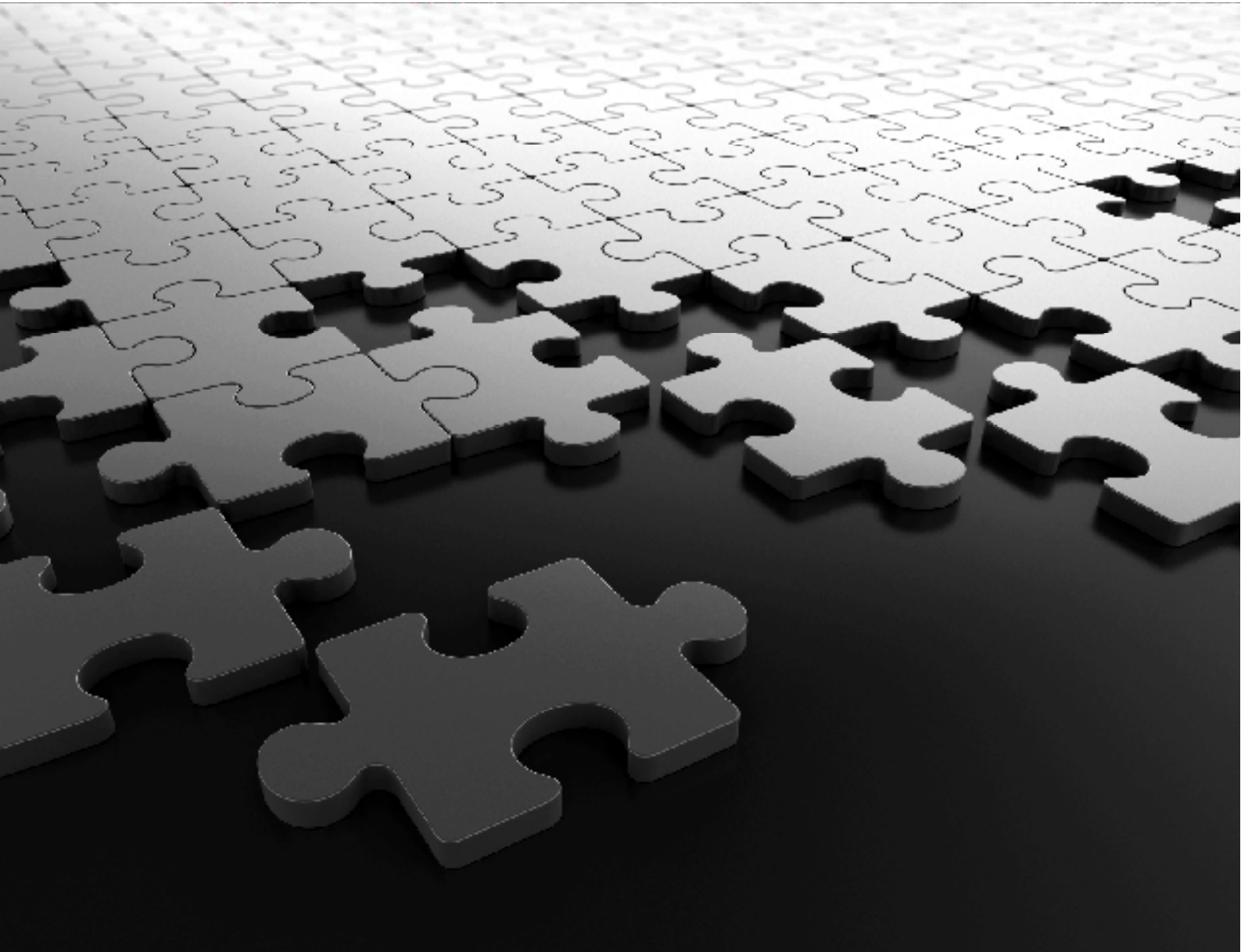


Admin Management Portal User Manual



COSEC CENTRA

Admin Management Portal

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.matrixcomsec.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 20

Release date: December 14, 2022

Contents

Introduction	1
Know your COSEC Admin Portal	3
Software Installation.....	5
<i>Getting Started with Admin Portal</i>	<i>17</i>
Company Configuration	27
<i>Profile</i>	<i>28</i>
<i>License and Services</i>	<i>35</i>
<i>Monitor Configuration</i>	<i>40</i>
COSEC Services	45
Manage Database	51
<i>Database Backup</i>	<i>52</i>
<i>Database Upgrade</i>	<i>53</i>
System Configuration	55
<i>Maintenance Configuration</i>	<i>56</i>
<i>Security</i>	<i>58</i>
<i>SMS Configuration</i>	<i>60</i>
<i>Email Configuration</i>	<i>65</i>
<i>General Settings</i>	<i>67</i>
<i>Multi-language Configuration</i>	<i>69</i>
<i>Login Policy</i>	<i>70</i>
<i>System Accounts</i>	<i>71</i>
<i>Help, Contact, About Us</i>	<i>72</i>
<i>Change Password</i>	<i>73</i>

Welcome

Thank you for choosing the Matrix COSEC Time Attendance and 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.

Organization of this Document

This System Manual exclusively focuses on COSEC Centra.

It contains the following topics:

- **Know Your COSEC Admin Portal** - describes the roles and functioning of Admin Portal for managing companies (clients) in COSEC.
- **Software Installation** - gives step-by-step instructions for installation and configuration of Admin portal.
- **Getting Started** - provides information about configuration of Database server and COSEC Services.

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.

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 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

Know your COSEC Admin Portal

COSEC Admin Management Portal enables the admin to configure the Company's profile, assign license and services, manages database of the company.

While installing the Admin Portal setup; the Company details must be entered on the “*Admin Management Portal DB details*” page. So when you login to Admin Portal web, company profile will get created automatically. See *Chapter: Software Installation for details*.

Once the COSEC setup is installed, Admin can access Admin Management portal. And the Admin can do following things:

- Change Company's database from Profile > database configuration as required.
- Update license verification mode from device based to server based or vice versa.

The System Architecture of COSEC Centra along with Admin Portal is shown below. 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.

Master Service

- Handles request from all other components.
- Provides updated 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.

Admin Portal Service is required for following functions:

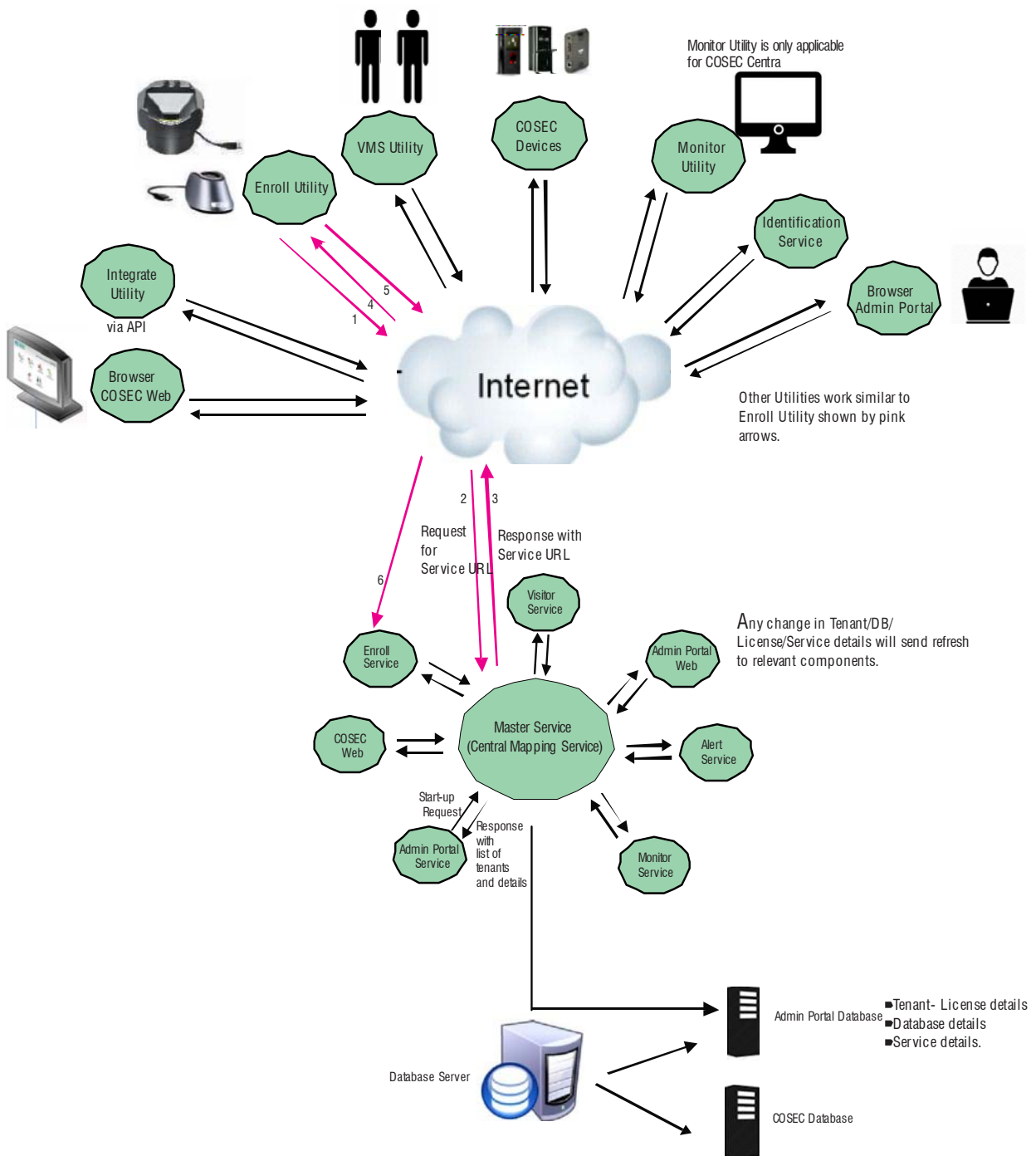
- Database upgrade (COSEC DBs)
- Post, Retrieve and Remove records.



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.

The Alert Service, Enroll Service, Monitor Service and Visitor Service details with configuration is explained in *Chapter: COSEC Services*.

System Architecture



Browser Requirement

The COSEC Admin Management Portal is best viewed in

- Internet Explorer- Version 9.0 and above,
- Mozilla Firefox- Version 24.0 and above
- Google Chrome- Version 30.0 and above

Recommended Screen resolution is 1366 X 768 and above.

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:** Non-Secure = 11001 & Secure = 11010
5. **Admin Portal Service:** Non-Secure = 14001 & Secure = 14010
6. **Visitor Service:** Non-Secure = 16001 & Secure = 16010

Installation of Admin Portal and Admin Portal Service

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 below mentioned functions.

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

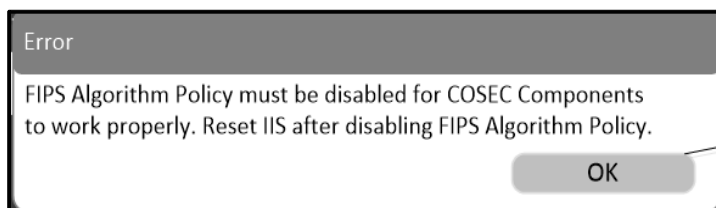
Hence if above functions are to be used then Admin Portal service must be installed with Admin portal Web or Admin Portal service must be accessible at different computer.



Admin Portal Service will be active and running only if Master service is running.

FIPS Algorithm Policy Check

To Install COSEC Admin Management Portal; 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.

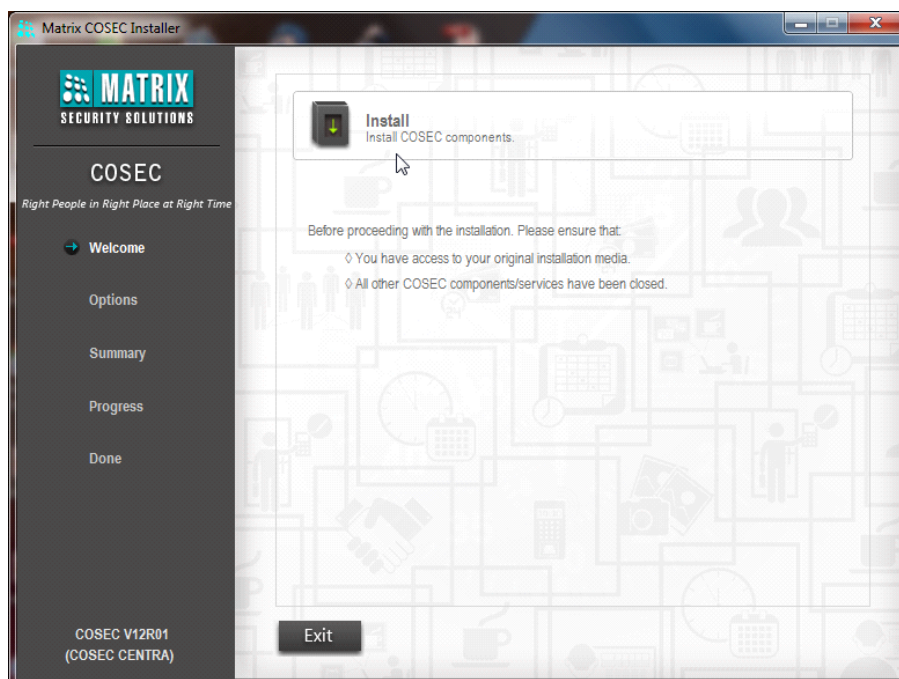
Then go to the path:

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

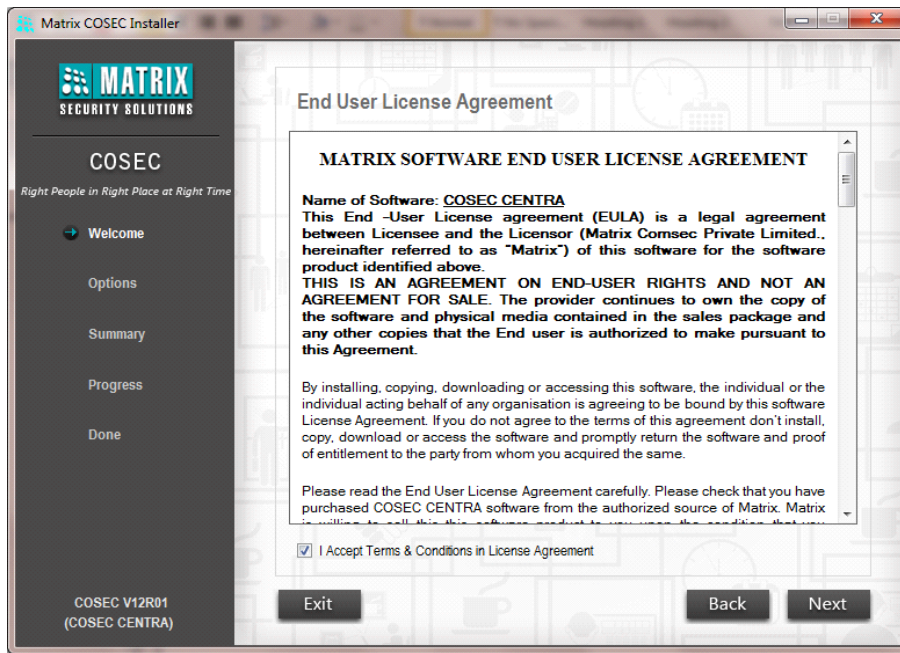
Now you can disable the FIPS Algorithm policy. Then Reset IIS Server and install the setup.

The COSEC CENTRA Admin Service Setup window is shown below.

- To start with the installation procedure, double click on **Setup** file and the following page will appear. Click on the **Install** button.



- Read and accept the COSEC User License Agreement, and then click **Next**.



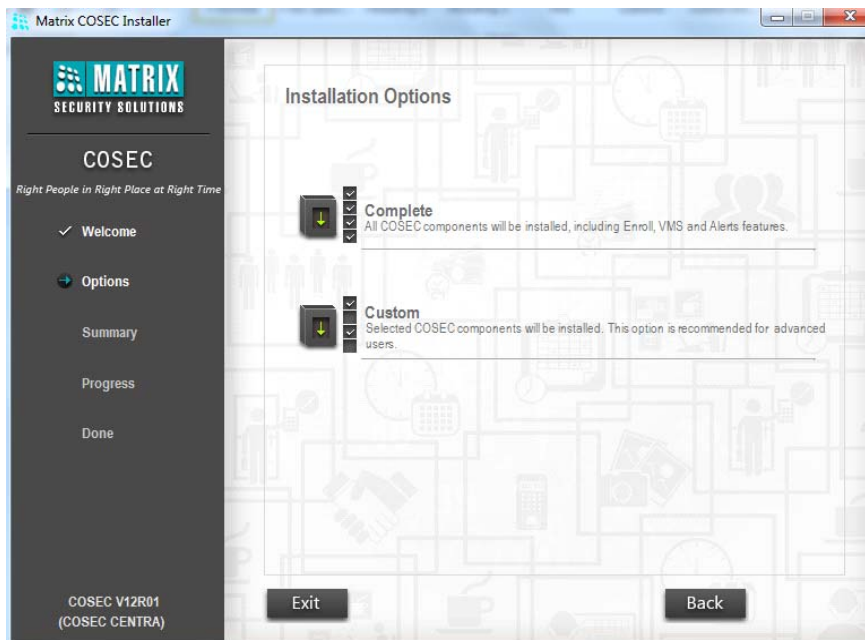
- Select either “**Complete**” or “**Custom**” depending on your preferred type of installation.

Select “Complete” to install all the components of COSEC.

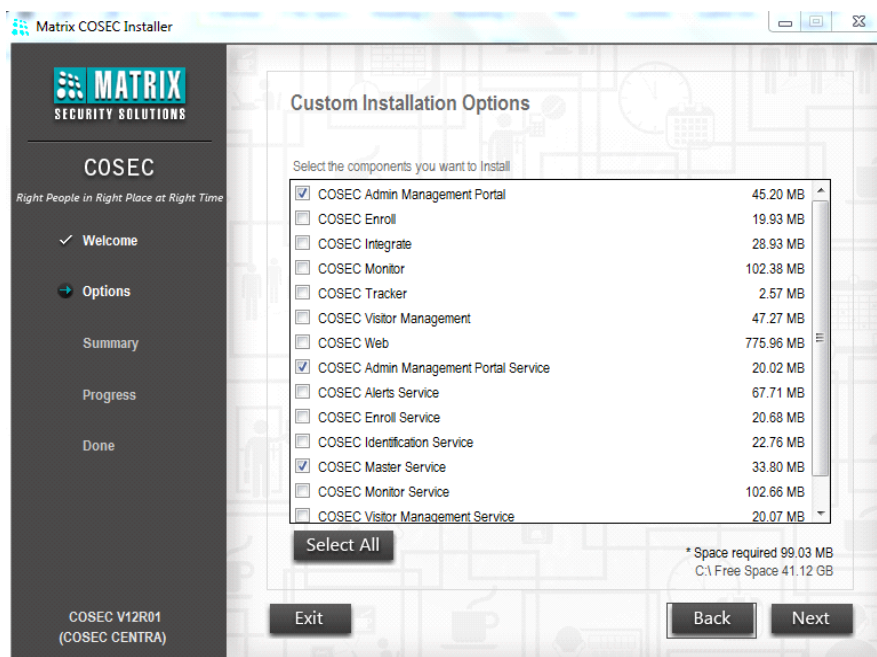
Select “Custom” to install the selected components of COSEC.



*To install only COSEC Admin Management Portal and its services, click on **Custom** installation*



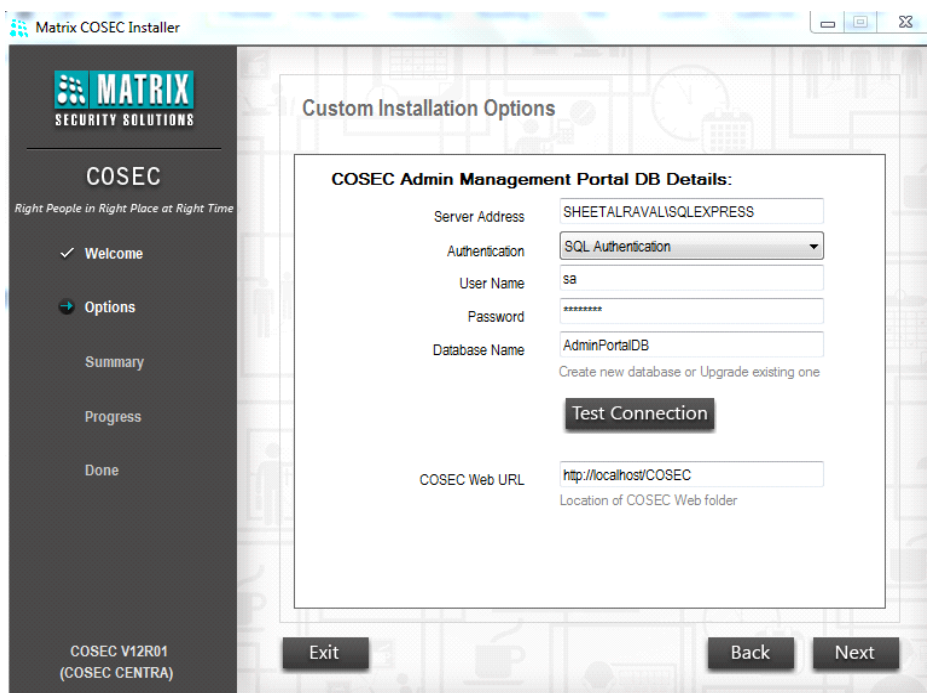
- Select the components you want to install.



