

In above example 3 hr is to be given as OT for each record then remaining hours will be given to C-OFF.

Pending (0)

Authorized (3)

Search

User ID	Name	OT Type	OT Hours	Auth as OT	Auth as C-OFF	Remarks	Details
DN	Dinesh	OT1	03:20	03:00	00:20		
DN	Dinesh	OT3	08:15	03:00	05:15		
DN	Dinesh	OT5	42:30	03:00	39:30		

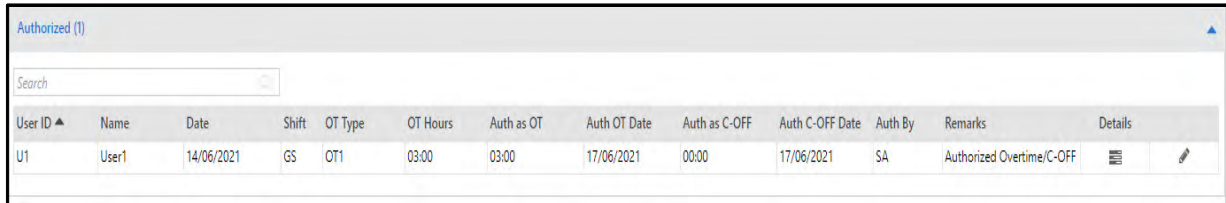
Define and Authorize

The authorized records will be shown in Authorized section.



Authorized Overtime/C-OFF




Click the **Authorized** collapsible panel.

This section lists all the OT/C-OFF Authorizations for the selected user or user groups for the specified time period.



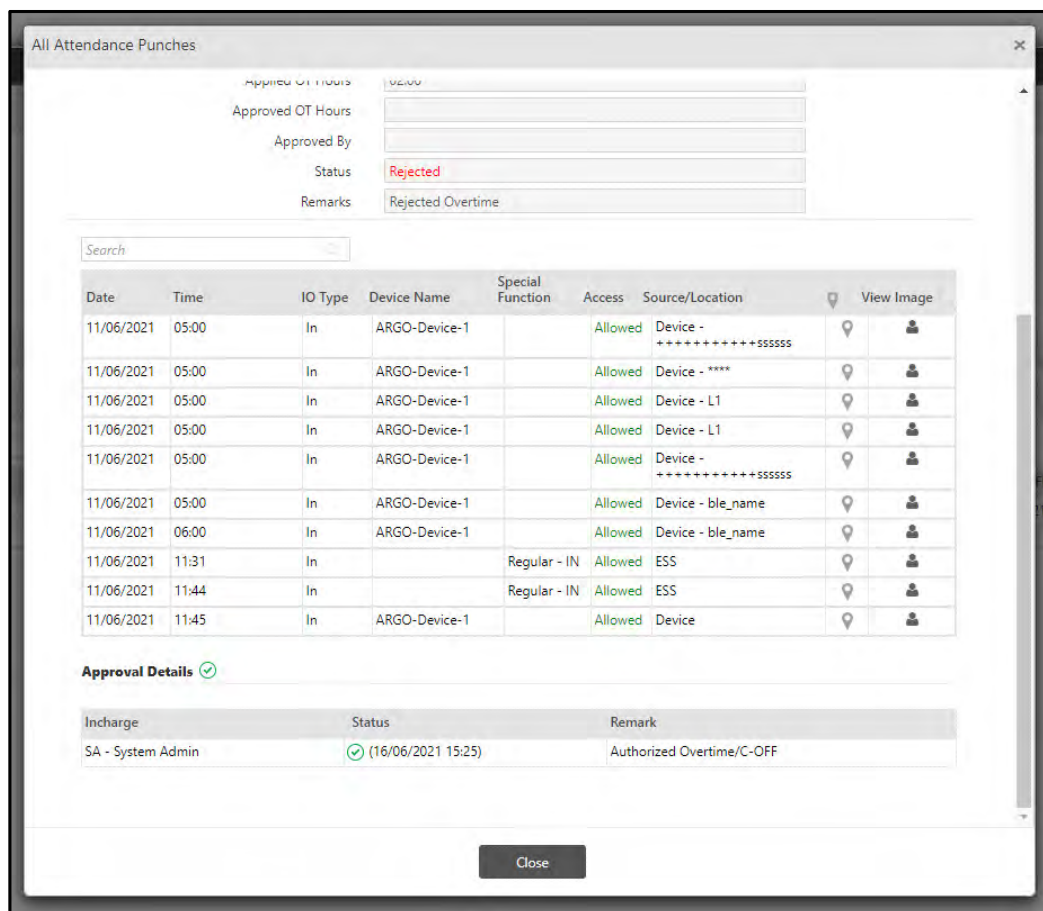
The screenshot shows a window titled "Authorized (1)" with a search bar and a table of authorization records. The table has columns for User ID, Name, Date, Shift, OT Type, OT Hours, Auth as OT, Auth OT Date, Auth as C-OFF, Auth C-OFF Date, Auth By, Remarks, and Details. A single record is visible for User1 on 14/06/2021, Shift GS, OT Type OT1, OT Hours 03:00, Auth as OT 03:00, Auth OT Date 17/06/2021, Auth as C-OFF 00:00, Auth C-OFF Date 17/06/2021, Auth By SA, and Remarks Authorized Overtime/C-OFF.

User ID	Name	Date	Shift	OT Type	OT Hours	Auth as OT	Auth OT Date	Auth as C-OFF	Auth C-OFF Date	Auth By	Remarks	Details
U1	User1	14/06/2021	GS	OT1	03:00	03:00	17/06/2021	00:00	17/06/2021	SA	Authorized Overtime/C-OFF	 





















Click on **Edit**  to edit the Authorized OT, C-off Hours and the Remarks. Then click **OK**  to save or **Cancel**  to discard the changes.


Click the Details  icon to view the attendance details of the corresponding user.


All Attendance Punches window appears as shown below:



The screenshot shows the "All Attendance Punches" window. It has a top section for "Applied OT Hours", "Approved OT Hours", "Approved By", "Status" (set to Rejected), and "Remarks" (set to Rejected Overtime). Below this is a search bar and a table of attendance punches. The table has columns for Date, Time, IO Type, Device Name, Special Function, Access, Source/Location, and View Image. The table contains 10 rows of data, mostly for "ARGO-Device-1" with "Allowed" access. At the bottom, there is an "Approval Details" section with a table showing "Incharge" (SA - System Admin), "Status" (Approved with a green checkmark), and "Remark" (Authorized Overtime/C-OFF). A "Close" button is at the bottom right.

Date	Time	IO Type	Device Name	Special Function	Access	Source/Location	View Image
11/06/2021	05:00	In	ARGO-Device-1		Allowed	Device - *****\$SSSSSS	 
11/06/2021	05:00	In	ARGO-Device-1		Allowed	Device - ****	 
11/06/2021	05:00	In	ARGO-Device-1		Allowed	Device - L1	 
11/06/2021	05:00	In	ARGO-Device-1		Allowed	Device - L1	 
11/06/2021	05:00	In	ARGO-Device-1		Allowed	Device - *****\$SSSSSS	 
11/06/2021	05:00	In	ARGO-Device-1		Allowed	Device - ble_name	 
11/06/2021	06:00	In	ARGO-Device-1		Allowed	Device - ble_name	 
11/06/2021	11:31	In		Regular - IN	Allowed	ESS	 
11/06/2021	11:44	In		Regular - IN	Allowed	ESS	 
11/06/2021	11:45	In	ARGO-Device-1		Allowed	Device	 

Approval Details 

Incharge	Status	Remark
SA - System Admin	 (16/06/2021 15:25)	Authorized Overtime/C-OFF


Close

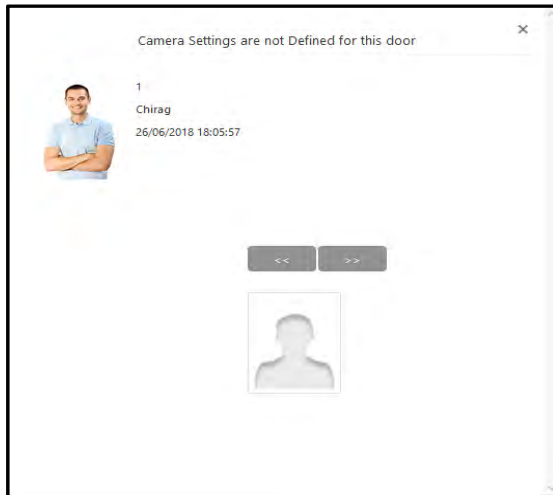
All Attendance Punches window displays the user's attendance and overtime details.

Click the  button to view source location co-ordinate details for an entry or exit event of the user.



If Map is not loaded; check the network connection of your PC or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

If there is a Built-in camera to capture the image of the user while punching on the door; you can view that image by clicking on the **View Image**  icon.



If the event is generated by API then there will not be any image popup window on clicking View Image icon.

All Attendance Punches window also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remark displays the comments provided by the Admin / RIC / System.

Click **Save** to save the authorization.

Daily Attendance Approval

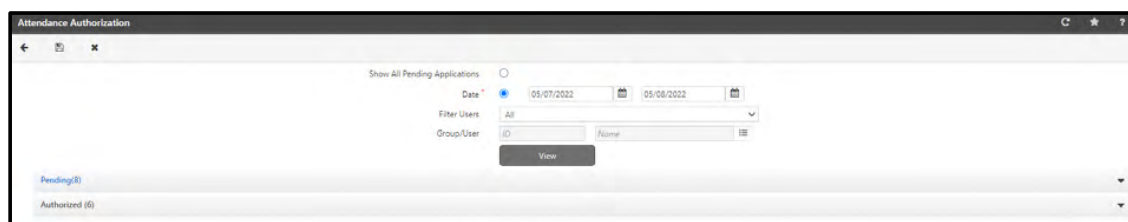
The HR administrator may want to review daily IN and OUT punch records for all users before approving these as the official attendance for the day. This may be especially useful in monitoring irregularity in the attendance patterns of employees and in keeping a check on suspected abuse of privileges such as punching on behalf of colleagues or unauthorized visitors.

Authorization for Daily Attendance can be enabled during the configuration of an Attendance Policy from **Time and Attendance > Policies > Attendance Policy > General**. Once enabled, every attendance event from the configured users will pass to the respective reporting in-charges and the COSEC Web system administrator for approval before the user is marked “present”.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to [“Reporting In-Charge”](#), [“Approval Policy”](#) and [“Configuring Users”](#).

To view and authorize daily attendance, select the **Time and Attendance module > Authorization/Approval > Daily Attendance**.

The **Attendance Authorization** page opens as follows:



You can either:

- view all the pending applications for Attendance Authorization
- set the filters — Date, Filter Users — to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Authorize** check box of the desired entry.

To know more, refer to [“Pending Authorization”](#).



The population on this page depends on the server's database. It might take time to load all pending applications.

Applications according to Set Filters

To Set the Filters,

- **Date:** Select this option to enable the date filter. Select the start and end date as the duration for which the applications for Attendance Authorization are to be viewed.
- **Filter Users:** You can filter records according to the desired Enterprise Group, All or for an Individual.

Select **All**, to view authorization status of the applications of all the active users on the system.

Select **Individual**, to view authorization status of the applications of a single user. Click the picklist to select the desired User ID/Name.

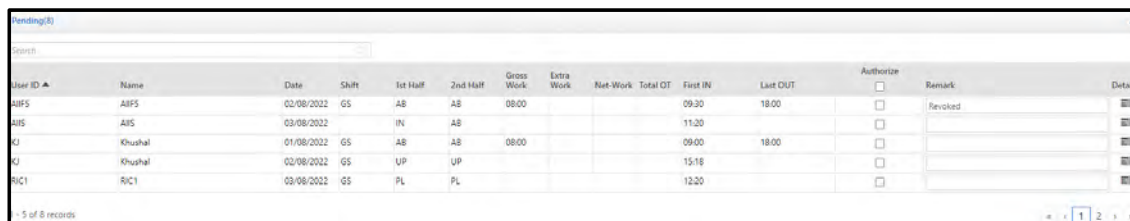
Select the desired Enterprise Group — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Group1/2/3 and then click the picklist to select the desired group's ID/Name, to view authorization status of these applications.

Click the **View** button to view the pending and authorized attendance records of the specified users and their details.

Pending Authorization

Click the **Pending** collapsible panel.

The **Pending** section lists daily attendance records of users that are yet to be sanctioned by the system administrator. All the records in this section are marked "AB" (absent) because they are unauthorized.



The screenshot shows a window titled "Pending(8)" with a search bar and a table of attendance records. The table has columns for User ID, Name, Date, Shift, 1st Half, 2nd Half, Gross Work, Extra Work, Net-Work, Total OT, First IN, Last OUT, Authorize, Remark, and Details. There are 8 records listed, all marked as "AB" (absent). The "Authorize" column has checkboxes for each record, and the "Remark" column has a text area for each record. The "Details" column has a magnifying glass icon for each record.

User ID	Name	Date	Shift	1st Half	2nd Half	Gross Work	Extra Work	Net-Work	Total OT	First IN	Last OUT	Authorize	Remark	Details
AIR5	AIR5	02/08/2022	GS	AB	AB	08:00				09:30	18:00	<input type="checkbox"/>	Revoked	
AIR5	AIR5	03/08/2022		IN	AB					11:20		<input type="checkbox"/>		
KJ	Khushal	01/08/2022	GS	AB	AB	08:00				09:00	18:00	<input type="checkbox"/>		
KJ	Khushal	02/08/2022	GS	UP	UP					15:18		<input type="checkbox"/>		
RIC1	RIC1	03/08/2022	GS	PL	PL					12:20		<input type="checkbox"/>		

When any application is in the Pending state it can be authorized by the Admin or RIC.

- To authorize the applications selectively, click the respective **Authorize** check box against the user.
- To authorize all the applications simultaneously, click the **Authorize** checkbox in the header column.

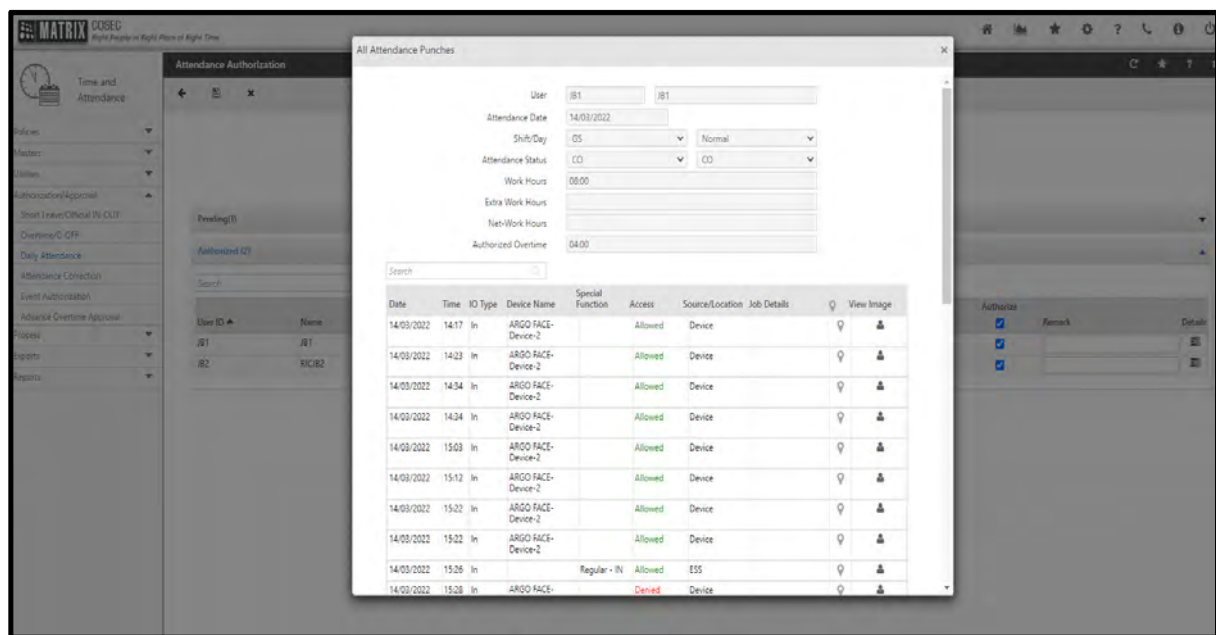
Once the Admin authorizes the application, the record will be moved from the **Pending** section to the **Authorized** section.

The default **Remark** for the Authorized application will appear in the respective fields. You can enter your Remark while authorizing the application.

Click the **Details**  icon to view the attendance details of the corresponding user.

All Attendance Punches window appears as shown below:

All Attendance Punches window appears as shown below:



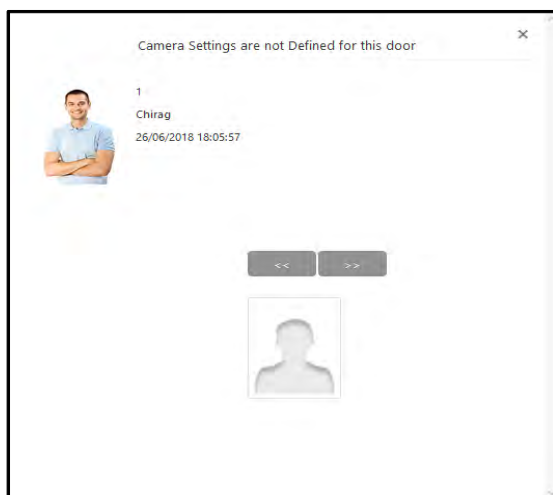
All Attendance Punches window displays the user's attendance and overtime details.

Click the button to view source location co-ordinate details for an entry or exit event of the user.



If Map is not loaded; check the network connection of your PC or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

If there is a Built-In Camera to capture the image of the user while punching on the door; you can view that image by clicking on the **View Image** icon.



If the event is generated by API then there will not be any image popup window on clicking View Image icon.

All Attendance Punches window also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer [“Approval Policy”](#).


Remarks displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.

Authorized Attendance

Click the **Authorized** collapsible panel.

This section lists all the daily attendance records that have been authorized. All the authorized records are now marked as “PR” (present) in the following example:

Pending (5)														
Authorized (1)														
Search														
User ID ▲	Name	Date	Shift	1st Half	2nd Half	Gross Work	Extra Work	Net Work	Total OT	First IN	Last OUT	Authorize	Remark	Details
1687	Aditi Gupta	01/12/2017	G2	PR	PR	10:00	01:00			09:00	19:00	<input checked="" type="checkbox"/>	Authorized Daily Attendance	



The attendance status (“AB”, “PR” etc.) after attendance is authorized, will depend on criteria such as shift timings, work hours etc. for the respective employee. For e.g. if punches do not match with assigned shift timings, user will be marked “AB”.

To revoke authorization, clear the **Authorize** checkbox against a user. Then this record will be moved from the **Authorized** section to the **Pending** section again.

Click the **Details**  icon to view the attendance details of the corresponding user.

All Attendance Punches window appears as shown below:

All Attendance Punches

User: JB2 RIC/JB2

Attendance Date: 14/03/2022

Shift/Day: Normal

Attendance Status: IN

Work Hours:

Extra Work Hours:

Net-Work Hours:

Authorized Overtime:

Search:

Date	Time	IO Type	Device Name	Special Function	Access	Source/Location	Job Details	View Image
14/03/2022	14:09	In	ARGO FACE-Device-2		Allowed	Device		

Approval Details ✓


Incharge	Status	Remark
SA - System Admin	✓ (14/03/2022 00:00)	

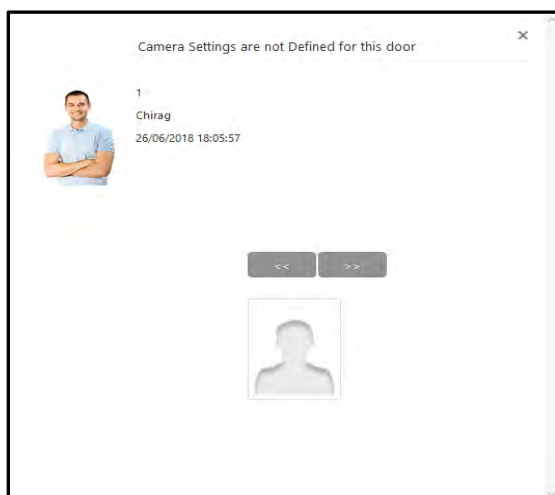
All Attendance Punches window displays the user's attendance and overtime details.

Click the  button to view source location co-ordinate details for an entry or exit event of the user.



If Map is not loaded; check the network connection of your PC or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

If there is a Built-In Camera to capture the image of the user while punching on the door; you can view that image by clicking on the **View Image**  icon.



If the event is generated by API then there will not be any image popup window on clicking View Image icon.

All Attendance Punches window also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remark displays the comments provided by the Admin / RIC / System.

Click **Save** to save the authorization.

Attendance Correction Approval

Attendance Correction may be required by an employee in several instances. It may be required to correct a missed or forgotten punch during the course of a working day or to request modification for an entry or exit event posted for a particular day's attendance data. COSEC allows employees to log in to the ESS module and apply for attendance data corrections.

These attendance correction applications however, are required to be authorized by the COSEC Web system administrator (likely an HR personnel) using the *Time and Attendance* module.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to ["Reporting In-Charge"](#), ["Approval Policy"](#) and ["Configuring Users"](#).



*Attendance correction performed by a System Account user will always be pre-approved.
Attendance Correction applications can also be approved by respective Reporting Group In-charges from the ESS application.*

To authorize attendance correction applications,

Select the **Time and Attendance module > Authorization/Approval > Attendance Correction**.

The **Attendance Correction Authorization** page will appear as follows:

You can either:

- view all the pending applications for Attendance Correction Authorization
- set the filters — Date, Filter Users — to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To know more refer to ["Pending Applications"](#).



The population on this page depends on the server's database. It might take time to load all pending applications.

Applications according to Set Filters

To Set the Filters,

- **Date:** Select this option to enable the date filter. Select the start and end dates by clicking the respective date selection buttons. This defines the period for which Attendance Correction Applications are to be viewed. The end date is by default set to the current date and authorization is not allowed for any later date.
- **Filter Users:** You can filter records according to the desired Enterprise Group, All or for an Individual.

Select **All**, to view authorization status of the applications of all the active users on the system.

Select **Individual**, to view authorization status of the applications of a single user. Click the picklist to select the desired User ID/Name.

Select the desired Enterprise Group — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Group 1/2/3 and then click the picklist to select the desired group's ID/Name, to view authorization status of these applications.

Click the **View** button to view all pending, approved and rejected attendance correction applications and their details.

Pending Applications

Click the **Pending** collapsible panel.

The **Pending** section lists all the attendance correction applications from users waiting to be sanctioned by the system administrator/RIC as shown.

Pending (2)											
Search											
User ID	Name	Application Date	Attendance Date	Shift	WO/PH	1st Punch	2nd Punch	3rd Punch	4th Punch	Approve	Reject
ais	ais	04/08/2022	03/08/2022	GS		11:20	19:00			<input type="checkbox"/>	<input type="checkbox"/>
AnyOneUser	AnyOneUser	04/08/2022	04/08/2022	GS		09:30	20:00			<input type="checkbox"/>	<input type="checkbox"/>

When any application is in the Pending state it can be authorized by the Admin or RIC.

- To approve/reject applications selectively, click the respective application check box against the user.
- To approve/reject all the applications simultaneously, click the Approve/Reject checkbox in the header column.

Once the Admin approves/ rejects the application, the record will be moved from the **Pending** section to the **Approved/ Rejected** section respectively.

The default **Remark** for the Approved and Rejected application will appear in the respective fields. You can enter your Remark while authorizing the application.

Click the **Details**  icon to view the attendance details of the corresponding user.

All Attendance Punches window appears as shown below:

The screenshot shows the 'All Attendance Punches' window with the following search filters:

- User: U4 (User4)
- Attendance Date: 07/06/2021
- Shift/Day: GS (Normal)
- Attendance Status: AB (AB)
- Attendance Values: Applied
- Reason: Personal

Below the filters is a search bar and a table of attendance punches:

Date	Time	Device Name	Access
07/06/2021	09:00		
07/06/2021	12:00		

Below the table is a 'Break' section with a search bar and a table:

Break	Date	Time	Special Function
Start			
End			

Below the break table is an 'Approval Details' section with a search bar and a table:

Incharge	Status	Remark
ric2 - RIC2	⊗	
ric1 - RIC1	⊗	

The **Attendance Values** has the following options:

The screenshot shows the 'All Attendance Punches' window with the 'Attendance Values' dropdown menu open. The dropdown menu has three options: 'Applied', 'On Application', and 'Current'. The 'Applied' option is currently selected.

The search filters are:

- User: 1551SU (Shalini User)
- Attendance Date: 2017/02/06
- Shift/Day: GS (Normal)
- Attendance Status: AB (AB)
- Attendance Values: Applied
- Reason: Applied
- Remark: Current

Below the filters is a search bar and a table of attendance punches:

Date	Time	Device Name	Access
2017/02/06	09:00		
2017/02/06	17:00		

- **On Application:** Displays punch details at the time of application.
- **Applied:** Displays applied punch values.
- **Current:** Displays current punch values for the selected date.

As per the option selected in **Attendance Values** the details will be displayed below.

All Attendance Punches window displays the user's attendance and break details. It also displays the status of user's attendance correction application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".






Remarks displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.

Approved Applications

Click the **Approved** collapsible panel.

The **Approved** section displays all the attendance correction applications that have been approved by the reporting group in-charge or the system administrator. The following screen displays the **Approved** section.

Pending (7)													
Approved (20)													
Search													
User ID	Name	Application Date	Attendance Date	Shift	WO/PH	1st Punch	2nd Punch	3rd Punch	4th Punch	Approve	Reject	Remark	Details
adminalert	adminalert	03/11/2017	05/09/2017	GS		09:00	18:30			<input checked="" type="checkbox"/>	<input type="checkbox"/>	approvwvee	
adminalert	adminalert	03/11/2017	05/10/2017	GS		09:00	18:30			<input checked="" type="checkbox"/>	<input type="checkbox"/>	approve	
NpunchAS	Npunchforautoshift	17/11/2017	15/11/2017	NS		21:00	05:00			<input checked="" type="checkbox"/>	<input type="checkbox"/>		
NpunchAS	Npunchforautoshift	17/11/2017	15/11/2017	GS		21:00	05:00			<input checked="" type="checkbox"/>	<input type="checkbox"/>		
NpunchAS	Npunchforautoshift	17/11/2017	02/10/2017	ES		05:00	21:00			<input checked="" type="checkbox"/>	<input type="checkbox"/>		
1 - 5 of 20 records													
<div> « < 1 2 3 4 > » </div>													
Rejected (10)													

Click the **Details**  icon to view the attendance details of the corresponding user.

All Attendance Punches window appears as shown below:

All Attendance Punches

User: U4 User4

Attendance Date: 07/06/2021

Shift/Day: GS Normal

Attendance Status: AB AB

Attendance Values: On Application

Reason: Personal

Search

Date	Time	Device Name	Access
No Data			

Break

Search

Break	Date	Time	Special Function
Start			
End			

Approval Details ✓

Incharge	Status	Remark
RI2 - Riili2	✓ (14/06/2021 16:18)	Approved Attendance RG2

The **Attendance Values** has the following options:

All Attendance Punches

User: 1551SU Shalini User

Attendance Date: 2017/02/06

Shift/Day: GS Normal

Attendance Status: AB AB

Attendance Values: Applied

Reason: On Application

Remark: Applied

Search

Date	Time	Device Name	Access
2017/02/06	09:00		
2017/02/06	17:00		

- **On Application:** Displays punch details at the time of application.
- **Applied:** Displays applied punch values.
- **Current:** Displays current punch values for the selected date.

As per the option selected in **Attendance Values** the details will be displayed below.

All Attendance Punches window displays the user's attendance and overtime details. It also displays the status of user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".


Remarks displays the comments provided by the Admin / RIC / System.

Click **Save** to save the authorization.

Rejected Applications

Click the **Rejected** collapsible panel.

This section lists all attendance correction requests that have been rejected. The following screen is an example of an **Rejected** list of attendance correction requests for a specific date range:

Rejected (5)													
Search													
User ID ▲	Name	Application Date	Attendance Date	Shift	WO/PH	1st Punch	2nd Punch	3rd Punch	4th Punch	Approve	Reject	Remark	Details
KJ	Khushal	03/08/2022	01/08/2022	GS		09:00	21:00			<input type="checkbox"/>	<input checked="" type="checkbox"/>	Rejected Attendance Correction	
KJ	Khushal	03/08/2022	01/08/2022	GS		09:00	19:00			<input type="checkbox"/>	<input checked="" type="checkbox"/>	Rejected Attendance Correction	
KJ	Khushal	03/08/2022	01/08/2022	GS		09:00	14:00			<input type="checkbox"/>	<input checked="" type="checkbox"/>	Rejected Attendance Correction	
KJ	Khushal	03/08/2022	01/08/2022	GS		09:00	18:00			<input type="checkbox"/>	<input checked="" type="checkbox"/>	Rejected Attendance Correction	

Click the **Details**  icon to view the attendance details of the corresponding user.

All Attendance Punches window appears as shown below:

The screenshot shows the 'All Attendance Punches' window. It includes search filters for User (U4, User4), Attendance Date (17/06/2021), Shift/Day (GS, Normal), Attendance Status, Attendance Values (On Application), and Reason (Personal). Below the filters is a search bar and a table with columns: Date, Time, Device Name, and Access. The table displays 'No Data'. There is also a 'Break' section with a search bar and a table with columns: Break, Date, Time, and Special Function. The 'Approval Details' section shows a table with columns: Incharge, Status, and Remark. The status is marked as rejected with a red 'X' icon.

Date	Time	Device Name	Access
No Data			

Break	Date	Time	Special Function
Start			
End			

Incharge	Status	Remark
SA - System Admin	(X) (17/06/2021 15:12)	Rejected Attendance Correction

The **Attendance Values** has the following options:

The screenshot shows the 'All Attendance Punches' window with the 'Attendance Values' dropdown menu open. The dropdown menu has three options: 'On Application', 'Applied', and 'Current'. The 'Applied' option is selected and highlighted in blue. The search filters are set to User (1551SU, Shalini User), Attendance Date (2017/02/06), Shift/Day (GS, Normal), Attendance Status (AB, AB), and Reason (Applied). Below the filters is a search bar and a table with columns: Date, Time, Device Name, and Access. The table displays two rows of data for the date 2017/02/06.

Date	Time	Device Name	Access
2017/02/06	09:00		
2017/02/06	17:00		

- **On Application** - Displays punch details at the time of application.
- **Applied** - Displays applied punch values.
- **Current** - Displays current punch values for the selected date.

As per the option selected in **Attendance Values** the details will be displayed below.

All Attendance Punches window displays the user's attendance and break details. It also displays the status of user's attendance correction application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remarks displays the comments provided by the Admin / RIC / System.

Click **Save** button to save the changes.

Event Authorization

The Event Authorization plays very important role in terms of attendance of employee. It specifies prior authorization required for the events that should be considered for Attendance. It allows reporting In-charge or System Administrator to validate these events.



*The events will occur only when Authorization Required is enabled from **Time and Attendance module > Policies > Attendance Policy > General Parameters > Event Authorization**.*

Also, the events will depend on the parameters selected from Event Source list-box. Only the selected Event sources will be displayed here.

The System Administrator can Authorize the events from this page in absence of reporting in-charge.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to [“Reporting In-Charge”](#), [“Approval Policy”](#) and [“Configuring Users”](#).

To authorize Events, select the **Time and Attendance module > Authorization/Approval > Event Authorization**.

The **Event Authorization** page will appear as follows:

You can either:

- view all the pending applications for Event Authorization
- set the filters — Date, Filter Users — to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Authorize** check box of the desired entry.

To know more refer to [“Pending Events”](#).



The population on this page depends on the server's database. It might take time to load all pending applications.

Applications according to Set Filters

To Set the Filters,

- **Date:** Select this option to enable the date filter. Select the start and end dates by clicking the respective date selection buttons. This defines the period for which User Events are to be viewed. The end date is by default set to the current date and authorization is not allowed for any later date.
- **Filter Users:** You can filter records according to the desired Enterprise Group, All or for an Individual.

Select **All**, to view authorization status of the applications of all the active users on the system.

Select **Individual**, to view authorization status of the applications of a single user. Click the picklist to select the desired User ID/Name.

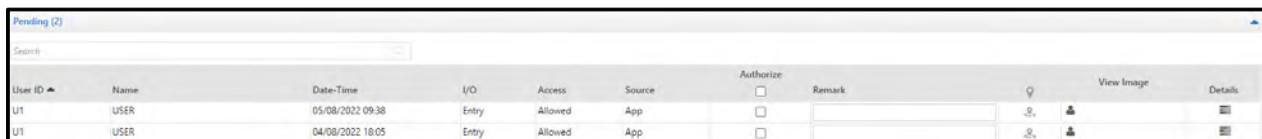
Select the desired Enterprise Group — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Group1/2/3 and then click the picklist to select the desired group's ID/Name, to view authorization status of these applications.

Click the **View** button to view all pending and authorized events and their details.

Pending Events

Click the **Pending** collapsible panel.

The **Pending** section lists all the events from users waiting to be sanctioned by the system administrator as shown:



User ID	Name	Date-Time	I/O	Access	Source	Authorize	Remark	View Image	Details
U1	USER	05/08/2022 09:38	Entry	Allowed	App	<input type="checkbox"/>			
U1	USER	04/08/2022 18:05	Entry	Allowed	App	<input type="checkbox"/>			

- **Access:** Specifies whether the access is allowed/denied to the user.
- **Source:** Displays the sources from where the punch is marked i.e. ESS, Device, Mobile Application, etc.


Select the **Authorize** checkbox against an event to authorize it. The administrator can also select all the applications to authorize at the same time and give the verdict by checking the common Authorized checkbox on the header column.

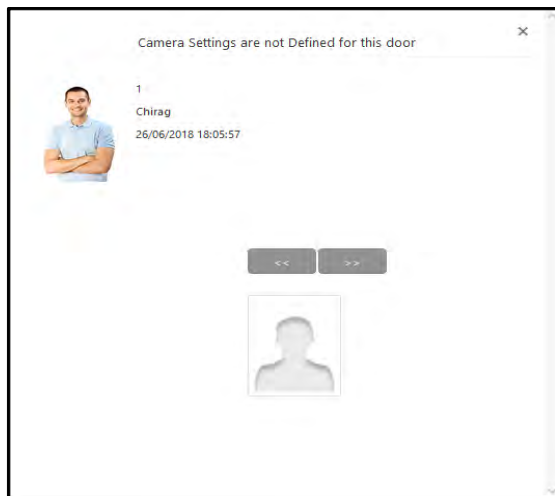
The default **Remark** for the Authorized event application will appear in the respective fields. You can enter your Remark while authorizing the application.

Click the  button to view source location co-ordinate details for an entry or exit event of the user.




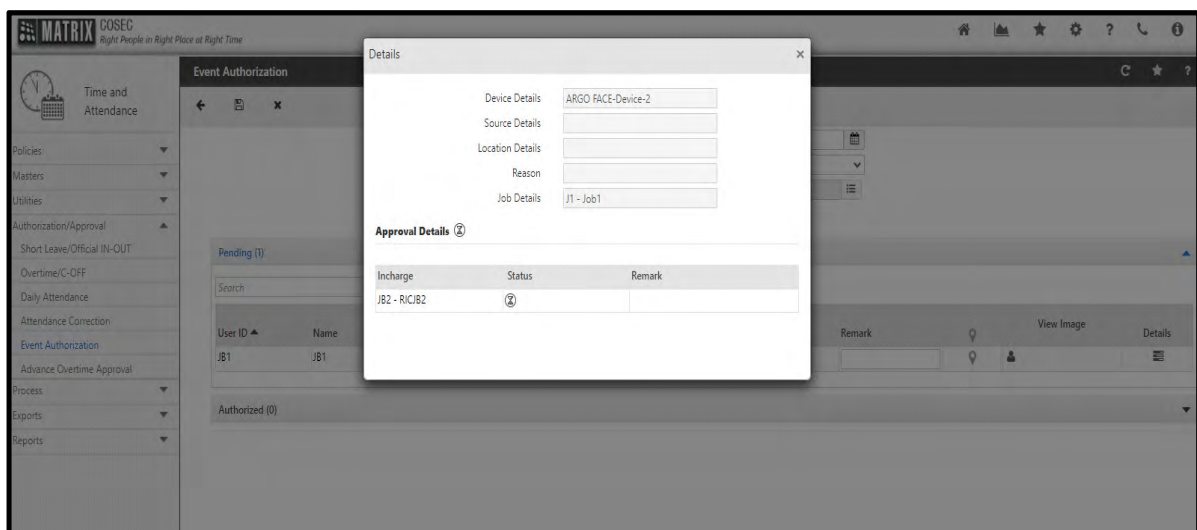
If Map is not loaded; check the network connection or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

If there is a Built-In Camera to capture the image of the user while punching on the door; you can view that image by clicking on the **View Image**  icon.



If the event is generated by API then there will not be any image popup window on clicking View Image icon.

The Reason for punching from unassigned location (when punch is made from Application) can be viewed from **Details** . Click on **Details** and the below window appears:



You can view details like — Device Details, Source Details, Location Details, Reason.

It also displays the status of user's event authorization request under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer [“Approval Policy”](#).

Remarks displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.

Authorized Events

Click the **Authorized** collapsible panel.

The **Authorized** section displays all the events that have been authorized by the reporting group in-charge or the system administrator. The following screen displays the **Authorized** section.

User ID	Name	Date-Time	I/O	Access	Source	Authorize	Remark	View Image	Details
52	Dinesh	03/08/2019 15:36	Entry	Allowed	Device	<input checked="" type="checkbox"/>	Authorized Event		
52	Dinesh	03/08/2019 15:34	Entry	Allowed	Device	<input checked="" type="checkbox"/>	Authorized Event		
52	Dinesh	03/08/2019 15:32	Entry	Allowed	Device	<input checked="" type="checkbox"/>	Authorized Event		
52	Dinesh	03/08/2019 15:21	Entry	Allowed	Device	<input checked="" type="checkbox"/>	Authorized Event		

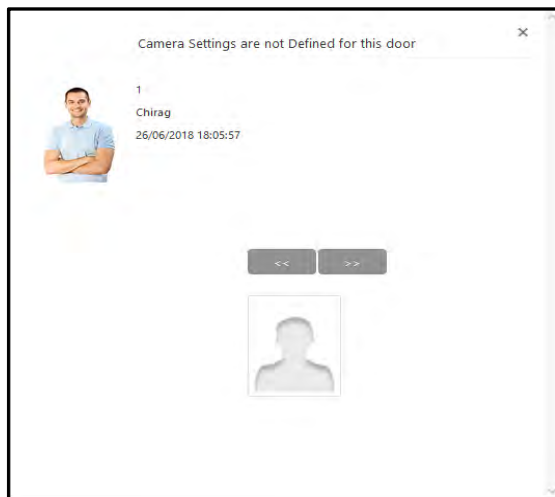
Here, Authorized events can be viewed only.

Click the button to view source location co-ordinate details for an entry or exit event of the user.



If Map is not loaded; check the network connection or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

If there is a Built-In Camera to capture the image of the user while punching on the door; you can view that image by clicking on the **View Image** icon.



If the event is generated by API then there will not be any image popup window on clicking View Image icon.

Click on **Details** and the below window appears.

Details

Device Details

ARGO FACE-Device-2

Source Details

Location Details

Reason

Job Details

J1 - Job1

Approval Details

Incharge	Status	Remark
JB2 - RIC/JB2		

You can view details like — Device Details, Source Details, Location Details, Reason.

It also displays the status of user's event authorization request under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer [“Approval Policy”](#).

Remarks displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.

Advance Overtime Authorization

The Advance Overtime Authorization is providing prior approval for the Advance Overtime Applications of the users. This page will be displayed for System Administrator.



Authorization of Advance Overtime Application performed by a System Account user will always be pre-approved.

Advance Overtime Applications can also be approved by respective Reporting Group In-charges from the ESS application.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to [“Reporting In-Charge”](#), [“Approval Policy”](#) and [“Configuring Users”](#).

To approve the applications,

Select the **Time and Attendance > Authorization/Approval > Advance Overtime Authorization**.

The **Advance Overtime Authorization** page will appear as follows:

You can either:

- view all the pending applications for Advance Overtime Approval
- set the filters — Overtime Date, Filter Users — to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To know more refer to [“Pending Overtime/C-OFF”](#).

Applications according to Set Filters

To Set the Filters,

- **Overtime Date:** Set the start and end dates by clicking the respective date selection buttons. This defines the applications to be displayed within the set dates.
- **Filter Users:** You can filter records according to the desired Enterprise Group, All or for an Individual.

Select **All**, to view authorization status of the applications of all the active users on the system.

Select **Individual**, to view authorization status of the applications of a single user. Click the picklist to select the desired User ID/Name.

Select the desired Enterprise Group — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Group 1,/2/3 and then click the picklist to select the desired group's ID/Name, to view authorization status of these applications.

Click the **View** button to view all pending, authorized and rejected application and their details.

Pending Applications

Click the **Pending** collapsible panel. The **Pending** section lists all the applications of the users awaiting approval by the System Administrator/RIC as shown below.

Show All Pending Applications ☒

Overtime Date ☐ From Date To Date

Filter Users

Group/User

Pending (1)

Search

User	Name	OT Date	OT Hours	Application Date	Approved Hours	Approve	Reject	Remark	Details
1	Athira	12/01/2021	05:00	07/01/2021	05:00	<input type="checkbox"/>	<input type="checkbox"/>		<input type="button" value="Details"/>

When any application is in the Pending state it can be authorized by the Admin or RIC.

- To approve/reject applications selectively, click the respective application check box
- To approve/reject all the applications simultaneously, click the Approve /Reject checkbox in the header column.

Once the Admin approves/ rejects the application, the record will be moved from the **Pending** section to the **Approved/ Rejected** section respectively.

The default **Remark** for the Approved and Rejected application will appear in the respective fields. You can enter your Remark while authorizing the application.

To view the details of a particular application, click on the **Details** . The **Advance Overtime Application Detail** window appears as shown below:

Advance Overtime Application Detail

User U1 User1

Application Details

Application Date 17/06/2021

OT Date 18/06/2021

OT Hours 05:00

Reason Overtime

Address

Contact Number

Approval Details ⓘ

Incharge	Status	Remark
SA - System Admin	ⓘ	

Advance Overtime Application Detail window displays the user's advance overtime application.

This window also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

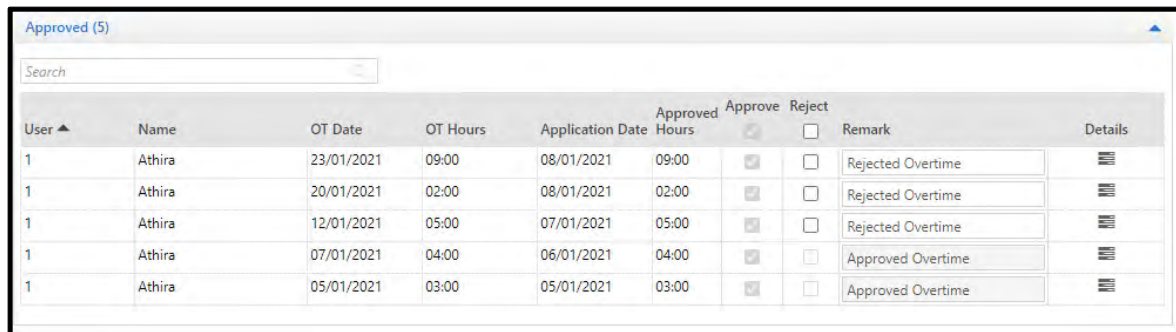
System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".






Remarks displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.

Approved Applications

Click the **Approved** collapsible panel. The **Approved** section lists all the applications of the users that have been approved by the Reporting Group In-Charge/System Administrator as shown below.



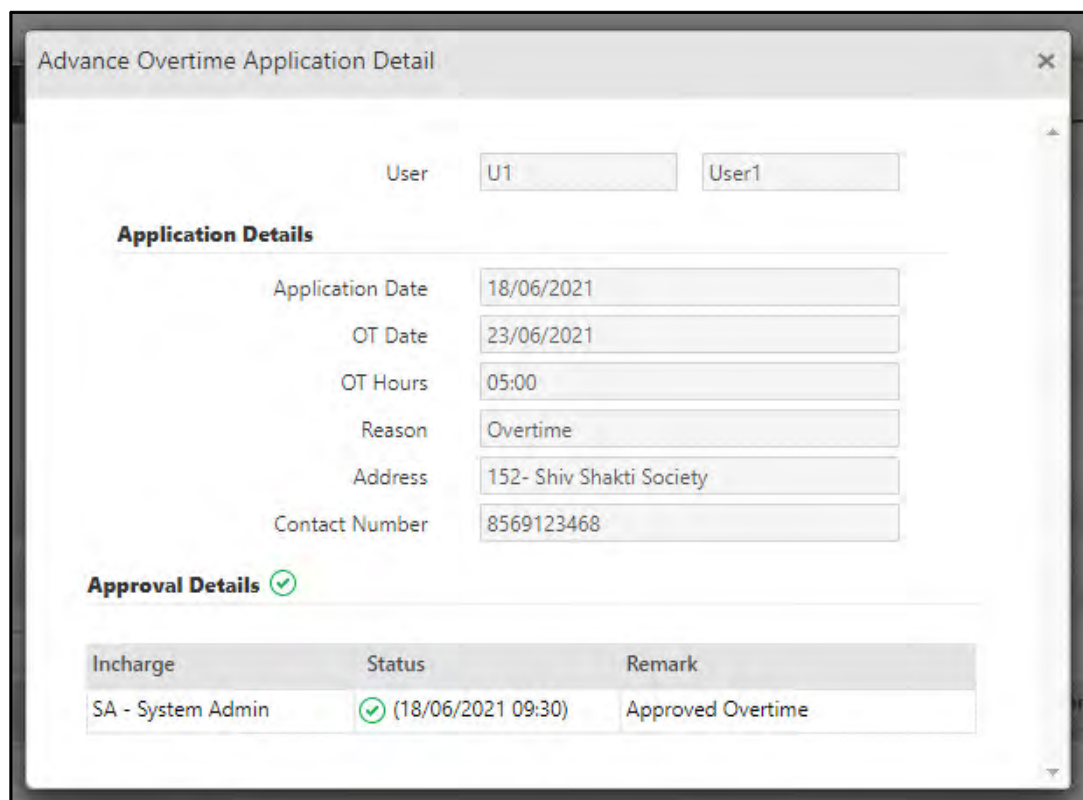
User	Name	OT Date	OT Hours	Application Date	Approved Hours	Approve	Reject	Remark	Details
1	Athira	23/01/2021	09:00	08/01/2021	09:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Rejected Overtime	
1	Athira	20/01/2021	02:00	08/01/2021	02:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Rejected Overtime	
1	Athira	12/01/2021	05:00	07/01/2021	05:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Rejected Overtime	
1	Athira	07/01/2021	04:00	06/01/2021	04:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Overtime	
1	Athira	05/01/2021	03:00	05/01/2021	03:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Overtime	

The Approved applications of present as well as of future dates can be rejected by the RIC, if required. To do so, select the **Reject** checkbox of the respective application.

The Approved applications of the past dates can only be viewed.

Click the **Details**  icon to view the attendance details of the corresponding user.

Advance Overtime Application Detail window appears as shown below:



User

U1

User1

Application Details

Application Date

18/06/2021

OT Date

23/06/2021

OT Hours

05:00

Reason


Overtime


Address

152- Shiv Shakti Society

Contact Number

8569123468

Approval Details 

Incharge	Status	Remark
SA - System Admin	 (18/06/2021 09:30)	Approved Overtime

Advance Overtime Application Detail window displays the user's advance overtime application details. It also displays the status of user's application under **Approval Details**. The application's status is displayed in the **Status** column.

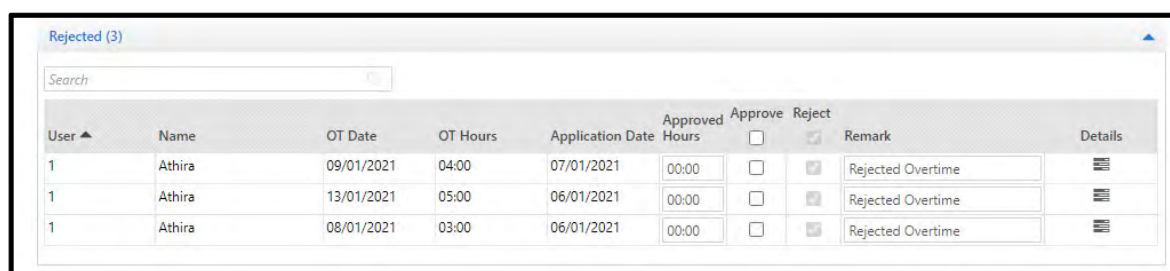
System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer [“Approval Policy”](#).

Remark displays the comments provided by the Admin / RIC / System.

Click **Save** to save the authorization.

Rejected Applications

Click the **Rejected** collapsible panel. The **Rejected** section lists all the applications of the users that have been rejected by the Reporting Group In-Charge or the System Administrator as shown below.



User ▲	Name	OT Date	OT Hours	Application Date	Approved Hours	Approve <input type="checkbox"/>	Reject <input checked="" type="checkbox"/>	Remark	Details
1	Athira	09/01/2021	04:00	07/01/2021	00:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Rejected Overtime	
1	Athira	13/01/2021	05:00	06/01/2021	00:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Rejected Overtime	
1	Athira	08/01/2021	03:00	06/01/2021	00:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Rejected Overtime	

The Rejected applications of present as well as future dates can be approved by the Reporting Group In-Charge/ System Administrator, if required. To do so, select the **Approved** checkbox of the respective application and specify the **Approved Hours**.

The Rejected applications of the past dates can only be viewed.

Click the **Details** icon to view the attendance details of the corresponding user.

Advance Overtime Application Detail window appears as shown below:

Advance Overtime Application Detail

User

U1

User1

Application Details

Application Date

18/06/2021

OT Date

23/06/2021

OT Hours

05:00

Reason

Overtime

Address

152- Shiv Shakti Society

Contact Number

8569123468

Approval Details

Incharge	Status	Remark
SA - System Admin	⊗ (18/06/2021 09:38)	Rejected Overtime

Advance Overtime Application Detail window displays the user's advance overtime application details. It also displays the status of user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remark displays the comments provided by the Admin / RIC / System.

Click **Save** button to save the changes.



System Administrator can delete pending/approved/rejected application.

Processing Attendance

This option enables an HR user to manually run certain processes required for generation of shifts, daily attendance and month-end attendance data. Attendance data for users is generated as per their entry/exit punches and scheduled entry/exit time. This is achieved by assigning the shifts to the users for each day of the attendance period. Shift schedule generation does the process of assigning shift for each day of the month as per the schedule group allotted to user.

To Process Daily Attendance [See “Processing Daily Attendance” on page 1625.](#)

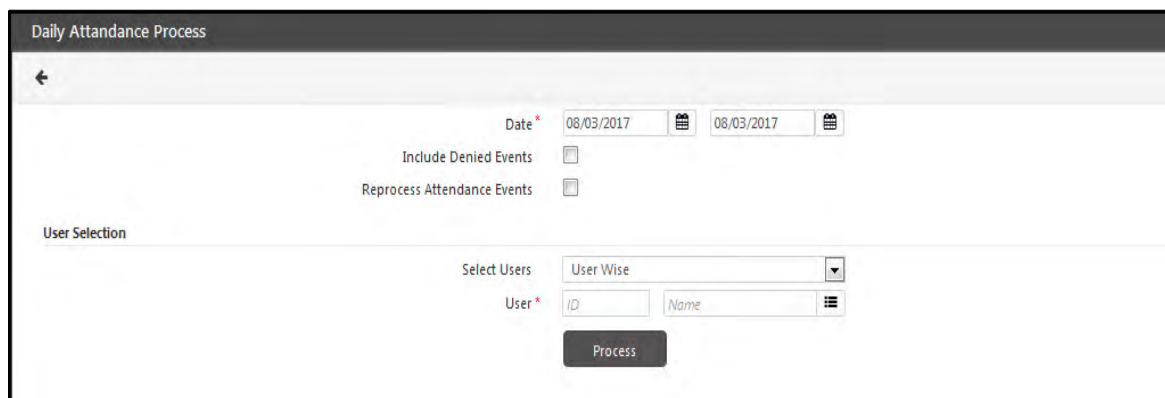
To Process Monthly Attendance [See “Processing Monthly Attendance” on page 1626.](#)

Processing Daily Attendance

This process will enable the HR user to calculate the times related to attendance marking as per scheduled shift and then mark the attendance for a day. This is on regularized, authorized and summarized based on the Attendance Policy which generate the attendance summary data which can be used as input for salary calculation by any other application after importing the data in required format. Based on the attendance marking events of the day the system calculates the working hours, overtime hours and late-in/early-out hours for the day.

To run the Attendance process, select the **Time and Attendance module > Process > Daily Attendance**.

The **Daily Attendance Process** page appears as shown:



The following options appear on the **Daily Attendance Process** page for configuration:

- **Date:** Specify the Start and End dates to define the period for which daily attendance is to be processed.
- **Include Denied Events:** Select this checkbox to enable denied user events to be considered for daily attendance processing.
- **Reprocess Attendance Events:** Select this checkbox to reprocess all attendance events based on the new policy settings:

When Time & Attendance policy or shift of user for previous day is changed then it is required to Reprocess Attendance events to correct the attendance calculation.

Example: If user is assigned GS from 1st to 10th of a month. And user is coming in NS from 4th to 7th of month. When you are running the Daily Attendance process on 10th; then it is must to Reprocess Attendance Events to calculate the punches as per the assigned shift.

For the events that requires authorization, Only the authorized events will be considered when **Process** is clicked. Hence, the User Denied Events are not considered for Authorization.



Indiscriminate use of the **Reprocess Attendance Events** option is not recommended as it will revert all changes made using the **Manual Correction** option.



For Site based and Location based Auto Tour feature; when the Tour application is automatically applied/ generated; then it cannot be revert back even after reprocessing events. The user has to manually delete/ apply for cancellation if needed.

- **Select Users:** Specify the group of users whose daily attendance data is to be processed in this section. To specify users, select one of the following options in the User Filter dropdown list:
 - **User Wise:** Enables administrator to randomly select users from the user Picklist window.
 - **Group Wise:** Enables the administrator to select all users belonging to a particular group.
 - **All:** Enables administrator to select all active users in the database.

Click the **Process** button to start processing daily attendance data.

Processing Monthly Attendance

This process will enable the HR user to generate a summary of the attendance period as per the defined attendance policy. In addition, previous adjustment data will be generated for allowed previous closed attendance period. Once this is done, the system allows the HR user to close the current attendance period.

To start the process, select the **Time & Attendance module > Process > Monthly Attendance**.

The **Monthly Attendance Process** page appears as shown:

The following options appear on the **Monthly Attendance Process** page:

- **Attendance Period:** Select the month and the year for which the process is to be run.
- **Send Alert to Users:** Select this checkbox if an alert message is to be sent to the assigned users at the end of the process.

- **Close Attendance Period:** Select this checkbox to close the chosen attendance period after the process is run. This will ensure that no data can be changed or processed for this period any further.

Suppose the Attendance period for June 2018 is closed and there are pending Award/Penalty authorization applications of June so

- those applications will not be allowed to authorize if Attendance Correction in Attendance Policy is disabled.
- those applications will be allowed to authorize if Attendance Correction in Attendance Policy is enabled for the valid period of adjustment.



Close Attendance Period check-box will not appear if “Adjustment Generated for Closed Period” in Attendance Policy is enabled.

- **Select Users:** Specify the group of users whose monthly attendance data is to be processed in this section. To specify users, select one of the following options in the **User Filter** dropdown list:
 - **User Wise:** Enables administrator to randomly select users from the user Picklist window.
 - **Group Wise:** Enables the administrator to select all users belonging to a particular group.
 - **All:** Enables administrator to select all active users in the database.

Click the **Process** button to start processing monthly attendance data.



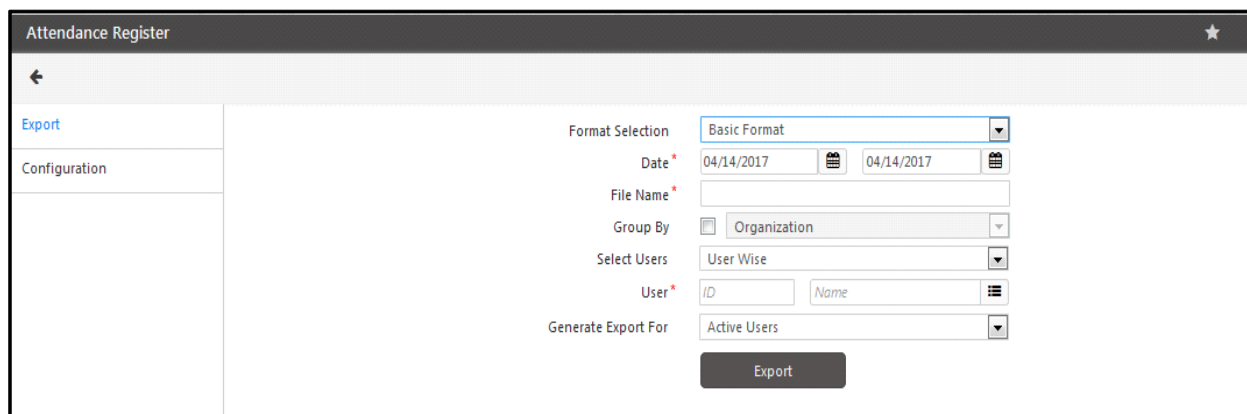
Monthly Attendance Process can be run for one month in future for custom attendance period. But if process is attempted for an entirely future attendance period w.r.t. current date; then it will not be processed.

Attendance Register Export

The COSEC system has the functionality to export attendance register data for a particular period in Excel format. The administrator needs to configure output code for each combination of the attendance status based on the site requirements.

To access this functionality, Select the **Time and Attendance module > Exports > Attendance Register**.

The **Attendance Register** page opens as follows:



The screenshot shows the 'Attendance Register' page with a sidebar on the left containing 'Export' and 'Configuration' links. The main area contains the following fields:

- Format Selection: Basic Format (dropdown)
- Date: 04/14/2017 (calendar icon) to 04/14/2017 (calendar icon)
- File Name: (empty text field)
- Group By: Organization (dropdown)
- Select Users: User Wise (dropdown)
- User: ID (text field) Name (text field) (list icon)
- Generate Export For: Active Users (dropdown)
- Export button

Export



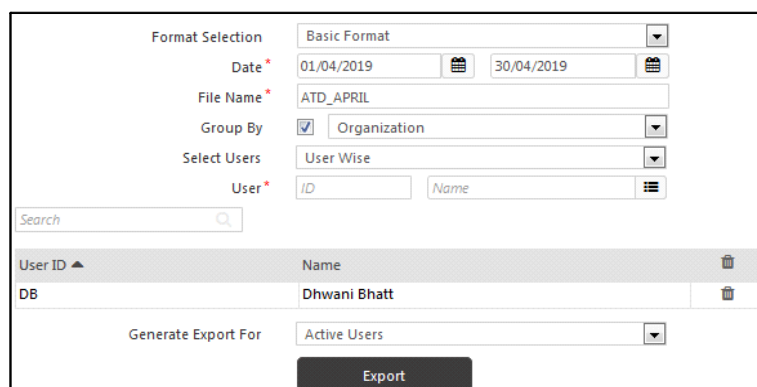
Before Exporting you must do **“Configuration”** for the Export parameters.

Format Selection: Select the Format from the options of **Basic Format** and **Form 25**.

Basic Format

Date: If Basic Format is selected then select a date range for data export using the date selection buttons.

Filename: Enter an appropriate Filename for the file to be exported as shown.



The screenshot shows the 'Attendance Register' page with the following values filled in:

- Format Selection: Basic Format (dropdown)
- Date: 01/04/2019 (calendar icon) to 30/04/2019 (calendar icon)
- File Name: ATD_APRIL
- Group By: ☒ Organization (dropdown)
- Select Users: User Wise (dropdown)
- User: ID (text field) Name (text field) (list icon)
- Search: (empty text field)
- User ID: DB (dropdown)
- Name: Dhvani Bhatt (text field)
- Generate Export For: Active Users (dropdown)
- Export button

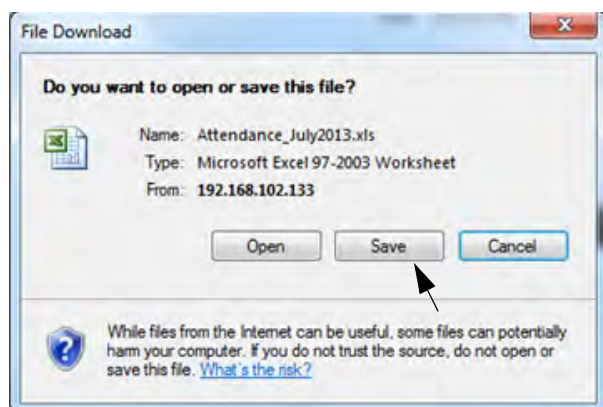
Group By: Check the box and select the Enterprise group.

Select Users: Select the user based on one of the following filters from the drop down list:

- **User Wise** - To select users randomly by clicking the User picklist.
- **Group Wise**- To select all users associated with a particular enterprise group using the **Select Group** dropdown list.
- **ALL** - To select all users active in the system.

Generate Export For: You can Generate Export For All Users, Active Users or Inactive users.

Click the **Export** button. You can open or save the exported file at a desired location.



Save the file at a desired location. The following figure illustrates an attendance register exported as an Excel file for the month of July, 2013:

SrNo	User ID	Name	Designation	01Jul Mon	02Jul Tue	03Jul Wed	04Jul Thu	05Jul Fri	06Jul Sat	07Jul Sun	08Jul Mon	09Jul Tue	10Jul Wed	11Jul Thu	12Jul Fri	13Jul Sat	14Jul Sun	15Jul Mon	16Jul Tue
1	11	SALIM ANSARI	Engineer	W	P	P	P	P	P	W	P	P	P	P	P	P	W	P	P
2	10	RAJENDRA GOSWAMI	Team Leader	W	P	P	P	P	P	W	P	P	P	CL	P	P	W	P	P
3	1001	ANKITKUMAR SOHLIYA	Engineer	P	P	P	P	P	P	W	P	P	P	P	P	W	W	P	P
4	1002	MEGHA H SHUKLA	Engineer	P	P	P	P	P	P	W	P	P	P	P	P	W	W	CL	P
5	1003	UMESH M TALANPURI	Team Leader	P	P	P	P	P	P	W	P	P	P	P	P	W	W	P	P
6	1004	DARSHAK B PATEL	Engineer	P	P	P	P	P	P	W	P	P	P	P	P	W	W	????	P
7	1007	DHAVAL I PATEL	Engineer	P	P	P	P	P	P	W	P	P	P	P	P	W	W	P	P
8	1008	MAYANK K KORAT	Engineer	P	P	P	P	P	P	W	P	P	P	P	P	W	W	P	P
9	1009	DIPTI K RATHWA	Team Leader	????	P	P	P	P	CL	W	CL	CL	CL	CL	CL	W	W	CL	P
10	1010	RAHUL S SHAH	Engineer	P	P	P	P	P	CL	W	P	P	P	P	P	W	W	P	P
11	1011	PARIKA S PANDEY	Engineer	P	P	P	P	OD	P	W	P	P	P	P	P	W	W	P	P

Form 25

Month-Year: If Form 25 is selected then select the month and year for which the data is to be exported.

Custom Attendance Period: Check the box to enable the custom attendance period and select the **month start date- end date** for which the data is to be exported. The month end date is automatically generated as per start date selection.

Attendance Register

[Export](#)

Configuration

Format Selection: Form 25

Month-Year: April 2017

Custom Attendance Period: ☐

Month Start-End Date: 2 1

File Name: Attendance_april

Select Users: User Wise

User: ID Name

Search

User ID	Name
07	Aditi
101	Khushbu
1567	Sheetal
2	Chirag

Generate Export For: Active Users

Export

Filename: Enter an appropriate Filename for the file to be exported.

Select Users: Select the user based on the filters of User Wise, Group Wise or All.

Generate Export for: You can Generate Export For All Users, Active Users or Inactive users.

Click the **Export** button. You can open or save the exported file at a desired location.



Before exporting data run the monthly attendance process for the users.

The Form 25 will be generated in excel format as shown below:

Attendance_april [Read-Only] [Compatibility Mode] - Microsoft Excel

FileHomeInsertPage LayoutFormulasDataReviewView

CutCopyFormat Painter

Paste

Clipboard

Arial10

B*I*U

Font

Wrap Text

Merge & Center

Alignment

General

\$ % +

Number

Conditional Formatting

Format as Table

Cell Styles

Styles

Insert

Delete

Format

Cells

AutoSum

Fill

Clear

Editing

Sort & Filter

Find & Select

AN28

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	
1	Form No. 25																																								
2	Matrix RnD Form25																																								
3	Register of Muster Roll for the Month of April-2017																																								
4	Dated: 05/02/2017 16:19																																								
5	S.No.	Name of the User	Father/Spouse Name	Designation Nature of Work	Date of Birth to be Supported by Extract from Birth			Place of Employment	FOR THE PERIOD ENDING DAYS																												No. of Days Worked	No. of Days of Leave with Wages	No. of Days Absent		
					Date	Month	Year		Saturday	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday										
6	1	2	3	4	5			6	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	10	11	12
7	07	Aditi	AK	Designation-1	9	Februar	1993	Branch-1	P	??	P	P	P	P	P	??	P	P	P	P	P	P	P	??	P	P	P	P	P	A	A	??	A	A	A	A	A	??	23	0	7
8	101	Khushbu		Designation-1	11	Novemb	1993	Branch-1	A	A	A	A	A	A	A	A	??	A	A	A	A	A	A	??	A	A	A	A	A	A	A	A	A	A	A	A	A	??	0	28	
9	1567	Sheetal		Designation-1	12	May	1987	Branch-1	P	A	P	A	P	A	P	??	A	A	A	A	A	A	A	??	A	A	A	A	A	A	A	A	A	A	A	A	A	??	9	0	21
10	2	Chirag		Designation-1	9	May	1990	Branch-1	A	A	??	??	??	??	A	??	A	A	A	A	A	A	A	??	A	A	A	A	A	A	A	A	A	A	A	A	A	2	4	24	



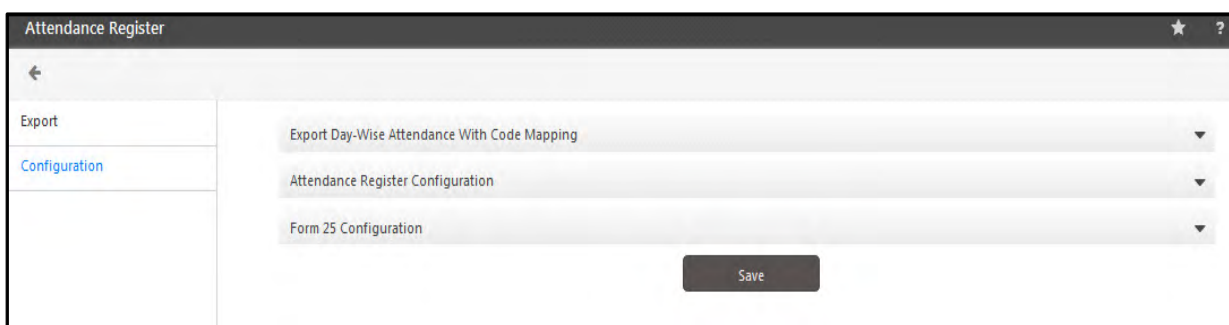
In case if user applied leave for some future date and was made inactive before that date, then too its reflection in any field after it is made inactive will not be shown anywhere.

In "Basic Format" if proper data is required then "Daily Process" must be called.

Configuration

Attendance Register Export can be configured to determine which data appears in the exported file and how.

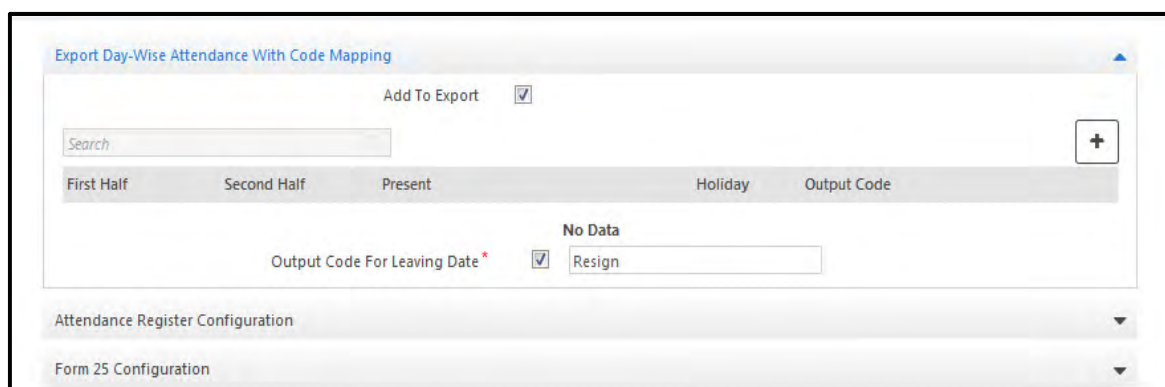
To do this, On the **Attendance Register** page, select the **Configuration** tab as shown.



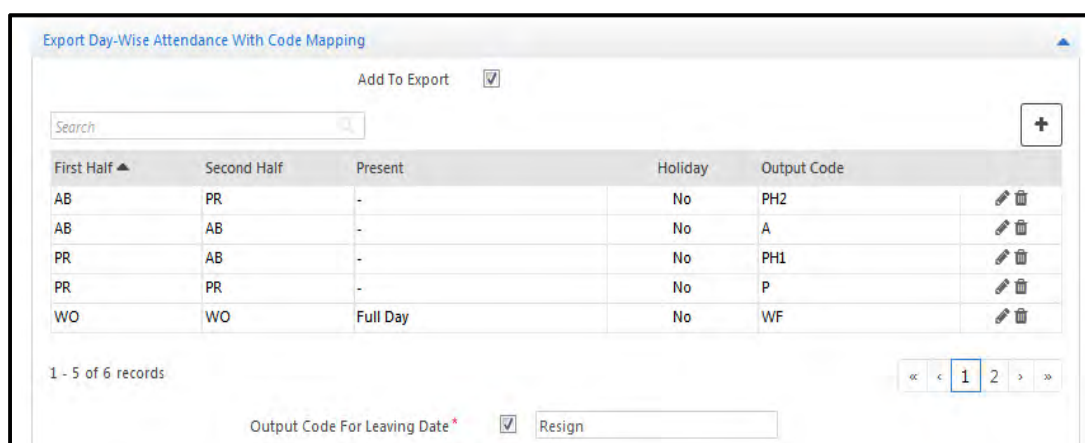
Export Day-Wise Attendance With Code Mapping

Select the **Add to Export** button to include day-wise attendance with the configured code in the exported file.

This section enables the administrator to map different combinations of attendance statuses for a day to a user defined output code.



Click **Add** button to configure the output code for different combinations of first half and second half status.



In the above example, the output code for a combination of a “Present” status in the first half, and “Absent” status in the second half for a user is defined as “PH1”. User can also set separate codes for full day present and half day present on a Week Off/Public Holiday, as shown above.

An output code can also be defined against a user’s Leaving Date i.e. the last day of the user in the organization (e.g. “Resign”).

Attendance Register Configuration

Select Fields to Export: Select the checkboxes for the Fields to include them during export from the COSEC database.

Export Day-Wise Attendance With Code Mapping

Attendance Register Configuration

Select Fields To Export

Search

Fields	
User ID	<input checked="" type="checkbox"/>
User Name	<input checked="" type="checkbox"/>
Organization Code	<input type="checkbox"/>
Organization Name	<input checked="" type="checkbox"/>
Branch Code	<input type="checkbox"/>

1 - 5 of 63 records

Include Summary in Export ☒

Export Per Leave Summary

Add To Export ☒

Search

Leave ID	Leave Name	Output Code
01	Paid Leave	PL1

Form 25 Configuration

Save

Include Summary in Export: Enable this check box to provide the sum total of the values of specific fields in export.

The following fields can be included in the summation.

- 1.<Daily> Work Hours
- 2.<Daily> Loss Hours
- 3.<Daily> Extra Work Hours
- 4.<Shift-Wise> Attendance
- 5.Shift-Allowance Presence
- 6.Present
- 7.Absent
- 8.Leaves
- 9.Holiday-Present
- 10.PH-HD/FD-Present
- 11.Work-Hours-On-Holiday
- 12.Week-Off-Present
- 13.WO-HD/FD-Present
- 14.Work-Hours-On Week-Off
- 15.Generated Overtime

- 16.Total Authorized Overtime
- 17.Authorized OT1
- 18.Authorized OT2
- 19.Authorized OT3
- 20.Authorized OT4
- 21.Authorized OT5
- 22.Gross-Work Hours
- 23.Total Planned-Hours
- 24.Net-Work-Hours
- 25.Extra-Work-Hours
- 26.Total-Late-In
- 27.Total-Early-Out
- 28.Total-Loss-Hours
- 29.Total-Paid-Leaves
- 30.Total-Unpaid-Leaves
- 31.Total-Lay-Off
- 32.Total-C-Off
- 33.Total-Tour
- 34.Week <no>-Work Hours
- 35.Payable Days
- 36.Total Days
- 37. Short Leave
- 38. Official Hour

Export Per Leave Summary

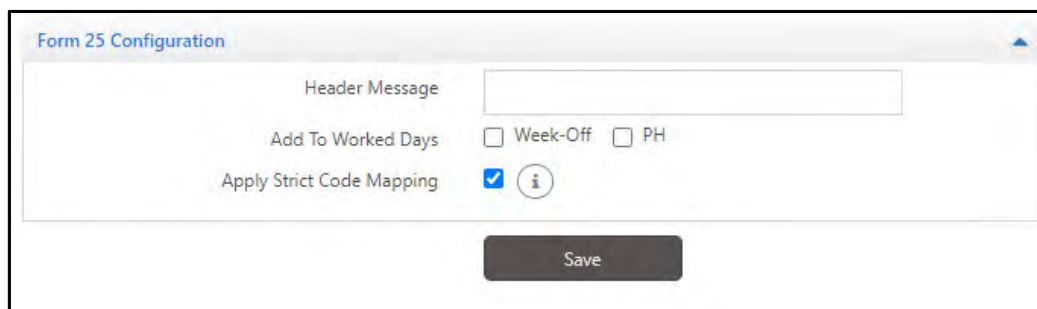
Enable the **Add to Export** checkbox to include the leave summary in exported file.

This section enables the user to define codes for various leave types in the exported file. Eg: The output code for Paid leave is set as "PL1".

Form 25 Configuration

Form 25 format displays the attendance details of employees. These may differ from organization to organization. You can configure them as per your requirement.

Enter a custom **header message** that will appear on Form 25.

The image shows a 'Form 25 Configuration' dialog box. It has a title bar with the text 'Form 25 Configuration' and a close button. Inside the dialog, there is a text input field labeled 'Header Message'. Below this, there are two checkboxes: 'Add To Worked Days' and 'Week-Off'. The 'Week-Off' checkbox is checked, and there is an information icon (i) next to it. To the right of the 'Week-Off' checkbox is another checkbox labeled 'PH'. At the bottom of the dialog, there is a 'Save' button.

Select the **Week-Off** and/or **PH** checkboxes to include week-offs and/or public holidays in working days for the selected month.

Select **Apply Strict Code Mapping** checkbox to apply Code Mapping on all the attendance data which are to be exported. You can configure code mapping from **Export Day-Wise Attendance with Code Mapping**.

To know more about **Export Day-Wise Attendance with Code Mapping**, refer [“Export Day-Wise Attendance With Code Mapping”](#).

Example: Export data on 21/05/2021

Case 1: If Apply Strict Code Mapping = Disabled

Export Day-Wise Attendance with Code Mapping

First IN	Second IN	Output Code
IN	AB	AB

In this case, the code mapping is applicable till the date 20/05/2021 while exporting the data.

Case 2: If Apply Strict Code Mapping = Enabled

Export Day-Wise Attendance with Code Mapping

First IN	Second IN	Output Code
IN	AB	AB

In this case, the code mapping is applicable till the date 21/05/2021 while exporting the data.

Click the **Save** button to save these configurations for the next export.

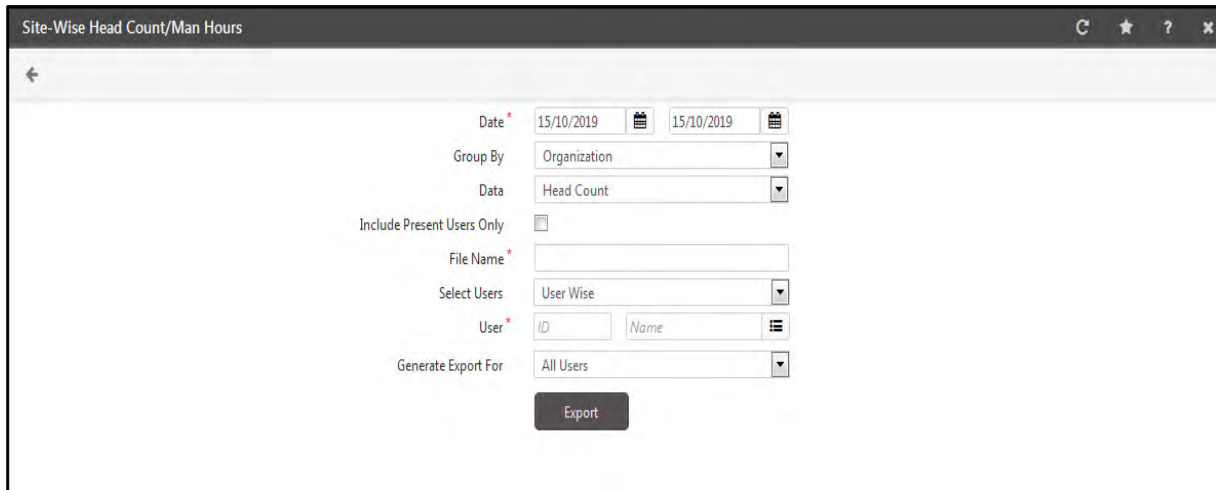
The Exported file is shown in [“Export”](#) section.

Site-Wise Head Count/Man Hours Export

The COSEC Time and Attendance module enables the export of data in Excel format based on both the total head count of personnel as well as the total man-hours count for all sites associated with a particular enterprise group (such as *Organization*, *Branch* etc).

To access this functionality, Select the **Time and Attendance module > Exports > Site-Wise Headcount/Man Hours**.

The **Site-Wise Headcount/Man Hours** page opens as follows:

A screenshot of a web application window titled "Site-Wise Head Count/Man Hours". The window contains a form with the following fields: "Date" with two date pickers set to "15/10/2019"; "Group By" with a dropdown menu showing "Organization"; "Data" with a dropdown menu showing "Head Count"; "Include Present Users Only" with an unchecked checkbox; "File Name" with an empty text input field; "Select Users" with a dropdown menu showing "User Wise"; "User" with two input fields labeled "ID" and "Name"; and "Generate Export For" with a dropdown menu showing "All Users". An "Export" button is located at the bottom right of the form.

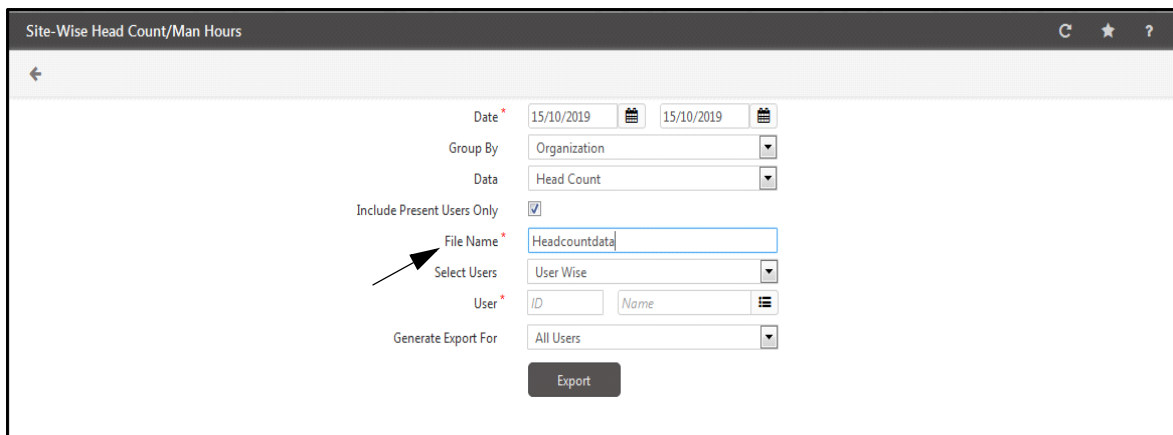
Date: Select a date range for data export by selecting the date selection buttons.

Group By: Select an enterprise group from the Group By drop down list, for which the data is to be exported.

Data: Select the option as **Head Count**, **Man-hours** or **Work Hours** based on which the Site Wise data is to be exported.

Include Present Users Only: Enable this checkbox to ensure that the headcount is increased only if a user is present for a full day for an attendance date within the specified date range.

Filename: Enter an appropriate Filename for the file to be exported as shown.

A screenshot of the same web application window as above, but with the "File Name" field highlighted by a blue border and a black arrow pointing to it. The text "Headcountdata" is entered into the "File Name" field. All other fields and the "Export" button remain the same as in the previous screenshot.

Select Users: Select the user based on one of the following filters from the drop down list:

- **User Wise** - To select users randomly by selecting the user from the picklist.
- **Group Wise** - To select all users associated with a particular enterprise group using the **Select Group** dropdown list.
- **ALL** - To select all active users in the system.

Generate Export for: Select the users as All, Active or Inactive for which Site-wise headcount/Man Hours are to be exported.

Click the **Export** button.

Site-Wise Head Count/Man Hours

Date: 15/10/2019

Group By: Organization

Data: Head Count

Include Present Users Only: ☒

File Name: Headcountdata

Select Users: User Wise

User: ID Name

Search

User ID	Name
1	Yagnesh
123	Suresh
13	Sujal
15	Rushi
2	Yesha

1 - 5 of 7 records

Generate Export For: Active Users

Export

You can open or save the file in a suitable location. The following figure illustrates a sample Excel file with the site-wise head count for Organization.

Site-Organization Wise Head Count Summary From 05/01/2017 To 05/01/2017			
Sr No	Site Name	Organization-1[1]	Matrix[2]
1	HO Site	0	2
2	Matrix- RnD	0	2

The data based on Man hours is shown as below.

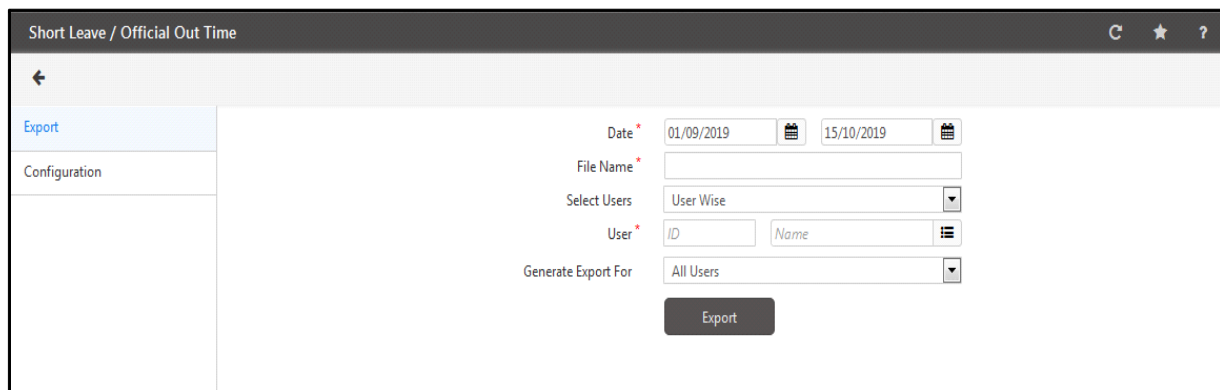
Site-Organization Wise Man Hours Summary From 05/01/2017 To 05/01/2017			
Sr No	Site Name	Organization-1[1]	Matrix[2]
1	HO Site	00:00	18:00
2	Matrix- RnD	00:00	09:02

Short Leave/Official Out Time Export

This functionality enables you to export specific data related to Short Leave/Official IN-OUT marking of users such as total duration of short leaves (authorized/unauthorized), total duration of Official Out Time (authorized/unauthorized), reason-wise hours authorized as short leave or official marking etc. The data can be exported in Excel format.

To access this functionality, Select the **Time and Attendance module > Exports > Short Leave/Official Out Time**.

The page opens as follows:

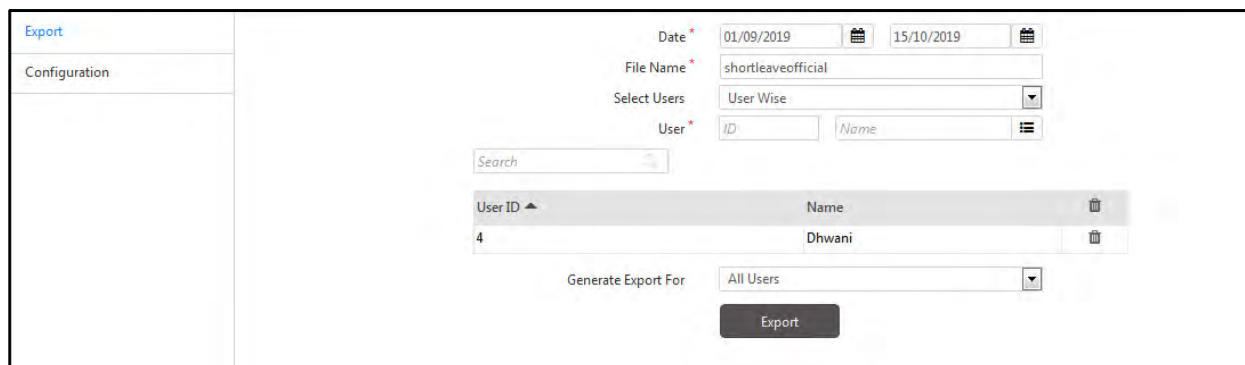


Export



Before Exporting you must do **“Configuration”** for the Export parameters.

- You can select the **date** range to export the Short leave, Official out time for the desired duration of the month.
- Specify the alphanumeric **filename** with upto 20 character as the name of the file to be exported.
- **Select Users:** You can select the users based on filter options of User Wise, Group Wise (Enterprise groups) or All users (active/inactive/ all).
- **Generate Export for:** Select the users as **All, Active** or **Inactive** for which Short leave, Official out time is to be exported.



Finally Click on Export button to Export the Short leave, Official out time for the selected user.

Short Leave / Official Out Time From 04/01/2017 To 04/30/2017											
	A	B	C	D	E	F	G	H	I	J	K
1	Short Leave / Official Out Time From 04/01/2017 To 04/30/2017										
2	User ID	Name	Total Late-IN-Hours	Total Early-OUT-Hours	OUT Meeting with Client Hours	OUT Health not fine Hours	IN Presentation Hours	Total-Out-Time	Total-Authorized-Short-Leave-Hours	Total-Unauthorized-Short-Leave-Hours	Total-Authorized-Official-IN/OUT-Hours
3	1567	Sheetal	00:12		08:00	00:30	00:30	09:00	00:30		08:30
4											

Configuration

The **Short Leave/Official Out Time** export can be configured to determine which data is to be exported in the exported file.

Select Fields to Export: Select the appropriate checkboxes against the required fields to include them during the export of Short Leave/Official Out time.

Reason-Wise Out Time: You can select the IN/OUT reasons for which the IN/OUT timings are to be exported.

- Select the **Add to Export** checkbox to add the authorized personal or official out time corresponding to the selected IN/OUT Reasons. To configure In/OUT reasons go to T&A> Masters > In/Out Reasons.
- Select the **Total Out Time** and **No Reason** checkboxes to add these fields to the export.

- Select one or more **IN/OUT Reasons** using the corresponding picklist.
- Click the **Save** button to save these configurations for the next export.

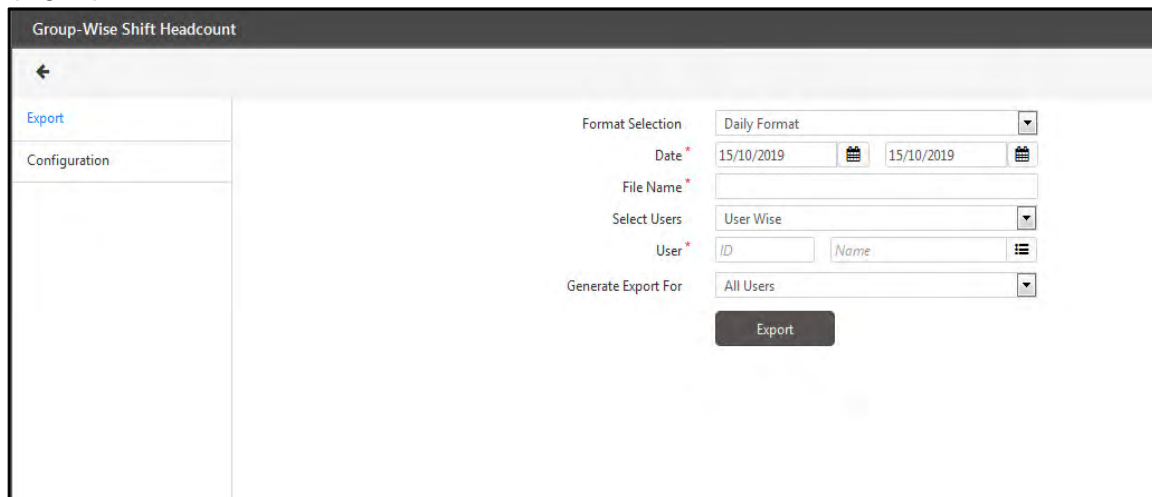
The Exported file is shown in [“Export”](#) section.

Group-Wise Shift Head Count Export

This feature enables the export of data in Excel format for the overall count of users belonging to different enterprise groups (branches, departments, grades etc. say, in a manufacturing facility), reporting across different shifts (say, day and night shifts). The data can be exported in daily and monthly formats once the enterprise groups, shift groups and shift codes have been configured using the Configuration tab.

To access this functionality, Select the **Time and Attendance module > Exports > Group-Wise Shift Headcount**.

The page opens as follows:



Export



Before Exporting you must do **“Configuration”** for the Export parameters.

Format Selection: Select the export format as **Daily Format** or **Monthly Format**.

Date: Select a date range for data export by selecting the date selection buttons.

File Name: Enter an appropriate Filename for the file to be exported.

Select Users: Select one of the following filters from the drop down list:

- **Use Wise** - To select users randomly by clicking the **Select User** button.
- **Select Group** - To select all users associated with a particular enterprise group using the **Select Group** dropdown list.
- **ALL** - To select all users active on the system.

Generate Export for: Select the users as **All**, **Active** or **Inactive** for which Group-wise shift headcount is to be exported.

Click on **Export** and save the file at the required location.

Configuration

The Group-Wise Shift Headcount Export can be configured to view the shift wise head count in the exported file.

The screenshot shows the 'Enterprise Group Configuration' section of the 'Group-Wise Shift Headcount' application. It features a sidebar with 'Export' and 'Configuration' tabs. The main area contains dropdown menus for 'Group-1' (Organization), 'Group-2' (Branch), and 'Group-3' (Department). Below these is a 'Filter By' dropdown set to 'Group-1' and a 'Select Organization' dropdown set to 'Selected'. A search bar is present. A table lists two organizations: 'Organization-1' (ID 1) and 'Matrix' (ID 2), both with checkboxes for selection. A 'Shift Configuration' section is partially visible at the bottom, and a 'Save' button is at the bottom right.

ID	Name	
1	Organization-1	<input checked="" type="checkbox"/>
2	Matrix	<input checked="" type="checkbox"/>

Enterprise Group Configuration

In the Enterprise Group Configuration section, select enterprise groups for Group-1, Group-2 and Group-3 for which shift-based headcount data is to be exported.

Use the **Filter By** dropdown list to select Group-1, Group-2 or Group-3 and select single or multiple groups to filter users based on the selection. For e.g., if Group-1 is set as "Organization", and **Filter By** as Group-1, the user can select single or multiple organizations to filter users.

Shift Configuration

In the **Shift Configuration** section, select 2 shift groups and specify shifts to be included in each group.

The screenshot shows the 'Shift Configuration' section of the 'Group-Wise Shift Headcount' application. It features a sidebar with 'Export' and 'Configuration' tabs. The main area has a 'Select Shifts For Export' section with dropdowns for 'Group-1 Shifts' and 'Group-2 Shifts'. Below these are two tables. The first table lists 'General Shift' (ID GS) and 'Night Shift' (ID NS). The second table lists 'Day' (ID NS) and 'Night' (ID NS). A 'Shift Groups Code For Export' section is at the bottom, and a 'Save' button is at the bottom right.

ID	Name	
GS	General Shift	<input checked="" type="checkbox"/>
NS	Night Shift	<input checked="" type="checkbox"/>

User can also define codes for each shift group as shown above.

Click the **Save** button to save these configurations for the next export.

The exported file is shown as below:

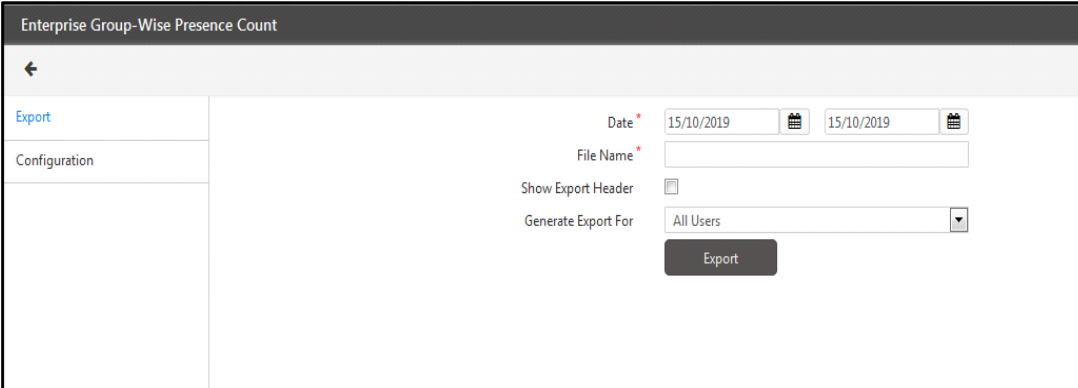
Group-Wise Shift Headcount From 01/05/2017 To 03/05/2017										
Branch	Department	Organization-1			Matrix			Total Reported Users For Organization		
		Day	Night	Total	Day	Night	Total	Day	Night	Total
Branch-1	Department-1	3	0	3	0	0	0	3	0	3
	Total Reported Users	3	0	3	0	0	0	3	0	3
RnD	Department-1	0	3	3	0	0	0	0	3	3
	Total Reported Users	0	3	3	0	0	0	0	3	3
Total Reported Users For Branch		3	3	6	0	0	0	3	3	6

Enterprise Group-Wise Presence Count Export

This feature enables the export of data for the count of presence in selected enterprise groups or shifts out of all the assigned users. Data can be exported in the Excel format once the relevant enterprise groups/shifts have been selected using the *Configuration* tab.

To access this functionality, select the **Time and Attendance module > Exports > Enterprise Group-Wise Presence Count**.

The page opens as follows:



The screenshot shows a web interface titled "Enterprise Group-Wise Presence Count". On the left, there is a sidebar with two tabs: "Export" (highlighted in blue) and "Configuration". The main area contains the following fields and controls:

- Date ***: Two date pickers, both showing "15/10/2019".
- File Name ***: A text input field.
- Show Export Header**: A checkbox, currently unchecked.
- Generate Export For**: A dropdown menu with "All Users" selected.
- Export**: A dark button.

Export



Before Exporting you must do "**Configuration**" for the Export parameters.

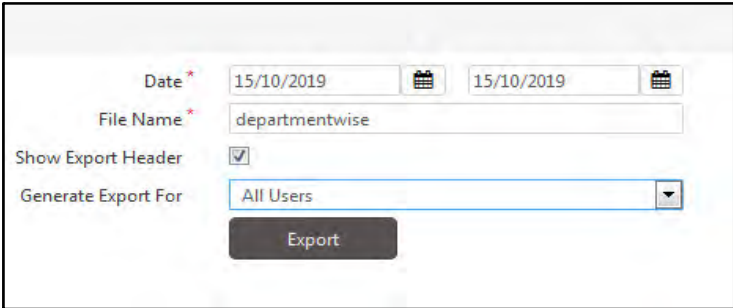
Date: Select a date range using the date selection buttons for the data to be exported.

Filename: Enter the alphanumeric **filename** with upto 20 character as the name of the file to be exported.

Show Export Header: Check the box to add the header in exported Excel file.

Generate Export for: Select the users as **All**, **Active** or **Inactive** for which Enterprise Group-Wise Presence Count is to be exported.

Click on **Export** and save the file at the required location.



This is a detailed view of the export form fields:

- Date ***: Two date pickers, both showing "15/10/2019".
- File Name ***: A text input field containing "departmentwise".
- Show Export Header**: A checkbox, currently checked.
- Generate Export For**: A dropdown menu with "All Users" selected.
- Export**: A dark button.

Sr. No.	Department	Assigned Users of	1-Branch-1	2-Branch-2	3-RnD	4-HO	Total PR Users
1	05/01/2017						
2	1 Certification	2	0	0	2	0	2
3	2 Training	2	0	0	0	1	1
4	Total	4	0	0	2	1	3

Configuration

The *Enterprise Group-Wise Presence Count Export* can be configured to determine which data is to be exported in the exported file.

Enterprise Group-Wise Presence Count

Export

Configuration

Group-1: Department

Group-2: Branch

Filter By: Group-1

Select Department: Selected

Search

ID	Name	
1	Department-1	
2	Certification	<input checked="" type="checkbox"/>
3	Training	<input checked="" type="checkbox"/>

Save

Group: Select two group types Group-1 and Group-2 based on which presence count data of users is to be sent. The same value can be selected for both Group-1 and Group-2 as well.

Select Group-1 as a filter using the **Filter By** option. Now, select specific enterprise groups or shifts associated with Group-1 to filter presence count for these groups only. Two Departments have been selected for Group-1 in the example below:

Now, select Group-2 using the **Filter By** option. Select specific enterprise groups or shifts associated with Group-2 to filter presence count for these groups only.

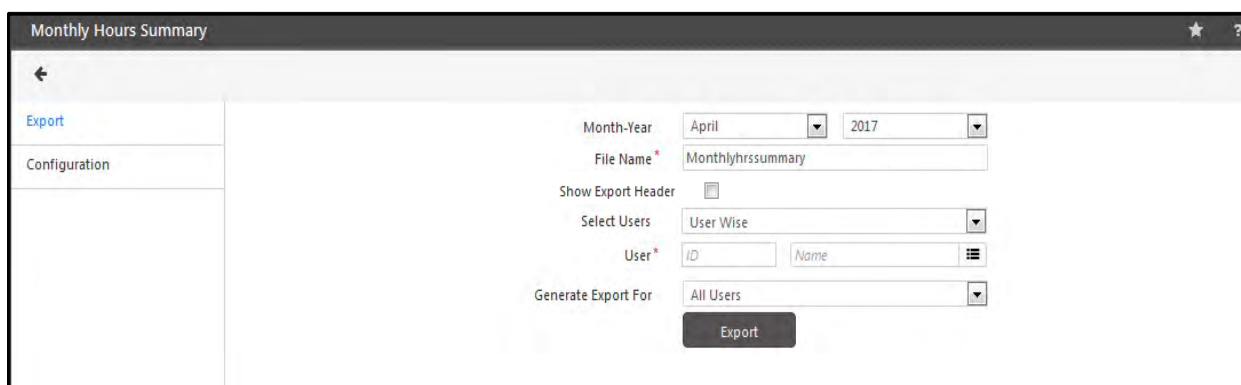
Click the **Save** button to save these configurations for the next export.

The Exported file is shown in **“Export”** section.

Monthly Hours Summary Export

This export displays authorized overtime components as configured, net-work hours, work hours, shift duration, loss hours, altogether, along with, configurable Attendance Status combinations.

The Export page has two tabs: Export and Configuration.



Export

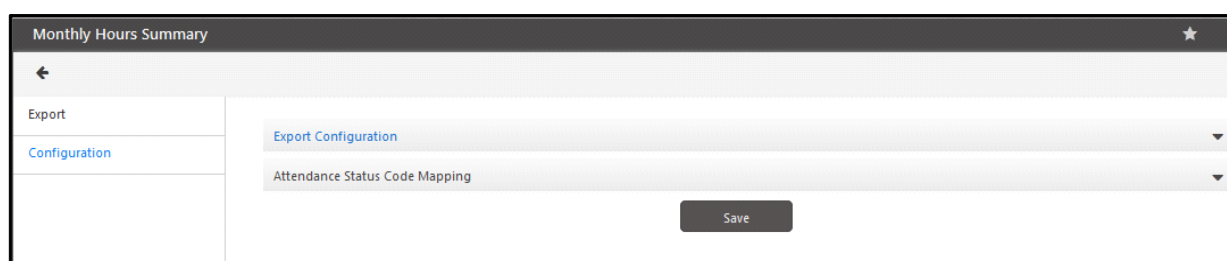


Before Exporting you must do **“Configuration”** for the Export parameters.

- You can select **month** and **year** to export the summary for the desired month of year.
- Specify the alphanumeric **filename** with upto 20 character as the name of the file to be exported.
- **Show Export Header:** Check the box to add the header in exported Excel file.
- **Select Users:** You can select the users based on filter options of User Wise, Group Wise(Enterprise groups) or All users(active/inactive/ all).
- **Generate Export for:** Select the users as All, Active or Inactive for which Monthly Hours Summary is to be exported.

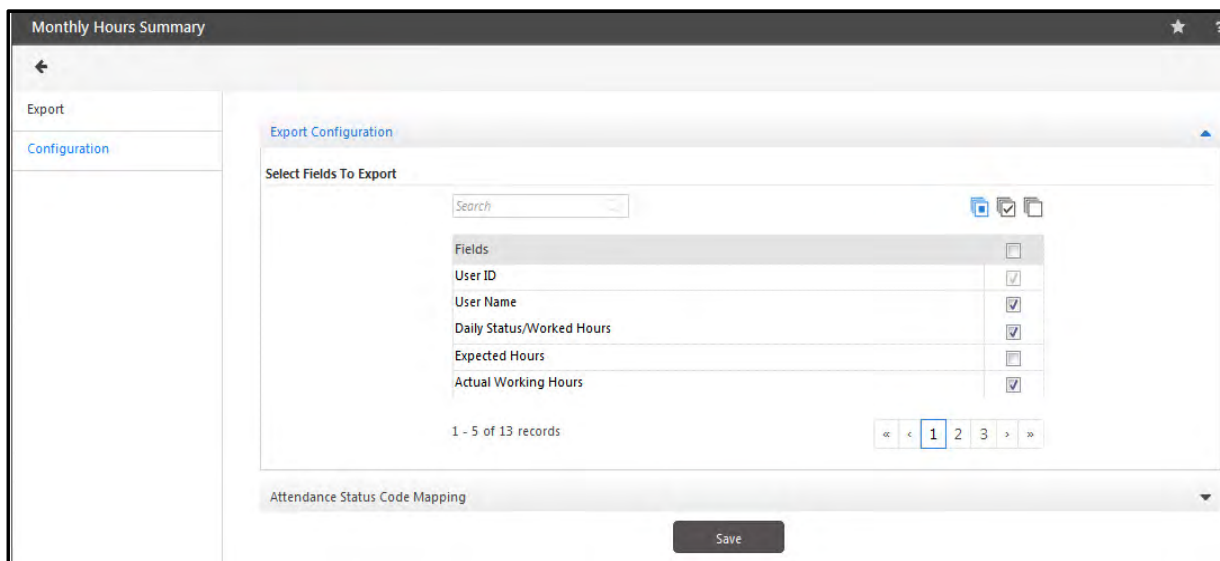
Finally Click on Export button to Export the monthly hours summary for the selected user.

Configuration

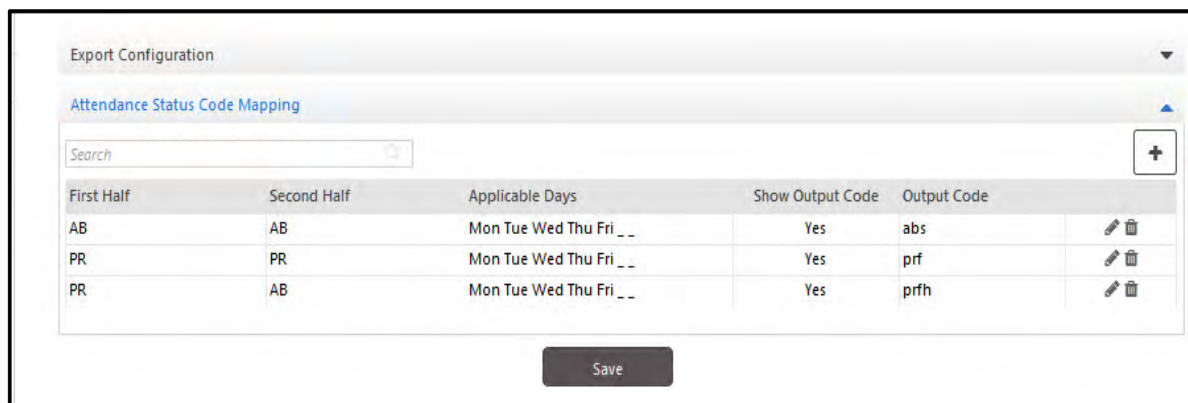


In Configuration tab, click on **Export Configuration**:

Select the fields to be exported in the monthly hours summary export file. You can select Normal/Actual working hours, OT1 to OT5, Total overtime, Total hours etc.



Click on **Attendance Status Code Mapping** section. Click on Add button to configure the output code for various combinations of attendance.



Attendance Status: Select the **First Half** and **Second Half** status from the drop down options.

Applicable Days: Select the applicable days for which attendance status will be mapped with the output code.

Show Output Code If Work Not Done: If work is not done on some day then attendance status for that day can be marked by the user configured output code.

For this enable this checkbox. Then the mentioned output code will be shown if hours for that day are found as 00:00. Enable the checkbox to display the output code in exported file.

Output Code: Specify any code of your choice to map with the attendance status. For eg: for attendance status AB AB in both halves, output code will be shown as abs.

Click on **Save** to save the configuration.

The Export file in Excel will be generated as shown below:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
User ID	Name	01/04/2017	02/04/2017	03/04/2017	04/04/2017	05/04/2017	06/04/2017	07/04/2017	08/04/2017	09/04/2017	10/04/2017	11/04/2017	12/04/2017
07	Aditi	9.00		9.00	0.55	9.00	0.05	prf			3.36	0.12	p
1	Shalini												
101	Khushbu	abs		abs	abs	abs	abs	abs	abs		abs	abs	ab
1567	Sheetal	8.00		7.45	7.00	8.00	7.00	8.00	7.43		6.00	abs	ab
1678	Supriya									abs	abs	abs	ab
1782	Nidhi	abs		abs	8.00	4.30	abs	abs	abs		abs	abs	ab
2	Chirag	abs						abs	abs		abs	abs	ab
3	Isha	abs		abs	abs	abs	abs	abs	abs		abs	abs	ab
4	Sweta												

Site Wise Monthly Summary Export

This export displays site wise records for user's attendance summary. It is a monthly level export. It is supposed to have individual records for site-wise work done on consecutive date range of selected month.

The Export page has two tabs: Export and Configuration.

Export



Before Exporting you must do **“Configuration”** for the Export parameters.

- You can select **month** and **year** to export the summary for the desired month of year.
- Specify the alphanumeric **filename** with upto 20 character as the name of the file to be exported.
- Show Export Header:** Check the box to add the header in exported Excel file.
- Select Users:** You can select the users based on filter options of User Wise, Group Wise(Enterprise groups) or All users(active/inactive/ all).
- Generate Export for:** Select the users as All, Active or Inactive for which Site wise Monthly Summary is to be exported.

Finally Click on Export button to Export the Site wise monthly summary for the selected user.

The Export file in Excel will be generated as shown below:

UserR ID	UserR Name	Range Start	Range End	Site ID	Site	Total	Present	Absents	Week	Holiday	Leaves	Tours	C.OFF	All	bn	Non Working Days	AB/Lea	AB/Lea	No Of AB/Leave
2192	chirag	01/12/2016	15/12/2016	1	Site-1	15	0	11.0	2	0	1.0	0	1.0	30.0	15		2 01/12/20	03/12/20	3.0
2192	chirag	01/12/2016	15/12/2016	1	Site-1	15	0	11.0	2	0	1.0	0	1.0	30.0	15		2 05/12/20	06/12/20	2.0
2192	chirag	01/12/2016	15/12/2016	1	Site-1	15	0	11.0	2	0	1.0	0	1.0	30.0	15		2 08/12/20	10/12/20	3.0
2192	chirag	01/12/2016	15/12/2016	1	Site-1	15	0	11.0	2	0	1.0	0	1.0	30.0	15		2 12/12/20	12/12/20	1.0
2192	chirag	01/12/2016	15/12/2016	1	Site-1	15	0	11.0	2	0	1.0	0	1.0	30.0	15		2 14/12/20	16/12/20	2.0
2192	chirag	16/12/2016	23/12/2016	2	Site-2	8	1.0	3.5	0	0	1.0	0	0	13.5	9.0		0 17/12/20	18/12/20	2.0
2192	chirag	16/12/2016	23/12/2016	2	Site-2	8	1.0	3.5	0	0	1.0	0	0	13.5	9.0		0 22/12/20	22/12/20	1.0
2192	chirag	16/12/2016	23/12/2016	2	Site-2	8	1.0	3.5	0	0	1.0	0	0	13.5	9.0		0 23/12/20	24/12/20	0.5
2192	chirag	24/12/2016	31/12/2016	1	Site-1	8	0	0	0	0	0	0	0	8	8		0		

Configuration

Site Wise Monthly Summary

Export
Configuration

Select Fields To Export

Fields	
User ID	<input checked="" type="checkbox"/>
User Name	<input checked="" type="checkbox"/>
Organization Code	<input type="checkbox"/>
Organization Name	<input type="checkbox"/>
Branch Code	<input type="checkbox"/>

1 2 3 4 5 6

Custom Export Field Configuration

Export New Entries For Occurrences

Absent ☒ ⓘ

Leave/Tour/C-OFF ☒ ⓘ

Save

Select the fields to be exported in the Site wise monthly summary export file.

Custom Export Field Configuration

You can configure customized formula based field to export sheet. It can be created using Field and Operator from the Field Value list.

Field Name: Enter a name for the column to be generated in export sheet.

Example:

Select a field say “Presents” and click >. The field “Presents” will move to right side.

Then select operator “+” and click >. The field “+” will move to right side.

Similarly move the “Week Offs” and “Holidays”.

Custom Export Field Configuration

Field Name: PR-WO-PH

Field Value

Field Value	
+	
-	
Total Days	
Presents	
Absents	
Week Offs	
Holidays	
Leaves	
Tours	
COFF	

> <

Add Cancel

Click **Add** button. The custom field will be shown in the grid.

The screenshot shows a window with two buttons at the top: 'Add' and 'Cancel'. Below them is a table with two columns: 'Field Name' and 'Field Value'. The first row shows 'PR-WO-PH' as the field name and 'Presents+Week Offs+Holidays' as the field value. To the right of each row is a trash icon. Below the table is a section titled 'Export New Entries For Occurrences' with two checked checkboxes: 'Absent' and 'Leave/Tour/C-OFF', each with an information icon. At the bottom is a 'Save' button.

Export New Entries for Occurrences

Absent- Enabling this check box will create new record in export sheet for every Absent range. It will export absent date range and number of days.

Leave/Tour/C-OFF- Enabling this check box will create new record in export sheet for every Leave/Tour/C-OFF range. It will export Leave/Tour/C-OFF Code, Date Range, Reason and No. of Days.

Example:

The export configuration is shown below.

The screenshot shows a window titled 'Custom Export Field Configuration'. It has a 'Field Name' text box and a 'Field Value' list box. The list box contains a scrollable list of items: 'Total Days', 'Presents', 'Absents', 'Week Offs', 'Holidays', 'Leaves', 'Tours', and 'COFF'. There are '+' and '-' buttons next to the list box. Below the list box are 'Add' and 'Cancel' buttons. At the bottom is a table with two columns: 'Field Name' and 'Field Value'. The first row shows 'All' as the field name and 'Total Days+Presents+Absents+Week Offs+Holidays+Leaves+Tours+COFF' as the field value. The second row shows 'bn' as the field name and 'Total Days+Presents+Holidays-Tours' as the field value. The third row shows 'Non Working Days' as the field name and 'Week Offs+Holidays' as the field value. To the right of each row is a trash icon. Below the table is a section titled 'Export New Entries For Occurrences' with a checked checkbox for 'Absent' and an information icon.

Site Wise Monthly Summary

←

Export

Configuration

Month-Year

December

2016

Filename

NonWorkingdays

File Format

Excel

UserR Filter

Randomly

UserR

ID

Name

UserR ID

Name

2192

chirag

Generate Export For

Active UserRs

Export

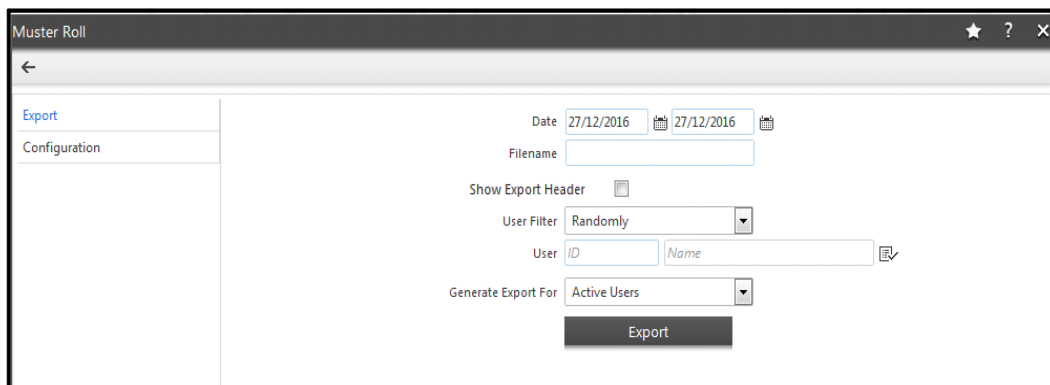
The exported file is shown below.

UserR ID	UserR Name	Range Start	Range End	Site ID	Site	Total	Present	Absents	Week	Holiday	Leaves	Tours	C-OFF	All	bn	Non Working Days	AB/Lea	AB/Lea	No Of AB/Leave
2192	chirag	01/12/2016	15/12/2016	1	Site-1	15	0	11.0	2	0	1.0	0	1.0	30.0	15	2	01/12/20	03/12/20	3.0
2192	chirag	01/12/2016	15/12/2016	1	Site-1	15	0	11.0	2	0	1.0	0	1.0	30.0	15	2	05/12/20	06/12/20	2.0
2192	chirag	01/12/2016	15/12/2016	1	Site-1	15	0	11.0	2	0	1.0	0	1.0	30.0	15	2	08/12/20	10/12/20	3.0
2192	chirag	01/12/2016	15/12/2016	1	Site-1	15	0	11.0	2	0	1.0	0	1.0	30.0	15	2	12/12/20	12/12/20	1.0
2192	chirag	01/12/2016	15/12/2016	1	Site-1	15	0	11.0	2	0	1.0	0	1.0	30.0	15	2	14/12/20	16/12/20	2.0
2192	chirag	16/12/2016	23/12/2016	2	Site-2	8	1.0	3.5	0	0	1.0	0	0	13.5	9.0	0	17/12/20	18/12/20	2.0
2192	chirag	16/12/2016	23/12/2016	2	Site-2	8	1.0	3.5	0	0	1.0	0	0	13.5	9.0	0	22/12/20	22/12/20	1.0
2192	chirag	16/12/2016	23/12/2016	2	Site-2	8	1.0	3.5	0	0	1.0	0	0	13.5	9.0	0	23/12/20	24/12/20	0.5
2192	chirag	24/12/2016	31/12/2016	1	Site-1	8	0	0	0	0	0	0	0	8	8	0			

Muster Roll Export

This export generates information of employees' details such as their attendance status, leaves, week-offs pertaining to the shifts assigned to them.

The Export page has two tabs: Export and Configuration.



The screenshot shows the 'Muster Roll' application window with the 'Export' tab selected. The interface includes a left sidebar with 'Export' and 'Configuration' tabs. The main area contains the following fields and controls:

- Date:** Two date pickers set to 27/12/2016.
- Filename:** A text input field.
- Show Export Header:** A checkbox that is currently unchecked.
- User Filter:** A dropdown menu set to 'Randomly'.
- User:** Two input fields for 'ID' and 'Name', with a search icon to the right.
- Generate Export For:** A dropdown menu set to 'Active Users'.
- Export:** A large button at the bottom.

Export

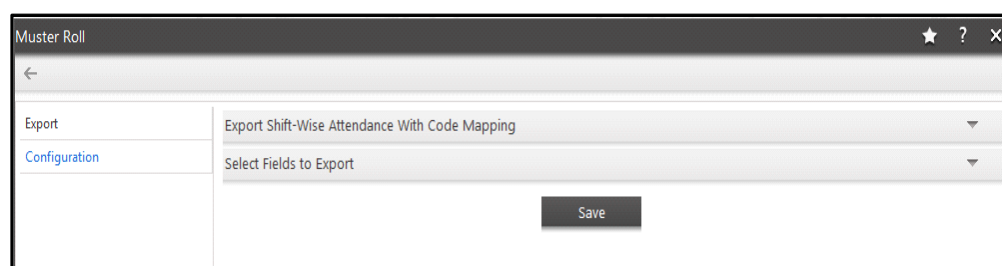


Before Exporting you must do **“Configuration”** for the Export parameters.

- You can select **From** and **To date** for which the export is to be done.
- Specify the alphanumeric **filename** with as the name of the file to be exported.
- **Show Export Header:** Check the box to add the header in exported Excel file.
- **Users:** You can select the users Randomly, by selected group(Enterprise groups) or all users(active/ inactive/ all).
- **Generate Export for:** Select the users as All, Active or Inactive for which Muster Export is to be exported.

Finally Click on Export button to Export the monthly hours summary for the selected user.

Configuration



The screenshot shows the 'Muster Roll' application window with the 'Configuration' tab selected. The interface includes a left sidebar with 'Export' and 'Configuration' tabs. The main area contains the following elements:

- Export Shift-Wise Attendance With Code Mapping:** A dropdown menu.
- Select Fields to Export:** A dropdown menu.
- Save:** A button at the bottom.

In Configuration tab, click on **Export Shift-Wise Attendance With Code Mapping**:

Click on Add button. Then select the Shift and map the code for First half and second half. You can do mapping configurations upto **999999**.

Shift	First Half	Second Half	Present	Holiday	Output Code 1	Output Code 2	
FB	PR	PR	-	No	PRF	PRS	
GS	PR	PR	-	No	PRF	PRS	
NS	PR	PR	-	No	PRF	PRS	
RS	PR	PR	-	No	PRF	PRS	
FB	PR	AB	-	No	PRF	ABS	

Add to Export: If this checkbox is enabled, then only the mapped output codes will be visible in export.

Filter Shifts: Select the option as **All** or **Randomly** to filter the shift based on which export will be done.

- **Shift:** If “Randomly” filter is selected, then select the shift from the picklist.

Attendance Status: Select the first half and second half attendance status.

- **Present:** The Present field will be enabled only If Attendance status selected is WO-Week-Off or PH-Holiday in both drop-downs. When Present checkbox is enabled, you can select full day or half day to mark present on week off day.
- **Holiday:** The Holiday field will be enabled only If Attendance status selected is WO-Week-Off in both drop-downs.

Add To Export ☒

Filter Shifts Randomly

Shift GS General Shift

Attendance Status WO-Week-Off WO-Week-Off

Present ☒ Full Day

Holiday ☐

Output Code WHOF WHOS

Update Cancel

Shift	First Half	Second Half	Present	Holiday	Output Code 1	Output Code 2
RS	RH	RH	-	No	RHF	RHS
GS	WO	WO	Full Day	No	WHOF	WHOS

Select Fields to Export

Save

Output Code: Specify any code of your choice to map with Shifts and Attendance Status for First half and second half.

For eg: for attendance status AB AB in both halves, output code will be shown as ABS.

Click on **Add** to store the configuration. Then **Save** the configuration.

In Configuration tab, click on **Select Fields to Export**:

Muster Roll

Export Shift-Wise Attendance With Code Mapping

Select Fields to Export

Select Fields To Export

Fields	
User ID	<input checked="" type="checkbox"/>
User Name	<input checked="" type="checkbox"/>
Reference ID	<input type="checkbox"/>
Aadhar No	<input type="checkbox"/>
PF No	<input type="checkbox"/>

1 2 3 4 5 6 7 8 9 10 ... >>

Save

Select the fields to be exported in the Muster Roll export file. You can select Present, Absent, leaves, Week-offs etc.

The fieldnames Field1, Field 2, Field 3 and Field 4 are customizable according to the names defined in Admin > Global Policy > User > Custom Fields.

Hours Utilization: This field shows the utilization of Hours in the form of Percentage in exported sheet.

- Hours Utilization = (Gross Work Hours/ Total Planned Hours) *100
If Total Planned Hours = 0 then, value of Hours Utilization =0

Exceeding Planned Hours: This field shows the value of Hours worked more than planned hours in exported sheet

- If Gross Work Hours > Total Planned Hours, then Exceeding Planned Hours= Gross Work Hours -Total Planned Hours
- If Gross Work Hours < Total Planned Hours, then the value of Exceeding Planned Hours= 0.

Click on **Save** to save the configuration.

Then Export the file from “**Export**” The Export file in Excel will be generated as shown below:

Sr No.	User ID	Name	Organization Name	Reporting-Incharge2		01Dec Thu	02Dec Fri	03Dec Sat	04Dec Sun	05Dec Mon	06Dec Tue
1	GSNS	GSNS User1	Organization 2		Shift	GS	GS	GS	NS	NS	NS
					First Half	PRF	PRF	PRF	PRF	????	INF
					Second Half	PRS	ABS	ABS	ABS	????	UPS
					First Punch	09:00	09:00	15:00	07:00	23:00	07:00
					Last Punch	18:00	14:00	19:00	23:00		
					Work Hours	09:00	05:00	04:00	16:00	00:00	00:00
					Loss Hours	00:00	03:00	04:00	00:00	00:00	04:00
					Extra Work Hours	01:00	01:00	01:00	16:00	00:00	16:00
2	GSShift1	GS Shift Use 1	Organization-1	Test2	Shift	GS	GS	GS	GS	GS	GS
				Test2	First Half	PRF	WOF	WOF	ABF	ABF	PRF
				Test2	Second Half	PRS	WOS	WOS	ABS	ABS	PRS
				Test2	First Punch	09:00					09:00
				Test2	Last Punch	18:00					18:00
				Test2	Work Hours	09:00	00:00	00:00	00:00	00:00	09:00
				Test2	Loss Hours	00:00	00:00	00:00	08:00	08:00	00:00
				Test2	Extra Work Hours	01:00	00:00	00:00	00:00	00:00	01:00
3	NSShift1	NightShift user 1	Organization-1	Test2	Shift	NS	NS	NS	NS	NS	NS
				Test2	First Half	PRF	PRF	PLF	WOFF	PRF	COF
				Test2	Second Half	PRS	PRS	ABS	WOFS	PRS	ABS
				Test2	First Punch	23:00	21:00		21:00	21:00	
				Test2	Last Punch	07:00	10:00		08:00	08:00	
				Test2	Work Hours	08:00	13:00	00:00	11:00	11:00	00:00
				Test2	Loss Hours	00:00	00:00	04:00	00:00	00:00	04:00
				Test2	Extra Work Hours	00:00	05:00	00:00	03:00	03:00	00:00

Time and Attendance Reports

These reports can be obtained using the **Reports** section under the **Time and Attendance** add-on module. The **Time and Attendance** Reports can be categorized as follows:

- “Time Management”
- “Absenteeism”
- “Overtime”
- “Exceptions”
- “Monthly Reports”
- “Registers”
- “Yearly Reports”
- “User Defined Reports”
- “Statutory Reports”
- “Charts”



Before generating Reports, it is must to run Daily Attendance Process and Monthly Attendance Process to get the proper data in reports.



Certain Time and Attendance Reports such as Attendance Summary, Attendance Register, Muster Roll etc. provide an **Include Archived Data** check-box on the report generation page.

Select this check-box to enable archived data (if any) to be included at the time of report generation. Retrieving data from archives may take a significantly long time.

Time Management

The *Time Management* Reports are an assortment of detailed and focused reports on the time activities of the users on a site. These include the following reports:

- **Late In** - Generates a group-wise listing of employees with details of *Late In* events during the specified time period as shown.

The Optional parameter of Duration and Count can be specified.

Select the Organization name as per User selection or Customized Report. This helps in displaying the report header as the Organization name as per selection instead of default organization name.

Example: If Duration is > 30 mins; then event with Late IN of more than 30 mins will be displayed in the Report. Now if Count> 1, then event of user with more than 1 Late IN will be displayed in the Report.

The allowed Grace Time for Shift Late- IN is 10 mins. And maximum Late- IN allowed is 30 mins. After 10 mins of grace; user will be considered Late- IN.

If a user punches at 9:25 then Late- IN of 10 minutes is considered.

Matrix							
Organization-Wise Late-IN From 10/09/2020 To 14/09/2020							
Run by: System Admin				Date: 14/09/2020 17:42			
Sr No	User ID	Name	Date	Shift	IN	OUT	Late By
Organization :		Matrix					
1	1	Athira	12/09/2020	GS	09:20	19:45	00:10
Late By Group Total:							00:10
Late By Grand Total:							00:10

- **Early In** - Generates a group-wise listing of employees with details of *Early In* events during the specified time period as shown.

The Optional parameter of Duration and Count can be specified.

Select the Organization name as per User selection or Customized Report. This helps in displaying the report header as the Organization name as per selection instead of default organization name.

Example: If Duration is > 10 mins; then event with Early IN of more than 10 mins will be displayed. Suppose If Count> 1; then event of user with more than 1 Early IN will be displayed.

Early-IN

Date * 14/09/2020 14/09/2020

Optional Parameters

Group By Organization

Group By Organization

Duration (>) 0 (Mins)

Count (>) * 0

Organization Name in Header As Per User Selection

Early-IN

Back

Find... 1 of 1 100%

Main Report

Organization-1 Page 1 of 1

Organization-Wise Early-IN From 01/10/2019 To 23/10/2019

Run by: System Admin Date: 23/10/2019 07:25

Sr No	User ID	Name	Date	Shift	IN	OUT	Early-IN
Organization :							
1	501	Ramesh	14/10/2019	GS	08:01		00:59
2	503	Meet	10/10/2019	GS	07:30		01:30
3	503	Meet	14/10/2019	GS	08:00		01:00
4	503	Meet	23/10/2019	GS	07:00		02:00
5	504	Gunjan	10/10/2019	GS	07:32		01:28
6	504	Gunjan	14/10/2019	GS	08:00		01:00
7	504	Gunjan	23/10/2019	GS	07:00	16:19	02:00
Early-IN Group Total:							09:57
Early-IN Grand Total:							09:57

- **Early Out** - Generates a group-wise listing of employees with details of *Early Out* events during the specified time period as shown.

Select the Organization name as per User selection or Customized Report. This helps in displaying the report header as the Organization name as per selection instead of default organization name.

Suppose Grace Period for Early Out is defined as 5 mins in Shift Configuration. And maximum Early Out allowed is defined as 15 mins in Early OUT policy. So user can go out 20 minutes early than shift end.

If user punches out at 17:55 or afterwards; then that record will not be shown in Early Out Report. Similarly if user punches before 17:40 then it is more than Early Out allowed so that record will not be shown here.

Early Out duration is calculated as 17:55 - 17:46 = 00:09 as shown below in first record. similarly for other records.

Organization-1							Page 1 of 1
Organization-Wise Early-OUT From 03/09/2018 To 18/09/2018							
Run by: System Admin				Date: 18/09/2018		18:53	
Sr No	User ID	Name	Date	Shift	IN	OUT	Early-OUT
1	101	Khushbu Gorawala	11/09/2018	GS	09:00	17:46	00:09
2	3	Isha Shah	10/09/2018	GS	09:00	17:44	00:11
3	3	Isha Shah	12/09/2018	GS	08:55	17:54	00:01
4	3	Isha Shah	14/09/2018	GS	09:00	17:40	00:15
Early-OUT Group Total:							00:36
Early-OUT Grand Total:							00:36

- **Overstay** - Generates a group-wise listing of employees with details of *Overstay* during the specified time period.

The Optional parameter of Duration and Count can be specified to get the overstay hours beyond specific duration (mins) and count.

Select the Organization name as per User selection or Customized Report. This helps in displaying the report header as the Organization name as per selection instead of default organization name.

Overstay

Date * 14/09/2020 14/09/2020

Optional Parameters

Group By Organization

Group By Organization

Duration (>) 0 (Mins)

Count (>) * 0

Organization Name in Header As Per User Selection

User Selection

Select Users User Wise

User * ID Name

Generate Report For All Users

Generate Report

Suppose the Shift is from 09:00 to 18:00 hours so the duration after 18:00 hours for which user has worked is counted in Overstay hours as shown below.

Overstay

Back

Find... 1 of 1 100%

Main Report

Organization-1 Page 1 of 1

Run by: System Admin Date: 18/09/2018 17:21

Organization-Wise Overstay From 01/09/2018 To 18/09/2018

Sr No	User ID	Name	Date	Shift	IN	OUT	Overstay
1	101	Khushbu Gorawala	03/09/2018	GS	09:00	19:00	01:00
2	101	Khushbu Gorawala	04/09/2018	GS	10:00	21:00	03:00
3	101	Khushbu Gorawala	05/09/2018	GS	08:00	21:00	03:00
4	101	Khushbu Gorawala	06/09/2018	GS	09:41	19:00	01:00
5	101	Khushbu Gorawala	07/09/2018	GS	09:30	19:00	01:00
6	2	Chirag	03/09/2018	GS	09:00	19:00	01:00
7	2	Chirag	05/09/2018	GS	09:00	20:00	02:00
8	3	Isha Shah	03/09/2018	GS	07:00	20:00	02:00
9	3	Isha Shah	04/09/2018	GS	07:30	19:30	01:30
10	3	Isha Shah	05/09/2018	GS	09:15	19:00	01:00
11	3	Isha Shah	06/09/2018	GS	09:35	20:00	02:00
12	3	Isha Shah	07/09/2018	GS	09:39	19:00	01:00
13	3	Isha Shah	10/09/2018	GS	09:40	19:00	01:00
Overstay Group Total:							20:30
Overstay Grand Total:							20:30

- **Attendance** - Generates attendance data for a specific period and specified users. Users can select from one of the four available templates to view the data in the required format.

Eg: Format1

Attendance														
Main Report														
Organization-1														
Organization-Wise Attendance From 03/09/2018 To 18/09/2018														
Run by:	System Admin	Date: 18/09/2018 17:31												
User ID	Name	Shift	IN-SPFID	OUT-SPFID	IN-SPFID	OUT-SPFID	1st Half	2nd Half	Late -IN	Early -OUT	Over Time	Auth OTC-OFF	Work Hrs	Man Entry Reason
03/09/2018 (Monday)														
1	Sheetal	GS					PR	PR			01:00		09:00	Yes
101	Khushbu Gorawala	GS	09:00	19:00			PL	PL						
1583	Shilpa	GS												
1687	Aditi Gupta	GS												
2	Chirag	GS	09:00	19:00			PR	PR					09:00	Yes
3	Isha Shah	GS	07:00	20:00			PR	PR			04:00		12:00	Yes
W1	Sunil	GS												
04/09/2018 (Tuesday)														
1	Sheetal	GS					AB	PR			03:00		10:00	Yes
101	Khushbu Gorawala	GS	10:00	21:00			PL	PL						
1583	Shilpa	GS												
1687	Aditi Gupta	GS												
2	Chirag	GS	09:00	14:00			PR	SL					04:00	Yes
3	Isha Shah	GS	07:30	19:30			PR	PR			03:00		11:00	Yes
W1	Sunil	GS												
05/09/2018 (Wednesday)														
1	Sheetal	GS					PR	PR			04:00		12:00	Yes
101	Khushbu Gorawala	GS	08:00	21:00			PL	PL						
1583	Shilpa	GS												
1687	Aditi Gupta	GS												
2	Chirag	GS	09:00	20:00			PR	PR					10:00	Yes

- **Attendance Summary** - Generates Group-wise attendance summary for a selected period as shown.

Attendance Summary

←

Back

Find...

1 of 1

100%

Main Report

Organization-1

Page 1 of 1

Run by: System Admin

Organization-Wise Attendance Summary From 03/09/2018 To 18/09/2018

Date:18/09/2018 17:34

Sr No	Date	Scheduled	PR	AB	WO	PH	LV	PR%	AB%	WO%	PH%	LV%
Organization-1												
1	03/09/2018	7.0	3.0	3.0	0.0	0.0	1.0	42.86	42.86	0.00	0.00	14.3
2	04/09/2018	7.0	2.0	3.5	0.0	0.0	1.5	28.57	50.00	0.00	0.00	21.4
3	05/09/2018	7.0	3.0	3.0	0.0	0.0	1.0	42.86	42.86	0.00	0.00	14.3
4	06/09/2018	7.0	1.5	4.5	0.0	0.0	1.0	21.43	64.29	0.00	0.00	14.3
5	07/09/2018	7.0	2.0	4.0	0.0	0.0	1.0	28.57	57.14	0.00	0.00	14.3
6	08/09/2018	7.0	0.0	7.0	0.0	0.0	0.0	0.00	100.00	0.00	0.00	0.0
7	09/09/2018	7.0	0.0	6.0	1.0	0.0	0.0	0.00	85.71	14.29	0.00	0.0
8	10/09/2018	7.0	1.0	6.0	0.0	0.0	0.0	14.29	85.71	0.00	0.00	0.0
9	11/09/2018	6.0	0.0	6.0	0.0	0.0	0.0	0.00	100.00	0.00	0.00	0.0
10	12/09/2018	7.0	0.0	7.0	0.0	0.0	0.0	0.00	100.00	0.00	0.00	0.0
11	13/09/2018	6.0	0.0	6.0	0.0	0.0	0.0	0.00	100.00	0.00	0.00	0.0
12	14/09/2018	7.0	0.0	7.0	0.0	0.0	0.0	0.00	100.00	0.00	0.00	0.0
13	15/09/2018	7.0	0.0	7.0	0.0	0.0	0.0	0.00	100.00	0.00	0.00	0.0
14	16/09/2018	7.0	0.0	6.0	1.0	0.0	0.0	0.00	85.71	14.29	0.00	0.0
15	17/09/2018	7.0	0.0	7.0	0.0	0.0	0.0	0.00	100.00	0.00	0.00	0.0
16	18/09/2018	7.0	0.0	7.0	0.0	0.0	0.0	0.00	100.00	0.00	0.00	0.0

To view the details of Attendance for particular date, click on that Date. The report for the selected Date will appear as shown below.

Attendance Summary

Back

Find...

1 of 1

100%

Main Report 06/09/2018

Organization-Wise Attendance Detail From 03/09/2018 To 18/09/2018

Run by: System Admin

Date: 18/09/2018 17:36

Sr No	User ID	Name	1st Half	2nd Half
06/09/2018	Organization-1			
1	1	Sheetal		
2	101	Khushbu Gorawala	AB	PR
3	1583	Shilpa	AB	AB
4	1687	Aditi Gupta		
5	2	Chirag	LW	LW
6	3	Isha Shah	PR	PR
7	W1	Sunil		

- **Late Arrival Memo** - This option enables the administrator to generate and print individual or multiple *Late Arrival Memos* as shown.

Late Arrival Memo

←

↺

★

?

×

Date *

14/09/2020

14/09/2020

Optional Parameters

New Page For Each Group

☐

Organization Name in Header As Per

User Selection

▼

User Selection

Select Users

User Wise

▼

User *

ID

Name

Generate Report For

All Users

▼

Generate Report

Late Arrival Memo

Back

Find... 1 of 1 100%

Main Report

Organization-1
Late Arrival Memo From 01/10/2019 To 23/10/2019

Run by: System Admin Date: 23/10/2019 11:12
 User : 501 Ramesh Branch : Branch-1
 Department : Department-1 Designation : Designation-1

Sr No	Date	Shift	IN	Late-IN
1	22/10/2019	GS	09:30	00:20
2	23/10/2019	GS	09:12	00:02
				Total: 00:22

You have been marked late on above dates between 01/10/2019 and 23/10/2019
 Total 2 day(s) 00:22 hrs.

Organization-1
Late Arrival Memo From 01/10/2019 To 23/10/2019

Run by: System Admin Date: 23/10/2019 11:12
 User : 502 Shyam Branch : Branch-1
 Department : Department-1 Designation : Designation-1

Sr No	Date	Shift	IN	Late-IN
1	18/10/2019	GS	09:17	00:07
2	22/10/2019	GS	09:32	00:22
3	23/10/2019	GS	10:02	00:52
				Total: 01:21

You have been marked late on above dates between 01/10/2019 and 23/10/2019
 Total 3 day(s) 01:21 hrs.

- **Grace Time Usage** - Generates group-wise details of grace time usage for a specified time period for all or selected users.

Grace Time Usage

Date * 03/09/2018 18/09/2018

Optional Parameters

Group By Organization

Grace Type

☒ IN Grace

☒ OUT Grace

User Selection

Select Users All

Generate Report For All Users

Generate Report

Suppose the Grace period for Late-IN is set as 10 mins and Grace period for Early-Out is set as 5 mins in Shift configuration. So if the user avails this grace period; then the record is displayed in report.

The shift is **09:00** to **18:00** hours. If user punches IN at **09:10** then Grace IN is **00:10** and user punches out at **17:56** then Grace OUT is **00:04**. Hence total grace time used is **00:14** as shown below.

Grace Time Usage									
Back									
Find... 1 of 1 100%									
Main Report									
Organization-1									
Page 1 of 1									
Organization-Wise Grace Time Usage From 03/09/2018 To 18/09/2018									
Run by: System Admin									
Date: 18/09/2018 17:52									
Sr No	User ID	Name	Department	Designation	Grace Usage Count	Grace IN	Grace OUT	Total Grace Time	
Organization-1									
1	3	Isha Shah	Department-1	Designation-1	2	00:10	00:04	00:14	
2	101	Khushbu Gorawala	Department-1	Designation-1	1	00:07	00:00	00:07	

- **Net Work-Time** - Generates user-wise details of net work-time for a specified period.

Net Work-Time												
Back												
Find... 1 of 93 100%												
Main Report												
ORGANISATION 1.												
Net Work-Time From 01/01/2013 To 02/01/2013												
Run by: System Admin												
Date: 20/06/2014 15:04												
1 -- SALIM ANSARI												
SR NO	Date	Shift	First In-Time	Last Out-Time	1st Half	2nd Half	Gross Work Hrs	Out Time	Net Work Hrs	Status	Man Entry	Reason
1	01/01/2013	23			WO	WO	00:00	00:00	00:00	W	NO	
2	02/01/2013	23	08:26	17:01	PR	PR	08:05	00:00	00:00	P	YES	
10 -- RAJENDRA GOSWAMI												
SR NO	Date	Shift	First In-Time	Last Out-Time	1st Half	2nd Half	Gross Work Hrs	Out Time	Net Work Hrs	Status	Man Entry	Reason
1	01/01/2013	23			WO	WO	00:00	00:00	00:00	W	NO	
2	02/01/2013	23	08:23	17:00	PR	PR	08:07	00:00	00:00	P	NO	
1001 -- ANKITKUMAR SOHLIYA												
SR NO	Date	Shift	First In-Time	Last Out-Time	1st Half	2nd Half	Gross Work Hrs	Out Time	Net Work Hrs	Status	Man Entry	Reason
1	01/01/2013	GS	09:28	20:00	PR	PR	10:02	00:00	00:00	P	NO	
2	02/01/2013	GS	09:23	19:32	PR	PR	09:39	00:00	00:00	P	NO	

- **Daily Work Hours** - Generates user-wise details of daily work hours for a selected period.

Daily Work Hours

Date: 13/08/2020 to 14/09/2020

Work Hours Based Calculation: ☐

Optional Parameters

Group By: Organization (dropdown), User (dropdown)

Group Needed In Report: ☐

New Page For Each Date/User: ☒

Include In Lost Hours: ☒ Late-IN, ☒ Early-OUT

Add Custom Footer: ☒

Department Head Approval: _____

Organization Name in Header As Per: User Selection (dropdown)

User Selection

Select Users: User Wise (dropdown)

User: ID (text), Name (text)

Generate Report For: All Users (dropdown)

Here Late- IN and Early- OUT both are included in Loss hours. So **Lost hours**= Late-IN/Early OUT hours

Main Report

Organization-1

Daily Work Hours From 01/09/2018 To 19/09/2018

Run by: System Admin

Date: 19/09/2018 10:00

Date	Day	Shift	IN-SPFID	OUT-SPFID	IN-SPFID	OUT-SPFID	FH	SH	Late -IN	Early -OUT	Lost Hours	Auth OT	Work Hrs	Net Break	Remark
01/09/2018	Sat	GS					AB	AB							S-No Punches Available
02/09/2018	Sun	GS					WO	WO							
03/09/2018	Mon	GS	07:00	20:00			PR	PR					12:00	01:00	M-Attendance Corrected
04/09/2018	Tue	GS	07:30	19:30			PR	PR					11:00	01:00	M-Attendance Corrected
05/09/2018	Wed	GS	09:15	19:00			PR	PR	00:05		00:05		08:45	01:00	M-Attendance Corrected
06/09/2018	Thu	GS	09:36	20:00			PR	PR	00:25		00:25		09:25	01:00	M-Attendance Corrected
07/09/2018	Fri	GS	09:39	19:00			PR	PR	00:29		00:29		08:21	01:00	M-Attendance Corrected
08/09/2018	Sat	GS	09:00	17:55			PR	PR					07:55	01:00	M-Attendance Corrected
09/09/2018	Sun	GS					WO	WO							
10/09/2018	Mon	GS	09:00	17:44			PR	PR		00:11	00:11		07:44	01:00	M-Attendance Corrected
11/09/2018	Tue	GS	09:10	17:55			PR	PR					07:45	01:00	M-Attendance Corrected
12/09/2018	Wed	GS	09:55	17:54			PR	PR		00:01	00:01		07:59	01:00	M-Attendance Corrected
13/09/2018	Thu	GS	09:00	17:20			PR	AB					07:20	01:00	M-Attendance Corrected
14/09/2018	Fri	GS	09:00	17:40			PR	PR		00:15	00:15		07:40	01:00	M-Attendance Corrected
15/09/2018	Sat	GS	09:00	17:39			PR	AB					07:39	01:00	M-Attendance Corrected
16/09/2018	Sun	GS					WO	WO							
17/09/2018	Mon	GS					AB	AB							S-No Punches Available
18/09/2018	Tue	GS					AB	AB							S-No Punches Available
19/09/2018	Wed	GS													
Total:									00:59	00:27	01:26	00:00	103:33	00:00	12:00

Department Head Approval: _____

When **Work Hours based Calculation** check-box is enabled; then Report will be generated along with Net-work hours as shown below.

On 5th, The punches are In Punch: 09:15 hours and OUT punch: 19:00 hours.

The work hours in shift (09:00 to 18:00) - break hours = 8:45 - 01:00 = 7:45 hours. Now as Grace period of 10 minutes is used so 07:45 + 00:10 = 07:55 hours

Similarly Network hours for selected dates are shown in report.

Daily Work Hours

Back

Find... 1 of 1 100%

Main Report

Organization-1

Page 1 of 1

Run by: System Admin

Daily Work Hours From 01/09/2018 To 19/09/2018

Date: 19/09/2018 10:14

Date	Day	Shift	IN-SPFID	OUT-SPFID	IN-SPFID	OUT-SPFID	FH	SH	Late	Early	Lost	Auth	Work Hrs	Net Work Hrs	Break	Remark
01/09/2018	Sat	GS					AB	AB								S-No Punches Available
02/09/2018	Sun	GS					WO	WO								
03/09/2018	Mon	GS	07:00	20:00			PR	PR					12:00	08:00	01:00	M-Attendance Corrected
04/09/2018	Tue	GS	07:30	19:30			PR	PR					11:00	08:00	01:00	M-Attendance Corrected
05/09/2018	Wed	GS	09:15	19:00			PR	PR	00:05		00:05		08:45	07:55	01:00	M-Attendance Corrected
06/09/2018	Thu	GS	09:35	20:00			PR	PR	00:25		00:25		09:25	07:35	01:00	M-Attendance Corrected
07/09/2018	Fri	GS	09:39	19:00			PR	PR	00:29		00:29		08:21	07:31	01:00	M-Attendance Corrected
08/09/2018	Sat	GS	09:00	17:55			PR	PR					07:55	08:00	01:00	M-Attendance Corrected
09/09/2018	Sun	GS					WO	WO								
10/09/2018	Mon	GS	09:00	17:44			PR	PR		00:11	00:11		07:44	07:49	01:00	M-Attendance Corrected
11/09/2018	Tue	GS	09:10	17:55			PR	PR		00:10	00:10		07:48	07:50	01:00	M-Attendance Corrected
12/09/2018	Wed	GS	09:55	17:54			PR	PR		00:01	00:01		07:59	07:59	01:00	M-Attendance Corrected
13/09/2018	Thu	GS	09:00	17:20			PR	AS					07:20	08:00	01:00	M-Attendance Corrected
14/09/2018	Fri	GS	09:00	17:40			PR	PR		00:15	00:15		07:40	07:45	01:00	M-Attendance Corrected
15/09/2018	Sat	GS	09:00	17:39			PR	AS					07:39	08:00	01:00	M-Attendance Corrected
16/09/2018	Sun	GS					WO	WO								
17/09/2018	Mon	GS					AS	AS								S-No Punches Available
18/09/2018	Tue	GS					AS	AS								S-No Punches Available
19/09/2018	Wed	GS					AS	AS								S-No Punches Available
Total:										00:59	00:37	01:36	00:00	103:38	94:24	12:00

- **Hourly Attendance** - This report generates a listing of day-based hourly attendance for selected users over a specified date range.

Hourly Attendance

Back

Find... 1 of 64 100%

Main Report

ORGANISATION 1.

Page 1 of 64

Run by: System Admin

Hourly Attendance from 03/06/2013 to 04/06/2013

Date: 28/01/2014 17:34

Date	Day	Shift	IN	OUT	IN	OUT	Late IN	Early OUT	Gross Work	Extra Work	Net Work	Total OT
1 - SALIM ANSARI												
03/06/2013	Mon	23	08:27	12:19	12:49	17:01			08:04	00:03	08:04	00:00
04/06/2013	Tue	23	08:28	12:09	12:37	17:04			08:08	00:02	08:08	00:00
Total							00:00	00:00	16:12	00:05	16:12	00:00
10 - RAJENDRA GOSWAMI												
03/06/2013	Mon	23							00:00	00:00	00:00	00:00
04/06/2013	Tue	23	08:26	12:53	13:16	17:02			08:13	00:04	08:13	00:00
Total							00:00	00:00	08:13	00:04	08:13	00:00
1001 - ANKITKUMAR SOHLIYA												
03/06/2013	Mon	GS	09:25	19:25					09:10	00:00	09:10	00:00
04/06/2013	Tue	GS	09:22	19:10					08:58	00:00	08:58	00:00
Total							00:00	00:00	18:08	00:00	18:08	00:00

- **Work Hours Summary** - Generates a listing of day-wise work hours summary for selected users for a specified date range.

Work Hours Summary

Back

Find... 1 of 47 100%

Main Report

ORGANISATION 1. Page 1 of 47

Work Hours Summary Report From 01/07/2013 To 02/07/2013

Run by: System Admin Date: 28/01/2014 17:41

Date	First IN	Last OUT	Gross Work Hours	Extra Work Hours	Net-Work Hours	Total Overtime	Less Work Hours
1 - SALIM ANSARI							
01/07/2013			00:00	00:00	00:00	00:00	00:00
02/07/2013	08:29	17:02	08:03	00:01	08:03	00:00	00:00
		Total	08:03	00:01	08:03	00:00	00:00
10 - RAJENDRA GOSWAMI							
01/07/2013			00:00	00:00	00:00	00:00	00:00
02/07/2013	08:26	17:02	08:09	00:04	08:09	00:00	00:00
		Total	08:09	00:04	08:09	00:00	00:00
1001 - ANKITKUMAR SOHLIYA							
01/07/2013	09:25	19:19	09:04	00:00	09:04	00:00	00:00
02/07/2013	09:35	19:19	08:54	00:00	08:54	00:00	00:00
		Total	17:58	00:00	17:58	00:00	00:00

- **Daily Details** - Generates group-wise daily time and attendance details for a specified date-range and in a specified format.

Daily Details

Date * 01/09/2018 19/09/2018

Optional Parameters

Group By Organization

Group by User

Format Selection All Punches

New Page For Each Date/User ☒

User Selection

Select Users All

Generate Report For All Users

Generate Report

In this Loss Hours = Shift hours - Actual working hours in shift
 = 08:00 - 07:45 = 00:15 hours as shown below

When there is no punch on a day; then Loss hours = Shift hours= 8 hours
 On Week Off, there is no loss work hours.

DADB														
Organization-Wise Daily Summary From 01/01/2017 To 07/01/2017														
Run by: System Admin		Date: 27/07/2022 11:14												
User ID	Name	Shift	Day Status	First IN	Last OUT	Early IN	Late IN	Early OUT	Late OUT	Hourly Paid Leave	Hourly Unpaid Leave	Gross Hours	Net Work Hours	Within Shift
01/01/2017 (Sunday)														
DADB	mtali	OS	N			08:00	08:00	00:00	00:00			00:00	00:00	00:00
ORG2	mtali	OS	N			08:00	08:00	00:00	00:00			00:00	00:00	00:00
02/01/2017 (Monday)														
DADB	mtali	OS	N			08:00	08:00	00:00	00:00			00:00	00:00	00:00
ORG2	mtali	OS	N			08:00	08:00	00:00	00:00			00:00	00:00	00:00
03/01/2017 (Tuesday)														
DADB	mtali	OS	N			08:00	08:00	00:00	00:00			00:00	00:00	00:00
ORG2	mtali	OS	N			08:00	08:00	00:00	00:00			00:00	00:00	00:00
04/01/2017 (Wednesday)														
DADB	mtali	OS	N			08:00	08:00	00:00	00:00			00:00	00:00	00:00
ORG2	mtali	OS	N			08:00	08:00	00:00	00:00			00:00	00:00	00:00

- **Daily Work Details-** Displays the Report with daily work details of selected users for selected period.

Daily Work Details

Date *
01/09/2018
19/09/2018

Optional Parameters

Group By
Organization

New Page For Each User
☒

Add Custom Footer
☐

Remark:

User Selection

Select Users
User Wise

User *
ID
Name

Search

User ID	Name	
3	Isha Shah	
101	Khushbu Gorawala	

Generate Report For
All Users

Generate Report

Less Hours: "Late-IN + Early-OUT" for the Punch Date.

Daily Work Details

Back

Find... 2 of 2 100%

Main Report

Organization-1

Organization-Wise Daily Work Details Report From 01/09/2018 To 19/09/2018

Run by: System Admin Date: 19/09/2018

Date	Day	1 IN	2 OUT	3 IN	4 OUT	5 IN	6 OUT	Last IN	Last OUT	Net-Work Hours	Less Work	Auth OT	Site	Remarks
Organization-1														
01/09/2018	Saturday									09:00	08:00	00:00		
02/09/2018	Sunday									00:00	00:00	00:00		
03/09/2018	Monday	07:00	20:00					07:00	20:00	00:00	00:00	00:00		Attendance C
04/09/2018	Tuesday	07:30	19:30					07:30	19:30	00:00	00:00	00:00		Attendance C
05/09/2018	Wednesday	09:15	19:00					09:15	19:00	00:00	00:00	00:00		Attendance C
06/09/2018	Thursday	09:35	20:00					09:35	20:00	00:00	00:00	00:00		Attendance C
07/09/2018	Friday	09:39	19:00					09:39	19:00	00:00	00:00	00:00		Attendance C
08/09/2018	Saturday	09:00	17:55					09:00	17:55	00:00	00:05	00:00		Attendance C
09/09/2018	Sunday									00:00	00:00	00:00		
10/09/2018	Monday	09:00	17:44					09:00	17:44	00:00	00:16	00:00		Attendance C
11/09/2018	Tuesday	09:10	17:55					09:10	17:55	00:00	00:15	00:00		Attendance C
12/09/2018	Wednesday	08:55	17:54					08:55	17:54	00:00	00:01	00:00		Attendance C
13/09/2018	Thursday	09:00	17:20					09:00	17:20	00:00	00:40	00:00		Attendance C
14/09/2018	Friday	09:00	17:40					09:00	17:40	00:00	00:20	00:00		Attendance C

- **Break Deviation** - When break deviation is allowed for a shift, i.e. for shifts with fixed but flexible break duration, a report can be generated to view the difference between the defined break duration and the actual break taken by employees. This difference is defined as break deviation.

Break Deviation

Back

Find... 1 of 5 100%

Main Report

Organization-1

Organization-Wise Break Deviation Report From 01/10/2019 To 24/10/2019

Run by: System Admin Date: 24/10/2019 12:04

Sr No	User ID	Name	Date	Break Start	Break End	Assigned Shift	Defined Duration	Actual Duration	Deviation
Organization-1									
1	1	Yagnesh	16/10/2019			GS	01:00	01:00	
2	1	Yagnesh	17/10/2019			GS	01:00	01:00	
3	1	Yagnesh	18/10/2019			GS	01:00	01:00	
4	1	Yagnesh	19/10/2019			GS	01:00	01:00	
5	1	Yagnesh	20/10/2019			GS	01:00	01:00	
6	1	Yagnesh	21/10/2019			GS	01:00	01:00	
7	1	Yagnesh	22/10/2019			GS	01:00	01:00	
8	1	Yagnesh	23/10/2019			GS	01:00	01:00	
9	1	Yagnesh	24/10/2019			GS	01:00	01:00	
10	13	Sujal	01/10/2019			GS	01:00	01:00	
11	13	Sujal	02/10/2019			GS	01:00	01:00	
12	13	Sujal	03/10/2019			GS	01:00	01:00	
13	13	Sujal	04/10/2019			GS	01:00	01:00	
14	13	Sujal	05/10/2019			GS	01:00	01:00	
15	13	Sujal	06/10/2019			GS	01:00	01:00	
16	13	Sujal	07/10/2019			GS	01:00	01:00	
17	13	Sujal	08/10/2019			GS	01:00	01:00	
18	13	Sujal	09/10/2019			GS	01:00	01:00	
19	13	Sujal	10/10/2019			GS	01:00	01:00	
20	13	Sujal	11/10/2019			GS	01:00	01:00	
21	13	Sujal	12/10/2019			GS	01:00	01:00	
22	13	Sujal	13/10/2019			GS	01:00	01:00	
23	13	Sujal	14/10/2019			GS	01:00	01:00	
24	13	Sujal	15/10/2019			GS	01:00	01:00	

- **Shift-Wise Count Summary** - Generates user summary for all shifts configured on COSEC. Shift Summary fields to be viewed are user selectable.

Shift-Wise Count Summary

Page 1 of 1

Organization-1

Shift-Wise Count Summary For 10/10/2019

Run by: System Admin

Date: 24/10/2019 12:07

Not Yet

Shift ID	Name	Assigned	Scheduled	On Leave/Tour	On Week-OFF	On Holiday	Reported	Reported
GS	General Shift	7	7	0	0	0	3	4

Assigned

User ID	Name	Shift	First Punch	Last Punch	First Half	Second Half
13	Sujal	GS			AB	AB
5	Keval	GS			AB	AB
501	Ramesh	GS			AB	AB
502	Shyam	GS	09:04		IN	AB
503	Meet	GS	07:30		IN	AB
504	Gunjan	GS	07:32		IN	AB
54	Hitesh	GS			AB	AB

Scheduled

User ID	Name	Shift	First Punch	Last Punch	First Half	Second Half
13	Sujal	GS			AB	AB
5	Keval	GS			AB	AB
501	Ramesh	GS			AB	AB
502	Shyam	GS	09:04		IN	AB
503	Meet	GS	07:30		IN	AB
504	Gunjan	GS	07:32		IN	AB
54	Hitesh	GS			AB	AB

Reported

User ID	Name	Shift	First Punch	Last Punch	First Half	Second Half
502	Shyam	GS	09:04		IN	AB
503	Meet	GS	07:30		IN	AB
504	Gunjan	GS	07:32		IN	AB

Not Yet Reported

User ID	Name	Shift	First Punch	Last Punch	First Half	Second Half
13	Sujal	GS			AB	AB
5	Keval	GS			AB	AB
501	Ramesh	GS			AB	AB
54	Hitesh	GS			AB	AB

- **First-IN Last-OUT Punch Details** - Generates user details for First-IN and Last-OUT Punches on COSEC.

First IN-Last OUT Punch Details

←

Back

Find...

2 of 12

100%

Main Report

Organization-1

Page 2 of 12

First IN-Last OUT Punch Details From 05/08/2019 To 05/09/2019

Run by: System Admin

Date: 05/09/2019 13:07

User ID	Name	Date	First IN	Last OUT	IN Device	OUT Device	Total Hours(100)
111	Komal Shah	05/08/2019	05/08/2019	05/08/2019			11.00
			09:00:00	20:00:00			
111	Komal Shah	06/08/2019	06/08/2019	06/08/2019			10.67
			09:20:00	20:00:00			
111	Komal Shah	07/08/2019	07/08/2019	07/08/2019			4.75
			09:00:00	13:45:00			
111	Komal Shah	08/08/2019	08/08/2019	08/08/2019			13.00
			09:00:00	22:00:00			
111	Komal Shah	09/08/2019	09/08/2019	09/08/2019			11.00
			09:00:00	20:00:00			
111	Komal Shah	10/08/2019	10/08/2019	10/08/2019			12.00
			09:00:00	21:00:00			
111	Komal Shah	11/08/2019	11/08/2019	11/08/2019			10.67
			09:20:00	20:00:00			

Absenteeism

This section allows the user to generate *Absenteeism* related attendance reports. The following reports fall under this category:

- **Absentee** - Generates a group wise listing of the employees with details of the Absent days during the specified time period as shown.

Absentee							
Back							
Find... 1 of 1 100%							
Main Report							
Organization-1							
Page 1 of 1							
Organization-Wise Absentee From 24/10/2019 To 24/10/2019							
Run by: System Admin				Date: 24/10/2019 12:59			
Sr No	User ID	Name	Date	Shift	1st Half	2nd Half	
Organization : Organization-1							
1	1	Yagnesh	24/10/2019	GS	AB	AB	
2	13	Sujal	24/10/2019	GS	AB	AB	
3	5	Keval	24/10/2019	GS	AB	AB	
4	501	Ramesh	24/10/2019	GS	AB	AB	
5	502	Shyam	24/10/2019	GS	AB	AB	
6	503	Meet	24/10/2019	GS	AB	AB	
7	504	Gunjan	24/10/2019	GS	AB	AB	
8	54	Hitesh	24/10/2019	GS	AB	AB	

- **Absenteeism Memo** - This option enables the administrator to generate and print multiple or individual Absent Memos as shown.

Absenteeism Memo

←

Back

Main Report

Organization-1

Absenteeism Memo From 24/10/2019 To 24/10/2019

Run by: System Admin Date:24/10/2019 14:57

User	: 1 Yagnesh	Branch	: Branch-1	
Department	: Department-1	Designation	: Designation-1	
Sr No	Date	Shift	1st Half	2nd Half
1	24/10/2019	GS	AB	AB

You have been marked absent on above dates between 24/10/2019 and 24/10/2019
total 1 day(s)

Organization-1

Absenteeism Memo From 24/10/2019 To 24/10/2019

Run by: System Admin Date:24/10/2019 14:57

User	: 13 Sujal	Branch	: Branch-1	
Department	: Department-1	Designation	: Designation-1	
Sr No	Date	Shift	1st Half	2nd Half
1	24/10/2019	GS	AB	AB

You have been marked absent on above dates between 24/10/2019 and 24/10/2019
total 1 day(s)

Organization-1

Absenteeism Memo From 24/10/2019 To 24/10/2019

Run by: System Admin Date:24/10/2019 14:57

User	: 5 Keval	Branch	: Branch-1	
Department	: Department-1	Designation	: Designation-1	
Sr No	Date	Shift	1st Half	2nd Half
1	24/10/2019	GS	AB	AB

You have been marked absent on above dates between 24/10/2019 and 24/10/2019

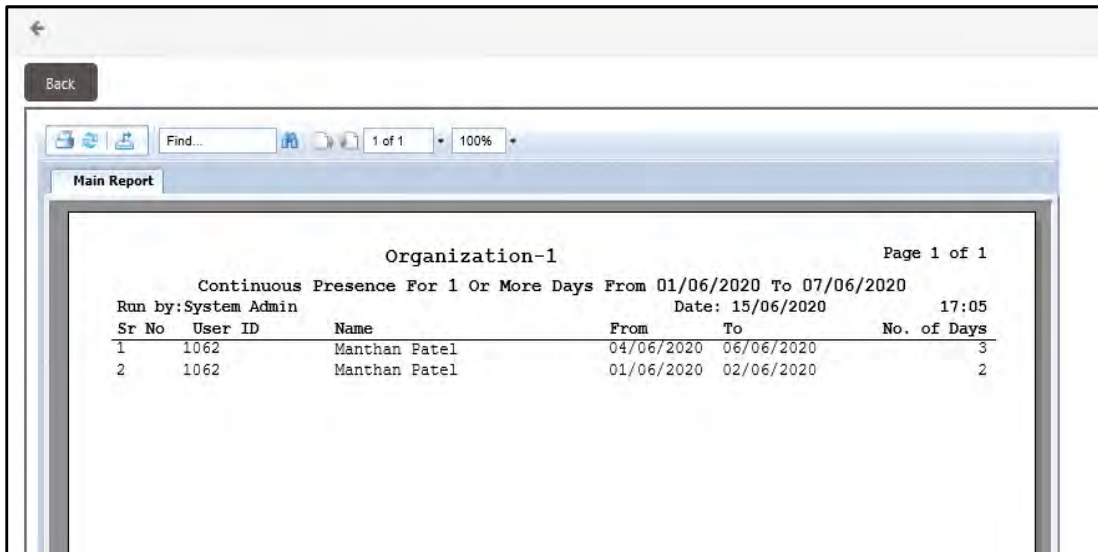
- **Continuous Absence/Presence** - The continuous Absence/Presence report allow you to generate the attendance summery of user, if he/she is absent or present continuously for many days/hours.

Specify the Report type as **Continuous Absence** or **Continuous Presence**.

Continuous Presence:

For the optional parameters configuration and related example, [See "Example: Continuous Absence/Presence" on page 340.](#)

Configure the **User Selection** and click on **Generate Report** button.



Sr No	User ID	Name	From	To	No. of Days
1	1062	Manthan Patel	04/06/2020	06/06/2020	3
2	1062	Manthan Patel	01/06/2020	02/06/2020	2

Continuous Absence:

For the optional parameters configuration and related example, [See "Example: Continuous Absence/Presence" on page 340.](#)

Configure the **User Selection** and click on **Generate Report** button.

Back

Find... 1 of 1 100%

Main Report

Organization-1 Page 1 of 1

Continuous Absence For 1 Or More Days From 01/06/2020 To 07/06/2020

Run by: System Admin Date: 15/06/2020 16:40

Sr No	User ID	Name	From	To	No. of Days
1	1062	Manthan Patel	07/06/2020	07/06/2020	1
2	1062	Manthan Patel	03/06/2020	03/06/2020	1

- **Week Off & Holiday** - This report will generate list of all coinciding Week Offs and holidays during the specified time period.

Week Off & Holiday On Same Day

Back

Find... 1 of 15 100%

Main Report

ORGANISATION 1. Page 1 of 15

Organization-Wise Week Off & Holiday On Same Day from 01/01/2013 to 31/12/2013

Run by: System Admin Date: 28/01/2014 18:30

Sr No	User ID	Name	Date	Day	Holiday
1	1053	JINU SAM	15/01/2013	TUESDAY	Makar Sankranti
2	1053	JINU SAM	19/08/2013	MONDAY	24TH 2ND SAT WORKING
3	1054	PARSHV SHAH	15/01/2013	TUESDAY	Makar Sankranti
4	1054	PARSHV SHAH	19/08/2013	MONDAY	24TH 2ND SAT WORKING

Overtime

This section lists all Overtime-related attendance reports as follows:

- **Overtime Report** - Generates a group wise listing of the employees with details of their Overtime during the specified time period.

Overtime

←

Back

Find... 1 of 6 75%

Main Report

ORGANISATION 1. Page 1 of 6

Organization-Wise Overtime Report from 01/01/2013 to 02/01/2013

Run by: System Admin Date: 28/01/2014 18:36

Sr No	User ID	Name	Date	Shift	In	Out	Overtime	Authorized	Credit	Debit	Availed	Available
ORGANISATION 1.												
1	1057	JANPRIYA MALVIYA	01/01/2013	G3	09:23	19:44	01:14	00:00	00:00	00:00	00:00	00:00
2	1062	MANTHAN PATEL	01/01/2013	G3	09:23	19:51	01:21	00:00	00:00	00:00	00:00	00:00
3	1062	MANTHAN PATEL	02/01/2013	G3	09:23	21:14	02:44	00:00	00:00	00:00	00:00	00:00
4	808	Chintan H Patil	01/01/2013	G3	08:02	22:02	03:32	00:00	00:00	00:00	00:00	00:00
5	808	Chintan H Patil	02/01/2013	G3	07:58	22:55	04:25	00:00	00:00	00:00	00:00	00:00
6	812	Bhadrasinh Gurkha	02/01/2013	G4	00:00	22:51	03:51	00:00	00:00	00:00	00:00	00:00
7	813	Manohar Male	01/01/2013	G3	00:00	19:49	01:19	00:00	00:00	00:00	00:00	00:00
8	813	Manohar Male	02/01/2013	G3	00:00	19:40	01:10	00:00	00:00	00:00	00:00	00:00
9	864	R G SHARMA	01/01/2013	G3	22:29	06:00	11:30	00:00	00:00	00:00	00:00	00:00
10	864	R G SHARMA	02/01/2013	G3	20:59	06:00	11:30	00:00	00:00	00:00	00:00	00:00
11	865	FIRDOSH MANSURI	01/01/2013	11	07:45	18:01	01:01	00:00	00:00	00:00	00:00	00:00
12	865	FIRDOSH MANSURI	02/01/2013	11	07:53	18:03	01:03	00:00	00:00	00:00	00:00	00:00
13	892	HEMANT KUMAR MARCO	01/01/2013	G3	23:59	05:32	11:02	00:00	00:00	00:00	00:00	00:00
Overtime Group Total:							55:42	00:00	00:00	00:00	00:00	00:00

- **Overtime Details** - Generates user-wise Overtime details for a specified period.
- **Total Head Count & Overtime** - Generates shift-wise total headcount and overtime hours for the specified date-range.
- **Users Presence & Overtime** - Generates site-wise user attendance and overtime details for the specified period.
- **Weekly Working Hrs & Overtime** - Lists day-wise working hours and overtime hours for the specified week as shown in the figure below.

ORGANISATION 1. Page 1 of 30

Weekly Working Hrs & Overtime From 21/01/2013 To 27/01/2013

Run by: System Admin Date: 07/10/2014 23:12

Sr No	User ID	Name	Department	Daily OT	Weekly OT	OT On	WO/PH	WrkHrs
1	1	SALIM ANSARI	Assembly	00:00	00:00	00:00	00:00	37:23
		21 (MON)	22 (TUE)	23 (WED)	24 (THU)	25 (FRI)	26 (SAT)	27 (SUN)
Overtime		02:01	02:02	-	02:00	-	-	-
Auth. OT		-	-	-	-	-	-	-
Work Hrs		09:43	09:44	08:06	09:50	-	-	-
2	10	RAJENDRA GOSWAMI	Repairing	00:00	00:00	00:00	00:00	49:15
		21 (MON)	22 (TUE)	23 (WED)	24 (THU)	25 (FRI)	26 (SAT)	27 (SUN)
Overtime		-	-	-	-	-	-	01:00
Auth. OT		-	-	-	-	-	-	-
Work Hrs		08:18	08:18	07:56	08:15	08:13	-	08:15
3	1001	ANKITKUMAR SOHLIYA	SDG - Security	00:00	00:00	00:00	00:00	46:15
		21 (MON)	22 (TUE)	23 (WED)	24 (THU)	25 (FRI)	26 (SAT)	27 (SUN)
Overtime		01:31	-	-	01:06	-	-	-
Auth. OT		-	-	-	-	-	-	-
Work Hrs		09:49	09:19	09:01	09:20	08:46	-	-

Exceptions

This section enables the user to generate reports related to attendance exceptions of employees for a defined time period. The following reports can be generated using this section:

- **Exceptions** - This report lists group-wise attendance exceptions for selected employees for the specified date-range as shown.

ORGANISATION 1.									
Organization-Wise Exception from 01/01/2012 to 31/12/2012									
Run by: System Admin					Date: 29/01/2014 11:54				
Sr No	User ID	Name	Date	Shift	In	Out	1st Half	2nd Half	Reason
ORGANISATION 1.									
1	1053	JINU SAM	11/05/2012	GS			AB	AB	No Punches available
2	1053	JINU SAM	17/05/2012	GS			AB	AB	No Punches available
3	1053	JINU SAM	18/05/2012	GS			AB	AB	No Punches available
4	1053	JINU SAM	19/05/2012	GS			AB	AB	No Punches available

- **Attendance Exception** - This report generates a listing of selected users Attendance Exceptions for each day, wherever exceptions has occurred. The exceptions that will be considered are as follows:
 - Absent on Normal Shift
 - Worked on Week-off
 - Worked on Holiday
 - Worked on Leave

ORGANISATION 1.									
Organization-Wise Attendance Exception Report From 05/02/2013 To 20/02/2013									
Run by: System Admin					Date: 24/04/2014 18:57				
Sr No	Date	User ID	Name	First Half	Second Half	FirstLast IN OUT	Shift	Work Hrs	Remark
ORGANISATION 1.									
1	05/02/2013	1055	SANDIP FATEL	AB	AB	08:47 20:08	GS	10:31	Absent
2	06/02/2013	1055	SANDIP FATEL	AB	AB	08:59 19:59	GS	10:10	Absent
3	07/02/2013	1055	SANDIP FATEL	AB	AB	09:24 19:32	GS	09:18	Absent
4	08/02/2013	1055	SANDIP FATEL	AB	AB	08:51 20:00	GS	10:19	Absent
5	11/02/2013	1055	SANDIP FATEL	AB	AB	08:51 20:10	GS	10:29	Absent
6	12/02/2013	1055	SANDIP FATEL	AB	AB	08:58 19:56	GS	10:08	Absent
7	13/02/2013	1055	SANDIP FATEL	AB	CL	08:49 13:30	GS	04:41	Absent
8	15/02/2013	1055	SANDIP FATEL	CL	AB	12:57 20:03	GS	06:16	Absent
9	15/02/2013	1055	SANDIP FATEL	CL	AB	12:57 20:03	GS	06:16	Worked On Leave
10	16/02/2013	1055	SANDIP FATEL	AB	AB	08:49 19:58	GS	10:19	Absent
11	18/02/2013	1055	SANDIP FATEL	AB	AB	08:56 19:59	GS	10:13	Absent
12	19/02/2013	1055	SANDIP FATEL	AB	AB	09:26 20:37	GS	10:21	Absent
13	20/02/2013	1055	SANDIP FATEL	AB	AB	09:11 20:29	GS	10:28	Absent

- **Manual Correction** - This report generates a listing of all the attendance records for the selected period where manual correction has been done.

