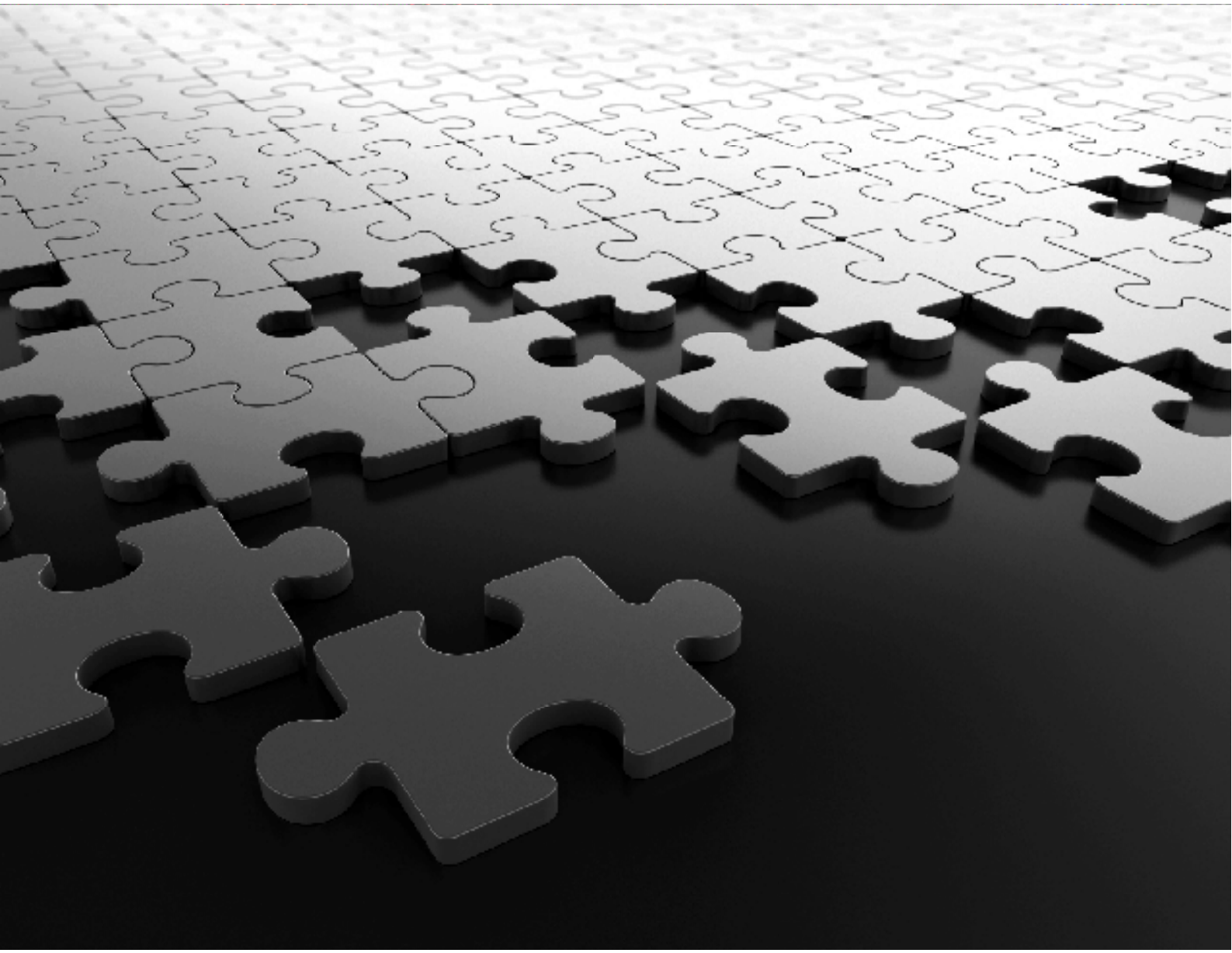
Admin Management Portal
User Manual



MATRIX
SECURITY SOLUTIONS

MATRIX
SECURITY SOLUTIONS

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:
www.matrixcomsec.com

Copyright

Version 26
Release date: May 15, 2024

Contents

CHAPTER 1

Introduction

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

CHAPTER 2

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 to the desired — Device Based, Server Based or Virtual License.

If you change the License Verification Mode from Dongle based to Virtual License, it will remove all details associated with the previous license mode permanently. The server will only function with the newly configured license verification mode.

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 the modes- Dongle on Server, Dongle on Device or Virtual License.
- On Premise- Responsible for COSEC DB upgrade as well.
- Responsible for Admin Portal DB Upgrade.

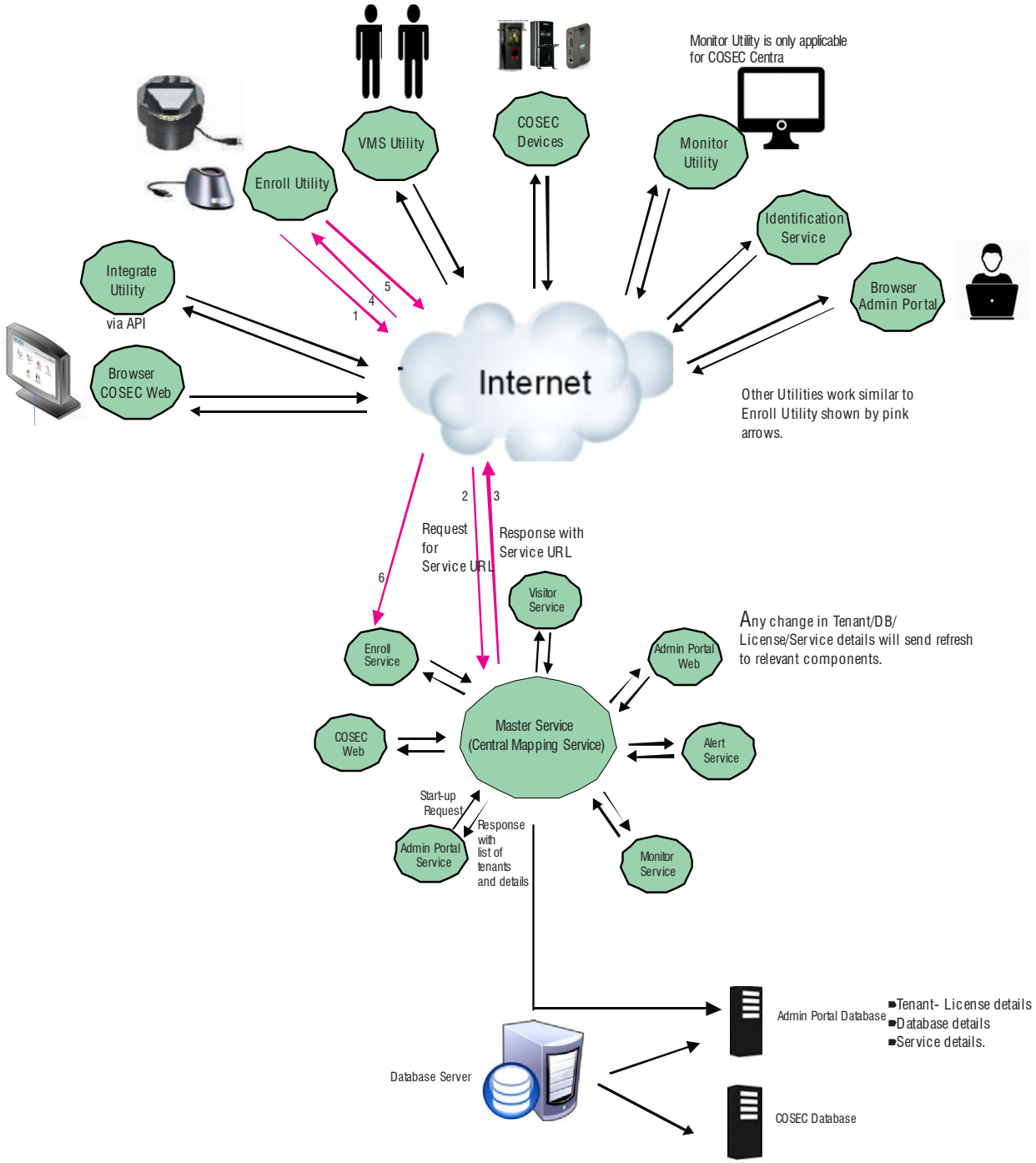
Admin Portal Service is required for following functions:

- 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.

For details and configuration of the various services — Alert Service, Enroll Service, Monitor Service, Visitor Service, refer to *"COSEC Services".*

System Architecture



CHAPTER 3

Software Installation

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.