- Enter the required details for the Database creation.

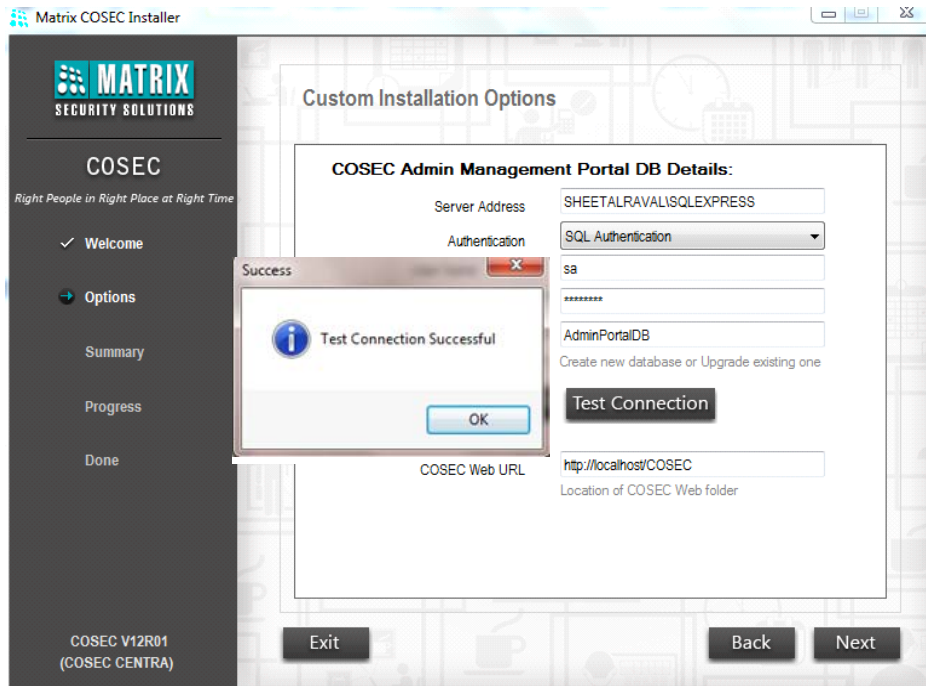


This step in custom installation appears only when “COSEC Master Service” component is selected in the previous step.

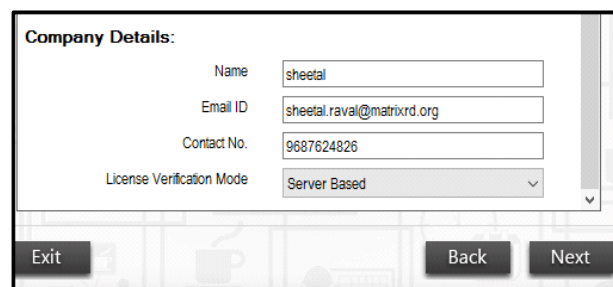
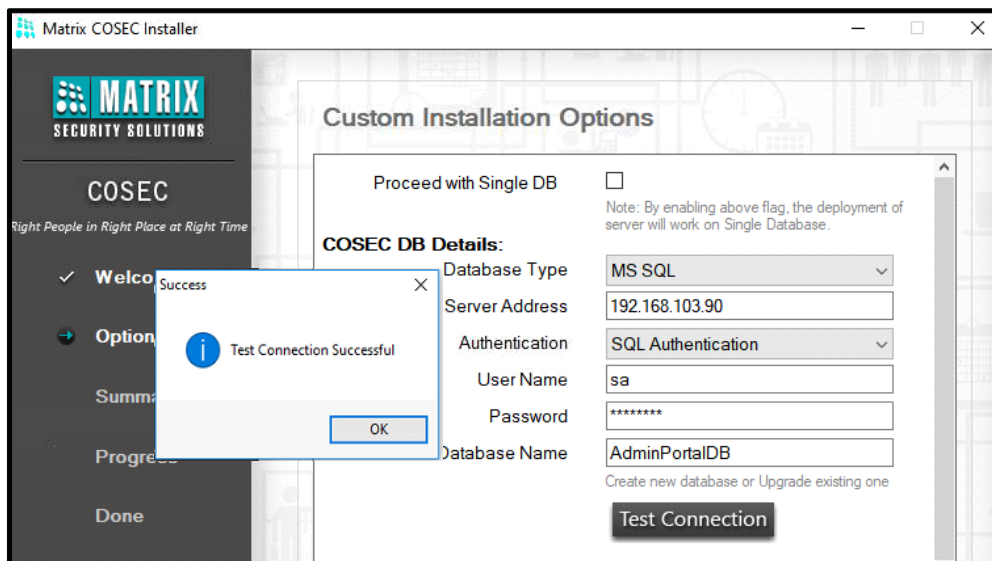


Enter the required details for the Database creation. To know more, refer **COSEC Software Installation Guide**.

- Click on **Test Connection** button to check the connectivity with the Database and then click on **Next** to proceed with the installation.



- Enter the required Company Details. Select the License Verification Mode as **“Server Based”** or **“Device Based”**.



- 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 Panel lite V2 in server mode can be used for Device based license verification.
You must ensure that Vega and Panel lite V2 is in CENTRA connection mode.

Server based License Reading

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

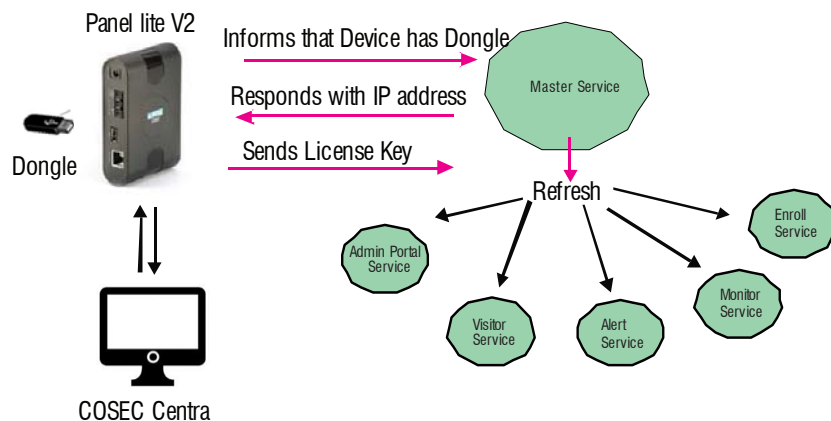
Master service checks for the presence of dongle. If dongle is available, then Master service sends Refresh command to all other services.

Device based License Reading & Writing

In device based licensing Vega direct door or Panel lite V2 can be used. The Company must be device based.

The license dongle is connected to either Vega direct door or Panel lite V2.

- The device (Vega/Panel lite V2) 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.

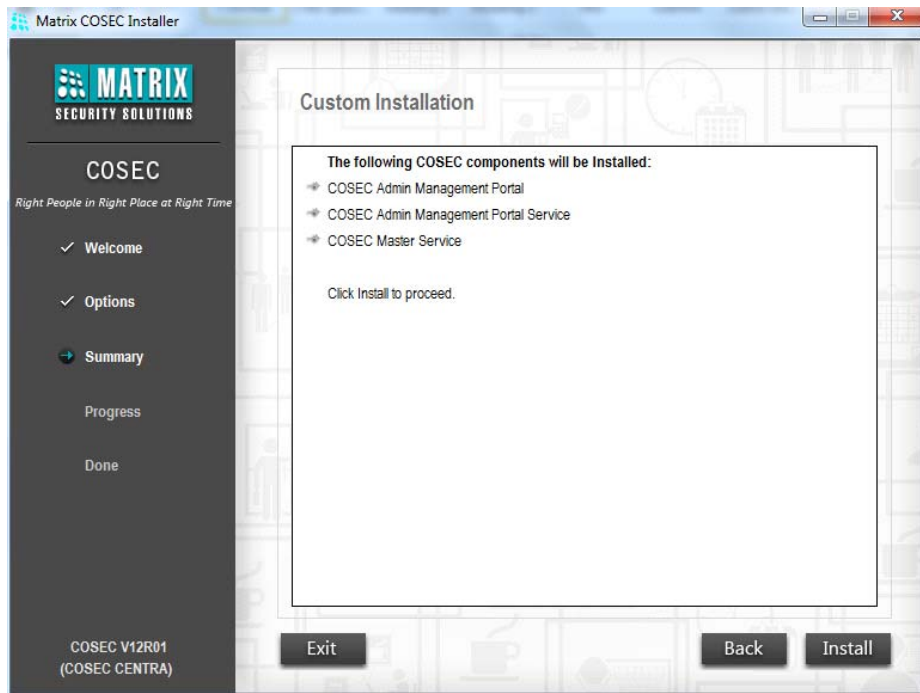


In the Server Settings of Panel lite V2; Enter the URL for COSEC Centra server as the IP address of the computer where Monitor Service is running.

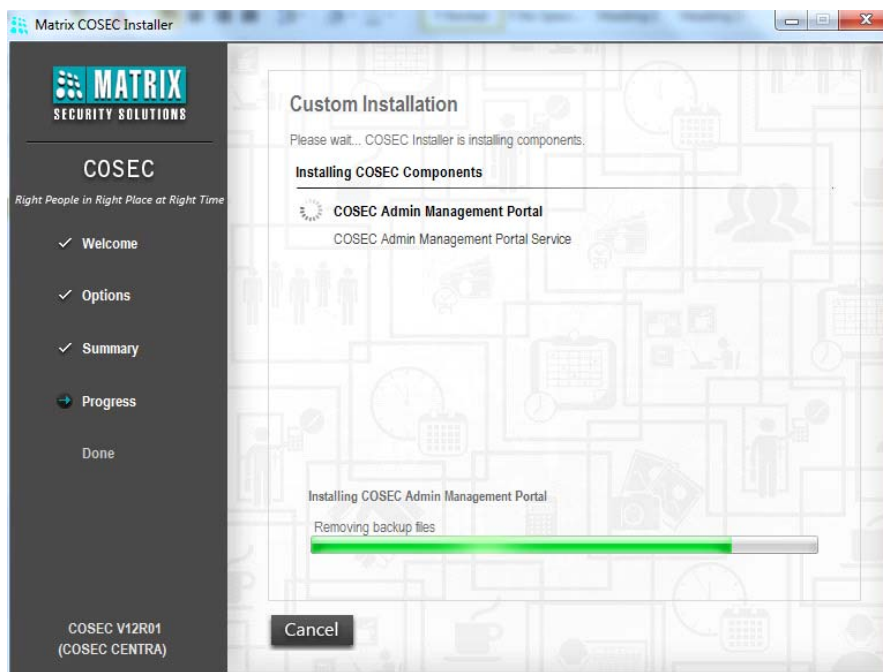
And enter the License Server URL as the IP address of the computer where Master Service is running.

Once the license verification mode is selected and test connection is successful, Click **Next** to proceed with the installation.

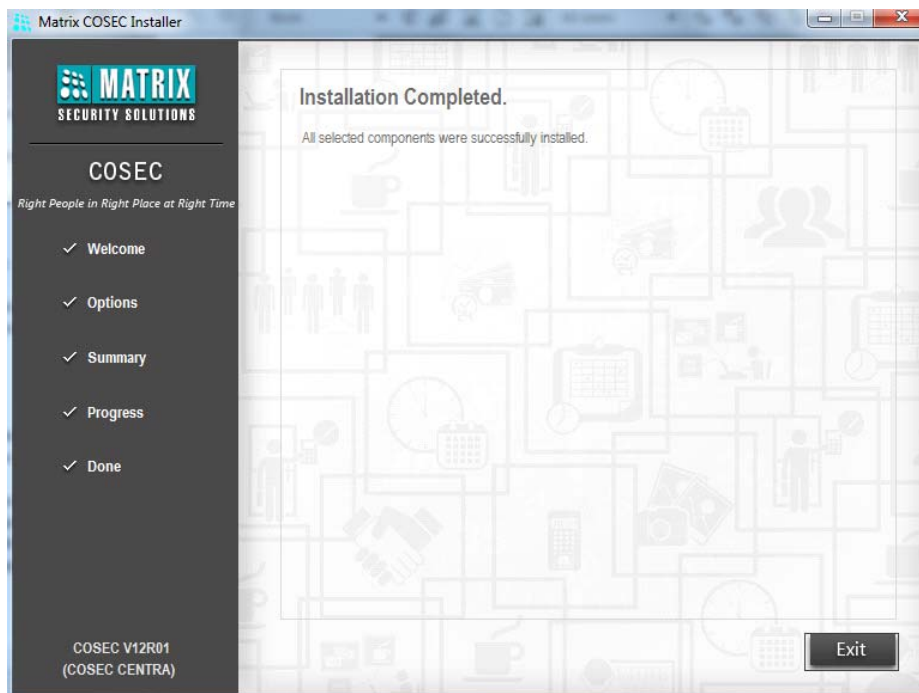
- Click **Install** to confirm the installation of the Admin Management Portal and its Services.





- Wait for the COSEC components to install on your system. The Installation process of each component will be shown.




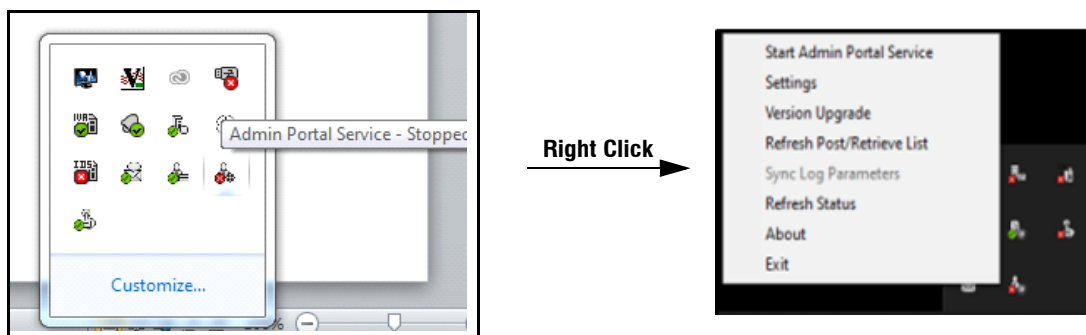
After the successful installation of COSEC Admin Management Portal, "Installation Complete" window will be shown as below. Then close the window by clicking on **Exit** button.



Start the COSEC Admin Service Application by browsing the folder from **All Programs> Matrix > COSEC > COSEC Admin Portal Service.**

When Admin Management Portal Service starts, Admin Portal Service's  icon will be displayed in the System Tray (Notification area) on the right side of the taskbar. When Admin Management Portal Service stops, Admin Portal Service's  icon will be displayed.

Right click on this  icon.



The options displayed are — Start/Stop Admin Portal Service, Settings, Version Upgrade, Refresh Post/Retrieve List, Sync Log Parameters, Refresh Status, About and Exit.

To start this service through the Service Manager Tray, click on **Start Admin Portal Service.**



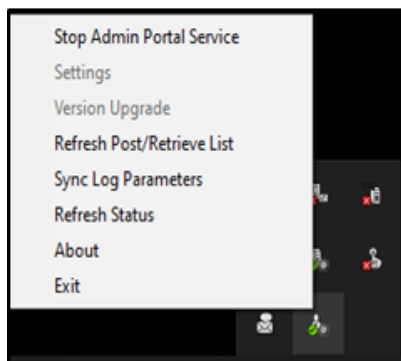
At the time of Admin Management Portal Service start-up, if the service entry is not found in General Settings of Admin Portal, then this service will self-register itself. When Admin Portal Service URL in Admin Portal > System Configuration > General Settings is blank then service will self-register itself.

The screenshot shows the 'System Configuration' window with a left sidebar containing various configuration categories. The 'General Settings' category is selected. The main area displays several configuration fields:

Maintenance Configuration	Master Service URL	net.tcp://192.168.103.155:15001/Me
Security	Master Service Secured URL	net.tcp://192.168.103.155:15010/Me
SMS Configuration	Master Service Device Listening Port Number	15005
Email Configuration	Admin Portal Service URL	net.tcp://192.168.103.155:14001/AC
General Settings	Admin Portal Secured Service URL	net.tcp://192.168.103.155:14010/AC
Multi-Language Configuration	Admin Portal Web Access Port Number	14000
Login Policy	COSEC Web URL (Internal) *	localhost/COSEC
	COSEC Web URL (External)	<Server Address>:< Port>/<Virtual >
	COSEC Visitor URL (Internal) *	localhost/COSECVisitor
	COSEC Visitor URL (External)	<Server Address>:< Port>/<Virtual >
	Portal Time Zone	(UTC+05:30) Chennai, Kolkata, A. v
	Central NTP Server	

At the bottom of the window are 'Save' and 'Cancel' buttons.

- To configure the settings of Admin Management Portal Service, first stop this service by clicking **Stop Admin Portal Service**, and then click **Settings**. To know more, refer [“Settings”](#).



- To upgrade the version of Admin Management Portal Service, click **Version Upgrade**.
- To refresh the post of this service or retrieve the list, click **Refresh Post/Retrieve List**.
- To enable debug logs of the Admin Management Portal Service, click **Sync Log Parameters**. This is used for trouble-shooting by the Technical Support Team.
- 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**.



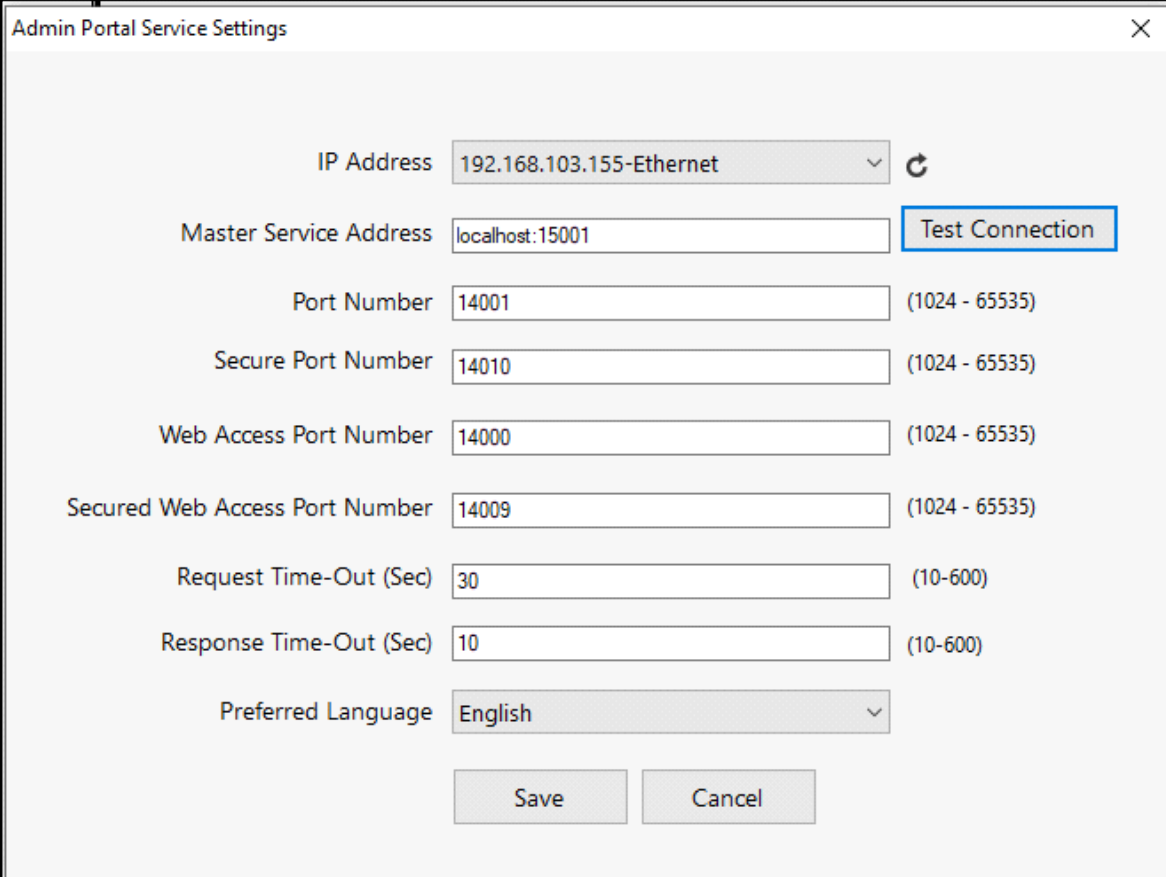
When service is running and Admin database loses connectivity or is unavailable then the service will keep running for 24 hours by default after which it will stop.

The maximum hours allowed for service is given as the configurable tag in Settings.xml file from **C:\Program Files (x86)\Matrix\COSEC Admin Portal Service**.

Settings

To configure the settings of Admin Management Portal Service, first stop this service, then click on **Settings** from the Service Manager Tray option.

Admin Portal Service Settings window appears as shown below.



Configure the following parameters:

- **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 first 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.