Format 1

Manual Correction

←

Date * 01/10/2017 31/10/2017

Optional Parameters

Group By Organization

Format Selection Format 1

User Selection

Select Users User Wise

User * ID Name

Search

User ID ▲	Name	
1895	Priya S	

Generate Report For All Users

Generate Report

Matrix

Page 1 of 1

Organization-Wise Manual Correction From 01/10/2017 To 31/10/2017

Run by: System Admin Date: 08/11/2017 17:50

Sr No	User ID	Name	Attendance Date	1st Half	2nd Half	Work Hours	Correction Date	Corrected By	Remark
Cafeteria									
1	1895	Priya S	09/10/2017	PR	PR	09:32	12/10/2017	System Admin	
2	1895	Priya S	10/10/2017	PR	PR	09:45	11/10/2017	System Admin	
3	1895	Priya S	11/10/2017	PR	PR	09:41	11/10/2017	System Admin	

Format 2

Manual Correction

←

Date * 01/10/2017 31/10/2017

Optional Parameters

Group By Organization

Format Selection Format 2

User Selection

Select Users User Wise

User * ID Name

Search

User ID ▲	Name	
1895	Priya S	

Generate Report For All Users

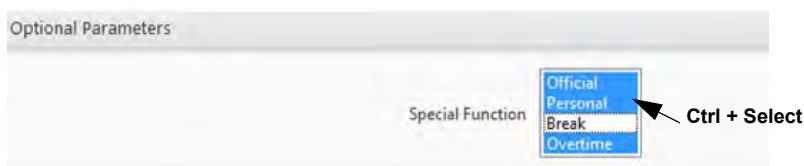
Generate Report

Matrix Organization-Wise Manual Correction From 01/10/2017 To 31/10/2017							Page 1 of 1
Run by: User ID	System Admin Name	Department	Attendance Date	Changed Parameter	Previous value	Current Value	Date: 08/11/2017 Corrected By Correction Date
Cafeteria							
1895	Priya S		09/10/2017	IN Punch 1	09:00	System Admin	12/10/2017
1895	Priya S		09/10/2017	OUT Punch 2	18:32	System Admin	12/10/2017
1895	Priya S		10/10/2017	IN Punch 1	09:00	System Admin	11/10/2017
1895	Priya S		10/10/2017	OUT Punch 2	13:30	System Admin	11/10/2017
1895	Priya S		10/10/2017	IN Punch 3	13:45	System Admin	11/10/2017
1895	Priya S		10/10/2017	OUT Punch 4	19:00	System Admin	11/10/2017
1895	Priya S		11/10/2017	IN Punch 1	09:00	System Admin	11/10/2017
1895	Priya S		11/10/2017	OUT Punch 2	19:00	System Admin	11/10/2017

- **Pending Authorization** - This report generates a date and group-wise listing of all records which are pending for authorization, depending on the **Approval Type** selected. In this example, the Approval Type selected was *Attendance Correction*.

ORGANISATION 1. Organization-Wise Pending Authorizations From 01/01/2013 To 24/07/2014							Page 2 of 1
Run by: User ID	System Admin Name	Department	Attendance Date	Authorization Type	Reporting Group	Reason	Date:24/07/2014 17:5
Matrix Comsec Pvt. Ltd.							
26	YOGENDRA MEHTA	Accounts	29/04/2013	Attendance Correction	Prakash Punjabi		
31	ASHUTOSH PRADHAN	Purchase	22/02/2013	Attendance Correction	Yogesh Sharma		
31	ASHUTOSH PRADHAN	Purchase	21/03/2013	Attendance Correction	Yogesh Sharma		
31	ASHUTOSH PRADHAN	Purchase	02/05/2013	Attendance Correction	Yogesh Sharma		
31	ASHUTOSH PRADHAN	Purchase	16/09/2013	Attendance Correction	Yogesh Sharma		
31	ASHUTOSH PRADHAN	Purchase	03/10/2013	Attendance Correction	Yogesh Sharma		
324	ARJUN G PATEL	Call Centre	09/09/2013	Attendance Correction	yogesh panchal		
324	ARJUN G PATEL	Call Centre	25/09/2013	Attendance Correction	yogesh panchal		
33	GOPAL TANK	Call Centre	20/06/2013	Attendance Correction	Vimal Gami		
387	MALVIK SHETH	Marketing	12/01/2013	Attendance Correction			

- **Special Function Punch** - Generates a function wise listing of all employees who have made use of the special function during the specified time period as shown. Hold down the *Control key (Ctrl)* on the keyboard and click on the functions to select multiple special functions on the **Special Function Punch** report page before generating the report (as shown below).



- **Shift Change** - Generates all records of organization-wise change of shifts for selected users during the specified period as shown.

ORGANISATION 1. Organization-Wise Shift Change from 01/01/2013 to 31/01/2013						Page 1 of 1
Run by: System Admin						Date:29/01/2014 12:21
Sr No	User ID	User Name	Date	Scheduled Shift	Current Shift	
Matrix Comsec Pvt. Ltd.						
1	255	GAUTAM RATHOD	04/01/2013	EU	GS	
2	255	GAUTAM RATHOD	10/01/2013	EU	GS	
3	255	GAUTAM RATHOD	31/01/2013	EU	GS	
4	540	FARESH C GOSAI	04/01/2013	GS	21	
5	540	FARESH C GOSAI	07/01/2013	GS	21	
6	540	FARESH C GOSAI	11/01/2013	GS	23	

- **Shift Allowance** - Generates a listing of cumulative shift allowance of selected users per shift for the selected date range.
- **Authorization Status** - Generates an group-wise listing of application records for selected users, based on their approval status (i.e. approved, rejected or both).

Monthly Reports

The following reports are available under the *Monthly Reports* option.

- **Muster Roll** - Generates a group- wise muster roll with the system-defined attendance status as well as the leave status as shown.

ORGANISATION 1.

Muster Roll For JUNE-2013

Page 3 of 12

Run by: System Admin

Sr No User ID Name Designation PR WO PH PL TR AB UL

Date: 17/06/2014 12:10

Marketing

14 1095 ABHAY JOSHI Team Leader 9.5 7.0 0.0 1.5 12.0 0.0 0.0

Shift 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Stat1 GS

Stat2 FR WO CO FR FR FR FR WO WO FR FR FR CL FR TR WO TR TR TR TR TR WO WO TR TR TR TR TR WO

15 1108 DHEERAJ GUPTA BUSINESS MANAGER 10.0 2.0 0.0 0.0 0.0 0.0 0.0

Shift 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Stat1 GN

Stat2 FR WO FR FR FR FR FR FR WO FR FR FR FR FR FR FR FR FR FR FR FR FR FR FR FR FR FR FR WO

16 1109 SHALINI YADAV Engineer 17.0 7.0 0.0 2.5 0.0 3.5 0.0

Shift 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Stat1 GS

Stat2 CL WO CL CL AB AB AB AB WO WO FR WO

Support

17 1110 NISHIT PARESHKUMAR GANDHI Engineer 21.0 7.0 0.0 1.0 1.0 0.0 0.0

Shift 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Stat1 GS

Stat2 TR WO FR FR FR FR FR WO WO FR FR FR FR FR FR CL WO FR FR FR FR FR FR FR FR FR FR FR FR FR FR WO

- **Muster Summary** - This report generates a summary of the data presented in the Muster roll.

Muster Summary														
Back														
Find... 1 of 1 100%														
Main Report														
Matrix														
Organization-Wise Muster Summary For AUGUST-2017														
Run by:	System Admin	User											Date:	2017/09/06
Sr No	ID	Name/Designation	PR	WO	PH	TR	PL	AB	UL	LO	Total OT	Auth OT	Total WkTime	Total C-OFF
1	1320	SHRUTI SAGAR PATKI	0.0	8	0	0.0	0.0	23.0	0.0	0.0	00:00	00:00	00:00	00:00
2	1690	Priyank Bora	0.5	4	3	0.0	4.0	19.5	0.0	0.0	00:50	00:50	21:33	00:00
3	2192	chirag Shah designation	4.0	8	2	0.0	0.0	17.0	0.0	0.0	43:00	00:15	43:00	41:00

- **Previous Adjustment Summary** - Generates the list of Previous adjustment transactions which have occurred in the specified month for selected users.
- **Salary Data** - This report generates a Salary Data statement for the specified month for selected users.
- **Absentee Detail** - Generates a list of all employees along with the dates on which they have been absent during the selected month as shown.

ORGANISATION 1.					Page 1 of 27
Organization-Wise Absentee Detail For JANUARY-2013					
Run by: System Admin			Date: 29/01/2014 12:33		
User ID			Total AB Days		
Sr No	Name	Designation	Absent Dates	Days	
ORGANISATION 1.					
1 1053	JINU SAM	Engineer	3h,	0.5	
2 1055	SANDIP PATEL	Engineer	1h, 4, 5, 12, 25, 30, 31	6.5	
3 1056	RITESH RAJPUT	Engineer	3, 25	2.0	
4 1059	PRATIK PATEL	Engineer	16, 29, 30, 31	4.0	
5 1063	KISHOR HEMNANI	Engineer	18h,	0.5	

- **Monthly Details** - Generates group-wise attendance details of specific employees for the selected month in a specified format. Available report formats are: *Count-wise, Day-Wise, Day-Wise with Status, Month-Wise Attendance and Status & Count Summary* (shown in the example below).

DADB											Page 1 of 4		
Organization-Wise Monthly Details For APRIL-2017													
Run by: System Admin		Date: 18/08/2022									17:21		
User	User Name	N	WO	PH	PL	UL	TR	PR	AB	SL	Net-Work	Auth OT	Loss Hours
ID													
DADB													
EOgraceexceed	Earlyout grace duration exceeds	24	5	1	1.0	0.0	0.0	2.0	21.0	2	18:19	00:00	00:00
FB	OT for FB	24	5	1	1.0	0.0	0.0	1.0	22.0	0	09:00	00:00	00:00
firsthalfabsent	First half absent sent	24	5	1	1.0	0.0	0.0	1.5	21.5	2	09:30	00:00	00:00
Firsthalfave	User with first half leave	24	5	1	3.5	0.0	0.0	1.0	19.5	0	09:00	00:00	00:00
Flexible	flexibleuser	24	5	1	1.0	0.0	0.0	0.0	23.0	0	12:30	00:00	00:00
FlexibleOT	OT for flexible user	24	5	1	1.0	0.0	0.0	0.0	23.0	0	16:00	00:00	00:00
Fulldayleave	User with full day leave	24	5	1	3.5	0.0	0.0	0.0	20.5	0	00:00	00:00	00:00
Inpunch	User with In pucnh only	24	5	1	0.5	0.0	0.0	0.0	23.5	0	00:00	00:00	00:00
Jpodefaultenter	Job coseting user with default job of enterpr	24	5	1	1.0	0.0	0.0	0.5	22.5	0	09:30	00:00	00:00
JPCmergejob	JPC merged Job	24	5	1	0.5	0.0	0.0	2.0	21.5	0	18:00	00:00	00:00
Lategraceexceed	User with exceed grace period	24	5	1	1.0	0.0	0.0	2.0	21.0	2	18:04	00:00	00:00
Latein	user punches on latein only	24	5	1	1.0	0.0	0.0	2.0	21.0	1	18:00	00:00	00:30
Lateinduraxceed	Late in Duration exceed	24	5	1	1.0	0.0	0.0	2.0	21.0	2	18:30	00:00	00:00
Lateingrace	User have pucnges on grace latein	24	5	1	1.0	0.0	0.0	3.0	20.0	0	27:01	00:00	00:00
Lessworkhours	Less work hours for daily limit	24	5	1	1.0	0.0	0.0	4.0	19.0	0	35:20	00:00	00:00
manualOT	User with Manual Overtime	24	5	1	1.0	0.0	0.0	2.0	21.0	0	24:30	00:00	00:00
mitali	mitali	29	1	0	0.0	0.0	3.5	2.5	0.0	1	26:08	00:00	00:20
mixshift	mixshifts	0	0	0	0.0	0.0	0.0	0.0	0.0	0	00:00	00:00	00:00
NetworkHrs	Networkhours bt no OT Component	24	5	1	1.0	0.0	0.0	1.0	22.0	0	28:00	00:00	00:00
NightShift	NightShift	24	5	1	1.0	0.0	0.0	2.0	21.0	0	18:00	00:00	00:00
Normal	normal user	24	5	1	1.0	0.0	0.0	2.0	21.0	0	18:00	00:00	00:00
npgraceEO	Npunch user with grace in EO and EO duration	24	5	1	1.0	0.0	0.0	9.0	14.0	8	84:51	00:00	00:10

User Defined Reports

- **Muster Roll** - Generates a department wise muster roll with user-defined attendance status as well as leave status as shown.

ORGANISATION 1.																																		Page 1 of 75	
Muster Roll For JANUARY-2012																																		Date:29/01/2014 14:55	
Run by: System Admin		Sr No		User ID		Name		Designation		PR		MD		PH		PL		TR		AB		UL													
Department-1																																			
1		1050		ANIL MODI		Team Leader		21.0		5.0		2.0		2.5		0.0		0.5		0.0															
Shift		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
Status		W	22	23	23	23	23	23	22	22	23	23	23	23	22	22	23	23	23	23	23	23	22	22	23	23	23	23	22	22	23	23			
		W	P	P	P	P	P	P	W	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P				
2		1060		PRIVESH SHAH		Team Leader		19.0		7.0		1.0		1.0		1.0		2.0		0.0															
Shift		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
Status		GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS				
		W	P	P	P	P	P	P	W	P	P	P	P	A	W	W	A	P	P	P	P	?	W	P	P	P	H	?	W	W	P	P			
3		109		DHIRENDRA SAVLA		Team Leader		22.0		7.0		1.0		0.0		0.0		1.0		0.0															
Shift		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
Status		GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS				
		W	P	P	P	P	P	P	A	W	P	P	P	P	W	W	P	P	P	P	P	P	P	P	P	P	H	P	W	W	P	P			



Use the **Attendance Status Template** option in this section to customize the Output Code for different Attendance Status combinations for first and second half. Output codes defined here will reflect accordingly in the User-defined **Muster Roll** report.

- **Attendance Status Template**- You can customize the output code for different combinations of first half and second half by selecting the status from drop down options. The reason for the status can be selected by clicking “Select Reason” button.

Attendance Status Template

ID

1

Output Status Length

1

Attendance Status

PR-Present

AB-Absent

Select Reason

Absent due to early out

Output Code

1

Search

First Half ▲	Second Half	Output Code
PR	AB	1
AB	PR	2
PR	PR	P
WO	WO	W
AB	AB	A
IN	AB	I

- **Custom Attendance Register** - This is a customized attendance register report generated with user-specified fields. Select fields from the **Available Fields** scroll list and click the **Add** button to enter these in the **Selected Fields** list.

Custom Attendance Register

Attendance Period: ☐ November 2017 ☒ 15/10/2017 to 31/10/2017

Optional Parameters

Available Fields: ☒ Shift ☐ Shift Start Time ☐ Shift End Time ☐ First IN

Selected Fields: ☐ Shift ☐ Shift Start Time ☐ Shift End Time ☐ Late-IN

User Selection

Select Users:

User*

Search

User ID	Name	
10011	User 1001	<input type="button" value="Delete"/>
1002	User 1002	<input type="button" value="Delete"/>
1004	User 1004	<input type="button" value="Delete"/>
1005	User 1005	<input type="button" value="Delete"/>

Generate Report For:

Custom Attendance Register

Matrix

Custom Attendance Register From 15/10/2017 To 31/10/2017

Run by: System Admin

Sr No	User ID	Name	Department	Designation	Brancha	PR	WO	PH	PL	TR	AB	UL					
1	10011	User 1001	department	designation	branch1	0.0	0	0	0.0	0.0	17.0	0.0					
	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue
Shift	DL	DL	DL	DL	DL	DL	DL	DL	DL	DL	DL	DL	DL	DL	DL	DL	DL
Shift Start Time	21:00	21:00	21:00	21:00	21:00	21:00	21:00	21:00	21:00	21:00	21:00	21:00	21:00	21:00	21:00	21:00	21:00
Shift End Time	05:00	05:00	05:00	05:00	05:00	05:00	05:00	05:00	05:00	05:00	05:00	05:00	05:00	05:00	05:00	05:00	05:00
Late-IN																	
Early-OUT																	
WkHrs																	
Overtime																	
Stat1																	
Stat2																	
2	1005	User 1005	department	designation	branch1	0.0	6	1	0.0	0.0	10.0	0.0					
	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue
Shift	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS	GS
Shift Start Time	09:00	09:00	09:00	09:00	09:00	09:00	09:00	09:00	09:00	09:00	09:00	09:00	09:00	09:00	09:00	09:00	09:00
Shift End Time	18:00	18:00	18:00	18:00	18:00	18:00	18:00	18:00	18:00	18:00	18:00	18:00	18:00	18:00	18:00	18:00	18:00
Late-IN	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00
Early-OUT	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00
WkHrs	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00
Overtime	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00
Stat1	WO	WO	AB	PH	AB	AB	AB	WO	WO	AB	AB	AB	AB	AB	WO	WO	AB
Stat2																	

Statutory Reports

These are reports based on the requirement of certain governmental organizations that are required to follow statutory formats for the employee data.

- **FormT-** The Form T is based on the statutory norms of government monthly attendance summary register. The selection parameters and the sample report is shown as below:

For Month-Year: October 2013

Custom Attendance Period: ☐

Month Start-End Date: 2

Optional Parameters

Message: Statutory Report for Form T

Organization Name: ABC Ltd.

Organization Address: GIDC, Makarpura

Leave:

ID	Name
PL	PRIVILEGE LEAVE

Save

Filter

Select Users: Randomly




User:

ID	Name
----	------




Form T

←

Back

Find...

1 of 1

100%

Main Report

Muster Roll
Statutory Report
ABC Ltd.

Wages Period From: 01/10/2013 To: 31/10/2013

Sr. No	Ref. No	Name Designation	Daily Attendance																															
1	10	RAJENDRA GOSWAMI Team Leader	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
			W	P	P	P	P	W	?	P	?	P	P	P	W	P	?	P	P	P	P	W	P	P	?	P	P	P	P	W	P	P	?	P

- **Form 18-** The Form18 is based on the statutory norms of government yearly leave wage register. The selection parameters and the sample report is shown as below:

Year: 2013

Custom Attendance Period: ☐

Month Start-End: February

Optional Parameters

Header Message: Statutory Report for Form18

Organization Name: ABC Ltd.

Organization Address: GIDC, Makarpura

Leave:

ID	Name
PL	PRIVILEGE LEAVE

Footer Message: Form18

Save

Filter

Select Users: Randomly

Form 18

Back

Find... 1 of 1 100%

Main Report

Statutory Report for Form 18

FORM NO. 18 Register of Leave with Wages

1	Full Name	RAJENDRA GOSWAMI			4	Department	Repairing			7	Date of Discharge/ Dismissal while in Service					
2	Sex	Male			5	Designation	Team Leader			8	Date of Payment in lieu of					
3	Sr. No. in the Register	10			6	Date of Joining	31-10-1992			9	Whether Leave in Accordance with 79(8) Refused.					
Calendar Year of Service (i.e. Previous)	Leave Due as at Jan. of Year in Col.	Leave availed during the Year.			Dates		Leave refused out of total leave mentioned in Col.	No. of working days for computation of leave during the year mentioned in Co.				Regular leave earned for the Year mentioned in Col.	Balance of leave admissible on 1st Jan. of the Year following the Year mentioned in Col.	Refused (Col. 3+4-5-6)	Leave Period (i.e. Col. 4+5 in days)	
	Refused	Refused	Refused	Refused	From	To		ABC Ltd.								
	Present	Off	Paid Holiday	Restricted Holiday	PL			GIDC, Makarpura								
	1	2	3	4	5	6		7	8	9	10					11

- **Form 28-** The Form 28 is based on the statutory norms of government monthly wage register. The selection parameters and the sample report is shown as below:

Monthly Summary

For Month-Year April 2017

Optional Parameters

Group By Organization

Format Selection Status Summary

Organization Name in Header As Per User Selection

User Selection

Select Users User Wise

User ID Name

Generate Report For All Users

Generate Report

COMBINED MUSTER ROLL CUM REGISTER OF WAGES																																						
Name and Address of the Establishment																																						
Month/Year: April/2017																																						
Sr. No.	Ref. No.	Name of the User & Father/Spouse	Male/ Female	Designation/ Department	Date of Joining	ESI No. (6) PF No. (7)	Wages fixed including VDA	Attendance (Please mention the date of suspension of employees, if any (9))																														No. of Pay Days
								1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
1		2	3	4	5		8																														10	
1	mitel1 mitel1			Designation-1/Department-1		-		?	?	?	?	?	?	?	?	?	?	?	?	?	?	P	F	P	?	?	?	?	?	?	?	?	?	?	?	?	30	
						-																																
2	mitel11 mitel11			Designation-1/Dept2		-		?	?	?	?	?	?	?	?	?	?	?	?	?	P	A	P	?	A	?	?	?	?	?	?	?	?	?	?	?	30	
						-																																

- **Form 26-** The Form 26 is based on the statutory norms of government's act: "The Shops and Establishment Act." The selection parameters and the sample report is shown as below:

Form 26

For Month-Year: May 2019

Custom Attendance Period: [Calendar Icon]

Month Start-End Date: 2 End Date: [Date Picker]

Optional Parameters

Sub-Header Message	Statutory Report
Left Align Upper Label	100 Chars
Left Align Lower Label	100 Chars
Right Align Upper Label	100 Chars
Right Align Lower Label	100 Chars
Footer Message	MatrixComSec

Save

User Selection

Select Users: User Wise

User * ID Name

Search [Text Box]

User ID ▲	Name	[Icon]
DB	Dhwani Bhatt	[Icon]

Generate Report For: All Users

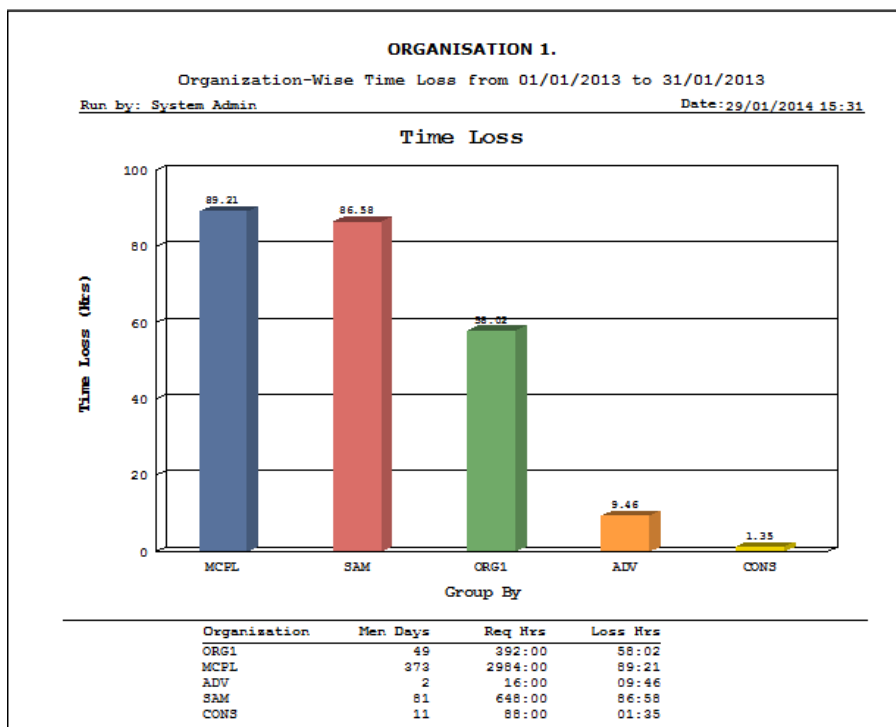
Generate Report

[illegible]

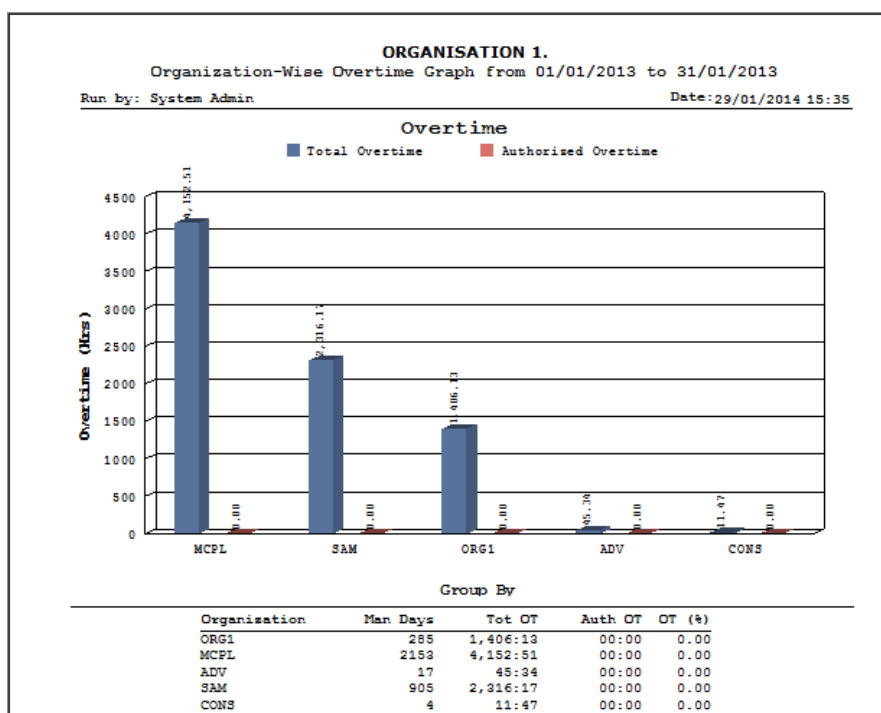
Charts

The COSEC system also provides the option of extracting certain reports in the form of *pie charts* and *bar graphs*. The following reports fall under this category:

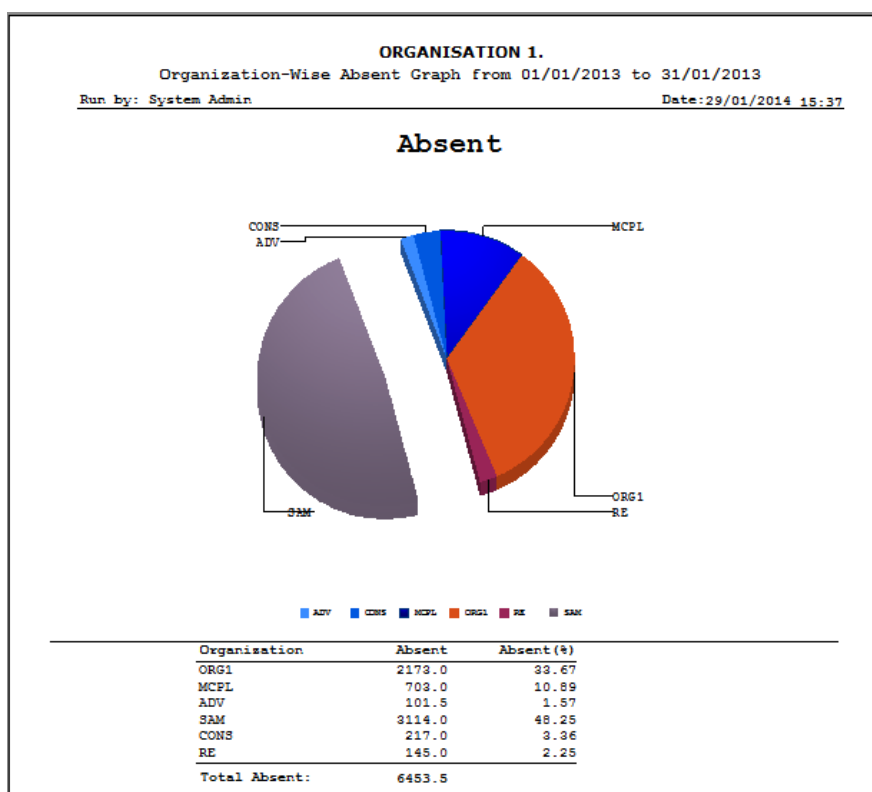
- **Time Loss** - Displays the group-wise time loss data for selected groups during the selected time period in the form of a bar graph as shown in the following figure.



- **Overtime** - Displays the group wise Overtime data for selected groups during the selected time period in a bar chart as shown.



- **Absent** - Generates a pie chart denoting the comparative department-wise absentee details for the specified period.



- **User Absent** - Generates a bar graph denoting the user wise absent count for selected users. In the event of selecting all users the top ten absentees will be shown on the bar graph while the details of other users will be displayed below the graph.
- **User Late In** - Generates a bar graph denoting the user-wise Late In occurrences for selected users. In the event of selecting all users the top ten users with the maximum number of Late In occurrences will be shown on the bar graph while the details of other users will be displayed below the graph.
- **User Early Out** - Generates a bar graph denoting the user wise Early Out occurrences for selected users. In the event of selecting all users the top ten users with the maximum number of Early Out occurrences will be shown on the bar graph while the details of other users will be displayed below the graph.
- **User Irregularity** - Generates a bar graph denoting the user wise Early Out, Late In and Absent occurrences for selected users. In the event of selecting all users the top ten users with the maximum number of the above occurrences will be shown on the bar graph while the details of other users will be displayed below the graph.
- **Monthwise Overtime** - Generates a bar graph denoting the month-wise total and authorized overtime hours for the specified months as shown in the following figure.
- **Attendance Summary** - Generates a pie chart denoting the attendance summary for the specified time period as shown.

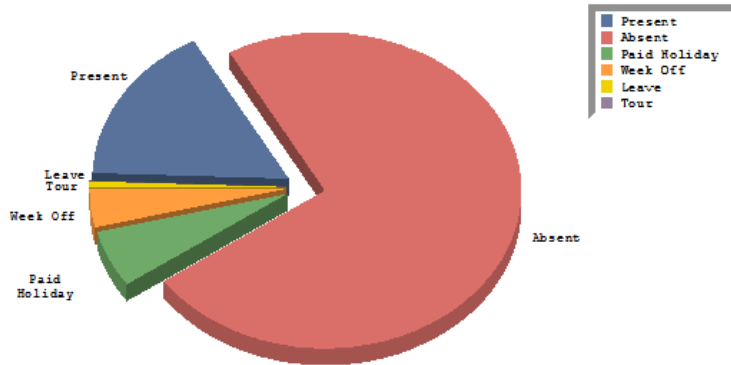
ORGANISATION 1.

Attendance Summary from 01/01/2013 To 31/01/2013 of ORG1 Organization

Run by: System Admin

Date: 29/01/2014 15:48

Attendance Summary



	Total	Percent
Man Days	2965	
Present (PR)	486.0	16.39
Absent (AB)	2173.0	73.29
Paid Holiday (PH)	175.0	5.90
Week Off (WO)	114.0	3.84
Leave (LV)	15.0	0.51
Tour (TR)	2.0	0.07

The COSEC Leave Management gives wide options for HR to create different leave types like PL, CL, SL, EL, ML, OD etc. with different parameters like balance check enable/disable, paid/unpaid leave, lay off, accumulation, minimum and maximum leaves availed at a time etc.

With the COSEC Leave Management module, you have an efficient way to:

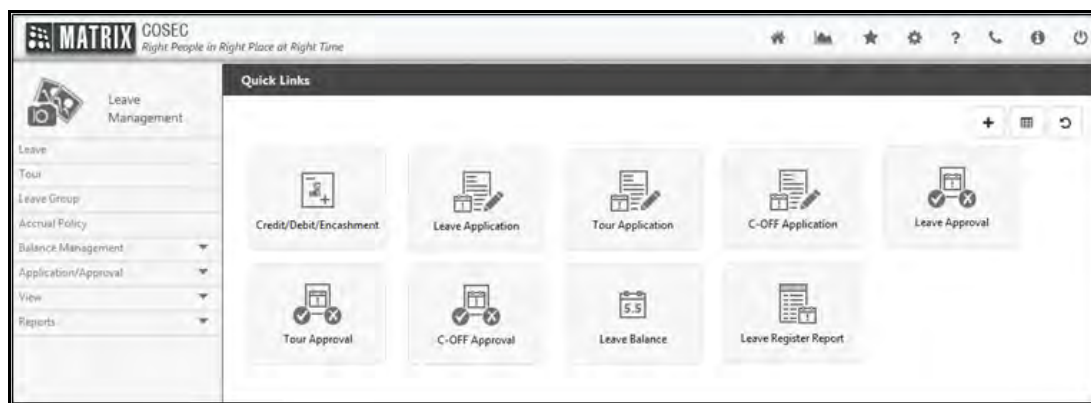
- Set up and change leave rules and policies
- Submit and record a leave request, before, during or after the leave occurs.
- Change or cancel a leave request
- Get information on leave entitlements
- Review employee leave data including leave summary.

To use this functionality, click on the **Leave Management**




module. The *Leave Management* page will



appear on your screen as shown below.

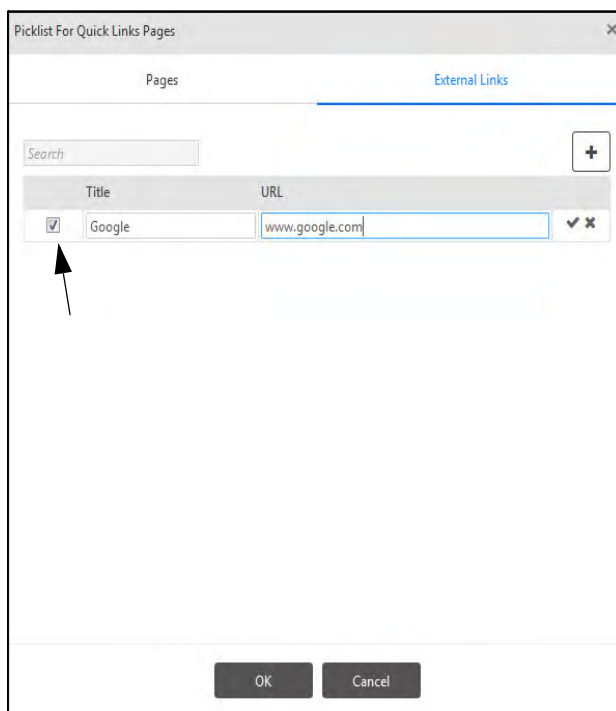



*This functionality is available only with the COSEC **Time and Attendance** module license.*

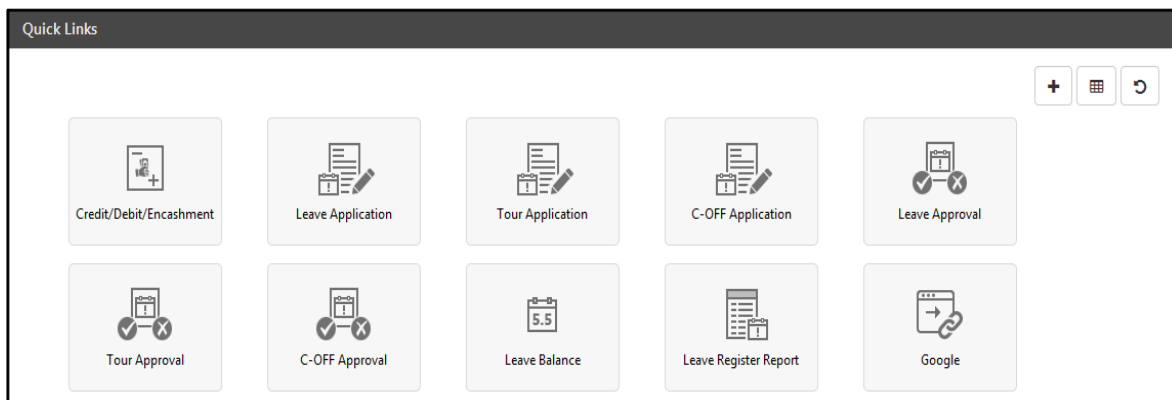
The page displays a menu and **Quick Links** to go to the required page in just one click. Quick Links are shortcuts to reach to a specific page easily. It also contains following three buttons:



- **Add Quick Link:** Click  button to add a quick link. A picklist for Quick Link pages appears for selecting the page or External Link for which the quick link is to be created. Maximum **20** quick links can be added.
- For Adding **Pages** in Quick Link, Select the Pages and click on OK

- For Adding **External Links**, Select External Link tab, click on  button to add new external link.
- Configure the **Title** and **URL** of the external link under the respective fields.click on checkbox to get the configured link on quick link screen as shown below. To save the configuration click on .



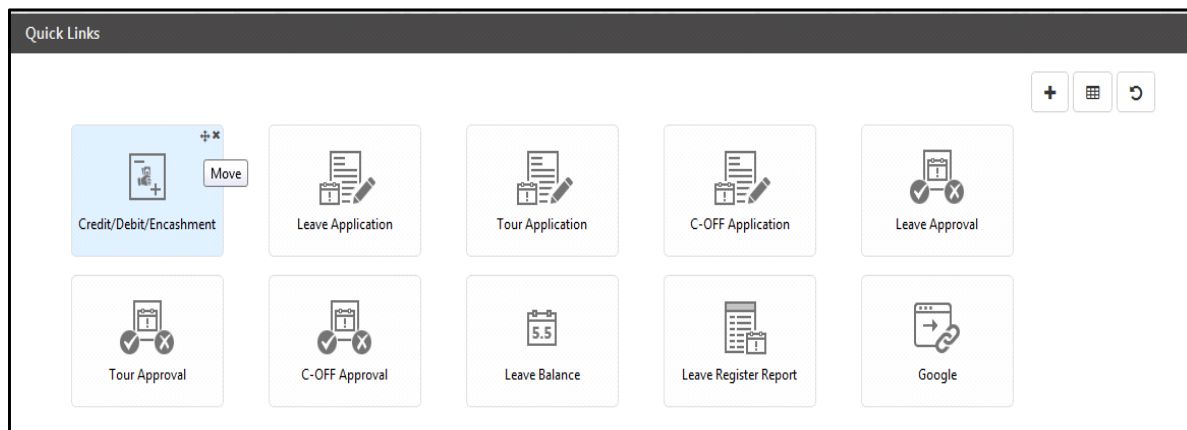
- To edit the saved configuration, click on .
- Click on OK to save the link configuration on Quick Link screen. The external link will be displayed as shown below:



- **Select Layout:** Click  button to select a layout for the quick links.You can select 5x4 or 4x5 layout to manage the quick links.
- **Reset Quick Links:** Click  button to reset the quick links to the default quick links.

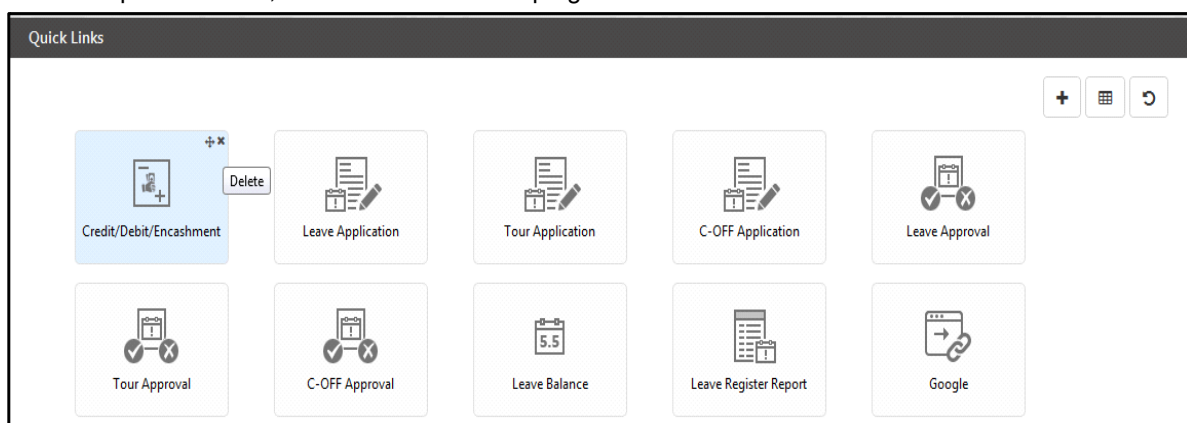
Move the Link

To move the link from one place to another, hover on the link on top right corner and click on “Move” icon as shown below. Then drag the quick link to the desired place. It will be placed at the desired location on the quick links page.




Delete the Link

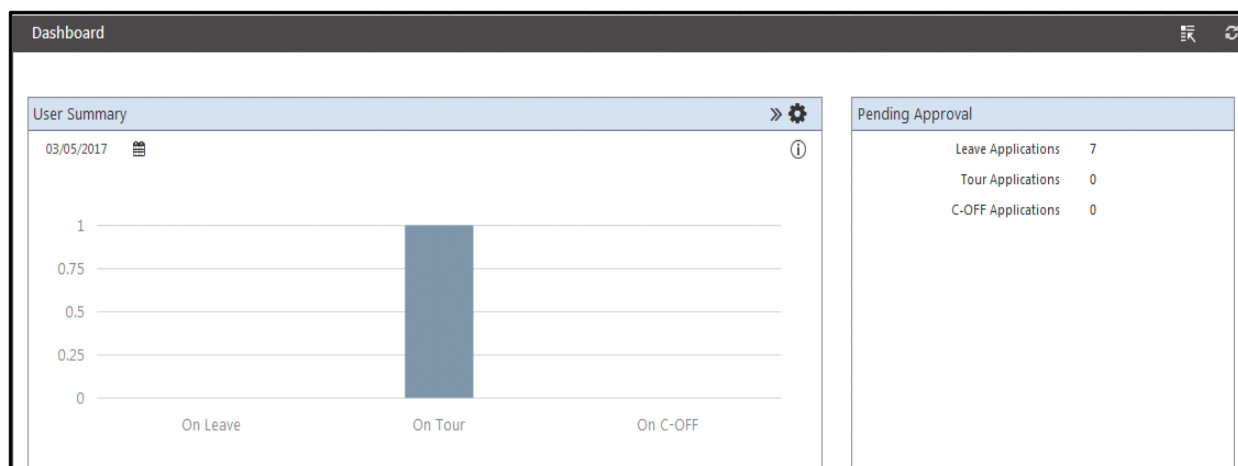
To delete a particular link, hover on the link on top right corner and click on “Delete” icon as shown below.



Quick links are displayed as per rights given to System Account and ESS users.

Leave Management Dashboard

To view the **Leave Management** Dashboard, click the Dashboard button  on the **Leave Management** page. The Dashboard displays two panels: User Summary and Pending Approval as shown below.



User Summary

User Summary panel displays a bar graph indicating the number of users on leave, on tour and on C-OFF for particular month or day as per the settings configured. Click **Settings** icon on the title bar of the panel and the following screen appears.

The screenshot shows the 'User Summary' settings dialog box. It contains three dropdown menus for configuration: 'View' (set to 'Cumulative Data'), 'Period' (set to 'Daily'), and 'User Selection' (set to 'All Users'). Below these menus are two buttons: 'View' and 'Cancel'.

Configure the following details based on which the graph is to be obtained.

- **View:** Select the view from the dropdown list to be displayed in the graph. Options are: Cumulative Data and Trending Data.
- **Period:** Select the period for which data is to be obtained as monthly or daily.
- **User Selection:** Select the users from the enterprise groups or All users based on which the data is to be obtained.

Click **View** button and the data is displayed in the form of a graph as shown below.

User Summary

Settings

View

Trending Data

Period

Monthly

Feb 2017

May 2017

User Selection

All Users

View

Cancel



Pending Approval

It displays the total number of leave applications, tour applications and C-OFF applications in pending state. This number will depend on the login user based on their rights on users/groups.



The information displayed here will consider only such group of users on whom the login user has rights.

Click on **Advanced** button to view the advanced details of leave management dashboard.

Advanced

Pending Approval

Leave Applications

0

Tour Applications

0

Dashboard

User Summary

Settings

View

Cumulative Data

Period

Daily

User Selection

All Users

View

Cancel

Pending Approval

Leave Applications

0

Tour Applications

0

C-OFF Applications

0

Leave Summary

Paid Leaves

0

Unpaid Leaves

0

On-Duty/Tour

0

C-OFF

0

Restricted Holiday

0

Lay-Off

0

Accrual Policy Summary

Total Accrual Policies

1

Configured Fixed Policy

1

Configured Calculated Policy

0

Leave Group Summary

Configured Leave Groups

1

Default Leave Group

1

Added Leaves


0

Added Tours

0

Added C-OFFs

0

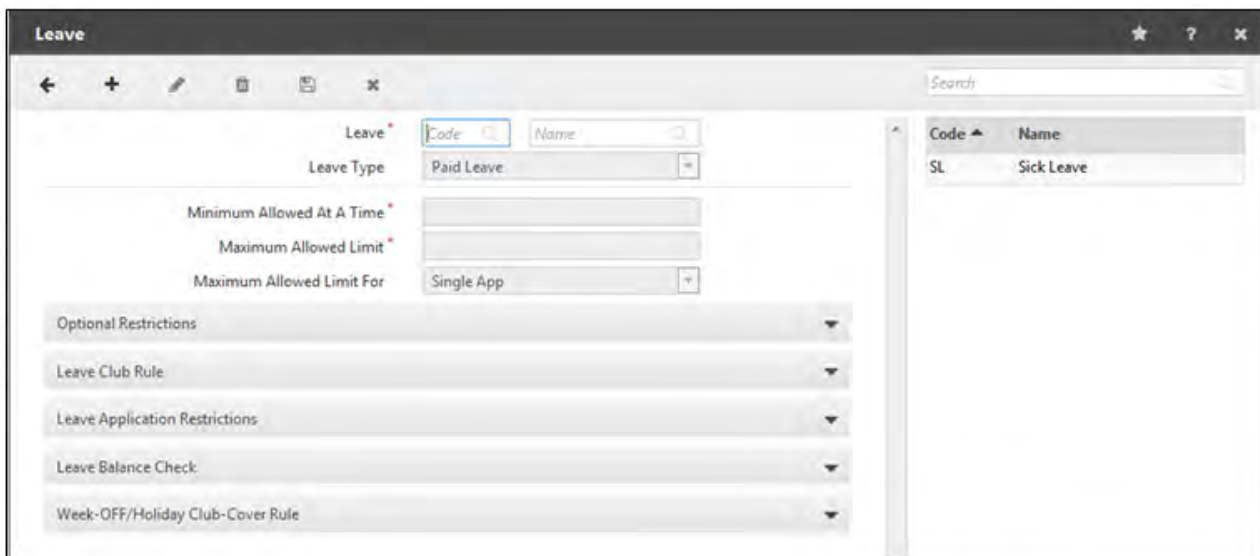
For more information on the above Dashboard options, click the respective information links on the Dashboard. The latest values on Dashboard are updated on clicking the Refresh  button.

Configuring Leaves

The COSEC Leave Management module enables the HR administrator to define multiple leaves as per the company policy. Leaves other than the commonly used leaves, can also be created and parameters for such leaves can be defined as per the organization's requirement.

Defining New Leaves

To define a new leave, go to **Leave Management > Leave** and the following page appears.



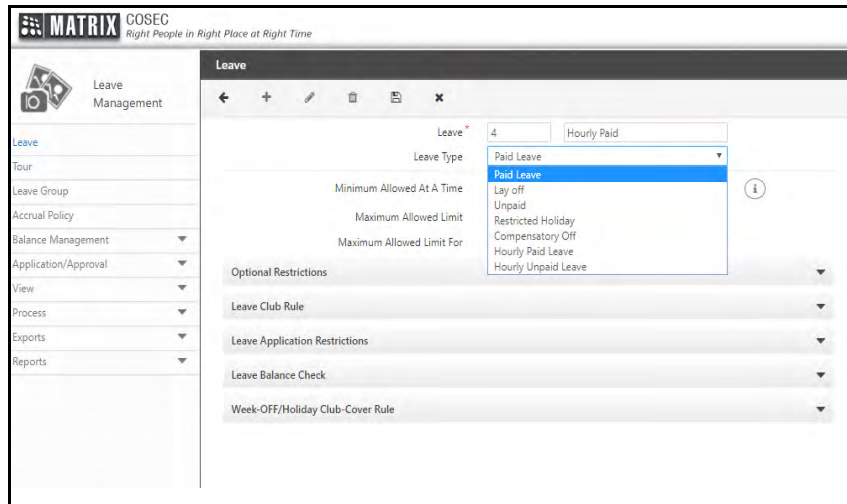
The page displays configurations on the left side and to the right is a grid containing existing created leaves.

To add a new leave, click the new button  and configure the below given parameters:

- **Leave:** Every new leave must be defined with a **Code** and a **Name**. Enter the details in the respective fields. The leave code can be of maximum 2 alphanumeric characters. For example, for the leave name "Maternity Leave", the leave code can be "ML".
- **Leave Type:** Select the type of leave or the leave category from the dropdown list to indicate whether the leave is one of the following types —
 - **Paid Leave-** This leave can be availed when the user has sufficient balance. When the user avails the paid leave, then his salary for that day is not deducted as it is managed by deducting from the total leave balance.

If you select **Paid Leave**, then configure the below parameters:

- *"Optional Restrictions"*
- *"Leave Club Rule"*
- *"Leave Application Restrictions"*
- *"Keeping Check on Leave Balance"*
- *"Week-OFF/Holiday Club-Cover Rule"*



- **Lay Off-** This leave is granted to regularize unexplained absence resulting into discontinuation of service. It is a type of unpaid leave.

If you select **Lay Off**, then configure the below parameters:

- *“Optional Restrictions”*
- *“Leave Club Rule”*
- *“Leave Application Restrictions”*
- *“Week-OFF/Holiday Club-Cover Rule”*

- **Unpaid-** This leave can be availed when the user do not have Paid leave balance. This will result in loss of pay for the day when leave is availed.

If you select **Unpaid**, then configure the below parameters:

- *“Optional Restrictions”*
- *“Leave Club Rule”*
- *“Leave Application Restrictions”*
- *“Week-OFF/Holiday Club-Cover Rule”*

- **Restricted Holiday-** This is an optional holiday which the user can avail for cultural reasons or celebrations.

If you select **Restricted Holiday**, then configure the below parameters:

- *“Optional Restrictions”*
- *“Leave Club Rule”*
- *“Leave Application Restrictions”*
- *“Keeping Check on Leave Balance”*
- *“Week-OFF/Holiday Club-Cover Rule”*

- **Compensatory Off-** This is an hourly based leave which can be availed when the user has authorized overtime hours.

If you select **Compensatory Off**, then configure the below parameters:

- *“Optional Restrictions”*
- *“Leave Club Rule”*
- *“Leave Application Restrictions”*
- *“Week-OFF/Holiday Club-Cover Rule”*

- **Hourly Leave** - This is an hourly based leave, where the user can get leave considering hours as per their requirement instead of taking *Full Day* or *Half Day* leave.

Select **Hourly Paid Leave** or **Hourly Unpaid Leave** from given drop down list.

Hourly Paid Leave will be deducted from the accumulated Leave balance whereas **Hourly Unpaid Leave** will result in salary deduction.

If you select **Hourly Leave**, then configure the below parameters:

- *“Optional Restrictions”*
- *“Leave Club Rule”*
- *“Leave Application Restrictions”*
- *“Week-OFF/Holiday Club-Cover Rule”*



*If you select the “**Hourly Unpaid Leave**” in leave type, then the option of **Leave balance Check** will be disabled.*

If you select **Leave Type** other than **Hourly Paid Leave** or **Hourly Unpaid Leave**, then configure the following parameters:

- **Minimum Allowed At a Time:** Specify the minimum number of days for which the employees can apply leave at one time.
- **Maximum Allowed Limit:** Specify the maximum number of days for which the employees can apply leave.
- **Maximum Allowed Limit For:** Select the application for which the maximum limit can be set.
- **Single App:** If this option is selected and the maximum allowed limit is configured as 2, then an employee will be able to apply for a maximum of 2 leaves at a time.
- **Consecutive Apps:** In this case, the maximum allowed limit applies not only to a single application but to all applications made consecutively for the same leave type before or after it.

E.g.: In case of this leave, an employee can apply for a total of 2 leaves inclusive of all applications for the same leave type before or after the current leave application. So if an employee applies for a “Sick Leave” from 2nd-3rd December, he will not be allowed to apply for a sick leave for 4th-5th December in this case. But if he applies leave from 5th-7th December, he will be able to do so.

However, for Single Application, a new sick leave of 2 days can be applied for, 4th-5th December.

If you select **Leave Type** as **Hourly Paid Leave** or **Hourly Unpaid Leave**, then configure below parameters:

- **Minimum Allowed Duration**

Set the minimum hours that should be used while applying for hourly leaves. (i.e., if the minimum value is set as 01:00, and the user wishes to apply hourly leave with less than 01:00 of applied duration, then the system will not allow for such leave application.)

- **Max Allowed Duration Per Application**

Set the maximum hours per application that should be used while applying for hourly leaves. (i.e., if the maximum value is set as 04:00, and the user wishes to apply hourly leave with more than 04:00 of applied duration, then the system will not allow for such leave application.)

- **Max Allowed Duration Per Day**

Set the maximum hours per day that should be used while applying for Hourly leaves.



Minimum allowed duration, maximum allowed duration per day/per application are applicable on posted duration and not on applied duration.

Click **Save** to define the new leave on the system successfully. The leave gets displayed in the grid as shown in the screen below.

Example: Hourly Leave

1. Shift Configuration (*Shifts and Schedules Module > Shift Configuration*)

Shift	9:00 - 18:00
Minimum hours required for Half Day	2 hours
Minimum hours required for Full Day	4 hours
Break (Break Deviation - Disable)	12:00 - 13:00
Grace for Shift Late IN (Overlap Grace time with Shift Late IN - Disable)	30 minutes
Include Grace in Work Hours	Enable
Late IN	60 minutes
Add Break Late IN in Total Late IN	Enable
Early OUT	60 minutes

Add Break Early OUT in Total Early OUT	Enable
--	--------

2. Hourly Leave Configuration *(Leave Management Module> Leave)*

Type	Hourly Paid Leave
Minimum Allowed Duration	00:00
Max Allowed Duration Per Application	08:00
Max Allowed Duration Per Day	12:00
Add Leave Hours into Work Hours	Enable

3. User Punches for 1st January

IN Punch	OUT Punch	IN Punch	OUT Punch
10:00	11:30	13:00	14:00

4. Hourly Leave Applied for 1st January *(Leave Management Module> Leave Application)*

Attendance Date	01/01/2021
From	02/01/2021
To	02/01/2021
Applied	03:30
Posted	03:30

5. Attendance Details *(Time and Attendance Module> Attendance Correction > Attendance Details)*

Status	PR - PR
Work Hours:	6 hours
Grace Time:	30 minutes (09:00 - 09:30)
Late IN	30 minutes (09:30 - 10:00)
Early OUT Total	60 minutes [30 minutes Shift Early OUT (17:30 - 18:00) + 30 minutes Break Early OUT (11:30 - 12:00)]

Code	Name
SL	Sick Leave

- Now, select the desired leave from the grid and click **Edit** to configure additional parameters for the leave as described in the following sections.



Once used on the system (e.g. for leave application), a leave cannot be modified or deleted. Therefore the HR administrator must configure leaves with care before they are used on the system.

Optional Restrictions

These options can be used to impose certain leave application rights and requirements on employees. To configure this, expand the Optional Restrictions panel and the following screen appears.

- Allowed Users:** Select an option specifying whether the selected leave should be applicable to all users or to either male or female users.
- Medical Certificate Required:** Select the desired option from the drop down list— None, Ensure Availability, Upload Document.

Select **None** if you do not want the applicant to submit the medical certificate.

Select **Ensure availability**, if you just want to check the documents are available with the applicant and keep the medical document upload optional.

Select **Upload Document**, if you want to make it mandatory for the applicant to upload the document.

- Min. Leave For Certificate Compulsion:** Specify a minimum period (in days) for leave application within which the applicant needs to submit the medical certificate.

Example: If 3 days are specified, then the user will be required to submit a medical certificate on taking leave for 3 or more than 3 days. And if he takes leave for 2 days then medical certificate is not required to be submitted to the company.

Leave Club Rule

The concept of **Leave Club Rule** in COSEC allows employees to use the selected leave along with other leaves configured in the system. For instance, an employee may be allowed to club a Compensatory Off with a Casual Leave in certain organizations, while others may not allow it. To define this rule, expand the **Leave Club Rule** panel as shown below.

- **Allowed With All Other Leaves:** Select the checkbox to allow the selected leave to be clubbed with any other leave pre-configured in the system.
- **Leaves Which Cannot Be Clubbed:** If some leaves are not to be allowed for clubbing with the selected leave, specify such leaves by selecting the appropriate checkboxes corresponding to each leave. Scroll up or down to view the entire list of available leaves on the system. These are the pre-created leaves.



While configuring a new Leave, if you do not wish to club this leave with other leaves, click the **Self** check box. After this Leave is saved the name assigned to this leave will be displayed instead of Self.

- **Check Clubbing Across:** Select the option for checking the leave clubbing rule across weekdays, week offs or both.

Suppose if invalid leave clubbing is detected (e.g. say, two leaves which cannot be clubbed are applied on either side of a Week-Off), user will not be able to apply for the leave.

- **Week-Offs & PH Only:** In this leave clubbing will be checked only for WO and PH.
- **Normal Days:** In this leave clubbing will be checked only for Normal days i.e. week days.
- **Both:** In this leave clubbing will be checked for both WO, PH and Week days.

Example1: Leaves Which Cannot Be Clubbed

Create a PL leave and configure the parameter “**Leaves Which Cannot Be Clubbed**” as shown in the above screen.

Now, apply one Casual Leave on 14th November either from ESS module or from Leave Management module and then apply one Paid Leave on 15th November.

On applying leave for 15th November, the system displays an error message stating “This leave should not be clubbed with CL” as shown in the screen below.

Leave Application

! This Leave should not be clubbed with CL

From Date: 05/11/2016 Full Day
To Date: 05/11/2016 Full Day
Applied Days: 1
Posted Days:
Leave: P - Paid Leave
Current Balance: 10.00

Reason And Contact Info
Reason: 30 Char
Address: 30 Char
Contact Number: 20 Char
Medical Certificate Required: ☐

Submit Cancel

Oct 2016 Dec 2016 Available Leaves: 1

32.5 days Absent 1 day Pending 0 day Approved 0 day Rejected

Attendance Details

Date	Shift	1st Half	2nd Half	First IN	Last OUT	Work Hours
09/11/2016	NS	AB	AB			
08/11/2016	NS	AB	AB			
07/11/2016	GS	AB	AB			
05/11/2016	GS	AB	AB			
04/11/2016	GS	AB	AB			
03/11/2016	GS	IN	AB	12:26		
02/11/2016	GS	AB	AB			

8 - 14 of 38 records

Thus, if you try to apply Casual Leave and Paid Leave one after another, the system will not allow to do so and displays the error message as shown in the above screen.

Example 2: Check Clubbing Across Week-Off/Holiday

Create a PL leave and configure the parameters “**Leaves Which Cannot Be Clubbed**” and select **Check Clubbing Across** as “**Week-Offs & PH only**” as shown in the below screen.

Leave Club Rule

Allowed With All Other Leaves: ☐

Leaves Which Cannot Be Clubbed: ☒ Casual Leave ☐ Head Office ☒ Paid Leave

Check Clubbing Across Week-Off/Holiday: ☒

Check Clubbing Across: Normal Days, Normal Days, **Week-offs & PH Only**, Both

5th Nov	6th Nov	7 Nov	Remarks
CL	WO	PL	CL and PL cannot be clubbed

Now, apply one Casual Leave on 5th November either from ESS module or from Leave Management module and then apply one Paid Leave on 7th November. 6th November is the Week-Off.

On applying leave for 7th November, the system displays an error message stating “This leave should not be clubbed with CL” as shown in the screen below.

Thus, if **Check Clubbing Across Week-Off & PH** option is enabled while configuring the leave and if you try to apply Casual Leave and Paid Leave one after another, the system will not allow to do so and will display an error message as shown in the above screen.

Similarly, if leaves are applied between the Public Holidays, then also the user will be restricted from applying.

Example 3: Check Clubbing across Normal days

Friday	Saturday	Sunday	Monday	Tuesday	Remarks
GS	WO	WO	GS	GS	
			SL	PL	SL and PL cannot be clubbed on normal days

The rule is configured to not allow SL & PL together so if the user has applied leave on Monday & Tuesday so while trying to approve the leaves; the leave on Tuesday will not be allowed to be approved.

Example 4: Check Clubbing for both i.e. across Normal days and WO/PH

Friday	Saturday	Sunday	Monday	Tuesday	Wednesday	Remarks
GS	WO	WO	GS	GS	GS/PH	
			SL	SL	PL	SL and PL cannot be clubbed on normal days

Normal Days include public holidays falling on weekdays.

The rule is configured to not allow SL & PL together so if the user has applied for leave on Public Holiday then the leave of Wednesday will not be allowed to be approved.

Leave Application Restrictions

Certain restrictions can be enabled for the leave application process in an organization, making it mandatory for an employee to follow some rules while applying for leaves. For e.g., hospitals and other emergency care facilities often need to arrange for substitutes beforehand, for any employee who goes on a leave. In such cases, employees may be required compulsorily to offer leave notification in advance.

To apply such restrictions, click the **Leave Application Restrictions** panel and configure the required parameters as shown below.

Leave Type = Paid Leave, Lay off, Unpaid, Restricted Holiday and Compensatory Off

The screenshot shows the 'Leave Application Restrictions' panel with the following settings:

- Application Allowed Before Leave:** ☒
- Minimum Days Before Leave Start Date:**
- Application Allowed After Leave:** ☒
- Maximum Days After Leave End Date:**
- Restrict Application Within Specified Period:** ☐
- Restriction Type:**
- Restriction Period:**

Leave Type = Hourly Paid Leave / Hourly Unpaid Leave

The screenshot shows the 'Leave Application Restrictions' panel with the following settings:

- Application Allowed Before Leave:** ☒
- Minimum Duration Before Leave Start Date:**
- Application Allowed After Leave:** ☒
- Maximum Duration After Leave End Date:**
- Restrict Application Within Specified Period:** ☐
- Restriction Type:**
- Restriction Period:**



The effect of these configurations are reflected while applying for leave from the ESS module.

Leave can be applied prior to the Leave Start Date as well as after the Leave End Date depending on the restriction applied. Leave can be applied even on the Leave Start Day.

- **Application Allowed Before Leave:** Select this checkbox to permit users to apply a leave request prior to as well as on the Leave Start Date.
- **Minimum Days Before Leave Start Date:** When the **Leave Type** is — Paid Leave, Lay off, Unpaid, Restricted Holiday and Compensatory Off, set the minimum day/s required for users to apply a leave request prior to the Leave Start Date.

When the **Leave Type** is Hourly Paid Leave or Hourly Unpaid Leave, you will be required to select desired format — Days or Hours, in which you wish to restrict a user for applying a leave.

If you select **Days**, then set the minimum day/s required for users to apply a leave request prior to the Leave Start Date.

If you select **Hours**, then set the minimum hours required for users to apply a leave request prior to the Leave Start Date/Time.

Users will be restricted to apply the leave request before / after the specified period.

If **Application Allowed Before Leave** is enabled and **Minimum Days Before Leave Start Date** is not specified then the user can apply leave before/ on the Leave Start Date.

Example 1: Minimum Days Before Leave Start Date = 2 Days

Leave Date: 19/11/2016

In this case, the User will be allowed to apply leave on 17/11/2016.

If the user tries to apply leave on 18/11/2016, he/she will be restricted and the system will display an error as shown below:

The screenshot shows the 'Leave Application' form with a red error message at the top: 'Paid Leave application allowed only 2 days before leave start...'. The 'From Date' is 18/11/2016 and 'To Date' is 18/11/2016. The 'Leave' type is 'P - Paid Leave' and 'Current Balance' is 7.50. The 'Reason' is '50 Ctr'. The 'Attendance Details' table shows the following data:

Date	Shift	1st Half	2nd Half	First IN	Last OUT	Work Hours
18/11/2016	GS	AB	AB			
17/11/2016	GS	AB	AB			
16/11/2016	GS	AB	AB			
12/11/2016	NS	AB	AB			
11/11/2016	NS	AB	AB			
10/11/2016	NS	AB	AB			
09/11/2016	NS	AB	AB			

Example 2: Minimum Days Before Leave Start Date (Leave Type = Hourly Paid/Unpaid Leave) = Format: Hours and Minimum Time: 2 Hours

Leave Date and Time: 19/11/2016 and 09.00 to 18:00

In this case, the User will be allowed to apply leave on 19/11/2016 at 07:00.

If the user tries to apply leave at 08:00, he/she will be restricted and the system will display an error.



If you set the **Minimum Days Before Leave Start Date**, then **Application Allowed After Leave** and **Max. Days After Leave End Date** will not be configurable.

- **Application Allowed After Leave:** Select this checkbox to permit users to apply a leave request after the Leave End Date.
- **Maximum Days After Leave End Date:** When the **Leave Type** is — Paid Leave, Lay off, Unpaid, Restricted Holiday and Compensatory Off — set the maximum day/s required for users to apply a leave request after the Leave End Date.

When the **Leave Type** is — Hourly Paid Leave or Hourly Unpaid Leave — you will be required to select the desired format — Days or Hours — in which you wish to restrict a user for applying a leave.

If you select **Days**, then set the maximum day/s required for users to apply a leave request after the Leave End Date.

If you select **Hours**, then set the maximum hours required for users to apply a leave request after the Leave End Date/ Time.

Users will be restricted to apply the leave request after the specified period.

Example: **Maximum Days After Leave End Date** = 1

Leave Date: 16/11/2016

In this case, the User will be allowed to apply leave on 17/11/2016.

If the user tries to apply leave on 18/11/2016, he/she will be restricted and the system will display an error.

Example 2: Maximum Days After Leave End Date (Leave Type = Hourly Paid/Unpaid Leave) =
Format: Hours and Maximum Time: 2 Hours

Leave Date and Time: 19/11/2016 and 09:00 to 18:00

In this case, the User will be allowed to apply leave on 19/11/2016 till 20:00 hour.

If the user tries to apply leave at 21:00 hour, he/she will be restricted and the system will display an error.

There are many different cases related to — **Application Allowed Before Leave, Minimum Days Before Leave Start Date, Application Allowed After Leave, Maximum Days After Leave End Date** — one may encounter while applying a leave. So to understand such scenarios, refer the following cases.

CASE 1: Consider all the possibilities for Leave types other than Hourly Leave.

A user wants to apply a leave from **20-02-2020** to **22-02-2020**.

Application Allowed Before Leave	Minimum Days Before Leave Start Date	Application Allowed After Leave	Maximum Days After Leave End Date	Valid Leave Application Date Range
Disabled	-	Disabled	-	Not Allowed
Enabled	-	Disabled	-	Till 20-02-2020
Enabled	2	Disabled	-	Till 18-02-2020

Application Allowed Before Leave	Minimum Days Before Leave Start Date	Application Allowed After Leave	Maximum Days After Leave End Date	Valid Leave Application Date Range
Disabled	-	Enabled	-	From 20-02-2020 onwards
Disabled	-	Enabled	0	From 20-02-2020 till 22-02-2020
Disabled	-	Enabled	3	From 20-02-2020 till 25-02-2020
Enabled	-	Enabled	-	All dates
Enabled	-	Enabled	0	Till 22-02-2020
Enabled	-	Enabled	3	Till 25-02-2020
Enabled	2	Enabled	3	Not Possible

CASE 2: Consider all the possibilities for Leave types — Hourly Paid Leave and Hourly Unpaid Leave.

A user wants to apply a leave on **20-02-2020** from **14:00 to 18:00 hours**.

Application Allowed Before Leave	Minimum Days Before Leave Start Date Format = Hours	Application Allowed After Leave	Maximum Days After Leave End Date Format = Hours	Valid Leave Application Date Range
Disabled	-	Disabled	-	Not Allowed
Enabled	-	Disabled	-	Till 20-02-2020 14:00 hours
Enabled	05:00	Disabled	-	Till 20-02-2020 09:00 hours
Disabled	-	Enabled	-	From 20-02-2020 14:00 hours onwards
Disabled	-	Enabled	03:00	From 20-02-2020 14:00 hours to 21:00 hours
Enabled	-	Enabled	-	All dates
Enabled	-	Enabled	03:00	Till 20-02-2020 21:00 hours
Enabled	02:00	Enabled	03:00	Not Possible

CASE 3: Consider all the possibilities for Leave types — Hourly Paid Leave and Hourly Unpaid Leave.

A user wants to apply a leave on **20-02-2020** from **14:00 to 18:00 hours**.

Application Allowed Before Leave	Minimum Days Before Leave Start Date Format = Days	Application Allowed After Leave	Maximum Days After Leave End Date Format = Days	Valid Leave Application Date Range
Disabled	-	Disabled	-	Not Allowed
Enabled	-	Disabled	-	Till 20-02-2020
Enabled	2	Disabled	-	Till 18-02-2020
Disabled	-	Enabled	-	From 20-02-2020 onwards
Disabled	-	Enabled	0	From 20-02-2020 to 21-02-2020
Disabled	-	Enabled	3	From 20-02-2020 to 24-02-2020
Enabled	-	Enabled	-	All days allowed
Enabled	-	Enabled	0	Till 21-02-2020
Enabled	-	Enabled	3	Till 24-02-2020
Enabled	2	Enabled	3	Not Possible

CASE 4: Consider all the possibilities for Leave types — Hourly Paid Leave and Hourly Unpaid Leave.

A user wants to apply a leave from **20-02-2020, 20:00 hours** to **21-02-2020, 04:00 hours**.

Application Allowed Before Leave	Minimum Days Before Leave Start Date Format = Hours	Application Allowed After Leave	Maximum Days After Leave End Date Format = Days	Valid Leave Application Date Range
Disabled	-	Disabled	-	Not Allowed
Enabled	-	Disabled	-	Till 20-02-2020 20:00 hours
Enabled	05:00	Disabled	-	Till 20-02-2020 15:00 hours
Disabled	-	Enabled	-	From 20-02-2020 onwards
Disabled	-	Enabled	-	20-02-2020 to 21-02-2020
Disabled	-	Enabled	3	20-02-2020 to 24-02-2020
Enabled	-	Enabled	-	All days at any time
Enabled	-	Enabled	0	Till 21-02-2020
Enabled	-	Enabled	3	Till 24-02-2020
Enabled	02:00	Enabled	3	Not Possible

CASE 5: Consider all the possibilities for Leave types — Hourly Paid Leave and Hourly Unpaid Leave.

A user wants to apply a leave from **20-02-2020, 20:00 hours** to **21-02-2020, 04:00 hours**.

Application Allowed Before Leave	Minimum Days Before Leave Start Date Format = Days	Application Allowed After Leave	Maximum Days After Leave End Date Format = Hours	Valid Leave Application Date Range
Disabled	-	Disabled	-	Not Allowed
Enabled	-	Disabled	-	Till 20-02-2020
Enabled	2	Disabled	-	Till 18-02-2020
Disabled	-	Enabled	-	From 20-02-2020 20:00 hours onwards
Disabled	-	Enabled	05:00	From 20-02-2020 20:00 hours to 21-02-2020 09:00 hours
Enabled	-	Enabled	-	All days at any time
Enabled	-	Enabled	05:00	Till 21-02-2020 09:00 hours
Enabled	02:00	Enabled	03:00	Not Possible

- **Restrict Application Within Specified Period:** Enable the checkbox to impose a restriction on leave application for a specific period. This is usually used in certain organizations where employees are restricted from taking paid leaves during their probationary period.
- **Restriction Type:** Select the type of restriction till which an employee cannot apply for leave. The restriction type can be till the employee's Confirmation Date or for a specific duration (**Restriction Period**) starting from the employee's Joining Date.

For this restriction to work, care must be taken to save user's joining and confirmation dates in COSEC before any leaves are applied. Also, any auto-attendance correction or attendance regularization using leaves for dates that fall within the Restriction Period will be overruled.

Example: Consider The restriction type as "Joining Date" and specify the Restriction Period as "month" and number of months as "6" for "PL" leave type. Current month is "November".

Now, if a user Rosy has joined in the month of July and she tries to apply for leave, then she will not be allowed for the restricted period.

Keeping Check on Leave Balance

This option allows the HR administrator to keep a check on the leave balance of any user configured in COSEC. To do this, expand the **Leave Balance Check** panel as shown below.

The screenshot shows the 'Leave Balance Check' configuration panel. It contains several sections with checkboxes and input fields:

- Enable Balance Check:** A checkbox that is checked.
- Maximum Limit In Attendance Period:** A section with an 'Enable' checkbox (unchecked) and a 'Maximum Limit' input field.
- Carry Forward To Next Year:** A section with an 'Enable' checkbox (unchecked) and a 'Maximum Carry Forward Limit Check' input field.
- Balance Mgmt. From Other Leave:** A section with an 'Enable' checkbox (checked), a 'Balance To Be Managed From' dropdown menu set to 'Casual Leave', and a 'Multiplication Factor For Deduction' input field set to '1'.
- Leave Encashment:** A section with an 'Enable' checkbox (unchecked) and a 'Min. Balance Check After Encashment' input field.
- Maximum Accumulation Check:** A section with an 'Enable' checkbox (unchecked) and a 'Maximum Accumulation Check' input field set to '0.00'.

- **Enable Balance Check:** Select the checkbox to enable users to check their leave balance. If disabled for a particular leave then users cannot credit/debit/encash leaves to this type of leave. But when the user will apply for leave from the ESS module it will act as unpaid leave. But it is recommended that this option is enabled so that the user can use other facilities of leaves.

Maximum Limit in Attendance Period

Select the checkbox to maintain an upper limit restriction for leaves applied in Attendance Period. Specify the maximum allowed leave limit in attendance period for the specific leave type.

Example: Suppose the maximum limit in Attendance Period is 4 for Casual Leave type. Then user will be allowed to apply leave for 4 days only. Now, if user tries to apply leave for more than 4 days in a month then he will not be allowed to apply for any more casual leave in that particular month and will receive an error message on the screen as shown below.

Carry Forward To Next Year

- **Enable:** Select the checkbox to enable the unused leave balance to be carried over to the next year.
- **Maximum Carry Forward Limit Check:** Select the checkbox to put a restriction on the number of leaves to be carry forwarded to the next year. Specify the maximum number of leaves in the textbox that can be carried forward to the next year. E.g. If for one year the leave balance is 40 leaves and the maximum leave to be carry forwarded is 10, then only 10 leaves will be carry forwarded to the next year. While the remaining 30 leaves will get lapsed.

Balance Mgmt. From Other Leave

- **Enable:** Select the checkbox, if the balance of another leave defined on the system is to be managed from the currently selected leave.

- **Balance To Be Managed From:** Select the leave from the dropdown list to be managed from the leave being configured.
- **Multiplication Factor For Deduction:** Enter a value for this balance management. E.g. If the value specified is 1 for Casual Leave, then 1 leave of Privilege Leave will be given to the Casual leave when the Casual Leave balance becomes 0 and still Casual Leave is applied.

Example: Balance to be Managed From is selected as “Casual Leave” and the multiplication factor is specified as “1” for Privilege type of leave.

Leave Application Scenario

Suppose the Availed Balance of Casual Leave is 2 days in the Leave Balance page as shown in the screen below.

Year	Month	Code	Name	Opening	Credit	Debit	Encashment	Availed	Closing	Overflow
2016	Dec	CL	Casual Leave	0.00	10.00	0.00	0.00	2.00	8.00	0.00
2016	Dec	PL	Privilege	0.00					0.00	0.00
2016	Dec	SL	Sick Leave	0.00					0.00	0.00

Now apply one Privilege leave.

From	To	Leave	Application Date	Application Type	Status
15/12/2016	15/12/2016	PL	19/12/2016	New	✓
12/12/2016	13/12/2016	CL	19/12/2016	New	✓

Once the leave gets applied, check the balance from the Leave Balance page.

Year	Month	Code	Name	Opening	Credit	Debit	Encashment	Available	Closing	Overflow
2016	Nov	CL	Casual Leave	0.00	20.00	0.00	0.00	3.0	17.00	0.00
2016	Nov	PL	Privilege Leave	0.00				0.0	0.00	0.00
2016	Nov	SL	Sick Leave	0.00	10.00	0.00	0.00	0.0	10.00	0.00

The Available balance of Casual Leave becomes 3 and Privilege Leave is still 0. This is because the Privilege Leave balance is managed from Casual Leave balance. Hence, any leave applied, credited, debited or encashed will be deducted from Casual Leave only and not from the Privilege Leave.

Credit Scenario

Now if 3 leaves are credited for Privilege Leave from **Balance Management > Credit/Debit/Encashment** page, then the balance of 3 leaves will be credited to Casual Leave. The number of leaves credited to Privilege Leave can be viewed from the **Leave Balance** page.

Debit Scenario

If 3 leaves are debited for Privilege Leave from **Balance Management > Credit/Debit/Encashment** page, then the balance of 3 leaves will be debited from Casual Leave and not the Privilege Leave. The number of leaves debited from Privilege Leave can be viewed from the **Leave Balance** page.

Encashment Scenario

If 3 leaves are encashed for Privilege Leave from **Balance Management > Credit/Debit/Encashment** page, then the balance of 3 leaves encashed will be deducted from the Casual Leave only. The number of leaves encashed for Privilege Leave can be viewed from the **Leave Balance** page. For encashment the Leave Encashment checkbox should be enabled.

Leave Encashment

- **Enable:** Select the checkbox to make the selected leave available for encashment.
- **Min. Balance Check After Encashment:** Select the checkbox to define whether the system should maintain a certain balance before allowing encashment. If enabled, enter the minimum required leave balance for allowing encashment.

Example: If 2 is specified and out of total 5 leaves; 4 leaves are applied for encashment, then the user will not be allowed as minimum 2 leaves are required to be left in the leave balance after encashment.

Maximum Accumulation Check

- **Enable:** Select the checkbox and enter a value for Maximum Accumulation Check to enable restriction on maximum leave balance accumulation for a year. In case a leave credit is made that causes the leave balance to exceed the specified Maximum Accumulation limit, only a partial credit will be allowed.

Example: Say, a user's leave balance is 48 and Maximum Accumulation limit is of 50 leaves, then a maximum leave credit of 2 leaves shall be allowed.

Week-Off/Holiday Club-Cover Rule

This is a conditional rule that enables the administrator to determine whether a Week-Off/Holiday that lies in continuity with a leave (either before, after or on both sides of Week-Off/Holiday), should be allowed. If this is not allowed, then the Week-Off/Holiday will be clubbed/covered by the system as a leave.

To apply this rule, expand the **Week-Off/Holiday Club-Cover Rule** panel as shown below.

The screenshot shows a configuration panel titled "Week-Off/Holiday Club-Cover Rule". It is divided into two sections: "Week-Off Club/Cover Rule" and "Holiday Club/Cover Rule".

Week-Off Club/Cover Rule

- Allowed On Single Sided Leave: ☒
- Allowed On Both Sided Leave: ☒
- Atleast Full Day Leave For Club-Cover: ☐
- Enable Minimum Limit Check: ☒
- Minimum Limit Around Week-Off *:

Holiday Club/Cover Rule

- Allowed On Single Sided Leave: ☒
- Allowed On Both Sided Leave: ☒
- Atleast Full Day Leave For Club-Cover: ☐
- Enable Minimum Limit Check: ☐
- Minimum Limit Around Holiday:

Select the appropriate checkboxes to apply Week-Off/Holiday club and cover rule for the following conditions:

Week-Off Club/Cover Rule

- **Allowed on Single Sided Leave:** Leave is allowed only if the user is on leave on any one side of the Week-Off. Single side can be second half of previous day or first half of next day or either of the full day.

E.g. If Week Off is on 6th November (Sunday) and Leave is applied for 5th November (Saturday) then user will be allowed to apply. But if the user applies for leave on 7th November (Monday) also then he will not be allowed to apply and an error message will be displayed on the screen.
- **Allowed on Both Sided Leave:** Leave is allowed only if the user is on leave on both sides of a Week-Off. The both sides can be second half of previous day or first half of the next day or full day on both the sides of Week-Off. In this case single sided leave will not be considered. i.e. If leave is applied for 5th November only and Week Off is on 6th November, then user will not be allowed. He will have to apply for leave on 7th November also.
- **Atleast Full Day Leave For Club-Cover** - Applies club-cover rule for the following scenarios:
 - When **Allowed on Single Sided Leave** is also checked, Week-Off will be allowed only if the user is on a *full day leave* on any one side of a Week-Off.

- When **Allowed on Both Sided Leave** is also checked, Week-Off will be allowed only if the user is on a *full day leave* on both sides of a Week-Off.
- **Enable Minimum Limit Check** - Select this checkbox to enable a check on the minimum number of leaves that can be availed on both sides of a Week-Off.
- **Minimum limit around Week-Off**: Specify the minimum number of leaves that can be applied around the week-off. This check will be applicable only for similar leave types on both sides of a Week-Off.

Example: Consider Minimum Limit Around Week-Off as “3” as shown in the screen below.

Now apply Casual Leave from 4th November to 8th November as shown in the screen below.

From	To	Leave	Application Date	Application Type	Status
18/11/2016	18/11/2016	11	17/11/2016	New	✓
21/10/2016	21/10/2016	P1	17/11/2016	New	✓

The user will not be allowed to apply leave and an error message will be displayed as shown in the screen above.

This is because only “3” leaves can be applied around the week-off and in the above example leave is applied for “4” days.

Thus, the user will not be allowed to apply leave more than the number configured in the parameter “Minimum Limit Around Week-Off”.

Holiday Club/Cover Rule



The Holiday Club/Cover Rule will work similar to the Week-Off Club/Cover rule. Hence, for examples and better understanding of parameters See “Week-Off Club/Cover Rule” on page 1716.

- **Allowed on Single Sided Leave** - Holiday is allowed only if the user is on leave on any one side of the Holiday. Single side can be second half of previous day or first half of next day or either of the full day.
- **Allowed on Both Sided Leave** - Holiday is allowed only if the user is on leave on both sides of a Holiday. The both sides can be second half of previous day or first half of the next day or full day on both the sides of holiday.
- **Atleast Full Day Leave For Club-Cover** - Applies club-cover rule for the following scenarios:
 - When **Allowed on Single Sided Leave** is also checked, Holiday will be allowed only if the user is on a *full day leave* on any one side of a Holiday.
 - When **Allowed on Both Sided Leave** is also checked, Holiday will be allowed only if the user is on a *full day leave* on both sides of a Holiday.
- **Enable Minimum Limit Check** - Select this checkbox to enable a check on the minimum number of leaves that can be availed on both sides of a Public Holiday.
- **Minimum limit around Holiday**: Specify the minimum number of leaves that can be applied around the holiday. This check will be applicable only for similar leave types on both sides of a Holiday.

Once all the parameters get configured, click **Save** button and the created leave gets displayed in the grid as shown in the screen below.

Code	Name
11	1234
C1	C-OFF1
C2	C-OFF2
C3	C-OFF3
CF	C-OFF
CL	Casual Leave
P	Paid Leave
P1	Primary Leave
PL	Privelege Leave
SL	Sick Leave

You can also delete the created leave by selecting the leave from the grid and clicking **Delete** button.

Tours

A tour is an official trip undertaken by an employee for work-related purposes. Many organizations follow a formal procedure for tour application and approval. This procedure may vary depending upon organizational norms and practices. For example, some establishments may allow employees to club tours with other leaves, while others may not.

The *Leave Management* module supports creation of customized tour types alongside a flexible option to generate tour applications and tour authorization by the concerned personnel. This section will describe the process of tour configuration, application and approval as performed using the *Leave Management* module.



*Tour Application and Approval can be performed both using the **Leave Management** module by system-account users with appropriate page rights, as well as using the **Employee Self Service** module by employees and their respective reporting in-charges. For more information on tour application/approval via ESS, please refer to the respective user documentation.*

Defining New Tours

To define a new tour, go to **Leave Management** module > **Tour** and the following page appears.

The screenshot shows the 'Tour' configuration page. On the left, there are fields for 'Tour' (with a dropdown showing 'HO' and 'Head Office'), 'Tour Type' (with a dropdown showing 'Tour / ON Duty'), 'Minimum Allowed At A Time' (with a value of 1.0), 'Maximum Allowed Limit' (with a value of 5.0), and 'Maximum Allowed Limit For' (with a dropdown showing 'Single App'). Below these are expandable sections for 'Optional Restrictions', 'Tour Club Rule', 'Tour Application Restrictions', and 'Week-Off/Holiday Club-Cover Rule'. On the right, there is a search bar and a table with two columns: 'Code' and 'Name'. The table contains two rows: 'HO' with 'Head Office' and 'US' with 'USA'.

Code	Name
HO	Head Office
US	USA

The page displays configurations on the left side and a grid containing existing tours on the right hand side.



Tours and Leaves on COSEC have a similar configuration. To know more about configuring for leaves, refer to [“Defining New Leaves”](#).

- **Tour:** Every new tour must be defined with a **Code** and a **Name**. Enter the details in the respective fields. The tour Code can be of maximum 2 alphanumeric characters. For example, for the tour name “Head Office”, the leave code has been assigned as “HO”.
- **Tour Type:** Select the tour type as **Tour/ON Duty**.
- **Minimum Allowed At A Time:** Specify the minimum number of tours in days which will be allowed to employees at a time.
- **Maximum Allowed Limit:** Specify the maximum number of tours in days which will be allowed to employees at a time.

- **Maximum Allowed Limit For:** The maximum allowed limit can be set for:
 - **Single App** - Here the maximum allowed limit is applicable only to a single tour application. Hence when, the Maximum Allowed Limit for a Single Application is 5, then an employee will be able to apply for a maximum of 5 days of tour at a time.
 - **Consecutive Apps** - Here the maximum allowed limit applies not only to a single application but to all applications for the same tour made consecutively before or after it.

Optional Restrictions

This options can be used to impose certain tour application rights and requirements on employees. To configure this, expand the **Optional Restrictions** panel as shown below.

Optional Restrictions	
Allowed Users	All
Tour Document Required	Upload Document
Min. Tour Days For Document Compulsion	15.0

- **Allowed Users:** Select an option from the dropdown list to specify whether the tour should be applicable to all users or only to either male or female users.
- **Tour Document Required:** Select the desired option from the drop down list— None, Ensure Availability, Upload Document.

Select **None** if you do not want the applicant to submit the tour document.

Select **Ensure availability**, if you just want to check the documents are available with the applicant and keep the tour document upload optional.

Select **Upload Document**, if you want to make it mandatory for the applicant to upload the document.

- **Min. Tour Days for Document Compulsion:** Specify a minimum period (in days) for Tour application within which the applicant needs to submit the tour document.

Example: If 2 days are configured as **Min. Tour Days for Document Compulsion**, then user will be required to submit document on tour within 2 or more days

Tour Club Rule

The concept of **Tour Club Rule** in COSEC allows employees to use the selected tour along with other leaves configured in the system. To define this rule, expand the **Tour Club Rule** tab as shown below.

- **Allowed With All Other Tour:** Select the checkbox to allow the selected tour to be clubbed with any other leave pre-configured in the system.
- **Tours Which Cannot Be Clubbed:** If all leaves are not to be allowed for clubbing with the selected tour, specify such leaves by selecting the appropriate checkboxes corresponding to each leave. Scroll up or down to view the entire list of available leaves on the system.
- **Check Clubbing Across:** Select the option for checking the tour clubbing rule across weekdays, week offs or both.
Suppose if invalid tour clubbing is detected (e.g. say, two leaves which cannot be clubbed are applied on either side of a Week-Off), user will not be able to apply for the leave.
 - **Week-Offs & PH Only:** In this tour clubbing will be checked only for WO and PH.
 - **Normal Days:** In this tour clubbing will be checked only for Normal days i.e. week days.
 - **Both:** In this tour clubbing will be checked for both WO, PH and Week days.

Tour Application Restrictions

Certain restrictions can also be enabled for the tour application process in an organization, making it mandatory for an employee to follow some rules when applying for tours. To apply such restrictions, expand the **Tour Application Restrictions** panel as shown below.

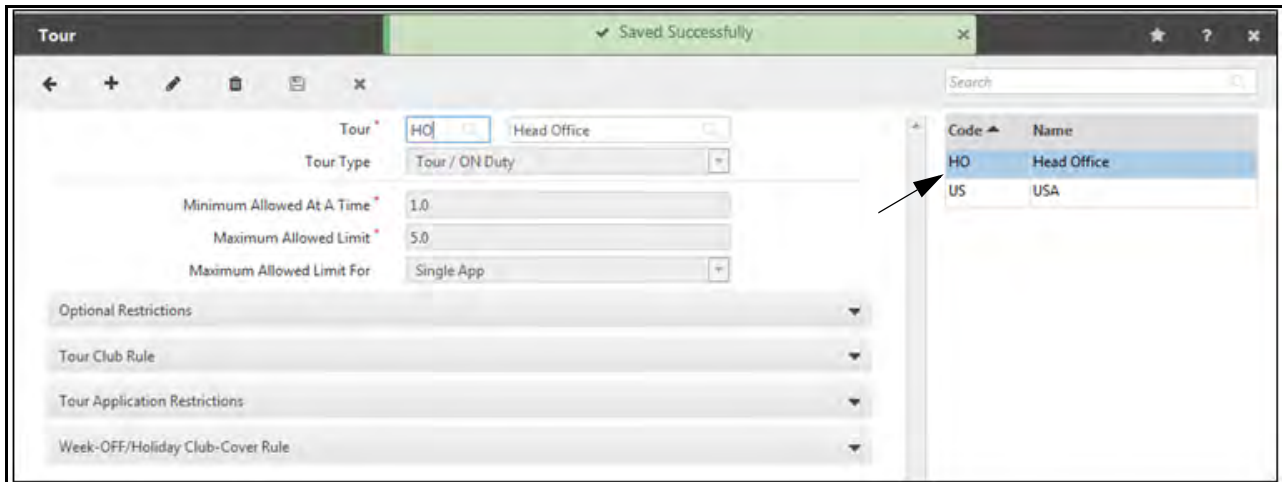
- **Application Allowed Before Tour:** Select this option for allowing employees to apply before going on tour. By default it is in enabled state.
- **Min. Days Before Tour Start Date:** Specify the minimum number of days from the tour start date, after which application for the tour taken will not be allowed any more.
- **Application Allowed After Tour:** Select this option for allowing employees to apply after going on tour. By default it is in enabled state.

- **Max. Days After Tour End Date:** Specify the maximum number of days after the tour ends, after which application for the tour taken won't be allowed any more.

Week-OFF/Holiday Club-Cover Rule

To configure this option for tours, refer to [“Week-OFF/Holiday Club-Cover Rule”](#) for leave configuration.

Once all the parameters get configured, click **Save** button and the created tour gets displayed in the grid as shown in the screen below.



The screenshot shows a software window titled "Tour" with a green status bar at the top indicating "Saved Successfully". The window contains a form for configuring a tour and a table on the right.

Tour Configuration Form:

- Tour:** HO (selected from a dropdown)
- Head Office:** (empty text field)
- Tour Type:** Tour / ON Duty (selected from a dropdown)
- Minimum Allowed At A Time:** 1.0
- Maximum Allowed Limit:** 5.0
- Maximum Allowed Limit For:** Single App (selected from a dropdown)
- Optional Restrictions:** (collapsed section)
- Tour Club Rule:** (collapsed section)
- Tour Application Restrictions:** (collapsed section)
- Week-OFF/Holiday Club-Cover Rule:** (collapsed section)

Tour Grid:

Code	Name
HO	Head Office
US	USA

An arrow points from the "HO" entry in the grid to the "Tour" dropdown in the form.

You can also delete the created tour by selecting the tour from the grid and clicking **Delete** button.



Tour cannot be deleted if it is being used in the system or assigned to a user.

Leave Group

This option enables the user to club multiple leaves into groups to assign them to users. The COSEC system has a capacity to create unlimited leave groups with different IDs and leaves as member of the groups.

To create a new leave group, go to **Leave Management module > Leave Group** and the following screen appears.

Leave Group

Leave Group ID: Leave Group2

Default ☒

Enable Pro-rata ☒

Leave Rounding Parameters

Enable Leave Rounding ☐

Credit Leave in Multiples Of: 0

Rounding Limit: Lower

Group Members

Leave ID: Name:

Auto	Adjustment	Priority	Code	Name	Leave Type	Up/Down	
------	------------	----------	------	------	------------	---------	--

ID	Name
1	Leave Group-1

Leave Group: Enter a **Name** for the new leave group. The ID will be generated by the system while saving the group.

Default: Select the Default checkbox to make the leave group as default.

Enable Pro-rata: Select the checkbox to enable leave credit on pro-rata basis (i.e. on the basis of the actual number of days worked by an employee). This shall be applicable to all leaves added in the new leave group.

Eg: The user has joined a company on 21st of month. You are crediting 10 leaves but actually 3.5 leaves will be credited to the user on Pro-rata basis.



"The users who are expected to get credited leaves using pro-rata should be assigned a Leave group where "Enable Pro-rata" flag is set.

"Apply Pro-rata" flag should also be checked at "Credit/Debit/Encashment" page to apply pro-rata for the selected users.

Leave Rounding Parameters

- **Enable Leave Rounding:** If “Enable Pro-rata” is checked, then you can enable leave rounding. This will allow the leaves to be credited in multiples of value as entered in "Credit Leave in Multiples Of" field.
- **Credit Leave in Multiples of:** You can enter a value, in whose multiples, the leave will be credited. The Valid values are 0.00 to 1.00.
- **Rounding Limit:** Select the rounding limit as Lower or Upper.
If "Lower" is selected, credited leave should be rounded to largest multiple of value entered at "Credit Leave in Multiples Of" textbox which is less than the actual leave value calculated as per Pro-rata.

If "Upper" is selected, credited leave should be rounded to smallest multiple of value entered at "Credit Leave in Multiples Of" textbox which is greater than the current leave value calculated as per Pro-rata.

Example: Pro-rata with rounding

Suppose

“Joining Date of selected User = 21/06/2016

"Credit Leave for June, 2016 = 1.75. [for whole month]

"Credit Leaves in Multiples of = 0.25

"Thus, according to pro-rata calculation, the credited leave =

$(\text{No. of leaves to be credited in month} / \text{No. of days in month}) * [(\text{No. of days in month} - \text{Date of joining}) + 1] = [(1.75/30)*(30-21+1)] = 0.58$

0.58 will be rounded off to lower limit as 0.5 days or Upper limit as 0.75 days as described in table:

Rounding Limit	Selection of value as per rounding limit and comparison with credited leave	
Lower	select a value in multiples of 0.25 such that it is the greatest value in multiples of 0.25 which is less than the current leave value calculated as per pro-rata feature.	The leave amount credited for selected user for June, 2016 is 0.5 days.

Rounding Limit	Selection of value as per rounding limit and comparison with credited leave	
Upper	select a value in multiples of 0.25 such that it is the smallest value in multiples of 0.25 which is greater than the current leave value calculated as per pro-rata feature.	The leave amount credited for selected user for June, 2016 is 0.75 days.

Group Members

This section enables to add leaves to the leave group.

- **Leave:** Select leaves to be included in the leave group using the picklist. These leaves are created from the Leave page. The selected leaves are displayed in the grid as shown below.

The current leaves in the leave group are displayed as follows:

The user can use the **Up/Down** arrow buttons to arrange these leaves in the group to define the priority in which the leaves will be used to cover any absence in attendance. By default, priority will be defined by the order in which the leaves are added to the leave group.

Also, each leave added in the group has a **Auto Adjustment** check box, which will determine whether it is to be considered for auto-adjustment.

Read T&A > Attendance Policy > Auto Attendance Correction > Auto Adjustment with Leave

Click on **Delete** button to remove an added leave from the grid.

Click **Save** button to save the configured leave group.

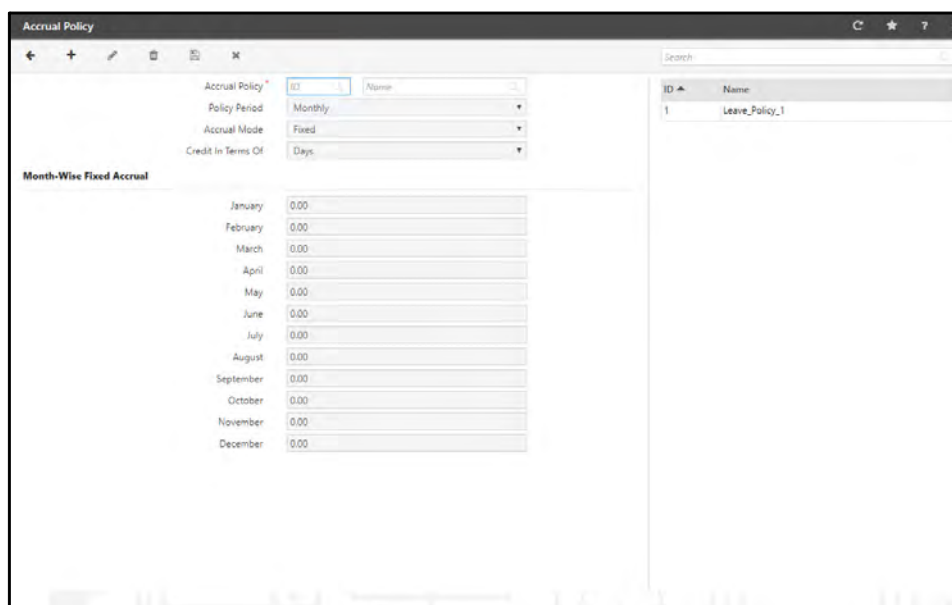


The Leave Group must be then assigned to the user from **User** module > **User Configuration** > **Group** page so that he can use the leaves available in the leave group, provided he has sufficient leave balance.

Accrual Policy

Many organizations prefer the concept of providing leaves to their employees in the form of accruals i.e. advance credit of paid leave balance which can be used over a definite period of time. This leave balance is credited to employees as per the accrual policy of the organization. The Accrual Policy feature in COSEC enables the HR administrator to set parameters for crediting leaves to an employee based on predefined rules. The user can configure a set of rules and group them together in policies.

To define an Accrual Policy, go to **Leave Management module > Accrual Policy** and the following screen appears.



Month	Value
January	0.00
February	0.00
March	0.00
April	0.00
May	0.00
June	0.00
July	0.00
August	0.00
September	0.00
October	0.00
November	0.00
December	0.00

ID	Name
1	Leave_Policy_1

The page displays configurations on the left side and a grid on the right hand side containing created accrual policies.

To add a new accrual policy click the New button and provide the following parameters:

- **Accrual Policy:** Every new leave policy is automatically assigned a system-generated **ID**. Enter a suitable **Name** for the new policy.
- **Policy Period:** Select the policy period for monthly or yearly accrual of leaves.



An organization should always operate either on Yearly period or Monthly period approach completely for leave management. Using a mixed period approach must be avoided to prevent data mismatch.

- **Accrual Mode:** Select the mode which determines how leaves are to be credited to users on whom this Accrual Policy applies. This will depend on the Policy Period selected. Specify the Accrual Mode as one of the following:

- **Fixed** - For Monthly accrual, this mode enables the user to define the number of leaves to be credited for each month of the year as shown in the following figure:

The screenshot shows the 'Accrual Policy' window with the following settings:

- Accrual Policy:
- Policy Period: Monthly
- Accrual Mode: Fixed
- Credit In Terms Of: Days

Month-Wise Fixed Accrual

Month	Credit Days
January	0.00
February	0.00
March	0.00
April	0.00
May	0.00
June	0.00
July	0.00
August	0.00
September	0.00
October	0.00
November	0.00
December	0.00

On the right, a list of policies is shown:

ID	Name
1	Leave_Policy_1
2	Leave_Policy_2

For **Yearly** accrual, define number of credit days for single credit of leaves for the entire year.

The screenshot shows the 'Accrual Policy' window with the following settings:

- Accrual Policy:
- Policy Period: Yearly
- Accrual Mode: Fixed
- Credit In Terms Of: Days

Year-Wise Fixed Accrual

Credit Days
21

- **Credit In Terms of:** Select the type of term for which you want to credit the accrual policy. You will get only two option in the list *Days* and *Hours*.

The screenshot shows the 'Accrual Policy' window with the following settings:

- Accrual Policy:
- Policy Period: Yearly
- Accrual Mode: Fixed
- Credit In Terms Of:
 - Days
 - Days**
 - Hours

Year-Wise Fixed Accrual

Credit Days
21

- If you select **Days** from the list then you have to enter credit days.
- If you select **Hours** from the list then you have to enter credit hours in HHH:MM format.

The screenshot shows the 'Accrual Policy' form. The 'Accrual Policy' field is set to 'Leave_Policy_2'. The 'Policy Period' is 'Yearly', and the 'Accrual Mode' is 'Fixed'. The 'Credit In Terms Of' dropdown is set to 'Days'. Below this, the 'Year-Wise Fixed Accrual' section shows 'Credit Days' set to '21'.

The screenshot shows the 'Accrual Policy' form. The 'Accrual Policy' field is set to 'Leave_Policy_2'. The 'Policy Period' is 'Yearly', and the 'Accrual Mode' is 'Fixed'. The 'Credit In Terms Of' dropdown is set to 'Hours'. Below this, the 'Year-Wise Fixed Accrual' section shows 'Credit Hours' set to '120 : 00'.

- **Calculated** - This mode enables the user to configure parameters for leave credit based on the attendance of the user in a previous attendance period. This previous attendance period can be defined using the **Previous Months to consider** (in case of Monthly accrual) or **Previous Year to Consider** (in case of Yearly accrual) drop-down list. Specify the number of months (or year) from the previous attendance period against which the leave accrual is to be calculated as shown below.

The screenshot shows the 'Accrual Policy' form. The 'Accrual Policy' field is set to 'Leave_Policy_2'. The 'Policy Period' is 'Yearly', and the 'Accrual Mode' is 'Calculated'. The 'Credit In Terms Of' dropdown is set to 'Hours'. Below this, the 'Considered Attendance' section shows 'Previous Year To Consider' set to '1', 'Attendance Days' set to 'Payable Days', and 'Payable Days' set to 'Presents'. There is an 'Optional Parameters For Calculation' dropdown. At the bottom, there is a table with columns 'From', 'To', 'Replace Value', and 'Fixed Value', and a 'No Data' message.

- **Attendance Days:** Once the previous attendance period is defined, specify whether the attendance days to be considered for calculation should be the user's **Payable Days** or **Non-Payable Days** as shown.
- **Payable Days:** If user's Payable Days are selected for calculation, specify one of the following components against which the leave credit calculation is to be performed:
 - **Presents** - Total number of days on which the user was present.
 - **Paid Leaves** - Total number of days on which the user took paid leaves.

- **Presents/Paid Leaves** - Total number of days on which the user was either present or took paid leave.
- **Non-Payable Days**: If user's Non-Payable Days are selected for calculation, specify one of the following components against which the leave credit calculation is to be performed:
 - **Un-Paid Leaves** - Total number of days on which the user took un-paid leaves.
 - **Absents** - Total number of days on which the user was absent.
 - **Un-Paid Leaves/Absents** - Total number of days on which the user was either absent or took un-paid leave.

Considered Attendance				
<input type="text" value="Search"/>				+
From ▲	To	Replace Value	Fixed Value	
1	19	Fixed	1.00	
20	25	Fixed	3.00	

Click **Add** button. Enter the Calculated Days Range (From-To) and specify the fixed value of leave which will be credited to the user.



The From day value can start with "0" and you can enter the values in multiples of 0.5

The administrator can credit a fixed number of leaves to a user, based on the previous attendance data, as specified above.

For example, the administrator can specify that a user who was present for a minimum of *20 days* and a maximum of *25 days* in the previous *1 month* attendance period, will be credited *3 leaves*. This can be configured as shown in the above example.

Click **Save** to define this new Accrual Policy on the system. Every new policy created on the system, will be reflected on the policy list on the right hand side of the **Accrual Policy** page as shown below.

Accrual Policy

✓ Saved Successfully

← + ✎ 🗑️ 📄 ✕

Accrual Policy *

2

Leave_Policy_2

Policy Period

Yearly

Accrual Mode

Fixed

Credit In Terms Of

Hours

Year-Wise Fixed Accrual

Credit Hours

120

:

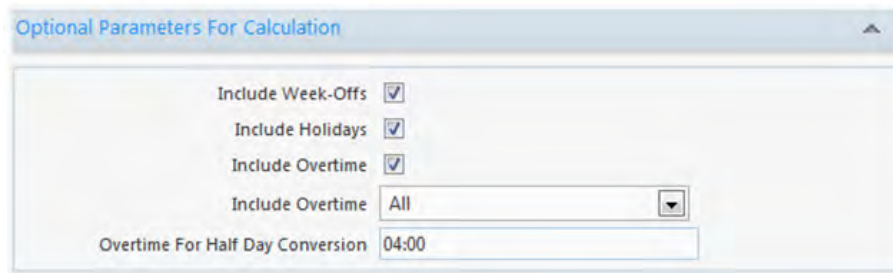
00

Search

ID ▲	Name
1	Leave_Policy_1
2	Leave_Policy_2

Optional Parameters For Calculation

Optionally, the following parameters can be defined for a calculated Accrual Policy, on expanding the **Optional Parameters For Calculation** tab as shown:



Optional Parameters For Calculation

Include Week-Offs ☒

Include Holidays ☒

Include Overtime ☒

Include Overtime All

Overtime For Half Day Conversion 04:00

- **Include Week-Offs** - Select this checkbox to include week-offs of the previous attendance period in the leave credit calculation.
- **Include Holidays** - Select this checkbox to include holidays of the previous attendance period in the leave credit calculation.
- **Include Overtime** - Select this checkbox to include overtime of the previous attendance period in the leave credit calculation. In the **Include Overtime** dropdown list, specify which overtime hours are to be considered when overtime is included in leave credit calculation.
- **Overtime For Half Day Conversion** - Specify the minimum number of hours required for overtime to be converted to a half day in leave credit calculation.

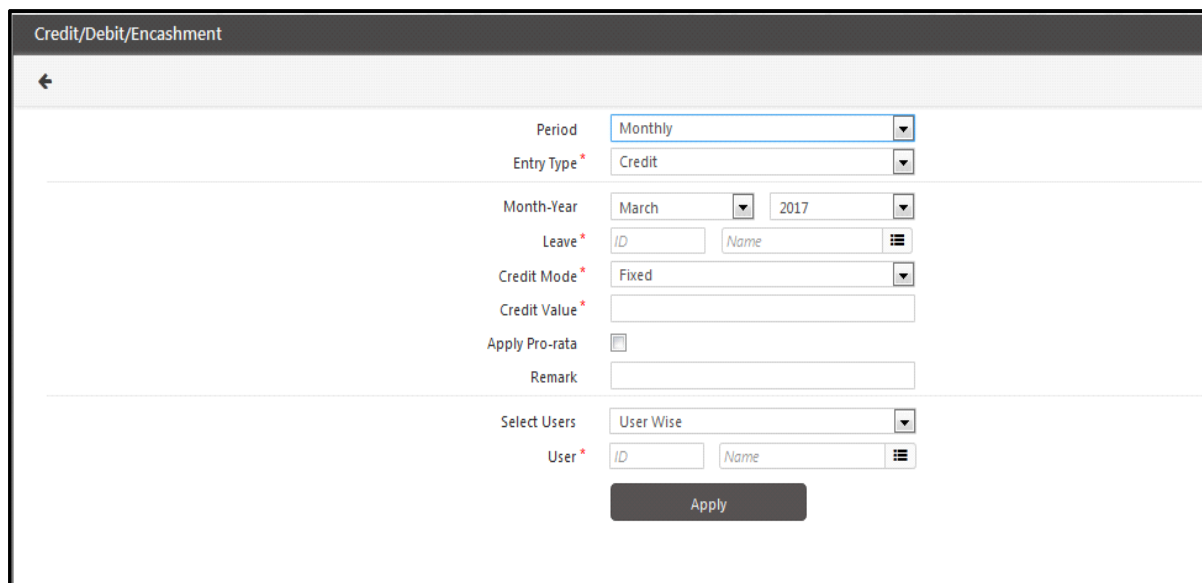
Click the **Add** button to save this configuration.

Leave Credit/Debit/Encashment

This option enables the HR administrator to credit a certain value of leave to the user on monthly or yearly basis. Also the leave can be debited or encashed from the existing leave balance and thus helps in the Leave balance adjustment process. The leave balance adjustment can be done for a single user or multiple users.

Also See [“How to credit leaves to the Employees automatically?”](#) on page 1734.

To credit or debit leaves for users, go to **Leave Management module> Balance Management > Credit/Debit/Encashment** and the following screen appears.

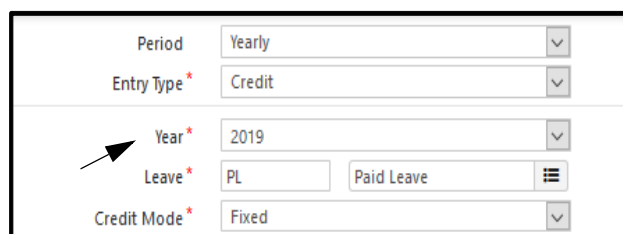


Period: Select the period as Monthly or Yearly for the credit/debit of leaves.

- For Monthly period, specify the **Month-Year** for which the leave credit/debit is to be performed.
- For Yearly period, specify the **Year** for which the leave credit/debit is to be performed.



For Custom yearly period say for April 2018 to March 2019; leave can be credited by selecting year 2019 as shown below.



Entry Type: Select the entry type as **Credit** or **Debit** (For encashing of leaves see “”)



An organization should always operate either on Yearly period or Monthly period approach completely for leave management. Using a mixed period approach must be avoided to prevent data mismatch.

Leave: Select a Leave from the leave selection picklist which is to be credited or debited to the user. The leaves are created from the Leave page

The screenshot shows the 'Credit/Debit/Encashment' form with the following fields:

- Period: Monthly
- Entry Type: Credit
- Month-Year: January 2020
- Leave: HP (Hourly Paid Leave)
- Credit Mode: Fixed
- Credit Value: 1000
- Apply Pro-rata: [checkbox]
- Remark: [text area]
- Select Users: User Wise
- User: [ID, Name]

The 'Picklist For Leave Masters' dialog is open, showing a table of leave types:

LeaveID	Name
1	RANDOM LEAVE
2	Diwali
3	Random Leave 2
HP	Hourly Paid Leave
PL	Paid Leave

Credit Mode: If leaves are to be credited, select the mode as one of the following:

- **Fixed:** On selecting this option, specify the number of leaves to be credited in the **Credit Value** field.
- **Using Accrual Policy:** On selecting this option, select the Accrual Policy using the pick list button based on which leaves will be credited.



If user's joining date lies in the current year then yearly credit/debit of leave should be done in the joining month-year. Also leave cannot be credited after the leaving date of user.

For the Fixed Credit Mode/Fixed Accrual Mode (See "[Accrual Policy](#)"), the administrator has an option to apply Pro-rata calculation on the credit of leaves.

Apply Pro-rata: Select the checkbox to enable credit of leaves on pro-rata basis (i.e. on the basis of the actual number of days worked). For more details on Pro-rata see [“Leave Group”](#).

The screenshot shows the 'Credit/Debit/Encashment' form with the following fields and values:

- Period: Monthly
- Entry Type: Credit
- Month-Year: March 2017
- Leave: PL
- Credit Mode: Fixed
- Credit Value: 10
- Apply Pro-rata: ☐
- Remark: (empty)
- Select Users: User Wise
- User: ID 1567, Name Sheetal

A table below the form lists the selected user:

User ID	Name
1567	Sheetal

An 'Apply' button is located at the bottom of the form.

Remark: If required provide remark for crediting or debiting the leave.

Select Users: Select a user or multiple users for whom the selected leave is to be credited or debited from the dropdown list.

Users can be selected from the filter options of User Wise, Group Wise, and All.

Debit Value: If a leave is to be debited from users, specify the number of days to be debited from the current leave balance in the **Debit Value** field as shown. In the following example, 2 leaves are being debited from the user's leave balance for "PL".

The screenshot shows the 'Credit/Debit/Encashment' form with the following fields and values:

- Period: Monthly
- Entry Type: Debit
- Month-Year: March 2017
- Leave: PL
- Debit Value: 2
- Apply Pro-rata: ☐
- Remark: (empty)
- Select Users: User Wise
- User: ID 1678, Name Supriya

A table below the form lists the selected user:

User ID	Name
1678	Supriya

An 'Apply' button is located at the bottom of the form.

Using Accrual Policy, leave credit is done as shown below

The screenshot shows a web form titled "Credit/Debit/Encashment". It contains several fields for configuring a leave credit entry. The "Period" is set to "Monthly". The "Entry Type" is set to "Credit". The "Month-Year" is set to "March 2017". The "Leave" field is set to "SL" (Sick Leave). The "Credit Mode" is set to "Using Accrual Policy". The "Accrual Policy" is set to "1". The "Apply Pro-rata" checkbox is checked. The "Remark" field is empty. The "Select Users" dropdown is set to "All". An "Apply" button is at the bottom right.

Period	Monthly
Entry Type *	Credit
Month-Year	March 2017
Leave *	SL Sick Leave
Credit Mode *	Using Accrual Policy
Accrual Policy *	1 Leave_Policy_1
Apply Pro-rata	<input checked="" type="checkbox"/>
Remark	
Select Users	All

Apply

How to credit leaves to the Employees automatically?

Prerequisites:

"User/Employee should be assigned the Leave group which consists of the leave to be credited.

"If different number of leave is to be credited, then Accrual Policy is to be defined.

"The COSEC Alert Service on the server computer should be "ON" before setting the Task Scheduler.

To credit the leaves automatically, following steps should be performed:

A. Set "Schedule Parameters"

1. Go to Admin > System Utilities > Task Scheduler.
2. Create a task scheduler for the task Leave Credit Schedule by clicking on Add button.
3. Specify the Schedule Run Time at which the leave will be credited automatically say at 9:00 am.
4. Select the Schedule Run Day from the options of Monthly or Weekly.

"For Monthly option, check the boxes to select the months and select the date of the month on which the leave is to be credited.

" For Weekly option, select the day of the week on which the leave is to be credited.

B. Set "Task Parameters"

1. To credit a fixed number of leave for every month, select the credit method as Fixed.
Now select the leave to be credited and specify the number of leaves say 1.5 PL as shown in below figure.

The screenshot shows the 'Task Scheduler' window. The 'Schedule Name' is 'Leave Schedule' and it is 'Active'. Under 'Schedule Parameter', the 'Task' is 'Leave Credit Schedule', 'Run Schedule' is 'Monthly', and 'Every(Day Of The Month)' is '1'. All months from Jan to Dec are selected. The 'Schedule Run Time' is 'HH:MM'. A 'Task Parameters' sub-window is open, showing 'Leave Selection' with 'Credit Method' as 'Fixed', 'Leave' as 'Paid Leave', 'No of Days' as '1.50', and 'Apply Pro-rata' as unchecked. The 'Processing Period' is set to 'Current'. A 'Filter' button is at the bottom left. On the right, a table lists the schedule:

ID	Schedule Name
1	Leave Credit Task

2. To credit a variable number of leave for different months, select the credit method as Policy. Now select the leave to be credited and select the leave credit policy i.e. the accrual policy from the picklist as shown in below figure.

3. Now, Select the Processing period i.e. the period (month or week) for which leave is to be credited.
For example:

If Processing period is Next. On first of January, 1.5 PL will be credited for February.

If Processing period is Current. On first of January, 1.5 PL will be credited for January.

If Processing period is Previous. On first of January, 1.5 PL will be credited for December.



The "Previous" option for Processing Period is available from COSEC V7R2 onwards.

C. Select the Users

1. Select the user filter option of User Wise if selected user is required to be credited the leaves.
2. Select the user filter option of Group Wise if a particular group of users are required to be credited the leaves.
3. Select the user filter option of All if all the active users are required to be credited the leaves.

Click on **Save** button to save the leave credit schedule.

Leave Encashment

It has been described earlier how some leaves can be defined as encashable leaves i.e. an employee can receive remuneration against such leaves, when unused over a defined attendance period ("Configuring Leaves"). Using the Leave Encashment feature, the administrator can assign encashment to selected users for a definite attendance period.

To encash leave, go to **Leave Management module > Balance Management > Credit/Debit/Encashment** and the following screen appears.

The screenshot shows the 'Credit/Debit/Encashment' form. It has a title bar with a back arrow, a star, and a question mark. The form is divided into several sections. The first section contains 'Period' (Yearly), 'Entry Type' (Encashment), 'Year' (2016), 'Leave' (CL), 'Encashment Mode' (Available), 'Encashment Value', 'Apply Pro-rata' (checkbox), and 'Remark'. The second section contains 'Select Users' (User Wise) and a table of users. The table has columns for 'User ID' and 'Name'. The first row shows '1567' and 'Sheetal'. There is an 'Apply' button at the bottom.

User ID	Name
1567	Sheetal

Entry Type: Select the Entry Type as **Encashment** from the dropdown list as shown above.

Period: Specify the Month-Year for which the leave encashment is to be performed.

Leave: Select a leave using the picklist which is to be encashed by the user. This picklist contains only those leaves for which the Leave Encashment checkbox is enabled while configuring the leave.



*For a leave to be available for encashment, the user must ensure that the **Leave Encashment** option is enabled while defining the particular leave. To know more, please refer to ["Defining New Leaves"](#). The same leave must also be added to the default Leave Group applicable to the organization.*

Encashment Mode: Select the encashment mode from the dropdown list which can be used to define the number of leaves to be encashed from current leave balance for selected user. You can select one of the following options:

- **Defined:** Encash leaves for the number of days as defined in the **Encashment Value** field. Example: If available CL is 5, and defined encashment value is 3 then 3 CL out of available 5 CL will be encashed.
- **Available:** Encash all available leaves in leave balance. Example: If available CL is 5, then 5 CL will be encashed.

Remark: If required provide remark for encashing the leave.

Select Users: Select a user or multiple users for whom the selected leave is to be encashed from the dropdown list. Users can be selected from the filter options of User Wise, Group Wise or All.

Click the **Apply** button to apply the leave encashment settings on the specified users.

The number of Encashed leave appears in Leave Balance page as shown below.

Leave Balance

User ID: 1567 Sheetal

Leaves

Period: Yearly
Balance Year: 2016

Search

Year	Code	Name	Opening	Credit	Debit	Encashment	Availed	Closing	Overflow
2016	CL	Casual Leave	0.00	5.00	0.00	5.00	0.00	0.00	0.00

C-OFF

C-OFF Encashment

Sometimes, employees may choose to encash accumulated C-OFFs instead of using them, if C-OFF encashment is permitted by the organization. C-OFF encashment is a concept similar to Leave encashment. On COSEC, this feature can be configured by an HR administrator using the *C-OFF Encashment* functionality.

To encash C-OFFs for a user, go to **Leave Management module > Balance Management > C-OFF Encashment** and the following screen appears.

The page displays configurations on the left hand side and to the right is a grid containing details like: the month and year in which the C-Off hours is credited, the leave type, C-Off hours availed and the date of applying for encashment.

To encash C-Off click the **New** button and enter the following parameters:

- **User:** Select a **User** from the user picklist for whom the C-OFF encashment is to be performed.
- **Leave:** Select a leave from the dropdown list. All *Compensatory-Off* type of leaves available to this user will appear in this dropdown list for selection.



For a leave to be available for C-OFF encashment, the user must ensure that the **Leave Encashment** option is enabled while defining a *Compensatory-Off* leave type. To know more, please refer to [“Defining New Leaves”](#). The same leave must also be added to the default Leave Group applicable to the organization.

In the following example, there are two leaves available to the selected user:

- **Encashment Mode:** Select the mode for encashment from one of the following options -
 - **Defined** - This mode indicates that the encashment is to be performed against the number of C-OFF hours defined by the HR administrator in the **Total Hours** field. To specify the number of hours, click the Total Hours picklist button. The **C-OFF Selection** pop-up window displays the **Available C-OFF** hours for the selected user. In the **Select C-OFF** field, specify the number of hours (HH:MM format) from the Available C-OFF hours which are to be encashed for the user. Click the **Select** button.

In the following example for **Defined** mode, the available C-OFF for the selected user is 04:00 hours of which 03:00 hours are selected for encashment.

Attendance Date	Available C-OFF	Select C-OFF
01/10/2016	04:00	03:00
03/10/2016	01:00	

Update Close

- **Available** - This mode indicates that the encashment is to be performed against the total available C-OFF hours for the selected user. Hence, for the same user as the above example, in the Available mode, the encashment will be performed for 5:00 hours as shown below.

User: 1 Rosy

Leave: C1 - C-OFF1

Encashment Mode: Available

Total Hours: 05:00

Apply

Month Year Leave C-OFF Hours Entry Date

No Data

Click the **Apply** button to apply for encashment and the saved leave gets displayed in the grid as shown below.

✓ Saved Successfully

User: perry perry

Leave: C1 - C-OFF1

Encashment Mode: Available

Total Hours: 01:00

Apply

Month	Year	Leave	C-OFF Hours	Entry Date
Nov	2016	C1	01:00	09/11/2016
Nov	2016	C1	04:00	09/11/2016

Overflow Management

Overflow Adjustment is a concept essential in order to check an employee's leave balance from overflowing at any point of time. This means that the leave balance of an employee should never accumulate more leaves than the maximum accumulation limit set for the employee.



The administrator can set a check on the maximum accumulation of leaves in a user's leave balance using the **Leave Balance Check** option while defining a new leave. To know more about this configuration, refer to ["Defining New Leaves"](#).

Cancellation of leave applications may be a common cause for such overflow because it restores the leave balance that was deducted on application of a leave. This may sometimes cause any additionally credited leaves to overflow over the maximum leave accumulation limit for the user. To manage this, the HR administrator can determine how the overflowing leaves should be treated, as per the company policy.

In such a scenario, one of the following can be done:

- Allowing the overflowing leaves to be *reused*.
- *Encashment* of overflowing leaves.
- *Discarding* the overflowing leaves.

To manage leave overflow, go to **Leave Management module > Balance Management > Overflow Management** and the following screen appears.

User: Select a User from the picklist for whom the overflow adjustment is to be performed.

Leave: Select a leave from the dropdown list for which the overflow is to be adjusted. This list contains only those leaves in which the "maximum accumulation check" checkbox is enabled at the time of configuration of the selected leave.

Overflow: The system automatically retrieves and displays the number of overflowing leaves in the field. This value is generated when the accumulated leave exceeds its maximum leave specified from the ["Keeping Check on Leave Balance"](#) section.

I.e. If the maximum accumulated check specified is 20 days and the user applies leave for 2 days. Then the leave balance becomes 18 days. Now, if the admin credits 2 days then again the leave balance will become 20 days. Now, in case for any reason if the applied leave gets rejected or cancelled then it gets

credited to the user giving a balance of 22 leaves which is more than the value specified in the Maximum Accumulated check. So this extra 2 days is the value displayed in overflow.

Adjustment Type: Select the adjustment type for the overflowing leaves as **Discard**, **Reuse** or **Encash** as shown below.

A screenshot of a web form showing the 'Adjustment Type' dropdown menu. The menu is open, displaying three options: 'Discard', 'Reuse', and 'Encash'. The 'Discard' option is currently selected and highlighted in blue. Above the dropdown, the 'User' field is set to 'overflow1' and 'Ramesh'. The 'Leave' field is set to 'O1 - SL' and the 'Overflow' field is set to '1.00'.

Adjustment Value: Specify the number of overflowing leaves to be discarded, reused or encashed in the field.

- If the **Adjustment Type** is **Reuse** or **Encash**, then specify the period for which adjustment is to be done.

A screenshot of the same web form with the 'Adjustment Type' dropdown menu set to 'Reuse'. The 'Adjustment Value' field is set to '1.00'. The 'Period' dropdown menu is set to 'Monthly'. The 'Credit/Encash To Period' fields are set to 'March' and '2017'. An 'Apply' button is visible at the bottom.

A screenshot of the same web form with the 'Adjustment Type' dropdown menu set to 'Encash'. The 'Adjustment Value' field is set to '1.00'. The 'Period' dropdown menu is set to 'Yearly'. The 'Credit/Encash To Period' field is set to '2017'. An 'Apply' button is visible at the bottom.

- Select the **Period as Monthly** for monthly adjustment of overflow leaves.
 - Select the month and year for which the overflow leave is to be credited in Reuse adjustment or encashed in Encash type of adjustment.
- Select the **Period as Yearly** for yearly adjustment of overflow leaves.

- Select the year for which the overflow leave is to be credited in Reuse adjustment or encashed in Encash type of adjustment.
- If **Discard** option is selected only specify the adjustment value of leave to be discarded.



An organization should always operate either on Yearly period or Monthly period approach completely for leave management. Using a mixed period approach must be avoided to prevent data mismatch.

Click the **Apply** button to perform the overflow adjustment.

The overflow leave is shown in Leave Balance page as shown below.


Year	Month	Code	Name	Opening	Credit	Debit	Encashment	Availed	Closing	Overflow
2017	Mar	O1	SL	0.00	7.50	0.00	0.00	0.00	6.50	1.00
2017	Mar	O2	PL	1.00	0.00	0.00	0.00	0.00	1.00	0.00
2017	Mar	O3	OF	0.00					0.00	0.00

After the encash adjustment of overflow leave, it will be shown in Encashment as shown below.

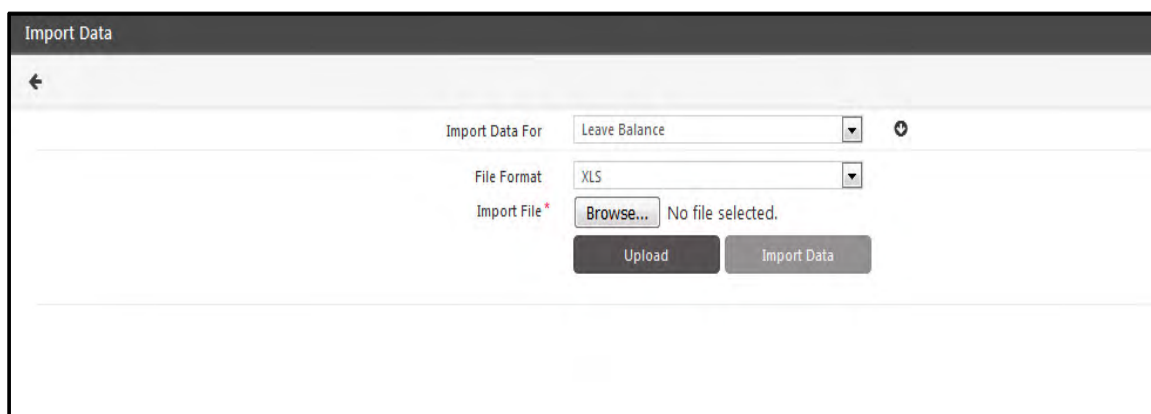
Year	Month	Code	Name	Opening	Credit	Debit	Encashment	Availed	Closing	Overflow
2017	Mar	O1	SL	0.00	7.50	0.00	1.00	0.00	6.50	0.00
2017	Mar	O2	PL	1.00	0.00	0.00	0.00	0.00	1.00	0.00
2017	Mar	O3	OF	0.00					0.00	0.00

Import Leave Balance

The COSEC application has an inbuilt utility for enabling users to import data from excel files with predefined format. This would thus save the end user a lot of time and effort in having to make individual data entries at the application level.

This can be done by downloading the sample import file by clicking the  button on the **Import Data** page. The user can thus insert all the data in the sample file and then upload it to the system.

To import leave balance data from a file, go to **Leave Management module > Balance Management > Import Leave Balance** and the following screen appears.



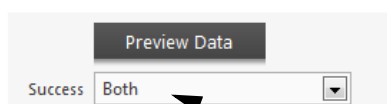
The following options appear for configuration on the **Import Data** page.

- **Import Data For** - Select the table from the dropdown list to which the data is to be imported.
- **File Format** - Select the file format of the specific file from the dropdown list. The options available are XLS and CSV.
- **Import File** - Browse and select the file from which the data is to be imported.

The **Preview Data** button enables the administrator to view the data in the respective worksheets to confirm that the data is in order prior to giving the import command.

Click on **Import Data**. The system will import all the relevant valid entries from the sheet and will display the status in the bottom grid. On successful import the, "Success" status will appear in the data preview as "Yes". Else, a "No" status will appear with an error description as shown.

User can also filter import result records on the basis of their success value (Yes/No) using the **Success** dropdown list.



Administrator needs to ensure that the ASP.NET user has full rights on the folder containing the Excel or .csv file for the import data operation.

Leave Application/Approval

Leave Application is a formal mode of requesting leave approval before or after an employee has taken a leave. It enables an organization to keep a track of all requested and approved leaves and enables the HR administrator or reporting in-charge to address issues such as irregularities in the attendance of employees or shortage of resources due to overlapping leaves.

The Leave applications can be made by:

- System Account User
- On Behalf System Account User
- Using the ESS Self Service Module

COSEC Web enables all *System Account users* with appropriate page rights to make leave applications using the *Leave Management* module. All applications made by the System Account user are *pre-approved* by default.

COSEC Web also enables all On Behalf System Account User with appropriate page rights to make leave applications using the *Leave Management* module. All applications made by the On Behalf System Account User are *pre-approved* by default. For creating and assigning the roles and rights to the On Behalf System Account User. Refer to [“On Behalf System Account User”](#).

For leave applications made using the *Employee Self Service* module, the leave approval has to be done by the respective supervisors of the reporting group by logging into the ESS. However, such leaves can also be sanctioned by a System Account user from the Leave Management module on the COSEC Web Application.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to [“Reporting In-Charge”](#), [“Approval Policy”](#) and [“Configuring Users”](#).

For leave approval [See “Leave Approval” on page 1753.](#)



ESS users can apply for leaves only using the ESS module and such leave applications require approval either from the reporting group in-charge or the COSEC Web system account user. Leaves directly approved by the system administrator do not require any further approval from respective supervisors.



Applied leaves can be modified or cancelled after they have been approved or rejected. Once a leave application is modified it will be submitted for approval, and once the verdict is given, it can be modified again.

Once the modification/cancellation application is approved/rejected, an employee can apply for modification/cancellation of it ones again.



The Leave applied from Leave Management module gets approved automatically.

Applying for a Leave

This section describes how to apply for a leave using the Leave Management module.

To do this, go to **Leave Management module > Application/Approval > Leave Application** and the following screen appears.

The screenshot shows the 'Leave Application' interface. On the left, there are input fields for 'User' (ID and Name), 'Application Date', 'Consideration In Terms Of' (set to 'Both'), 'From' and 'To' dates, 'Applied Duration', 'Posted Duration', 'Leave' (a dropdown menu), 'Current Balance', and 'Reason And Contact Info' (Reason, Address, and Contact Number fields). On the right, there is a summary of leave status: '0 day Absent', '0 Pending', '0 Approved', and '0 Rejected'. Below this is an 'Attendance Details' table with columns for Date, Shift, 1st Half, 2nd Half, First IN, Last OUT, and Work Hours. The table currently displays 'No Data'.

The page displays configurations on the left hand side and to the right is the attendance details of the user along with all the leave application details of a particular user for a particular month. It also displays the number of leaves availed, total absent days, total leaves pending, approved and rejected.

To apply a new leave, click **New** button and enter the following parameters:

User: Select user from the picklist for whom the leave application is to be made.

Application Date: It indicates the date for which application is going to be created. Thus, "Application Date" is not editable because its an system-generated field which shows current date.

Consideration In Terms Of: Select the option for which type of leave you want to apply, from the given list.

From/To Date: Select the starting and ending date for the leave period using the date selection button. For a single day select the same date in both the fields.

- Specify whether the leave should be considered for **Full Day**, **First Half** or **Second Half** for a single day. For more than 1 leave specify the starting day of leave as full day or second half and ending leave day as full day or first half as shown below.



For a particular user, if **Restrict Half Day Considerations** is enabled in the page User > User configuration > T&A, then in **From/To Date** only full day attendance options will be visible and all the other half day options will be disabled for that particular user as shown in the screen below.

Leave Application

User * 2551 Rushi Shah

Application Date 17/01/2020

Consideration In Terms Of Both

From * From Date Full Day

To * To Date Full Day

Applied Duration

Posted Duration

Leave 2 - Diwali

Current Balance »

Reason And Contact Info

Reason * Personal

Address 30 Char

Contact Number 20 Char

Submit Cancel

Applied Duration: It displays the total time duration for which the leave has been applied.

Posted Duration: It displays the number of working duration posted between the leave applied. It is automatically calculated by the system.

Leave Application

User * 2551 Rushi Shah

Application Date 17/01/2020

Consideration In Terms Of Both

From * 18/01/2020 Full Day

To * 18/01/2020 Full Day

Applied Duration 1

Posted Duration

Leave PL - Paid Leave

Current Balance 1.75 »

Reason And Contact Info

Reason * Sick

Address 30 Char

Contact Number 20 Char

Medical Certificate Available ☒

Submit Cancel

Dec 2019 Feb 2020

1 day Absent 0 Pending

Attendance Details

Date	Shift
17/01/2020	

Leave: Select the type of leave to be applied from the dropdown list. This list displays all leaves defined on the system as shown below.




1. This feature cannot be used to apply for Compensatory-OFF leave types. Hence such leaves defined on the system will not appear on the Leave selection list. To know more about applying for C-OFF, refer to [“C-OFF Application/Approval”](#).


2. The application and Approval of Restricted holiday type leave is described in [“Restricted Holidays”](#).

Current Balance: It displays the current leave balance which guides the user to apply for the leave and accordingly the applied leave will be deducted from the leave balance.



The leaves are credited to the user manually by the administrator or through the scheduler using Accrual Policy. See [“Leave Credit/Debit/Encashment”](#) and [“Accrual Policy”](#)

You can also view the leave balance detail by clicking Details  icon next to the text-box. The **Leave Balance Detail** window will appear which shows the details of Paid Leave type and Restricted Leave type provided if user has the available balance for the leave.

Example: The user is applying leave on 7th as shown above. Before applying the type of leave; you must know which leave type has available balance. So click on  to view the available balance.

Leave Balance Detail

User

2551

Rushi Shah

Attendance Period

Jan

2020


Search

Code	Name	Opening	Credit	Debit	Encashed	Availed	Closing	Overflow
1	RANDOM LEAVE	00:00	04:00	00:00	00:00	01:15	02:45	00:00
3	Random Leave 2	0	5	0	0	4.5	0.5	0
HP	Hourly Paid Leave	00:00	05:00	00:00	00:00	00:00	05:00	00:00
PL	Paid Leave	0	1.75	0	0	0	1.75	0

Now you know that Paid Leave has balance of 1.75; so you can select the Paid Leave type leave in drop down and click Submit button to apply for leave.


Reason and Contact Info

- **Reason:** Enter reason for requesting leave.
- **Address:** Provide address of the user for whom the leave application is being made.
- **Contact Number:** Provide the contact number of the user for whom the leave application is being made.
- **Medical Certificate Available:** Select the checkbox to make it mandatory for the applicant to produce a medical certificate as a proof to testify the reason behind the current leave.

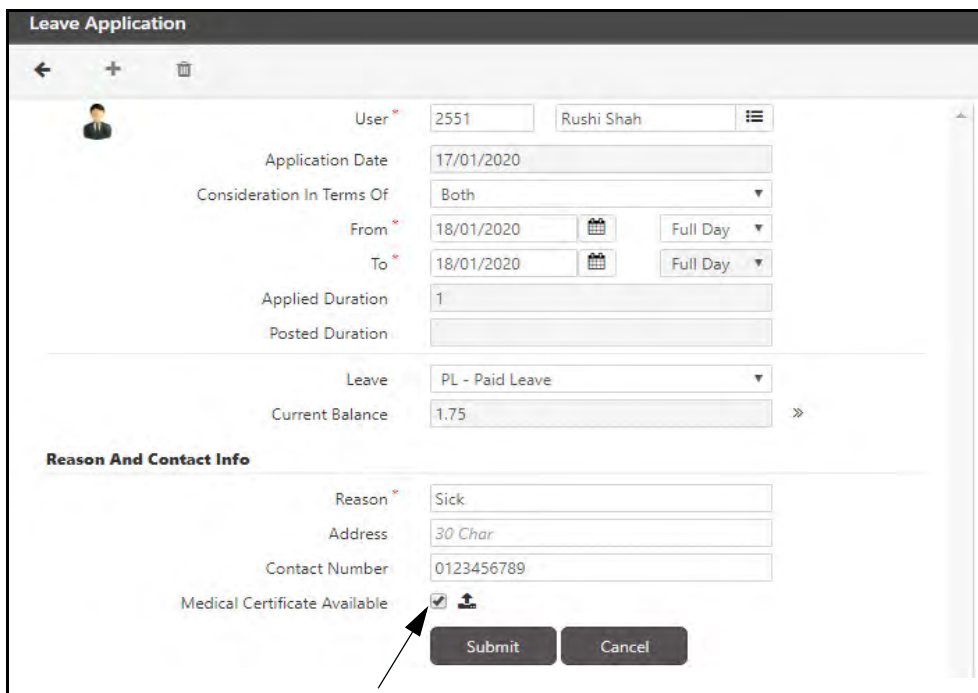
Select this checkbox if you have a Medical Certificate as a proof and reason for the current leave. To upload this certificate, click on the **Upload**  button.

Select the desired file as per the supported formats (.jpg, .bmp, .png, .pdf) and size.

Click **Update**.

The document will be uploaded and can be previewed by clicking on **Preview**  button.

This option is available only if it is enabled during configuration of the selected leave from the Leave page. For more information, refer [“Optional Restrictions”](#) in Leave page.



The screenshot shows the 'Leave Application' form. The 'Reason And Contact Info' section is highlighted. It includes fields for 'Reason' (Sick), 'Address' (30 Char), and 'Contact Number' (0123456789). The 'Medical Certificate Available' checkbox is checked, and an arrow points to it. Below the form are 'Submit' and 'Cancel' buttons.

Click **Submit** button to apply for the leave as shown below.

The applied leave gets displayed in the Application Details grid as shown below. If the number of days of the applied leave is more than the current leave balance, then the system will not allow the application to be made.

The screenshot shows the 'Leave Application' form. On the left, the form fields include: User (U4), Application Date (14/06/2021), Consideration In Terms Of (Both), From (21/06/2021), To (21/06/2021), Applied Duration (1.0), Posted Duration (1.0), Leave (PL - Paid Leave), and Current Balance (81.50). Below these are fields for Reason (Personal), Address (30 Chars), Contact Number (20 Chars), Application Status (Approved (14/06/2021 18:00)), and Remark (Approved Leave n2). At the bottom, there are buttons for 'Submit' and 'Cancel', and links for 'Apply For Cancellation' and 'Apply For Modification'.

On the right, a red box highlights the 'Application Details' section. It shows a summary: 3.5 days Absent, 0 Pending, 6 Approved, and 4 Rejected. Below this is a table with the following data:

From	To	Leave	Application Date	Application Type	Status	Approval Details
21/06/2021	21/06/2021	PL	14/06/2021	New	✓	
19/06/2021	19/06/2021	PL	14/06/2021	New	✓	
18/06/2021	18/06/2021	PL	14/06/2021	New	✓	
16/06/2021	16/06/2021	PL	14/06/2021	New	✓	
15/06/2021	15/06/2021	PL	11/06/2021	New	✗	
14/06/2021	14/06/2021	PL	14/06/2021	New	✗	
11/06/2021	11/06/2021	PL	10/06/2021	Modification	✗	

Below the table, it says '1 - 7 of 10 records' and has pagination controls.

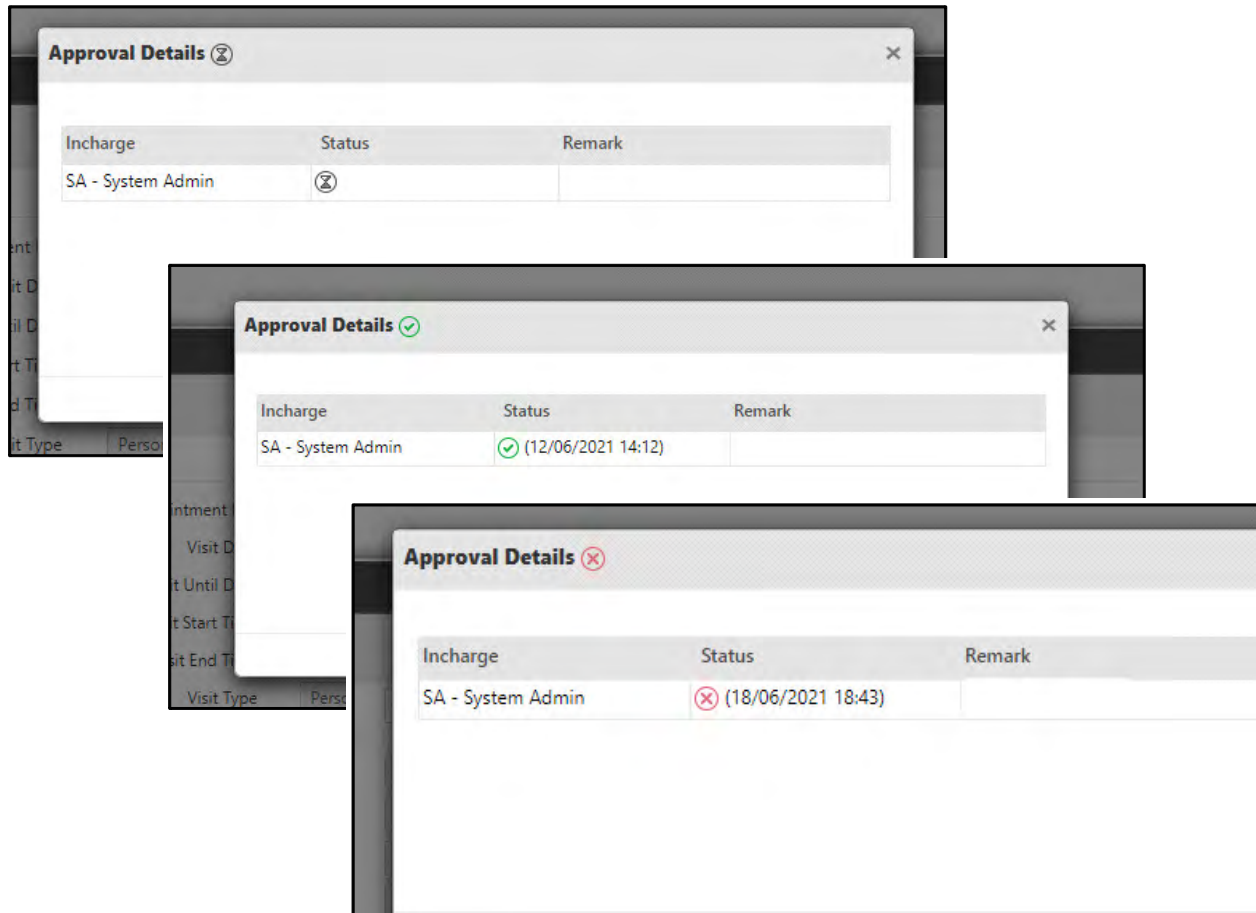
From this page you can also view the details of leaves which have been applied for cancellation or for modification from the ESS module, once they get approved or rejected.

To view the leave cancellation details, select a leave from the grid on the right hand side and the data gets loaded as shown in the screen below.

This screenshot is similar to the previous one, but the 'Apply For Cancellation' link at the bottom left is highlighted in blue. The 'Application Date' field is now set to 18/06/2021, and the 'Cancellation Reason' field is set to 50 Chars. The 'Application Status' remains 'Approved (14/06/2021 18:00)'. The 'Application Details' grid on the right is the same as in the previous screenshot.

Similarly, you can also view the leave modification details, by selecting a leave from the grid on the right hand side and the data gets loaded as shown in the screen below.

Approval Details window appears as shown below:



It displays the status of the user's application under **Approval Details**, that is, whether it is — pending, approved or rejected.

The application's status is displayed in the **Status** column as Pending ⌚ , Approved ✓ or Rejected ✗ .

Remark displays the comments provided by the Admin/ RIC/ System.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Leave Approval

The system administrator can view, approve or reject leaves that have been applied by the ESS user. The administrator also has the right to reject any pre-approved leaves and vice-versa, if required.

To access this functionality,

Go to **Leave Management module > Application/Approval > Leave Approval** and the following screen appears.

The screenshot shows the 'Leave Approval' web application interface. At the top, there's a header 'Leave Approval' with navigation icons. Below it, a section titled 'Show All Pending Applications' has a radio button selected. There are date pickers for 'Leave Date' (18/12/2019 to 01/02/2020), a 'Filter Users' dropdown set to 'Individual', and a 'User' input field containing '2551' and 'Rushi Shah'. A 'View' button is below these filters. The main content area has three collapsible panels: 'Pending (0)' (collapsed), 'Approved (5)' (expanded), and 'Rejected (0)' (collapsed). The 'Approved (5)' panel contains a search bar and a table of approved leave applications. The table has columns: User, Name, From, To, Leave, Application Date, Posted Duration, Approve, Reject, Remark, and Details. The data rows show five approved leave applications for user 2551, Rushi Shah, including 'Paid Leave', 'Random Leave 2', and 'RANDOM LEAVE'.

User	Name	From	To	Leave	Application Date	Posted Duration	Approve	Reject	Remark	Details
2551	Rushi Shah	23/01/2020	23/01/2020	Paid Leave	17/01/2020	1.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
2551	Rushi Shah	20/01/2020	22/01/2020	Random Leave 2	16/01/2020	2.5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Leave Modification	
2551	Rushi Shah	18/01/2020	19/01/2020	Random Leave 2	17/01/2020	2.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
2551	Rushi Shah	17/01/2020 10:00	17/01/2020 10:45	RANDOM LEAVE	16/01/2020	00:45	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Leave	
2551	Rushi Shah	16/01/2020 10:00	16/01/2020 10:30	RANDOM LEAVE	16/01/2020	00:30	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Leave	

By default, the Admin can view all pending applications from the last one month period. However, sometimes users may also apply for leaves on future dates.

You can either:

- view all the pending Leave Approval Applications
- set the filters — Date, Filter Users — to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter. You can view all pending leave applications, including those made for future dates.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To know more, refer to [“Pending Applications”](#).

Applications according to Set Filters

To Set the Filters,

- **Leave Date:** Select and specify the start and end dates using the calendar buttons to define the period for which leave approval status is to be viewed.
- **Filter Users:** You can filter records according to the desired Enterprise Group, All or for an Individual.

Select **All**, to view authorization status of the applications of all the active users on the system.

Select **Individual**, to view authorization status of the applications of a single user. Click the picklist to select the desired User ID/Name.

Select the desired Enterprise Group — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Group 1,2/3 and then click the picklist to select the desired group's ID/Name, to view authorization status of these applications.

- Click the **View** button and all the pending, approved and rejected leave applications along with their details will be displayed.

Pending Applications

Click the **Pending** collapsible panel. The **Pending** section lists all the leave/cancellation/modification applications pending for authorization by the reporting in-charge or HR administrator as shown below.

The screenshot shows the 'Leave Approval' application window. At the top, there are filters for 'Leave Date' (24/10/2017 to 08/12/2017), 'Filter Users' (All), and 'Group/User' (ID/Name). A 'View' button is present. Below the filters, the 'Pending (4)' section is expanded, showing a table of pending applications. The table has columns for User ID, Name, From Date, To Date, Leave, Application Type, Application Date, Posted Days, Approve, Reject, Remark, and Details. An arrow points to the 'Details' icon in the first row.

User ID	Name	From Date	To Date	Leave	Application Type	Application Date	Posted Days	Approve	Reject	Remark	Details
apta	apta user	01/11/2017	01/11/2017	Paid Leave	New	02/11/2017	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Leave	
apta	apta user	30/10/2017	30/10/2017	Paid Leave	New	31/10/2017	1.0	<input type="checkbox"/>	<input type="checkbox"/>		
apta	apta user	27/10/2017	27/10/2017	Leave without pay	Modified	31/10/2017	0.5	<input type="checkbox"/>	<input type="checkbox"/>		
apta	apta user	24/10/2017	24/10/2017	Maternity Leave	New	31/10/2017	0.5	<input type="checkbox"/>	<input type="checkbox"/>		

Below the table, there are sections for 'Approved (3)' and 'Rejected (0)'.

When any application is in the Pending state it can be authorized by the Admin or RIC.

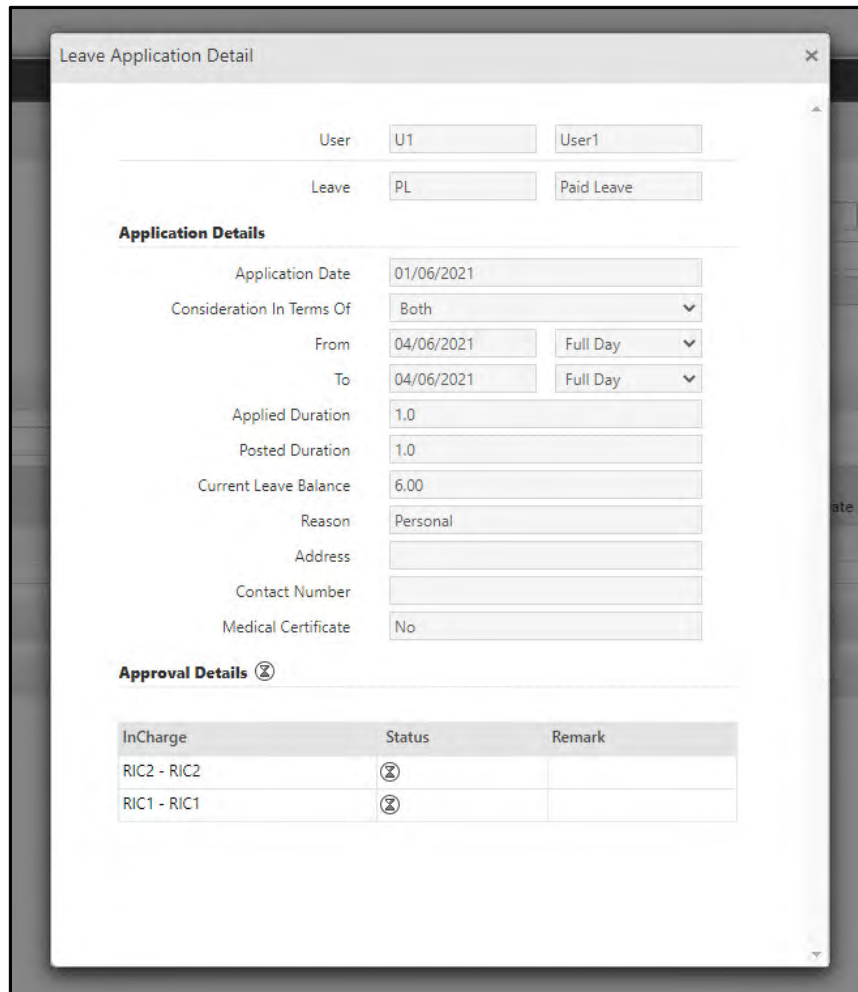
- To approve/reject applications selectively, click the respective application check box against the user.
- To approve/reject all the applications simultaneously, click the Approve /Reject checkbox in the header column.

Once the Admin approves/ rejects the application, the record will be moved from the **Pending** section to the **Approved/ Rejected** section respectively.

The default **Remark** for the Approved and Rejected application will appear in the respective fields. You can enter any customized Remark while authorizing the application.

Click the **Details**  icon to view the details of the applied leave.

Leave Application Detail window appears as shown below:



User	
U1	User1

Leave	
PL	Paid Leave

Application Details

Application Date	01/06/2021
Consideration In Terms Of	Both
From	04/06/2021
To	04/06/2021
Applied Duration	1.0
Posted Duration	1.0
Current Leave Balance	6.00
Reason	Personal
Address	
Contact Number	
Medical Certificate	No

Approval Details

InCharge	Status	Remark
RIC2 - RIC2	P	
RIC1 - RIC1	P	

Leave Application Detail window displays the user's application details.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer ["Approval Policy"](#).

Remark displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.



The pending applications can not be authorized if the attendance period is closed while doing monthly attendance process and “Attendance Correction in Closed Period” checkbox is disabled from Time and Attendance> Policies >Attendance Policy> General.

Even though; the period is closed but if “Attendance Correction in Closed Period” checkbox in Policy is enabled then authorization can be made.

Approved Application

Click the **Approved** collapsible panel.

The **Approved** section displays all the leave/cancellation/modification applications that have been approved by the reporting group in-charge or the system administrator. Leave applications generated using the **Leave Management** module on COSEC Web will appear in this section by default as they are pre-approved.

User ID	Name	From Date	To Date	Leave	Application Date	Posted Days	Approve	Reject	Details
1	Rosy	18/11/2016	21/11/2016	P -Paid Leave	15/11/2016	4.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1	Rosy	11/11/2016	14/11/2016	P -Paid Leave	10/11/2016	4.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1	Rosy	04/11/2016	07/11/2016	P -Paid Leave	10/11/2016	4.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1	Rosy	03/11/2016	03/11/2016	PL -Privelege Leave	03/11/2016	1.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1	Rosy	02/11/2016	02/11/2016	P -Paid Leave	10/11/2016	1.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

To change the authorization verdict of any application, select **Reject** check box against the corresponding user. Once you reject an approved application, the record will be moved to the **Rejected** section.

Click the **Details** icon to view the application details of the corresponding user.

Leave Application Detail window appears as shown below:

Leave Application Detail

User: U4 User4

Leave: PL Paid Leave

Application Details

Application Date: 14/06/2021

Consideration In Terms Of: Both

From: 21/06/2021 Full Day

To: 21/06/2021 Full Day

Applied Duration: 1.0

Posted Duration: 1.0

Current Leave Balance: 81.50

Reason: Personal

Address:

Contact Number:

Medical Certificate: No

Approval Details ✓

Incharge	Status	Remark
ri1 - Riini1	✓ (14/06/2021 18:00)	Approved Leave ri1
ri2 - Riini2	✓ (14/06/2021 18:00)	Approved Leave ri2

Leave Application Detail window displays the user's application details.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer ["Approval Policy"](#).

Remark displays the comments provided by the Admin / RIC / System.

Click **Save** to save the authorization.

Rejected Application





Click the **Rejected** collapsible panel.

The **Rejected** section displays all the leave/cancellation/modification applications that have been rejected by the reporting group in-charge or the system administrator.

The following screen displays the **Rejected** section with rejected leave applications:

Rejected (4)

Search

User ID	Name	From Date	To Date	Leave	Application Date	Posted Days	Approve	Reject	Details
1	Rosy	18/11/2016	21/11/2016	P -Paid Leave	15/11/2016	0.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
1	Rosy	07/11/2016	08/11/2016	P -Paid Leave	10/11/2016	0.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
1	Rosy	07/11/2016	08/11/2016	P -Paid Leave	10/11/2016	0.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
1	Rosy	04/11/2016	04/11/2016	PL-Privelege Leave	03/11/2016	0.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

To change the authorization verdict of any application, select **Approve** check box against the corresponding user. Once you approve a rejected application, the record will be moved to the **Approved** section.

Click the **Details**  icon to view the application details of the corresponding user.

Leave Application Detail window appears as shown below:

Leave Application Detail

User: U4 User4

Leave: PL Paid Leave

Application Details

Application Date: 11/06/2021

Consideration In Terms Of: Both

From: 15/06/2021 Full Day

To: 15/06/2021 Full Day

Applied Duration: 1.0

Posted Duration: 0.0

Current Leave Balance: 81.50

Reason: Personal

Address:

Contact Number:

Medical Certificate: No

Application Verdict: Rejected

Verdict Date: 11/06/2021

Modification Application Details

Application Date: 11/06/2021

From: 15/06/2021 Full Day

To: 15/06/2021 Full Day


Reason: Applied Leave Modification

Address:

Contact Number:

Medical Certificate: No

Approval Details

Incharge	Status	Remark
RG2	 (11/06/2021 10:50)	Reject Modification RG2

Leave Application Detail window displays the user's application details.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remarks displays the comments provided by the Admin / RIC / System.

Click **Save** button to save the changes.



System Administrator can delete pending/approved/rejected application.

Half Day Restriction on posted days

On the Leave Approval page, **Half Day restriction on posted days** feature restricts the administrator to approve the posted half day leave application for that particular user.

Consider a scenario where the user has applied for the half day leave from the ESS login page and the Application has been sent for approval to the administrator.

Suppose after posting the half day leave application, **Restrict Half Day Considerations** has been enabled in the page User > User configuration > T&A for that particular user. Now when the Administrator will try to approve the Leave Application for that user, then it will show the error in the Error List that "Half-day Application is restricted for this User" as shown in the screen below.

The screenshot shows the 'Leave Approval' window. At the top, there is a blue banner with the text 'Check Process Error List For User Record Not Processed.' Below this, there are filters for 'Show All Pending Applications', 'Leave Date' (From Date, To Date), 'User Selection' (All), and 'Group/User' (ID, Name). A 'View' button is present. Below the filters, there is a section for 'Pending (17)' and an 'Error List' section. The 'Error List' section contains a table with the following data:

User ID	Name	Appl Date	From Date	To Date	Leave	Status	Description
1687	Aditi Gupta	07/18/2017	07/06/2017	07/06/2017	CL-ggg	Pending	Half-day Application is restricted for this User

An arrow points to the 'Description' column of the error list, highlighting the message 'Half-day Application is restricted for this User'.

Tour Application/Approval

An employee who has to go out of the office premises for official work E.g. Meeting, for specific number of days or hours, often needs to use this type of leave. The application process for Tour on COSEC Web is similar to the leave application.

The Tour applications can be made by:

- System Account User
- On Behalf System Account User
- Using the ESS Self Service Module (For more details refer COSEC Employee Self Service User Manual)

COSEC Web enables all *System Account users* with appropriate page rights to make tour applications using the *Leave Management* module. All applications made by the System Account user are *pre-approved* by default.

COSEC Web also enables all On Behalf System Account User with appropriate page rights to make leave applications using the *Leave Management* module. All applications made by the On Behalf System Account User are *pre-approved* by default. For creating and assigning the roles and rights to the On Behalf System Account User. Refer to “[On Behalf System Account User](#)”.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to “[Reporting In-Charge](#)”, “[Approval Policy](#)” and “[Configuring Users](#)”.



The Tour applied from System Administrator login gets approved automatically.

Applying for Tour

This section describes how to apply for a tour using the Leave Management module.

To do this, go to the **Leave Management module > Application/Approval > Tour Application** and the following screen appears.

Tour Application

User: 1 Shalini

From Date: From Date Full Day

To Date: To Date Full Day

Applied Days

Posted Days

Tour: TR - Tour1

Reason And Contact Info

Reason: 50 Char

Address: 30 Char

Contact Number: 20 Char

Submit Cancel

Mar 2017 May 2017 Availed Tours : 0

26 days Absent 0 Pending 0 Approved 0 Rejected

Attendance Details

Date	Shift	1st Half	2nd Half	First IN	Last OUT	Work Hours
04/17/2017		AB	AB			
03/29/2017	GS	AB	AB			
03/28/2017	GS	AB	AB			
03/27/2017	GS	AB	AB			
03/25/2017	GS	AB	AB			
03/24/2017	GS	AB	AB			
03/23/2017	GS	AB	AB			

1 - 7 of 26 records

< 1 2 3 4 >

The page displays configurations on the left hand side and to the right is the attendance details of the user along with all the tour application details of a particular user for a particular month. It also displays the number of tours availed, total absent days, total tours pending, approved and rejected.

To apply a new tour for a user, click **New** button.

User: Select the user for whom the tour is to be applied.

From Date: Select the starting date for the tour period using the date selection button and specify whether the tour is to be considered for Full Day or start only from the Second Half.

To Date: Select the end date for the tour period using the date selection button and specify whether the tour is to be considered for Full Day or end right after the First Half.



For a particular user, if **Restrict Half Day Considerations** is enabled in the page User > User configuration > T&A, then in **From/To Date** only full day attendance options will be visible and all the other half day options will be disabled for that particular user as shown in the screen

below.

Applied Days: The system automatically calculates the number of days the tour has been applied for.

Posted Days: The posted days are the actual days for which the tour will be applied. It will be automatically calculated by the system after saving the application.

Tour: Select a tour from the Tour drop down list, for which the application is to be made. It displays the list of tours available in the Leave Group assigned to the user.




Tours and Leaves on COSEC have a similar configuration and application process. To know more about applying for leaves, refer to ["Leave Application/Approval"](#).

Reason and Contact Info

- **Reason:** Enter reason for requesting the tour.


- **Address:** Enter the address of the user for whom the tour application is being made.
- **Contact Number:** Enter the contact number of the user for whom the tour application is being made.
- **Tour Document Available:** Select the checkbox to make it mandatory for the applicant to produce a tour document to specify the reason behind the current tour.

This option is available only if it is enabled during configuration of the selected tour from the **Tour** page. For more information, refer "[Optional Restrictions](#)" in Tour page.

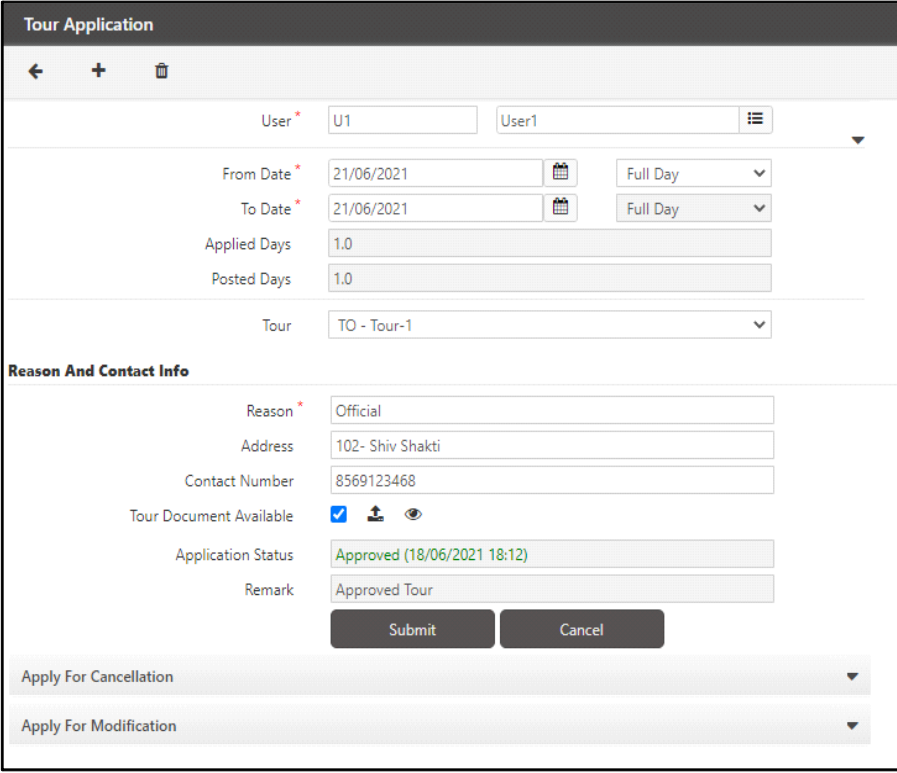
Click on the **Upload**  button and select the respective document.

Select the desired file as per the supported formats (.jpg, .bmp, .png, .pdf).

Then click **Update**.

The document will be uploaded and can be previewed by clicking on **Preview**  button.

Click the **Submit** button to apply for the tour. If applied successfully, the **Application Status** for the tour will be updated to "Approved".



Tour Application

User * U1 User1

From Date * 21/06/2021 Full Day

To Date * 21/06/2021 Full Day

Applied Days 1.0

Posted Days 1.0



Tour TO - Tour-1

Reason And Contact Info

Reason * Official

Address 102- Shiv Shakti

Contact Number 8569123468

Tour Document Available ☒  

Application Status Approved (18/06/2021 18:12)

Remark Approved Tour

Submit Cancel

Apply For Cancellation

Apply For Modification

From this page you can also view the details of tours which have been applied for cancellation or for modification from the ESS module.



Once the tour gets approved or rejected, it can be requested for modification or cancellation from the ESS module.

Tour Cancellation

The tour cancellation details can be viewed by selecting the tour from the grid on the right hand side as shown below.

The screenshot displays the 'Tour Application' interface. On the left, the 'User' is 'Shalini'. The 'From Date' is '03/10/2017' and the 'To Date' is '03/11/2017', both set to 'Full Day'. 'Applied Days' and 'Posted Days' are both '2.0'. The 'Tour' is 'TR - Tour1'. Under 'Reason And Contact Info', the 'Reason' is '50 Char', 'Address' is '30 Char', and 'Contact Number' is '20 Char'. The 'Application Status' is 'Approved (04/20/2017 14:39)'. Below this, the 'Apply For Cancellation' section shows 'Cancellation Reason' as 'Tour postpone required' and 'Cancellation Status' as 'Applied (04/20/2017 14:49)'. On the right, a summary bar shows '22 days Absent', '2 Pending', '1 Approved', and '0 Rejected'. Below this is a table of application details.

From	To	Leave	Application Date	Application Type	Status
04/04/2017	04/06/2017	TR	04/20/2017	New	✓
03/10/2017	03/11/2017	TR	04/20/2017	Cancellation	✗
03/08/2017	03/09/2017	TR	04/20/2017	Modification	✗

Tour Modification

You can view the tour modification details, by selecting a tour from the grid on the right hand side and the data gets loaded as shown in the screen below.

Tour Application

User: U1 | User1

From Date: 23/06/2021 | Full Day

To Date: 23/06/2021 | Full Day

Applied Days: 1.0

Posted Days: 1.0

Tour: TO - Tour-1

Reason And Contact Info

Reason: Official

Address: ATLADARA

Contact Number: 84569895565

Tour Document Available: ☒

Application Status: Approved (18/06/2021 18:19)

Buttons: Submit, Cancel

Apply For Cancellation

Apply For Modification

From Date: 23/06/2021 | Full Day

To Date: 23/06/2021 | Full Day

Applied Days: 1.0

Posted Days: 1.0

Modification Reason: Applied Tour Modification

Tour Document Available: ☒

Modification Status: Applied (18/06/2021 18:20)

Application Summary

May 2021 | Jul 2021

5 days Absent | 1 Pending | 1 Approved | 0 Rejected

Application Details | Show All

From	To	Tour	Application Date	Application Type	Status	Approval Details
23/06/2021	23/06/2021	TO	18/06/2021	Modification		
21/06/2021	21/06/2021	TO	18/06/2021	New		

Click **Details** icon from the grid available on the left side of the page to view the Approval Details of the already applied application.

Approval Details window appears as shown below:

Approval Details

Incharge	Status	Remark
SA - System Admin		




Approval Details

Incharge	Status	Remark
SA - System Admin	(12/06/2021 14:12)	

Approval Details

Incharge	Status	Remark
SA - System Admin	(18/06/2021 18:43)	

It displays the status of the user's application under **Approval Details**, that is, whether it is — pending, approved or rejected.

The application's status is displayed in the **Status** column as Pending  , Approved  or Rejected  .

Remark displays the comments provided by the Admin/ RIC/ System.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer [“Approval Policy”](#).

Tour Approval

The system administrator can view, approve or reject tour applications made by ESS users using the *Tour Approval* functionality. The administrator also has the right to reject any pre-approved tours asnd vice-versa, if required.

To access this functionality, go to the **Leave Management module > Application/Approval > Tour Approval** and the following screen appears.

You can either:

- view all the pending Tour Approval Applications
- set the filters — Date, Filter Users — to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter. You can view all pending tour applications, including those made for future dates.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

- To reject the application, select the **Reject** check box of the desired entry.

To know more, refer to [“Pending Applications”](#)

Applications according to Set Filters

To Set the Filters,

- **Tour Date:** Select the start and end dates as the period for which tour approval status is to be viewed.
- **Filter Users:** You can filter records according to the desired Enterprise Group, All or for an Individual.

Select **All**, to view authorization status of the applications of all the active users on the system.

Select **Individual**, to view authorization status of the applications of a single user. Click the picklist to select the desired User ID/Name.

Select the desired Enterprise Group — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Group 1,/2/3 and then click the picklist to select the desired group's ID/Name, to view authorization status of these applications.

Click the **View** button to view all pending, approved and rejected tour applications and their details.

Pending Applications

Click the **Pending** collapsible panel. The **Pending** section lists all the tour applications pending for approval by the reporting in-charge/SA as shown below.

When any application is in the Pending state it can be authorized by the Admin or RIC.

- To approve/reject applications selectively, click the respective application check box against the user.
- To approve/reject all the applications simultaneously, click the Approve /Reject checkbox in the header column.

Once the Admin approves/ rejects the application, the record will be moved from the **Pending** section to the **Approved/ Rejected** section respectively.

The default **Remark** for the Approved and Rejected application will appear in the respective fields. You can enter any customized Remark while authorizing the application.

Click the **Details**  icon to view the application details of the corresponding user.

Tour Application Detail window appears as shown below:

Tour Application Detail

User: U1, User1

Tour: TO, Tour-1

Application Details

Application Date: 18/06/2021

Half Day Consideration: Both

From Date: 23/06/2021, Full Day

To Date: 23/06/2021, Full Day

Applied Days: 1.0

Posted Days: 1.0

Reason: Official

Address: ATLADARA

Contact Number: 84569895565

Tour Document: Yes

Application Verdict: Approved

Verdict Date: 18/06/2021

Modification Application Details

Application Date: 18/06/2021

From Date: 23/06/2021, Full Day

To Date: 23/06/2021, Full Day

Reason: Applied Tour Modification

Tour Document: Yes

Approval Details

Incharge	Status	Remark
SA - System Admin	⊗	

Tour Application Detail window displays the user's tour application details.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remark displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.



The pending applications can not be authorized if the attendance period is closed while doing monthly attendance process and "Attendance Correction in Closed Period" check-box is disabled.

Even though; the period is closed but if "Attendance Correction in Closed Period" check-box in Policy is enabled then authorization can be made.

The **Auto generated Tour applications** will also be listed in Pending application if “Auto Authorize Location based Tour applications” is disabled from User Configuration > T&A > Attendance.

The screenshot shows the 'Tour Approval' window. At the top, there are filters: 'Show All Pending Applications' (radio button), 'Tour Date' (calendar icons), 'Filter Users' (dropdown set to 'All'), and 'Group/User' (ID and Name fields). A 'View' button is below these filters. Below the filters is a section titled 'Pending (1)' with a search bar. A table lists the pending application:

User	Name	From Date	To Date	Tour	Application Type	Application Date	Posted Days	Approve	Reject	Remark	Details
1	Chirag	27/06/2018	27/06/2018	Tour1	New	27/06/2018	1.0	<input type="checkbox"/>	<input type="checkbox"/>		

If the location from where the Tour is automatically applied is not available in Location master; then it can be added by clicking **Add this location** as shown below.

The screenshot shows the 'Tour Application Detail' window. It displays the following information:

- User: 1 (Chirag)
- Tour: TR (Tour1)
- Application Details**
 - Application Date: 27/06/2018
 - Half Day Consideration: Both
 - From Date: 27/06/2018 (Full Day)
 - To Date: 27/06/2018 (Full Day)
 - Applied Days: 1.0
 - Posted Days: 1.0
 - Reason: Auto Tour Application by System
 - Address:
 - Contact Number:
 - Location Details: GPS - (+22.2575, +073.1851)

At the bottom right, there is a button labeled 'Add this location'.