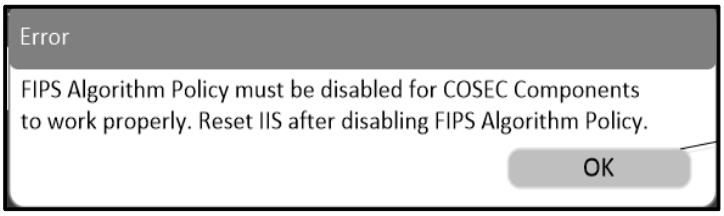
- Database upgrade (COSEC DBs)
- Post, Retrieve and Remove records.

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.

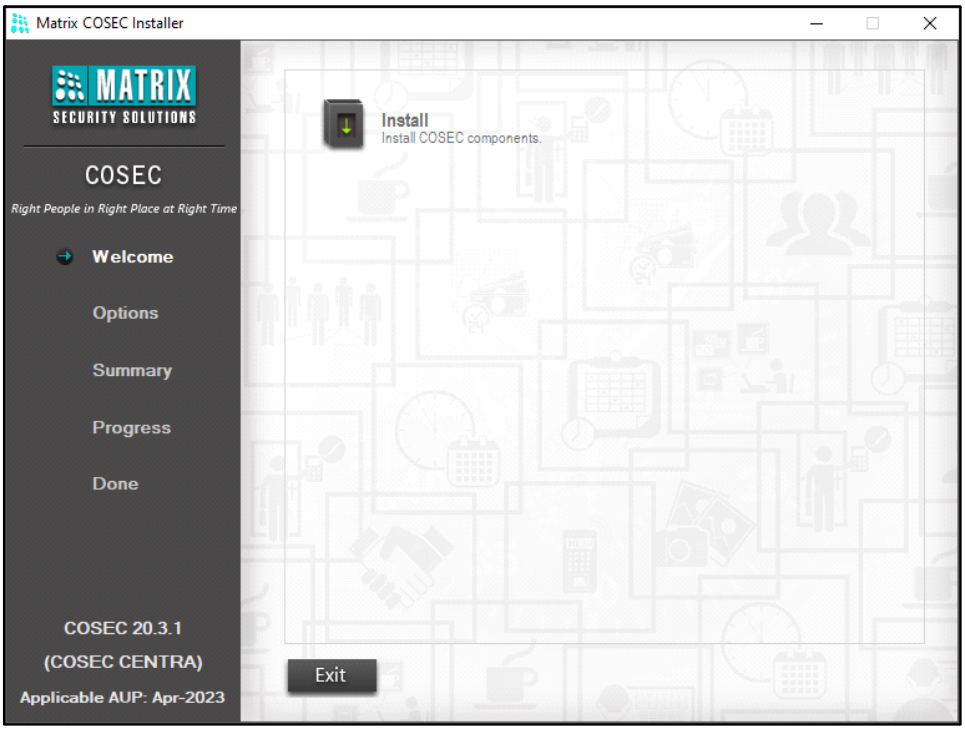


To disable FIPS Algorithm policy go to Registry Editor by typing regedit from the start menu of your computer.

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.

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

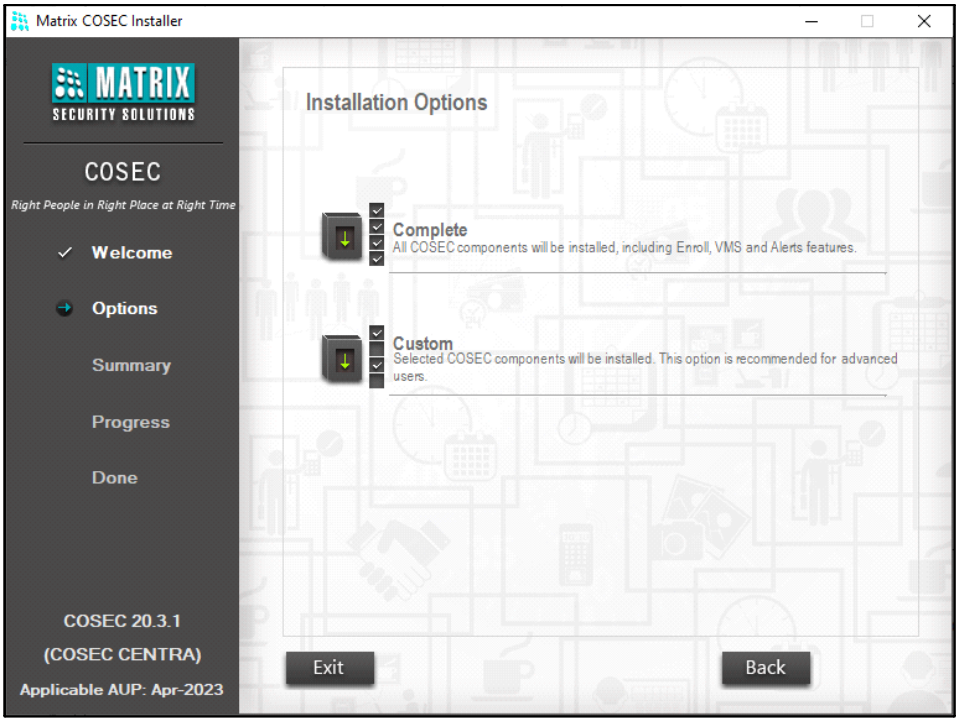


This Installer automatically checks the computer for the prerequisites required for the installation of the applications prior to starting the installation process. Prior to running the Installer utility it is necessary to ensure that the logged in user has administrator rights on the computers where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

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

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

- Click the check box to accept the Terms and Conditions in the License Agreement and click **Next**. The window appears with the following installation options:



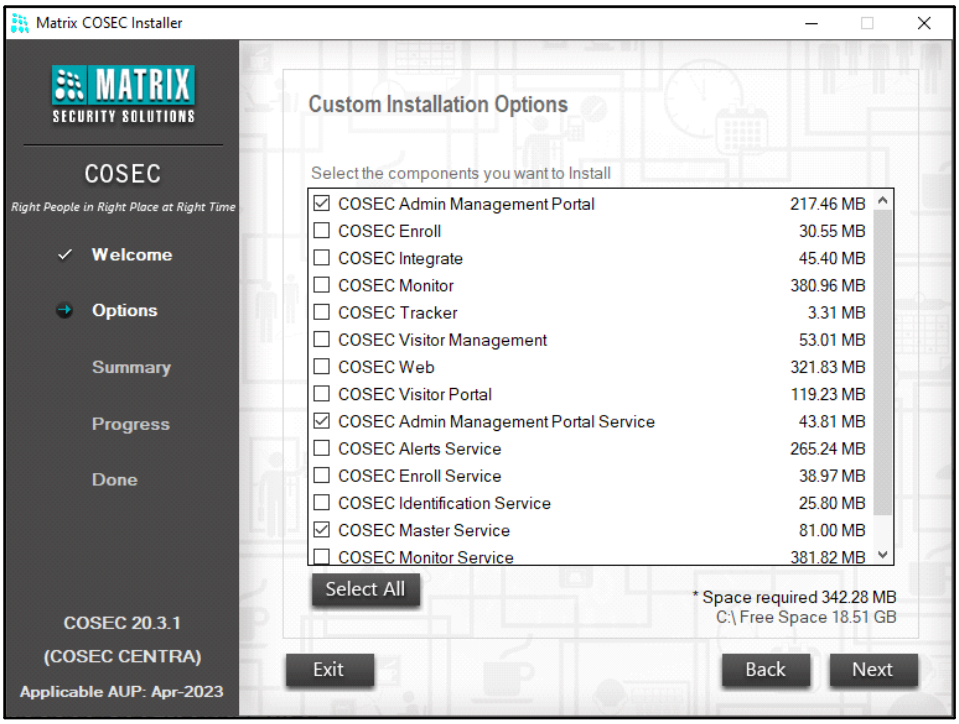
- Select either **Complete** or **Custom** depending on your preferred type of installation.

  Select **Complete** to install all the components of the COSEC application.

  Select **Custom** to install the selected components of the COSEC application.