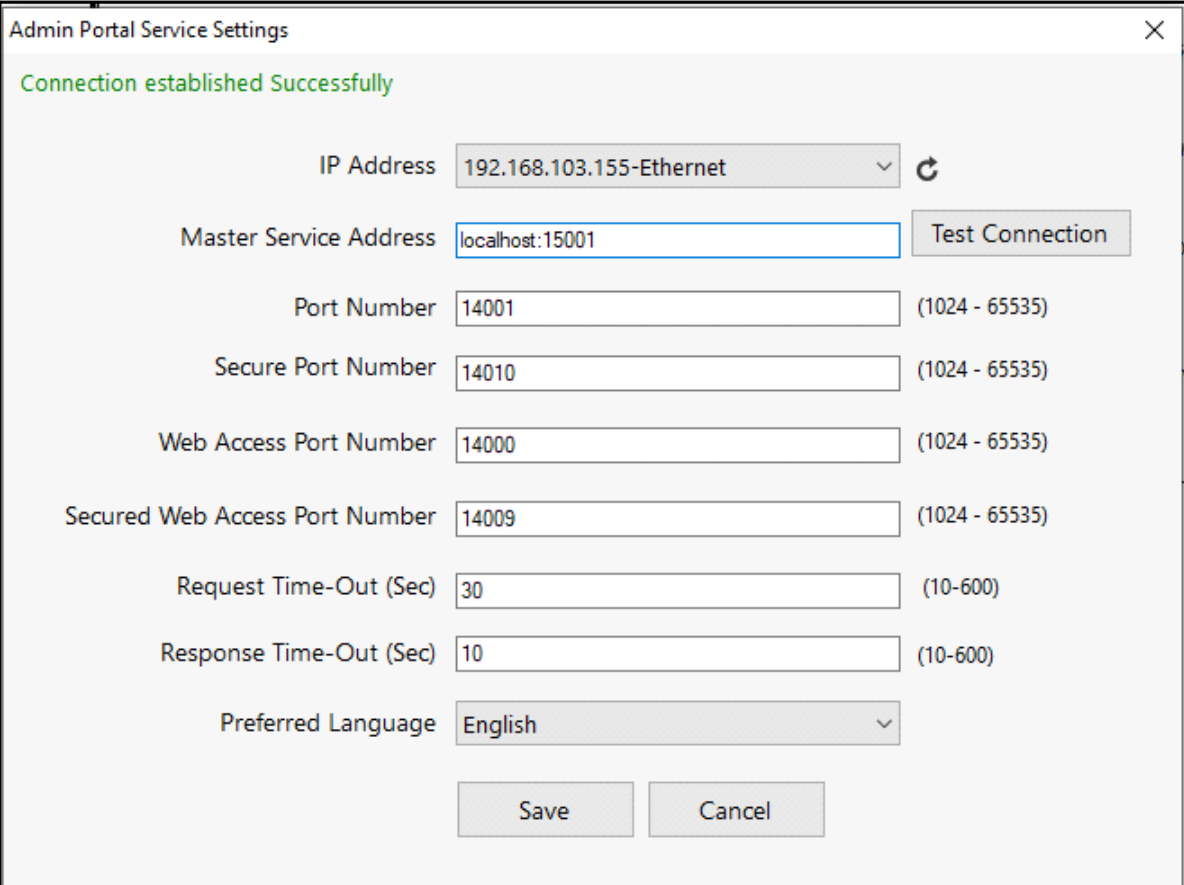
If the PC is assigned a DHCP Addressing scheme, then whenever the IP Address changes, the same will be updated against every service.

Click **Refresh IP List**  to update the list of all network adapters (network connections).

- **Master Service Address:** Enter the IP Address or URL of the Master Service.


On changing or updating the Master Service Address, connection with the Master Service must be tested.

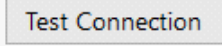
Click Test Connection to test the connection of Admin Management Portal Service with Master service.



Admin Portal Service Settings

Connection established Successfully

IP Address: 192.168.103.155-Ethernet 

Master Service Address: localhost:15001 

Port Number: 14001 (1024 - 65535)

Secure Port Number: 14010 (1024 - 65535)

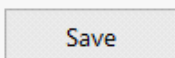
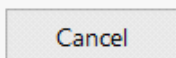
Web Access Port Number: 14000 (1024 - 65535)

Secured Web Access Port Number: 14009 (1024 - 65535)

Request Time-Out (Sec): 30 (10-600)

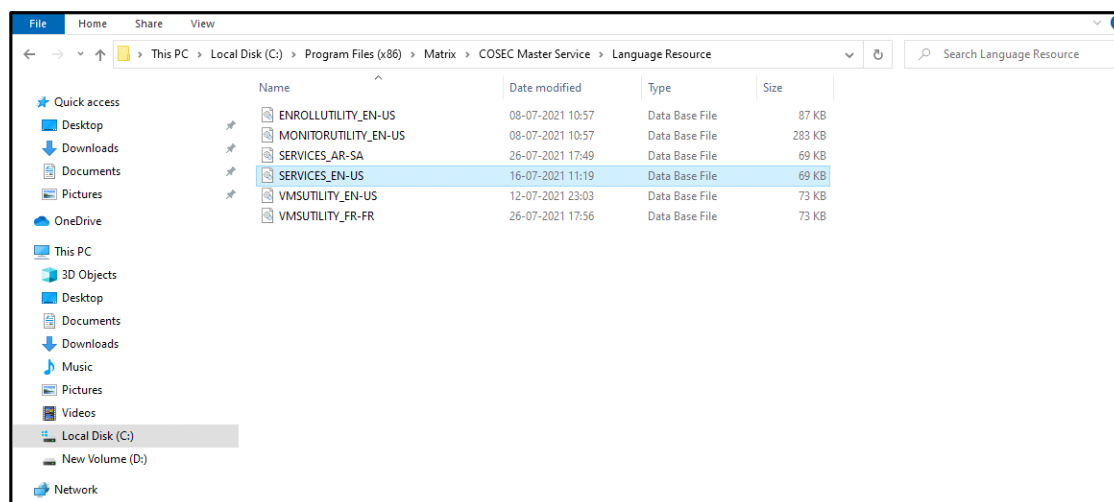
Response Time-Out (Sec): 10 (10-600)

Preferred Language: English

- **Port Number:** Enter the port number at which the Admin Management Portal Service is accessible.
- **Secured Port Number:** Enter the port number at which the Admin Management Portal Service is accessible on the SSL mode.
- **Web Access Port Number:** Enter the port number of the computer at which COSEC Web can access the Admin Management Portal Service.
- **Secured Web Access Port Number:** Enter the port number of the computer at which COSEC Web can access the Admin Management Portal Service on SSL mode.
- **Request Time-Out (Sec):** Enter the request time-out duration in seconds for the Admin Management Portal Service approaching Master Service for connection.
- **Preferred Language:** Select the desired language from the provided dropdown list.

The languages listed here will be as per the language files present in the *C:\Program Files (x86)\Matrix\COSEC Master Service\Language Resource*.



The default language file provided will be of English language.

Name of the English language file for services will be: SERVICES_EN-US.

Name of the language file differs as per the language. For example, name of the Arabic (Saudi Arabia) language file for services will be SERVICES_AR-SA.



If you prefer a different language other than the default language file (i.e. English), you can translate this default language into the desired language with the help of COSEC Multi-Language Utility. To know more, refer to the Multi-Language Utility User Guide.

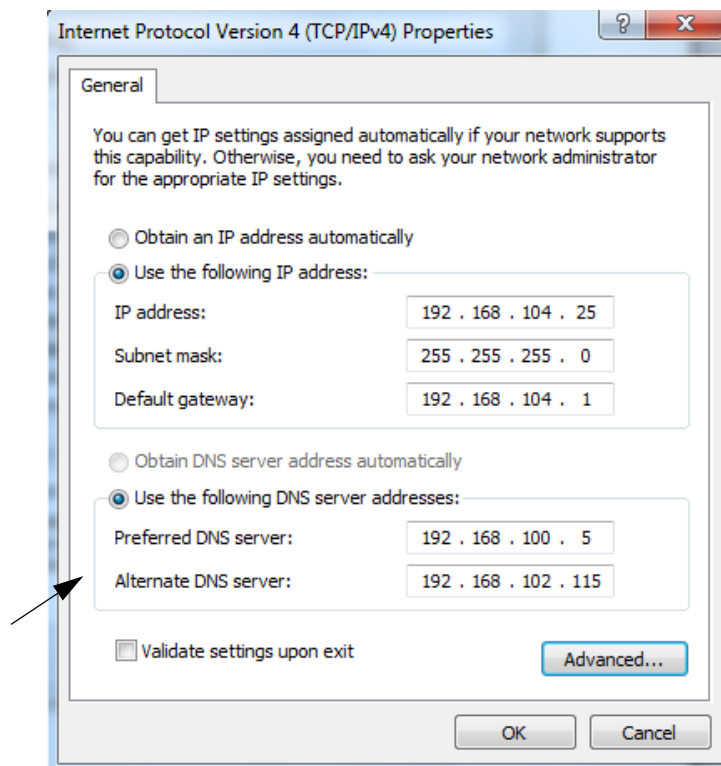
Click **Save** to save the settings.

Getting Started with Admin Portal

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

<http://localhost/cosecadmin>

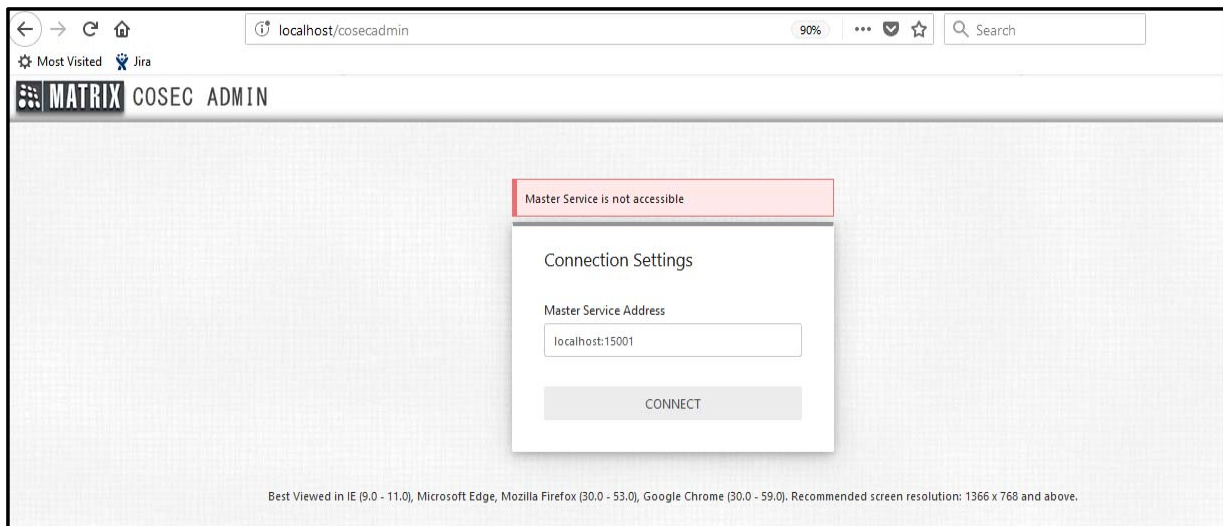
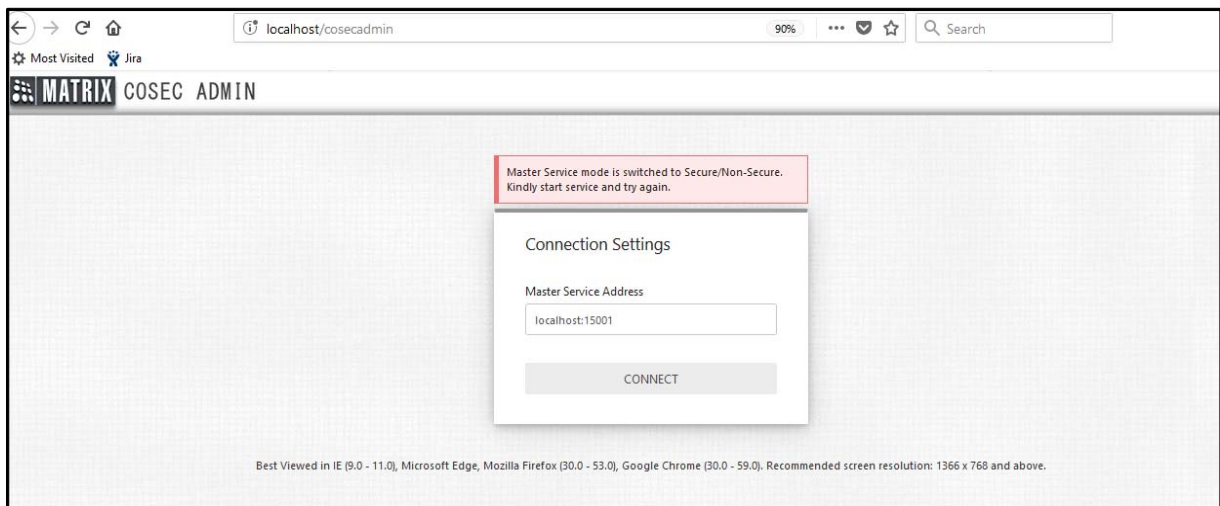
If the network where portal is installed and the PC from where the Portal is being used are in different network then make sure that “Alternate DNS server” is configured with the IP address where you have installed the Portal.



LOGIN

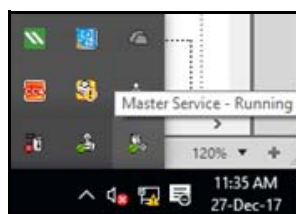
Once the COSEC CENTRA setup is installed and the services are started; login to Admin Portal by typing **localhost/cosecadmin** in the browser.

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 to establish connection with Admin Portal Web. You can start the Master service from Service tray as shown below.



The Login page appears as shown below. Enter the Login ID and Password. When you are login for the first time, you will have to set the password.



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

localhost/COSECADMIN/ 90% Search

MATRIX COSEC ADMIN

User ID, Email or Mobile

Password OTP

Password

☐ Remember Me [Forgot Password?](#)

LOGIN

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.

Enter the default login ID i.e. **“sa** and the default password as blank. Click **Login** button which will redirect to Set Password page from where you can set the password as shown below.

sa

Password OTP

Password

☐ Remember Me [Forgot Password?](#)

LOGIN

Set Password

New Password

Confirm Password

Email ID

Contact

SET

CANCEL

Set Password

Password

Confirm Password

Email ID

Contact

SET

CANCEL

Enter the **New Password** and re-enter it to confirm. Enter the **Email ID** and **Contact** number through which you can retrieve your account when you forget your password. The entered Email ID and Contact will also appear on System Accounts page. Also the OTP can be received on this Email ID and Contact number.

Then click **Set** to save the details.

Then Enter the **Login ID** as **User ID/Mobile Number/Email ID** to login into Admin Portal using the newly created password. You can login using OTP once Email/SMS 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**.

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. [See “Forgot Password” on page 24.](#)

You must ensure that the Login ID being used has the respective correct icon. [See “Icon of Login ID” on page 23.](#)



If you change the password then the cookie will still have older password and same will be loaded by default on login page. To update the password; browser cookies must be cleared. And again “Remember me” can be enabled.

Password or OTP

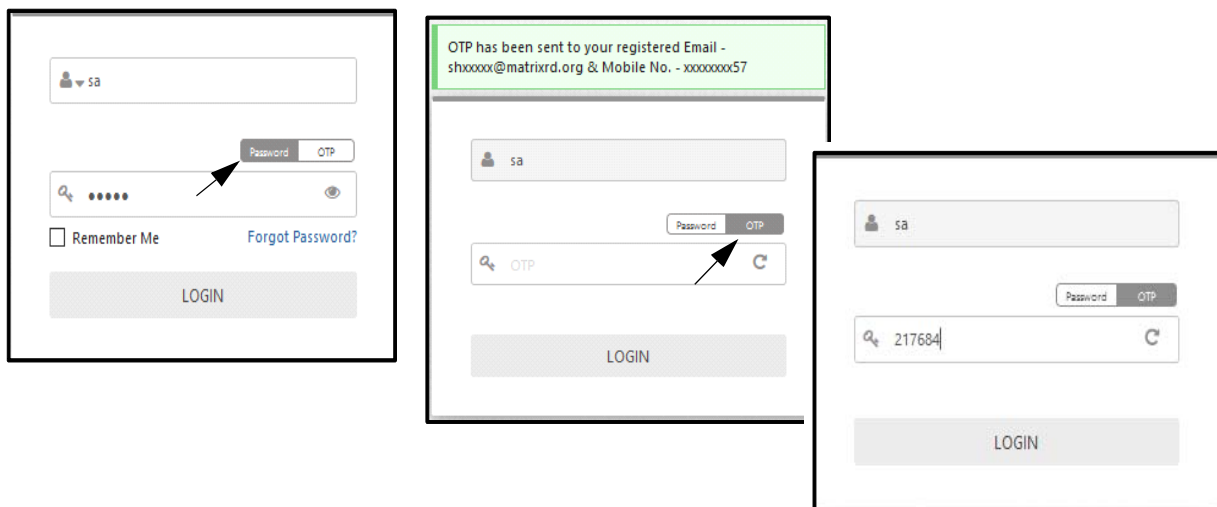
In this authentication mode, you can enter either Password of login ID or OTP for accessing the Admin Portal.

User ID with Password or OTP

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

You can also login using OTP by clicking OTP button. The OTP is sent to the contact details (Email ID and contact number as available in System Accounts page) of login user. Enter the OTP and click **Login** button to login into Admin Portal.

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



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 Admin Portal.

The first screenshot shows the login form with the email 'sheetal.raval@matrixrd.org' and a password field. The second screenshot shows a message 'OTP has been sent to your registered Email - shxxxxx@matrixrd.org & Mobile No. - xxxxxxxx57' and the login form with the OTP field. The third screenshot shows the login form with the OTP '874444' entered.

Mobile Number with Password or OTP

You can also login with your **Mobile number**. Then enter the login password or OTP which is sent to the registered contact details. Then click Login to login into Admin Portal.

The first screenshot shows the login form with the mobile number '9586243157' and a password field. The second screenshot shows a message 'OTP has been sent to your registered Email - shxxxxx@matrixrd.org & Mobile No. - xxxxxxxx57' and the login form with the OTP field. The third screenshot shows the login form with the OTP '568128' entered.

Password Then OTP

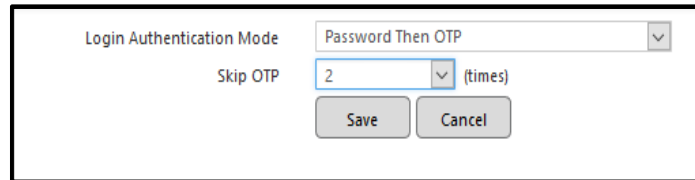
In this authentication you have to enter both Password and then OTP for accessing Admin Portal.

User ID with Password Then OTP

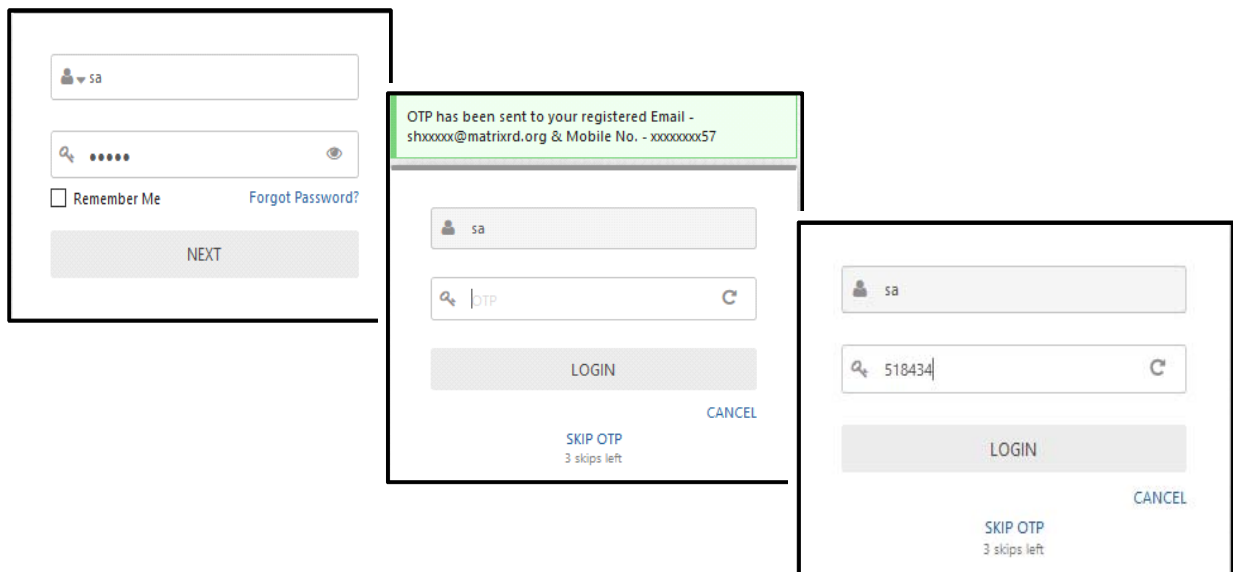
Enter the User ID of login user. Then enter the password and click **Next** button.

Now you will have to enter the OTP which is sent to the contact details (Email ID and contact number as available in System Accounts page) of login user. After entering OTP click **Login**, to login into Admin Portal. 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 Admin Portal without requiring OTP. The number of times OTP can be skipped is configured in Login policy of System Configuration.