Approved Application

Click the **Approved** collapsible panel.

The **Approved** section displays all the tour/cancellation/modification applications that have been approved by the reporting group in-charge or the system administrator. Tour applications generated using the **Leave Management** module on COSEC Web will appear in this section by default as they are pre-approved.

The following screen displays the **Approved** section with approved tour application:

Pending (0)									
Approved (1)									
Search									
User ID ▲	Name	From Date	To Date	Tour	Application Date	Posted Days	Approve	Reject	Details
1687	Aditi Gupta	08/12/2017	08/12/2017	TOUR	03/12/2017	1.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<div>Remark</div> <div>Approved Tour</div>

To change the authorization verdict of any application, select **Reject** check box against the corresponding user. Once you reject an approved application, the record will be moved to the **Rejected** section.

Click the **Details**  icon to view the application details of the corresponding user.

Tour Application Detail window appears as shown below:

Tour Application Detail

User

U4

User4

Tour

TO

Tour-1

Application Details

Application Date

23/06/2021

Half Day Consideration

Both

From Date

24/06/2021

Full Day

To Date

25/06/2021

Full Day

Applied Days

2.0

Posted Days

2.0

Reason

Official

Address

12-A Pashabhai Park

Contact Number

8989562374

Tour Document


Yes

Approval Details

Incharge

SA - System Admin

Status

 (23/06/2021 09:43)

Remark

Approved Tour

Tour Application Detail window also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer ["Approval Policy"](#).

Remark displays the comments provided by the Admin / RIC / System.

Click **Save** to save the authorization.



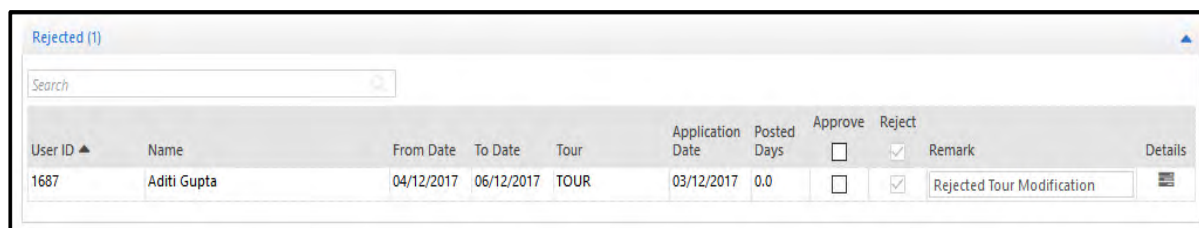
When system applies Auto Tour Application from location which is not configured as base location or not from base location group, and 'Auto Authorize Location Based Auto Tour Application' is enabled, then in detail page of such applications, Location Details will be displayed.


Rejected Application

Click the **Rejected** collapsible panel.

The **Rejected** section displays all the tour/cancellation/modification applications that have been rejected by the reporting group in-charge or the system administrator.

The following screen displays the **Rejected** section with rejected tour applications:



User ID ▲	Name	From Date	To Date	Tour	Application Date	Posted Days	Approve	Reject	Remark	Details
1687	Aditi Gupta	04/12/2017	06/12/2017	TOUR	03/12/2017	0.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Rejected Tour Modification	

To change the authorization verdict of any application, select the **Approve** check box against the corresponding user.

Once you approve a rejected application, the record will be moved to the **Approved** section.

Click the **Details**  icon to view the application details of the corresponding user.

Tour Application Detail window appears as shown below:

Tour Application Detail

User: U1 User1

Tour: TO Tour-1

Application Details

Application Date: 18/06/2021

Half Day Consideration: Both

From Date: 23/06/2021 Full Day

To Date: 23/06/2021 Full Day

Applied Days: 1.0

Posted Days: 0.0

Reason: Official

Address: ATLADARA

Contact Number: 84569895565

Tour Document: Yes

Application Verdict: Rejected

Verdict Date: 18/06/2021

Modification Application Details

Application Date: 18/06/2021

From Date: 23/06/2021 Full Day

To Date: 23/06/2021 Full Day

Reason: Applied Tour Modification

Tour Document: Yes

Approval Details (X)

Incharge	Status	Remark
SA - System Admin	(X) (18/06/2021 18:43)	Rejected Tour

Tour Application Detail window displays the tour application details.

Tour Application Detail window also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer ["Approval Policy"](#).

Remarks displays the comments provided by the Admin / RIC / System.

Click **Save** button to save the changes.



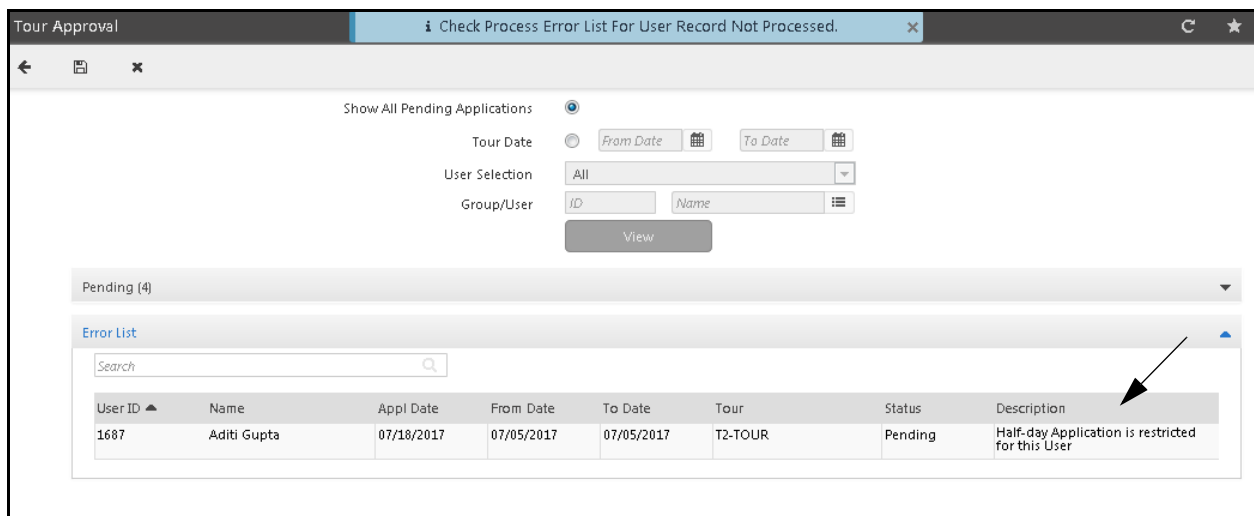
System Administrator can delete pending/approved/rejected application.

Half Day Restriction on posted days

On the Tour Approval page, **Half Day restriction on posted days** feature restricts the administrator to approve the posted half day Tour application for that particular user.

Consider a scenario where the user has applied for the half day tour from the ESS login page and the Application has been sent for approval to the administrator.

Suppose after posting the half day tour application, **Restrict Half Day Considerations** has been enabled in the page User > User configuration > T&A for that particular user. Now when the Administrator will try to approve the Tour Application for that user, then it will show the error in the Error List that “Half-day Application is restricted for this User” as shown in the screen below.



The screenshot displays the 'Tour Approval' interface. At the top, a blue notification bar states 'Check Process Error List For User Record Not Processed.' Below this, there are filters for 'Show All Pending Applications' (selected), 'Tour Date' (From Date and To Date), 'User Selection' (All), and 'Group/User' (ID and Name). A 'View' button is present. Below the filters, a dropdown menu shows 'Pending (4)'. Underneath, the 'Error List' section contains a search bar and a table with one entry. An arrow points to the 'Description' column of this entry.

User ID	Name	Appl Date	From Date	To Date	Tour	Status	Description
1687	Aditi Gupta	07/18/2017	07/05/2017	07/05/2017	T2-TOUR	Pending	Half-day Application is restricted for this User

C-OFF Application/Approval

An employee who has accumulated C-OFF hours often needs to use these within a validity period. C-OFF Application is a formal way of requesting a Complimentary-Off. The application process for C-OFF on COSEC Web is however, distinguished from the application process for other leave types, though both follow a similar functioning. The Application and Approval rights for a C-OFF are similar to those for a leave application. For a better understanding of C-OFF Application and Approval, also refer to [“Leave Application/Approval”](#).

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to [“Reporting In-Charge”](#), [“Approval Policy”](#) and [“Configuring Users”](#).

Applying for a C-OFF

This section describes how to apply for a C-OFF using the Leave Management module.

To do this, go to the **Leave Management module > Application/Approval > C-OFF Application** and the following screen appears.

The page displays configurations on the left hand side and to the right is the attendance details of the user along with all the C-OFF application details of a particular user for a particular month. It also displays the number of C-OFFs availed, total absent days, total C-OFFs pending, approved and rejected.

To apply a C-OFF for a user, click **New** button.

User: Select the user for whom the C-OFF is to be applied.

From Date: Select the starting date for the C-OFF using the date selection button and specify whether the C-OFF is to be considered for FullDay or start only from the Second Half.

To Date: Select the end date for the C-OFF using the date selection button and specify whether the C-OFF is to be considered for FullDay or end right after the First Half.



For a particular user, if **Restrict Half Day Considerations** is enabled in the page **User > User configuration > T&A**, then in **From/To Date** only full day attendance options will be visible and all the other half day options will be disabled for that particular user as shown in the screen below.

Applied Days: The system automatically calculates the number of days the C-OFF has been applied for.

Posted Days: The posted days are the number of working days posted between the C-OFF applied. It will be automatically calculated by the system after saving the application. E.g. If a C-OFF is applied for 3 days from 29th October to 31st October and there is a week off in the middle, then posted days will be 2 days only as only the actual working days are considered for C-OFF and not the week off i.e. 30th October.



The minimum C-OFF balance (in hours) required for taking a half day or full day off is determined during C-OFF Policy configuration. To know more about this, refer to [“C-OFF Policy”](#).

While considering Half day application, the value for “Minimum allowed at a time” and “Maximum Allowed Limit” for the leave type is also checked.



To know more about how to create a C-OFF type leave, refer to [“Configuring Leaves”](#).

- **Leave:** Select the type of leave to be applied from the dropdown list. This list displays all C-OFFs defined on the system.
- **Current Balance:** The system automatically retrieves and displays the current balance of C-OFF type leave.
- **Required Balance:** Once the leave is selected, the system retrieves and displays the balance required for applying leave. The user can successfully apply for a C-OFF only if the required balance for leave is lesser than or equal to the current C-OFF hours balance. For e.g., in the following figure, the user has sufficient C-OFF hours balance to apply for 2 days leave which requires a minimum of 18 hours C-OFF as per C-


OFF policy. In such a scenario the system will allow the C-OFF application to be made. If the balance is less then the system application will not allow to apply for C-OFF.

- **Selected C-OFF For Application:** You can select the C-OFF to be applied using the picklist, if the available C-OFF balance of a user is more than the required balance. The number of C-OFF hours which are to be selected for conversion can be entered in the picklist Leave Balance Detail pop-window as shown in the screen below. Enter the value and click **Select** button, the value appears on the main screen.

Attendance Date	Available C-OFF	Select C-OFF
29/10/2016	28:00	08:00


Reason and Contact Info

- **Reason:** Enter reason for requesting C-Off leave.
- **Address:** Provide address of the user for whom the C-Off application is being made.
- **Contact Number:** Provide the contact number of the user for whom the C-Off application is being made.
- **Medical Certificate Available:** Select the checkbox to make it mandatory for the applicant to produce a medical certificate as a proof to testify the reason behind the current C-Off.


Select this checkbox if you have a Medical Certificate as a proof and reason for the current leave. To upload this certificate, click on the **Upload**  button.

Select the desired file as per the supported formats (.jpg, .bmp, .png, .pdf) and size.


Click **Update**.

The document will be uploaded and can be previewed by clicking on **Preview**  button.


Click the **Submit** button to apply for the C-OFF. If applied successfully, the **Application Status** for the C-OFF will be updated to "Approved".

Click **Details**  icon from the grid available on the left side of the page to view the Approval Details of the already applied application.

May 2021



Jul 2021



3.5 days Absent

1 Pending

0 Approved





1 Rejected

Application Details

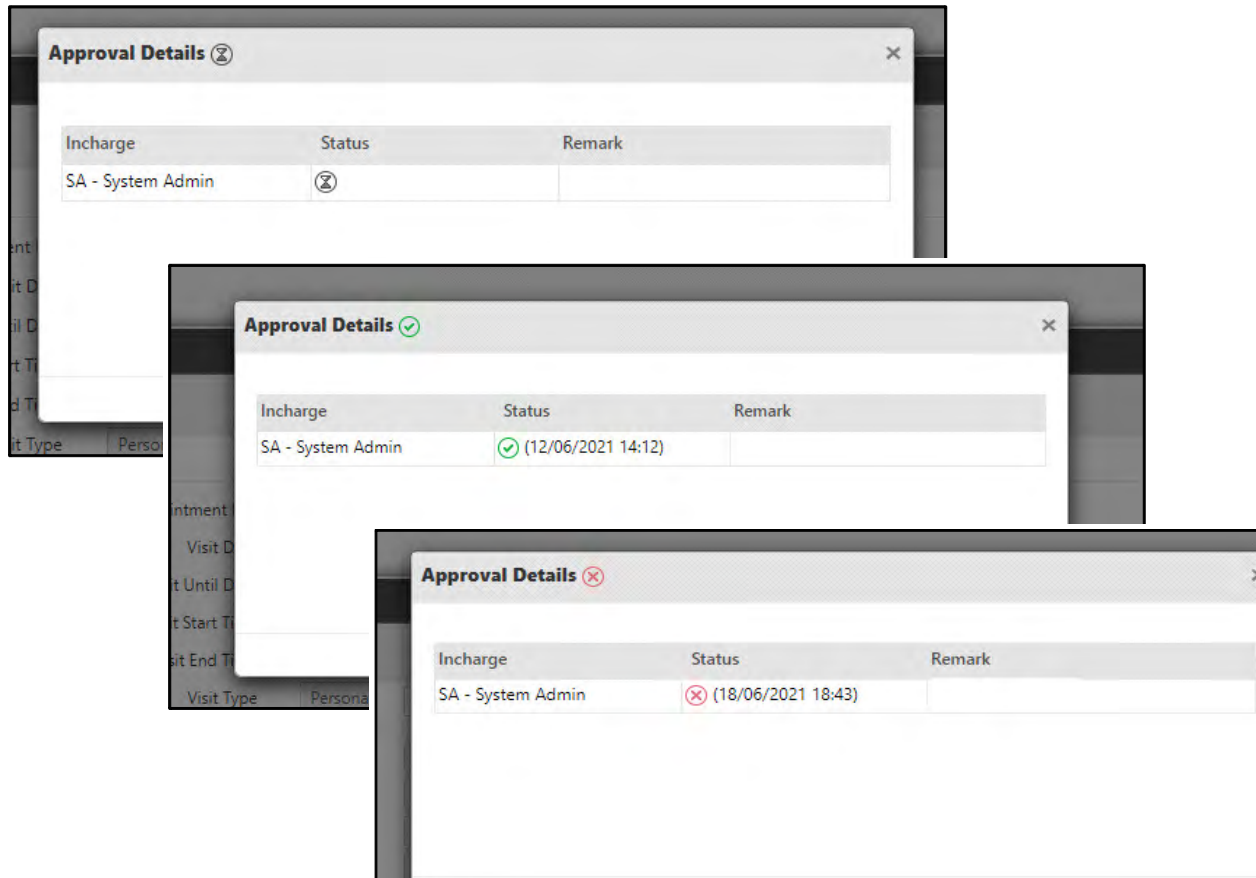
▼

Show All

▼

From ▼	To	Leave	Application Date	Application Type	Status	Approval Details
23/06/2021	23/06/2021	CF	23/06/2021	New		
09/06/2021	09/06/2021	CF	23/06/2021	New		

Approval Details window appears as shown below:



It displays the status of the user's application under **Approval Details**, that is, whether it is — pending, approved or rejected.

The application's status is displayed in the **Status** column as Pending ⌚ , Approved ✓ or Rejected ✗ .

Remark displays the comments provided by the Admin/ RIC/ System.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer [“Approval Policy”](#).

C-OFF Approval

The system administrator can view, approve or reject C-OFFs that have been applied for by any ESS user. The administrator also has the right to reject any pre-approved leaves and vice-versa, if required.

To access this functionality, go to the **Leave Management module > Application/Approval > C-OFF Approval** and the following screen appears.

User ID	Name	From Date	To Date	C-OFF	Application Type	Application Date	Posted Days	Approve	Reject	Remark	Details
15	TEst-bug	04/07/2017	04/07/2017	CO	New	07/07/2017	1.0	<input type="checkbox"/>	<input type="checkbox"/>		
16	Bug1-test	02/08/2017	02/08/2017	CO	New	29/08/2017	1.0	<input type="checkbox"/>	<input type="checkbox"/>		
1687	Aditi Gupta	12/12/2017	12/12/2017	cofff	New	03/12/2017	1.0	<input type="checkbox"/>	<input type="checkbox"/>		
1687	Aditi Gupta	04/07/2017	04/07/2017	CO	New	18/07/2017	0.5	<input type="checkbox"/>	<input type="checkbox"/>		
25	new club user 18 aug 1-2	03/09/2017	03/09/2017	CO	New	25/09/2017	0.0	<input type="checkbox"/>	<input type="checkbox"/>		

You can either:

- view all the pending C-OFF Approval Applications
- set the filters — Date, Filter Users — to view the desired applications

All Pending Applications

To view only Pending Applications,

By default, the Admin can view all pending C-OFF applications from the last one month period. However, sometimes users may also apply for tours on future dates.

- **Show All Pending Applications:** Select this option to enable the pending application filter. You can view all pending C-OFF applications, including those made for future dates.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To know more, refer to [“Pending Applications”](#).

Applications according to Set Filters

To Set the Filters,

- **C-OFF Date:** Select and specify the start and end dates using the calendar buttons to define the period for which C-OFF approval status is to be viewed.

- **Filter Users:** You can filter records according to the desired Enterprise Group, All or for an Individual.

Select **All**, to view authorization status of the applications of all the active users on the system.

Select **Individual**, to view authorization status of the applications of a single user. Click the picklist to select the desired User ID/Name.

Select the desired Enterprise Group — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Group 1,/2/3 and then click the picklist to select the desired group's ID/Name, to view authorization status of these applications.

Click the **View** button and all the pending, approved and rejected C-OFF applications along with their details gets displayed in the grid.

Pending Applications

Click the **Pending** collapsible panel.

The **Pending** section lists all the C-OFF /cancellation applications waiting to be sanctioned by the reporting in-charge or HR administrator as shown.

Pending (24)											
Search											
User ID ▲	Name	From Date	To Date	C-OFF	Application Type	Application Date	Posted Days	Approve	Reject	Remark	Details
15	TEst-bug	04/07/2017	04/07/2017	CO	New	07/07/2017	1.0	<input type="checkbox"/>	<input type="checkbox"/>		
16	Bug1-test	02/08/2017	02/08/2017	CO	New	29/08/2017	1.0	<input type="checkbox"/>	<input type="checkbox"/>		
1687	Aditi Gupta	12/12/2017	12/12/2017	cofff	New	03/12/2017	1.0	<input type="checkbox"/>	<input type="checkbox"/>		
1687	Aditi Gupta	04/07/2017	04/07/2017	CO	New	18/07/2017	0.5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved C-OFF for half day	
25	new club user 18 aug 1-2	03/09/2017	03/09/2017	CO	New	25/09/2017	0.0	<input type="checkbox"/>	<input type="checkbox"/>		

1 - 5 of 24 records


« < 1 2 3 4 5 > »

When any application is in the Pending state it can be authorized by the Admin or RIC.

- To approve/reject applications selectively, click the respective application check box against the user.
- To approve/reject all the applications simultaneously, click the Approve /Reject checkbox in the header column.

Once the Admin approves/ rejects the application, the record will be moved from the **Pending** section to the **Approved/ Rejected** section respectively.

The default **Remark** for the Approved and Rejected application will appear in the respective fields. You can enter any customized Remark while authorizing the application.

Click the **Details**  icon to view the application details of the applied C-OFF.

C-OFF Application Detail window appears as shown below:

C-OFF Application Detail

User: U1 User1

C-OFF: CO COFF

Application Details

Application Date: 17/06/2021

Half Day Consideration: Both

From Date: 15/06/2021 Full Day

To Date: 17/06/2021 Full Day

Applied Days: 3.0

Posted Days: 3.0

Reason: Personal

Address:

Contact Number:

Medical Certificate: No

Approval Details

Incharge	Status	Remark
SA - System Admin		

C-OFF Application Detail window displays the user's application details.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remark displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.



The pending applications can not be authorized if the attendance period is closed while doing monthly attendance process and "Attendance Correction in Closed Period" checkbox is disabled from Time and Attendance> Policies> Attendance Policy> Event Authorization.

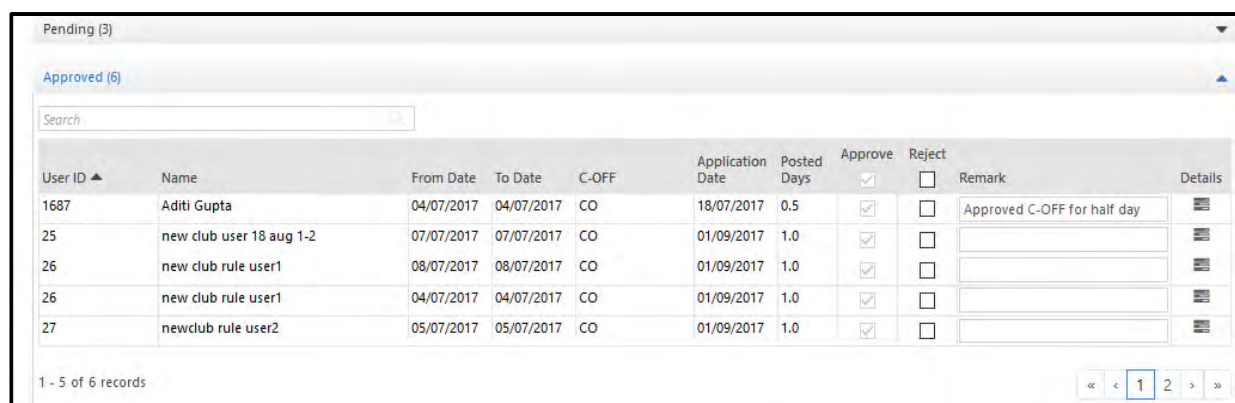
Even though; the period is closed but if "Attendance Correction in Closed Period" checkbox in Policy is enabled then authorization can be made.

Approved Application

Click the **Approved** collapsible panel.

The **Approved** section displays all the C-OFF/cancellation applications that have been approved by the reporting group in-charge or the system administrator. C-OFF applications generated using the **Leave Management** module on COSEC Web will appear in this section by default as they are pre-approved.

The following screen displays the **Approved** section with approved C-OFF applications:



The screenshot shows a web interface with a 'Pending (3)' tab and an 'Approved (6)' tab. Below the tabs is a search bar. The main area contains a table with the following columns: User ID, Name, From Date, To Date, C-OFF, Application Date, Posted Days, Approve, Reject, Remark, and Details. The table lists five records. The first record is for User ID 1687, Aditi Gupta, with a C-OFF of CO, Application Date 18/07/2017, and Posted Days 0.5. The remaining four records are for new club rule users with C-OFF of CO and Application Dates ranging from 01/09/2017 to 01/09/2017. Each record has an 'Approve' checkbox checked and a 'Reject' checkbox unchecked. The 'Remark' column contains 'Approved C-OFF for half day' for the first record and is empty for the others. The 'Details' column contains a magnifying glass icon for each record. At the bottom, it says '1 - 5 of 6 records' and has a pagination control showing '1' selected.

User ID	Name	From Date	To Date	C-OFF	Application Date	Posted Days	Approve	Reject	Remark	Details
1687	Aditi Gupta	04/07/2017	04/07/2017	CO	18/07/2017	0.5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved C-OFF for half day	
25	new club user 18 aug 1-2	07/07/2017	07/07/2017	CO	01/09/2017	1.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
26	new club rule user1	08/07/2017	08/07/2017	CO	01/09/2017	1.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
26	new club rule user1	04/07/2017	04/07/2017	CO	01/09/2017	1.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
27	newclub rule user2	05/07/2017	05/07/2017	CO	01/09/2017	1.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>		

To change the authorization verdict of any application, select **Reject** check box against the corresponding user. Once you reject an approved application, the record will be moved to the **Rejected** section.

Click the **Details**  icon to view the application details of the corresponding user.

C-OFF Application Detail window appears as shown below:

C-OFF Application Detail

User: U1 User1

C-OFF: CO COFF

Application Details

Application Date: 17/06/2021

Half Day Consideration: Both

From Date: 15/06/2021 Full Day

To Date: 17/06/2021 Full Day

Applied Days: 3.0

Posted Days: 3.0

Reason: Personal

Address:

Contact Number:

Medical Certificate: No

Approval Details ✓

Incharge	Status	Remark
SA - System Admin	✓ (18/06/2021 13:40)	Approved C-OFF

C-OFF Application Detail window displays the user's application details.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer ["Approval Policy"](#).

Remark displays the comments provided by the Admin / RIC / System.

Click **Save** to save the authorization.

Rejected Application

Click the **Rejected** collapsible panel.

The **Rejected** section displays all the C-OFF/cancellation applications that have been rejected by the reporting group in-charge or the system administrator.

The following screen displays the **Rejected** section with rejected leave applications:

Pending (3)

Approved (6)

Rejected (1)

Search

User ID ▲	Name	From Date	To Date	C-OFF	Application Date	Posted Days	Approve	Reject	Remark	Details
1687	Aditi Gupta	04/07/2017	04/07/2017	CO	18/07/2017	0.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

Click the **Details**  icon to view the application details of the corresponding user.

C-OFF Application Detail window appears as shown below:

C-OFF Application Detail

User: U1 User1

C-OFF: CO COFF

Application Details

Application Date: 17/06/2021

Half Day Consideration: Both

From Date: 15/06/2021 Full Day

To Date: 17/06/2021 Full Day

Applied Days: 3.0

Posted Days: 3.0

Reason: Personal

Address:

Contact Number:

Medical Certificate: No

Approval Details (X)

Incharge	Status	Remark
SA - System Admin	(X) (10/06/2021 17:41)	

C-OFF Application Detail window displays the user's application details.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer ["Approval Policy"](#).

Remarks displays the comments provided by the Admin / RIC / System.

Click **Save** button to save the changes.



System Administrator can delete pending/approved/rejected application.

Half Day Restriction on posted days

On the C-OFF Approval page, **Half Day restriction on posted days** feature restricts the administrator to approve the posted half day C-OFF application for that particular user.

Consider a scenario where the user has applied for the half day tour from the ESS login page and the Application has been sent for approval to the administrator.

Suppose after posting the half day tour application, **Restrict Half Day Considerations** has been enabled in the page User > User configuration > T&A for that particular user. Now when the Administrator will try to approve the C-OFF Application for that user, then it will show the error in the Error List that “Half-day Application is restricted for this User” as shown in the screen below.

The screenshot shows the 'C-OFF Approval' interface. At the top, there is a message bar that says 'Check Process Error List For User Record Not Processed.' Below this, there are filters for 'Show All Pending Applications', 'C-OFF Date' (with 'From Date' and 'To Date' date pickers), 'User Selection' (set to 'All'), and 'Group/User' (with 'ID' and 'Name' search boxes). A 'View' button is present. Below the filters, a dropdown menu shows 'Pending (5)'. Underneath, there is an 'Error List' section with a search bar. A table displays the error details:

User ID	Name	Appl Date	From Date	To Date	C-OFF	Status	Description
1687	Aditi Gupta	07/18/2017	07/04/2017	07/04/2017	CO-CO	Pending	Half-day Application is restricted for this User

An arrow points to the 'Description' column of the error list.

Leave Balance

This functionality enables the system administrator to view the leave balance details for a particular user for a particular attendance period.

To view leave balance for a user, go to the **Leave Management module > View > Leave Balance** and the following screen appears.

The screenshot shows the 'Leave Balance' screen with the following filters: User ID (ID), Name, Period (Monthly), and Balance Month-Year (March, 2017). A search field is present. The table below the filters is empty, displaying 'No Data'. The table headers are: Year, Month, Code, Name, Opening, Credit, Debit, Encashment, Availed, Closing, and Overflow. A 'C-OFF' section is visible at the bottom.

- **User ID:** Select a User from the user picklist for whom the leave balance is to be viewed.
- **Period:** Specify the period as Month and Year for which the balance is to be viewed.
- **Balance:** For Monthly Period, select the Month and Year for which balance is to be viewed. For Yearly Period select the year to view the yearly balance.

The Leave and C-OFF Balance details appears on your screen as shown below. You can also search for a particular record by using the **Search** field.

The screenshot shows the 'Leave Balance' screen with the following filters: User ID (1), Name (Shalini), Period (Yearly), and Balance Year (2017). A search field is present. The table below the filters displays data for 2017. The table headers are: Year, Code, Name, Opening, Credit, Debit, Encashment, Availed, Closing, and Overflow. The data rows are:

Year	Code	Name	Opening	Credit	Debit	Encashment	Availed	Closing	Overflow
2017	PL	Paid Leave	0.00	20.00	0.00	0.00	1.50	18.50	0.00
2017	SL	Sick Leave	0.00	10.00	0.00	0.00	0.00	10.00	0.00

A 'C-OFF' section is visible at the bottom.

To view C-OFF balance for the selected user, select the **C-OFF** section. The details of the selected user's C-OFF balance, such as validity period, total hours and available C-OFF details will be displayed as follows:

Leave Balance

←

User ID

4

Sweta

☰

Leaves

C-OFF

Validity Period

01/14/2017

03/14/2017

Total Hours

02:00

Available C-OFF Details

Search

🔍

Date ▲	Authorized	Manual Credit	Manual Debit	Encashed	Availed	Available
02/20/2017		02:00				02:00

Leave Balance

←

User ID

NP

Nisha

☰

Leaves

C-OFF

Validity Period

11/03/2017

11/05/2017

Total Hours

02:00

Available C-OFF Details

Search

🔍

Date ▲	Authorized	Manual Credit	Manual Debit	Encashed	Availed	Available
02/05/2017	02:00					02:00

Leave Balance Process

Leave Balance Process generates the leave balance records of the user till selected month year.

Suppose if organization's policy is of yearly leave crediting and user does not avail leave for first 4 months. In such scenario leave balance record for only start month of the year is available in Database. If user visits leave application page/leave balance view page then no data is shown as record is not available for corresponding month.

So you must run the Leave Balance Process to update the details.

To process the leave balance for a user, Select the **Leave Management module >Process > Leave Balance Process**

The **Leave Balance Process** page appears on your screen as follows:

Leave Management

Leave Balance Process

Balance Month-Year * April 2017

Select Users User Wise

User * ID Name

Search

User ID 1320 Name SHRUTI SAGAR PATKI

Process

Select the **Balance Month-Year** upto which the leave balance is to be processed to view the available balance of leaves.

Select the **user** by filtering the options of User Wise, Group Wise or All for whom the leave balance process is to be run.

Click on **Process** button to execute the process.

The Leave Balance details can be viewed from Leave Management module> View > Leave Balance as shown below.

Leave Balance

User ID 1320 SHRUTI SAGAR PATKI

Leaves

Period Monthly

Balance Month-Year April 2017

Search

Year	Month	Code	Name	Opening	Credit	Debit	Encashment	Availed	Closing	Overflow
2017	Apr	CL	cl	45.00					45.00	0.00
2017	Apr	KL	KLL	0.00					0.00	0.00
2017	Apr	LP	PAID LL	0.00					0.00	0.00
2017	Apr	PL	Paid Leave	0.00					0.00	0.00
2017	Apr	PM	pm	0.00					0.00	0.00

1 - 5 of 7 records

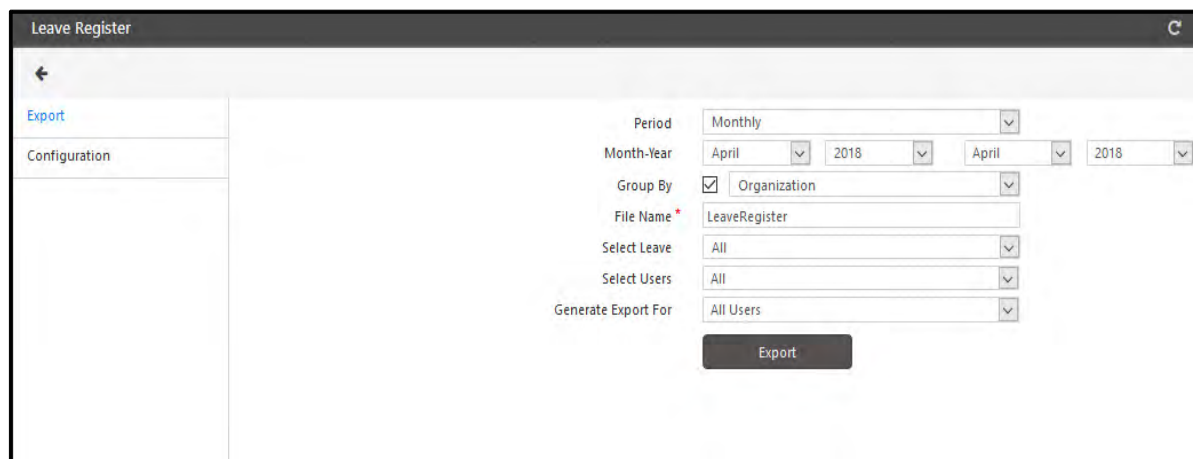
C-OFF

Leave Register Export

To export the records of leave select **Leave Management module > Exports > Leave Register**.

Export

The **Leave Register** page appears as shown below:

The screenshot shows a web application window titled "Leave Register". On the left is a sidebar with a back arrow icon and two menu items: "Export" (highlighted in blue) and "Configuration". The main area contains a form for configuring the export. The form includes the following fields: "Period" (a dropdown menu set to "Monthly"), "Month-Year" (two dropdown menus for month and year, both set to "April" and "2018" respectively), "Group By" (a checkbox that is checked, followed by a dropdown menu set to "Organization"), "File Name*" (a text input field containing "LeaveRegister"), "Select Leave" (a dropdown menu set to "All"), "Select Users" (a dropdown menu set to "All"), and "Generate Export For" (a dropdown menu set to "All Users"). At the bottom of the form is a dark "Export" button.

Before Exporting you can do **"Configuration"** for the Export parameters.

Period: Specify the Period as Monthly or Yearly for which the leave records for user is to be exported.

Month-Year: Specify the **Month-Year** (for Monthly period) or **Year** (for Yearly period) for which the leave is to be exported.

Group By: Enable the Group By checkbox and select the Enterprise group to export data by grouping them with the Enterprise Group for which the leave is to be exported.

File Name: Enter the name of the file to be exported.

Select Leave: Select the option as **All** or **Selected** for selecting the leaves. For Selected option; select the leaves from the picklist.

Select Users: Select the user based on filter options of User Wise, Group Wise or All.

Leave Register

Export

Configuration

Period: Monthly

Month-Year: April 2018

Group By: ☒ Organization

File Name: LeaveRegister

Select Leave: Selected

Leave: ID, Name (2 Leave(s) Selected)

Select Users: User Wise

User: ID, Name

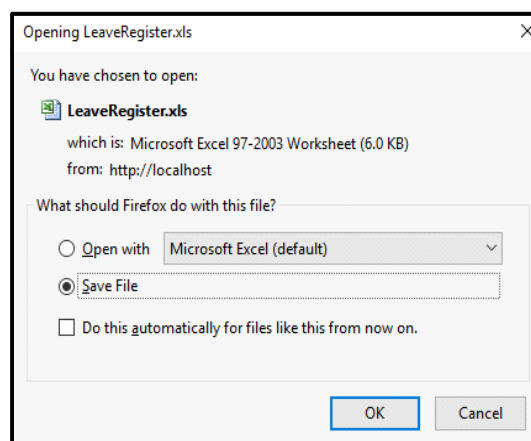
Search

User ID	Name
1687	Aditi Ajay Gupta_Ahmedabad
101	Khushbu

Generate Export For: All Users

Export

Click on **Export** button. You can open or Save the exported file.



The Leave Register will be exported as shown below.

User ID	Name	Leave Code	Leave Name	Month	Year	Opening Bal	Credit	Debit	Encashed	Available	Closing Bal
101	Khushbu	PL	Paid Leave	Apr	2018	0.00	10.00	0.00	0.00	0.0	10.00
101	Khushbu	SL	Sick Leave	Apr	2018	0.00	8.00	0.00	0.00	0.0	8.00
1687	Aditi Ajay	PL	Paid Leave	Apr	2018	0.00	10.00	0.00	0.00	0.0	10.00
1687	Aditi Ajay	SL	Sick Leave	Apr	2018	0.00	8.00	0.00	0.00	0.0	8.00

Configuration

In Configuration tab, select the check-boxes for the fields to be exported in Leave register. To export the Enterprise group details in export sheet, you must select the desired enterprise code and/ enterprise name checkboxes.

The screenshot shows the 'Leave Register' configuration window. On the left is a sidebar with 'Export' and 'Configuration' tabs, where 'Configuration' is selected. The main area is titled 'Select Fields to Export' and contains a search bar and a table of fields with checkboxes for selection.

Fields	
User ID	<input checked="" type="checkbox"/>
User Name	<input checked="" type="checkbox"/>
Reference ID	<input type="checkbox"/>
Field 1	<input type="checkbox"/>
Field 2	<input type="checkbox"/>

Below the table, it says '1 - 5 of 37 records'. At the bottom right, there is a 'Save' button and a pagination control showing '1' as the current page.

Click on **Save** to save the configuration. Now you can export the leave register from "Export" tab.

Leave Reports

The COSEC Leave Management module allows you to create and view an assortment of detailed and focused reports related to the leave management system. These reports can be viewed on the screen or printed at any time. The following *Leave Reports* can be generated using the **Reports** section under the **Leave Management** module:

- "Leave"
- "Leave Group"
- "Leave Application"
- "Leave Encashment"
- "Leave Credit/Debit"
- "Leave Register"
- "COFF Register"
- "Monthly Leave Details"
- "Statutory Leave Reports"

Leave

View a detailed listing of all leaves configured on the system as shown below.

Run by: System Admin

ORGANISATION 1.
Leave

Date: 29/09/2014 16:22

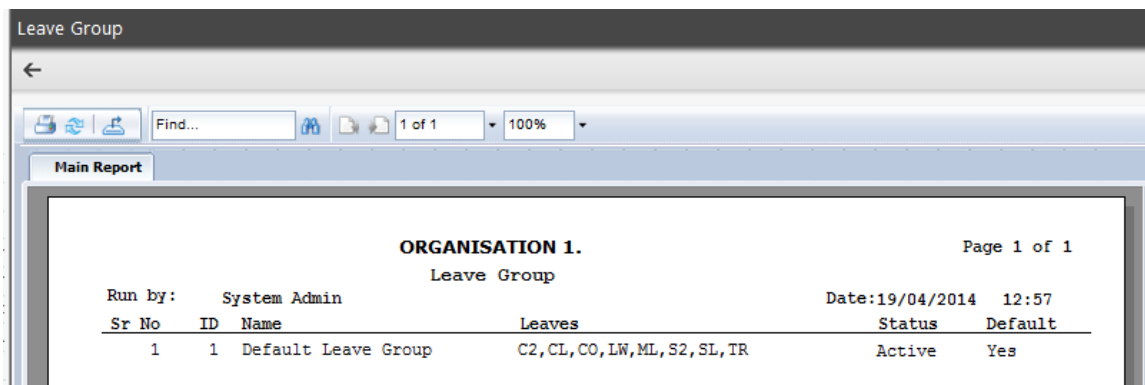
Page 1 of 1

Code	Name	Max LV	Min LV	Type	Bal Chk	Bal Ded	CF From	Ratio	Other	With	Not Allow	WO	PH	ENC	Min Bal Req	Max Bal Aft	Max Bal Acc	Max Bal CF	Max Bal Limit
C2	C-OFF2	99.0	0.0	C	Y	N		0.0	Y			Y	Y	Y	Y	0.00	N	0.00	
CL	CASUAL LEAVE	99.0	0.0	P	Y	N		0.0	Y			Y	Y	Y	Y	0.00	N	0.00	
CO	C-OFF	2.0	0.5	P	Y	N		0.0	Y			Y	Y	Y	N	0.00	N	0.00	N
LW	LEAVE WITHOUT PAY	99.0	0.0	A	N	N		0.0	Y			Y	Y	Y	N	0.00	N	0.00	N
ML	MATERNITY LEAVE	999.0	0.0	P	N	N		0.0	Y			Y	Y	Y	N	0.00	N	0.00	
PL	PRIVILEGE LEAVE	99.0	0.0	P	N	N		0.0	Y			Y	Y	Y	N	0.00	N	0.00	N
TR	TOUR	99.0	0.0	T	N	N		0.0	Y			Y	Y	Y	N	0.00	N	0.00	

- It shows **Max LV**-Max allowed limit for leave and **Min LV**-Min allowed leave at a time.
- The type of leave is shown as **C** for C-Off, **P** for Paid leave, **L** for Lay off type leave, **A** for Un-paid leave, **R** for Restricted leave and **T** for Tour.
- **Bal Chk** column shows whether the leave balance is checked(Y) or not (N). And **Allw with Other** shows whether the leave can be clubbed with other leave or not.
- **ENC Allw** shows the leave which can be encashed and **Min Bal Req Aft ENC** shows the minimum balance of leaves required after encashment.
- **Max Acc Bal** shows maximum available balance of the leave.

Leave Group

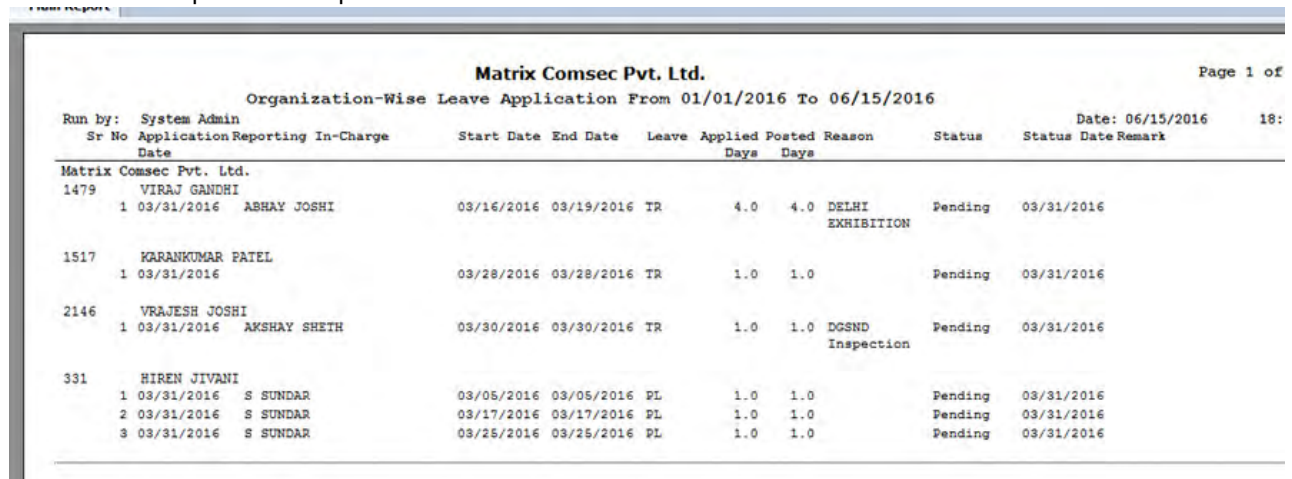
View a detailed listing of all leave groups configured on the system and the leaves grouped under them.



Sr No	ID	Name	Leaves	Status	Default
1	1	Default Leave Group	C2,CL,CO,LW,ML,S2,SL,TR	Active	Yes

Leave Application

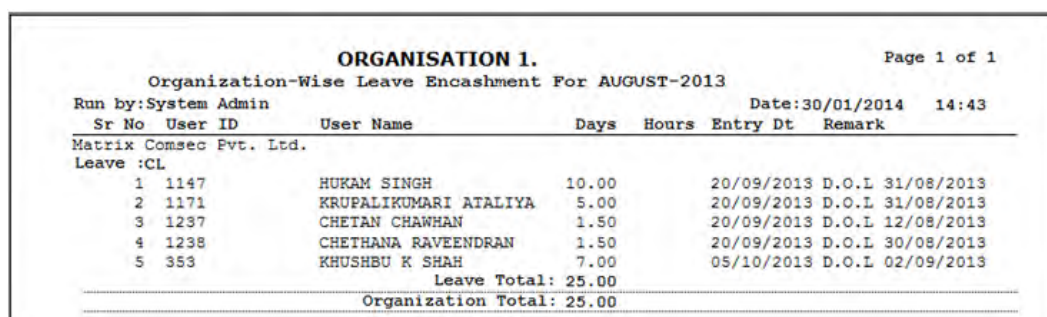
This report generates a detailed listing of leave applications made during the specified date range. The figure below illustrates a sample for this report. The filter such as User/Date and Leave/Tour-wise can be used.



Sr No	Application Date	Reporting In-Charge	Start Date	End Date	Leave Type	Applied Days	Posted Days	Reason	Status	Status Date	Remark
1479	03/31/2016	ASHAY JOSHI	03/16/2016	03/19/2016	TR	4.0	4.0	DELHI EXHIBITION	Pending	03/31/2016	
1517	03/31/2016	KARANKUMAR PATEL	03/28/2016	03/28/2016	TR	1.0	1.0		Pending	03/31/2016	
2146	03/31/2016	AKSHAY SHETH	03/30/2016	03/30/2016	TR	1.0	1.0	DGSND Inspection	Pending	03/31/2016	
331	03/31/2016	S SUNDAR	03/05/2016	03/05/2016	PL	1.0	1.0		Pending	03/31/2016	
	03/31/2016	S SUNDAR	03/17/2016	03/17/2016	PL	1.0	1.0		Pending	03/31/2016	
	03/31/2016	S SUNDAR	03/25/2016	03/25/2016	PL	1.0	1.0		Pending	03/31/2016	

Leave Encashment

View a detailed listing of group-wise leave encashment for users over the specified period as shown in the sample report below.



Sr No	User ID	User Name	Days	Hours	Entry Dt	Remark
1	1147	HUKAM SINGH	10.00		20/09/2013	D.O.L 31/08/2013
2	1171	KRUPALIKUMARI ATALIYA	5.00		20/09/2013	D.O.L 31/08/2013
3	1237	CHETAN CHAWHAN	1.50		20/09/2013	D.O.L 12/08/2013
4	1238	CHEETHANA RAVEENDRAN	1.50		20/09/2013	D.O.L 30/08/2013
5	353	KHUSHBU K SHAH	7.00		05/10/2013	D.O.L 02/09/2013
Leave Total:			25.00			
Organization Total:			25.00			

Leave Credit/Debit

Gives a detailed group-wise listing of all leaves credited or debited from the leave balance of the employees.

Leave Register

Gives a user-wise listing of all leave details of employees for the specified date range as shown.

Matrix Comsec Pvt. Ltd.							Page 1 of 172
Leave Register From JANUARY-2016 To JUNE-2016							
Run by: System Admin		Date: 06/15/2016 18:51					
Year	Month	Opening Bal	Credit	Debit	Encashed	Availed	Closing Bal
Matrix Comsec Pvt. Ltd.							
1-SALIM ANSARI							
CL - CASUAL LEAVE							
2016	JAN	0.00					0.00
2016	FEB	0.00					0.00
2016	MAR	0.00					0.00
CO - C-off							
2016	JAN	0.00					0.00
2016	FEB	0.00					0.00
2016	MAR	0.00					0.00
ML - MATERNITY LEAVE							
2016	JAN	0.00					0.00
2016	FEB	0.00					0.00
2016	MAR	0.00					0.00
PL - PAID LEAVE							
2016	JAN	0.00	2.50	0.00	0.00	0.0	2.50
2016	FEB	2.50	2.50	0.00	0.00	1.0	4.00
2016	MAR	4.00	3.50	0.00	0.00	1.5	6.00
10-RAJENDRA GOSWAMI							
CL - CASUAL LEAVE							
2016	JAN	0.00					0.00
2016	FEB	0.00					0.00
2016	MAR	0.00					0.00

COFF Register

Gives a user-wise listing of all Complimentary-Off details of employees for the specified date range.

Monthly Leave Details

Gives month and enterprise-group-wise details of dates on which approved leave applications exist for specified users and selected leave types or tours.

Statutory Leave Reports

Generates annual leave transaction reports **Form B**, **Form 15** and **Form Q** as per statutory norms (see sample reports below).

Form B

Form B		REGISTER OF				See Rule 7 (2)	
National Festival Holidays, Casual & Sick Leave							
[Under the Punjab Industrial Establishment (National, Festival, Casual & Sick Leave) Rules, 1995]							
Name		Sanjay P. Shah		For The Year:		2014	
Father/Spouse's Name:		Late. Motilal		Whether Covered By The Employee's		State Insurance Scheme - Yes/No	
Date Of Joining Service:		May-30-2011					

1	2			3			4	5
Serial No.	No. Of National Festival Holidays/Casual/Sick Leave Due At The Beginning Of The Year			Period For Which National Festival Holidays/Casual/Sick Leave Applied For			Whether Granted Or Refused	Remarks
	Festival	Casual	Sick	From	TO	Kind Of Leave		
3	9.0	30.0	0.0					
		0.0	0.0	01-07-2014	01-07-2014	CO		
				01-14-2014	01-15-2014	PH		
				01-17-2014	01-17-2014	TR		
				01-18-2014	01-18-2014	PH		
		29.0	0.0	01-20-2014	01-20-2014	PL		
		28.0	0.0	01-21-2014	01-21-2014	PL		
				01-24-2014	01-24-2014	TR		
				01-27-2014	01-27-2014	TR		

Form 15

Form No. 15		Register Of Leave With Wages															
		Name Of Factory: Shreeram Mills															
Serial No:		1		Name:		Jameer Ahmed											
Department:		Repairing		Father/Spouse's Name:													
Serial No In the Register:		10		Date Of Discharge:													
Date Of Joining Service:		Oct-31-92		Date & Amount Of Pay Due:													

Calendar Year Of Service	Wages during From... To...	Wages Earned During The Wages Period	No. of days worked during the calendar year					Leave to credit			Whether Leave In Accordance With Scheme Under Section 49 (8) Was Refused	Leave Enjoyed		Balance Of Leave To Credit	Normal Rate Of Wages	Cash Equivalent Of Advantages Occurring Through Conversion Of Fixed Grant And Other	Date Of Wages For The Leave Passed (Total Of Cols 15 And 16)	Remarks
			No. Of Days Work Performed	No. Of Days Of Lay Off	No. Of Days Of Maternity Leave	No. Of Days Of Leave Enjoyed	Total Of Cols 4 To 7	Balance Of Leave For Preceding Year	Leave Earned During The Year Mentioned In Col 1	Total Of Cols 9 To 10		From	To					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
Jan-2015			15.5	0.0	0.0	2.5	18.0	0.0	2.5	2.5		01/03/2015-01/03/2015 01/17/2015-01/17/2015 01/19/2015-01/19/2015 01/22/2015-01/22/2015	0.0					
Feb-2015			24.0	0.0	0.0	1.0	24.0	0.0	2.5	2.5		02/17/2015-02/17/2015	1.5					
Mar-2015			4.0	0.0	0.0	0.0	4.0	0.0	2.5	4.0		-	4.0					
Apr-2015			0.0	0.0	0.0	0.0	0.0	0.0	0.0	4.0		-	0.0					
May-2015			0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		-	0.0					
Jun-2015			0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		-	0.0					
Jul-2015			0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		-	0.0					
Aug-2015			0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		-	0.0					
Sep-2015			0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		-	0.0					
Oct-2015			0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		-	0.0					
Nov-2015			0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		-	0.0					
Dec-2015			0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		-	0.0					
			42.50			3.50	46.00	0.00	7.50									

Form Q

FORM - Q REGISTER OF EMPLOYMENT FOR SHOPS AND ESTABLISHMENTS

See Sub Rule (1) of Rule 16 of the Tamil Nadu Shops and Establishments Rules, 1948

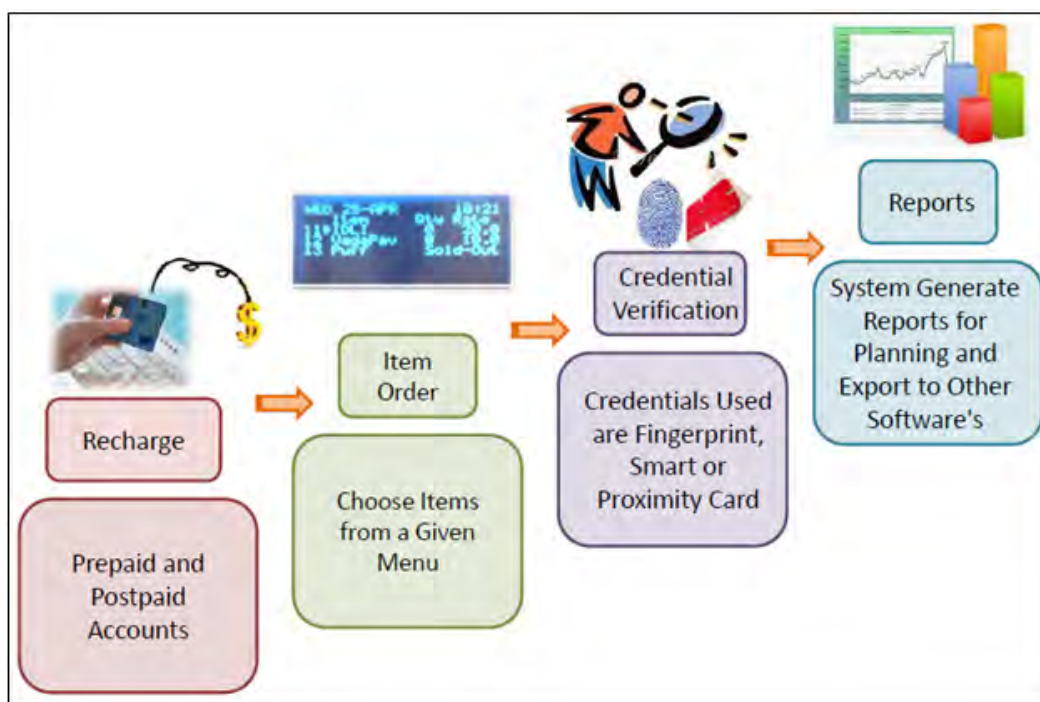
Leave Available During the Month		Leave Balance		Daily Hours of Work Done														
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2.00	5.00	28.00	-	08:30	08:30	08:30	08:30	08:30	WO	WO	08:30	08:30	10:00	??	??	WO	WO	08:00

Form Q includes fields like: *Month, Year, Serial No., Employee Name, Employee Id, Date of Joining, Age/Date of Birth, Designation, Leave Credit at the beginning of the Month, Leave Available During the Month, Leave Balance, Daily Hours of Work Done Including Overtime (If any), Total Hours of Over time Worked, Total Hours of work done during the Month and Total No. of days Maternity Leave availed by the Employee.*

The COSEC Cafeteria is a Web based cafeteria management tool offering unparalleled ease of use in managing cafeteria operations for a large number of users or employees.



This functionality is not available with the COSEC Application basic platform license.



The following are the features of the Cafeteria module.

- Reduced waiting time at the cafeteria thus improving employee productivity
- Meal payment cycle completion within seconds
- Instant reconciliation of contractors invoice/monthly statement
- Easy tracking of usage of subsidized meal/snack programs
- Tracking cafeteria usage by outsiders/visitors
- Trouble free cash management

Configuration Basics

Configure your Cafeteria system in the order noted below:

Refer to the specified module sections for configuration instructions.

1. Configure Cafeteria Devices from Device Configuration of **Devices** module.
2. Define items from **Items** option of Cafeteria
3. Define menus and assign items to each menu from **Menus** option.
4. Configure menu schedule for each cafe device from **POS (Point Of Sale) Device Configuration** option.
5. Configure parameters for pre-paid and post-paid accounts from the **Payment Methods** option.
6. Assign Cafeteria devices to users from the **User Configuration** option of **Users** module.






The Monthly process must be run at the end of the month to generate proper cafeteria transactions.

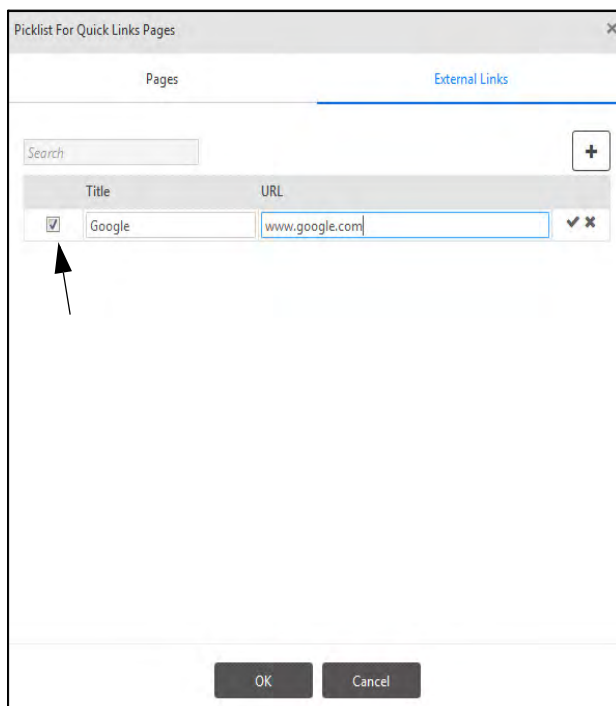
To use the Cafeteria functionality, click on **Cafeteria**  module and the following screen appears.



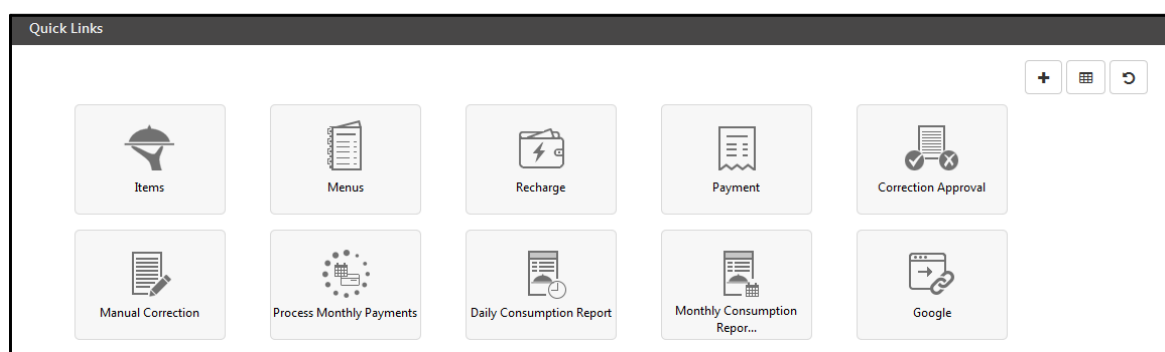
The page displays a menu and **Quick Links** to go to the required page in just one click. Quick Links are shortcuts to reach to a specific page easily. It also contains following three buttons:



- **Add Quick Link:** Click  button to add a quick link. A picklist for Quick Link pages appears for selecting the page or External Link for which the quick link is to be created. Maximum **20** quick links can be added.
- For Adding **Pages** in Quick Link, Select the Pages and click on OK
- For Adding **External Links**, Select External Link tab, click on  button to add new external link.

- Configure the **Title** and **URL** of the external link under the respective fields. click on checkbox to get the configured link on quick link screen as shown below. To save the configuration click on .



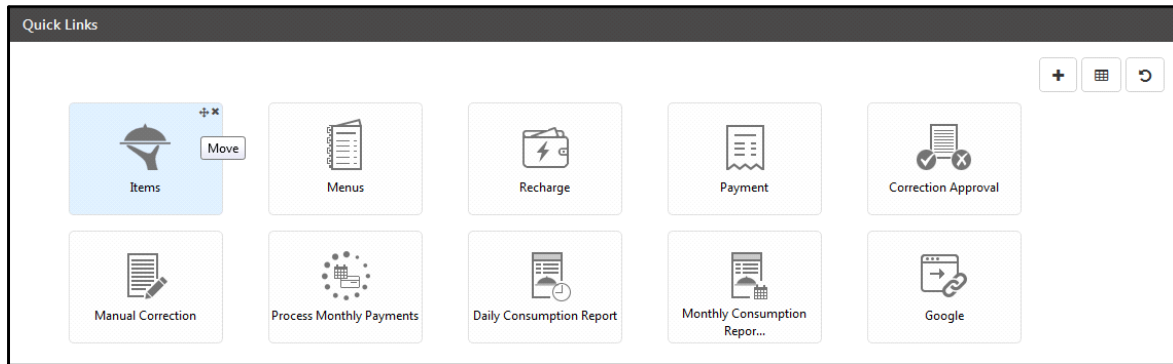
- To edit the saved configuration, click on .
- Click on OK to save the link configuration on Quick Link screen. The external link will be displayed as shown below:



- **Select Layout:** Click  button to select a layout for the quick links. You can select 5x4 or 4x5 layout to manage the quick links.
- **Reset Quick Links:** Click  button to reset the quick links to the default quick links.

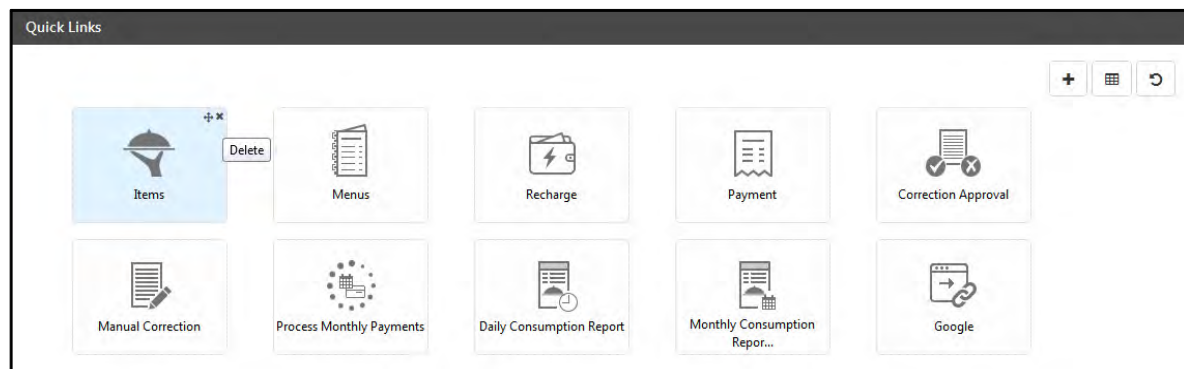
Move the Link

To move the link from one place to another, hover on the link on top right corner and click on “Move” icon as shown below. Then drag the quick link to the desired place. It will be placed at the desired location on the quick links page.




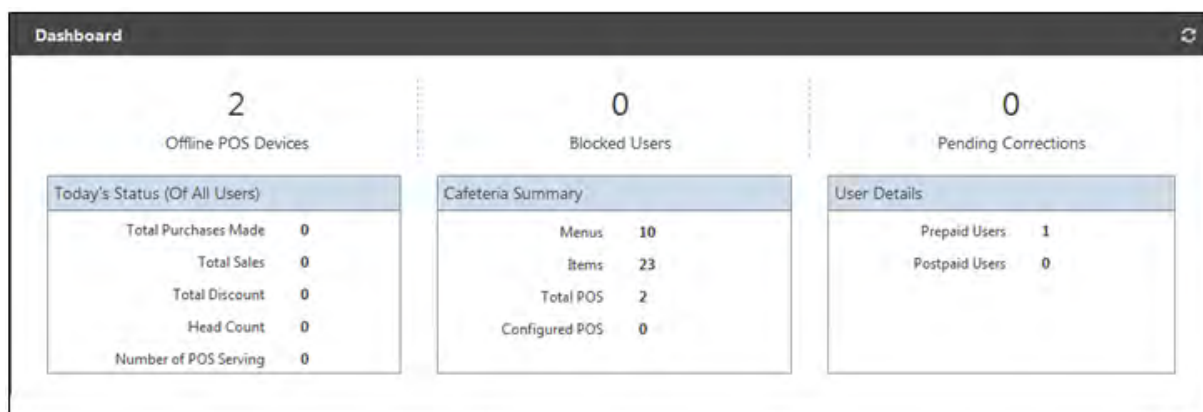
Delete the Link

To delete a particular link, hover on the link on top right corner and click on “Delete” icon as shown below.



Cafeteria Dashboard

To view the **Cafeteria** Dashboard, click the Dashboard button  on the **Cafeteria** page and the following screen appears.



The Dashboard displays the basic information on Cafeteria module relating to the COSEC Software under the following groups:

- Offline POS Devices: Total no. of POS device which are offline.
- Blocked Users: Total no. of users who are blocked.

- Pending Corrections: Total no. of pending corrections on current day.

Today's Status (Of All Users)


- Total Purchases Made: Total no. of transactions that were recorded on current day.
- Total Sales: Sum of all the current day transactions amount.
- Total Discount: Sum of all the current day transactions discounts.
- Head Count: Total no. of unique user id found in all the current day transactions.
- Number of POS Serving: Total no. of configured POS with at least one of the menu which is scheduled for today.

Cafeteria Summary

- Menus: Total no. of menus created in the system.
- Items: Total no. of items configured in the system.
- Total POS: Total no. of devices configured for Cafeteria.
- Configured POS: Total no. of canteen devices to which at least 1 menu assigned to it and also at least one active menu scheduled.

User Details

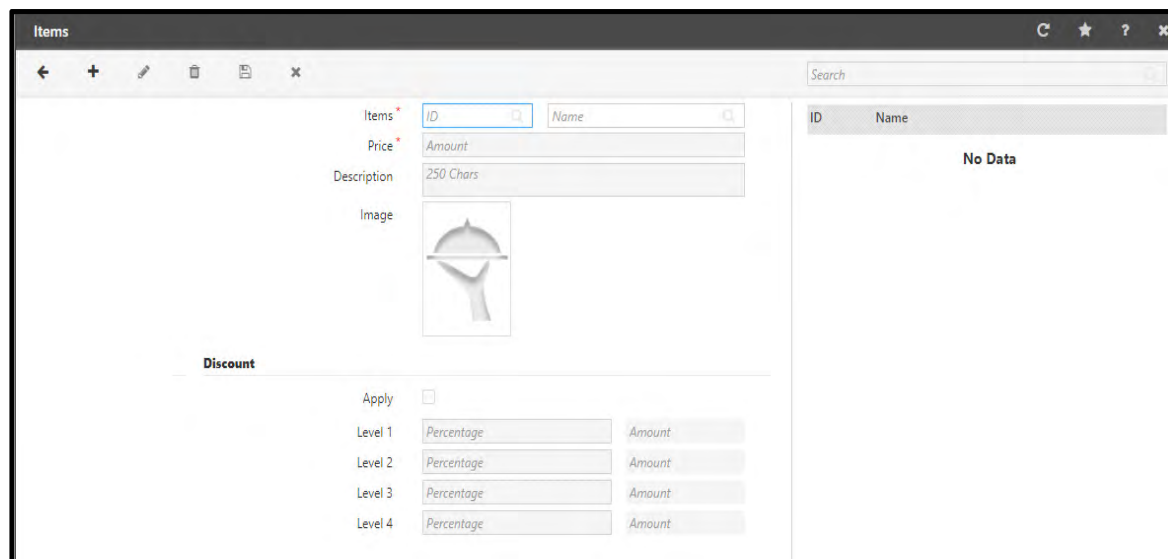
- Prepaid Users: Total no. of canteen users (active) with their account type as prepaid.
- Postpaid Users: Total no. of canteen users (active) with their account type as postpaid.

For more information on the above Dashboard options, click the respective information links on the Dashboard. The latest values on Dashboard are updated on clicking the Refresh  button.

Items

The Cafeteria module enables to define a list of items that are to be served by the in-house cafeteria during the various menu schedules. You can create maximum **255** items. These items can then be assigned to various menus from the **Menu** option.

To define view items page, go to **Cafeteria Management module > Items** and the following screen appears:



The page displays configurations and a list of items which are already defined in the right pane as shown above.

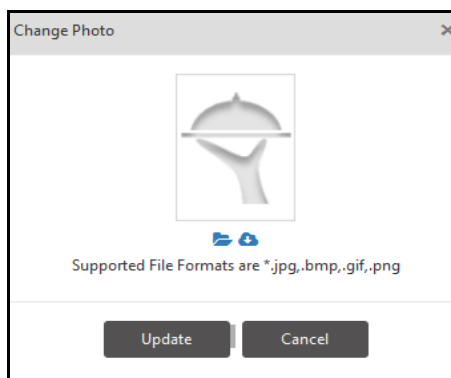
To create a new item click the **New** button and provide the following details:

Items: Enter a **Name** for the new item. The **ID** will be generated by the system while saving the item.

Price: Specify the cost of the item.

Description: Provide a brief description of the item.

Image: Click on the Image field to change/upload the photo of the item. A pop-up is generated as shown below. Click on **Browse** image button to select the image and click on **Update** to save the Image.



Maximum allowed Size to upload the image is 10KB.

Discount

- **Apply:** In the event of a discount being applicable on the item, select the checkbox and specify the discount levels as a percentage of the item cost as shown below in the first textbox. The Discount Amount is automatically calculated and displayed in the second textbox based on the Percentage value specified. E.g.: For Level 1, if 50% discount is specified the calculated percentage for 20Rs i.e. 10Rs gets displayed in the second box.

Discount Levels can be assigned to different users. For eg: Discount level 2 with more discount can be given to workers and Discount level1 with less discount can be assigned to managers.

The screenshot shows the 'Items' form in the Matrix COSEC System. A green banner at the top indicates 'Saved Successfully'. The form contains the following fields:

- Items:** 4
- Price:** 20
- Description:** 250 chars
- Image:** A photo of a samosa.
- Discount:**
 - Apply:** ☒
 - Level 1:** 50 (Discount Amount: 10.00)
 - Level 2:** 75 (Discount Amount: 15.00)
 - Level 3:** 0 (Discount Amount: 0.00)
 - Level 4:** 0 (Discount Amount: 0.00)

On the right side, there is a table listing items:

ID	Name
1	Rice
2	Dal
3	Wafers
4	Samosa

An arrow points to the 'Samosa' entry in the table.

Click on **Save** to add the Item to the list. The newly added item gets displayed in the grid on the right side as shown above.

Menus

This tab enables to define menus which may consist of the items defined from the “Items” page. You can create maximum **999** Menus. These menus can then be assigned to the various Cafeteria devices as per a configured time schedule from the **POS Device Configuration** option.

For defining the Menu, go to **Cafeteria Management Module > Menus** and the following page appears:

ID	Name
1	Lunch

The above page displays configurations and a grid on the right hand side shows a list of created menus.

To create a new menu, click on the **New** button and enter the following parameters:

- **Menu:** Enter a **Name** for the new menu. The **ID** will be generated by the system while saving the menu.
- **Activate:** Select the checkbox to enable the menu and set it as active.
- **Contains Default Item:** Enable to set the first assigned item as the default item. In the event of the user directly punching at the Cafeteria door without selecting any item, the system automatically takes the default item as the item ordered and processes the transaction.



*Useful for Canteens selling fixed Breakfast/ Lunch/Dinner.
Most Selling item can be set as Default.*

Item List

This section enables to assign items from the item list to the menu.



Maximum 99 items can be added to a Menu.

Click on the Item picklist button and select the item from the item list window. The selected items get displayed in the grid as shown below.

Click on **Save** to save the Menu list consisting the selected items. The configured item will be shown in the grid as shown below:

Menus

✓ Saved Successfully

←

+

✎

🗑

📄

✕

Search

2

Breakfast

Activate

☒

Contains Default Item

☐

First Item Will Be Default Item

Item List

Item

ID

Name

3

Wafers

5

0

0

0

0

▼

🗑

4

Samosa

20

10

15

0

0

▲

🗑

ID ▲

Name

1

Lunch

2

Breakfast

Matrix COSEC System Manual

1805

POS Devices Configuration

The POS Device Configuration functionality enables to assign the menus to devices and allows to schedule the Menu on defined Cafeteria devices for different time periods and days.

For assigning the Menu to device, go to **Cafeteria Management > POS Devices Configuration** tab and the following page appears as shown below:

ID	Name
5	Wireless Door 1st Floor

The page displays configurations and a grid on the right side containing devices configured for Cafeteria.

Select a device from the grid and the parameters get loaded in the respective fields

- **Active:** Select the checkbox to activate the selected device.

Assign Menu

This section enables to assign menus to the selected device. Maximum 99 menus can be assigned to a single device.

Menu No	ID	Menu Name
1	2	Breakfast
2	1	Lunch

- **Menu:** Select menu by clicking on the Picklist button. The selected menu gets displayed in the grid as shown above.

Schedule Menus

After assigning a menu, schedule can be assigned during which the menu is to be displayed.

Click on **Add** button and the following screen appears.

The screenshot shows the 'POS Devices Configuration' window. At the top, there's a search bar. Below it, the 'POS Device' is set to '5' and 'Wireless Door 1st Floor'. The 'Active' checkbox is checked. The 'Assign Menus' section is expanded, showing the 'Schedule Menus' sub-section. A search bar is present above a table. The table has columns: Menu No, ID, Menu Name, Start Time, End Time, and Schedule Days. There are two rows of data: Menu No 1 with ID 2, Menu Name 'Breakfast', Start Time 08:45, End Time 09:00, and Schedule Days '_ Mo Tu We Th Fr _'; and Menu No 2 with ID 1, Menu Name 'Lunch', Start Time 12:30, End Time 14:00, and Schedule Days '_ Mo Tu We Th Fr _'. To the right of the table is a sidebar with a search bar and a list of devices, with '5 Wireless Door 1st Floor' selected.

Menu No	ID	Menu Name	Start Time	End Time	Schedule Days
1	2	Breakfast	08:45	09:00	_ Mo Tu We Th Fr _
2	1	Lunch	12:30	14:00	_ Mo Tu We Th Fr _

Enter the required details:

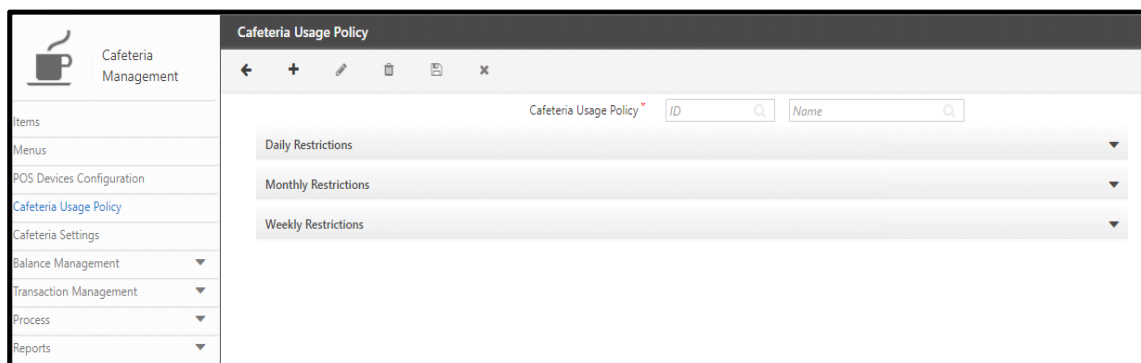
- **Menu Name:** Select the Menu using the picklist button.
- **Start Time/End Time:** Configure the time period by specifying the **Start Time** and the **End Time** during which the menu will be valid at the selected Cafeteria device.
- **Schedule Days:** Select the checkbox against the appropriate **days** on which the menu is to be considered as valid.
- Click on **OK** to add the selected menu to schedule on the device. Similarly, additional menu schedules can be configured for the selected Cafeteria device.

Click on **Save** once done.

Cafeteria Usage Policy

The **Cafeteria Usage Policy** enables the administrator to configure cafeteria restrictions based on Item, Menu, Transaction and Shift Duration for Cafeteria Users. You can configure maximum **99** Cafeteria usage policy.

To configure this, go to **Cafeteria Management > Cafeteria Usage Policy** and the following page appears as shown below:



By configuring Cafeteria Usage Policy you can:

- configure maximum allowed transactions for cafeteria on **Daily**, **Monthly** and **Weekly** basis.
- restrict transaction per menu on daily and monthly basis.
- restrict quantity per items in a menu.
- restrict cafeteria user to access cafeteria out of shift duration & scheduled days.
- allow transactions without discount on exceeding maximum configured limit for all provided restrictions.
- assign defined “Cafeteria Usage Policy” to cafeteria user(s) & any enterprise structure.

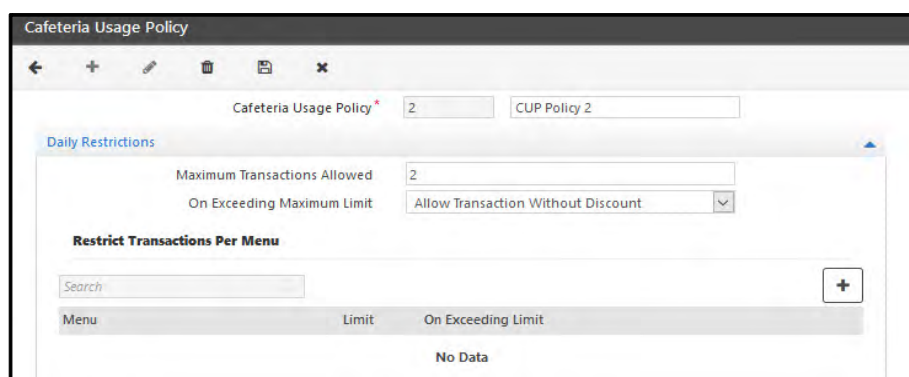
To configure new policy, click on **New** button.

Enter the **Name** of policy. The ID will be auto-generated by the system when the policy is saved.

Daily Restrictions

Maximum Transaction Allowed: Enter the number of cafeteria transactions allowed in a day. The allowed Range is from 1 to 99.

On Exceeding Maximum Limit: When the cafeteria transaction exceeds the maximum allowed limit; then further transaction can be denied by selecting the option **Deny transaction** or allowed without discount by selecting the option **Allow transaction without discount**.



Restrict Transactions Per Menu

To restrict the cafeteria transaction based on menu, Click on **Add** button. The new row will appear as shown below.

Restrict Transactions Per Menu			
Search			
Menu		Limit	On Exceeding Limit
ID	Name	0-99	Deny Transaction

Menu: Click the picklist and select the Menu for which restriction is to be made.

Limit: Enter the number of transactions allowed in a day for the selected menu. The allowed Range is from 0 to 99.

On Exceeding Limit: When the cafeteria transaction for the selected menu exceeds the maximum allowed limit; then further transaction can be denied by selecting the option **Deny transaction** or allowed without discount by selecting the option **Allow transaction without discount**.

Click **OK** to save the restrictions on menu. Similarly you can add another menu for applying the restriction on transaction. Then click **Save** button to save the changes to the policy.

Cafeteria Usage Policy

✓ Saved Successfully

Cafeteria Usage Policy* 2 CUP Policy 2

Daily Restrictions

Maximum Transactions Allowed 2

On Exceeding Maximum Limit Allow Transaction Without Discount

Restrict Transactions Per Menu			
Search			
Menu		Limit	On Exceeding Limit
Breakfast1		2	Deny Transaction
Lunch		1	Allow Transaction Without Discount

Restrict Transactions Per Item

To restrict the cafeteria transaction based on item, Click on **Add** button. The new row will appear as shown below.

Restrict Quantity Per Item

Select Item

15

Poha

Menu

Any Menu

Select Menus

ID

Name

Maximum Quantity Allowed

1

On Exceeding Max Quantity

Deny Transaction

Add

Cancel

Search

Item	Menu	Quantity	On Exceeding Max. Quantity	
No Data				

Select Item: Click the picklist and select the Item for which restriction is to be made.

Menu: Select the option for Menu as **Any Menu** or **Menu Wise**. Depending on the selection of menu, if item is included in that menu then restriction will be applied on the item of the menu.

For eg: Here Poha is selected for Any Menu, so where-ever Poha item is available in Menu, it will be restricted. If Poha is selected for particular Menu say "Breakfast1" then Poha will be restricted for Breakfast1 only.

Select Menus: For **Menu Wise** selection of Menu; click the picklist and select the menus in which the selected item is to be restricted.

Maximum Quantity Allowed: Enter the number of transactions allowed in a day for the selected item. The allowed Range is from 1 to 99.

On Exceeding Maximum Quantity: When the cafeteria transaction for the selected item exceeds the maximum allowed quantity; then further transaction can be denied by selecting the option **Deny transaction** or allowed without discount by selecting the option **Allow transaction without discount**.

Click **Add** to save the item on which restriction is done. Similarly you can add another item for applying the restriction on transaction.

Restrict Quantity Per Item

Select Item

16

Idli Samb

Menu

Menu Wise

Select Menus

26

Breakfast1

Maximum Quantity Allowed

2

On Exceeding Max Quantity

Allow Transaction Without Discount

Update

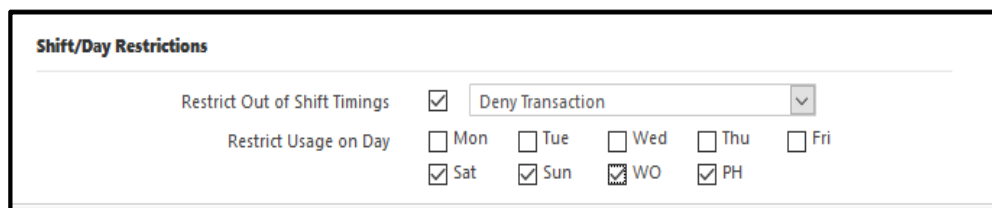
Cancel

Search

Item	Menu	Quantity	On Exceeding Max. Quantity	
Poha	Any Menu	1	Deny Transaction	
Idli Samb	Breakfast1	2	Allow Transaction Without Discount	

Shift/Day Restrictions

You can also restrict the cafeteria transaction based on Shift/Day.



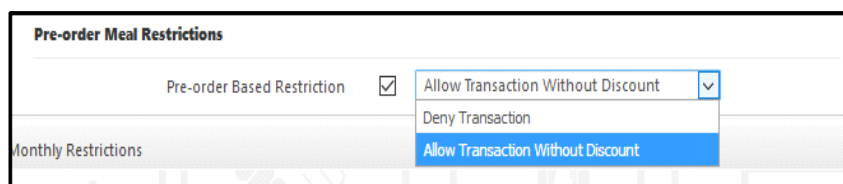
The screenshot shows a form titled "Shift/Day Restrictions". It contains two main sections. The first section, "Restrict Out of Shift Timings", has a checked checkbox and a dropdown menu set to "Deny Transaction". The second section, "Restrict Usage on Day", has checkboxes for each day of the week: Mon, Tue, Wed, Thu, Fri, Sat, Sun, WO, and PH. The checkboxes for Sat, Sun, WO, and PH are checked.

Restrict Out of Shift Timings: When the cafeteria transaction is done out of shift timings; then the transaction can be denied by selecting the option **Deny transaction** or allowed without discount by selecting the option **Allow transaction without discount**.

Restrict Usage on Day: The transactions can be restricted on the particular days by selecting the respective check-box. For eg: Here Sat, Sun, WO and PH are restricted for cafeteria transaction.

Pre-order Meal Restrictions

You can also restrict the cafeteria transaction based on Pre-ordered meal. You can impose restriction on overflowing Pre-ordered quantity.

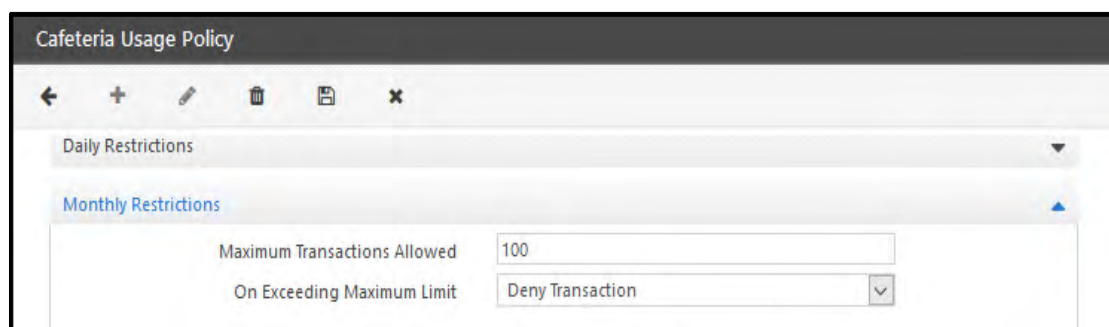


The screenshot shows a form titled "Pre-order Meal Restrictions". It contains a section "Pre-order Based Restriction" with a checked checkbox and a dropdown menu. The dropdown menu is open, showing three options: "Allow Transaction Without Discount", "Deny Transaction", and "Allow Transaction Without Discount". The "Allow Transaction Without Discount" option is highlighted in blue. Below this section is a section titled "Monthly Restrictions".

Enable the **Pre-order Based Restriction** checkbox. Then you can select either of the options:

- **Allow Transaction without Discount-** If item's consumed quantity exceeds the pre-ordered quantity of the item in selected menu then it will allow the transaction with discount.
- **Deny Transaction** -If item's consumed quantity exceeds the pre-ordered quantity of the item in selected menu then it will deny the transaction.

Monthly Restrictions



The screenshot shows a form titled "Cafeteria Usage Policy". It has a toolbar with icons for back, forward, edit, delete, save, and close. Below the toolbar are two sections: "Daily Restrictions" and "Monthly Restrictions". The "Monthly Restrictions" section is expanded, showing a text input field for "Maximum Transactions Allowed" with the value "100" and a dropdown menu for "On Exceeding Maximum Limit" set to "Deny Transaction".

Maximum Transaction Allowed: Enter the number of cafeteria transactions allowed in a month. The allowed Range is from 1 to 9999.

On Exceeding Maximum Limit: When the cafeteria transaction exceeds the maximum allowed limit; then further transaction can be denied by selecting the option **Deny transaction** or allowed without discount by selecting the option **Allow transaction without discount**.

Restrict Transactions Per Menu

To restrict the cafeteria transaction based on menu, click on **Add** button. The new row will appear as shown below.

Restrict Transactions Per Menu			
Menu		Limit	On Exceeding Limit
ID	Name		
		0-9999	Deny Transaction

Menu: Click the picklist and select the Menu for which restriction is to be applied.

Limit: Enter the number of transactions allowed in a month for the selected menu. The allowed Range is from 0 to 9999.

On Exceeding Limit: When the cafeteria transaction for the selected menu exceeds the maximum allowed limit; then further transaction can be denied by selecting the option **Deny transaction** or allowed without discount by selecting the option **Allow transaction without discount**.

Click **OK** to save the restrictions on menu. Similarly you can add another menu for applying the restriction on transaction. Then click **Save** button to save the changes to the policy.

Restrict Transactions Per Menu		
Menu	Limit	On Exceeding Limit
menu3	100	Allow Transaction Without Discount

Restrict Transactions Per Item

To restrict the cafeteria transaction based on item, click on **Add** button. The new row will appear as shown below.

Restrict Quantity Per Item

Select Item

15

Poha

Menu

Any Menu

Select Menus

ID

Name

Maximum Quantity Allowed

1

On Exceeding Max Quantity

Deny Transaction

Add

Cancel

Search

Item	Menu	Quantity	On Exceeding Max. Quantity	
No Data				

Select Item: Click the picklist and select the Item for which restriction is to be applied.

Menu: Select the option for Menu as **Any Menu** or **Menu Wise**. Depending on the selection of menu, if item is included in that menu then restriction will be applied on the item of the menu.

For eg: Here Poha is selected for Any Menu, so where-ever Poha item is available in Menu, it will be restricted. If Poha is selected for particular Menu say "Breakfast1" then Poha will be restricted for Breakfast1 only.

Select Menus: For **Menu Wise** selection of Menu; click the picklist and select the menus in which the selected item is to be restricted.

Maximum Quantity Allowed: Enter the number of transactions allowed in a month for the selected item. The allowed Range is from 1 to 9999.

On Exceeding Maximum Quantity: When the cafeteria transaction for the selected item exceeds the maximum allowed quantity; then further transaction can be denied by selecting the option **Deny transaction** or allowed without discount by selecting the option **Allow transaction without discount**.

Click **Add** to save the item on which restriction is done. Similarly you can add another item for applying the restriction on transaction.

Restrict Quantity Per Item

Select Item

16

Idli Samb

Menu

Menu Wise

Select Menus

26

Breakfast1

Maximum Quantity Allowed

2

On Exceeding Max Quantity

Allow Transaction Without Discount

Update

Cancel

Search

Item	Menu	Quantity	On Exceeding Max. Quantity	
Poha	Any Menu	1	Deny Transaction	
Idli Samb	Breakfast1	2	Allow Transaction Without Discount	



It is advised to configure Daily & Monthly Level limits properly to avoid false restrictions. Suppose Maximum Transactions / Item Limit / Menu Limit on Monthly Level is configured less than Daily Level, in such cases user will be restricted on reaching monthly allowed limit.

Weekly Restrictions

Weekly Restriction: Select this check box if you wish to apply weekly restrictions on users based on transaction amount.

Maximum Weekly Limit: Enter the maximum transaction amount that will be allowed to users. When the user's transactions exceed this amount, further transactions will be denied.

Week Start Day: Select the desired day from the drop down list. This day will be considered as the starting day of the week for the user. For example, if you select Tuesday, the week for the user will begin on Tuesday - November 2 and end on Monday - November 8.

If you want the week for the users to begin from the day they join, then 7 different policies for each day of the week need to be created. These can then be assigned as per the joining day of the users. For example, if you have set the Week Start Day as Monday, User1 joins on Tuesday and User2 joins on Wednesday. In this case, we need to create separate policies, wherein in Policy1 the Week Start day will be set as Monday, in Policy2 it will be Tuesday and in Policy3 it will be set as Wednesday. Now, you can assign Policy2 to User1 and Policy3 to User2.

If you desire updating the **Week Start Day** for any existing Cafeteria Usage Policy assigned to users, it is recommended you update the day a day before the newly configured **Week Start Day**, to make sure the changes are applied effectively.

For example, the **Week Start Day** is initially configured as Monday and later you wish to update it as Saturday, then you must update the **Week Start Day** on:

- Friday after all the transactions for the day have been completed
OR
- Saturday before any transaction for the day is to be encountered.

Weekly Restrictions are applicable to ARGO, ARGO FACE and VEGA devices only. If you want to print the Current Balance/ Current Month Usage and Weekly Remaining Limit on the Cafeteria receipt, refer to "[Printer Settings](#)" in VEGA Door, "[Printer Settings](#)" in ARGO Door and "[Printer Settings](#)" in ARGO FACE.



Weekly Restriction is applicable only if the device is connected to the server.

The unused weekly balance will not be carry-forwarded to the next week.

Pre-ordered meals will not be considered for Weekly Restriction

Cafeteria Settings

The **Cafeteria Settings** page enables the administrator to configure parameters for **prepaid** and **postpaid** accounts as per the site requirements.

To configure this, go to **Cafeteria Management > Cafeteria Settings** and the following page appears as shown below:

The screenshot shows the 'Cafeteria Settings' interface. On the left, there are three tabs: 'Prepaid' (selected), 'Postpaid', and 'Other Settings'. The main area contains the following settings:

- Limit Recharge Amount:** ☒
- Maximum Recharge Amount *:** 500
- Balance Management:** Server Based (dropdown)
- Device-Server Balance Check:** ☒
- Monthly Limit:**
 - Block User On Max Usage Limit:** ☒
 - Maximum Usage Limit Per Month *:** 50
- Daily Limit:**
 - Block User On Max Usage Limit:** ☒
 - Maximum Usage Limit Per Day *:** 22.5
 - Restore User On Date Change:** ☒

There are three types of settings as described below:

- Prepaid
- Postpaid
- Other Settings

Prepaid

Prepaid method provides the simple option of recharging the Smart Card to store balance information as and when needed. This eliminates the need of managing cash all the time.

This screenshot is identical to the one above, showing the 'Cafeteria Settings' interface with the 'Prepaid' tab selected. The settings are the same: Limit Recharge Amount (checked), Maximum Recharge Amount (500), Balance Management (Server Based), Device-Server Balance Check (checked), Monthly Limit (Block User On Max Usage Limit checked, Maximum Usage Limit Per Month 50), and Daily Limit (Block User On Max Usage Limit checked, Maximum Usage Limit Per Day 22.5, Restore User On Date Change checked).

The parameters are:

Limit Recharge Amount: Select to enable a limitation to be set on maximum recharge amount for prepaid accounts.

Maximum Recharge Amount: Specify the maximum amount with which a prepaid account can be recharged.

Balance Management: Specify whether the balance management process for prepaid users should take place at the device side or server side. For Server Based balance management, user credentials supported are fingerprint, Read-Only card and Smart card. For Device Based balance management, however, only Smart Cards are supported.

Device-Server Balance Check: For Server Based balance management, You can enable Device-Server Balance Check to enable Device to check Server-side balance before allowing cafeteria transaction. For this, Device and Server must be connected.



For server communication in the prepaid server based mode, the admin must set HTTP Server configuration on the device webpage for all configured Cafeteria devices.

Monthly Limit

This section enables to set a maximum monthly usage limit for a prepaid user.

Block User on Max Usage Limit: Enable to block a user whose usage has exceeded the monthly limit.

Max Usage Limit Per Month: Specify the maximum limit of usage per month.

Daily Limit

This section enables to set a maximum daily usage limit for a prepaid user.

Block User on Max Usage Limit: Enable to block a user whose usage has exceeded the daily limit.

Maximum Usage Limit Per Day: Specify the maximum limit of usage per day.

Restore User On Date Change: Enable to allow a user to be blocked only for a single day and then restore the user at midnight.

Postpaid

Postpaid method provides the choice of having the bill deducted directly from a user's payroll. Hence, there is no need for manual cash handling at any time.

The screenshot shows the 'Cafeteria Settings' window with the 'Postpaid' tab selected. The left sidebar has 'Prepaid', 'Postpaid', and 'Other Settings' options. The main area contains the following settings:

- Account Reset Mode:** A dropdown menu set to 'Reset To Zero'.
- Allowed Usage Per Month *:** A text input field containing '100'.
- Reset Account Automatically:** An unchecked checkbox.
- Monthly Limit:**
 - Block User On Max Usage Limit:** A checked checkbox.
 - Maximum Usage Limit Per Month *:** A text input field containing '52'.
 - Accumulate Usage Limit:** A checked checkbox.
- Daily Limit:**
 - Block User On Max Usage Limit:** A checked checkbox.
 - Maximum Usage Limit Per Day *:** A text input field containing '12.63'.
 - Restore User On Date Change:** A checked checkbox.

The parameters are:

Account Reset Mode: Select a mode from the dropdown list to reset the account. The two modes are:

- **Reset to Zero:** Select this option to reset the postpaid users' accounts to 0 at the start of the month.
- **Deduct User's Allowed Usage:** Select this option to reset the account by using one of the following methods based on the actual usage of postpaid user:

If the total amount (actual usage for the month + previous due) is less than the users allowed usage per month (see below), the account is reset to zero and the total amount is recorded as payment transaction.

If the total amount (actual usage for the month + previous due) is more than the users allowed usage per month, the account will be reset to zero and the balance due "total accumulated amount - allowed usage amount" will be added and stored in the users previous due record. In this case the user's allowed usage amount will be recorded as user's payment transaction.



On running the Monthly Payments Process, a postpaid account will be reset based on the account reset mode specified by the admin. For more information, See ["Process-Monthly Payments"](#) on page 1845.

Allowed Usage Per Month: Specify the amount for the allowed monthly usage for postpaid accounts. This amount is used specifically as a base for the calculation of a user's accumulated dues and account reset calculations as explained before.

Reset Account Automatically: Select the checkbox if the postpaid accounts are to be automatically reset everytime the month changes.



The Alert Service must be running to function Reset Account automatically.

Monthly Limit

This section enables to specify the maximum usage limit amount for a month for a postpaid user. This is not to be confused with *Allowed Usage Per Month* which is used to determine a user's payment dues for a month.

Block User on Max Usage Limit: Select the checkbox if the users with postpaid accounts are to be blocked as and when the maximum usage limit is crossed for a month.

Maximum Usage Limit Per Month: Specify the maximum limit of usage per month.

Accumulate Usage Limit: Enable, if the user has not consumed the *Allowed Usage Per Month* limit for a selected month, and the balance is to be carried forward to the next month's allowed usage.

Daily Limit

This section enables to specify the maximum usage limit amount for a day for a postpaid user.

Block User on Max Usage Limit: Enable to block a user whose usage has exceeded the daily limit.

Maximum Usage Limit Per Day: Specify the maximum limit of usage per day.

Restore User On Date Change: Enable to allow a user to be blocked only for a single day and then restore the user at midnight.



*The Cafeteria Settings will be the default settings applicable to all Cafeteria enabled users in the system. These settings can however, be overridden from the **User Configuration** page of the **Users** module.*

Other Settings

From the Other Settings page one can enable the Pre-ordering feature.

The Cafeteria User can pre-order items beforehand from respective menus for the selected date. This helps Cafeteria Admin to have an estimate about the quantity of food to be prepared on given date.

Enable: Select to activate the Pre-ordering feature.

Allowed in Advance(Days): Specify the number of days before which the Cafeteria user can order the meals in advance. Eg: If 10 days is set. Then on 12th September, you can pre-order meals for upto 22 September.

Restrict Before Menu Start: Specify the number of **Days** or **Hours** before which the cafeteria user must finish the ordering of meals so that the food can be prepared for the required quantity.

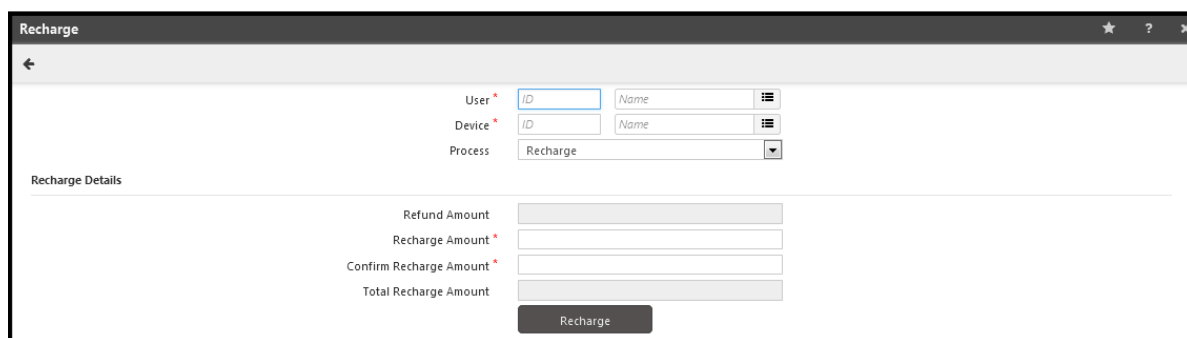
- **Days:** Select Days from the dropdown list and mention the number of days
- **Hours:** Select the hours from the dropdown list and mention the number of hours.
[See “Pre-ordered Meals” on page 1833.](#)

Finally, click on **Save** button to save the settings.

Recharge

The Balance Management option of the Cafeteria module enables the user to recharge the **prepaid** user card from the Cafeteria device. The COSEC Web application sends the configured recharge command to the Cafeteria device from the COSEC Monitor application.

To view the recharge page, go to **Cafeteria Management > Balance Management > Recharge** option and the following page appears as shown below:



- **User:** Select a user from the Cafeteria Prepaid users picklist. The picklist contains users configured from the User module and who have been assigned the Prepaid account from the **Users > User Configuration > Cafeteria** page.
- **Device:** Select a device from the Cafeteria device picklist. The device for the Cafeteria application can be assigned from the *Application* parameter of **Devices module > Device Configuration > Profile** page.



Only those devices which are enabled for cafeteria are available for the selection.



The Device picklist will be enabled for those prepaid user for whom the Balance Management is set as Device based from the User configuration> Cafeteria> Settings.



For server based balance management, the device web page must be updated with the HTTP server address.

- **Process:** Select the Process from the options of **Recharge** or **Reset**.

Recharge Process

The screenshot shows a mobile application window titled "Recharge". At the top, there is a back arrow, a star icon, a question mark icon, and a close icon. Below the header, there are three input fields: "User" with the value "07" and a dropdown menu showing "Aditi"; "Device" with the value "3" and a dropdown menu showing "NGT Ground Floo"; and "Process" with a dropdown menu showing "Recharge". Below these fields is a section titled "Recharge Details". This section contains four input fields: "Refund Amount" with the value "0", "Recharge Amount" (empty), "Confirm Recharge Amount" (empty), and "Total Recharge Amount" (empty). At the bottom of the "Recharge Details" section is a button labeled "Recharge".

Recharge Details

- **Refund Amount:** It displays the amount to be refunded to the user by the system. It is an auto generated field.
For e.g: In Prepaid user case, when the user punches at the Cafeteria door the amount is deducted for the selected item. But when the user goes to take that item, if the item is not available at that time so the user is left without that item. In such case he has to be refunded for the item price.
- **Recharge Amount:** Enter the recharge amount by which the prepaid user can be recharged.
- **Confirm Recharge Amount:** Re-enter the recharge amount for confirmation.
- **Total Recharge Amount:** This is the auto generated total amount which includes the summation of Refund Amount and Recharge amount with which the user card will be recharged.

Click on **Recharge**. The system will send the recharge command to the Cafeteria device. The selected user will be prompted to display the card at the device for the recharge process to be completed.

Reset Process

The screenshot shows a mobile application window titled "Recharge". At the top, there is a back arrow, a star icon, a question mark icon, and a close icon. Below the header, there are three input fields: "User" with the value "07" and a dropdown menu showing "Aditi"; "Device" with the value "3" and a dropdown menu showing "NGT Ground Floo"; and "Process" with a dropdown menu showing "Reset". Below these fields is a section titled "Recharge Details". This section contains one input field: "Reset Type" with a dropdown menu showing "Reset The Account To Zero (0)". At the bottom of the "Recharge Details" section is a button labeled "Reset".

- **Reset Type:** Select the Reset option from the dropdown list of Process field and select the Reset type from the below options:
 - **Reset the Account to Zero(0):** Select this option to reset the value on the prepaid card to 0.
 - **Reset the Account to Available Balance:** If this option is selected, **Reset Amount** field will display the last available balance of the user as found in the COSEC database based on the user's transaction to which the balance on the user card will be reset.

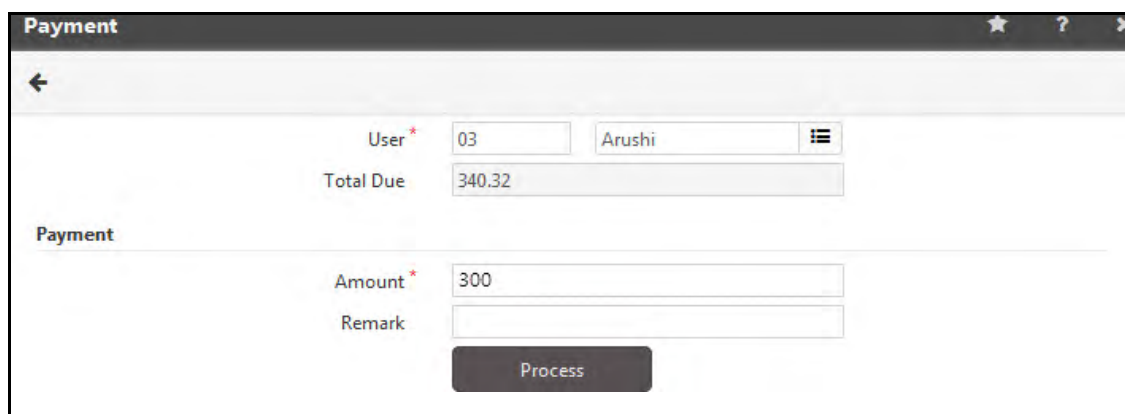
For E.g.: If the user has balance of Rs.100, he punches for a value of Rs.20, then available balance will be Rs.80 in user card and COSEC Database. If user punches next time for any value and if due to any reason the card gets garbage value. Then the card can be reset to the available balance in COSEC database i.e. Rs.80.

Click on the **Reset** button after selecting the appropriate option.

Payment

The Balance Management option of the Cafeteria module enables to record payment transactions against dues for the **postpaid** users.

For making the Payment, go to **Cafeteria Management Module > Balance Management > Payment** and the following page appears as shown below:



The screenshot shows a mobile application interface for the 'Payment' screen. At the top, there is a title bar with a back arrow, a star icon, a question mark icon, and a close icon. Below the title bar, the form is divided into two main sections. The first section contains a 'User' field with a dropdown menu showing '03' and 'Arushi', and a 'Total Due' field displaying '340.32'. The second section, titled 'Payment', contains an 'Amount' field with '300' and a 'Remark' field. A 'Process' button is located at the bottom of the form.

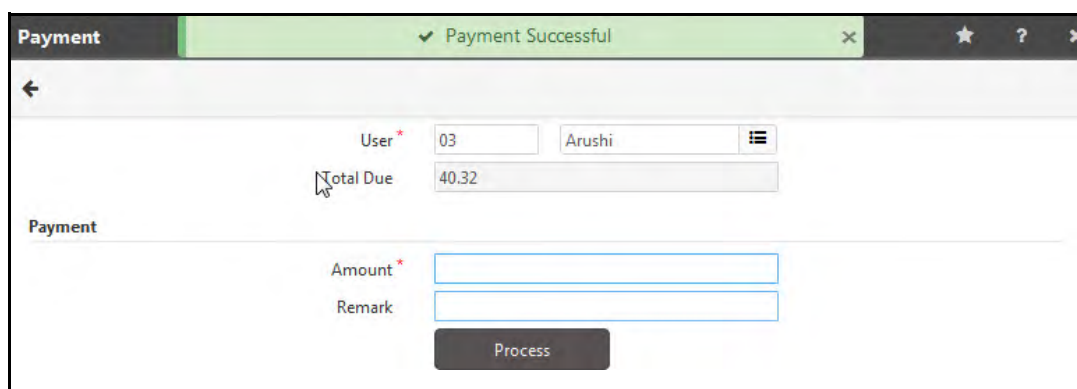
- **User:** Select the user from the picklist. The picklist contains users configured from the User module and who have been assigned the Postpaid account from the **Users > User Configuration > Cafeteria** page.
- **Total Due:** It displays the total amount due for the selected user.

Payment

- **Amount:** Enter the payment amount.
- **Remark:** The user can enter any remark during the payment process.

Click on the **Process** button to process the Payment.

After doing payment of say for Rs. 300, the left over due is shown in **Total Due** field and **Payment Successful** message is displayed as shown below.



The screenshot shows the same 'Payment' screen as before, but with a green banner at the top indicating 'Payment Successful'. The 'Total Due' field now displays '40.32', reflecting the payment of Rs. 300. The 'Amount' and 'Remark' fields are empty, and the 'Process' button remains at the bottom.

Manual Adjustment

This option enables the administrator to perform manual adjustments to user accounts.

Suppose due to some reasons, if the user's punch is not detected, in that case, we can manually adjust the user's account by debiting the required amount manually.

For making the manual adjustment, go to **Cafeteria Management Module > Balance Management > Manual Adjustment**



You can do Manual Adjustment for both the users, Prepaid and Postpaid.

Prepaid Users

For Prepaid users, following screen appears.

ID	Name
07	Aditi
1567	Sheetal
1678	Supriya
1782	Nidhi


The page displays the grid on the right hand side, containing a list of users (both Prepaid and Postpaid) who are enabled for canteen.

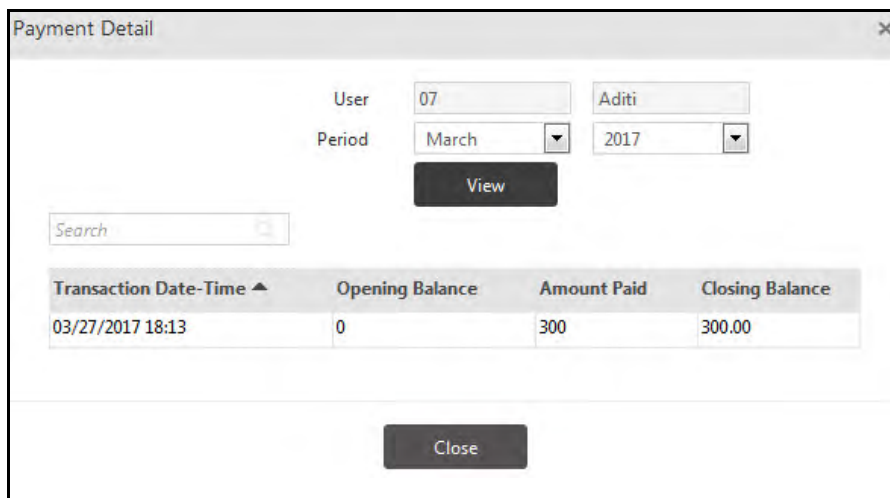
Enter the following parameters:

- **User:** Select user from the user picklist or from the grid on right for whom the manual adjustments are to be done.

Account Details for Current Month

It displays the account details of the selected user as **Previous** and **Current Expense**, **Correction Amount**, **Total Recharge**, and **Total Balance**.

- **Previous Balance:** It displays the previous balance which is carry forwarded to next month for the pre-paid user.
- **Current Expense:** It displays the expense of the month for the pre-paid user.
- **Correction Amount:** It displays the Refund amount to be paid back to the user in case of transaction error. It is equal to the Adjustment Balance + Refund Balance - Reset Balance.
- **Total Recharge:** It displays the total amount of recharge done in current month. Click on  to view the Payment Detail of recharge done by the user for a particular month as shown below.



Payment Detail

User: 07 Aditi
Period: March 2017
View

Search

Transaction Date-Time ▲	Opening Balance	Amount Paid	Closing Balance
03/27/2017 18:13	0	300	300.00

Close

- **Total Balance:** It is equal to the Previous balance+ Current balance- Correction amount- Total recharge
- **Adjustment:** Select the Process type from the options of **Credit** or **Debit**.
- **Amount:** Specify the amount to be credited or debited from the user account.
- **Remark:** Specify any remarks for the manual adjustment done.

Click on **Process** to process the manual adjustment and the following screen will appear.

Manual Adjustment ✓ Process Completed Successfully

User * Aditi

Search

Account Details For Current Month

Previous Balance	0.00
Current Expense	85.00
Correction Amount	-20.00
Total Recharge	300.00
Total Balance	195.00

Adjustment: Credit

Amount *

Remark

Process

ID	Name
07	Aditi
1567	Sheetal
1678	Supriya
1782	Nidhi

Now since, Adjustment has been set to Debit and Amount has been set to 20 so, In the above screen shot, it is shown with the arrow that the **Correction Amount** has changed from 0 to 20 and also, 20 has been deducted from the **Total Due**.

Postpaid Users

For Postpaid users, following screen appears.

Manual Adjustment ★ ? ✕

User * Nidhi

Search

Account Details For Current Month

Previous Due	0.00
Current Due	60.00
Correction Amount	0.00
Total Payment	50.00
Total Due	60.00

Adjustment: Credit

Amount *

Remark

Process

ID	Name
07	Aditi
1567	Sheetal
1678	Supriya
1782	Nidhi


The page displays the grid on the right hand side, containing a list of users (both Prepaid and Postpaid) who are enabled for canteen.

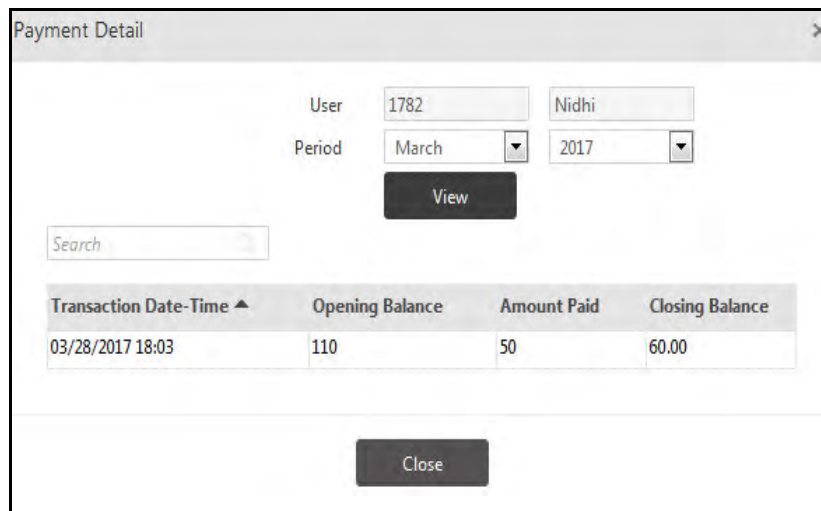
Enter the following parameters:

- **User:** Select user from the user picklist or from the grid on right for whom the manual adjustments are to be done.

Account Details for Current Month

It displays the account details of the selected user as **Previous** and **Current Due**, **Correction Amount**, **Total Payment**, and **Total Due**.

- **Previous Due:** It displays the previous due which is carry forwarded to next month for the post-paid user.
- **Current Due:** It displays the due of the month for the post-paid user.
- **Correction Amount:** It displays the Refund amount to be paid back to the user in case of transaction error. It is equal to the Adjustment Balance - Reset Balance + Refund Balance.
- **Total Payment:** It displays the total amount of payment done in current month. (Transactions can be done weekly or 4 times in a month). Click on  to view the Payment Detail of the user for a particular month as shown below.



The screenshot shows a 'Payment Detail' window. At the top, there are input fields for 'User' (1782) and 'Nidhi', and 'Period' (March 2017). Below these is a 'View' button. A search bar is also present. The main part of the window contains a table with the following data:

Transaction Date-Time ▲	Opening Balance	Amount Paid	Closing Balance
03/28/2017 18:03	110	50	60.00

At the bottom of the window is a 'Close' button.

- **Total Due:** It is equal to the Previous due+ Current due- Correction amount- Total payment
- **Adjustment:** Select the Process type from the options of **Credit** or **Debit**.
- **Amount:** Specify the amount to be credited or debited from the user account.
- **Remark:** Specify any remarks for the manual adjustment done.

Click on **Process** to process the manual adjustment and the following screen will appear.

Manual Adjustment

Process Completed Successfully

Star

Help

Close

Back

Search

User *

1782

Nidhi

Menu

Account Details For Current Month

Previous Due

0.00

Current Due

60.00

Correction Amount

20.00

Total Payment

70.00

Menu

Total Due

40.00

Adjustment

Credit

Dropdown

Amount *

Remark

50 Chars

Process

ID

Name

07

Aditi

1567

Sheetal

1678

Supriya

1782

Nidhi

Now since, Adjustment has been set to Debit and Amount has been set to 20 so, In the above screen shot, it is shown with the arrow that the **Correction Amount** has changed from 0 to 20 and also, 20 has been deducted from the **Total Due**.

Blocked Users

The COSEC Cafeteria module helps in monitoring Prepaid as well as Postpaid users and helps avoid treacherous usage by allowing users to be blocked on certain violations. Both Prepaid and Postpaid users can be blocked when their usage exceeds a fixed daily or monthly limit as configured for their Cafeteria accounts.

The Blocked Users page of the Cafeteria module enables the administrator to view the list of blocked users as well as restore blocked users as and when required. The two ways to Reinstate a blocked user are

- Pay full or part of the Due Amount
- Increase the Usage Limit

Blocked User

User * 3 Palak

Department Department-1

Designation Designation-1

Current Month Account Details

Previous Due 0.00

Current Due 145.00

Total Payments 0

Total Due 145.00

Blocked On 09/11/2017

Max Usage Limit Per Month 140.00

Previous Month's Accumulated Limit 0

New Usage Limit Per Month

Unblock

ID	Name
3	Palak

The grid on the right displays a list of all the users who are currently blocked due to exceeding the maximum usage limit.

Eg: Here the user Palak has purchased the items of price 145.00 which is more than the "Max Usage Limit Per month" of 140; so on next transaction on door; he will be blocked with reason Monthly consumption limited exceeded. The transactions are shown below.

Transaction Summary

Date * 09/10/2017 09/11/2017

Filter User Individual

User * 3 Palak

View

Purchase (6)

User ID	Name	Transaction Date-Time	POS Device	Item	Unit Price	Discount	Quantity	Payable
3	Palak	09/11/2017 10:50	NGT Direct Door-Device-2	Vadapav	40	20	1	20.00
3	Palak	09/11/2017 10:41	NGT Direct Door-Device-2	Vadapav	40	20	1	20.00
3	Palak	09/11/2017 10:40	NGT Direct Door-Device-2	Vadapav	40	20	1	20.00
3	Palak	09/11/2017 10:40	NGT Direct Door-Device-2	Puff	40	20	3	60.00
3	Palak	08/11/2017 11:32	NGT Direct Door-Device-2	Roti	20	10	1	10.00
3	Palak	08/11/2017 11:32	NGT Direct Door-Device-2	Sabji	30	15	1	15.00

Payment (0)

Recharge (0)

Reset (0)

Manual Credit/Debit (0)

Now you can unblock or restore the user by specifying the **New Usage Limit Per Month** for the selected user. Enter the New usage limit value as shown below.

The screenshot shows the 'Blocked User' interface. At the top, there's a search bar. Below it, user details are displayed: User ID 3, Name Palak, Department Department-1, and Designation Designation-1. A table titled 'Current Month Account Details' shows the following values: Previous Due (0.00), Current Due (145.00), Total Payments (0), Total Due (145.00), and Blocked On (09/11/2017). Below this table, there are fields for Max Usage Limit Per Month (140.00), Previous Month's Accumulated Limit (0), and New Usage Limit Per Month (160). An 'Unblock' button is located at the bottom right of the form. On the right side, there is a table with columns ID and Name, showing a single entry with ID 3 and Name Palak.

Current Month Account Details	
Previous Due	0.00
Current Due	145.00
Total Payments	0
Total Due	145.00
Blocked On	09/11/2017

ID	Name
3	Palak

Also the limit can be increased from User Configuration>

Click on **Unblock** to unblock the selected user. The user will be restored and he can purchase the item from cafeteria device.

The screenshot shows the 'Blocked User' interface after the 'Unblock' action. A green banner at the top indicates 'User Restored Successfully'. The user details section now shows empty fields for User ID, Name, Department, and Designation. The 'Current Month Account Details' table is also empty. The 'New Usage Limit Per Month' field is now empty. The 'Unblock' button is still present. On the right side, the table with columns ID and Name now displays 'No Data'.

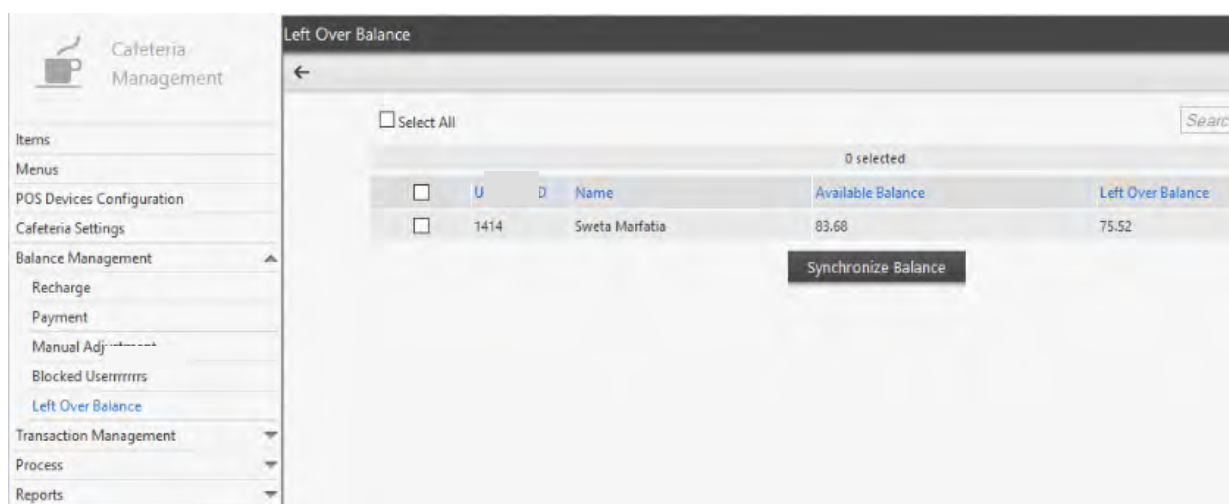
Current Month Account Details	
Previous Due	
Current Due	
Total Payments	
Total Due	
Blocked On	

ID	Name
No Data	

Left Over Balance

Left Over Balance page will allow admin to view users whose Left Over Balance and Available Balance are out of sync. When due to some exceptional cases Left Over Balance is decremented and event is not received from Device or vice versa then Left Over Balance can be manually sync to Available Balance.

For Synchronizing, go to **Cafeteria Management > Balance Management > Left Over Balance** and the following screen appears as shown below:



The grid shows list of all active users (Prepaid Server Based + Device-Server Balance Check -Enabled) for whom Left Over Balance is not equal to Actual balance.

Click **Synchronize Balance** for all selected users to make Left Over Balance = Actual balance for current month.

Pre-ordered Meals

Pre-ordered Meals enable the Cafeteria Admin to view and have an estimation about the quantity of food to be prepared on the selected date.

Select **Transaction Management > Pre-ordered Meals** from Cafeteria page. The page appears as shown below:

The screenshot shows the 'Pre-ordered Meals' interface. At the top, there's a title bar with a star and a question mark icon. Below it, a filter section contains a 'Date' field with a calendar icon (set to 05/05/2017), a 'Filter User' dropdown (set to 'All'), and a 'Group/User' section with 'ID' and 'Name' input fields and a list icon. A 'View' button is positioned below these filters. Under the 'Ordered Items' section, there is a search bar. Below the search bar is a table with the following structure:

Menu ID	Name	Item ID	Name	Total Quantity
No Data				

Date: Select the Date for which list of pre-ordered meals is to be viewed.

User: Select the user by filtering from the options of enterprise group or individual user.



The Pre-ordering of items is done from the ESS account of Cafeteria enabled users.

The settings for pre-ordering of meals is done from Cafeteria Management module> Cafeteria Settings > Other Settings.

Click on **View** button to view the ordered list. It shows the date wise list of items which is pre-ordered by the cafeteria users.

This screenshot shows the same 'Pre-ordered Meals' interface as before, but with data in the table. The 'View' button has been clicked, and the table now displays one row of data:

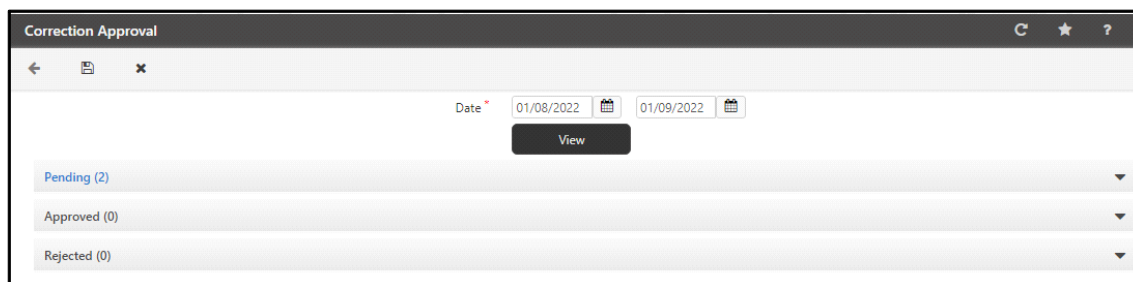
Menu ID	Name	Item ID	Name	Total Quantity
3	Evening snack	5	Puff	4

Correction Approval

The COSEC application allows the users to apply for corrections to existing transactions from the Cafeteria Transaction Correction page of COSEC ESS module. These applications can be authorized by the administrator from the Correction Approval page of the Cafeteria module.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to [“Reporting In-Charge”](#), [“Approval Policy”](#) and [“Configuring Users”](#).

For giving correction approval, go to **Cafeteria Management > Transaction Management > Correction Approval** and the following page appears as shown below:



You can either:

- view all the pending applications for Correction Approval
- set the date filters to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To know more, refer to [“Pending Applications”](#)



The population on this page depends on the server's database. It might take time to load all pending applications.

Applications according to Set Filters

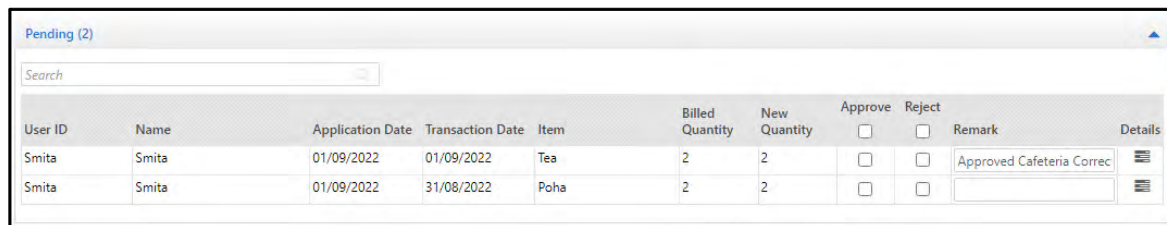
To Set the Filters,

- **Date:** Select this option to enable the date filter. Select the start and end dates by clicking the respective date selection buttons. This defines the period for which the applications are to be viewed.

Click the **View** button to view all the pending, approved and rejected applications.

Pending Applications

Click the **Pending** collapsible panel. All the applications in pending state are displayed.




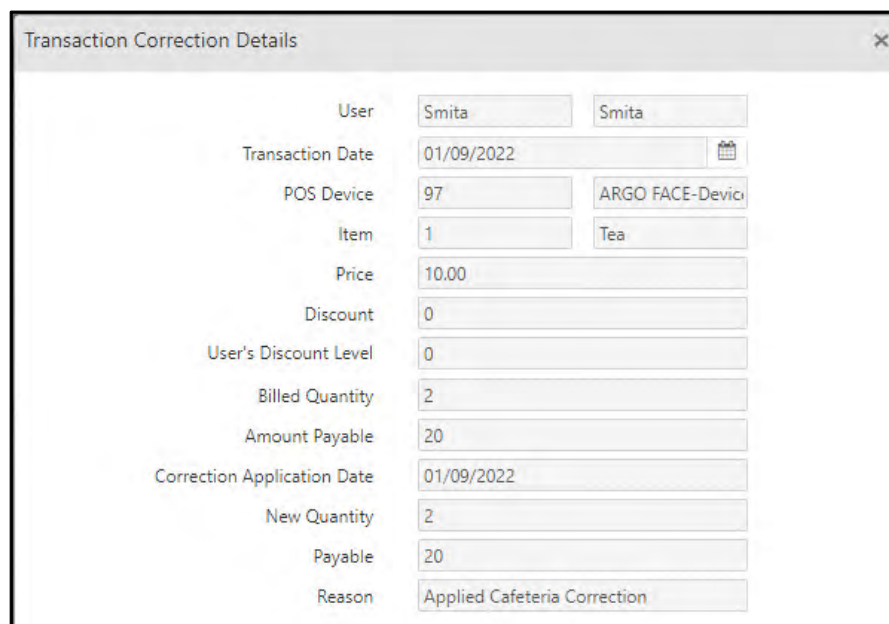
User ID	Name	Application Date	Transaction Date	Item	Billed Quantity	New Quantity	Approve	Reject	Remark	Details
Smita	Smita	01/09/2022	01/09/2022	Tea	2	2	<input type="checkbox"/>	<input type="checkbox"/>	Approved Cafeteria Correc	
Smita	Smita	01/09/2022	31/08/2022	Poha	2	2	<input type="checkbox"/>	<input type="checkbox"/>		

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

The application will be displayed under respective panel.

You also, click **Details**  of view the details of the transaction. The Transaction Correction Details page appears as shown below:




User	Smita	Smita
Transaction Date	01/09/2022	
POS Device	97	ARGO FACE-Device
Item	1	Tea
Price	10.00	
Discount	0	
User's Discount Level	0	
Billed Quantity	2	
Amount Payable	20	
Correction Application Date	01/09/2022	
New Quantity	2	
Payable	20	
Reason	Applied Cafeteria Correction	

Then click on **Save** button to save the authorization.

Approved Applications


Click the **Approved** collapsible panel to view the approved applications and their details.


Approved (1)									
<input type="text" value="Search"/>									
User ID	Name	Application Date	Transaction Date	Item	Billed Quantity	New Quantity	Remark	Details	
Smita	Smita	01/09/2022	01/09/2022	Tea	2	2	Approved Cafeteria Correction		

Click **Details**  of view the details.

Rejected Applications

Click the **Rejected** collapsible panel to view the rejected applications and their details.

Rejected (1)									
<input type="text" value="Search"/>									
User ID	Name	Application Date	Transaction Date	Item	Billed Quantity	New Quantity	Remark	Details	
Smita	Smita	01/09/2022	31/08/2022	Poha	2	2	Rejected Cafeteria Correction		

Click **Details**  of view the details.

Manual Correction

Manual Correction page allows Cafeteria user to modify existing transactions as well as add new transactions.

The Correction can be made by:

- System Account User
- On Behalf System Account User
- Using the ESS Self Service Module (For more details refer COSEC Employee Self Service User Manual)

COSEC Web enables all *System Account users* with appropriate page rights to make Manual Correction using the *Cafeteria* module. All applications made by the System Account user are *pre-approved* by default.

COSEC Web also enables all On Behalf System Account User with appropriate page rights to make Manual Correction using the *Cafeteria* module. All applications made by the On Behalf System Account User are *pre-approved* by default. For creating and assigning the roles and rights to the On Behalf System Account User. Refer to [“On Behalf System Account User”](#).

For doing Manual Correction, go to **Cafeteria Management > Transaction Management > Manual Correction** and the following page appears as shown below:

The screenshot shows the 'Manual Correction' web application interface. On the left, there are input fields for 'User' (with a dropdown menu), 'Transaction Date-Time' (with a date and time picker), 'POS Device' (with a dropdown menu), 'Menu' (with a dropdown menu), 'Item' (with a dropdown menu), 'Application Date' (with a date picker), 'Transaction Value' (with 'Quantity' and 'Payable' fields), 'Correction' (with 'New Quantity' (with a dropdown menu), 'Payable' (with a dropdown menu), 'Reason' (with a text area), 'Application Status' (with a dropdown menu), and 'Remark' (with a text area). On the right, there is a table with the following columns: 'Transaction Date-Time', 'Item', 'Quantity', 'New Quantity', 'Application Date', and 'Status'. The table contains one row with the following data: '15/11/2021 12:00:00', 'Puff', '10', '15/11/2021', and a green checkmark in the 'Status' column.

The page displays configurations on the left hand side and to the right is a grid containing a list of all user's device-based cafeteria transactions as well as transaction correction applications in pending, approved and rejected state.

User: Select a user from the picklist for whom the manual correction is to be made. The transactions of the user will be listed on the right grid.

Select the transaction from the right grid for which correction is to be done.

Manual Correction

User * 12 Geeta_Prepaid user

Transaction Date-Time * 05/05/2017 11:35

POS Device * 7 NGT-34

Menu * 2 Breakfast

Item * 4 Samosa

Application Date 05/05/2017

Transaction Value

Quantity 1

Payable 10.00

Correction

New Quantity * 2

Payable 20.00

Reason punch was not detected second time

Application Status

Remark

Transaction Date-Time	Item	Quantity	New Quantity	Application Date	Status
05/05/2017 11:35:11	Samosa	1			
05/05/2017 11:27:54	Wafers	1			
05/05/2017 11:25:14	Wafers	1			
05/05/2017 11:23:40	Wafers	1			
05/05/2017 11:23:30	Samosa	1			
05/05/2017 11:23:30	Wafers	1			
05/05/2017 11:23:12	Wafers	1			

New Quantity: Enter the value for updating the quantity of item.

Reason: Specify the reason for correction application.

Then Click **Save** button to save the manual correction.

Manual Correction

User * 12 Geeta_Prepaid user

Transaction Date-Time * HH:MM

POS Device * ID Name

Menu * ID Name

Item * ID Name

Application Date

Transaction Value

Quantity

Payable

Correction

Transaction Date-Time	Item	Quantity	New Quantity	Application Date	Status
05/05/2017 11:35:11	Samosa	1	2	05/05/2017	✓
05/05/2017 11:27:54	Wafers	1			
05/05/2017 11:25:14	Wafers	1			
05/05/2017 11:23:40	Wafers	1			
05/05/2017 11:23:30	Samosa	1			
05/05/2017 11:23:30	Wafers	1			
05/05/2017 11:23:12	Wafers	1			

The application will be saved and Status will be shown as above. The application will be approved if correction is done from System Administrator login.

To add a new transaction, select the user and click **New** button.

Transaction Date-Time: Select the date and enter the time on which transaction is to be entered.

POS Device: Select the device using the picklist. The picklist contains devices created from the Devices module and enabled for the Cafeteria application.

Menu: Select the menu from the picklist. The picklist contains menus created from the Menus tab.

Item: Select the item from the picklist. The picklist contains items created from the Items tab.

Application Date: It displays the date on which correction application is being done.

Transaction Value

- **Quantity:** It displays the current quantity.
- **Payable:** It displays the current payable amount calculated at the time of transaction.

Correction

It displays the fields to be corrected.

- **New Quantity:** Enter the new quantity value for the item. When 'Pre-order Based Restriction' is enabled and Deny Transaction is selected in cafeteria usage policy then entered new quantity should not exceed the pre-ordered quantity of selected item for selected menu.
- **Payable:** It displays the payable amount as per the new quantity specified.
- **Reason:** You can enter the reason for correction.
- **Application Status:** It displays the status of application.
- **Remark:** It displays the remark provided from the Transaction Correction Details window of the Correction Approval page.

Click on **Save** button to save the transaction to the grid. The transaction correction application is then sent for transaction approval.

Manual Correction
★ ? ✕

← + ✎ 📄 ✕

Search

🔍

User * 11 Namrata_Postpaid user

Transaction Date-Time * 05/05/2017 13:30

POS Device * 7 NGT-34

Menu * 2 Breakfast

Item * 3 Wafers

Application Date 05/05/2017

Transaction Value

Quantity

Payable

Correction

New Quantity * 2

Payable 10.00

Reason Punches were not detected

Application Status Approved

Remark

Transaction Date-Time

Item Quantity New Quantity Application Date Status

05/05/2017 13:30:00 Wafers 2 05/05/2017 ✓

The application will be approved if correction is done from System Administrator login.

For other users, the Manual Correction Application can be approved by the Reporting In-charge of the user or the administrator. To know more about Correction Approval click on ["Correction Approval"](#).

Transaction Summary

Transaction Summary helps the admin to track/analyze all the transactions in cafeteria management module.



The Monthly process must be run at the end of the month to generate proper cafeteria transactions.

For viewing Transaction Summary, go to **Cafeteria Management > Transaction Management > Transaction Summary** and the following page appears as shown below:

Transaction Summary

Date * 04/05/2017 05/05/2017

Filter User All

Group/User ID Name

View

Purchase (0)

Payment (0)

Recharge (0)

Reset (0)

Manual Credit/Debit (0)

Date: Select the date range by using the Calendar button for which the transaction is to be viewed.

Filter User: Select the user based on Enterprise groups or Individual user.

Group/User: Select the User or Group from the User picklist button.

Click on **View** to view the transactions divided into **Purchase, Payments, Recharge, Reset** and **Manual Credit/Debit**.

The Purchase, Recharge and Manual Credit/ Debit transactions are shown below:

Transaction Summary

Date * 04/05/2017 05/05/2017

Filter User All

Group/User ID Name

View

Purchase (9)

Search

User ID	Name	Transaction Date-Time	POS Device	Item	Unit Price	Discount	Quantity	Payable
13	Dinesh_Pre server based	05/05/2017 13:45	NGT-34	Rice	10	0	1	10.00
11	Namrata_Postpaid user	05/05/2017 13:30	NGT-34	Wafers	5	0	2	10.00
12	Geeta_Prepaid user	05/05/2017 11:35	NGT-34	Samosa	20	10	2	20.00
12	Geeta_Prepaid user	05/05/2017 11:27	NGT-34	Wafers	0	0	1	
12	Geeta_Prepaid user	05/05/2017 11:25	NGT-34	Wafers	0	0	1	
12	Geeta_Prepaid user	05/05/2017 11:23	NGT-34	Wafers	0	0	1	
12	Geeta_Prepaid user	05/05/2017 11:23	NGT-34	Wafers	0	0	1	
12	Geeta_Prepaid user	05/05/2017 11:23	NGT-34	Wafers	0	0	1	
12	Geeta_Prepaid user	05/05/2017 11:23	NGT-34	Wafers	0	0	1	

Purchase (9)

Payment (0)

Recharge(3)

Search

User ID ▲	Name	Transaction Date-Time	Opening Balance	Recharge Amount	Closing Balance
13	Dinesh_Pre server based	05/05/2017 11:41	0	50	50
12	Geeta_Prepaid user	05/05/2017 11:22	0	10	10
12	Geeta_Prepaid user	05/05/2017 10:12	0	50	50

Reset (0)

Manual Credit/Debit (2)

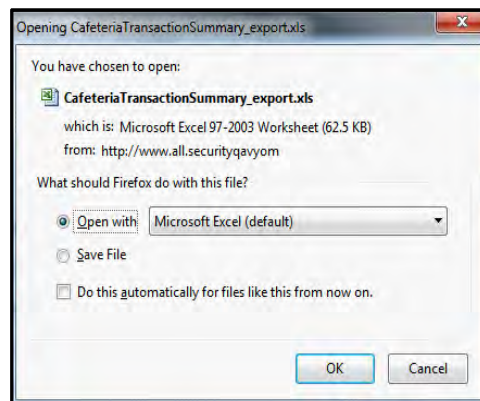
Manual Credit/Debit (2)

Search

User ID ▲	Name	Transaction Date-Time	Adjustment Type	Opening Balance	Adjustment Amount	Closing Balance	Remark
11	Namrata_Postpaid user	05/05/2017 15:48	Debit	0	10	10	
13	Dinesh_Pre server based	05/05/2017 14:45	Debit	50	10	40	

Export

Click on **Export** button. You can open or Save the exported file.



The Cafeteria Transaction Summary will be exported as shown below.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	User ID	Name	Transaction Date-Time	POS Device ID	POS Device Name	Event No	Roll Over Count	Flash Count	Menu ID	Item ID	Item Name	Unit Price	Discount	Quantity
2	PreServer	Prepaid server based	2017/08/17 17:57:92		NGT Direct Door-Device-92 IP78	135	0	1	2	9	test-09	20	0	1
3	caf	caf inactive postpaid user	2017/08/17 17:31:92		NGT Direct Door-Device-92 IP78	127	0	1	2	9	test-09	20	0	1
4	post1	postpaid 1	2017/08/17 17:30:92		NGT Direct Door-Device-92 IP78	124	0	1	2	9	test-09	20	0	1
5	poshtpaid	poshtpaid	2017/08/17 17:03:92		NGT Direct Door-Device-92 IP78	118	0	1	2	8	8-item	10.63	0	1
6	poshtpaid	poshtpaid	2017/08/17 17:03:92		NGT Direct Door-Device-92 IP78	119	0	1	2	9	test-09	20	0	1
7	poshtpaid	poshtpaid	2017/08/17 17:03:92		NGT Direct Door-Device-92 IP78	120	0	1	2	10	item 10	10	0	1
8	poshtpaid	poshtpaid	2017/08/17 16:04:92		NGT Direct Door-Device-92 IP78	114	0	1	2	8	8-item	10.63	0	1
9	poshtpaid	poshtpaid	2017/08/17 16:04:92		NGT Direct Door-Device-92 IP78	115	0	1	2	10	item 10	10	0	1
10	poshtpaid	poshtpaid	2017/08/17 16:01:92		NGT Direct Door-Device-92 IP78	107	0	1	2	2	item2	12.52	0	1
11	poshtpaid	poshtpaid	2017/08/17 16:01:92		NGT Direct Door-Device-92 IP78	108	0	1	2	7	drfydfg	786	0	0
12	poshtpaid	poshtpaid	2017/08/17 16:01:92		NGT Direct Door-Device-92 IP78	109	0	1	2	8	8-item	10.63	0	1
13	poshtpaid	poshtpaid	2017/08/17 16:01:92		NGT Direct Door-Device-92 IP78	110	0	1	2	9	test-09	20	0	1
14	poshtpaid	poshtpaid	2017/08/17 16:01:92		NGT Direct Door-Device-92 IP78	111	0	1	2	10	item 10	10	0	1
15	poshtpaid	poshtpaid	2017/08/17 16:00:92		NGT Direct Door-Device-92 IP78	104	0	1	2	2	item2	12.52	0	2
16	poshtpaid	poshtpaid	2017/08/17 16:00:92		NGT Direct Door-Device-92 IP78	105	0	1	2	8	8-item	10.63	0	1
17	poshtpaid	poshtpaid	2017/08/17 15:27:92		NGT Direct Door-Device-92 IP78	102	0	1	2	8	8-item	10.63	0	2
18	poshtpaid	poshtpaid	2017/08/17 15:09:92		NGT Direct Door-Device-92 IP78	99	0	1	2	2	item2	12.52	0	1
19	poshtpaid	poshtpaid	2017/08/17 15:09:92		NGT Direct Door-Device-92 IP78	100	0	1	2	9	test-09	20	0	1
20	poshtpaid	poshtpaid	2017/08/17 14:20:92		NGT Direct Door-Device-92 IP78	97	0	1	2	9	test-09	20	0	1
21	ca	caf user server	2017/08/17 12:36:22		ngt test fake				2	3	item3	15	0	2
22	post1	postpaid 1	2017/08/17 12:00:22		ngt test fake				1	3	item3	15	0	2
23	post1	postpaid 1	2017/08/17 11:17:92		NGT Direct Door-Device-92 IP78	89	0	1	2	8	8-item	10.63	0	2
24	post1	postpaid 1	2017/08/17 11:17:92		NGT Direct Door-Device-92 IP78	90	0	1	2	9	test-09	20	0	0
25	post1	postpaid 1	2017/08/16 18:03:92		NGT Direct Door-Device-92 IP78	87	0	1	2	9	test-09	20	0	0

Import

Click on **Import** button for importing the Cafeteria transaction summary

Import Transaction Summary

Import Data
For
Import File

Purchase
File Format
XLS
Browse... No file selected.
Upload
Preview Data
Process
Cancel

Import Data For: The Data can be imported for Purchase, Payment, Recharge, Reset and Manual Credit/Debit. You can download the sample import file and enter the data for Cafeteria. Then the updated file can be imported here.

File Format - Select the format for the file to be imported. The options available are XLS or CSV.

Import File - Browse the path of the file and select the file from which the data is to be imported.

Click **Upload** button to save the file.

Import Transaction Summary

Import Data
For
Import File

Purchase
File Format
CSV
Browse... CafeteriaTransactionSummary_import.csv
Upload
Preview Data
Process
Cancel

The **Preview Data** button enables the administrator to view the data in the respective worksheets to confirm that the data is in order prior to giving the process command.

User ID	Name	Transaction Date-Time	POS Device ID	POS Device Name	Event No	Roll Over Count	Flash Count	Menu ID
PreServer	Prepaid server based	2017/08/17 17:57	92	NGT Direct Door-Device-92 IP78	135	0	1	2
caf	caf inactive postpaid user	2017/08/17 17:31	92	NGT Direct Door-Device-92 IP78	127	0	1	2
post1	postpaid 1	2017/08/17 17:30	92	NGT Direct Door-Device-92 IP78	124	0	1	2
poshtpaid	poshtpaid	2017/08/17 17:03	92	NGT Direct Door-Device-92 IP78	118	0	1	2
poshtpaid	poshtpaid	2017/08/17 17:03	92	NGT Direct Door-Device-92	119	0	1	2

Now you can click on **Process** to process the import of data.



The value specified in Name, Transaction Date-Time, Opening Balance & Closing Balance fields will be ignored on import. Hence the presence of these fields in imported sheet is optional.

Process-Monthly Payments

This option enables the administrator to manually run certain processes required for reconciliation of the postpaid user accounts. The following processes will run on selecting this option.

- Updation of users' account details by subtracting the users' allowed usage amount or reset to zero (as set from the Payment page) from the total due amount and recording transactions for the payments processed along with their details.
- If a user is blocked and if after the payment the user's new balance is less than the user's max usage limit, then the user should be unblocked and the change is to be updated to all the canteen devices.
- Perform the same process as that of automatic reset function.

To run the monthly payment process, go to **Cafeteria Management > Process > Monthly Payments** and the following page appears as shown below.

The screenshot shows a web application window titled "Process Monthly Payments". At the top, there is a navigation bar with a back arrow, a star icon, a question mark, and a close button. Below the navigation bar, the "Attendance Period" is set to "February" and "2017". Under the "Select Users" section, there is a "Select Users" dropdown menu currently set to "User Wise". Below this, there are input fields for "User ID" and "Name", with a "Search" button. A table lists the selected users, showing "User ID" and "Name" columns. The table has one row with "07" and "Aditi". A "Process" button is located at the bottom of the form.

User ID	Name
07	Aditi

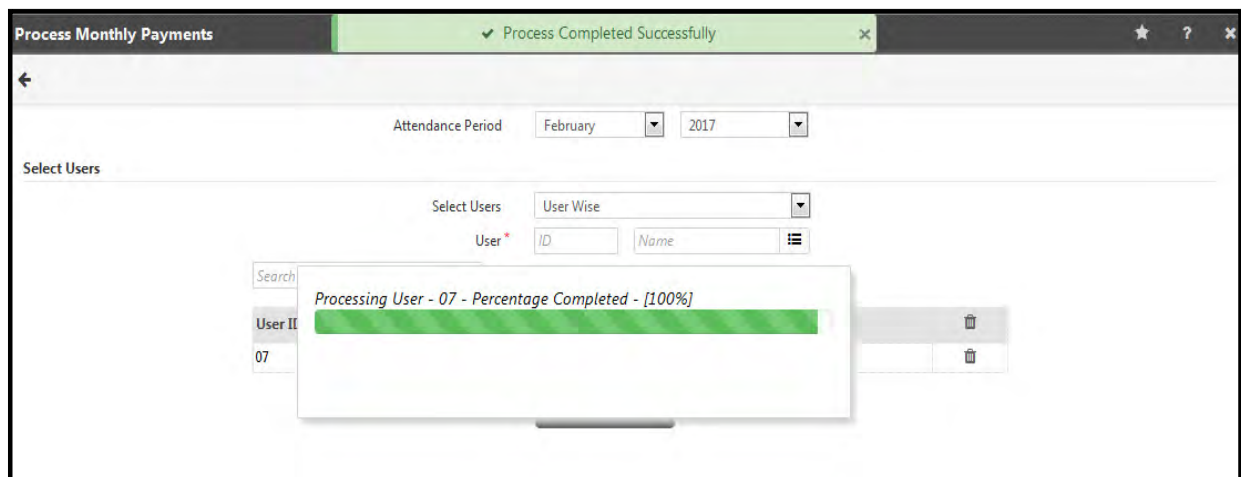
Attendance Period: Select the month and the year for which the monthly payment process is to be run.

The administrator can now select the group of users whose monthly payment is to be processed.

Select Users: The Multiple users can be selected based on the following filter options:

- **User Wise:** Enables administrator to select users from the User Picklist window.
- **Group Wise:** Enables the administrator to select all users belonging to a particular group.
- **All:** Enables administrator to select all active users in the database.

Once the users have been selected, click on the **Process** button to start the process as shown on the screen below.



Cafeteria Monthly Payment Process can also be automated using the Task Scheduler.

*Go to **Admin > System Utilities > Task Scheduler** and select "Cafeteria Payment Process" to automate the Monthly Payment.*

Menu




DADE						Page 1 of 1		
Menu								
Run by: System Admin			Date: 19/08/2022			09:55		
Menu ID: 1		Name: M1		Contains Default Items: Yes		Active: Yes		
Sr. No	Item	Price	Sr. No	Item	Price	Sr. No	Item	Price
1	I1	10.00	2	I2	10.00	3	I3	10.00

Menu Schedule




Menu Scheduling

←

Back



Find...



1 of 1

100%

Main Report

Organization 2

Page 1 of 1

Menu Schedule

Run by: System Admin

Date: 2014/01/18 12:44

Device ID: 4

Device Name: e-cant door

Active: Yes

Sr No	Menu Code	Menu Name	Scheduled Days	Start Time	End Time
1	1	Breakfast	Mon Tue Wed Thu	09:00	10:00
2	2	Lunch	Mon Tue Wed Thu Fri	13:00	14:30

User Reports

Head Count

This report will generate a listing of the total number of users using the Cafeteria service on a given day as shown.

Head Count																																																						
←																																																						
Back																																																						
Find... 1 of 12 100%																																																						
Main Report																																																						
<div> <div>ORGANISATION 1.</div> <div>Page 1 of 12</div> </div> <div> <div>e-Canteen Head Count From 01/01/2012 To 31/12/2012</div> <div>Run by: System Admin Date:11/01/2014 18:45</div> </div> <div> <div>Date: 20/04/2012</div> <table> <tr> <th>Sr No.</th><th>Menu ID</th><th>Menu Name</th><th>Device Name</th><th>Head Count</th></tr> <tr> <td>1</td><td>1</td><td>Lunch HO</td><td>Canteen HO</td><td>39</td></tr> </table> <div>Date: 21/04/2012</div> <table> <tr> <th>Sr No.</th><th>Menu ID</th><th>Menu Name</th><th>Device Name</th><th>Head Count</th></tr> <tr> <td>1</td><td>1</td><td>Lunch HO</td><td>Canteen HO</td><td>32</td></tr> </table> <div>Date: 23/04/2012</div> <table> <tr> <th>Sr No.</th><th>Menu ID</th><th>Menu Name</th><th>Device Name</th><th>Head Count</th></tr> <tr> <td>1</td><td>1</td><td>Lunch HO</td><td>Canteen HO</td><td>49</td></tr> </table> <div>Date: 24/04/2012</div> <table> <tr> <th>Sr No.</th><th>Menu ID</th><th>Menu Name</th><th>Device Name</th><th>Head Count</th></tr> <tr> <td>1</td><td>1</td><td>Lunch HO</td><td>Canteen HO</td><td>39</td></tr> </table> <div>Date: 25/04/2012</div> <table> <tr> <th>Sr No.</th><th>Menu ID</th><th>Menu Name</th><th>Device Name</th><th>Head Count</th></tr> <tr> <td>1</td><td>1</td><td>Lunch HO</td><td>Canteen HO</td><td>39</td></tr> </table> </div>					Sr No.	Menu ID	Menu Name	Device Name	Head Count	1	1	Lunch HO	Canteen HO	39	Sr No.	Menu ID	Menu Name	Device Name	Head Count	1	1	Lunch HO	Canteen HO	32	Sr No.	Menu ID	Menu Name	Device Name	Head Count	1	1	Lunch HO	Canteen HO	49	Sr No.	Menu ID	Menu Name	Device Name	Head Count	1	1	Lunch HO	Canteen HO	39	Sr No.	Menu ID	Menu Name	Device Name	Head Count	1	1	Lunch HO	Canteen HO	39
Sr No.	Menu ID	Menu Name	Device Name	Head Count																																																		
1	1	Lunch HO	Canteen HO	39																																																		
Sr No.	Menu ID	Menu Name	Device Name	Head Count																																																		
1	1	Lunch HO	Canteen HO	32																																																		
Sr No.	Menu ID	Menu Name	Device Name	Head Count																																																		
1	1	Lunch HO	Canteen HO	49																																																		
Sr No.	Menu ID	Menu Name	Device Name	Head Count																																																		
1	1	Lunch HO	Canteen HO	39																																																		
Sr No.	Menu ID	Menu Name	Device Name	Head Count																																																		
1	1	Lunch HO	Canteen HO	39																																																		

User Transactions

This report generates a user wise or device wise list of transactions for the selected date range. The user wise list of transactions report is shown.

User Transactions

Back

Find...

1 of 1

100%

Main Report

Organization 2

Page 1 of 1

User-Wise Transactions From 2014/01/01 To 2014/01/18

Run by: System Admin

Date:2014/01/18 12:46

User ID 4 User Name Meera

Sr No	DateTime	Device Name	Previous Balance	Transaction Amount	Transaction
1	2014/01/16 12:36	System	0.0	400.0	Adjustment

User ID 5 User Name Resham

Sr No	DateTime	Device Name	Previous Balance	Transaction Amount	Transaction
1	2014/01/16 12:37	System	0.0	350.0	Adjustment

Users Account Details

This report generates a detailed list of users' account details, who have been assigned the Cafeteria application as shown.

Users Account Details																																																																							
Back																																																																							
Find... 1 of 1 100%																																																																							
Main Report																																																																							
<div> <div>Organization 2</div> <div>Page 1 of 1</div> </div> <div> <div>ORGANIZATION-Wise Users e-Canteen Account Details</div> <div>Run by: System Admin Date:2014/01/18 12:54</div> </div> <div> <div>Organization-1</div> <table> <tr> <th>Sr No</th><th>User ID</th><th>Name</th><th>Account Type</th><th>Discount Level</th><th>Allowed Usage</th><th>Max Usage Limit</th><th>Blocked Status</th></tr> <tr> <td>1</td><td>1</td><td>Namrata D</td><td>Postpaid</td><td>Level 1</td><td>300.0</td><td>0.0</td><td></td></tr> <tr> <td>2</td><td>1000</td><td>Khushbu</td><td>Postpaid</td><td>Level 1</td><td>300.0</td><td>0.0</td><td></td></tr> <tr> <td>3</td><td>151</td><td>Sheetal</td><td>Postpaid</td><td>Level 1</td><td>200.0</td><td>0.0</td><td></td></tr> <tr> <td>4</td><td>3</td><td>Ananya</td><td>Postpaid</td><td>Level 1</td><td>300.0</td><td>0.0</td><td></td></tr> <tr> <td>5</td><td>4</td><td>Meera</td><td>Prepaid</td><td>Level 1</td><td>0.0</td><td>0.0</td><td></td></tr> <tr> <td>6</td><td>5</td><td>Resham</td><td>Postpaid</td><td>Level 1</td><td>300.0</td><td>300.0</td><td>Blocked</td></tr> <tr> <td>7</td><td>6</td><td>Aayaan</td><td>Postpaid</td><td>Level 1</td><td>300.0</td><td>0.0</td><td></td></tr> </table> </div>								Sr No	User ID	Name	Account Type	Discount Level	Allowed Usage	Max Usage Limit	Blocked Status	1	1	Namrata D	Postpaid	Level 1	300.0	0.0		2	1000	Khushbu	Postpaid	Level 1	300.0	0.0		3	151	Sheetal	Postpaid	Level 1	200.0	0.0		4	3	Ananya	Postpaid	Level 1	300.0	0.0		5	4	Meera	Prepaid	Level 1	0.0	0.0		6	5	Resham	Postpaid	Level 1	300.0	300.0	Blocked	7	6	Aayaan	Postpaid	Level 1	300.0	0.0	
Sr No	User ID	Name	Account Type	Discount Level	Allowed Usage	Max Usage Limit	Blocked Status																																																																
1	1	Namrata D	Postpaid	Level 1	300.0	0.0																																																																	
2	1000	Khushbu	Postpaid	Level 1	300.0	0.0																																																																	
3	151	Sheetal	Postpaid	Level 1	200.0	0.0																																																																	
4	3	Ananya	Postpaid	Level 1	300.0	0.0																																																																	
5	4	Meera	Prepaid	Level 1	0.0	0.0																																																																	
6	5	Resham	Postpaid	Level 1	300.0	300.0	Blocked																																																																
7	6	Aayaan	Postpaid	Level 1	300.0	0.0																																																																	

User Consumption

This report generates a listing of the user consumption for the selected month as shown.

User Consumption																																																											
Back																																																											
Find... 1 of 11 100%																																																											
Main Report																																																											
<div> <div>ORGANISATION 1.</div> <div>Page 1 of 11</div> </div> <div> <div>Organization-</div> <div>Run by: System Admin Date:18/01/2014 15:16</div> </div> <div> <div>Organization : ORGANISATION 1.</div> <table> <tr> <th>Sr No</th><th>User ID</th><th>Name</th><th>Total Amount</th><th>Total Discount</th><th>Total Due</th></tr> <tr> <td>1</td><td>1053</td><td>JINU SAM</td><td>880.0</td><td>440.0</td><td>440.0</td></tr> <tr> <td>2</td><td>1054</td><td>FARSHV SHAH</td><td>760.0</td><td>380.0</td><td>380.0</td></tr> <tr> <td>3</td><td>1055</td><td>SANDIP PATEL</td><td>670.0</td><td>335.0</td><td>335.0</td></tr> <tr> <td>4</td><td>1056</td><td>RITESH RAJPUT</td><td>680.0</td><td>340.0</td><td>340.0</td></tr> <tr> <td>5</td><td>1057</td><td>JANPRIYA MALVIYA</td><td>840.0</td><td>420.0</td><td>420.0</td></tr> <tr> <td>6</td><td>1059</td><td>PRATIK PATEL</td><td>740.0</td><td>370.0</td><td>370.0</td></tr> <tr> <td>7</td><td>1060</td><td>FRIYESH SHAH</td><td>1040.0</td><td>520.0</td><td>520.0</td></tr> <tr> <td>8</td><td>1061</td><td>DARSHAN PATEL</td><td>960.0</td><td>480.0</td><td>480.0</td></tr> </table> </div>						Sr No	User ID	Name	Total Amount	Total Discount	Total Due	1	1053	JINU SAM	880.0	440.0	440.0	2	1054	FARSHV SHAH	760.0	380.0	380.0	3	1055	SANDIP PATEL	670.0	335.0	335.0	4	1056	RITESH RAJPUT	680.0	340.0	340.0	5	1057	JANPRIYA MALVIYA	840.0	420.0	420.0	6	1059	PRATIK PATEL	740.0	370.0	370.0	7	1060	FRIYESH SHAH	1040.0	520.0	520.0	8	1061	DARSHAN PATEL	960.0	480.0	480.0
Sr No	User ID	Name	Total Amount	Total Discount	Total Due																																																						
1	1053	JINU SAM	880.0	440.0	440.0																																																						
2	1054	FARSHV SHAH	760.0	380.0	380.0																																																						
3	1055	SANDIP PATEL	670.0	335.0	335.0																																																						
4	1056	RITESH RAJPUT	680.0	340.0	340.0																																																						
5	1057	JANPRIYA MALVIYA	840.0	420.0	420.0																																																						
6	1059	PRATIK PATEL	740.0	370.0	370.0																																																						
7	1060	FRIYESH SHAH	1040.0	520.0	520.0																																																						
8	1061	DARSHAN PATEL	960.0	480.0	480.0																																																						

Credit/Debit







This report generates a listing of each postpaid user's monthly credit due as shown.

Credit/Debit

★

←

Back

   Find...    1 of 8 100%

Main Report

ORGANISATION 1.

Page 1 of 8

Organization-Wise User Credit/Debit for the Month JANUARY-2013

Run by: System Admin

Date: 18/01/2014 15:17

Organization : ORGANISATION 1.

Sr No	User ID	Name	Carryover Due	Current Due	Payment	Outstanding Due
1	1053	JINU SAM	0.0	420.0	420.0	0.0
2	1054	PARSHV SHAH	0.0	380.0	380.0	0.0
3	1055	SANDIP PATEL	0.0	335.0	335.0	0.0
4	1056	RITESH RAJPUT	0.0	320.0	320.0	0.0
5	1057	JANPRIYA MALVIYA	0.0	400.0	400.0	0.0
6	1059	PRATIK PATEL	0.0	370.0	370.0	0.0
7	1060	PRIYESH SHAH	0.0	500.0	500.0	0.0
8	1061	DARSHAN PATEL	0.0	460.0	460.0	0.0
9	1062	MANTHAN PATEL	0.0	40.0	40.0	0.0

Blocked Users

This report generates a listing of all the Cafeteria users currently blocked in the system.

Blocked Users							
←							
Find... 1 of 1 100%							
Main Report							
ORGANISATION 1.							
Blocked Users							
Run by: System Admin				Date: 18/01/2014 15:19			
Sr No	User ID	Name	Current Acc Type	Discount Level	Max Usage Limit	Total Due	Blocked on
1	1255	SUDESHNA NIYOGI	Postpaid	Level 1	600.0	60.0	16/01/2014
2	1256	VISHAL HARGUNANI	Postpaid	Level 1	600.0	245.0	16/01/2014
3	1257	VIHARKUMAR SONI	Postpaid	Level 1	600.0	200.0	16/01/2014
4	1263	AASHISH GANDHI	Postpaid	Level 1	600.0	20.0	16/01/2014
5	1265	PARIKSHIT PANDEY	Postpaid	Level 1	600.0	200.0	16/01/2014
6	1266	ASHUTOSH PATHAK	Postpaid	Level 1	600.0	200.0	16/01/2014
7	1267	PRATIK PAREKH	Postpaid	Level 1	600.0	180.0	16/01/2014
8	1268	KEYURKUMAR ZINABHAI PATEL	Postpaid	Level 1	600.0	160.0	16/01/2014
9	1269	MAITRI THAKKAR	Postpaid	Level 1	600.0	60.0	16/01/2014

Cafeteria Reports

Sales

This report will generate a listing of the total sales per menu on a day in the cafeteria.



For a Cafeteria Item, there will be multiple entries for each discount level (maximum entries as per the discount levels are 5 (Maximum Discount Level: Level 0, Level 1, Level 2, Level 3 and Level 4).

Duplicate entries in the report can be displayed in cases where transactions for an item with and without discount level are encountered, wherein the discount level is applied but the discount amount is set to 0.00.

Sales

Back

Find... 1 of 64 100%

Main Report

ORGANISATION 1.

Page 1 of 64

Sales From 18/01/2013 To 18/05/2013

Run by: System Admin Date: 18/01/2013 15:25

ORGANISATION 1.

Date: 18/01/2013 Total Sales Amount: 460.0 Total Discount: 205.0

Sr No	Item Code	Item Name	Total Quantity	Unit Price	Total Sales	Discount@			
						Level 1	Level 2	Level 3	Level 4
1	1	Lunch	9	40.0	360.0	180.0	0.0	0.0	0.0
2	1	Lunch	2	40.0	80.0	0.0	20.0	0.0	0.0
3	2	Breakfast	2	10.0	20.0	0.0	5.0	0.0	0.0
Total Amount:					460.0	180.0	25.0	0.0	0.0

Date: 19/01/2013 Total Sales Amount: 330.0 Total Discount: 155.0

Sr No	Item Code	Item Name	Total Quantity	Unit Price	Total Sales	Discount@			
						Level 1	Level 2	Level 3	Level 4
1	1	Lunch	7	40.0	280.0	140.0	0.0	0.0	0.0
2	1	Lunch	1	40.0	40.0	0.0	10.0	0.0	0.0
3	2	Breakfast	1	10.0	10.0	5.0	0.0	0.0	0.0
Total Amount:					330.0	145.0	10.0	0.0	0.0

In the screen below:

- First entry is when the Discount Level is set as 0.
- Third entry is when the Discount Level is applied but the Discount Amount is set to 0.00.

1 of 1

100%

Organization-1

Page 1 of 1

Sales From 13/06/2022 To 13/06/2022

Run by: System Admin

Date: 20/06/2022 09:54

Organization-1

Date: 13-06-2022

Total Sales Amount: 70.00

Total Discount: 14.00

Sr No	Item Name ID	Total Quantity	Unit Price	Total Sales	Discount @			
					Level 1	Level 2	Level 3	Level 4
1	2 Dinner	2	10.00	20.00	0.00	0.00	0.00	0.00
2	2 Dinner	1	10.00	10.00	2.00	0.00	0.00	0.00
3	2 Dinner	2	10.00	20.00	0.00	4.00	0.00	0.00
4	2 Dinner	1	10.00	10.00	0.00	0.00	0.00	0.00
5	2 Dinner	1	10.00	10.00	0.00	0.00	0.00	8.00
Total Amount:				70.00	2.00	4.00	0.00	8.00

Device-Wise Consumption

This report displays device-wise details of the items consumed for a selected date range on the selected cafeteria devices.




You can select the format as *Daily Item Consumption* or *Item Consumption Summary*.

Device-Wise Consumption




★

←

Back

Find...

1 of 1

100%

Main Report

org3

Page 1 of 1

Device-Wise Consumption From 15/05/2016 To 29/05/2016

Run by: System Admin

Date:31/05/2016 12:36

Device ID	Device Name	Menu ID	Menu Name	Menu Consumption	Item ID	Item Name	Item Consumption	Payable Amount
16/05/2016								
22	NGT Direct Door-Device-22	1	Menu1	2	1	B. Pakoda	2	10.00
					2	parantha	0	0.00
					14	I14	0	0.00
					24	I24	0	0.00
41	Wireless Door-Device-41	1	Menu1	2	1	B. Pakoda	2	10.00
Total:							4	20.00
17/05/2016								
22	NGT Direct Door-Device-22	1	Menu1	12	1	B. Pakoda	6	27.75
					2	parantha	2	20.00
					3	sandwich	0	0.00
					4	Pizza	3	131.13
					5	Poha	1	1.56
41	Wireless Door-Device-41	1	Menu1	31	1	B. Pakoda	24	112.35
					2	parantha	3	27.50
					4	Pizza	4	179.70
Total:							43	499.99

Item-Wise Consumption

This report will generate a listing of the total number of items consumed on a given day in the cafeteria.

Item-wise Consumption																																																																																																																																																																							
Back																																																																																																																																																																							
Find... 1 of 185 100%																																																																																																																																																																							
Main Report																																																																																																																																																																							
<div> <div>ORGANISATION 1.</div> <div>Page 1 of 185</div> </div> <div> <div>Item-Wise Consumption from 18/01/2013 to 18/02/2013</div> <div>Run by: System Admin</div> <div>Date:18/01/2014 15:31</div> </div> <table> <tr> <th>Sr No</th><th>Item Code</th><th>Item Name</th><th>Quantity</th><th>Price/Item</th><th>Total Price</th><th>Total Discount</th><th>Total Payable</th></tr> <tr> <td colspan="8">User ID : 10</td></tr> <tr> <td colspan="8">Date : 06/02/2013</td></tr> <tr> <td>1</td><td>3</td><td>Lunch Fac</td><td>1</td><td>36.0</td><td>36.0</td><td>18.0</td><td>18.0</td></tr> <tr> <td colspan="5">Total</td><td>36.0</td><td>18.0</td><td>18.0</td></tr> <tr> <td colspan="8">Date : 07/02/2013</td></tr> <tr> <td>1</td><td>3</td><td>Lunch Fac</td><td>1</td><td>36.0</td><td>36.0</td><td>18.0</td><td>18.0</td></tr> <tr> <td colspan="5">Total</td><td>36.0</td><td>18.0</td><td>18.0</td></tr> <tr> <td colspan="8">Date : 08/02/2013</td></tr> <tr> <td>1</td><td>3</td><td>Lunch Fac</td><td>1</td><td>36.0</td><td>36.0</td><td>18.0</td><td>18.0</td></tr> <tr> <td colspan="5">Total</td><td>36.0</td><td>18.0</td><td>18.0</td></tr> <tr> <td colspan="8">Date : 09/02/2013</td></tr> <tr> <td>1</td><td>3</td><td>Lunch Fac</td><td>1</td><td>36.0</td><td>36.0</td><td>18.0</td><td>18.0</td></tr> <tr> <td colspan="5">Total</td><td>36.0</td><td>18.0</td><td>18.0</td></tr> <tr> <td colspan="8">Date : 11/02/2013</td></tr> <tr> <td>1</td><td>3</td><td>Lunch Fac</td><td>1</td><td>36.0</td><td>36.0</td><td>18.0</td><td>18.0</td></tr> <tr> <td colspan="5">Total</td><td>36.0</td><td>18.0</td><td>18.0</td></tr> <tr> <td colspan="8">Date : 12/02/2013</td></tr> <tr> <td>1</td><td>3</td><td>Lunch Fac</td><td>1</td><td>36.0</td><td>36.0</td><td>18.0</td><td>18.0</td></tr> <tr> <td colspan="5">Total</td><td>36.0</td><td>18.0</td><td>18.0</td></tr> </table>								Sr No	Item Code	Item Name	Quantity	Price/Item	Total Price	Total Discount	Total Payable	User ID : 10								Date : 06/02/2013								1	3	Lunch Fac	1	36.0	36.0	18.0	18.0	Total					36.0	18.0	18.0	Date : 07/02/2013								1	3	Lunch Fac	1	36.0	36.0	18.0	18.0	Total					36.0	18.0	18.0	Date : 08/02/2013								1	3	Lunch Fac	1	36.0	36.0	18.0	18.0	Total					36.0	18.0	18.0	Date : 09/02/2013								1	3	Lunch Fac	1	36.0	36.0	18.0	18.0	Total					36.0	18.0	18.0	Date : 11/02/2013								1	3	Lunch Fac	1	36.0	36.0	18.0	18.0	Total					36.0	18.0	18.0	Date : 12/02/2013								1	3	Lunch Fac	1	36.0	36.0	18.0	18.0	Total					36.0	18.0	18.0
Sr No	Item Code	Item Name	Quantity	Price/Item	Total Price	Total Discount	Total Payable																																																																																																																																																																
User ID : 10																																																																																																																																																																							
Date : 06/02/2013																																																																																																																																																																							
1	3	Lunch Fac	1	36.0	36.0	18.0	18.0																																																																																																																																																																
Total					36.0	18.0	18.0																																																																																																																																																																
Date : 07/02/2013																																																																																																																																																																							
1	3	Lunch Fac	1	36.0	36.0	18.0	18.0																																																																																																																																																																
Total					36.0	18.0	18.0																																																																																																																																																																
Date : 08/02/2013																																																																																																																																																																							
1	3	Lunch Fac	1	36.0	36.0	18.0	18.0																																																																																																																																																																
Total					36.0	18.0	18.0																																																																																																																																																																
Date : 09/02/2013																																																																																																																																																																							
1	3	Lunch Fac	1	36.0	36.0	18.0	18.0																																																																																																																																																																
Total					36.0	18.0	18.0																																																																																																																																																																
Date : 11/02/2013																																																																																																																																																																							
1	3	Lunch Fac	1	36.0	36.0	18.0	18.0																																																																																																																																																																
Total					36.0	18.0	18.0																																																																																																																																																																
Date : 12/02/2013																																																																																																																																																																							
1	3	Lunch Fac	1	36.0	36.0	18.0	18.0																																																																																																																																																																
Total					36.0	18.0	18.0																																																																																																																																																																

Daily Consumption

This report generates a listing of the daily consumption for the selected month, user and item. Also report can be viewed either item wise or user wise for the selected date range. The user wise report is shown below.

Daily Consumption									
←									
Back									
Find... 1 of 1 100%									
Main Report									
ORGANISATION 1.									
User-Wise Daily Consumption From 10/01/2013 To 15/01/2013									
Run by: System Admin						Date: 29/07/2014		05:14	
Sr No	Date	Item ID	Item Name	Quantity	Price/Item	Total Price	Total Discount	Total Payable	
1002	MEGHA H SHUKLA								
1	12/01/2013	1	Lunch	1	40.0	40.0	20.0	20.0	
			Total :	1	40.0	40.0	20.0	20.0	
1004	DARSHAK B PATEL								
1	10/01/2013	1	Lunch	1	40.0	40.0	20.0	20.0	
2	11/01/2013	1	Lunch	1	40.0	40.0	20.0	20.0	
3	12/01/2013	1	Lunch	1	40.0	40.0	20.0	20.0	
			Total :	3	120.0	120.0	60.0	60.0	

Monthly Consumption

This report generates a listing of the monthly consumption for the selected month, user and item. Also report can be viewed either item wise or user wise for the selected date range. The user wise report is shown below.