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

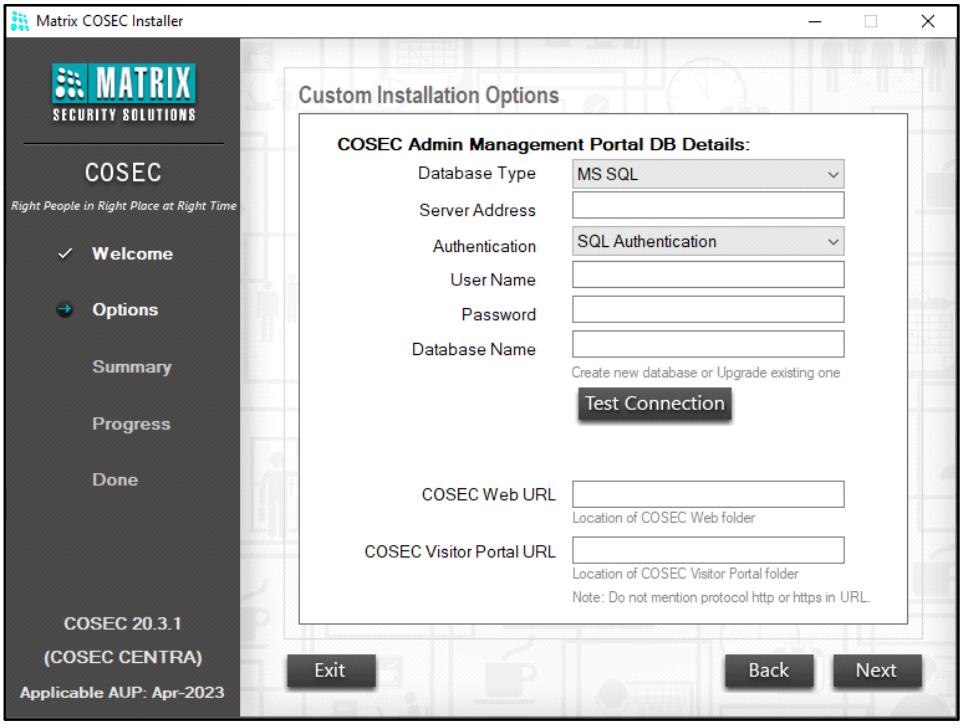
- Select the components you wish to install.



- Click **Next**. The Database creation page appears from where you can configure Admin Management Database and COSEC Database.

COSEC Admin Management Portal DB Details

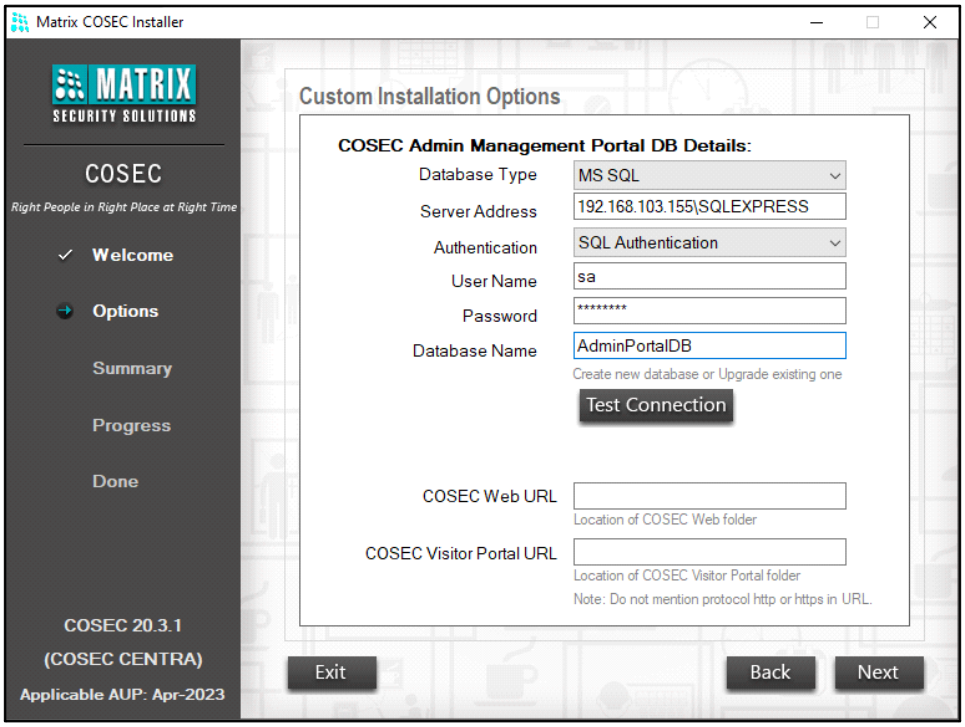
Enter the details to configure Admin Management Portal Database.



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

MS SQL Database Type

If you select **MS SQL** as the **Database Type**, configure the following parameters:



Server Address: Enter the Server Address where the database of Admin Management Portal is to be created. For example: 192.168.103.155\SQLEXPRESS.

Authentication: Select the desired authentication type — SQL Authentication or Windows Authentication**.**

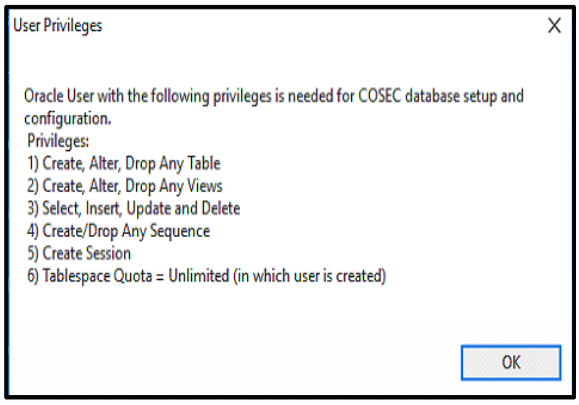
- If you select Authentication Type as **SQL Authentication**, configure the following:
  - **User Name:** Specify the user name as created during sql server instance. For example: sa
  - **Password:** Specify the password as created during sql server instance. For example: matrix_1
- If you select Authentication Type as **Windows Authentication**, you do not need to configure any parameter.

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

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

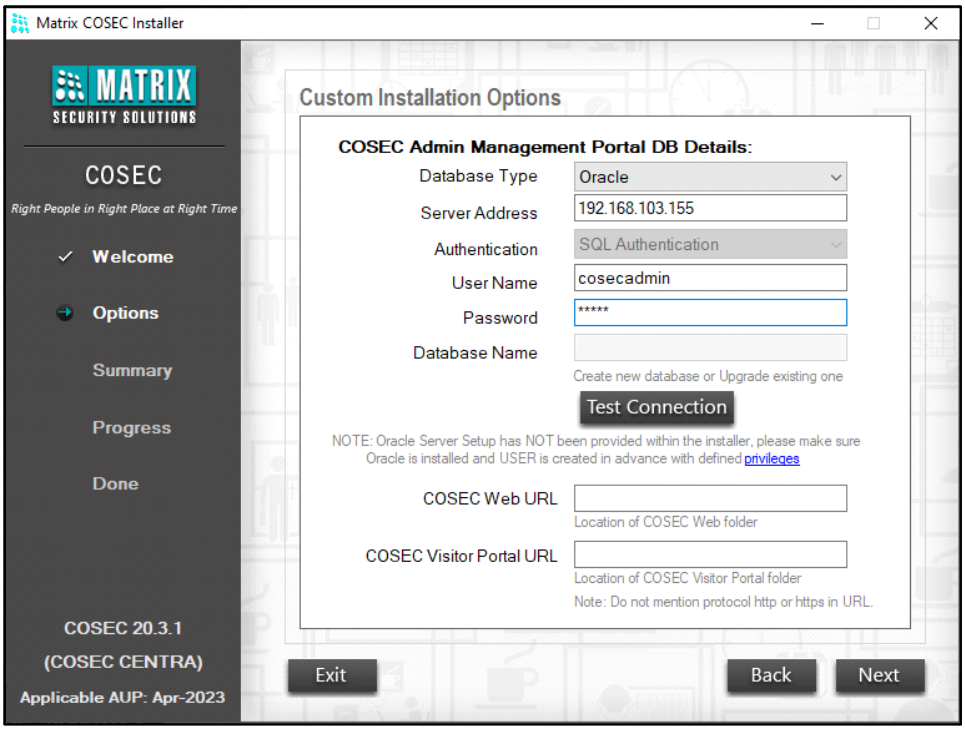
Oracle Database Type

Make sure you have created the user in ORACLE will following privileges.



For details, refer to Installing Prerequisites > Oracle Installation in the COSEC Software Installation Guide.