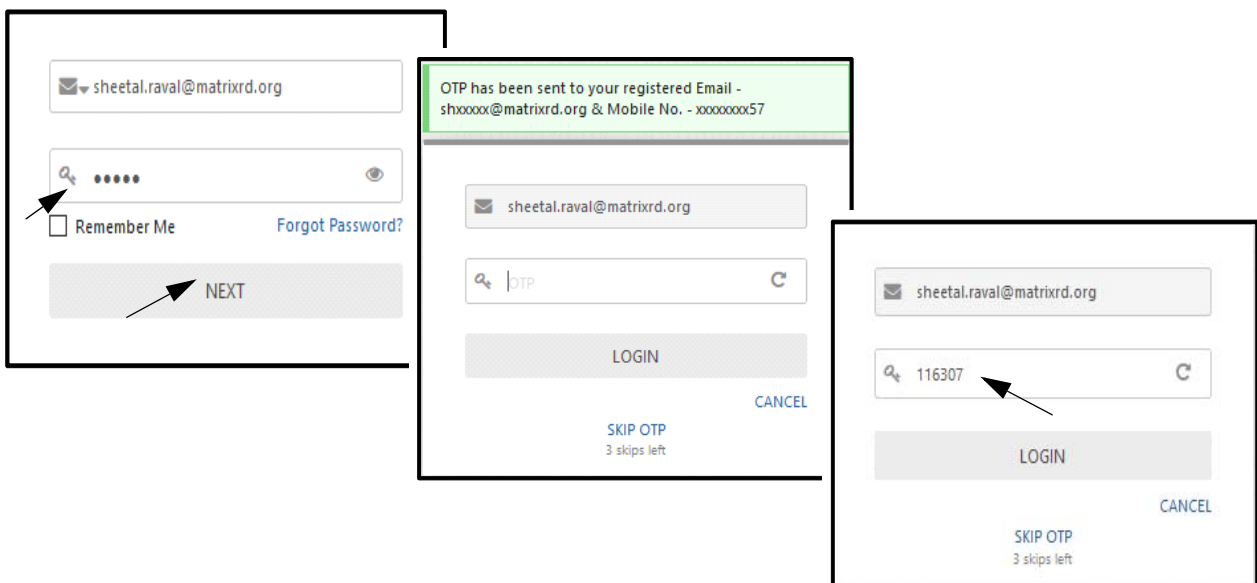
Eg: If Skip OTP is set as 2, the user can click on SKIP OTP for 2 times. When later if SKIP OTP in Login policy is changed to 5; then for 3 more times user can use SKIP OTP.



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 of login user. Then enter the OTP and click **Login** button to login to Admin Portal. You can also skip entering OTP by clicking on **SKIP OTP** link.



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 contact details of login user. Then enter the OTP and click **Login** button to login to Admin Portal. You can also skip entering OTP by clicking on **SKIP OTP** link.

The first screenshot shows the initial login screen with a mobile number field (9586243157), a password field (masked with dots), a 'Remember Me' checkbox, a 'Forgot Password?' link, and a 'NEXT' button.

The second screenshot shows a green notification banner stating 'OTP has been sent to your registered Email - shxxxxx@matrixrd.org & Mobile No. - xxxxxxxx57'. Below the banner, the mobile number field is pre-filled with 9586243157, and there is an OTP field. A 'LOGIN' button is present, along with a 'SKIP OTP' link (3 skips left) and a 'CANCEL' link.

The third screenshot shows the mobile number field (9586243157) and the OTP field (725570). The 'LOGIN' button is highlighted, and the 'SKIP OTP' link (3 skips left) and 'CANCEL' link are also visible.

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.

The first screenshot shows the login screen with a user ID field (SR), a password field (masked with dots), a 'Remember Me' checkbox, a 'Forgot Password?' link, and a 'LOGIN' button. An arrow points to the user ID field.

The second screenshot shows the login screen with an email ID field (sheetal.raval@matrixrd.org), a password field (masked with dots), a 'Remember Me' checkbox, a 'Forgot Password?' link, and a 'LOGIN' button. An arrow points to the email ID field.

The third screenshot shows the login screen with a mobile number field (9586243157), a password field (masked with dots), a 'Remember Me' checkbox, a 'Forgot Password?' link, and a 'LOGIN' button. An arrow points to the mobile number field.

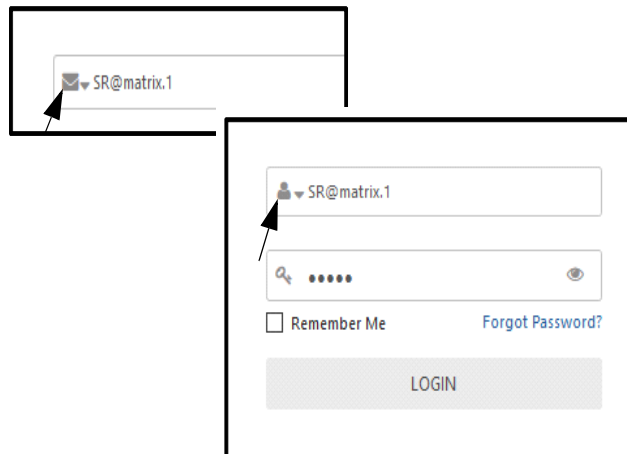




Icon of Login ID

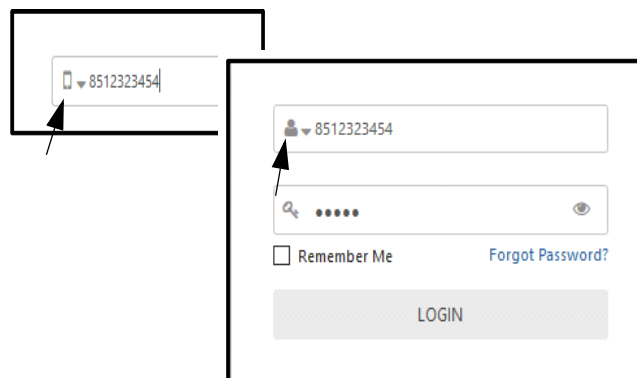
Suppose you are logging into COSEC with your User ID  which is similar to Email ID  configuration

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.



Forgot Password

If you forget the login password, then you can click on Forgot Password to get new one time password.

Forgot Password

A 6-digit OTP will be sent to your registered Mobile number and Email ID.

SEND

CANCEL

Enter 6-digit OTP

880616

VERIFY

CANCEL

Set Password

New Password

Confirm Password

SET

CANCEL

Now click **Send** button to get the password on registered Email ID and/or registered mobile number of the login user. Then Enter the 6-digit OTP and click **Verify**. After verification you can set your new password from Set Password window. Then you can login to Admin Portal using your login ID and new password.



To get the OTP on SMS and Email, you have to do SMS Configuration and Email Configuration from System Configuration.

The Email ID and Contact number of the user is registered on System Accounts page.

For eg: SA user will get OTP on Email ID: sheetal.raval@matrixrd.org and Contact number: 9384526175

[See "SMS Configuration" on page 60.](#)

[See "Email Configuration" on page 65.](#)

Now the Admin Management Portal home page appears as shown below:

The screenshot shows the MATRIX COSEC ADMIN interface. The left sidebar contains a menu with options: Company Configuration, Profile (selected), License and Services, Monitor Configuration, COSEC Services, and Manage Database. The main content area is titled 'Profile' and contains the following fields:

- ID:
- Name:
- Active: ☒
- Time Zone:
- License Verification Mode:
- Contact Details:
- Address Details:
- Database Configuration:

On the right side, there is a table with the following data:

ID	Name	Status
1	sheetal	Active

Company here, is the client as well as the end-user who will be using COSEC for Access Control/Time and Attendance solutions. Profile page allows the Admin portal to view/modify/ the Company details.

The COSEC License assignment as per the requirement of company is done from the License section of the Company Configuration. The license key can also be updated by providing enhanced features to the Company.

The assignment of services such as Alert Service, Enroll Service, Visitor Service, Monitor Service and Identification Service is also done from Services section of Company Configuration. COSEC Devices connect to the assigned monitor service of the company which is used for the Time and Attendance functionality and Access Control solution.

Click on the links for various configurations:

[“Profile”](#)

[“License and Services”](#)

[“Monitor Configuration”](#)

Profile

The Company Configuration Profile page allows the user to view or modify the company details. Company are the clients who use COSEC web application. Once the Premise based setup for COSEC is installed, Profile will be created automatically with the configurations as defined during the installation of setup.

You can configure the following on this page:

- Modify the name and activate the user to access COSEC.
- Select the License Verification Mode for the user.
- Reset the GDPR Process.

Configure Time Settings, Contact Details, Address Details and Database configuration related details.

ID	Name	Status
1	Kunal	Active

Select the user from the right panel to modify the following details on the **Profile** page:

ID: Displays the ID of the selected user in the COSEC Admin Portal.

Name: Displays the name of the user profile in the COSEC Admin portal. You may modify it if you desire.

Active: Enabling the Active check box will activate the client's profile access to COSEC.

License Verification Mode: There are two modes for License Verification — Server Based and Device Based.

- **Server Based:** If the licensing mode is set to Server based, then dongle must be inserted in the PC where Master service is installed.
- **Device Based:** If the licensing mode is set to Device Based, then license key shall be fetched from the dongle connected to the device.



Only Vega Direct Door and Panel lite V2 in server mode can be used for Device based license verification. You must ensure that Vega and Panel lite V2 is in CENTRA connection mode.

Once dongle is connected to the device (Vega or Panel lite V2); 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.

Reset Personal Data Protection Process Flag: General Data Protection Regulation (GDPR) aims in providing safety and privacy to users data. They limit the access to the users personal data. Enabling GDPR will result in data masking and encryption. To know more about GDPR refer to the COSEC System Manual.

Reset Personal Data Protection Process Flag button is applicable if you have enabled/disabled **General Data Protection Regulation (GDPR)** in COSEC Web > Admin > System Configuration > Global Policy > Basic.

Click **Reset** if you desire resetting the GDPR process in case of failure or when the GDPR process remains in in-progress state for a prolonged period.



*For proper functioning of **Reset Personal Data Protection Process Flag**, ensure that the **Master Service** and **Admin Portal Service** is running successfully.*

*Make sure you save all the previous changes, if done in other pages before you click the **Reset** button.*

The Reset functionality is applicable in the below mentioned cases:

- If the system has derived failure in the GDPR process/ GDPR reversal process.

In such cases, the COSEC Web login screen displays the error message “Processing Failed. Kindly contact Administrator”

OR

- When the GDPR process remains in in-progress state for a prolonged period.

In such cases, the COSEC Web login screen displays the error message “Admin has temporarily stopped the access” will be displayed.

In such cases, you can click the **Reset** button, the system will verify if the database is valid or not.



Before pressing the Reset button, make sure you have manually restored a valid database (this database may be the last database backup taken either before GDPR was enabled or after GDPR was enabled) in your Database Server.

- If the database is valid, you will be able to re-login into the COSEC Web.
- But if the database is not valid, an error message “Database restored is not valid. Kindly restore a valid database.” will be displayed.



*The **Reset** functionality will only work with a valid database.*

Make sure you reset the IIS and restart all the Services (applicable for COSEC CENTRA) and Utilities after the Reset Process.

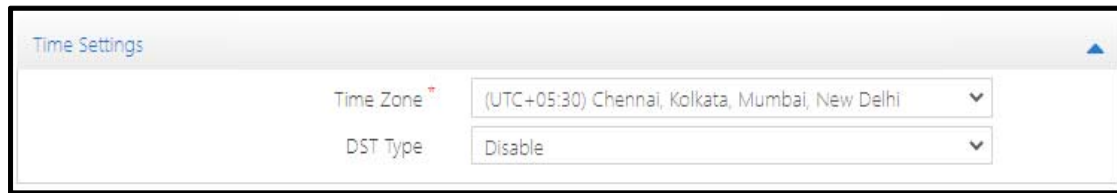
*The **Reset** functionality will reset the GDPR process status to its initial stage. If you desire, you may restart the GDPR process again.*

Select the respective link for further configuration:

- [“Time Settings”](#)
- [“Contact Details”](#)
- [“Address Details”](#)
- [“Database Configuration”](#)

Time Settings

Click on the **Time Settings** collapsible panel to configure the time as per the company location.



The screenshot shows a 'Time Settings' panel with two dropdown menus. The 'Time Zone' dropdown is set to '(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi'. The 'DST Type' dropdown is set to 'Disable'.

Configure the following parameters:

Time Zone: Select the desired time zone from the drop down list as per the location of your company.

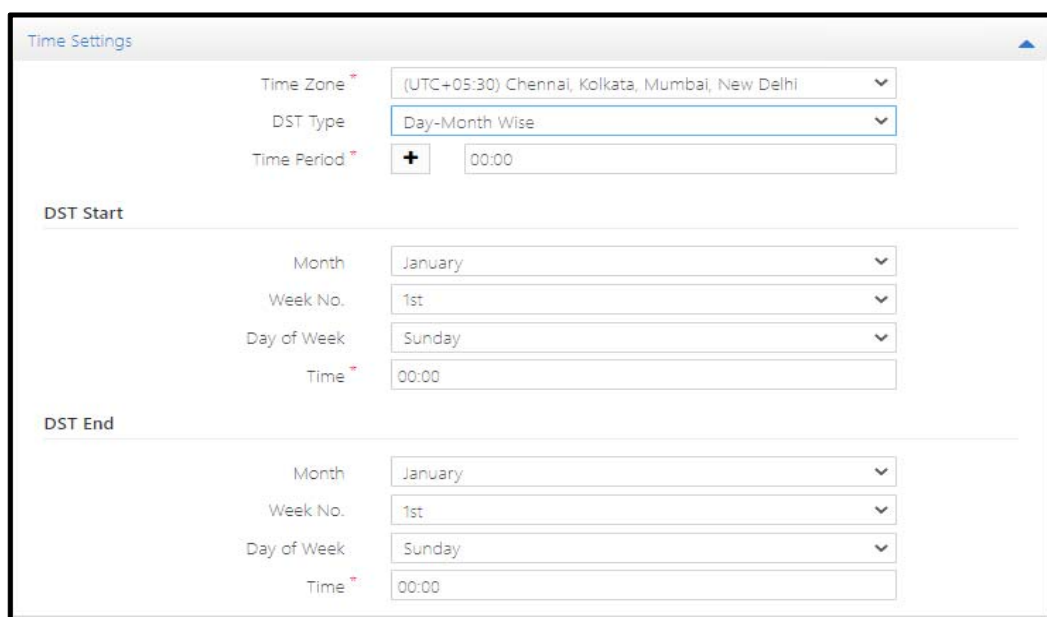
DST Type: Select the desired type of DST from the drop down list — **Disable**, **Day- Month Wise**, or **Date-Month Wise**.



The screenshot shows the 'DST Type' dropdown menu with three options: 'Disable', 'Day-Month Wise', and 'Date-Month Wise'. The 'Date-Month Wise' option is currently selected and highlighted in blue.

Time Period: Enter the time period (HH:MM) the system should add in the DST Start Time (if you select the plus sign) or the system should minus from the DST Start Time (if you select the minus sign). Default: 00:00.

- Select **Disable**, if you do not wish to apply DST.
- Select **Day-Month Wise** type DST, if the DST in your country starts and ends on a particular day of the month. For example, if DST starts on the Second Sunday of March and ends on the First Sunday of October.



The screenshot shows the 'Time Settings' panel with the 'DST Type' set to 'Day-Month Wise'. The 'Time Period' is set to '+ 00:00'. Below this, there are two sections: 'DST Start' and 'DST End'. Each section has four dropdown menus: 'Month' (January), 'Week No.' (1st), 'Day of Week' (Sunday), and 'Time' (00:00).

- Configure the **DST Start** and **DST End** time.

DST Start

- Select the **Month** when DST begins: January to December.
- Select the **Week No.** when DST begins: 1st Week, 2nd Week, 3rd Week, 4th Week, 5th Week.
- Select the **Day** of the week when DST begins: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.
- Set the **Time** when you want DST to begin in 24 hours format

DST End

- Select the **Month** when DST ends: January to December.
- Select the **Week No.** when DST ends: 1st Week, 2nd Week, 3rd Week, 4th Week, 5th Week.
- Select the **Day** of the week when DST ends: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.
- Set the **Time** when you want DST to end in 24 hours format.
- Select **Date-Month Wise** type DST, if the DST in your country starts and ends on a particular date of the month. For example, if DST starts on October 12 and ends on March 15.

Time Settings

Time Zone * (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

DST Type Date-Month Wise

Time Period * + 00:00

DST Start

Month January

Date 1

Time * 00:00

DST End

Month January

Date 1

Time * 00:00

- Configure the **DST Start** and **DST End** time.

DST Start

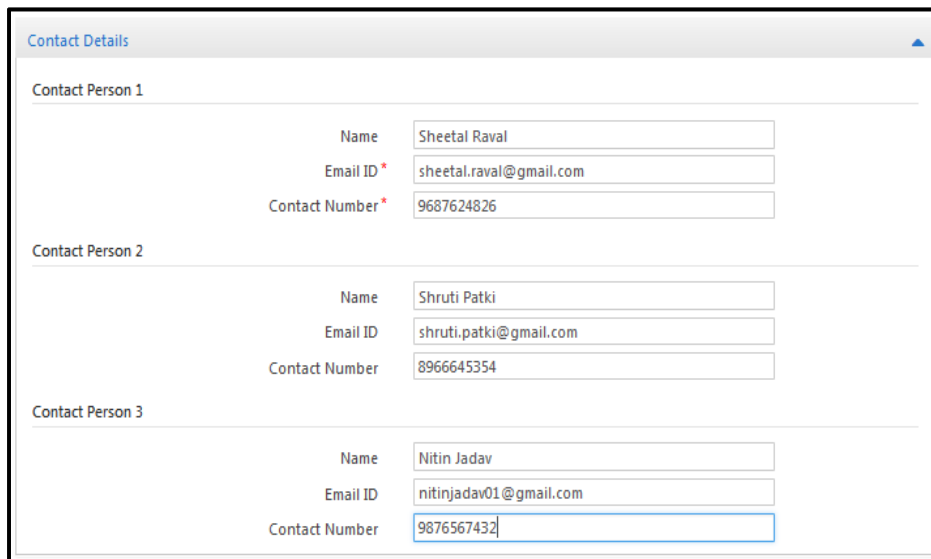
- Select the **Month** when DST begins — January to December.
- Select the **Date** on which DST begins — 1 to 31.
- Set the **Time** when DST begins in 24 hours format.

DST End

- Select the **Month** when DST ends — January to December.
- Select the **Date** on which DST ends — 1 to 31.
- Set the **Time** when DST ends in 24 hours format.

Contact Details

Click the **Contact Details** collapsible panel. You can configure contact details of 3 persons on Company side.



The screenshot shows a web form titled "Contact Details" with a blue header bar. It contains three sections for contact persons, each with input fields for Name, Email ID, and Contact Number. The first section is for "Contact Person 1" with values: Name: Sheetal Raval, Email ID: sheetal.raval@gmail.com, Contact Number: 9687624826. The second section is for "Contact Person 2" with values: Name: Shruti Patki, Email ID: shruti.patki@gmail.com, Contact Number: 8966645354. The third section is for "Contact Person 3" with values: Name: Nitin Jadav, Email ID: nitinjadav01@gmail.com, Contact Number: 9876567432. The Contact Number field for the third person is highlighted with a blue border.

Contact Person	Name	Email ID *	Contact Number *
Contact Person 1	Sheetal Raval	sheetal.raval@gmail.com	9687624826
Contact Person 2	Shruti Patki	shruti.patki@gmail.com	8966645354
Contact Person 3	Nitin Jadav	nitinjadav01@gmail.com	9876567432

Name: Enter the name of the Person in-charge on Company side.

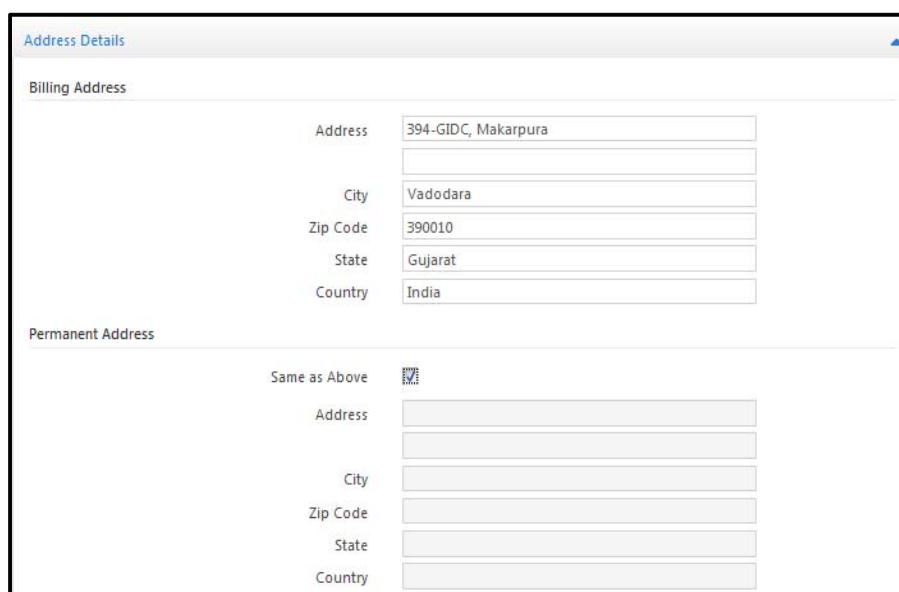
Email ID: Enter the Email ID of 1st contact person to which the Web URL and Company user name will be sent. You can enter Email ID of other 2 contacts as well. This Email-ID will be used when the Company (SA user) forgets password.

Eg: sheetal.raval@matrixrd.org

Contact Number: Enter the Contact number of the Company. This Contact Number will be used when the user (SA user) forgets password.

Address Details

Click on Address Details collapsible panel to configure Address Details on the Company side.