Monthly Consumption									
←									
Back									
Find... 1 of 1 100%									
Main Report									
ORGANISATION 1.									
User-Wise Monthly Consumption From 18/01/2013 To 29/01/2013									
Run by: System Admin						Date: 29/07/2014		05:18	
Id	Item Code	Item Name	Quantity	Price/Item	Total Price	Total Discount	Total Payable		
1001	ANKITKUMAR SOHLIYA								
1	1	Lunch	9	40.0	360.0	180.0	180.0		
		Total :	9	40.0	360.0	180.0	180.0		
1004	DARSHAK B PATEL								
1	1	Lunch	4	40.0	160.0	80.0	80.0		
2	2	Breakfast	5	10.0	50.0	25.0	25.0		
		Total :	9	50.0	210.0	105.0	105.0		

Cafeteria Devices

E-canteen Devices

←

Find... 1 of 1 100%

Main Report

ORGANISATION 1.
E-canteen Devices

Page 1 of 1

Run by: System Admin Date: 18/01/2014 15:35

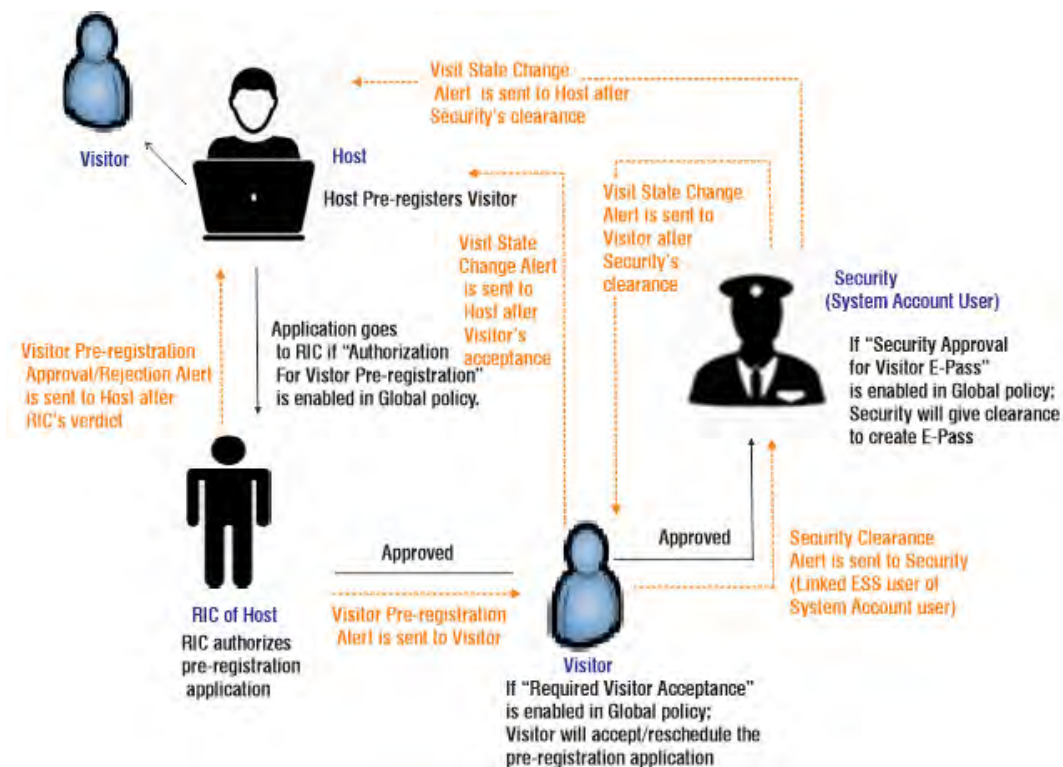
Device ID	Device Name	Printer	Printer Type	Baud Rate	Company Name	Company Address	Punch Line
16	Canteen HO	EpsonTM88IV	USB	115200	Matrix Comsec Pvt. Ltd.		ALWAYS RESPECT THE FOOD.....!!
27	Canteen Factory	None	RS232	115200			

The COSEC VMS tracks and manages visitors to the organization increasing overall security and enhancing productivity of security and reception personnel.

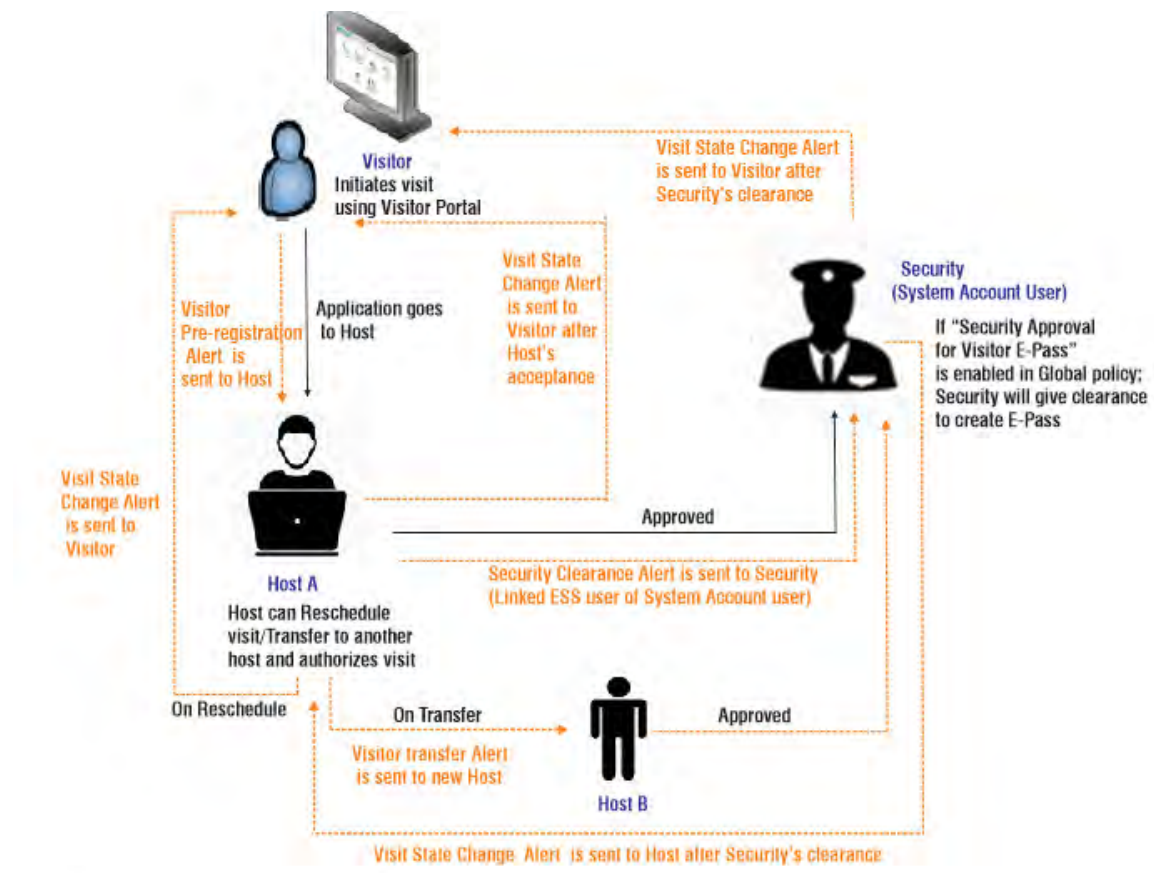



This functionality is not available with the COSEC Application basic platform license.

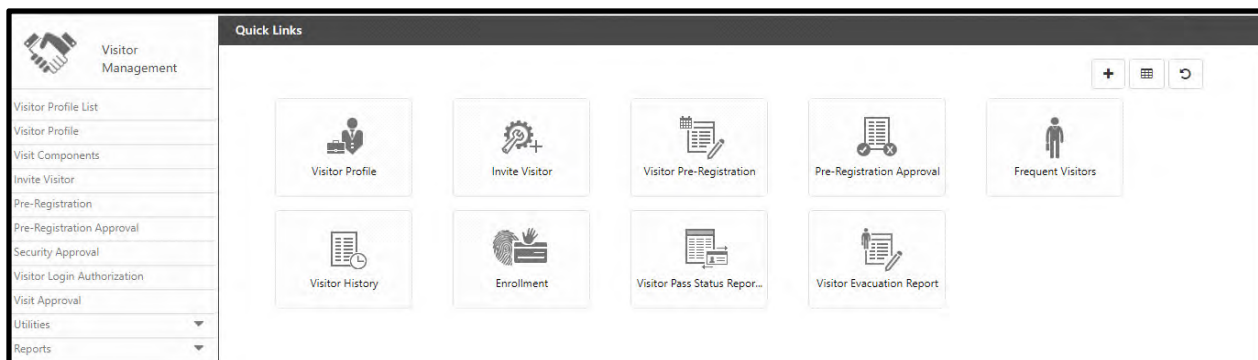
Host Initiated Visit




Visitor Initiated Visit





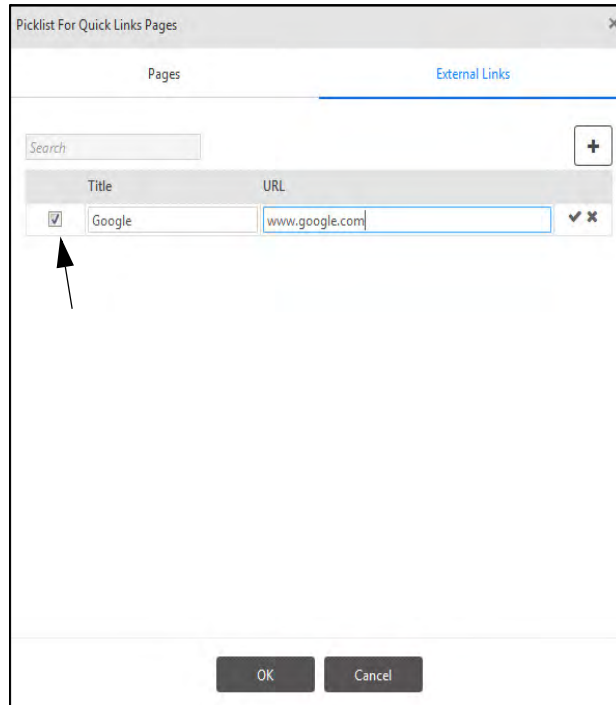
To use the Visitor Management functionality, Click on **Visitor Management**  Module. The Visitor Management Page will appear on your screen.



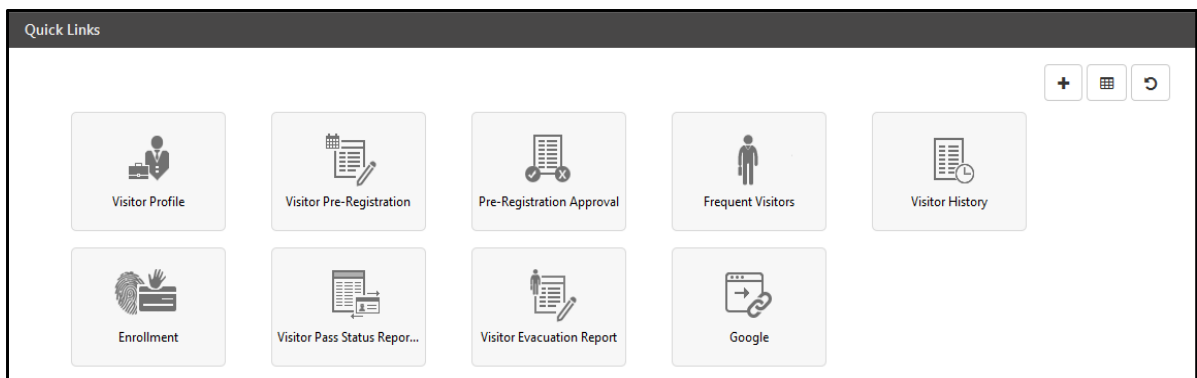
The page displays a menu and **Quick Links** to go to the required page in just one click. Quick Links are shortcuts to reach to a specific page easily. It also contains following three buttons:



- **Add Quick Link:** Click  button to add a quick link. A picklist for Quick Link pages appears for selecting the page or External Link for which the quick link is to be created. Maximum **20** quick links can be added.
- For Adding **Pages** in Quick Link, Select the Pages and click on OK

- For Adding **External Links**, Select External Link tab, click on  button to add new external link.
- Configure the **Title** and **URL** of the external link under the respective fields.click on checkbox to get the configured link on quick link screen as shown below. To save the configuration click on  .



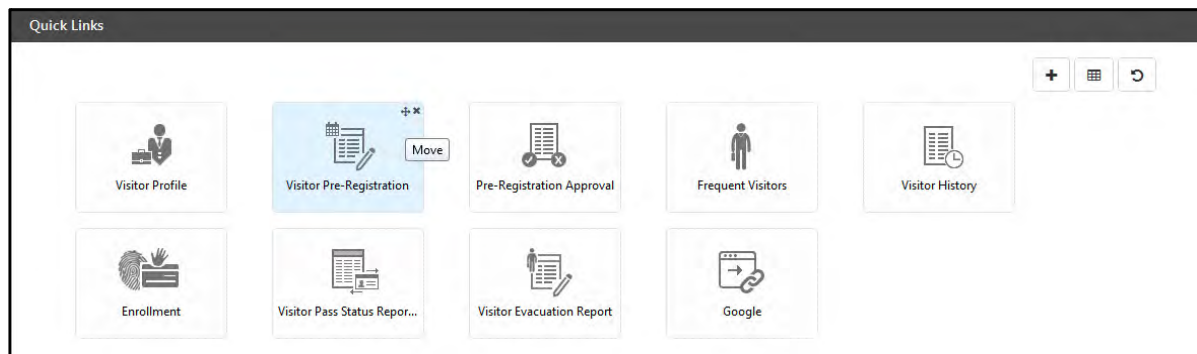
- To edit the saved configuration, click on  .
- Click on OK to save the link configuration on Quick Link screen. The external link will be displayed as shown below:



- **Select Layout:** Click  button to select a layout for the quick links.You can select 5x4 or 4x5 layout to manage the quick links.
- **Reset Quick Links:** Click  button to reset the quick links to the default quick links.

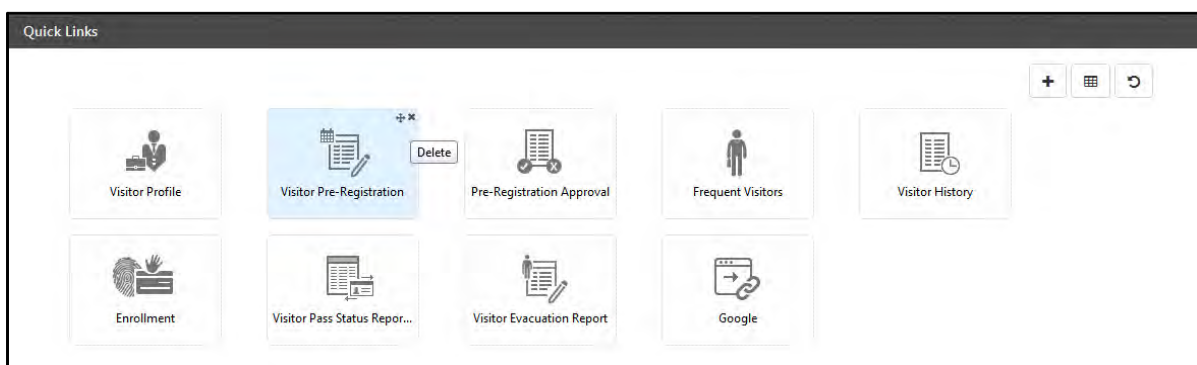
Move the Link

To move the link from one place to another, hover on the link on top right corner and click on “Move” icon as shown below. Then drag the quick link to the desired place. It will be placed at the desired location on the quick links page.




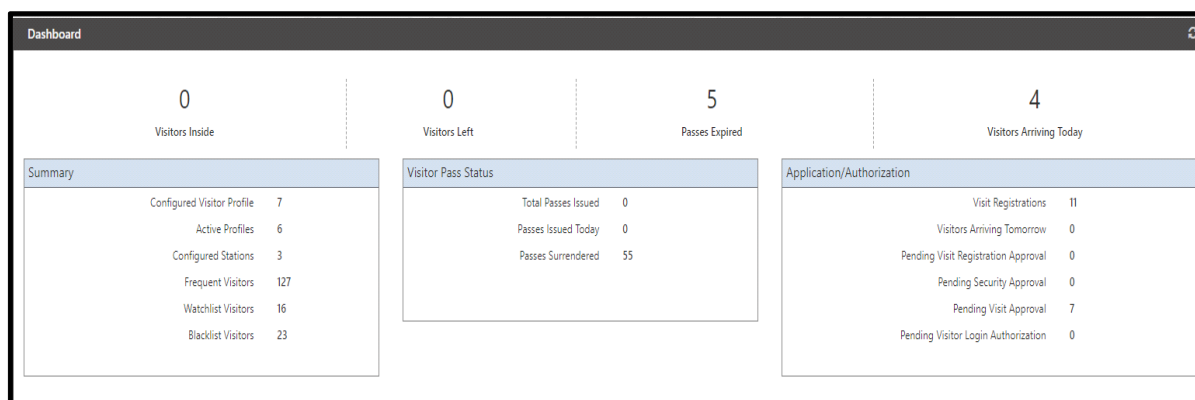
Delete the Link

To delete a particular link, hover on the link on top right corner and click on “Delete” icon as shown below.



Visitor Management Dashboard

To view the **Visitor Management** Dashboard, click the Dashboard button  on the **Visitor Management** page and the following screen appears.



The Dashboard displays the basic information on VMS module relating to the COSEC Software under the following groups:

- **Visitors Inside**- Total number of visitors whose pass is created on the current day and Visit Start time has begun.
- **Visitors Left**- Total number of visitors whose passes have been surrendered.
- **Passes Expired**- Total number of the visitors whose Visit time has ended but passes have not been surrendered.
- **Visitors Arriving Today**- Total number of Pre-registrations of visitor who are arriving on current day.Count of only Approved visitors is displayed who belong to the Host users as per logged in System Account's User Rights.

Example: Suppose DN is system account user having rights of Organization R&D and AS is system account user having rights of Organization HO (Group-wise rights).

When DN logs into COSEC Web then VMS dashboard will show visitor registration details made by the host users belonging to R&D only. DN cannot view the details of visitors of HO.

Summary

- Configured Visitor Profile- Total number of visitor profiles created in system.
- Active Profiles- Total number of visitor profiles which are currently Active.
- Configured Stations- Total number of Stations configured in the System.
- Frequent Visitors- Total number of visitors registered in the module.
- Watchlist Visitors- Total number of visitors added to the watchlist.
- Blacklist Visitors- Total number of visitors added to the Blacklist

Visitor Pass Status

- Total Passes Issued- Total number of passes created from all stations which have not yet been surrendered or expired.
- Passes Issued today- Total number of passes that are created today from all stations.
- Passes Surrendered- Total number of expired passes which have been surrendered.

Application/Authorization

- Visit Registrations- Total number of Pre-registrations of visitor whose arriving date is either current day or future date who belong to the Host users as per logged in System Account's User Rights.



Along with current logic, only Host Initiated Visitor Pre-Registration applications will be considered for count.

- Visitors Arriving Tomorrow- Total number of Pre-registrations of visitor whose arriving date is current date +1; who belong to the Host users as per logged in System Account's User Rights.
- Pending Authorization- Total number of Pre-registrations whose authorization is pending; who belongs to the Host users as per logged in System Account's User Rights.



Along with current logic, Only Host Initiated Visitor Pre-Registration applications will be considered for count.

- Pending Visit Registration Approval- It displays the number of visits initiated by Host or Visitor pending for approval by the RIC.
- Pending Security Approval- Total number of visit request for which security clearance is pending.
- Pending Visit Approval- It displays the number of visits initiated by the Visitor pending for approval by the Host.

- Pending Visitor Login Authorization- The number of pending authorizations when the visitor accesses the **Skip to Login** feature while logging in into the Visitor Web Portal.

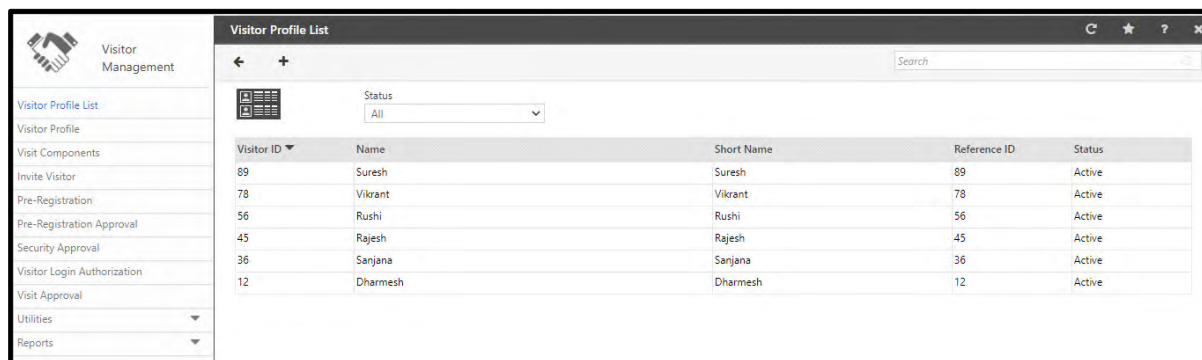
For more information on the above Dashboard options, click the respective information links on the Dashboard.

The latest values on Dashboard are updated on clicking the Refresh  button.

Visitor Profile List

The Visitor Profile List displays all the visitor profiles configured in COSEC.

To view the existing visitors or to add a new visitor, click on the option **Visitor Profile List** from Visitor Management module. The Page appears as shown below:



Visitor ID	Name	Short Name	Reference ID	Status
89	Suresh	Suresh	89	Active
78	Vikrant	Vikrant	78	Active
56	Rushi	Rushi	56	Active
45	Rajesh	Rajesh	45	Active
36	Sanjana	Sanjana	36	Active
12	Dharmesh	Dharmesh	12	Active

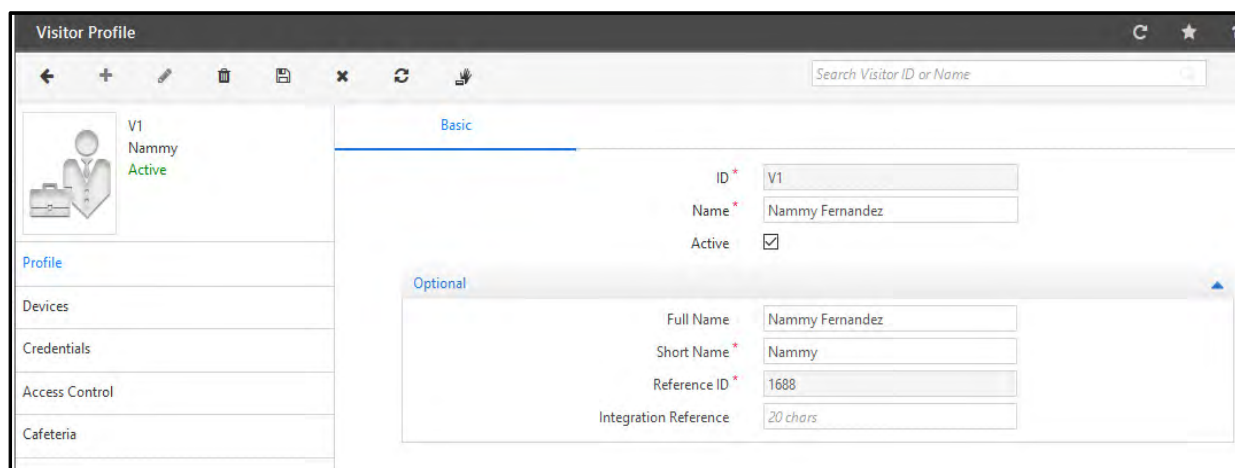
The Visitor Profile List will display only those profiles for which rights are assigned to the SA, that is as per the enterprise groups assigned to the visitor profile.

For example, if for Visitor Profile1 in Groups, Organization is ORG1 and if the rights for ORG1 are not assigned to the SA, then through the SA login the Visitor Profile List will not display Visitor Profile1.

For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#) as well as [“Group”](#) under [“Visitor Profile”](#).

Adding Visitor

To add a new visitor, click on **New** button. The Visitor Profile page will appear.



Visitor Profile

Search Visitor ID or Name

Basic

ID * V1

Name * Nammy Fernandez

Active ☒

Optional

Full Name Nammy Fernandez

Short Name * Nammy

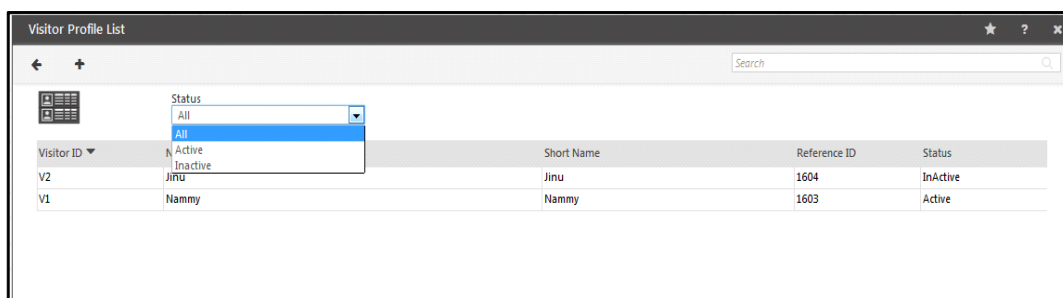
Reference ID * 1688


Integration Reference 20 chars

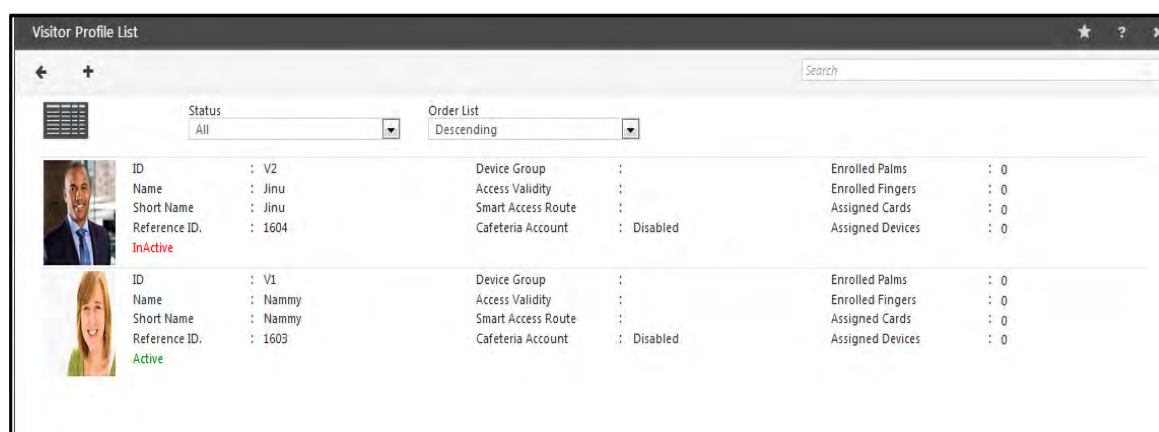
Enter the **ID** and **Name** of the visitor. Then save the details. The Visitor will be added to the list. For detailed configuration see **VMS module> Visitor Profile**.

Viewing Visitor List

The user can view the visitor profiles based on **All/ Active/ Inactive** Status by selecting the desired filter.



Click on the **Photo View**  button on the left. The Visitor Profile information with the photograph is displayed as shown below.



Visitor Profile

Visitor Profile page enables to add the visitor, assign devices to visitor, enroll the credentials and configure visitor for Cafeteria and Access Control policies.

- "Profile"
- "Devices"
- "Credentials"
- "Group"
- "Enroll Credentials"
- "Access Control"
- "Cafeteria"
- "Face Recognition"

To add and configure the Visitor, Click **Visitor Profile** in the Visitor Management module. The Page appears as shown below:

Profile

Click on **New** to add new Visitor.

Basic

Enter the **ID** and **Name** of the visitor. This is the Visitor ID which will appear in the Visitor ID picklist in the Visit Details section while creating a pass for the visitor from VMS Utility.

You can create an ID for a regular visitor (eg: Nammy) and assign to that visitor on arrival from the VMS Utility.

Also the generic visitor IDs can be created and assigned to the visitor. Eg: ID: 1, Name: VMS1 is given to visitor Rashmi. Once the pass of Rashmi is surrendered or expired, then VMS1 can be re-issued to another visitor.

Check the **Active** box to activate the visitor on the system.

Optional

Full Name- You can also specify the Full name of the visitor with maximum 200 characters. The supported values are: **A-Z, a-z, 0-9, () , [] _ (underscore), - (Hyphen), . (full Stop), /, &, , (comma), @, ' (single quote), [space]**



A function name followed by (bracket is invalid in full name. Eg: Thomas S/O Round (will be invalid.

The **Short Name** and **Reference ID** fields will be auto generated. You can change the “Short Name” anytime but the reference ID can be edited only before saving the visitor details.

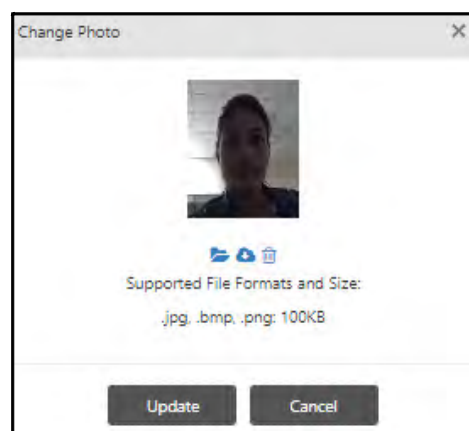
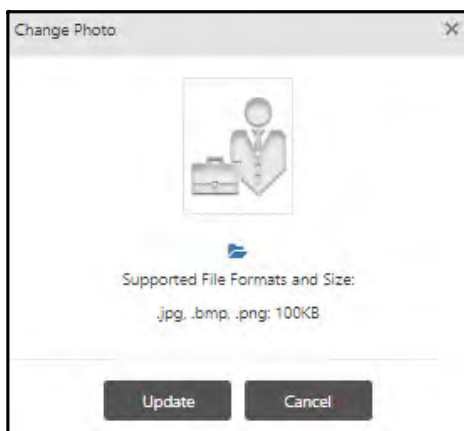


When Full name of visitor is entered and Name and Short name are blank then Name will be auto updated with 45 characters of full name excluding special characters and Short name will be updated with 15 characters of full name.

Specify the **Integration reference**. This field is provided for integration with third party software applications (eg: Payroll). In third party applications where the visitor ID has more number of characters (say alphanumeric up to 20 characters) and if it wants to integrate with COSEC Application then it can use Integration reference to map COSEC to third party software.

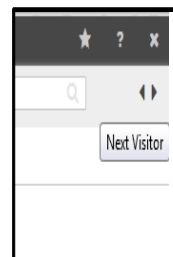
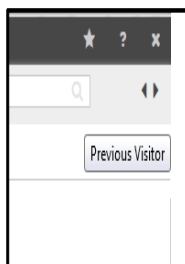
Upload Photo

Click on the image on left side to upload or change the **Photo**. Browse the image and click on **Update** to upload the photo for the visitor.



Finally click on **Save** button from the toolbar to save the basic details of the visitor

To navigate to previous and next visitor in the list, click on the arrows as shown below.



During check-in by the visitor, the uploaded profile photo (if available) will be displayed for the assigned Visitor Profile. Else, the default profile photo for the assigned Visitor Profile will be displayed.

Devices

To assign COSEC devices to visitor, click **Devices**. The page appears as shown below:

The screenshot shows the 'Assign' tab in the COSEC system interface. The left sidebar contains a menu with 'Devices' selected. The main area has two tabs: 'Assign' and 'Configure'. Under 'Assign', there are search bars for 'Device Group' and 'Device', and a table with columns 'DGID' and 'Device Group Name'. The table is empty, showing 'No Data'. Below this is another search bar and a table with columns 'Device Name', 'Type', 'Restrict Access', and 'Action'. This table is also empty, showing 'No Data'.

You can assign Device group or individual devices to the visitor so that the visitor can access the assigned devices using the enrolled credential or visitor card.



*When **Auto Device Assignment** is enabled from Admin> System Configuration> Global Policy> Visitor Management, the devices assigned to the Host will now be assigned to the visitor. The **Devices** tab will not be configurable.*

When any Visitor Profile is assigned to the visitor, then the device list from User Module > User Configuration > Visitor Management will be reflected here in read-only mode.

Assign

Select the **Device Group** or **Device** from the picklist. The picklist is shown below.

The screenshot shows the 'Select Device' dialog box. It has a search bar and a 'Show Selected' link. Below is a table with 4 records selected. The table has columns 'Name' and 'Type'. The records are: ARGO (ARGO), PATH (Path V2), FMX (Door FMX), and Door PVR (PVR Door). There are 'OK' and 'Cancel' buttons at the bottom.

Name	Type
ARGO	ARGO
PATH	Path V2
FMX	Door FMX
Door PVR	PVR Door

Select the desired devices and click OK. The devices will be listed in the grid.

Search			
Device Name ▲	Type	Restrict Access	Action
ARGO	ARGO	<input type="checkbox"/>	
Door PVR	PVR Door	<input checked="" type="checkbox"/>	
FMX	Door FMX	<input checked="" type="checkbox"/>	
PATH	Path V2	<input type="checkbox"/>	

You can also Unassign the particular device from the assigned Device Group by clicking on icon. Click on the icon to assign the device again.

The **Restrict Access** column is provided to enable the administrator to restrict access to selected devices as and when required. In the event of this option being checked against a particular device, the device will only register the visitor punch but will not activate the door relay.

Configure

You can edit the settings on the individual controllers assigned to the visitor as shown below. This option is only available with the Access Control add on module.

Assign	Configure
<div>Device Vega- Direct Door</div> <div>Type Vega Controller</div> <hr/> <div>Active <input checked="" type="checkbox"/></div> <div>Cafeteria Device <input checked="" type="checkbox"/></div>	

Device: Select the door from the drop down list. The list will show the devices assigned to the visitor.

Check the **Active** box to enable the visitor credentials on the controller. Check the **Cafeteria Device** option if the device is to be set for Cafeteria access.

Click on **Save** button to save the visitor configuration.

Credentials

To assign credentials to visitor, click the option **Credentials**. The page appears as shown below.

Visitor Profile

Search Visitor ID or Name

V3
Parshv
Active

Profile

Devices

Credentials

Access Control

Cafeteria

Face Recognition

PIN 101

Biometric Group No. 7

Roaming User ☐

Access Card 1

Access Card 2

Enrolled Fingers(Suprema Proprietary) 0

Enrolled Fingers(Suprema ISO) 0

Enrolled Fingers(Lumidigm ISO) 0

Enrolled Palm 0

Enrolled Face 0

- **PIN:** Specify the PIN number for the visitor. The PIN number is used as a credential to punch on the door with which the visitor would be recognised by the device, irrespective of the fingerprints. Visitor PIN should be a numeric value consisting maximum of 15 digits. The value entered in this field will only be visible to the System Administrator (SA) user. For all other login users the value in this field will be masked.



*If Dynamic PIN On Pass Creation in Admin> System Configuration> Global Policy> Visitor Management is enabled, then **PIN** will not be configurable. You will be able to view PIN here only during the visit time i.e. when the visitor with the configured Visitor Profile checks-in.*

- **Biometric Group No.:** Specify the Biometric group number to be assigned to the visitor if applicable. It is a number allotted to a group of visitors assigned on a device. This enables the device to match a template against only those visitors who are part of the same Biometric Group thus reducing processing time.

This value is used for Palm/Face Identification of visitor on Identification Server in shorter time span considering visitor first specifies Group No and then punches on the device.

Identification Server will be allocating templates to its child threads on the basis of this field.

- **Access Card 1 & 2:** Enter the Card Serial Number or a Comma separated CSN which is to be assigned to the Visitor Profile.

Format:

- **Card Serial Number** = 1343933547.
- **Comma separated CSN** = 12,345789



The maximum character limit for Card Serial Number (CSN) is 20 digits. While the maximum character limit for Comma separated CSN is 21 digits.

To configure a comma separated card value, make sure you configure a 26-bit card format in the system and then assign the same to the device. To know more, refer "[Card Formats](#)".

This Access Card number will be synced with the devices to allow/deny access to visitors.

COSEC accepts up to two cards per visitor. So if available, the **Access Card 2** number will be displayed.



*If **Access via QR** in Admin> System Configuration> Global Policy> Visitor Management is enabled, then Access Card 2 will not be configurable.*

Once you save the configurations, hover your mouse over the Comma separated CSN value of any Access Card, the system will display an encoded (converted) value of Comma separated CSN.

- **Enrolled Fingers:** It displays the number of fingerprint templates enrolled for the selected visitor.
- **Enrolled Palms:** It displays the number of palm vein templates enrolled for the selected visitor.
- **Enrolled Face:** It displays the number of Face templates enrolled against the selected visitor.

Group

This option enables you to assign the Enterprise groups, Reporting group, Approval Policy, Leave group and Week off group to the Visitor.


The screenshot shows a web application interface for assigning groups to a visitor. On the left is a sidebar with a user profile icon and a list of options: Profile, Devices, Credentials, Group (highlighted), Access Control, Cafeteria, and Face Recognition. The main area is titled 'Group' and contains a search bar 'Search Visitor ID or Name'. Below the search bar is a table with two columns: a list of group types with dropdown menus, and a list of available groups with picklist buttons. The group types and their selected values are: Organization (1), Branch (1), Department (1), Section (1), Category (1), Grade (2), Designation (1), Custom Group 1 (1), Custom Group 2 (1), and Custom Group 3 (1). The corresponding available groups are: Organization-1, Branch-1, Department-1, Section-1, Category-1, Grade-2, Designation-1, Custom Group 1, Custom Group 2, and Custom Group 3. Each available group has a picklist button to its right.

Group Type	Selected Value	Available Groups
Organization *	1	Organization-1
Branch *	1	Branch-1
Department *	1	Department-1
Section *	1	Section-1
Category *	1	Category-1
Grade *	2	Grade-2
Designation *	1	Designation-1
Custom Group 1 *	1	Custom Group 1
Custom Group 2 *	1	Custom Group 2
Custom Group 3 *	1	Custom Group 3

The default groups will be shown in the respective fields. Click on the picklist buttons and select the appropriate enterprise groups — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Groups) to assign to the Visitor.

The picklist options that appear in each enterprise group will be as per the rights assigned to the SA. For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#).

Enroll Credentials

The Administrator can enroll credentials for the visitor by clicking **Enroll Credentials**  as shown below.

The screenshot shows the 'User Configuration' interface. At the top is a title bar 'User Configuration'. Below it is a toolbar with various icons. The 'Enroll Credentials' icon, which is a hand, is highlighted with a red rectangle. Below the toolbar, on the left, is a user profile card for 'Sasha' with ID '1' and status 'Active'. On the right, there is a button labeled 'Enroll Credentials (Alt+U)'.

The **Enroll Credentials** window appears as shown below:

The screenshot shows the 'Enroll Credentials' window. At the top, there is a 'Door' dropdown menu with 'ID' and 'Name' options. Below this is a 'Device Readers' section with a list of configuration options: Enrollment Type (Select), Number of Cards (One), Number of Fingers (One), Number of Palms (One), Access Card Selection (Access Card 1), and Number of Faces (1). An 'Enroll' button is located at the bottom right.

- **Door:** Select the desired door from the picklist on which the enrollment is to done.

Device Readers

Device Readers displays the information of the readers configured in the selected **Door**.

This screenshot shows the 'Enroll Credentials' window with the 'Device Readers' section highlighted by a red rectangle. The section lists three reader types: Card Reader, Biometric Reader, and External Reader. Below this list are the same configuration options as in the first screenshot: Enrollment Type (Select), Number of Cards (One), Number of Fingers (One), Number of Palms (One), Access Card Selection (Access Card 1), and Number of Faces (1). The 'Enroll' button is at the bottom.

Card Reader, Biometric Reader and External Reader information are displayed here.

This screenshot shows the 'Enroll Credentials' window with 'Door' set to '2' and 'ARGO' selected. The 'Device Readers' section is highlighted by a red rectangle and shows specific reader information: Card Reader (MiFare Reader), Biometric Reader (None), and External Reader (HID Prox Reader). Below this, the 'Enrollment Type' is set to 'Read Only Card' and 'Number of Cards' is 'One'. The 'Enroll' button is at the bottom.

- **Enrollment Type:** Select the desired enrollment type — Read Only Card, Smart Card, Biometrics, BiometricsThenCard, Face and Mobile — from the drop-down list.
Based on the selection of the **Door** and **Enrollment Type**, below parameters will be displayed for configuration.



Below parameters also depend on the Readers configured in the Door. To configure the desired Reader, refer Readers section under Devices > Device Configuration (of the desired Door) > Profile > Readers.

1. **Enrollment Type** = Read Only Card

Number of Cards: Select the desired number of cards from the drop down list.

2. **Enrollment Type** = Smart Card

Number of Cards: Select the desired number of cards from the drop down list.

Details on Smart Card

Select the desired check boxes of the parameters — **Visitor ID**, **Facility Code (FC)**, **Additional Security Code (ASC)** — which are to be displayed on the Smart Card.

Select the desired number of **Finger Templates** from the drop down list.

If the **Door** is selected as PVR Door, **Palm Templates** parameter will be visible. Select the check box of this parameter if you wish to display it on the Smart Card.

To store palm templates, MiFare 4k reader must be configured in the PVR Door.



Door PVR must be set in the Adaptive mode (configure from Admin> System Configuration> Global Policy) for the palm templates to be saved into the Smart Card.

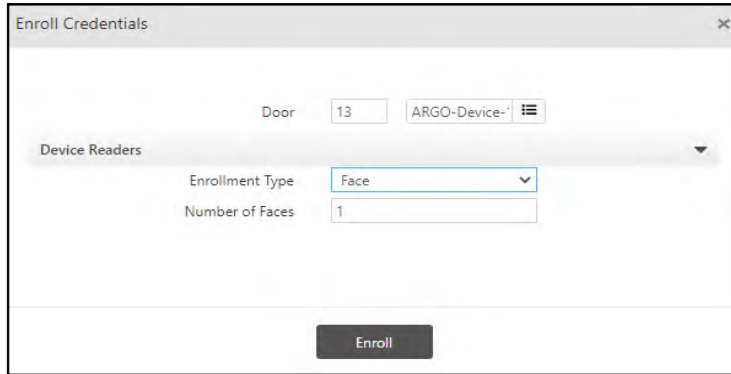
Additional Details on Smart Card

Other than the parameters mentioned in the Details on Smart Card, you can display additional details on Smart Card.

Select the **Short Name** check box to display it on the Smart Card.

3. Enrollment Type = Face

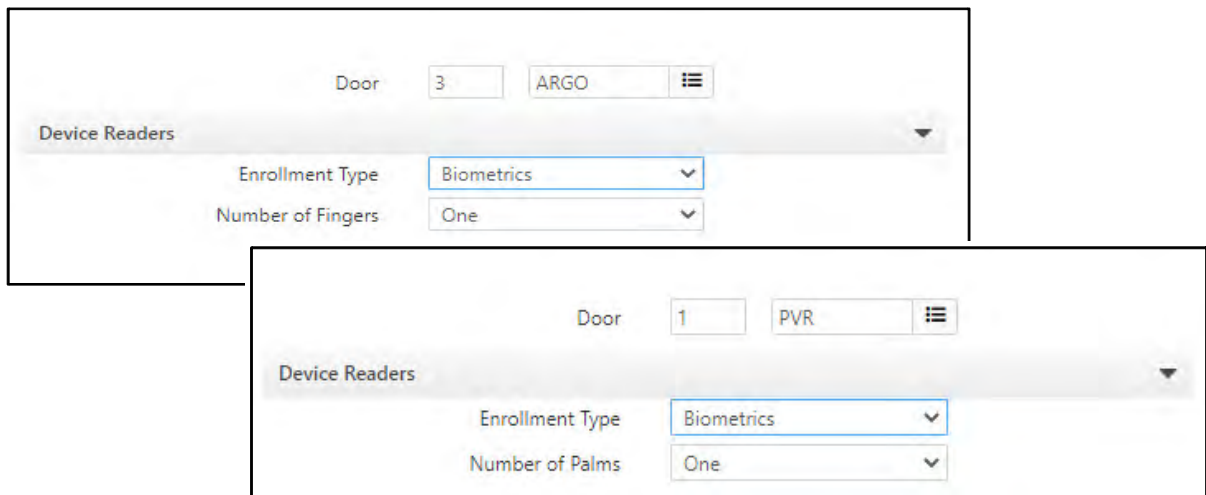
Number of Faces: Select the desired number of faces from the dropdown list.



The screenshot shows the 'Enroll Credentials' window. At the top, there is a 'Door' field with the value '13' and a device selection dropdown showing 'ARGO-Device-'. Below this is a 'Device Readers' section with a dropdown arrow. Underneath, the 'Enrollment Type' is set to 'Face' and the 'Number of Faces' is set to '1'. At the bottom, there is an 'Enroll' button.

4. Enrollment Type = Biometrics

Number of Fingers/ Number of Palms: Select the desired number of fingers or palms from the drop-down list.

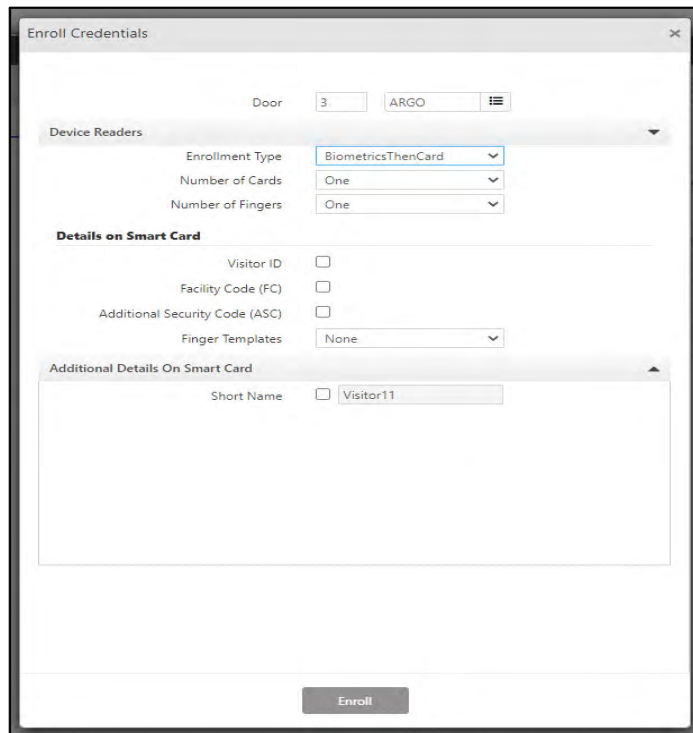


The image contains two screenshots of the 'Enroll Credentials' window. The top screenshot shows the 'Enrollment Type' set to 'Biometrics' and the 'Number of Fingers' set to 'One'. The bottom screenshot shows the 'Enrollment Type' set to 'Biometrics' and the 'Number of Palms' set to 'One'. Both screenshots show the 'Door' field and the 'Device Readers' section.

5. Enrollment Type = BiometricsThenCard

Number of Cards: Select the desired number of cards from the drop-down list.

Number of Fingers/ Number of Palms: Select the desired number of fingers or palms from the drop-down list.



Details on Smart Card

Select the desired check boxes of the parameters — **Visitor ID**, **Facility Code (FC)**, **Additional Security Code (ASC)** — which are to be displayed on the Smart Card.

Select the desired number of **Finger Templates** from the drop-down list.

If the **Door** is selected as PVR Door, **Palm Templates** parameter will be visible. Select the check box of this parameter if you wish to display it on the smart card.

To store palm templates, MiFare 4k reader must be configured in the PVR Door.



Door PVR must be set in the Adaptive mode (configure from Admin> System Configuration> Global Policy) for the palm templates to be saved into the Smart Card.

Additional Details on Smart Card

Other than the parameters mentioned in the Details on Smart Card, you can display additional details on Smart Card.

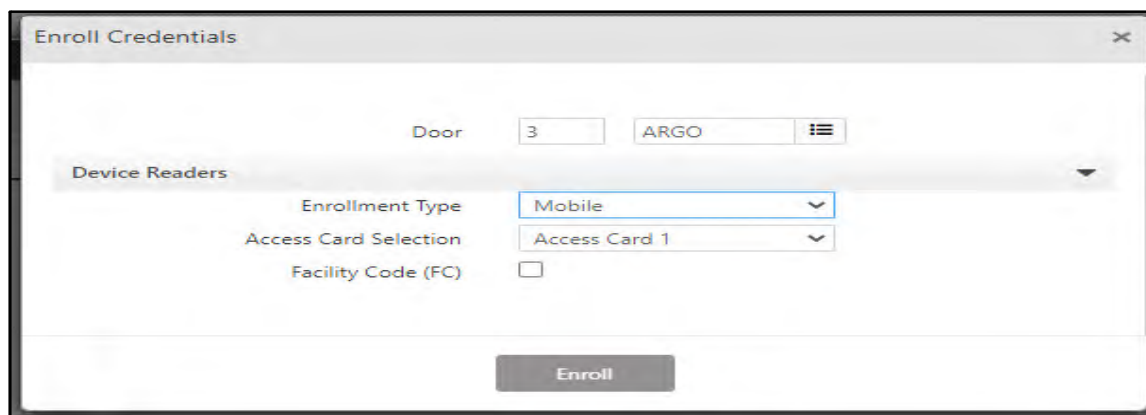
Select the **Short Name** check box to display it on the Smart Card.

6. Enrollment Type = Mobile



*To select **Enrollment Type** as Mobile, the particular device must have BLE support and ensure Bluetooth is ON in the mobile.*

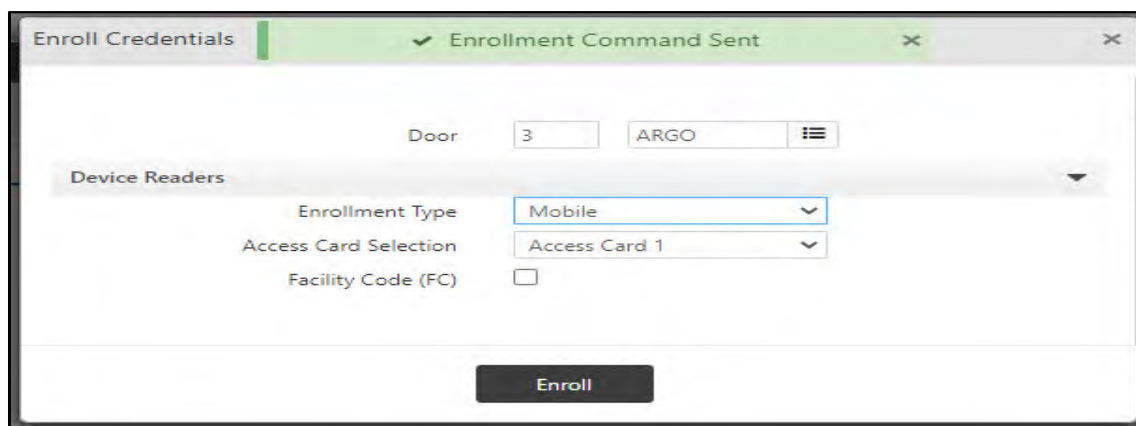
Access Card Selection: Select the desired Access Card from the drop down list.



The screenshot shows the 'Enroll Credentials' dialog box. At the top, there is a 'Door' field with the value '3' and a dropdown menu showing 'ARGO'. Below this is a 'Device Readers' section with a dropdown arrow. Underneath, there are three fields: 'Enrollment Type' with a dropdown menu showing 'Mobile', 'Access Card Selection' with a dropdown menu showing 'Access Card 1', and 'Facility Code (FC)' with an unchecked checkbox. At the bottom center is an 'Enroll' button.

Facility Code (FC): Select this check box to enroll the Facility Code (FC) against the visitor.

Click **Enroll** to initiate the enrollment process.



This screenshot shows the same 'Enroll Credentials' dialog box, but with a green banner at the top that reads '✓ Enrollment Command Sent'. The fields and buttons remain the same as in the previous screenshot.

To know more about enrolling credentials of visitors, refer ["Enrollment"](#).

Access Control

To configure Access Control feature for the visitor, click the option **Access Control**. The page appears as shown below.



This option is only available with the Access Control add on module.

Basic

ByPass Finger: You can enable this check-box to bypass the identification of finger on device when the finger print image is not clear or when there is any problem in identifying the visitor.

If the device is set to Access mode as biometrics + card or biometrics+ PIN or any other combinations. Then visitor can access the door using PIN or card, thus bypassing the finger identification.

ByPass Palm: You can enable this checkbox to bypass the identification of Palm on device when the Palm Vein image is not clear or when there is any problem in identifying the visitor.

If the device is set to Access mode as biometrics + card or biometrics+ PIN or any other combinations. Then visitor can access the door using PIN or card, thus bypassing the Palm identification.

Access Validity: Enable this option if the visitor credential is to be activated for a predefined period.

Access Validity Date: Select the date from the calendar button on which the visitor validity will end.

Access Level: Select the Access Level to be assigned to the visitor in Smart Identification (SI) mode. If the Access level of visitor is greater than the Access level of device; only then the visitor can access the device.

Holiday Schedule: Select the Holiday schedule to be assigned to the visitor from the drop down list. The Holiday Schedule is configured from Shifts and Schedule module.

Advance

The screenshot shows the 'Visitor Profile' window with the 'Advance' tab selected. The left sidebar contains a profile card for 'V3 Parshv Active' and a menu with options: Profile, Devices, Credentials, Access Control (highlighted), and Cafeteria. The main content area has two sections: 'Enable Advance Access Control' with a checked checkbox, and 'Smart Access Route' with fields for 'ID' and 'Name' (both empty) and a 'Max Route Level' dropdown set to '75'. Below this is another section: 'Enable Elevator Access Control' with a checked checkbox, and 'Elevator Floor Group' with a dropdown set to '1' and a 'RnD Elevator Group' button.

Enable Advance Access Control: Check this box to enable the advance access control feature.

Smart Access Route: Select the Smart Access Route to be assigned to the visitor from the Access Route picklist. The Smart Access Route is configured from **Access Control module> Smart Access> Smart Access Route**.

Max Route Level: Select the route level upto which the visitor is to be allowed access from the drop down list. Suppose if Max Route level of visitor is 5, then devices in the route with Access level greater than 5 will not be allowed to access by the visitor.

Enable Elevator Access Control: Check this box to enable the Elevator access control feature for the visitor.

Elevator Floor Group: Click the picklist and select the Elevator floor group to be assigned to the visitor. The visitor can access the floors of the Elevators included in Elevator Floor Group.

The Elevator Floor group is created from Access Control> Elevator Access Control> Elevator floor group

Cafeteria

This option is only available with the Cafeteria add on module. On clicking the Cafeteria option the following page appears.

Setting

The screenshot shows the 'Visitor Profile' settings window. On the left is a sidebar with a profile card for 'XYZ XYZ' (Active) and a menu with options: Profile, Devices, Credentials, Group, Access Control, Cafeteria (highlighted), and Face Recognition. The main area is titled 'Settings' and contains the following configuration options:

Enable Account	<input checked="" type="checkbox"/>
Enable Offline Transaction	None
Discount Level	None
Account Type	Pre-Paid
Balance Management	Device Based
Device-Server Balance Check	<input type="checkbox"/>
Cafeteria Usage Policy	ID: <input type="text"/> Name: <input type="text"/>

Enable Account: Check the box to enable the visitor to access the assigned Cafeteria devices.

Enable Offline Transaction- Select the desired option from the drop-down list for the visitor to perform the offline transaction

- Select **None**, if you do not want to allow transactions to be made by the Visitor when the device is in offline mode.
- Select **Allow With Discount**, if you want to allow transactions with discount to be made by the Visitor, when the device is in offline mode.
- Select **Allow Without Discount**, if you want to allow transactions without discount to be made by the Visitor, when the device is in offline mode.

Discount Level: Select the appropriate Discount Level from the drop down list.

Account Type: Select the Account Type from the options of **Pre-Paid** and **Post-Paid**.

Pre-paid Account

- For **Pre-Paid** account type, specify whether the **Balance Management** should be **Device-based** or **Server-based**.
- When Balance Management is selected as **Server based**, then you can enable **Device-Server Balance Check**. This will allow Device to check Server-side balance before allowing transaction. For this, Device and Server must be connected.

Post-paid Account

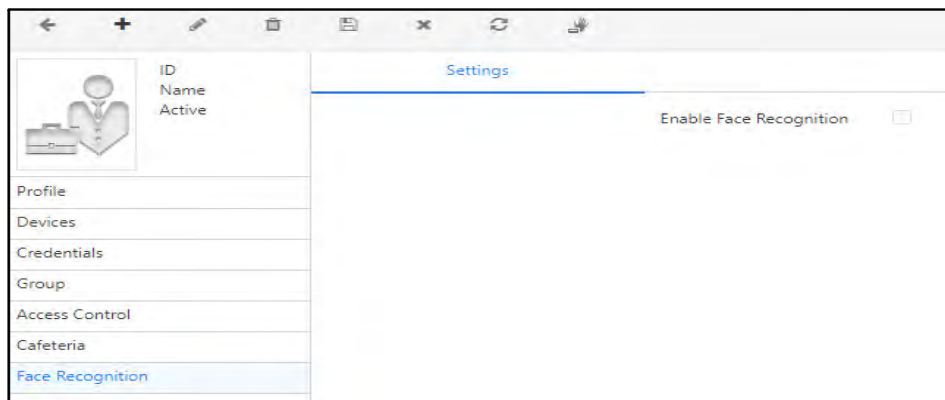
- For **Post-Paid** account type, enter the **Allowed Usage Per Month** based on which monthly dues for the user can be calculated.

Enable Account	<input checked="" type="checkbox"/>	
Enable Offline Transaction	None	
Discount Level	None	
Account Type	Post-Paid	
Allowed Usage Per Month *	0.00	
Cafeteria Usage Policy	ID	Name

Cafeteria Usage Policy- Select the cafeteria usage policy to assign to the user based on which cafeteria transaction restrictions will be applied to the Visitor.

Face Recognition

In this feature, visitor can access the device or mark the attendance by verifying his Face as the credential. The Face Recognition tab appears as shown below:



Enable Face Recognition: Check this box to enable Face Recognition feature for access control of visitors.

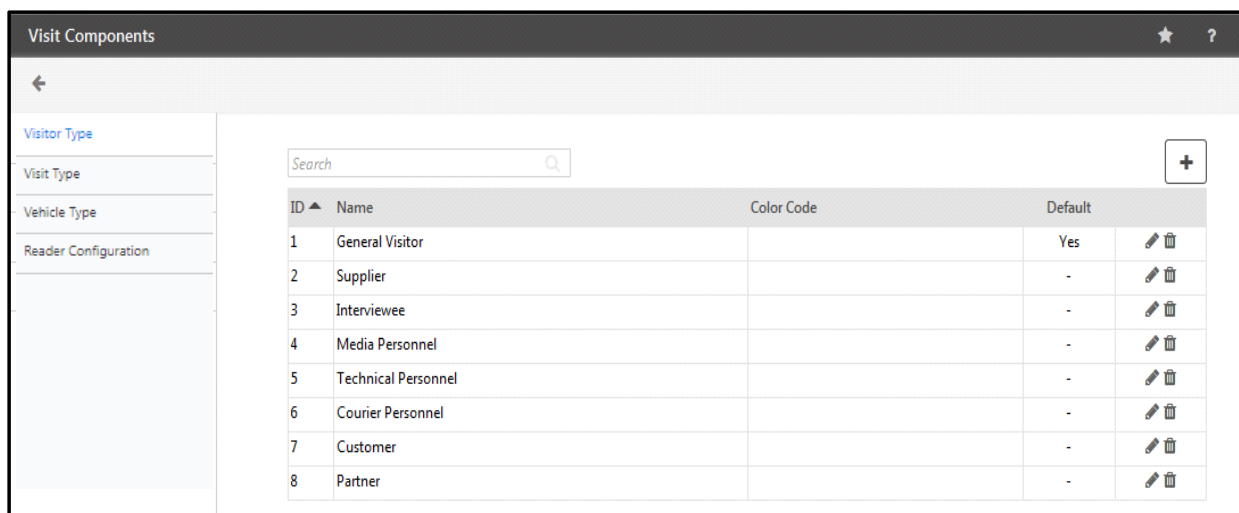
Visit Components

Visit Components display the Visitor Types, Visit Types, Vehicle Type and Station Location of Visitor.

To view and add the Visit Components, select **Visitor Management module > Visit Component**. The Page appears as shown below:

Visitor Type

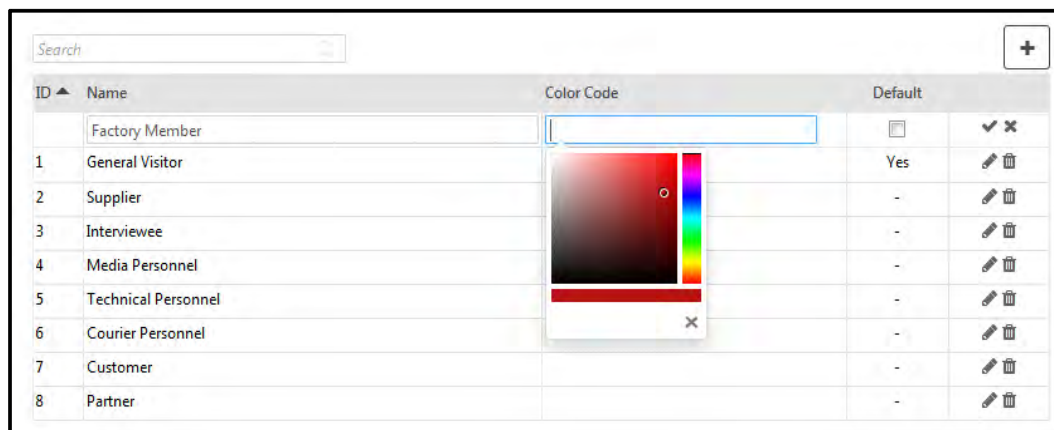
The Visitor Type option enables the user to define various types of visitors as per the site requirements.



The screenshot shows the 'Visit Components' application window. On the left is a sidebar with a back arrow and four menu items: 'Visitor Type' (highlighted), 'Visit Type', 'Vehicle Type', and 'Reader Configuration'. The main area features a search bar and a table of visitor types. A '+' button is in the top right corner.

ID ▲	Name	Color Code	Default	
1	General Visitor		Yes	
2	Supplier		-	
3	Interviewee		-	
4	Media Personnel		-	
5	Technical Personnel		-	
6	Courier Personnel		-	
7	Customer		-	
8	Partner		-	

To add a new visitor type click on **Add** button. The new row will appear where you can enter the details of visitor type.




This screenshot shows the application after clicking the '+' button. A new row, 'Factory Member', has been added at the top of the table. The 'Color Code' field for this row is active, and a color picker dialog is open, showing a color selection interface. The rest of the table remains the same as in the previous screenshot.

ID ▲	Name	Color Code	Default	
	Factory Member		<input type="checkbox"/>	
1	General Visitor		Yes	
2	Supplier		-	
3	Interviewee		-	
4	Media Personnel		-	
5	Technical Personnel		-	
6	Courier Personnel		-	
7	Customer		-	
8	Partner		-	

Specify the **Name** of the Visitor type like Customer, Supplier, Interviewee etc.

Click on the **Color Code** box. Select the **Color** for the visitor type by dragging the mouse. The respective Color and the **Color Code** appears with the color selection as shown below.

ID ▲	Name	Color Code	Default	
	Factory Member	#c2191e	<input checked="" type="checkbox"/>	✓ ✕
1	General Visitor		Yes	✎ ✕
2	Supplier		-	✎ ✕
3	Interviewee		-	✎ ✕
4	Media Personnel		-	✎ ✕
5	Technical Personnel		-	✎ ✕
6	Courier Personnel		-	✎ ✕

Check the **Default** box to set this as the default visitor type.

Click on **OK** to save the visitor type. The **ID** will be automatically generated. The visitor type will be displayed in the grid as shown below. The details can be edited by clicking **Edit** button.

ID ▲	Name	Color Code	Default	
1	General Visitor		-	✎ ✕
2	Supplier		-	✎ ✕
3	Interviewee		-	✎ ✕
4	Media Personnel		-	✎ ✕
5	Technical Personnel		-	✎ ✕
6	Courier Personnel		-	✎ ✕
7	Customer		-	✎ ✕
8	Partner		-	✎ ✕
9	Factory Member	#c2191e	<input checked="" type="checkbox"/>	✎ ✕

Visit Type

Visit Type option enables the user to define various types of visits as per the site requirements.

Visit Components

Visitor Type

Visit Type

Vehicle Type

Reader Configuration

Search

ID ▲	Name	Default	
1	Personal	Yes	✎ ✕
2	Official	-	✎ ✕

To add a new visit type click on **Add** button. The new row will appear where you can enter the name of visit type.

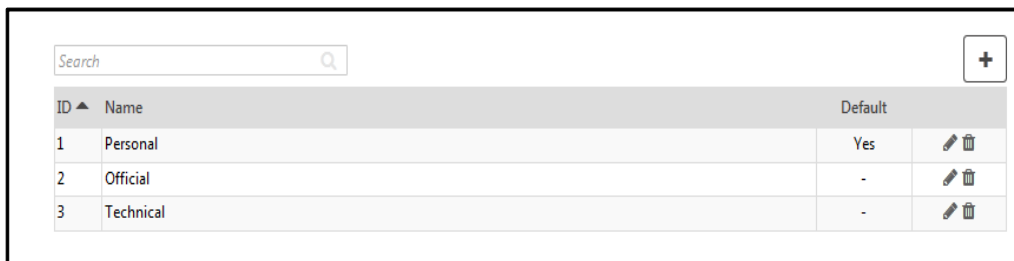
Search







ID ▲	Name	Default	
	Technical	<input checked="" type="checkbox"/>	✓ ✕
1	Personal	Yes	✎ ✕
2	Official	-	✎ ✕

Specify the **Name** of the Visit type.

Check the **Default** box to set this as the default visit type. You cannot delete the default visit type.

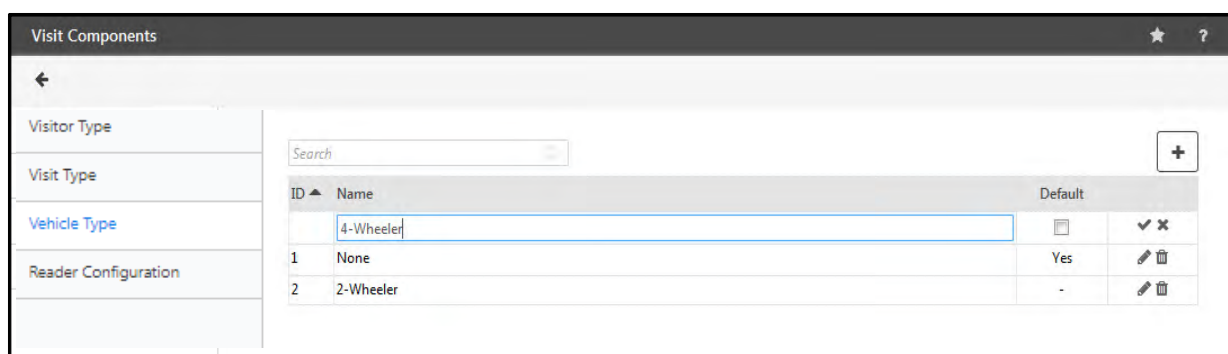
Click on **OK** to save the Visit type. The **ID** will be automatically generated. The visit type will be displayed in the grid as shown below. The details can be edited by clicking **Edit** button.









ID ▲	Name	Default	
1	Personal	Yes	 
2	Official	-	 
3	Technical	-	 

Vehicle Type

Vehicle Type option enables the user to define the types of vehicles carried by the visitors as per the site requirements.



ID ▲	Name	Default	
	4-Wheeler	<input type="checkbox"/>	 
1	None	Yes	 
2	2-Wheeler	-	 

To add a new vehicle type click on **Add** button. The new row will appear where you can enter the name of vehicle type.

Specify the **Name** of the Vehicle type which the visitor would be carrying.

Check the **Default** box to set this as the default vehicle type. You cannot delete the default vehicle type.

Click on **OK** to save the Vehicle type. The **ID** will be automatically generated.

Reader Configuration

In this section, System Account User can map VMS Utility field & Response tag. Click Add button.

Select the **VMS field names** which are VMS Utility fields from the drop down list.

Enter the **Response tag** for the selected VMS field names as shown below.

So, whenever a document (say Driving License, PAN Card, Passport etc) is scanned with Samsotech scanning device in VMS Utility, the visitor's detail will be received in response with its respective tag. Now, this received visitor's data will automatically appear in Visitor details section in VMS Utility.

The visitor details will appear according to the mapping done on 'Reader Configuration' page.

Visit Components

Visitor Type

Visit Type

Vehicle Type

[Reader Configuration](#)

Search

ID	VMS - Field Name	Response Tag
	Visitor Name	

For example: Visitor Name field is mapped with Response <firstName> as shown below.

ID	VMS - Field Name	Response Tag
	Mobile No	<personalNumber>
1	Visitor Name	<firstName>

The other fields are mapped with the respective tags as shown below.

Visit Components

✓ Saved Successfully

Search

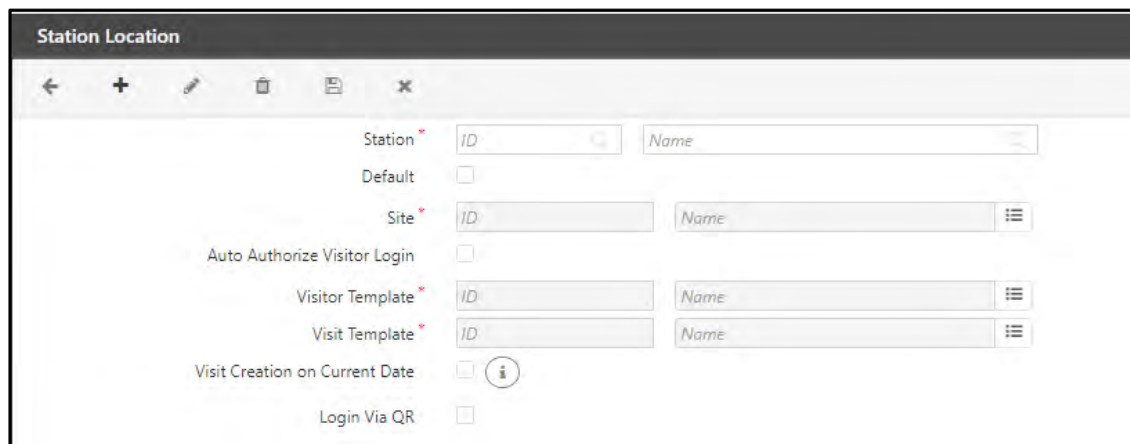
ID	VMS - Field Name	Response Tag
1	Visitor Name	<firstName>
2	Mobile No	<personalNumber>
3	Organization	CompanyNameEnglish
4	D.O.B	<dateOfBirth>
5	Nationality	<nationality_fullname>
6	Gender	<gender>

Station Location

The Virtual Entry location of the visitor where the visitor pass has been created is referred to as **Station location**. It is mandatory to surrender this pass at the particular station from where it has been created.

This option enables the Admin to define multiple COSEC VMS Stations. Each COSEC VMS location can be assigned a unique Station Location.

To view and add the Station Location, select **Visitor Management module > Station Location**. The page appears as shown below:



To add a new station location click on **Add** button and configure the following parameters:

- **Station:** Enter the **Name** of the location which is to be considered as Station Location for the visitor entry.
- **Default:** Select this checkbox to set this Station as the default Station Location.
- **Site:** Select a **Site** from the picklist to which this Station Location is to be assigned.

Multiple Station Locations can be assigned to a single site.

- **Auto Authorize Visitor Login:** Select this checkbox to authorize the Visitor's login automatically in the Visitor Web Portal.

If disabled, then the Admin will have to approve the visits manually from Visitor Login Authorization page. For more information, refer ["Visitor Login Authorization"](#).



*Make sure all the pending Visitor login requests are cleared as auto-authorization process will be applicable only on those login requests that are created after **Auto Authorize Visitor Login** checkbox is enabled.*

- **Visitor Template:** Select the desired Visitor template from the picklist.
- **Visit Template:** Select the desired Visit template from the picklist.



To create Visit and Visitor templates, select Visitor Management Module> Visit Template/Visitor Template. For more information refer ["Visit Template"](#) and ["Visitor Template"](#).

- **Visit Creation on Current Date:** Select this checkbox to permit the visitor to create a visit for the current (present) date. It is applicable only when the visitor initiates the visit.



Irrespective of the value set for **Minimum/Maximum Days Before Allowing Visit** in *Admin> System Configuration> Global Policy> Visitor Management> Visit Creation Restriction*, if **Visit Creation on Current Date** is enabled, then Visitor Pre-Registration will be allowed on the current date. To know more about **Minimum/Maximum Days Before Allowing Visit**, refer "[Visit Creation Restriction](#)".

Example: Visit on Current Date

Current Date= 20/11/2020

Minimum Days Before Allowing Visit= 2

Visit Creation on Current Date= Checked

The visitor will be allowed to create a visit request for the current date that is 20/11/2020.

If the visitor needs to create another visit for date 22/11/2020, the visit request can be created on 20/11/2020.

- **Login via QR:** Select this checkbox to allow a visitor to login into the Visitor Web Portal via scanning QR Code. The visitor can login into the Visitor Web Portal via QR Code only during his/her visit duration i.e from his/her check-in time until the check-out time.

The visitor can login into the Visitor Web Portal via Appointment ID QR code or the Dynamic ID QR code.

Appointment ID QR Code: Appointment number inserted in the QR Code. It is of 12 digits.

Dynamic ID QR Code: Unique Dynamic ID inserted in the QR Code. It is of 8 digits.

Dynamic ID will be generated only when **Access via QR** is enabled from *Admin> System Configuration> Global Policy> Visitor Management*.

Then the system inserts Dynamic ID QR Code in the visitor e-pass and the visitor can login into the Visitor Web Portal by scanning this QR Code.

If **Access via QR** is disabled, then the system inserts Appointment ID QR Code in the visitor e-pass and the visitor can login into the Visitor Web Portal via Appointment ID QR code.

The visitor will be denied access to the Visitor Web Portal if:

- The Dynamic ID received from the QR code is incorrect.
- Tries to login into the Visitor Web Portal before/after the visit duration.

Let us understand the functionality of **Access via QR** and **Login via QR** with few cases:

Access via QR	Login via QR	Access Granted to Devices	Login Granted to VMS Web Portal via QR code
Enabled	Enabled	Yes	Yes
Enabled	Disabled	Yes	No (cause flag on station disabled, though the Dynamic ID QR code will be generated)
Disabled	Enabled	No	Yes

Case 1: Access via QR = Enabled and Login via QR = Enabled.

A visit has been created for the time interval: 10:00 am- 11:00 am.

Now the Dynamic ID QR is generated and the visitor scans that QR Code in the VMS Web Portal at 11:10 am.

So, in this case access will not be granted to the VMS Web Portal via QR code as the visitor tries to access the VMS Web Portal after the visit time.

Case 2: Access via QR = Disabled and Login via QR = Enabled.

A visit has been created for the time interval: 10:00am- 11:00am.

Now, the visitor scans the Appointment ID QR Code generated to access the VMS Web Portal, in this case the login to the VMS Web Portal will be granted even if the Dynamic ID QR is not generated.

Case 3: Access via QR = Enabled and Login via QR = Enabled.

A repeating visit (repeat = daily) has been created for time interval- 10:00am- 11:00am from 06/04/2021 - 08/04/2021.

Dynamic ID QR is generated.

Now, visitor scans the QR Code generated to access the VMS Web Portal at 11:10am on 06/04/2021.

In this case login to the VMS Web Portal will be granted. i.e. for repeating visits, login will be granted from Visit Start Date to Visit End date.

Reason Being- Visitor Profile will be assigned to the Visitor for Visit Start Date till the Visit End Date, hence the Dynamic ID generated will also be stored against that visitor profile for that duration.

Once you configure all the parameters, click **Save**.

Credentials

Configure the following parameters to enable Credential Enrollment of a visitor through Visitor Web Portal by predefining them at the Station Location.

Before accessing Visitor Web Portal, make sure you upload a valid proprietary SSL Certificate (self signed SSL is not recommended) to perform Credential Enrollment and Face Recognition in the portal for security purposes.

COSEC enables the SA to configure the following:

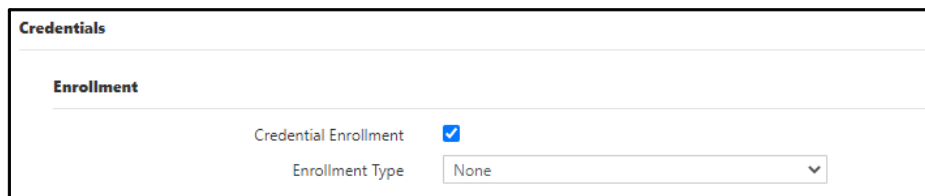
- “Enrollment”
- “Identification”
- “IDS Configuration”

Enrollment

Configure the following parameters:

- **Credential Enrollment:** Select this checkbox to enable Credential Enrollment of visitors through Visitor Web Portal.

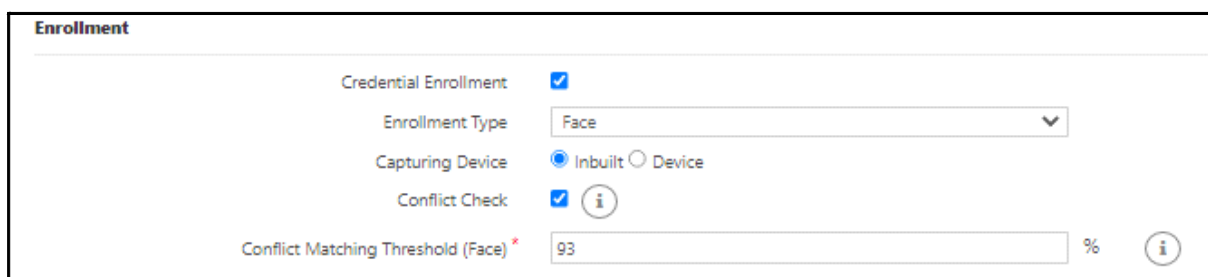
Once enabled, you will be able to configure the following parameters.



The screenshot shows the 'Credentials' configuration page. Under the 'Enrollment' section, the 'Credential Enrollment' checkbox is checked. The 'Enrollment Type' dropdown menu is set to 'None'.

- **Enrollment Type:** Select a desired enrollment type from the dropdown list — None, Face, Biometrics, Card, BiometricsThenCard.

1. Enrollment Type = Face



The screenshot shows the 'Enrollment' configuration page with 'Face' selected in the 'Enrollment Type' dropdown. Other settings include: 'Credential Enrollment' checked, 'Capturing Device' set to 'Inbuilt', 'Conflict Check' checked, and 'Conflict Matching Threshold (Face)' set to 93%.



Make sure FR is enabled for the Visitor Profile from Visitor Management> Visitor Profile> Face Recognition, to enroll the face credential of a visitor.

Configure the following parameters for Enrollment Type = Face:

- **Capturing Device:** When you configure Enrollment Type as Face, then the capturing device can be Inbuilt or Device.

If you select **Inbuilt** as the Capturing Device option, then configure the following:

- **Conflict Check:** Select this check box for the system to check if the captured visitor's face image conflicts with already enrolled faces of all the users and visitors stored in the database of the system, during the enrollment of a new Visitor's face credentials.
- **Conflict Matching Threshold:** Enter the Conflict Matching Threshold value in percentage.

It is used to identify the face of a visitor during face enrollment process and along with checking conflicts with already enrolled faces of all users or visitors.

If you select **Device** as the Capturing Device option, then configure the following:

- **Device:** Select a desired device from the picklist using which the Visitor's credentials can be enrolled.
- **Device Approach Time (Sec):** Enter the desired time in seconds for a Visitor to approach the device for the enrollment/ identification process.
- **Maximum Enrollment Time (Sec):** Enter maximum time for which the Visitor Web Portal will wait to get the status of **Credential Enrollment** process.

It is the maximum time allotted to wait for an enrollment cycle to get complete.

Maximum Enrollment Time should be set depending upon the number of credentials to be enrolled, to avoid any delays or improper functioning of the enrollment process.

Special Case

It is recommended to set **Credential Type** = Face and **Capturing Device** = Inbuilt on a **Default Station Location** when a Visitor is invited via **Visitor Invite Link**. This **Default Station Location** will be assigned to the visitor with the parameters configured on the same.

Reason being, if a visitor is invited via **Visitor Invite Link** and if the visitor is not inside or near the premises, then the Face credential of the visitor can be enrolled via his/her phone (i.e Inbuilt Device).

Configure the following parameters for Enrollment Type — Biometrics, Card and BiometricsThenCard:

2. Enrollment Type = Biometrics

The screenshot shows a web interface for configuring credentials. The main heading is 'Credentials'. Below it, there's a section titled 'Enrollment'. In this section, the 'Credential Enrollment' checkbox is checked. The 'Enrollment Type' is set to 'Biometrics' via a dropdown menu. The 'Device' field is empty and has a picklist icon. The 'Device Approach Time (Sec)' is set to 3, and the 'Maximum Enrollment Time (Sec)' is set to 5. Both time fields have an asterisk indicating they are required.

3. Enrollment Type = Card

The screenshot shows the 'Enrollment' section of the 'Credentials' configuration page. The 'Credential Enrollment' checkbox is checked. The 'Enrollment Type' dropdown is set to 'Card'. The 'Device' field is empty with a picklist icon. The 'Device Approach Time (Sec)' is set to 3. The 'Maximum Enrollment Time (Sec)' is set to 5. The 'Access Card' field is set to 'Access Card 1'.

4. Enrollment Type = BiometricsThenCard

The screenshot shows the 'Enrollment' section of the 'Credentials' configuration page. The 'Credential Enrollment' checkbox is checked. The 'Enrollment Type' dropdown is set to 'BiometricsThenCard'. The 'Device' field is empty with a picklist icon. The 'Device Approach Time (Sec)' is set to 3. The 'Maximum Enrollment Time (Sec)' is set to 5. The 'Access Card' field is set to 'Access Card 1'.

- **Device:** When you configure **Enrollment Type** as Biometric or Card or BiometricsThenCard, then select a desired device from the picklist using which the Visitor's credentials can be enrolled.

Device selection varies based on the selected **Enrollment Type**.

The Device picklist will always display the list of active devices. To activate any device, select *Devices> Device Configuration > Profile> Basic*.



Visitor Profile must be assigned to the Device on which the enrollment is to be done or the Device on which enrollment is to be done should be assigned to a Visitor Profile.

Readers required for enrolling a particular credential must be configured with the device.

- **Number of Palms/Number of Fingers:** Enter the maximum number of Palms/Fingers to be enrolled per visitor.

You will be able to configure this parameter only when the **Device** selected supports the palm/ finger enrollment type.

Before enrolling the finger/ palm of a visitor, the system will first check the values of **Fingers On Device Per User** and **Palm Templates On Device Per User** configured in the *Admin> System Configuration> Global Policy> User*. The value configured for these parameters will be the limit for enrolling palm and fingers of a visitor on a Station.

For example: **Fingers On Device Per User** = 8.

Then in this case, the drop-down of **Number Of Fingers** on Station Location will have the maximum value as 8. i.e. the drop-down will have One, Two, Three, Four, Five, Six, Seven and Eight as values.

- **Device Approach Time (Sec):** Enter the desired time in seconds for a Visitor to approach the device for the enrollment/ identification process.
- **Maximum Enrollment Time (Sec):** Enter maximum time for which the Visitor Web Portal will wait to get the status of **Credential Enrollment** process.

It is the maximum time allotted to wait for an enrollment cycle to get complete.

Maximum Enrollment Time should be set depending upon the number of credentials to be enrolled, to avoid any delays or improper functioning of the enrollment process.

For example, if you want to enroll 5 fingers and you have set **Maximum Enrollment Time** = 5 seconds, then it is impossible to enroll all 5 fingers in 5 seconds as the system may take 5 seconds to enroll 1 finger.

- **Access Card:** It displays the type of Access Card that will be stored against a Visitor via Visitor Web Portal.

Identification

For Visitor's face identification, configure the following parameters:

Face Identification: Select this checkbox to enable face identification functionality in Visitor Web Portal.

The screenshot shows the 'Credentials' configuration page. The 'Enrollment' section is at the top, with 'Credential Enrollment' as an unchecked checkbox and 'Enrollment Type' as a dropdown menu set to 'None'. Below this, the 'Identification' section is highlighted with a red rectangular border. Inside this section, 'Face Identification' is an unchecked checkbox. Under 'Face Mask Compulsion', there is an 'Enable' checkbox (unchecked) with an information icon, and a 'Mask Detection Time Out (Sec)' input field containing '1-99'. The 'Face Anti-Spoofing' section includes an 'Enable' checkbox (unchecked), a 'Camera Mount' dropdown set to 'Wall Mount' with an information icon, a 'Face Anti-Spoofing Mode' dropdown set to 'Advance', and a 'Face Anti-Spoofing Threshold' input field containing '1.00-99.99' followed by a '%' symbol. The 'IDS Configuration' section at the bottom contains an 'Identification Server' table with columns 'ID' and 'Name', a 'Configure Alternate Server Address' checkbox, a 'Server Address' input field, a 'Web Listening Port' input field with '1024-65535' and an asterisk, and an 'Identification Time-Out Duration (Sec)' input field with '1-99' and an asterisk.

Face Mask Compulsion

Face Mask Compulsion feature is used to enforce visitors to wear masks while they are within the premises.

Configure the following parameters for visitors:

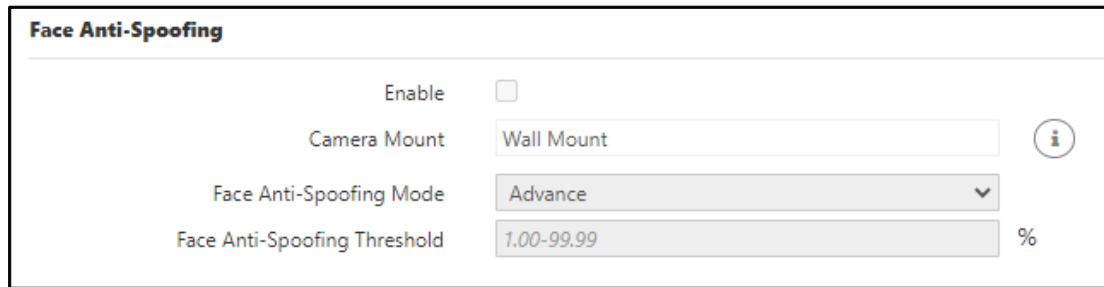
Enable: Select this checkbox to enable Face Mask Compulsion feature of the specific Station.

Mask Detection Time-out: Enter the maximum timeout duration for which Visitor Web Portal will wait to detect the visitor's face mask.

Face Anti-Spoofing

Face Anti-Spoofing prevents false facial verification by photo, video, mask or a different substitute for an authorized user's face.

To use this feature, select the **Enable** checkbox and configure the following parameters:



Face Anti-Spoofing	
Enable	<input type="checkbox"/>
Camera Mount	Wall Mount (i)
Face Anti-Spoofing Mode	Advance ▼
Face Anti-Spoofing Threshold	1.00-99.99 %

- **Camera Mount:** It displays **Wall Mount**. It is a non-editable field.



For Wall Mount, make sure the distance between camera and visitor is less than 3 feet for proper detection of face.

- **Face Anti-Spoofing Mode:** Liveness Detection helps to limit the fierce risk of spoofing attacks by using several anti-spoofing approaches.

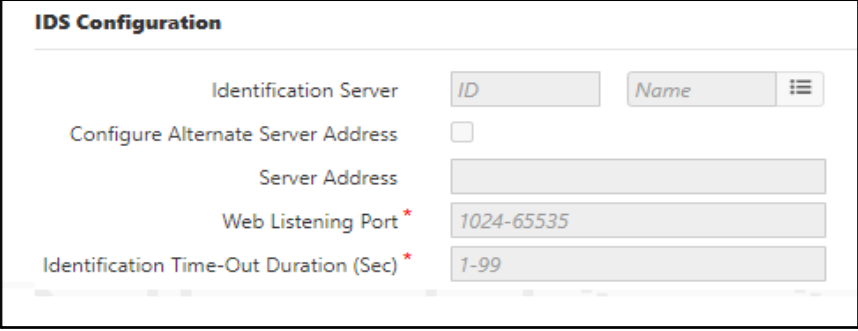
Select the Face Anti-Spoofing Mode for liveness detection from the following:

1. **Basic:** This mode detects face as well as photos from the mobile phones.
Select this option when the distance between Camera and Face is more than 3 feet.
2. **Moderate:** This mode analyzes the texture of face.
Select this option when the distance between Camera and Face is less than 1.5 feet
3. **Advance:** This mode combines the features of **Basic Mode** and **Moderate Mode** of Face Anti-Spoofing.
Select this option when the distance between Camera and Face is more than 1.5 feet and less than 3 feet.

- **Face Anti-Spoofing Threshold:** Enter the Face Anti-Spoofing threshold value in percentage within the range from 1.00 to 99.99 to identify visitor's face liveness for considering him/her as genuine person. This Threshold value will vary as per **Face Anti-Spoofing Mode** selected by you.

IDS Configuration

Identification Server (IDS) enables you to enroll and identify the credentials.



The screenshot shows the 'IDS Configuration' page. It features a table with configuration parameters. The 'Identification Server' row has a picklist with 'ID' and 'Name' options. The 'Configure Alternate Server Address' row has a checkbox. The 'Server Address' row has a text input field. The 'Web Listening Port' row has a text input field with the value '1024-65535'. The 'Identification Time-Out Duration (Sec)' row has a text input field with the value '1-99'.

IDS Configuration	
Identification Server	<input type="text" value="ID"/> <input type="text" value="Name"/> <input type="button" value="Menu"/>
Configure Alternate Server Address	<input type="checkbox"/>
Server Address	<input type="text"/>
Web Listening Port *	<input type="text" value="1024-65535"/>
Identification Time-Out Duration (Sec) *	<input type="text" value="1-99"/>

In this page, it will enroll and identify the Face credential of a visitor.

The configuration of this server can be done from *Admin Module > System Configuration > Identification Server Configuration*. For more information, refer ["Identification Server"](#).

When Face Identification is enabled on Station, then all the face templates will be synced on the configured (selected) IDS Server on Station Location Page.

Now configure the following parameters:

- **Identification Server:** Select a desired Identification Server from the picklist. It will be assigned to the Station.

Make sure you start the Identification Service from the service tray.

- **Server:** It displays the IP Address of the selected Identification Server.
- **Configure Alternate Server Address:** Select this checkbox to configure alternate IP address of an Identification Server.
- **Server Address:** Enter the alternate Server IP address which will be used for accessing identification server.
- **Web Listening Port:** Enter the Web Listening Port for the IDS. The range of the Port number is 1024-65535.
- **Identification Time-Out Duration (Sec):** Enter the Identification Time-Out Duration. It is a timer for which the Visitor Web Portal will wait for the response from IDS.

Meanwhile, the IDS will identify the face template of the visitor and will give a response to the Visitor Web Portal.

If it fails to give a response to the Visitor Web Portal within the specified time, then a time-out error message will be displayed.

Example: Identification Time-Out Duration = 10 seconds

The Identification Server will start the identification process of a face template and will try to give a response to the Visitor Web Portal within 10 seconds.

If it fails to give a response to the Web Portal within 10 seconds, a time-out error message will be displayed to the Visitor.

Form

Click the **Form** collapsible panel and the following page appears.

The screenshot shows a web interface titled 'Forms'. It contains three collapsible panels, each with a title bar and a content area. The first panel is 'On Visitor Login', the second is 'On Visit Check-In', and the third is 'On Visit Check-Out'. Each panel has three rows of configuration options: 'Form' with a text input and a picklist icon, 'Execution On' with a dropdown menu, and 'Validity' with two input fields labeled 'Month(s)' and 'Day(s)'.

After you add the required forms, you can display different forms at different times as per your requirement. You can select the desired options from:

- On Visitor Login
- On Visit Check-In
- On Visit Check-Out

On Visitor Login

- **Form:** Select the desired form from the picklist. This form will be displayed on the Visitor Login.
- **Execution On:** Select when you want the form to be displayed to the visitor — **All Login** or **First Login**.

If you select **All Login**, the form will be displayed on every login.

If you select **First Login**, the form will be displayed on the first login and you must configure the **Validity**.

- **Validity:** After the expiry of the configured time period the form will be displayed again on login until the required criteria are achieved. Valid Values for Month(s) / Year(s): 1to 99 and Day(s): 1 to 999.

On Visitor Check-In

- **Form:** Select the desired form from the picklist. This form will be displayed on the Visitor Check-In.
- **Execution On:** Select when you want the form to be displayed to the visitor — **All Visits** or **First Visit**.

If you select **All Visits**, the form will be displayed on every visit check-in.

If you select **First Visit**, the form will be displayed on first visit check-in and you must configure the **Validity**.

- **Validity:** After the expiry of the configured time period the form will be displayed again on visit check-in until the required criteria are achieved. Valid Values for Month(s) / Year(s): 1to 99 and Day(s): 1 to 999.

On Visitor Check-Out

- **Form:** Select the desired form from the picklist. This form will be displayed on the Visitor Check-Out.
- **Execution On:** Select when you want the form to be displayed to the visitor — **All Visits** or **First Visit**.

If you select **All Visits**, the form will be displayed on every visit check-out.

If you select **First Visit**, the form will be displayed on first visit check-out and you must configure the **Validity**.

- **Validity:** After the expiry of the configured time period the form will be displayed again on visit check-out until the required criteria are achieved. Valid Values for Month(s) / Year(s): 1 to 99 and Day(s): 1 to 999.

Click **Save**, to save the configurations.

Visitor Template



Make sure SA has the necessary rights to access Visitor Template. Refer [“Roles and Rights Configuration”](#).

This page enables the Admin to create multiple Visitor templates. Once you create the Visitor template, you can assign any of these templates to a Station Location. For details refer to [“Station Location”](#).




To view and create a new Visitor template, select **Visitor Management module > Visitor Template**. The page appears as shown below:

To create a customized template, do the following:

- You can select the desired parameters from the list — **Basic**, **Personal**, **Details**, **Address**, sections. In **Details** section, custom fields will be displayed.



To configure custom fields, select Admin> System Configuration> Global Policy> Visit Management.

- You can edit only the parameters with the edit icon. Click on **Edit**  .
- Select Mandatory checkbox, if you want a particular parameter to be configured by the Visitor compulsorily.
- Select Active checkbox, if you want a particular parameter to be displayed in the template.
- To save the particular parameter details click **OK**  or click **Cancel**  to discard.

Once you configure all the parameters, click **Save**.

Invite Visitor

The Invite Visitor option is used by Host to invite a registered/ non-registered Visitor through Link via Email/SMS.

The Link will be sent as SMS/Email as per the Alert Configurations done. Make sure you have selected Visitor Management as the Alert Filter and Invite Visitor as the Event. Now, under Additional Message Parameters, make sure you select the desired option — SMS or Email or both.

Here Host needs to initiate a link and send it to the Visitor, which results in registration of the Visitor on the application and passes the parameters which would automatically create a visit.

Restrictions will be imposed if configured in Visit Creation Restriction under *“Visitor Management Policy”*.

When a Visitor accepts the visit request without making any change, then that application will be sent to the host's RIC for further approval.

When a Visitor makes some changes or updates any his/her information in the application, then it will be sent first to the Host for approval and then it will be sent to the RIC for approval/rejection.

Once the host clicks on Invite Visitor tab, below page will appear:

Invite Visitor

← + ✎ 🗑️ 💾 ✕

Visitor Details

Name

Mobile No.

Email ID

Organization Name

Visit Details

Host User ID Name ⋮

Visit Date 19/09/2022 📅

Visit Until Date 19/09/2022 📅 ⌚

Visit Start Time 11:51

Visit End Time 12:51

Purpose

Additional Visitors

Copy Link

Click on the **Add** button to create a new visit invitation for a visitor.

Visitor Details

Enter the basic details of a visitor for whom the invitation is being created.

- **Name:** Enter the name of a visitor.

- **Mobile No.:** Enter the valid 10 digit contact number of the respective visitor.
- **Email Id:** Enter the valid email id of the respective visitor.



Make sure you configure atleast one — Mobile No. or Email ID, so that the Invite Link can be sent.

If you have selected SMS in Alert Configuration, make sure you configure the Mobile No. and if you have selected Email, make sure you configure the Email Id. If there is a mis-match the Link will not be sent.

If you have selected SMS and Email in Alert Configuration, make sure you configure both the Mobile No. and Email Id.

- **Organization Name:** Enter the name of an organization, the respective visitor belongs to.

Visit Details

Enter the basic details of the Visit.


- **Host User:** Enter the name of the Host; who is inviting the respective Visitor or choose the name from the provided picklist.
- **Visit Date:** Enter the date of Visit of the Visitor.
- **Visit Until Date:** Enter the end date of the Visit of the Visitor.
- **Visit Start Time:** Enter the official start time of the Visit of the Visitor.
- **Visit End Time:** Enter the end time of the visit of the Visitor.



While entering the time make sure that the Visit Time should be later than or equal to the current time i.e. the time when the host is creating the Invitation Link.

- **Purpose:** Provide the purpose of this Visit. E.g. Interview, Official Meeting, Personal etc.
- **Additional Visitors:** Enter the number of additional Visitors who are going to visit along with the respective Visitor.

After entering all the details about the visitor and the visit, click on **Send Link**.

You can even copy the link and send it to the visitor. To do so, click on **Copy Link**  .


To edit any of the above details, click on the **Edit** button. After editing click on **Save** button.

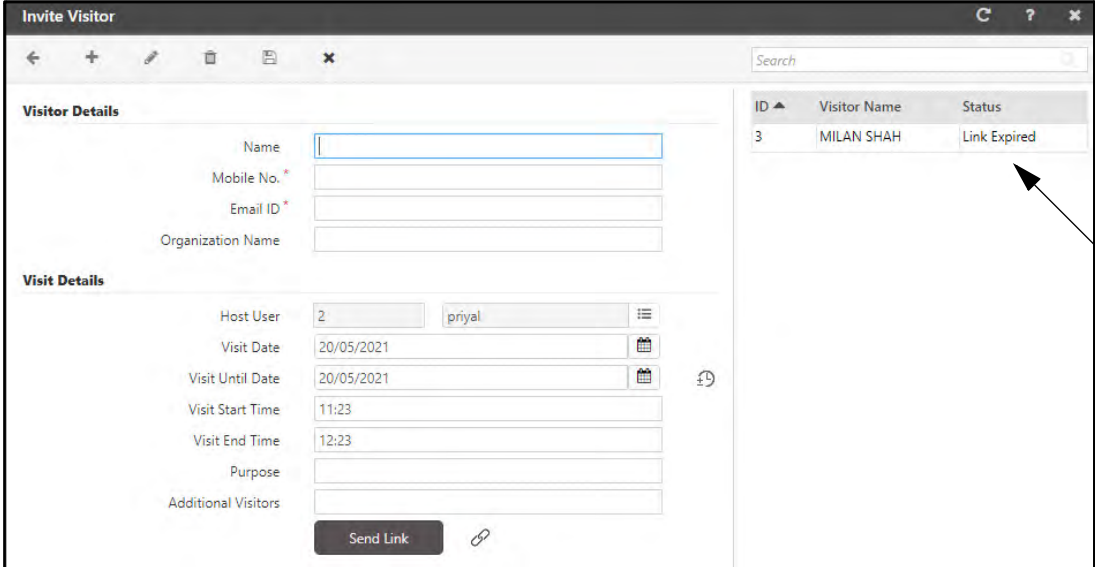


The Visit application will be sent to RIC only if 'Authorization For Visitor initiated Visit' parameter in Admin> System Configuration> Global Policy> Visitor Management is set to 'Always' or if the visit is outside the shift in global policy.

Link Expiry

The Invite Visitor Link will expire after its expiry date and the status of that link will be displayed on the left side grid.

Copy Link  will no longer be accessible once the link is expired.



ID	Visitor Name	Status
3	MILAN SHAH	Link Expired

When any Invite Visitor Link is accessed by a visitor, the system will compare the current system date with the Expiry Date.

- If Current Date is before or same as the Expiry Date, then access to the Link will be allowed.
- If Current Date is after the Expiry Date, then access to Link will be restricted.

Let's understand this with the help of the following cases:

- **Case 1:** When a Visit Date is defined in the Invite, then the system considers Visit Date as an Expiry Date.

For example: Invite for Visitor is generated on 1st of March 2021, and Invite is generated with Visit Date as 10th March 2021, then Link Expiry Date will be 10th of March 2021.

- **Case 2:** When a Visit Date is not defined in the Invite, then the system considers Expiry Date = Request Date + 15 days.

For example: Invite for Visitor is generated on 1st of March 2021, then Link Expiry should be 16th of March 2021.



Value of Expiry Date will not be updated whenever the application data is modified.

Pre-Registration

Pre-Registration option is used by the host (i.e. an employee to whom the visitor is expected to meet) by providing the details of the visitor and expected date and time.

Pre-registration can be done from COSEC Web Application or COSEC ESS Application.

The Pre-registration can be made by:

- System Account User
- On Behalf System Account User
- Using the ESS Self Service Module (For more details refer COSEC Employee Self Service User Manual)

COSEC Web enables all *System Account users* with appropriate page rights to make Pre-registration using the *Visitor Management* module. All applications made by the System Account user are *pre-approved* by default.

COSEC Web also enables all On Behalf System Account User with appropriate page rights to make Pre-registration using the *Visitor Management* module. All applications made by the On Behalf System Account User are *pre-approved* by default. For creating and assigning the roles and rights to the On Behalf System Account User. Refer to "[On Behalf System Account User](#)".

The Employee Self Service module enables users to login and enter details of their expected visitors. The pre-registration of the visitors is then sent for the approval to the Reporting In-charge.
















Both "*Host Initiated*" and "*Visitor Initiated*" pre-registration applications will be displayed on this Pre-Registration page.

For more information refer, "[Visitor Management Policy](#)".

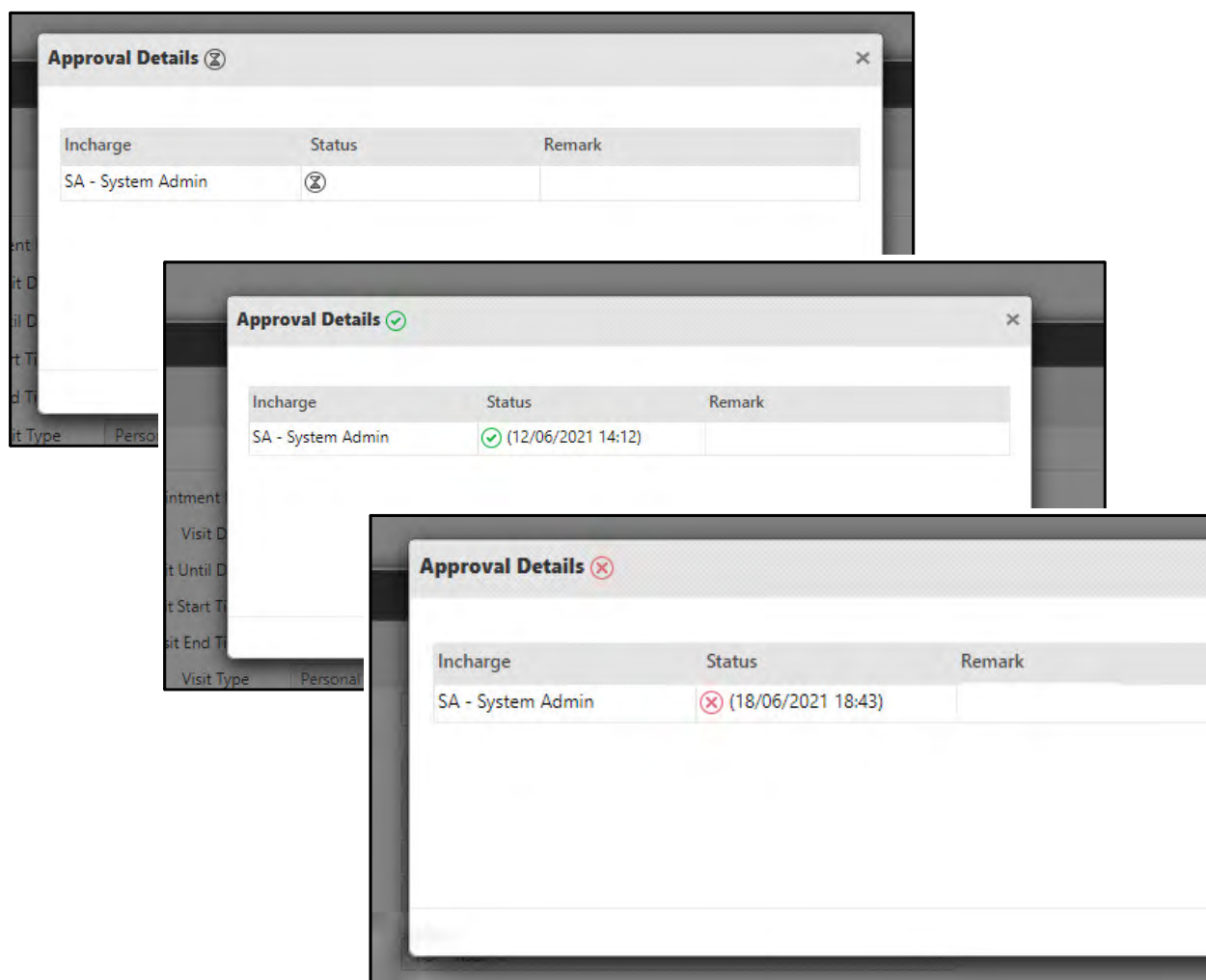
For Pre-registering the visitors from COSEC Web Application, Select **Visitor Management module> Pre-Registration**. The Page appears as shown below:

Visitor Pre-Registration			
Appointment No.		<input type="text"/>	
Host Details			
Host User*	<input type="text" value="Host"/>	<input type="text" value="Host"/>	
Additional Hosts	<input type="text" value="ID"/>	<input type="text" value="Name"/>	
Visitor Details			
Mobile No.*	<input type="text"/>		
Visitor Name *	<input type="text"/>		
Organization Name *	<input type="text"/>		
Visitor Type	<input type="text" value="General Visitor"/>		
Additional Visitors	<input type="text"/>		
Visit Details			
Visit Date *	<input type="text" value="21/10/2021"/>		
Visit Until Date *	<input type="text" value="21/10/2021"/>		
Visit Start Time *	<input type="text" value="HH:MM"/>		
Visit End Time *	<input type="text" value="HH:MM"/>		
Visit Type	<input type="text" value="Personal"/>		
Location Selection	<input type="text" value="Select"/>		
Purpose	<input type="text"/>		
Status	<input type="text"/>		
f1 *	<input type="text"/>		
f2 *	<input type="text"/>		
f3	<input type="text" value="Date"/>	<input type="text"/>	
f4 *	<input type="text" value="Date"/>	<input type="text"/>	
Field 6	<input type="text"/>		
Field 7	<input type="text"/>		
Field 8	<input type="text"/>		
Field 9	<input type="text"/>		
Field 10	<input type="text"/>		
Vehicle Details			
Registration No.	<input type="text" value="15 Chars"/>		
Vehicle Type	<input type="text" value="None"/>		
Description	<input type="text" value="50 Chars"/>		




Click **Details** icon from the grid available on the left side of the page to view the Approval Details of the already applied application.

Appointment No.	Visit Date ▲	Visitor Name	Status	Approval Details
210612000001	12/06/2021	1515	Applied	
210610000001	10/06/2021	visitor 1	Applied	
210610000002	10/06/2021	visitor 1	Applied	
210609000001	09/06/2021	visitor 1	Applied	
210609000002	09/06/2021	visitor 1	Applied	
210609000003	09/06/2021	visitor 1	Applied	
210609000004	09/06/2021	visitor 1	Applied	
210609000005	09/06/2021	visitor 1	Applied	
210609000006	09/06/2021	visitor 1	Applied	
210609000007	09/06/2021	visitor 1	Applied	
210609000008	09/06/2021	visitor 1	Applied	
210609000009	09/06/2021	visitor 1	Applied	
210609000010	09/06/2021	visitor 1	Applied	

Approval Details window appears as shown below:



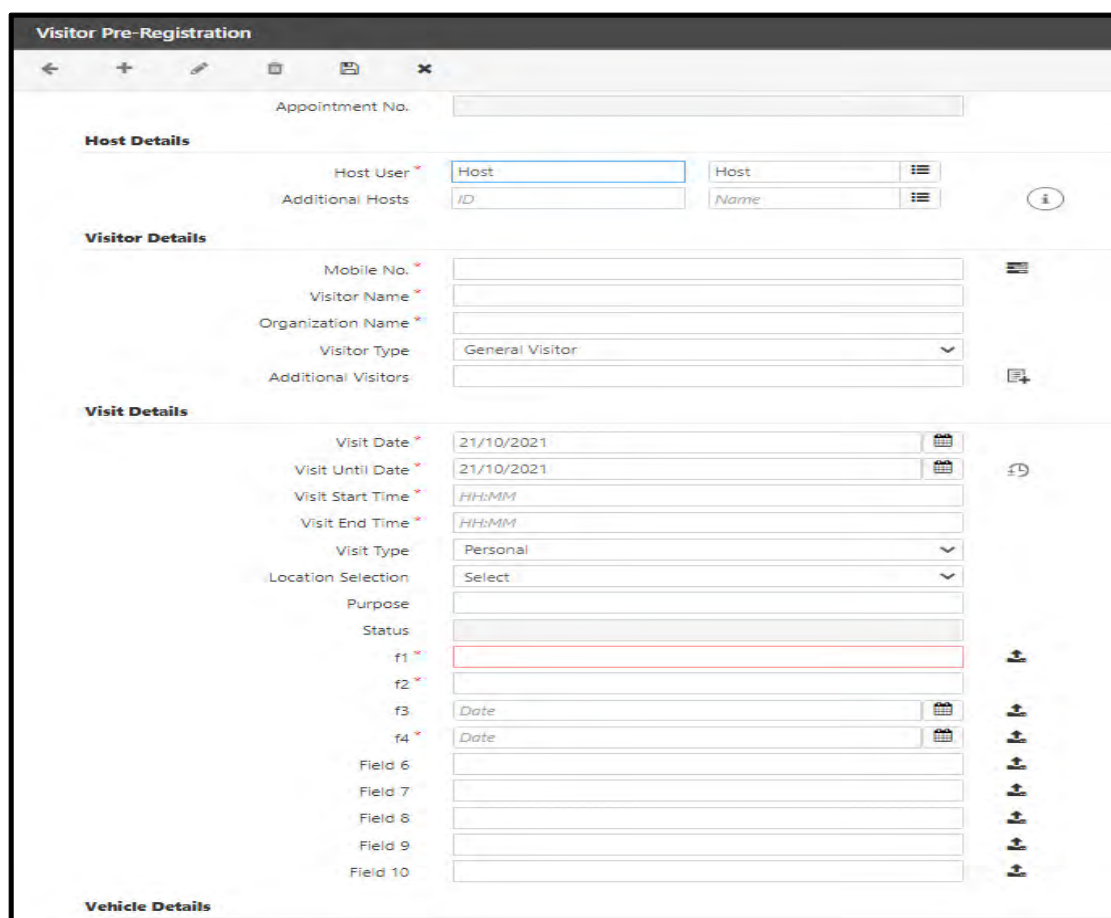
It displays the status of the user's application under **Approval Details**, that is, whether it is — pending, approved or rejected.

The application's status is displayed in the **Status** column as Pending  , Approved  or Rejected  .

Remark displays the comments provided by the Admin/ RIC/ System.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Click **Add** to pre-register a visitor.



Appointment No.: It is the auto generated number based on the registration date. The format is YYMMDD00000(N+1) where N is auto incremented number starting from 0, considering the visitor pre-registration date.

Host Details




The Host Details form is a rectangular box with a title bar. Inside, there are two rows of input fields. The first row is labeled 'Host User *' and contains two text boxes for 'ID' and 'Name', followed by a menu icon. The second row is labeled 'Additional Hosts' and also contains two text boxes for 'ID' and 'Name', followed by a menu icon. An information icon is located to the right of the second row.

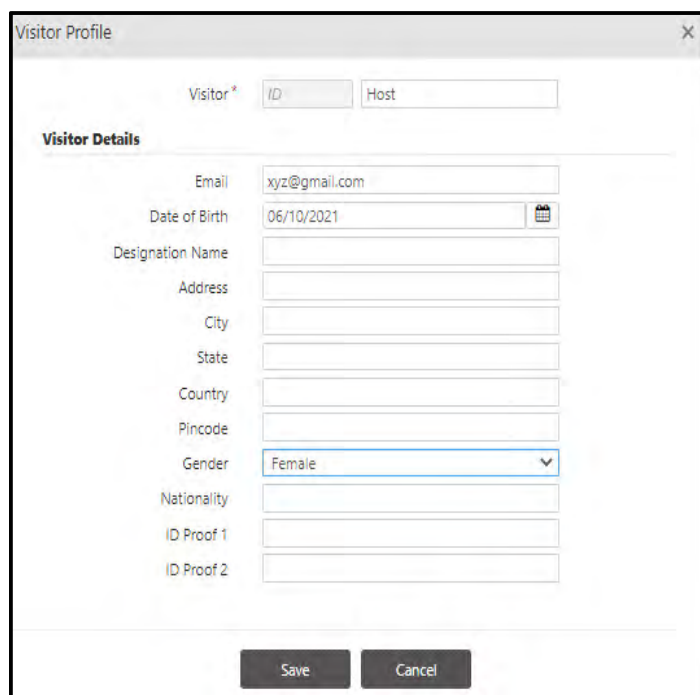
Host User: Select the host from the picklist to whom the visitor will meet or who has called the visitor to meet him. The host user picklist shows the list of authorized host users. See Visitor Management module > Utilities > Authorized host users.

Additional Hosts: Select the additional host from the picklist who will be additional host user for the visit. Maximum 99 host users can be selected.

Visitor Details

Mobile No.: Specify the mobile no. of the visitor.

To add the visitor details, click on . The Visitor Profile page appears as shown below. Enter the mandatory details and the required details. Then click Save button. The details will appear in Visitor Details section.




The Visitor Profile form is a window titled 'Visitor Profile' with a close button. It contains a 'Visitor *' section with 'ID' and 'Host' fields. Below this is the 'Visitor Details' section with the following fields: Email (xyz@gmail.com), Date of Birth (06/10/2021 with a calendar icon), Designation Name, Address, City, State, Country, Pincode, Gender (Female with a dropdown arrow), Nationality, ID Proof 1, and ID Proof 2. At the bottom are 'Save' and 'Cancel' buttons.

Visitor Name: Specify the Name of the Visitor.

Organization Name: Specify the Visitor's company name.

Visitor Type: Select the appropriate visitor type from the drop down list.

Additional visitors: To add the Additional visitors click on . The Additional Visitor Details page appears as shown below. Add the visitor and click OK.

SRNO	Name	Gender	Mobile No.
	Sathya Narayan	Male	9823456765

Visit Details

Visit Date: Enter the expected date of the Visitor in dd/mm/yyyy format or just click on the date Picklist button and select the date.

Visit Until Date: Enter the date or select the date until the visit is expected to continue.

- If the visit is for single day then Repeat button will be disabled.
- If the visit is expected for multiple days; then select the Visit Until date accordingly. And click on Repeat button to set the repeat pattern for visit.

Suppose Visit is from 2/10/2018 to 20/10/2018. Now click on **Repeat** button. The **Repeat Visit** window appears.

You can select **Repeat Mode** as Daily or Weekly. Then select the Repeat Days (for weekly) on which visit is to be repeated. Then click OK to save the settings.

Visit Start Time: Enter the expected time for the start of visit in hh:mm format.

Visit End Time: Enter the expected time for the end of visit in hh:mm format.

Visit Type: Select the visit type from the drop down options of **Personal** and **Official**.

Location Selection: The location can be selected where visit is to be held from the options of Configured location or Custom Location.


- If "Configured Location" is selected; then you can select the **location** from the picklist.
- If "Custom Location" is selected; then you can select the **location** from Google Map. The latitude and longitude of location will appear accordingly.

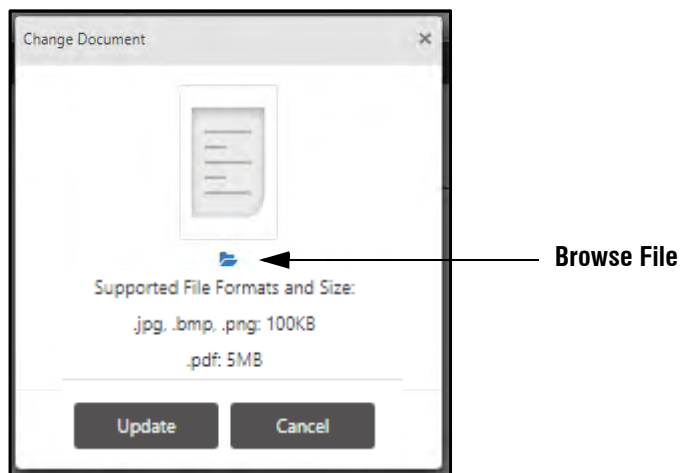
Purpose: Specify the purpose or the reason of the visit.

Status: It will show the status of application. If the pre-registration entry is done by a system account user (i.e. sa, se, so type users) then the entry will be auto approved with the login user's id itself.

Custom Fields: There are 10 additional fields in which you can enter the desired details of the visitors as per your requirement.

These are visible only after they are configured in **Visit Custom Fields** from **Admin> System Configuration> Global Policy> Visitor Management**. For example Security Number, ID Proof, Nominee Name. To know how to configure custom fields, refer "[Visit Custom Fields](#)".


You can upload the documents in Custom Fields, by clicking **Upload**  button. Then **Change Document** pop-up appears as shown below.





Click **Browse File**  .

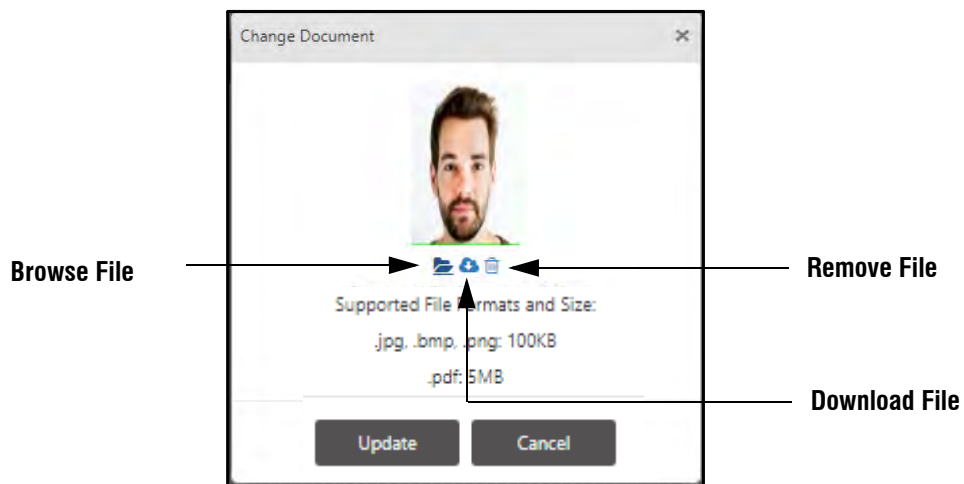
Select the desired file as per the supported formats and size (.jpg, .bmp, .png, pdf) from your local PC.

After uploading the file, if you wish to upload a different file instead of the current uploaded file, click **Browse File**


 again and select the desired file from your local PC. The previously uploaded file will get replaced with the new file.

To download the uploaded file, click **Download File**  .

To remove the uploaded file, click **Remove File**  .



Then click **Update**.

The document will be uploaded and can be previewed by clicking on **Preview**  button.

Vehicle Details

For pre-registration of a visitor's vehicle also, enter the vehicle's registration no., vehicle type and description.

Vehicle Details	
Registration No.	<input type="text" value="15 Chars"/>
Vehicle Type	<input type="text" value="None"/> ▼
Description	<input type="text" value="50 Chars"/>

Click on **Save** to save the visitor details for pre-registration.

The Pre-registered Visitor will be reflected in the COSEC VMS Application (desktop application) through which the security personnel or reception person can monitor the visitor and issue the pass.



In order to receive an alert when Watchlist visitor creates a visit make sure you have configured an alert in Admin> System Configuration> Alert Message Configuration. Set the Alert Filter as Visitor Management and Event as Create Visit- Watchlist/Blacklist. For details refer to ["Configuring Alert Messages"](#).



The SA/Host will not be able to create a visit for a Blacklist visitor.

Visit Logs

This section is visible only when the application is in View or Edit mode.

Visitor Pre-Registration

Designation Name
Visitor Type
Additional Visitors

Host Details
Host User * 1 Khushbu
Additional Hosts ID Name

Vehicle Details
Registration No. 15 Chars.
Vehicle Type
Model 15 Chars.
Color 15 Chars.

Visit Logs
Application Date Time
RIC Approval
Host/Visitor Approval
Security Clearance
Visitor Checked-IN
Visit Started
Visit Stopped
Visitor Checked-OUT

Appointment No.	Visit Date	Visitor Name	Status
181002000001	02/10/2018		Approved

Application Date Time: It displays the date and time when visitor has successfully planned visit.

RIC Approval: This is visible only when 'Authorization for Visitor Pre-Registration' is set in global policy & final verdict is given for respective application.

Host/Visitor Approval: This is visible when host/Visitor has either Approved/Rejected any visit application.

Security Clearance: If *Security Approval For Visitor E-Pass* is enabled in global policy, then Security Clearance = "<Verdict> by <Security Name> -<EpassDateTime>"

Visitor Checked IN: This is Date & Time when visitor has checked-IN.

Visit Started: This is Date & Time when Host has started visit.

Visit Stopped: This is Date & Time when Host has stopped visit.

Visitor-Checked-Out: This is Date & Time when visitor has checked out.

Reschedule/Cancel/Transfer Visit

You can reschedule, cancel or transfer the visit of a pre-registered visitor to another host.

To **Reschedule** the visit, select the desired pre-registered visitor from the right pane. The details will be displayed on the left side. You can modify the details as per your requirement.

To **Cancel** the visit, refer "[Cancel Visit](#)".

To **Transfer** the visit to another host, refer "[Transfer Visit](#)".



Cancel Visit and Transfer Visit is not applicable for rejected applications.



Before the visitor has checked in, you can reschedule, cancel or transfer visit as per your requirement.

Cancel Visit

Select the desired pre-registered visitor from the right pane.

Click **Cancel Visit** collapsible panel and configure the following parameters.



Cancel: Select this check box, to enable Cancel Visit for a pre- registered visitor.

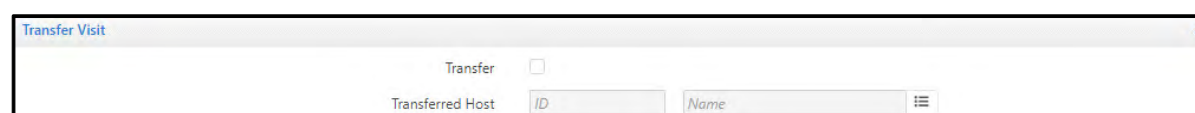
Cancellation Reason: Specify the reason for which you want to cancel the visit for a pre-registered visitor.

Click **Save**. The status of the visit is updated as Rejected in the right pane.

Transfer Visit

Select the desired pre-registered visitor from the right pane.

Click **Transfer Visit** collapsible panel and configure the following parameters.



Transfer: Select this check box, to enable Transfer Visit for a pre-registered visitor to another host.

Transferred Host: Enter the ID and Name of the Host or select the Transferred Host from the picklist. The picklist displays the authorized host list.

Click **Save**. The visit is transferred to the new host.

Visit Registration Approval

The Visit Registration requests of visitors can be approved/rejected by an Admin or the RIC of the user.

If the visit registration entry is done by a system account user (i.e. SA, SE, SO users) then the entry will be auto approved with the login user's id itself.

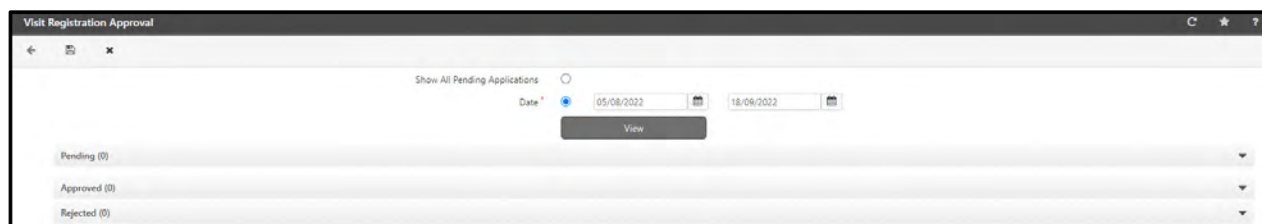
SA can approve/reject Visit Registration applications initiated by both Visitor and Host.

To approve a Visitor Initiated Visit requests SA needs to:

1. Approve the request from Visit Approval Page. To know more about Visit Approval, refer ["Visit Approval"](#).
2. Approve the request from Visit Registration Approval page.

The approval is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to ["Reporting In-Charge"](#), ["Approval Policy"](#) and ["Configuring Users"](#).

For the visit registration approval of visitors, Click **Visit Registration Approval** in the Visitor Management Page and the page appears as shown below:



You can either:

- view all the pending Visit Registration Applications
- set the date filter to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To know more, refer to ["Pending Application"](#).



The population on this page depends on the server's database. It might take time to load all pending applications.

Applications according to Set Filters

To Set the Filters,

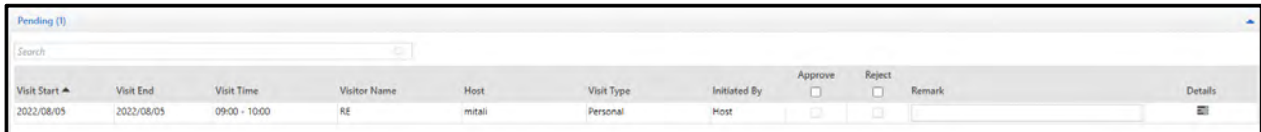
- **Date:** Select this option to enable the date filter. Select the start and end dates by clicking the respective date selection buttons for which authorization status is to be viewed for Visit Registration.


Click **View** to view the pending, approved and rejected status of all Visit Registration applications.

Pending Application

When any application is in the Pending state it can be authorized by the Admin or RIC.

Click the **Pending** collapsible panel.




Visit Start	Visit End	Visit Time	Visitor Name	Host	Visit Type	Initiated By	Approve	Reject	Remark	Details
2022/08/05	2022/08/05	09:00 - 10:00	RE	mitali	Personal	Host	<input type="checkbox"/>	<input type="checkbox"/>		

- To approve/reject applications selectively, click the respective application check box against the user.
- To approve/reject all the applications simultaneously, click the Approve /Reject check box in the header column.

Once the Admin approves/ rejects the application, the record will be moved from the **Pending** section to the **Approved/ Rejected** section respectively.

The default **Remark** for the Approved and Rejected application will appear in the respective fields. You can enter any customized Remark while authorizing the application.

To view the details of the Visit registration for the pending application, click **Details** . The **Visit Registration Detail** window appears as shown below.

Visit Registration Detail

Visit Details

Appointment No.
210609000001
Visit Date
09/06/2021
Visit Until Date
09/06/2021
Visit Start Time
18:00
Visit End Time
19:00
Visit Type
Personal
Location Selection
Select
Purpose

Visitor Details

Mobile No.
1
Email
Visitor Name
visitor 1
Organization Name
matrix
Designation Name
Visitor Type
General Visitor
Additional Visitors
0

Host Details

Host User
U3
User3

Additional Hosts

Search

Sr. No.	ID	Name
No Data		

Vehicle Details

Registration No.
Vehicle Type
None
Description

Visit Logs

Application Date Time
09/06/2021 17:14:23
Security Clearance
Visitor Checked-IN
Visit Started
Visit Stopped
Visitor Checked-OUT

Approval Details

Incharge	Status	Remark
SA - System Admin		

Visit Registration Detail window displays the visitor's registration details.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remark displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.

Approved Applications

The **Approved** section displays all the applications that have been approved by the RIC or the System Administrator.


Click the **Approved** collapsible panel.

The following screen displays the **Approved** section with approved applications:

Visit Date ▲	Arrival Time	Visitor Name	Host	Visit Type	Remark	Details
19/10/2018	23:23	mix	host2	Personal		
19/10/2018	21:00	shruti	Hostuser2	Personal	Approved Visitor Pre-Registration	
19/10/2018	20:20	8	robin1	Personal		
19/10/2018	20:20	66	robin1	Personal		Details
19/10/2018	20:20	55	robin1	Personal		

1 - 5 of 34 records

« < 1 2 3 ... 7 > »

Click the **Details**  icon to view the visit registration details of the corresponding user.

Visit Registration Detail window appears as shown below:

Visit Registration Detail

Visit Details

Appointment No. 210609000001
Visit Date 09/06/2021
Visit Until Date 09/06/2021
Visit Start Time 18:00
Visit End Time 19:00
Visit Type Personal
Location Selection Select
Purpose

Visitor Details

Mobile No. 1
Email
Visitor Name visitor 1
Organization Name matrix
Designation Name
Visitor Type General Visitor
Additional Visitors 0

Host Details

Host User U3 User3

Additional Hosts

Search

Sr. No.	ID	Name
No Data		

Vehicle Details

Registration No.
Vehicle Type None
Description

Visit Logs

Application Date Time 09/06/2021 17:14:23
Security Clearance
Visitor Checked-IN
Visit Started
Visit Stopped
Visitor Checked-OUT

Approval Details

Incharge	Status	Remark
SA - System Admin	(10/06/2021 15:20)	

Visit Registration Detail window displays the visitor's registration details.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer [“Approval Policy”](#).

Remark displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.

Rejected Applications

Click the **Rejected** collapsible panel.

The **Rejected** section displays all the applications that have been rejected by the RIC or the System Administrator.

The following screen displays the **Rejected** section with rejected applications:

Pending (3)						
Approved (34)						
Rejected (10)						
Search						
Visit Date ▲	Arrival Time	Visitor Name	Host	Visit Type	Remark	Details
19/10/2018	12:12	2312312	robin1	Personal	Rejected Visitor Pre-Registration	
19/10/2018	16:00	7774441111	Hostuser2	Personal	Rejected Visitor Pre-Registration	
19/10/2018	21:21	2	robin1	Personal	Rejected Visitor Pre-Registration	
19/10/2018	22:22	5	robin1	Personal	Rejected Visitor Pre-Registration	
19/10/2018	18:18	3333	robin1	Personal	Rejected Visitor Pre-Registration	
1 - 5 of 10 records						

Click the **Details** icon to view the visit registration details of the corresponding user.

Visit Registration Detail window appears as shown below:

Visit Registration Detail

Visit Details

Appointment No.210609000001
Visit Date09/06/2021
Visit Until Date09/06/2021
Visit Start Time18:00
Visit End Time19:00
Visit TypePersonal
Location SelectionSelect
Purpose

Visitor Details

Mobile No.1
Email
Visitor Namevisitor 1
Organization Namematrix
Designation Name
Visitor TypeGeneral Visitor
Additional Visitors0

Host Details

Host UserU3User3

Additional Hosts

Search

Sr. No.	ID	Name
No Data		

Vehicle Details

Registration No.
Vehicle TypeNone
Description

Visit Logs

Application Date Time09/06/2021 17:14:23
Security Clearance
Visitor Checked-IN
Visit Started
Visit Stopped
Visitor Checked-OUT

Approval Details

Incharge	Status	Remark
SA - System Admin		Rejected Visitor Visit

Visit Registration Detail window displays the visitor's registration details.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer [“Approval Policy”](#).

Remarks displays the comments provided by the Admin / RIC / System.

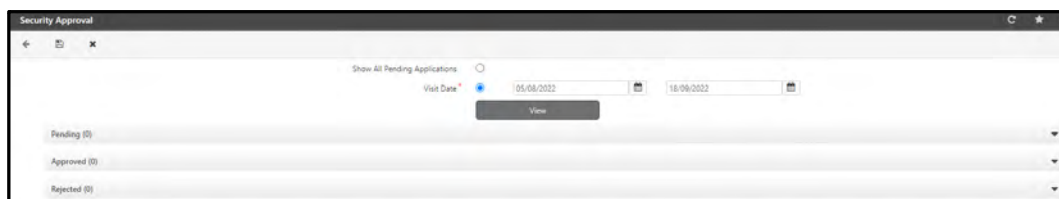
Click **Save** button to save the changes.

Security Approval

A visit request generated either from VMS utility or Visitor Portal after approval of host user is displayed in **Security Approval** page. Hence, this page enables the Security User or System Admin User to give clearance for approved Visit request application, allowing visitors to generate E-pass and perform visit successfully.

The visit requests on this page will only be received when **Security Approval For Visitor E-Pass** = 'Checked' from **Global Policy > Visitor Management Policy**.

For the Security approval of visit request, Click on **Visitor Management > Security Approval** option from the Visitor Management Page. The Page appears as shown below:



You can either:

- view all the pending Security Approval Applications
- set the date filter to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To know more, refer to ["Pending Applications"](#).



The population on this page depends on the server's database. It might take time to load all pending applications.

Applications according to Set Filters

To Set the Filters,

- **Visit Date:** Select this option to enable the visit date filter. Select the start and end dates by clicking respective date selection buttons for which security clearance is to be given.

Click the **View** button to view the **Pending**, **Approved** and **Rejected** status of all Visit applications.


Pending Applications

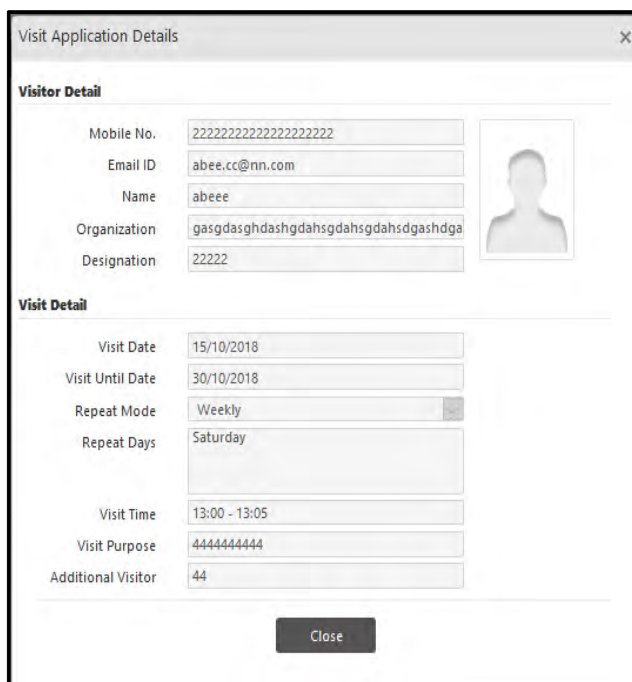
Click the **Pending** collapsible panel.



The screenshot shows a web interface with a 'Pending (4)' panel. Inside the panel is a search bar and a table of pending visit applications. The table has columns for Visit Start, Visit End, Visit Time, Host Name, Visitor Name, Visit Purpose, Approve, Reject, Remark, and Details. There are four rows of data.

Visit Start	Visit End	Visit Time	Host Name	Visitor Name	Visit Purpose	Approve	Reject	Remark	Details
15/10/2018	24/10/2018	11:00 - 11:15	host2	aaaaaa		<input type="checkbox"/>	<input type="checkbox"/>		
15/10/2018	30/10/2018	13:00 - 13:05	host2	abeee	444444444	<input type="checkbox"/>	<input type="checkbox"/>		
18/10/2018	21/10/2018	20:00 - 21:00	Hostuser1	ppp		<input type="checkbox"/>	<input type="checkbox"/>		
20/10/2018	20/10/2018	10:00 - 11:00	Hostuser2	7774441111		<input type="checkbox"/>	<input type="checkbox"/>		

To view the visit request detail, click the corresponding Details  button. The Visit Application Details window appear as shown below.



The screenshot shows a 'Visit Application Details' window. It is divided into two sections: 'Visitor Detail' and 'Visit Detail'. The 'Visitor Detail' section includes fields for Mobile No., Email ID, Name, Organization, and Designation, along with a placeholder for a visitor photo. The 'Visit Detail' section includes fields for Visit Date, Visit Until Date, Repeat Mode, Repeat Days, Visit Time, Visit Purpose, and Additional Visitor. A 'Close' button is at the bottom.

Visitor Detail

Mobile No. 22222222222222222222

Email ID abee.cc@nn.com

Name abeee

Organization gasgdasghdashgdahsgdahsgdashgdashdga

Designation 22222

Visit Detail

Visit Date 15/10/2018

Visit Until Date 30/10/2018

Repeat Mode Weekly

Repeat Days Saturday

Visit Time 13:00 - 13:05

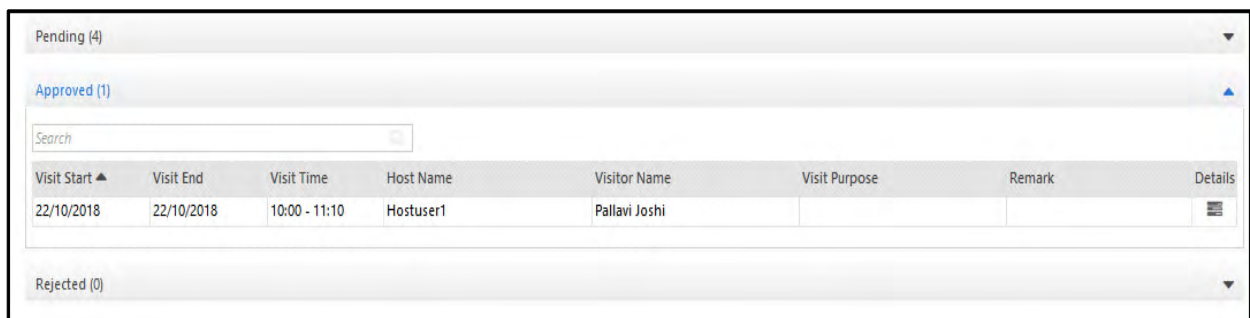
Visit Purpose 4444444444

Additional Visitor 44

Close

To approve or reject a visit request application; select the Approve/Reject checkbox to authorize and mention the Remark.

Click the **Save** button. The selected entries will now be moved from the Pending section to the Approved or Rejected section as per the authorization.



The screenshot shows a web interface with three collapsible panels: 'Pending (4)', 'Approved (1)', and 'Rejected (0)'. The 'Approved (1)' panel is expanded, showing a table of approved visit applications. The table has columns for Visit Start, Visit End, Visit Time, Host Name, Visitor Name, Visit Purpose, Remark, and Details. There is one row of data.

Visit Start	Visit End	Visit Time	Host Name	Visitor Name	Visit Purpose	Remark	Details
22/10/2018	22/10/2018	10:00 - 11:10	Hostuser1	Pallavi Joshi			

Visit State change Alert will be dispatched to Visitor and Host with Security Clearance state.

Approved Application

Click the **Approved** collapsible panel.

The approved applications with their details are displayed.

Rejected Application

Click the **Rejected** collapsible panel.

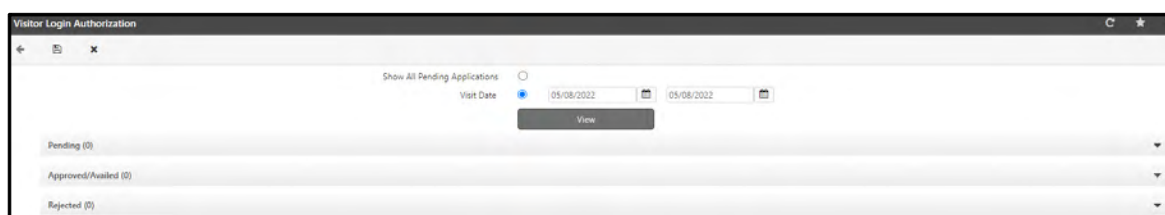
The rejected applications with their details are displayed.

Visitor Login Authorization

To access Visitor Portal OTP is required. But when the visitor is not allowed to carry Mobile Phone, in that case visitor won't be able to login via SMS or Email. Hence visitor can click on "Skip to Login" to login into Visitor Portal. Such visitors will be verified and given verdict by Security User or System Admin User using **Visitor Login Authorization** page.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to "[Reporting In-Charge](#)", "[Approval Policy](#)" and "[Configuring Users](#)".

For the approval of visitor login, select **Visitor Management > Visitor Login Authorization** option from the Visitor Management Page. The page appears as shown below:



You can either:

- view all the pending Visitor Login Authorizations
- set the date filter to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To know more, refer to "[Pending Login Requests](#)".



The population on this page depends on the server's database. It might take time to load all pending applications.

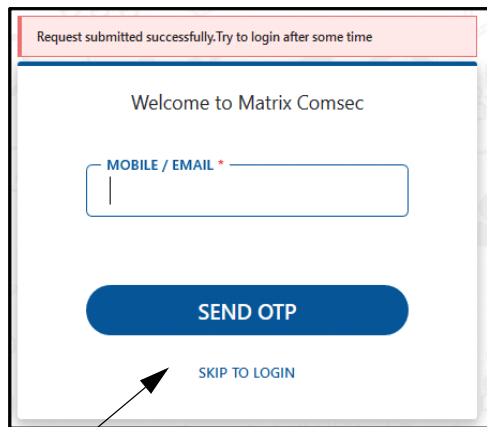
Applications according to Set Filters

To Set the Filters,

- **Visit Date:** Select this option to enable the visit date filter. Select the start and end dates by clicking respective date selection buttons for which login requests are to be fetched.

Once the visitor enters details in Basic, Personal, Document and Address section of Visitor Portal then the login request will be generated and can be fetched by the Security User or System Admin User to give the verdict.

These requests can be seen under **Pending** collapsible panel of Visitor Login Authorization Page.



Request submitted successfully. Try to login after some time

Welcome to Matrix Comsec

MOBILE / EMAIL *

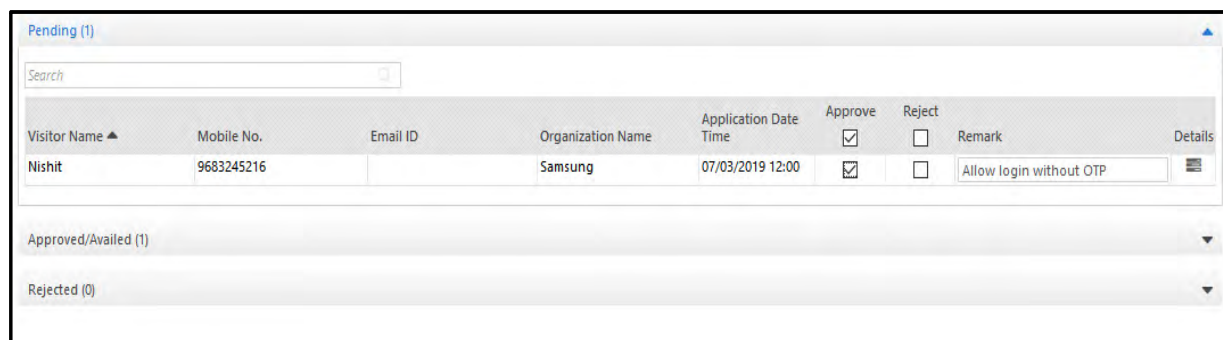
SEND OTP

SKIP TO LOGIN

Click the **View** button to view the **Pending**, **Approved** and **Rejected** status of all Visit Login Authorization Requests.

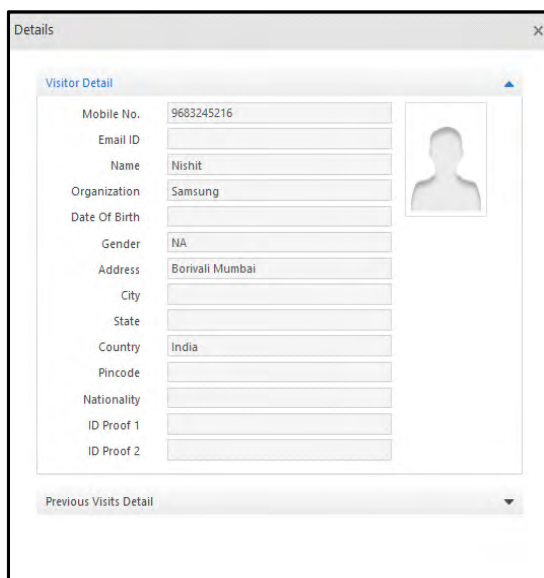
Pending Login Requests

Click the **Pending** collapsible panel.



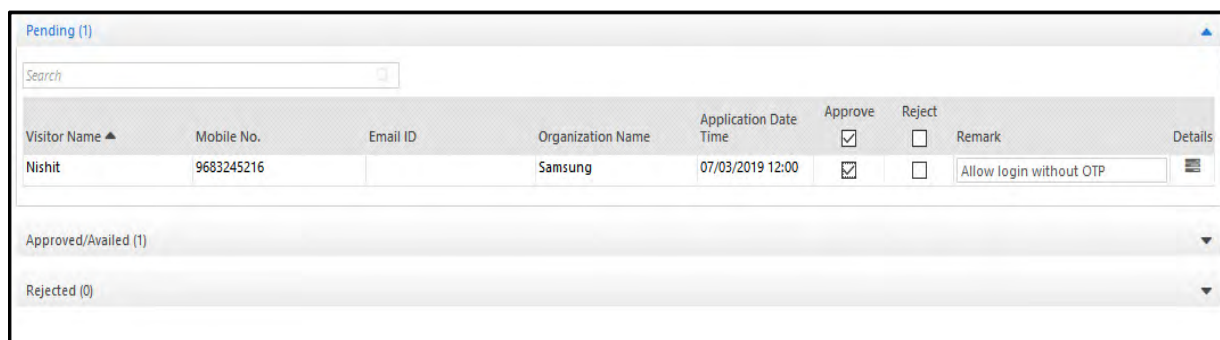
Pending (1)								
Search								
Visitor Name ▲	Mobile No.	Email ID	Organization Name	Application Date Time	Approve	Reject	Remark	Details
Nishit	9683245216		Samsung	07/03/2019 12:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Allow login without OTP	
Approved/Availed (1)								
Rejected (0)								

To view the visitor details, click the corresponding Details  button. The Details window appear as shown below.




The Details window displays a form for Visitor Detail. The form includes fields for Mobile No., Email ID, Name, Organization, Date Of Birth, Gender, Address, City, State, Country, Pincode, Nationality, ID Proof 1, and ID Proof 2. A placeholder image for a profile picture is shown on the right. Below the form is a dropdown menu labeled 'Previous Visits Detail'.

To give verdict to a visitor login application, select the Approve or Reject checkbox and click on **Save**.



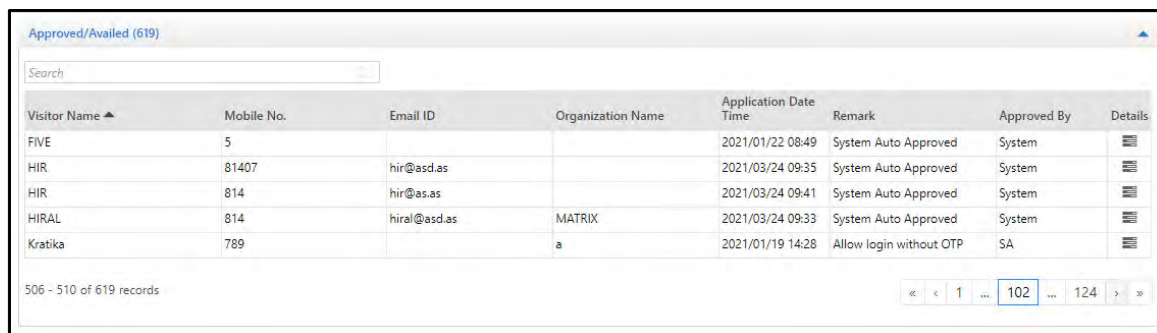
The Pending (1) window displays a table of visitor login applications. The table has columns for Visitor Name, Mobile No., Email ID, Organization Name, Application Date Time, Approve, Reject, Remark, and Details. The first row shows a pending application for Nishit from Samsung, dated 07/03/2019 12:00. The Approve checkbox is checked, and the Reject checkbox is unchecked. The Remark field contains 'Allow login without OTP'.

Visitor Name	Mobile No.	Email ID	Organization Name	Application Date Time	Approve	Reject	Remark	Details
Nishit	9683245216		Samsung	07/03/2019 12:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Allow login without OTP	






Depending on the given verdict, the request will now be visible either under Approved/Availed panel.

Approved/Availed Login Requests

Click the **Approved/Availed** collapsible panel.



The Approved/Availed (619) window displays a table of approved login requests. The table has columns for Visitor Name, Mobile No., Email ID, Organization Name, Application Date Time, Remark, Approved By, and Details. The first row shows an approved request for FIVE, dated 2021/01/22 08:49, with the Remark 'System Auto Approved' and Approved By 'System'. The table shows 506 - 510 of 619 records.

Visitor Name	Mobile No.	Email ID	Organization Name	Application Date Time	Remark	Approved By	Details
FIVE	5			2021/01/22 08:49	System Auto Approved	System	
HIR	81407	hir@asd.as		2021/03/24 09:35	System Auto Approved	System	
HIR	814	hir@as.as		2021/03/24 09:41	System Auto Approved	System	
HIRAL	814	hiral@asd.as	MATRIX	2021/03/24 09:33	System Auto Approved	System	
Kratika	789		a	2021/01/19 14:28	Allow login without OTP	SA	

All the approved requests with their details are displayed.

All auto approved visitor login request entries will be also be displayed in Approved/Availed panel, where Approved By displays System. To know how to auto authorize a visitor's login, refer **Auto Authorize Visitor Login** in [“Station Location”](#).

Approved/Availed (3)							
Search							
Visitor Name ▲	Mobile No.	Email ID	Organization Name	Application Date Time	Remark	Approved By	Details
HIR	81407	hir@asd.as		2021/03/24 09:35	System Auto Approved	System	
HIR	814	hir@as.as		2021/03/24 09:41	System Auto Approved	System	
HIRAL	814	hiral@asd.as	MATRIX	2021/03/24 09:33	System Auto Approved	System	

Rejected Login Requests

Click the **Rejected** collapsible panel.

All the rejected requests with their details are displayed.

Rejected (1)							
Search							
Visitor Name ▲	Mobile No.	Email ID	Organization Name	Application Date Time	Remark	Rejected By	Details
3	3		3	2020/12/30 11:52	Restrict to login without OTP	SA	

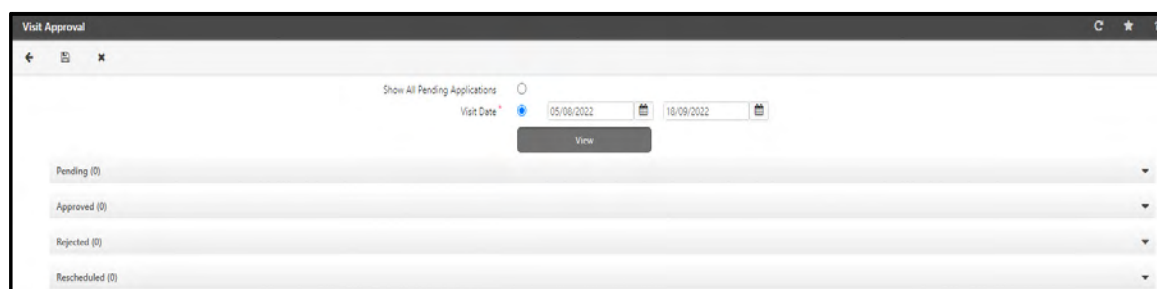
Visit Approval

The System Account User can give verdict on any visit request initiated/rescheduled by a visitor.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to [“Reporting In-Charge”](#), [“Approval Policy”](#) and [“Configuring Users”](#).

For giving verdict (approve, reject, reschedule & transfer) on visit request, following the steps given below:

Click **Visitor Management >Visit Approval**. The Visit Approval page appears as shown below:



You can either:

- view all the pending Visit Approvals
- set the date filter to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To reschedule the application, select the **Reschedule** check box of the desired entry.

To transfer the application, select the **Transfer** check box of the desired entry.

To know more, refer to [“Pending Visit Approvals”](#).



The population on this page depends on the server's database. It might take time to load all pending applications.

Applications according to Set Filters

To Set the Filters,

- **Visit Date:** Select this option to enable the visit date filter. Select the start and end dates by clicking respective date selection buttons for which visit approval to visitor is to be given.

Click **View** to view the pending, approved, rejected and rescheduled status of all Visit requests. There are four collapsible panels — Pending, Approved, Rejected and Rescheduled.

You can approve, reject, reschedule or transfer the visit request by checking the respective box. Click the desired collapsible panel to perform the desired action.

Pending Visit Approvals

Click the **Pending** collapsible panel.

The Pending Requests with Visit Date, Visit Time, Visitor Name, Host Name, Visit Purpose and Application Current Status are displayed as shown below:


Pending (1)									
Search									
Visit Date	Visit Time	Visitor Name	Host Name	Visit Purpose	Application Current Status	Approve	Reject	Reschedule	Transfer
2022/07/24	11:26 - 12:26	33	visitorhost		Transferred by System Admin	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

You can perform the following actions:

- “Approve a Visit”
- “Reject a Visit”
- “Reschedule a Visit”
- “Transfer a Visit”

Approve a Visit

Select the check box if you wish to approve the visit request application.

Click  . The Visit Approve Configuration pop-up appears from where the verdict can be configured.

Additional Hosts

Visit Location

Configured Location

Select

Configured Location

Custom Location

Location

Configured Location


Custom Location

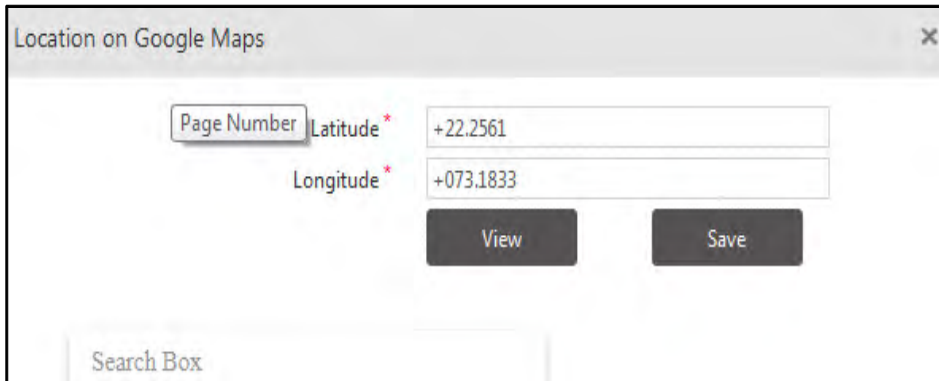
1 Host Users are selected

OK

Visit Approve Configuration

- **Additional Hosts:** Enter the Additional Hosts ID and Name manually or select the same from the picklist.

- **Visit Location:** Select the location of the Visit from the drop down list — Configured Location or Custom Location.
- If you select **Configured Location**, then configure the Location Code and Name. You can either enter the Location Code and Name manually or you can select the same from the picklist.
- If you select **Custom Location**, then click  , to select the location from the Google Map. The Location on Google Maps pop-up appears as shown below.



The 'Location on Google Maps' pop-up window contains a 'Page Number' label, a 'Latitude *' input field with the value '+22.2561', and a 'Longitude *' input field with the value '+073.1833'. Below these fields are 'View' and 'Save' buttons. At the bottom left, there is a 'Search Box'.

- **Location on Google Maps**

Latitude: Specify the Latitude of the location on Google Maps.

Longitude: Specify the Longitude of the location on Google Maps.

Click **View**, to view the location.


Click **Save**, to save the location.

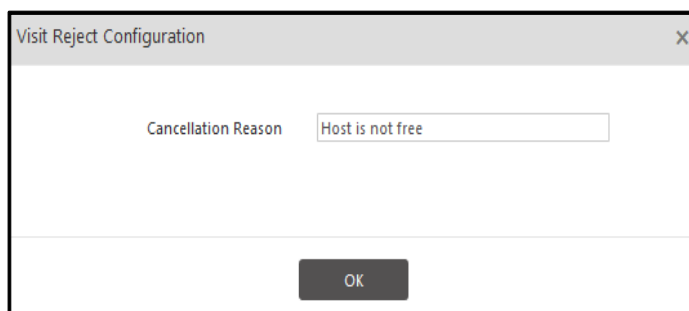
Click **OK** to save the Visit Approve Configuration.

Click **Save**  , to save the changes. The application will now appear in the Approved panel.

Reject a Visit

Select the check box if you wish to reject the visit request application.

Click  . The Visit Reject Configuration pop-up appears as shown below.



The 'Visit Reject Configuration' pop-up window features a 'Cancellation Reason' label and an input field containing the text 'Host is not free'. An 'OK' button is located at the bottom center.

Visit Reject Configuration

- **Cancellation Reason:** Specify the reason for which you want to cancel the visit of the visitor.

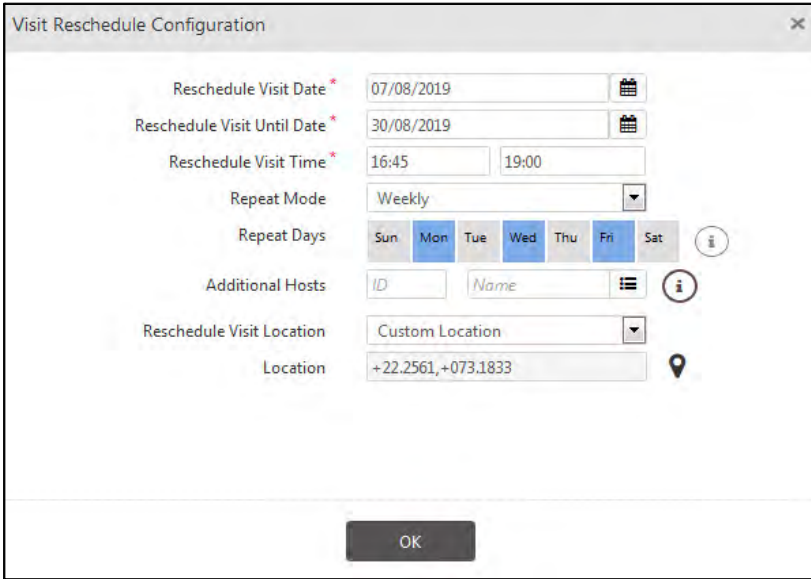
Click **OK** to save the Visit Reject Configuration.

Click **Save**  to save the changes. The application will now appear in the Rejected panel.

Reschedule a Visit

Select the check box if you wish to reschedule a visit for the visitor. Restrictions will be imposed if configured in Visit Creation Restriction under [“Visitor Management Policy”](#).

Click . The Visit Reschedule Configuration pop-up appears as shown below.



The screenshot shows a 'Visit Reschedule Configuration' dialog box. It contains the following fields and controls:

- Reschedule Visit Date ***: A date input field showing '07/08/2019' with a calendar icon.
- Reschedule Visit Until Date ***: A date input field showing '30/08/2019' with a calendar icon.
- Reschedule Visit Time ***: Two time input fields showing '16:45' and '19:00'.
- Repeat Mode**: A dropdown menu set to 'Weekly'.
- Repeat Days**: A row of buttons for days of the week: Sun, Mon, Tue, Wed, Thu, Fri, Sat. 'Mon' and 'Fri' are highlighted in blue.
- Additional Hosts**: Two input fields for 'ID' and 'Name', with a list icon and an information icon.
- Reschedule Visit Location**: A dropdown menu set to 'Custom Location'.
- Location**: An input field showing '+22.2561,+073.1833' with a location pin icon.
- OK**: A button at the bottom center.

Visit Reschedule Configuration

- **Reschedule Visit Date:** Select the desired date on which the visit needs to be rescheduled.
- **Reschedule Visit Until Date:** Select the desired date until which the visit needs to be rescheduled.
- **Reschedule Visit Time:** Specify the new visit time on which the visit needs to be rescheduled.
- **Repeat Mode and Repeat Days:** Select the Repeat Mode from the drop down list—weekly or daily, if you wish to repeat the Visit. Select the days for which you wish to repeat the Visit.
- **Additional Hosts:** Enter the Additional Hosts ID and Name manually or select the same from the pick list.
- **Reschedule Visit Location:** Select the location of the Visit from the drop down list—Configured Location or Custom Location. For details, refer [“Visit Approve Configuration”](#).


Click **OK** to save the Visit Reschedule Configuration.

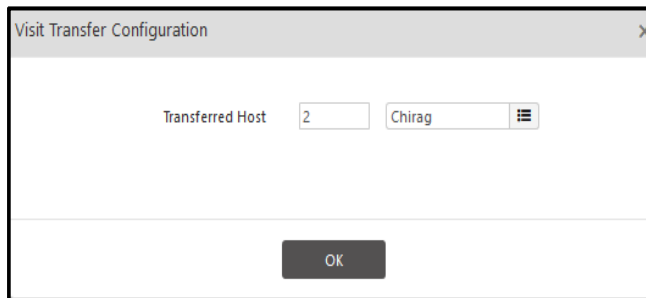
Click **Save**  to save the changes. The application will now appear in the Rescheduled panel.

Transfer a Visit

The visit can be transferred to another host user by selecting the host from the pick list.

For transferring the visit of a visitor to another host, select the check box.

Click . The Visit Transfer Configuration pop-up appears as shown below.




The dialog box titled "Visit Transfer Configuration" has a close button (X) in the top right corner. It contains a label "Transferred Host" followed by a text input field containing the number "2" and a pick list showing "Chirag" with a transfer icon. At the bottom center is an "OK" button.

Visit Transfer Configuration

- **Transferred Host:** Enter the ID and Name of the Host manually or select the Transferred Host from the pick list.

Click **OK** to save the Visit Transfer Configuration.

Click **Save**  to save the changes. The application will now appear in the Pending panel with the updates.

If "Security Clearance for Visitor E-Pass" is enabled in Global policy then the approved application will go to the Security (Linked ESS user with System Account) for Security Clearance. Then 'Visit Transfer Alert' will be sent to Visitor.




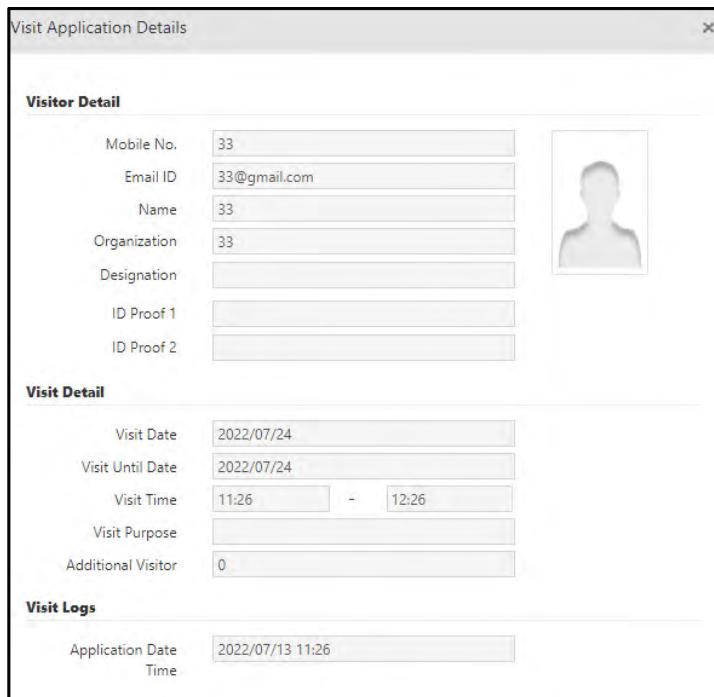
Make sure you have configured an alert for Visit Transfer. To do so:

Click Admin Module > System Configuration > Alert Message Configuration.

*In the **Alert Filter** select Visitor Management from the drop-down list and select the **Event** as Visit Transfer from the drop down list. To know more, refer ["Configuring Alert Messages"](#)*

Details

Click the corresponding **Details**  to view the visit application details. It displays the parameters of Visitor Detail, Visit Detail and Visit Logs. The Visit Application Details pop-up appears as shown below.



Visit Application Details

Visitor Detail

Mobile No. 33

Email ID 33@gmail.com

Name 33

Organization 33

Designation

ID Proof 1

ID Proof 2

Visit Detail

Visit Date 2022/07/24

Visit Until Date 2022/07/24

Visit Time 11:26 - 12:26

Visit Purpose

Additional Visitor 0

Visit Logs

Application Date and Time 2022/07/13 11:26

Approved Visit Approvals

Click **Approved** collapsible panel.

The Approved applications with Visit Date, Visit Time, Visitor Name, Host Name, Visit Purpose and Application Current Status are displayed as shown below:



Visit Date	Visit Time	Visitor Name	Host Name	Visit Purpose	Application Current Status	Reject	Reschedule	Transfer	Details
2022/07/14	10:33 - 11:33	33	mitali		Security Clearance - Pending	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2022/07/14	17:33 - 18:30	TEST	visitorhost		Pending by RIC	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Select the respective check box, if you wish to reject, reschedule or transfer the visit request.

To reject the visit request, refer ["Reject a Visit"](#).

To reschedule the visit request, refer ["Reschedule a Visit"](#).

To transfer the visit request, refer ["Transfer a Visit"](#).

Rejected Visit Approvals

Click **Rejected** collapsible panel.

The Rejected applications with Visit Date, Visit Time, Visitor Name, Host Name, Visit Purpose and Application Current Status are displayed as shown below:

Rejected (7)							
Search							
Visit Date	Visit Time	Visitor Name	Host Name	Visit Purpose	Application Current Status	Reschedule	Transfer
2022/07/14	09:05 - 10:00	TEST	visitorhost		Rejected by visitorhost	<input type="checkbox"/>	<input type="checkbox"/>
2022/07/14	09:05 - 10:00	TEST	visitorhost		Rejected by Visitor	<input type="checkbox"/>	<input type="checkbox"/>
2022/07/14	16:06 - 17:51	TEST	visitorhost		Rejected by Visitor	<input type="checkbox"/>	<input type="checkbox"/>
2022/07/14	17:04 - 18:00	TEST	visitorhost		Rejected by Visitor	<input type="checkbox"/>	<input type="checkbox"/>

Select the respective check box, if you wish to reschedule or transfer the visit request.

To reschedule the visit request, refer [“Reschedule a Visit”](#).

To transfer the visit request, refer [“Transfer a Visit”](#).

Rescheduled Visit Approvals

Click **Rescheduled** collapsible panel.

The Rescheduled applications with Visit Date, Visit Time, Visitor Name, Host Name, Visit Purpose and Application Current Status are displayed as shown below:

Rescheduled (2)							
Search							
Visit Date	Visit Time	Visitor Name	Host Name	Visit Purpose	Application Current Status	Reject	Reschedule
2022/07/19	10:38 - 11:38	33	mitali		Rescheduled by System Admin - Pending	<input type="checkbox"/>	<input type="checkbox"/>
2022/07/21	11:00 - 12:00	33	mitali		Rescheduled by System Admin - Pending	<input type="checkbox"/>	<input type="checkbox"/>

Select the respective check box, if you wish to reject, reschedule or transfer the visit request.

To reject the visit request, refer [“Reject a Visit”](#).

To reschedule the visit request, refer [“Reschedule a Visit”](#).

To transfer the visit request, refer [“Transfer a Visit”](#).

Form Summary

After the Forms are submitted by the Visitors, the details are displayed in the Form Summary. Form Summary displays the complete form response submitted by the Visitor along with its score summary.

To view Form Summary,

- Click **Visitor Management> Form Summary**.
- The **Form Summary** page appears. You can filter the records by settings various filter as per your requirement.

The screenshot shows the 'Form Summary' page. At the top, there are filter fields: 'Station' (with a dropdown arrow), 'Visitor' (with a dropdown arrow), 'Date' (with a date range selector), and 'Form Type' (with a dropdown arrow). Below these filters is a 'Preview' button. Below the filters, there is a table header with columns: 'Sr. No.', 'Date/Time', 'Form', 'Attempt', 'Final Score', 'Assessment Criteria(%)', 'Agreement', and 'Status'. Below the header, the text 'No Data' is displayed.

- **Station:** You can enter the Station ID or Name manually or you can click the picklist to select the same. This is the Station from where the response Form was submitted.
- **Visitor:** You can enter the desired Visitor's Mobile Number or Name manually or you can click the picklist to select the same.
- **Date:** Enter the desired From and To dates. This is the range during which the response Form was submitted by the Visitor.
- **Form Type:** Select the desired Form Type— Login, Check-In, Check-Out from the drop down list.

Click **Preview**. The records are displayed in the Response Table as per the set filters.

Sr. No.	Date/Time	Form	Attempt	Final Score	Assessment Criteria(%)	Agreement	Status
1	05/07/2022 00:42:14	Editedform1	13	0	NA	Accepted	Pass
2	04/07/2022 17:11:11	Editedform1	12	0	NA	Accepted	Pass
3	04/07/2022 16:09:43	Editedform1	11	0	NA	Accepted	Pass
4	04/07/2022 16:07:38	Editedform1	10	0	NA	Accepted	Pass
5	04/07/2022 15:50:29	Editedform1	9	0	NA	Accepted	Pass

1 - 5 of 13 records

Response Table: The Response Table displays the records with the following details:

- **Sr. No.:** It displays numerical sequence of the Form.
- **Date/Time:** It displays the date and time when the particular Form was submitted.
- **Form:** It displays the Form name.
- **Attempt:** It displays the number of attempts made by the Visitor for filling the Form.
- **Final Score:** It displays the score achieved by the Visitor along with the maximum achievable score.



This is applicable only for Single-Choice and Multi-Choice questions.

- **Assessment Criteria:** It displays the assessment criteria applied to the form. This parameter depends on the configuration done in **Admin Module> Form Builder**. For more details, refer to [“Form Builder”](#).
- **Agreement:** It displays whether the Agreement is accepted, declined or not provided with the Form.
- **Status:** It displays the status of the Visitor’s Form as Pass or Fail.

Click the Form whose details you wish to view.

The **Form** collapsible panel appears.

The screenshot shows a web interface titled 'Form' with a tab labeled 'Section 1'. It contains three question entries:

Question	Marks Obtained
(1) What is the actual name of company Provided Answer Matrix Comsec Pvt. Ltd. Ⓢ Correct Answer Matrix Comsec Pvt. Ltd. Ⓢ	1
(2) Which is logical Address? Provided Answer MAC Address Correct Answer IP Address	0
(3) Which are the products of matrix cosec company Provided Answer PBX Correct Answer PBX Access Control System	0

Click the **Form** collapsible panel.

The complete Form response submitted by the Visitor along with the details — section, question number, question, provided answer, correct answer and marks obtained is displayed.



The marks obtained is applicable only for Single-Choice and Multi-Choice questions.

Set and Sync Credentials

The **Set and Sync Credential** option provides a simple method of setting visitor credentials to devices. However the administrator needs to ensure that the visitors have been created in the system. And the visitor credentials are enrolled from Visitor Profile.