If you select **Oracle** as the **Database Type**, configure the following parameters:



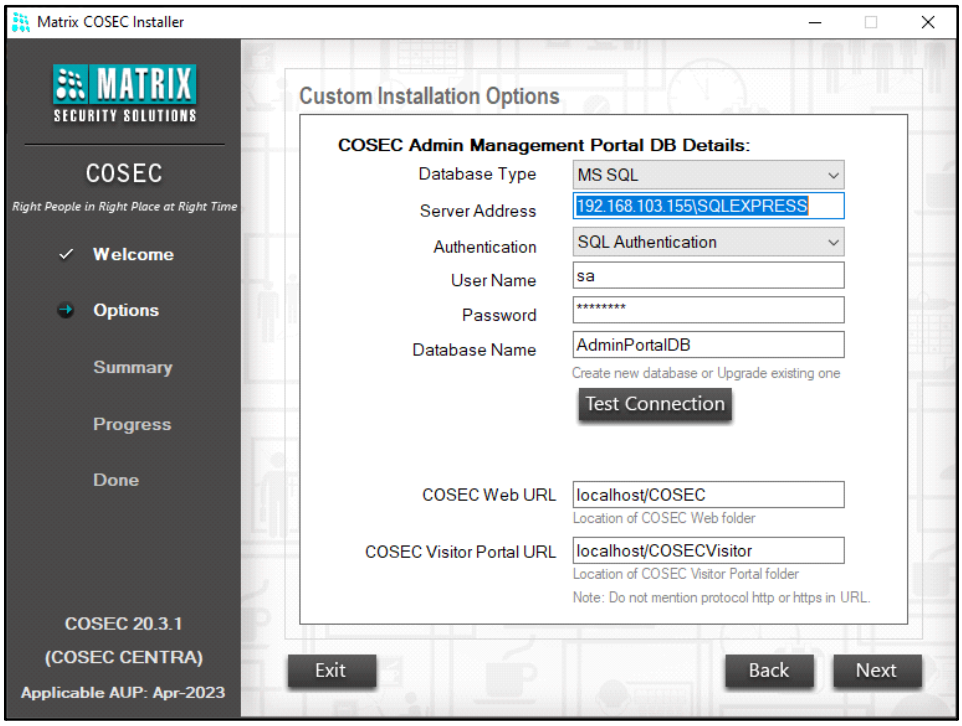
Server Address: Enter the Server Address where the database of Admin Management Portal is to be created. For example: 192.168.104.23.

User Name: Specify the user name as the name of the user created from Oracle system. For example: cosecadmin

Password: Specify the password as created while creating the user in Oracle. For example: admin

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

If you have selected Database Type as **MS SQL** or **Oracle**, configure the following parameters:



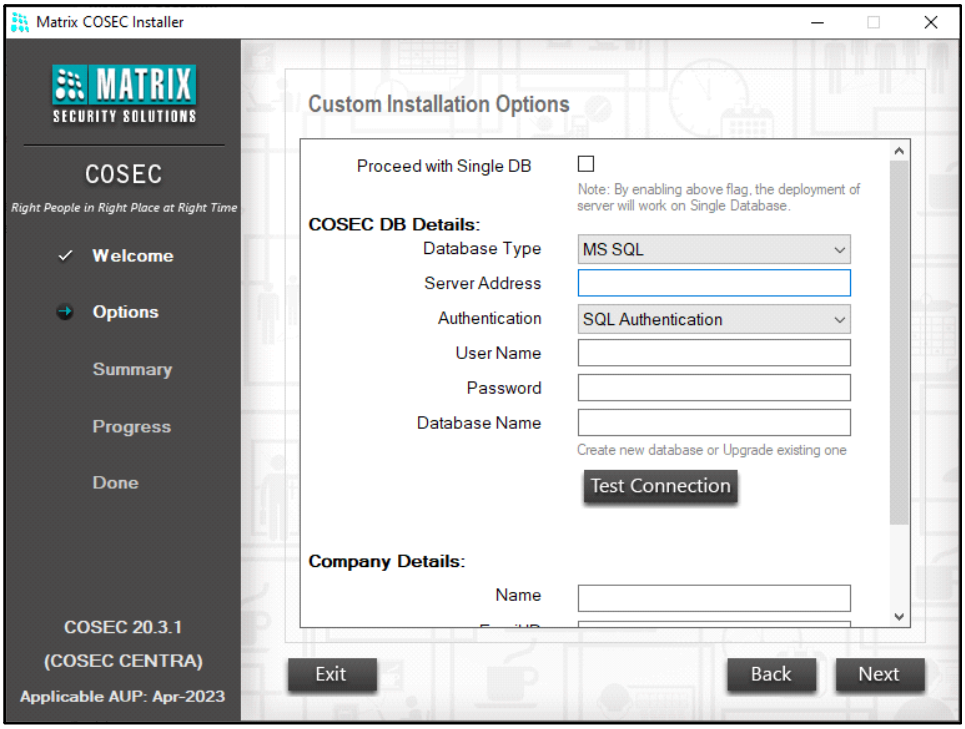
COSEC Web URL: Enter the URL through which COSEC Web is to be accessed. If you are installing COSEC Web in PC2 and accessing from PC1; then give IP of PC2 where Web is installed. If Web is to be accessed locally then IP or localhost can be given in URL.

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

Now click on **Next** button.

COSEC DB Details

Configure the parameters for COSEC Database.

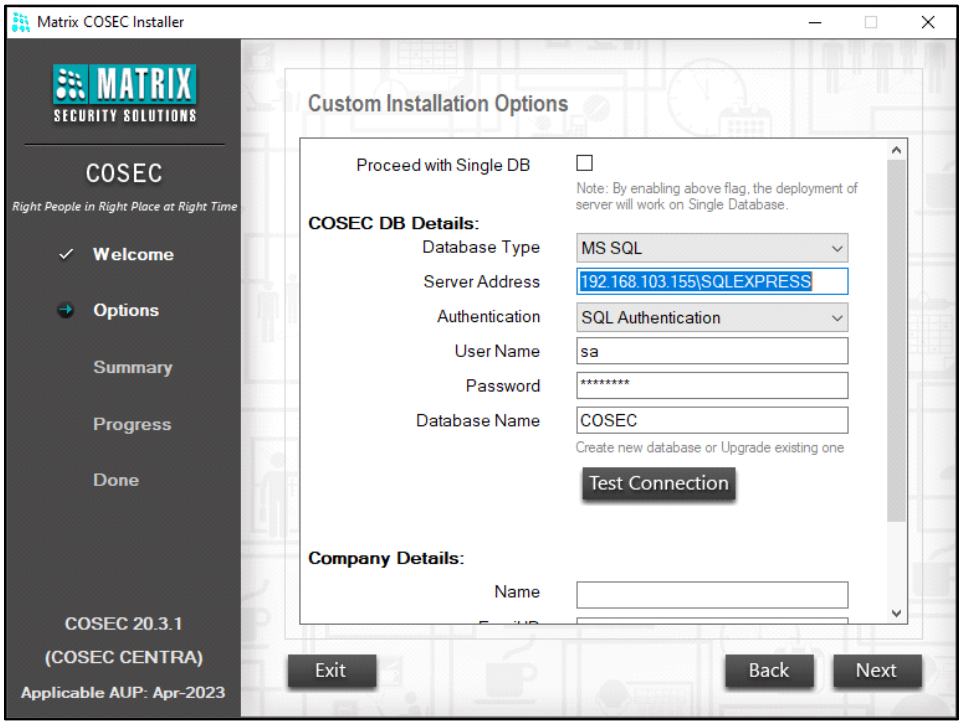


Proceed with Single DB: Select this check box to complete the installation with creation of single database for Admin Portal and COSEC. The details will be auto-filled as configured under **COSEC Admin Management Portal DB Details**.

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

MS SQL Database Type

If you select **MS SQL** as the **Database Type**, configure the following parameters:



Server Address: Enter the Server Address where the database of Admin Management Portal is to be created. For example: 192.168.103.155\SQLEXPRESS.

Authentication: Select the desired authentication type — SQL Authentication or Windows Authentication**.**

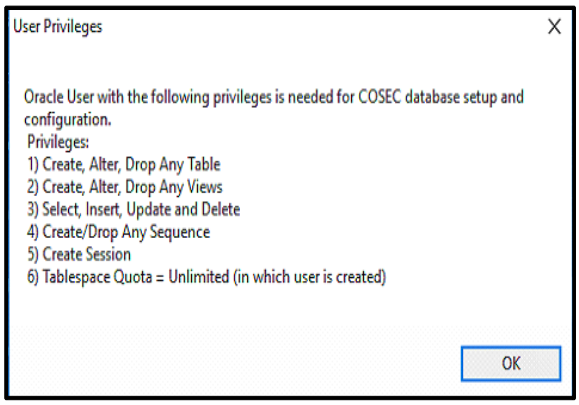
- If you select Authentication Type as **SQL Authentication**, configure the following:
  - **User Name:** Specify the user name as created during sql server instance. For example: sa
  - **Password:** Specify the password as created during sql server instance. For example: matrix_1
- If you select Authentication Type as **Windows Authentication**, you do not need to configure any parameter.