The screenshot shows a web form titled "Address Details" with a blue header bar. It contains two sections: "Billing Address" and "Permanent Address". The "Billing Address" section has input fields for Address (394-GIDC, Makarpura), City (Vadodara), Zip Code (390010), State (Gujarat), and Country (India). The "Permanent Address" section has a "Same as Above" checkbox (checked) and input fields for Address, City, Zip Code, State, and Country, all of which are currently empty.

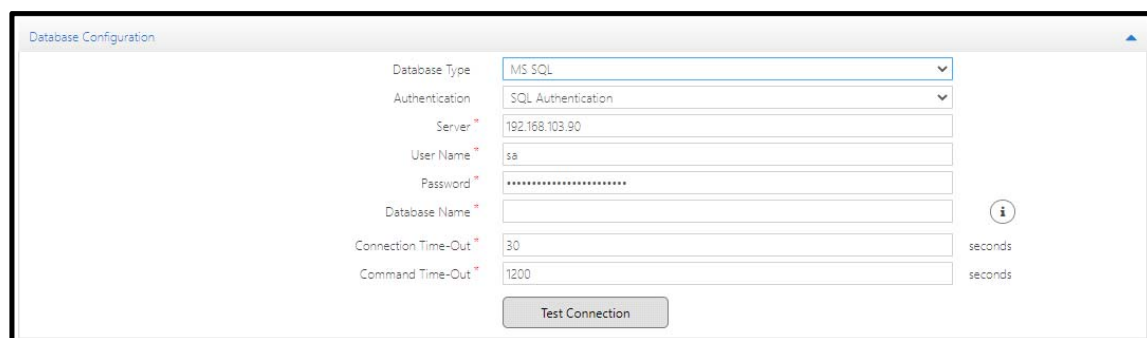
Section	Field	Value
Billing Address	Address	394-GIDC, Makarpura
	City	Vadodara
	Zip Code	390010
	State	Gujarat
	Country	India
Permanent Address	Same as Above	<input checked="" type="checkbox"/>
	Address	
	City	
	Zip Code	
	State	
	Country	

Billing Address: Enter the Address of the Company at which billing is to be done.

Permanent Address: If the permanent address is same as billing address, then select Same as Above or else enter the permanent address of the Company.

Database Configuration

Database Configuration for MS SQL

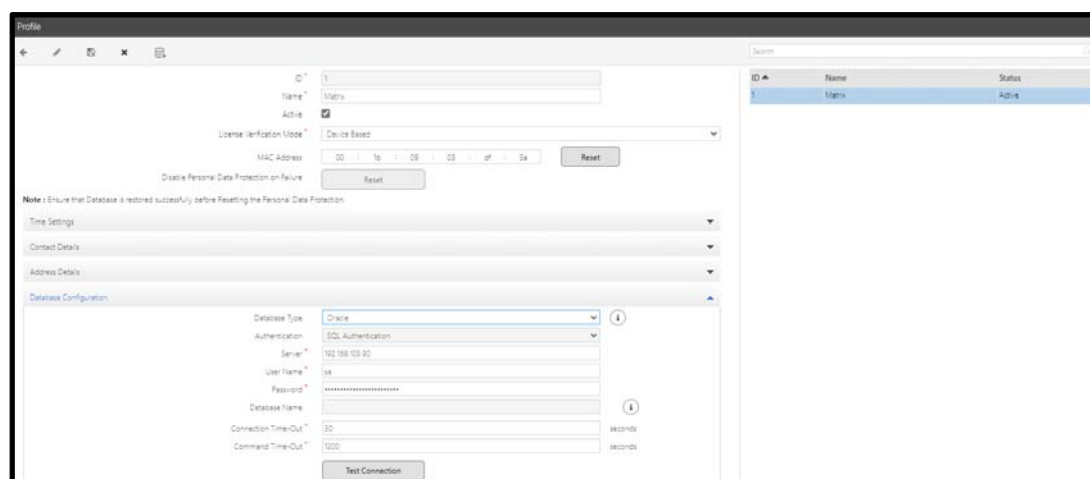


The screenshot shows a 'Database Configuration' window. It contains the following fields and values:

- Database Type: MS SQL (dropdown)
- Authentication: SQL Authentication (dropdown)
- Server: 192.168.103.90
- User Name: sa
- Password: (masked with asterisks)
- Database Name: (empty)
- Connection Time-Out: 30 seconds
- Command Time-Out: 1200 seconds

A 'Test Connection' button is located at the bottom center. An information icon (i) is on the right side.

Database Configuration for Oracle



The screenshot shows a 'Profile' window with a 'Database Configuration' section. It contains the following fields and values:

- Database Type: Oracle (dropdown)
- Authentication: SQL Authentication (dropdown)
- Server: 192.168.103.90
- User Name: sa
- Password: (masked with asterisks)
- Database Name: (empty)
- Connection Time-Out: 30 seconds
- Command Time-Out: 1200 seconds

A 'Test Connection' button is located at the bottom center. An information icon (i) is on the right side. The window also shows other sections like 'Time Settings', 'Contact Details', and 'Address Details' on the left, and a table on the right.

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

Authentication: Select the authentication type as SQL Authentication or Windows Authentication for MS SQL database.

Server: Enter the server address from where the COSEC database is to be accessed.

- For **SQL authentication**, specify the server where the database is to be created or accessed.
Eg: 192.168.104.12\\sqlcxpress or localhost\\sqlcxpress
- 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**, specify the server where the database is to be created or accessed. The Username and Password will be disabled in this mode.

For **Oracle database**, Enter the **Server** address where Oracle database is installed. Eg: 192.168.104.12 or localhost.

- **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 the corresponding Access rights.

Database Name: Enter a name for the database server to be created for MS SQL.



*Database Name will be auto-filled if **Proceed with Single DB** checkbox is selected during installation. Hence, same database will be created for Admin and COSEC.*

*You can change the name of the database here, by entering the desired name in **Database Name**. By doing so two databases will be created.*

Connection Time-Out: Enter the duration in seconds for database connection time out.

Command Time-Out: Enter the duration in seconds for session time out.

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

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



Whenever new database is created; then the upgrade request is sent to Admin Portal Service. So Admin Portal Service must be running to upgrade the database.

License and Services

License and Services allows management of company's license and services. From here the management can modify/reassign License Key and COSEC Services to the Company. You can also activate/deactivate desired modules from Current License Profile. In COSEC Web such Modules will be visible or hidden as per your action.

For details refer [“License Key”](#), [“Services”](#) and [“Current License Profile”](#).

The screenshot shows the 'License and Services' management page. It includes fields for Company (1), Matrix, and Database Name (test). The 'License Key' section shows the current key and a field for a new key with 'Update' and 'Cancel' buttons. The 'Services' section lists various services like Alert Service, Enroll Service, Visitor Service, Identification Service, and Monitor Service, each with a value and a dropdown menu. A table at the bottom shows the 'Monitor Service' with ID 3 and Name 'MonitorService - 4CCC6A5A8F39'. The 'Current License Profile' section on the right shows the product variant (COSEC PLT), activation status (ACTIVATED), and a list of users (AUP, Platform, ACM, CMM, VMM, TAM, CWM, JPC, FVM, ESS, FR) with their counts and checkboxes for activation. A 'Save' button is at the bottom of this section. A note at the bottom right states: 'Note: By Enabling/Disabling the flag user can Activate/Deactivate the license. Once you deactivate your license, the module and its reflections will be removed from COSEC.'

Company: It displays the company profile name. The name of the company is configured during installation of the setup.

Database Name: It displays the COSEC database name of the company. The name is configured during installation of the setup. This COSEC database can be changed from Profile > Database Configuration.

License Key

Current License Key: It displays the current license key available in dongle.

Click on **License Upgrade**  icon for upgrading the License structure. The warning will appear as shown below.

The warning dialog box has a title bar 'Warning' and a close button. The text inside reads: 'COSEC CENTRA License needs Upgrading. Please proceed by accepting the same. Note: Once upgraded, reverting to any previous version(s) will not be allowed. License Upgrade may take few minute(s) after posting request.' At the bottom is an 'Accept & Proceed' button.



Only SA user can upgrade the license structure.

Click on **Accept & Proceed**. The Master service will upgrade the license key to new structure.

New License Key: When new module is to be added in COSEC, then you must update the license key. Enter the new license key.

Company

Database Name

License Key

Current License Key

New License Key

Click on **Update** to update company's License Key with the new one. This will add new features to the existing license key by keeping the COSEC License Platform (Serial No.) as it is.

Services

There is provision to assign Alert Service, Enroll Service, Visitor Service, Identification Service and multiple Monitor Services to the Company profile. Once the services are installed, the default services will be assigned to the company as shown below.

License and Services

Company

Database Name

License Key

Current License Key

New License Key

Services

Alert Service

Enroll Service

Visitor Service

Monitor Service

Identification Service

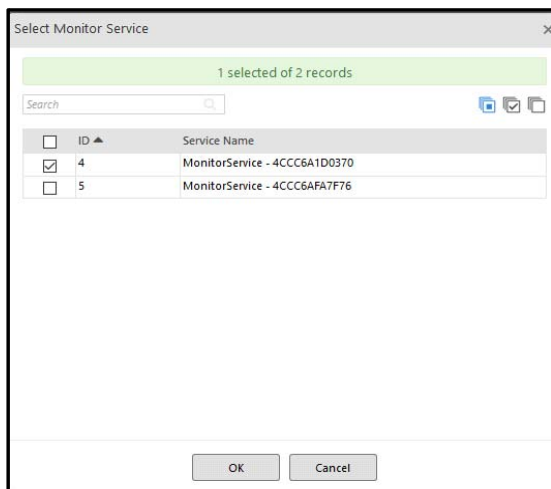
Current License Profile

Product Variant	COSEC PLT
Activation Status	ACTIVATED
AUP Validity	December-2021
Platform Users	5010
ACM Users	5005
CMM Users	5005
VMM Users	5001
TAM Users	5005
CWM Users	5005
JPC Users	5005
FVM Users	5005
ESS Users	5005
FR Users	5005

Monitor Service can be one or more as per company's device requirements. By default 1st Monitor Service will be marked as default.

But the services (Say Monitor Service) running on one computer can access Master service running on another computer. This will self-register the monitor service and will appear in the service picklist.

- Example: The Monitor Service on computer 192.168.104.24 is using Master service running on computer 192.168.104.12 so picklist of Services will show this additional Monitor service of 192.168.104.24 as shown below.



*Whenever any Monitor Service is deleted then on save, all the devices assigned to this service will be moved to the default Monitor Service.
This change will be done in Company's COSEC DB.*

Alert Service: Select the Alert service from the picklist to be assigned to the selected Company.

Enroll Services: Select the Enroll service from the picklist to be assigned to the selected Company.

Visitor Service: Select the Visitor service from the picklist to be assigned to the selected Company. This service will be required if the Visitor Utility is to be used.


Monitor Service: Select one or more Monitor service from the picklist to be assigned to the selected Company.

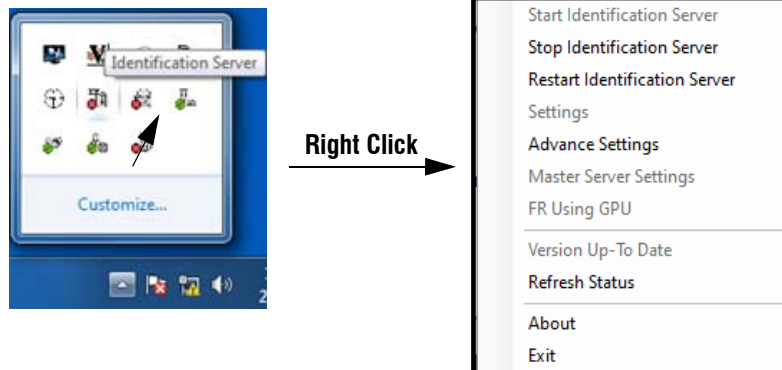
The assigned Monitor service will appear in the list as shown below

ID	Monitor Service Name	Default
4	MonitorService - 8CEC4B401530	<input checked="" type="checkbox"/>

Identification Service: Select the Identification Service from the pick list. To make sure this service functions as the Centralized Identification Service, follow the steps as mentioned:

- Click **Save**.

- Right-click on the IDS Tray Service .

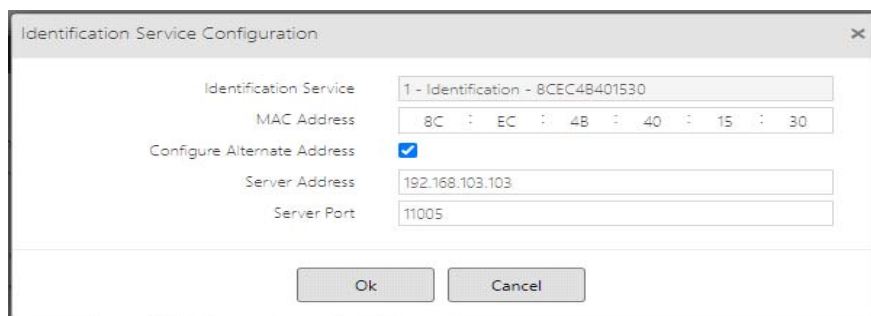


- Click **Restart Identification Server**.



The features — Group FR (Mark Group Attendance), Exceptional Face Enrollment and Face Enrollment via Web will function using this IDS only. For more details refer COSEC System Manual (COSEC > System Configuration > Global Policy > Face Recognition).

Click the Settings  icon. The **Identification Service Configuration** pop-up appears as shown below:



It displays the following details:

- Identification Service:** Displays the name of the Identification Service.
- MAC Address:** Displays the MAC Address of the computer where the Identification Service is running.
- Configure Alternate Address:** By default this check box is enabled. The **Server Address** will be displayed automatically.

Clear this check box, if you do not wish to opt for an Alternate Server Address.

- Server Port:** Displays the Port number used to access the Identification Service.

Click **OK** to save the configuration.



*These services are listed in **"COSEC Services"** section.*

Current License Profile

The Current License Profile displays the list of all the Module Users licenses.

The screenshot shows the 'License and Services' interface. The 'Current License Profile' section on the right displays the following information:

Product Variant	COSEC PLT
Activation Status	ACTIVATED
AUP Validity	December-2022
Platform Users	5010
ACM Users	5005 <input checked="" type="checkbox"/>
CMM Users	5005 <input checked="" type="checkbox"/>
VMM Users	0 <input type="checkbox"/>
TAM Users	5005 <input checked="" type="checkbox"/>
CWM Users	5005 <input checked="" type="checkbox"/>
JPC Users	5005 <input checked="" type="checkbox"/>
FVM Users	5005 <input checked="" type="checkbox"/>
ESS Users	0 <input checked="" type="checkbox"/>
FR Users	5005 <input checked="" type="checkbox"/>

Below the table is a 'Save' button. A note states: 'Note: By Enabling/Disabling the flag user can Activate/Deactivate the license. Once you deactivate your license, the module and its reflections will be removed from COSEC.'

Each type of Module User license has a corresponding check box for activating/deactivating the module.

You can select (activate) / clear (deactivate) the check boxes of the desired Module User licenses as per your requirement. However, if you deactivate any Module User license, the module and its reflections in other modules will be removed in COSEC Web.

By default the check box will be selected (enabled) for those modules whose license is activated and have more than 5 user license.

By default the check box will be clear (disabled) for those modules whose license is activated but have 5 or less than 5 user license. Such modules and their reflections in other modules will be removed in COSEC Web. The behavior for these modules will be the same as those modules that have 0 users. For example, there are 5 VMM Users and the check box is clear, then in COSEC Web the Visitor Management Module will not be visible on the Home page as well as its reflections in other module will be removed, for example, in User Module > User Configuration > Visitor Management tab will not be visible and so on.

Monitor Configuration

The Management team of the Company has to ensure the proper device assignment to Monitors. They can assign/re-assign devices among the monitor services assigned to the Company.

Once the device is configured by user, it gets assigned to the monitor which is marked as 'Default Monitor'.



The Admin Management team must Identify if new monitor service is required to serve the company's devices or any of the existing monitor service can accommodate all devices of the Company. Depending on this, new monitor service can be configured and then assigned to the Company.

Monitor Configuration

Company: 1 sheetal

Monitor Name:

Default: ☐

Optional Parameters

Stand By Monitor: --None--

Export Events: Disabled

IP:

Port Number:

Re-Try Count:

Polling Interval: seconds(1-999)

Assign Devices

Device: ID Name

Search:

ID	Name	Type
No Data		

Company: It displays the company profile name. The monitor services assigned to the company will appear in the grid on right side. Select the Monitor service from the grid to view the assigned devices to the respective monitor service.

Monitor Configuration

Company: 1 sheetal

Monitor Name: MonitorService - 4CCC6A1D0370

Default: ☒

Optional Parameters

Stand By Monitor: --None--

Export Events: Disabled

IP:

Port Number:

Re-Try Count:

Polling Interval: seconds(1-999)

Assign Devices

Device: ID Name

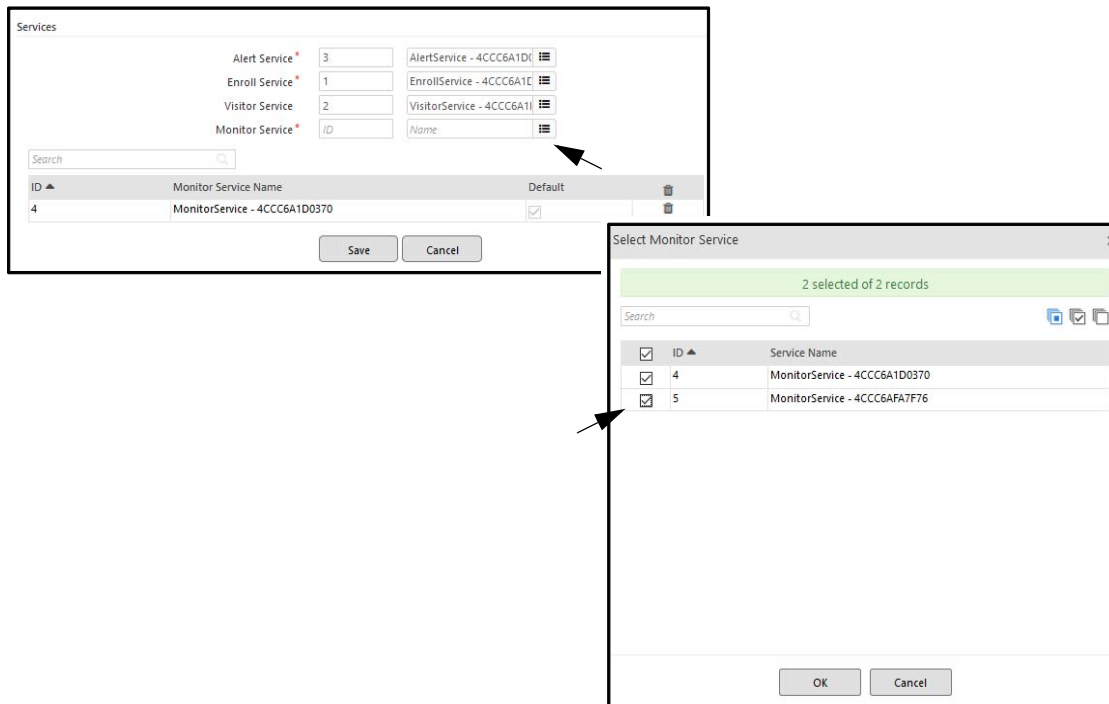
Search:

ID	Name	Type
1	PVR Door-Device-1	PVR Door

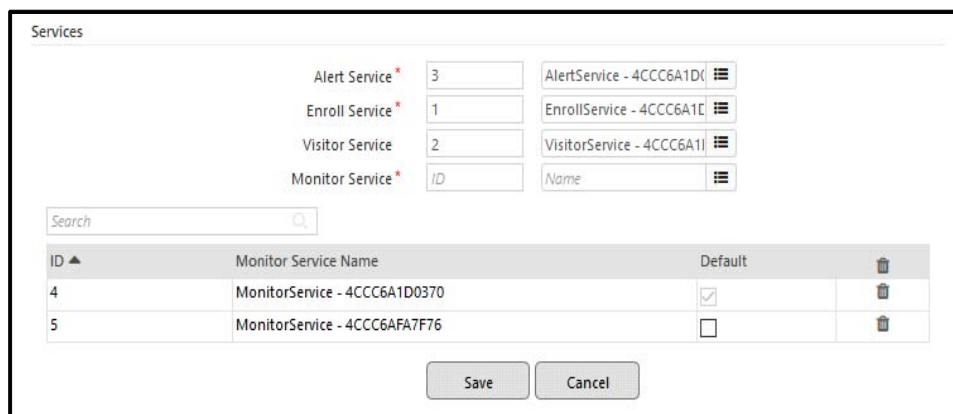
The Monitor Service is assigned to the company from “License and Services” page.

Only default monitor service will appear in the right grid till another monitor service is assigned to the company.

For assigning another monitor service click the Monitor Service pick-list on License and Services page. Then select the check-box for the monitor service which is to be assigned to the company. Then click OK and Save the settings.



The assigned Monitor service will appear in the list as shown below:



The new monitor service is now available in monitor configuration as well.

Monitor Configuration

Company: 1 sheetal

Monitor Name:

Default: ☐

Optional Parameters

Stand By Monitor: --None--

Export Events: Disabled

IP:

Port Number:

Re-Try Count:

Polling Interval: seconds(1-999)

Assign Devices

Device: ID Name

Search:

ID	Name	Type
No Data		

ID	Monitor Name	Total no. Of Devices
4	MonitorService - 4CCC6A1D0370	1
5	MonitorService - 4CCC6AFA7F76	0

Optional Parameters

- **Standby Monitor:** Select the standby monitor from the drop-down list which acts as standby to the selected monitor. When main monitor fails working, then standby monitor takes over and starts serving the devices which the main monitor was serving.