The COSEC system has six major types of visitor credentials which can be assigned to visitors:

- PIN
- Cards (Read only and Smart Cards)
- Fingerprint Templates
- Palm Templates
- Visitor Photo
- Face Template

To access this functionality, select the **Visitor Management module > Utilities > Set and Sync Credentials**.

The **Set and Sync Credentials** page appears as shown below.

Single Visitor

Visitor - Select a visitor from the visitor picklist whose credentials are to be set to the device.

Credential - Select the specific credential of the visitor which is to be set. The options are —

- PIN
- Cards
- FP Template
- Palm Template
- User Photo
- Face Template

Depending on the credential configure the values of the same.



*If **Dynamic PIN On Pass Creation** in Admin> System Configuration> Global Policy> Visitor Management is enabled, then PIN will not be configurable. You will be able to view PIN here only during the visit time i.e. when the visitor with the configured Visitor Profile checks-in.*

*If **Access via QR** in Admin> System Configuration> Global Policy> Visitor Management is enabled, then Card 2 will not be configurable.*

Visitor* V3 Parshv

Credential PIN

PIN Number* 501

Sync To All Allotted Devices

Set & Sync Credentials

Visitor* V1 Nammy

Credential Cards

Card 1 1942906695

Card 2

Sync To All Allotted Devices

Set & Sync Credentials

Set And Sync Credentials

Single Visitor

Multiple Visitors

Visitor* 1000 Parth

Credential FP Template

FP Templates (Suprema Proprietary) 0

FP Templates (Suprema ISO) 0

FP Templates (Lumidigm ISO) 0

FP Templates (Lumidigm Proprietary) 1

Sync To Device

Search

☒ Select All

<input checked="" type="checkbox"/>	ID	Name	Type
<input checked="" type="checkbox"/>	3	82_fmx_parth1	Door FMX
<input checked="" type="checkbox"/>	4	Vega Dimple_85	Vega Controller

Set And Sync Credentials

Visitor* V3 Parshv

Credential Palm Template

Number Of Palm Templates 1

Sync To Device

Search

☒ Select All

<input checked="" type="checkbox"/>	ID	Name	Type
<input checked="" type="checkbox"/>	1	PVR direct door	PVR Door
<input checked="" type="checkbox"/>	1	Panel Lite V2	Panel Lite V2
<input checked="" type="checkbox"/>	2	Panel Lite	Panel Lite

Set And Sync Credentials

Visitor * V3 Parshv

Credential User Photo

Sync To Device

Search

☒ Select All

<input checked="" type="checkbox"/>	ID ▲	Name	Type
<input checked="" type="checkbox"/>	1	Panel Lite V2	Panel Lite V2
<input checked="" type="checkbox"/>	3	Vega Door	Vega Controller
<input checked="" type="checkbox"/>	4	Door FMX	Door FMX
<input checked="" type="checkbox"/>	6	MODE Device1	MODE

Set And Sync Credentials

Visitor * V3 Parshv

Credential Face Template

Enrolled Faces 1

Sync To Device

Search

☒ Select All

<input checked="" type="checkbox"/>	ID ▲	Name	Type
<input checked="" type="checkbox"/>	3	Vega Door	Vega Controller
<input checked="" type="checkbox"/>	4	Door FMX	Door FMX
<input checked="" type="checkbox"/>	6	MODE Device1	MODE

Set And Sync Credentials

Select the devices where the specified credentials are to be set for the selected visitor.



The Visitor Photo can be set on allotted NGT and Vega devices only.

Click **Set and Sync Credentials** to set the visitor credential on the selected devices.

Set Credential command sent successfully

Visitor * 1225 Shalini

Credential FP Template

Number Of FP Templates 1

Sync To Device

Search

☒ All Devices

<input checked="" type="checkbox"/>	ID ▲	Name	Type
<input checked="" type="checkbox"/>	17	NGT Direct Door-Device-17 -140	NGT Direct Door
<input checked="" type="checkbox"/>	20	Door V3-Device-20 185	Door V3

Set & Sync Credentials

Multiple Visitors

Credential - Select the credential to be set for multiple visitors. The credential options are —

- FP Template
- Palm Template
- User Photo
- Face Template

Select Visitor- You can select the individual visitors by selecting **Visitor Wise** option or all the visitors by selecting option **All**. For **Visitor Wise** option select the individual visitors from the picklist.

The screenshot shows the 'Set And Sync Credentials' window with the 'Multiple Visitors' tab selected. The 'Credential' dropdown is set to 'Palm Template'. The 'Select Visitor' dropdown is set to 'Visitor Wise'. Below this, there is a search bar and a table of visitors. The table has columns for 'User ID', 'Name', and a delete icon. The data rows are V1 (Nammy) and V3 (Parshv). At the bottom, the 'Sync To' dropdown is set to 'All Allotted PVR Devices', and there is a 'Set & Sync Credentials' button.

User ID	Name	
V1	Nammy	
V3	Parshv	

The screenshot shows the 'Set And Sync Credentials' window with the 'Multiple Visitors' tab selected. The 'Credential' dropdown is set to 'Palm Template'. The 'Select Visitor' dropdown is set to 'All'. Below this, there is a search bar and the 'Sync To' dropdown is set to 'All Allotted PVR Devices'. There is a 'Set & Sync Credentials' button at the bottom.

Sync To - Select the Devices where the selected credentials are to be set for the multiple visitor. The options for Sync will depend on the credential selected.

- **All Allotted Devices** - This option appears for FP Template only. Select this to set credentials on all allotted devices.
- **All Allotted PVR Devices** - This option appears for Palm Template only. Select this to set credentials on all allotted PVR devices.
- **All Allotted NGT & Vega Controllers** - This option appears for Visitor Photo only. Select this to set credentials on all allotted NGT and Vega controllers.
- **All Allotted MODE, Vega and FMX Devices**- This option appears for Face Template only. Select this to set face credential on all MODE, Vega and FMX devices.

Click the **Set & Sync Credentials** button to set the multiple visitors credential on the selected devices.

Delete Credentials

The **Delete Credential** option provides a simple method of Deleting visitor credentials from devices.

To access this functionality, Select the **Visitor Management module > Utilities > Delete Credentials**.

The **Delete Credentials** page appears as shown below.

Some parameter will change according to the selected option in “**Credential**”.



*If you select “**Palm Template**” from the Credential list then a parameter “**Number Of Palm Template**” will be added below. Thus, same will happen with other options.*

Single Visitor

Visitor - Select a visitor from the visitor pick-list whose credentials are to be deleted from the device.

Credential - Select the specific credential of the visitor which is to be deleted The options are —

- PIN
- Cards
- FP Template
- Palm Template
- User Photo
- Face Template

Depending on the credential selected, the available PIN number/Card number (CSN)/ FP template number/ Palm template/ Face Template number will be displayed.

Visitor * V3 Parshv

Credential PIN

PIN Number * 501

Delete From Entire System

Delete

Visitor * V3 Parshv

Credential Cards

Card 1 1131112263

Card 2

Delete From Entire System

Delete

Visitor * 1000 Parth

Credential FP Template

FP Template Type Lumidigm Proprietary

FP Templates (Suprema Proprietary) 0

FP Templates (Suprema ISO) 0

FP Templates (Lumidigm ISO) 0

FP Templates (Lumidigm Proprietary) 1

Delete From Entire System

Delete

- **FP Template Type-** If Credential is selected as FP Template; then you can select the Type of FP Template which is to be deleted. The options of template are Suprema Proprietary, Suprema ISO, Lumidigm ISO, Lumidigm Proprietary. You can also choose all the templates by selecting “All” option.

Visitor * V3 Parshv

Credential Palm Template

Number Of Palm Templates 1

Delete From Entire System

Entire System

Randomly Selected Devices

Enrolled Faces- If Credential is selected as Face Template; then the number of enrolled face templates for the selected visitor will be displayed.

Delete From- Select the option as **Entire System** or **Randomly Selected Devices** from where the specified credentials are to be deleted for the selected visitor.

Click **Delete** to delete the visitor credential from the selected devices.

Multiple Visitors

Select the **Multiple Visitors** tab.

Credential - Select the credential to be deleted for multiple visitors. The credential options are —

- PIN
- Cards

- FP Template
- Palm Template
- User Photo
- Face Template

FP Template Type - If Credential is selected as FP Template; then you can select the Type of FP Template which is to be deleted. The options of template are Suprema Proprietary, Suprema ISO, Lumidigm ISO, Lumidigm Proprietary. You can also choose all the templates by selecting "All" option.

Select Visitor- You can select the individual visitors by selecting **Visitor Wise** option or all the visitors by selecting option **All**. For **Visitor Wise** option select the individual visitors from the picklist.

Delete Credentials

Single Visitor

Multiple Visitors

Credential: Palm Template

Select Visitor: Visitor Wise

Visitor * ID Name

Search

User ID	Name	
V1	Nammy	
V2	Jinu	
V3	Parshv	

Delete From: Entire System

Delete

Delete Credentials

Single Visitor

Multiple Visitors

Credential: FP Template

FP Template Type: All

Select Visitor: All

Delete Credentials For: Active Visitors

Delete From: Entire System

Delete

Delete From - Select the Devices from where the selected credentials are to be deleted for the multiple visitor. The options for Delete will depend on the credential selected.

- **All Allotted Devices** - This option appears for FP Template only. Select this to delete credentials on all allotted devices.
- **All Allotted PVR Devices** - This option appears for Palm Template only. Select this to delete credentials on all allotted PVR devices.
- **All Allotted NGT & Vega Controllers** - This option appears for Visitor Photo only. Select this to delete credentials on all allotted NGT and Vega controllers.

Click the **Delete** button to delete the multiple visitors credential on the selected devices.

Sync From Device

The **Sync From Device** option enables the COSEC system to synchronize user credential details between the COSEC device and COSEC database. It enables the system to pull the credentials from the Devices and sync to the database.

To access this functionality, Select the **Visitor Management module > Utilities > Sync From Device**.

Single Visitor

The screenshot shows the 'Sync From Device' window. On the left, there's a sidebar with 'Single Visitor' (selected) and 'Multiple Visitors'. The main content area has a 'Sync From Device' section. It includes a 'Device' field with a value of '1' and a dropdown showing 'ARC DC 200 DDDR'. Below it is a 'Credential' dropdown set to 'Cards'. Further down is a 'Visitor' field with a value of '1581' and a dropdown showing 'Kinchit'. At the bottom center is a dark 'Sync' button.

- **Device**- Select the Device from the Picklist from which the credentials are to be pulled.
- **Credential** -Select the credential type from the options of **Card**, **FP Template** or **Palm Template**.

Sync From Device

- Select the **Visitor** from the picklist whose credentials from the device are to be restored to database.
- Click on **Sync** to save the credentials to the database.

Multiple Visitor

The screenshot shows the 'Sync From Device' window for multiple visitors. The sidebar has 'Multiple Visitors' selected. The main area has a 'Sync From Device' section. It includes a 'Device' field with a value of '1' and a dropdown showing 'DoorV1'. Below it is a 'Credential' dropdown set to 'Cards'. Further down is a 'Select Visitor' dropdown set to 'Visitor Wise'. Below that is a table with columns 'Visitor ID' and 'Name'. The table contains one row with 'V1' and 'Visitor1'. At the bottom center is a dark 'Sync' button.

- **Device**- Select the device from the picklist from where the multiple visitor credentials are to be pulled for syncing with database.

- **Credential** - Select the credential type from the options of **Card**, **FP Template** or **Palm Template** which is to be synced to database.

Sync From Device

- **Select Visitor**- You can select the individual visitors by selecting **Visitor Wise** option or all the visitors by selecting option **All**. For **Visitor Wise** option select the individual visitors from the picklist.
- Click on **Sync** to save the credentials to the database

Visitor Events

The **Visitor Events** page enables the Admin to view the information regarding the events of the Visitors and track their real time location.

Admin can view visitor's events that is check-in/check-out, auto punch, device punch events etc.

The possible sources from which visitor events can be marked are — Station (VMS Web Portal / VMS Utility), VMS Application, Email and Device.

Types of Visitor Events

Check-In/ Check-Out Events

- The visitor check-in and check-out events can be marked via — Station (VMS Web Portal/VMS Utility), Application, Email and Device.
- The visitor check-out event can be marked by the System as well when the visitor surrenders the visitor-pass.

Auto Punch Events

- When a visitor checks-in for a visit, a Visitor Profile ID is assigned to the visitor for that visit duration. To know more about the Visitor Profile, refer "[Visitor Profile](#)".
- Any events that are received during the visit duration against the Visitor Profile ID, such events will be stored by the system and will be displayed here. Once, the visitor checks-out, only check-in/check-out events will be stored against that Visitor Profile ID.

Offline Punch Events (Application/ Device)

- Offline punches are those punches that are stored locally by the application/device, when the connectivity to the server is lost.
- When the application/device regains the connectivity to the server, offline punches will be sent to the server.
- When the server receives any offline punches, then the sever will first check the visit-state corresponding to the Visitor Profile.

There can be two possible visit-states:

1. Visit-state= check-in
2. Visit-state= check-out

Case 1: Visit-state= check-in

In this case, server will accept all offline punches that are sent by the application/device.

Case 2: Visit-state= check-out

In this case, server will check the time of each offline punch. If the offline punch time is before the check-out punch time, then the server will accept the offline punch.

If the offline punch time is after the check-out punch time, server will discard that punch.

Hence, offline punches that are obtained before the check-out time will only be accepted by the server.

Device Punch Events

- Visitor punches via Device are stored against the Visitor Profile ID assigned to that Visitor.
- A Visitor Profile can be assigned to multiple Visitors with different Appointment Numbers and when different visitors punch via device, the events generated for these punches will be stored against the Visitor Profile along with the Appointment Numbers.

So when the Admin checks these events, s/he can view which punches were marked by which Visitors on the basis of Appointment Number.

To access this functionality, select the **Visitor Management module > Utilities > Visitor Events** and the page appears as shown below.

Date-Time	Mobile Number	Appointment Number	I/O Type	Access	Source Details	Source	View Image
14/10/2021 11:22:03	11	211014000001	Entry	Allowed	Default Location	Station	
14/10/2021 11:22:33	11	211014000001	Exit	Allowed	Default Location	Station	
14/10/2021 14:34:42	11	211014000029	Exit	Allowed		App	
14/10/2021 15:19:55	11	211014000039	Exit	Allowed		App	
14/10/2021 15:28:25	11	211014000040	Exit	Allowed		App	

Configure the following parameters to view events:

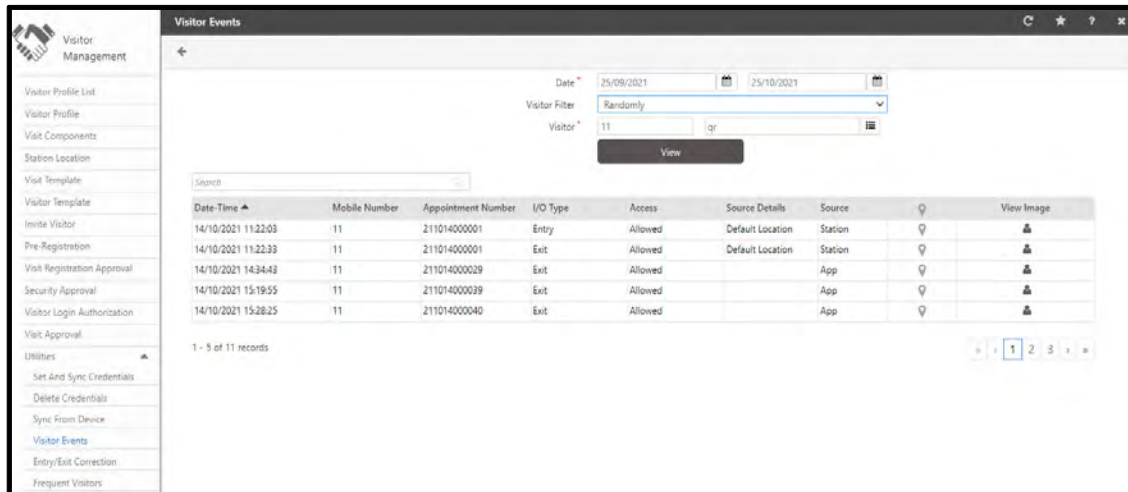
Date: Select the desired date range for which the events are to be viewed.

Visitor Filter: Select the desired filter from the drop down list.

- **All:** To view events of all the visitors.
- **Randomly:** To view events of the selected visitor. Select the desired **Visitor** from the pick list.

Visitor: Enter the **Mobile No.** of the visitor whose events are to be viewed. You can even select the desired visitor from the picklist.

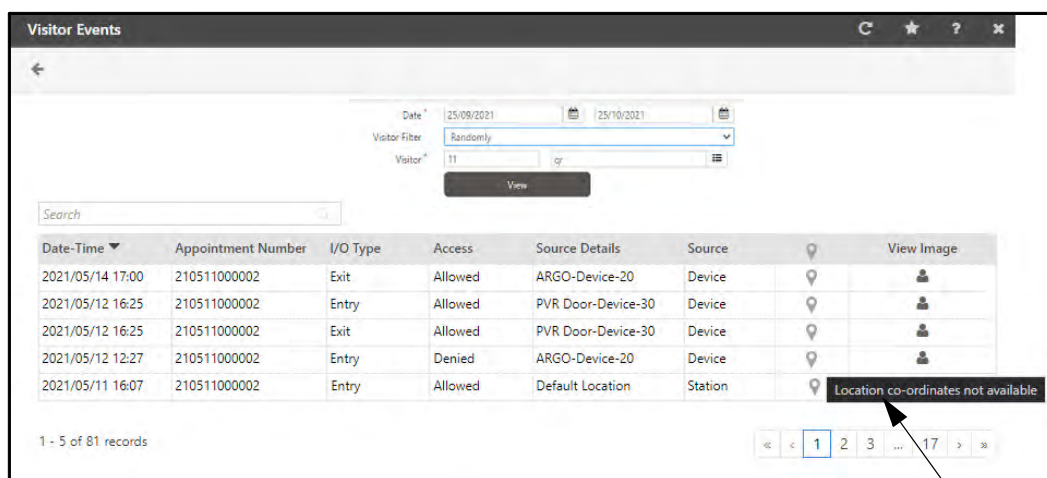
Click **View** and the visitor events will be displayed as shown below:



Visitor Events Details like — Date-Time, Appointment Number, I/O Type, Access, Source Details, Source, Location, View Image — are displayed.

When any event is marked through VMS Application, you will be able to view the Visitor's Location. To view the location details, click on **Location** 📍 icon.

Case 1: In case, the Location details are unavailable, on hovering your mouse over **Location** 📍 icon, a message will be displayed saying 'Location Co-ordinates not available' as shown below:




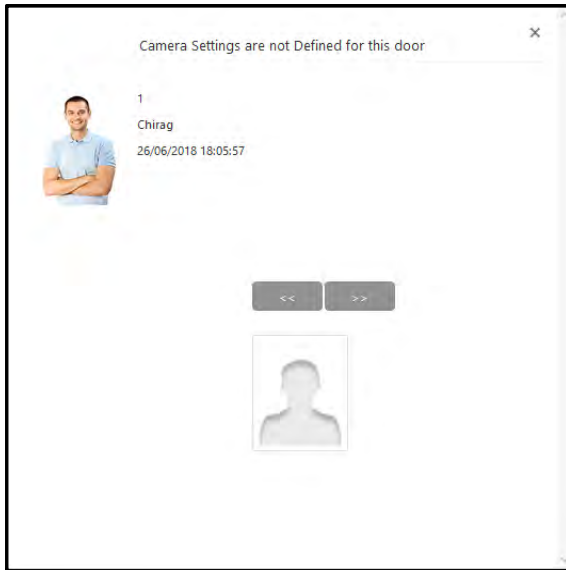
Case 2: If you have an Internet access and the Location details are available, click on **Location** 📍 icon and you will be directed to the Google Maps page.

Case 3: If you do not have an Internet access but the Location details are available, click on **Location** 📍 icon and a pop-up appears displaying the details of Location in terms of Latitude and Longitude.



If Map is not loaded; check the network connection of your PC or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

Click on **View Image**  to view the captured image of the visitor as shown below. If no image is captured, then this icon will be inactive.



Entry/Exit Correction

This option enables the application user to manually edit the entry and exit time of the Visitor. In case where the system is unable to recognise the credential of visitor or if the visitor pass is paper pass then the entry or exit of the visitor can be recorded manually.

To do the Entry/ Exit Correction, select **Visitor Management module > Utilities > Entry/ Exit Correction**. The Page appears as shown below:

The screenshot shows the 'Entry/Exit Correction' window. It has a search bar at the top right. Below it, there are input fields for 'Pass Issue Date' and 'Pass Number'. A 'Search' button is located below these fields. Below the search fields, there is a table with the following columns: 'Visit Date', 'Punch Time - In', 'Punch Time - Out', and 'Duration'. The table currently displays 'No Data'. On the right side of the window, there is a table with the following columns: 'Pass Issue Date', 'Pass Number', and 'Name'. The table contains three rows of data:

Pass Issue Date	Pass Number	Name
04/12/2017	170412000003	Dinesh
04/12/2017	170412000002	Jinu Sam
04/12/2017	170412000001	Jinu Sam

The grid on the right displays the Visitors with Pass issue date and Pass number.

Select a visitor from the grid whose Entry/Exit correction is to be done. The visitor Pass and In/Out details will be generated in the respective fields.

The screenshot shows the 'Entry/Exit Correction' window with a visitor selected. The 'Pass Issue Date' field is now populated with '04/12/2017' and the 'Pass Number' field is populated with '170412000003'. The 'Visit Date' field is now populated with '04/12/2017' and the 'Punch Time - In' field is populated with '16:38'. The 'Punch Time - Out' and 'Duration' fields are still empty. The table on the right side of the window is the same as in the previous screenshot, but the first row (Dinesh) is highlighted in blue.

To do the correction, Click the Edit button in the grid. Enter or edit the **IN-OUT Punch** fields with Entry and Exit time falling within the Visit Hours as shown in Visitor History section.

Then click OK to save the changes. The Duration will be automatically calculated based on entry-exit timings.

Visit Date ▲	Punch Time - In	Punch Time - Out	Duration	
04/12/2017	16:38	17:20		✓ ✕

Entry/Exit Correction

✓ Saved Successfully ✕

★

←

Search

Pass Issue Date

04/12/2017

Pass Number

170412000003

Search

Visit Date ▲	Punch Time - In	Punch Time - Out	Duration	
04/12/2017	16:38	17:20	00:42	

Pass Issue Date ▼

Pass Number

Name

04/12/2017	170412000003	Dinesh
04/12/2017	170412000002	Jinu Sam
04/12/2017	170412000001	Jinu Sam

Frequent Visitors

This option displays the list of Frequent Visitors who visits frequently to the company. It enables to add the frequent visitor either to watchlist or blacklist.

The watchlist visitor can be monitored and a blacklist visitor can be restricted for any further visit.

To add or view the frequent visitors, Click on **Visitor Management module > Utilities > Frequent Visitors**. The Page appears as shown below:

Click on the **New** button to add a new frequent visitor.

Enter the basic details like **Name, Organization, Mobile number, Last Visit Details** and the required **Additional Details**.

Additional Details

Additional Details

Address

City

State

Country

PIN/ZIP Code

Email ID

Gender NA

Date of Birth

Nationality

Enrolled Fingers

ID Proof 1

ID Proof 2

Custom Fields

Custom Field 1

Custom Field 2


Custom Field 3

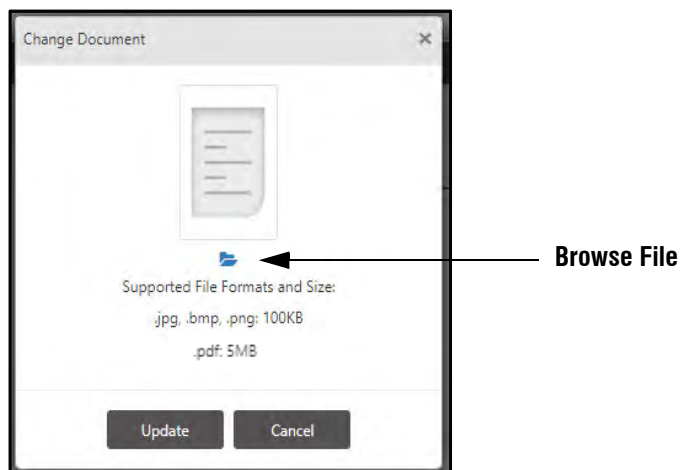
Custom Field 4

Custom Field 5




1. Enrolled fingers is the read only field.
2. The ID Proof 1, ID Proof 2 and Custom fields will appear as entered in Global Policy> Visitor Management.


Under **Additional Details**, you can upload the documents in Custom Fields, by clicking **Upload**  button. Then **Change Document** pop-up appears as shown below.




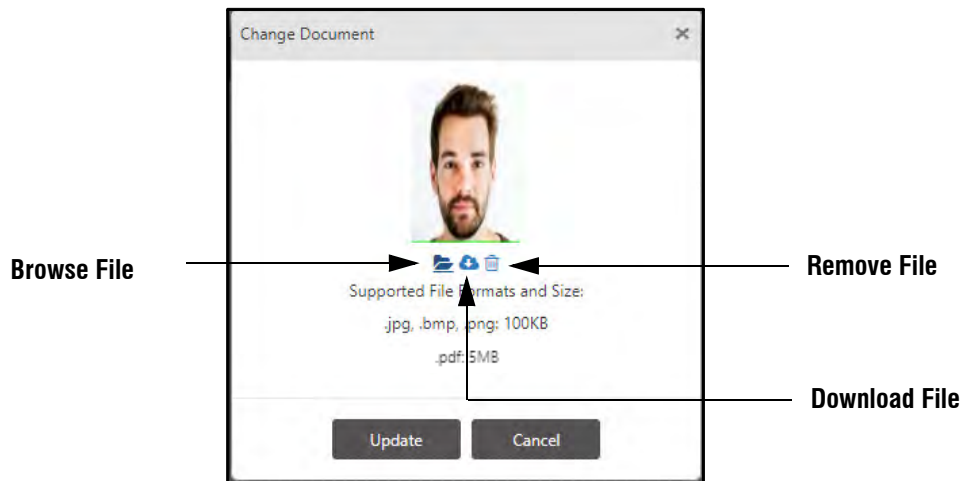
Click **Browse File** .

To upload, select the desired file as per the supported formats and size (.jpg, .bmp, .png, .pdf) from your local PC.


After uploading the file, if you wish to upload a different file instead of the current uploaded file, click **Browse File**  again and select the desired file from your local PC. The previously uploaded file will get replaced with the new file.

To download the uploaded file, click **Download File**  .

To remove the uploaded file, click **Remove File**  .



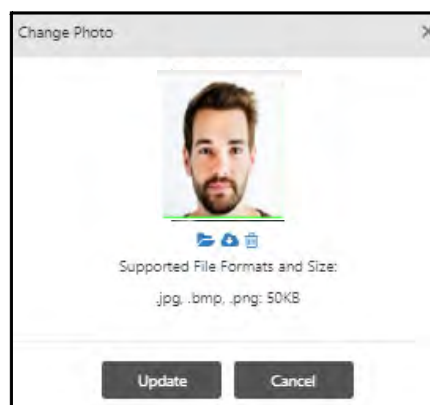
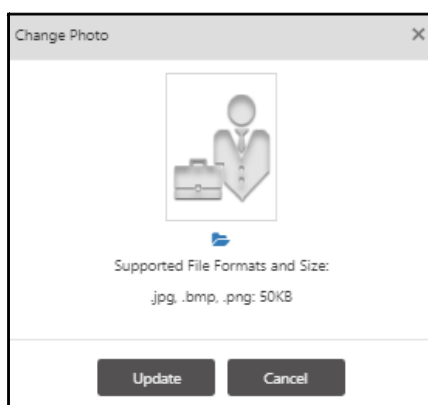
Then click **Update**.

The document will be uploaded and can be previewed by clicking on **Preview**  button.

Click **Save** to save the frequent visitor. The grid on the right displays the Visitors with their mobile numbers.

Frequent Visitor Photo


You can also upload the Visitor photo in Edit mode. Click on the Photo icon, browse the image and click the Update button. Then click Save button. to save the visitor photo.



The Last Visit details of the frequent visitor will be displayed here as per the details specified in the VMS Utility.

Frequent Visitors

← + ✎ 📄 ✕



Name * xyz

Organization * abc

Mobile Number * 369

Last Visit Details

Visit Period 20/10/2021 20/10/2021

Visit Hours 08:55 09:55

Host User 2686 Mayank Vishnori

Escort User

Additional Visitors 0

Purpose

Add To Watchlist Add To Blacklist

Additional Details


Credentials

Adding Frequent Visitors to the Watchlist

To add an existing frequent visitor to the Watchlist, click the desired visitor from the right pane and click Save or Cancel button. The **Add To Watchlist** button will get enabled.

Frequent Visitors

← + ✎ 📄 ✕



Name * xyz

Organization * abc

Mobile Number * 369

Last Visit Details

Visit Period 20/10/2021 20/10/2021

Visit Hours 08:55 09:55

Host User 2686 Mayank Vishnori

Escort User

Additional Visitors 0

Purpose

Add To Watchlist Add To Blacklist

Additional Details

Credentials

Search

Visitor Name	Mobile Number
xxx	141
xyz	369

121 - 122 of 122 records

« < 1 ... 7 8 9 > »

Now click **Add to Watchlist** button. The selected Visitor will be removed from the Frequent Visitors list and will be added to the Watchlist. For details refer "[Watchlist/Blacklist](#)".

Visitor Name	Mobile Number
WL	701
xyz	369



The frequent visitor can be moved to Watchlist from VMS Utility also.

Adding Frequent Visitor to the Blacklist

To add an existing frequent visitor to Blacklist, click the desired visitor from the right pane and click Save or Cancel button. The **Add to Blacklist** button will get enabled.

Visitor Name	Mobile Number
xxx	141
xyz	369

Now click **Add to Blacklist** button..The selected Visitor will be removed from the Frequent Visitors list and will be added to the Blacklist. For details refer [“Watchlist/Blacklist”](#).

The screenshot shows the 'Watchlist/Blacklist' interface. On the left, there's a form for a visitor named 'xyz' with organization 'abc' and mobile number '369'. Below this is the 'Last Visit Details' section with fields for Visit Period (20/10/2021), Visit Hours (08:55 to 09:55), Host User (2686, Mayank Vishnori), Escort User, Additional Visitors (0), Purpose, and Black Listed On (27/10/2021 16:09:13). A 'Restore Visitor' button is at the bottom. On the right, a table shows the status of visitors:

Total	Watchlist	Blacklist
39	16	23

Below the table is a list of visitors with columns for Visitor Name and Mobile Number. The visitor 'xyz' with mobile number '369' is highlighted. At the bottom right, it says '16 - 23 of 23 records' with pagination controls.



The frequent visitor can be moved to Blacklist from VMS Utility also.



In order to receive an alert when a frequent visitor is added to Watchlist/Blacklist make sure you have configured the alert in Admin> System Configuration> Alert Message Configuration. Set the Alert Filter as Visitor Management and Event as Visitor Added - Watchlist/Blacklist. For details refer to ["Configuring Alert Messages"](#).

Credentials

Configure the following parameters:

The screenshot shows the 'Credentials' configuration window. It contains several input fields for different types of biometric templates:

- Enrolled Fingers (Suprema Proprietary)
- Enrolled Fingers (Suprema ISO)
- Enrolled Fingers (Lumidigm ISO)
- Enrolled Fingers (Lumidigm Proprietary)
- Enrolled Palms
- Enrolled Faces

Enrolled Fingers: It displays the number of fingerprint templates enrolled against the selected visitor. Types of fingerprint templates are — Suprema Proprietary, Suprema ISO, Lumidigm ISO, Lumidigm Proprietary.

Enrolled Palms: It displays the number of palm vein templates enrolled against the selected visitor.

Enrolled Faces: It displays the number of face templates enrolled against the selected visitor.

Watchlist/Blacklist

This page displays the list of visitors under watchlist and blacklist. It enables to monitor the visitors creating problems and to restrict their entry into the organisation.

The SA can:

- view the details of the Watchlist/Blacklist visitor.
- edit the details of the Watchlist/Blacklist visitor.
- restore the visitor to frequent visitor from Watchlist/Blacklist .

Select **Visitor Management module > Utilities > Watchlist/Blacklist**. The page appears as shown below:

Visitor Name	Mobile Number
4567	4567
5678	5678
9667295144	9667295144
beforewatchlist	46547463
copatel	366
gdsig	3253
ghghg	345435
H8	3333
invite ul	12345
mitesh	1245
preregistration	4444
qr	11
terbre	5235435
vmwatch	456
watchlist1	3543657

Additional Details

Address

City

State

Country

PIN/ZIP Code

Email ID

Gender: NA

Date of Birth

Nationality

Enrolled Fingers

ID Proof 1

ID Proof 2

Custom Fields

- Custom Field 1
- Custom Field 2
- Custom Field 3
- Custom Field 4
- Custom Field 5

The grid in the right pane displays — **Total** visitors, **Watchlist** visitors and **Blacklist** visitors.

Total	Watchlist	Blacklist
39	16	23

Visitor Name ▲	Mobile Number
4567	4567
5678	5678
8160002595	8160002595
9687295144	9687295144
ad2	7777
beforewatchlist	46547463
BL	702
Blacklist1	121324354
Blacklist2	53443626
Blacklist4	43512452
Blacklist5	5465246
Blacklist6	24327567
Blacklist7	436575689
Blacklist8	37635676358
Blacklist9	645675373

1 - 15 of 39 records

« < 1 2 3 > »

- **Total:** Displays all the Visitors including Watchlist and Blacklist.
- **Watchlist:** Displays only Watchlist Visitors.
- **Blacklist:** Displays only Blacklist Visitors.

Click the desired tab — Total, Watchlist, Blacklist as per your requirement.

The list appears as per the option selected.

Click on the desired entry and the visitor details will be displayed in the left pane.

The basic details like Name, Organisation, Mobile number and all **Additional Details** except Enrolled fingers can be edited.

After editing click on **Save** button. The **Restore Visitor** button will be enabled.

Click on **Restore Visitor** button to restore the visitor from Watchlist/Blacklist to Frequent Visitors list.

Watchlist/Blacklist

Name *

xyz

Organization *

abc

Mobile Number *

369

Last Visit Details

Visit Period

20/10/2021

20/10/2021

Visit Hours

08:55

09:55

Host User

2686

Mayank Vishnori

Escort User

Additional Visitors

0

Purpose

Black Listed On

20/10/2021 09:12:28

Restore Visitor



The frequent visitor can be moved to Watchlist/Blacklist from VMS Utility also.

Additional Details

Additional Details

Address

City

State

Country

PIN/ZIP Code

Email ID

Gender

NA

Date of Birth

Nationality

Enrolled Fingers

ID Proof 1

ID Proof 2

Custom Field 1

Custom Field 2

Custom Field 3


Custom Field 4

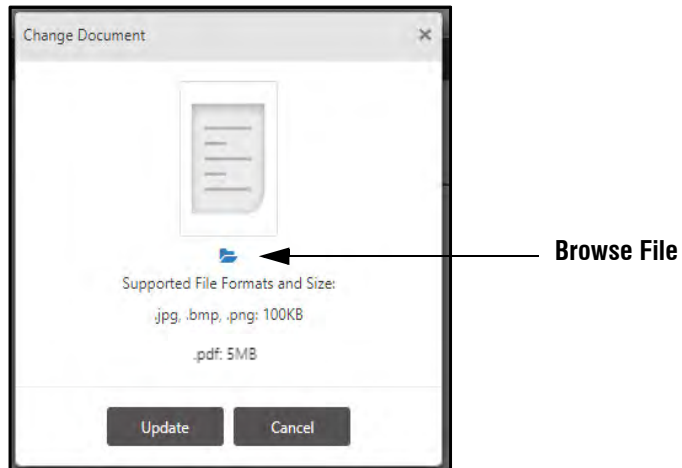
Custom Field 5



1. Enrolled fingers is the read only field.

2. The ID Proof 1, ID Proof 2 and Custom fields will appear as entered in Global Policy> Visitor Management.


Under **Additional Details**, you can upload the documents in Custom Fields, by clicking **Upload**  button. Then **Change Document** pop-up appears as shown below.





Click **Browse File**  .

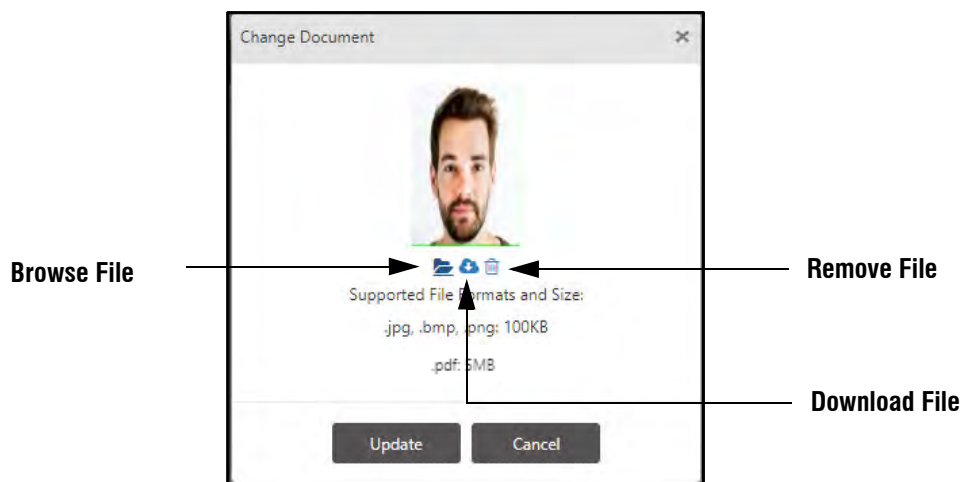
Select the desired file as per the supported formats and size (.jpg, .bmp, .png, pdf) from your local PC.

After uploading the file, if you wish to upload a different file instead of the current uploaded file, click **Browse File**


 again and select the desired file from your local PC. The previously uploaded file will get replaced with the new file.

To download the uploaded file, click **Download File**  .

To remove the uploaded file, click **Remove File**  .



Then click **Update**.

The document will be uploaded and can be previewed by clicking on **Preview**  button.

The **Last Visit Details** will be displayed as entered in VMS Utility.

Similarly, if required you can click on the Profile photo to change the same.

Visitor History

This option displays the list of all the passes created in database including issued,surrendered and expired.

To view the Visitor History, Click on **Visitor Management module > Utilities > Visitor History**. The Page appears as shown below:

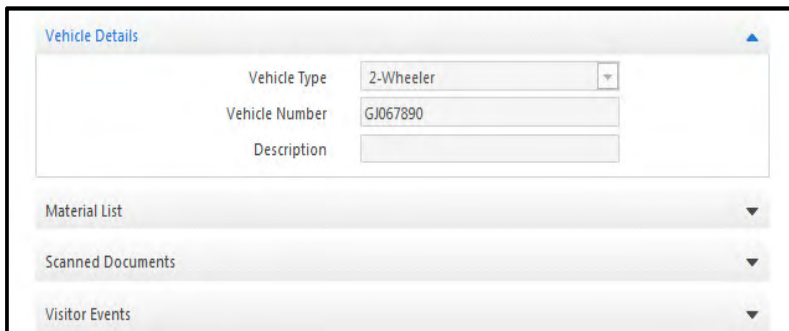
Custom Fields

Appointment No.	Issue Date	Pass Number	Visitor Name
210702000001	02/07/2021	210702000001	D
210625000004	25/06/2021	210625000001	MI
210625000005	25/06/2021	210625000002	MI
210625000006	25/06/2021	210625000003	MI
210625000007	25/06/2021	210625000004	MI
210625000008	25/06/2021	210625000005	MI
210625000009	25/06/2021	210625000006	MI
210625000010	25/06/2021	210625000007	MI
210625000011	25/06/2021	210625000008	MI
210625000012	25/06/2021	210625000009	MI
210625000013	25/06/2021	210625000010	MI

The grid on the right displays the list of visitors with their pass number and pass issue date.

Click on the Visitor from the grid to view the basic and visit details.

The other details like **Vehicle Details**, **Material List**, **Scanned Documents** and **Visitor Events** are displayed in the fields as configured from the VMS Utility.



The screenshot shows a software interface titled "Vehicle Details" with a blue header bar. Below the header, there are three input fields: "Vehicle Type" with a dropdown menu showing "2-Wheeler", "Vehicle Number" with the text "GJ067890", and "Description" which is empty. Below these fields are three expandable sections, each with a downward-pointing arrow: "Material List", "Scanned Documents", and "Visitor Events".

Vehicle Details display the information of the visitor's vehicle.

Material List describes the material carried by the visitor.

Scanned Document gives the list of visitor's document scanned during pass creation.

Visitor Events display the events that are recorded from the pass issue date-time to the surrender date-time.

Enrollment

To enroll a visitor on the desired device, select the **Visitor Management module > Utilities > Enrollment**.

The **Enrollment** page appears as shown below:

Enrollment

Door* ID Name

Device Readers

Visitor* ID Name

Visitor Enrollment Status

Enrollment Type Select

Number of Cards One

Number of Fingers One

Number of Palms Two

Access Card Selection Access Card 1

Number of Faces 1

Enroll

- **Door:** Select the desired door from the picklist on which the enrollment is to be done.

Device Readers

Device Readers displays the information of the readers configured in the selected **Door**.

Door* 3 ARGO

Device Readers

Card Reader MiFare Reader

Biometric Reader None

External Reader MiFare-U Reader

Card Reader, Biometric Reader and External Reader information are displayed here.

- **Visitor:** Select the desired visitor from the picklist for whom the enrollment is to be done.

Visitor Enrollment Status	
Enrolled Fingers (Suprema Proprietary)	0
Enrolled Fingers (Suprema ISO)	0
Enrolled Fingers (Lumidigm ISO)	0
Enrolled Fingers (Lumidigm Proprietary)	0
Enrolled Palms	0
Enrolled Card 1	
Enrolled Card 2	
Enrolled Faces	0

Visitor Enrollment Status

Visitor Enrollment Status displays the information related to the number of already enrolled credentials of the visitor like fingers, palms, cards and faces.

Details like — **Enrolled Fingers (Suprema Proprietary)**, **Enrolled Fingers (Suprema ISO)**, **Enrolled Fingers (Lumidigm ISO)**, **Enrolled Fingers (Lumidigm Proprietary)**, **Enrolled Palms**, **Enrolled Card 1**, **Enrolled Card 2** and **Enrolled Faces** — are displayed here.

- **Enrollment Type:** Select the desired enrollment type — Read Only Card, Smart Card, Face, Biometrics, BiometricsThenCard and Mobile — from the drop down list.

Based on the selection of the **Door** and **Enrollment Type**, below parameters will be displayed for configuration.



Below parameters also depend on the Readers configured in the Door. To configure the desired Reader, refer Readers section under Devices > Device Configuration (of the desired Door) > Profile > Readers.

1. Enrollment Type = Read Only Card

Number of Cards: Select the desired number of cards from the drop-down list.

Enrollment Type	Read Only Card
Number of Cards	One

2. Enrollment Type = Smart Card

Number of Cards: Select the desired number of cards from the drop-down list.

Details on Smart Card

Select the desired check boxes of the parameters — **Visitor ID**, **Facility Code (FC)**, **Additional Security Code (ASC)** — which are to be displayed on the Smart Card.

Select the desired number of **Finger Templates** from the drop down list.

If **Door** is selected as PVR Door, then **Palm Templates** parameter will be visible. Select the check box of this parameter if you wish to display it on the Smart Card.

To store the palm templates, MiFare 4k reader must be configured in the PVR Door.



Door PVR must be set in the Adaptive mode (configure from Admin> System Configuration> Global Policy) for the palm templates to be saved into the Smart Card.

Additional Details on Smart Card

Other than the parameters mentioned in the Details on Smart Card, you can display additional details on Smart Card.

Select the **Short Name** check box to display it on the Smart Card.

3. Enrollment Type = Face

Number of Faces: Select the desired number of face from the dropdown list.

4. Enrollment Type = Biometrics

Number of Fingers/ Number of Palms: Select the desired number of fingers or palms from the drop down list.

Enrollment Type: Biometrics
Number of Fingers: One

Enrollment Type: Biometrics
Number of Palms: One

5. Enrollment Type = BiometricsThenCard

Number of Cards: Select the desired number of cards from the drop down list.

Number of Fingers/ Number of Palms: Select the desired number of fingers or palms from the drop down list.

Enrollment Type: BiometricsThenCard
Number of Cards: One
Number of Fingers: One

Details on Smart Card

Visitor ID: ☐
Facility Code (FC): ☐
Additional Security Code (ASC): ☐
Finger Templates: None

Additional Details On Smart Card

Short Name: ☐ Visitor11

Enroll

Details on Smart Card

Select the desired check boxes of the parameters — **Visitor ID**, **Facility Code (FC)**, **Additional Security Code (ASC)** — which are to be displayed on the Smart Card.

Select the desired number of **Finger Templates** from the drop down list.

If the **Door** is selected as PVR Door, **Palm Templates** parameter will be visible. Select the check box of this parameter if you wish to display it on the Smart Card.

To store palm templates, MiFare 4k reader must be configured in the PVR Door.



Door PVR must be set in the Adaptive mode (configure from Admin> System Configuration> Global Policy) for the palm templates to be saved into the Smart Card.

Additional Details on Smart Card

Other than the parameters mentioned in the Details on Smart Card, you can display additional details on Smart Card.

Select the **Short Name** check box to display it on the Smart Card.

6. Enrollment Type = Mobile



To select **Enrollment Type** as *Mobile*, the particular device must have BLE support and ensure Bluetooth is ON in the mobile.

Access Card Selection: Select the desired Access Card from the drop down list.

Enrollment Type	Mobile
Access Card Selection	Access Card 1
Facility Code (FC)	<input type="checkbox"/>

Facility Code (FC): Select this check box to enroll the Facility Code (FC) against the visitor.

After the enrollment process, the visitor must tap on **Tap to Register > Matrix Device** from the ACS Application installed on respective mobile phone and select the same configured Door from **Available Doors**. Thereafter, that visitor can access the device through ACS application for Access Control purpose.

The value in Access Card selected will be consider as Access ID of the visitor. If Access Card selected has no value i.e blank, then after the enrollment process, the system will auto-generate 18 digits number as visitor Access ID and store the same value.

Click **Enroll** to initiate the enrollment process and the enrollment command is sent to the Door.

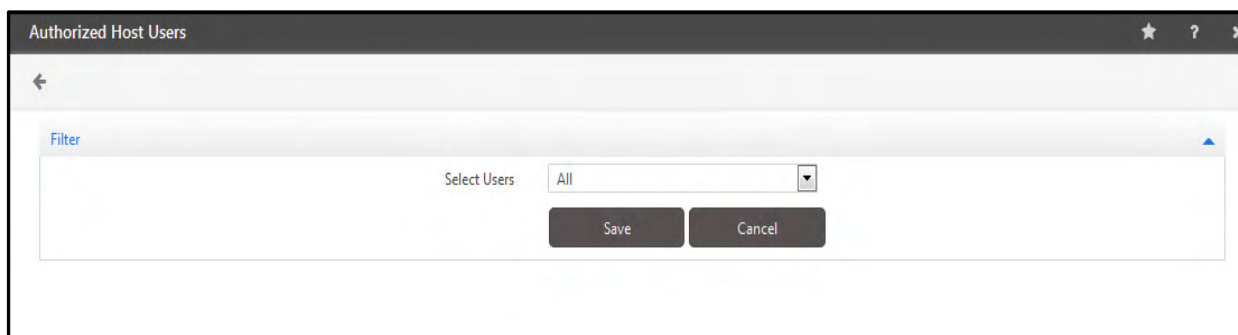
For Panel Door the command is sent to the Panel200 which will communicate further to the Door.

Once all the required credentials of an visitor are enrolled, the number of credentials enrolled will be displayed in the *Visitor Management > Visitor Profile (Select the particular Visitor Profile) > Credentials*.

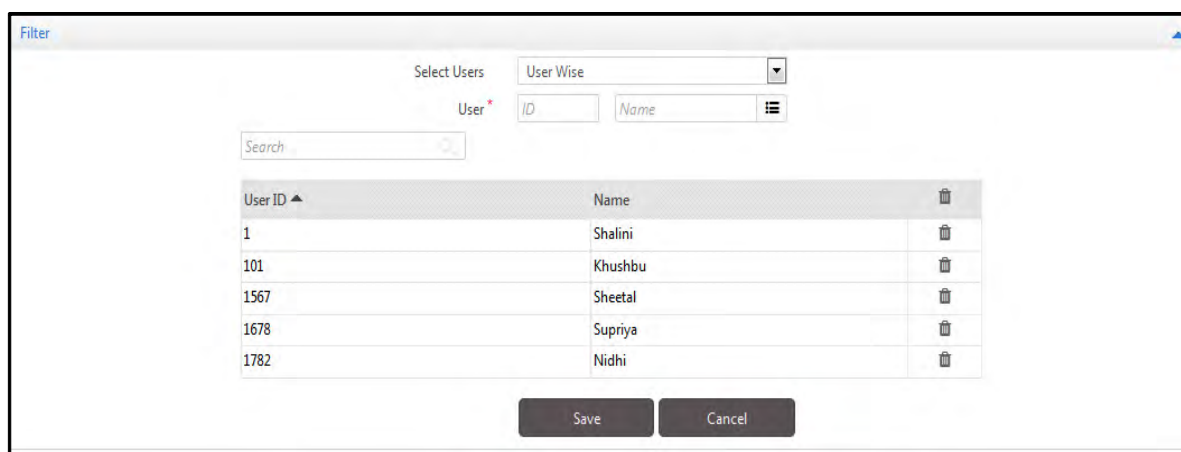
Authorized Host Users

The selected few users are required to be authorized host users.

Select **Visitor Management module> Utilities> Authorized Host Users**. The Authorized Host Users page appears as shown below:



Select Users based on the options — User Wise, Group Wise or All.



User ID	Name	
1	Shalini	
101	Khushbu	
1567	Sheetal	
1678	Supriya	
1782	Nidhi	



The **"Pre-Registration"** of visitors can be done only by authorized host users from ESS account.

A host can also be authorized from the following paths:

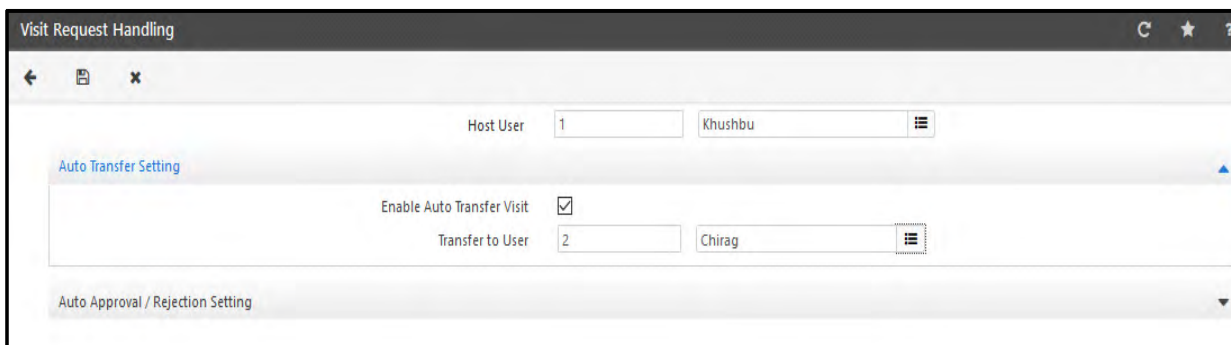
- Users> User Configuration> Visitor Management.
- Users> Multi-User Option> User Configuration
- Contract Worker Management> Worker> Worker Profile

Click **Save** to save the selected users. These authorized host users will be available in host user picklist when system account user pre-registers a visitor.

Visit Request Handling

The Visit Request handling page enables to configure any host user's (based on user rights) visit handling settings such as Auto Transfer & Auto Approval/Rejection of visits.

Select **Visitor Management module> Utilities> Visit Request Handling**. The page appears as shown below:



The screenshot shows the 'Visit Request Handling' window. At the top, there's a 'Host User' section with a dropdown menu showing '1' and a text field with 'Khushbu'. Below this is the 'Auto Transfer Setting' section, which includes a checkbox for 'Enable Auto Transfer Visit' (checked) and a 'Transfer to User' section with a dropdown menu showing '2' and a text field with 'Chirag'. At the bottom is the 'Auto Approval / Rejection Setting' section, which is currently collapsed.

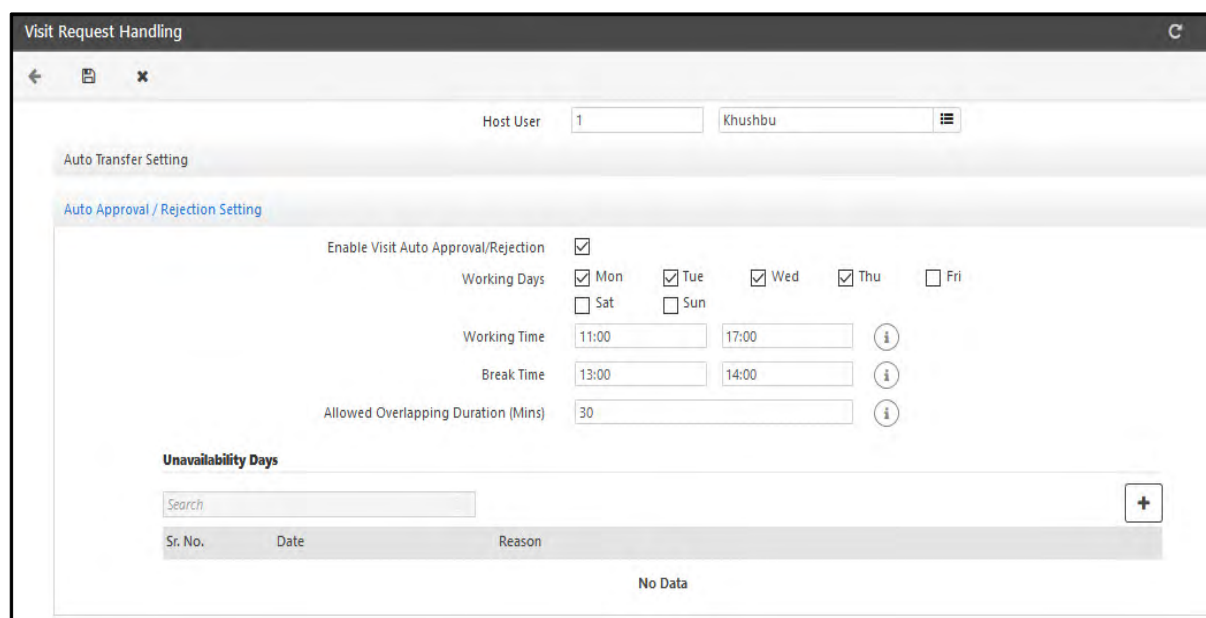
Host User: Select the host user for whom the visit request is to be handled.

Auto Transfer Setting

Enable Auto Transfer Visit: Enable this check-box to automatically transfer the visit to another user.

Transfer to User: Select the user from the picklist to whom the visit is to be transferred. The picklist contains all active authorized host users.

Auto Approval/Rejection Setting



The screenshot shows the 'Visit Request Handling' window with the 'Auto Approval / Rejection Setting' section expanded. It includes a checkbox for 'Enable Visit Auto Approval/Rejection' (checked). Below this is the 'Working Days' section with checkboxes for Mon, Tue, Wed, Thu, Fri, Sat, and Sun. The 'Working Time' section has two time input fields: '11:00' and '17:00'. The 'Break Time' section has two time input fields: '13:00' and '14:00'. The 'Allowed Overlapping Duration (Mins)' section has a text input field with '30'. At the bottom is the 'Unavailability Days' section, which includes a search bar and a table with columns 'Sr. No.', 'Date', and 'Reason'. The table is currently empty, showing 'No Data'.

Enable Visit Auto Approval/Rejection: Enable this check-box to automatically approve/reject the visit application.

Working Days: Select the days when the automatic visit approval/rejection is to be allowed.

Working Time: Enter the From time and To time in 24 hours format during which the visit can be auto approved.

Break Time: Enter the Start time and End time of Break duration during which the visit will be auto rejected.

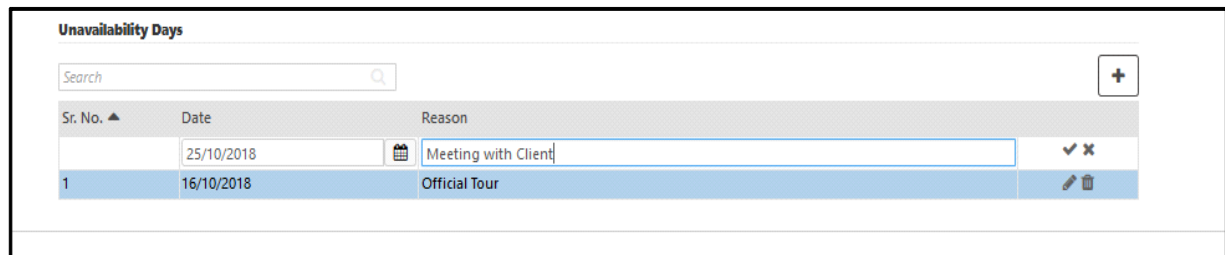
Allowed Overlapping Duration (Mins): Enter the duration in minutes. This duration must be overlapping within working time for the visit to auto approve. The valid range is 0 to 999 mins.

Unavailability Days

This section enables to configure days on which host user is not available i.e. the visit to host user can not be scheduled on the specified days.

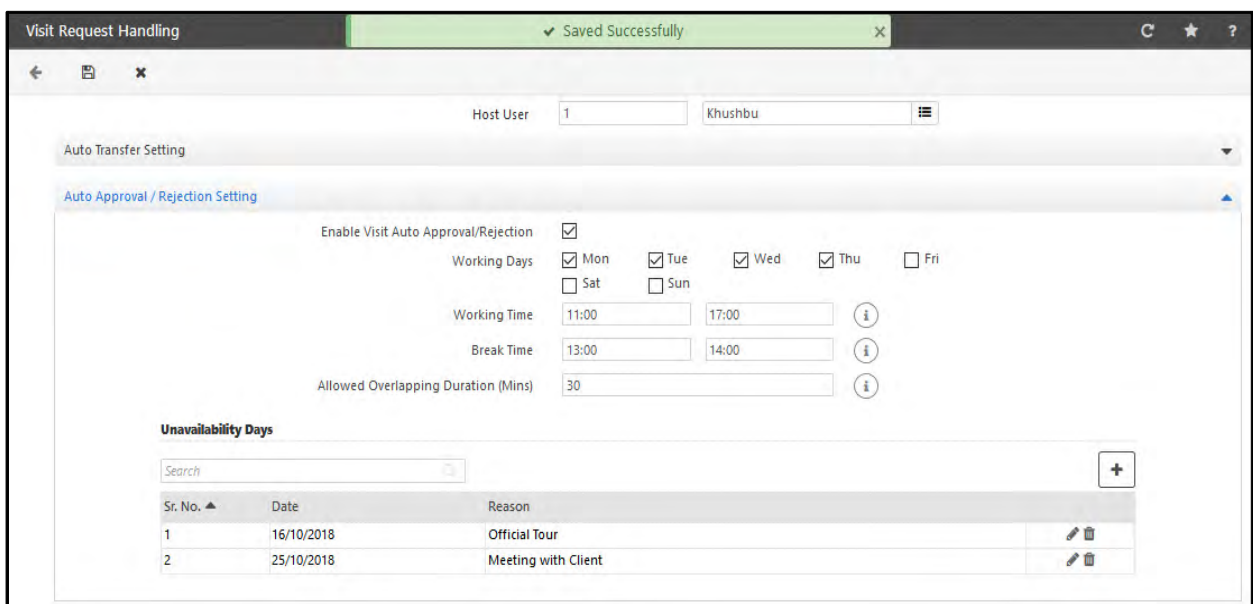
Click on **Add** button.

Select the **Date** from the calendar. Enter the **reason** for unavailability. Then click **OK** and **Save** to save the days.



The screenshot shows a window titled "Unavailability Days". It features a search bar at the top right with a "+" icon. Below is a table with columns: "Sr. No.", "Date", "Reason", and action icons. The table contains two entries:

Sr. No.	Date	Reason	
	25/10/2018	Meeting with Client	✓ ✕
1	16/10/2018	Official Tour	✎ ✕



The screenshot shows a "Visit Request Handling" window with a green status bar indicating "Saved Successfully". It includes fields for "Host User" (1) and "Khushbu". Below are sections for "Auto Transfer Setting" and "Auto Approval / Rejection Setting".

Auto Approval / Rejection Setting:

- Enable Visit Auto Approval/Rejection: ☒
- Working Days: ☒ Mon, ☒ Tue, ☒ Wed, ☒ Thu, ☐ Fri, ☐ Sat, ☐ Sun
- Working Time: 11:00 to 17:00
- Break Time: 13:00 to 14:00
- Allowed Overlapping Duration (Mins): 30

Unavailability Days:

Search bar with "+" icon. Table with columns: "Sr. No.", "Date", "Reason", and action icons.

Sr. No.	Date	Reason	
1	16/10/2018	Official Tour	✎ ✕
2	25/10/2018	Meeting with Client	✎ ✕

Delete Frequent Visitors

The Delete Frequent Visitors page enables to delete the frequent visitors as available in Visitor Utility.

Select **Visitor Management module> Utilities> Delete Frequent Visitors**. The page appears as shown below:

VisitorID	Visitor Name	Organization	Mobile No.	Visit Date Time
1	Pratibha Singh	Xylem	9824256789	



The frequent visitor's "Visit DateTime" will appear in the grid when pass is created for that frequent visitor.

Authorize Process

Username/Password: Enter the username and password of System Account user to authorize the deletion process. For example: "sa" and "admin".

Select Visitor

Select the frequent visitor to be deleted by checking the respective box. Then click on **Delete** button.

VisitorID	Visitor Name	Organization	Mobile No.	Visit Date Time
1	Pratibha Singh	Xylem	9824256789	

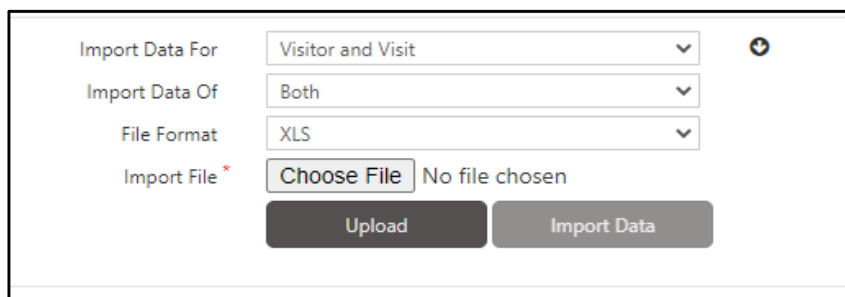
Click **OK** on Process Confirmation window. The selected visitor will be deleted from the COSEC system.

Import Visitor and Visit

The COSEC application has an inbuilt utility for enabling Admin to import Visitor and Visit data from files with predefined format.


To import data from a file follow the steps given below:

Select **Visitor Management > Utilities > Import Visitor and Visit** and the following screen appears:



Configure the following parameters:

- **Import Data For** - Select Visitor and Visit option from the drop down list for whom the data is to be imported.

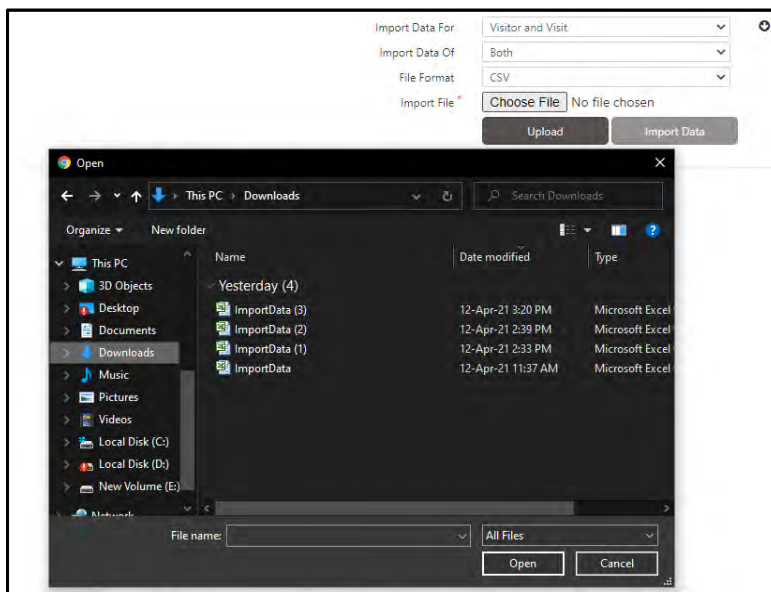
You can download a sample file by clicking **Download Sample Import file** . The downloaded import sheet displays the fields required for importing specific data.

You can even refer to the Import Data Document Guidelines in the downloaded import sheet.

Import Data Document Guidelines					
General Guidelines					
1 The sheet name should not be changed or the sheet will not be identified for import.					
2 The column names and the column position also should not be changed.					
3 For all date columns, the cell format should be "text" and date format should be same as configured in Web Server.					
USER Import Fields					
	Basic License	ACS License	T&A License	ACS + T&A License	
12 Organization	All fields	NA	All fields	All fields	
13 Branch	All fields	NA	All fields	All fields	
14 Department	All fields	NA	All fields	All fields	
15 Section	All fields	NA	All fields	All fields	
16 Category	All fields	NA	All fields	All fields	
17 Grade	All fields	NA	All fields	All fields	
18 Designation	All fields	NA	All fields	All fields	
19 Custom Group1	All fields	All fields	All fields	All fields	
20 Custom Group2	All fields	All fields	All fields	All fields	
21 Custom Group3	All fields	All fields	All fields	All fields	
User	UserId UserName Full Name ShortName Gender BloodGroup Father/Spouse Name BirthDate Joining Date Leaving Date PENO	Basic ScheduleGroupID StartShift	Basic ScheduleGroupID StartShift LeaveGroup WeekOffGroupID ReportingGroupID ApprovalPolicyID	Basic + ACS + T&A	

- **Import Data of:** To import data of a Visitor and/or a Visit, select the desired option — Visitor Only, Visit Only or Both.

- **File Format** - Select a file format from the dropdown list — XLS or CSV.
- **Import File** - Browse the path of the file from which the data is to be imported. Make sure the selected file's format is as per the configured File Format.



Click **Upload**. The file will be saved and you can preview the data.

The Administrator can preview the uploaded data to confirm if it is in order before giving the import command.

Click **Preview Data**. The preview data is displayed as below.

ID	Name	InCharge1ID	InCharge2ID	ApprovalPolicyID
4	HO Group	101	102	1
5	Factory Group	3	4	2

Now, click **Import Data** to start importing the uploaded data. The result of import is shown as Success or Failure along with result description as shown.

ID	Name	InCharge1ID	InCharge2ID	ApprovalPolicyID	Result	Result Description
4	HO Group	101	102	1	Success	New Reporting Group Added
5	Factory Group	3	4	2	Success	New Reporting Group Added

You can also filter imported result records on the basis of — Success, Failure or Both using the **Result** drop down options.

Once the data is imported successfully, data will be added or updated in COSEC Web.



Administrator needs to ensure that the ASP.NET user has full rights on the folder containing the Excel or .csv file for the import data operation.

Visitor Management Reports

COSEC Visitor Management module allows you to create and view an assortment of detailed and focused reports on the Visitor activities on your site. These reports can be viewed on the screen or printed at any time. Reports available within the COSEC Visitor management Module are as under:

[“Visitor Access”](#)

[“Visitor Pass”](#)

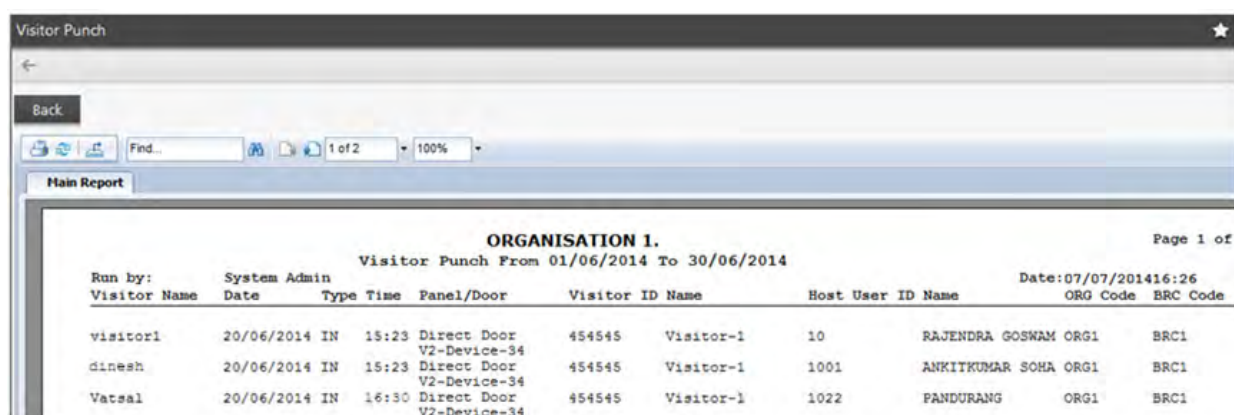
[“Visitor Summary”](#)

[“Visitor Evacuation”](#)

Visitor Access

Visitor Punch

Lists out details of all the Visitor punches in the defined date range.



ORGANISATION 1.									
Visitor Punch From 01/06/2014 To 30/06/2014									
Run by: System Admin									
Visitor Name	Date	Type	Time	Panel/Door	Visitor ID Name	Host User ID Name	ORG Code	BRC Code	
visitor1	20/06/2014	IN	15:23	Direct Door	454545	Visitor-1	10	RAJENDRA GOSWAM	ORG1
dinesh	20/06/2014	IN	15:23	Direct Door	454545	Visitor-1	1001	ANKITKUMAR SOHA	ORG1
Vatsal	20/06/2014	IN	16:30	Direct Door	454545	Visitor-1	1022	PANDURANG	ORG1

Visitor Punch Detail

The report generated will display details of the visitors including Name, Entry Date & Time as well as the Host Name for the selected date range. The Exit Date & Time and Total Time of his presence on the premises will also be listed.

Visitor Punch Exception

Exceptions like absence of In time or Out time of Visitors are listed in the report.

Visitor Enrollment Status

Generates a listing of all visitors who haven't been enrolled against a particular credential.

Visitor Enrollment Status							
Back							
Find... 1 of 1 100%							
Main Report							
<div> <div>ORGANISATION 1.</div> <div>Visitor Enrollment Status</div> <div>Run by: System Admin</div> <div>Date: 03/01/2014 16:49</div> <div>Page 1 of 1</div> </div>							
Sr No	Visitor ID	Name	Card1	Card2	PIN	Enrolled Fingers	Enrolled Palm
1	454545	Visitor-1	Not Enrolled	Not Enrolled	Not Enrolled	0	0
2	5001	Hetal Desai	Not Enrolled	Not Enrolled	Enrolled	2	0
3	9001	Visitor - 1	Not Enrolled	Not Enrolled	Enrolled	0	0

Panel Wise Visitor

Generates a PANEL wise listing of the Visitor cards defined in the system.

Visitor Access Denied

Lists out the invalid punch events of the Visitors at the various Door Controllers along with the reason.

Visitor Pass

Visitor Pass Validity

Date:

Time:

Specify the Pass Issue Date and the time falling in visit hours. Click on Generate. Lists out the valid Visitor passes for the selected date as well as the validity period of the passes.

Visitor Pass Validity							
Back							
Find... 1 of 1 100%							
Main Report							
<div> <div>ORGANISATION 1.</div> <div>Visitor Pass Validity On 22/08/2013 12:18</div> <div>Run by: System Admin</div> <div>Date: 03/01/2014 17:58</div> <div>Page 1 of 1</div> </div>							
Sr No	Name	Visitor Organization	Valid From	Valid UpTo	Host User	Host User Department	
1	test visitor	ABB	22/08/2013 12:18	22/08/2013 13:18	RAJENDRA	GOSWAM	Repairing







Visitor Pass Status

Lists out details of the Visitor pass status for the specified date range.

Visitor Pass Status

←

Back

   Find...    1 of 1 100%

Main Report

Visitor Pass Status as On 23/06/2014 18:36:29

Run by: System Admin

Date:23/06/2014 18:36

Visitor Name	Visitor ID Name	Valid From	Valid Upto	Surrender Date	Status
visitor100	visitor400 visitor400	23/06/2014 18:27	23/06/2014 18:29		Expired
Total:	<u>Prepared</u>	1	<u>Issued</u> 0	<u>Active</u> 0	<u>Surrendered</u> 0 <u>Expired</u> 1

Expired Passes

Lists out the Visitors whose passes are no longer valid but are yet to be surrendered.

Expired Passes					
Back					
Find... 1 of 1 100%					
Main Report					
ORGANISATION 1.					
Expired Passes from 03/01/2012 to 03/01/2014					
Run by:	System Admin				Date:03/01/201416:46
Sr No	ID Name	Date	Host User/Department	Valid From/UpTo	
130606000001	DASFESF	06/06/2013	UMESH M TALANPU	06/06/2013 15:59	
			Accounts	06/06/2013 16:59	

Visitor Summary

Visitor Watchlist/Blacklist

Lists out the banned visitors along with their details as well as Photograph wherever available.

Find... 1 of 4 100%

Main Report

Organization-1

Page 1 of 4

Visitor Watchlist/Blacklist

Run by: System Admin Date:27/10/2021 15:56

Visitor Name : qr

Visitor Organization : org

Contact No : 11

Type : Watchlist

Visitor Name : mitesh

Visitor Organization : 1245

Contact No : 1245

Type : Watchlist

Visitor Name : WL

Visitor Organization : fdsfs

Contact No : 701

Type : Watchlist

Pre-Registered Visitors






Date

Generate Report

Lists out all the pre-registered visitors along with their details.

Pre-Registered Visitors

Back

   Find...   1 of 1 100%

Main Report

ORGANISATION 1.

Pre-Registered Visitors From 01/01/2014 To 20/06/2014

Run by: System Admin Date: 20/06/2014 16:15

Sr No	Name/Organization	Host User/Department	Date/Purpose	Status	Remark
1	Rajesh Rawal BERJEN SYSTEM	ANIL MODI Department-1	15/02/2014 17:00	Approved	
2	Kareena Embee Corporaion	SMITA BARIA HR & ADMIN	22/04/2014 10:00 Knowledge transfer	Approved	
3	Prashant SBI	RONAK SHAH SDG - Telecom	23/04/2014 09:30 Cheque book delivery	Approved	
4	Sajid Automation Pvt.Ltd	RONAK SHAH SDG - Telecom	24/04/2014 11:00 Customer Requirement	Approved	
5	Sumit CDAC	SMITA BARIA HR & ADMIN	24/04/2014 13:00 Computer training	Approved	

Visitor History

This report generates a listing of all the visitors during the specified time period along with the visit details.

Select the "To-From Date" range from the date field.

Configure the **Optional Parameter** and **User Selection** as shown below:

Optional Parameter:

Select the **Group By** and **Select Station** as per your requirement.

Visitor History

Date: 19/03/2020

Optional Parameters

Group By: Organization

Select Station: Selected

Group Needed In Report: ☒

Search: []

ID	Name
2	Priyanka_location

User Selection

Generate Report

Enabling the check-box “**Group Needed In Report**” will display the name for that particular group in the generated report.

Visitor History

Organization-1 Visitor History From 27/12/2021 To 03/02/2022

Page 1 of 1

Run by:	Pass No	System Admin	Visitor Name	Visitor Profile	Organization	Contact No.	Host User	Pass IN Date-Time	Pass OUT Date-Time	Check IN Date-Time	Check OUT Date-Time	Date	Surrender By
Organization :					Organization-1								
Default Location													
220201000001	NEW4	Visitor5/Visitor5			1515	D1-Dummy1		31/01/2022 17:47	31/01/2022 18:46	31/01/2022 17:48	01/02/2022 13:56	01/02/2022 13:56	Visitor
220201000001	NEW4	Visitor5/Visitor5			1515	D1-Dummy1		01/02/2022 18:57	01/02/2022 14:57	01/02/2022 18:57	01/02/2022 14:04	01/02/2022 14:04	Visitor
220201000008	CK15	Visitor1/Visitor1			999	D1-Dummy1		01/02/2022 15:05	01/02/2022 16:03	01/02/2022 15:04	01/02/2022 15:05	01/02/2022 15:05	Visitor
220201000009	CK15	Visitor1/Visitor1			999	D1-Dummy1		01/02/2022 15:07	01/02/2022 16:05	01/02/2022 15:06	01/02/2022 15:08	01/02/2022 15:08	Visitor
220201000011	NEW4	Visitor2/Visitor2			1515	U1-User1		01/02/2022 15:14	01/02/2022 16:14	01/02/2022 15:15	01/02/2022 15:17	01/02/2022 15:17	Visitor
Organization :					ORG4								
Default Location													
220201000004	V1	Visitor3/Visitor3			9797	D4-Dummy4		01/02/2022 14:30	01/02/2022 15:26	01/02/2022 14:27	01/02/2022 14:30	01/02/2022 14:30	Visitor
220201000005	V1	Visitor2/Visitor2			9797	D4-Dummy4		01/02/2022 14:32	01/02/2022 15:30	01/02/2022 14:31	01/02/2022 14:33	01/02/2022 14:33	Visitor
220201000007	V1	Visitor1/Visitor1			9797	D4-Dummy4		01/02/2022 14:43	01/02/2022 15:40	01/02/2022 14:41	01/02/2022 14:42	01/02/2022 14:42	Visitor
Organization :					ORG3								
Default Location													
220201000002	NEW4	Visitor2/Visitor2			1515	D3-Dummy3		01/02/2022 14:05	01/02/2022 15:03	01/02/2022 14:05	01/02/2022 14:09	01/02/2022 14:09	Visitor
220201000003	NEW4	Visitor2/Visitor2			1515	D3-Dummy3		01/02/2022 14:05	01/02/2022 15:03	01/02/2022 14:11	01/02/2022 14:11	01/02/2022 14:11	Visitor
Organization :					ORG6								
Default Location													
220201000006	V1	Visitor5/Visitor5			9797	D6-Dummy		01/02/2022 14:33	01/02/2022 15:33	01/02/2022 14:34	01/02/2022 14:39	01/02/2022 14:39	Visitor

User Selection:

Select User Wise, Group Wise or All from the drop down list.

Visitor History

Date: 19/03/2020 19/03/2020

Optional Parameters

User Selection

Select Users: User Wise

User: ID Name

Generate Report For: All Users

Generate Report

Select **User** as per your requirement and Also select the options for “**Generate Report For**”.

Picklist For All Users

Total Selected : 2 Records

Search

Show Selected

<input type="checkbox"/>	User ID	Name
<input checked="" type="checkbox"/>	001A	priyanka thakur
<input type="checkbox"/>	001BRCode	d
<input checked="" type="checkbox"/>	002A	noshift
<input type="checkbox"/>	002BRCode	rt
<input type="checkbox"/>	002CC	regression
<input type="checkbox"/>	003A	fb
<input type="checkbox"/>	003CC	DONOTDELETE-KHUSHBU
<input type="checkbox"/>	004A	ot
<input type="checkbox"/>	005A	admin
<input type="checkbox"/>	006A	Shalee

1 - 10 of 383 records

OK Cancel

User Selection

Select Users: User Wise

User: ID Name

Search

User ID	Name
001A	priyanka thakur
002A	noshift

Generate Report For: All Users

Generate Report

Visitor Head Count

This report generates a department wise listing of the visitor head count for the specified time period.

Visitor Head Count			
←			
Back			
Find... 1 of 1 100%			
Main Report			
ORGANISATION 1. Page 1 of 1			
Visitor Head Count from 03/01/2012 to 03/01/2014 Run by: System Admin Date: 03/01/2014 16:44			
Sr No	Department ID	Department Name	No of Visitors
1	3	Marketing	1
2	5	Accounts	2
3	8	Assembly	1
4	13	Repairing	2
5	15	HR & ADMIN	1

Visitor Evacuation

Generates a list of people who are present and missing in/from a secured zone at the time of emergency. The site can be selected from optional parameters. The visitors can be filtered from Active and Inactive visitors.

Visitor Evacuation						
←						
Back						
Find... 1 of 1 100%						
Main Report						
Matrix Comsec Pvt. Ltd. Page 1 of 1						
Visitor Evacuation From 01/01/2016 00:00 To 06/15/2016 18:15 Run by: System Admin Date: 06/15/2016 18:16						
Site ID	Name	IN Count	OUT Count	Who Is IN	Assembly Count	Missing Count
1	Site-1	1	0	1	0	1
Total		1	0	1	0	1

Contract Worker Management

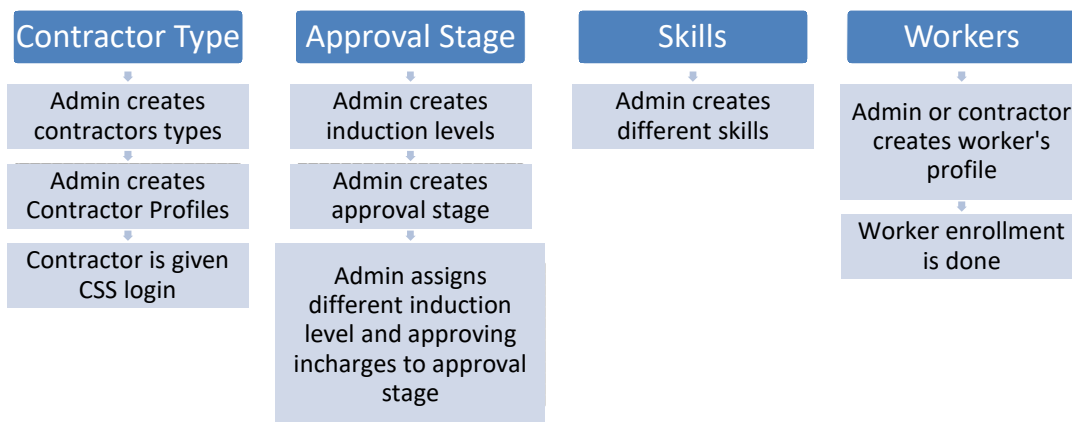
Contract Worker Management (CWM) System is the system which can be used by big and small industries to meet their demand of skilled manpower supply and hence monitoring the contract workers.

CWM comprises of readily available computer hardware, card readers, biometric fingerprint/palm readers, webcams and the software. A typical installation consist of a server where database of all contract workers is maintained.



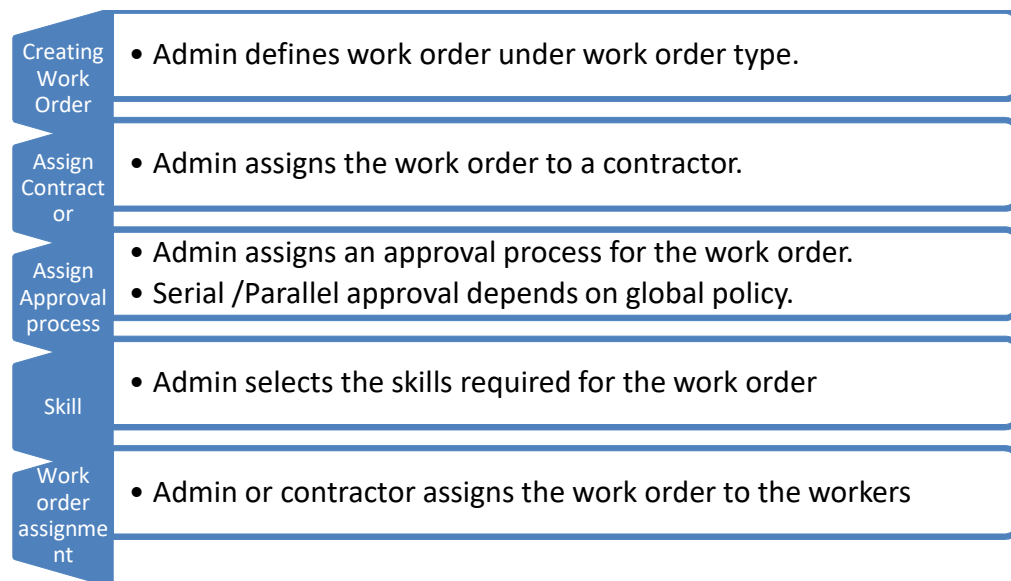
*This functionality will be available only with the COSEC **CWM** license.*

The contract worker management configuration is explained in the following diagram. To start with CWM, the contractor type, approval stages and skills are configured through CWM module. Then workers can be added through CWM or CSS.



Work Order creation & Worker assignment

After the contractor and workers are added in the system, the work order is created and assigned to the workers as mentioned below.



Features

1. Approvals and Training through Induction Levels
2. Enrollment of the contract workers based on
 - RFID Cards
 - Biometric Fingerprints
 - Palm Vein Templates
3. Planning and Scheduling for future Work Orders
4. Location wise Entry/Exit Access Control
5. Maintaining Attendance Records of Workers
6. Detailed Reports

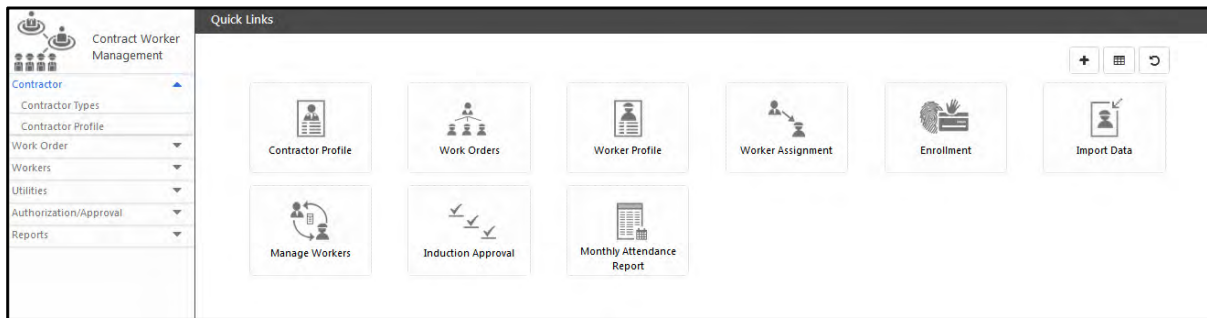
Benefits of CWM

1. The probability of payroll inflation by falsifying the records of workers deployed gets totally eliminated.
2. The company gets reports on the time spent by each worker to enable accurate calculating of billing for various contractors.
3. It will ensure that the blacklisted workers do not get entry into the work area, even under different identity or through another contractor.
4. The company can get warnings when a worker is nearing maximum number of days' attendance after which he will become eligible to various benefits which regular employees are entitled to.
5. Workers can be scheduled more accurately, thus minimizing the possibility of excess worker hiring.
6. The company can ensure that workers of the desired skill only get deployed.




To use this functionality, Click on the **Contract Worker Management** module. The Contract Worker Management page will appear on your screen.

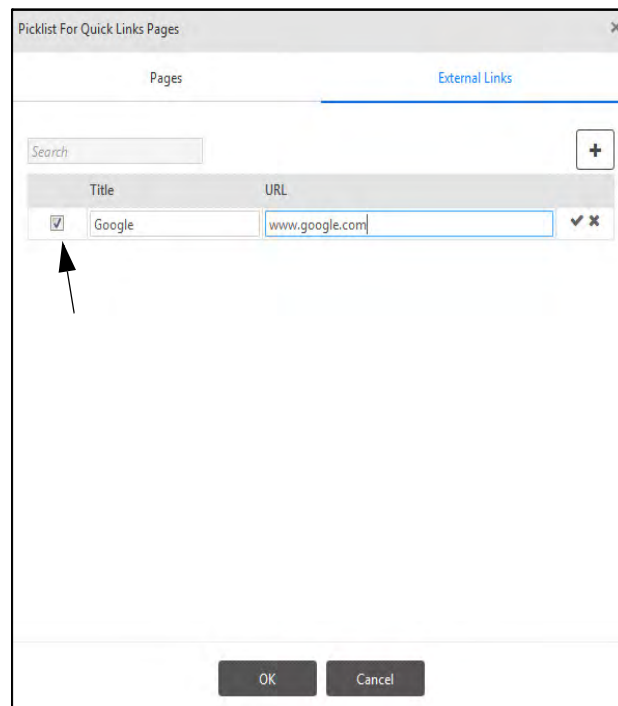



module. The Contract Worker

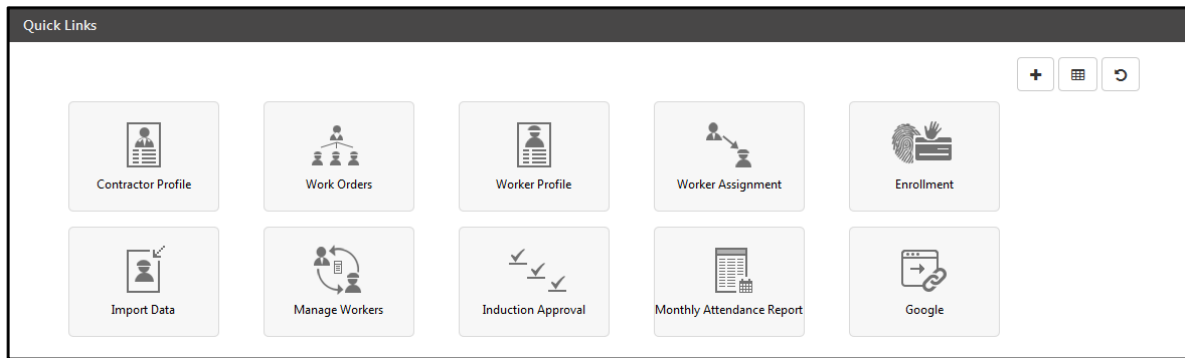




The page displays a menu and **Quick Links** to go to the required page in just one click. Quick Links are shortcuts to reach to a specific page easily. It also contains following three buttons:

- **Add Quick Link:** Click  button to add a quick link. A picklist for Quick Link pages appears for selecting the page or External Link for which the quick link is to be created. Maximum **20** quick links can be added.
- For Adding **Pages** in Quick Link, Select the Pages and click on OK
- For Adding **External Links**, Select External Link tab, click on  button to add new external link.
- Configure the **Title** and **URL** of the external link under the respective fields. click on checkbox to get the configured link on quick link screen as shown below. To save the configuration click on .



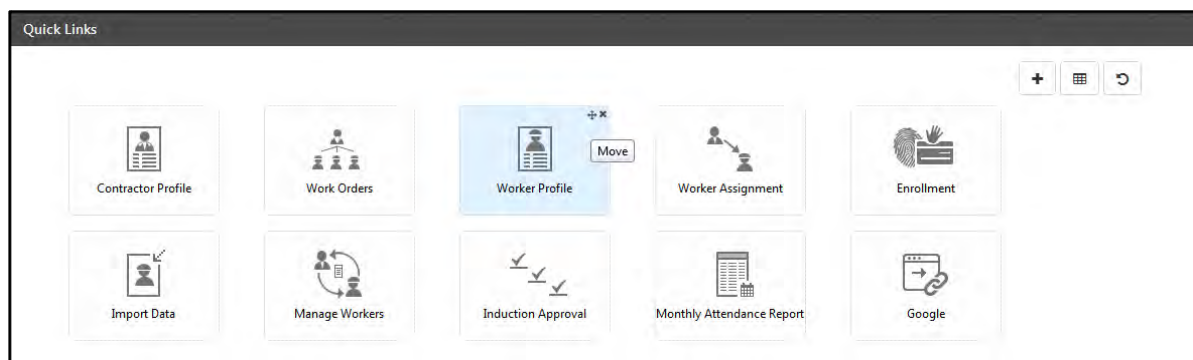
- To edit the saved configuration, click on .
- Click on OK to save the link configuration on Quick Link screen. The external link will be displayed as shown below:



- **Select Layout:** Click  button to select a layout for the quick links. You can select 5x4 or 4x5 layout to manage the quick links.
- **Reset Quick Links:** Click  button to reset the quick links to the default quick links.

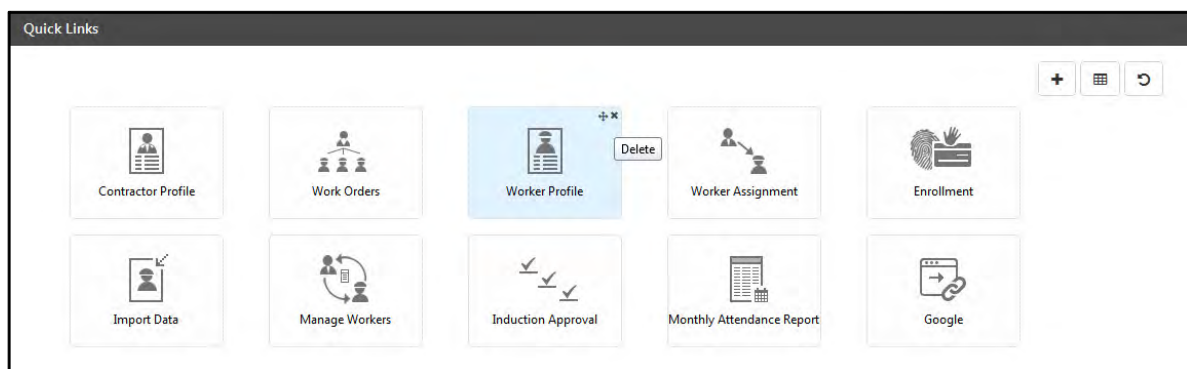
Move the Link

To move the link from one place to another, hover on the link on top right corner and click on “Move” icon as shown below. Then drag the quick link to the desired place. It will be placed at the desired location on the quick links page.




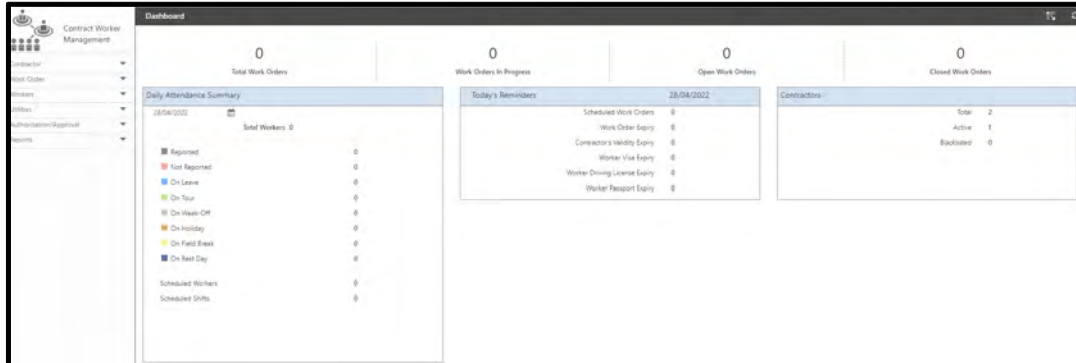
Delete the Link

To delete a particular link, hover on the link on top right corner and click on “Delete” icon as shown below.



Contract Worker Management Dashboard

To view the **Contract Worker Management** Dashboard, select the Dashboard button  on the **CWM** page. The Dashboard displays the basic information set and configured in CWM module under the following groups:



The Dashboard displays basic information related to work orders, contractors and workers:

- Total Work Orders- Total work orders created in COSEC.
- Work Orders In-Progress - Sum of all In Progress work orders.
- Open Work Orders- Sum of all work orders that haven't started yet.
- Closed Work Orders - Sum of all work orders that are already over.

Daily Attendance Summary



This section is displayed only if TAM license is available.

- Reported- Total number of workers who have shifts scheduled today and have at least one punch on current day.
- Not Reported- Total of all unreported workers who have no punch for current day, though their shift is scheduled and are not on WO, PH or leave.
- On Leave - Total number of workers on leave on current day.
- On Tour - Total number of workers on tour on current day.
- On Week-Off- Total number of workers on week-off on current day.
- On Holiday- Total number of workers on holiday on current day.
- On Field Break - Total number of workers on Field on current day.
- On Rest Day - Total number of workers on rest day on current day.
- Scheduled Workers - Total number of workers who are scheduled to start work on current day.
- Scheduled Shifts - Total number of workers' shifts that are scheduled to start on current day.


Today's Reminders

- Scheduled Work Orders - Total of all such active work orders starting on current day.
- Work Order Expiry- Total of all such active work orders whose validity is expiring on current day.
- Contractor's Validity Expiry- Total of all such active contractors whose validity is expiring on current day.
- Worker Visa Expiry- Total of all such active workers whose visa validity is expiring on current day.
- Worker's Driving License Expiry- Total of all such active workers whose driving license is expiring on current day.
- Worker's Passport Expiry- Total of all such active workers whose passport is expiring on current day.

Contractors

- Total - Total contractors created in contractor master.
- Active - Contractor having: Current Date < = Validity Date.
- Blacklisted- Total contractors marked as Blacklisted by the administrator.

Workers


- Total - Sum of all Active and Inactive workers. Click on  button. The Import Data page opens from where data can be imported in XLS and CSV format.

Active

- Approved - All Active Workers, having assignment Status as Approved.
- Pending- All Active Workers, having assignment Status as Pending.
- Rejected- All Active Workers, having assignment Status as Rejected.
- Free- All Active Workers, having assignment Status as Free.
- Blacklisted- All Active Workers, having assignment Status as Blacklisted.

Inactive

- Free- All Inactive Workers, having assignment Status as Free.
- Blacklisted- All Inactive Workers, having assignment Status as Blacklisted.

For more information on the above Dashboard options, click the respective information links on the Dashboard. The Latest values on Dashboard are updated on clicking the Refresh  button.

Contractor Types

For execution of a big project, different types of contractors like civil contractor, mechanical contractor, IT contractor etc are required.

To create the type of contractors go to **Contract Worker Management > Contractor > Contractor Types**

The screenshot shows the 'Contractor Types' form. On the left, there is a 'Contractor Types' label with a red asterisk, followed by an 'ID' input field containing the value '1' and a 'Name' input field containing 'Contractor Type-1'. Below these fields is a 'Default' checkbox which is currently unchecked. On the right, there is a table with two columns: 'ID' and 'Name'. The table contains one row with the ID '1' and the Name 'Contractor Type-1'.

ID	Name
1	Contractor Type-1

Click on **Add** button to add a contractor type.

Specify the **Name** of the contractor type.

Click on **Save**. The ID of contractor type is auto-generated and all the contractor types will be listed in the right grid.

Check the box to make the contractor type as **default**. There is always one default contractor type which cannot be deleted. Also any contractor type can be made as default.

The screenshot shows the 'Contractor Types' form after adding a second entry. The 'Contractor Types' label is followed by an 'ID' input field containing '2' and a 'Name' input field containing 'Civil Contractor'. The 'Default' checkbox remains unchecked. The table on the right now has two rows: the first row has ID '1' and Name 'Contractor Type-1', and the second row has ID '2' and Name 'Civil Contractor'.

ID	Name
1	Contractor Type-1
2	Civil Contractor

Contractor Profile

Contractor Profile is the detailed profile of the contractors belonging to one of the contractor type.

For example: TCE, HPCL, Hiranandani, Alps Engineers etc are configured as Contractor Profiles under the Civil Contractor.

To create the contractor profile go to **Contract Worker Management > Contractor > Contractor Profile**

The screenshot shows the 'Contractor Profile' form. It has a header bar with a search icon and a close button. Below the header, there are four input fields: 'ID' with value 'C01', 'Name' with value 'HPCL', 'Type' with a dropdown menu showing 'Contractor Type-1' and 'Civil Contractor' (selected), and 'Validity End Date' with a calendar icon. To the right of these fields is a table with columns 'ID', 'Name', 'Type', and 'Validity End'. The table is currently empty, showing 'No Data'. Below the input fields are five expandable sections: 'Address', 'Contact Information', 'Details', 'License Information', and 'Account Information', each with a downward arrow icon.

Click on **Add** button to add a contractor profile.

Specify the **ID** of the contractor profile. This ID would be the CSS login ID and should be different from employee's ID and worker's ID.

Specify the **Name** of the contractor profile. For eg: HPCL is a contractor profile.

Select the **Type** from the drop down list of contractor types. For Eg: HPCL is a profile of civil contractor type.

Select the **Validity End Date** from the calendar button which is the end date for the contractor validity.

This screenshot shows the 'Contractor Profile' form with the following values filled in: 'ID' is 'C01', 'Name' is 'HPCL', 'Type' is 'Civil Contractor' (selected from the dropdown), and 'Validity End Date' is '31/05/2017'. The calendar icon next to the date field is visible.

Specify the **Address**, **Contact Information**, **Details**, **License Information** and **Account Information** by clicking the respective tabs.

Address:

Address	
Address	421 GIDC, Makarpura
Street	Vadar Road
City	Vadodara
Pincode	390011
State	Gujarat
Country	India
Phone	0265 2631666

Contact Information:

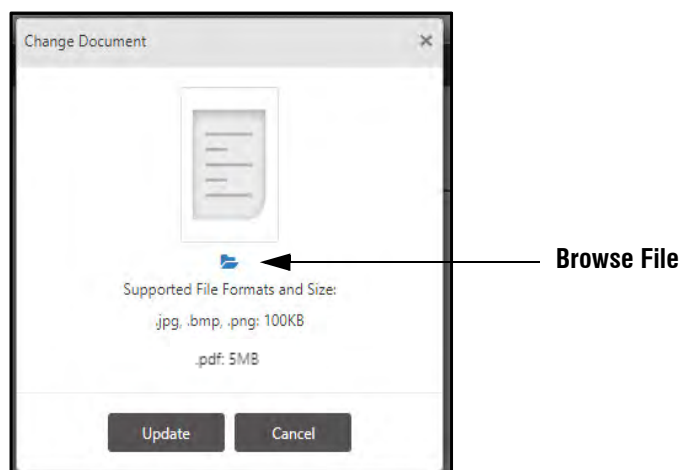
Contact Information	
Contact Person 1	Parth Thakar
Mobile	9685623486
Email	parththakar@gmail.com
Contact Person 2	Sanjay Mistry
Mobile	8912352562
Email	sanjaymistry1@gmail.com

Details:

Details		
Service Tax No.		↑
PAN	30 Chars	↑
PF No.	30 Chars	↑
ESI No.		↑

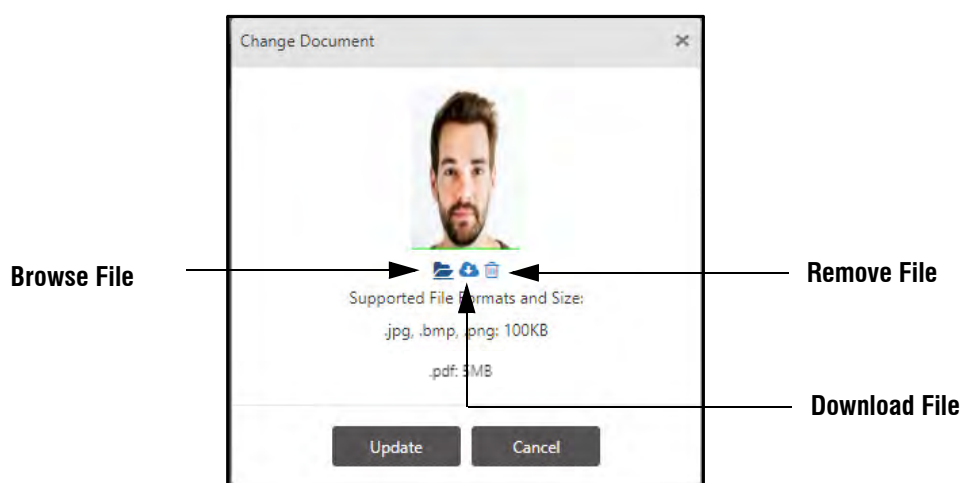
There are 10 additional fields in which you can enter the desired details of the Contractor as per your requirement. These are visible only after they are configured from **Admin > System Configuration > Global Policy > CWM**. For details refer [“Custom Fields For Contractors”](#). For example Security Number, ID Proof, Nominee Name, etc.

You can upload certain documents by clicking **Upload**  button. Then **Change Document** pop-up appears as shown below.





Click **Browse File**  .


To upload, select the desired file as per the supported formats and size (.jpg, .bmp, .png, pdf) from your local PC.




After uploading the file, if you wish to upload a different file instead of the current uploaded file, click **Browse File**

 again and select the desired file from your local PC. The previously uploaded file will get replaced with the new file.

To download the uploaded file, click **Download File**  .

To remove the uploaded file, click **Remove File**  .

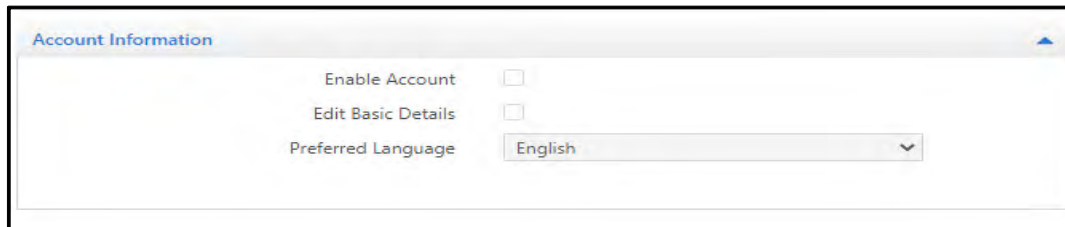
Then click **Update**.

The document will be uploaded and can be previewed by clicking on **Preview**  button.

License Information:

A screenshot of a web form titled "License Information". It contains two input fields: "License No. *" and "Description". To the right of the "License No." field is an upload icon. The form has a light blue header bar with the title and a small blue triangle icon on the right.

Account Information:

A screenshot of a web form titled "Account Information". It contains three fields: "Enable Account" with a checkbox, "Edit Basic Details" with a checkbox, and "Preferred Language" with a dropdown menu showing "English". The form has a light blue header bar with the title and a small blue triangle icon on the right.

The **Contractor Self Service (CSS)** account of the contractor can be enabled from the Account information tab by checking the **Enable Account** check box as shown above.

- The contractor can edit the basic details if **Edit basic details** check box is enabled.
- The preferred language can be selected from the drop down options.

Click on **Save** button to save the profile details.

After these details are entered, work order can be assigned to the contractor.

Multiple work orders can be assigned to a single contractor but each worker must be associated with one and only one Contractor.

A Contractor has assignment rights for only those Work Orders that are assigned to him, and those workers that are associated with him.

Induction Levels

Once assigned to a work order, a worker needs to go through levels of approval that may comprise background check, orientation, skill-based training, safety training etc. before the organization considers the worker fit for the work. These levels are defined in COSEC as *Induction Levels*. The HR administrator can create upto 7 induction levels for workers in COSEC.

Configuring the approval process for a worker involves the following:

- Defining Induction Levels
- Assigning Induction Levels to an Approval Stage
- Assigning Approving In-Charges to each Induction Level in an Approval Stage

To define a new Induction Level, go to: **Contract Worker Management > Work Order > Induction Levels**

The screenshot shows the 'Induction Level' form. The 'ID' field is set to 1, and the 'Name' field is 'Induction Level-1'. The 'Description' field contains 'IT Induction'. The 'Default' checkbox is unchecked. A search bar is visible at the top right.

Induction Level-1 is a system-defined default Induction Level. Click **New** to add a new level.

Enter a suitable **name** for the level (e.g. Medical Checkup, Safety Training etc.)

Enable the **Default** checkbox to make this the default induction level.

Enter a description for the level.

Click **Save** button to save the induction level.

New Induction Levels will appear in the grid list as shown:

The screenshot shows the 'Induction Level' form with ID 4, Name 'Induction Level-4', and Description 'Medical Checkup'. The 'Default' checkbox is unchecked. The grid list on the right shows four levels: Induction Level-1, Induction Level-2, Induction Level-3, and Induction Level-4.

ID	Name
1	Induction Level-1
2	Induction Level-2
3	Induction Level-3
4	Induction Level-4

Approval Stages

An Approval Stage is a sequence of Induction Levels that a worker must complete before finally being approved for a work order. Each Induction Level can be assigned an *Approving In-Charge* who shall be responsible for approving or rejecting a worker once the level is completed.

An *Approval Stage*, in turn, can be assigned to a *Work Order* and becomes subsequently applicable to all workers associated with this work order.

To create a new Approval Stage, go to: **Contract Worker Management > Work Order > Approval Stages**

ID	Name	Assigned Induction Levels
1	Approval Stage-1	1

Click **New**.

Enter an appropriate name for the Approval Stage.

Select the **Induction Level Assignment** section. This section allows you to select upto 7 Induction Levels for this Approval Stage in the required sequence using the respective pick-lists.

For each level, select an **Approving In-Charge** using the respective user picklist.

Click **Save**. The new Approval Stage appears in the grid list as shown.

The screenshot shows a web application window titled 'Approval Stages'. At the top, a green banner indicates 'Saved Successfully'. Below the banner, there's a search bar and a table with columns 'ID', 'Name', and 'Assigned Induction Levels'. The table contains two rows: 'Approval Stage-1' with ID 1 and 'Approval Stage-Technical' with ID 4. To the left of the table is a form for 'Induction Level Assignment' with fields for 'Level' and 'Approving In-Charge' for levels 1 through 7. The 'Approving In-Charge' field for Level 1 is populated with 'Isha', and for Level 2 with 'Chirag'. Other levels have empty fields or placeholder text like 'ID' and 'Name'.

A worker can successfully complete an Approval Stage only when he gets approved by all the designated Approving In-Charges. The worker approval request will get rejected if the worker gets rejected at any level of the approval stage.



If no Approving In-Charge is assigned for a particular Induction Level, then the approval request for this level will be sent directly to the system administrator.

Worker Approval Process

An Approval Request is generated in the following instances:

- When a Contractor creates a new Worker from CSS
- When a Contractor assigns Work Order to an existing Worker from CSS

Approval Requests generated by the admin are pre-approved. Approval Requests generated by a Contractor (from the *Contractor Self Service* account) are sent to the concerned approving in-charges depending on the type of approval policy defined in the COSEC Global Policy.

Based on the Global Policy, Worker Approval can be of two types as illustrated below:

- Direct Approval
- Approval Stage

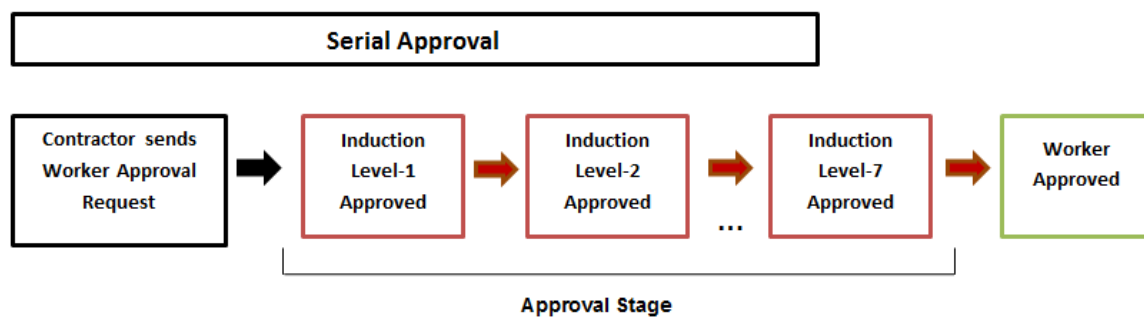
Direct Approval: In this type of approval, a worker approval request from CSS is sent directly to the system administrator, ignoring any Approval Stage that may be assigned to the Work Order.



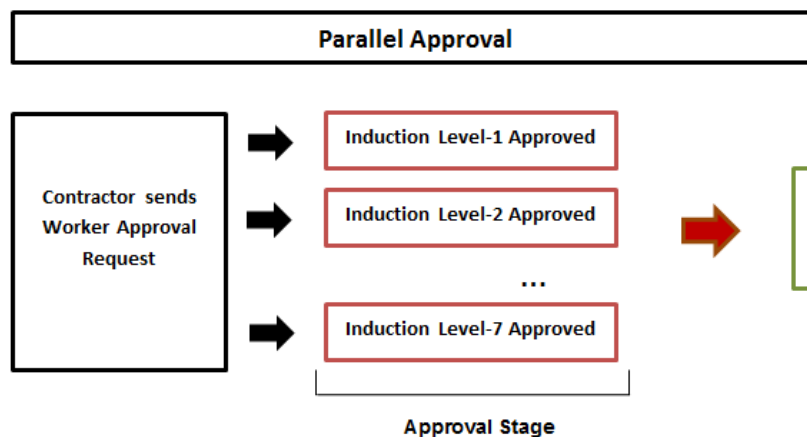
Approval Stage: In this type of approval, a worker approval request from CSS is sent to Approving In-Charges as per the *Approval Scheme* selected in Global Policy. There can be two types of Approval Scheme:

- Serial
- Parallel

In case of *Serial Approvals*, a worker must be approved serially by the designated Approving In-Charges, in the defined sequence of an Approval Stage.



In case of *Parallel Approvals*, worker approval requests are sent to all the Approving In-Charges at the same time and approvals may be performed in any sequence.

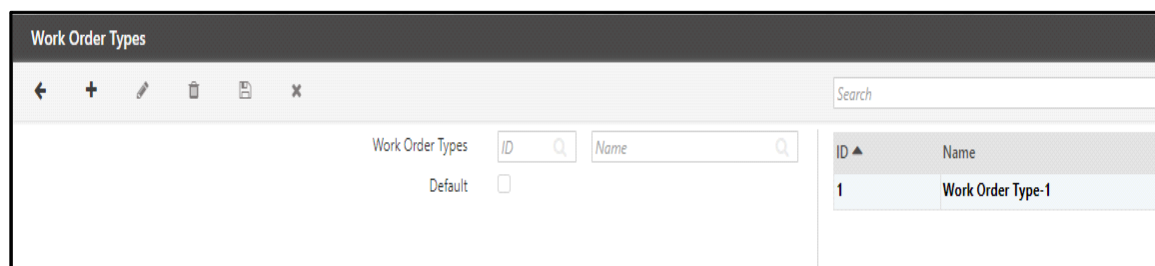


For more information on setting an approval type for the **Contract Worker Management** module, refer to Global Policy.

Work Order Types

Work Orders of similar nature can be classified or grouped together as a **Work Order Type**. For e.g. Work Orders for mending broken machinery or repairing a pump can be grouped as “Repair”, while a Work Order for fitting a light bulb may be assigned the type “Installation”.

To define a Work Order Type, go to **Contract Worker Management > Work Order > Work Order Types**



The screenshot shows the 'Work Order Types' form. It has a toolbar with icons for back, add, edit, delete, and search. Below the toolbar, there are input fields for 'Work Order Types' (ID and Name) and a 'Default' checkbox. The 'ID' field contains '1' and the 'Name' field contains 'Work Order Type-1'. The 'Default' checkbox is unchecked. A table on the right shows the current entry.

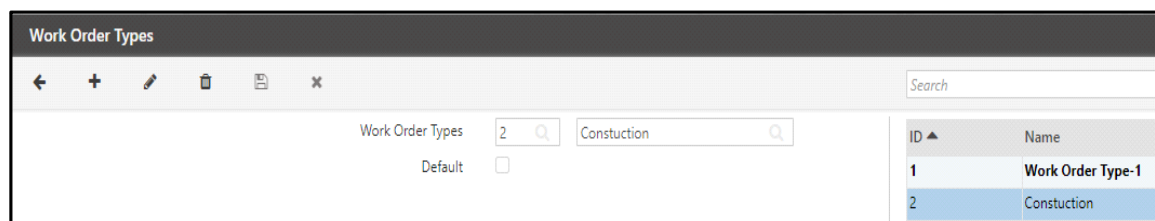
ID	Name
1	Work Order Type-1

Click the **New** button to add a work order type.

Enter the **name** for the Work Order Type. The ID will be generated automatically.

Select the **Default** checkbox to make this Work Order Type as default.

Click the **Save** button.



The screenshot shows the 'Work Order Types' form after adding a second entry. The 'ID' field contains '2' and the 'Name' field contains 'Constuction'. The 'Default' checkbox is unchecked. The table on the right now shows two entries.

ID	Name
1	Work Order Type-1
2	Constuction

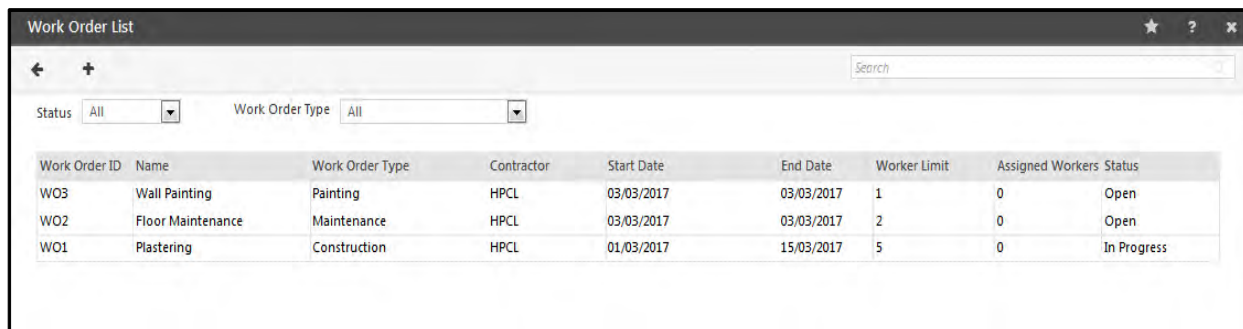


Once the Work Order type is created, you can create the work orders to be assigned to contractors by selecting the “type” created in Work Order type.

Work Order List

This page shows a list of all the created Work Orders. The list can be viewed based on the filters. The work orders can be searched by entering the key word in the Search box.

To view a Work Order List, go to **Contract Worker Management > Work Order > Work Order List**



Work Order ID	Name	Work Order Type	Contractor	Start Date	End Date	Worker Limit	Assigned Workers	Status
WO3	Wall Painting	Painting	HPCL	03/03/2017	03/03/2017	1	0	Open
WO2	Floor Maintenance	Maintenance	HPCL	03/03/2017	03/03/2017	2	0	Open
WO1	Plastering	Construction	HPCL	01/03/2017	15/03/2017	5	0	In Progress

Use the following Status filters to view all or specific Work Orders:

- All
- Open
- In Progress
- Closed

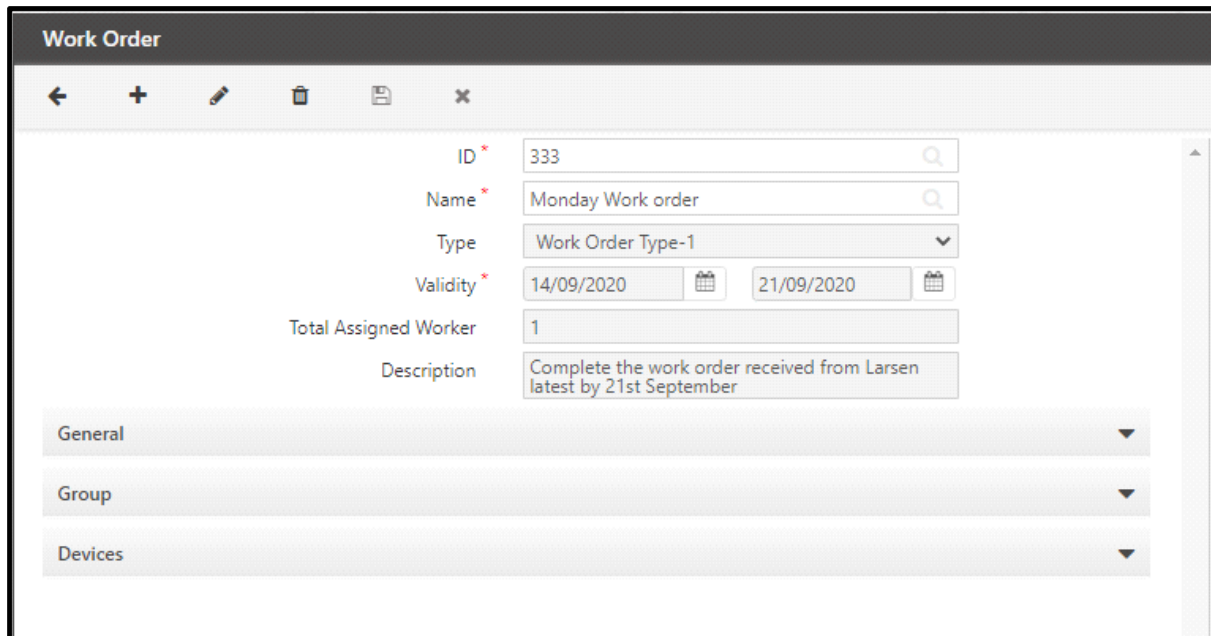
Select any work order in the list to go to the corresponding **Work Order** page.

Also you can create the work orders from this page by clicking on **New** button.

Work Order

Work Order is a work contract assigned to a Contractor to carry out a specific task within a stipulated time and cost. Hence a work order is always associated with a Contractor, who is responsible for completing the same by deploying suitable work force.

To create a new Work Order, go to: **Contract Worker Management > Work Order > Work Orders**



The screenshot shows the 'Work Order' form with the following fields and values:

Field	Value
ID *	333
Name *	Monday Work order
Type	Work Order Type-1
Validity *	14/09/2020 to 21/09/2020
Total Assigned Worker	1
Description	Complete the work order received from Larsen latest by 21st September

Below the form, there are three expandable sections: General, Group, and Devices.

Click **New** button.

Enter the Work Order **ID** and **Name**. Select a Work Order **Type** from the drop down list.



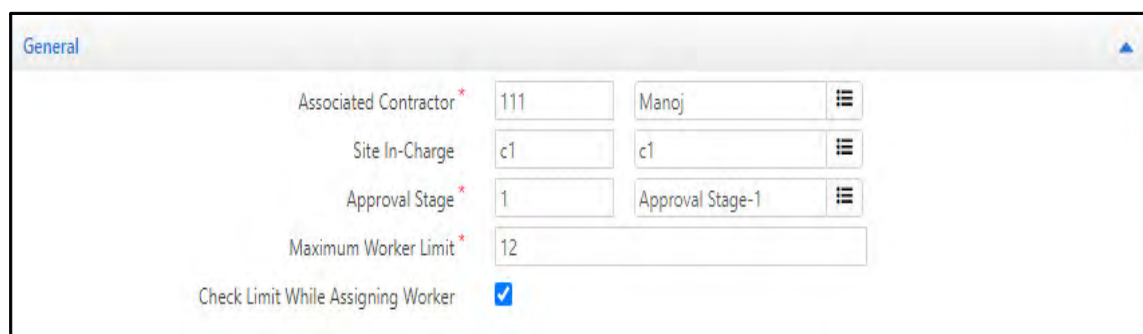
The drop down list shows the Work order types created in Work Order Type section.

Select a Start and End date as the **Validity** period of the Work Order.

Enter a **Description** of the Work Order, if required.

Select the **General** section to assign a *Contractor*, a *Site In-Charge* (Any ESS user), and an *Approval Stage* ([See "Approval Stages" on page 1995.](#)) to the Work Order.

Enter the maximum number of workers allowed for this Work Order (**Maximum Worker Limit**).



The screenshot shows the 'General' section of the Work Order form with the following fields and values:

Field	Value
Associated Contractor *	111 Manoj
Site In-Charge	c1 c1
Approval Stage *	1 Approval Stage-1
Maximum Worker Limit *	12
Check Limit While Assigning Worker	<input checked="" type="checkbox"/>

Check Limit While Assigning Worker: Enable the checkbox if maximum work order's limit & skill-wise limit for adding a worker needs to be checked.

When this checkbox is enabled, then while assigning the work order to a worker/workers, system will check the maximum worker limit provided for that particular work order.

If the no. of workers to whom particular work order is assigned in *CSS> Worker> Worker Profile* exceeds the maximum worker limit then the system will show error.

If disabled, then a contractor can assign a particular work order to more workers irrespective of the maximum worker limit provided.

Example:

Work Order: Labeling work

Max Worker Limit: 12

Check Limit While Assigning Worker: Enabled

Now while assigning the work order, if 13 workers are assigned for this work order, then an error message will be displayed saying "Maximum Worker Limit exceeded" if Check Limit While Assigning Worker is enabled.

Skill-Wise Worker Limit

Click **Add** button. You can select the skill from the picklist and enter the worker limit for that particular skill. Then click OK to save skill wise worker limit.

Skill ID	Name	Worker Limit
3	Engineering Skills	3
2	Supervisor Skills	2

You can also assign **Enterprise groups** and **device groups** to the new Work Order. These will in turn, be assigned to all workers assigned to this Work Order.

Organization * 1 Organization-1

Branch * 1 Branch-1

Department * 1 Department-1

Devices

Devices

Assign

Device Group ID Name

Search

DGID ▲	Device Group Name	
1	Device Group	

Click **Save** to save the Work Order.

You can also extend 'Work Order validity' by selecting the new To and From Date, from the Worker Order section.

Work Order

ID * W1

Name * AR Implement

Type Work Order Type-1

Validity * 12/03/2020 22/03/2020

Total Assigned Worker 1

Description 250 chars

General

Group

Devices

Mar 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
01	02	03	04	05	06	07
08	09	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	01	02	03	04
05	06	07	08	09	10	11

Once clicked on Save, Work Assignment popup window will appear and you can select **"New From Date"** & **"New From Date"**.

Work Order

←

+

×

Save (Alt+S)

W1

Name *

AR Implement

Type

Work Order Type-1

Validity *

12/03/2020

24/03/2020

Total Assigned Worker

1

Description

250 chars

General

Group

Devices

Worker Assignment

Search

Update

☒

Worker ID ▲

Name

Previous From Date

Previous To Date

New From Date

New To Date

Assignment Status

☒

WK1

Dhruv

12/03/2020

22/03/2020

11/03/2020

23/03/2020

Approved

Save

Mar 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
01	02	03	04	05	06	07
08	09	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	01	02	03	04
05	06	07	08	09	10	11

Click **Save** to save the Work Order

Skills

The skills are useful in assigning workers to work order based on their skill and also in defining worker limit in work order for different skills.

To create the skills of workers go to **Contract Worker Management >Workers > Skills**

The screenshot shows the 'Skill' management interface. It features a toolbar with icons for back, add, edit, delete, save, and close. Below the toolbar, there is a form with a 'Skill *' label, an 'ID' input field containing 'Supervisory Skills', and a 'Default' checkbox. To the right of the form is a table listing existing skills.

ID	Name
1	Skill-1
2	Engineering Skills

Click on **New** button to add a skill.

Specify the **Name** of the skill.

Click on **Save**.The ID of skill is auto-generated and all the skills will be listed in the right grid.

The skills can be searched by ID or Name from the search box on top right of the page.

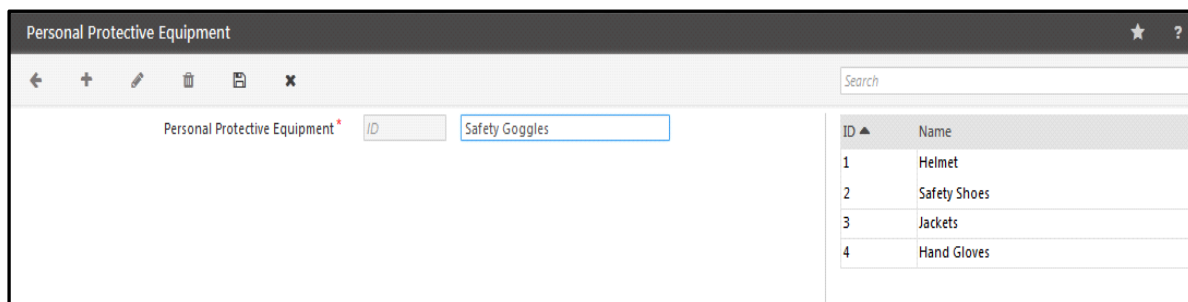
The screenshot shows the 'Skill' management interface after a new skill has been added. A green banner at the top indicates 'Saved Successfully'. The form now shows an 'ID' input field containing '3' and a 'Supervisory Skills' label. The table on the right now includes three skills.

ID	Name
1	Skill-1
2	Engineering Skills
3	Supervisory Skills

Personal Protective Equipment

Use this option to create a list of safety equipments that the organization issues to contract workers, for protection against hazards at work. Personal Protective Equipment (PPE) defined here can later be assigned to workers. This will help the administrator maintain records of the assigned equipments.

To define a new PPE, go to **Contract Worker Management > Workers > Personal Protective Equipment**

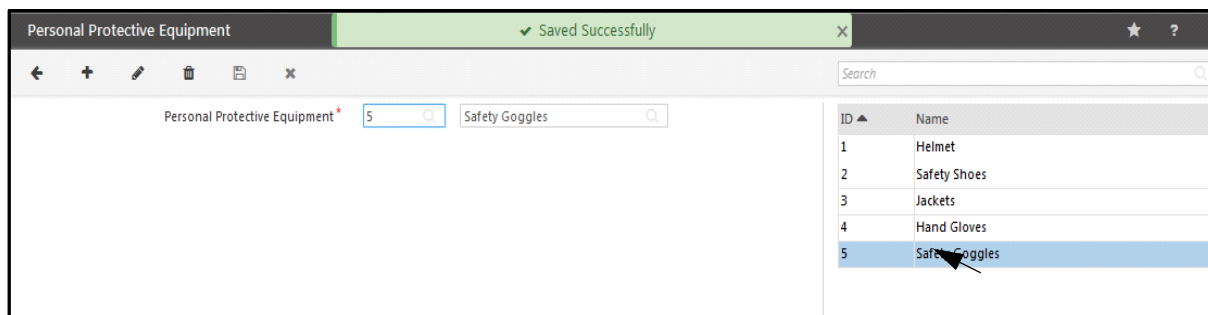


The screenshot shows the 'Personal Protective Equipment' form. On the left, there is a 'Personal Protective Equipment*' label, an 'ID' input field, and a 'Safety Goggles' input field. On the right, there is a table with the following data:

ID	Name
1	Helmet
2	Safety Shoes
3	Jackets
4	Hand Gloves

Click **New** button. Enter a **name** for the equipment (For e.g. Safety Shoes).

Click **Save**. The new equipment is successfully saved and appears on the grid list as shown.

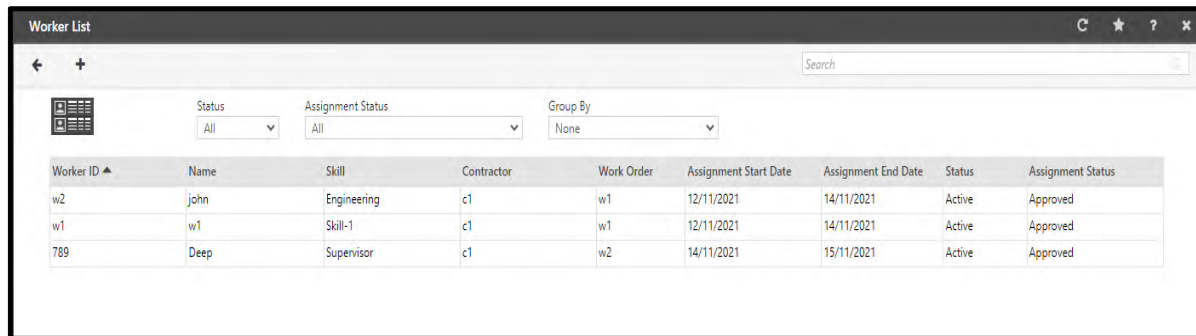


The screenshot shows the 'Personal Protective Equipment' form after saving. A green banner at the top says '✓ Saved Successfully'. The 'ID' input field now contains '5'. The 'Safety Goggles' input field is still present. The table on the right now includes the new equipment:

ID	Name
1	Helmet
2	Safety Shoes
3	Jackets
4	Hand Gloves
5	Safety Goggles

Worker List

To view the list of workers go to **Contract Worker Management > Workers > Worker List**.



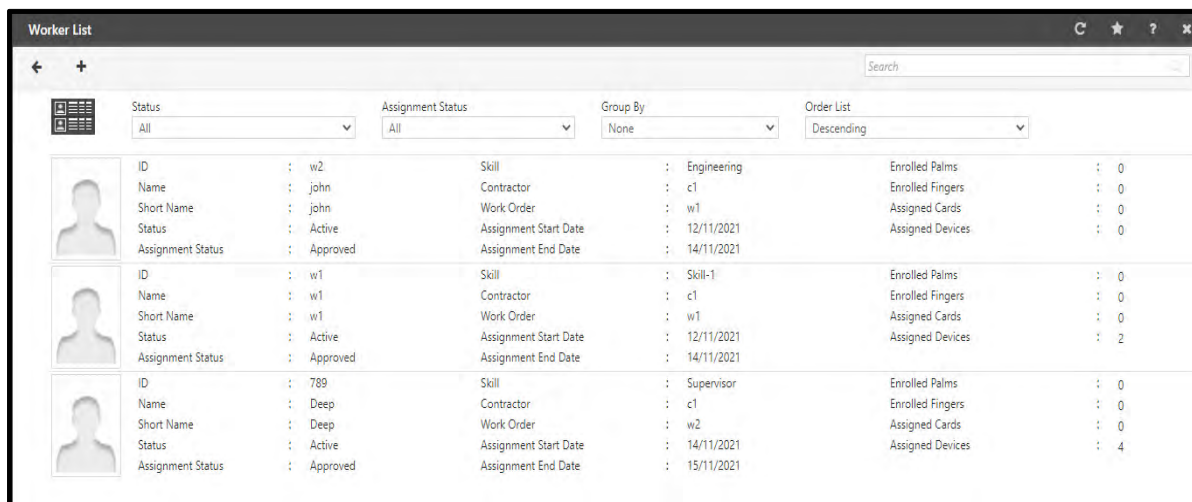
Worker ID	Name	Skill	Contractor	Work Order	Assignment Start Date	Assignment End Date	Status	Assignment Status
w2	John	Engineering	c1	w1	12/11/2021	14/11/2021	Active	Approved
w1	w1	Skill-1	c1	w1	12/11/2021	14/11/2021	Active	Approved
789	Deep	Supervisor	c1	w2	14/11/2021	15/11/2021	Active	Approved

The Worker List will display only those workers for which rights are assigned to the SA, that is as per the enterprise groups assigned to the workers.

For example, if for Worker1 in Groups, Organization is ORG1 and if the rights for ORG1 are not assigned to the SA, then through the SA login the Worker List will not display Worker1.

For details, refer to [“Assigning Group-Wise Rights”](#) under [“System Accounts”](#) as well as [“Group”](#) under [“Worker Profile- Group”](#).

The workers list can be viewed in **grid** and **photo** view. Click on  to view the workers in photo view.



ID	Name	Short Name	Status	Assignment Status	Skill	Contractor	Work Order	Assignment Start Date	Assignment End Date	Enrolled Palms	Enrolled Fingers	Assigned Cards	Assigned Devices
w2	John	John	Active	Approved	Engineering	c1	w1	12/11/2021	14/11/2021	0	0	0	0
w1	w1	w1	Active	Approved	Skill-1	c1	w1	12/11/2021	14/11/2021	0	0	0	2
789	Deep	Deep	Active	Approved	Supervisor	c1	w2	14/11/2021	15/11/2021	0	0	0	4

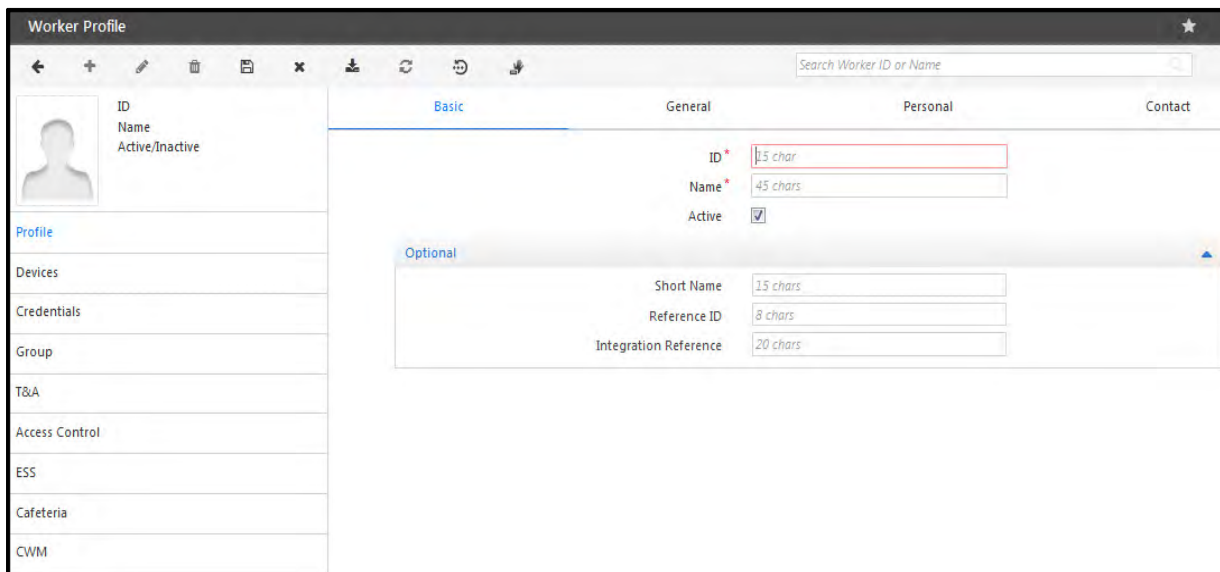
The list can be filtered on the basis of **Status**, **Assignment Status**, **Group By** and **Order List**.

- The Status options are All, Active and Inactive.
- The Assignment Status options are All, Pending, Approved, Rejected, Free and Blacklisted.
- The Group By filter is based on Work Order and Contractor.
- The Order List can be selected as Ascending or Descending.

The worker can be searched by either ID, Name, Skill, contractor or work order from the search box on top right of the page.

Click on the worker's entry in the grid. The respective worker's profile page appears.

Click on **Add** button. The Worker Profile page opens. The new worker can be added from this page.



Worker Profile

Search Worker ID or Name

ID
Name
Active/Inactive

Profile

Devices

Credentials

Group

T&A

Access Control

ESS

Cafeteria

CWM

Basic General Personal Contact

ID * 15 chars

Name * 45 chars

Active ☒

Optional

Short Name 15 chars

Reference ID 8 chars

Integration Reference 20 chars

To know about the addition of workers See [“Worker Profile”](#) on page 2008.

Worker Profile

Worker Profile enables to add new worker and edit/delete worker details. The worker details are displayed along with user details in the user configuration section of Users module.



The new worker can be added from CWM or CSS module only.

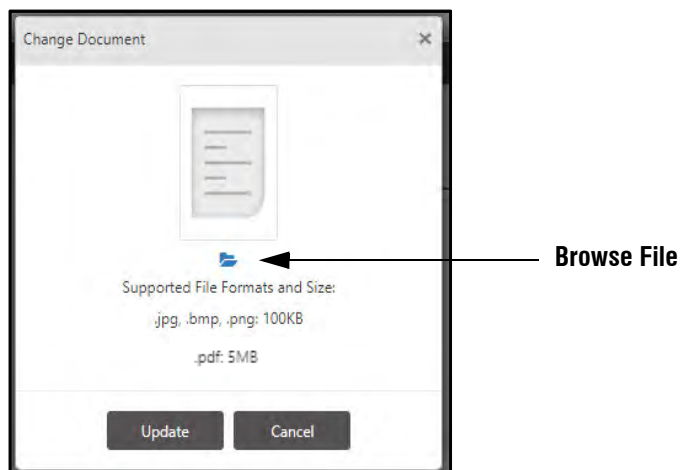
To add the worker select **Contract Worker Management > Workers > Worker Profile**.

Profile

Configure the Worker's **Basic**, **General**, **Personal** and contact details to create new worker. Click the **Add** button to add a new worker.

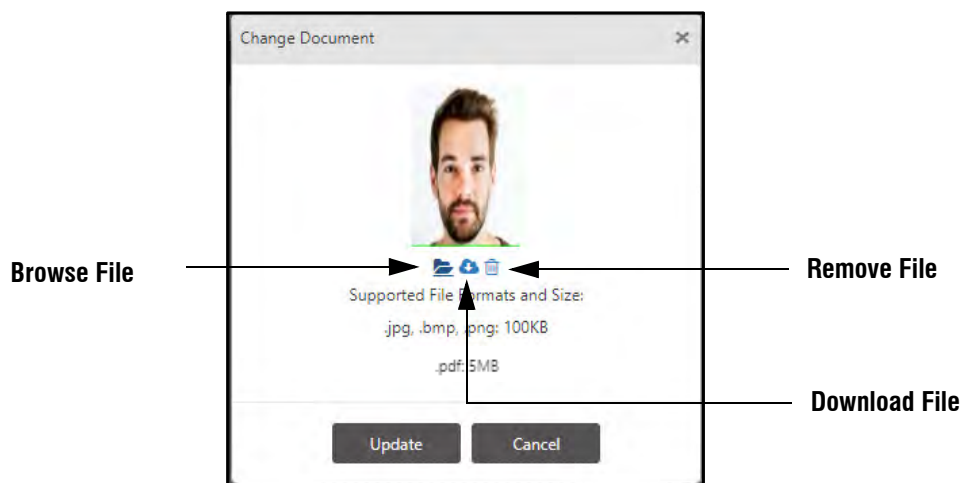
Under **General** tab, there are 10 additional fields in which you can enter the desired details of the workers as per your requirement. These are visible only after they are customized from **Admin > System Configuration > Global Policy > CWM**. For details refer "[Custom Fields For Contractors](#)". For example Security Number, ID Proof, Nominee Name.

You can upload the documents by clicking **Upload**  button. Then **Change Document** pop-up appears as shown below.





Click **Browse File**  .

To upload, select the desired file as per the supported formats and size (.jpg, .bmp, .png, pdf) from your local PC.




After uploading the file, if you wish to upload a different file instead of the current uploaded file, click **Browse File**

 again and select the desired file from your local PC. The previously uploaded file will get replaced with the new file.

To download the uploaded file, click **Download File**  .

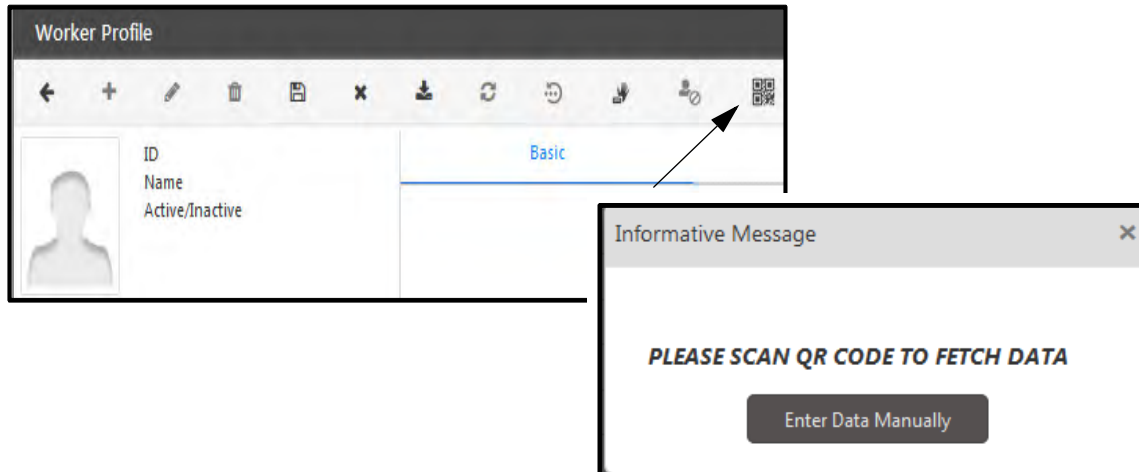
To remove the uploaded file, click **Remove File**  .

Then click **Update**.

The document will be uploaded and can be previewed by clicking on **Preview**  button.

The details can also be fetched directly from Worker's Aadhar Card. By Scanning the QR Code of Aadhar Card through 'QR Code Scanner', the information like Name, Gender, DoB, Address etc. available in Aadhar Card will be automatically fetched, and filled into the respective fields of above mentioned sections.

From the Top menu Bar click on the **QR Code** button and the pop-up will open as shown below.



Scan the worker's Aadhar Card QR through the QR Code scanner or click on the **Enter Data Manually** button to enter the details manually into a pop-up window.

Once the Aadhar Card is scanned and information is received by COSEC Server, the fetched details including Aadhar Number will display as shown below.

The image shows a 'Fetched User Data' pop-up window. It contains the following fields and values: Aadhaar No. (702351944240), Name (Bindu Singh), Gender (Female), Date Of Birth (15/09/1987), Address (A2-92-Sanidhya Township, Behin d Dasalad, Ajwa Road, Vadodara), Street (Waghodiya Road), City-Pincode (Vadodara - 390019), State (Gujarat), Country (India), and Father/Spouse Name (Roopnarayan Singh). At the bottom are 'OK' and 'Cancel' buttons.

You can edit the details if required.



The Aadhar Number must be unique from existing workers to configure a new one.

Click **OK** to save the details or **Cancel** to discard the configuration.

The fetched details will be placed into the fields of respective sections.

If the Admin has configured QR Code scanning optional then, the above step can be skipped and the details can be added manually as below.



You can also refer the User configuration in User module for your reference and configure the worker's profile the same way as described there.

Specify the worker's **ID**. If the Admin has configured Worker ID to be generated automatically then, a user does not need to specify this field. Once the further details are configured and saved, the unique ID will be automatically allocated to the worker.

Specify the name of the **worker**.



When Full name of worker is entered and Name and Short name are blank then Name will be auto updated with 45 characters of full name excluding special characters and Short name will be updated with 15 characters of full name.

Check the **Active** box to activate the worker. Whenever a worker is made inactive (i.e. **Active** checkbox is unchecked), the Admin will be prompted to choose whether all assigned devices should be revoked from the worker or not.

Optional

Full Name- You can also specify the Full name of the worker with maximum 200 characters. The supported values are: **A-Z, a-z, 0-9, () , [] _ (underscore), - (Hyphen), . (full Stop), /, &, , (comma), @, ' (single quote), [space]** .




A function name followed by (bracket is invalid in full name. Eg: Thomas S/O Round (will be invalid.

Short Name - Specify an alternative short name for the worker which will be displayed on the COSEC DOORs whenever there is an event related to this worker. (maximum up to 15 characters)

Reference ID - The system allots a random sequential Reference Code based on the last reference code allotted (numeric value with a maximum of 8 digits). This option is used to provide a linkage ID in the event of an organization using a different user ID format in another software application for e.g. the payroll application.

Integration Reference - This field is provided for integration with third party applications where the worker ID has to be alphanumeric and up to 20 characters.

Use the **Change Document**  button to browse and upload relevant worker documents for the above fields, where applicable (e.g. driving license, PAN card etc.)

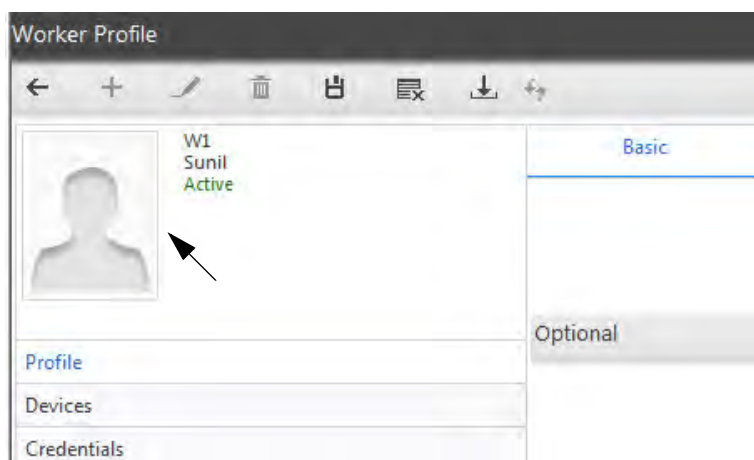
Click on **Save** button to save the worker profile.





*The worker profile will be saved only if contractor is assigned to the worker from the **CWM** tab.*

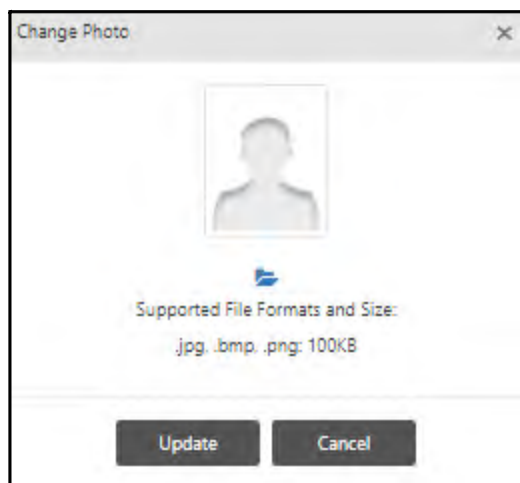
Adding Worker Photo


The administrator can add a profile photograph for each worker defined on the COSEC system, from the **Worker Profile** page as shown below.

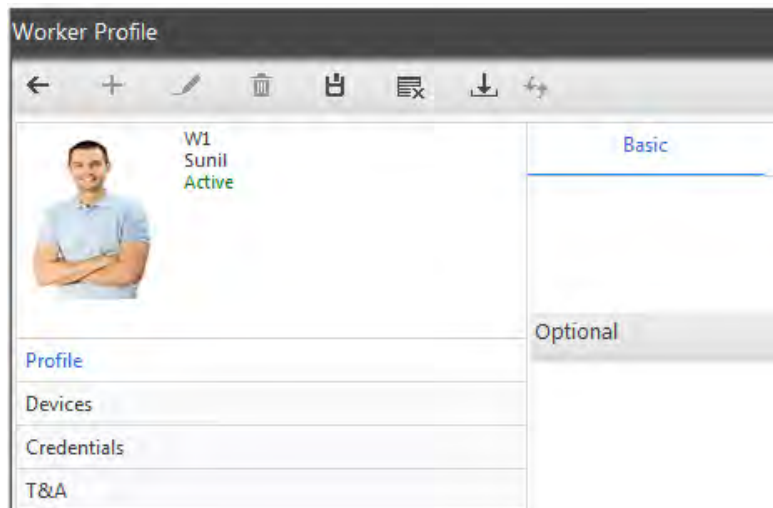


To add an image as the profile photograph for a worker,

1. On the **Worker Profile** page, click **Edit**  for the selected worker.
2. Click the **Change Photo** box.
3. On the **Change Photo** pop up window, click  to browse your computer for an image file. The Supported File Formats are *.jpg, .bmp and .png.



4. Once the required image file is selected, click the **Update** button.
5. Click **Save** . The worker photo is successfully updated on the **Worker Profile** page as shown.



Worker Profile- Devices

The **Devices** tab enables the administrator to assign the workers to the panels, direct doors and device groups already defined in the system.

On selection of the **Devices** tab, the following page is displayed:

The screenshot shows the 'Worker Profile' page for worker 4462, Utsav, who is Active. The 'Devices' tab is selected. The 'Assign' section is active, showing a search bar and a table for assigned devices. The table has columns: Device Name, Type, Restrict Access, Restrict Attendance, and Action. The table is currently empty, displaying 'No Data'.

1. In the **Assign** section under the **Devices** tab,

- Click the **Add** button.
- Select a **Device Group** using the Device Group picklist and the Devices using **Device** picklist..

The screenshot shows the 'Worker Profile' page for worker 4462, Utsav, who is Active. The 'Devices' tab is selected. The 'Assign' section is active, showing a search bar and a table for assigned devices. The table has columns: Device Name, Type, Restrict Access, Restrict Attendance, and Action. The table contains the following data:

Device Name	Type	Restrict Access	Restrict Attendance	Action
ARGO	ARGO	<input type="checkbox"/>	<input type="checkbox"/>	
Door PVR	PVR Door	<input type="checkbox"/>	<input type="checkbox"/>	
FMX	Door FMX	<input type="checkbox"/>	<input type="checkbox"/>	
PATH	Path V2	<input type="checkbox"/>	<input type="checkbox"/>	

You can also Unassign the particular device from the assigned Device Group by clicking on icon. Click on the icon to assign the device again.

- Select the corresponding **Restrict Access** and **Restrict Attendance** checkboxes to enable these restrictions for the selected user on the selected device as shown.

Search				
Device Name ▲	Type	Restrict Access	Restrict Attendance	Action
ARGO	ARGO	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Door PVR	PVR Door	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
FMX	Door FMX	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
PATH	Path V2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

2. In the **Configure** section under the **Devices** tab,

- Select a device from the **Device** drop down list. This list displays all devices on which the selected user was assigned earlier (as shown below).

The **Active** checkbox is selected by default to enable the user credentials on the selected device.

Assign
Configure

Device
panel_lite_sheetal

Type
Panel Lite

Active
☒

VIP
☐

Absentee Rule
☐

Absent Day(s) Count
60

Access Profile
Group-1

Functional Group
Staff

Home Zone
Zone-1

Visit Zone

Access Route

- Check the **VIP** box if the user is to be given unrestricted access rights.
- Option is provided for enabling **Absentee rule** feature at worker level for each PANEL and DIRECT DOOR V2. However, this option needs to be first enabled at the PANEL and DOOR levels.
- Specify the day count for the Absentee rule ranging from 1 to 365.
- In the event of a PANEL controller select the **Access Profile** to be assigned to the user from the drop down list.
- Select the **Functional Group** in the event of a PANEL controller to be assigned to the user from the pull down list.

- In the event of a PANEL controller select the user's **Home Zone** and the **Visit Zone** from the respective drop down lists.
- In the event of a PANEL device the administrator can also assign a defined access route to the user. Select the access route from the drop down list if required. Select another device and configure the access control options as applicable.




*This option is only available with the **Access Control** add on module.*

Worker Profile- Credentials

The **Credential** tab enables the configuration and enrollment of worker credentials in the COSEC system for the selected worker. On selection of the **Credentials** tab, the following page is displayed:

PIN	<input type="text"/>
Biometric Group No.	<input type="text"/>
Roaming User	<input type="checkbox"/>
Access Card 1	<input type="text"/>
Access Card 2	<input type="text"/>
Enrolled Fingers (Suprema Proprietary)	<input type="text"/>
Enrolled Fingers (Suprema ISO)	<input type="text"/>
Enrolled Fingers (Lumidigm ISO)	<input type="text"/>
Enrolled Fingers (Lumidigm Proprietary)	<input type="text"/>
Enrolled Palms	<input type="text" value="No. of Enrolled Palm"/>
Enrolled Faces	<input type="text"/>
Enable Self-Enrollment	<input type="checkbox"/>

The following parameters are available for configuration in the **Edit**  mode for the selected worker:

- **PIN:** Specify the PIN no. for the worker. PIN should be a numeric value ranging from 1 digit to a maximum of 15 digits. The value entered in this field will only be visible to the “sa” worker. For all other login workers the value in this field will be masked.
- **Biometric Group No.:** Specify the Biometric group number to be assigned to the worker if applicable. It is a number allotted to a group of workers assigned on a device. This enables the device to match a template against only those workers who are part of the same Biometric Group thus reducing processing time.

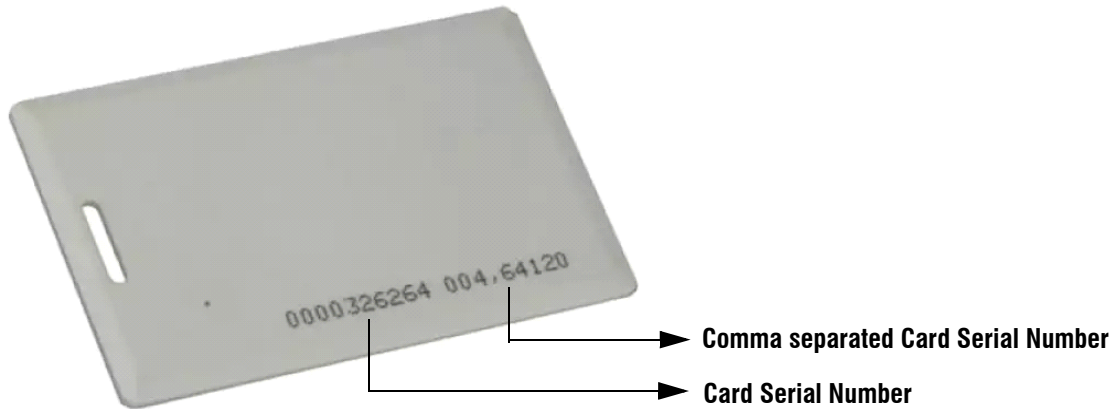
This value is used for Palm/Face Identification of worker on Identification Server in shorter time span considering worker first specifies Group No and then punches on the device.

Identification Server will be allocating templates to its child threads on the basis of this field.

- **Access Card 1:** Enter a Card Serial Number (CSN) or a Comma separated CSN which is to be assigned to the Worker Profile.

Format:

- **Card Serial Number** = 1343933547.
- **Comma separated CSN** = 12,345789



The maximum character limit for Card Serial Number (CSN) is 20 digits. While the maximum character limit for Comma separated CSN is 21 digits.

To configure a comma separated card value, make sure you configure a 26-bit card format in the system and then assign the same to the device. To know more, refer [“Card Formats”](#).

If there is any discrepancy while entering the Access Card number (CSN), the system will display an error.

This Access Card number will be synced with the devices to allow/deny access to workers.

COSEC accepts up to two cards per worker. So if required and available, enter the **Access Card 2** number.


Once you save the configurations, hover your mouse over the Comma separated CSN value of any Access Card, the system will display an encoded (converted) value of Comma separated CSN.

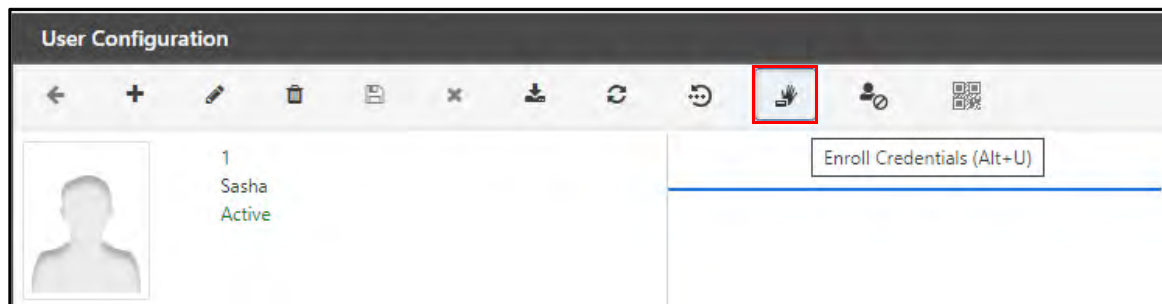
While importing the data of workers, make sure you enter the correct Access Card details in the desired format — Card Serial Number (CSN) or Comma separated CSN. To know more about importing workers, refer [“Import Workers”](#).

- **Enrolled Fingers:** This option displays the number of fingerprint templates enrolled against the selected worker.
- **Enrolled Palm:** This option displays the number of palm vein templates enrolled against the selected worker.
- **Enrolled Face:** This option displays the number of Face templates enrolled against the selected worker.
- **Enable Self-Enrollment:** This option can be enabled to allow a worker to enroll himself/herself on COSEC using an already provided access card/PIN.

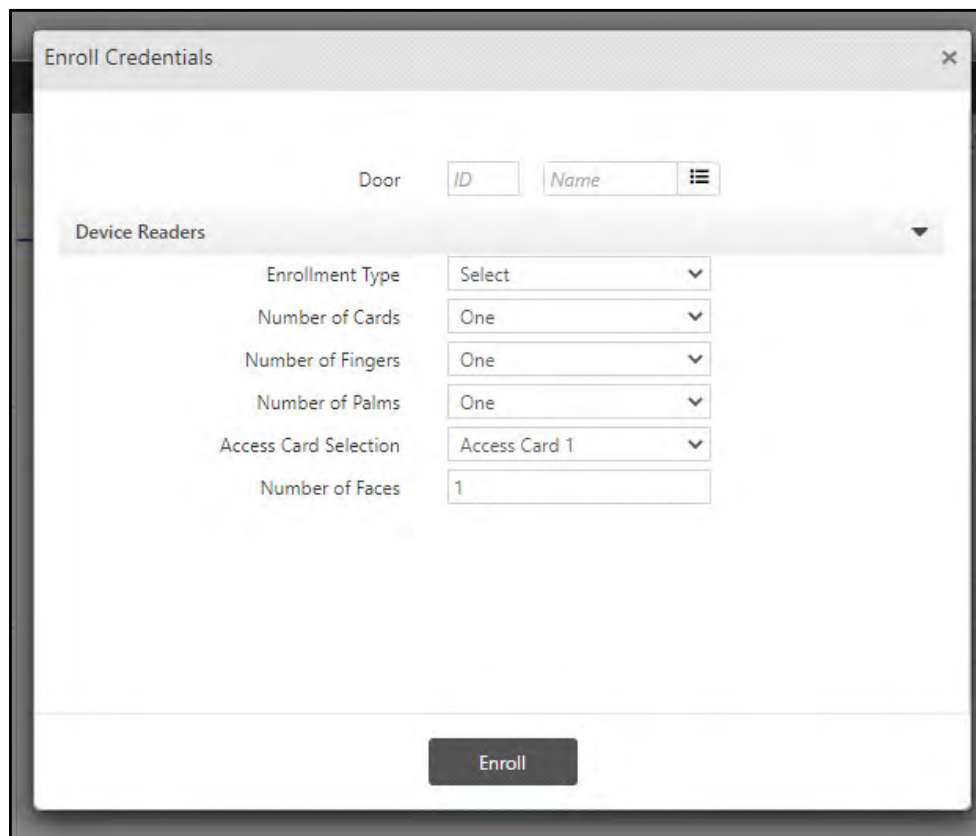
The administrator can also perform enrollment for the selected worker by clicking the **Enroll Credentials** button.

Enroll Credentials

The Administrator can enroll credentials for the worker by clicking **Enroll Credentials**  as shown below.



The **Enroll Credentials** window appears as shown below:



- **Door:** Select the desired door from the pick list on which the enrollment is to done.

Device Readers

Device Readers displays the information of the readers configured in the selected **Door**.

Enroll Credentials

Door

Device Readers

Card Reader

Biometric Reader

External Reader

Enrollment Type

Number of Cards

Number of Fingers

Number of Palms

Access Card Selection

Number of Faces

Enroll

Card Reader, Biometric Reader and External Reader information are displayed here.

Enroll Credentials

Door

Device Readers

Card Reader

Biometric Reader

External Reader

Enrollment Type

Number of Cards

Enroll

- **Enrollment Type:** From the dropdown list, select the desired enrollment type — **Read Only Card, Smart Card, Biometrics, BiometricsThenCard, Face, Mobile** or **Duress Finger**.

Based on the selection of the **Door** and **Enrollment Type**, below parameters will be displayed for configuration.



When Enrollment Type selected is Smart card or BiometricThenCard, Duress Finger Templates will not be written in the Smart Card.

Below parameters also depend on the Readers configured in the Door. To configure the desired Reader, refer Readers section under Devices > Device Configuration (of the desired Door) > Profile > Readers.

1. Enrollment Type = Read Only Card

Number of Cards: Select the desired number of cards from the drop down list.

2. Enrollment Type = Smart Card

Number of Cards: Select the desired number of cards from the drop down list.

Details on Smart Card

Select the desired check boxes of the parameters — **Worker ID**, **Facility Code (FC)**, **Additional Security Code (ASC)** — which are to be displayed on the Smart Card.

Select the desired number of **Finger Templates** from the drop down list.

If the **Door** is selected as PVR Door, **Palm Templates** parameter will be visible. Select the check box of this parameter if you wish to display it on the Smart Card.

To store palm templates, MiFare 4k reader must be configured in the PVR Door.



Door PVR must be set in the Adaptive mode (configure from Admin> System Configuration> Global Policy) for the palm templates to be saved into the Smart Card.

Additional Details on Smart Card

Other than the parameters mentioned in the Details on Smart Card, you can display additional details on Smart Card.

Select the desired check boxes of the parameters — **Short Name, Branch, Department, Designation, Emergency Contact, Blood Group** and **Medical History**— which are to be displayed on the Smart Card.

The values of these additional details are displayed as well. Make sure the values of these additional details are not blank for successful enrollment process.

3. Enrollment Type = Face

Number of Faces: Select the desired number of faces from the dropdown list.

The screenshot shows a window titled "Enroll Credentials". It contains the following fields and controls:

- Door:** A text box containing the value "13".
- Device Readers:** A section with a header "Device Readers" and a dropdown arrow. Below it, the "Enrollment Type" is set to "Face" (shown in a dropdown menu) and the "Number of Faces" is set to "1" (shown in a text box).
- Enroll:** A button at the bottom center of the window.

4. Enrollment Type = Biometrics

Number of Fingers/ Number of Palms: Select the desired number of fingers or palms from the dropdown list.

The image displays two screenshots of the Matrix COSEC System configuration interface. The top screenshot shows a configuration for Door 3 with the device reader set to ARGO. The enrollment type is Biometrics, and the number of fingers is set to One. The bottom screenshot shows a configuration for Door 1 with the device reader set to PVR. The enrollment type is Biometrics, and the number of palms is set to One.

5. Enrollment Type = BiometricsThenCard

Number of Cards: Select the desired number of cards from the drop down list.

Number of Fingers/ Number of Palms: Select the desired number of fingers or palms from the drop down list.

The screenshot shows the 'Enroll Credentials' window with the following settings:

- Door:** 3, ARGO
- Device Readers:**
 - Enrollment Type: BiometricsThenCard
 - Number of Cards: One
 - Number of Fingers: One
- Details on Smart Card:**
 - Worker ID: ☐
 - Facility Code (FC): ☐
 - Additional Security Code (ASC): ☐
 - Finger Templates: None
- Additional Details On Smart Card:**
 - Short Name: ☐ w1
 - Branch: ☐ DFLTBR
 - Department: ☐ DFLTDPT
 - Designation: ☐ DFLTDSG
 - Emergency Contact: ☐
 - Blood Group: ☐ NA
 - Medical History: ☐

An 'Enroll' button is located at the bottom right. A tooltip near the 'Finger Templates' dropdown states: 'Duress Finger Templates will not be written in the Smart Card'.

Details on Smart Card

Select the desired check boxes of the parameters — **Worker ID**, **Facility Code (FC)**, **Additional Security Code (ASC)** — which are to be displayed on the Smart Card.

Select the desired number of **Finger Templates** from the drop down list.

If the **Door** is selected as PVR Door, **Palm Templates** parameter will be visible. Select the check box of this parameter if you wish to display it on the Smart Card.

To store palm templates, MiFare 4k reader must be configured in the PVR Door.



Door PVR must be set in the Adaptive mode (configure from Admin> System Configuration> Global Policy) for the palm templates to be saved into the Smart Card.

Additional Details on Smart Card

Other than the parameters mentioned in the Details on Smart Card, you can display additional details on Smart Card.

Select the desired check boxes of the parameters — **Short Name, Branch, Department, Designation, Emergency Contact, Blood Group** and **Medical History**— which are to be displayed on the Smart Card.

The values of these additional details are displayed as well. Make sure the values of these additional details are not blank for successful enrollment process.

6. Enrollment Type = Mobile



To select **Enrollment Type** as **Mobile**, the particular device must have BLE support and ensure Bluetooth is ON in the mobile.

Access Card Selection: Select the desired Access Card from the drop down list.

Facility Code (FC): Select this check box to enroll the Facility Code (FC) against the worker.

Click **Enroll** to initiate the enrollment process.

Enroll Credentials

✓ Enrollment Command Sent

Door: 3, ARGO

Device Readers: [Dropdown]

Enrollment Type: Mobile

Access Card Selection: Access Card 1

Facility Code (FC): ☐

Enroll

7. Enrollment Type = Duress Finger

Number of Fingers: Select the desired number of fingers that you want to enroll as **Duress Finger** from the drop-down list— **One** or **Two**.

Enroll Credentials

Door: 1, ARGO Device

Device Readers: [Dropdown]

Enrollment Type: Duress Finger

Number of Fingers: One

Enroll

Click **Enroll** to initiate the enrollment process.

To know more about enrolling credentials of workers, refer [“Enrollment”](#).

Worker Profile- Group

The Group section enables to assign the Enterprise groups, Reporting group, Approval Policy, Leave group and Week off group to the worker. On selection of the **Group** tab, the following page is displayed:

Field	Value	Action
Organization *	1	Organization-1
Branch *	1	Branch-1
Department *	1	Department-1
Section *	1	Section-1
Category *	1	Category-1
Grade *	1	Grade-1
Designation *	1	Designation-1
Custom Group 1 *	1	Custom Group 1
Custom Group 2 *	1	Custom Group 2
Custom Group 3 *	1	Custom Group 3
Reporting Group	ID	Name
Approval Policy	ID	Name
Leave Group *	1	Leave Group-1
Week Off Group	ID	Name

This page will be available with the Time & Attendance add on module.

The default groups will be shown in the respective fields. Click on the picklist buttons and select the appropriate enterprise groups (Organization, Branch, Department, Section, Category, Grade, Designation) to assign the worker.



The Enterprise Groups changed from here will be effective from the current date only. For the changed group to be effective from previous date, change the group from User module> Utilities> Change Group.

The picklist options that appear in each enterprise group will be as per the rights assigned to the SA. For details, refer to "Assigning Group-Wise Rights" under "System Accounts".

Reporting Group: Select the group from the picklist to be assigned as reporting group for the worker. The In-charge of the selected group will be the in-charge of the worker. The different applications of worker will require authorization of the in-charge of the group.

To create the Reporting group; go to *Users module> Reporting In-charge> Reporting Group*.

Approval Policy: When Reporting group is assigned to the worker only then you can select the approval policy from the pick-list to assign to the worker.

The Approval policy is created from *Users module> Reporting In-charge> Approval Policy*.

The Approval Policy set in Enterprise Structure> Master page will be set as default approval policy when new worker is created. Eg: Suppose Organization 1 is assigned Approval Policy1; when new worker is added in Organization1 then by default Approval policy1 will be assigned to the worker.

Leave Group: Select the leave group from the pick-list to assign a group of leaves to the worker.



To assign the new leave to the worker, add the leave to the Leave group and assign the leave group to the worker.

Week Off Group: Select the week off group from the picklist to assign the configured week offs to the worker.



To create the Week Off group, go to Shifts and Schedule module > Week Off Group

Group			
Organization *	1	Organization-1	
Branch *	1	Branch-1	
Department *	1	Department-1	
Section *	1	Section-1	
Category *	1	Category-1	
Grade *	1	Grade-1	
Designation *	1	Designation-1	
Custom Group 1 *	1	Custom Group 1	
Custom Group 2 *	1	Custom Group 2	
Custom Group 3 *	1	Custom Group 3	
Reporting Group	5	Factory Group	
Approval Policy	4	Both Final-2	
Leave Group *	1	Leave Group-1	
Week Off Group	ID	Name	



If 'Shift Based Access' flag is enabled in User Configuration, then effect of Week Off group assigned to worker differently won't be effective.

Also if flag of 'Deny Access On Week Off' is enabled in Shift Schedule assigned to worker, then worker won't be granted access though worker did not have week off based on Week Off group.