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

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

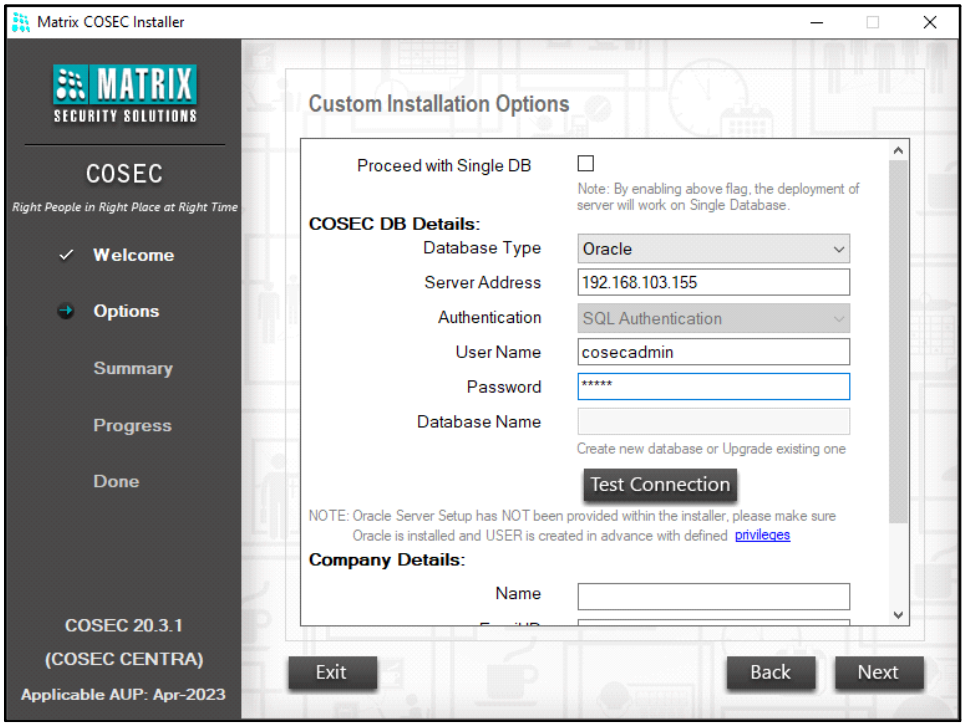
Oracle Database Type

Make sure you have created the user in ORACLE will following privileges.



For details, refer to Installing Prerequisites > Oracle Installation in the COSEC Software Installation Guide.

If you select **Oracle** as the **Database Type**, configure the following parameters:



Server Address: Enter the Server Address where the database of Admin Management Portal is to be created. For example: 192.168.103.155.

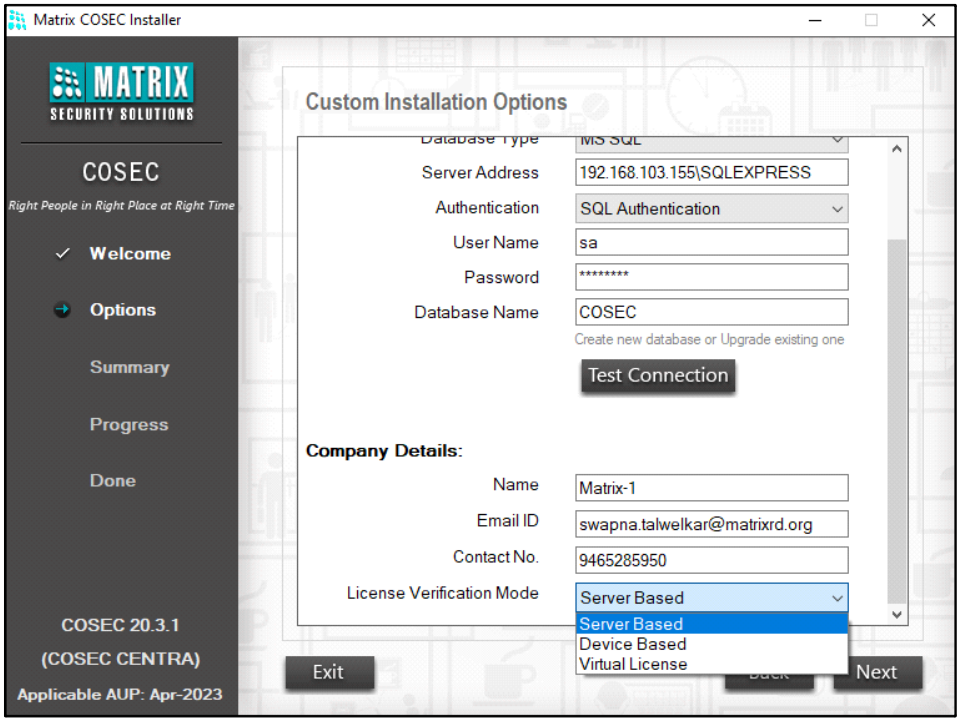
User Name: Specify the user name as the name of the user created from Oracle system. For example: cosecadmin

Password: Specify the password as created while creating the user in Oracle. For example: admin

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

Company Details

If you have selected Database Type as **MS SQL** or **Oracle**, configure the following parameters:



Name: Enter the name of the company which will be created by default in the Admin Management Portal.This Name will appear in the Admin Management Portal > Company Configuration > Profile.

Email ID: Enter the Email ID of the company. This Email ID will appear in the Admin Management Portal > Company Configuration > Profile > Contact Details.

Contact No: Enter the Contact Number of the company. This Contact No. will appear in the Admin Management Portal > Company Configuration > Profile > Contact Details.

License Verification Mode: Select the License Verification Mode as **Server Based** or **Device Based** or **Virtual License.**

The License Verification Mode selected here will be set automatically in **Company Configuration > Profile**.

License Verification Mode

- If you select **Server Based,** License will be verified from the Dongle connected to the PC where Master Service is installed. For details refer to “Server Based”
- If you select **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. For details refer to “Device Based”

For Device Based License Verification, the devices — VEGA, ARGO, ARGO FACE Direct Doors and Panel lite V2/Panel200 in Server Mode — can be used.

*Make sure you have a **COSEC CENTRA** connection mode and the devices are configured in the same application.*

- If you select **Virtual License**, the License will be verified thorough the Virtual License Manager Server. For details refer to "Virtual License".

You can opt for Virtual License in the following scenarios:
- *Fresh installation of COSEC CENTRA. For details, refer to "Virtual License".*
- *You already have a Dongle License but you wish to migrate to Virtual License. For details contact Matrix Support Team.*

Server Based

Make sure the License Dongle is connected in the USB port of the computer where the Master Service is running. Master Service checks for the presence of this License Dongle. If the Dongle is available, then the Master Service sends the Refresh command to all other services. Also make sure the License Verification Mode is configured as Server Based.

The Dongle only has the GENERIC License. You need to purchase and update the licenses as per your requirement, click **Company Configuration > License and Services**.For details, refer to "Supported Licenses" and "License and Services".

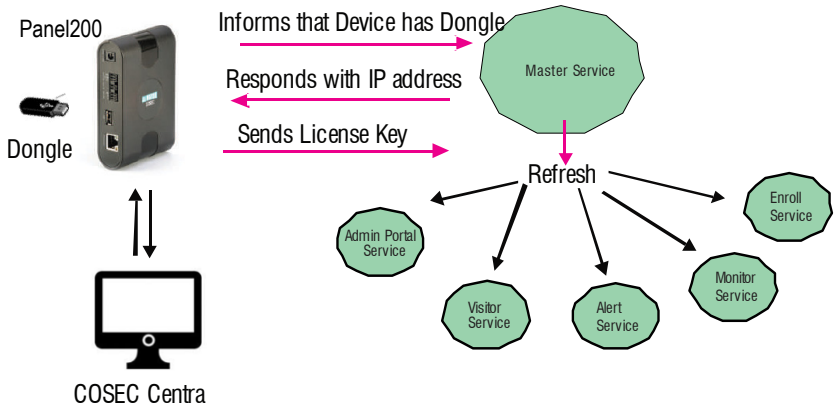
Device Based

In Device Based licensing VEGA, ARGO, ARGO FACE Direct Doors or Panel200 (Server Mode) can be used. Also make sure the Tenant/ Company is configured with License Verification Mode as Device Based.

Make sure the License Dongle is connected to the desired device.The **MAC Address** of this device will be displayed in **Company Configuration > Profile**.

The Dongle only has the GENERIC License. You need to purchase and update the licenses as per your requirement, click **Company Configuration > License and Services**. For details, refer to "Supported Licenses" and "License and Services".

Let us understand this with the help an example:
- The device (in this case Panel200) sends information to the Master Service that device has the 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 the same to the 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 be refreshed.