Monitor Configuration

Company: 1 sheetal

Monitor Name: MonitorService - 4CCC6A1D0370

Default: ☒

Optional Parameters

Stand By Monitor: --None--

Export Events: MonitorService - 4CCC6AFA7F76

IP:

Port Number:

Re-Try Count:

Polling Interval: seconds(1-999)

Assign Devices

Device: ID Name

Search:

ID	Name	Type
1	PVR Door-Device-1	PVR Door

ID	Monitor Name	Total no. Of Devices
4	MonitorService - 4CCC6A1D0370	1
5	MonitorService - 4CCC6AFA7F76	0

- **Export Events:** Select the Export events from the dropdown list to be exported to third party application.
- Specify the **IP address** and **Port Number** where the events are to be exported.
- **Re-Try Count:** Specify the re-try count upto which system will try exporting events and if not sent within this count then that event will be skipped. Later the event can be obtained through API.
- **Polling Interval (Seconds):** Specify the polling interval in seconds. It is the period for which COSEC Monitor will wait in idle state (the state in which no event is being sent to server). It is 30 seconds by

default. Thus if no event is sent for 30 seconds, a polling request is used to keep the connection with the server alive in idle period.

Assign Devices

You can assign devices to the selected monitor by selecting the devices from the device picklist. The devices assigned to the monitor service will be displayed in the grid.

If this monitor service is set as **default** from “License and Services”, then newly added device will be directly added in the grid.

To add a device (PVR Door) to Monitor

1. Open the Webpage of PVR Door by accessing Door's IP address (192.168.104.113) in browser. Configure the Gateway and DNS settings as shown below.

MATRIX PVR Door - PVR Door-Device-1 (1)

Settings

LAN Settings

IP Assignment: Static

IP Address: 192.168.104.113

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.104.1

Preferred DNS: 192.168.50.100

Alternate DNS:

MAC Address: 00:1b:09:03:f2:b0

Submit Cancel Default

Enter URL

Test Connection

2. Configure the Basic Profile. Select the server connection as COSEC CENTRA.

MATRIX PVR Door - PVR Door-Device-1 (1)

Settings

Basic Profile

Connectivity Status: Ethernet: Failed to connect with Server. Please verify configurations on server.

Door Type: Direct Door

Server Connection: COSEC CENTRA

Firmware Version: V01R33 (Oct 3 2017 - 13:59:31)

Firmware Upgrade Time: Jan 02 2018 - 12:42:20

System Up-Time: 2 days 4 hrs 38 mins

Submit Cancel

Readers

Readers	Mode	Configured Reader	Detected Reader
Internal - Card	Entry	MiFare -U Reader - Active	MiFare -U Reader
Internal - Palm	Entry	Palm Vein Reader - Active	Palm Vein Reader
External - Card	Exit	None	None

3. Configure the Server Settings. Enter the URL as 192.168.104.12 as the IP address of computer where monitor service is running and the Port as the Device Listening port.

4. The PVR door will be added to the default Monitor Service in Monitor Configuration. If the monitor service to which door is to be assigned is not default, then you have to add the door to it. Once the door is connected to monitor service at 192.168.104.12, then connectivity will display as Online.

To change the Monitor service of device

Identify which devices has to be removed/assigned/re-assigned to which monitor service.

Example: PVR door is in Monitor Service-4. Now PVR door is to be assigned to Monitor Service- 5. Follow the below mentioned steps.

1. Change the Server Settings of PVR with the IP address of computer where Monitor Service-5 is running.
2. Go to Company configuration > Monitor configuration. Remove the device from Monitor Service-4.
3. Then re-assign door to Monitor service-5 by selecting the PVR door from the pick-list. On saving, PVR will communicate to the newly assigned/re-assigned monitor service.

Example: 10 devices of Company ABC are served by default monitor. But as the service gets slow, new monitor service can be assigned to some or all of the 10 devices of Company ABC.

The COSEC Utilities such as Enrollment, Monitoring of Devices, Visitor Management, Alert notifications are managed by dedicated services. These services are installed from the COSEC application Setup.

Alert Service is required for sending notification alert.

Monitor Service is required for communicating with COSEC devices.

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

Once the services are started and running, it will automatically get assigned to the company.

By default following COSEC services can be managed:

- **Alert Service**
- **Enroll Service**
- **Monitor Service**
- **Visitor Service**

The screenshot shows the 'COSEC Services' configuration window. On the left, there is a form for configuring a service. The 'Service' dropdown is set to '4' and 'MonitorService - 4CCC6A1D0370'. The 'Service Type' dropdown is set to 'Monitor Service'. The 'Default' checkbox is checked. The 'MAC Address' field shows '4C : CC : 6A : 1D : 03 : 70'. The 'IP Address' field shows '192 . 168 . 104 . 12'. The 'Domain Name' field is empty. The 'Web Access Port Number' field shows '11001'. The 'Secured Web Access Port Number' field shows '11010'. The 'Device Port Number' field shows '11000'. The 'Secured Device Port Number' field shows '11009'. The 'Assigned Devices' field shows '0'. On the right, there is a table with the following data:

ID	Service Type	Name
1	Enroll Service	EnrollService - 4CCC6A1D0370
2	Visitor Service	VisitorService - 4CCC6A1D0370
3	Alert Service	AlertService - 4CCC6A1D0370
4	Monitor Service	MonitorService - 4CCC6A1D0370



The new services cannot be configured here. But the services (Say Monitor Service) running on one computer can access Master service running on another computer. This will self-register the monitor service and will appear in the list shown on right side.

The Monitor Service on computer 192.168.104.24 is using Master service running on computer 192.168.104.12 so COSEC Services of 192.168.104.12 will list this additional Monitor service of 192.168.104.24 as shown below.

COSEC Services

Service *

5

MonitorService - 4CCC6AFA7F76

Service Type

Monitor Service

Default

☐

MAC Address *

4C : CC : 6A : FA : 7F : 76

IP Address *

192 . 168 . 104 . 24

Domain Name

Web Access Port Number *

11001

Secured Web Access Port Number *

11010

Device Port Number

11000

Secured Device Port Number

11009

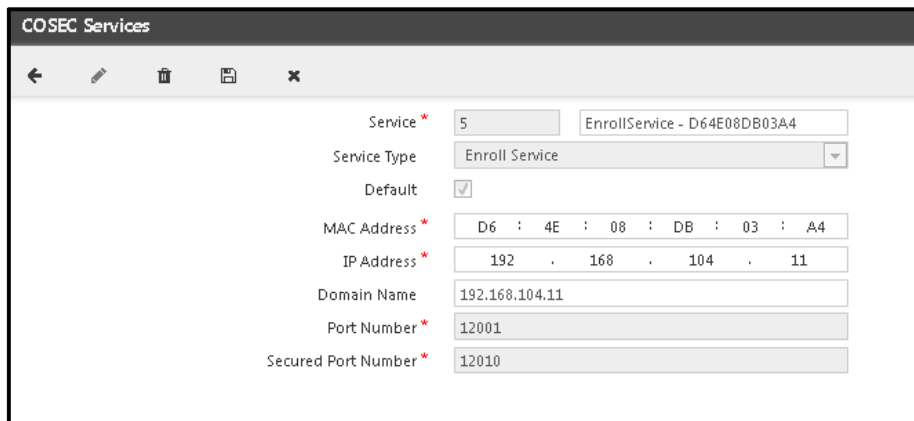
Assigned Devices

0

Search

ID ▲	Service Type	Name
1	Enroll Service	EnrollService - 4CCC6A1D0370
2	Visitor Service	VisitorService - 4CCC6A1D0370
3	Alert Service	AlertService - 4CCC6A1D0370
4	Monitor Service	MonitorService - 4CCC6A1D0370
5	Monitor Service	MonitorService - 4CCC6AFA7F76

Enroll Service



The screenshot shows a web browser window titled "COSEC Services". The interface has a top navigation bar with icons for back, edit, delete, save, and close. The main content area displays a form for configuring an "Enroll Service". The form fields are as follows:

Field	Value
Service *	5
Service Type	Enroll Service
Default	<input checked="" type="checkbox"/>
MAC Address *	D6 : 4E : 08 : DB : 03 : A4
IP Address *	192 . 168 . 104 . 11
Domain Name	192.168.104.11
Port Number *	12001
Secured Port Number *	12010

MAC address: Enter the MAC address of the computer where the Enroll service is installed.

IP Address: Enter the IP address of the computer on which the Enroll service is accessible.

Domain Name: Enter any name as the domain name to assign with the Enroll service. While creating new service, the domain name as set on "General Settings" page will be fetched here.
The valid characters are **A-Z, a-z,0-9, -, _** and .

Port Number: This shows the port number at which device will communicate with Enroll Service. This port number is entered from Enroll Service Settings.

Secure Port Number: This shows the port number at which device will communicate with Enroll Service on SSL mode. This port number is entered from Enroll Service Settings.

Alert Service

The screenshot shows the 'COSEC Services' configuration window. It contains the following fields and values:

Field	Value
Service *	3
Service Type	AlertService - D64E08DB03A4
Service Type (dropdown)	Alert Service
Default	<input checked="" type="checkbox"/>
MAC Address *	D6 : 4E : 08 : DB : 03 : A4
IP Address *	192 . 168 . 104 . 11
Domain Name	192.168.104.11
Web Access Port Number *	13001
Secured Web Access Port Number *	13010

MAC address: Enter the MAC address of the computer where the Alert service is installed.

IP Address: Enter the IP address of the computer on which the Alert service is accessible.

Domain Name: Enter any name as the domain name to assign with the Alert service. The valid characters are **A-Z, a-z,0-9, -, _** and **.**

Web Access Port Number: This shows the port number of the computer at which COSEC Web can access the Alert Service. This port number is entered from Alert Service Settings.

Secured Web Access Port Number: This shows the port number of the computer at which COSEC Web can access the Alert Service on SSL mode. This port number is entered from Alert Service Settings.

Alert Service- time zone

When client is situated in a time zone other than Alert Service's time zone; Alert Service will take company's time zone into consideration while processing scheduled tasks or generating scheduled reports.

"The time of execution for any task = Schedule Time + (Portal's Time Zone - Company's Time Zone)

Example:

Company's Time Zone = GMT - 05:30

Portal's Time Zone = GMT + 05:30

Suppose a task has been scheduled to run every day at 10:00 hours

So this task should be executed everyday by Alert Service as per it's time zone difference at
[10:00 + (GMT + 05:30) - (GMT - 05:30)]
= **21:00 hours**

Monitor Service

The screenshot shows the 'COSEC Services' configuration window. It contains the following fields and values:

Field	Value
Service *	4
Service Type	Monitor Service
Default	<input checked="" type="checkbox"/>
MAC Address *	D6 : 4E : 08 : DB : 03 : A4
IP Address *	192 . 168 . 104 . 11
Domain Name	192.168.104.11
Web Access Port Number *	11001
Secured Web Access Port Number *	11010
Device Port Number	11000
Secured Device Port Number	11009
Assigned Devices	106

MAC address: Enter the MAC address of the computer where the Monitor service is installed.

IP Address: Enter the IP address of the computer on which the Monitor service is accessible.

Domain Name: Specify a domain name to assign with the Monitor service. While creating new service, the domain name as set on “General Settings” page will be fetched here. The valid characters are **A-Z, a-z,0-9, -, _** and **.**

Web Access Port Number: This shows the port number of the computer at which COSEC Web can access the Monitor Service. This port number is entered from Monitor Service Settings.

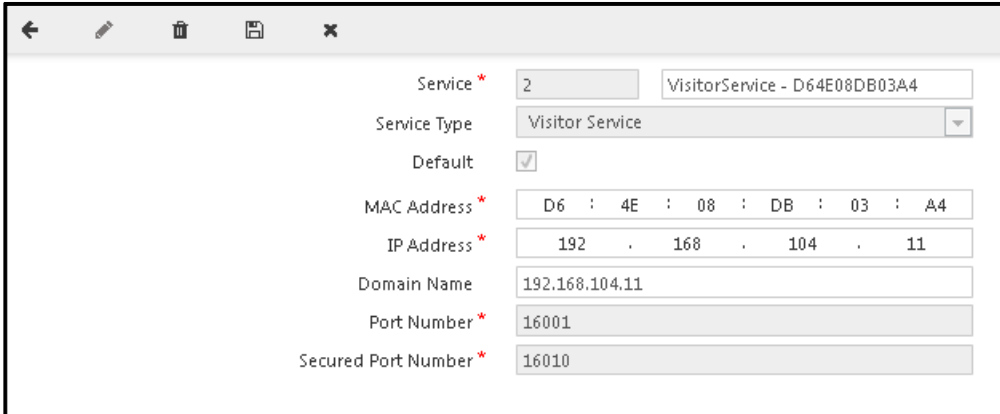
Secured Web Access Port Number: This shows the port number of the computer at which COSEC Web can access the Monitor Service on SSL mode. This port number is entered from Monitor Service Settings.

Device Port Number: This shows the port number at which device will communicate with Monitor Service. This port number is entered from Monitor Service Settings.

Secured Device Port Number: This shows the port number at which device will communicate with Monitor Service on SSL mode. This port number is entered from Monitor Service Settings.

Assigned Devices: This shows the number of devices assigned to the selected Monitor Service. It will be displayed once device is added from COSEC Web.

Visitor Service



The screenshot shows a configuration window for a 'Visitor Service'. The window has a title bar with standard icons (back, edit, delete, save, close). The form contains the following fields:

Service *	2	VisitorService - D64E08DB03A4
Service Type	Visitor Service	
Default	<input checked="" type="checkbox"/>	
MAC Address *	D6 : 4E : 08 : DB : 03 : A4	
IP Address *	192 . 168 . 104 . 11	
Domain Name	192.168.104.11	
Port Number *	16001	
Secured Port Number *	16010	

MAC address: Enter the MAC address of the computer where the Visitor service is installed.

IP Address: Enter the IP address of the computer on which the Visitor service is accessible.

Domain Name: Specify a domain name to assign with the Visitor service. While creating new service, the domain name as set on "General Settings" page will be fetched here. The valid characters are **A-Z, a-z,0-9, -, _** and **.**

Port Number: This shows the port number at which service is accessible.

Secured Port Number: This shows the port number at which service is accessible on SSL mode.

The requests for database management activities like post/retrieve are processed by the Admin portal service. The service processes the requests and update status for the same in company's COSEC database.

Every time a new post/retrieve request is submitted from COSEC Web, system will trigger Admin Portal Service about adding up the same in the process queue.

Admin Portal Service maintains the COSEC Database location for company against the submitted task. It then takes up the request one by one and process the same. It will also update task's status accordingly in the Company's COSEC Database > Post/Retrieve Table.

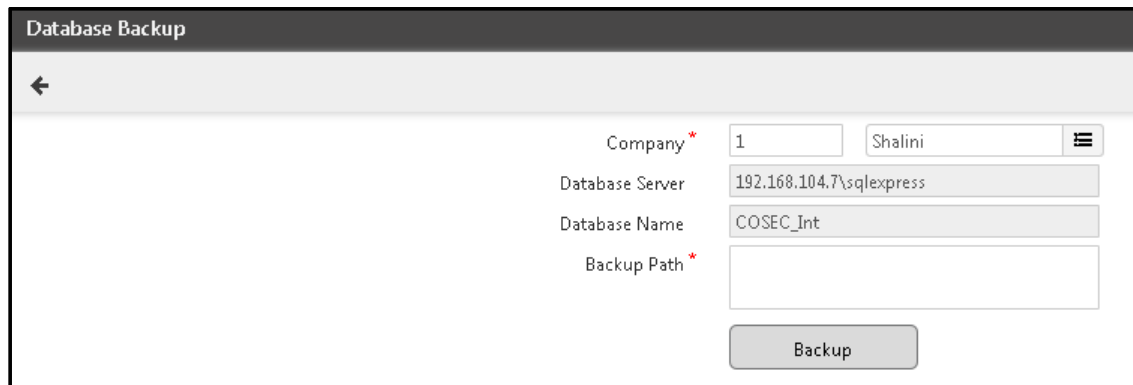
The Company administrator can take backup of company's database. See ["Database Backup"](#).

The Company administrator can upgrade the company's database. See ["Database Upgrade"](#)

Database Backup

The Company Management team can take backup of the Company's COSEC Database through Admin portal.

To take backup of database; go to **Manage Database > Database Backup**.



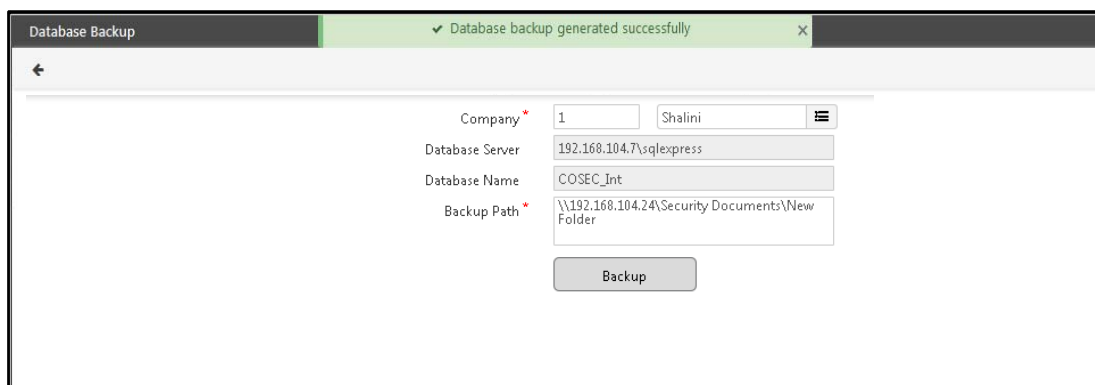
The screenshot shows a web form titled "Database Backup". It has a back arrow icon in the top left. The form contains the following fields:

- Company ***: A dropdown menu with "1" selected and "Shalini" displayed next to it.
- Database Server**: A text input field containing "192.168.104.7\sqlexpress".
- Database Name**: A text input field containing "COSEC_Int".
- Backup Path ***: An empty text input field.
- Backup**: A button at the bottom right of the form.

Company: It displays the company profile name whose database backup is to be taken.

The **Database Server** and **Database Name** of Company is displayed as shown above.

Backup Path: Enter the path where the backup of COSEC database is to be created.



This screenshot shows the same "Database Backup" form, but with a green success message at the top: "✓ Database backup generated successfully". The fields are now populated with the following values:

- Company ***: "1" (selected) and "Shalini" (displayed).
- Database Server**: "192.168.104.7\sqlexpress".
- Database Name**: "COSEC_Int".
- Backup Path ***: "\\192.168.104.24\Security Documents\New Folder".
- Backup**: A button at the bottom right.

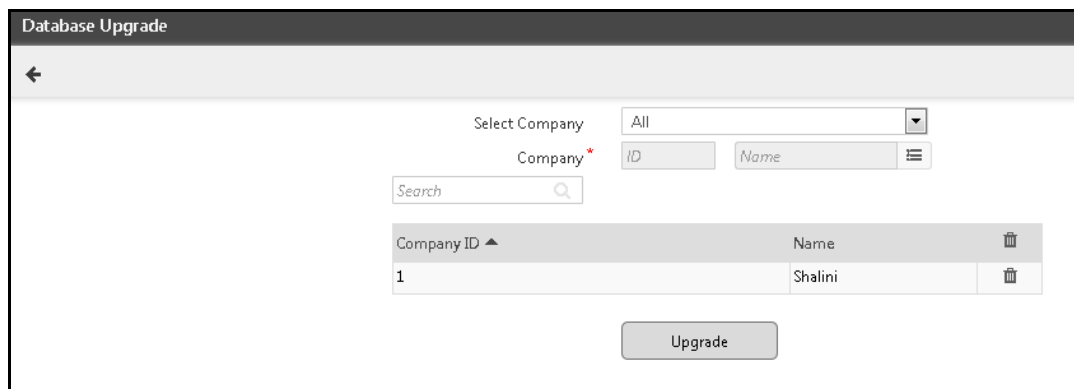
Database Upgrade

The company management team can upgrade the Company's COSEC Database through Admin Portal.

To upgrade the database of company; go to **Manage Database > Database Upgrade**.

Select Company: You can select the option as **All** or **Select Randomly** depending on the upgradation required.

When option is selected as "Select Randomly", then select the **Company profile** from the picklist whose database is to be upgraded.



Database Upgrade

Select Company: All

Company: ID Name

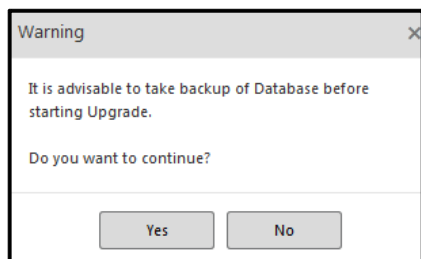
Search

Company ID	Name
1	Shalini

Upgrade

After selecting the company, the profile will be displayed in the grid. Click on **Upgrade** button.

A Warning appears as shown below. You can take backup of database before upgrading. Click **No** and take the backup of existing database from "Database Backup". If backup is not required; then click **Yes** to continue upgrade.



Warning

It is advisable to take backup of Database before starting Upgrade.

Do you want to continue?

Yes No

The database upgrade will be started and the status will be displayed as **In Progress**.

Database Upgrade

←

Select Company

All

Company *

ID

Name

Search

Q

Company ID ▲	Name	Status	
1	Shalini	In Progress	

Refresh

Acknowledge

Then click on Refresh to refresh the status of upgradation. Once the database is upgraded, the status will show as Success.