Worker Profile- T&A

This tab will be available only for the *Time and Attendance license* Here, the administrator can enter the attendance and the working policy related information for the worker:

The screenshot shows the 'Worker Profile' window with the 'T&A' tab selected. The left sidebar lists various profile settings, with 'T&A' highlighted. The main area is divided into 'Attendance' and 'Policy' sections. The 'Policy' section contains the following settings:

- Enable Attendance Calculation: ☒
- Restrict Half Day Considerations: ☐ ⓘ
- Attendance Marking Type: Normal (dropdown)
- Max Punches To Be Considered: Select (dropdown)
- Bypass Finger/Palm/Face For Attendance: ☐
- Max Short Leaves Allowed: (empty field)
- OT/C-OFF Eligibility: None (dropdown)
- Authorize C-OFF On: ☐ WO ☐ PH ☐ WO/PH ☐ FB ☐ RD ☐ Normal Day
- Bus Route: ID (input) Name (input) ⓘ
- Enable Site Based Auto Tour Application: ☐
- Tour: Select (dropdown)
- Base Site Selection: ID (input) Name (input) ⓘ
- Auto Authorize Site Based Tour Application: ☐

This screenshot shows a detailed view of the 'Enable Location Based Auto Tour Application' settings. The settings are as follows:

- Enable Location Based Auto Tour Application: ☒
- Tour: T2 - Tour2 (dropdown)
- Base Location Assignment: Selected (dropdown)
- Location: Code (input) Name (input) ⓘ
- Location Group: ID (input) Name (input) ⓘ
- Auto Authorize Location Based Tour Application: ☒
- Show Attendance Details On Device: ☒

A notification box on the right indicates: ⓘ 1 Location(s) are selected



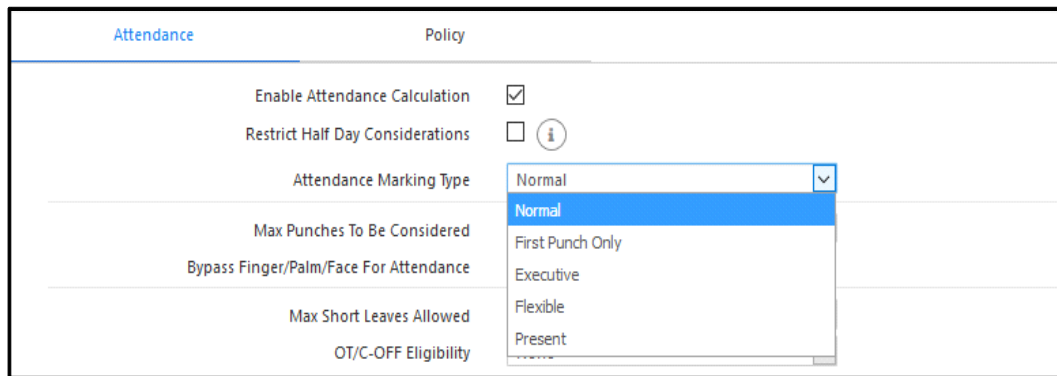
If the Attendance Policy for the worker is configured then assign that policy to the worker. There is no need to configure same parameters i.e. "Max Punches to be considered" and "Max Short Leaves Allowed" here. Still If configured, then parameters configured here will be applicable for the worker.

Attendance

In the **Attendance** section, configure the following parameters:

Enable Attendance Calculation - This field is checked by default. uncheck this box if you want to disable attendance calculation for this worker. This option has to be enabled for configuring any of the other parameters on this page.

:



Restrict Half Day Considerations - Enabling this option will restrict the half day markings and will consider only the full day attendance calculations.

For Example:

If the worker has completed only the half of the required working hours, and **Restrict Half Day Considerations** is enabled for him, then his attendance will be considered as full day absent and the half day consideration will be restricted.

Attendance Marking Type - In case the attendance calculation is enabled then the worker needs to select the attendance marking type from the drop down list.

The following options are available:

- **Normal:** type will be default for all workers.
- **First Punch Only:** type workers need only entry punch at the start of the shift. In this case the system will assume that the shift end time is the last out Punch for the day. All other calculations remain the same as for normal type workers.
- **Executive:** type workers will be marked full day present if at least one punch (entry/exit) is available in the day. There will not be any late/early & overtime calculation like it is done for normal and single punch type workers.
- **Present:** category workers do not require any punch for them to be marked full day present. All workers belonging to this category are marked present by default.
- **Flexible:** category workers' working will be checked against required minimum working and if it is more than required, full day attendance will be marked. In this case the minimum working hours required in a day for full day attendance and half day attendance can also be defined for each worker as explained below.
- **Minimum Working Hours Required** - In the event of selecting the Flexible type for a worker the administrator can also specify the minimum working hours required in a day to be marked **Full Day** or **Half Day** present. Specify the hours in hh:mm format.

Attendance		Policy	
Enable Attendance Calculation	<input checked="" type="checkbox"/>		
Restrict Half Day Considerations	<input type="checkbox"/>		
Attendance Marking Type	Flexible		
Min Working Hours Required			
Half Day	02:00		
Full Day	04:00		
Max Punches To Be Considered	2		
Bypass Finger/Palm/Face For Attendance	<input type="checkbox"/>		

Max Punches to be Considered - This parameter specifies the maximum entry/exit events per worker to be considered in a day for attendance calculation.

Specify a value in this field if the value defined at the global level is to be overridden for this worker. The options available are 2, 4, 6, 8, 10, 12 and N-Punch. N-Punch allows unlimited number of punches in IN/OUT pair.

Max Punches To Be Considered	2		
Bypass Finger/Palm/Face For Attendance	Select		
Max Short Leaves Allowed	2		
OT/C-OFF Eligibility	4		
Authorize C-OFF On	6		
	8		
	10		
Bus Route	12		
	N-Punch		
Enable Site Based Auto Tour Application	<input type="checkbox"/>		

Bypass Finger/Palm/Face For Attendance - On checking this option, the worker can punch in or out using any of the assigned credentials and the same will be considered for attendance calculation. On selection of this option, finger/palm/face identification is not required for marking attendance. The worker can use pin or card to mark the attendance.

Max Short Leaves Allowed - This parameter specifies the maximum number of short leaves (personal hours) to be allowed to selected workers in an attendance period. This parameter is also defined at the global system configuration level and can be overridden for specific workers using this option. The administrator can specify a value of a maximum two digits in this field.

OT/C-OFF Eligibility: This parameter enables the administrator to determine whether the overtime authorization for this worker is to be done in one of the following ways:

- **None** - Extra work cannot be authorized as overtime or C-OFF for worker.
- **Only Overtime** - Extra Work can only be authorized as overtime.
- **Only C-OFF** - Extra Work can only be authorized as C-OFF.
- **Both** - Extra Work can be authorized both as overtime and C-OFF.

On selecting **Both**, worker can set the extra hours to be authorized as OT or C-OFF separately for Normal Day, WO, PH, WO/PH, FB and RD.



If only Compensatory off is to be given to the worker, then you must select Only C-OFF option.

Bus Route: Click on the Pick-list button and select the bus route to be assigned to the worker.

Enable Site Based Auto Tour Application: Select this checkbox so that tour application will be automatically applied for a particular worker, if he punches from some site other than the Base Site.

- **Tour:** Select the tour application from the dropdown list which will be automatically applied.
- **Base Site Selection:** Select the base site to be assigned to the worker.
- **Auto Authorize Site Based Tour Application:** Select this checkbox to automatically authorize the tour application for a particular worker, if auto tour application feature is enabled.
- **Enable Location Based Auto Tour Application:** Select this checkbox so that tour application will be automatically applied for a particular worker, if he punches from some location other than the Base location.

If a worker goes for official activity to some location other than base location; then new location can be assigned to the worker and tour application will be automatically applied for that day when event is generated from the new location.

- **Tour:** Select the tour application from the dropdown list which will be automatically applied when worker goes to other location. The Tour application will be available in the drop-down only if it is added in the leave group assigned to the user.
- **Base Location Assignment:** Select the base location to be assigned to the user as **All** or **Selected**.

1. For **All** option; all the locations configured in Location Master will be assigned to the worker. When new location is added to Location master then it will be automatically assigned to the worker if "All" is selected.
2. For **Selected** option; Location and Location Group will be enabled for the selection which is to be assigned to the user.
 - **Location-** Select the Location pick-list and select the locations to be assigned to the worker.
 - **Location Group-** Select the Location group pick-list and select the groups to be assigned to the worker. If Selected Location groups are assigned to worker and whenever new location is added to the location group then newly added location in location group will also be assigned to the worker.



You can see the example for Location Based Auto Tour in User module> T&A.

- **Auto Authorize Location Based Tour Application:** Select this checkbox to automatically authorize the tour application for a particular worker, if auto tour application feature is enabled.

Show Attendance Details on Device: Select the checkbox to display the attendance summary of the worker on Vega and or FMX direct door. Hence the Vega/FMX direct doors assigned to the worker will display the current month's data (as per device time) when the worker is allowed access to the door.

See details in Device Configuration> Advanced > Settings (of Vega Door/ FMX Door).

Policy

In the **Policy** section assign different Policies to the selected worker. This page will be available only with the **Time & Attendance** add on module.

Attendance	Policy	
Attendance Policy	1	Attendance Policy-1
Absentee Policy	1	Absentee Policy-1
Overtime Policy	1	OverTime Policy-1
Late-IN Policy	2	Late-In 2
Early-OUT Policy	1	Early Out Policy-1
C-OFF Policy	1	COFF Policy-1

The default policies will automatically be assigned to the new worker. It will be displayed in the respective fields as shown above.

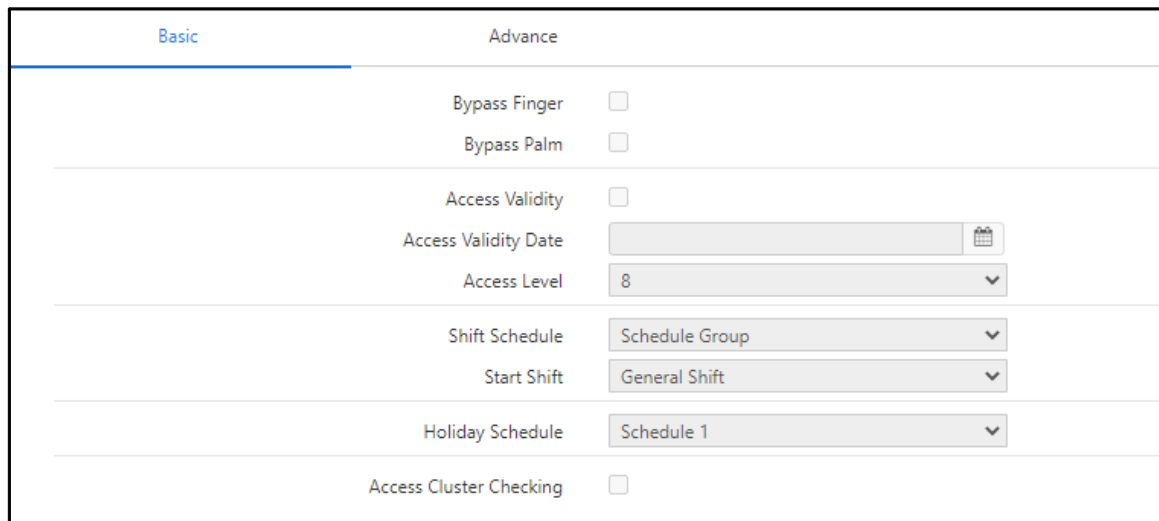
To change the policies from current date, click the respective picklist and select the policy to be assigned to the worker. If the policies (other than Attendance Policy) are to be assigned from previous date, then go to *T&A > Utilities > Change Policy*.



To configure the Policies go to T&A> Policies.

Worker Profile-Access Control

On selection of the **Access Control** tab, the following page is displayed:



Basic	Advance
Bypass Finger <input type="checkbox"/>	
Bypass Palm <input type="checkbox"/>	
Access Validity <input type="checkbox"/>	
Access Validity Date <input type="text" value=""/>	
Access Level <input type="text" value="8"/>	
Shift Schedule <input type="text" value="Schedule Group"/>	
Start Shift <input type="text" value="General Shift"/>	
Holiday Schedule <input type="text" value="Schedule 1"/>	
Access Cluster Checking <input type="checkbox"/>	

Basic

In the **Basic** section, the administrator can define access parameters for the selected worker. This tab offers the following sections for configuration:

Bypass Finger - This option can be enabled in the event of the Finger Print image not being in order and the system thus has problems identifying the worker. In such cases, the system administrator can disable the Finger Print check for the worker thus enabling the worker to gain access using either the assigned pin or card.

Bypass Palm - This option can be enabled in the event of the Palm Vein image not being in order and the system thus has problems identifying the worker. In such cases, the system administrator can disable the Palm vein check for the worker thus enabling the worker to gain access using either the assigned pin or card.

Access Validity - Enable this option if the worker credential is to be activated for a predefined period.

Access Validity Date - Specify the end date of the validity in this field.

Access Level - Specify the access level for which the Smart Identification feature will be applicable to the worker.

Shift Schedule - Assign a shift schedule to the selected worker from the dropdown list.

Start Shift - In case of multiple shifts in the schedule group, the starting shift needs to be selected from the drop down list.

Holiday Schedule - Select the Holiday schedule to be assigned to the worker from the drop down list.

Access Cluster Checking - Select this checkbox to enable checking for access cluster restrictions for the selected worker. It is available only with the Access Control add-on license.

Advance

The **Advance** section is available only with the Access Control add-on module. Here, the administrator can define access parameters for the selected worker. The **Advance** page appears as follows:

Enable Advance Access Control: Check this box to enable the advance access control feature.

Shift based Access: This parameter allows the administrator to enable worker access based on the shift working time of the worker.



*In the event of not selecting the **Shift Based Access** option then the system will apply the **Default Access Settings** as defined on a Panel200 as the access settings for the worker.*

Smart Access Route - Select the Smart Access Route to be assigned to the worker from the Access Route picklist window.

Maximum Route Level: Select the route level up to which the worker is to be allowed access from the drop down list.

Enable Elevator Access Control: Check this box to enable the Elevator access control feature for the worker.

Elevator Floor Group: Click the picklist and select the Elevator floor group to be assigned to the worker. The worker can access the floors of the Elevators included in Elevator Floor Group.

The Elevator Floor group is created from Access Control> Elevator Access Control> Elevator floor group



Certain parameters when configured for a specific worker may over-ride corresponding parameters pre-defined at the Global Policy level.

Worker Profile-ESS

The **ESS** tab is available only with the *ESS* module. This is used to enable and configure ESS account access for the selected worker. On selection of the **ESS** tab, the following page is displayed:

The screenshot displays the 'Worker Profile' window with the 'ESS' tab selected. The left sidebar lists various management options, with 'ESS' highlighted. The main panel shows the 'Settings' section for the ESS account. Key configuration items include: 'Enable Account' (checked), 'Edit Basic Details' (checked), 'Punch Marking Via ESS' (checked), 'ESS Role Rights' (set to 1), 'Preferred Language' (English), 'Login Via Active Directory' (unchecked), 'Auto Authorize (ME) Registration' (unchecked), 'Punch Marking Via API' (checked), 'Mark Punch As Per' (Server Time Zone), 'Auto-Punch Marking' (unchecked), 'Manual Punch Marking' (unchecked), 'Face Mandatory for Punch' (None), 'APTA Face Anti-Spoofing' (unchecked), 'Capture Photo' (unchecked), 'Allow Offline Punch' (unchecked), 'Location Mandatory for Punch' (None), 'Reason For Punching From Unassigned Location' (unchecked), 'Location Assignment' (All), 'Location' (Code and Name fields), 'Location Group' (ID and Name fields), 'Allow Door Access Through API' (unchecked), and 'PIN Authentication For Door Access' (unchecked). A 'Default Domain' button is also visible.

Settings

The **Settings** section under the **ESS** tab offers the following parameters for configuration:

Enable Account - Select this checkbox to enable ESS account access for the selected worker.

Edit Basic Details - Select this checkbox to enable the selected workers to edit basic details on their respective ESS accounts.

Punch marking via ESS - Select this checkbox to enable workers to mark their attendance punch manually from their respective ESS accounts.

ESS Role Rights- Select the Role Rights from the picklist to be assigned to the worker.

Preferred Language- Specifies the language preferred for the selected ESS Users as *English, Arabic, Spanish, Albanian, Turkish or Vietnamese*.

Login via Active Directory - Select this checkbox to enable the selected ESS user to login using his Active Directory credentials.

User name - Assign a user name to the selected ESS user for Active Directory login.

Domain - Specify the Active Directory domain name in this field for Active Directory login.

Auto -Authorize IMEI Registration -Select this checkbox to automatically authorize the user request through device with registered IMEI number in COSEC database. If the box is unchecked, the user request (attendance, leave application etc.) goes to the **IMEI Authorization** which can be then authorized by the administrator.

Mobile Identification Number - Specify the Mobile Identification Number which is the unique number of the mobile device from which the ESS application is to be used. This can consist of maximum 40 alphanumeric characters.

Punch Marking Via API - Select this checkbox to enable user to mark punches by firing API. Auto-Punch and Manual-Punch marking checkbox will be activated only if Punch marking via API is enabled.

Mark Punch As Per- Select the option of Time Zone which is to be applied for punch time (punch marked from API)

- **Server Time Zone-** The date- time of the punch will be as per the server time zone.
- **Local Time Zone-** The date-time of the punch will be as per the time zone of the place from where the punch is marked.

Auto-Punch Marking - Select this checkbox to enable the auto-attendance marking feature for the selected user from the COSEC APTA mobile application. On enabling this feature, if the user's current location matches any of the assigned locations; a punch will be marked automatically for the user from the mobile application.

Manual Punch Marking - Select this checkbox to enable manual punch marking from the COSEC APTA mobile application.

Face Mandatory For Punch - When Manual Punch Marking and Face Recognition feature is enabled for user then you can select the specific option for which face is to be made mandatory for the punch. The options are **Attendance, Access Control, Both** and **None**.

For Access Control and Both option; you must enable “Allow Door Access Through API” checkbox.

APTA Face Anti-Spoofing - When **Manual Punch Marking** is enabled and **Face Mandatory For Punch** is selected as — **Attendance, Access Control** or **Both** — then select **APTA Face Anti-Spoofing** checkbox to enable **Face Anti-Spoofing** feature via COSEC APTA Application to prevent false face verification by using a photo, video, mask or a different substitute for an unauthorized person’s face.

Allow Offline Punch - This checkbox is activated only when “Punch marking via API” and “Manual Punch Marking” are enabled. This allows users to apply for offline punches.

In Mobile devices, when there is no connectivity between server and the Mobile device, the punches, with their timings can be stored through offline punch and send to server when connectivity is restored.

Location Mandatory For Punch - This field determines if information regarding the source location from where the punch has been marked should accompany a punch marking by user. Select None if location information should not accompany a punch. For *Manual Punch Marking*, select Any Location (locations need not be configured). For *Auto-Punch Marking* (auto-attendance feature), select Configured Locations Only (locations must be configured on “Location Master”).

Reason For Punching From Unassigned Location: This checkbox will be activated only when ‘Location Mandatory For Punch’ has either **None** or **Any Location** as values. By enabling this checkbox, the In-charge Users can know the reason for which the punch is made from unassigned location by the employee user.

Location Assignment- Select the option as “All” or “Selected” for assigning location to user.

1. For **All** option; all the locations configured in Location Master will be assigned to the user. When new location is added to Location master then it will be automatically assigned to the user if “All” is selected.
2. For **Selected** option; Location and Location Group will be enabled for the selection which is to be assigned to the user.
 - **Location-** Select the Location pick-list and select the locations to be assigned to the user.
 - **Location Group-** Select the Location group pick-list and select the groups to be assigned to the user. If Selected Location groups are assigned to user and whenever new location is added to the location group then newly added location in location group will also be assigned to the user.



Locations can be configured from COSEC Web Application > Admin > System Configuration > Location Master.

Allow Door Access Through API- Select this check-box to allow the access to device through API.

PIN Authentication For Door Access- Enable this check-box for Dual Authentication with PIN when Bluetooth or QR based access is used for Access control feature in COSEC APTA mobile application.



Pin Authentication For Door Access can be enabled only when Allow Door Access Through API is enabled.

Worker Profile-Cafeteria

This **Cafeteria** tab is available only with the *Cafeteria* module. The Cafeteria tab displays the following page:

Settings

Enable Account - Select this checkbox to enable Cafeteria account access for the selected worker.

Enable Offline Transaction- Select the desired option from the drop-down list for the Worker to perform the offline transaction

- Select **None**, if you do not want to allow transactions to be made by the Worker when the device is in offline mode.
- Select **Allow With Discount**, if you want to allow transactions with discount to be made by the Worker, when the device is in offline mode.
- Select **Allow Without Discount**, if you want to allow transactions without discount to be made by the Worker, when the device is in offline mode.

Discount Level - Select the appropriate discount level from the drop down list as shown.

Discount Level	None
Account Type	None Discount Level 1 Discount Level 2 Discount Level 3 Discount Level 4

Account Type - Specify the account type as **Pre-Paid** or **Post-Paid** by selecting from the drop down list.

Pre-paid Account

- For **Pre-Paid** account type, specify whether the **Balance Management** should be **Device-based** or **Server-based**.
- When Balance Management is selected as **Server based**, then you can enable **Device-Server Balance Check**. This will allow Device to check Server-side balance before allowing transaction. For this, Device and Server must be connected.

Post-paid Account

- For **Post-Paid** account type, enter the **Allowed Usage Per Month** based on which monthly dues for the worker can be calculated.

Enable Account	<input checked="" type="checkbox"/>
Enable Offline Transaction	None
Discount Level	None
Account Type	Post-Paid
Allowed Usage Per Month *	0.00
Cafeteria Usage Policy	ID <input type="text"/> Name <input type="text"/>

Cafeteria Usage Policy- Select the cafeteria usage policy to assign to the user based on which cafeteria transaction restrictions will be applied to the Worker.

Worker Profile-CWM

This tab is available for configuration only for the *Contract Worker Management (CWM)* module worker when an existing worker is selected from the *Worker List*. This enables the administrator to assign Contractor, Work Order, Skills and PPE (Personal Protective Equipment) to the selected worker as well as add ID Proof and Address Proof.

The CWM tab for the worker is shown as below.

Assignment

After the worker is added in the system from **profile** tab, the contractor and the work order is to be assigned to him from the **Assignment** tab of **CWM**.

For the assignment:

Skill- Select the skill from the picklist to be assigned to the worker.

Contractor- Select the contractor from the picklist under whom the worker is to be assigned.

Work Order- Select a work order from the picklist which shows the list of work orders of the selected contractor to be assigned to the worker.

Assignment Period- The work order assignment period is auto generated based on the work order selected. The induction levels grid appear as shown. The assignment period can be changed by clicking on Edit button and selecting the assignment period from calendar buttons.

Assignment Status- This is the auto generated field. When all the stages are approved, the status is marked as approved. If any of the stage is rejected, the status is marked as rejected.

Approval Stage- This is the auto generated field based on the work order selected.

Click on **Save** button to save the worker assignment. The worker profile will be saved and listed under **Worker List**.

An the grid with the assigned induction levels are shown as below. There are maximum seven stages of induction which needs to be approved before the worker is approved for the work order.

Worker Profile

CWM2
Mangesh Yadav
Active

Profile
Devices
Credentials
T&A
Access Control
ESS
Cafeteria
CWM

Assignment Other Details

Skill 3 Electrician

Contractor C101 Samarth

Work Order WO2 Electrical Installation

Assignment Period 31/08/2014 31/12/2014

Assignment Status Approved

Approval Stage 2 Approval Stages-NonTechnical

Level	Induction Level Name	Status	Detail
1	Personal Interview	Approved	(i)
2	Police Verification	Approved	(i)
3	Medical Checkup	Approved	(i)
4	Health Training	Approved	(i)

Click on **Details** (i) button to view the induction level details.

Induction Level Detail

Induction Level 1 Personal Interview

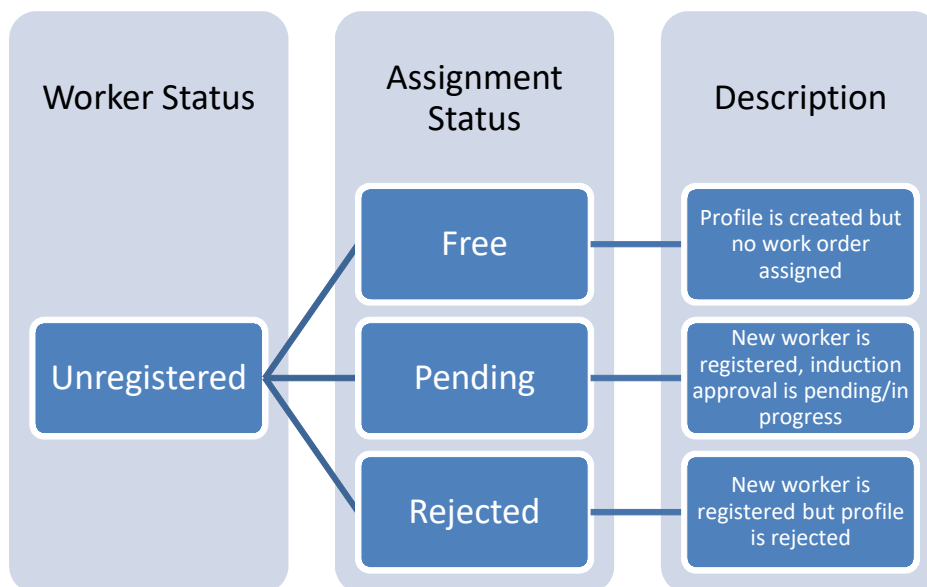
In-Charge 1263 AASHISH GANDHI

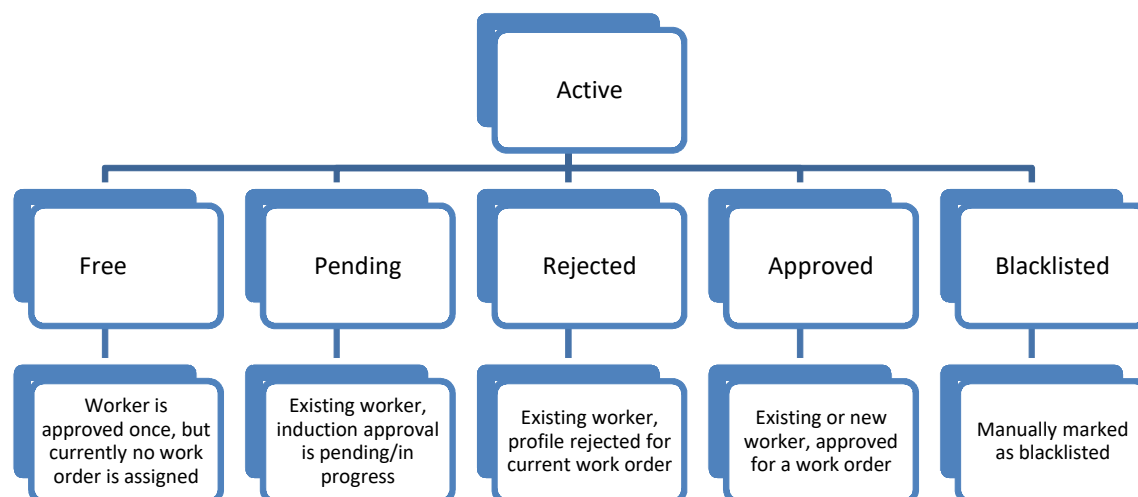
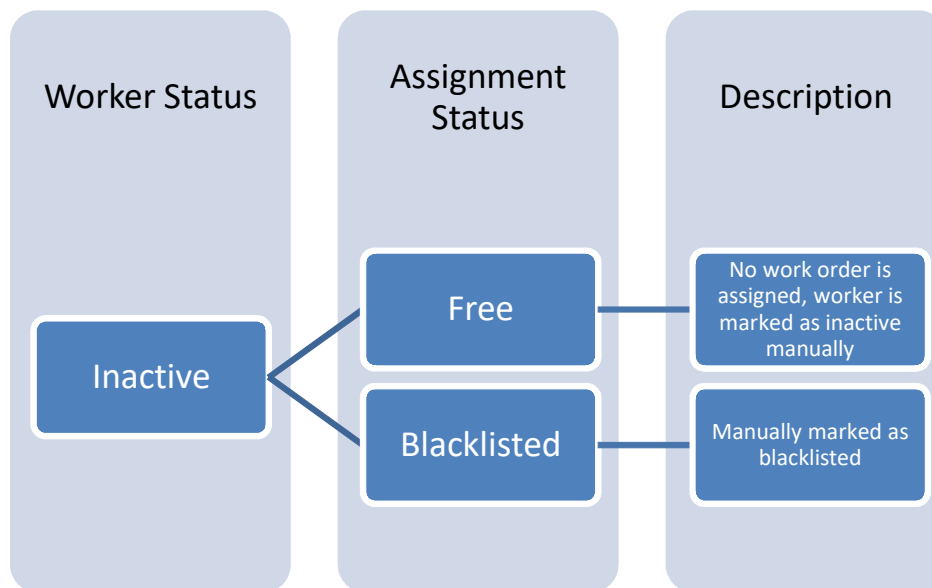
Status Approved

Remark

Close

The various worker status and the respective assignment status is shown in the below figures:




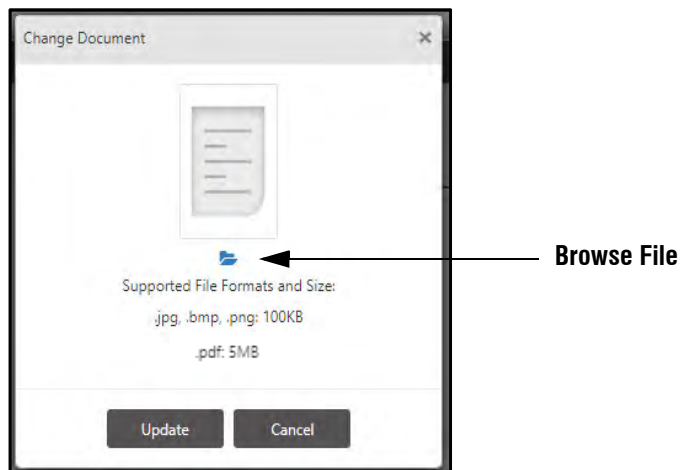


Other Details

The screenshot shows the 'Other Details' tab of an 'Assignment' form. It contains the following fields:

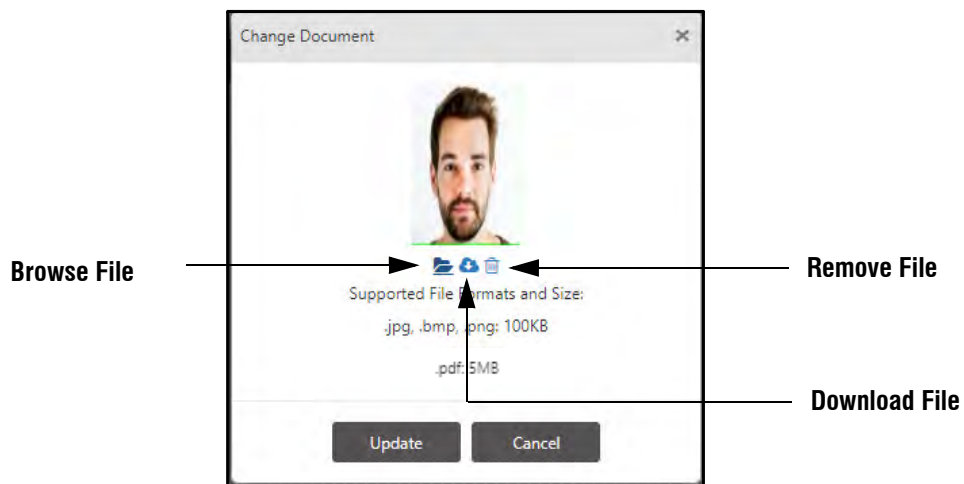
- ID Proof:** A text field with 'Photo ID' entered, accompanied by an upload icon and a search icon.
- Address Proof:** A text field with 'Driving License' entered, accompanied by an upload icon.
- PPE:** Two empty text fields, each with a checkmark icon.
- Table:** A table with two columns: 'ID' and 'Name'. It contains two rows of data: '1' with 'Helmet' and '2' with 'Safety Shoes'. Each row has a delete icon (trash can) to its right.

ID Proof- Specify the name of the ID proof and upload the document. You can upload the documents by clicking **Upload**  button. Then **Change Document** pop-up appears as shown below.




Click **Browse File**  .


To upload, select the desired file as per the supported formats and size (.jpg, .bmp, .png, pdf) from your local PC.




After uploading the file, if you wish to upload a different file instead of the current uploaded file, click **Browse File**

 again and select the desired file from your local PC. The previously uploaded file will get replaced with the new file.


To download the uploaded file, click **Download File** .


To remove the uploaded file, click **Remove File** .

Then click **Update**.

The document will be uploaded and can be previewed by clicking on **Preview**  button.

Address Proof- Specify the name of the Address proof and upload or change the document similar to ID proof.

The documents can be deleted by clicking **delete**  button.

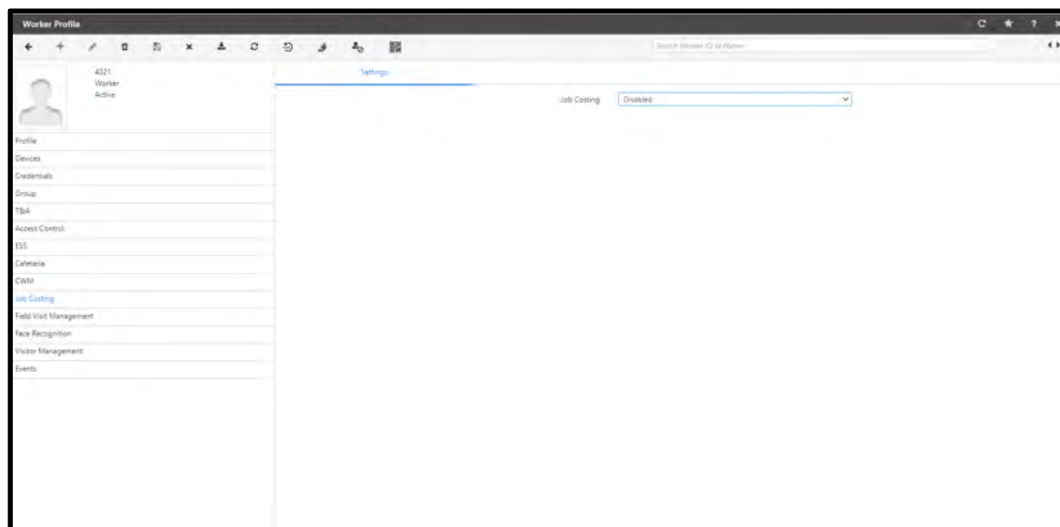
The documents can be viewed by clicking Preview  button.

PPE (Personal Protective Equipment)- Select the protective equipment meant for workers from the picklist. The equipments will be added to the grid.


Click on **Save** button to save the details.

Worker Profile-Job Costing

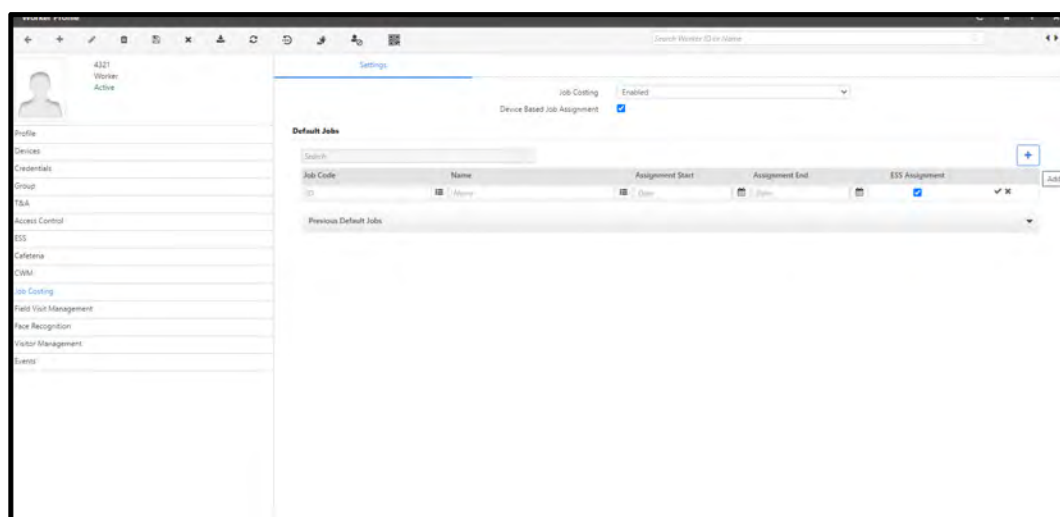
Click **Contract Worker Management >Workers >Worker Profile >Job Costing**.



- **Job Costing-** From the drop down list select **Enabled** to enable **Job Costing** feature for the worker.
- **Device based Job Assignment-** Enable the check box. The Job codes are assigned to the worker as per device configuration on which worker punches.

Default Jobs: Click **Add**  to assign default jobs to the worker.

The Multiple default jobs can be assigned with non-overlapping Assignment Date Ranges. Only 'In Progress' Jobs will be assigned.



- **Job Code:** Select the desired Job Code from the pick list.
- **Name:** Select the desired Name from the pick list.
- **Assignment Start** and **Assignment End:** Define the Start date and End date for the selected job from the calendar.

- **ESS Assignment:** The check box is enabled by default. This Job will be displayed in the list of Jobs assigned to the worker through the ESS login. If you do not want this job to be displayed, clear the check box.



The ESS Assignment column will not be displayed if the **Show All Jobs while Punching** check box is enabled. For details, refer to “Job Costing” in “Defining Global Policies”.

- Click **OK**  to save the details.



Jobs are created from **Job Processing and Costing module > Project Management> Job**.

After adding the job, click **Save** to save the default job to the user.

Default Jobs Grid should consist of currently assigned default jobs (i.e. Current Date <= Assignment End Date).

Example:

On date 15/01/2015, Assign Job-1 (15/01/2015 - 30/03/2015) as default.

On date 25/03/2015, Same Job-1 will be visible in default jobs grid.

Since date 01/04/2015, Job-1 will be moved from Default jobs grid to Previous Jobs Grid.

The applicable devices are:

- DOOR V3
- Wireless DOOR
- PVR
- NGT
- Vega Controller
- DOOR V4



Worker configuration will be resent to devices only when there is some change in Job Assignment.

When new worker is added or existing user's Enterprise group is changed. Then if worker is assigned to the Enterprise group with which Job costing parameters are associated, then the configured job costing parameters will be reflected in User Configuration > Job Costing Tab

Worker Profile-Field Visit Management

On selecting Field Visit Management tab, the following page appears.

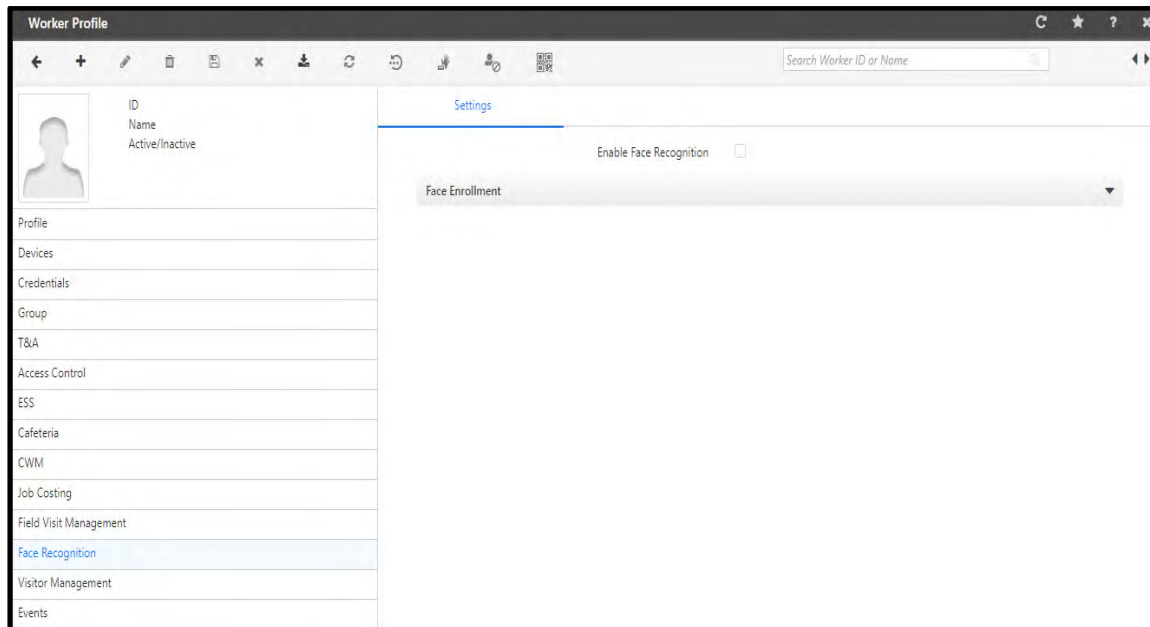
The screenshot shows the 'Worker Profile' interface. On the left is a sidebar with a list of tabs: Profile, Devices, Credentials, T&A, Access Control, ESS, Cafeteria, CWM, Job Costing, and Field Visit Management (which is highlighted in blue). The main area on the right is titled 'Settings' and contains a single checkbox labeled 'Enable FVM' which is currently unchecked. Above the checkbox, there is a header section with a placeholder for a worker's photo and fields for 'ID', 'Name', and 'Active/Inactive'.

In this module, you can assign schedules to the workers and keep a track of their activities, while on site and also check if the assigned tasks are being fulfilled correctly or not.

In the **Settings** tab, check the **Enable FVM** box to consider the selected worker as FVM user.

Worker Profile-Face Recognition

In this feature, worker can access the device or mark the attendance by verifying his Face as the credential. On selecting Face Recognition tab, the following page appears.



Settings

Enable Face Recognition: Check this box to enable Face Recognition feature for the worker.

1. Create a Worker. Enable Face Recognition feature.
2. Assign Vega, FMX, ARGO or ARGO FACE door to the user.
3. Connect the FR module and IP Camera to the network. Ensure that COSEC Device, FR Module and IP Camera are in the same subnet.

If you are connecting the ARGO FACE device, it has an in-built FR Module and camera.

4. Configure IP camera to be used for capturing face credential. Select the Capturing device as IP Camera in Video Surveillance section of Device Configuration and configure the snapshot URL.
5. Configure FR settings on Device. Go to Identification Server of Device Configuration. Enable FR and select the Face capturing mode. Select the FR mode as Local/Server-Assisted. Enter the FR Server Address as the IP address of FR module. Enter FR Server Port as 12000 which is default port for Identification Service.
6. Now Tap on Device screen. The motion streaming of camera will appear on COSEC Device.
7. Now Enroll the worker for Face credential using Enroll Utility.
8. When you show your face in front of camera, the camera will capture your face and identify with the enrolled template. If it matches, you will be allowed access on the door.

Face Enrollment via Web

This functionality enables the SA to enroll face/s against a worker. Face Enrollment can be done by either directly uploading the images of the desired worker or by capturing and then uploading the images.



To use the capture functionality for images, make sure you have a secure login, that is you have logged in using HTTPS.

Using Face Enrollment you can:

- Replace existing images (if any) with new images
- Add new images
- Remove enrolled images

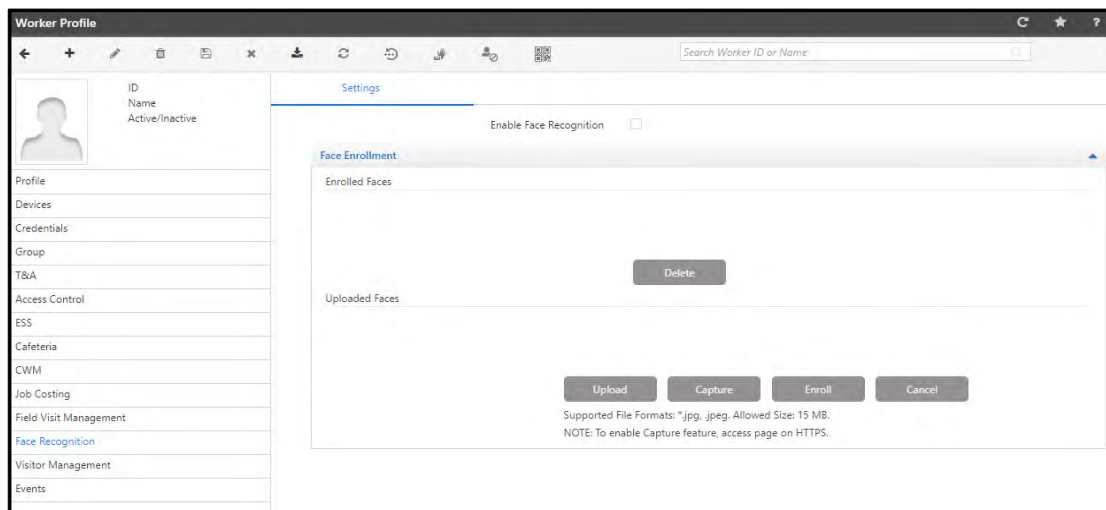
Click the **Face Enrollment** collapsible panel in order to enroll faces against a worker.



For Face Enrollment via Web feature to work, ensure that Identification Service is defined in COSEC Admin > License and Service. For more details refer Admin Management Portal User Manual.

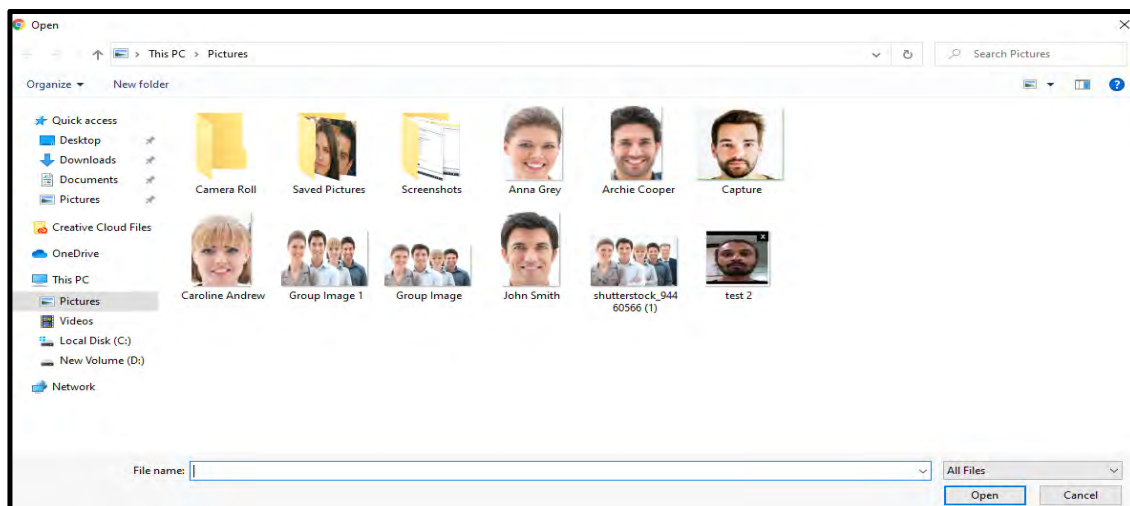
To Upload the images directly, refer **“Upload”**

To Capture and then upload the images, refer **“Capture”**

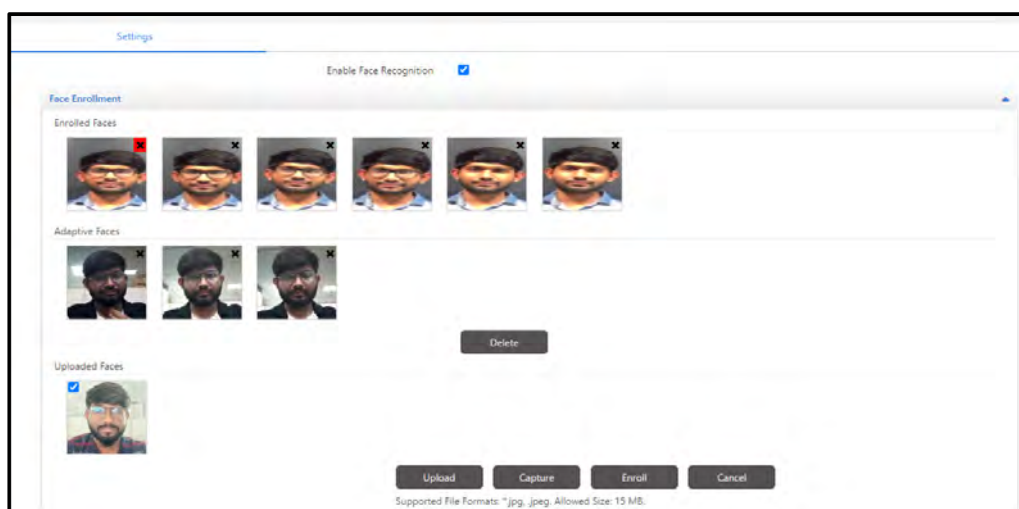


Upload

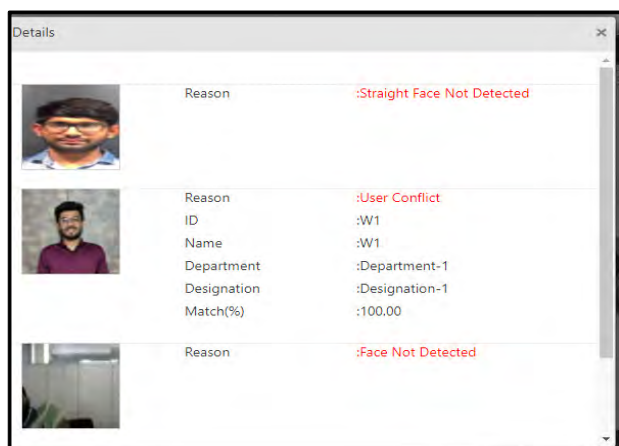
- In order to upload face/s against a worker click **Upload** in **Face Enrollment**.
- Browse to select the desired file from your local PC wherein the image is stored.
- Make sure the selected image is in the .jpg or .jpeg format.
- Click **Open**.



- All the faces that are uploaded will be reflected in **Uploaded Faces** Grid.
- Select the face/s that you want to enroll by clicking the checkbox provided on the top left corner of the uploaded face.

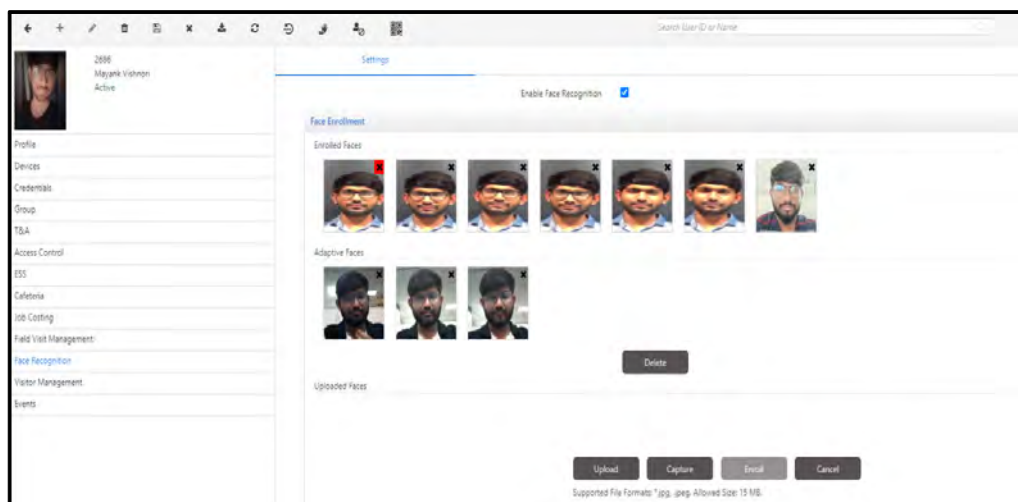


- While uploading a face if any error occurs, the **Info** icon will be displayed.
- On clicking the **Info** icon a pop up with the discarded face/s will be displayed along with the possible reason for discarding the image.

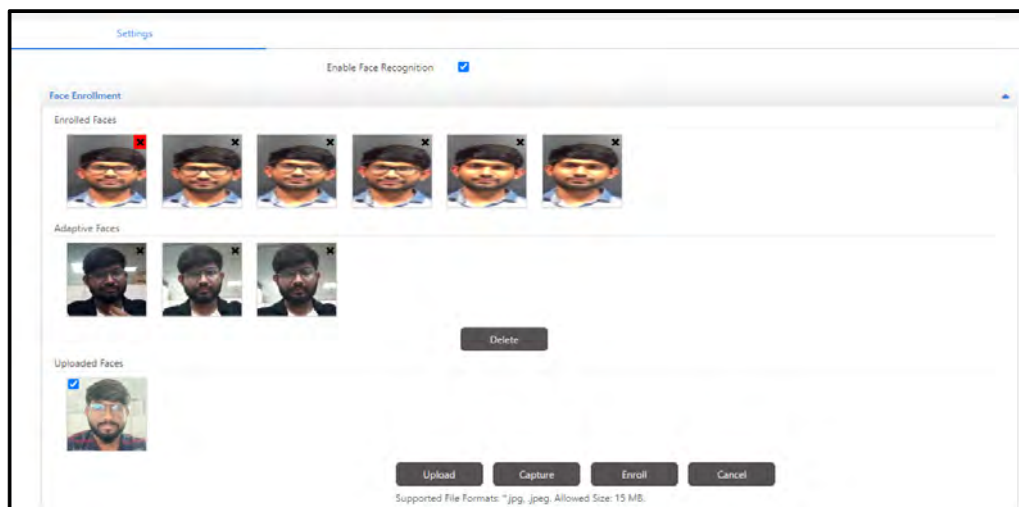


Let us understand this with the help of an example, you have uploaded 5 faces out of which 3 got discarded and then again you uploaded 5 more faces out of which 2 got discarded then the pop-up will display all the 5 discarded faces with the probable reasons for discarding.

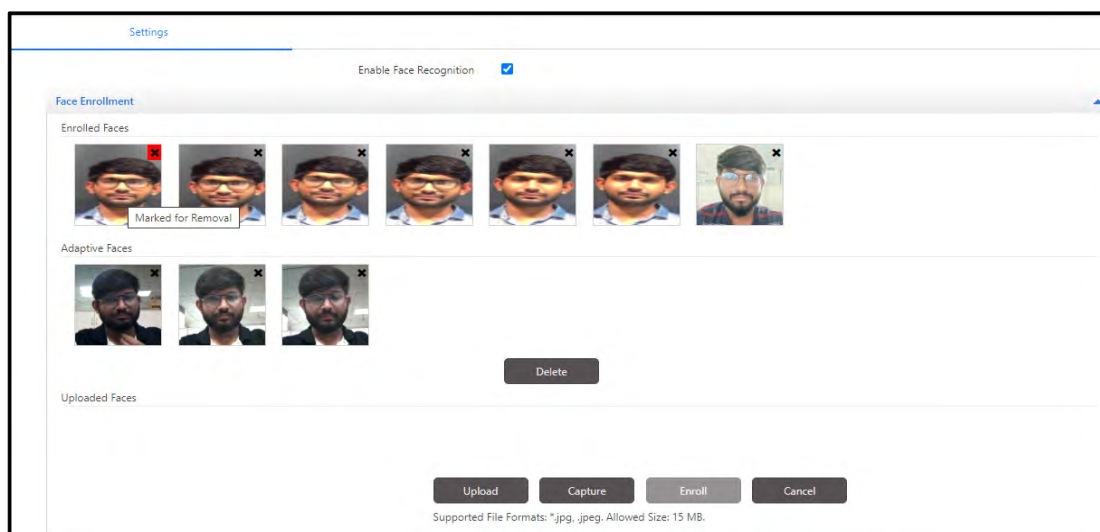
- To add the new image as the enrolled face,
- Select the check box of the desired image under **Uploaded Faces**.
- Click **Enroll** in order to enroll the selected face/s. The selected face/s will be reflected in the **Enrolled Faces** grid.




- To replace an existing enrolled faces,
- Click on the desired image, the red cross icon appears on the top right corner of the face under **Enrolled Faces**.
- Select the check box of the desired image under Uploaded Faces.
- Click **Enroll**.



- To remove an existing enrolled faces,
 - Click on the desired image, the red cross icon appears on the top right corner of the face under **Enrolled Faces**.
 - Click **Delete**.

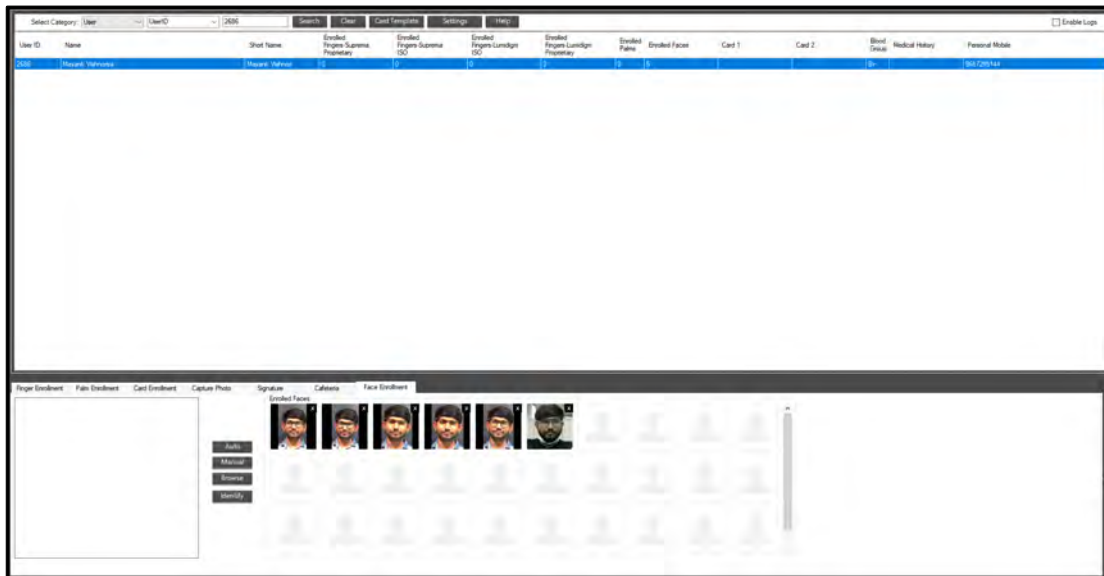


*Make sure the number of faces you consider for enrollment is lesser than or equal to the defined value in **Maximum No. of Faces** in Admin >System configuration> Global Policy >User.*

- If there is an occurrence of an adaptive face, it will be displayed under the **Adaptive Faces** grid, a sub-section under **Enrolled Faces** grid. If you desire, you may delete the image. To do so, follow the same instructions as mentioned above.
- Click the Save  in order to save all the enrolled faces. The faces will be successfully saved and considered for face recognition.

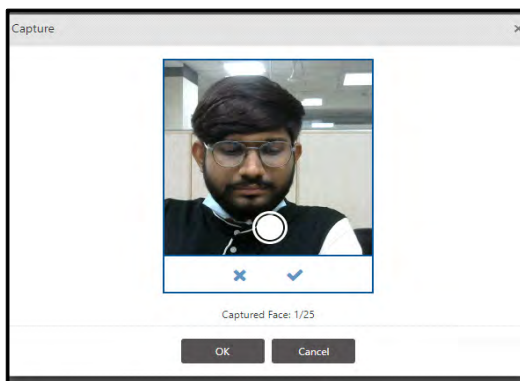


The enrolled faces of the user will be successfully reflected in the Enroll Utility under **Face Enrollment**. Refer the COSEC Enroll User Manual for more details.

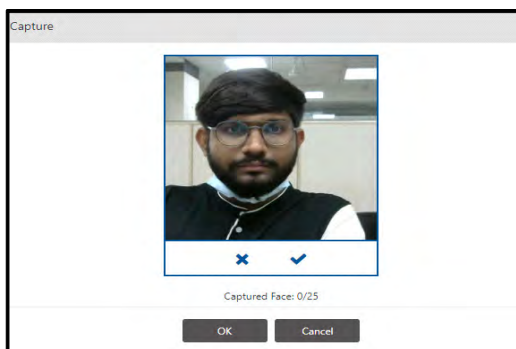




Capture

- In order to capture face/s, click **Capture** in Face Enrollment.
- The **Capture** pop-up will be displayed.



- Set the camera in a desired angle and capture the image.



- If the image captured is appropriate click the icon  . Now, you can again capture a new image if required.
- If the image clicked is not appropriate then click the icon  and a retake will be considered.
- After completing the capture, click **OK** to upload the image. Click **Cancel** if you desire to restart the **Capture**.
- The uploaded faces will be reflected in **Uploaded Faces** Grid.
- Now, refer to “[Upload](#)” for further instructions.

Worker Profile-Visitor Management

In this page you can authorize a host user, restrict the visitor pre-registration on the basis of no.of days and assign device groups and devices to the visitors.

Assign

- **Authorized Host User:** Select the checkbox to authorize a Host user. Once you authorize the host, the host user will be added in the list of Authorized Host Users in *Visitor Management> Utilities> Authorized Host Users*. For more information, refer [“Authorized Host Users”](#).

Visit Creation Restriction

- **Minimum Days before Allowing Creation:** The minimum days configured in *Admin> System Configuration> Global Policy> Visitor Management* will be displayed here as the default value.

You can change the number of minimum days as per your requirement.


For more details, refer [“Visit Creation Restriction”](#) in *Admin> System Configuration> Global Policy> Visitor Management*.

- **Maximum Days Before Allowing Creation:** The maximum days configured in *Admin> System Configuration> Global Policy> Visitor Management* will be displayed here as the default value.

You can change the number of maximum days as per your requirement.

For more details, refer [“Visit Creation Restriction”](#) in *Admin> System Configuration> Global Policy> Visitor Management*.

- **Device Group:** Select the desired device group/s from the picklist to assign it to the Visitor.
- **Device:** Select the desired device/s from the picklist.

To add devices which are assigned to the host, click **Add Host's Devices** .

Configure

This option enables the Admin to change the settings of the devices assigned to the Visitor.

To know more about the configurations, refer [“Configure”](#) in *User> User Configuration> Devices*.

Panel Door

Assign	Configure
Device	Panel
Type	Panel
Active	<input checked="" type="checkbox"/>
VIP	<input type="checkbox"/>
Access Profile	Access Group-1
Functional Group	Staff
Home Zone	Zone-1
Visit Zone	Select
Access Route	Select

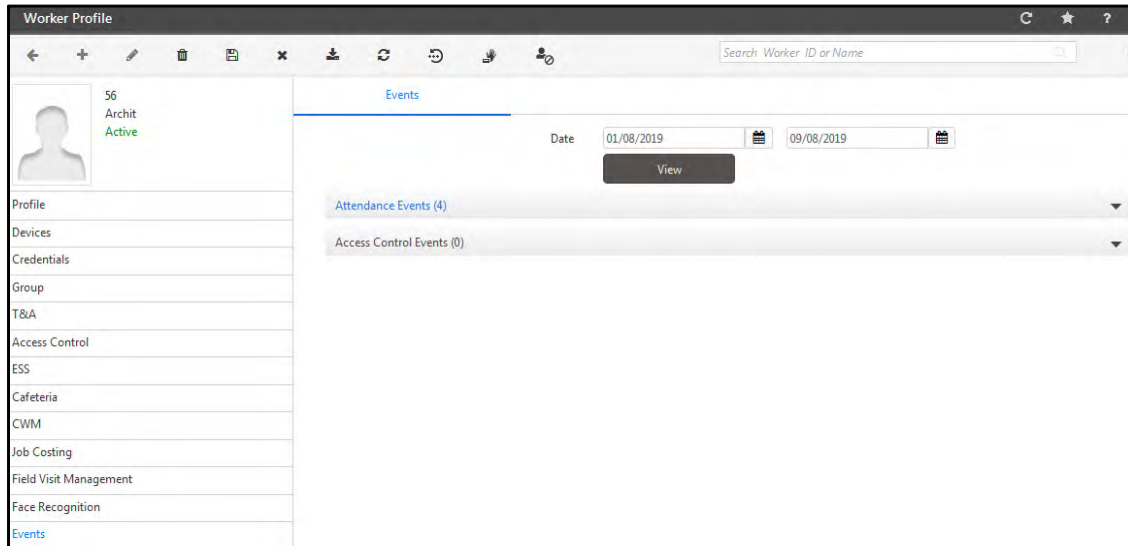
Direct Door

Configure	
Device	Argo Door
Type	ARGO
Active	<input checked="" type="checkbox"/>
VIP	<input type="checkbox"/>

Worker Profile-Events

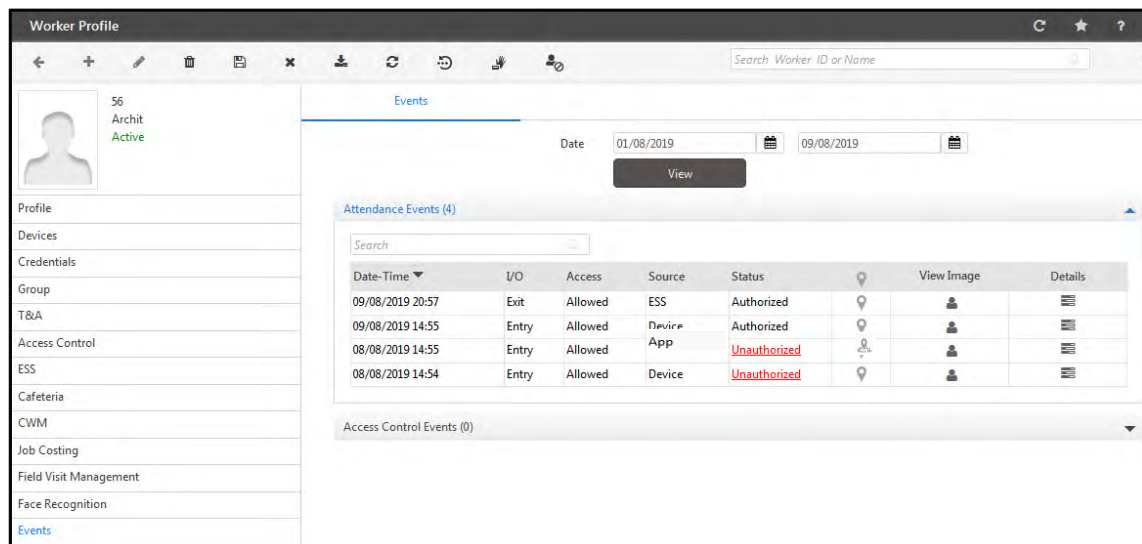
The Events tab is used for the security purpose by monitoring the workers in the organization. The Attendance Events and Access Control Events can be viewed by filtering the date range.

In cases of infringement or suspicion; the security supervisor can blacklist, delete or inactivate the worker creating problems in the organization. On selecting Events tab, the following page appears.



Date: Select the date range for which events are to be viewed.


Click on **View** button to view the Attendance events and Access Control events.



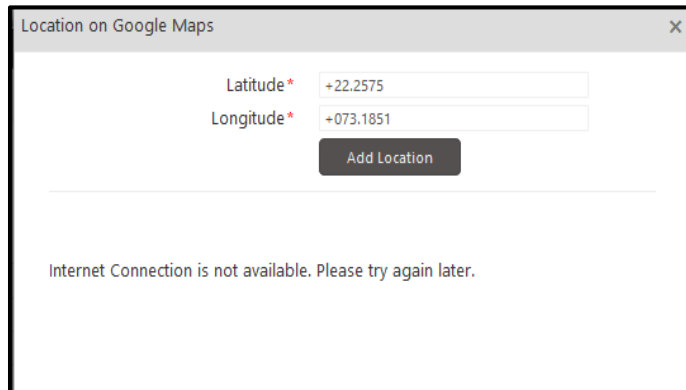
The Attendance Events shows the Date and time when the event is generated along with the I/O, Access, Source, Status and Location details. It also displays Image and Details of the punch.

The location details will display Latitude/Longitude or MAC address from where event has generated.

- You can view the location on Map if the GPS/GSM location is configured in Location Master by clicking on View Map icon.

- If the location is not configured in Location Master then you can add this location by clicking on **Add this Location**  icon shown in above figure.

Now click on **Add Location** button which will redirect to Location Master page from where you can add this location.



Location on Google Maps

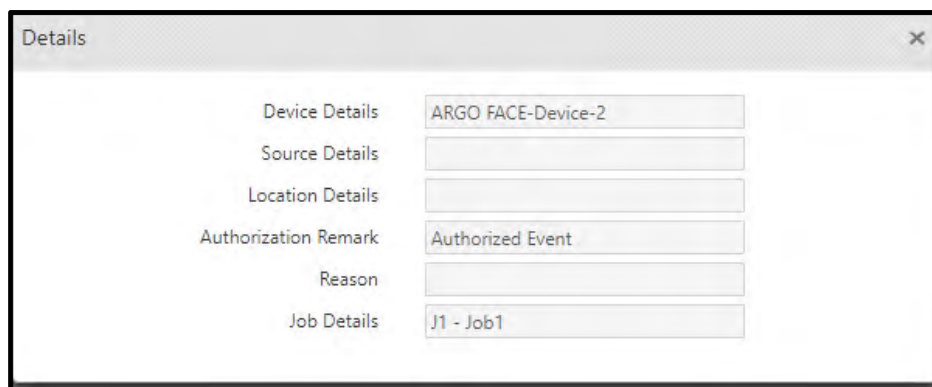
Latitude * +22.2575

Longitude * +073.1851

Add Location

Internet Connection is not available. Please try again later.

After the location is added, the location Name will be updated and map can be viewed by clicking **Details** as shown below.



Details

Device Details ARGO FACE-Device-2

Source Details

Location Details

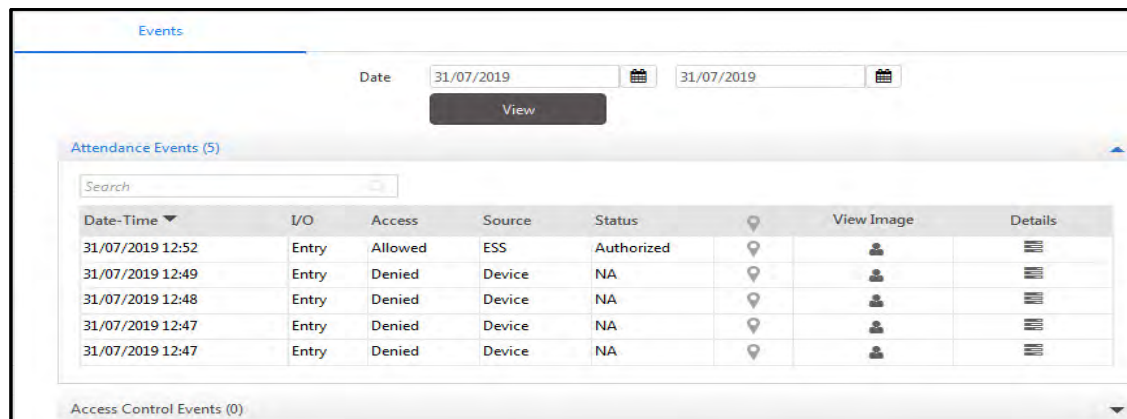
Authorization Remark Authorized Event

Reason

Job Details J1 - Job1

The Status of event, i.e. whether it is authorized or unauthorized is displayed under Status.

- If the status is Unauthorized, it will display a link which on clicking will be redirected to Events Authorization Page as per login user's rights.
- If the status is shown as NA, then Authorized status will be Null and the access will be shown as **Denied** as shown below:



Events

Date 31/07/2019 31/07/2019

View

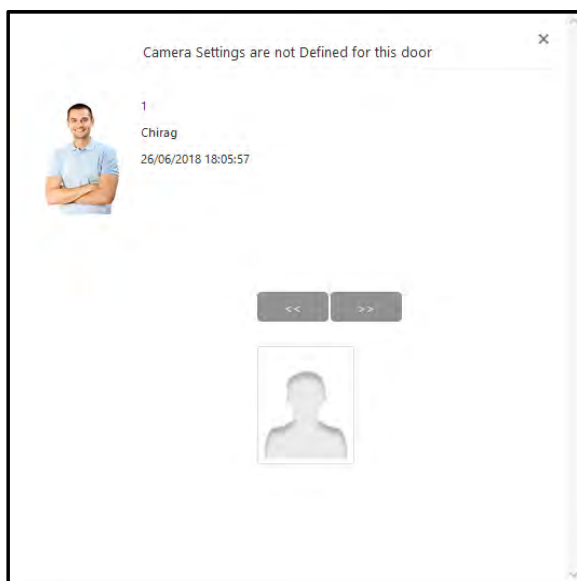
Attendance Events (5)

Date-Time	I/O	Access	Source	Status		View Image	Details
31/07/2019 12:52	Entry	Allowed	ESS	Authorized			
31/07/2019 12:49	Entry	Denied	Device	NA			
31/07/2019 12:48	Entry	Denied	Device	NA			
31/07/2019 12:47	Entry	Denied	Device	NA			
31/07/2019 12:47	Entry	Denied	Device	NA			


Access Control Events (0)

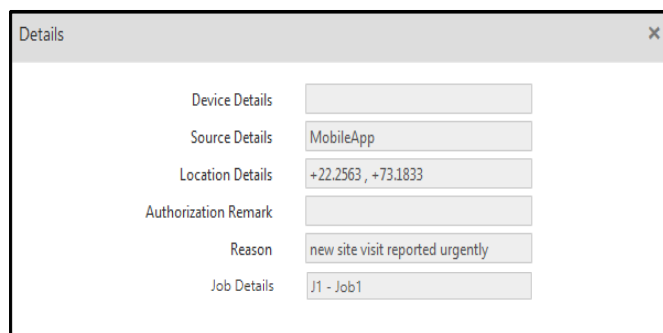
You can view the image captured by the Built-In Camera by clicking on **View Image** icon.

If there is camera to capture the image of the worker punching on door; then his image will be captured and can be viewed for that event by clicking on View Image icon.



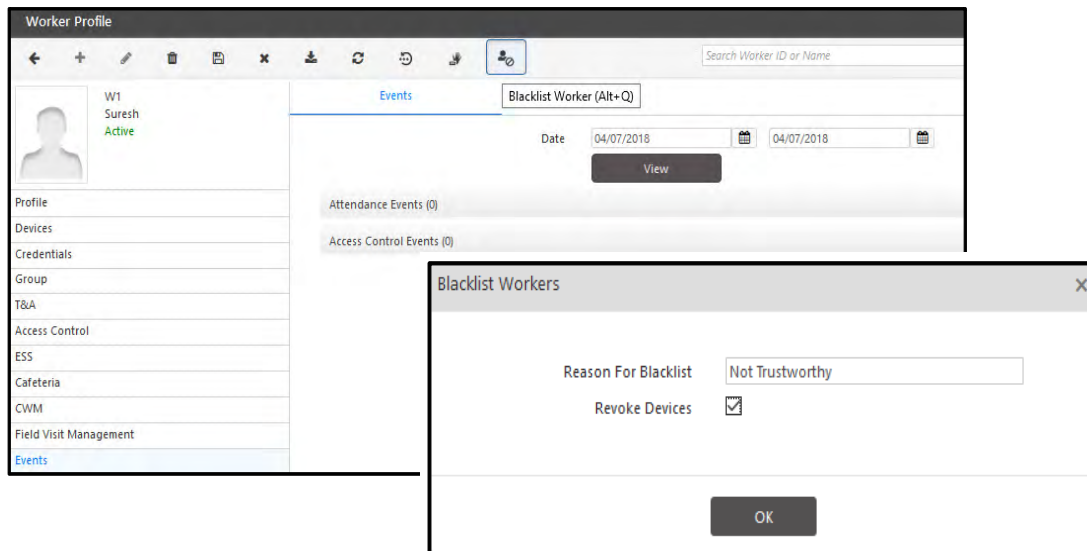
If the event is generated by API then there will not be any image popup window on clicking View Image icon.

The Reason for punching from unassigned location can be known by clicking on Details icon  as shown in the figure below:



Blacklist

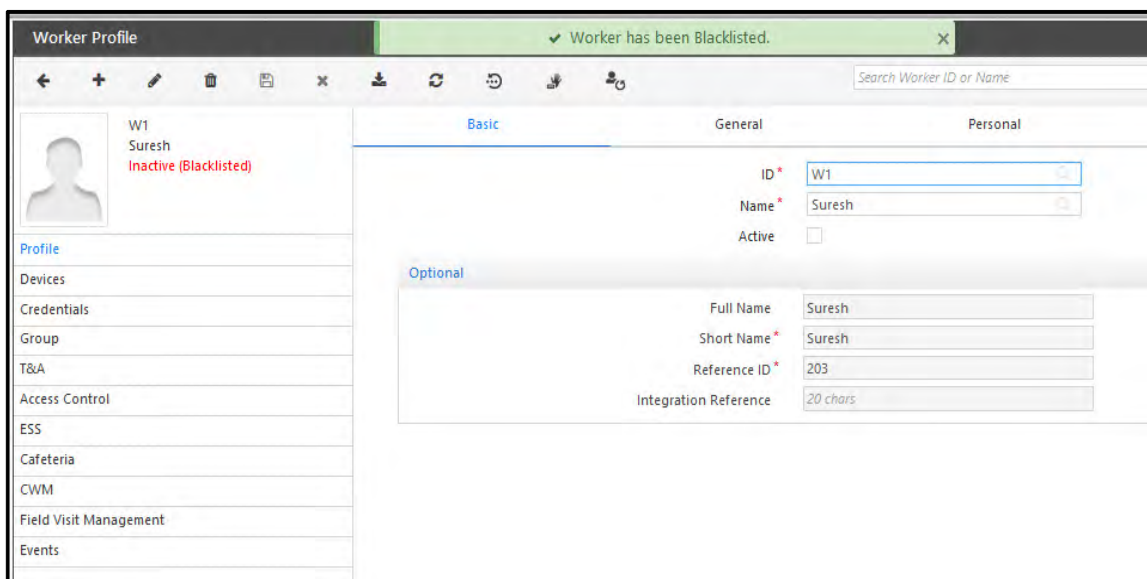
Click on the **Blacklist Worker** button. The Blacklist Workers window appears.



Enter the **Reason** for Blacklisting the worker.

Click on **Revoke Devices** to remove the assignment of devices from the worker.

Click **OK** and **Save** button to save the changes. The worker will be blacklisted and Inactive as shown below.



The blacklisted worker can be revoked by clicking **Restore and Activate Worker** button. It will make the worker active.

Worker Profile

←

+

Search Worker ID or Name

W1

Suresh

Inactive (Blacklisted)

Profile

Devices

Credentials

Group

T&A

Access Control

ESS

Cafeteria

CWM

Field Visit Management

Events

Basic

Restore and Activate Worker (Alt+Q)

Personal

ID *

W1

Name *

Suresh

Active

☐

Optional

Full Name

Suresh

Short Name *

Suresh

Reference ID *

203

Integration Reference

20 chars

Worker Assignment

Worker Assignment enables to assign worker to the work order and also view already assigned workers having assignment status as Approved and Pending. Workers can be assigned for as many number of days within the work order depending on the requirements of work order. Also workers can be un-assigned from the work order.

To assign the workers to the work order go to **Contract Worker Management > Workers > Worker Assignment**

The screenshot shows the 'Worker Assignment' window. On the left, there are input fields for 'Work Order' (ID, Name), 'Validity' (From, To), 'Contractor' (ID, Name), and 'Status'. Below these are three tabs: 'Current Assignment', 'Unregistered Workers', and 'Past Assignments'. On the right, there is a table with the following data:

ID	Work Order Name	Status	Current Assignment
WO6	Servicing	In Progress	0

Work order- Select the work order from the grid on the right or through the work order picklist. The **Validity, Contractor ID, Name** and **Status** of the selected work order are displayed in the respective fields.

The screenshot shows the 'Worker Assignment' window with the following data populated in the fields:

- Work Order: WO6, Servicing
- Validity: 04/27/2017, 05/24/2017
- Contractor: C01, HPCL
- Status: In Progress

The table on the right remains the same as in the previous screenshot.

Current Assignment

It displays already assigned workers to the selected work order. Further new workers can be assigned to the work order.





To assign the new workers for the selected work order, select the **worker** from the picklist. The worker with the assignment details will appear in the grid.

The screenshot shows the 'Current Assignment' window. It has an 'Assignment Period' field with dates 04/27/2017 and 05/24/2017. Below it is a 'Worker' section with a search bar and a table of assigned workers. The table has the following data:


ID	Worker Name	From	To	Assigned Days	Assignment Status
AP	Aakash	04/27/2017	04/28/2017	2	Approved
RG	Rutuja	04/27/2017	05/02/2017	28	Free

Below the table are three tabs: 'Unregistered Workers', 'Past Assignments', and 'Current Assignment'. An 'OK' button is located at the bottom right.

To change the assigned days click on **Edit** button. Then specify the from and to date. Then click on **OK** button.

Search <input type="text"/>						
ID ▲	Worker Name	From	To	Assigned Days	Assignment Status	
AP	Aakash	04/27/2017	04/28/2017	2	Approved	 
RG	Rutuja	04/27/2017	05/02/2017	6	Free	 

Click on **Save** button from the menu bar to save the assignment of worker to the work order.

Search <input type="text"/>						
ID ▲	Worker Name	From	To	Assigned Days	Assignment Status	
AP	Aakash	04/27/2017	04/28/2017	2	Approved	 
RG	Rutuja	04/27/2017	05/02/2017	6	Approved	 

Unregistered Workers

It displays the total count of (Unregistered + pending) workers who were added by contractor and are in pending stage.

Current Assignment <input type="text"/>						
Unregistered Workers <input type="text"/>						
Search <input type="text"/>						
ID ▲	Worker Name	From	To	Assigned Days	Assignment Status	
2	Dinesh	04/27/2017	04/29/2017	3	Pending	
Past Assignments <input type="text"/>						

The **Past Assignments** tab shows the workers who were previously assigned the selected work order.

Past Assignments <input type="text"/>						
Search <input type="text"/>						
ID ▲	Worker Name	From	To	Assigned Days	Assignment Status	
AP	Aakash	04/27/2017	04/27/2017	1	Approved	

If some work order's validity is over and contractor or site in-charge forgot to extend its validity, in such cases it might be required to create a new work order and assign same workers to this work order. Also it can be required to assign same workers to some similar work order.

So You can click **Copy Workers from** icon and select the workers from the expired work orders to be assigned to the current work order as shown below.

The screenshot shows the 'Worker Assignment' window. In the toolbar, the 'Copy Workers from' icon (a document with a plus sign) is highlighted with a red box. Below the toolbar, the 'Work Order' is 'WO6', 'Servicing' is selected, 'Validity' is '04/27/2017' to '05/24/2017', 'Contractor' is 'C01', 'HPCL', and 'Status' is 'In Progress'. On the right, a table shows the current assignment:

ID	Work Order Name	Status	Current Assignment
WO6	Servicing	In Progress	1

The screenshot shows the 'Copy Workers From' dialog box. It has a 'Work Order' field with 'WO4' and a dropdown menu with 'Electrical design'. Below this, it says '1 Selected'. A table lists workers:

Worker ID	Name
<input checked="" type="checkbox"/> CWM2	Amit
<input type="checkbox"/> CWM3	Aakash

An 'Ok' button is at the bottom right.

The selection will be updated in the Current Assignment from where the days can be assigned to the worker.



Work Orders having status as “In Progress” or “Open” can be assigned workers from some “Closed” work order having same contractor.

*While creating a work order, enable the **Check Limit While Assigning Worker**, so while assigning a work order to any of the worker, Max Worker Limit and Skill-Wise Worker Limit will be checked.*

Enrollment

The COSEC Access Control System supports enrollment of worker cards, finger print templates, palm templates and special cards. The enrollment process can be initiated from the COSEC application or from the Door Controller by using special cards or Menu.

To enroll the worker credentials, select **Contract Worker Management > Workers > Enrollment**

The screenshot shows the 'Enrollment' window. On the left is a sidebar menu under 'Contract Worker Management' with items: Contractor, Work Order, Workers, Skills, Personal Protective Equipment, Worker List, Worker Profile, Worker Assignment, Enrollment (selected), Utilities, Authorization/Approval, and Reports. The main area contains the following fields:

- Door*: ID (text input), Name (text input)
- Device Readers (dropdown menu)
- Worker*: ID (text input), Name (text input)
- Worker Enrollment Status (dropdown menu)
- Enrollment Type: Select (dropdown menu)
- Number of Cards: One (dropdown menu)
- Number of Fingers: One (dropdown menu)
- Number of Palms: Two (dropdown menu)
- Access Card Selection: Access Card 1 (dropdown menu)
- Number of Faces: 1 (text input)
- Enroll (button)

- **Door:** Select the desired door from the pick list on which the enrollment is to done.

Device Readers

Device Readers displays the information of the readers configured in the selected **Door**.

The screenshot shows the 'Device Readers' section of the Enrollment form. At the top, the Door* field is set to 3 and the Name field is set to ARGO. Below this is a table with the following data:

Device Readers	
Card Reader	MiFare Reader
Biometric Reader	None
External Reader	MiFare-U Reader

Card Reader, Biometric Reader and External Reader information are displayed here.

- **Worker:** Select the desired worker from the picklist for whom the enrollment is to be done.

Worker Enrollment Status

Worker Enrollment Status displays the information related to the number of already enrolled credentials of the worker like fingers, palms, cards and faces.

Details like — **Enrolled Fingers (Suprema Proprietary)**, **Enrolled Fingers (Suprema ISO)**, **Enrolled Fingers (Lumidigm ISO)**, **Enrolled Fingers (Lumidigm Proprietary)**, **Enrolled Palms**, **Enrolled Card 1**, **Enrolled Card 2** and **Enrolled Faces** — are displayed here.

- **Enrollment Type:** Select the desired enrollment type — **Read Only Card**, **Smart Card**, **Face**, **Biometrics**, **BiometricsThenCard**, **Mobile** or **Duress Finger** — from the drop down list.

Based on the selection of the **Door** and **Enrollment Type**, below parameters will be displayed for configuration.



When Enrollment Type selected is Smart card or BiometricThenCard, Duress Finger Templates will not be written in the Smart Card.

Below parameters also depend on the Readers configured in the Door. To configure the desired Reader, refer Readers section under Devices > Device Configuration (of the desired Door) > Profile > Readers.

1. Enrollment Type = Read Only Card

Number of Cards: Select the desired number of cards from the drop down list.

2. Enrollment Type = Smart Card

Number of Cards: Select the desired number of cards from the drop down list.

Details on Smart Card

Select the desired check boxes of the parameters — **Worker ID**, **Facility Code (FC)**, **Additional Security Code (ASC)** — which are to be displayed on the Smart Card.

Select the desired number of **Finger Templates** from the drop down list.

If **Door** is selected as PVR Door, **Palm Templates** parameter will be visible. Select the check box of this parameter if you wish to display it on the Smart Card.

To store the palm templates, MiFare 4k reader must be configured in the PVR Door.



Door PVR must be set in the Adaptive mode (configure from Admin> System Configuration> Global Policy) for the palm templates to be saved into the Smart Card.

Additional Details on Smart Card

Other than the parameters mentioned in the Details on Smart Card, you can display additional details on Smart Card.

Select the desired check boxes of the parameters — **Short Name**, **Branch**, **Department**, **Designation**, **Emergency Contact**, **Blood Group** and **Medical History**— which are to be displayed on the Smart Card.

The values of these additional details are displayed as well. Make sure the values of these additional details are not blank for successful enrollment process.

3. Enrollment Type = Face

Number of Faces: Select the desired number of face from the dropdown list.

Enrollment Type	Face
Number of Faces	1

4. **Enrollment Type** = Biometrics

Number of Fingers/ Number of Palms: Select the desired number of fingers or palms from the drop down list.

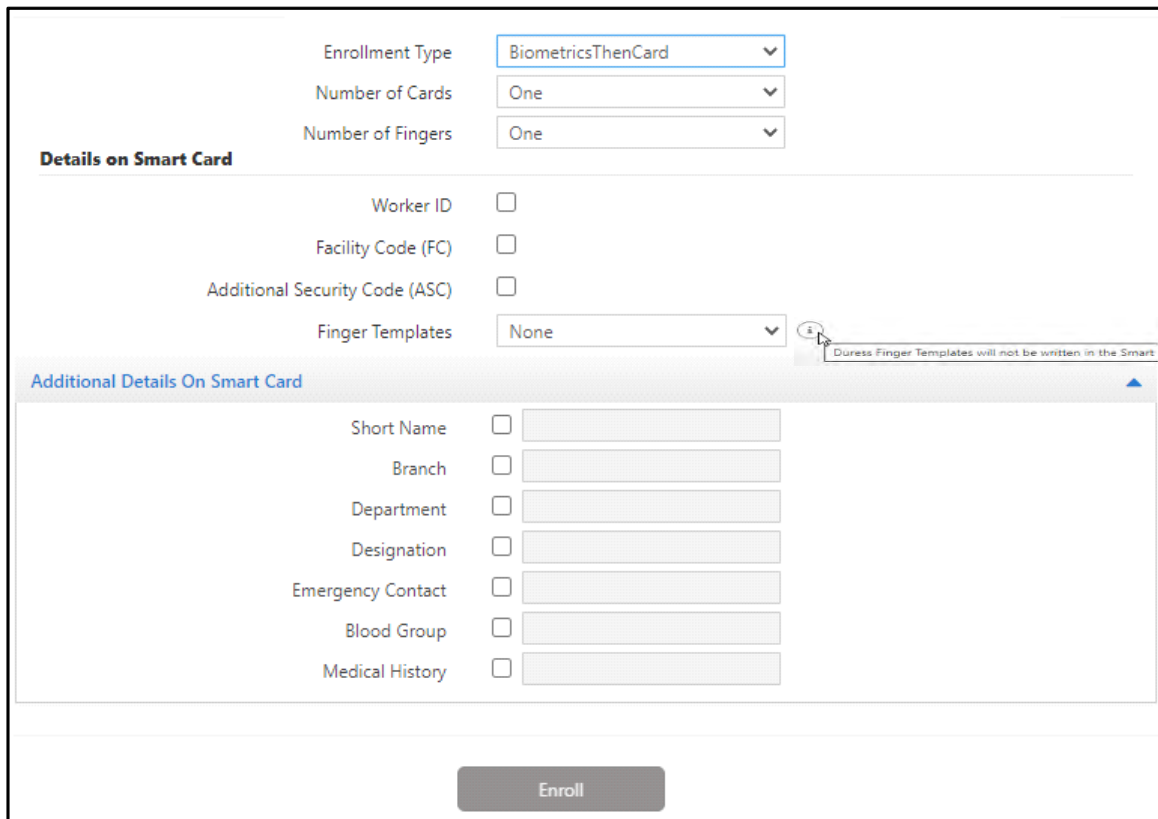
Enrollment Type	Biometrics
Number of Fingers	One

Enrollment Type	Biometrics
Number of Palms	One

5. **Enrollment Type** = BiometricsThenCard

Number of Cards: Select the desired number of cards from the drop down list.

Number of Fingers/ Number of Palms: Select the desired number of fingers or palms from the drop down list.



The screenshot shows a web-based enrollment form. At the top, there are three dropdown menus: 'Enrollment Type' set to 'BiometricsThenCard', 'Number of Cards' set to 'One', and 'Number of Fingers' set to 'One'. Below these is a section titled 'Details on Smart Card' containing four checkboxes: 'Worker ID', 'Facility Code (FC)', 'Additional Security Code (ASC)', and 'Finger Templates' (which is currently set to 'None' in a dropdown). A tooltip points to the 'Finger Templates' dropdown with the text 'Duress Finger Templates will not be written in the Smart Card'. Below this is a section titled 'Additional Details On Smart Card' with a blue header and a collapse arrow. It contains seven rows, each with a checkbox and a text input field: 'Short Name', 'Branch', 'Department', 'Designation', 'Emergency Contact', 'Blood Group', and 'Medical History'. At the bottom center is a grey 'Enroll' button.

Details on Smart Card

Select the desired check boxes of the parameters — **Worker ID**, **Facility Code (FC)**, **Additional Security Code (ASC)** — which are to be displayed on the Smart Card.

Select the desired number of **Finger Templates** from the drop down list.

If the **Door** is selected as PVR Door, **Palm Templates** parameter will be visible. Select the check box of this parameter if you wish to display it on the Smart Card.

To store palm templates, MiFare 4k reader must be configured in the PVR Door.



Door PVR must be set in the Adaptive mode (configure from Admin> System Configuration> Global Policy) for the palm templates to be saved into the Smart Card.

Additional Details on Smart Card

Other than the parameters mentioned in the Details on Smart Card, you can display additional details on Smart Card.

Select the desired check boxes of the parameters — **Short Name**, **Branch**, **Department**, **Designation**, **Emergency Contact**, **Blood Group** and **Medical History**— which are to be displayed on the Smart Card.

The values of these additional details are displayed as well. Make sure the values of these additional details are not blank for successful enrollment process.

6. Enrollment Type = Mobile



To select **Enrollment Type** as **Mobile**, the particular device must have BLE support and ensure Bluetooth is ON in the mobile.

Access Card Selection: Select the desired Access Card from the drop down list.

Enrollment Type: Mobile
Access Card Selection: Access Card 1
Facility Code (FC): ☐

Facility Code (FC): Select this check box to enroll the Facility Code (FC) against the worker.

7. Enrollment Type = Duress Finger

Number of Fingers: Select the desired number of fingers that you want to enroll as **Duress Finger** from the drop-down list— **One** or **Two**.

Click **Enroll** to initiate the enrollment process.

After the enrollment process, the worker must tap on **Tap to Register > Matrix Device** from the ACS Application installed on respective mobile phone and select the same configured Door from **Available Doors**. Thereafter, that worker can access the device through ACS application for Access Control purpose.

The value in Access Card selected will be consider as Access ID of the worker. If Access Card selected has no value i.e blank, then after the enrollment process, the system will auto-generate 18 digits number as worker Access ID and store the same value.

Click **Enroll** to initiate the enrollment process and the enrollment command is sent to the Door.

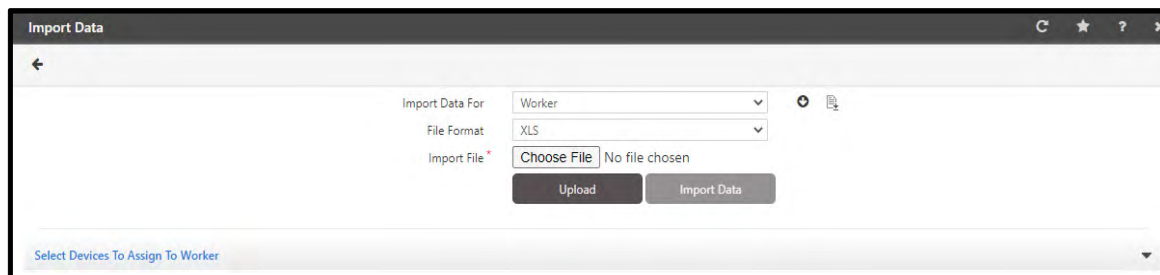
For Panel Door the command is sent to the Panel200 which will communicate further to the Door.

Once all the required credentials of an worker are enrolled, the number of credentials enrolled will be displayed in the Contract Worker Management > *Workers*> *Worker Profile* > *Credentials*.


Import Workers

The *Import Workers* utility helps in manually sending information about workers to selected devices. The data is sent in Excel or CSV file formats. The information to be sent can be previewed before actually importing it to device. Also, there is a provision to make multiple entries of workers at once.

To import worker's information to devices go to **Contract Worker Management > Utilities > Import Workers**.




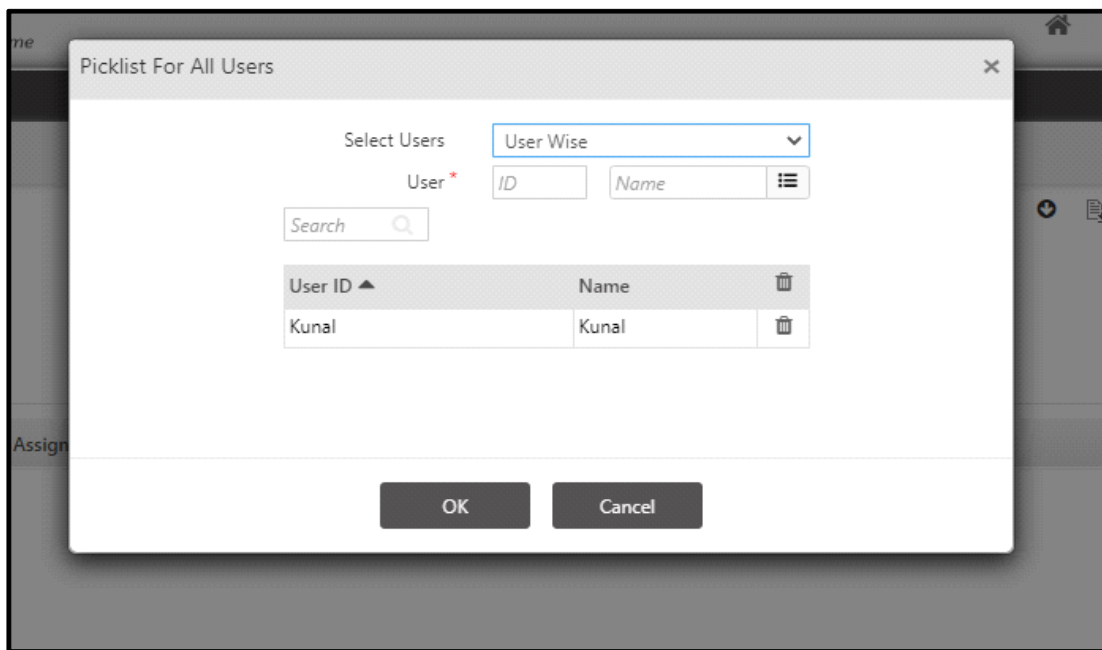
Configure the following parameters:

- **Import Data For** - Select the option from the drop-down list for which the data is to be imported. You can download sample import file by clicking on **Download Sample Import file**  button. The import sheet displays the fields required for importing specific data.

The mandatory fields list is given in **Document guidelines** section of Import sheet.

	BG	BH	BI	BJ	BK	BL	BM	BN	BO	BP	BQ	BR	BS	BT	BU	BV
1	SkillID	ContractorID	WorkOrderID	StartDate	EndDate	WeekOffGroupID	Field1	Field2	Field3	Field4	Field5	Field6	Field7	Field8	Field9	Field10
2	11	45	1	21/1/2020	2/2/2020											
3	23	564	2	28/1/2020	3/2/2020											
4	32	6556	3	25/1/2020	5/2/2020											
5	34	56	4	11/1/2020	4/2/2020											

To download detailed sheet, click on **Download Detailed Data Sheet**  button. On clicking this button, a pop-up will be displayed as shown below:

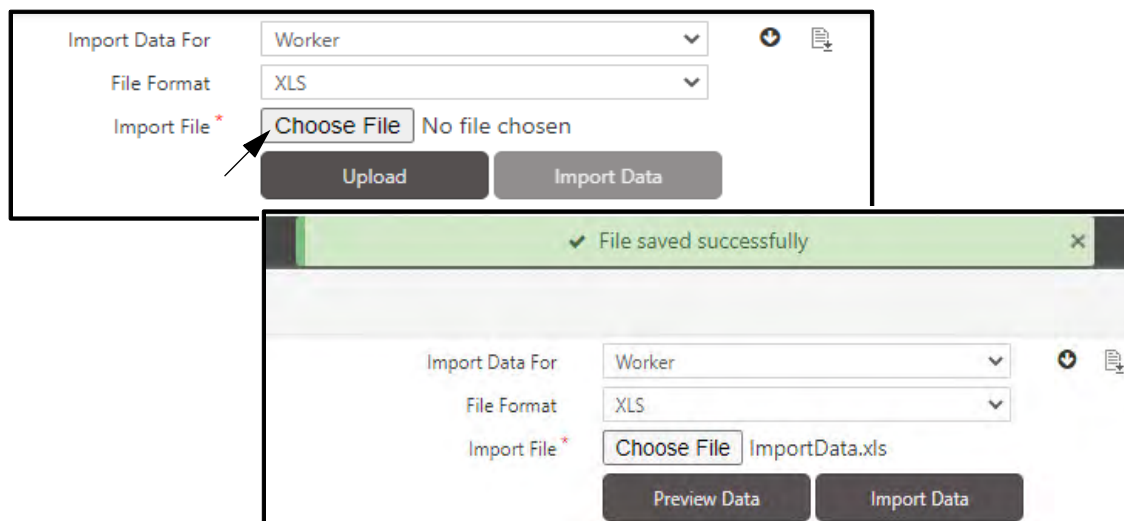


Select Users: Select the desired option — User Wise, Group Wise or All. If you select User Wise or Group Wise the select the desired users/groups from the picklist.

Click **OK** button to download the Data Sheet or click on **Cancel** button to abort the process.

The Detailed Data Sheet will be as per the selected option.

- **File Format** - Select the file format of the specific file from the drop-down list. The options available are XLS or CSV.
- **Import File** - Browse the path of the file from which the data is to be imported.



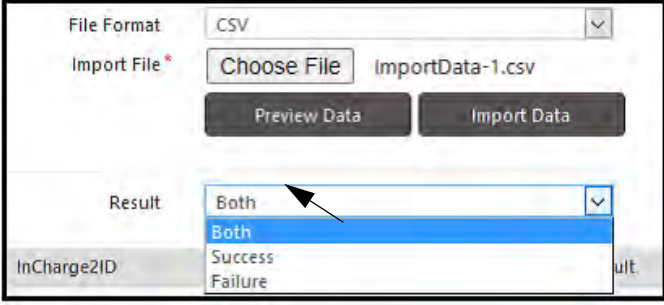
Click on **Upload** to save the file.

Click on **Preview Data** button to view the data in the respective worksheets to confirm that the data is in order prior to giving the import command.

Now click on **Import Data** to start importing the uploaded data. The result of import is shown as Success or Failure along with result description.

Select the **devices** to be assigned to the workers by checking the boxes against the relevant devices and click on **Import Data**. The system will import all the relevant valid entries from the sheet and will display the status in the bottom grid.

You can also filter import result records on the basis of their Success, Failure or Both using the **Result** drop-down options.



The screenshot shows a web interface for importing data. At the top, there is a 'File Format' dropdown set to 'CSV'. Below it, the 'Import File' section shows a 'Choose File' button and the filename 'ImportData-1.csv'. There are two buttons: 'Preview Data' and 'Import Data'. Below these, the 'Result' dropdown menu is open, showing three options: 'Both' (highlighted with a blue background), 'Success', and 'Failure'. An arrow points to the 'Both' option. At the bottom left, the text 'InCharge2ID' is visible.

Once the data is imported successfully, data will be added or updated in Worker Profile in COSEC Web.

Blacklist

This feature is used to blacklist workers and contractors. Blacklisting will ensure that contractor/worker is not assigned any work order.

To blacklist the workers go to **Contract Worker Management >Utilities > Blacklist**

The screenshot shows the 'Blacklist' application window. At the top, there are input fields for 'Blacklist' (a dropdown menu set to 'Worker'), 'Worker' (with 'ID' and 'Name' sub-inputs), and 'Reason' (a text box containing '50 Char'). Below these is a 'Search' button. A table with columns 'ID' and 'Name' is shown, but it contains no data. Below the table is an 'Add To Blacklist' button. Further down, there is a section for 'Blacklisted Workers (0)' with a search bar and a table with columns: 'Worker ID', 'Name', 'Blacklist Date-Time', 'Contractor', 'Reason For Blacklisting', and 'Restore'. This table also shows no data. At the bottom, there is a section for 'Restored Workers (0)'.

Blacklist- Select the option of workers or contractors to be blacklisted from drop down list.

Worker/Contractor- As per the blacklist selection, select the worker or contractor from the picklist.

Reason- Specify the reason for blacklisting the selected worker/contractor.

This screenshot shows the same interface as the previous one, but with a worker selected. The 'Blacklist' dropdown is still 'Worker'. The 'Worker' section now has 'ID' set to 'AP' and 'Name' set to 'Aakash'. The 'Reason' text box now contains 'Caught stealing company property'. The table below now has one entry with 'ID' 'AP' and 'Name' 'Aakash'. An arrow points to the 'Add To Blacklist' button.

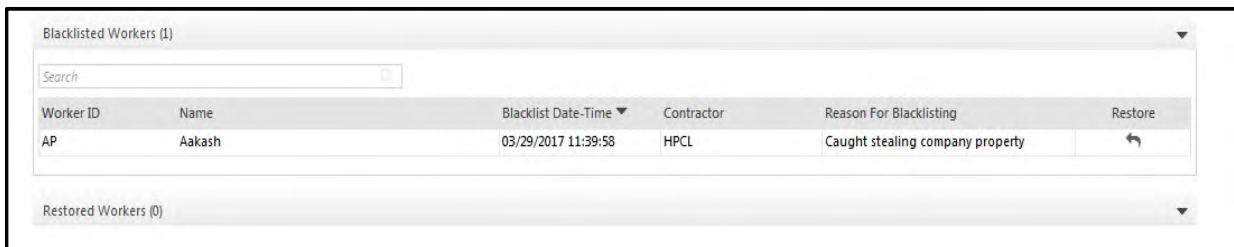
Click on **Add To Blacklist** button to blacklist the worker/contractor. A warning appears.


A warning dialog box with the title 'Warning' and a close button (X). The text inside asks: 'Would you like to revoke devices (as per device-wise rights)?'. At the bottom, there are two buttons: 'Yes' and 'No'.

If you select **Yes**, then worker/contractor will become inactive and worker's/contractor's data will be removed from the devices.

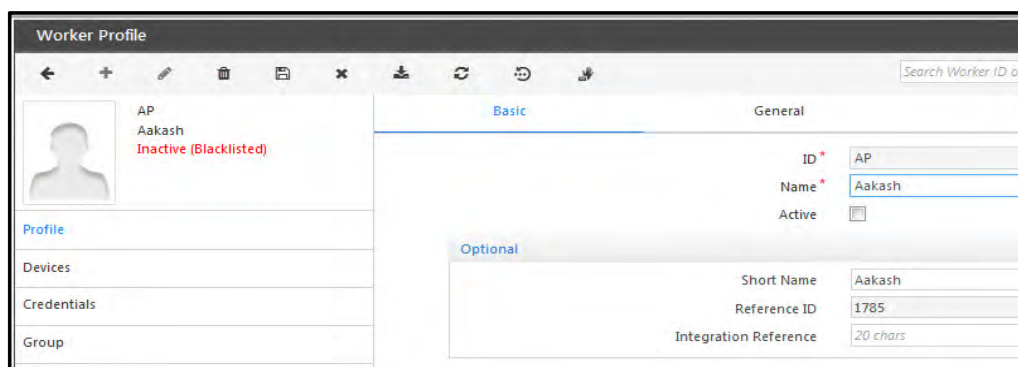
If you select **No**, then worker/contractor will become inactive but worker's/contractor's data will still be there on assigned devices.

The worker/contractor will get listed in Blacklisted Workers/Contractors section.



Worker ID	Name	Blacklist Date-Time	Contractor	Reason For Blacklisting	Restore
AP	Aakash	03/29/2017 11:39:58	HPCL	Caught stealing company property	

The blacklisted worker/contractor will be made inactive in the system.



Worker Profile


AP
Aakash
Inactive (Blacklisted)

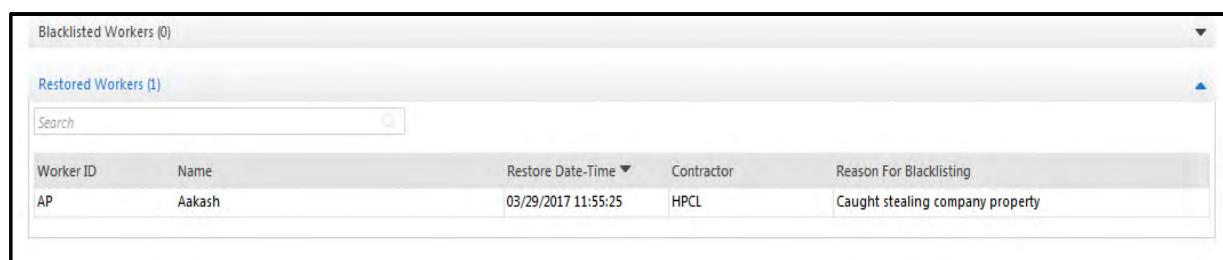
Basic

ID * AP
Name * Aakash
Active ☐

Optional

Short Name Aakash
Reference ID 1785
Integration Reference 20 chars

The blacklisted worker/contractor can be restored by clicking the **Restore**  button on the blacklisted workers/contractors grid. The restored worker/contractor will now be listed under the Restored Workers/Contractors tab.




Worker ID	Name	Restore Date-Time	Contractor	Reason For Blacklisting
AP	Aakash	03/29/2017 11:55:25	HPCL	Caught stealing company property




A Contractor cannot be blacklisted by the administrator in the following conditions:

- Any worker associated with the Contractor has a Pending status for work order assignment.
- Any associated work order is still in Progress (i.e. All work orders must be terminated).

After Restoring the worker, you have to activate the inactive worker by enabling the **Active** checkbox as shown below.

	AP Aakash Inactive
Profile	
Devices	
Credentials	
Group	

Then click **Save** button to save the changes.



AP

Aakash

Active

[Profile](#)

[Devices](#)

[Credentials](#)

[Group](#)

Manage Workers

The manage workers utility is used to change contractor, work order and assignment period for the selected workers.

To manage the workers go to **Contract Worker Management >Utilities >Manage Workers**

The screenshot shows the 'Manage Workers' window with the following search filters: Contractor (empty), Worker Assignment Status (Approved), and Work Order (empty). A 'View' button is located below the filters. The table below the filters is empty, displaying a red message 'No Record Found'.

<input type="checkbox"/>	Worker ID	Name	Contractor	Work Order	Update	Assignment Start Date	Assignment End Date
No Record Found							

Select a Contractor and Work Order from the respective picklists to view all associated workers. Use the **Worker Assignment Status** dropdown list to filter workers based on their assignment status.

The screenshot shows the 'Manage Workers' window with the following search filters: Contractor (C109), Worker Assignment Status (Approved), and Work Order (W05). A 'View' button is located below the filters. The table below the filters displays three workers.

<input type="checkbox"/>	Worker ID	Name	Contractor	Work Order	Update	Assignment Start Date	Assignment End Date
<input type="checkbox"/>	CWM31	Ranjan Parmar	Aggrawal Bros	Annual Lift Servicing		13/08/2014	31/12/2015
<input type="checkbox"/>	CWM32	Anil Aggarwal	Aggrawal Bros	Annual Lift Servicing		13/08/2014	31/12/2015
<input type="checkbox"/>	CWM35	Ramesh Pai	Aggrawal Bros	Annual Lift Servicing		13/08/2014	31/12/2015

Click the **Update** button against a worker to change his assignment. To apply changes to multiple workers, select workers using the checkboxes provided on the grid.

The screenshot shows the 'Assignment Changes' dialog box with the following fields: New Contractor (C101), New Work Order (W02), Validity (31/08/2014 to 31/12/2014), and Assignment Period (31/08/2014 to 31/12/2014). The 'Advanced Options' section is expanded, showing 'Apply Changes To' (Individual) and 'Update' and 'Close' buttons.

Apply Changes To:

Update Close

In the **Assignment Changes** pop up window, change the contractor, work order and assignment period as required. Specify whether the changes are to be applied to the individual worker, the selected workers or all the workers in the grid.



*To change only the assignment period for a worker, select the existing Contractor and Work Order in the **New Contractor** and **New Work Order** fields respectively.*

Click the **Update** button to update the assignment of new contractor, work order and period to the selected worker/workers. Once updated, the worker will be removed from the grid.

Work Order Progress

This utility helps in viewing the progress of all work orders as well as work orders specific to a selected contractor. On selection of a contractor, associated work orders and their details can be filtered based on their progress status.

To view the work order progress go to **Contract Worker Management >Utilities >Work Order Progress**

The screenshot shows the 'Work Order Progress' window. It features a filter section with three dropdown menus: 'Filter Contractors' set to 'Individual', 'Contractor' with 'C01' selected and 'HPCL' in a picklist, and 'Work Order Status' set to 'All'. A 'View' button is located below these filters.

Filter Contractors- Select the contractors from the option of All and Individual.

Contractor- The individual contractor can be selected from the picklist.

Work Order Status- Select the work order status from the options of *All*, *Closed*, *In Progress* and *Open* from the drop down list.

View- Click the **View** button. The details of work orders and their status are displayed in the grid as shown below.

The screenshot shows the 'Work Order Progress' window with the 'View' button clicked. Below the filter section is a search bar and a table displaying work order details. The table has columns for Work Order ID, Name, Contractor Name, Defined Start Date, Defined End Date, Worker Limit, Assigned Workers, Man Days, and Progress Status.

Work Order ID	Name	Contractor Name	Defined Start Date	Defined End Date	Worker Limit	Assigned Workers	Man Days	Progress Status
WO1	Plastering	HPCL	03/01/2017	03/15/2017	5	0	0	Closed
WO2	Floor Maintenance	HPCL	03/03/2017	03/03/2017	2	0	0	Closed
WO3	Wall Painting	HPCL	03/03/2017	03/03/2017	1	0	0	Closed
WO4	Designing	HPCL	03/16/2017	03/31/2017	2	1	0	Closed
WO5	Electrical Maintenance	HPCL	03/17/2017	03/31/2017	2	0	0	Closed
WO6	Servicing	HPCL	04/27/2017	05/24/2017	2	2	0.0	In Progress

Work Order Progress Grid

- **Defined Start Date** reflects start date of work order.
- **Defined End Date** reflects end date of work order.
- **Worker Limit** reflects the maximum worker limit as defined in the Work Order section.
- **Assigned Workers** reflect the workers which are in approved or in pending state.
- **Man Days** reflects number of days spent by workers for the work order. Suppose 10 workers worked for 10 days each, Man Days= 10*10 = 100 Man Days.

- **Progress Status** in grid reflects whether work order has started or not and if started then whether it has completed or not.
 - **In Progress** status reflects that work order has started but not completed yet.
 - **Closed** status reflects that work order has started and completed.
 - **Open** status reflects that work order has not started yet.

Induction Approval

The Induction Approval is used to view all pending, approved and rejected applications sent for approval for each induction level assigned to worker for the assigned work order. SA has rights to approve or reject a pending application.

If some worker needs to complete 5 induction levels and is rejected in even 1 of them then worker's assignment status will turn into Rejected and approval in other induction level will no longer be required.

To authorize the workers go to **Contract Worker Management > Authorization/Approval > Induction Approval**

Worker ID	Name	Application Date	Induction Level	Contractor	Work Order	Approve	Reject	Remark	Details
1	Dinesh	04/07/2018	Induction Level-1	HPCL	Servicing	<input type="checkbox"/>	<input type="checkbox"/>		
2	Ramesh	04/07/2018	Induction Level-1	HPCL	Servicing	<input type="checkbox"/>	<input type="checkbox"/>		



If global policy is set to direct authorization, induction level for workers will remain blank in such cases.

Filter Work Orders- Select the work orders from the option of All and Individual.

Work Order- The individual work order can be selected from the picklist.

View- Click on View button. The pending, approved and rejected work orders are displayed in the respective grids along with the available counts.

The worker details from the grid can be viewed by clicking on the **Details** button. The worker details pop window is displayed as shown below:

Worker ID	2	
Name	Ramesh	
Induction Level	1	Induction Level-1
Work Order	W02	Servicing
Application Date	04/07/2018	

General

Personal

Contact

Worker Details


Worker ID	w1
Name	Rohit
Induction Level	
Work Order	W01
	Plastering
Application Date	14/05/2019

General

Date Of Birth
Vehicle Registration No.

Driving License
Driving License Expiry
Passport No.
Passport Expiry
PAN

Driving License



The documents of the worker can be viewed by clicking the Preview document button. This will ensure the credibility of the worker.

After the verification of worker; the verdict can be given by checking the Approve or Reject check box along with Remark as shown below.

Induction Approval

Filter Work Orders

All

Work Order

ID

Name

View

Pending (2)

Search

Worker ID	Name	Application Date	Induction Level	Contractor	Work Order	Approve	Reject	Remark	Details
1	Dinesh	04/07/2018	Induction Level-1	HPCL	Servicing	<input type="checkbox"/>	<input type="checkbox"/>	Approved Induction Level	
2	Ramesh	04/07/2018	Induction Level-1	HPCL	Servicing	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Induction Level	

Approved (0)

Rejected (0)

Click on **Save** button to save the verdict. The authorized application will then move to Approved or Rejected section.

Pending (1)

Approved (1)

Search

Worker ID	Name	Application Date	Induction Level	Contractor	Work Order	Remark	Details
CWM1	Ramesh	04/07/2018	Induction Level-1	HPCL	Servicing	Approved Induction Level	

Rejected (0)

CWM Reports

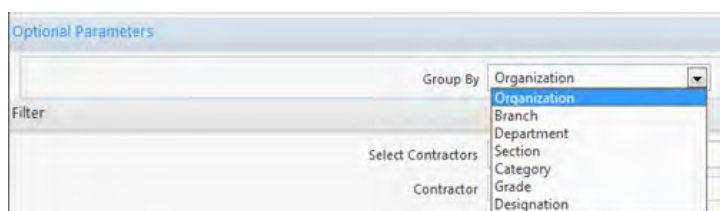
These reports can be obtained using the **Reports** section under the **Contract Worker Management** add-on module. The Reports can be categorized as follows:

- “Worker Details”
- “Contractor Details”
- “Work Order Details”
- “Blacklisted Workers”
- “Work Order Man Days”
- “Daily Head Count”
- “Daily Work Hours”
- “Status Summary”
- “Attendance Details”

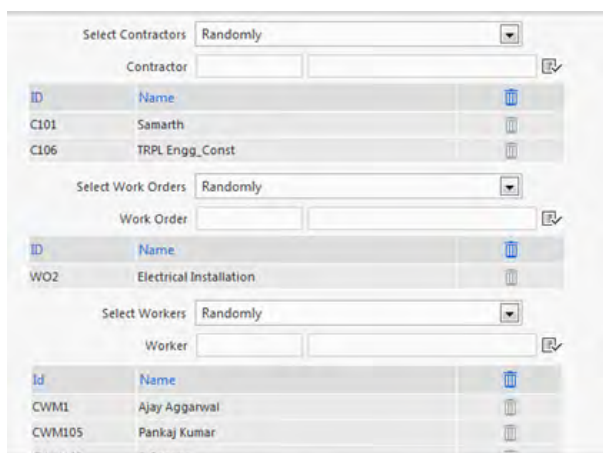
Worker Details

Worker Details Report provides the workers basic details against respective work order and contractor.

There is optional parameter where the **Group By** filter can be selected.



Select the Contractors, Work Orders and Workers from the options of **all** and **randomly** as shown below. And then Click on Generate Report.



The worker details report for the above selection is as shown below.

Worker Details

←

Back

Find... 1 of 1 100%

Main Report

ORGANISATION 1. Page 1 of 1

Organization-Wise Worker Details

Run by: System Admin Date: 17/10/2014 13:10

Samarth
Electrical Installation
ORGANISATION 1.

Worker ID	: CWM2	Name	: Mangesh Yadav
Gender	: Male	Qualification	:
Birth Date	:	Skill	: Electrician
Blood Group	: NA	Nationality	:
PF No	:	ESI No	:
Approved Mobile	:	Phone	:

Contractor Details

Contractor Details Report provides the basic details of respective contractor.

Select the Contractors from the options of **all** and **randomly** as shown below. And then Click on Generate Report.

Select Contractors Randomly

Contractor

ID	Name	
LAN	LANCO	
LT1	LandT	

Generate Report

The contractor details report for the above selection is as shown below.

Contractor Details

←

Back

Find... 1 of 1 100%

Main Report

Organization 2 Page 1 of 1

Contractor Details

Run by: System Admin Date: 2014/08/13 12:43

ID	: LAN	Name	: LANCO
Type	: Electrical Contractor	End Validity Date	: 2014/09/30
Service Tax	: adgc345sv	PAN	:
Phone	: 07911123446	Contact Person	: Mr. Romit Desai
Mobile	: 9764634445	Email	: desair@lanco.inn

ID	: LT1	Name	: LandT
Type	: Civil Contractor	End Validity Date	: 2014/09/30
Service Tax	: 12adbc4	PAN	:
Phone	: 0265222145	Contact Person	: Mr. Anish Mehta
Mobile	: 9825277789	Email	: larsentubro@yahoo.com

Work Order Details

Work Order Details Report provides the basic details of respective worker order.

Select the Contractors and work orders from the options of **all** and **randomly** as shown below. And then Click on Generate Report.

The work order details report for the above selection is as shown below.

Work Order Details

Back

Find... 1 of 1 100%

Main Report

Organization 2 Page 1 of 1

ORGANIZATION-Wise Work Order Details

Run by: System Admin Date: 2014/08/13 12:45

Work Order ID	Name	Type	Start Date	End Date	Worker Limit	Assigned Workers	Status
LT1	LandT						
Organization 2							
WO1	Concreting	Civil type	2014/08/20	2014/08/31	5	2	Open
WO2	Designing	Civil type	2014/08/20	2014/09/10	10	1	Open
WO3	Budgeting	Finance	2014/08/20	2014/09/10	5	1	Open

Blacklisted Workers

Blacklisted worker detail report provides the detail of workers who are blacklisted from organization against respective work order & contractor.

Work Order Man Days

Work Order Man Days Report shows the worker order wise comparison of Worker Limit, Assigned Workers and the approved workers. It also shows the total man-days invested on each work order. Work orders can be filtered based on Enterprise group.

It also shows the number of days invested on a specific work order by the workers assigned on that Work order.

ABC Pvt. Ltd.

Work Order Man Days From 2014/08/01 To 2014/08/31

Run by: System Admin Date: 2015/06/17

ABC Pvt. Ltd.

Contractor ID	Contractor Name	Work Order ID	Work Order Name	Start Date	End Date	Worker Limit	Registered Workers	Approved Workers	Work Days
1	LandT	WO1	Concreting	2014-08-20	2014-08-31	5	1	1	1
1	LandT	WO2	Designing	2014-08-20	2014-09-10	10	1	1	1
1	LandT	WO3	Budgeting	2014-08-20	2014-09-10	5	1	1	1

Daily Head Count

Daily Head Count Report shows the work order wise worker headcount for each date of the work order validity period. From this report the admin can get a daily basis comparison of expected workers and actually present workers.

Daily Work Hours

Daily Work Hours Report shows the worker's attendance status for each date against respective work order for respective contractor for selected dates. Work orders can also be filtered based on Enterprise group.

Matrix Comsec Pvt. Ltd.											Page 1 of 2
Daily Work Hours from 18/06/2015 To 18/06/2015											
Run by: System Admin										Date: 18/06/2015 00:16	
Organization : Matrix Comsec Pvt. Ltd.											
Work Order	E Contractor	E Name	Worker ID	Name	Skill	Category	Department	Shift	In	Out	Work Hours
WO2	contractor1		789	worker1	Skill-1	Category-1	Department-1	GS			-

Status Summary

Attendance Status Template

This page enables to define the output code for attendance status.

First Half	Second Half	Output Code
PR	PR	P

The Output Code for different Attendance Status combinations for first and second half can be created. The description for the status code can also be mentioned.

For example: Present for both 1st and 2nd half is given an output code of P.



The output codes defined here will reflect accordingly in the User-defined Muster Roll report in T&A module.

Daily Summary

Daily Summary Report shows the workers Daily Attendance summary against respective work order for respective contractor against date range selection.

Daily Summary																																																								
←																																																								
Back																																																								
Find... 1 of 1 100%																																																								
Main Report																																																								
ORGANISATION 1. Page 1 of 1 Organization-Wise Daily Summary From 2014/08/13 To 2014/08/21 Run by: System Admin Date: 2014/08/21 14:37 <table border="1"> <thead> <tr> <th>Worker ID</th><th>Name</th><th>Attendance Status</th></tr> </thead> <tbody> <tr> <td colspan="3">ORGANISATION 1.</td></tr> <tr> <td colspan="3">2014/08/18</td></tr> <tr> <td>Work_order WO</td><td></td><td>Contractor-1</td></tr> <tr> <td>_111.</td><td></td><td></td></tr> <tr> <td>Worker20</td><td>Worker 20 permanent</td><td>F-H</td></tr> <tr> <td colspan="3">2014/08/19</td></tr> <tr> <td>Work_order WO</td><td></td><td>Contractor-1</td></tr> <tr> <td>_111.</td><td></td><td></td></tr> <tr> <td>Worker20</td><td>Worker 20 permanent</td><td>F-A</td></tr> <tr> <td colspan="3">2014/08/20</td></tr> <tr> <td>Work_order WO</td><td></td><td>Contractor-1</td></tr> <tr> <td>_111.</td><td></td><td></td></tr> <tr> <td>Worker20</td><td>Worker 20 permanent</td><td>F-F</td></tr> <tr> <td colspan="3">2014/08/21</td></tr> <tr> <td>Work_order WO</td><td></td><td>Contractor-1</td></tr> <tr> <td>_111.</td><td></td><td></td></tr> <tr> <td>Worker20</td><td>Worker 20 permanent</td><td>A-B</td></tr> </tbody> </table>			Worker ID	Name	Attendance Status	ORGANISATION 1.			2014/08/18			Work_order WO		Contractor-1	_111.			Worker20	Worker 20 permanent	F-H	2014/08/19			Work_order WO		Contractor-1	_111.			Worker20	Worker 20 permanent	F-A	2014/08/20			Work_order WO		Contractor-1	_111.			Worker20	Worker 20 permanent	F-F	2014/08/21			Work_order WO		Contractor-1	_111.			Worker20	Worker 20 permanent	A-B
Worker ID	Name	Attendance Status																																																						
ORGANISATION 1.																																																								
2014/08/18																																																								
Work_order WO		Contractor-1																																																						
_111.																																																								
Worker20	Worker 20 permanent	F-H																																																						
2014/08/19																																																								
Work_order WO		Contractor-1																																																						
_111.																																																								
Worker20	Worker 20 permanent	F-A																																																						
2014/08/20																																																								
Work_order WO		Contractor-1																																																						
_111.																																																								
Worker20	Worker 20 permanent	F-F																																																						
2014/08/21																																																								
Work_order WO		Contractor-1																																																						
_111.																																																								
Worker20	Worker 20 permanent	A-B																																																						

Monthly Attendance

Monthly Attendance Report shows the workers Monthly Attendance summary against respective work order for respective contractor against Month-Year selection. Work orders can also be filtered based on Enterprise group.

Organisation - 4																														Page 2 of 2						
Monthly Attendance From 01/11/2015 To 30/11/2015																														Date: 28/01/2016 10:10						
Run by: System Admin																																				
Organization: Organisation - 4																																				
Work Order:work order 7																																				
Contractor: C20002																																				
Worker ID	Name	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	A	L	P	W	
Aakash100	Aakash100	W	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	9	0	13	4

Worker ID	Name	26	27	28	29	30	A	L	P	W
Aakash104	Aakash104	P	A	A	W	A	3	0	1	1

Attendance Details

Shift Schedule

This report shows the configured shifts of different workers under their respective contractors and work order types for each day of the specified month.

Muster Roll

This report generates a group-wise monthly muster roll with system-defined attendance status as well as leave status of workers for the specified month and year.

In large organizations, employees work on various jobs throughout the day and are paid on the basis of the job hours across the job's Cost Centre:

- Creating Projects, Phases, Jobs
- Planning Projects: Declaring hierarchy of phases and jobs under selected Project.
- Mapping Users to various Jobs.
- View invested job hours by users on various jobs/phases/projects.

This system will also be responsible for:

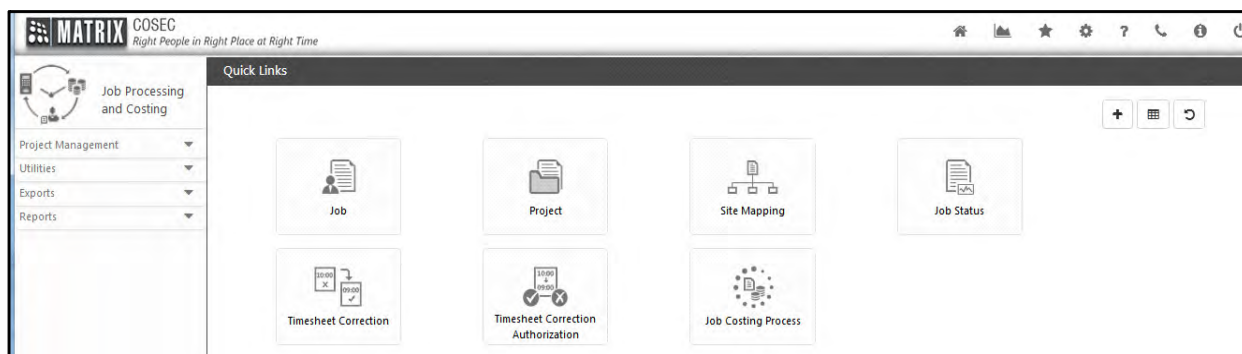
- Maintaining valid methods of mapping users to various jobs.
- Allow user to work on assigned jobs as per selection.
- Maintaining user's work records against different job codes.
- Allow correction/approval of daily Time Sheet.

A Project is divided into Phases. And Phase is divided into Jobs. The user is assigned the Job which he must complete within the estimated time. He can start the work by selecting the job from the assigned device.






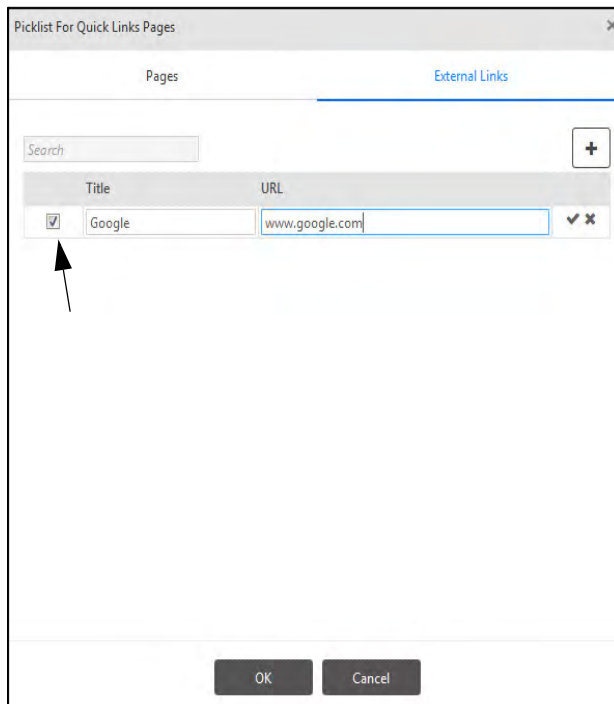
This functionality will be available only with the COSEC Job Processing and Costing license.

To access the JPC functionality with COSEC Web Application, click on the **JPC** Module on the module selection page. The **JPC** page will open on your screen.




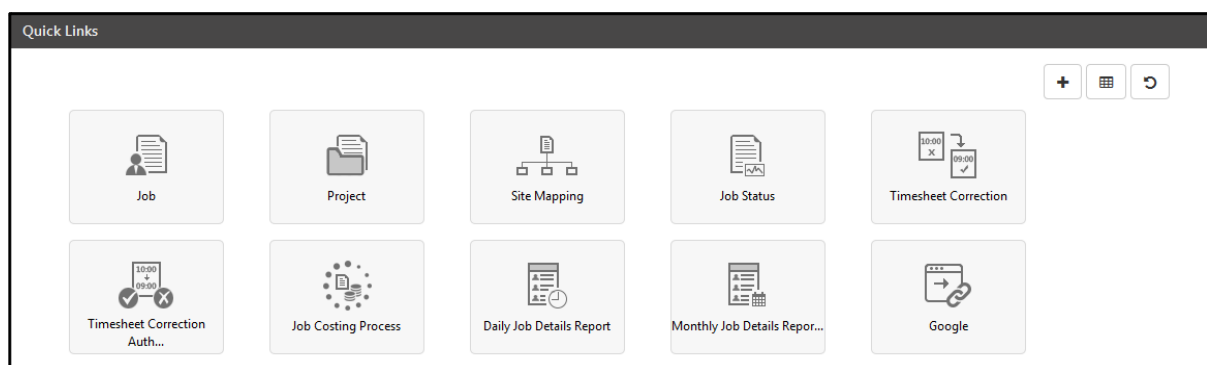
The page displays a menu and **Quick Links** to go to the required page in just one click. Quick Links are shortcuts to reach to a specific page easily. It also contains following three buttons:



- **Add Quick Link:** Click  button to add a quick link. A picklist for Quick Link pages appears for selecting the page or External Link for which the quick link is to be created. Maximum **20** quick links can be added.
- For Adding **Pages** in Quick Link, Select the Pages and click on OK
- For Adding **External Links**, Select External Link tab, click on  button to add new external link.
- Configure the **Title** and **URL** of the external link under the respective fields. click on checkbox to get the configured link on quick link screen as shown below. To save the configuration click on .



	Title	URL	
<input checked="" type="checkbox"/>	Google	www.google.com	<input checked="" type="checkbox"/> <input type="checkbox"/>

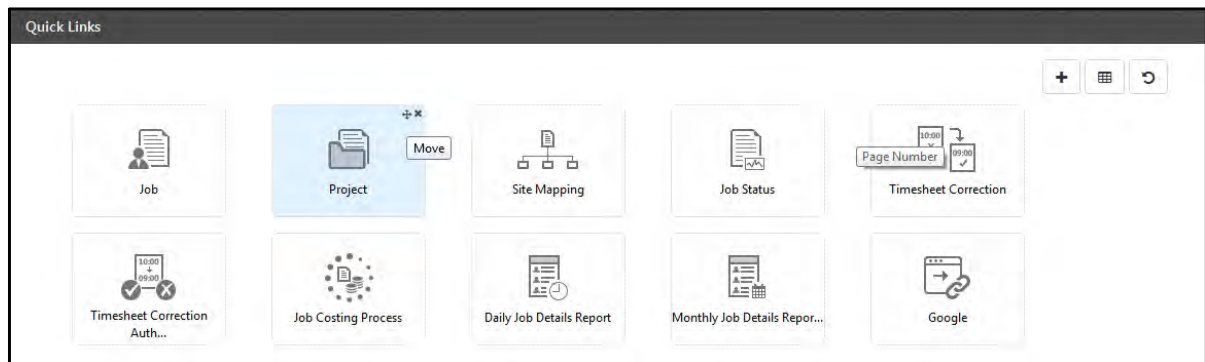
- To edit the saved configuration, click on .
- Click on OK to save the link configuration on Quick Link screen. The external link will be displayed as shown below:



- **Select Layout:** Click  button to select a layout for the quick links. You can select 5x4 or 4x5 layout to manage the quick links.
- **Reset Quick Links:** Click  button to reset the quick links to the default quick links.

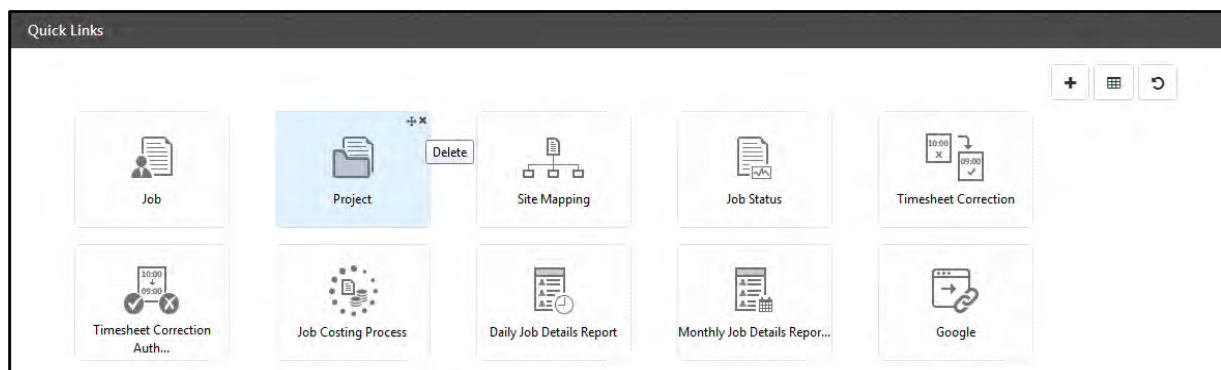
Move the Link

To move the link from one place to another, hover on the link on top right corner and click on “Move” icon as shown below. Then drag the quick link to the desired place. It will be placed at the desired location on the quick links page.



Delete the Link

To delete a particular link, hover on the link on top right corner and click on “Delete” icon as shown below.

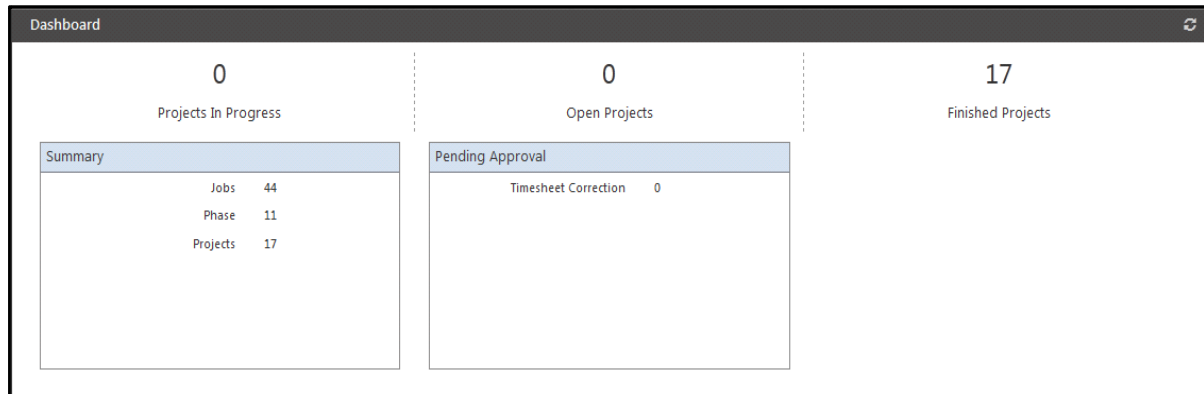


Quick links are displayed as per rights given to System Account and ESS users.

JPC Dashboard

To view the JPC Dashboard, click the Dashboard button  on the **JPC** page.

It displays basic information of the module under the following categories:



The Dashboard displays basic information :

- Projects In Progress - Total number of projects with “In Progress” status.
- Open Projects - Total number of projects with “Open” status.
- Finished Projects - Total number of projects with “Finished” status.

Summary

- Jobs - Total number of jobs configured in COSEC.
- Phase - Total number of phases configured in COSEC.
- Projects - Total number of projects configured in COSEC.

Pending Approval

- Timesheet Correction - Total number of timesheet correction requests in pending state.

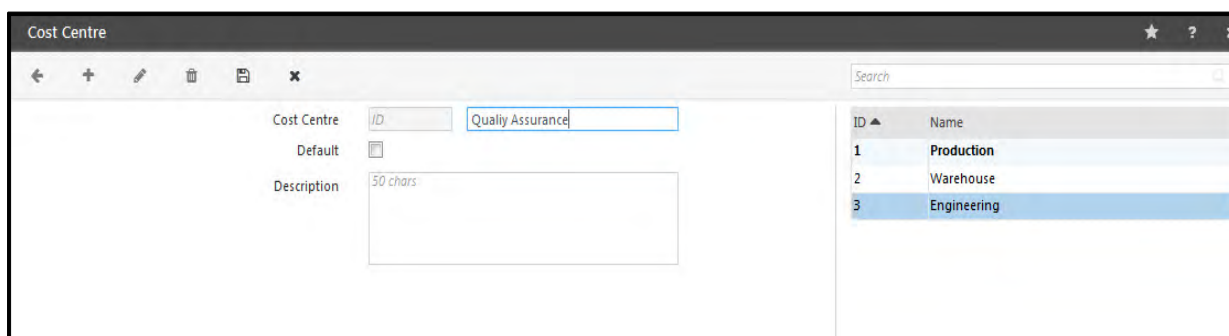
For more information on the above Dashboard options, click the respective information links on the Dashboard. The

Latest values on Dashboard are updated on clicking the Refresh  button.

Cost Centre

This page allows creating cost centre profiles to identify the man-days or man-hours against a particular project. A Cost Centre can be a defined task, department, division or any other unit in an organization for which costs are collected and reported. Creating cost centres and associating them with a project allows the management to calculate unit-wise investments on the project.

To create a new cost centre, go to **Job Processing and Costing > Project Management > Cost Centre**



The screenshot shows the 'Cost Centre' form. On the left, there are input fields: 'Cost Centre' with a dropdown showing 'ID' and a text box containing 'Quality Assurance'; 'Default' with an unchecked checkbox; and 'Description' with a text area containing '50 chars'. On the right, there is a table with columns 'ID' and 'Name'. The table contains three rows: 1 Production, 2 Warehouse, and 3 Engineering. The 'Engineering' row is highlighted in blue.

ID	Name
1	Production
2	Warehouse
3	Engineering

Click the **New** button to create a cost centre.

Cost Centre: Enter a user-friendly name for the new cost centre. The ID will be generated by the system automatically when the cost centre is saved.

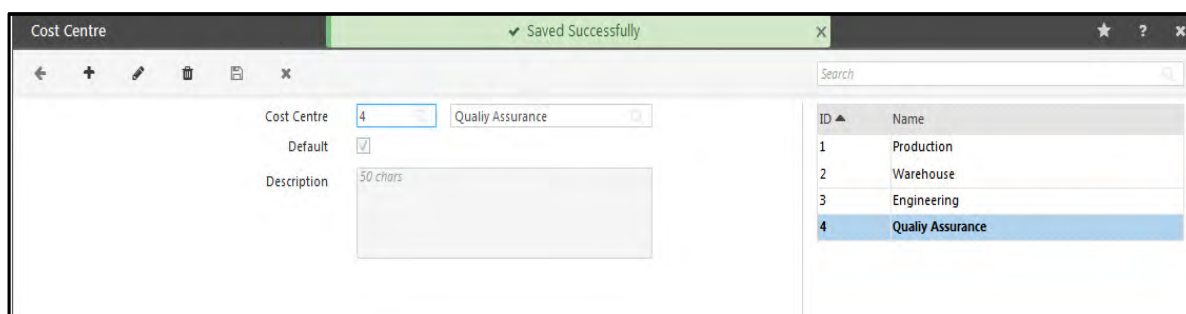
Default: To mark the new cost centre as default, enable the Default checkbox.

Description: You can also enter an optional description here.

Click **Save** button to save the cost centre. The new cost centre will appear on the grid list on the right hand side of the page.



The **Cost Centre** entity can also be renamed as per user requirement. To do this, go to **Admin > System Configuration > Rename Group**



The screenshot shows the 'Cost Centre' form after a successful save. A green banner at the top says 'Saved Successfully'. The 'Cost Centre' dropdown now shows '4' and the text box contains 'Quality Assurance'. The 'Default' checkbox is now checked. The 'Description' text area still contains '50 chars'. The table on the right now has four rows: 1 Production, 2 Warehouse, 3 Engineering, and 4 Quality Assurance. The 'Quality Assurance' row is highlighted in blue.

ID	Name
1	Production
2	Warehouse
3	Engineering
4	Quality Assurance

Job

This page enables the user to create new independent jobs which can later be assigned to some phase under a project. This allows a job to be started even before a parent project has been decided. The user can define an estimated duration for the execution of the job and also can also assign the job on selected devices. A maximum of 4294967294 jobs can be created in COSEC.

To create a new job, go to **Job Processing and Costing > Project Management > Job**

The screenshot shows a web-based form titled 'Job'. It has a toolbar at the top with icons for back, add, edit, delete, save, and close. The form fields are arranged in two columns. The left column contains: Project (ACTA), Phase (PSH1), Phase Date (31/05/2018), Code (PSD-W), Name (PSD Writing), Job Date (12/03/2018), Cost Centre (1), Estimated Hours (50), Merge Job (checkbox), Job Status (In Progress), and Allowance (checkbox). The right column contains: COSEC, SAD, 31/05/2018, PSD-W, PSD Writing, 30/03/2018, Cost Centre-1, and a list icon. At the bottom left, there is a button labeled 'Assign Devices'.

- Click the **New** button to create the job.
- Enter a **Job Code** and **Job Name** to identify the job. If the job already exists and has been assigned to a project, details of the corresponding project and phase will also appear.
- Select a start and end **Job Date**.
- Select a **Cost Centre** to be assigned to the job.
- Specify the **Estimated Hours** required to complete the job.
- Check the **Merge Job** box to add the transition time of shifting job in the succeeding or preceding Job.



The “Merge Job” option will appear here only if Merging option is selected from Global Policy. You can select the merging option as preceding or succeeding.

- There can be three status types which denote the completion status of a Job:
 - **Open** - Indicates that the job is yet to be started (as per assigned start date).
 - **In Progress** - Indicates that the job has been started and is yet to end (as per assigned end date).
 - **Finished** - Indicates that the assigned job duration has ended.
- **Allowance:** Check this box if the Allowance is to be given for the selected job. Eg: If food allowance is to be given for a specific Job say PSD-W; then enable the Allowance check-box.

Consider 3 Jobs: JB1, JB2 and JB3 performed by user in a month. Among these jobs JB1 and JB2 have Allowance checkbox as checked.

Case1: If Multiple transactions are available for same Job, then Allowance is count once only for single Job.


Example: If there is only one Job JB1(Allowance enabled) done on 20/02/2018 & are total 20 transactions; then Allowance = 1.

Case2: If Multiple Jobs are available, then Allowance is to be added for those Job which are enabled for Allowance.

Example: If there are two Job JB1,JB2 (both enabled for Allowance) done on 20/02/2018 & are total 20 transactions(10 of JB1 & 10 of JB2); then Allowance = 2.



To generate the Monthly data you must run the Monthly Attendance Process from T&A.

Click **Save**  . The new job will appear on the grid list on the right hand side of the page.

- Under **Assign Devices**, select one or more devices on which the job is to be assigned.



To assign a job on a device, ensure that the **Show Job Menu** checkbox is enabled on the **Devices > Device Configuration** page for the particular device.

This feature is applicable only for the following COSEC devices:

- Door V3
- Wireless Door
- PVR Door
- NGT Door
- Vega Controller
- Door V4



Jobs which are already in use cannot be deleted.

Job Group

This page allows the creation of job groups each of which can consist of multiple jobs. Once a job group has been defined, multiple jobs and devices can be assigned to the job group.

To create a new job group, go to **Job Processing and Costing > Project Management > Job Group**.

ID	Name
1	34

- Click the **New** button to create new job group.
- Enter a suitable **name** for the job group.
- In the **Assign Jobs** section, select one or more jobs from the picklist to be assigned to the job group. Only jobs in “Open” or “In Progress” state (i.e. unfinished jobs) can be assigned to a job group.
- In the **Assign Devices** section, select one or more devices to be assigned to the job group. The details of any job assigned to this job group will be sent to all the assigned devices.

MID	Name	Type
57	NGT Direct Door-Device-57	NGT Direct Door



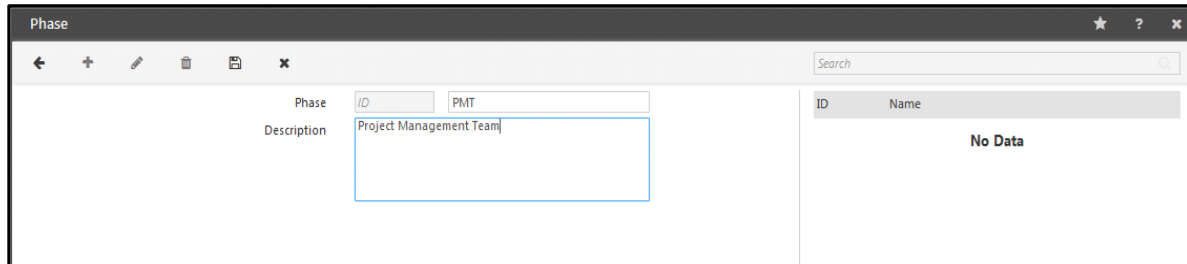
To assign a job group on a device, ensure that the **Show Job Menu** checkbox is enabled on the **Devices > Device Configuration** page for the particular device.

- Click **Save** button. The new job group will appear on the grid list on the right hand side of the page.

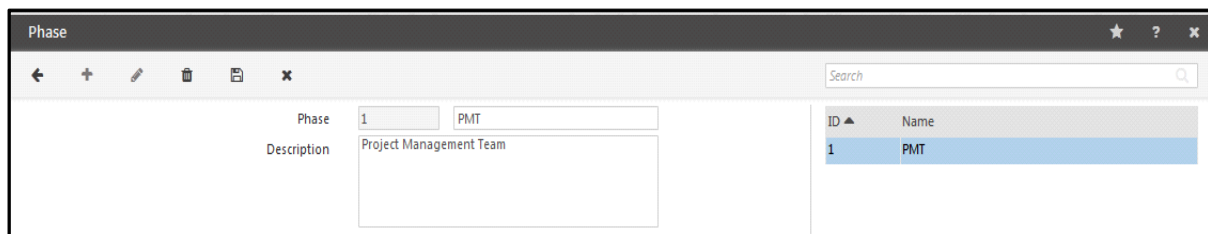
Phase

A large project may often be divided into multiple phases for better time and resource management. Hence a stage or section of a project may be defined as a Phase, say for example “Production”, which may in turn involve several jobs or tasks such as “Welding”, “Assembly” etc.

To create a new phase, go to **Job Processing and Costing > Project Management > Phase**



- Click the **New** button to create a phase.
- Enter a user-friendly name for the new phase. Eg: PMT
- You can also enter an optional description here. Eg: Project Management Team
- Click **Save** button. The new phase will appear on the grid list on the right side of the page.



*New Phases can also be created while Project is created from **Job Processing and Costing > Project Management > Project**. Here, a time duration can also be assigned to a phase, based on the project timeline.*

Project

This page enables the user to add new projects and edit existing ones. A complete project can be designed creating a hierarchy of underlying phases and jobs. This can be done either by adding existing phases and jobs to the new project or by creating new phases and jobs from this page.

To create a new project, go to **Job Processing and Costing > Project Management > Project**

The screenshot shows a web application window titled "Project". It has a toolbar with icons for back, add, edit, delete, save, and close. The main area is divided into two tabs: "Project" and "Phase". The "Project" tab is active and contains a form with the following fields:

- ID: PRJ1
- Name: COSEC Server
- Date: 2017/02/24 (start) and 2017/03/31 (end)
- Status: 6 char Code

Below the form is a section titled "Phase Configuration" with a table and an "Add" button (+).

Code	Phase	Start Date	End Date
No Data			

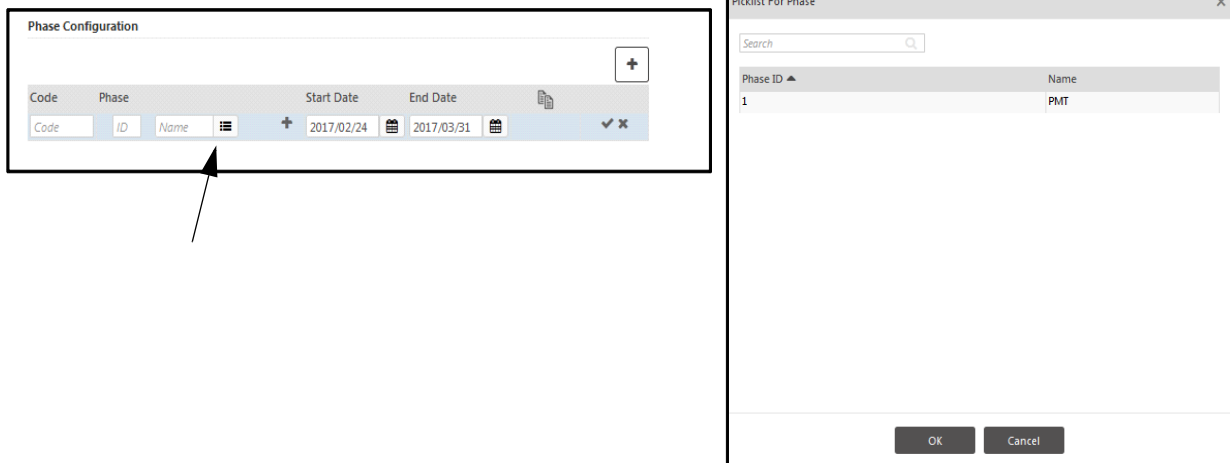
On the right side of the window, there is a search bar and a table with columns "Project Code", "Name", and "Status". The table currently displays "No Data".

- Click the **New** button to create a Project.
- Enter the **ID** as Project Code and **Name** of the project to identify the project.
- Select a start and end **Date** for the project duration.
- There can be three status types which denote the completion status of a project:
 - **Open** - Indicates that the project is yet to be started (as per assigned start date).
 - **In Progress** - Indicates that the project has been started and is yet to end (as per assigned end date).
 - **Finished** - Indicates that the assigned project duration has ended.

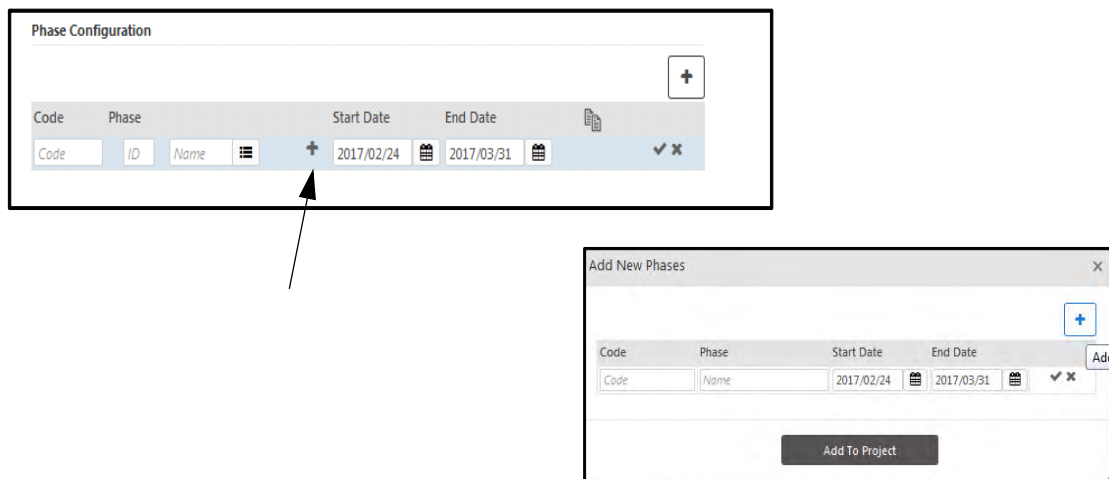
Phase Configuration

- You can add phase under the project to split the project into multiple phases. To add the phase click **Add** button.

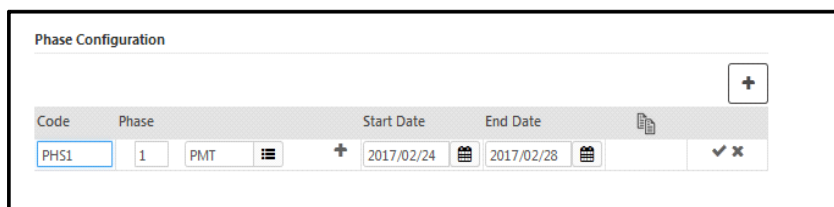
- Select an existing Phase using the picklist icon as shown below.



- If the phase is not available in picklist or if new phase is to be added in the project; then click on **Add** to add New Phases as shown below. The **Add New Phases** window appears from where new phase can be added as described above.



- Once a Phase is selected, assign a Phase **Code** to it. For eg: PMT phase is assigned code as PHS1.
- Select a start and end **Date** for the phase within the project time duration.



- Click **OK** to assign the selected phase to the project. Then click on **Save** button to save the Project as shown below.

Project

ID * PRJ1

Name * COSEC Server

Date * 2017/02/24 2017/03/31

Status 6 char Code

Phase Configuration

Code	Phase	Start Date	End Date
PHS1	PMT	2017/02/24	2017/02/28
PHS2	SAD	2017/02/27	2017/03/06

Project Code PRJ1 Name COSEC Server Status In Progress

Phase

- After selecting the configured Project from the right grid, click the **Phase** tab to view different phases assigned to the project and assign job in the particular phase.

Project

Project COSCLD COSEC ACTA

Phase SDT-F Feasibility

Phase Date 12/02/2018 06/03/2018

Job Configuration

Job	Start Date	End Date	Cost Centre	Estimated Hours
Feasibility	12/02/2018	02/03/2018	COSEC	100

Phase Code SDT-F Name Feasibility

SRS SRS Phase

UI UI Phase

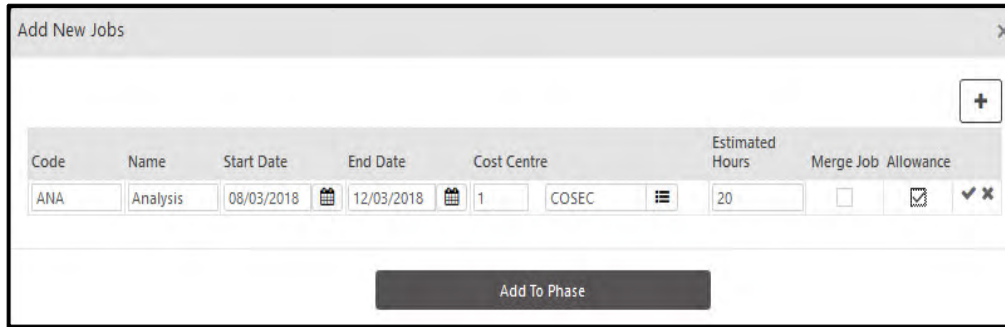
- Select a phase from the grid list to which jobs are to be assigned.
- In the **Job Configuration** section, user can add jobs under the phase by clicking Add button. Select an existing job using the picklist icon.

Job Configuration

Job Start Date End Date Cost Centre Estimated Hours

Feasibility 12/02/2018 02/03/2018 COSEC 100

- You can also create a new job by clicking **Add** button. The **Add New Jobs** window appears as shown below.

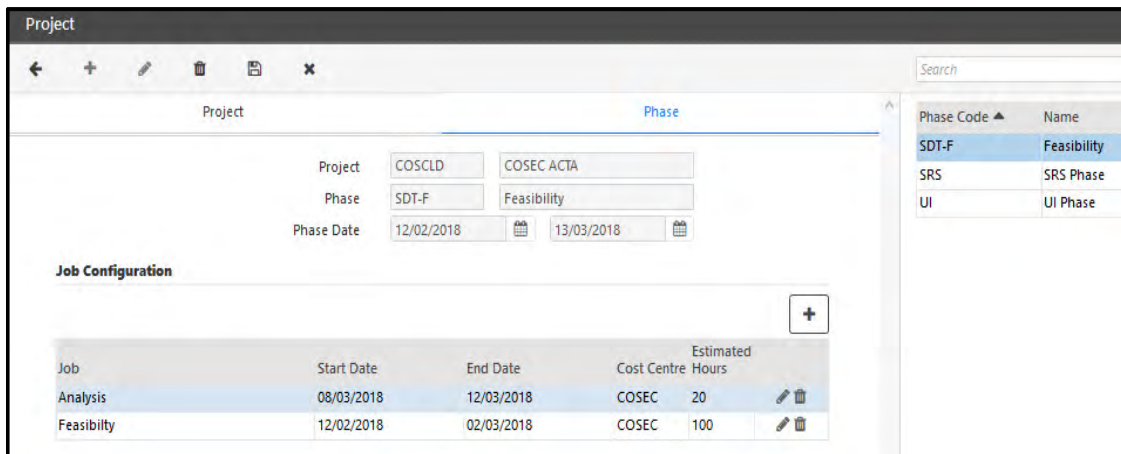


The 'Add New Jobs' dialog box contains a table with the following data:

Code	Name	Start Date	End Date	Cost Centre	Estimated Hours	Merge Job	Allowance
ANA	Analysis	08/03/2018	12/03/2018	1 COSEC	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Buttons: + (top right), Add To Phase (bottom center)

- Enter the **Code** and **Name** of Job.
- Select the Start and End **date** of job within the phase time duration.
- Select the **Cost center** applicable for the Job.
- Specify the **Estimated hours** for job completion.
- Enable the **Merge Job** checkbox to add the transition time of shifting job in the succeeding or preceding Job. The merging into succeeding or preceding is selected from Global policy.
- Enable the **Allowance** checkbox if the Allowance is to be given for the selected job.
- Click **OK** and **Add to Phase** to assign the selected job to the selected phase.



The 'Project' window shows the following configuration:

Project: COSCLD COSEC ACTA
Phase: SDT-F Feasibility
Phase Date: 12/02/2018 13/03/2018

Job Configuration

Job	Start Date	End Date	Cost Centre	Estimated Hours
Analysis	08/03/2018	12/03/2018	COSEC	20
Feasibility	12/02/2018	02/03/2018	COSEC	100

Right sidebar (Search):

Phase Code	Name
SDT-F	Feasibility
SRS	SRS Phase
UI	UI Phase

Once all phases and jobs have been configured under the new project, click **Save** button. The new project will appear in the grid list on the right side of the page.

Site Mapping

Site mapping refers to the assignment of multiple jobs as default jobs for a site. Default jobs can also be assigned to any specific enterprise group (i.e. organization, department, designation etc.) within the site. Setting a default job ensures that, for a certain day, the day's default job will be assigned to the user, based on the current date.

When a user's *Job Assignment Type* is **Device-based** (*Users module > User Configuration > Job Costing*), the default job for a user for a certain day is decided based on one of the following (in order of priority):

1. Default Job set on Device (*Devices module> Device Configuration > Job Costing*)
2. Default Job set for an Enterprise Group in a Site
3. Default Job set for a Site



Only jobs with status **Open** or **In Progress** can be assigned.

To set default jobs for a site, go to **Job Processing and Costing > Project Management > Site Mapping**

- Select a **Site** using the picklist button. The Site is created from Devices> Masters> Site.
- Click the **Edit** button.
- Under **Default Jobs**, Click **Add** button and select a **Job** from the picklist. Then set the **Assignment Date** of the job as required. Multiple default jobs can be assigned with non-overlapping *Assignment Date* ranges.
- Click **OK**. All added jobs will appear in the Default Jobs grid list.

Department Specific Jobs

On the **Site Mapping** page, select the **<Enterprise Group> Specific Jobs** tab. The Enterprise Group available for mapping will be decided as per *Global Policy> User> Job Costing* in Admin module.

Default Jobs

Search

+

Job Code ▲	Name	Assignment Start	Assignment End	
ANA	Analysis	2017/02/24	2017/02/28	

Department Specific Jobs

Search

+

Department ID	Name	Job Code ▲	Name	Assignment Start	Assignment End	
1	Department-1	PSD-W	PSD Writing	2017/02/24	2017/02/28	

Previous Job Assignment

- Select an <Enterprise Group> (e.g. Department, Designation etc.) using the picklist button. The above example shows a “Department” specific jobs assignment.
- Select a **Job** and set the **Assignment Date** as required. Multiple default jobs can be assigned with non-overlapping *Assignment Date* ranges.
- Click **OK** to save the Department specific jobs assignment.

Click **Save** button to apply the Site Mapping. Once the Assignment Date range for a job expires, the job will be moved to the **Previous Job Assignment** section as shown below.

Department Specific Jobs

Previous Job Assignment

Search

+

Department ID	Name	Job Code ▲	Name	Assignment Start	Assignment End	
1	Department-1	PSD-W	PSD Writing	24/02/2017	24/02/2017	

Location Mapping

Location mapping refers to the assignment of multiple jobs as default jobs for a location. Default jobs can also be assigned to any specific enterprise group (i.e. organization, department, designation etc.) within the location. Setting a default job ensures that, for a certain day, the day's default job will be assigned to the user, based on the current date.

In Location Mapping feature, user will punch using COSEC APTA and on the basis of available location details system will map punch to assigned job code for that configured location.

The screenshot shows the 'Location Mapping' window. At the top, there's a header bar with navigation icons. Below it, a 'Location' field is set to '34' and a dropdown menu shows 'Makarpura- HO'. The 'Default Jobs' section contains a search bar and a table with columns: 'Job Code', 'Name', 'Assignment Start', and 'Assignment End'. The table is currently empty, displaying 'No Data'. Below the table are two expandable sections: 'Department Specific Jobs' and 'Previous Job Assignment'.

Location: Select the location from the picklist. The location can be based on bluetooth i.e. BLE- Beacon, BLE- Device, GPS and Wi-Fi as configured from Admin> System Configuration> Location Master.

Default Jobs

Select the Default Jobs section. Click Add button to select the default job for the selected location.



Select the job from the picklist. This will be the default job assigned to the selected location. The **Assignment Date** will be auto-loaded in the field. You can change the assignment date as required.

This screenshot shows the same 'Location Mapping' window, but now a job is assigned. The table has one row with the following data: Job Code '123123', Name 'PSD-Analysis', Assignment Start '09/05/2017', and Assignment End '28/02/2099'. There are edit and delete icons at the end of the row.

Click on **Save** button to save the location mapping.





Department Specific Jobs

Search

Job Code	Name	Assignment Start ▲	Assignment End	
123123	PSD-Analysis	09/05/2017	28/02/2099	 

Department Specific Jobs

Search

Department ID	Name	Job Code	Name	Assignment Start	Assignment End	
5	PMT Dept	123123	PSD-Analysis	09/05/2017	28/02/2018	   

Previous Job Assignment

Select the **Department** and select the **Job** to assign the default job to the department.

Job Status

This page enables the user to view and monitor Jobs based on their current status. To view a job status, go to **Job Processing and Costing > Utilities > Job Status**.

The Job status page appears as shown below.

The screenshot shows the 'Job Status' page. At the top, there's a header bar with a back arrow, a star, and a question mark. Below the header, there are filter sections for Project, Phase, Job, and Job Status. Each filter has an 'ID' and 'Name' input field with a picklist button. To the right of these filters, it says '0 Phase(s) selected' and '0 Job(s) selected'. Below the filters is a 'View' button. A search bar is located below the filters. At the bottom, there's a table with columns: Job, Start Date, End Date, User Count, Job Hours, Estimated Hours, and Job Status. The table is currently empty, showing 'No Data'.

Select a **Project** using the picklist button.

Select multiple **Phases** and **Jobs** under the selected Project, for which records are to be viewed.

The screenshot shows a 'Picklist For Phase' dialog box. At the top, it says '3 selected of 3 records'. Below this is a search bar. The main area is a table with columns 'Phase Code' and 'Name'. There are three rows, each with a checked checkbox in the 'Phase Code' column. The rows are: PHS1 with Name 'PMT', PHS2 with Name 'SAD', and PHS3 with Name 'Devoplmnt phase'. At the bottom, there are 'OK' and 'Cancel' buttons.

The number of selected Phases and Jobs will be shown as below.

The screenshot shows the 'Job Status' window with the following filters: Project (PRJ1), COSEC Server project, 3 Phase(s) selected, 3 Job(s) selected, and Job Status (Open). A 'View' button is present. Below the filters is a search bar and a table with columns: Job, Start Date, End Date, User Count, Job Hours, Estimated Hours, and Job Status. The table currently displays 'No Data'.

Select the **Job Status** from the options of All, In Progress, Open or Finished based on which job status is to be viewed.

The User Count and Job hours is shown if the user who is assigned the job has worked. The Job Hours is calculated based on the Attendance period and Shift assigned to the user.

Click the **View** button to view the jobs status.

The screenshot shows the 'Job Status' window with the following filters: Project (PRJ1), COSEC Server project, 3 Phase(s) selected, 3 Job(s) selected, and Job Status (All). A 'View' button is present. Below the filters is a search bar and a table with columns: Job, Start Date, End Date, User Count, Job Hours, Estimated Hours, and Job Status. The table displays the following data:

Job	Start Date	End Date	User Count	Job Hours	Estimated Hours	Job Status
ANA-Analysis232	02/24/2017	02/28/2017	0		20:00	Finished
PSD-W-PSD Writing	02/24/2017	02/28/2017	0		11:00	Finished
SW-D-Soft development	03/10/2017	03/31/2017	1	12:58	20:00	In Progress

Daily Job View

This page displays information on total number of jobs performed on a day, number of users performing these jobs, details of Total Jobs, User Count, Job Hours, Un-Assigned Hours, OUT Time and Break Hours for a selected date range. User can view data for a date range of maximum 60 days.

To view daily job details, go to **Job Processing and Costing > Utilities > Daily Job View**

Date	Total Jobs	User Count	Job Hours	Un-Assigned Hours	Out Time	Break Hours
22/05/2017	4	5	22:54	06:01	00:50	00:24

Date: Select a start and end Date using the date selection buttons.

Click the **View** button to view daily job details for the selected date range.

Total Jobs: It displays total number of jobs done on the selected date.

User Count: It displays the number of users performing the job on selected date.

Job Hours: It displays the total hours spent in doing the assigned job.

Un- Assigned Hours: It displays the total hours spent on the selected date on un-assigned work.

Example: The user is doing job from 09:01 to 09:20 hrs. At 09:20 hrs user punches IN with Job code None. Then at 09:40 hrs user punches OUT with job code Continue. So the time between 09:20 to 09:40 is marked as Un-assigned hours.

Again at 09:50, user punches OUT with code None. And punches IN with code None. Hence this transaction is marked as Un-assigned hours.

Job Code	Phase Code	Project Code	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Count				
PSD-R	PSD-A	CLD	22/05/2017	09:01	22/05/2017	09:15	Job Hours	00:14	1				
PSD-R	PSD-A	CLD	22/05/2017	09:15	22/05/2017	09:20	Job Hours	00:05	1				
			22/05/2017	09:20	22/05/2017	09:40	Un-Assigned Hours	00:20					
SAD			22/05/2017	09:40	22/05/2017	09:50	Job Hours	00:10	1				
			22/05/2017	09:50	22/05/2017	09:55	Un-Assigned Hours	00:05					

Out Time: It displays the total hours for which users working on the job went outside.



You can enable the “OUT punch from Exit reader” in Attendance Policy of user to consider the punch for Out Time.

Break hours: It displays the total hours for which the users working on the job availed as break. It will be calculated based on the punches for Break Start and Break End.



The configuration for break hours is done from the Shift configuration assigned to the user.

Daily Job View

Date: 03/05/2017 03/05/2017

View

Search

Date	Total Jobs	User Count	Job Hours	Un-Assigned Hours	Out Time	Break Hours
03/05/2017	0	1		08:24		01:01

User: 1690 Priyank Bora

Date: 03/05/2017

Timesheet Correction

Search

Job Code	Phase Code	Project Code	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Job Count				
			03/05/2017	09:10	03/05/2017	13:29	Un-Assigned Hours	04:19					
			03/05/2017	13:29	03/05/2017	14:30	Break Hours	01:01					
			03/05/2017	14:30	03/05/2017	18:35	Un-Assigned Hours	04:05					

Time Sheet Correction

Time Sheet Correction helps in modifying job codes and split the transactions. So SA with appropriate rights can split the transactions by adding new punches between the transactions and apply job code to them if required.

The Time Sheet Correction can be made by:

- System Account User
- On Behalf System Account User
- Using the ESS Self Service Module (For more details refer COSEC Employee Self Service User Manual)

COSEC Web enables all *System Account users* with appropriate page rights to make Time Sheet Correction using the *Job Processing and Costing* module. All applications made by the System Account user are *pre-approved* by default.

COSEC Web also enables all On Behalf System Account User with appropriate page rights to make Time Sheet Correction using the *Job Processing and Costing* module. All applications made by the On Behalf System Account User are *pre-approved* by default. For creating and assigning the roles and rights to the On Behalf System Account User. Refer to “[On Behalf System Account User](#)”.