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

In the Server Settings of Panel200;

- *enter the URL for COSEC Centra Server as the IP Address of the computer where Monitor Service is running.*
- *enter the License Server URL as the IP Address of the computer where Master Service is running.*

Virtual License

With the introduction of Virtual License, the need of a Dongle is eliminated, but you need to make sure you have:

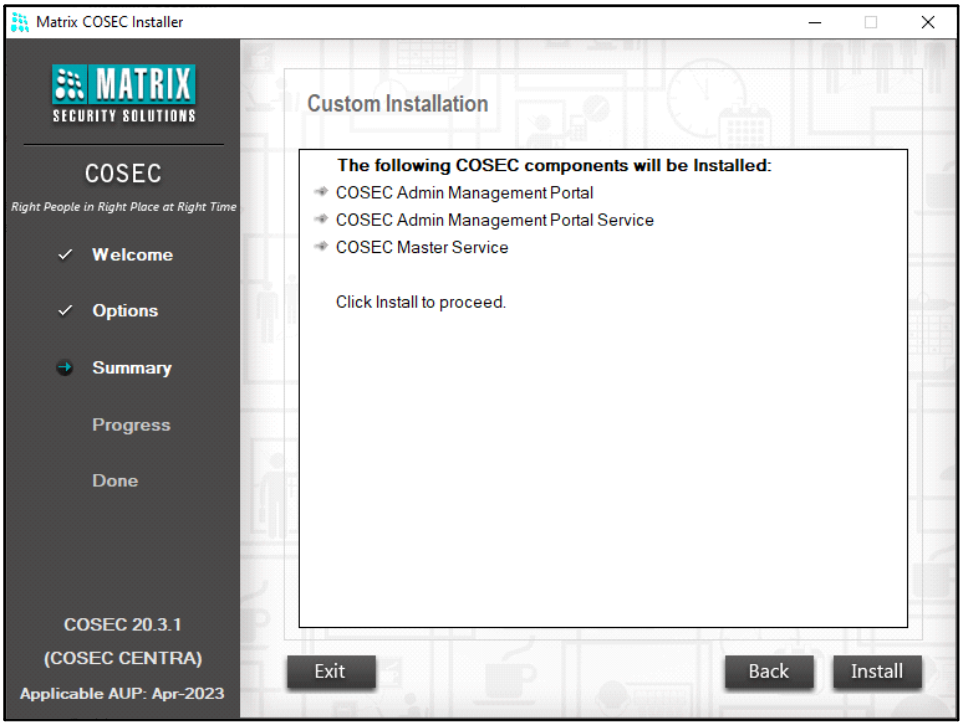
- Persistent Internet connection with good speed (where Master Service is running).
- Received the MATRIX VIRTUAL DONGLE300 Key in PDF form.
- Received the COSEC CENTRA PLATFORM Key in PDF form.
- Received the desired module activation License Keys in PDF form.

You need to purchase these keys. For details, refer to “Supported Licenses”.

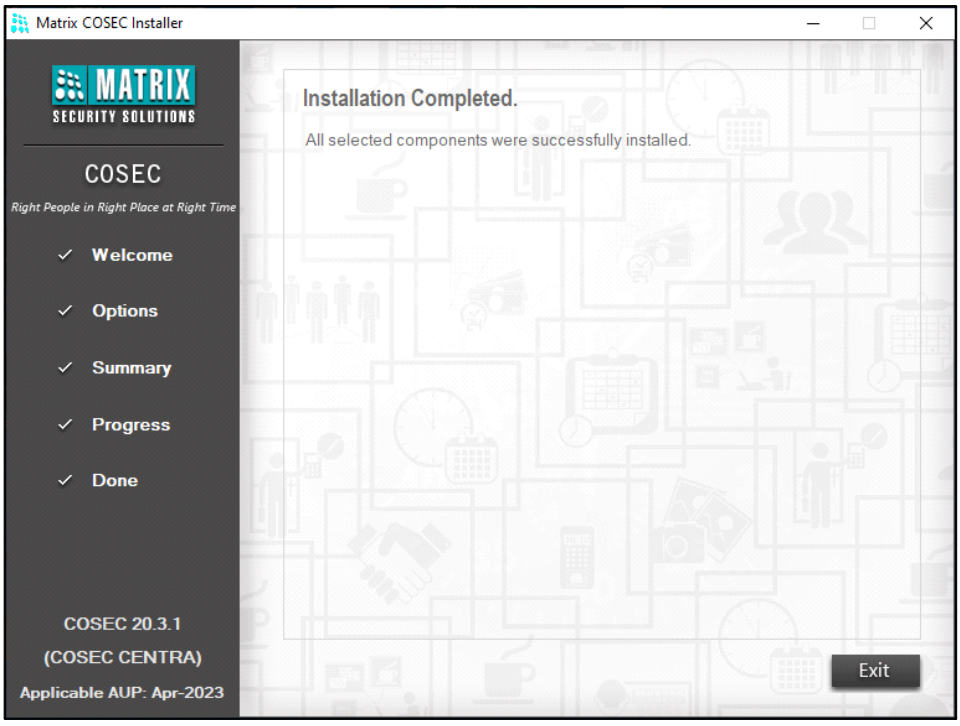
Once the key PDF’s are received you need to register the MATRIX VIRTUAL DONGLE300 Key. For details, refer to “License and Services”.

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.



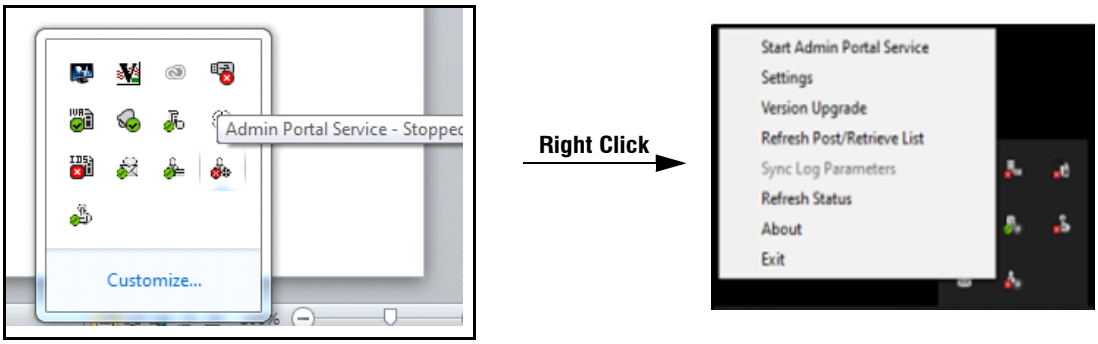
- After the successful installation of COSEC Admin Management Portal, Installation Completed window appears. Click **Exit**.



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.

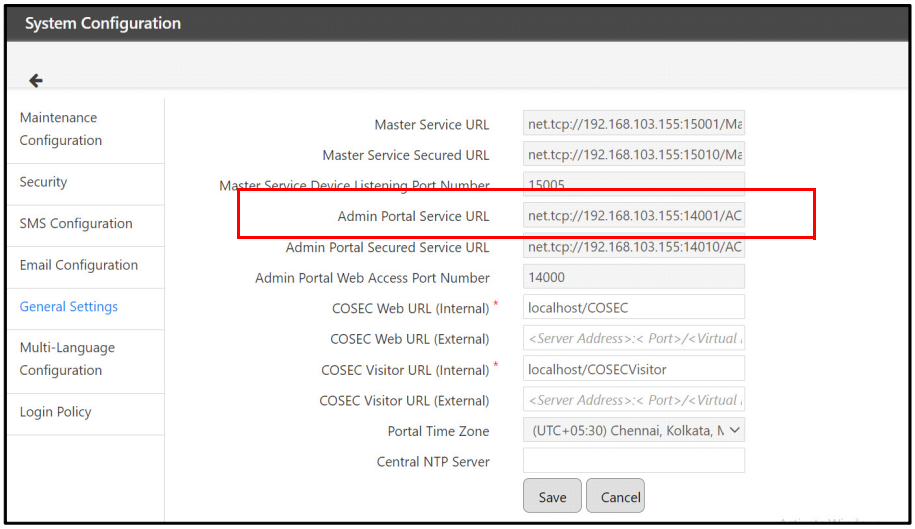
Right click on this  icon.



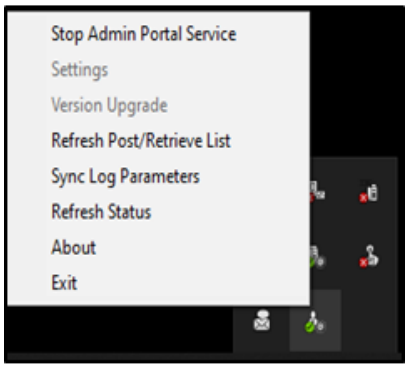
The options displayed are — Start/Stop Admin Portal Service, Settings, Version Upgrade, Refresh Post/Retrieve List, Sync Log Parameters, Refresh Status, About and Exit.

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.



- 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**.