Database Upgrade

←

Select Company

All

Company *

ID

Name

Search

Q

Company ID ▲	Name	Status	
1	Shalini	Success	

Refresh

Acknowledge

Click on **Acknowledge** button to acknowledge the success/fail of database upgrading.

System Configuration enables you to configure Maintenance schedule and inform the Company so they can manage the work accordingly.

The Secured connection can be established between the Company and the Server after configuring Security settings.

The SMS notification and Email notification can be sent after setting SMS and Email Configurations.

Using General Settings the Company management administrator can specify the Master Service URL, Port, Utility download URL and other important connection end points which will be used by the company for accessing COSEC Web application.

The screenshot displays the 'MATRIX COSEC ADMIN' interface. On the left, a sidebar lists navigation categories: 'Company Configuration' (with sub-items: Profile, License and Services, Monitor Configuration), 'COSEC Services', and 'Manage Database'. The main panel is titled 'System Configuration' and contains a list of configuration links: 'Maintenance Configuration', 'Security', 'SMS Configuration', 'Email Configuration', 'General Settings', 'Multi-Language Configuration', and 'Login Policy'. The 'SMS Configuration' section is currently selected and expanded, showing a 'Message' text area (500 chars), 'Maintenance Start Date-Time' and 'Maintenance End Date-Time' fields (both with HHMM format), and checkboxes for 'SMS' and 'Email' notifications. At the bottom of this section are 'Save & Send' and 'Reset' buttons. A top navigation bar includes icons for settings, help, phone, and user profile.

Click on the links for various configurations:

[“Maintenance Configuration”](#)

[“Security”](#)

[“SMS Configuration”](#)

[“Email Configuration”](#)

[“General Settings”](#)

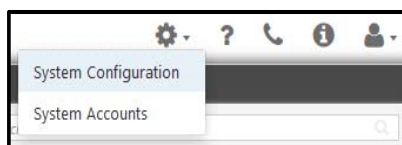
[“Multi-language Configuration”](#)

[“Login Policy”](#)

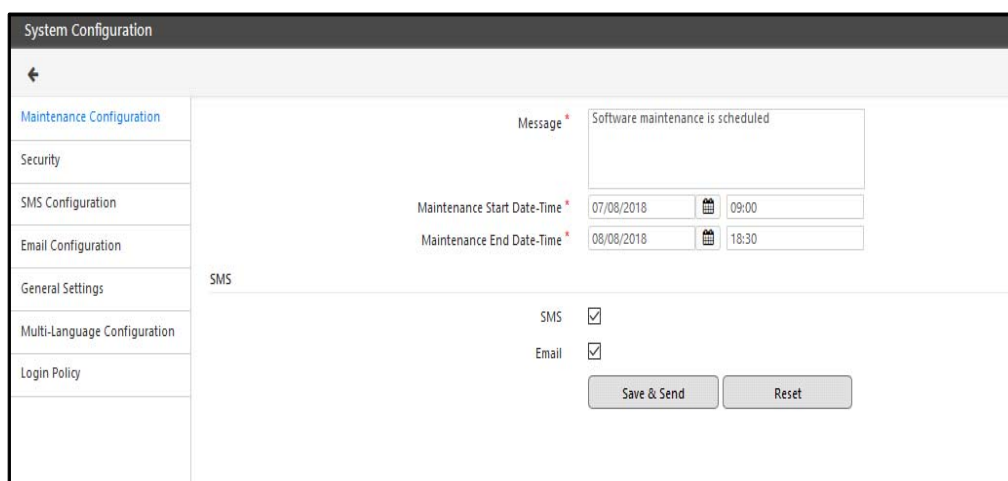
Maintenance Configuration

The COSEC System requires maintenance time during up-gradation of versions. During this time the company may not access COSEC application so the Maintenance duration can be configured from here which can be informed to the company.

To configure the maintenance information click on the option **System Configuration** from the Admin Menu.



Go to **System Configuration > Maintenance Configuration**. The page appears as shown below.

A screenshot of the 'Maintenance Configuration' page. On the left is a sidebar with a list of configuration options: Maintenance Configuration (selected), Security, SMS Configuration, Email Configuration, General Settings, Multi-Language Configuration, and Login Policy. The main content area has a 'Message' field with the text 'Software maintenance is scheduled'. Below this are two date-time pickers: 'Maintenance Start Date-Time' set to 07/08/2018 09:00 and 'Maintenance End Date-Time' set to 08/08/2018 18:30. There are checkboxes for 'SMS' and 'Email', both of which are checked. At the bottom right are 'Save & Send' and 'Reset' buttons.

Message: Enter a message which is to be sent to the company as maintenance display message.

Maintenance Start Date-Time: Select the date and specify the time at which maintenance will be started.

Maintenance End Date-Time: Select the date and specify the time at which maintenance will end.

Enable **SMS** check box to send SMS to all active company's contact number.

Enable **Email** check box to send Email to all active company's Email ID.

On the basis of this Mail is sent to the company informing the maintenance alert. Mail is to be updated considering individual company's time zone as well.



Enabling of SMS or Email Check-box is not mandatory to schedule the maintenance message.

Click **Save & Send** to save the configuration and send SMS/Email to the company.



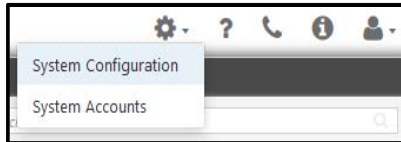
The company/user will get scheduled maintenance message on login page about 2 days prior to Schedule Start Date.

Click on **Reset** button if maintenance message is to be removed from displaying.

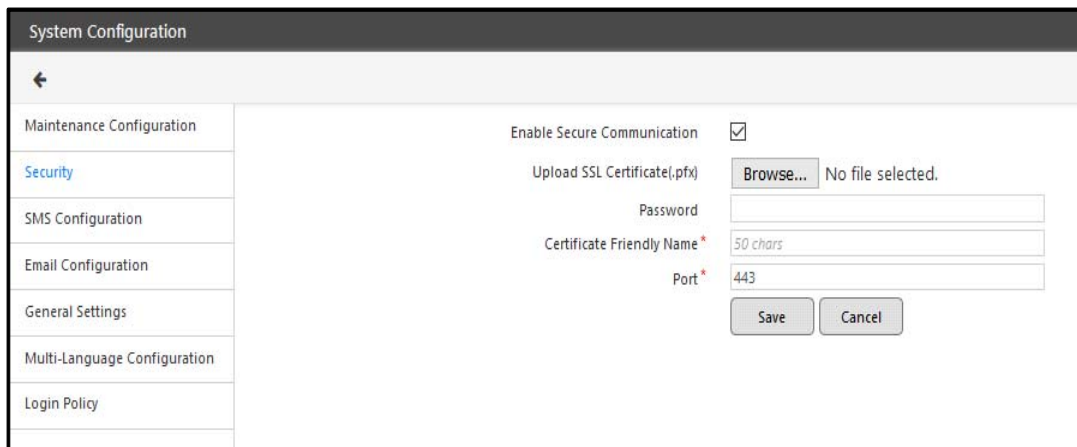
Suppose if the maintenance gets completed earlier than the End Date-time; then Reset button will stop displaying the current maintenance message.

Security

To configure the Secure Communication settings click on the option **System Configuration** from the admin menu.



Go to **System Configuration> Security**. The page appears as shown below.

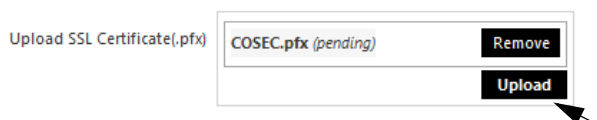
A screenshot of the 'System Configuration' page, specifically the 'Security' tab. On the left is a sidebar with links: Maintenance Configuration, Security (highlighted), SMS Configuration, Email Configuration, General Settings, Multi-Language Configuration, and Login Policy. The main content area has the title 'System Configuration' and a back arrow. It contains the following settings: 'Enable Secure Communication' with a checked checkbox; 'Upload SSL Certificate(.pfx)' with a 'Browse...' button and the text 'No file selected.'; 'Password' with an empty text field; 'Certificate Friendly Name*' with a text field containing '50 chars'; and 'Port*' with a text field containing '443'. At the bottom right are 'Save' and 'Cancel' buttons.

SSL or Secure Sockets Layer is a security protocol that enables to have secured communication between Client and Server by making use of asymmetric keys. These keys are defined in pairs of public-private key. Public key is available to all clients while private key is only available with the server owning the SSL certificate. These keys have following properties:

- Data encrypted by client using public key can only be decrypted by server using the private key.
- Data encrypted by server's private key can only be decrypted by using the public key.

SSL allows sensitive information (e.g. login credentials) to be transmitted securely.

- **Enable Secure Communication:** Select to enable secure communication using SSL encryption.
- **Upload SSL Certificate(.pfx):** Click to browse the file through your system and select the SSL certificate to be uploaded as a *.pfx file. Click **Upload**.



- **Password:** Enter the password required to access the uploaded SSL Certificate.
- **Certificate Friendly Name:** Enter a friendly name for the SSL Certificate. This will be used internally by IIS during certificate configurations.

- **Port:** Enter the port number on which secure communication is to be carried. The default Port for SSL communication is 443 (recommended). However, any other port can be used.



Some pre-defined ports do not support SSL communication. If the user configures SSL on such a port, settings will be saved successfully, but he/she will fail to access COSEC. In such a case, the user should manually change this Port setting in IIS and thereafter COSEC can be accessed.



The initial communication just after enabling SSL communication will be insecure. Later on, as soon as it is found from DB that SSL has been enabled, the communications made thereafter will be on SSL basis.

Enable Secure Communication
☒

Upload SSL Certificate(.pfx)
No file selected.

Password

Certificate Friendly Name *

Port *

Issuer	CN=localhost
SSL version	3
Valid From	01/02/2016 16:20:15
Valid To	01/02/2021 05:30:00



When Security mode is switched from Non-SSL to SSL or vice versa then all the services will be restarted.

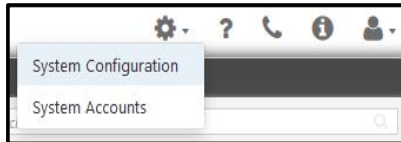
•Restarting Master Service will only be possible when Master Service is accessible from Admin Management Portal Web Server. If not then user has to restart it manually.

•Restarting any COSEC Service will only be possible when it is accessible from Master Service. If not then user has to restart it manually.

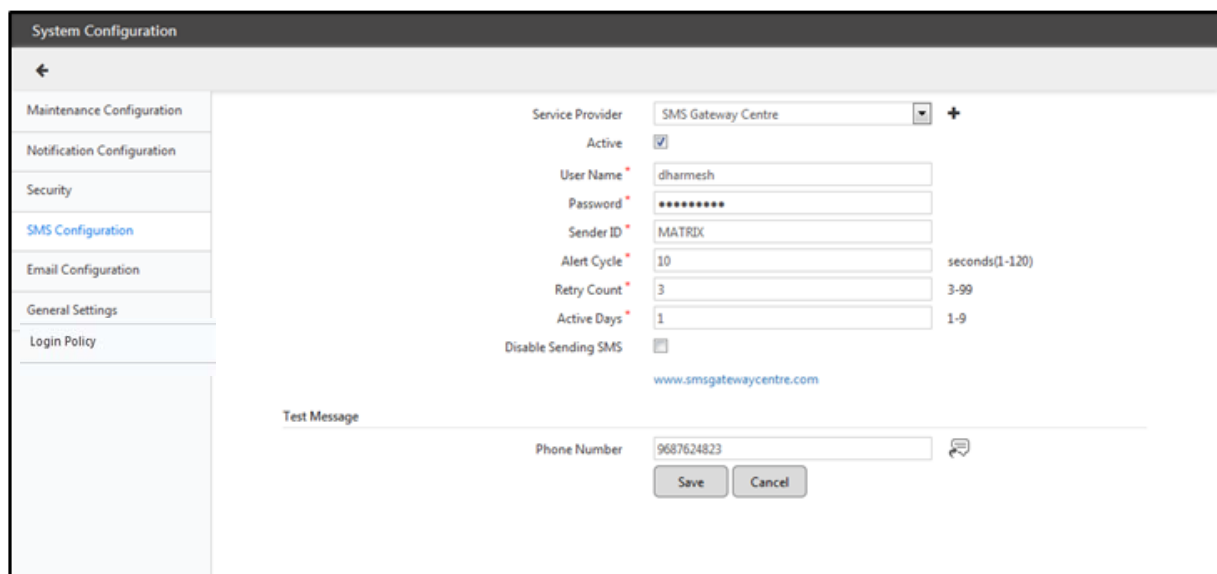
•There can be scenarios when the service is stopped and started. However by the time starting is attempted the ports are not freed. In such cases the service will stop giving reason as port unavailability. So user has to start it manually.

SMS Configuration

For SMS configuration settings click on the option **System Configuration** from the admin menu.



Go to **System Configuration> SMS Configuration**. The page appears as shown below.

A screenshot of the 'System Configuration' page, specifically the 'SMS Configuration' section. On the left is a sidebar menu with options: Maintenance Configuration, Notification Configuration, Security, SMS Configuration (highlighted in blue), Email Configuration, General Settings, and Login Policy. The main content area contains the following fields: 'Service Provider' (a dropdown menu set to 'SMS Gateway Centre'), 'Active' (a checked checkbox), 'User Name' (text field with 'dharmesh'), 'Password' (text field with masked characters), 'Sender ID' (text field with 'MATRIX'), 'Alert Cycle' (text field with '10' and a unit of 'seconds(1-120)'), 'Retry Count' (text field with '3' and a unit of '3-99'), 'Active Days' (text field with '1' and a unit of '1-9'), and 'Disable Sending SMS' (a disabled checkbox). Below these fields is a 'Test Message' section with a 'Phone Number' text field containing '9687624823' and 'Save' and 'Cancel' buttons. A URL 'www.smsgatewaycentre.com' is also visible.

If SA user forgets his password, then his OTP can be retrieved on his Mobile number if the SMS Configuration is done from this page.

For getting OTP on Mobile, the Contact number must be available in “System Accounts” Detail.



The user needs to ensure that the COSEC ALERTS computer has an internet connection for this functionality to work.

The SMS setting parameters need to be configured as described here.

Select the Service provider from the drop down list. The service providers already supported are:

- SMSGatewayCenter
- SMSLane
- BusinessSMS
- BulkSMS
- SNOWEBS

To add new service provider “[New Service Provider](#)”

After selecting the service provider, enable the **Active** checkbox to activate the service provider.

Enter the **Username, Password, and the registered Sender ID** in the respective fields as shown above.



The username, password and registered sender ID for different service providers can be found from Support Data or administrator.

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.

Active Days: Specify the number of days for which the pending messages will be treated as active in the event of the Alert service being temporarily stopped.

Disable Sending SMS: Check this box for temporarily disabling the SMS sending functionality.

Test Message:

Enter a phone number in the field provided and send a test message to test the settings. The user may now start the alert service to send the SMS.

New Service Provider

To add a new service provider, click the **+** button. The **API Configuration** window appears on your screen.

Enter the new service provider's name (e.g. "way2sms") and URL i.e. the actual service provider website used for registration etc. (e.g. "www.way2sms.in").

Service Provider Name: Enter the new SMS service provider's name (e.g. "way2sms")

Service Provider URL: Enter the URL of the service provider. This url is displayed on the main SMS Setting page as shown in the screen below.

Base URL: Enter the base url of the service provider as given in the API document. This is used for sending the message through SMS.

Example: In the following url: “localhost/way2sms.com?uname=test;pwd=test;number=test;sid=test”, the url before the question mark is the base url and the remaining part is the argument and its value as shown in the screen below.

Now add the **API arguments** by clicking on **Add** icon as shown below.

- **API Argument:** Enter the API argument name specified in the API document of the service provider.
- **Argument Value:** Select the argument value from the dropdown list which is to be associated with the API argument. Eg: Select the Argument value one by one from the drop down options. Eg: Select Argument value as “User Name” and specify API Argument as “uname” which will be used in the API argument.

This screenshot shows the 'API Configuration' dialog. The 'API Argument' field is empty, and the 'Argument Value' dropdown is open, showing a list of arguments including 'User Name', 'Password', 'Sender ID', 'Phone No.', 'Custom', and 'Message'. The 'Custom Value' field is empty. The 'Add' button (a plus sign in a square) is visible in the top right corner.

This screenshot shows the 'API Configuration' dialog after the 'Add' button has been clicked. The 'API Argument' field now contains 'uname', and the 'Argument Value' dropdown is set to 'User Name'. The 'Custom Value' field is empty. The 'Add' button is still visible in the top right corner.

Click **Add** icon to associate **API Arguments** with the **Argument value**. These API arguments are available in the API document of the service provider. The added arguments get displayed in the grid below.

This screenshot shows the 'API Configuration' dialog with the 'API Arguments' grid. The grid has three columns: 'API Argument', 'Argument Value', and 'Custom Value'. The arguments listed are 'pwd' (Password), 'number' (Phone No.), 'sid' (Sender ID), and 'uname' (User Name). Each row has an 'Add' (plus) and 'Delete' (trash) icon in the rightmost column.

One can also click **Delete** icon, if any argument is to be removed. Further, one can also edit any argument by clicking on it, editing the argument and then clicking **Update**.

- **Argument Separator:** Enter the argument separator to be used for firing a command. **Example.:** "&" or ";".
- **Request Method:** Select the method for sending the message via sms. The options are: **post** and **web**. If post is selected, you can send long messages without any limitation. If Web is selected, you can send only short messages.
- **Request Preview:** Displays the preview of the url with arguments as shown in the screen below.
- **Balance Check:** Select to allow balance check, if the service provider needs to use it.

This screenshot shows the 'API Configuration' dialog with the 'Request Preview' field. The 'Argument Separator' is set to '&', the 'Request Method' is set to 'Post', and the 'Request Preview' field displays the URL: 'localhost/way2sms/login?uname=test&pwd=test&sid=test&number=test'. The 'Balance Check' checkbox is checked, and the value '100' is entered in the adjacent field.

- **API Response:** Enter the API Response to be used for the selected **COSEC Response** from the dropdown list. Click **Add** button and the response gets displayed in the grid.

E.g. If "1" API Response is specified for the "**Success**" COSEC Response, then if the message is sent successfully then API will respond with 1 value and COSEC will respond with the value success.

API Response	COSEC Response
0	Failure
1	Success

Save Cancel

Click **Save** button to save the above API configurations. The new service provider will be created and will appear in drop down options of Service Provider.

System Configuration

✓ Saved Successfully

Maintenance Configuration

Notification Configuration

Security

SMS Configuration

Email Configuration

General Settings

Service Provider: way2sms

Active: ☐

User Name:

Password:

Sender ID:

Flash Message: ☐

Alert Cycle: 10 seconds (1-120)

Retry Count: 3 (3-99)

Active Days: 1 (1-9)


Disable Sending SMS: ☐

Test Message

Phone Number:

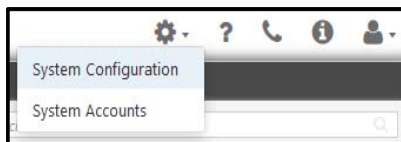
Save Cancel



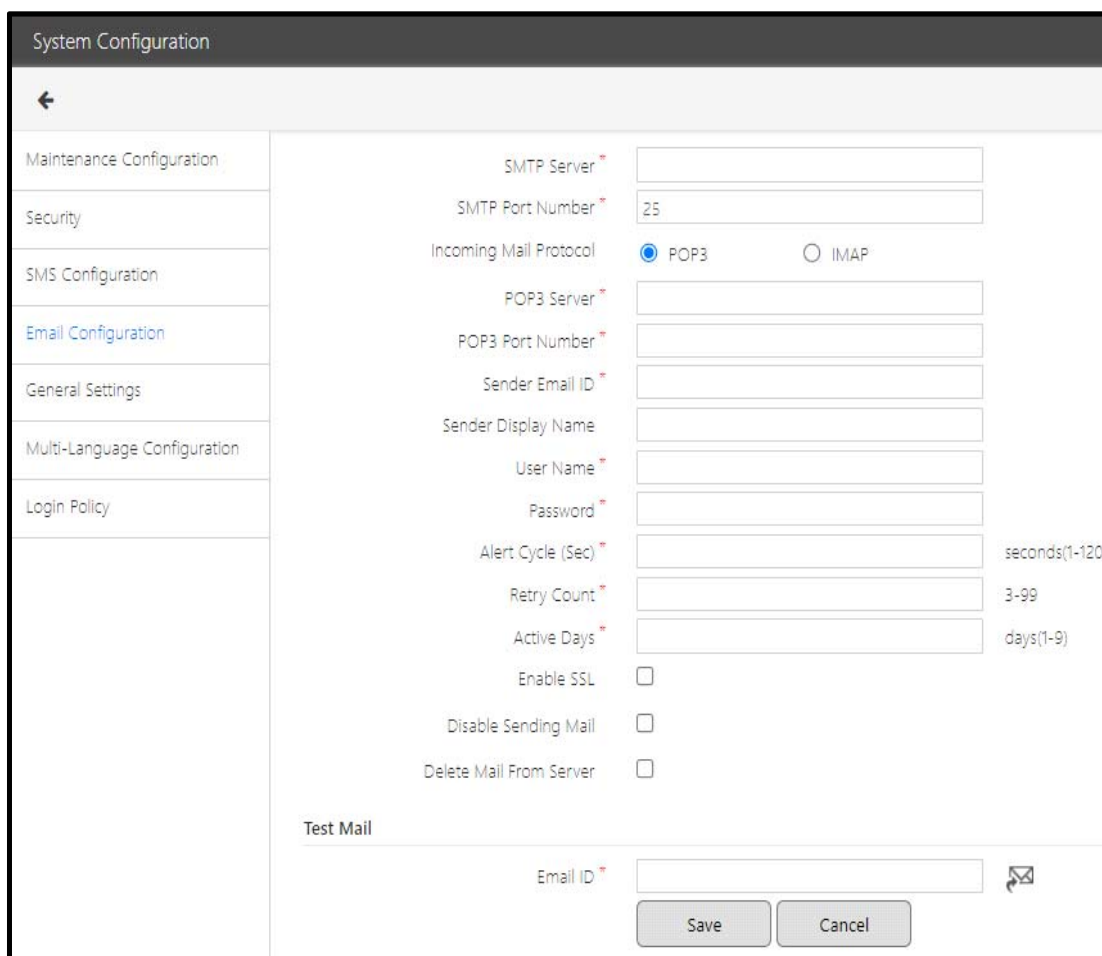
To edit API configuration for a user-defined service provider, on the **SMS Setting** page, select a service provider and click the Edit  button.