To do the Time Sheet Correction, go to **Job Processing and Costing > Utilities > Time Sheet Correction**

The screenshot shows the 'Timesheet Correction' web application. At the top, there's a title bar with 'Timesheet Correction' and a star icon. Below it, a navigation bar contains icons for back, edit, save, and close. The main form area has two input fields: 'User' with a dropdown menu showing 'ID' and 'Name', and 'Date' with a calendar icon and the date '22/05/2017'. Below these is a section titled 'Timesheet Correction' with a search bar. Underneath is a table with columns: Job Code, Phase Code, Project Code, Start Date, Start Time, End Date, End Time, Transaction Type, Hours, and Job Count. The table currently displays 'No Data'. At the bottom, there is a 'Job Summary' section with a dropdown arrow.

User: Select the User from the picklist. Ensure that the users are enabled for Job costing from the User module.

Date: Select the date from the calendar for which correction is to be done.

The transactions will be displayed as shown below.

Timesheet Correction

User: JCPS Nitin
Date: 22/05/2017

Search

Job Code	Phase Code	Project Code	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Count				
PSD-R	PSD-A	CLD	22/05/2017	09:05	22/05/2017	13:05	Job Hours	04:00	1				
PSD-R	PSD-A	CLD	22/05/2017	13:05	22/05/2017	13:29	Break Hours	00:24					
PSD-R	PSD-A	CLD	22/05/2017	13:29	22/05/2017	13:50	Job Hours	00:21	1				
INV	PAC	CLD	22/05/2017	13:50	22/05/2017	15:30	Out Time	01:40					
			22/05/2017	15:30	22/05/2017	17:30	Un-Assigned Hours	02:00					

1 - 5 of 6 records

Job Summary

Job Code: When the user punches on the device by selecting a job code, then that job code is displayed here.

Phase Code: When the selected job has been assigned to the phase of a project; then the respective Phase Code will be shown in this field.

Project Code: The Project Code for the selected job will be shown in this field.

Click on **Edit** button in the row where correction is to be made.

Timesheet Correction

Search

Job Code	Phase Code	Project Code	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Count				
PSD-R	PSD-A	CLD	22/05/2017	09:05	22/05/2017	13:05	Job Hours	04:00	1				
PSD-R	PSD-A	CLD	22/05/2017	13:05	22/05/2017	13:29	Break Hours	00:24					
PSD-R	PSD-A	CLD	22/05/2017	13:29	22/05/2017	13:50	Job Hours	00:21	1				
INV	PAC	CLD	22/05/2017	13:50	22/05/2017	15:30	Out Time	01:40					
			22/05/2017	15:30	22/05/2017	17:30	Un-Assigned Hours	02:00					

1 - 5 of 6 records

Corrections

- The **Job code** can be changed by selecting the option from the drop down list. If Job code is selected as **None**, then transaction type will be set as **Un-assigned**.
- The **Start Date** can be edited for only 1st transaction of the day by using left-right arrows.
- The **Start Time** can be edited for only 1st transaction of the day by specifying the time in hh:mm format.
- The **End Date** and **End Time** can be edited for all the transactions.
- The **Transaction type** can also be corrected. If some transaction is of **Un-assigned** type, then assigning some job code to the transaction will change the transaction type to **Job Hours** as shown below. Similarly if None is selected for any Job type transaction then its transaction type will get convert from Job to Unassigned.

Timesheet Correction										
Search										
Job Code	Phase Code	Project Code	Start Date ▲	Start Time	End Date	End Time	Transaction Type	Hours	Split	
COSCLD			03/09/2017	10:55	03/09/2017	14:55	Job Hours	04:00	⌵	✎

- The **Job Count** can be changed by editing the existing value.

Adjustment

Adjustment


Adjustment Type
Award

Hours *
00:10

Remark
50 chars

OK Cancel


Adjustment icon is visible against all transactions except the ones of 'Un-Assigned', 'Break Hours' and 'Out Time' transaction.

Click on Adjustment  button to assign either award or penalty. Both cannot be assigned simultaneously. Adjustment Hours (Penalty) should be less than or equal to corresponding Job Hours.



If some adjustment has been done against some transaction and user wishes to revert it back then he/she should enter 00:00 value in 'Hours' and click 'OK'.

Overtime

Click on Overtime  button to view the overtime details between start punch date time and end punch date time.

Overtime Within 22/05/2017 17:30:49 and 22/05/2017 19:30:27

OT1
HH:MM

OT2
01:00

OT3
HH:MM

OT4
HH:MM

OT5
HH:MM

Close

Merged Jobs

Click on **Merged Jobs** to view the Merged transactions.

Code	Project Code	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Job Count	Edit	Adjustment	Overtime	Merged Jobs	Split
	V9r5	2016/04/11	09:00	2016/04/11	11:00	Job Hours	02:00	1					
		2016/04/11	11:00	2016/04/11	11:30	Job Hours	00:30	1					
		2016/04/11	11:30	2016/04/11	13:00	Job Hours	01:30	1					

Actual Transaction details show the transactions that are to be merged. **Merged Transaction** shows the resultant transaction after merging.

Merged Transaction Details (Succeeding)													
Actual Transactions													
Job code	Phase Code	Project Code	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Job Count	Adjustment Type	Adjustment Time	Overtime	
004	344	V9r5	2016/04/11	09:00	2016/04/11	11:00	Job Hours	02:00	1				
0029			2016/04/11	11:00	2016/04/11	11:30	Job Hours	00:30	1				
Merged Transactions													
Job code	Phase Code	Project Code	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Job Count	Adjustment Type	Adjustment Time	Overtime	
0029			2016/04/11	09:00	2016/04/11	11:30	Job Hours	02:30	2				



1) Say, an X transaction has to be merged in a destination transaction Y (Succeeding/Preceding) which is not a "Job Hours" type transaction, in such a case, the Merged Jobs icon for X transaction should be visible but disabled to be clicked.

2) An X transaction has to be merged (Succeeding/Preceding) in a destination transaction Y, which does not have Job Code.

In such a case, icon should be visible in front of X transaction, but disabled to be clicked.

3) An X transaction has to be merged in a Succeeding/Preceding transaction, but, there is no, next/previous transaction available, respectively. In such a case, the icon should be visible but disabled in front of X transaction.

Split

Click on Split button to split the transaction and add new punches between the transaction. Split will be disabled if the transaction type is of "Out Time" and "Break". The Split Timesheet will appear as shown below:

Job Code	Phase Code	Project Code	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Job Count		
PSD-R	PSD-A	CLD	22/05/2017	09:05	22/05/2017	13:05	Job Hours	04:00	1		

OK Cancel

Click on **Edit** button and specify the new End time between existing start and end time to insert the new transaction as shown below:

Split Timesheet

Search

Job Code	Phase Code	Project Code	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Job Count	
PSD-R	PSD-A	CLD	22/05/2017	09:05	22/05/2017	10:00	Job Hours	04:00	1	✓ ✕ ⓘ

OK Cancel

Split Timesheet

Search

Job Code	Phase Code	Project Code	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Job Count	
PSD-R	PSD-A	CLD	22/05/2017	09:05	22/05/2017	10:00		00:55	1	✎ ⓘ
PSD-R	PSD-A	CLD	22/05/2017	10:00	22/05/2017	13:05		03:05	1	✎ ⓘ

OK Cancel



Whenever transaction of “Un-Assigned Hours” or “Job Hours” is tried to split and If the transaction’s punches are “IN-IN” or “IN-OUT” then the newly added punch will have IO type as “IN”.

If the transaction’s punches are “OUT-OUT” then the newly added punches will have IO type as “OUT”.

After all the corrections click on OK. Then click on Save button on the Menu bar to save the correction in Time sheet.

Job Summary displays the following details:

Timesheet Correction

User * JCP5 Nitin ⓘ

Date * 22/05/2017 ⓘ

Timesheet Correction

Job Summary

Total Job Hours-Count	06:21	3	ⓘ
Total Un-Assigned Hours	02:00		
Total Out Time	01:40		ⓘ
Total Award Hours	00:10		
Total Penalty Hours	HH:MM		
Overtime Hours	01:00		ⓘ

Total Job Hours- Count: Total job hours for the day are displayed and the details can be viewed by clicking ⓘ

Job Details For 22/05/2017

Job-PSD-R Hours-Count	06:21	3
Total Job Hours-Count	06:21	3

Close

Total Un-Assigned Hours: Total hours of the day when no job is assigned to the user, is displayed as un-assigned hours.

Total Out Time: Total hours of the day for which user has availed overtime, is displayed as Outtime. Also the Outtime details can be viewed.

Out Time Details For 22/05/2017

Out Time For Job-INV	01:40
Total Out Time	01:40

Close

Award Hours: Total hours given to user as an award which will be added in overtime hours.

Penalty Hours: Total hours given to user as the penalty which will be subtracted from the overtime hours.

Overtime Hours: Total hours of the day for which user has worked overtime, is displayed as Overtime hours. Also the Overtime hour details can be viewed as shown below.

Overtime Details For 22/05/2017

Job	PSD-R-PSD Review
OT1	HH:MM
OT2	01:00
OT3	HH:MM
OT4	HH:MM
OT5	HH:MM

Close

Time Sheet Correction Authorization

Time Sheet Correction Authorization helps in approving or rejecting an application of “Timesheet Correction” of ESS user.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to [“Reporting In-Charge”](#), [“Approval Policy”](#) and [“Configuring Users”](#).

You can either:

- view all the pending Timesheet Correction Authorizations
- set the filters — Date, Filter Users — to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To know more, refer to [“Pending Application”](#).



The population on this page depends on the server’s database. It might take time to load all pending applications.

Applications according to Set Filters

To Set the Filters,

- **Date:** Select this option to enable the date filter. Select the From and To date from the calendar to view the pending applications of time sheet correction.
- **Filter Users:** You can filter records according to the desired Enterprise Group, All or for an Individual.

Select **All**, to view authorization status of the applications of all the active users on the system.

Select **Individual**, to view authorization status of the applications of a single user. Click the picklist to select the desired User ID/Name.

Select the desired Enterprise Group — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Group1/2/3 and then click the picklist to select the desired group's ID/Name, to view authorization status of these applications.

Click on **View** to view the Pending, Approved and Rejected applications.

Pending Application

Click the **Pending** collapsible panel. The Pending Application with Job Hours, Un-Assigned Hours and Reason while applying for correction will be shown in the grid.




User ID	Name	Attendance Date	Job Hours	Un-Assigned Hours	Reason	Approve	Reject	Remark	Details
apijpc	apijpc	16/11/2017	14:30	00:00		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Authorized Timesheet Correction	

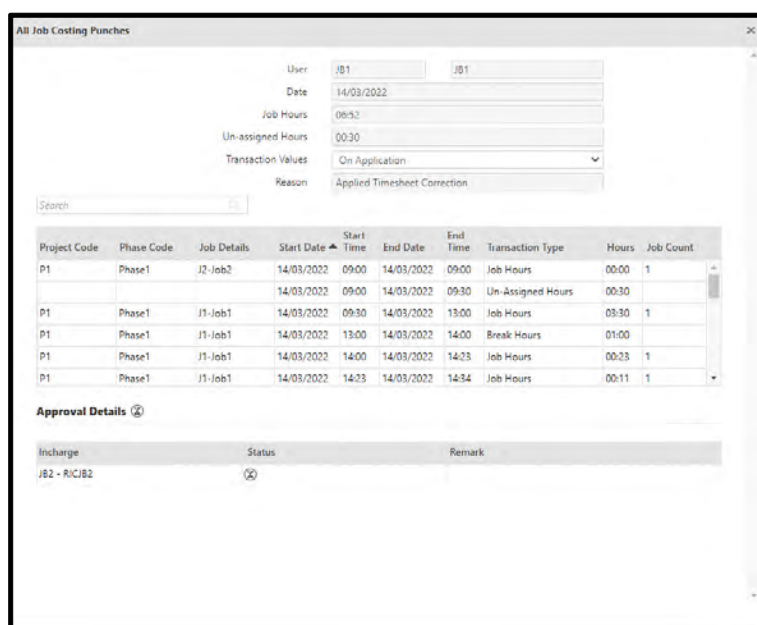
When any application is in the Pending state it can be authorized by the Admin or RIC.

- To approve/reject applications selectively, click the respective application check box against the user.
- To approve/reject all the applications simultaneously, click the Approve /Reject check box in the header column.

Once the Admin approves/ rejects the application, the record will be moved from the **Pending** section to the **Approved/ Rejected** section respectively.

The default **Remark** for the Approved and Rejected application will appear in the respective fields. You can enter any customized Remark while authorizing the application.

To view the details of the time sheet correction application, click **Details** . The **All Job Costing Punches** window appears as shown below.



Project Code	Phase Code	Job Details	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Job Count
P1	Phase1	J2-Job2	14/03/2022	09:00	14/03/2022	09:00	Job Hours	00:00	1
			14/03/2022	09:00	14/03/2022	09:30	Un-Assigned Hours	00:30	
P1	Phase1	J1-Job1	14/03/2022	09:30	14/03/2022	13:00	Job Hours	03:30	1
P1	Phase1	J1-Job1	14/03/2022	13:00	14/03/2022	14:00	Break Hours	01:00	
P1	Phase1	J1-Job1	14/03/2022	14:00	14/03/2022	14:23	Job Hours	00:23	1
P1	Phase1	J1-Job1	14/03/2022	14:23	14/03/2022	14:34	Job Hours	00:11	1

Incharge	Status	Remark
JB2 - RIC/JB2	X	

All Job Costing Punches window displays the time sheet correction details.

Transaction Values has the following options:

- **On Application:** The transaction values shown are the values at the time of the application being done.
- **Applied:** The transaction values after the correction is being made.
- **Current:** The current transaction values are same as On Application values.

This window also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer [“Approval Policy”](#).

Remark displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.

Approved Applications

Click the **Approved** collapsible panel.

The **Approved** section displays all the applications that have been approved by the RIC or the System Administrator.

The following screen displays the **Approved** section with approved Time Sheet Correction applications:

Pending (1)									
Approved (1)									
Search									
User ID	Name	Attendance Date ▼	Job Hours	Un-Assigned Hours	Reason	Approve	Reject	Details	
JCP3	Rahul	22/05/2017	00:34	04:27		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Rejected (0)									

Click the **Details**  icon to view the attendance details of the corresponding user.

All Job Costing Punches window appears as shown below:

Project Code	Phase Code	Job Details	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Job Count
P1	Phase1	J2-Job2	14/03/2022	09:00	14/03/2022	09:00	Job Hours	00:00	1
P1	Phase1	J1-Job1	14/03/2022	09:30	14/03/2022	13:00	Job Hours	03:30	1
P1	Phase1	J1-Job1	14/03/2022	13:00	14/03/2022	14:00	Break Hours	01:00	1
P1	Phase1	J1-Job1	14/03/2022	14:00	14/03/2022	14:23	Job Hours	00:23	1
P1	Phase1	J1-Job1	14/03/2022	14:23	14/03/2022	14:34	Job Hours	00:11	1

Incharge	Status	Remark
SA - System Admin	(16/03/2022 09:26)	Authorized Timesheet Correction

All Job Costing Punches window displays the time sheet correction details.

Transaction Values has the following options:

- **On Application:** The transaction values shown are the values at the time of the application being done.
- **Applied:** The transaction values after the correction is being made.
- **Current:** The current transaction values are same as On Application values.

This window also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer ["Approval Policy"](#).

Remark displays the comments provided by the Admin/ RIC/ System.


Click **Save** to save the authorization.

Rejected Applications

Click the **Rejected** collapsible panel.

The **Rejected** section displays all the applications that have been rejected by the RIC or the System Administrator.

The following screen displays the **Rejected** section with rejected Time Sheet Correction applications:

Rejected (1)									
Search									
User ID	Name	Attendance Date ▼	Job Hours	Un-assigned Hours	Reason	Approve	Reject	Remark	Details
U4	User4	21/06/2021	00:00	00:00	Applied Timesheet Correction	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Rejected Timesheet Correction	

Click the **Details**  icon to view the attendance details of the corresponding user.

All Job Costing Punches window appears as shown below:

User

JB1

JB1

Date

13/03/2022

Job Hours

00:00

Un-assigned Hours

14:45

Transaction Values

On Application ▼


Reason

Applied Timesheet Correction

Search

Project Code	Phase Code	Job Details	Start Date ▲	Start Time	End Date	End Time	Transaction Type	Hours	Job Count
			13/03/2022	07:00	13/03/2022	13:00	Un-Assigned Hours	06:00	
			13/03/2022	13:00	13/03/2022	14:00	Break Hours	01:00	
			13/03/2022	14:00	13/03/2022	22:45	Un-Assigned Hours	08:45	

Approval Details ✕

Incharge	Status	Remark
SA - System Admin	 (16/03/2022 10:27)	Rejected Timesheet Correction

All Job Costing Punches window displays the time sheet correction details.

Transaction Values has the following options:

- **On Application:** The transaction values shown are the values at the time of the application being done.
- **Applied:** The transaction values after the correction is being made.
- **Current:** The current transaction values are same as On Application values.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remarks displays the comments provided by the Admin / RIC / System.

Click **Save** button to save the changes.

Award Penalty Authorization

Award Penalty Authorization helps in approving or rejecting an application of award/penalty hours assignment to the user.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to [“Reporting In-Charge”](#), [“Approval Policy”](#) and [“Configuring Users”](#).

You can either:

- view all the pending Award/ Penalty Authorizations
- set the filters — Date, Filter Users — to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To know more, refer to [“Pending Application”](#).



The population on this page depends on the server’s database. It might take time to load all pending applications.

Applications according to Set Filters

To Set the Filters,

- **Date:** Select this option to enable the date filter. Select the From and To date from the calendar to view the pending applications of Award/ Penalty assignment.
- **Filter Users:** You can filter records according to the desired Enterprise Group, All or for an Individual.

Select **All**, to view authorization status of the applications of all the active users on the system.

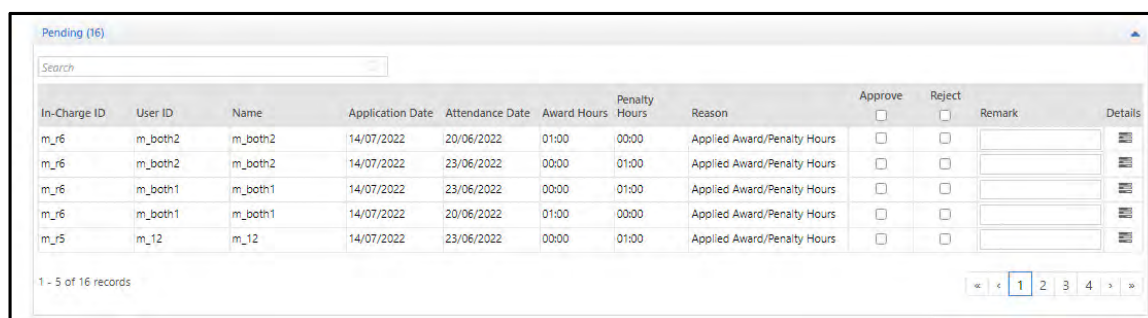
Select **Individual**, to view authorization status of the applications of a single user. Click the picklist to select the desired User ID/Name.

Select the desired Enterprise Group — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Group1/2/3 and then click the picklist to select the desired group's ID/Name, to view authorization status of these applications.

Click on **View** to view the Pending, Approved and Rejected applications.

Pending Application

Click the **Pending** collapsible panel. The **Pending** section displays all the applications that have are yet to be authorized by the RIC or the System Administrator.



In-Charge ID	User ID	Name	Application Date	Attendance Date	Award Hours	Penalty Hours	Reason	Approve	Reject	Remark	Details
m_r6	m_both2	m_both2	14/07/2022	20/06/2022	01:00	00:00	Applied Award/Penalty Hours	<input type="checkbox"/>	<input type="checkbox"/>		
m_r6	m_both2	m_both2	14/07/2022	23/06/2022	00:00	01:00	Applied Award/Penalty Hours	<input type="checkbox"/>	<input type="checkbox"/>		
m_r6	m_both1	m_both1	14/07/2022	23/06/2022	00:00	01:00	Applied Award/Penalty Hours	<input type="checkbox"/>	<input type="checkbox"/>		
m_r6	m_both1	m_both1	14/07/2022	20/06/2022	01:00	00:00	Applied Award/Penalty Hours	<input type="checkbox"/>	<input type="checkbox"/>		
m_r5	m_12	m_12	14/07/2022	23/06/2022	00:00	01:00	Applied Award/Penalty Hours	<input type="checkbox"/>	<input type="checkbox"/>		

1 - 5 of 16 records


« < 1 2 3 4 > »

When any application is in the Pending state it can be authorized by the Admin or RIC.

- To approve/reject applications selectively, click the respective application check box against the user.
- To approve/reject all the applications simultaneously, click the Approve /Reject check box in the header column.

Once the Admin approves/ rejects the application, the record will be moved from the **Pending** section to the **Approved/ Rejected** section respectively.

The default **Remark** for the Approved and Rejected application will appear in the respective fields. You can enter any customized Remark while authorizing the application.

To view the details of the time sheet correction application, click **Details** . The **All Job Costing Punches** window appears as shown below.

All Job Costing Punches

User: Test1 Test1

Attendance Date: 14/06/2021

Transaction Values: On Application

Reason: Applied Award/Penalty Hours

Search

Project Code	Phase Code	Job Code	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Job Count	Adjustment Type	Adjustment Time
		J1	14/06/2021	00:00	14/06/2021	01:00	Job Hours	01:00	2	Award	10:01
		J1	14/06/2021	01:00	14/06/2021	13:00	Job Hours	12:00	1	Award	01:02
		J1	14/06/2021	13:00	14/06/2021	13:00	Job Hours		1	Award	01:00
		JOB	14/06/2021	13:00	14/06/2021	13:00	Job Hours		1	Award	01:02
		JOB	14/06/2021	13:00	14/06/2021	13:00	Job Hours		1	Award	02:00

1 - 5 of 14 records

Approval Details

Incharge	Status	Remark
RG2		

All Job Costing Punches window displays the time sheet correction details.

Transaction Values has the following options:

- **On Application:** The transaction values shown are the values at the time of the application being done.
- **Applied:** The transaction values after the correction is being made.
- **Current:** The current transaction values are same as On Application values.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remark displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.



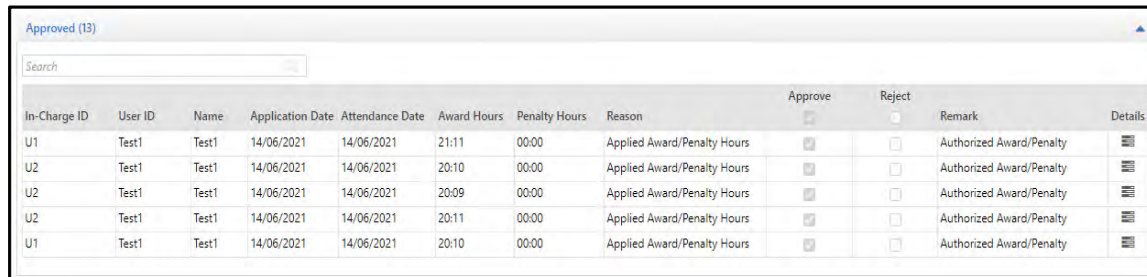
The pending applications can not be authorized if the attendance period is closed while doing monthly attendance process and "Attendance Correction in Closed Period" checkbox is disabled from Time and Attendance > Policies > Attendance Policy > Event Authorization.

Even though; the period is closed but if "Attendance Correction in Closed Period" check-box in Policy is enabled then authorization can be made.

Approved Applications

Click the **Approved** collapsible panel. The **Approved** section displays all the applications that have been approved by the RIC or the System Administrator.

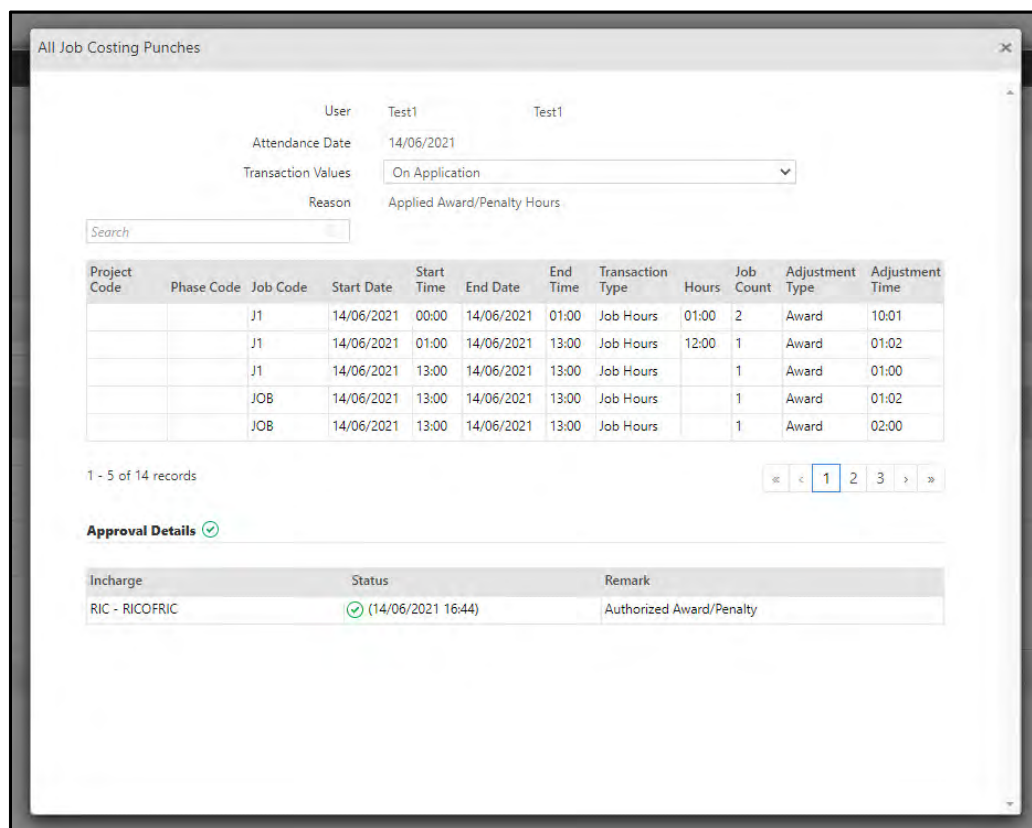
The following screen displays the **Approved** section with approved Award Penalty applications:



In-Charge ID	User ID	Name	Application Date	Attendance Date	Award Hours	Penalty Hours	Reason	Approve	Reject	Remark	Details
U1	Test1	Test1	14/06/2021	14/06/2021	21:11	00:00	Applied Award/Penalty Hours	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Authorized Award/Penalty	
U2	Test1	Test1	14/06/2021	14/06/2021	20:10	00:00	Applied Award/Penalty Hours	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Authorized Award/Penalty	
U2	Test1	Test1	14/06/2021	14/06/2021	20:09	00:00	Applied Award/Penalty Hours	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Authorized Award/Penalty	
U2	Test1	Test1	14/06/2021	14/06/2021	20:11	00:00	Applied Award/Penalty Hours	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Authorized Award/Penalty	
U1	Test1	Test1	14/06/2021	14/06/2021	20:10	00:00	Applied Award/Penalty Hours	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Authorized Award/Penalty	

Click the **Details** icon to view the details of the corresponding user.

All Job Costing Punches window appears as shown below:



User: Test1 Test1
Attendance Date: 14/06/2021
Transaction Values: On Application
Reason: Applied Award/Penalty Hours

Search

Project Code	Phase Code	Job Code	Start Date	Start Time	End Date	End Time	Transaction Type	Hours	Job Count	Adjustment Type	Adjustment Time
		J1	14/06/2021	00:00	14/06/2021	01:00	Job Hours	01:00	2	Award	10:01
		J1	14/06/2021	01:00	14/06/2021	13:00	Job Hours	12:00	1	Award	01:02
		J1	14/06/2021	13:00	14/06/2021	13:00	Job Hours		1	Award	01:00
		JOB	14/06/2021	13:00	14/06/2021	13:00	Job Hours		1	Award	01:02
		JOB	14/06/2021	13:00	14/06/2021	13:00	Job Hours		1	Award	02:00

1 - 5 of 14 records

Approval Details

Incharge	Status	Remark
RIC - RICOFRIC	(14/06/2021 16:44)	Authorized Award/Penalty

All Job Costing Punches window displays the time sheet correction details.

Transaction Values has the following options:

- **On Application:** The transaction values shown are the values at the time of the application being done.
- **Applied:** The transaction values after the correction is being made.
- **Current:** The current transaction values are same as On Application values.

Transaction Values has the following options:

- **On Application:** The transaction values shown are the values at the time of the application being done.
- **Applied:** The transaction values after the correction is being made.
- **Current:** The current transaction values are same as On Application values.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remarks displays the comments provided by the Admin / RIC / System.

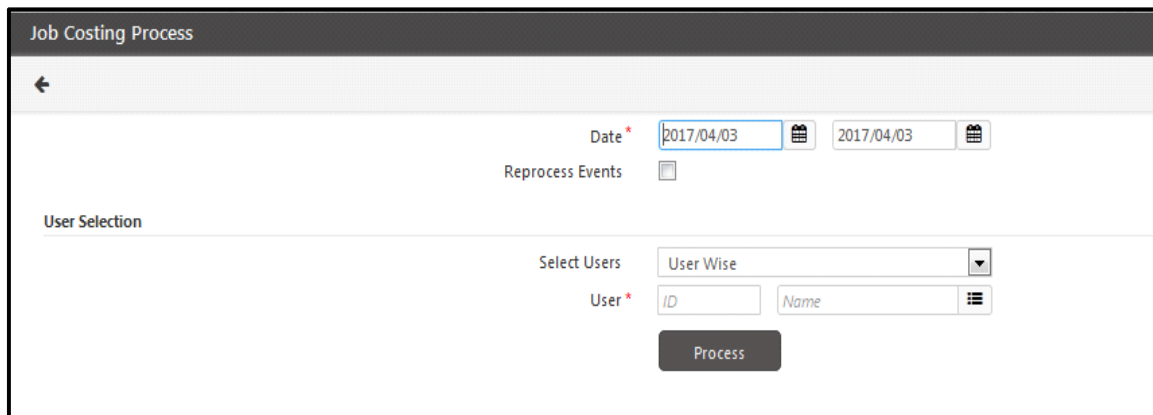
Click **Save** button to save the changes.

Job Costing Process

This page helps in processing attendance punches to generate accurate Job Costing data of users for a specified date range. Any changes in configuration made for a user on the *Job Processing and Costing* module requires the administrator to process the user's data first using this functionality.

"Job Costing Process" maps job code to the event on the basis of user/ device/ site/ location mapping configuration.

To process job costing data, go to **Job Processing and Costing > Utilities > Job Costing Process**

The screenshot shows a web interface titled "Job Costing Process". It features a date range selector with two date pickers, both showing "2017/04/03". Below the dates is a checkbox labeled "Reprocess Events". Underneath is a section titled "User Selection" which includes a dropdown menu labeled "Select Users" currently set to "User Wise". Below this are two input fields for "User", one labeled "ID" and one labeled "Name". At the bottom right of the form is a dark grey button labeled "Process".

Select a date range for which data is to be processed.

Select the **Reprocess Events** checkbox to enable the system to do the following:

- Reprocess all attendance events based on any new policy settings.
- Revert all attendance event related changes made through manual correction.



When job code is not assigned to user and user punches with that job code using Special function from door; then Reprocess Events should be enabled during Job Costing process.

Select the **Users** from the filter options of User Wise, Group Wise or all for whom the data is to be processed.

Click the **Process** button to start processing job data for all selected users.

Daily Timesheet

To export Daily Timesheet, go to **Job Processing and Costing > Export > Daily Timesheet**.

The Daily Timesheet page appears as shown below:

The screenshot shows the 'Daily Timesheet' export configuration interface. On the left, there is a sidebar with 'Export' (highlighted in blue) and 'Configuration' options. The main area contains the following fields:

- Date ***: Two date pickers showing '09/05/2017'.
- File Name ***: A text input field.
- Select Users**: A dropdown menu set to 'User Wise'.
- User ***: Two input fields for 'ID' and 'Name'.
- Generate Export For**: A dropdown menu set to 'All Users'.
- Export**: A dark button at the bottom.

Before exporting the Daily Timesheet data, you must do the ["Configuration"](#).

Export

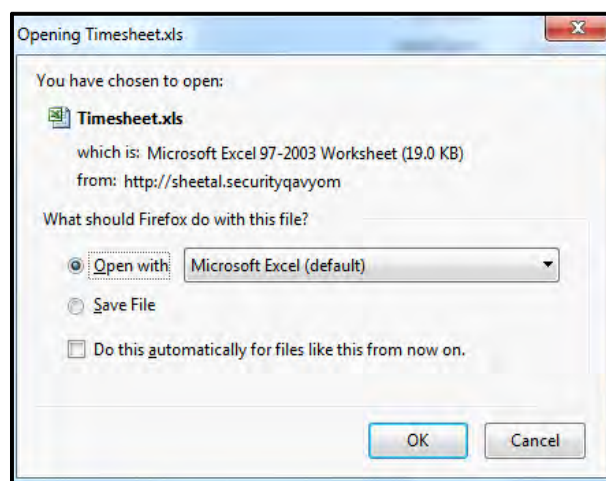
- Select the **date** range for which daily timesheet is to be exported.
- Specify the **filename** and the **file format** as Excel.
- You can filter the users by selecting users based on **User Wise, Group Wise or All**.
- You can **Generate Export for All Users, Active Users or Inactive Users**.

This screenshot shows the 'Daily Timesheet' export configuration page with an additional user list. The fields are similar to the previous screenshot, but with the following updates:

- Date ***: Date pickers showing '22/05/2017' and '23/05/2017'.
- File Name ***: Text input field containing 'Timesheet'.
- Select Users**: Dropdown menu set to 'User Wise'.
- User ***: Input fields for 'ID' and 'Name'.
- Generate Export For**: Dropdown menu set to 'All Users'.
- Export**: Dark button at the bottom.
- User List**: A table below the user fields showing a list of users with their IDs and names, and a search bar above it.

User ID	Name
JCP1	Vinit
JCP2	Piyush
JCP3	Rahul
JCP4	Hiren
JCP5	Nitin

Click on **Export** button. The daily timesheet can be opened or saved at desired location.



The export timesheet file will be generated as per the configuration as shown below:

Sr No	User ID	User Name	Attendance Date	Start Date-Time	End Date-Time	Project Code	Project Name	Phase Code	Job Code	Job Name	Job Hours	Actual OT1	Actual OT2	Actual OT3	Job Count
1	JCP1	Vinit	22/05/2017	22/05/2017 09:16:40	22/05/2017 09:22:07	CLD	COSEC Cloud	PSD-A	PSD-S	PSD Study	00:06	00:00	00:00	00:00	1
				22/05/2017 09:22:07	22/05/2017 12:57:29	CLD	COSEC Cloud	PSD-A	PSD-S	PSD Study	03:35	00:00	00:00	00:00	1
				22/05/2017 12:57:29	22/05/2017 14:02:16	CLD	COSEC Cloud	PSD-A	PSD-S	PSD Study	01:05	00:00	00:00	00:00	1
				22/05/2017 14:02:16	22/05/2017 14:40:37	CLD	COSEC Cloud	PSD-A	PSD-S	PSD Study	00:38	00:00	00:00	00:00	1
				22/05/2017 14:40:37	22/05/2017 14:45:21				SAD	SAD study	00:05	00:00	00:00	00:00	1
				22/05/2017 14:45:21	22/05/2017 14:47:50				SAD	SAD study	00:02	00:00	00:00	00:00	1
				22/05/2017 14:47:50	22/05/2017 17:05:27				SAD	SAD study	02:18	00:00	00:00	00:00	1
				22/05/2017 17:05:27	22/05/2017 20:05:27				SAD	SAD study	03:00	00:00	01:35	00:00	1
2	JCP2	Piyush	22/05/2017	22/05/2017 09:22:29	22/05/2017 09:22:45	CLD	COSEC Cloud	PAC	LAB	Labelling	00:00	00:00	00:00	00:00	1
				22/05/2017 09:22:45	22/05/2017 09:22:47	CLD	COSEC Cloud	PAC	LAB	Labelling	00:00	00:00	00:00	00:00	1
				22/05/2017 09:22:47	22/05/2017 09:26:59	CLD	COSEC Cloud	PAC	LAB	Labelling	00:04	00:00	00:00	00:00	1
				22/05/2017 09:26:59	22/05/2017 12:56:46	CLD	COSEC Cloud	PAC	LAB	Labelling	03:30	00:00	00:00	00:00	1
				22/05/2017 12:56:46	22/05/2017 14:36:49	CLD	COSEC Cloud	PAC	LAB	Labelling	01:40	00:00	00:00	00:00	1
3	JCP3	Rahul	22/05/2017	22/05/2017 09:01:21	22/05/2017 09:15:13	CLD	COSEC Cloud	PSD-A	PSD-R	PSD Review	00:14	00:00	00:00	00:00	1
				22/05/2017 09:15:13	22/05/2017 09:20:19	CLD	COSEC Cloud	PSD-A	PSD-R	PSD Review	00:05	00:00	00:00	00:00	1
				22/05/2017 09:20:19	22/05/2017 09:40:20						00:20	00:00	00:00	00:00	1
				22/05/2017 09:40:20	22/05/2017 09:50:18				SAD	SAD study	00:10	00:00	00:00	00:00	1
				22/05/2017 09:50:18	22/05/2017 09:55:16	CLD	COSEC Cloud	PAC	INV	Inventory	00:05	00:00	00:00	00:00	1
				22/05/2017 09:55:16	22/05/2017 13:11:12						03:16	00:00	00:00	00:00	1
				22/05/2017 13:11:12	22/05/2017 14:02:23						00:51	00:00	00:00	00:00	1
4	JCP4	Hiren	22/05/2017	22/05/2017 09:10:24	22/05/2017 10:30:45	CLD	COSEC Cloud	PSD-A	PSD-S	PSD Study	01:20	00:00	00:00	00:00	1
				22/05/2017 10:30:45	22/05/2017 10:40:25	CLD	COSEC Cloud	PSD-A	PSD-S	PSD Study	00:10	00:00	00:00	00:00	1
				22/05/2017 10:40:25	22/05/2017 10:50:23						00:10	00:00	00:00	00:00	1
				22/05/2017 10:50:23	22/05/2017 11:00:20						00:10	00:00	00:00	00:00	1

Configuration

You can select the fields to be exported by checking the respective box. Click on Save button to save the configuration for export.

Daily Timesheet

Export

Configuration

Select Fields To Export

Search

Fields

Project Name

Phase Code

Phase Name

Job Code

Job Name

☐
☒
☒
☐
☒

Matrix COSEC System Manual

2133

Job Processing and Costing Reports

These reports can be obtained using the **Reports** section under the **Job Processing and Costing** add-on module. The Reports can be categorized as follows:

- “Daily Job Details”
- “Monthly Job Details”
- “Job Transactions”
- “User Job Details”
- “Transaction-Wise Hours Summary”
- “Work Summary”

Daily Job Details

Generates the selected users' daily work details against various jobs, across multiple projects.

Daily Job Details

Date * 22/05/2017 23/05/2017

Optional Parameters

Group By Organization

User Selection

Select Users User Wise

User * ID Name

Search

User ID	Name
JCP5	Nitin

Generate Report For All Users

Generate Report

Organization-1						Page 1 of 1	
Organization-Wise Daily Job Details From 22/05/2017 To 23/05/2017							
Run by:	System Admin				Date:	23/05/2017	12:25
User ID	Name	Project	Job		Job Out Time	Break	Un-Assigned
					Hours	Hours	Hours
22-05-2017							
Organization-1							
JCP5	Nitin						02:00
JCP5	Nitin	CLD	INV:Inventory			01:40	
JCP5	Nitin	CLD	PSD-R:PSD Review		06:21		00:24
Total:					06:21	01:40	00:24
							02:00

Monthly Job Details

Generates the selected users' monthly attendance summary against their jobs under the respective projects.

Monthly Job Details

←

For Month-Year

May

2017

Optional Parameters

Group By

Organization

User Selection

Select Users

User Wise

User *

ID

Name

Search


1690

Priyank Bora

Generate Report For

All Users

Generate Report

	Organization2 Organization-Wise Monthly Job Details For MAY-2017
Run by: System Admin	
User ID: Organization2 1690	Name: Priyank Bora
	Jobs: 1 Projects: 0
Total Jobs	0
Total Projects	0
Job Hours	-
OutTime Hours	-
Break Hours	-
Unassigned Hours	00:23
	02 Tue 03 Wed 04 Thu 06 Sat 07 Sun 08 Mon 09 Tue 10 Wed 12 Fri 13 Sat 14 Sun 15 Mon 17 Wed 18 Thu
	0 0 0 0 0 0 0 0 0 0 0 1 0 0
	0 0 0 0 0 0 0 0 0 0 0 0 0 0
	- - - - - - - - - - - 10:58 - -
	- - - - - - - - - - - - - - - -
	- 01:01 01:00 01:10 01:10 - 01:10 - 00:59 - - - 01:20 00:55
	00:23 08:24 05:50 06:15 05:55 00:10 07:18 09:44 06:21 05:30 35:00 - 06:11 02:10

Job Transactions

This report shows the transaction details of selected users against their respective jobs.

Job Transactions

←

Date *

07/09/2020

07/09/2020

Optional Parameters

Group By

Organization

Group By

Date

Organization Name in Header As Per

User Selection

Group Needed In Report

User Selection

Select Users

User Wise

User *

ID

Name

Generate Report For

All Users

Generate Report

Organization-1				Page 1 of 1
User Job Details From 22/05/2017 To 23/05/2017				
Run by: System Admin		Date: 23/05/2017		12:29
Sr No	User ID	Name	Job	Hours
22-05-2017				
INV	Inventory			
1	JCP3	Rahul		00:05
Total:				00:05
LAB	Labelling			
1	JCP4	Hiren		00:40
Total:				00:40
PSD-R	PSD Review			
1	JCP3	Rahul		00:19
2	JCP5	Nitin		06:21
Total:				06:40
PSD-S	PSD Study			
1	JCP4	Hiren		02:20
Total:				02:20
SAD	SAD study			
1	JCP3	Rahul		00:10
Total:				00:10

Transaction-Wise Hours Summary

This report show the user's timesheet transactions on daily basis. Also the report shows output transaction wise overtime or adjustments.

Transaction-Wise Hours Summary

Date *
14/09/2020
14/09/2020

Show As Per Merged Transactions
☐

Optional Parameters

Group By
Organization
☐ Group Needed In Report

New Page For Each User
☐

Include Overtime

☒ OT1
☒ OT2
☒ OT3
☒ OT4
☒ OT5

Include Adjustment Section
☒

Add Custom Footer
☒

Organization Name in Header As Per
User Selection

User Selection

Select Users
User Wise

User *
ID
Name

Generate Report For
All Users

Organization-1

Page 1 of 1

Organization-Wise Transaction-Wise Hours Summary From 22/05/2017 To 23/05/2017

Run by: System Admin

Date: 23/05/2017

12:44

Date	Shift	Project	Job	Start	End	Award Hours	Penalty Hours	Total Hours	Standard Hours	OT1	OT2
JCP5	Nitin										
22/05/2017	GS	CLD	PSD-R:PSD Review	22/05/2017 09:05	22/05/2017 13:05						
22/05/2017	GS	CLD	PSD-R:PSD Review	22/05/2017 13:05	22/05/2017 13:29						
22/05/2017	GS	CLD	PSD-R:PSD Review	22/05/2017 13:29	22/05/2017 13:50	00:10					
22/05/2017	GS	CLD	INV:Inventory	22/05/2017 13:50	22/05/2017 15:30						
22/05/2017	GS			22/05/2017 15:30	22/05/2017 17:30						
22/05/2017	GS	CLD	PSD-R:PSD Review	22/05/2017 17:30	22/05/2017 19:30					01:00	
Total Days:				1		00:10				01:00	
Adjustments											
Date	Type	Hours	Remark								
22/05/2017	Award	00:10									
Matrix JPC											

Work Summary

These reports show the detailed job costing summary for selected jobs, phases or projects.

- **Project Summary** - Generates detailed project summary with phase count, user count, job hours and job count details.

Project Summary

←

Date *

07/19/2017

07/19/2017

Project Selection

Select Projects

Project Wise

ProjectCode *

ID

Name

Search

ID	Name	Group	
Newproject	New project	ProjectCode	
priyankpro	Projectpriyank	ProjectCode	
sh	shinjini	ProjectCode	
shalin	qa	ProjectCode	

Generate Report

Organization-1							Page 1 of 1	
Project Summary From 22/05/2017 To 23/05/2017								
Run by: System Admin						Date: 23/05/2017		12:47
Project Code	Name	Date	Phase Count	User Count	Job Hours	Job Count		
CLD	COSEC Cloud	22/05/2017	2	5	19:45	22		
		Summary	2	5	19:45	22		

- **Phase Summary** - Generates detailed phase summary with project count, user count and job hours details.

Phase Summary

←

Date * 07/19/2017 07/19/2017

Phase Selection

Select Phases Phase Wise

PhaseID * ID Name

Generate Report

Organization-1					Page 1 of 1
Phase Summary From 22/05/2017 To 23/05/2017					
Run by: System Admin		Date: 23/05/2017 12:50			
Phase ID	Name	Project Count	User Count	Job Hours	
1	PSD Writing	1	4	13:46	
7	Packing	1	3	05:59	

Click the **Project Count** link to view a Project details sub-report.

- **Job Summary** - Generates detailed job summary with projects, phases, user count and job hours details.

Job Summary

←

Date * 07/19/2017 07/19/2017

JOB Selection

Select JOBS JOB Wise

JobCode * ID Name

Generate Report

Organization-1					Page 1 of 1
Job Summary From 22/05/2017 To 23/05/2017					
Run by: System Admin		Date: 23/05/2017 14:00			
Job Code	Name	Project Code	Phase Code	User Count	Job Hours
INV	Inventory	CLD	PAC	1	00:05
LAB	Labelling	CLD	PAC	2	05:54
PSD-R	PSD Review	CLD	PSD-A	2	06:40
PSD-S	PSD Study	CLD	PSD-A	2	07:06
SAD	SAD study			2	05:35
Total:					25:20

The Field Visit Management (FVM) involves management of user's activities working on field. It allows management of Field Tasks done by users under various Field Schedules. The module shall facilitate viewing of locations and time of visit for the user and ease of punch marking for schedules (as per the rights assigned to them).

With this Module, you can:

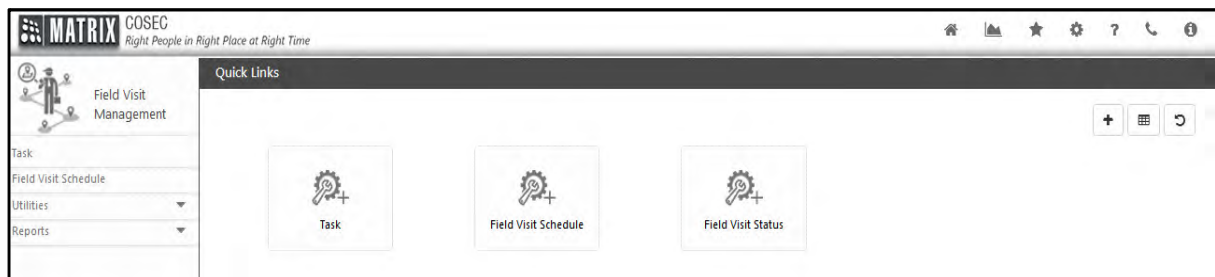
- Assign Daily Field Schedules and Add Locations and Tasks to it.
- Monitor User's Field activities across assigned Field Schedule.

To use the Field Visit Management functions, select the **FVM** module.






The **FVM** page appears as shown

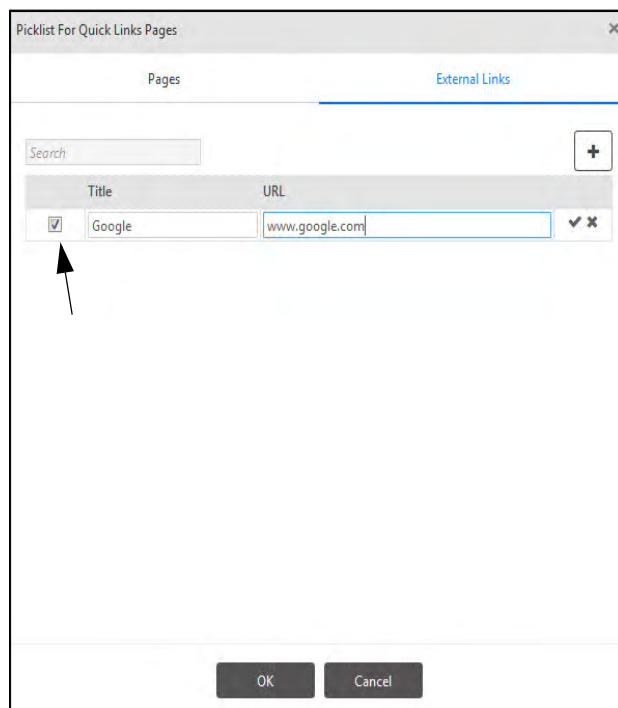
below.



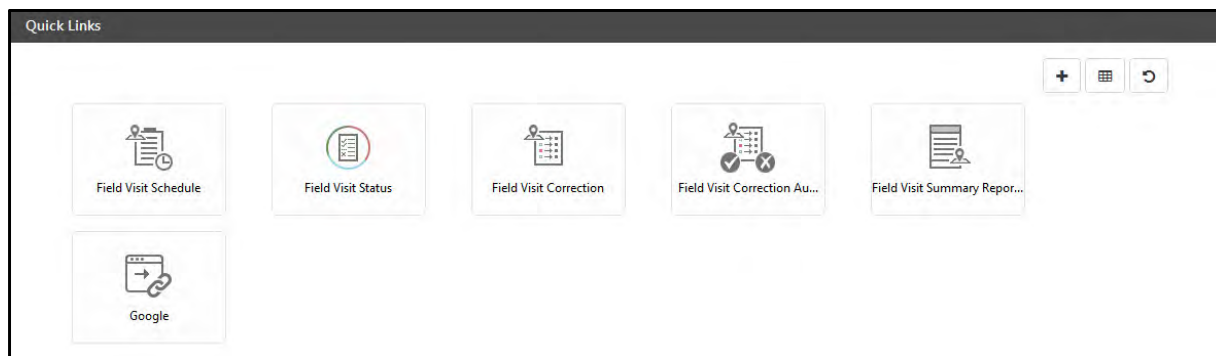
The page displays a menu and **Quick Links** to go to the required page in just one click. Quick Links are shortcuts to reach to a specific page easily. It also contains following three buttons:



- **Add Quick Link:** Click  button to add a quick link. A picklist for Quick Link pages appears for selecting the page or External Link for which the quick link is to be created. Maximum **20** quick links can be added.
- For Adding **Pages** in Quick Link, Select the Pages and click on OK
- For Adding **External Links**, Select External Link tab, click on  button to add new external link.

- Configure the **Title** and **URL** of the external link under the respective fields. click on checkbox to get the configured link on quick link screen as shown below. To save the configuration click on .



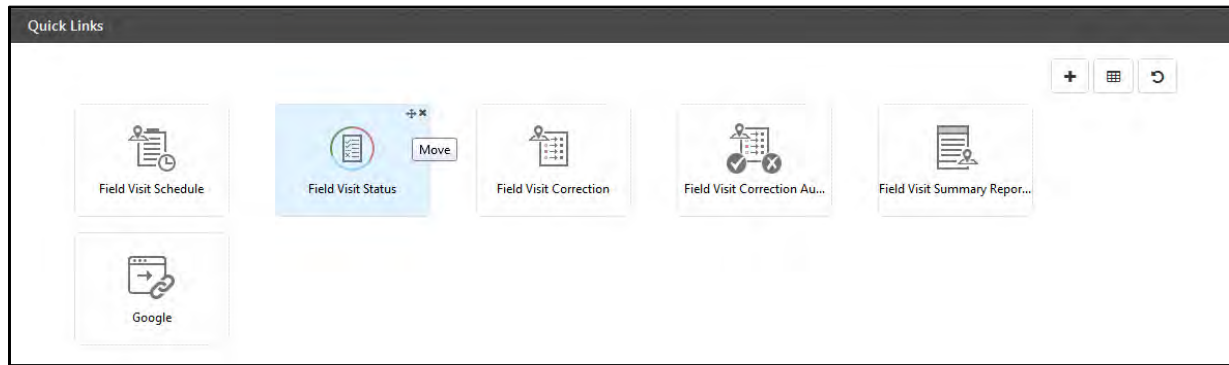
- To edit the saved configuration, click on .
- Click on OK to save the link configuration on Quick Link screen. The external link will be displayed as shown below:



- **Select Layout:** Click  button to select a layout for the quick links. You can select 5x4 or 4x5 layout to manage the quick links.
- **Reset Quick Links:** Click  button to reset the quick links to the default quick links.

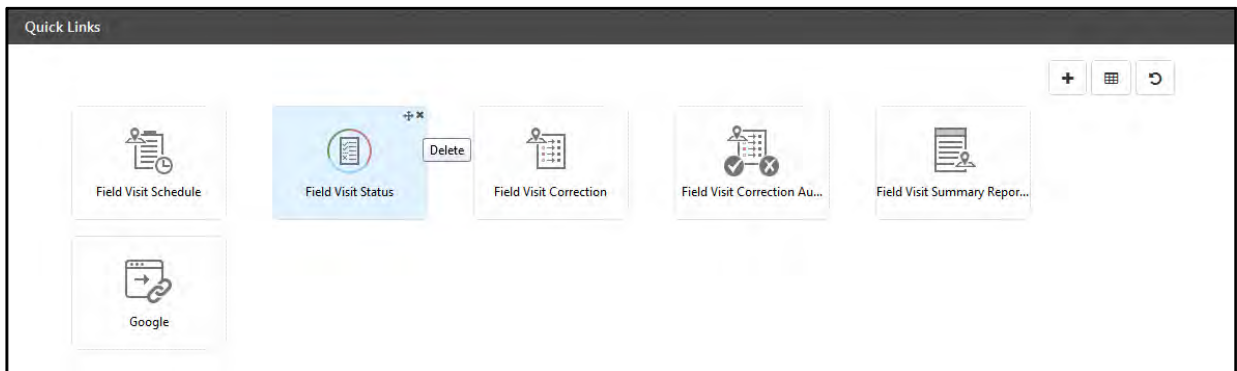
Move the Link

To move the link from one place to another, hover on the link on top right corner and click on “Move” icon as shown below. Then drag the quick link to the desired place. It will be placed at the desired location on the quick links page.



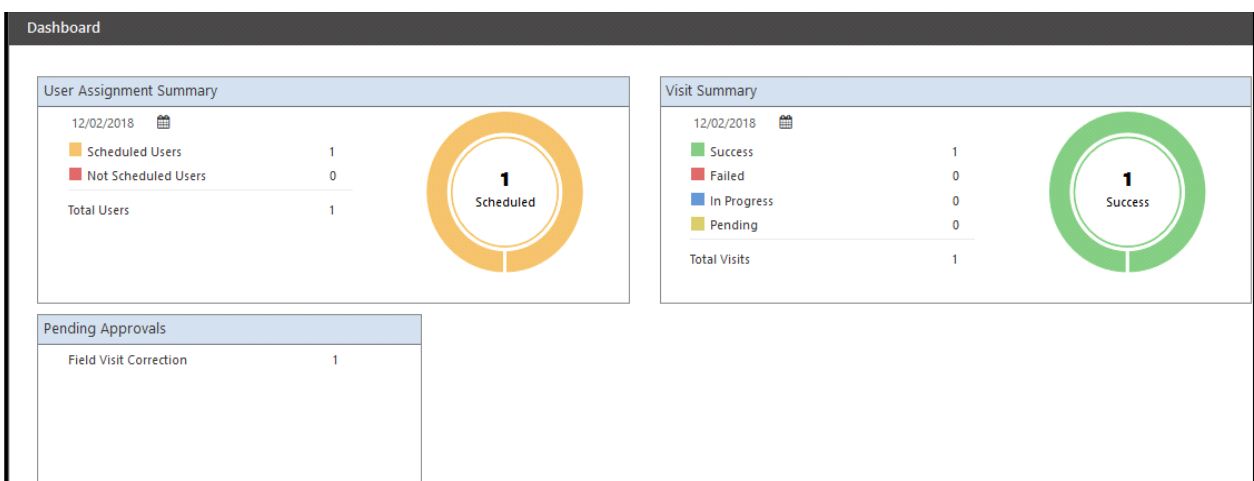
Delete the Link

To delete a particular link, hover on the link on top right corner and click on “Delete” icon as shown below.



Field Visit Management Dashboard

To view the **FVM** Dashboard, click the Dashboard button  on the **FVM** page and the following screen appears.



The Dashboard displays the basic information on Field Visit Management module relating to the COSEC Software under the following groups:

User Assignment Summary


- Scheduled Users - Total number of FVM enabled users having schedules assigned to them on the current date.
- Not Scheduled Users - Total number of FVM users without any assigned schedules on the current date.

Visit Summary

- Success- Shows the count of the FVM users with successfully completed schedules for the current date.
- Failed- Shows the count of the FVM users with the failed schedules for the current date.
- In Progress- Shows the count of the FVM users with the schedules in progress for the current date.
- Pending- Shows the count of the FVM users with pending schedules for the current date.

Pending Approvals

- Field Visit Correction - Shows the count of pending Field Visit Correction requests between current date and the previous year of all the users with login rights.

For more information on the above Dashboard options, click the respective information links on the Dashboard. The latest values on Dashboard are updated on clicking the Refresh  button.

Task

Task page enables to create a list of tasks to be performed by the user. Once the task is created, it is then assigned to the Schedule. Schedule assigned to the user includes various tasks along with the respective locations and time durations.

To create a Task, Select **Field Visit Management module >Task**

The screenshot shows a web application window titled "Task". It features a toolbar with icons for back, add, edit, delete, save, and close. The form has two main sections: "Task" and "Description". The "Task" section has a label "ID" and a text input field containing "Delivering Sample". The "Description" section has a label "Description" and a text area containing "Product sample needs to be delivered by weekend.". On the right side, there is a table with columns "ID" and "Name", and a message "No Data" below it.

Click **New** button to create a new task.

Task: Specify the name of a task to be done by the user. The ID will be autogenerated by the system after the task is saved.

Description: You can give a description for the task that allows the user to know the activities to be performed in the schedule for the day.

Click on **Save** button. The task will be listed in the grid with autogenerated ID.

The screenshot shows the same web application window after the task has been saved. A green notification bar at the top says "Saved Successfully". The "Task" section now shows an autogenerated ID of "1" and the name "Delivering Sample". The "Description" section remains the same. The table on the right now contains one row with ID "1" and Name "Delivering Sample".

The tasks which are created here, will be assigned in the **"Field Visit Schedule"** of the user.

Field Visit Schedule

Field scheduling is the daily activity of assigning field tasks to each user. The users in return are supposed to accomplish the task as per their field schedule.

Select **FVM> Field Visit Schedule**. The Field Visit Schedule page appears as shown below:

The screenshot shows the 'Field Visit Schedule' application window. It features a toolbar with icons for navigation and actions. The main form includes fields for 'User' (FVM1, Jinu), 'Date' (Date, Custom Months, 1), 'Shift/Day', 'Schedule Time' (Date, HHMM, Date, HHMM), 'Task' (ID, Name), 'Select Location' (Randomly), 'Location' (ID, Name), and 'Remark'. There are 'Add' and 'Cancel' buttons. A search bar is at the bottom left. A table at the bottom shows columns for 'Schedule Time', 'Task', and 'Location/Location Group' with 'No Data' below it. On the right, a 'Scheduled Visits' table shows 'No Data'.

User: Select the user from the picklist for whom the field visit is to be scheduled. Only the active users for whom the FVM is enabled from User Configuration, appears here in the picklist.

Date: Select the attendance date on which the field schedule is to be configured. The selection can be done in view mode only. You can also customize the selection by selecting the weekly or monthly option from drop down list.



Before assigning the field schedule, you must process the shift schedule of the FVM user.

Shift/Day: It displays the user's Working Shift on Schedule Date and Assigned Day on Schedule Date. The assigned day can be either Normal, WO, PH or WO/PH.

Schedule Time: Select the From- Date,Time and To-Date,Time to assign the schedule. Time is in HH:MM format.

Eg: In below schedule; 13:00 to 14:00 hours is set as schedule time.

Field Visit Schedule

User: FVM1 | Jinu

Date: 04/27/2017 | Custom Months | 1

Shift/Day: GS | Normal

Schedule Time: 04/27/2017 13:00 - 04/27/2017 14:00

Task: 1 | Delivering Sample

Select Location: Randomly

Location: ID | Name

Remark: Deliver the parcel to HO

Add Cancel

1 Location(s) are Selected

Schedule Time	Task	Location/Location Group
No Data		

Task: Select the task from the picklist which is to be assigned to the selected user.

Select Location: Select the option for location as Randomly or Location Group and select the location where the user is suppose to go and complete the task.



Location and Location groups can be configured from Admin module> System Configuration >Location Master & Location Group.



You must ensure that the location being assigned for the task is already assigned to the user from User Configuration >ESS> Settings> Location Assignment.

Remark: You can specify the Remark while assigning the schedule.

Finally click on **Add** button to add the field visit schedule. The schedule will be listed in the grid. Then Click on **Save** button to save the configured schedule.

Field Visit Schedule ✓ Saved Successfully

User: FVM1 | Jinu

Date: 04/27/2017 | Custom Months | 1

Shift/Day: GS | Normal

Schedule Time: 04/27/2017 HHMM - 04/27/2017 HHMM

Task: ID | Name

Select Location: Randomly

Location: ID | Name

Remark:

Add Cancel

Schedule Time	Task	Location/Location Group
04/27/2017 13:00 - 04/27/2017 14:00	Delivering Sample	Head Office

If **blue tooth** based location is selected then it will appear as shown below:

The screenshot shows the 'Field Visit Schedule' form. The 'Location' field is set to 'BLE'. Below the form, a table lists the schedule details:

Schedule Time	Task	Location/Location Group
2017/09/01 18:00 - 2017/09/01 19:00	task 1	BLE

An arrow points to the 'BLE' location in the table.

Export

You can export the field schedule of selected user.

The screenshot shows the 'Field Visit Schedule' form with the 'Export Field Visit Schedule (Alt+Shift+O)' button highlighted. The 'Date' is set to '04/27/2017'. Below the form, a table lists the schedule details:

Schedule Time	Task	Location/Location Group
04/27/2017 13:00 - 04/27/2017 14:00	Delivering Sample	Head Office

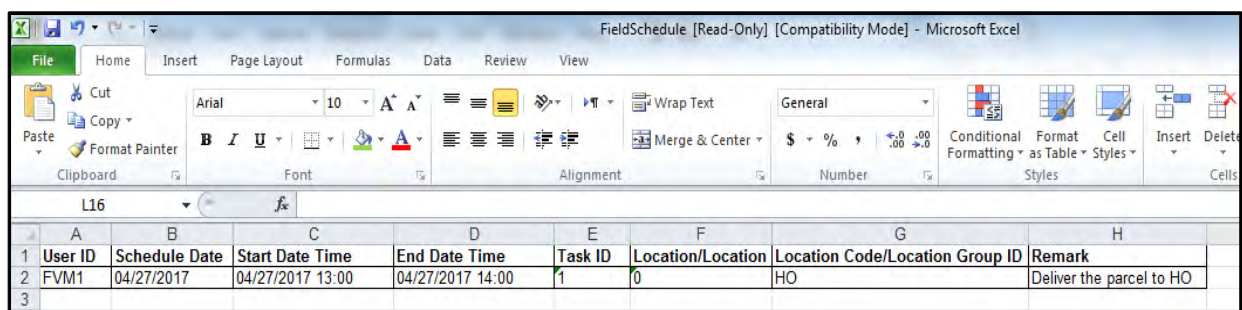
On the right side, a table shows the 'Scheduled Visits' for the selected date:

Date	Scheduled Visits
05/04/2017	1
04/27/2017	1

Select the Field Schedule from the right side which is to be exported.

Then click on **Export** button as shown above. Open or Save the Schedule by specifying the location on your computer.

The exported field schedule is shown as below:

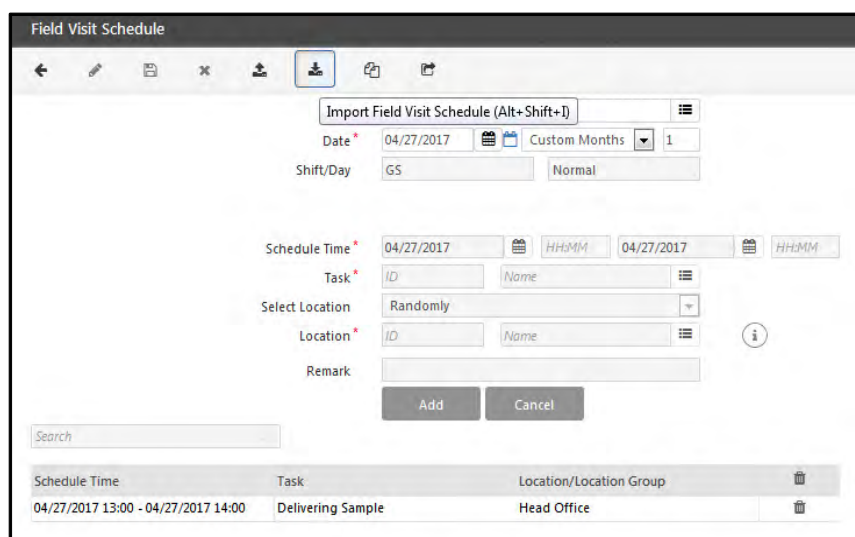


FieldSchedule [Read-Only] [Compatibility Mode] - Microsoft Excel

	A	B	C	D	E	F	G	H
	User ID	Schedule Date	Start Date Time	End Date Time	Task ID	Location/Location	Location Code/Location Group ID	Remark
1	FVM1	04/27/2017	04/27/2017 13:00	04/27/2017 14:00	1	0	HO	Deliver the parcel to HO
2								
3								

Import

The field schedule maintained in your record can be imported here.



Field Visit Schedule

Import Field Visit Schedule (Alt+Shift+I)

Date: 04/27/2017 Custom Months: 1

Shift/Day: GS Normal

Schedule Time: 04/27/2017 HHMM 04/27/2017 HHMM

Task: ID Name

Select Location: Randomly

Location: ID Name

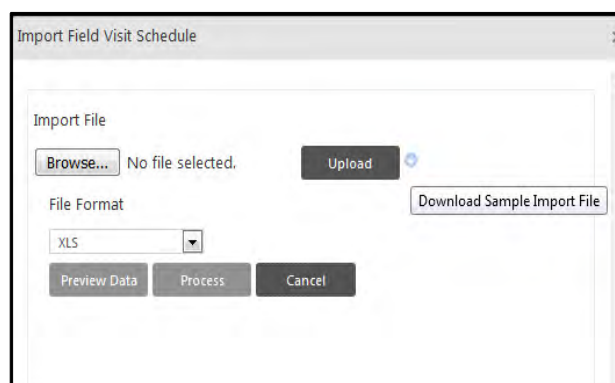
Remark:

Add Cancel

Search

Schedule Time	Task	Location/Location Group
04/27/2017 13:00 - 04/27/2017 14:00	Delivering Sample	Head Office

You can download sample import file and fill the data of multiple user.



Import Field Visit Schedule

Import File

Browse... No file selected. Upload

File Format

XLS

Download Sample Import File

Preview Data Process Cancel

Selecting the **File Format** from the options of XLS,CSV, XLSX. Then **Browse** the file. Click **Upload**. The file will be saved.

Import Field Visit Schedule

File saved successfully...

Import File

Browse... ImportData.csv Upload

File Format

CSV

Preview Data Process Cancel

To view the preview of data click **Preview Data**. The data will be shown as below. Now you can click **Process** to import the file. The success of import will be shown in the success column.

Import Field Visit Schedule

Import File

Browse... ImportData.csv Upload

File Format

CSV

Preview Data Process Cancel

Process Error Description

Search

User ID	Schedule Date	Start Date Time	End Date Time	Task ID	Location/Location Group Filter	Location Code/Location Group ID	Remark
FVM1	10/3/2016	4/5/2017 9:00	4/5/2017 11:00	1	0	HO	Deliver to HO
U1	10/3/2016	10/3/2016 13:00	10/3/2016 19:00	2	1	1	
U2	10/3/2016	10/3/2016 9:00	10/3/2016 13:00	1	0	LOC2	

Copy Field Schedule

You can copy/transfer field schedule from one user to multiple users.

The screenshot shows the 'Field Visit Schedule' window. At the top, there is a toolbar with icons for back, edit, save, delete, add, and copy. The 'Copy' icon is highlighted with a blue box. Below the toolbar, the 'User' field is set to 'Copy Field Visit Schedule (Alt+Shift+W)'. The 'Date' field is set to '05/04/2017' with a calendar icon. The 'Shift/Day' field is set to 'GS' and 'Normal'. The 'Schedule Time' field is set to '05/04/2017' with a calendar icon. The 'Task' field is set to 'ID' and 'Name'. The 'Select Location' field is set to 'Randomly'. The 'Location' field is set to 'ID' and 'Name'. The 'Remark' field is empty. There are 'Add' and 'Cancel' buttons. On the right side, there is a table with 'Date' and 'Scheduled Visits' columns. The table contains the following data:

Date	Scheduled Visits
05/05/2017	1
05/04/2017	1
05/03/2017	1
04/27/2017	1

At the bottom, there is a table with 'Schedule Time', 'Task', and 'Location/Location Group' columns. The table contains the following data:

Schedule Time	Task	Location/Location Group
05/04/2017 09:00 - 05/04/2017 10:00	Pickup Enclosure	Head Office

Select the Field Schedule to be copied. Then click on **Copy** button as shown above. The following Copy window appears.

The screenshot shows the 'Copy Task of FVM1' window. The 'Date' field is set to '05/04/2017' with a calendar icon. There is a 'Search' field. Below the search field, there is a table with 'Schedule Time', 'Task', 'Location/Location Group', and 'Remark' columns. The table contains the following data:

Schedule Time	Task	Location/Location Group	Remark
05/04/2017 09:00 - 05/04/2017 10:00	Pickup Enclosure	Head Office	

Below the table, there is a 'Copy To' section. The 'Date' field is set to '05/04/2017' with a calendar icon. The 'User' field is set to 'ID' and 'Name'. There is a 'Search' field. Below the search field, there is a table with 'User ID', 'Name', 'From Date', and 'To Date' columns. The table contains the following data:

User ID	Name	From Date	To Date
1678	Supriya	05/04/2017	05/04/2017

At the bottom, there is a 'Process' button.

You can select the task from the selected schedule to be copied by checking the respective boxes. Then select the **Date** and **User** to whom the schedule is to be copied. Now click on **Process** button to initiate the copy process.

Select the **Date** and **User** from the picklist to whom the task is to be assigned.

Then click on **Process** to reassign the task. The task will be removed from the current user schedule and will be assigned to the selected user.



Whenever any change is made in Field Schedule records then Tx_Schedule status, 1st IN and Last OUT punch should be reset to NULL. They will be updated once user executes daily process for the date after making changes in field schedule.

Field Visit Status

The users are supposed to accomplish the task as per their field schedule on daily basis. According to the punches from field, user's field records are considered as completed or not completed.

You can use COSEC APTA, ESS Module or Device for marking punch.

Field Visit Status page enables admin or reporting in-charge to view field status of selected user in a calendar view.

Select **FVM> Utilities> Field Visit Status**. The Field Visit Status page appears as shown below:

The screenshot shows the 'Field Visit Status' page. On the left is a sidebar with a 'Field Visit Management' icon and a menu with options: Task, Field Visit Schedule, Utilities (expanded), Field Visit Status (selected), Field Visit Correction, Field Visit Correction Authorization, and Reports. The main area has a header 'Field Visit Status' with a back arrow and a refresh icon. Below the header are input fields for 'User' (ID and Name), 'Attendance Period' (Month and Year), and a calendar grid. The calendar grid shows days of the week (MON to SUN) and dates (1 to 31). The date 4 is highlighted in blue.

Select the **User** from the picklist whose field visit status is to be viewed.

Select the **Attendance period** as Month and Year for which field visit status is to be viewed.

You can select the option to view as **Schedule Status** or **Visited Location**.

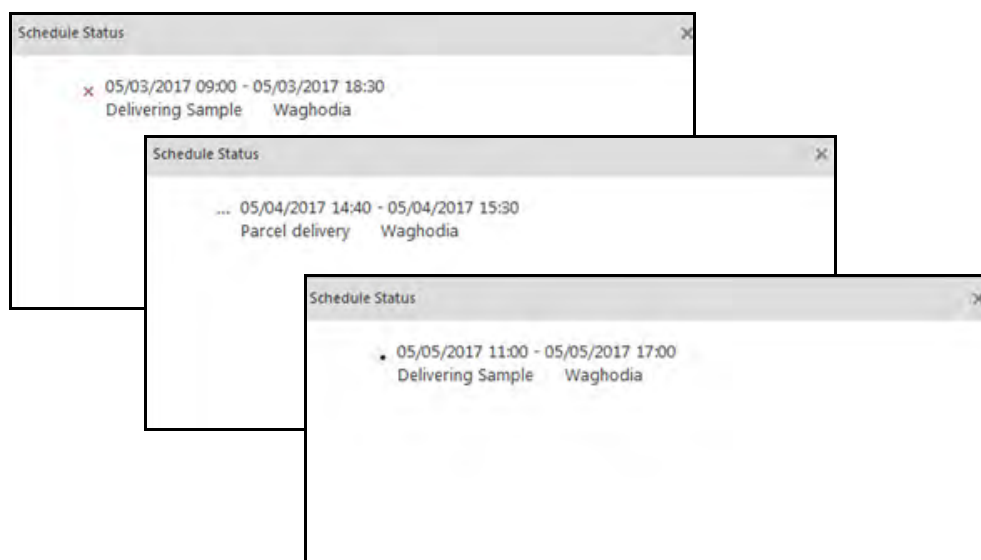
The screenshot shows the 'Field Visit Status' page with the 'Schedule Status' option selected. The calendar grid displays task status indicators for each day. The date 4 is highlighted in blue. An arrow points to the date 5, which has a '1' above it, indicating a future task. The calendar grid shows days of the week (MON to SUN) and dates (1 to 31). The date 4 is highlighted in blue.

Schedule Status: The status of completed, not completed, on-going and future task is shown in the calendar.

Visited Location: The visited location count will be shown for the respective date in the calendar.

- The green circular ring shows that task is completed.
- Partial green and remaining red shows partially completed task.
- Full red shows incomplete task.
- A number in the grid of future date shows future days task count.

Clicking on the window will show the task details. Tick displays completed task and Cross displays incomplete task. On going task are displayed by dotted. 2/3 shows that 2 task out of 3 are completed.



Once the user completes the field visit schedule and punches into COSEC APTA from the scheduled location then the field visit status will be marked as green as shown below.

<div> <div>User</div> <div>VP</div> <div>Vivek</div> <div>Attendance Period</div> <div>May</div> <div>2017</div> <div>Schedule Status</div> </div>						
MON	TUE	WED	THU	FRI	SAT	SUN
	2	3	4	5	6	7
	GS	GS	PR-PRIGS	PR-PRIGS	GS	WO
	9	10	11	12	13	14

If the user has visited the location, then the number will be shown on that date. In below figure 1 indicates that user Vivek has visited 1 location on 4th May2017.

User:

Attendance Period:

Visited Locations

	WED	THU	FRI	SAT	
3		4	5	6	7
GS	PR-PRGS	1	PR-PRGS	GS	WO
10	11	12	13	14	

Tasks View

- ☐ Schedule Status
- ☒ Visited Locations

You can use COSEC API to mark the user punches from the desired location.

The schedule based on **bluetooth based location** is shown as below.

Field Visit Status

User:

Attendance Period:

Schedule Status

MON	TUE	WED	THU	FRI	SAT	SUN
				1	2	3
				GS	PR-PRGS	WO
4	5	6	7	8	9	10
GS	WO	GS	GS	GS	GS	GS
11	12	13	14	15	16	17
WO	GS	WO	GS	GS	GS	GS

To know the status of the schedule click on the circle shown above and the schedule status appears as shown below.

Schedule Status

User: 2192 **Date:** 2017/09/01 **Shift:** GS

✓ 2017/09/01 18:00 - 2017/09/01 19:00 - task 1 - BLE

Field Visit Correction

The punches marked from COSEC APTA may require correction in some cases.

Suppose If user was scheduled for some task at some location and couldn't go because of any reason. So changing punch date-time and adding or modifying its comment would be possible from the Field Visit Correction page. Also the Location can be added or updated from this page.

The Field Visit Correction can be made by:

- System Account User
- On Behalf System Account User
- Using the ESS Self Service Module (For more details refer COSEC Employee Self Service User Manual)

COSEC Web enables all *System Account users* with appropriate page rights to make Field Visit Correction using the *Field Visit Management* module. All applications made by the System Account user are *pre-approved* by default.

COSEC Web also enables all On Behalf System Account User with appropriate page rights to make Field Visit Correction using the *Field Visit Management* module. All applications made by the On Behalf System Account User are *pre-approved* by default. For creating and assigning the roles and rights to the On Behalf System Account User. Refer to ["On Behalf System Account User"](#).

Select **FVM > Utilities > Field Visit Correction**. The Field Visit Correction page appears as shown below:

The screenshot displays the 'Field Visit Correction' interface. On the left is a sidebar with a 'Field Visit Management' icon and a list of options: Task, Field Visit Schedule, Utilities, Field Visit Status, Field Visit Correction (highlighted), Field Visit Correction Authorization, and Reports. The main content area is titled 'Field Visit Correction' and includes a search bar, a user selection dropdown, and a date picker. Below these are input fields for 'Attendance Date', 'Shift/Day', 'Attendance Status', 'Status Summary', 'Work Hours', and 'Schedule Status'. A table on the right shows columns for 'Date', 'Shift', '1st Half', '2nd Half', 'Work Hours', and 'Schedule Status', with a 'No Data' message. At the bottom, there is a table with columns for 'Date', 'Time', 'IO Type', 'Location', and 'Comment', also showing 'No Data'.

User: Select the User from the picklist for whom field visit correction is to be applied.

Field Visit Correction

User* FVM1 Jinu

Attendance Date 05/04/2017 Custom Months 1

Attendance Details

Shift/Day GS Normal

Attendance Status AB AB

Status Summary No Punches Available

Work Hours HH:MM

Schedule Status Fail

Events

Search

Date	Time	Location	Comment
No Data			

Attendance Date: Select the **Date** from the grid for which attendance correction is to be done or select the date from the calendar button. You can also select week or month filter to view the punches accordingly.

Field Visit Correction

User* FVM1 Jinu

Attendance Date 05/04/2017 Custom Months 1

Attendance Details

Shift/Day GS Normal

Attendance Status AB AB

Status Summary No Punches Available

Work Hours HH:MM

Schedule Status Fail

Events

Search

Date	Time	Location	Comment
05/04/2017	14:45	Waghodia	
05/04/2017	15:30	WAG Waghodia	Left after completing task

OK

You can edit the punches by clicking on **Edit** button in the attendance details row where the correction is to be done.

Click **Event** if you desire viewing events of the respective user.

To add the new punches click **Add** button.

Enter the **time** and select the **location** from the pick-list. The Bluetooth based location is selected in following example.

Search

Date	Time	Location	Comment
2017/09/01	18:00	BLE	
2017/09/01	21:00	Makarpura- HO	

+

You can mention the **comment**. Then click on OK and Save to save the correction.



If Map is not loaded; check the network connection of your PC or check the value of Google API Key from Admin Module > System Configuration > Global Policy > Basic tab.

The Field Visit Correction application will be authorized by the Reporting In-charge or Administrator.

[See “Field Visit Correction Authorization” on page 2159.](#)

The Schedule Status will show **Success** when the scheduled task is complete.

Date	Shift	1st Half	2nd Half	Work Hours	Schedule Status
2016/10/18	GS				
2016/10/17	GS				
2016/10/16	GS	AB	AB		
2016/10/15	GS	IN			Success
2016/10/14	GS	AB	AB		Success
2016/10/13	GS	IN			Success
2016/10/12	GS	AB	AB		
2016/10/11	GS	AB	AB		
2016/10/10	GS	AB	AB		

The FVM user punches within shift can also be viewed from Daily Attendance View of T&A module.

Field Visit Correction Authorization

ESS user have provision to add/edit punch date, time, IO type, location and add comment for each of the punches. Such corrections are required to be authorized. So the administrator can approve/reject field visit correction applications.

The authorization is dependent on the number of Reporting In-charge in the Routing Group, the Authorization Mode as well as the Approval Policy assigned by the system administrator. For details refer to [“Reporting In-Charge”](#), [“Approval Policy”](#) and [“Configuring Users”](#).

To authorize field visit correction application select **FVM > Utilities > Field Visit Correction Authorization**. The Field Visit Correction Authorization page appears as shown below:

You can either:

- view all the pending Field Visit Correction Authorizations
- set the filters — Date, Filter Users — to view the desired applications

All Pending Applications

To view only Pending Applications,

- **Show All Pending Applications:** Select this option to enable the pending application filter.
- Click the **Pending** collapsible panel. All the applications in pending state appear.

To approve the application, select the **Approve** check box of the desired entry.

To reject the application, select the **Reject** check box of the desired entry.

To know more, refer to [“Pending Application”](#).



The population on this page depends on the server's database. It might take time to load all pending applications.

Applications according to Set Filters

To Set the Filters,

- **Date:** Select this option to enable the date filter. Select the date range for which the Field Visit Correction Applications are to be viewed.
- **Filter Users:** You can filter records according to the desired Enterprise Group, All or for an Individual.

Select **All**, to view authorization status of the applications of all the active users on the system.

Select **Individual**, to view authorization status of the applications of a single user. Click the picklist to select the desired User ID/Name.

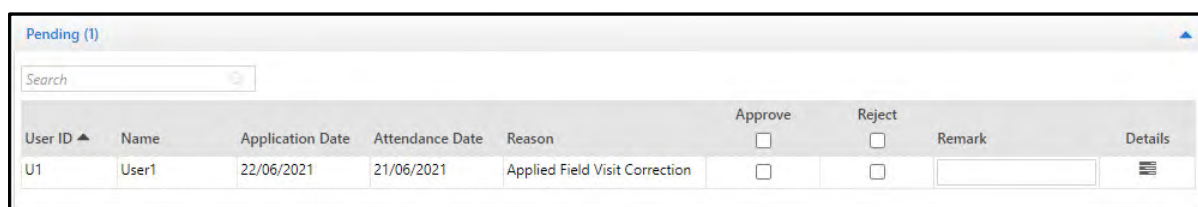
Select the desired Enterprise Group — Organization, Branch, Department, Section, Category, Grade, Designation, Custom Group1/2/3 and then click the picklist to select the desired group's ID/Name, to view authorization status of these applications.

Click on **View** to view the Pending, Approved and Rejected applications.

Pending Application

Click the **Pending** collapsible panel. The **Pending** section displays all the applications that yet to be authorized by the RIC or the System Administrator.

The following screen displays the **Pending** section.



The screenshot shows a web application window titled "Pending (1)". It contains a search bar and a table of pending applications. The table has columns for User ID, Name, Application Date, Attendance Date, Reason, Approve, Reject, Remark, and Details. A single row is visible for User ID "U1", Name "User1", Application Date "22/06/2021", Attendance Date "21/06/2021", and Reason "Applied Field Visit Correction". There are checkboxes for Approve and Reject, a text field for Remark, and a Details icon.

User ID ▲	Name	Application Date	Attendance Date	Reason	Approve	Reject	Remark	Details
U1	User1	22/06/2021	21/06/2021	Applied Field Visit Correction	<input type="checkbox"/>	<input type="checkbox"/>		

When any application is in the Pending state it can be authorized by the Admin or RIC.

- To approve/reject applications selectively, click the respective application check box against the user.
- To approve/reject all the applications simultaneously, click the Approve /Reject check box in the header column.

Once the Admin approves/ rejects the application, the record will be moved from the **Pending** section to the **Approved/ Rejected** section respectively.

The default **Remark** for the Approved and Rejected application will appear in the respective fields. You can enter any customized Remark while authorizing the application.

To view the details of the application, click **Details** . The **All Field Punches** window appears as shown below.

The screenshot shows a window titled "All Field Punches" with a close button (X) in the top right corner. The window contains the following fields and sections:

- User:** Two input fields, the first containing "U1" and the second containing "User1".
- Attendance Date:** A date input field containing "21/06/2021".
- Shift/Day:** Two dropdown menus. The first is set to "GS" and the second is set to "Normal".
- Attendance Status:** Two dropdown menus, both set to "TO".
- Attendance Values:** A dropdown menu set to "On Application".
- Schedule Status:** An empty input field.
- Reason:** An input field containing "Applied Field Visit Correction".
- Search:** A search bar with a magnifying glass icon.
- Table:** A table with 5 columns: Date, Time, IO Type, Location, and Comment. It contains one row with the following data:

Date	Time	IO Type	Location	Comment
11/06/2021	11:14	In		
- Approval Details:** A section header with a clock icon.
- Table:** A table with 3 columns: Incharge, Status, and Remark. It contains one row with the following data:

Incharge	Status	Remark
SA - System Admin		

All Field Punches window displays the attendance details.

Attendance Values has the following options:

- **On Application:** The transaction values shown are the values at the time of the application being done.
- **Applied:** The transaction values after the correction is being made.
- **Current:** The current transaction values are same as On Application values.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer ["Approval Policy"](#).

Remark displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.

Approved Applications

Click the **Approved** collapsible panel. The **Approved** section displays all the applications that have been approved by the RIC or the System Administrator.

The following screen displays the **Approved** section with approved applications:

Approved (5)									
Search									
User ID ▲	Name	Application Date	Attendance Date	Reason	Approve <input checked="" type="checkbox"/>	Reject <input type="checkbox"/>	Remark	Details	
U1	User1	22/06/2021	21/06/2021	Applied Field Visit Correction	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Field Visit Correction		
U1	User1	11/06/2021	10/06/2021	Applied Field Visit Correction	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Field Visit Correction RG1		
U4	User4	10/06/2021	02/06/2021	Applied Field Visit Correction	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Field Visit Correction RG2		
U4	User4	10/06/2021	07/06/2021	Applied Field Visit Correction	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Field Visit Correction RG2		
U5	User5	14/06/2021	11/06/2021	Applied Field Visit Correction	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Approved Field Visit Correction SA		

Click the **Details** icon to view the attendance details of the corresponding user.

All Field Punches window appears as shown below:

All Field Punches

User

U5

User5

Attendance Date

11/06/2021

Shift/Day

GS

Normal

Attendance Status

AB

AB

Attendance Values

On Application

Schedule Status

Reason

Applied Field Visit Correction

Search

Date	Time	IO Type	Location	Comment
11/06/2021	11:14	In		

Approval Details

Incharge

Status

Remark

SA - System Admin	<div><div></div><div>(14/06/2021 11:26)</div></div>	Approved Field Visit Correction SA
-------------------	---	------------------------------------

All Field Punches window displays the attendance details.

Attendance Values has the following options:

- **On Application:** The transaction values shown are the values at the time of the application being done.
- **Applied:** The transaction values after the correction is being made.

- **Current:** The current transaction values are same as On Application values.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remark displays the comments provided by the Admin/ RIC/ System.

Click **Save** to save the authorization.

Rejected Applications

Click the **Rejected** collapsible panel. The **Rejected** section displays all the applications that have been rejected by the RIC or the System Administrator.

The following screen displays the **Rejected** section with rejected applications:

Rejected (2)									
Search									
User ID ▲	Name	Application Date	Attendance Date	Reason	Approve	Reject	Remark	Details	
U1	User1	22/06/2021	21/06/2021	Applied Field Visit Correction	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Rejected Field Visit Correction		
U4	User4	10/06/2021	10/06/2021	Applied Field Visit Correction	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Rejected Field Visit Correction RG1		

Click the **Details** icon to view the attendance details of the corresponding user.

All Field Punches window appears as shown below:

The screenshot shows the 'All Field Punches' window with the following details:

- User:** U1 (ID) / User1 (Name)
- Attendance Date:** 21/06/2021
- Shift/Day:** GS (Shift) / Normal (Day)
- Attendance Status:** TO (Status)
- Attendance Values:** On Application (Value)
- Schedule Status:** (Empty field)
- Reason:** Applied Field Visit Correction

Below the form is a search bar and a table with the following data:

Date	Time	IO Type	Location	Comment
21/06/2021	09:00	In	HO	

Below the table is the **Approval Details** section, which includes a table showing the approval status:

Incharge	Status	Remark
SA - System Admin	⊗ (22/06/2021 10:58)	Rejected Field Visit Correction

All Field Punches window displays the attendance details.

Attendance Values has the following options:

- **On Application:** The transaction values shown are the values at the time of the application being done.
- **Applied:** The transaction values after the correction is being made.
- **Current:** The current transaction values are same as On Application values.

It also displays the status of the user's application under **Approval Details**. The application's status is displayed in the **Status** column.

System can auto approve / reject an application if the Reporting In-charge or SA fails to authorize it as per the Approval Policy assigned to the Reporting Groups. To know more about the Approval Policy, refer "[Approval Policy](#)".

Remarks displays the comments provided by the Admin / RIC / System.

Click **Save** button to save the changes.

Field Visit Management Reports

These reports can be obtained using the **Reports** section under the **Field Visit Management** add-on module. The Reports can be categorized as follows:

[“Schedule Status Summary”](#)

[“Field Visit Summary Report”](#)

Schedule Status Summary

This report gives information about whether user went to each location as per the schedule or not. This report shows status of each schedule date and for each mapping of time slot-task-location. It will also convey about the time spent in that location..



Daily Attendance Process must be done to get correct information in the report.

Status Summary							
Find...							
1 of 1 100%							
Report							
Organization-1							
Page 1 of 1							
Organization-Wise Schedule Status Summary From 2016/05/15 To 2016/06/14							
Run by: System Admin		Date: 2016/06/14		14:58			
Schedule Start	Schedule End	Task	Schedule Location	Transaction Status	IN Punch	OUT Punch	Time Spent
Organization-1							
2							
2016/06/02		Schedule Status:	Success				
2016/06/02-09:00	2016/06/02-10:00	1-Task 1	L1-Location 1	Success	2016/06/02-09:01		
2016/06/02-10:00	2016/06/02-11:00	2-Task 2	L2-Location 2	Success	2016/06/02-10:30	2016/06/02-10:30	00:00
2016/06/02-13:00	2016/06/02-14:00	3-Task 3	L3-Location 3	Success	2016/06/02-13:00	2016/06/02-13:15	00:15
2016/06/08							
2016/06/08-10:00		Schedule Status:	Success				
	2016/06/08-20:00	2-Task 2	L2-Location 2	Success	2016/06/08-15:00		
4							
2016/06/01		Schedule Status:	Fail				
2016/06/01-09:00	2016/06/01-12:00	1-Task 1	L1-Location 1	Success		2016/06/01-11:07	
2016/06/01-15:00	2016/06/01-18:00	2-Task 2	L2-Location 2	Fail			
2016/06/01-15:00	2016/06/01-18:00	2-Task 2	L3-Location 3	Fail			







Field Visit Summary Report

This report shows the time spent by the user in travelling between two locations and time spent at a particular location. Along with this, it also shows visiting time spent for selected date range so that the Administrator can get an overview of the actual work done by employees.

Field Visit Summary

←

Back

   Find...    1 of 1 100%

Main Report

Organization-1

Page 1 of 1

Organization-Wise Field Visit Summary From 2016/05/15 To 2016/06/14

Run by: System Admin Date: 2016/06/14 14:45


Sr No	Location	IN Punch Date-Time-SPFID	OUT Punch Date-Time-SPFID	Visit Time	Travel Time
Organization-1					
2		User 2			
2016/06/02					
1	L1-Location 1	02/06/2016 09:01:00			
2	L2-Location 2		02/06/2016 10:30:00		01:29
3	L1-Location 1		02/06/2016 10:30:00		00:00
4	L2-Location 2	02/06/2016 10:30:00			00:00
5	L3-Location 3		02/06/2016 11:00:00		00:30
6	L2-Location 2	02/06/2016 11:11:00			00:11
7	L3-Location 3	02/06/2016 13:00:00	02/06/2016 13:15:00	00:15	01:49
Total :				00:15	03:59
2016/06/08					
1	L2-Location 2	08/06/2016 15:00:00			
Total :				00:00	00:00
Grand Total :				00:15	03:59
4		User 4			

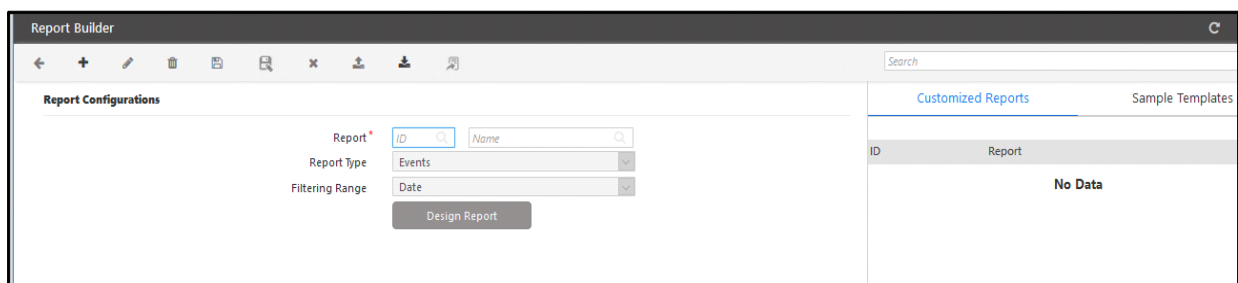
Report Builder helps the users to design their own report template, format the fields as per their expectations and generate reports as and when required.

After designing the Reports; it can be deployed in desired module.

With this Module, you can:

- Design new reports
- Define Calculated fields
- Enrich reports with various formatting styles
- Import/Export report templates

To use the Report Builder, select the **Report Builder** module . The **Report Builder** page appears as shown below.




Multi-language is not supported in Reports generated via Report Builder.

Example of Report Designs

Event Type Report

Report Builder

IN/OUT Punch Posting Report

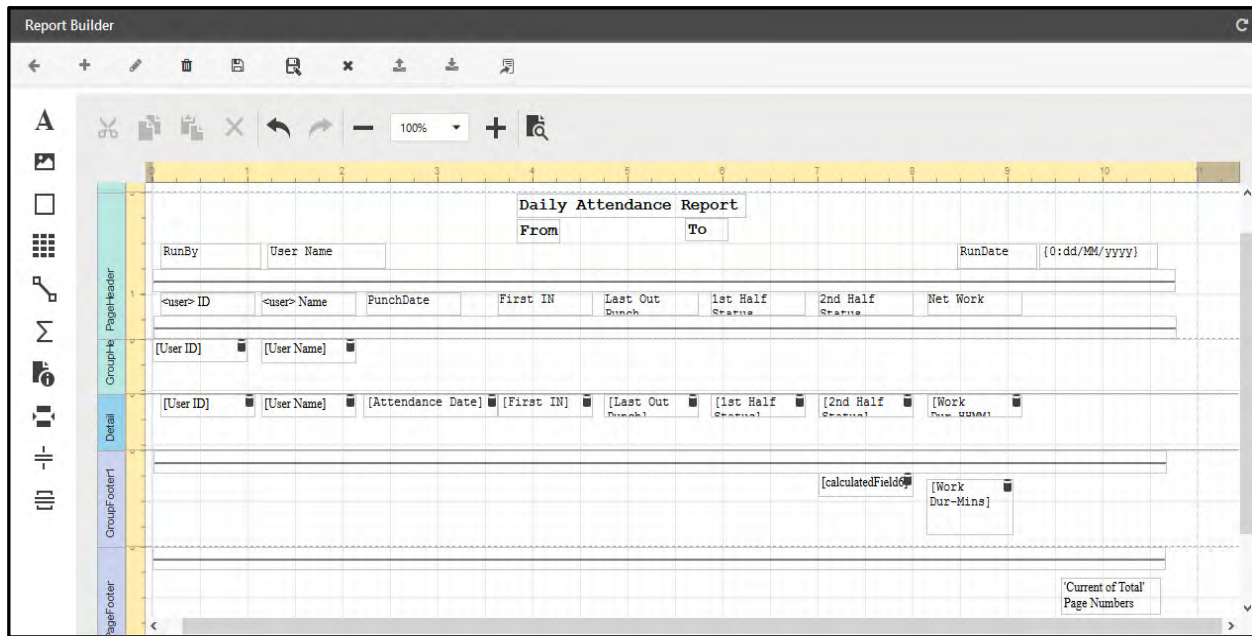
Run By: User Name Current Date and Time

Sr.No.	User ID	User Name	Designation	Department	Punch Date	Punch Time	Punch Delay	Entry/Exit Type	Device Name	Site Name
[Department ID] [Department Name]										
tableCell[User ID] [User Name] [Designation] [Department] [punch date] [event time] [event delay] [event type] [Device Name] [Site Name]										

Preview of Report:

IN/OUT Punch Posting Report										
Run By:		System Admin			31 January 2018					
Sr.No.	User ID	User Name	Designation	Department	Punch Date	Punch Time	Punch Delay	Entry/Exit Type	Device Name	Site Name
1		Department1								
1	1	User 1	Designation1	Department1	01/11/2017	9:0	0:30	Main Entrance	Site-1	
2	1	User 1	Designation1	Department1	01/11/2017	18:30	0:5	Main Entrance	Site-1	

Daily Attendance Details type Report

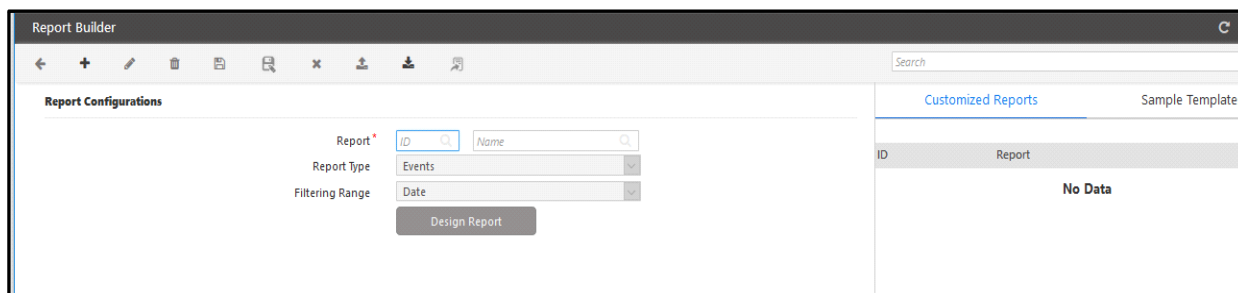


Preview of Report:

Daily Attendance Report							
RunBy	System Admin	From To		RunDate 31/01/2018			
<user> ID	<user> Name	PunchDate	First IN	Last Out	1st Half Status	2nd Half Status	Net Work
1	User 1						
1	User 1	01/11/2017 00:00:00	31/01/2018 09:00:00	31/01/2018 18:30:00	FR	FR	08:30
1	User 1	02/11/2017 00:00:00	31/01/2018 08:30:00	31/01/2018 18:30:00	FR	FR	10:00
1	User 1	03/12/2017 00:00:00			WO	WO	00:00
						199:17	1110
10	User 10						
10	User 10	10/10/2015 00:00:00	31/01/2018 08:00:00	31/01/2018 22:00:00	FR	FR	13:30

Report Configuration

The Report Configuration page appears showing the Customized Reports and Sample Templates.



Report Builder

Report Configurations

Report * ID Name

Report Type Events

Filtering Range Date

Design Report

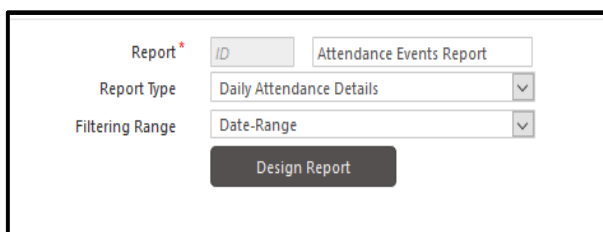
Customized Reports Sample Templates

ID	Report
No Data	

Add New Customized Report

To add a new report format click on **New** button.

Report: Enter the Name of report template. The ID will be auto-generated by the system when the report is saved.



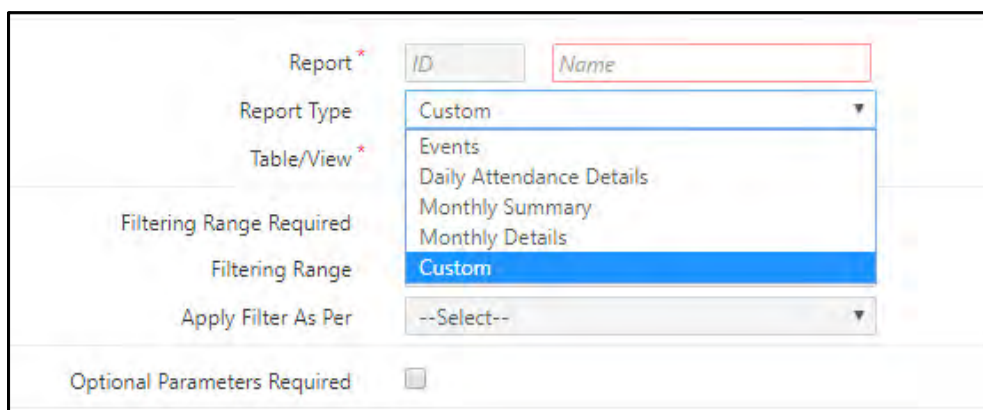
Report * ID Attendance Events Report

Report Type Daily Attendance Details

Filtering Range Date-Range

Design Report

Report Type: Select the type of Report from the options like: Events, Daily Attendance Details, Monthly Summary, Monthly Details and Custom. The Field List will be available as per the selected Report Type.



Report * ID Name

Report Type Custom

Table/View * Events
Daily Attendance Details
Monthly Summary
Monthly Details
Custom

Filtering Range Required

Filtering Range

Apply Filter As Per --Select--

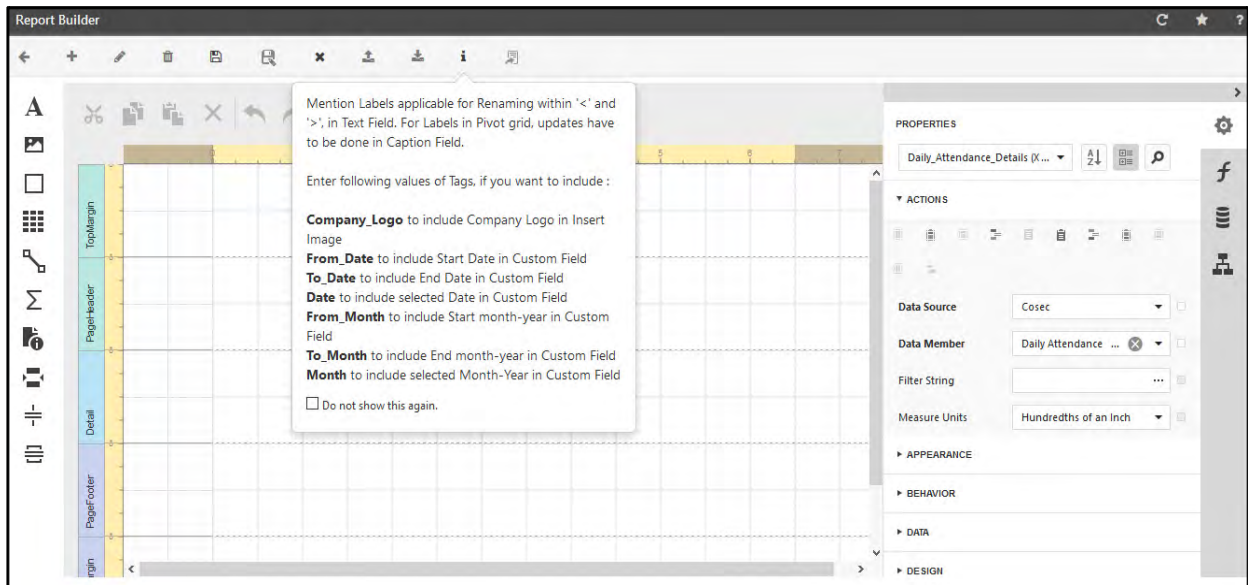
Optional Parameters Required ☐



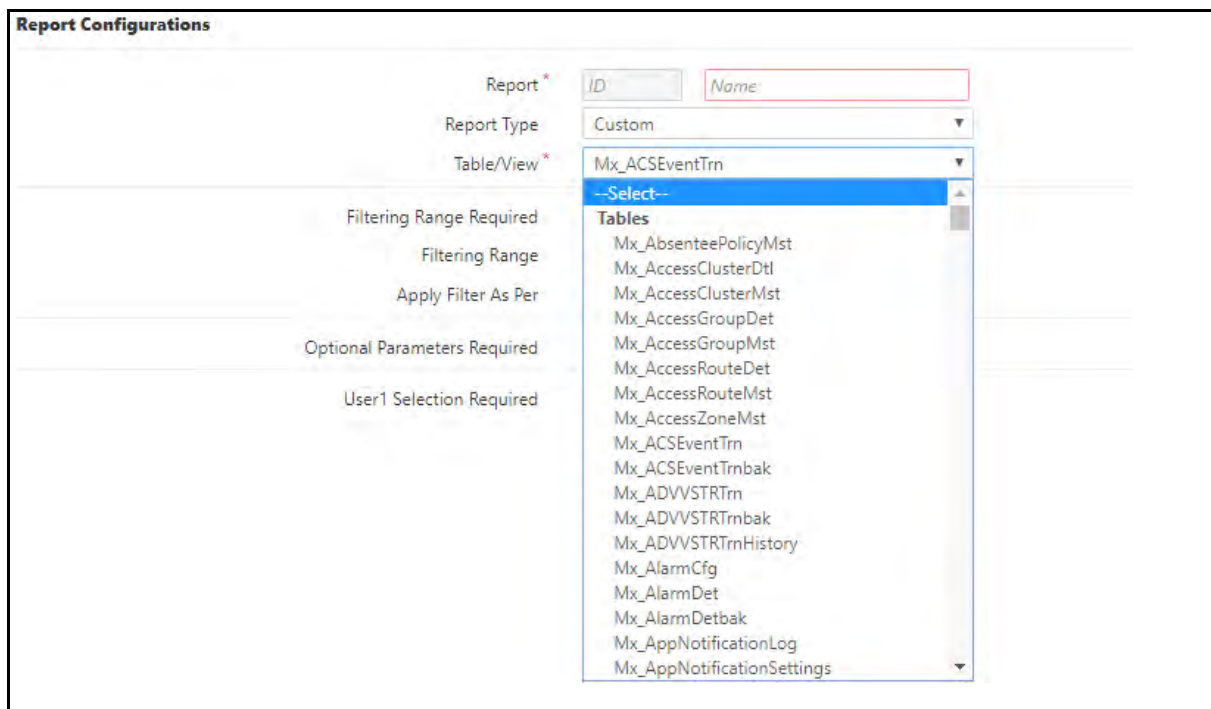
Report Type depends on available license. Daily Attendance Details, Monthly Summary & monthly details will be available only if T&A license is available.

Filtering Range: Select the filtering range for report. It depends on selection of Report Type, i.e., Date and Date-Range for Type= Events/Daily Attendance and Month and Month -Range for type= Monthly

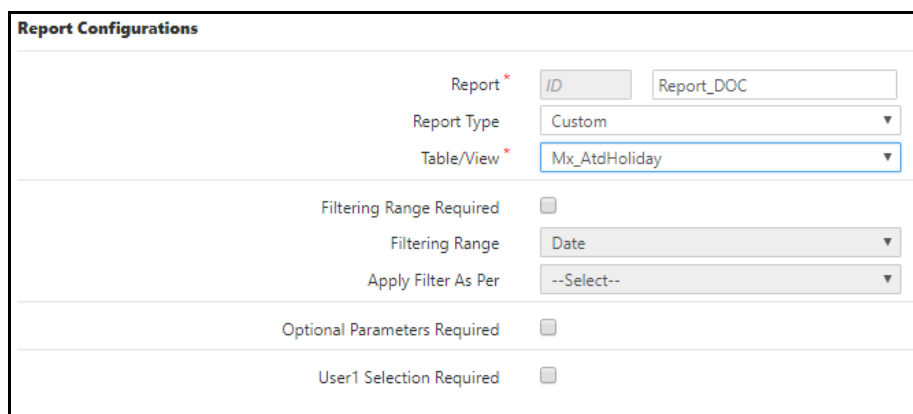
Click on **Design Report** button. The Report Builder window appears as shown below from where report template can be designed.



If the report type is selected as '**Custom**' then user can design report as desired. The configuration is as explained below.



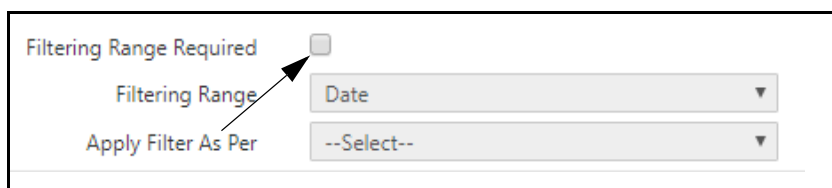
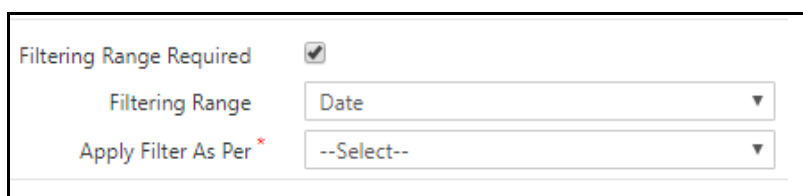
Table/View: Select (database) “Table” from the drop-down list as per your requirement. For example: ‘Mx_AtdHoliday’, Mx_AppNotificationLog etc.




The below mentioned History tables have been removed from the system. If you have used these tables in your report configurations, then those reports will not work. You must re-configure these reports.

Removed History tables: Mx_ADVSTRTrnHistory, Mx_AtdCorrectionHistory, Mx_ATDEventAuthHistory, Mx_DATDAuthHistory, Mx_DATDShtLVOclHistory, Mx_FVMFieldCorrHistory, Mx_JPCAwrdPenHistory, Mx_JPCTimeSheetCorrHistory, Mx_LeaveTrnHistory and Mx_OTAdvanceHistory.

Check On the **Filtering Range Required** check box to enable ‘Filtering Range’ and ‘Apply Filter As Per’ fields as shown below.

Filtering Range: Select option from the drop-down list for filtering range of the report from the options; Date, Date-Range, Month, Month-Range.

Apply Filter As Per: Select the option from the given list in which you want to apply filtering range. For example: HLDDT (Holiday Date). This field value changes according to selected options from ‘Filtering Range’.

Filtering Range Required ☒

Filtering Range

Date
Date
Date-Range
Month
Month-Range

Apply Filter As Per *

Optional Parameters Required

Filtering Range Required ☒

Filtering Range

Date
--Select--
--Select--
HLDDT

Apply Filter As Per *

Optional Parameters Required

Optional Parameters Required: Enable to allow the optional parameter to be included into the report.

Optional Parameters Required ☐

Optional Parameters Required ☒

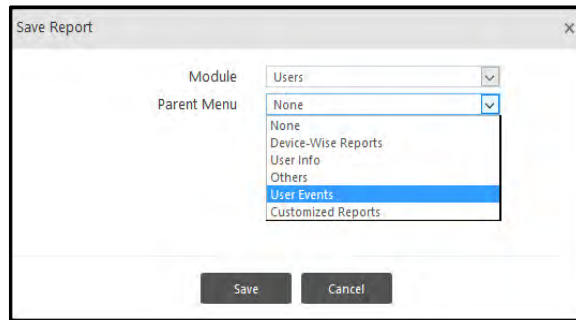
User Selection Required: Enabling this parameter will allow you to decide for which users report is to be generated. You can select user on the basis of User-Wise, Group-Wise, and All -User.

User1 Selection Required ☒

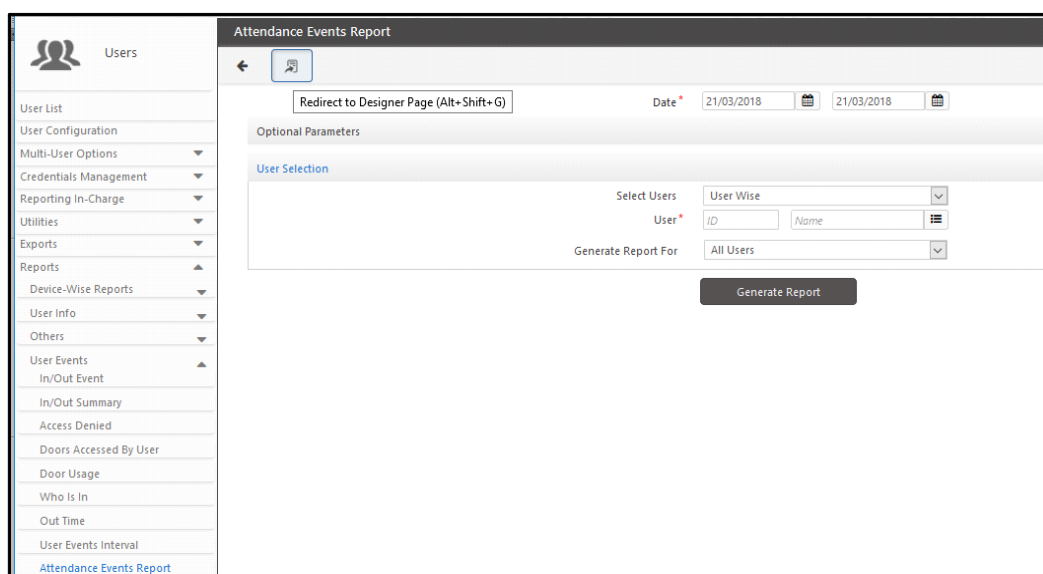
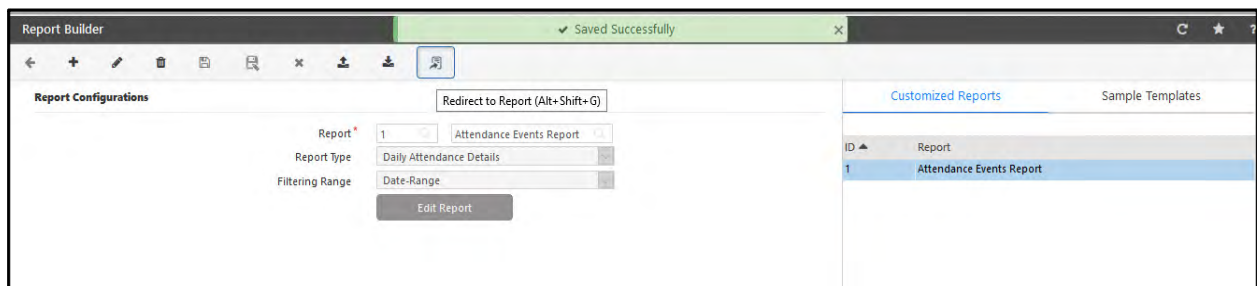
Field	Select Column
User1 *	--Select--
Organization	--Select--
Branch1	--Select--
Department2	--Select--
Section3	--Select--
Category4	--Select--
Grade5	--Select--
Designation6	--Select--
Custom Group 11	--Select--
Custom Group 22	--Select--
Custom Group 33	--Select--

For designing report See “[Designing Report](#)” on page 2182.

After designing the report, click **Save** button.



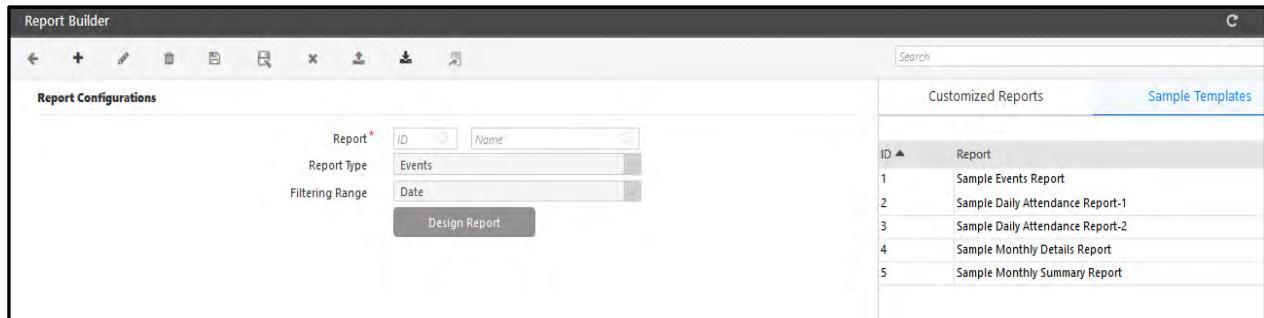
- **Module:** Here the “User” module is selected. It is the selection of the COSEC module where the report is to be placed.
- **Parent Menu:** Here the parent menu can be selected. The report will appear under the selected parent menu i.e.the Report will appear under “User Events” of User module. You can also select the option as **Customized Reports** which will be a new parent menu in the module.
- Click **Save** button. The Report builder page will appear. The created report will be saved and displayed in **Customized Reports** list. The **Redirect to Report** icon will get enabled by clicking which you can go to the module page where report is placed.



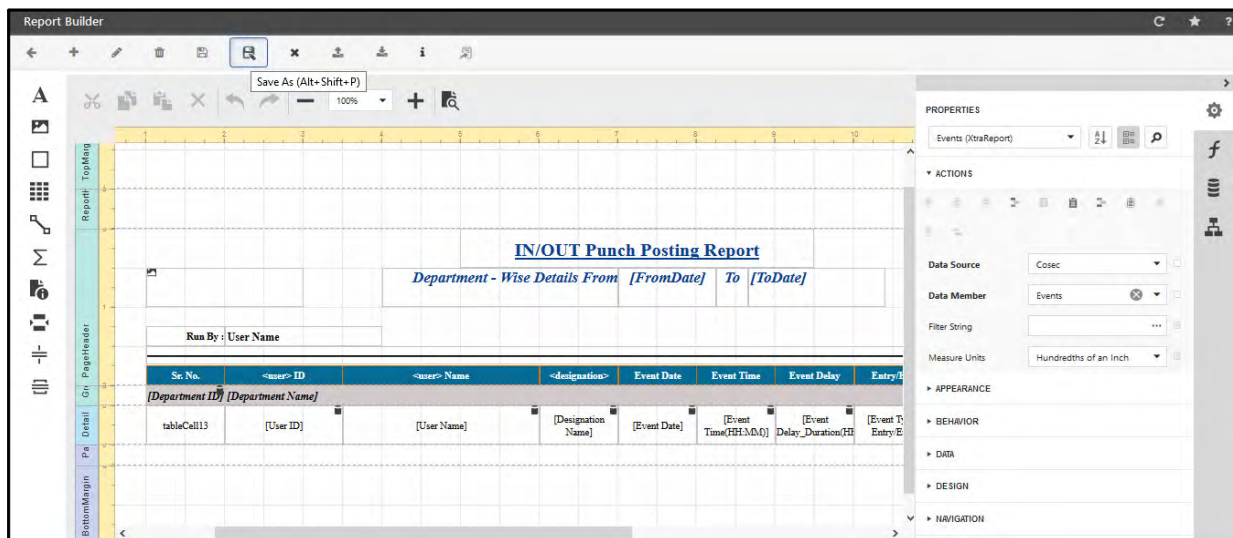
You can click on **Redirect to Designer Page** to switch back to designer page. For more Details [See “Customized Report Page” on page 2223.](#)

Sample Templates and Copy of Sample Template

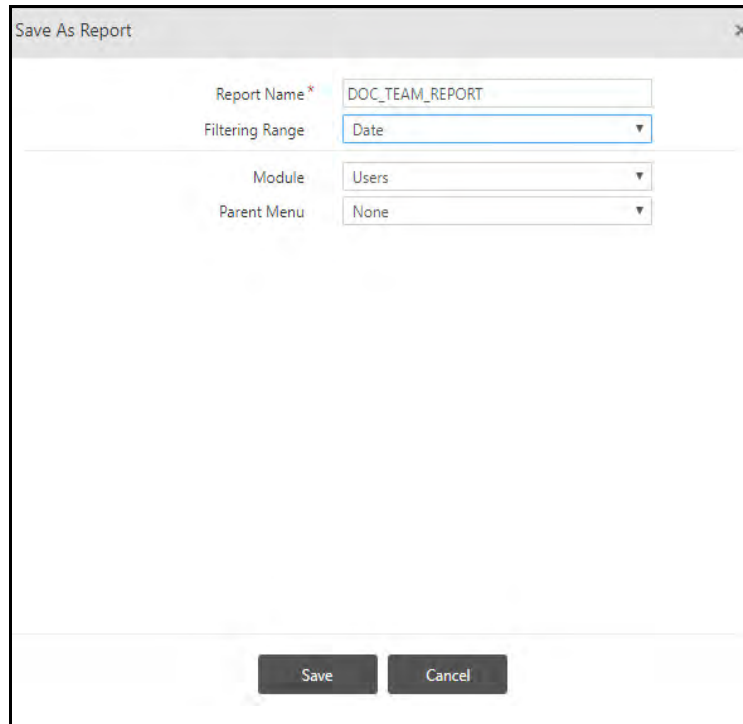
Click on Sample Templates to view the sample report templates.



Clicking on a sample template will open its report designer page as shown below.



You can save a copy of the sample template by clicking **Save As** button as shown above. The Save As Report window appears.



The 'Save As Report' dialog box contains the following fields:

- Report Name ***: Text input field containing 'DOC_TEAM_REPORT'.
- Filtering Range**: Dropdown menu with 'Date' selected.
- Module**: Dropdown menu with 'Users' selected.
- Parent Menu**: Dropdown menu with 'None' selected.

At the bottom, there are two buttons: **Save** and **Cancel**.

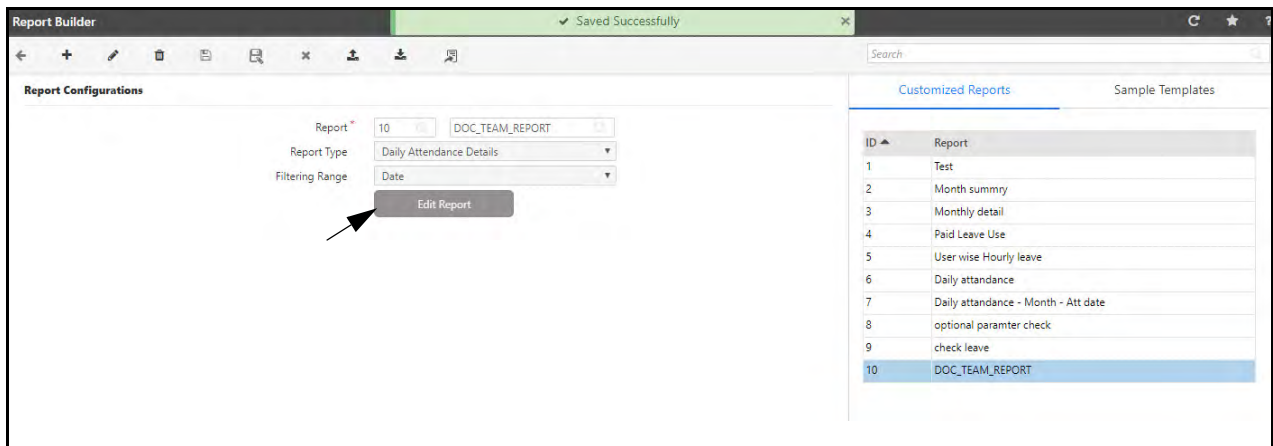
In this enter the **Report Name** as the name of the report. Then select the **Module**, **Parent Menu** and **Filtering-Range**.

Select the **Filtering Range** as Date or Date-Range.

- If **Date** is selected; then only single date selection will appear in report.
- If **Date-Range** is selected; then From-To date range selection will appear in the report.

Then click **Save** button.

The report will be saved and appear in Customized Reports list.



The 'Report Builder' interface shows a green status bar at the top indicating 'Saved Successfully'. The main area is divided into two panels:

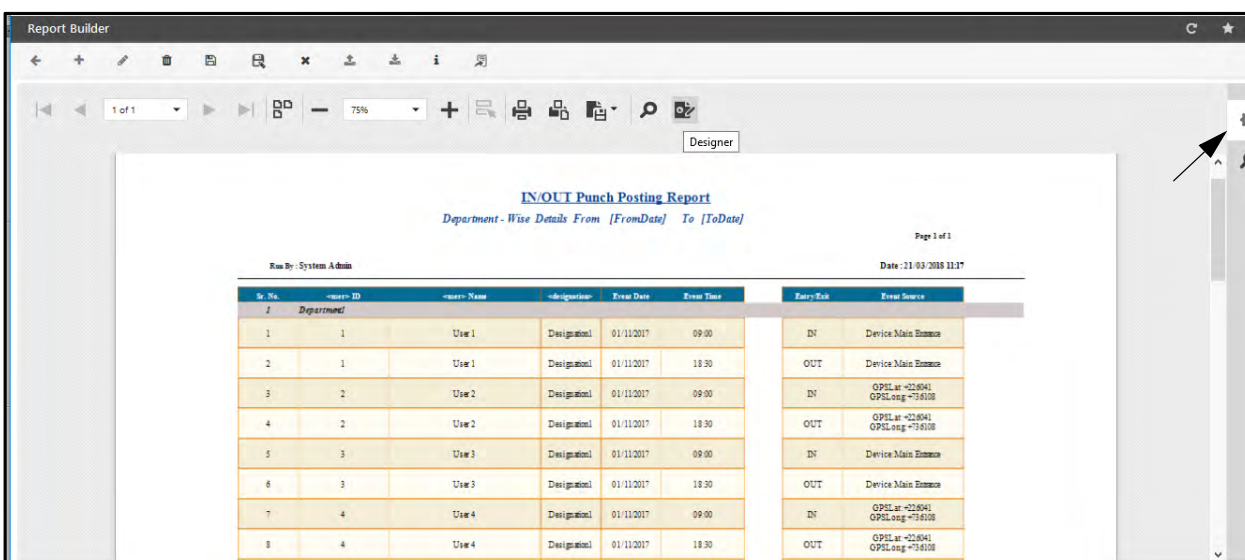
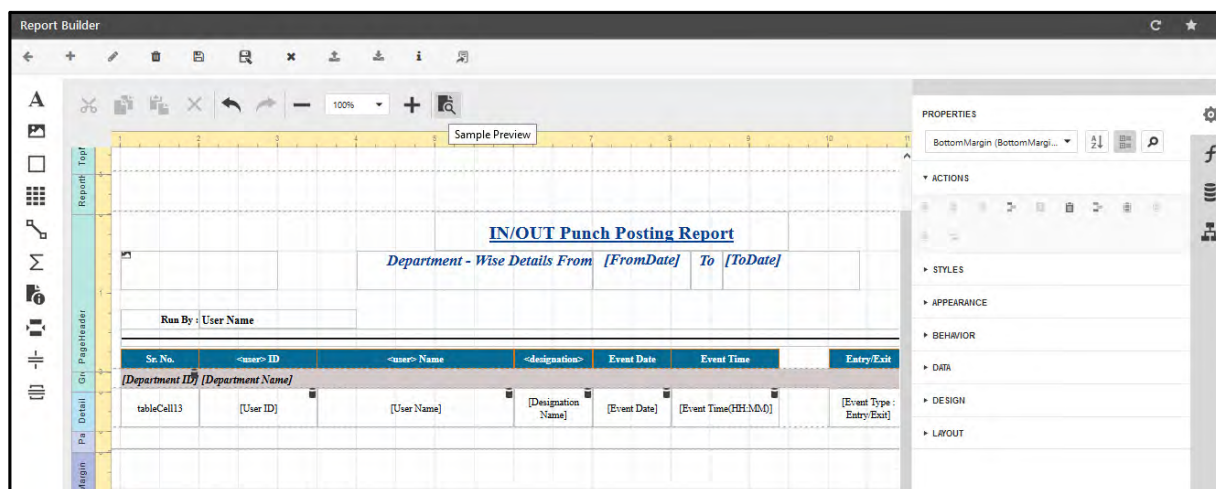
- Report Configurations**: Contains fields for 'Report *' (10), 'Report Type' (Daily Attendance Details), and 'Filtering Range' (Date). An 'Edit Report' button is located below these fields, with an arrow pointing to it.
- Customized Reports**: A table listing saved reports. The report 'DOC_TEAM_REPORT' (ID 10) is highlighted in blue.

ID	Report
1	Test
2	Month summary
3	Monthly detail
4	Paid Leave Use
5	User wise Hourly leave
6	Daily attendance
7	Daily attendance - Month - Att date
8	optional paramter check
9	check leave
10	DOC_TEAM_REPORT

Now you can click **Edit Report** button to edit the report. This will take you to designer page from where you can edit or modify the design as per your requirement. For designing details you can [See "Designing Report" on page 2182](#).

Sample Preview

Suppose the report template is modified as shown below. The preview of the report can be viewed by clicking **Sample Preview** button.



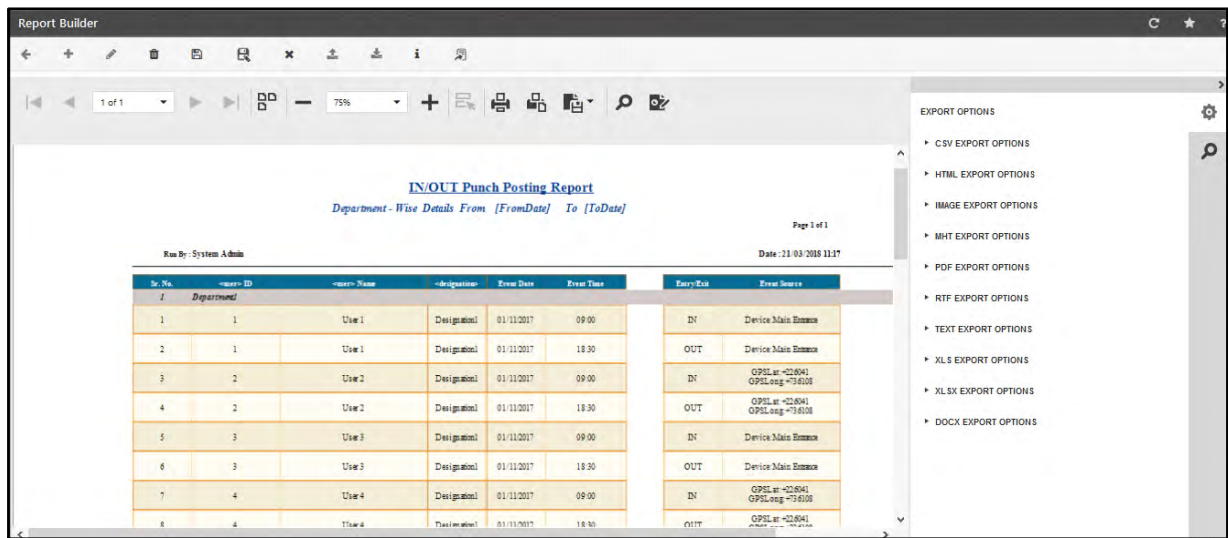
To go back to the designer page click on **Designer** button.

Export Options

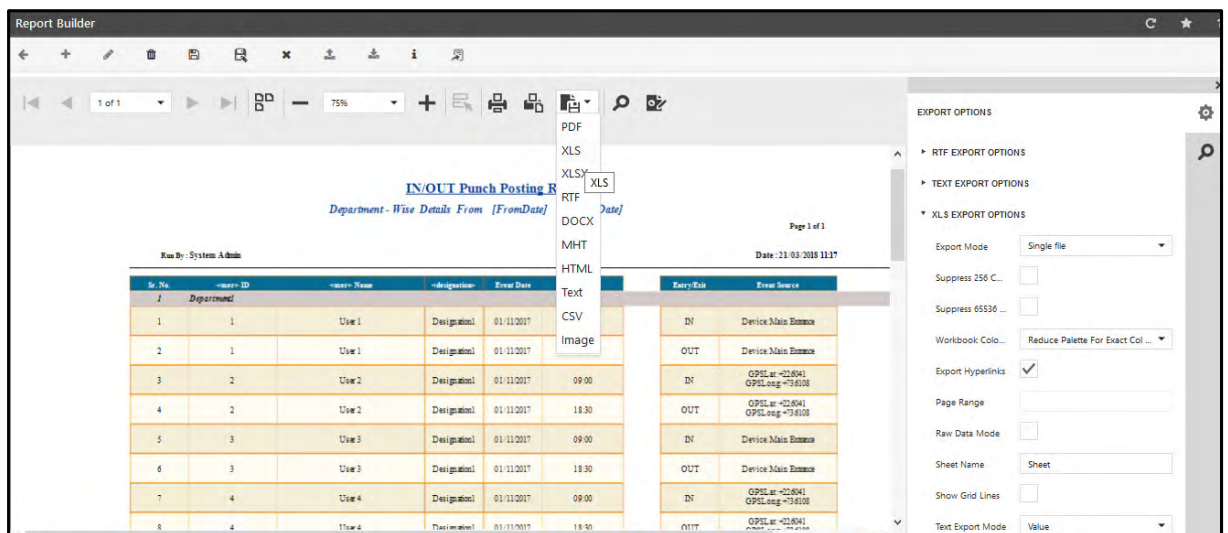
While viewing the preview; if you want to export the report preview then you can click **Export Options** button. The different export options will be listed as shown below.



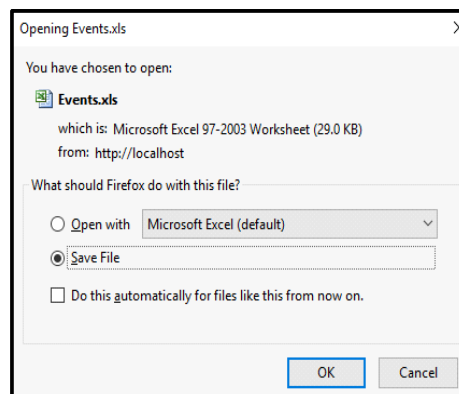
If the check-box in Global Policy > Reports > Report Export Output in PDF only is enabled; then here the options will show PDF export only.



Suppose you want to export this report preview in **XLS** format. Then configure the XLS export option and select Export to XLS as shown below.



The file can be opened or saved in XLS format as shown below.



Events(1) [Compatibility Mode] - Microsoft Excel

File Home Insert Page Layout Formulas Data Review View Acrobat

Clipboard Font Alignment Number Conditional Formatting Styles Cell Styles Insert Delete Format AutoSum Fill Sort & Find & Filter Select

R2

IN/OUT Punch Posting Report

Department - Wise Details From [FromDate] To [ToDate]

Page 1 of 1

Run By : System Admin Date : 21/03/2018 11:27

Sr. No.	<user> ID	<user> Name	<designation>	Event Date	Event Time	Entry/Exit	Event Source
1	Department1						
1	1	User 1	Designation1	01-11-2017	09:00	IN	Device:Main Entrance
2	1	User 1	Designation1	01-11-2017	18:30	OUT	Device:Main Entrance
3	2	User 2	Designation1	01-11-2017	09:00	IN	GPSLat:+22.6041 GPSLong:+73.6108
4	2	User 2	Designation1	01-11-2017	18:30	OUT	GPSLat:+22.6041 GPSLong:+73.6108
5	3	User 3	Designation1	01-11-2017	09:00	IN	Device:Main Entrance
6	3	User 3	Designation1	01-11-2017	18:30	OUT	Device:Main Entrance



Save button will be disabled if any of the sample templates are selected.

Import

It enables to import a New Report design template format and add the Report template to the specified location in particular module.

Import Report

Report Template Path * No file chosen

Report Name *

Report Type

Filtering Range

Module

Parent Menu

Report Template Path: Browse and select the template file (.RepX file) for importing it.

Report Name: Report Name allows to create report and its Report page with that name.

Report Type: It displays the type of Report from the options of Events, Daily Attendance Details, Monthly Summary, Monthly Details and Custom.

New Parameter will appear, if '**Custom**' is selected as Report Type.

Import Report

Report Template Path * No file chosen

Report Name *

Report Type

Table/View *
Events
Daily Attendance Details
Monthly Summary
Monthly Details
Custom

Filtering Range Required ☐

Filtering Range

Apply Filter As Per

Optional Parameters Required ☐

User1 Selection Required ☐

Field	Select Column
User1	--Select--
Organization	--Select--
Branch1	--Select--
Department2	--Select--



The type of Repx file imported and Report Type selected must always match.

Filtering Range: It displays Date or Date-Range when report type is Events or Daily Attendance Details and Month or Month-Range when report type is Monthly Summary or Monthly Details.

Module: Select the module from drop down options. It shows the COSEC modules (except Admin and ESS) available as per the license.

Parent Menu: Select the respective parent menu under which the report is to be placed.

Export

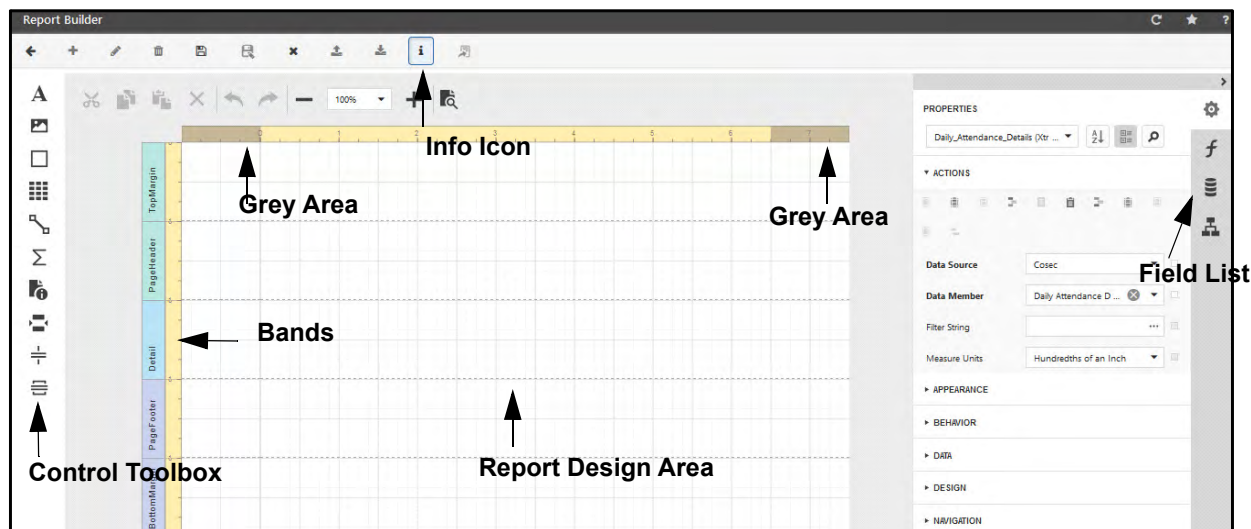
It enables to export the selected report template format. The file will be exported in .REPX format. You can check the Downloads folder in your computer to see the exported file. This file can be used for importing in some other COSEC server.

The screenshot shows the 'Report Builder' window. At the top is a toolbar with various icons, including an 'Export' icon (a document with an arrow) which is highlighted with a blue box. Below the toolbar, the 'Report Configurations' section is visible. It contains the following fields and controls:

- Report ***: A text input field containing the number '5'.
- Report Type**: A dropdown menu currently showing 'Events'.
- Filtering Range**: A dropdown menu currently showing 'Date-Range'.
- Export (Alt+Shift+O)**: A button located above the Report Type dropdown.
- Modified Event Report**: A text input field.
- Edit Report**: A button located below the Filtering Range dropdown.

Designing Report

Report Design Page is shown below. It shows the Control toolbox on left, Properties and Field List on Right and Report design section in center. The Info icon is provided which shows information regarding values to be entered in Tag for different functions.

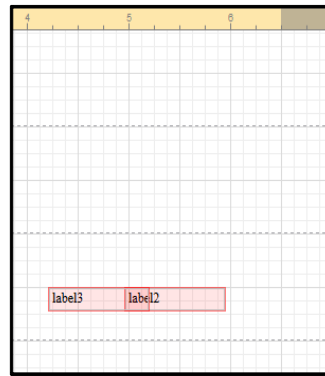
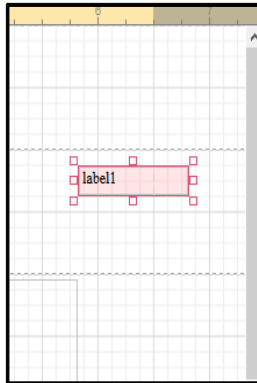


To understand the designing of report, you can refer following topics:

- [“Information Icon details”](#)
- [“Binding Report Elements to Data”](#)
- [“Filter String \(Filter Editor\)”](#)
- [“Table Report”](#)
 - [“Styles”](#)
 - [“Conditional Appearance \(Conditional formatting\)”](#)
- [“Multi-Column Report”](#)
- [“Cross-tab Report \(Pivot Grid\)”](#)
- [“Calculated field”](#)
- [“Adding Page Numbers and System information to Report”](#)
- [“Page Setting”](#)

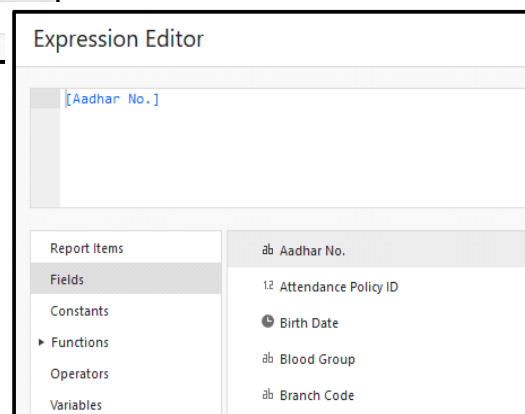
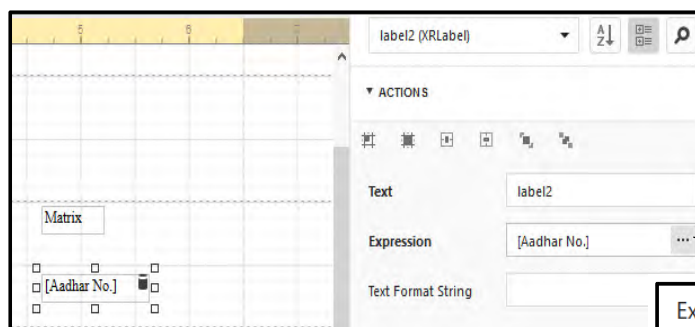
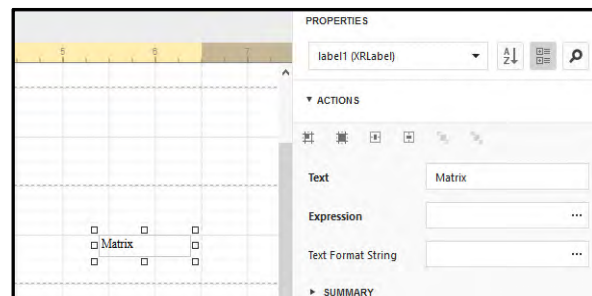
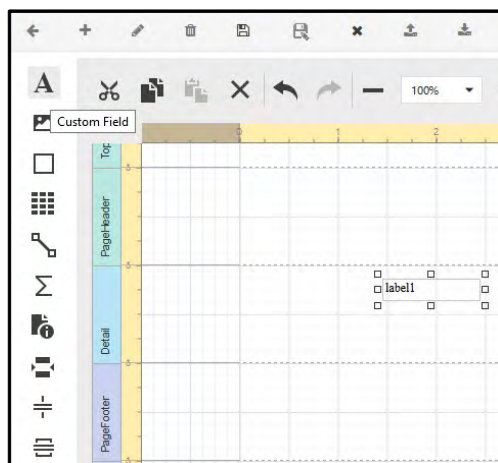
Warning

The red color of the control is the warning that the control is outside the page margin, and this will cause extra pages to be printed. So you must align the controls in the design area excluding the grey area. Also this warning will be shown when the controls are overlapping. So place the controls accordingly.




Create/Insert Report Control

To add a control to the currently opened report, drag and drop the control from the control toolbox on the appropriate report band. For eg: Custom Field control is placed on Detail band as shown below.



Following are the different report controls which can be added to the report.

1. **Custom Field**  - It is used to display a text. For Eg: A text can be entered which will remain fixed such as name of the company. Also custom field can bind to database field from Expression to display the actual data. Eg: Aadhaar No. field is bind to display actual Aadhaar number of the user as shown in above screenshot.

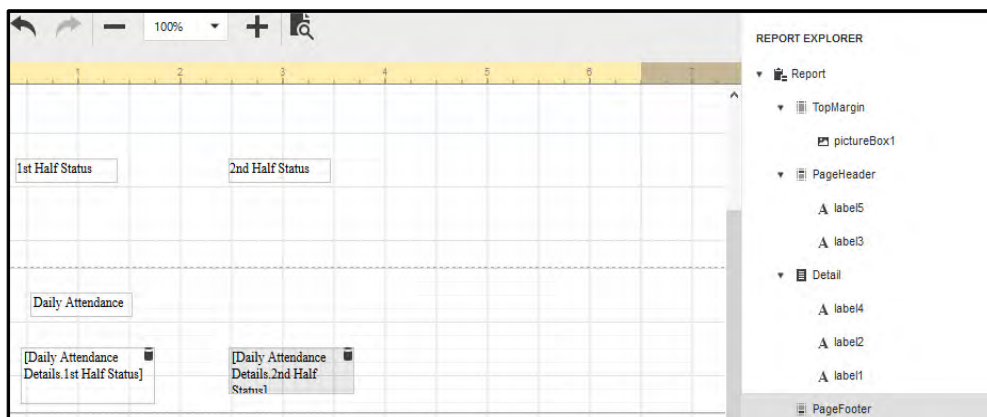
Static and Dynamic Elements






In a report, static and dynamic information is displayed using appropriate controls.

Dynamic information changes through a report, such as values from a database (which comprise the main report data) or service information (such as current user name or page numbers).





Static information is text or images that aren't obtained from a data source, and therefore don't change through the report, and don't depend on the current computer. Static information can be printed only once (e.g. in a Report Header), can repeat on each page (e.g. in a Page Header) or can repeat with every entry in your report's data source (a data-bound label, which is placed onto the Detail band).

Data-bound controls are indicated by a database icon in their top-right corner, both in the Design Panel and Report Explorer.



2. **Image**  - To display image in the report. An image can be selected from an external file or from a web location using the specified Image URL.
3. **Panel**  - It is a box that includes separate controls to allow them to be easily moved, copied and pasted, and visually unite them in the report's preview. (with borders or a uniform color background).
4. **Table**  - It is used for tabular based report. It consist of rows comprised of individual cells. Both rows and cells can be selected and customized individually.
5. **Line**  - It is used for drawing a line of a specified direction, style, width and color. It can be used for both decoration and visual separation of report sections within report bands.
6. **Pivot Grid**  - It represents dynamic data obtained from a data source in cross-tab form. Column headers display unique values from one data field, and row headers - from another field. Each cell

displays a summary for the corresponding row and column values. By specifying different data fields, you can see different totals. This allows you to get a compact layout for a complex data analysis.

7. **Page Info**  - It is intended to add page numbers and system information (the current date and time or the current user name) into your report.
8. **Page Break**  -Its purpose is to insert a page delimiter at any point within a report.
9. **Cross Band Line**  - It allows you to draw a line through several report bands.
10. **Cross Band Box**  - It allows you to draw a rectangle through several report bands.

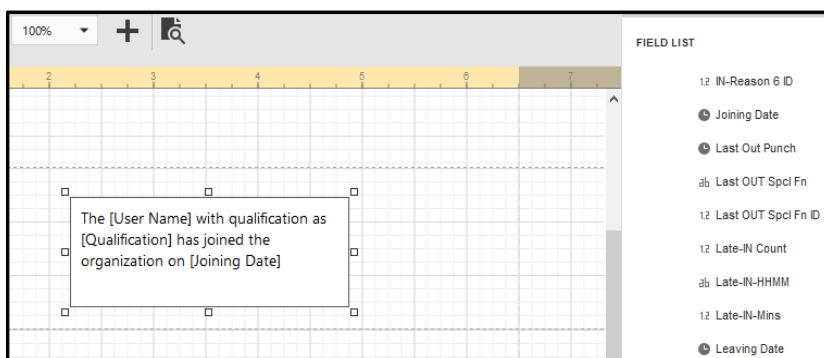
Report controls of appropriate types are created automatically, after you drag items from the **Field List** on the report surface.

After creating a report element, you can bind it to data, customize element layout and appearance.

Merging of Static and Dynamic field

Static and dynamic content can be combined within the same control (e.g. append some text prefix or postfix to a value obtained from a database), or even a control can be bind to multiple data fields at one time.

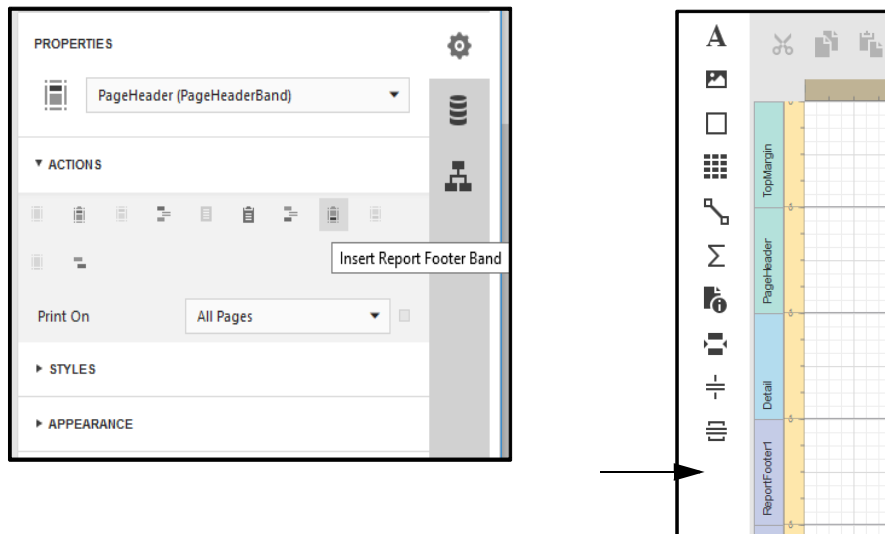
To embed dynamic data into a control's static content, type in data field names surrounded by [square brackets] as shown below.



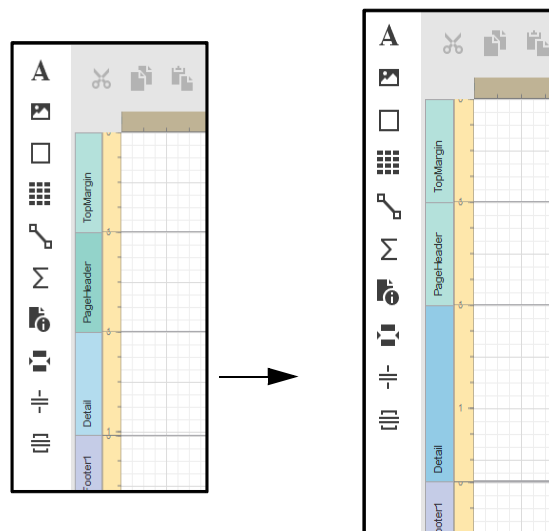
Create/Insert Report Band

To insert the Report bands; select the **Properties** panel. Go to **Action** and select the desired report band.

For example: select **Insert Report Footer Band** as shown below. The Report Footer band will appear in the bands as shown below.

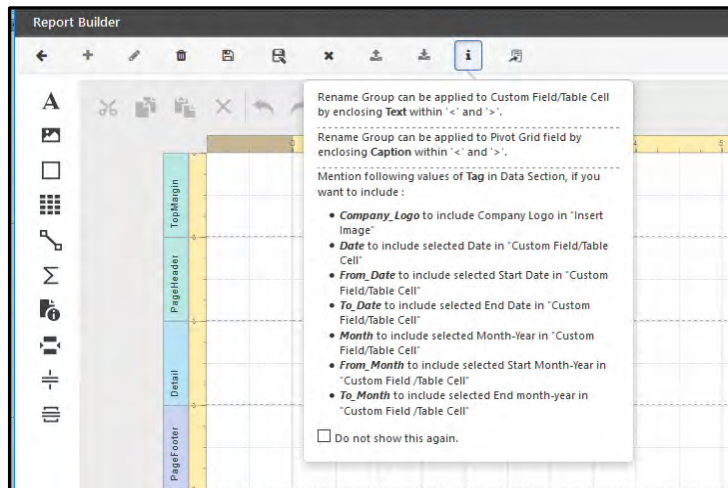


To resize a band, drag its header strip.



Information Icon details

To view the information; click on icon. To close this call-out; click on icon again. Clicking on “Do not Show this again” check-box will keep this call-out closed when new report is added.



Select the **Custom Field** from the control toolbox. Then go to **Properties** section on right side. Expand **Data** and enter the **Tag** from the options shown in information icon.

Example: Consider a report whose filtering range is selected as Date-Range as shown below.

Report *	17	Attendance Details
Report Type	Daily Attendance Details	
Filtering Range	Date-Range	
<input type="button" value="Edit Report"/>		

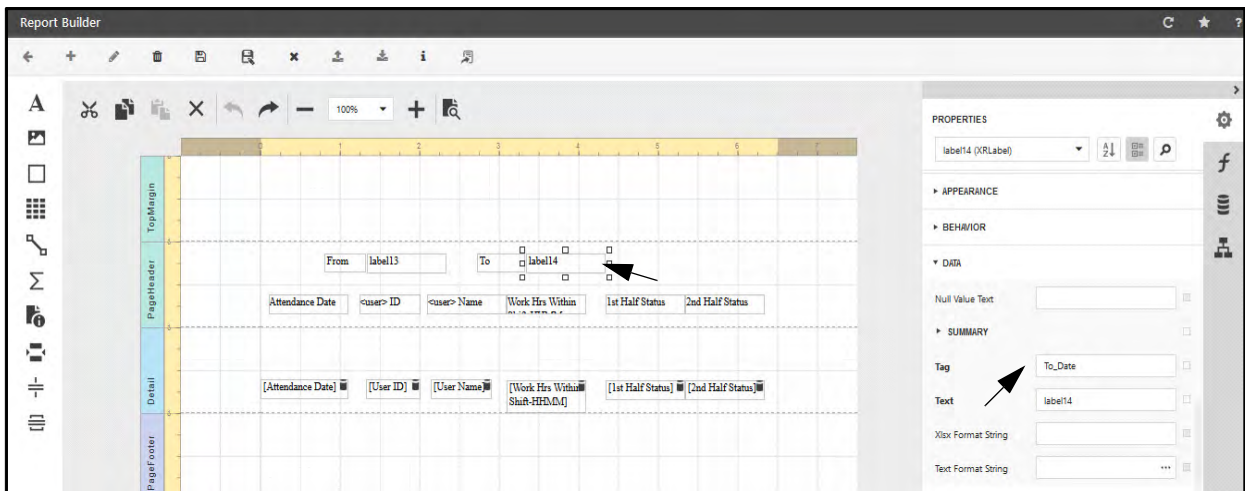
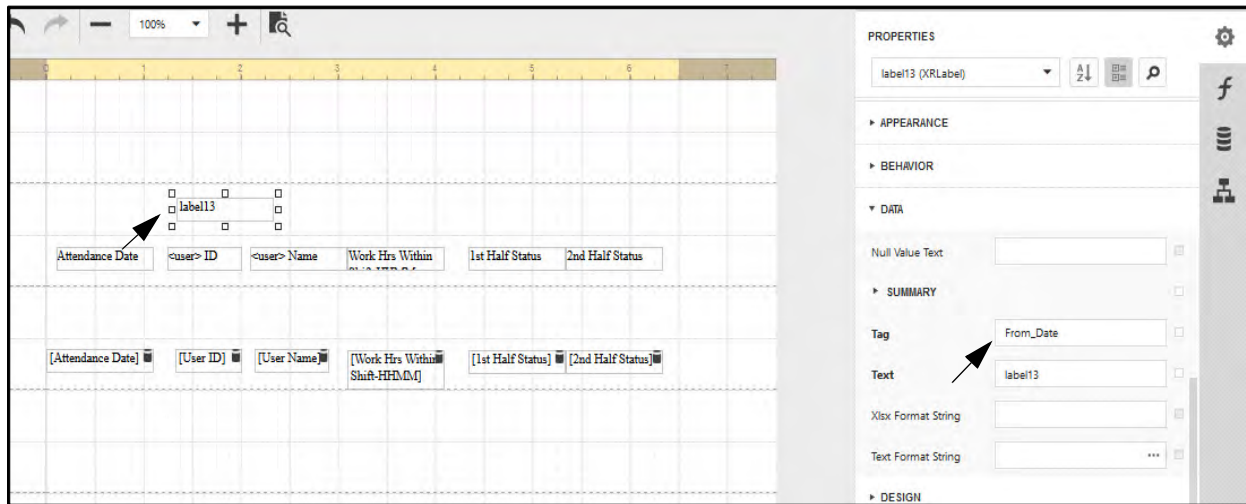
Now the custom field is selected. The label13 is given the Tag **From_Date** and label14 as Tag **To_Date** as shown in below screen-shots.



*If Filtering range is selected as Date; then the custom field should be tagged as **Date**. So in the generated report selected Date will be displayed.*



*Similarly for Report type as Monthly Summary and Monthly details you can select the filtering range as Month or Month-Range. Depending on this you can give **From_Month**, **To_Month** or **Month** tag to the custom fields.*



These labels with Tag will display the actual “From date” and “To date” as selected from the filtering range in the report.

In Sample preview the tagged label will show as label only.

From	label13	To	label14			
Attendance Date	<user> ID	<user> Name	Work Hrs Within Shift-HH:MM	1st Half Status	2nd Half Status	
01/11/2017 00:00:00	1	User1	08:00	PR	PR	
02/11/2017 00:00:00	1	User1	09:00	PR	PR	
03/12/2017 00:00:00	1	User1	00:00	WO	WO	

Attendance Details

Date *

01/01/2018

02/01/2018

Optional Parameters

User Selection

Select Users

All

Generate Report For

All Users

Generate Report

When the report is re-directed to report page in module and From date and To date are selected as shown above. Then the report will be generated as shown below. The tagged label displays the selected date. You can select the format of the date in report designer page.

Attendance Details						
Back						
1 of 1						
From 01/01/2018 00:00:00 To 02/01/2018 00:00:00						
Attendance Date	User ID	User Name	Work Hrs Within Shift-HH:MM	1st Half Status	2nd Half Status	
01/01/2018 00:00:00	1	Chirag	8:00	PR	PR	
02/01/2018 00:00:00	1	Chirag	7:45	PR	PR	
01/01/2018 00:00:00	101	Khushbu	0:00	AB	AB	

For Company Logo

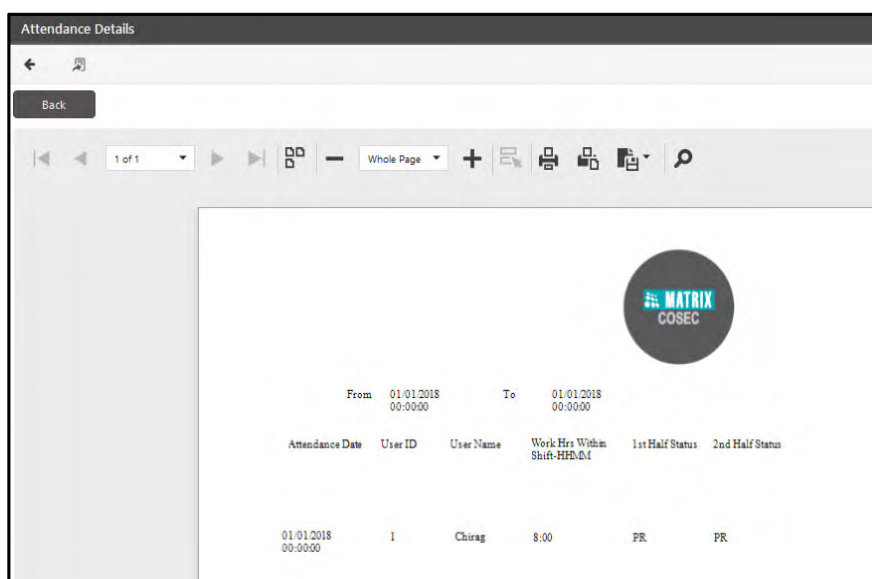
For getting company logo in report select the Insert Image control and give the tag as **Company_Logo**

The screenshot shows a report designer interface with a grid layout. The grid has four sections: TopMargin, PageHeader, Detail, and PageFooter. The Detail section contains a table with columns: Attendance Date, User ID, User Name, Work Hrs Within Shift-HH:MM, 1st Half Status, and 2nd Half Status. The table is populated with data for two users: Chirag and Khushbu. The image control is placed in the Detail section, and its properties are shown in the right-hand panel.

PROPERTIES

- pictureBox1 (XRPictureBox)
- Bookmark:
- Parent Bookmark:
- STYLES
- APPEARANCE
- BEHAVIOR
- DATA
 - Image: (none)
 - Image URL:
 - Tag: Company_Logo
- DESIGN
- LAYOUT
- NAVIGATION

This will display the logo image as uploaded in Admin module> System Configuration> Enterprise Profile.

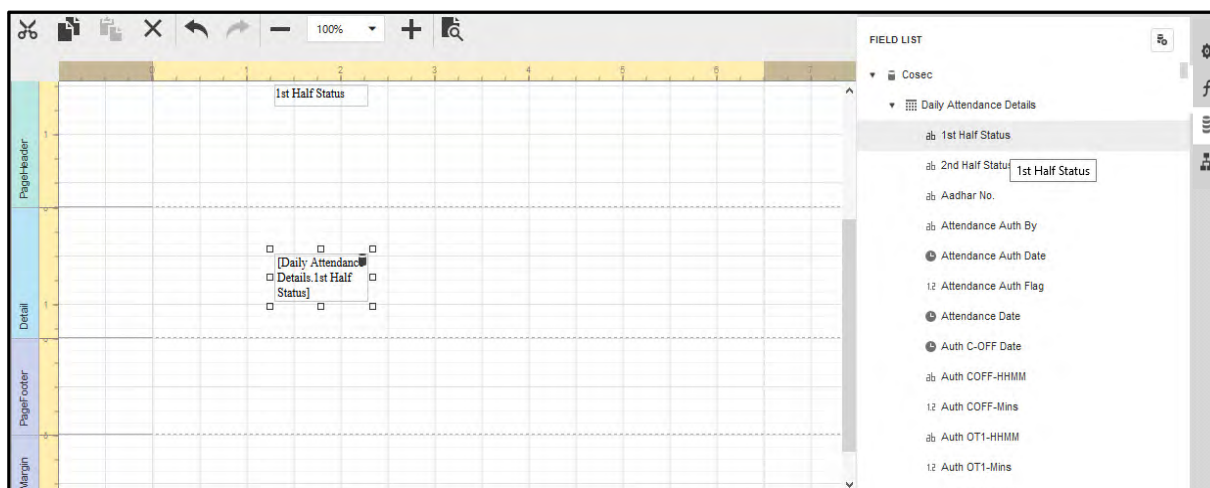


Binding Report Elements to Data

To embed dynamic information to a report, if this information is contained in the report's data source, this can easily be done using one of the following approaches.

1. Using the Field List

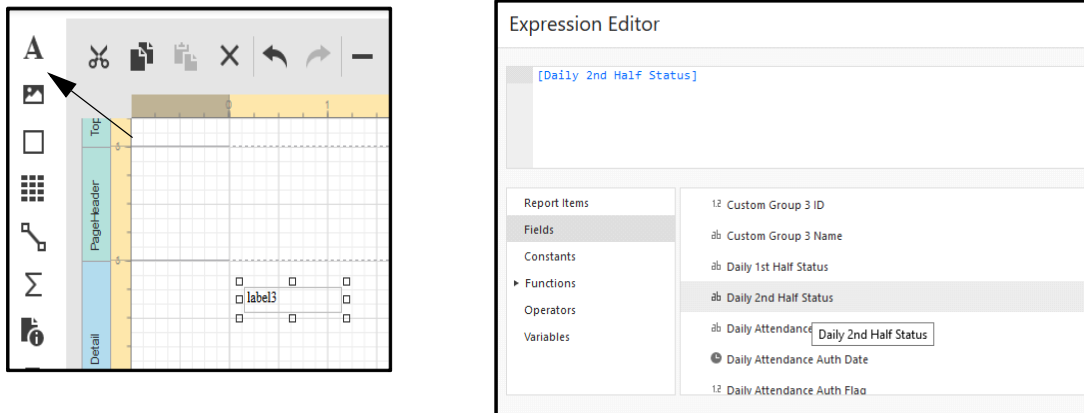
To bind an existing report control to a data field, click the required field item in the Field List, and then drag and drop it onto the control. The database icon inside it will indicate that it's been successfully bound.



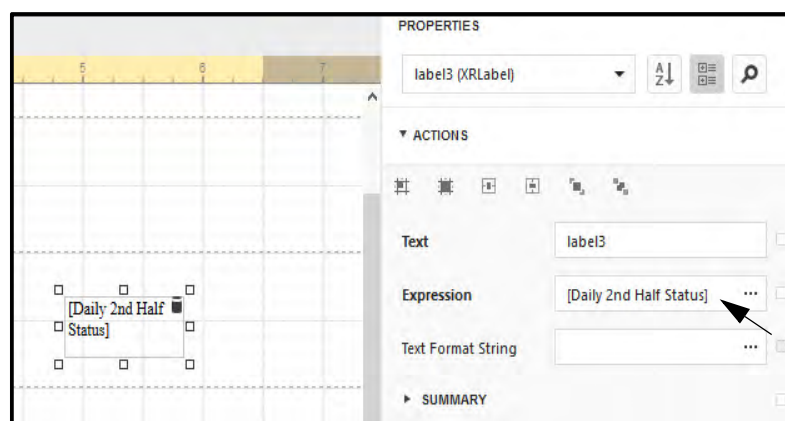
Eg: 1st Half Status field from the Field list is dropped in Details band as shown above. Its associated header “1st Half Status” will automatically appear in the header which will remain a static label in the generated report and the dropped field will change as per the database values.

2. Using the Property Grid

Select a control from left side. In the Properties section at right, expand the “ACTIONS” section and click the ellipsis button. In the Expression Editor; select the field to be mapped for control.



The selected field eg: Daily 2nd Half Status will appear in Expression as shown below.

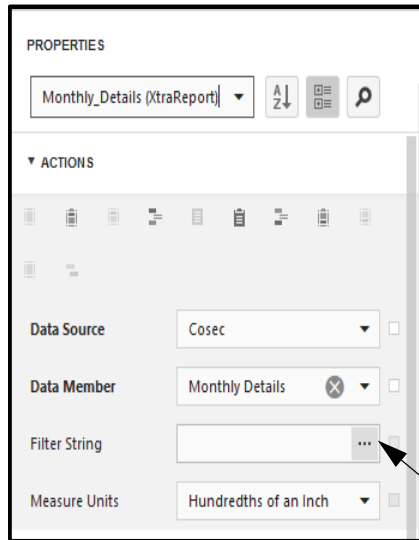


Filter String (Filter Editor)

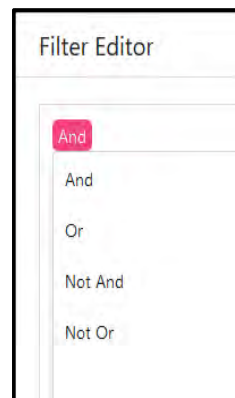
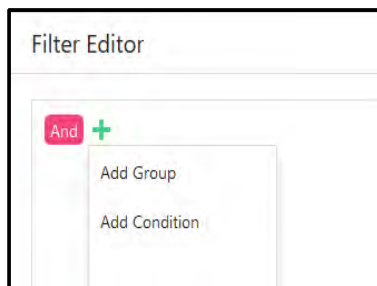
You can apply filter to the report based on which report preview will be generated. If a condition is always to be applied before generating the report so that condition can be set in the report builder filter string.

For Example: If data of users between User ID 1000 to 2000 is required then this condition can be set in the filter string. Based on this filter, sample preview will be obtained.

Then in Report page, if data (say attendance details) of users belonging to specific department (Say QA Dept) is required then again filter can be done which will be applied on ID filtered users.

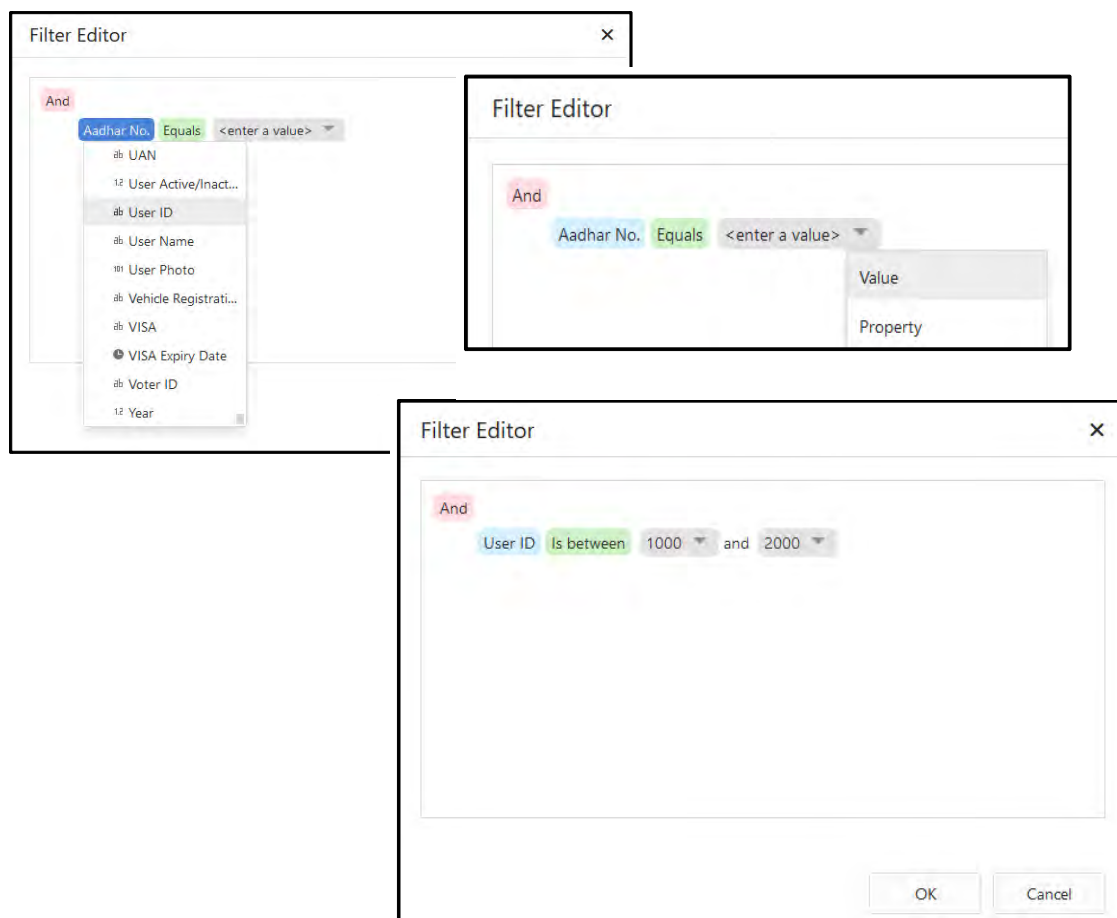


Select the Report in Properties section. Click on Filter String ellipsis button. The Filter Editor page will appear as shown above. Place the cursor on **And**. The + sign will appear. Then click on + to add **Group** or **Condition**. You can click on **And** to change the group to **Or**, **Not And**, **Not Or**.