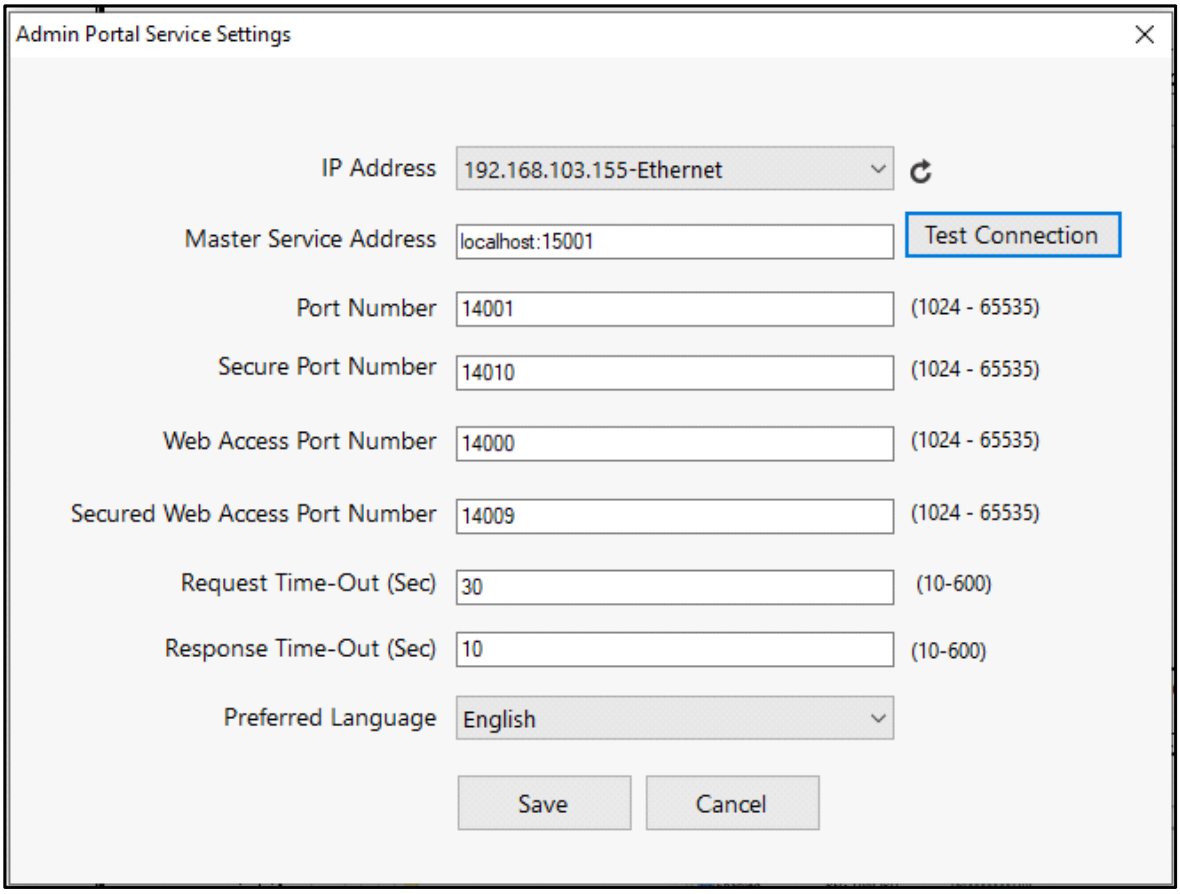
When service is running and Admin database loses connectivity or is unavailable then the service will keep running for 24 hours by default after which it will stop.

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.

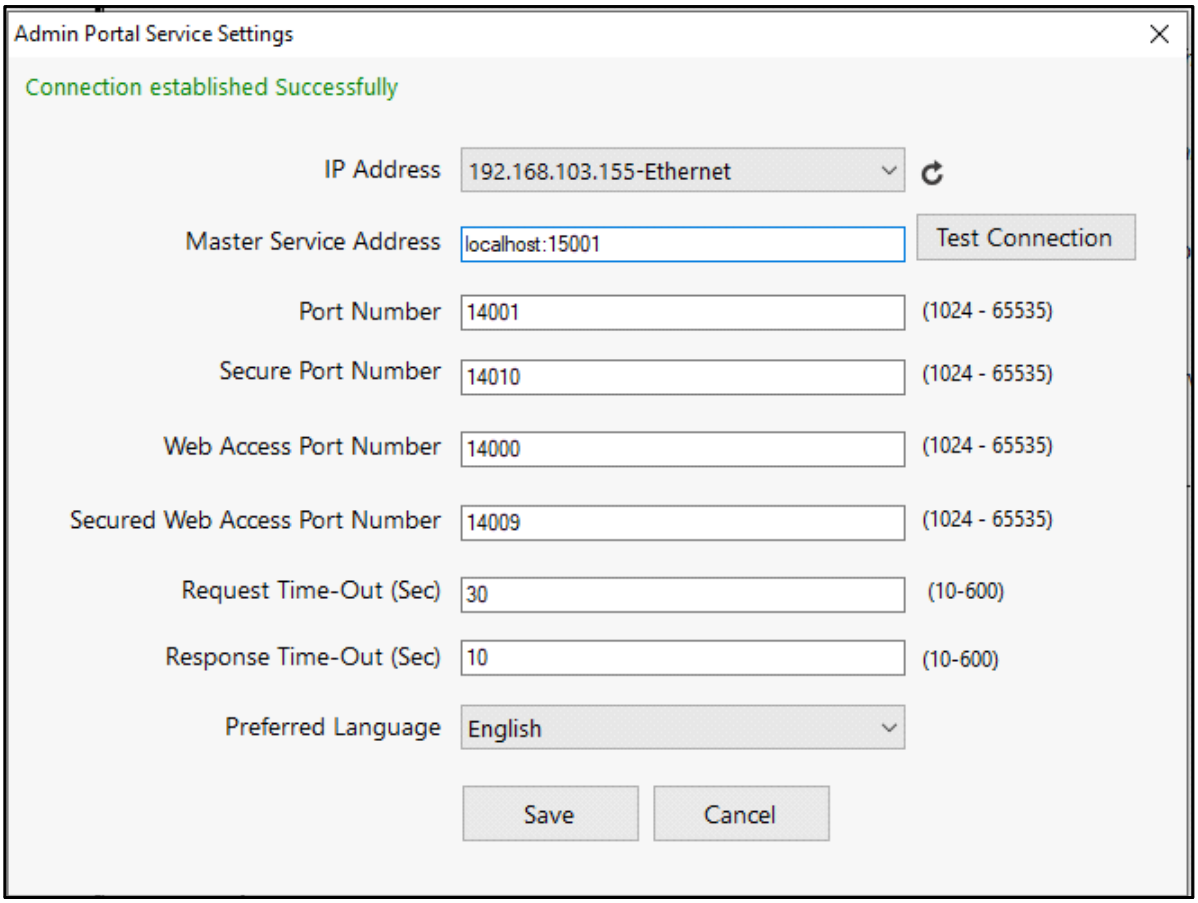
If the PC is assigned a DHCP Addressing scheme, then whenever the IP Address changes, the same will be updated against every service.

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.

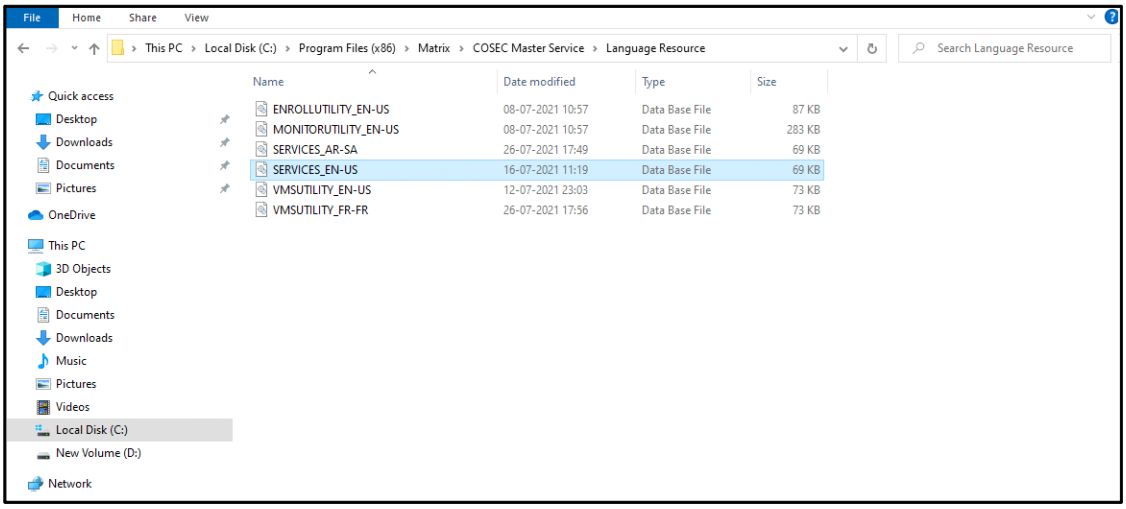
  On changing or updating the Master Service Address, connection with the Master Service must be tested.

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



- **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.