Email Configuration

For Email configuration settings click on the option **System Configuration** from the admin menu.



Go to **System Configuration> Email Configuration**. The page appears as shown below.

A screenshot of the 'System Configuration' page, with the 'Email Configuration' tab selected. The left sidebar contains a list of configuration categories: Maintenance Configuration, Security, SMS Configuration, Email Configuration (highlighted), General Settings, Multi-Language Configuration, and Login Policy. The main content area contains various email settings. On the right, there are input fields for SMTP Server, SMTP Port Number (set to 25), POP3 Server, POP3 Port Number, Sender Email ID, Sender Display Name, User Name, Password, Alert Cycle (Sec) (with a range of 1-120 seconds), Retry Count (with a range of 3-99), and Active Days (with a range of 1-9 days). There are also checkboxes for 'Enable SSL', 'Disable Sending Mail', and 'Delete Mail From Server'. At the bottom, there is a 'Test Mail' section with an 'Email ID' input field and a 'Send' icon. 'Save' and 'Cancel' buttons are located at the bottom right.

If SA user forgets his password, then his OTP can be retrieved on his Email ID if the Email Configuration is done from this page.

For getting OTP on Email, the Email ID must be available in "System Accounts" Detail.

The user needs to ensure that an SMTP Server has been set up on the network. The E-mail setting parameters need to be configured as described here.

SMTP Server: Enter 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. Select POP3 if emails are to be popped from the server to the client. **E.g.** Microsoft Outlook. Select IMAP if emails are to be stored in the server only like gmail or yahoo where the emails are stored on the server only.

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 sender Email ID in this field.

Sender Display Name: Specify the user name as to be displayed in the emails.

User Name: Specify the user name as set in the outlook account on the Alert PC.

Password: Specify the password as set in the outlook account.

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: Select the check box, if the communication via email is to be made secured using SSL (Secure Socket Layer).

Example: In the event of using an external SMTP server like gmail, the enable SSL option needs to be enabled.

Disable Sending Mail: Check this box for temporarily disabling the mail sending functionality.

Delete Mail from server: Check this box for deleting all mails from the server as soon as they are downloaded to the client.

Test Mail

- **E-mail ID:** Specify the email id on which the test mail can be sent. Click **Send Mail** button to send the test mail.

Once the above settings are done click **Save** button.

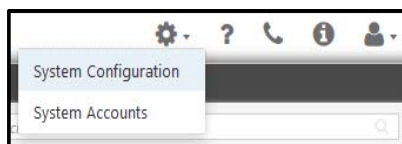
The User needs to start the Alert service by clicking on the **Start Service** button.

General Settings

General Settings allow the Company management administrator to specify the Master Service URL, Admin Portal Service URL and Utility download URL.

Once the service URLs are entered, then the fields shown below will be non-editable.

For General settings click on the option **System Configuration** from the admin menu.



Go to **System Configuration> General Settings**. The page appears as shown below.

A screenshot of the 'System Configuration' page. The page has a dark header with the title 'System Configuration' and a back arrow icon. On the left, there is a sidebar menu with the following items: 'Maintenance Configuration', 'Security', 'SMS Configuration', 'Email Configuration', 'General Settings' (highlighted in blue), 'Multi-Language Configuration', and 'Login Policy'. The main content area contains a list of configuration fields. The first four fields are for Master Service and Admin Portal settings, and the last four are for COSEC and Portal settings. The fields are: 'Master Service URL' (net.tcp://192.168.103.120:15001/MasterService/), 'Master Service Secured URL' (net.tcp://192.168.103.120:15010/MasterService/), 'Master Service Device Listening Port Number' (15005), 'Admin Portal Service URL' (net.tcp://192.168.103.120:14001/ACMSAdminService/), 'Admin Portal Secured Service URL' (net.tcp://192.168.103.120:14010/ACMSAdminService/), 'Admin Portal Web Access Port Number' (14000), 'COSEC Web URL (Internal)' (localhost/COSEC), 'COSEC Web URL (External)' (<Server Address>:< Port>/<Virtual Directory>), 'COSEC Visitor URL (Internal)' (localhost/COSECVisitor), 'COSEC Visitor URL (External)' (<Server Address>:< Port>/<Virtual Directory>), 'Portal Time Zone' ((UTC+05:30) Chennai, Kolkata, Mumbai, New D), and 'Central NTP Server'. At the bottom right, there are 'Save' and 'Cancel' buttons.

When the Master service and Admin Portal service are self-registering, then the URLs of services will be fetched and displayed here.

Master Service URL: This is the URL to access the system where master service is hosted or installed.

Master Service Secured URL: This is the secured URL to access the system where master service is hosted or installed.

Master Service Device Listening Port Number: This is the port number at which device will communicate with Master service.

The device will request to the Master service. The Master service will serve the device either on port 15005 or 15025. So according to the communication between device and master service, the “Master Service Device Listening Port” in General Settings will be updated and displayed in General Settings.

Admin Portal Service URL: This is the URL where the Admin portal service is installed/hosted.

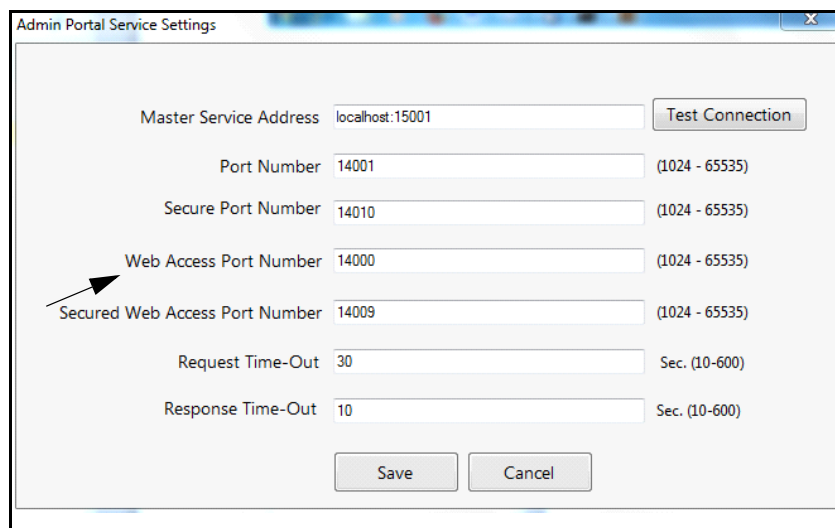
Admin Portal Secured Service URL: This is the secured URL where the Admin portal service is installed/hosted.

Admin Portal Web Access Port Number: This is the port number of the computer at which COSEC Web can access the Admin Portal Service.

The Client accessing COSEC Web does the communication with Admin Portal (say for Licensing purpose) on this Admin portal web access port number.

The COSEC Web will request to the Admin Port Service. The Admin Portal Service will serve the Web on port 14000 or 14009. So according to the communication between Web and Admin Portal, the “Admin Portal Web Access Port Number” port will be updated and displayed in General Settings.

This port can be configured from “Admin Portal Service Settings” as shown below.



COSEC Web URL (Internal): Specify the URL of Internal network for accessing COSEC Web application. Once this URL is entered during installation of setup, then the COSEC Web URL will automatically appear here.

COSEC Web URL (External): Specify the URL of External for accessing COSEC Web application. Once this URL is entered during installation of setup, then the COSEC Web URL will automatically appear here.

COSEC Visitor Portal URL (Internal): Specify the URL of Internal for accessing COSEC Visitor Portal application. Once this URL is entered during installation of setup, then the COSEC Visitor Portal URL will automatically appear here.

COSEC Visitor Portal URL (External): Specify the URL of External network for accessing COSEC Visitor Portal application. Once this URL is entered during installation of setup, then the COSEC Visitor Portal URL will automatically appear here.

Portal Time Zone: It is the time zone of the location where Admin Portal Service is running.



When client (company) is situated in a time zone other than Alert Service's time zone; Alert Service will take company's time zone into consideration while processing scheduled tasks or generating scheduled reports.

For example “[Alert Service](#)”

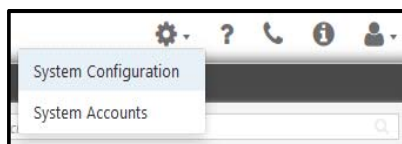
Central NTP Server: Specify the NTP server for the clock synchronization between the systems.

Multi-language Configuration

General Settings allow the Company management administrator to specify the Master Service URL, Admin Portal Service URL and Utility download URL.

Once the service URLs are entered, then the fields shown below will be non-editable.

For configuration of Multi-language click on the option **System Configuration** from the Admin Menu.



Go to **System Configuration > Multi-language Configuration**. The page appears as shown below.

A screenshot of the 'System Configuration' page. On the left, there is a sidebar menu with the following items: Maintenance Configuration, Security, SMS Configuration, Email Configuration, General Settings, Multi-Language Configuration (highlighted in blue), and Login Policy. The main content area on the right is titled 'Multi-Language Configuration'. It contains a checkbox labeled 'Support Multi-Language Input' which is checked. Below it, there is a dropdown menu labeled 'Input Alignment' with 'Left To Right' selected. At the bottom right of this section are 'Save' and 'Cancel' buttons.

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 and storing the same in database will support UTF-8 characters.

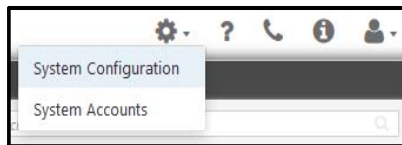
Input From: Select the orientation of multi-language input data from “Left to right” or “Right to left”. **E.g.** If “Right to Left” option is selected, then the input is entered from right side of the textbox and goes to left.

"The list of invalid characters is as follows:

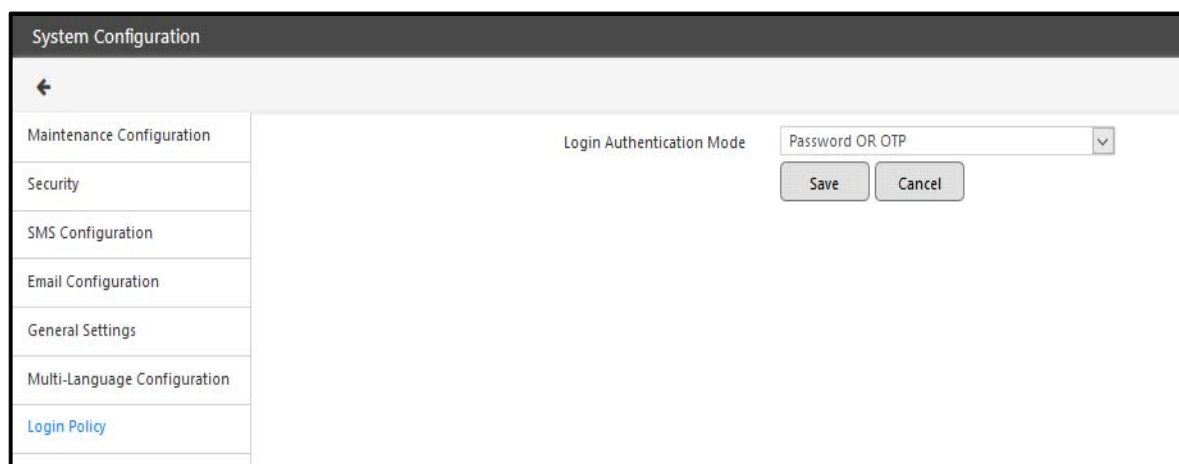
% ^ = ' " { } | ; < > ? & *

Login Policy

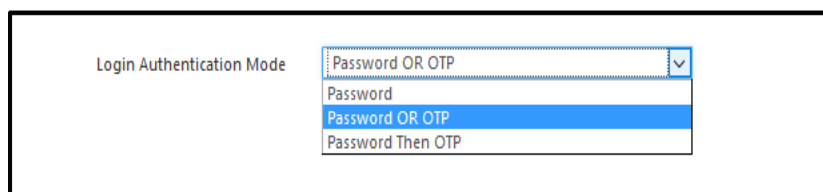
For configuration of Login Policy click on the option **System Configuration** from the admin menu.



Go to **System Configuration> Login Policy**. The page appears as shown below.



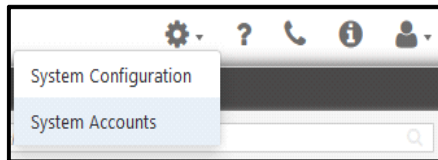
Login Authentication Mode: Select the option to allow users to login into system via Password, Password OR OTP or Password Then OTP.



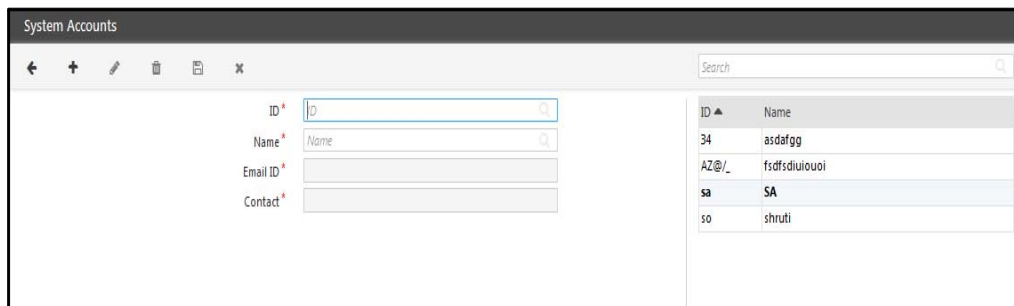
If "Password or OTP" and "Password Then OTP" is selected; then SMS Configuration and or Email Configuration must be done to get OTP on SMS and or Email.

System Accounts

To create the system account users click on the option **System Accounts** from the admin menu.



The System Accounts page appears as shown below.

A screenshot of the 'System Accounts' page. On the left, there is a form to create a new user with fields for ID, Name, Email ID, and Contact. On the right, there is a table listing existing users. The table has two columns: ID and Name. The users listed are: 34 asdafgg, AZ@/_ fsdfsdliuouoi, sa SA, and so shruti. The 'sa' user is highlighted in blue.

ID	Name
34	asdfgg
AZ@/_	fsdfsdliuouoi
sa	SA
so	shruti

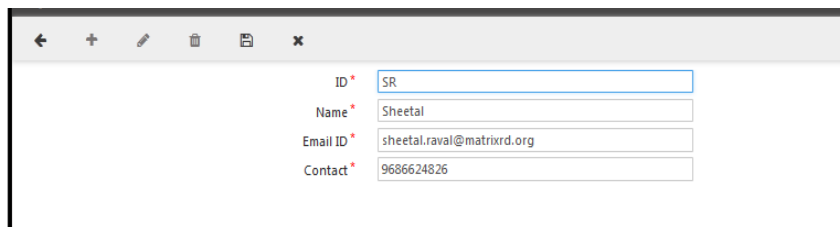
Click on **New** to create new system account user.

ID: Enter the ID of the user.

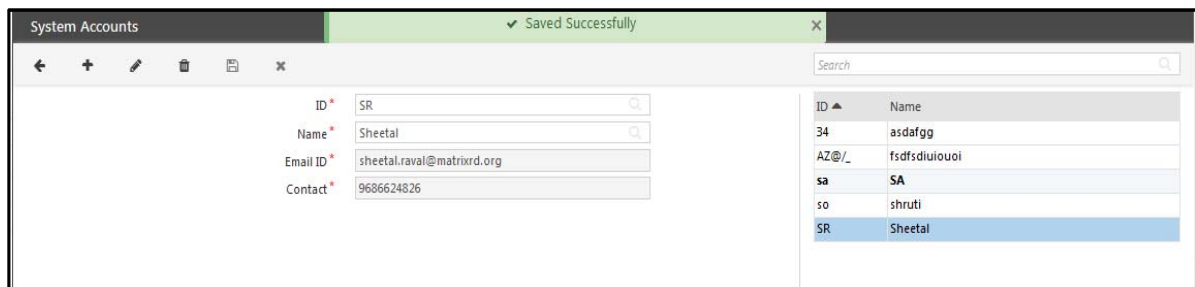
Name: Enter the name of the user.

Email ID: Enter the Email ID of the user.

Contact: Enter the Contact number of the user.

A screenshot of the 'System Accounts' page with the form filled out. The ID field contains 'SR', the Name field contains 'Sheetal', the Email ID field contains 'sheetal.raval@matrixrd.org', and the Contact field contains '9686624826'. The 'New' button is visible at the bottom right of the form.

Click **Save** button to save the system account user.

A screenshot of the 'System Accounts' page after saving a new user. A green banner at the top says 'Saved Successfully'. The form on the left still shows the details of the user 'SR'. The table on the right now includes the new user 'SR Sheetal' at the bottom, highlighted in blue.

ID	Name
34	asdfgg
AZ@/_	fsdfsdliuouoi
sa	SA
so	shruti
SR	Sheetal

Help, Contact, About Us

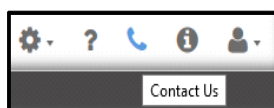
Help

To view the Help manual of Admin Portal; click on the **Help** option from the admin menu. The pdf manual will open which will guide you for the management of portal.

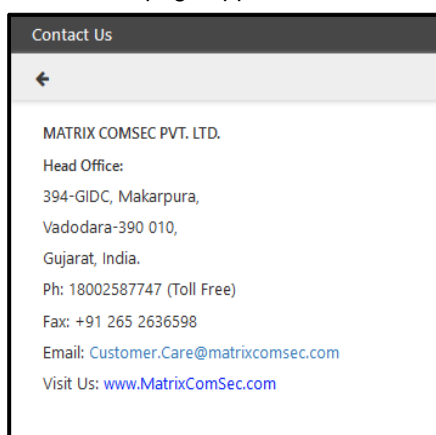


Contact Us

To view the Contact details of Matrix Comsec Pvt. Ltd.; click on the **Contact Us** option from the admin menu.



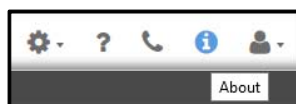
The Contact Us page appears as shown below.



The Address and phone number details are displayed. You can visit the matrix website by clicking on Visit Us link.

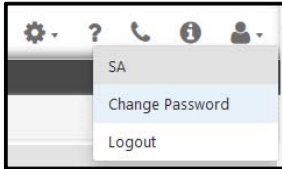
About

To view the version and product details of software; click on the **About** option from the admin menu.

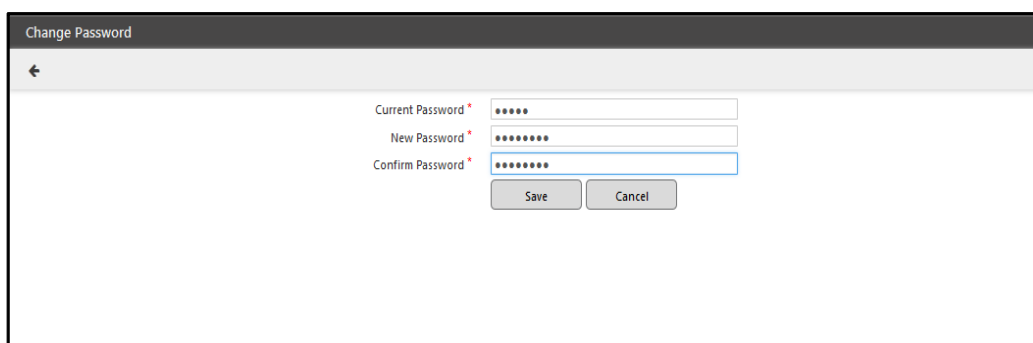


Change Password

To change the login password of Admin Portal click on the option **Change Password** from the admin menu



The Change Password page appears as shown below.

A screenshot of the 'Change Password' page. The page has a dark header with the title 'Change Password' and a back arrow icon. Below the header, there are three input fields, each with a red asterisk indicating a required field. The first field is labeled 'Current Password' and contains six dots. The second field is labeled 'New Password' and contains eight dots. The third field is labeled 'Confirm Password' and contains eight dots. Below the input fields are two buttons: 'Save' and 'Cancel'.

Enter the **Current Password** of the Admin Portal.

Enter the **New Password** to be updated.

Re-enter the New Password for confirmation.

Click on **Save** to save the changes.



MATRIX COMSEC

Head Office:

394-GIDC, Makarpura, Vadodara - 390010, India.

Ph: (+91)18002587747

E-mail: Tech.Support@MatrixComSec.com

www.MatrixSecuSol.com