Add Group- This will add the logical groups **Add**, **Or**, **Not And**, **Not Or**.

Add Condition- This will add the condition to be applied in the filter.



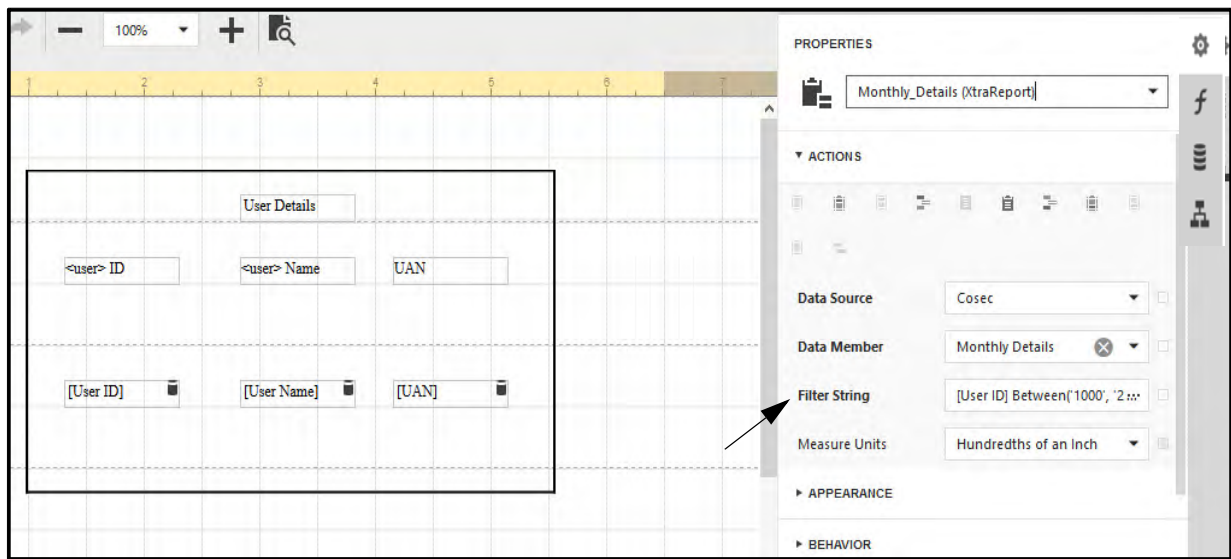
You can select **Value** or **Property** for comparing in the condition. The field will be compared to value or property in the condition to hold true.

If 2 conditions are required, then click **+** and specify condition again.



So Filter will be applied when Condition1 **And** Condition2 are satisfied.

The filter string will be updated with the expression as shown below.



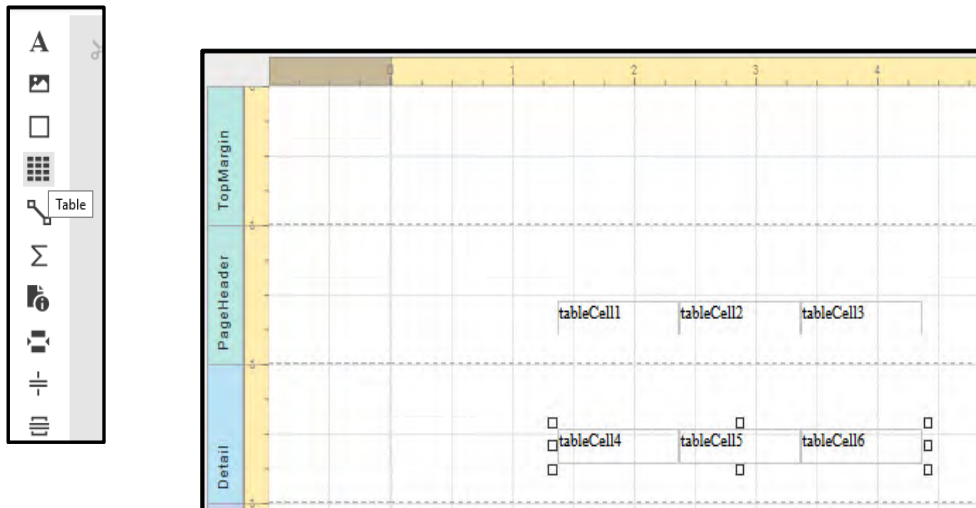
The Sample Preview will show the data after applying the conditions.

User Details		
<user> ID	<user> Name	UAN
2	User 2	99876543211
2	User 2	99876543211

Table Report

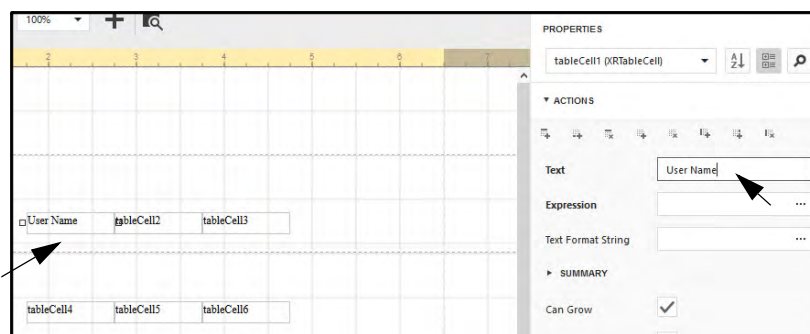
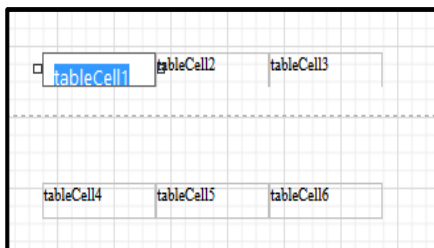
For creating Table Report drag the Table report control from the Toolbox and drop it on the Report designer page.

Place two Table controls to the report's Page Header and Detail band as shown below.



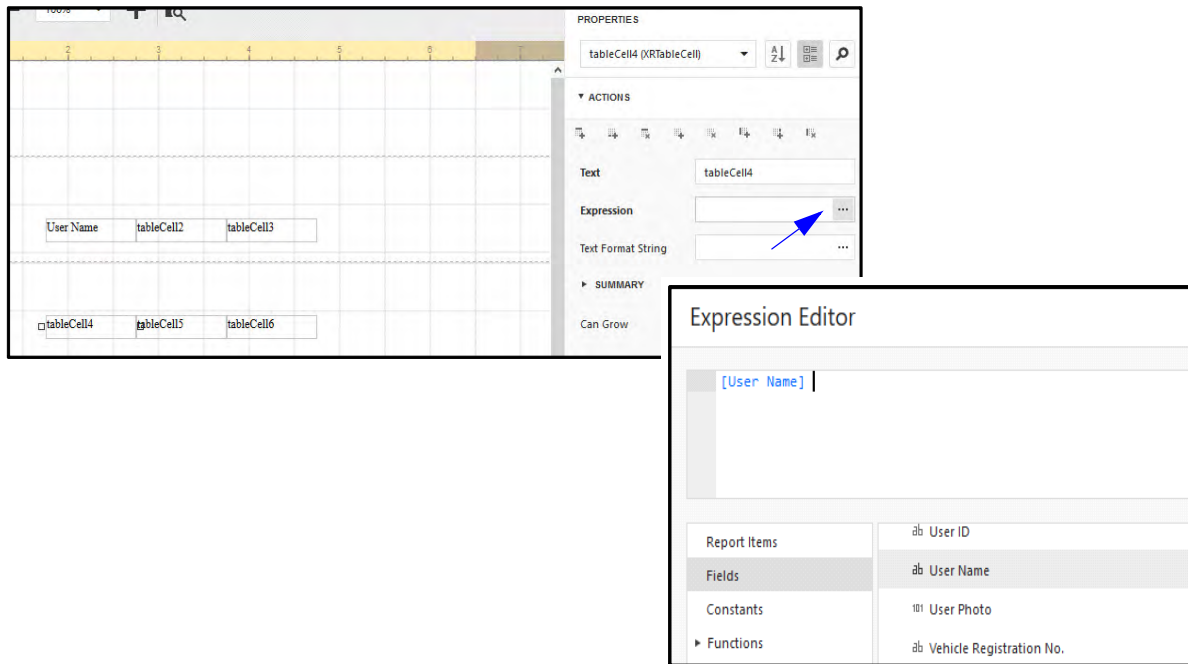
One table will be used as a header, and the other one - for the report's detail information.

Type the headers into the upper table's cells. Eg: tableCell1 is edited with text "User Name". You can also enter the text in Properties grid which will be reflected in the cells in design area.

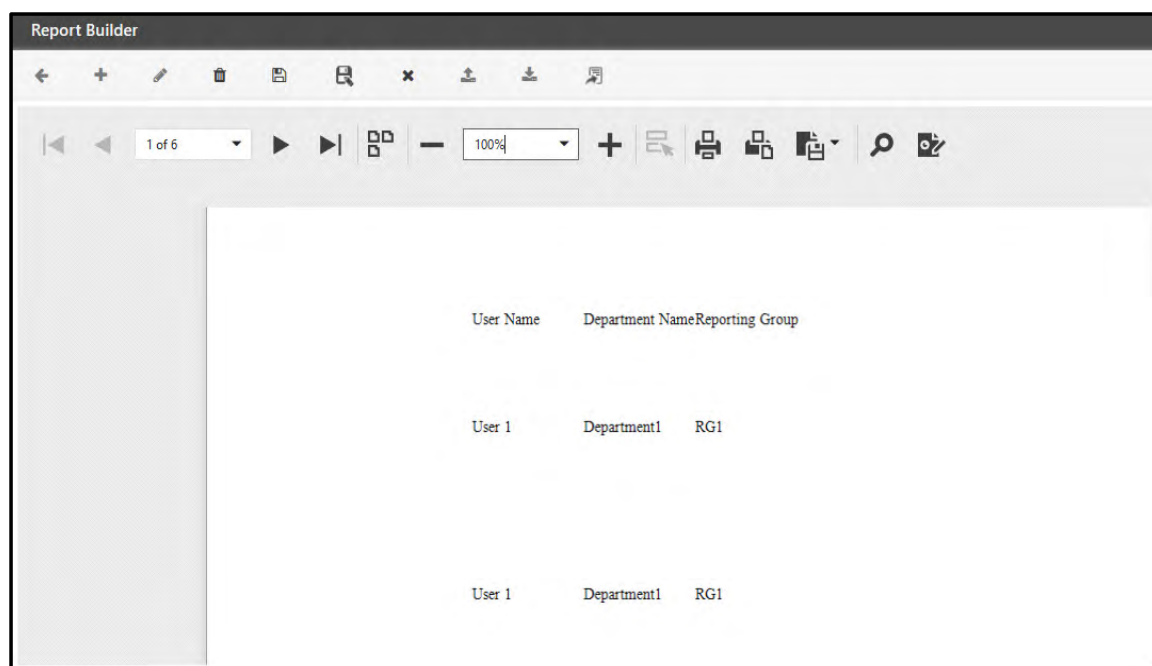
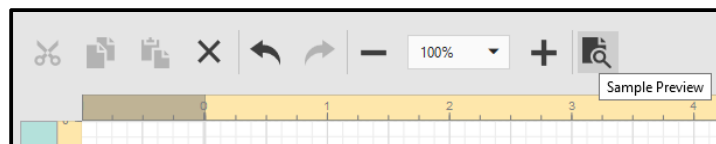



Then bind the corresponding cells in the detail section to the appropriate data fields. To do this, select a table cell and set its Data Field in the Expression as shown below.

Example: Cell4 is bind to User Name; Cell5 to Department Name, Cell6 to Reporting Group Name.

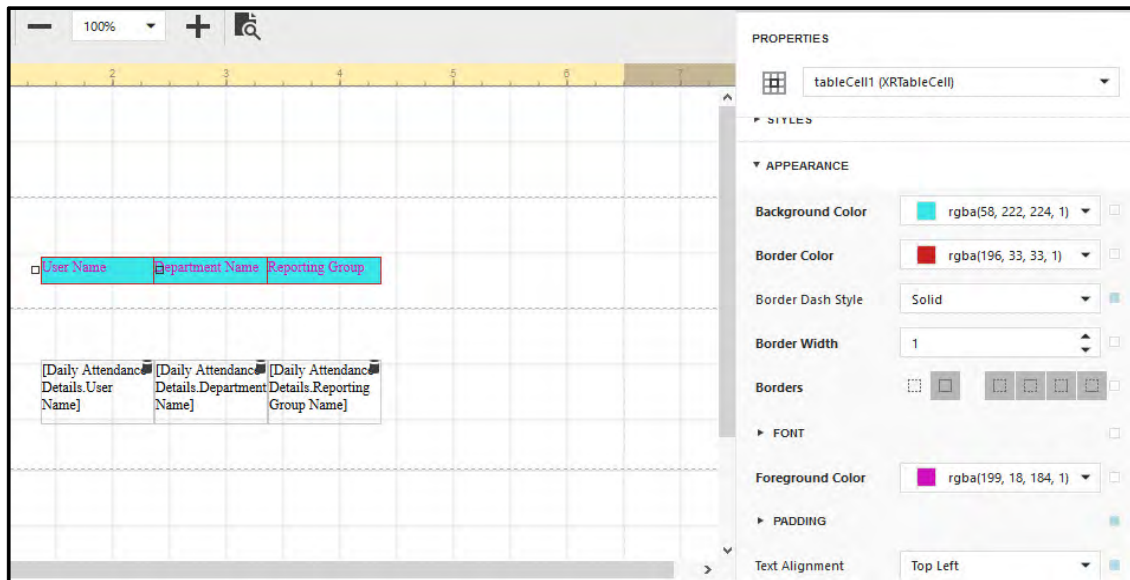


Now you can view the preview of designed report by clicking on **Sample Preview** button as shown below.



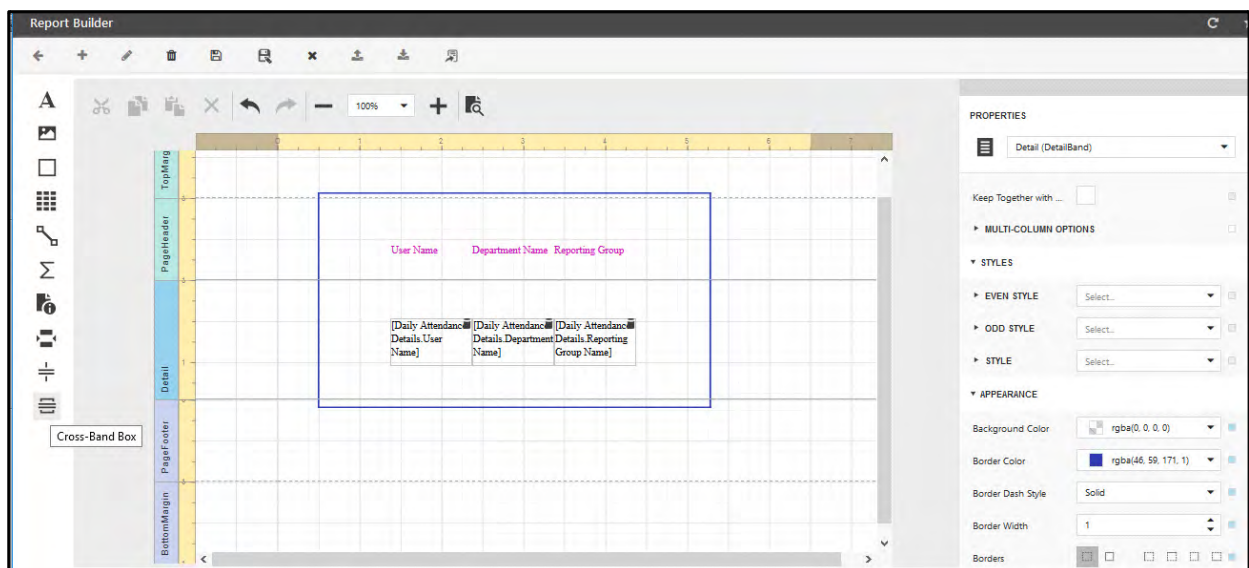
You can switch back to designer page by clicking **Designer**  button from above page.

Finally, you can customize various properties of the tables to improve their appearance. For example, in the **Appearance** category of the Properties Panel, you can define the Borders property, as well as the Background Color property. To customize cell text options, specify the **Font** property. You can also specify **odd-even** styles for the detail table.



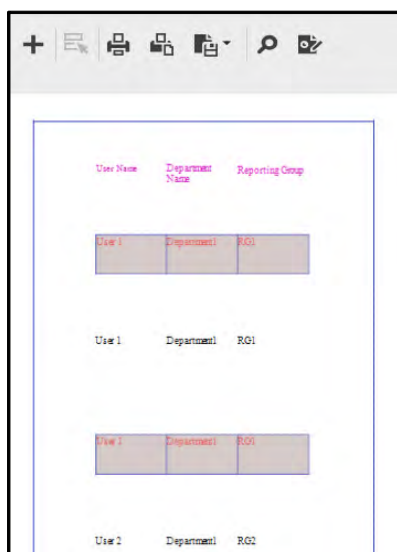
Cross-Band Box

The Cross-band Box control allows you to draw a rectangle through several bands of report. This is useful if border is required in a report.



For this drag the Cross-Band Box control on the report designer page. Stretch the corners of the box through the bands to make it a border of the report. You can also change the color of the border from Appearance.

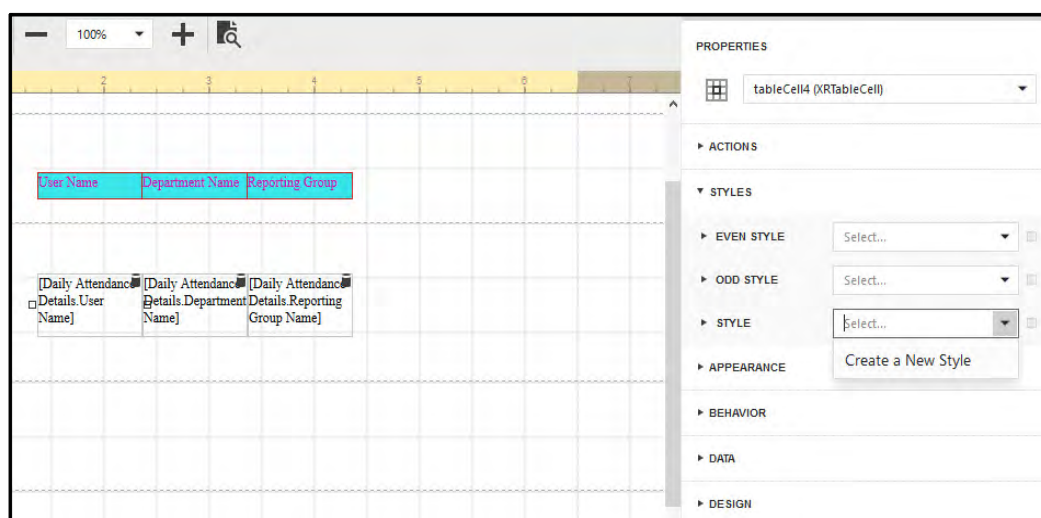
Then click Sample Preview to view the report preview.



Styles

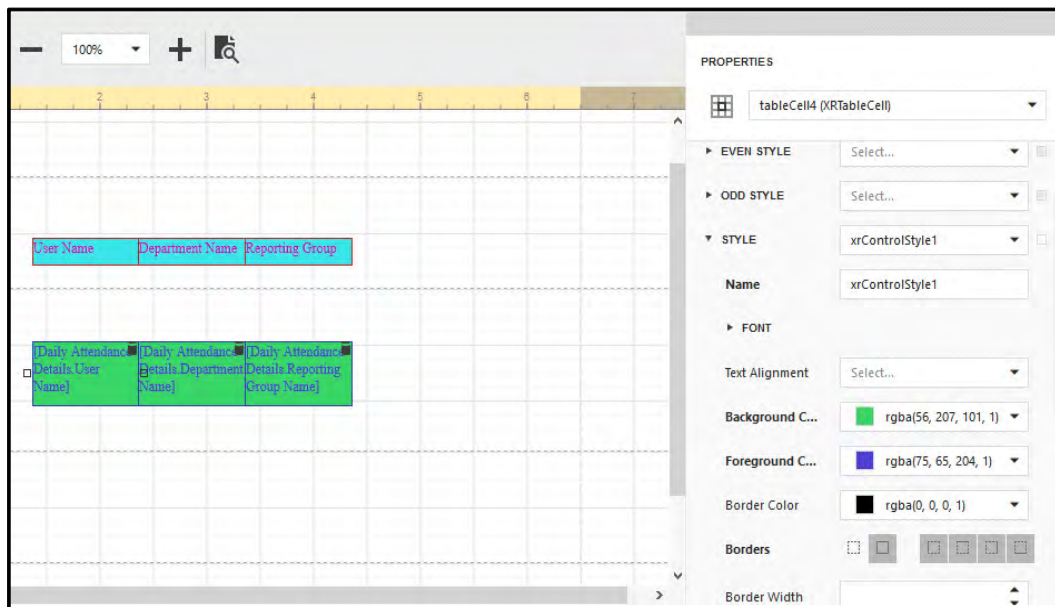
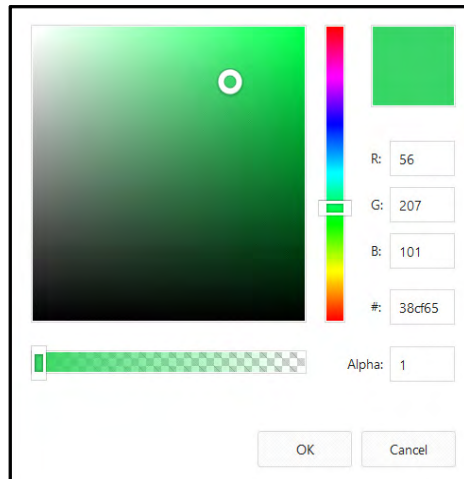
A style that is assigned to a band applies to all controls in that band.

To assign a particular style to a control, select this control and in the Properties Panel, expand the Styles category and configure it as described below.

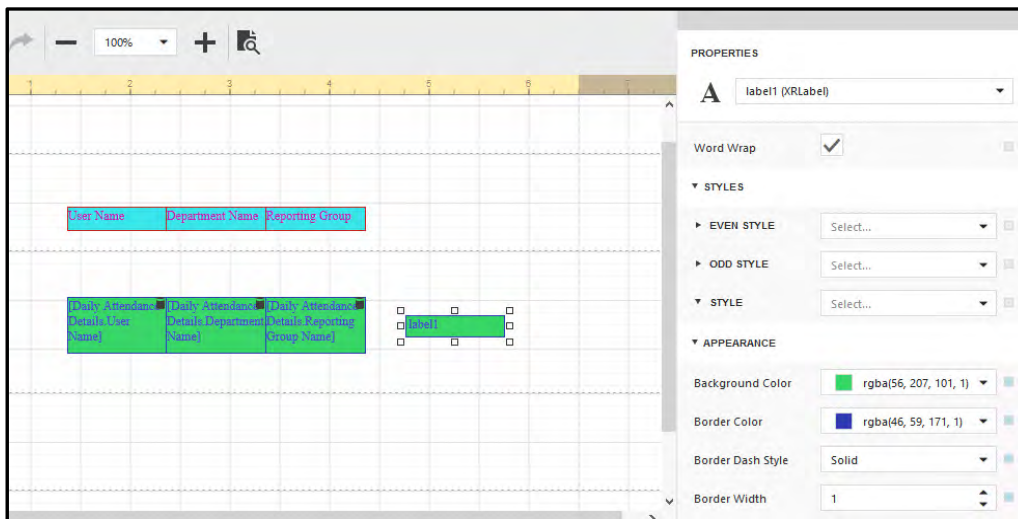


Click the drop-down list for the Style property and click **Create New Style** or select an existing style.

Select the Background color as shown below. The foreground color i.e. the color for the text can be selected in the same way. You can configure other style parameters like font, borders, padding etc.

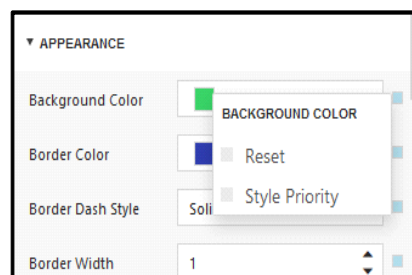


The configuration of style will be reflected in Appearance also. When new control is placed in the band configured with style; then the new label will also get the same style.



When both styles and individual appearance settings are assigned to an element, the style's appearance property has a higher priority than an element's appearance property.

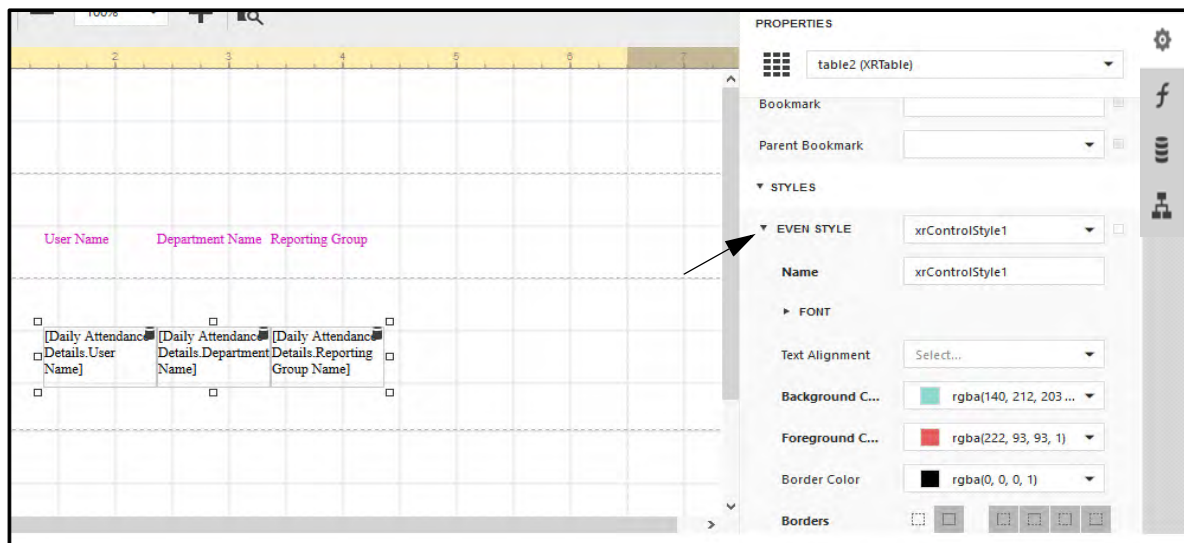
To assign a higher priority to an element's appearance property, click the Advanced Options button and then click Style Priority.



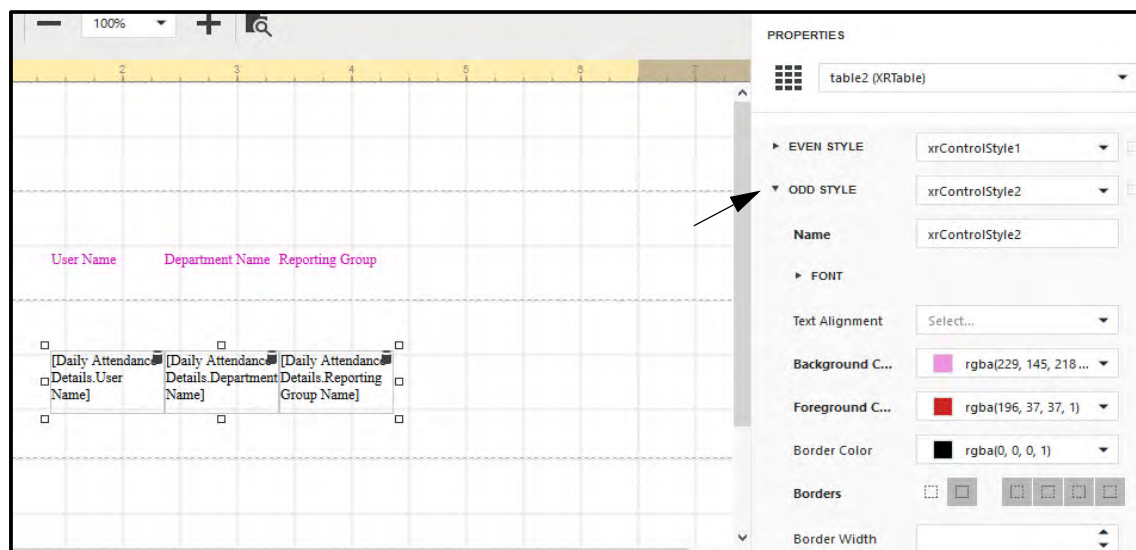
Odd and Even Style

This is mostly used to alternate the background color for each record.

Select the Detail table (table in Details band). Go to Properties panel. Select Styles category and click the drop down for **Even Style**. Create a new style. For creating the style; you can select the background color, foreground color, border, font etc. After creating a style; assign it to the Even Style.



Similarly create another style and assign it to the **Odd style**.

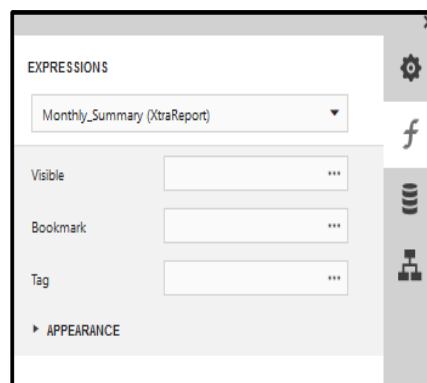


To view the preview of Report; click Sample Preview. The Report preview will be shown as below with odd and even background colors in different rows.

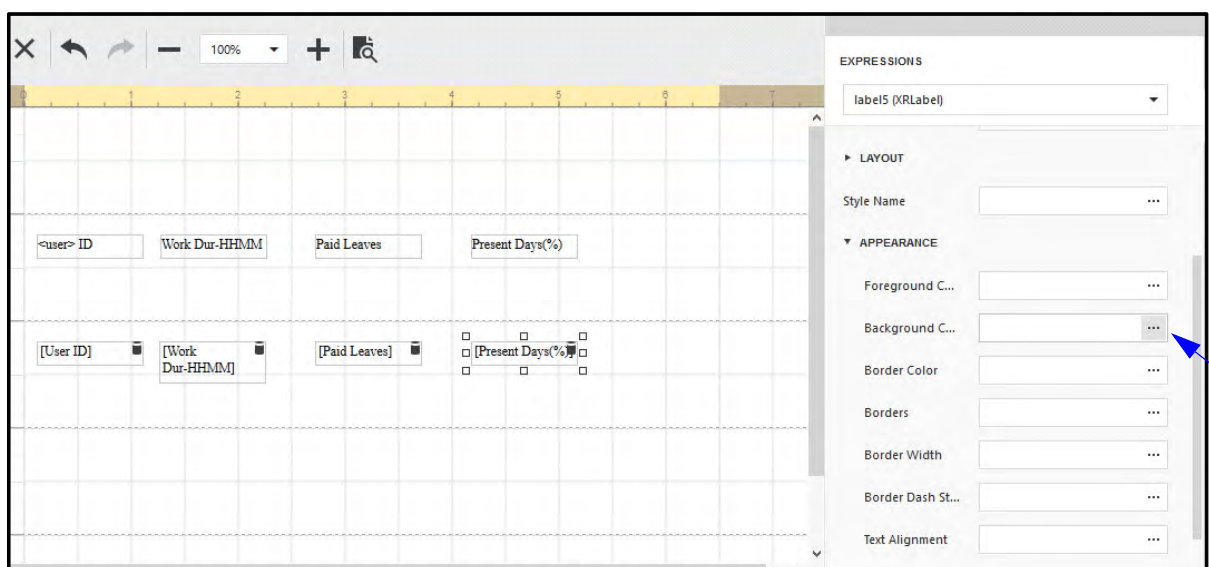
User Name	Department Name	Reporting Group Name
User 1	Department1	RG1
User 1	Department1	RG1
User 1	Department1	RG1
User 2	Department1	RG2

Conditional Appearance (Conditional formatting)

Create a report and bind it to a data source. Select the **Expression** Panel, expand the **Appearance** category.

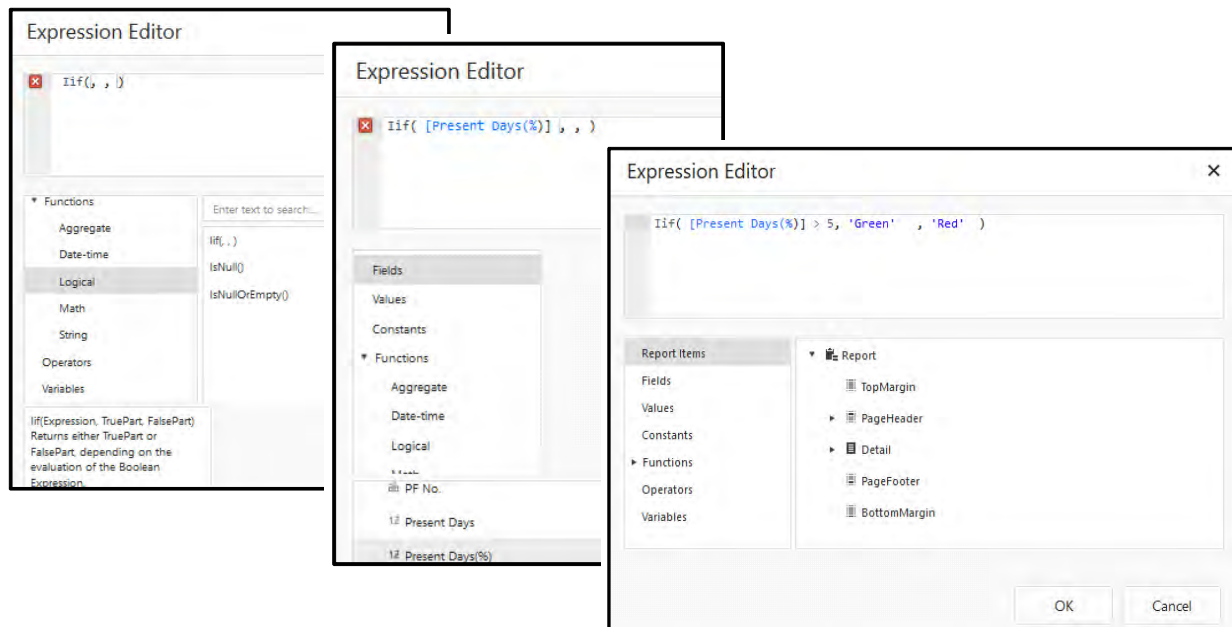


To configure conditional appearance for a control, select the required report control.

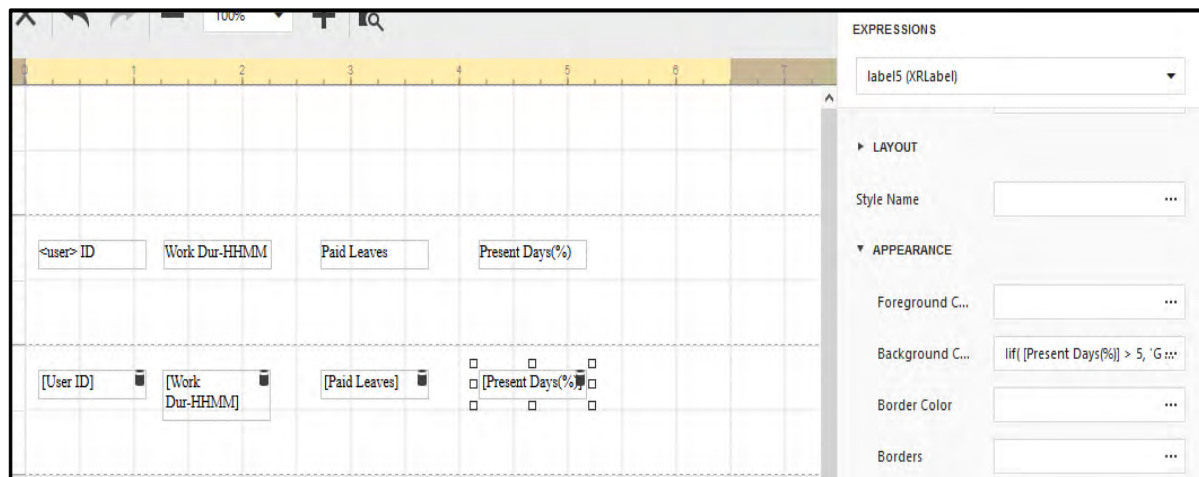


Click the ellipsis button to configure the appearance settings based on condition for **Foreground color**, **Background color**, **Text Alignment** and **Border related** options. When the conditions defined in expression is fulfilled then report control will appear as per the configured conditional appearance.

The Expression Editor will appear. You can create the required Boolean condition based on which appearance formatting will be applied to the report control. Here the expression for background color is defined.



This means when Present Days% >5, then the associated control will show background as green or else will show red color.



The report preview shows the background color as green for which present days is greater than 5%.

<user> ID	Work Dur- HH:MM	Paid Leaves	Present Days(%)
1	0.75	0	8.67
2	0.979166666667	0	8.67
3	0.25	0	8.67
4	0.8125	0	8.67
5	0.541666666667	1	8.33

Multi-Column Report

Select the Details band. In the Properties Panel, expand the Actions or Behavior category. Then, expand the Multi-Column Options section and set the required **Mode**.

- **Use Column Count:** In this number of columns is manually specified. After selecting “Use Column Count”; Set the Column Count to 2, and Column Spacing to 10.
- **Use Column Width:** In this column width is fixed.

PROPERTIES

Detail (DetailBand)

▼ MULTI-COLUMN OPTIONS

Column Count: 1

Column Width: 0

Column Spacing: 0

Layout: First Down, then Across

Mode: Use Column Width

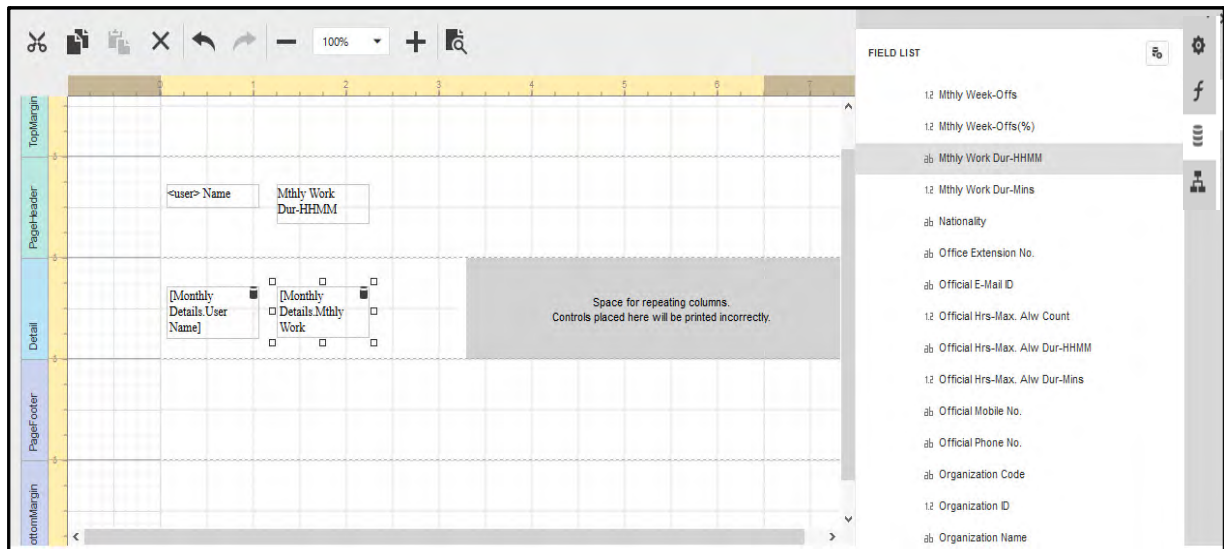
► STYLES

► APPEARANCE

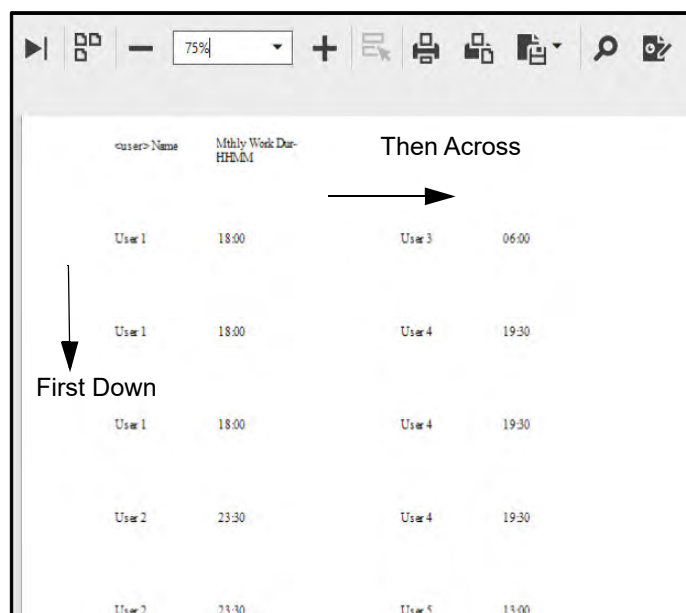
► BEHAVIOR

Layout determines the order in which records of the same group are processed. You can select “First Down, then Across” or “First Across then Down”.

Now, on the Detail band's surface, a grey area appears, delimiting the available column's width.

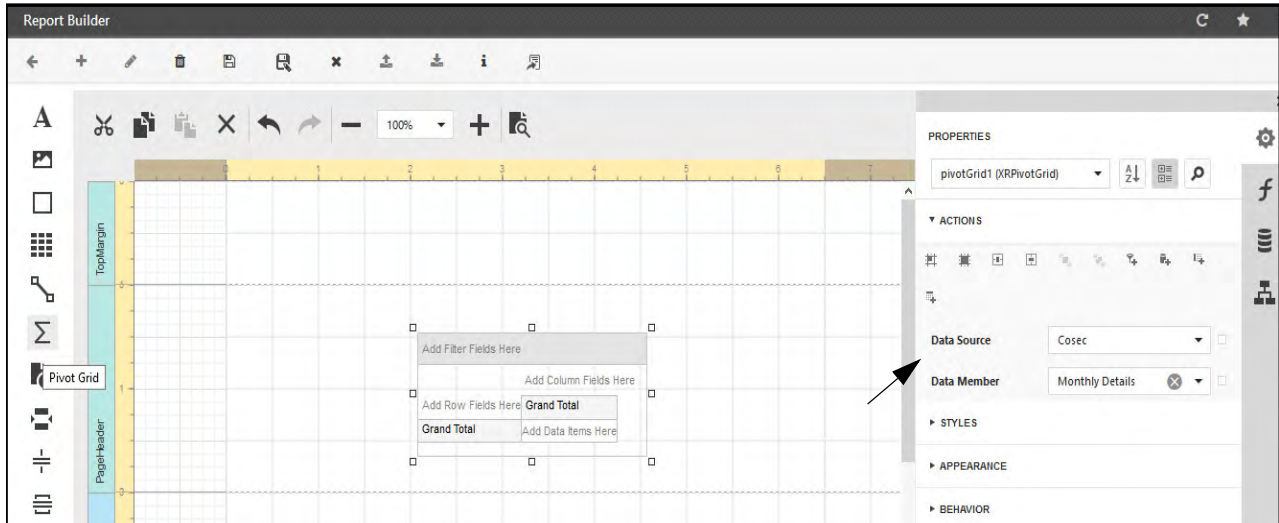


Place the field list elements and adjust the controls width, so that they fit within the effective borders. The preview of the report is shown below.



Cross-tab Report (Pivot Grid)





This is the cross -tab report using a **Pivot Grid** that calculates automatic summaries and grand totals across a large number of grouped rows and columns.



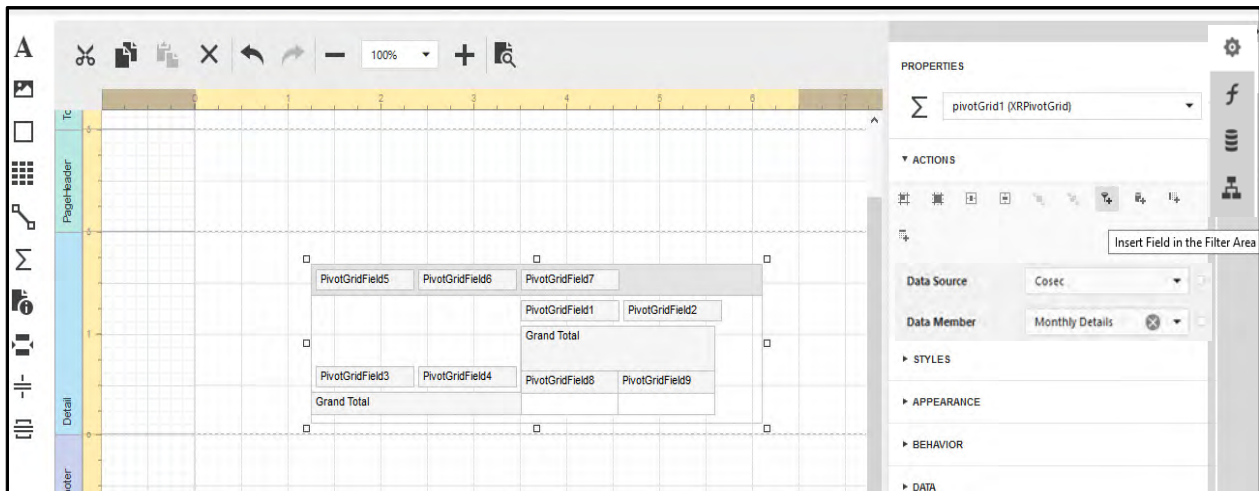
Place the **Pivot Grid** control from the Control box on the report's Detail band as shown above.

The Pivot Grid will get bind to **Data Source** and **Data Member** as shown above. The Data Member property defines from which table or view of your dataset the grid obtains its data.

To add a field to the particular grid area, expand the Actions category and click one of the following buttons.

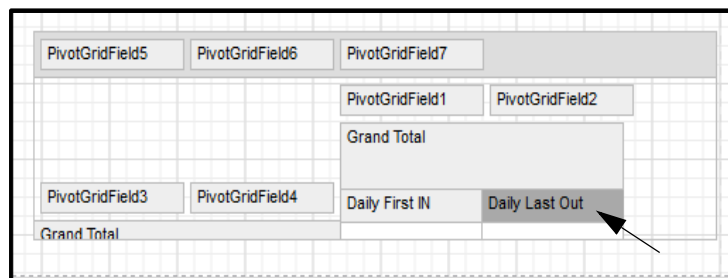
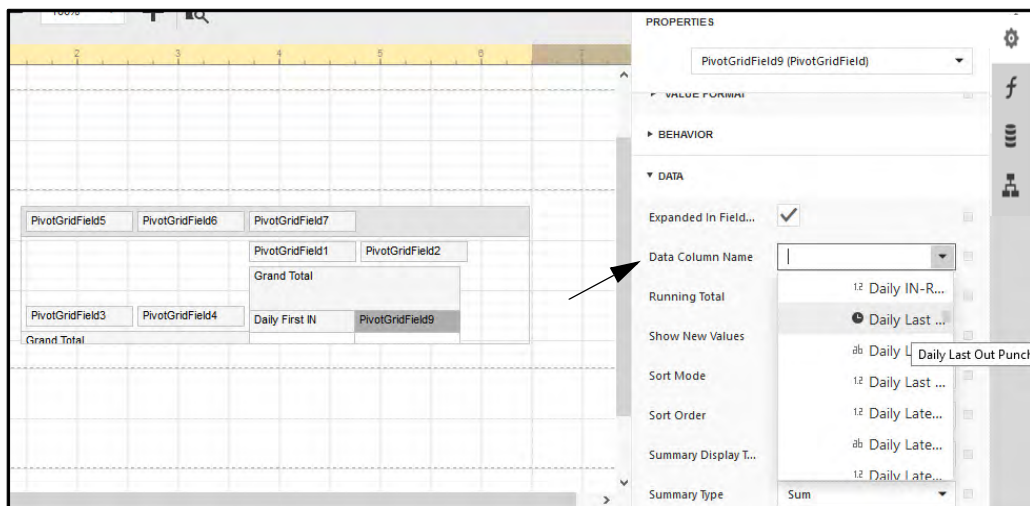
1. **Insert Field in the Filter Area**  : It adds a field to the Filter Header area. This field is available for further customizations.
2. **Insert Field in the Data Area**  : It adds a field to the Data Header area. The summaries will be calculated for all the cells, each cell is identified by a specific column and row.
3. **Insert Field in the Column Area**  : It adds a field to the Column Header area. This field's values will represent column headers.
4. **Insert Field in the Row Area**  : It adds a field to the Row Header area. This field's values will represent row headers.

Add two column fields, two row fields and two data fields, by clicking the above described buttons. You can also add several filter fields.



The Data binding of PivotGridField9 is shown below. For this Expand **Data** and then expand **Fields**. Select the **PivotGridField9**. Now click the drop down arrow and select the desired field for **Data Column Name**.

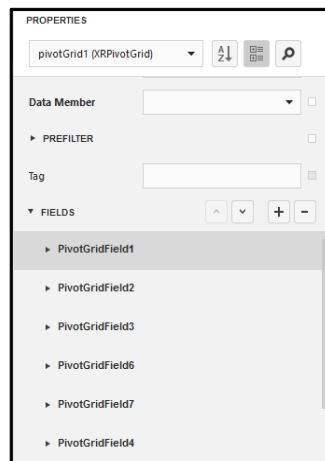
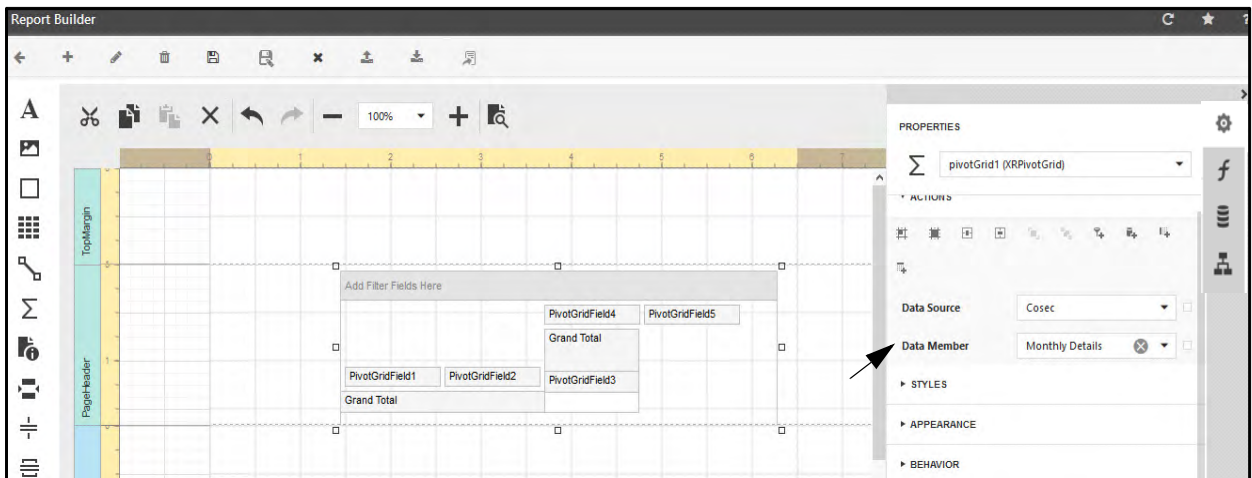
For eg: **Daily Last Out Punch** is selected as shown below.

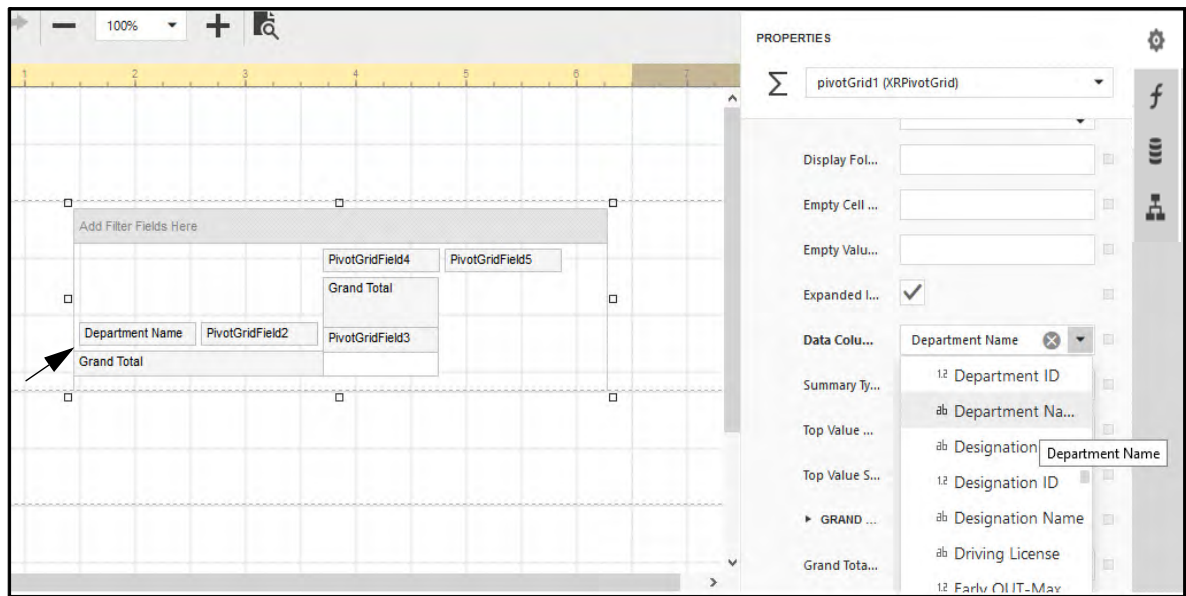


The other pivot grid fields are updated in same way.

Report Group ID	1st Half Status	2nd Half Status	
		Daily Attendanc...	Daily Schdule Sh...
		Grand Total	
User ID	User Name	Daily First IN	Daily Last Out
Grand Total			

Example: Pivot Grid based Report





All the fields are mapped as shown below.

Daily Site ID			
		Month	
		Grand Total	
Department Name	User ID	Work Duration	Late- IN Count
Grand Total			

The report preview is shown below:

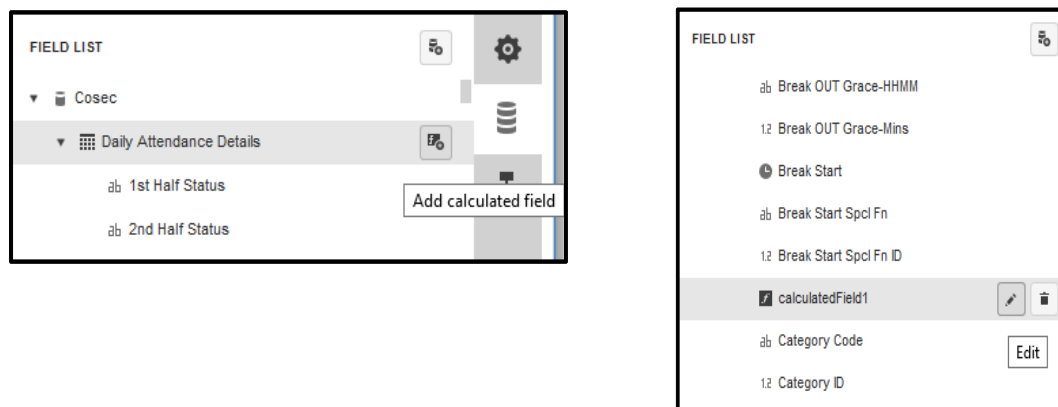
Daily Site ID			
Work Duration	Late- IN Count	Month	
11			
Department Name	User ID	Work Duration	Late- IN Count
Department1	1	0	£0.00
	2	0	£0.00
	3	0	£0.00
	4	0	£0.00
	5	0	£0.00
	6	0	£0.00
	7	0	£3.00
Department1 Total		0	£3.00
Department2	10	0	£0.00
	8	0	£0.00
	9	0	£0.00
Department2 Total		0	£0.00
Grand Total		0	£3.00

Calculated field

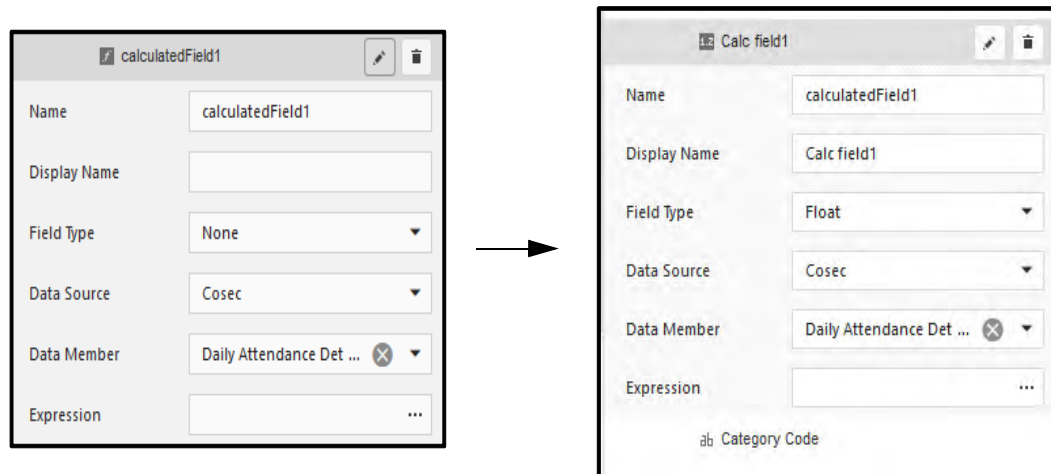
If it's required to perform some pre-calculations over the data field to which a control is bound, this can be done by creating a calculated field, and binding the control to it.

The main purpose of calculated fields is to perform pre-calculations over data fields based on a specific expression.

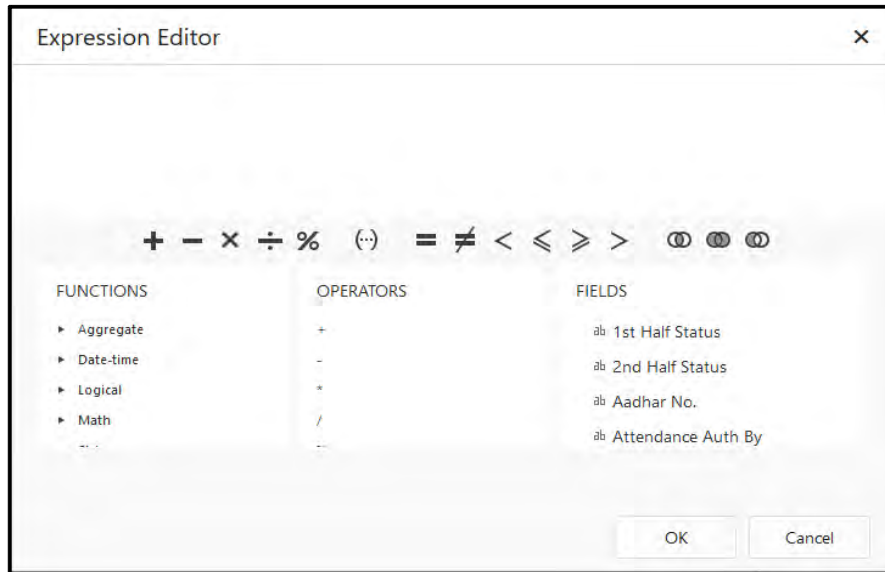
To create a calculated field, in the Field List, Click on Data Source. The icon of Add Calculated field will appear as shown below. Click on **Add Calculated Field**. The field will be created in the field list as shown below.



Click the **Edit** button to configure the calculated field and specify the values of different attributes such as **Display Name**, **Field Type**, **Data Source**, **Data Member** and **Expression**. You can change the **Field Type** property in which the result of calculated field is required.



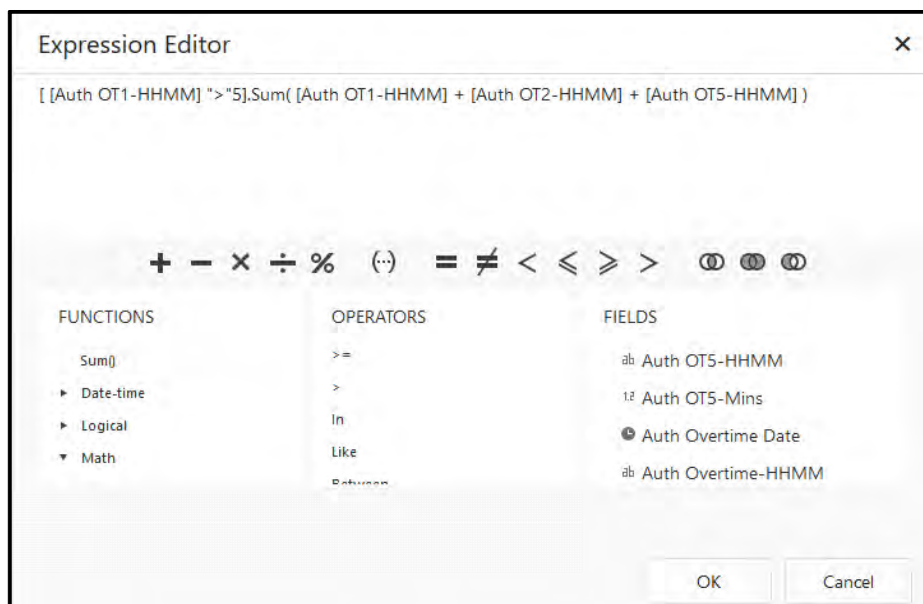
Now, create an expression for the calculated field. Click  in the Expression section. The Expression Editor window appears as shown below.



To perform different string, date-time, logical, and math operations over data, use standard functions from the **Functions** list. To add a data field or report parameter to this expression, double-click the required name in the **Fields** list. A data field is inserted into the expression's text using its name in [square brackets]. To add **operators** between field names, use the toolbar or Operators list.

Select and double-click on the function. Eg: Sum(). Then double-click on the fields to move them to the expression string. Eg: Select Authorized OT1, OT2 and OT5 and click the operator(eg +) between fields from the tool-bar as shown below.

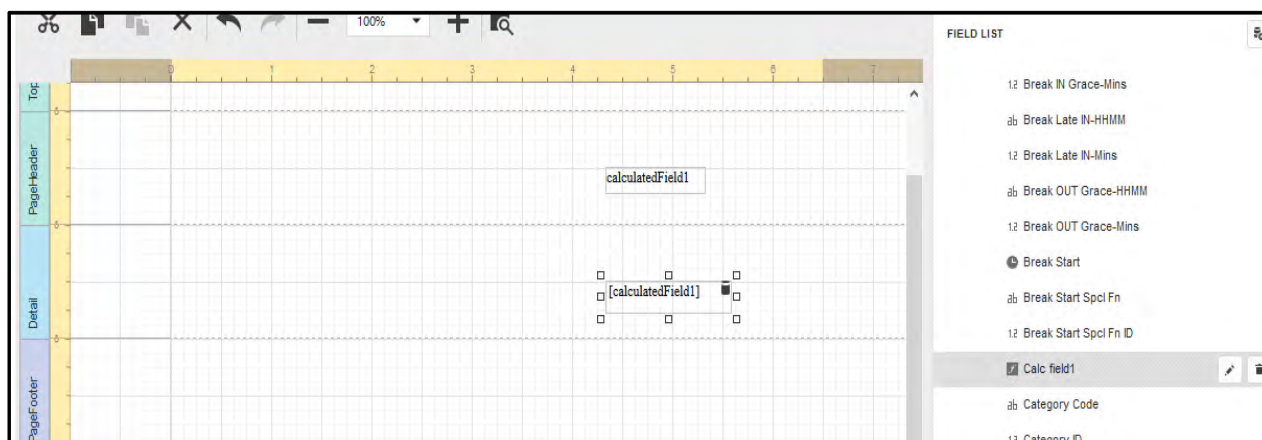
The function [sum()] implies that if some condition is true then sum of defined fields will be done. Eg: If Authorized OT1 is greater than 5 then sum of OT1, OT2 and OT5 will be done.



Then click **OK** to save the expression.

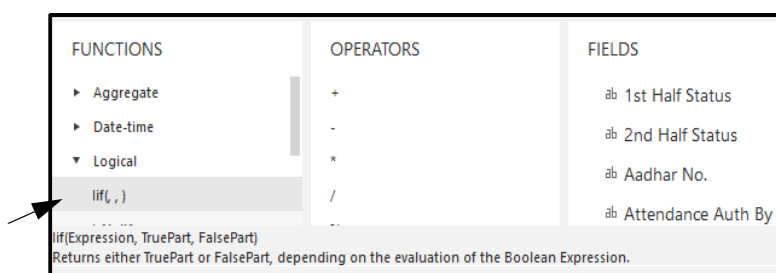
This expression will calculate the sum of all OT1, OT2 & OT5 of all records and will return the overall sum. For calculating sum of individual record, you have to simply specify OT1+OT2+OT5.

Finally, drag the calculated field from the Field List onto the required band, just like an ordinary data field.



Example1- Logical function

For conditional based sum; **lif(,,)** can be used. For this select the function **lif(,,)** from logical functions.

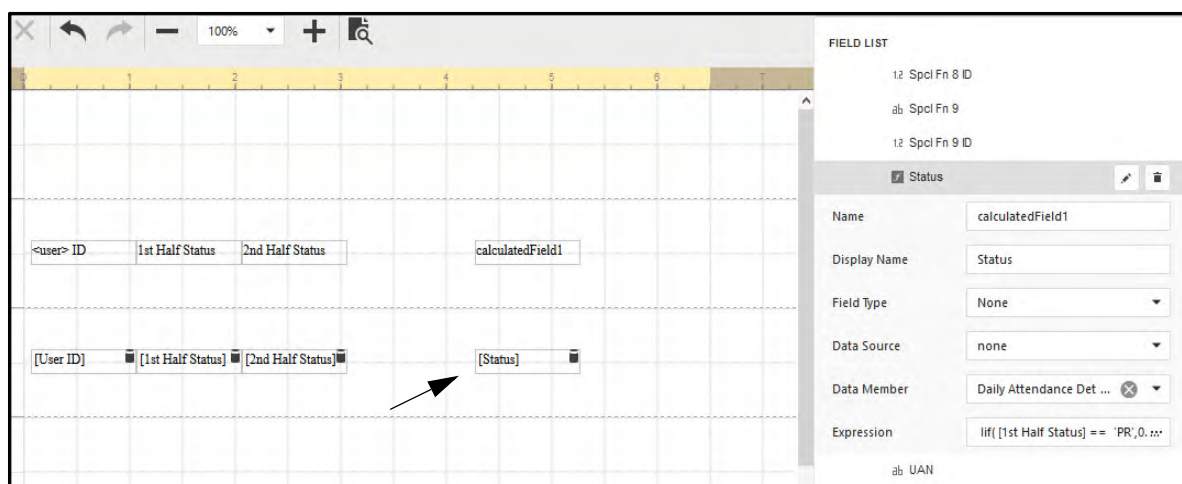


Then select the field to create the expression i.e. If 1st Half Status is equal to PR then display true value as 0.5 or else display 0. The **equal to** operator can be selected from the operators list.

Another expression can also be added to this expression by using **+** operator. Then create expression as If 2nd Half Status is equal to PR then display true value as 0.5 or else display 0. If both 1st half and 2nd half status is PR, PR then resultant will be displayed as 1.



Now this calculated field can be dropped on the Report Detail band as shown below.

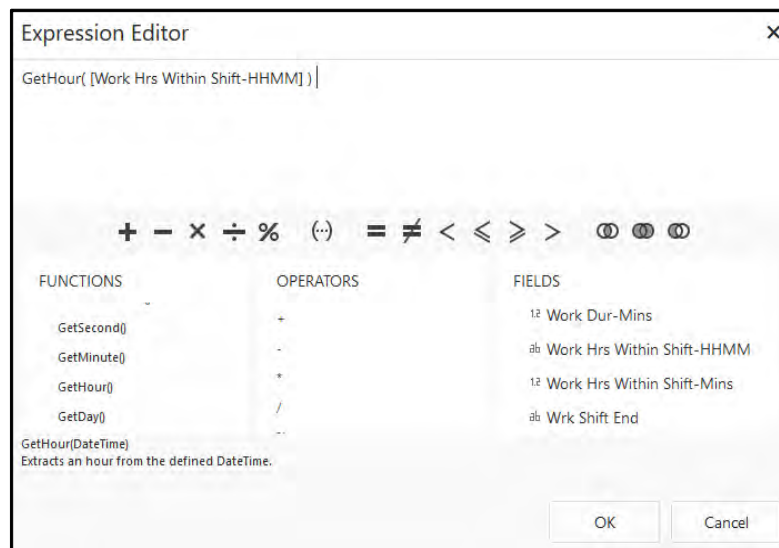


The Report Preview page appears as shown below:

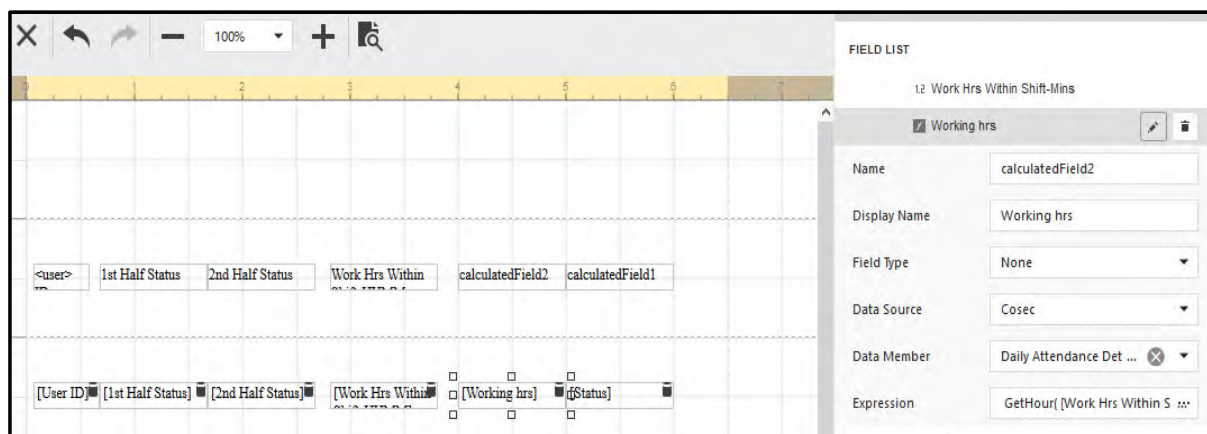
<user> ID	1st Half Status	2nd Half Status	calculatedField1
1	PR	PR	1
1	PR	PR	1
1	WO	WO	0
2	PR	PR	1
2	PR	PR	1

Example2- Date-time function

Select the **GetHour()** function from the Date-time function.



Then select the field- Work Hrs within shift-HHMM.



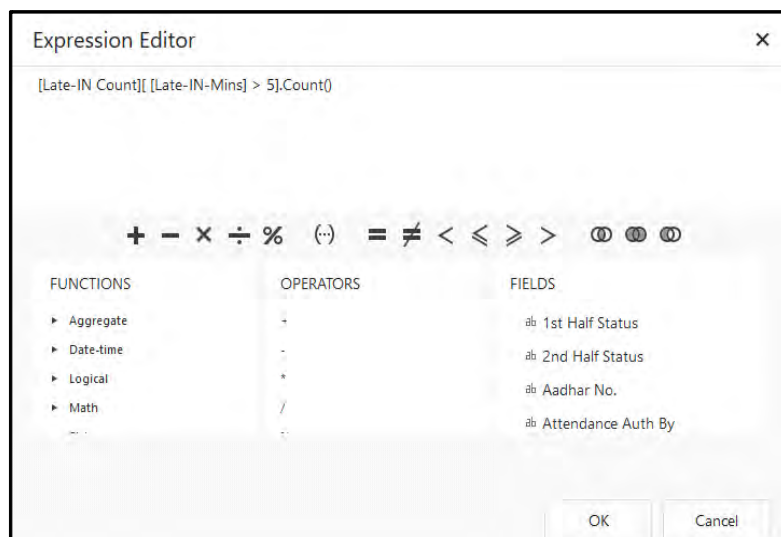
This calculated field when placed in Report will get the value in hours from value in HHMM.

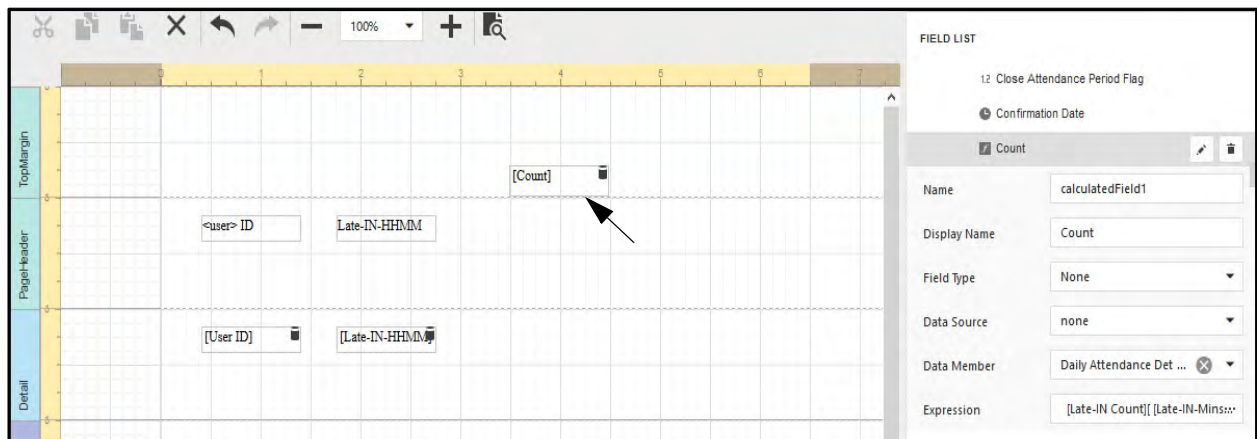
Case ID	1st Half Status	2nd Half Status	Work Hrs Within Shift-HH:MM	calculatedField2	calculatedField1
1	PR	PR	08:00	8	1
1	PR	PR	09:00	9	1
1	WO	WO	00:00	0	0
2	PR	PR	09:00	9	1
2	PR	PR	09:00	9	1

Example3- Aggregate function- Count

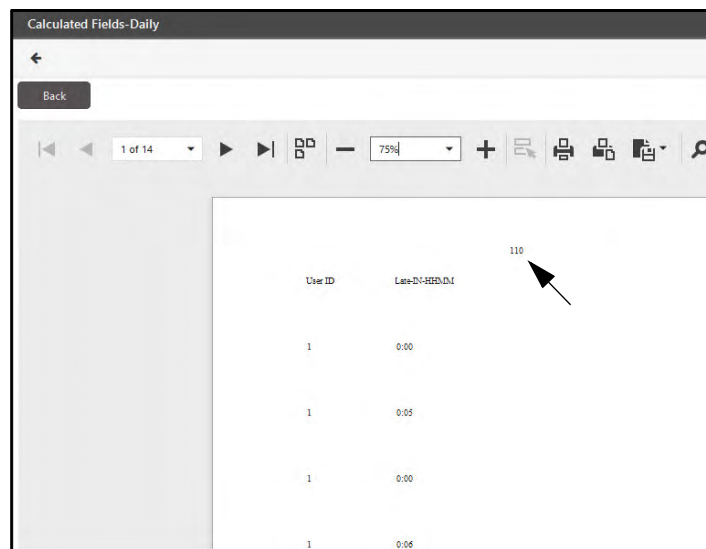
The syntax for Aggregate function is **[Collection] [Condition].Function([Field])**. Count Aggregate function does not require field values to count records so leave round brackets empty.

Select the Aggregate function **Count()**. Then specify Collection as **Late- IN Count**. And condition (optional) as **Late- IN Mins >5**. It returns number of entries in collection based on specified condition. Here If Late-IN Mins is greater than 5 then late-IN count will be displayed.



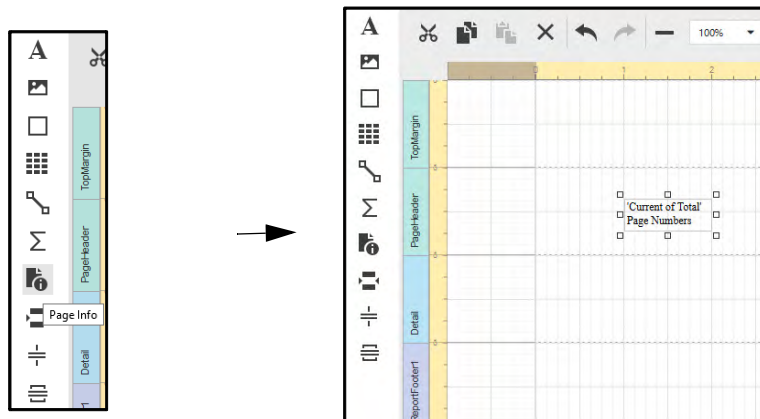


In actual report the calculated field will be shown as below.



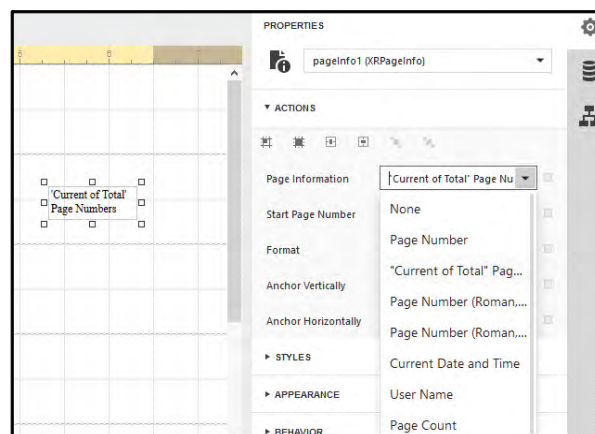
Adding Page Numbers and System information to Report

To add page numbers or system information to a report, drag and drop the **Page Info** control from the Control Toolbox to the Page header band as shown below.



1. For Page Number

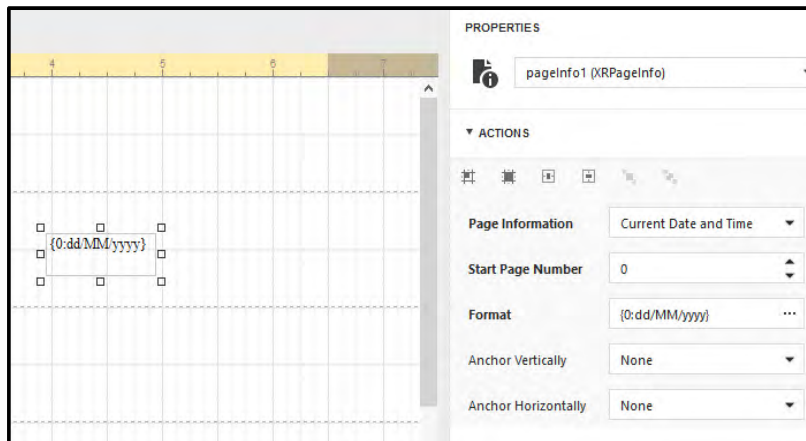
a. Go to Properties > Action. Select whether to display only the page number (Latin or Roman - uppercase or lowercase), or the current page number with total pages.



b. To format the control's text, specify the required format (e.g. Page {0} of {1}). You can also specify the starting page number, and the running band (e.g. this option is available when there are groups in a report, and it's required to apply independent page numbering for them).

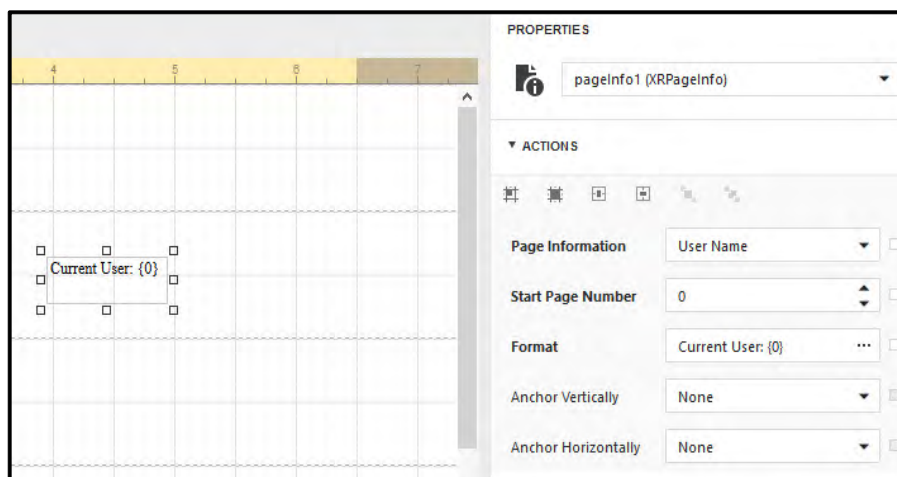
2. For Date and Time

a. Go to Properties > Action. Select Page Information as **Current Date and Time** to display the date and time. Select the required format eg: dd/MM/yyyy Eg: date-time can be used to mention datetime of report generation.

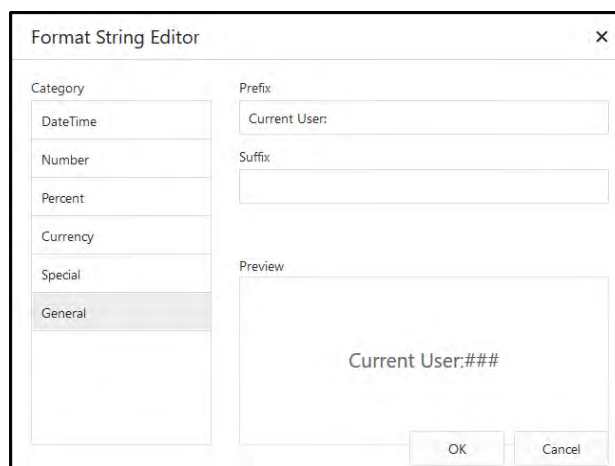


3. For User Name

a. Go to Properties > Action. Select Page Information as **User Name** to display the name of current user. Eg: UserName can be used to mention logged in username. Specify the required format by selecting from the Format(**e.g. Current User: {0}**).



The Format String Editor enables to set Prefix and Suffix as shown below.

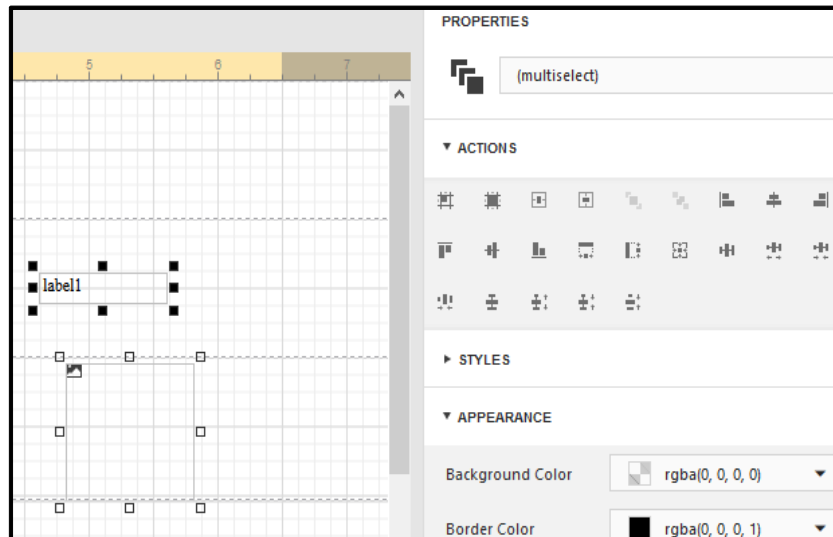


If nothing is specified; then only User Name will be displayed

Controls Positioning

When a control is selected then its related Actions will be activated.

When multiple controls are selected by pressing CTRL and selecting the controls, then Actions related to both the controls are activated as shown for “Custom Field” and “Insert Image” controls.



By pressing **Align to Grid**; the control will get aligned to the nearest grid cell. You can select **Center Horizontally** for moving the control in the horizontal center of the report or **Center Vertically** to move the control in the vertical center of the report.



Page Setting

In the Report Designer, you can change page layout settings before you print a report.

To specify the report's page settings, switch to the **Properties** Panel, and in the Report Controls drop-down list, select the report. Expand the **Page Settings** category and adjust the required page settings.

To create your own paper size, set the Paper Kind property to Custom, and then specify the Page Width and Page Height properties.

Events (XtraReport) Z↓

NAVIGATION

PAGE SETTINGS

Landscape ☒

Roll Paper ☐

Page Width 1100

Page Height 850

Paper Kind Letter

MARGINS

Left 100

Right 135

Top 108

Bottom 100

When you enable Landscape then page orientation will be landscape or else it will be potrait.


When you enable Roll Paper then document will be printed on a roll of paper i.e., as a single uninterrupted page.

Customized Report Page

The Customized Report Page is the user created report as designed from Report builder module. In the report page user can specify the conditions in filter while generating reports.

Example: Events Report Template placed in User module

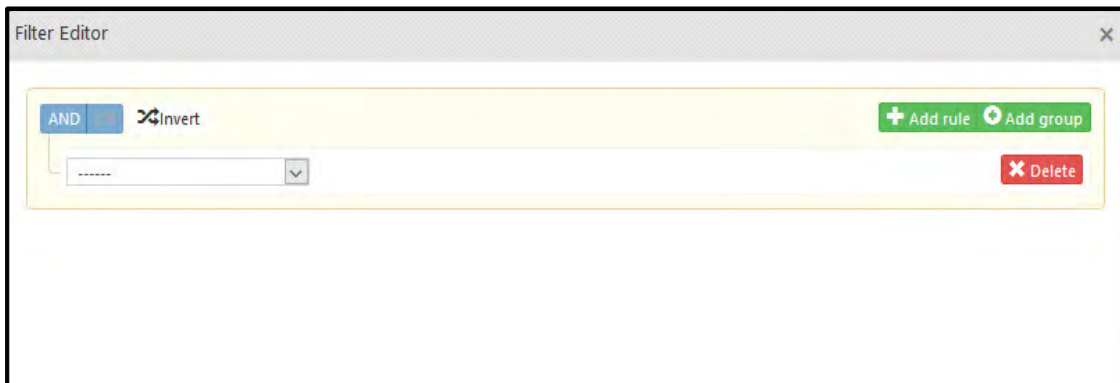
The screenshot shows the 'Modified Event Report' page within the 'Users' module. On the left is a sidebar menu with options like 'User List', 'User Configuration', 'Multi-User Options', 'Credentials Management', 'Reporting In-Charge', 'Utilities', 'Exports', 'Reports', 'Device-Wise Reports', 'User Info', 'Others', 'User Events', 'In/Out Event', 'In/Out Summary', 'Access Denied', 'Doors Accessed By User', 'Door Usage', 'Who Is In', 'Out Time', 'User Events Interval', 'Modified Event Report', and 'Customized Reports'. The main area is titled 'Modified Event Report' and contains a 'Date' field with two date pickers set to 30/01/2018. Below this is an 'Optional Parameters' section with a 'User Selection' sub-section. It includes a 'Select Users' dropdown set to 'User Wise', a 'User' field with 'ID' and 'Name' input boxes, and a 'Generate Report For' dropdown set to 'All Users'. A 'Generate Report' button is at the bottom right of this section.

You can click on **Redirect To Designer Page**  button to switch back to Report Designer for modifying the report design.

Click on **Optional Parameters** panel. In this you can design your own filter to be applied for generating the report.

This screenshot shows the 'Filter' section within the 'Optional Parameters' panel of the 'Modified Event Report' page. It features a 'Date' field with two date pickers set to 03/01/2018 and 04/01/2018. Below the date field is a large empty box labeled 'Filter'. At the bottom, there is a 'Filter Events' dropdown set to 'Both' and a 'Filter Editor' button. An arrow points to the 'Filter Editor' button.

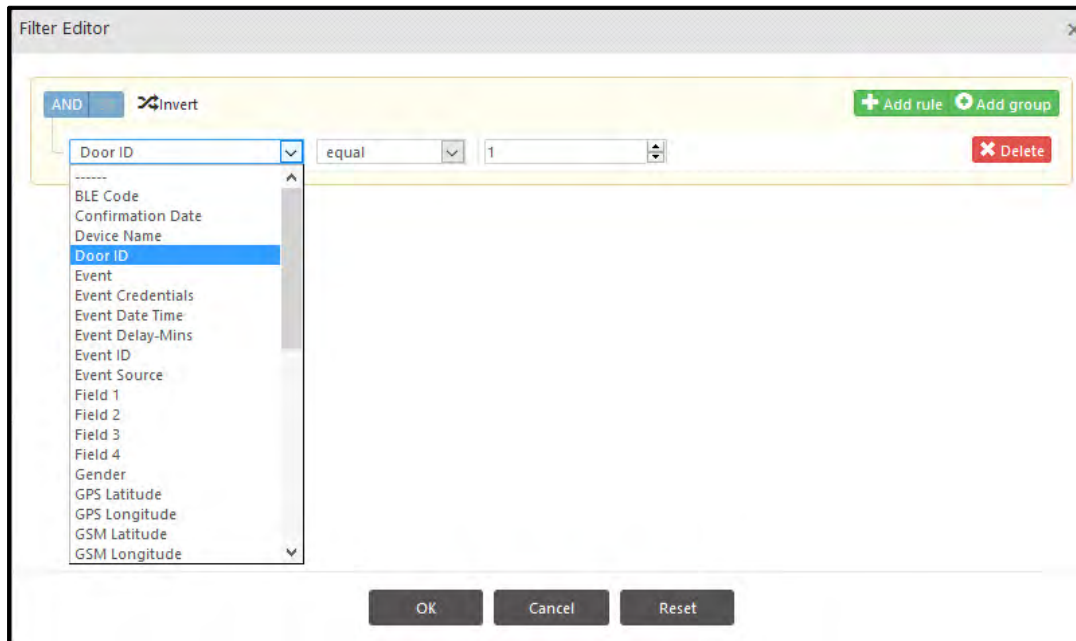
Click **Filter Editor** button. The Filter Editor window opens as shown below.



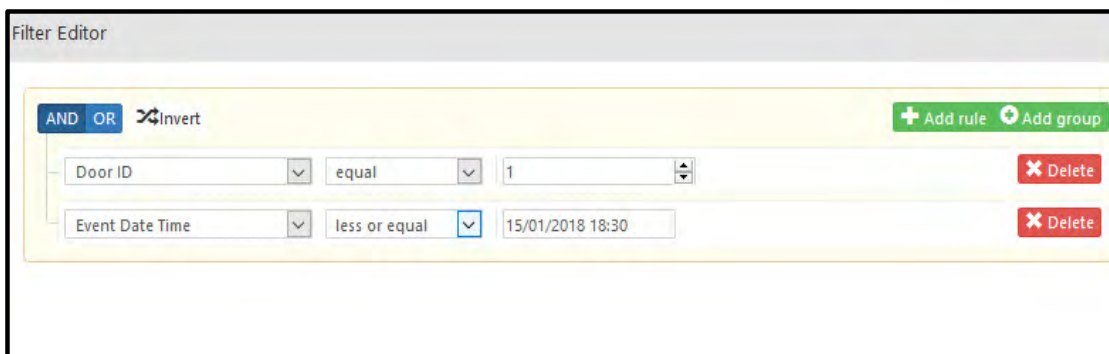
The Invalid characters for filter editor controls are ~ # % ^ * = { } | \ ; " ' < > ?

The **Invert** option changes the group from **AND** to **OR** and vice versa. It also changes values of function from **not equal** to **equal** and vice-versa. Select the logical group.

Now click the drop down list and select the field for defining the rule/condition. Eg: Door ID is set equal to 1.



Then click **Add rule** to define another rule/condition.



Now when Rule1 AND Rule2 are true i.e. where both the conditions are satisfied then report will be generated based on the set filter.

Click **OK**. This filter rule will be reflected in the filter expression as shown below.

Example: Here Event Report will be generated for Door ID=1 and for the events whose generation date-time is before 15/01/2018 18:30.

The screenshot shows the 'Modified Event Report' window. At the top, there are date pickers for 'Date' with values '02/01/2018' and '31/01/2018'. Below this is the 'Optional Parameters' section. It contains a 'Filter' field with the expression '[Door ID] = 1 AND [Event Date Time] <= 15/01/2018 18:30'. An arrow points to this field. Below the filter field is a 'Filter Events' dropdown menu set to 'Both'. In the 'User Selection' section, there are two dropdown menus: 'Select Users' set to 'All' and 'Generate Report For' set to 'All Users'. At the bottom right is a 'Generate Report' button.



For Event based report, you can filter events based on Attendance Events, Access Control events or Both.

You can select the users and click on Generate Report.

The Event Report is shown below.

The screenshot shows the 'Modified Event Report' window displaying the generated event report. The window has a 'Back' button and a toolbar with various icons. The report is titled 'Events Template' and features the 'MATRIX' logo. The report contains a table with the following data:

User Name	Event Source	Event	Event Date Time	Device Name
Chirag	Device	Allowed	03/01/2018 09:00:54	PVR.Door-Device-1
Chirag	Device	Allowed	03/01/2018 16:28:55	PVR.Door-Device-1
Chirag	Device	Allowed	03/01/2018 16:28:55	PVR.Door-Device-1

Glossary of Terms

2-Person Groups: The 2-person rule feature can be used to require that two people enter valid access codes to access a secure area. This is typically used in high security areas or in areas where industrial safety is an issue.

Absentee Rule: This rule sets the maximum number of days for non-use of an ID. On expiration (no ID usage - for the maximum number of days set) the User will be automatically disabled or deleted.

Access Groups: Access Group can be defined as group of users having similar roles and need equal access privileges throughout the day. The access may be restricted to certain times by the use of a time profile.

Access Zones: ACCESS ZONE can be defined as an area with well defined boundaries and access to this area can be controlled using single or multiple doors.

Additional Security: In order to keep Additional level of security check other than Facility code and card number check, smart cards can be written with additional security code that takes security to the next higher level.

Anti-Pass-Back (APB): The Anti Pass Back or APB feature is used to require users to pass through an entry reader followed by passing through an exit reader before their ID will be accepted a second time at another designated entry reader. Hard APB restricts the entry/exit of a person in case of an APB violation while Soft APB does not restrict the person from re-entering/leaving on an APB Violation but reports the same and maintains a log.

Anti-Tamper: A means of detecting unauthorized removal of covers from security equipment.

AWG: American Wire Gauge, denotes the size of wire conductors used in a system.

Badge: To use an access card at a reader to gain access to secure areas.

Blocked User: Blocked Users are users whose credentials have been temporarily blocked due to inactivity, as defined in the Absentee Rule.

Dead Man Timer: This condition allows the system to track the safety and security of a user while a specific task is being performed, by requiring the user to badge his card within the pre-defined dead man time period.

Debounce Time: It defines the minimum time an input interface must be in a given state i.e. up or down, before being reported.

Degraded Mode: Degraded mode allows a valid user to access the facility even if the door controller is not communicating with the master.

DND Zones: DND feature allows the user to declare that a particular zone is not to be accessed by other users for a specific period of time thereby ensuring that the users inside the zone are not disturbed by others.

Door Force Open: A door forced open condition results from a state wherein the door is sensed to be in an open state without an associated valid credential transaction or an associated REX signal.

Door Sense: Contact switch activated whenever a door is opened. This switch monitors the door status (open or closed).

Door Relay: This relay is used to control the locking and unlocking functions of door hardware in an access control system.

Duress detection: Duress detection enables the card holder to trigger an alarm or output device in the event of threats or being forced to grant access to an unauthorized person. The Duress Digit is added at the end of a User's normal Code.

Electric Door Strike: An electric door locking device that unlocks the door when electrical power is applied to it and is thus a fail secure locking device.

Electromagnetic Lock (EM Lock): An electro-magnet must be powered at all times to keep the door locked. It is a fail safe locking device that will automatically unlock if power is removed.

Enrollment: It is defined as the process where in the controller is accepting and storing the user credential inputs against that particular user in any of the modes available viz. Fingerprint, Card, Fingerprint + Card, Smartcard.

Facility Code: Facility code is unique 8 or 16 bits of every HID Prox card number specific to a site and is encoded in to the card by the manufacturer.

First-In Users: First in users are users defined in the system whose card or fingerprint is used to unlock the Access to a particular zone.

Form C Relay: A type of relay which has contacts including a common, a normally open (NO) and a normally closed (NC).

Functional Groups: Functional Group can be defined as cluster of individuals formed to organize them in hierarchical manner and their roles.

Guard Tour: A guard tour is defined as a series of checkpoints where the guard has to badge his credential within a given amount of time.

Home Zone: Home zone is a pre-defined valid access Zone assigned to the user during working and break hours. In other words it can be defined as the assigned work place of the user/employee. User is allowed to access Home zone during working and break hours without checking the access levels and the event is recorded.

Inter Digit Wait Timer: It is the time period between two digits for which the system waits before considering the user input to be complete.

Mantrap: Mantrap, also known as security interlock system provides safety, security and environmental control between two or more rooms by ensuring that opening any door causes all other doors to lock until the opened door returns to the closed position.

Multi Access Wait Timer: Specifies the period within which user needs to present the next credential when Zone access modes are defined for more than one credentials to be used to grant access.

Occupancy Control: Occupancy Control is a feature that monitors and controls the number of users permitted within a secured area or controlled zone. Occupancy controls require entry and exit readers on the controlled area.

Pulse Time: It is the time for which the relay will be energized for a valid credential or input.

REX: REX means Request-To-Exit. A REX device can be used to mask an alarmed Door for authorized exit and to unlock magnetic locks for exit. REX devices can be push-button or motion sensors. A REX Push-button can be installed at a receptionist's desk to manually grant access at an intercom controlled visitor's entry door.

Software Override: The override function allows user to change the current status of a system temporarily from the Software application.

Supervised Inputs: Passive, non-current supplying inputs capable of 4 state monitoring with end of line resistors are supervised inputs.

Time Zones: Time Zones are used to manage the use of IDs and the scheduling of automatic events. Time Zones are made up of a start time, an end time, and a set of valid days.

Use Count Control: Use count control sets a maximum number of times an authorized user can use their credential in order to enter/exit a controlled area after which the credential is blocked.

Visit Zone: Visit zone like the Home Zone is again another predefined valid access zone assigned to the user. Here again the user is allowed to access visit zone during working and break hours without checking the access levels and the event should be recorded.

Visitor Escort Rule: This rule requires all Visitors to be accompanied by an escort and the credential of the visitor has to be followed by the credential of the Escort within the stipulated time period.

Wiegand: A communication protocol widely accepted as an industry standard in the manufacturing of access control equipment. Wiegand data is typically the protocol used between the reader and the host controller.

Zone Access Mode: Zone Access Mode defines the type and number of credentials required to identify and validate a user. Once defined it is assigned to access zones.

GDPR Reflections

General Data Protection Regulation basically ensures security for the users personal data. If you desire implicating with GDPR norms, select the **Personal Data Protection** checkbox in Admin > System Configuration > Global Policy > Basic. To know more refer [“General Data Protection Regulation”](#).

Enabling GDPR will result in data masking and encryption. Set of defined fields revealing users personal data from the respective modules will be considered for masking on the server end, at the same time this data will be encrypted in the database.

The general fields considered for masking and encryption irrespective of the modules are tabulated below:

Profile Photo	Passport Expiry	UAN No	Blood Group	Medical History
Date of Birth	PAN	Voter Id	Height	Marital Status
Driving License No.	Aadhar No	Visa	Weight	Father / Spouse Name
Driving License Expiry	ESI No.	Visa Expiry	Qualification	Official - Mobile, Phone, Email
Passport No.	PF No.	Gender	Experience	Personal - Mobile, Phone , Email
Local - Address, Street, City - Pincode, State, Country	Permanent - Address, Street, City - Pincode, State, Country	PIN	Document File	IMEI number
Mobile Identification Number	Custom Fields	Nationality	Cards (Access cards and Enrolled Cards)	CardCsv (Access cards and Enrolled Cards)
Address Proof	ID Proof 1 ID Proof 2	Signature	Service Tax No.	License No.

Further for detailed reflections, refer to the respective links of the modules as mentioned below:

- [“User Module”](#)
- [“Contract Worker Management”](#)
- [“Time and Attendance”](#)
- [“Visitor Management Module”](#)



Masking will not be applicable for modules other than the above mentioned modules, only relevant data will be encrypted.

Depending on the roles and rights provided to the respective users in Admin> System Accounts > Roles And Rights Configuration, the user data will be considered for masking.

- For all user defined System Account Users or system defined System Engineer/Operator having the roles and rights as **View**, the data will be displayed in masked form.

- For all user defined System Account Users or system defined System Engineer/Operator having the roles and rights as **View**, **Edit** and **Add**, the data will be displayed in unmasked form. These users can edit data for the desired module as existing.

For the Visitor Management Module, you need to make sure the rights for relevant pages are provided. Refer to "[Visitor Management Module](#)" for details.

To know more about Roles and Rights, refer "[Roles and Rights Configuration](#)"



- Make sure while assigning rights for the respective module, provide **View** as well as **Edit** / **Add** right to the parent entity or else you will not be able to edit any field of the child entity. Despite providing necessary rights, the data displayed will be in masked form.

For example: If you have provided all the rights for **Invite User** page (child entity) and assigned only **View** right to the **User Configuration** page (parent entity) then you will not be able to edit any field in the **Invite User** page and data will be displayed in masked form.

User Module

The symbol indicate the following action:

✓	Masked
---	--------

TABS	SUB TABS	FIELD	REFLECTION
User Configuration > Profile	General	Profile Image	Dummy Image
User Configuration > Profile	General	Signature	Hidden
User Configuration > Profile	General	Date of Birth	✓
User Configuration > Profile	General	Driving License	✓
User Configuration > Profile	General	Driving License Expiry	✓
User Configuration > Profile	General	Passport No.	✓
User Configuration > Profile	General	Passport Expiry	✓
User Configuration > Profile	General	PAN	✓
User Configuration > Profile	General	Aadhaar No.	✓
User Configuration > Profile	General	PF No	✓
User Configuration > Profile	General	UAN	✓
User Configuration > Profile	General	ESI No.	✓
User Configuration > Profile	General	Voter ID	✓
User Configuration > Profile	General	Visa	✓

TABS	SUB TABS	FIELD	REFLECTION
User Configuration > Profile	General	Visa Expiry	✓
User Configuration > Profile	General	Custom Fields	✓
User Configuration > Profile	Personal	Gender	✓
User Configuration > Profile	Personal	Blood Group	✓
User Configuration > Profile	Personal	Height (cm)	✓
User Configuration > Profile	Personal	Weight (kgs)	✓
User Configuration > Profile	Personal	Medical History	✓
User Configuration > Profile	Personal	Marital Status	✓
User Configuration > Profile	Personal	Father/Spouse Name	✓
User Configuration > Profile	Personal	Phone	✓
User Configuration > Profile	Personal	Mobile	✓
User Configuration > Profile	Personal	Email	✓
User Configuration > Profile	Personal	Phone	✓
User Configuration > Profile	Personal	Extn	✓
User Configuration > Profile	Personal	Mobile	✓
User Configuration > Profile	Personal	Email	✓
User Configuration > Profile	Personal	Address	✓
User Configuration > Profile	Personal	Street	✓
User Configuration > Profile	Personal	City	✓
User Configuration > Profile	Personal	Pincode	✓
User Configuration > Profile	Personal	State	✓
User Configuration > Profile	Personal	Country	✓
User Configuration > Profile	Personal	Address	✓

TABS	SUB TABS	FIELD	REFLECTION
User Configuration > Profile	Personal	Street	✓
User Configuration > Profile	Personal	City	✓
User Configuration > Profile	Personal	Pincode	✓
User Configuration > Profile	Personal	State	✓
User Configuration > Profile	Personal	Country	✓
User Configuration > Profile	Aadhar QR Popup (Enter Data Manually)	Aadhar No.	✓
User Configuration > Profile	Aadhar QR Popup (Enter Data Manually)	Gender	✓
User Configuration > Profile	Aadhar QR Popup (Enter Data Manually)	Date of Birth	✓
User Configuration > Profile	Aadhar QR Popup (Enter Data Manually)	Address	✓
User Configuration > Profile	Aadhar QR Popup (Enter Data Manually)	Street	✓
User Configuration > Profile	Aadhar QR Popup (Enter Data Manually)	City	✓
User Configuration > Profile	Aadhar QR Popup (Enter Data Manually)	Pincode	✓
User Configuration > Profile	Aadhar QR Popup (Enter Data Manually)	State	✓
User Configuration > Profile	Aadhar QR Popup (Enter Data Manually)	Country	✓
User Configuration > Profile	Aadhar QR Popup (Enter Data Manually)	Father/ Spouse Name	✓
User Configuration > Credentials	-	PIN	✓
User Configuration > Credentials	-	Access Card 1	✓
User Configuration > Credentials	-	Access Card 2	✓
User Configuration > ESS	-	Mobile Identification Number	✓
User Configuration > Face Recognition	Face Enrollment collapsible panel	-	Hidden
User Configuration > Events	Attendance events collapsible panel	View Image	View Image icon disabled
User Configuration > Events	Access Control Events collapsible panel	View Image	View Image icon disabled

TABS	SUB TABS	FIELD	REFLECTION
Credential Management > Enrollment	User Enrollment Status collapsible panel	Enrolled Card 1	✓
Credential Management > Enrollment	User Enrollment Status collapsible panel	Enrolled Card 2	✓
Credential Management > Enrollment	User Enrollment Status collapsible panel	Blood Group	✓
Credential Management > Enrollment	User Enrollment Status collapsible panel	Medical History	✓
Credential Management > Set And Sync Credentials	Single User	PIN Number	✓
Credential Management > Set And Sync Credentials	Single User	Card 1	✓
Credential Management > Set And Sync Credentials	Single User	Card 2	✓
Credential Management > Delete Credentials	Single User	PIN Number	✓
Credential Management > Delete Credentials	Single User	Card 1	✓
Credential Management > Delete Credentials	Single User	Card 2	✓
Utilities > Invite User	Icon (Grid)	Add User	Icon will not be displayed when User Configuration/ Worker Profile Rights= View only
Utilities > Invite User	Icon (Grid)	Add Worker	Icon will not be displayed when User Configuration/ Worker Profile Rights= View only
Utilities > Invite User	Grid > User Details > Basic	Profile Photo	Dummy Image
Utilities > Invite User	Grid > User Details > Basic	Enrolled Face Images	Dummy Image
Utilities > Invite User	Grid > User Details > General	Date Of Birth	✓
Utilities > Invite User	Grid > User Details > General	Driving License	✓
Utilities > Invite User	Grid > User Details > General	Driving License Expiry	✓

TABS	SUB TABS	FIELD	REFLECTION
Utilities > Invite User	Grid > User Details > General	Passport No.	✓
Utilities > Invite User	Grid > User Details > General	Passport Expiry	✓
Utilities > Invite User	Grid > User Details > General	PAN	✓
Utilities > Invite User	Grid > User Details > General	Aadhar No.	✓
Utilities > Invite User	Grid > User Details > General	PF No.	✓
Utilities > Invite User	Grid > User Details > General	UAN	✓
Utilities > Invite User	Grid > User Details > General	ESI No.	✓
Utilities > Invite User	Grid > User Details > General	Voter ID	✓
Utilities > Invite User	Grid > User Details > General	Visa	✓
Utilities > Invite User	Grid > User Details > General	Visa Expiry	✓
Utilities > Invite User	Grid > User Details > General	Field 1	✓
Utilities > Invite User	Grid > User Details > General	Field 2	✓
Utilities > Invite User	Grid > User Details > General	Field 3	✓
Utilities > Invite User	Grid > User Details > General	Field 4	✓
Utilities > Invite User	Grid > User Details > Personal	Nationality	✓
Utilities > Invite User	Grid > User Details > Personal	Qualification	✓
Utilities > Invite User	Grid > User Details > Personal	Experience	✓
Utilities > Invite User	Grid > User Details > Personal	Gender	✓
Utilities > Invite User	Grid > User Details > Personal	Blood Group	✓
Utilities > Invite User	Grid > User Details > Personal	Hieght	✓
Utilities > Invite User	Grid > User Details > Personal	Weight	✓

TABS	SUB TABS	FIELD	REFLECTION
Utilities > Invite User	Grid > User Details > Personal	Medical History	✓
Utilities > Invite User	Grid > User Details > Personal	Marital Status	✓
Utilities > Invite User	Grid > User Details > Personal	Father/Spouse Name	✓
Utilities > Invite User	Grid > User Details > Contact (Contact Info Collapsible Panel)	Personal - Phone	✓
Utilities > Invite User	Grid > User Details > Contact (Contact Info Collapsible Panel)	Personal- Mobile	✓
Utilities > Invite User	Grid > User Details > Contact (Contact Info Collapsible Panel)	Personal -Email	✓
Utilities > Invite User	Grid > User Details > Contact (Contact Info Collapsible Panel)	Official- Phone	✓
Utilities > Invite User	Grid > User Details > Contact (Contact Info Collapsible Panel)	Official- Mobile	✓
Utilities > Invite User	Grid > User Details > Contact (Contact Info Collapsible Panel)	Official- Email	✓
Utilities > Invite User	Grid > User Details > Contact (Address Collapsible Panel)	Local -Address	✓
Utilities > Invite User	Grid > User Details > Contact (Address Collapsible Panel)	Local -Street	✓
Utilities > Invite User	Grid > User Details > Contact (Address Collapsible Panel)	Local -City	✓
Utilities > Invite User	Grid > User Details > Contact (Address Collapsible Panel)	Local -Pincode	✓
Utilities > Invite User	Grid > User Details > Contact (Address Collapsible Panel)	Local -State	✓
Utilities > Invite User	Grid > User Details > Contact (Address Collapsible Panel)	Local -Country	✓
Utilities > Invite User	Grid > User Details > Contact (Address Collapsible Panel)	Permanent -Address	✓

TABS	SUB TABS	FIELD	REFLECTION
Utilities > Invite User	Grid > User Details > Contact (Address Collapsible Panel)	Permanent -Street	✓
Utilities > Invite User	Grid > User Details > Contact (Address Collapsible Panel)	Permanent -City	✓
Utilities > Invite User	Grid > User Details > Contact (Address Collapsible Panel)	Permanent -Pincode	✓
Utilities > Invite User	Grid > User Details > Contact (Address Collapsible Panel)	Permanent -State	✓
Utilities > Invite User	Grid > User Details > Contact (Address Collapsible Panel)	Permanent-Country	✓
Utilities >Exceptional Face Authorization	-	-	Page Hidden
Utilities > IMEI Authorization	Pending Collapsible Panel	IMEI Number	✓
Utilities > IMEI Authorization	Authorized Collapsible Panel	IMEI Number	✓
Utilities > IMEI Authorization	Rejected Collapsible Panel	IMEI Number	✓
Utilities >User Events	Attendance Events Collapsible Panel	View Image	Dummy Image (View Image-disabled)
Utilities >User Events	Access Control Events Collapsible Panel	View Image	Dummy Image (View Image-disabled)
Utilities >User Events	Visitor Events Collapsible Panel	View Image	Dummy Image (View Image-disabled)
Utilities >Blacklist Cards	-	Select Card	Blacklisted Cards Collapsible Panel hidden
Utilities >Blacklist Cards	Blacklisted Card Events Collapsible Panel	Card Number	✓
Report > User Info	Access Profile	Card	Hidden
Report > User Info	Profile Info	Birth Date	Hidden
Report > User Info	Profile Info	Blood Group	Hidden
Report > User Info	Profile Info	Qualification	Hidden
Report > User Info	Profile Info	Nationality	Hidden
Report > User Info	Profile Info	Marital Status	Hidden

TABS	SUB TABS	FIELD	REFLECTION
Report > User Info	Profile Info	Gender	Hidden
Report > User Info	Contact Info	Local Address	Hidden
Report > User Info	Contact Info	Permanent Address	Hidden
Report > User Info	Contact Info	Personal Contact Number	Hidden
Report > User Info	Contact Info	Official Contact Number	Hidden
Report > User Info	Contact Info	Personal Cell	Hidden
Report > User Info	Contact Info	Official Cell	Hidden
Report > User Info	Contact Info	Personal Email	Hidden
Report > User Info	Contact Info	Official Email	Hidden
Report > User Info	Official Info	Qualification	Hidden
Report > User Info	Official Info	Experience	Hidden
Report > User Info	Retirement Info	Date of Birth	Hidden
Report > User Info	Enrollment Info	Card 1	Hidden
Report > User Info	Enrollment Info	Card 2	Hidden
Report > User Info	Enrollment Info	PIN	Hidden

Contract Worker Management

The symbol indicates the following action:

✓	Masked
---	--------

TABS	SUB TABS	FIELD	REFLECTION
Contractor > Contractor Profile	Address Collapsible Panel	Address	✓
Contractor > Contractor Profile	Address Collapsible Panel	Street	✓
Contractor > Contractor Profile	Address Collapsible Panel	City	✓
Contractor > Contractor Profile	Address Collapsible Panel	Pincode	✓
Contractor > Contractor Profile	Address Collapsible Panel	State	✓
Contractor > Contractor Profile	Address Collapsible Panel	country	✓
Contractor > Contractor Profile	Address Collapsible Panel	phone	✓
Contractor > Contractor Profile	Contact Information Collapsible Panel > Contact Person 1	mobile	✓

Contractor > Contractor Profile	Contact Information Collapsible Panel > Contact Person 1	Email	✓
Contractor > Contractor Profile	Contact Information Collapsible Panel > Contact Person 2	Mobile	✓
Contractor > Contractor Profile	Contact Information Collapsible Panel > Contact Person 2	email	✓
Contractor > Contractor Profile	Details Collapsible Panel	Service Tax no.	✓
Contractor > Contractor Profile	Details Collapsible Panel	PAN	✓
Contractor > Contractor Profile	Details Collapsible Panel	PF No.	✓
Contractor > Contractor Profile	Details Collapsible Panel	ESI No.	✓

Contractor > Contractor Profile	License info Collapsible Panel	License No.	✓
Dashboard > Worker Visa Expiry	Visa Expiry pop - up	Visa	Hidden
Dashboard > Worker Driving License Expiry	Driving License Expiry pop - up	Driving License	Hidden
Dashboard > Worker Passport Expiry	Passport Expiry pop - up	Passport	Hidden
Workers > Worker List	-	Profile Image	Dummy Image
Worker Profile> Profile	-	Profile Image	Dummy Image
Worker Profile> Profile	-	Signature	Hidden
Worker Profile> Profile	General	Date of Birth	✓
Worker Profile> Profile	General	Driving License	✓
Worker Profile> Profile	General	Driving License Expiry	✓
Worker Profile> Profile	General	Passport No.	✓
Worker Profile> Profile	General	Passport Expiry	✓
Worker Profile> Profile	General	PAN	✓
Worker Profile> Profile	General	Aadhar No.	✓
Worker Profile> Profile	General	PF No	✓

Worker Profile> Profile	General	UAN	✓
Worker Profile> Profile	General	ESI No.	✓
Worker Profile> Profile	General	Voter ID	✓
Worker Profile> Profile	General	Visa	✓
Worker Profile> Profile	General	Visa Expiry	✓
Worker Profile> Profile	General	Custom Fields	✓
Worker Profile> Profile	Personal	Gender	✓
Worker Profile> Profile	Personal	Blood Group	✓
Worker Profile> Profile	Personal	Height (cm)	✓
Worker Profile> Profile	Personal	Weight (kgs)	✓
Worker Profile> Profile	Personal	Medical History	✓
Worker Profile> Profile	Personal	Marital Status	✓
Worker Profile> Profile	Personal	Father/Spouse Name	✓
Worker Profile> Profile	Contact	Contact Info Collapsible Panel - Phone (Personal)	✓
Worker Profile> Profile	Contact	Contact Info Collapsible Panel - Mobile (Personal)	✓
Worker Profile> Profile	Contact	Contact Info Collapsible Panel - Email (Personal)	✓
Worker Profile> Profile	Contact	Contact Info Collapsible Panel - Phone (Official)	✓
Worker Profile> Profile	Contact	Contact Info Collapsible Panel - Extn. (Official)	✓
Worker Profile> Profile	Contact	Contact Info Collapsible Panel - Mobile (Official)	✓
Worker Profile> Profile	Contact	Contact Info Collapsible Panel - Email (Official)	✓
Worker Profile> Profile	Contact	Address Collapsible Panel - Address (Local)	✓
Worker Profile> Profile	Contact	Address Collapsible Panel - Street (Local)	✓
Worker Profile> Profile	Contact	Address Collapsible Panel - City (Local)	✓
Worker Profile> Profile	Contact	Address Collapsible Panel - Pincode (Local)	✓

Worker Profile> Profile	Contact	Address Collapsible Panel - State (Local)	✓
Worker Profile> Profile	Contact	Address Collapsible Panel - Country (Local)	✓
Worker Profile> Profile	Contact	Address Collapsible Panel - Address (Permanent)	✓
Worker Profile> Profile	Contact	Address Collapsible Panel - Street (Permanent)	✓
Worker Profile> Profile	Contact	Address Collapsible Panel - City (Permanent)	✓
Worker Profile> Profile	Contact	Address Collapsible Panel - Pincode (Permanent)	✓
Worker Profile> Profile	Contact	Address Collapsible Panel - State (Permanent)	✓
Worker Profile> Profile	Contact	Address Collapsible Panel - Country (Permanent)	✓
Worker Profile > Profile	Aadhar QR Popup (Enter Data Manually)	Aadhar No.	✓
Worker Profile > Profile	Aadhar QR Popup (Enter Data Manually)	Gender	✓
Worker Profile > Profile	Aadhar QR Popup (Enter Data Manually)	Date of Birth	✓
Worker Profile > Profile	Aadhar QR Popup (Enter Data Manually)	Address	✓
Worker Profile > Profile	Aadhar QR Popup (Enter Data Manually)	Street	✓
Worker Profile > Profile	Aadhar QR Popup (Enter Data Manually)	City	✓
Worker Profile > Profile	Aadhar QR Popup (Enter Data Manually)	Pincode	✓
Worker Profile > Profile	Aadhar QR Popup (Enter Data Manually)	State	✓
Worker Profile > Profile	Aadhar QR Popup (Enter Data Manually)	Country	✓

Worker Profile > Profile	Aadhar QR Popup (Enter Data Manually)	Father/ Spouse Name	✓
Worker Profile > Credential	Credentials	PIN	✓
Worker Profile > Credential	Credentials	Access Card 1	✓
Worker Profile > Credential	Credentials	Access Card 2	✓
Worker Profile > Credential	Other Details	ID Proof	✓
Worker Profile > Credential	Other Details	Address Proof	✓
Worker Profile > ESS	Settings	Mobile Identification Number	✓
Worker Profile > Face Recognition	Settings	Face Enrollment Collapsible Panel	Hidden
Worker Profile > Events	Events	View Image (Access Control Events Collapsible Panel)	Disabled
Worker Profile > Events	Events	View Image (Access Control Events Collapsible Panel)	Disabled
Authorization/Approval > Induction Approval	General Collapsible Panel	Date Of Birth	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	Driving license	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	Driving License Expiry	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	Passport No.	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	Passport Expiry	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	PAN	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	AADHAR No.	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	PF No.	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	UAN	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	ESI No.	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	Voter ID	✓

Authorization/Approval > Induction Approval	General Collapsible Panel	Visa	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	Visa Expiry	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	Custom fields	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	ID Proof	✓
Authorization/Approval > Induction Approval	General Collapsible Panel	Address Proof	✓
Authorization/Approval > Induction Approval	Personal Collapsible Panel	Nationality	✓
Authorization/Approval > Induction Approval	Personal Collapsible Panel	Qualification	✓
Authorization/Approval > Induction Approval	Personal Collapsible Panel	Experience	✓
Authorization/Approval > Induction Approval	Personal Collapsible Panel	Gender	✓
Authorization/Approval > Induction Approval	Personal Collapsible Panel	Blood group	✓
Authorization/Approval > Induction Approval	Personal Collapsible Panel	Height	✓
Authorization/Approval > Induction Approval	Personal Collapsible Panel	Weight	✓
Authorization/Approval > Induction Approval	Personal Collapsible Panel	Medical history	✓
Authorization/Approval > Induction Approval	Personal Collapsible Panel	Marital status	✓
Authorization/Approval > Induction Approval	Personal Collapsible Panel	Father/spouse Name	✓
Authorization/Approval > Induction Approval	Contact Collapsible Panel	Phone	✓
Authorization/Approval > Induction Approval	Contact Collapsible Panel	Mobile	✓
Authorization/Approval > Induction Approval	Contact Collapsible Panel	Email	✓
Authorization/Approval > Induction Approval	Contact Collapsible Panel	Address	✓
Authorization/Approval > Induction Approval	Contact Collapsible Panel	Street	✓
Authorization/Approval > Induction Approval	Contact Collapsible Panel	City-Pincode	✓

Authorization/Approval > Induction Approval	Contact Collapsible Panel	State	✓
Authorization/Approval > Induction Approval	Contact Collapsible Panel	Country	✓
Authorization/Approval > Induction Approval	Worker Details	View	Dummy Image
Reports > Worker Details	-	Gender	Hidden
Reports > Worker Details	-	Birth Date	Hidden
Reports > Worker Details	-	Blood group	Hidden
Reports > Worker Details	-	PF No.	Hidden
Reports > Worker Details	-	Mobile	Hidden
Reports > Worker Details	-	Qualification	Hidden
Reports > Worker Details	-	Nationality	Hidden
Reports > Worker Details	-	ESI No.	Hidden
Reports > Worker Details	-	Phone	Hidden
Reports > Contractor Details	-	Phone	Hidden
Reports > Contractor Details	-	Mobile	Hidden
Reports > Contractor Details	-	PAN	Hidden
Reports > Contractor Details	-	Email	Hidden
Reports > Contractor Details	-	Contact No.	Hidden

Time and Attendance

The symbol indicates the following action:

✓	Masked
---	--------

TABS	SUB TABS	FIELD	REFLECTION
Utilities > Daily Attendance View	Template Configuration	Any GDPR defined field data shown in the grid view	✓
Utilities > Mark Group Attendance	-	-	Hidden

Visitor Management Module

The symbol indicates the following action:

✓	Masked
---	--------

TABS	SUB TABS	FIELD	REFLECTION	PAGE RIGHTS
Visitor Profile List > Photo View		Profile Image	Dummy Image	Visitor Profile
Visitor Profile		View Image	Dummy Image	Visitor Profile
Visitor Profile > Change Photo		Image	Dummy Image	Visitor Profile
Visitor Profile > Credentials		PIN	✓	Visitor Profile
Visitor Profile > Credentials		Access Card 1	✓	Visitor Profile
Visitor Profile > Credentials		Access Card 2	✓	Visitor Profile
Invite Visitor		Mobile No.	✓	Invite Visitor
Invite Visitor		Email ID	✓	Invite Visitor
Visitor Pre-Registration		Mobile No.	✓	Pre-Registration
Visitor Pre-Registration		Email	✓	Pre-Registration
Visitor Pre-Registration		Date of Birth	✓	Pre-Registration
Visitor Pre-Registration		Address	✓	Pre-Registration
Visitor Pre-Registration		City	✓	Pre-Registration
Visitor Pre-Registration		State	✓	Pre-Registration
Visitor Pre-Registration		Country	✓	Pre-Registration
Visitor Pre-Registration		Pincode	✓	Pre-Registration
Visitor Pre-Registration		Gender	✓	Pre-Registration
Visitor Pre-Registration		Nationality	✓	Pre-Registration
Visitor Pre-Registration		ID Proof 1	✓	Pre-Registration
Visitor Pre-Registration		ID Proof 2	✓	Pre-Registration
Visitor Pre-Registration		Gender	✓	Pre-Registration
Visitor Pre-Registration		Mobile No.	✓	Pre-Registration
Visit Registration Approval		Mobile No.	✓	Visit Registration Approval
Visit Registration Approval		Email ID	✓	Visit Registration Approval

Security Approval		Mobile No.	✓	Security Approval
Security Approval		Email ID	✓	Security Approval
Security Approval		Designation Name	✓	Security Approval
Security Approval		Profile photo	Dummy Image	Security Approval
Visitor Login Authorization		Mobile No.	✓	Visitor Login Authorization
Visitor Login Authorization		Email ID	✓	Visitor Login Authorization
Visit Approval		ID Proof 1	✓	Visit Approval
Visit Approval		ID Proof 2	✓	Visit Approval
Utilities > Set and Sync Credentials > Single Visitor		PIN Number	✓	Set and Sync Credentials
Utilities > Set and Sync Credentials > Single Visitor		Card 1	✓	Set and Sync Credentials
Utilities > Set and Sync Credentials > Single Visitor		Card 2	✓	Set and Sync Credentials
Utilities > Delete Credentials > Single Visitor		PIN Number	✓	Delete Credentials
Utilities > Delete Credentials > Single Visitor		Card 1	✓	Delete Credentials
Utilities > Delete Credentials > Single Visitor		Card 2	✓	Delete Credentials
Utilities > Visitor Events		Searchbox > Mobile No.	Suggestions under Mobile No. will not be displayed	Frequent Visitor
Utilities > Visitor Events		Picklist > Mobile Number	Will function only if exact number is provided	Frequent Visitor
Visitor Events		Mobile Number	✓	Frequent Visitor
Visitor Events		View Image	Dummy Image	Frequent Visitor
Utilities > Frequent Visitor		View Image	Dummy Image	Frequent Visitor
Utilities > Frequent Visitor > Change Photo		Image	Dummy Image	Frequent Visitor
Utilities > Frequent Visitor		Mobile Number	✓	Frequent Visitor
Utilities > Frequent Visitor	Last Visit Details	Gender	✓	Frequent Visitor
Utilities > Frequent Visitor	Last Visit Details	Mobile No.	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	Address	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	City	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	State	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	Country	✓	Frequent Visitor

Utilities > Frequent Visitor	Additional Details	PIN/ZIP Code	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	Email ID	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	Gender	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	Date Of Birth	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	Nationality	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	ID Proof 1	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	ID Proof 2	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	Custom Field 1	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	Custom Field 2	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	Custom Field 3	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	Custom Field 4	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	Custom Field 5	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	Mobile Number	✓	Frequent Visitor
Utilities > Frequent Visitor	Additional Details	Gender	✓	Frequent Visitor
Utilities > Watchlist/Blacklist	Grid > Total	Mobile Number	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Grid > Watchlist	Mobile Number	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist >	Grid > Blacklist	Mobile Number	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist		Mobile Number	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	Address	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	City	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	State	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	Country	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	PIN/ZIP Code	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	Email ID	✓	Watchlist/Blacklist

Utilities > Watchlist/Blacklist	Additional Details	Gender	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	Date Of Birth	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	Nationality	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	ID Proof 1	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	ID Proof 2	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	Custom Field 1	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	Custom Field 2	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	Custom Field 3	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	Custom Field 4	✓	Watchlist/Blacklist
Utilities > Watchlist/Blacklist	Additional Details	Custom Field 5	✓	Watchlist/Blacklist
Utilities > Visitor History		Image	Dummy Image	Frequent Vistor
Utilities > Visitor History		Mobile number	✓	Frequent Vistor
Utilities > Visitor History		ID Proof 1	✓	Frequent Vistor
Utilities > Visitor History		ID Proof 2	✓	Frequent Vistor
Utilities > Visitor History		Vehicle Number	✓	Frequent Vistor
Utilities > Visitor History	Additional Vsitor's Details	Gender	✓	Frequent Vistor
Utilities > Visitor History	Additional Vsitor's Details	Mobile No.	✓	Frequent Vistor
Utilities > Delete Frequent Visitors	Select Visitor	Mobile No.	✓	Delete Frequent Visitors
Reports > Visitor Access > Visitor Enrollment Status		Card 1	Hidden	Visitor Profile
Reports > Visitor Access > Visitor Enrollment Status		Card2	Hidden	Visitor Profile
Reports > Visitor Access > Visitor Enrollment Status		PIN	Hidden	Visitor Profile

Reports > Visitor Summary > Visitor Watchlist/ Visitor Blacklist			Hidden	Frequent Visitor
Reports > Visitor History			Hidden	Frequent Visitor
Visitor Evacuation > Missing Count Link			Hidden	Frequent Visitor

Visitor Management Module - Authorized Host User Login

The symbol indicates the following action:

✓	Masked
---	--------

TABS	SUB TABS	FIELD	REFLECTION	PAGE RIGHTS
Visitor Magement > Invite Visitor		Mobile No.	✓	Logged in user is Authorized Host user
Visitor Magement > Invite Visitor		Email ID	✓	Logged in user is Authorized Host user
Visitor Magement > Visitor Pre Registration		Mobile No.	✓	Logged in user is Authorized Host user
Visitor Magement > Visitor Pre Registration > Additional Visitors Details		Gender	✓	Logged in user is Authorized Host user
Visitor Magement > Visitor Pre Registration > Additional Visitors Details		Mobile No.	✓	Logged in user is Authorized Host user
Visitor Magement > Visitor Pre Registration > Additional Visitors Details > Visitor Profile		Email	✓	Logged in user is Authorized Host user
Visitor Pre Registration > Additional Visitors Details > Visitor Profile		Date of Birth	✓	Logged in user is Authorized Host user
Visitor Pre Registration > Additional Visitors Details > Visitor Profile		Designation Name	✓	Logged in user is Authorized Host user
Visitor Pre Registration > Additional Visitors Details > Visitor Profile		Address	✓	Logged in user is Authorized Host user
Visitor Pre Registration > Additional Visitors Details > Visitor Profile		City	✓	Logged in user is Authorized Host user

Visitor Pre Registration > Additional Visitors Details > Visitor Profile		State	✓	Logged in user is Authorized Host user
Visitor Pre Registration > Additional Visitors Details > Visitor Profile		Country	✓	Logged in user is Authorized Host user
Visitor Pre Registration > Additional Visitors Details > Visitor Profile		Pincode	✓	Logged in user is Authorized Host user
Visitor Pre Registration > Additional Visitors Details > Visitor Profile		Gender	✓	Logged in user is Authorized Host user
Visitor Pre Registration > Additional Visitors Details > Visitor Profile		Nationality	✓	Logged in user is Authorized Host user
Visitor Pre Registration > Additional Visitors Details > Visitor Profile		ID Proof 1	✓	Logged in user is Authorized Host user
Visitor Pre Registration > Additional Visitors Details > Visitor Profile		ID Proof 2	✓	Logged in user is Authorized Host user
Visitor Magement > Visit Approval > Visit Application Details (when Visitor Approve Configuration icon is clicked)		Mobile No.	✓	Logged in user is Authorized Host user
Visitor Magement > Visit Approval > Visit Application Details (when Visitor Approve Configuration icon is clicked)		Email	✓	Logged in user is Authorized Host user
Visitor Magement > Visit Approval > Visit Application Details (when Visitor Approve Configuration icon is clicked)		Designation	✓	Logged in user is Authorized Host user
Visitor Magement > Visit Approval > Visit Application Details (when Visitor Approve Configuration icon is clicked)		ID Proof 1	✓	Logged in user is Authorized Host user
Visitor Magement > Visit Approval > Visit Application Details (when Visitor Approve Configuration icon is clicked)		ID Proof 2	✓	Logged in user is Authorized Host user

Technical Specifications

COSEC Panel200:

Product	COSEC Panel200
CPU	ARM Cortex-A8 32-bit RISC Micro-processor
Flash Memory	256 MB
RAM	512 MB
Input Power	12VDC @ 2A
Control Relay Outputs	1 Alarm Relay (SPDT, 1A @ 30VDC)
Auxiliary Outputs	-
Supervised Inputs	1 Alarm Input
Power Output Ports	-
Reader Power Output	-
LAN	10/100 Mbps
RS485	YES (with 120Ohms Fix EOL Termination)
User Capacity	25,000 (per PANEL)
Event Buffer	500,000 (per PANEL)
Slave Door Controllers	Up to 32 door controllers supported on RS485. Up to 75 door controllers supported on Ethernet.
Physical Dimensions (H x W x D)	104mm x 80mm x 27mm mounted in a plastic enclosure (4.09" x 3.15" x 1.03")
Operating Temperatures	-10°C to 50°C (14°F to 122°F)
Humidity Range	5% to 95% RH Non condensing

COSEC DOOR CONTROLLERS:

Product	Wireless Door/ Door V3	NGT Door	PVR Door	VEGA Door	FMX Door
CPU	32-bit ARM Micro-controller	32-bit ARM Micro-controller	ARM Cortex-A8 32-bit RISC Micro-processor	ARM Cortex-A8 32-bit RISC Micro-processor	800 MHz ARM Cortex A8 based Processor
Flash Memory	256 MB	256 MB	256 MB	256 MB	256 MB
RAM	128 MB	128 MB	512 MB	512 MB	512 MB DDR3 RAM
Input Power	12VDC @ 2A	12VDC @ 2A	12VDC @ 2A	12VDC @ 2A	12VDC @ 2A
Reader I/F Type	Wiegand, RS232	Wiegand, RS232	Wiegand, RS232	Wiegand, RS232	RS-232 and Wiegand IN/OUT mode
Reader Types	RFID (EM Prox, Mifare, HID iClass, HID Prox), Biometric	RFID (EM Prox, Mifare, HID iClass, HID Prox), Biometric	RFID (EM Prox, Mifare, HID iClass, HID Prox), Palm Vein Reader	RFID (EM Prox, Mifare), Biometric	1 Port for Card Reader / Finger Reader / Card Finger Combo Reader / UHF Reader
Control Relay Outputs	1 Lock Relay (SPDT, 1A @ 30VDC)	1 Lock Relay (SPDT, 1A @ 30VDC)	1 Lock Relay (SPDT, 1A @ 30VDC)	1 Lock Relay (SPDT, 1A @ 30VDC)	Relay SPDT, Form C, 1A @ 30 VDC
Auxiliary Outputs	1 Relay (SPDT, 1A @ 30VDC)	1 Relay (SPDT, 1A @ 30VDC)	1 Relay (SPDT, 1A @ 30VDC)	1 Relay (SPDT, 1A @ 30VDC)	Relay SPDT, Form C, 1A @ 30 VDC
Supervised Inputs	4 inputs 1) 2 inputs (Auxiliary & Door Status) capable of 4 state monitoring 2) 2 inputs (Exit Switch & Tamper) have only 2 state monitoring	4 inputs 1) 2 inputs (Auxiliary & Door Status) capable of 4 state monitoring 2) 2 inputs (Exit Switch & Tamper) have only 2 state monitoring	4 inputs 1) 2 inputs (Auxiliary & Door Status) capable of 4 state monitoring 2) 2 inputs (Exit Switch & Tamper) have only 2 state monitoring	4 inputs 1) 2 inputs (Auxiliary & Door Status) capable of 4 state monitoring 2) 2 inputs (Exit Switch & Tamper) have only 2 state monitoring	4 inputs 1) 2 inputs (Auxiliary & Door Status) capable of 4 state monitoring 2) 2 inputs (Exit Switch & Tamper) have only 2 state monitoring
Reader Power Output	12VDC @ 500mA	12VDC @ 500mA	12VDC @ 500mA	12VDC @ 500mA	Internal 12 VDC @ 0.2 A or External
LAN	10/100 Mbps	10/100 Mbps	10/100 Mbps	10/100 Mbps	10/100 Mbps
RS485	YES (with 120Ohms EOL Termination through Switch)	YES (with 120Ohms EOL Termination through Switch)	-	-	-
User Capacity	50,000	10,000	10,000	50,000	50,000

Product	Wireless Door/ Door V3	NGT Door	PVR Door	VEGA Door	FMX Door
Templates Capacity	9,600 (1:N mode), and 1 lakh (1:1 mode)	9,600	20,000	9,600 (1:N mode), and 1 lakh (1:1 mode)	9600 (1:N mode), and 1 lakh (1:1 mode)
Event Buffer	5,00,000	1,00,000	1,00,000	5,00,000	5,00,000
Operating Temperature	- 10 °C to + 50 °C	- 10 °C to + 50 °C	- 10 °C to + 50 °C	- 10 °C to + 50 °C	0 °C to + 50 °C
Humidity Range	5% to 95% RH Non-Condensing	5% to 95% RH Non-Condensing	5% to 95% RH Non-Condensing	5% to 95% RH Non-Condensing	5% to 95% RH Non-Condensing

PSBB Specifications:

Mains Supply Rating	100-265 VAC, 47-63Hz, 60W max.
Mains supply fuse	1A fast blow, glass fuse 5 x 20mm
Output ratings: “Output Voltage “Output Current	13.8 VDC 2A
Max. Ripple Voltage	< 100mV
Battery Type	12V sealed lead acid (3.2Ah)
Output ratings - Charger Battery Charge Voltage Battery Charge current	13.8V 1A
Battery Dimensions (H x W x D) in mm and inches	67mm x 134mm x 67 mm (2.64" x 5.28" x 2.64") - Vision model cp 1232 or equivalent

Cable Specifications:

Cable Type	Length	Specification
Ethernet	328 feet (100 m)	Cat5, Cat5E, and Cat6
RS-485 *	1000 m to host	Use Belden 3105A, 22AWG twisted pair, shielded 100Ω cable, or equivalent.
External Readers (Serial)	15 feet (4.57 m) for RS232 reader to COSEC Door Controller	ALPHA 1299C 22AWG, 13 conductor, stranded, overall shield (Fewer conductors needed if all control lines are not used)
External Readers (Wiegand)	500 feet (150 m) to reader	ALPHA 1299C 22AWG, 13 conductor, stranded, overall shield (Fewer conductors needed if all control lines are not used)
Input Circuits *	500 feet (150 m)	2-conductor, shielded, using ALPHA 1292C (22AWG), or equivalent.

Cable Type	Length	Specification
Output Circuits *	500 feet (150 m)	2-conductor, using ALPHA 1172C (22AWG) or equivalent.

* Minimum wire gauge depends on cable length and current requirements.

Card Compatibility Matrix:

Reader	Type	Function	Support
EM Prox Card Reader	125 KHz	Read Only	All EM Prox Cards
HID Prox Reader	125 KHz	Read Only	HID Prox Cards: 26 Bit format with FC (Base P/N H10301) 37 Bit format without FC (Base P/N H10302) 37 Bit format with FC (Base P/N H10304)
Mifare Card Reader	13.56 Mhz	Read & Write	Mifare Smart Cards: Mifare 1k Card Mifare 4k Card Mifare Ultralight (only CSN read)
HID iClass Reader	13.56 Mhz	Read & write	HID iClass Smart Cards (26 and 37 bit format) 2K/2 Card (base P/N 2000 series) 16K/2 Card (base P/N 2001 series) 16K/16 Card (base P/N 2002 series) All types of Mifare Cards (only CSN read)
Fingerprint Reader	Optical	Enroll & scan	9600 FP templates
Fingerprint Reader	Capacitive	Enroll & scan	9600 FP templates
Palm Vein Reader	Infrared	Enroll & scan	20,000 palm templates

Disposal of Products/Components after End-Of-Life

Main components of Matrix products are given below:

- **Soldered Boards:** At the end-of-life of the product, the soldered boards must be disposed through e-waste recyclers. If there is any legal obligation for disposal, you must check with the local authorities to locate approved e-waste recyclers in your area. It is recommended not to dispose-off soldered boards along with other waste or municipal solid waste.
- **Batteries:** At the end-of-life of the product, batteries must be disposed through battery recyclers. If there is any legal obligation for disposal, you may check with local authorities to locate approved batteries recyclers in your area. It is recommended not to dispose off batteries along with other waste or municipal solid waste.
- **Metal Components:** At the end-of-life of the product, Metal Components like Aluminum or MS enclosures and copper cables may be retained for some other suitable use or it may be given away as scrap to metal industries.
- **Plastic Components:** At the end-of-life of the product, plastic components must be disposed through plastic recyclers. If there is any legal obligation for disposal, you may check with local authorities to locate approved plastic recyclers in your area.

After end-of-life of the Matrix products, if you are unable to dispose-off the products or unable to locate e-waste recyclers, you may return the products to Matrix Return Material Authorization (RMA) designation.

Make sure these are returned with:

- proper documentation and RMA number
- proper packing
- pre-payment of the freight and logistic costs.

Such products will be disposed-off by Matrix.

"SAVE ENVIRONMENT SAVE EARTH"

Open Source Licensing Terms and Conditions



These licensing terms and conditions are applicable only for the 'COSEC Jeeves' onboard web application.

- The firmware of this product also includes some of the Open-Source software released under GNU General Public License (GPL) Version 2. Terms of this license is printed in full below.
- The source of the open source software used in this product is available on CD, upon written request from:

R&D Team
MATRIX COMSEC PVT. LTD.
394, Makarpura GIDC,
Vadodara - 390 010
Gujarat
India.

Customer shall bear the shipping and handling charges.

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any

part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include

anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that

system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year>  <name of author>
```

```
This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.
```

```
This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public License for more details.
```

```
You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

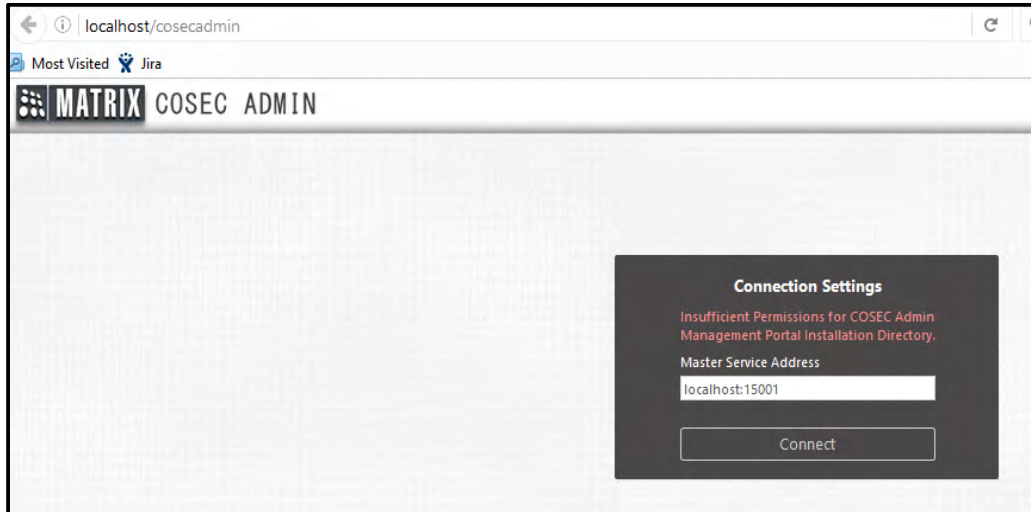
```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.
```

```
<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice
```

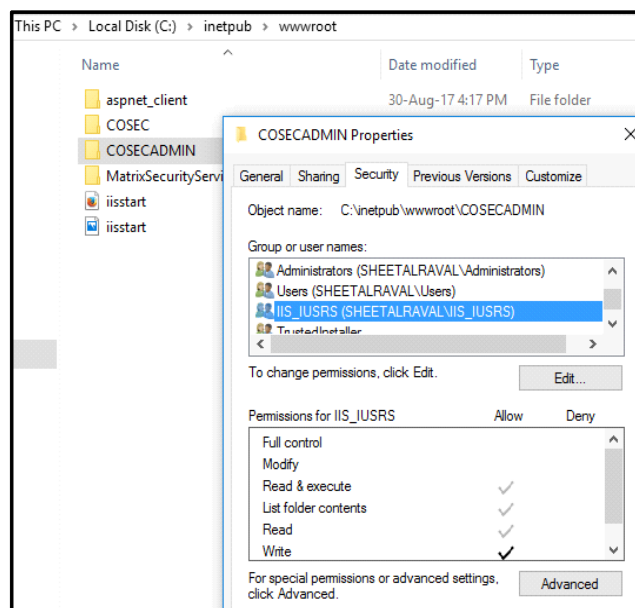
This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

Troubleshooting

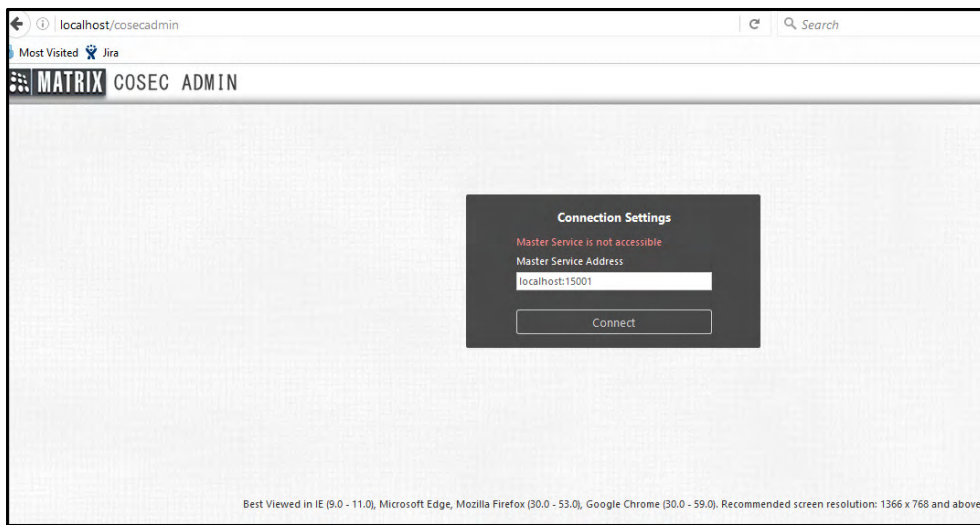
1. *When I login to Admin Portal, and permissions are insufficient to access the portal; then*



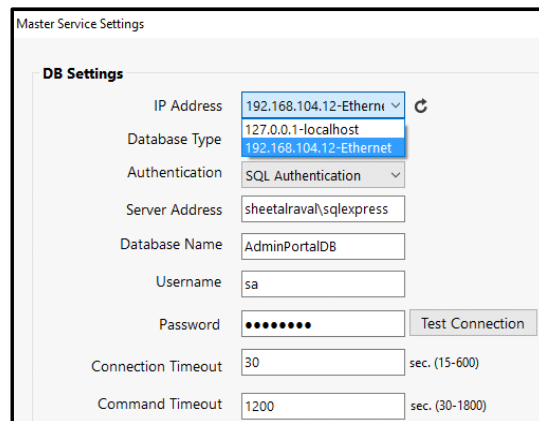
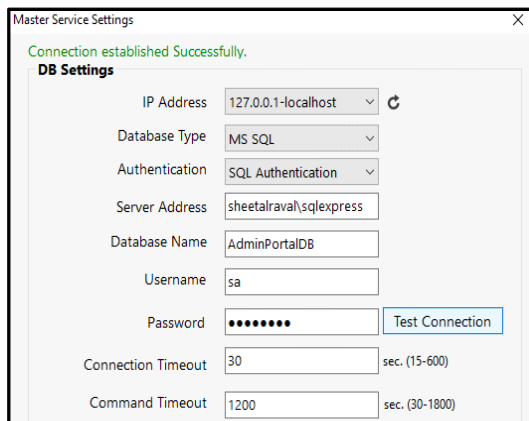
- Check the rights on COSECADMIN folder. For this go to path C:\inetpub\wwwroot. The IIS user must be given full control rights. So click Edit and enable Full control checkbox. Then apply the changes. Now you can login to Admin Portal.



2. **When I login to Admin Portal and Master Service is not accessible; then**



- Check the database settings. Ensure that connection of Admin Portal database is established with database server.
- Check that the IP address at which Master service is running is correctly selected. If the IP address has gone to 127.0.0.1 - Localhost; then you must manually select the IP address from the drop down list at which master service would be running.
- Then start the Master service from the service tray. Once the Admin portal database is upgraded then Master service will be started.



3. **When Admin Portal is running and error comes on Monitor configuration page; then**

- Ensure that Admin Portal's database and Tenant's database are different. If same database is kept, conflict in columns may occur.
- You must upgrade the existing database of tenant when new setup is installed. You can create new database of Tenant from Tenants > Database Configuration.

4. **When License voucher invalid/does not exist in COSEC VYOM; then**

- Check the Matrix Licensing Server URL in General Settings. Ensure that the license key and voucher is available on the specified licensing server.

- Ensure that the PC where Admin Portal is installed can access the Licensing server IP.

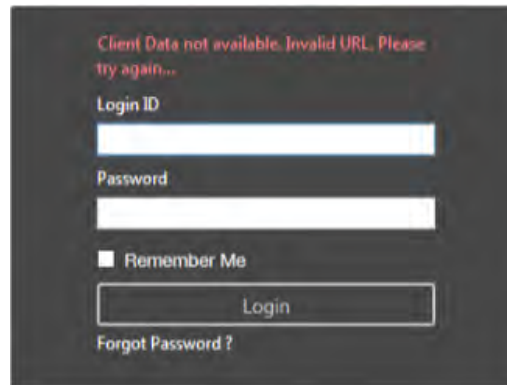


Enter the Matrix licensing Server URL in System Configuration > General Settings before creating a tenant.

Current Balance		As on Date: 08/11/2017	
Platform:	0	VMM:	0
TAM:	0	CMM:	0
ACM:	0	JPC:	0
FVM:	0	ESS:	0
CWM:	0		

5. **When you login to COSEC Web and following error comes, then ensure that License voucher of COSEC is activated.**

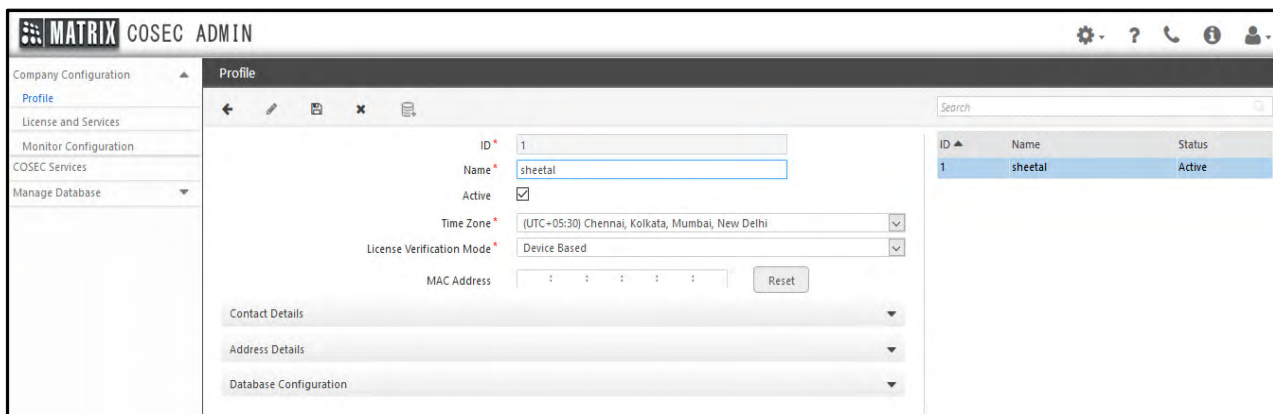
6. **When Client Data is not available; then check that Client URL is available in the Web config file at path C:\inetpub\wwwroot\COSEC**



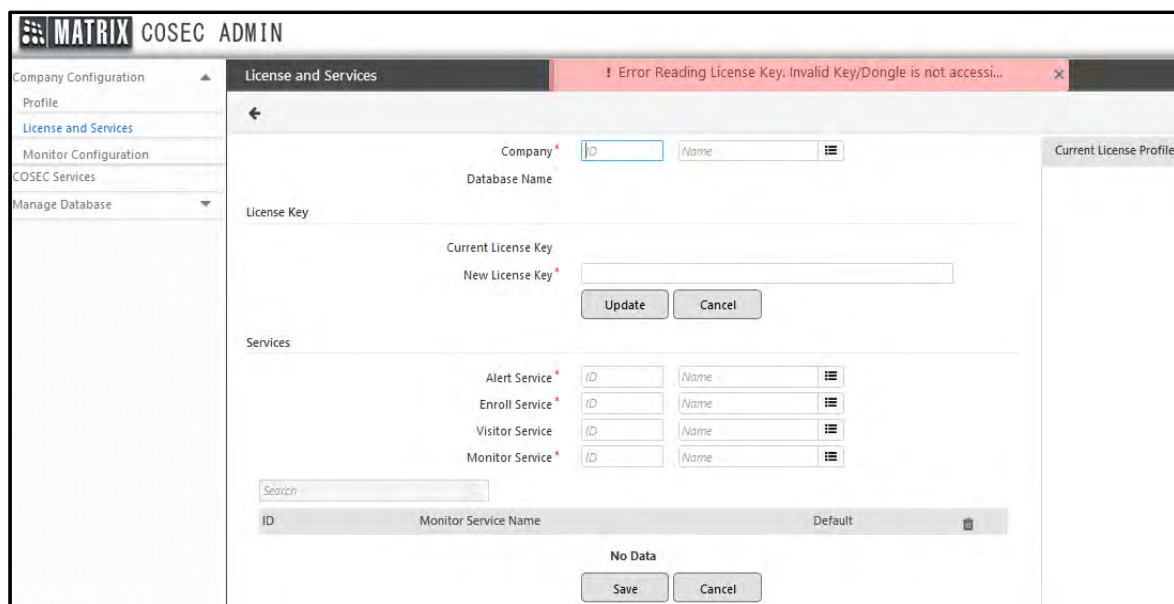
7. *How to configure Device based License verification mode.*

Connect the dongle on Panel200(or Vega controller)

Make the tenant/company as Device based for license verification mode. Save the settings.

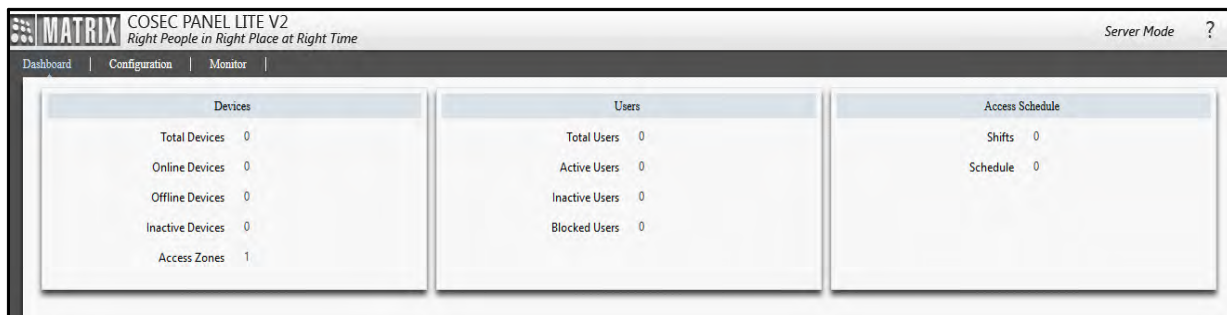


Now check the License and Services page.

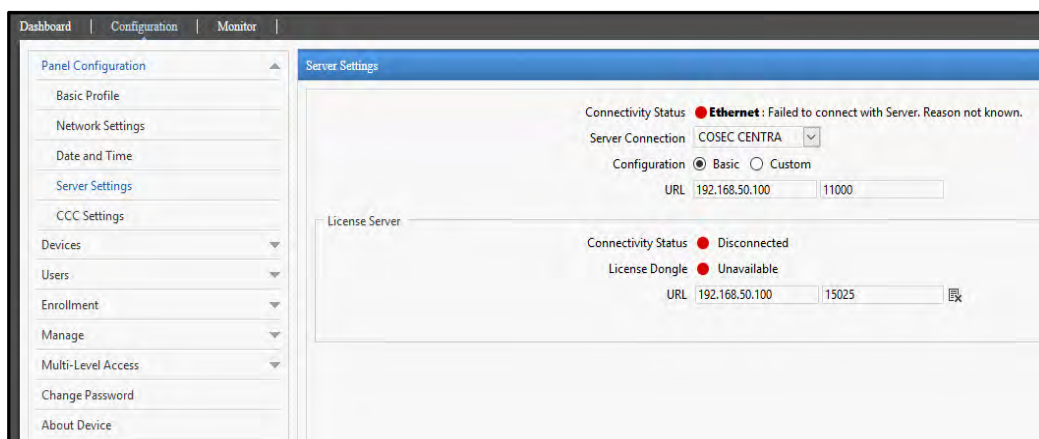


If there is Error in reading license key, then check the Device settings.

Now login to the webpage of Panel200. Ensure that Panel200 is in Server mode. If it is in standalone mode, change the mode to Server mode from Configuration > Panel Configuration> Basic Profile> Panel Mode.



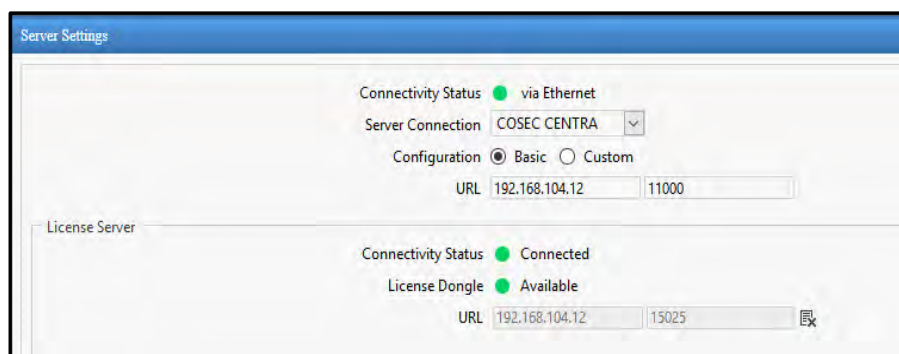
Now go to Panel Configuration> Server Settings. The default settings are shown.



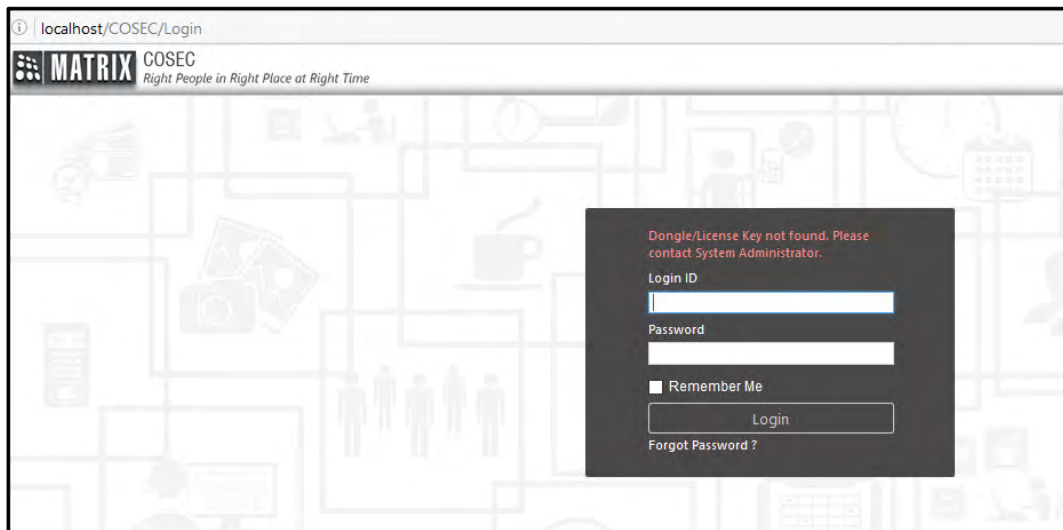
The URL for COSEC Centra server is the IP address of the computer where Monitor Service is running.

The License Server URL is the IP address of the computer where Master Service is running.

If Monitor service and Master service are on same computer then enter the same IP address with the respective port as shown below.

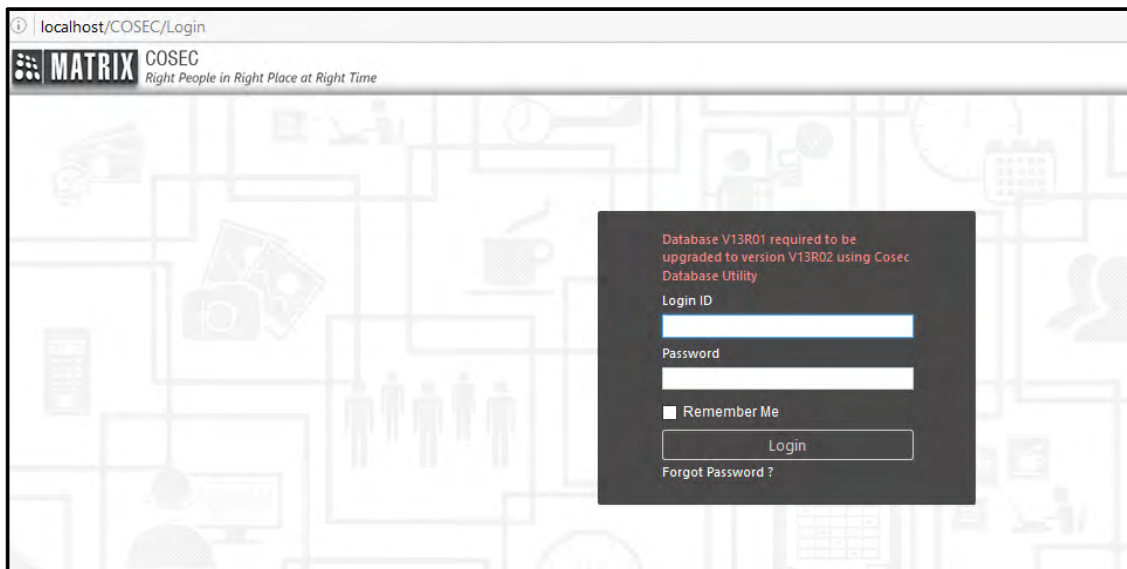


8. *I have re-installed the setup; when I login to COSEC Web, license key is not found.*

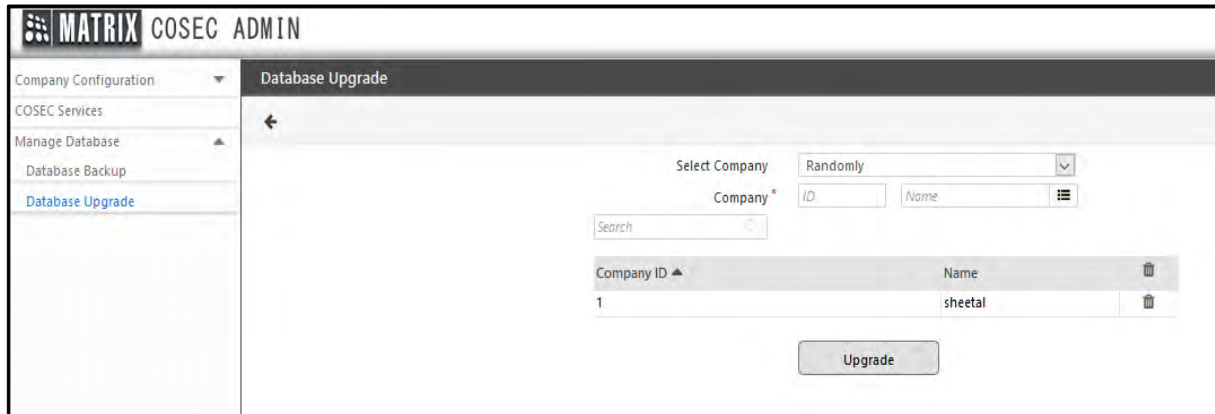


- Login to Admin Portal. Check the license verification mode in the Profile.
- If it is server based then insert the dongle to the CPU where Master service is installed.
- If it is device based then insert the dongle to Panel200 or Vega controller with which it was configured before. Or you can also Reset to use another device.

9. *When I login to COSEC Web and database is required to be upgraded.*



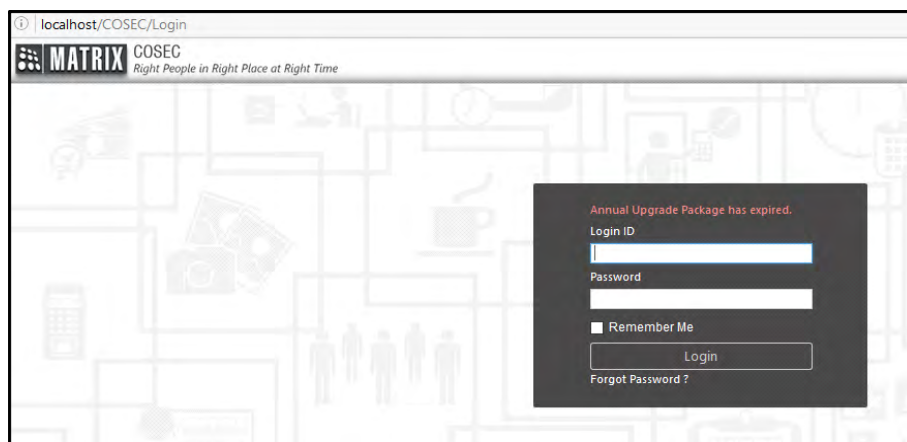
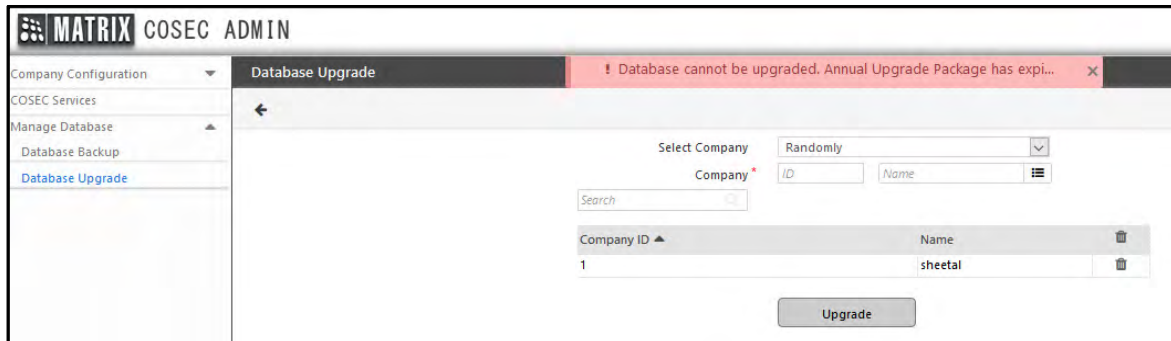
- Login to Admin Portal. Go to Manage Database> Database Upgrade.
- Select the company and click on Upgrade.
- Then click on Refresh. Once database is upgraded, status will be updated to Success. Now you can login to COSEC web.



10. *I have to change the database of COSEC Web. How can I do?*

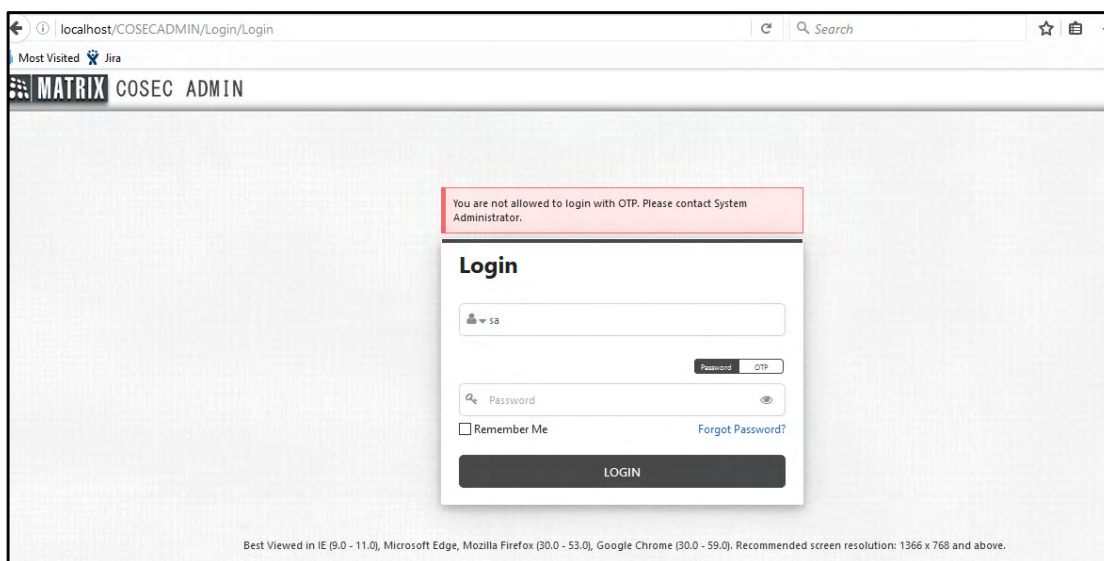
- Login to Admin Portal. Go to Profile> Database Configuration.
- You can change the type of database or different database of the current type. Then click Test Connection to test the connection with database and click Save to save the changed database.
- Now you can login to COSEC web with changed database.

11. *When I am trying to upgrade database; Annual Upgrade Package has expired and I am not able to login into COSEC. What to do?*



You have to upgrade the Annual package of License. For this contact Matrix channel partner.

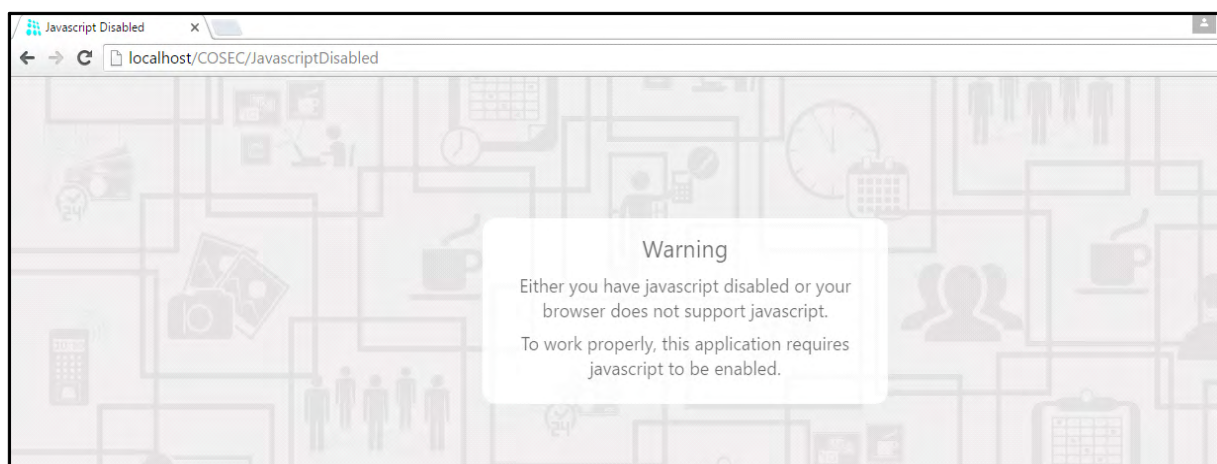
12. *I am not allowed to login into COSEC Admin Portal using OTP. What to do?*



- Login into Admin Portal with password. Then go to System Configuration> Login Policy and verify that the login policy is set as **Password OR OTP**.
- Ensure that SMS Configuration/Email Configuration are done.
- The Email ID and Contact number must be available on the System Accounts page so that OTP can be sent to the configured number and or Email ID.

Similarly you can select **Password Then OTP** option to enable 2 step authentication during login.

13. *I am not allowed to login into COSEC Web and COSEC Admin Portal due to disabled Javascript. What to do?*



You must enable Javascript on the browser.

- For this open the browser. Go to the Settings section.
- Go to the JavaScript section. Also you can search by keyword.
- Enable the option "Allow all Sites to run JavaScript".



MATRIX COMSEC

Head Office:

394-GIDC, Makarpura, Vadodara - 390010, India.

Ph: (+91)18002587747

E-mail: Tech.Support@MatrixComSec.com

www.matrixaccesscontrol.com