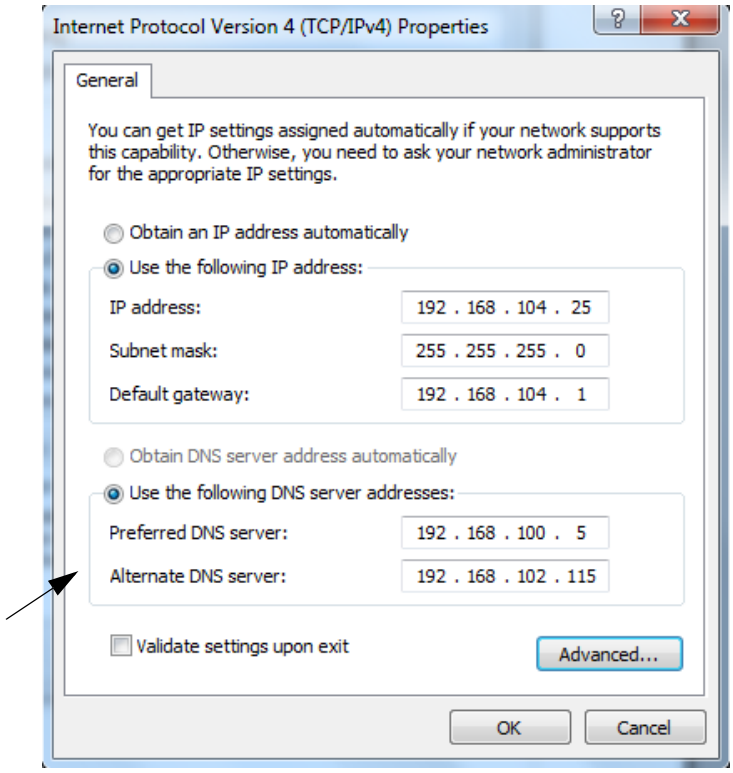
If you prefer a different language other than the default language file (i.e. English), you can translate this default language into the desired language with the help of COSEC Multi-Language Utility. To know more, refer to the Multi-Language Utility User Guide.

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

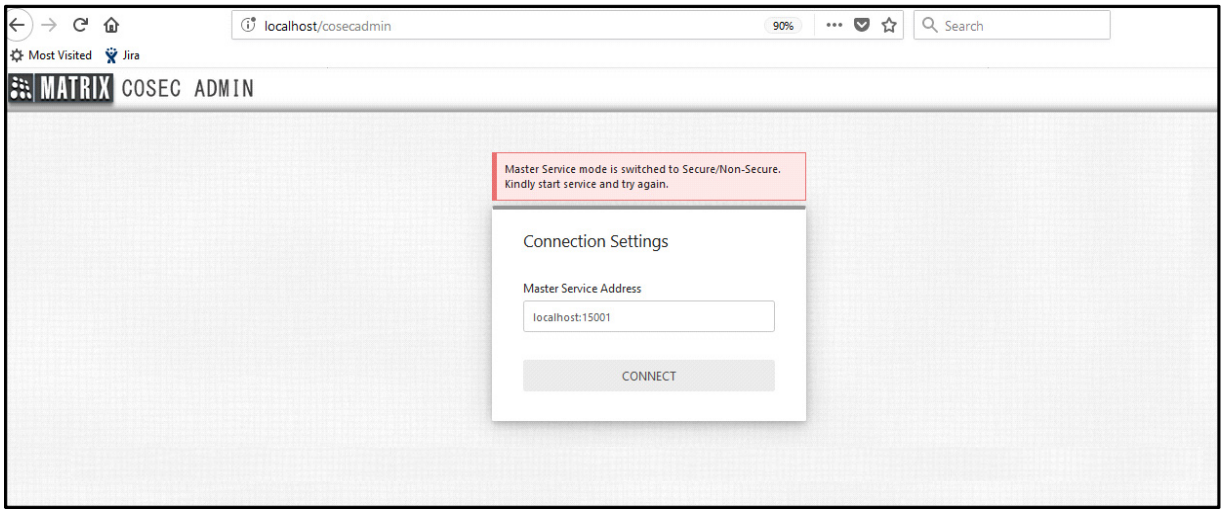
If the network where portal is installed and the PC from where the Portal is being used are in different network then make sure that “Alternate DNS server” is configured with the IP address where you have installed the Portal.

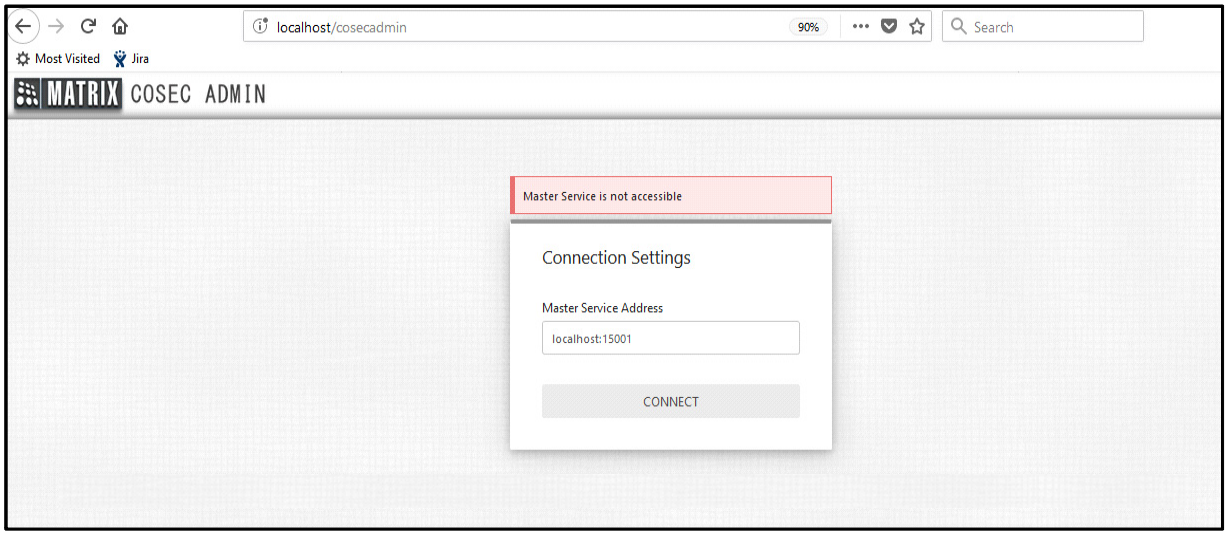


LOGIN

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

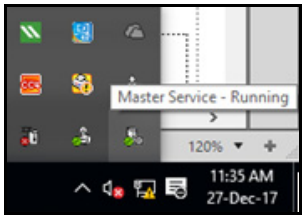
- The Connection Settings page will appear as shown below:





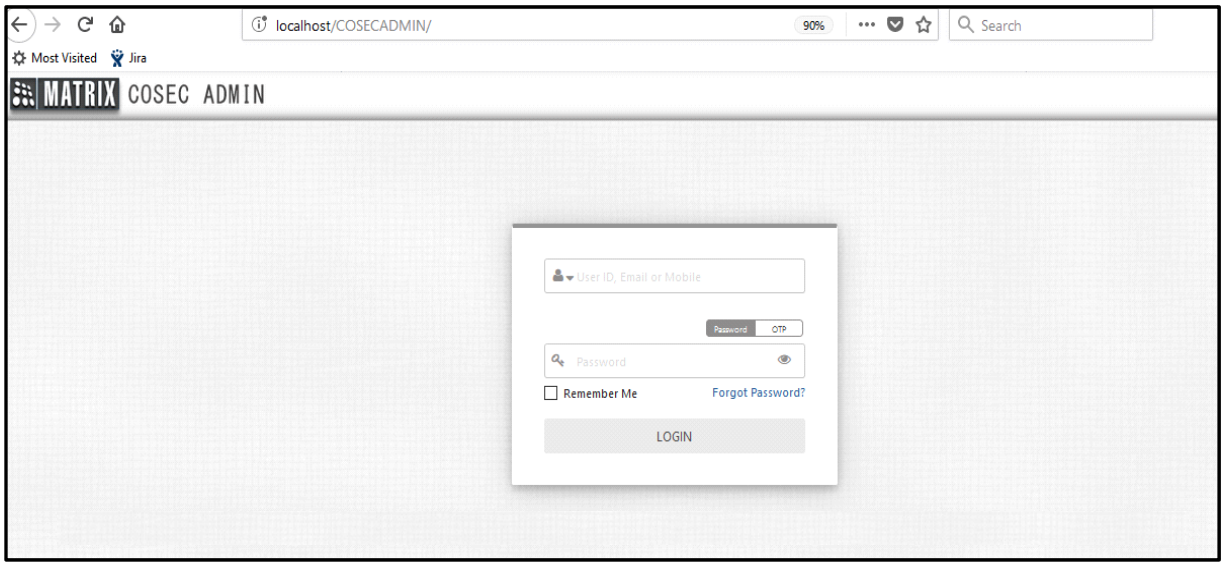
Enter the **Master Service Address** to connect with the database and click **Connect.** The Admin Portal will get connected with its database through the Master service.

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.

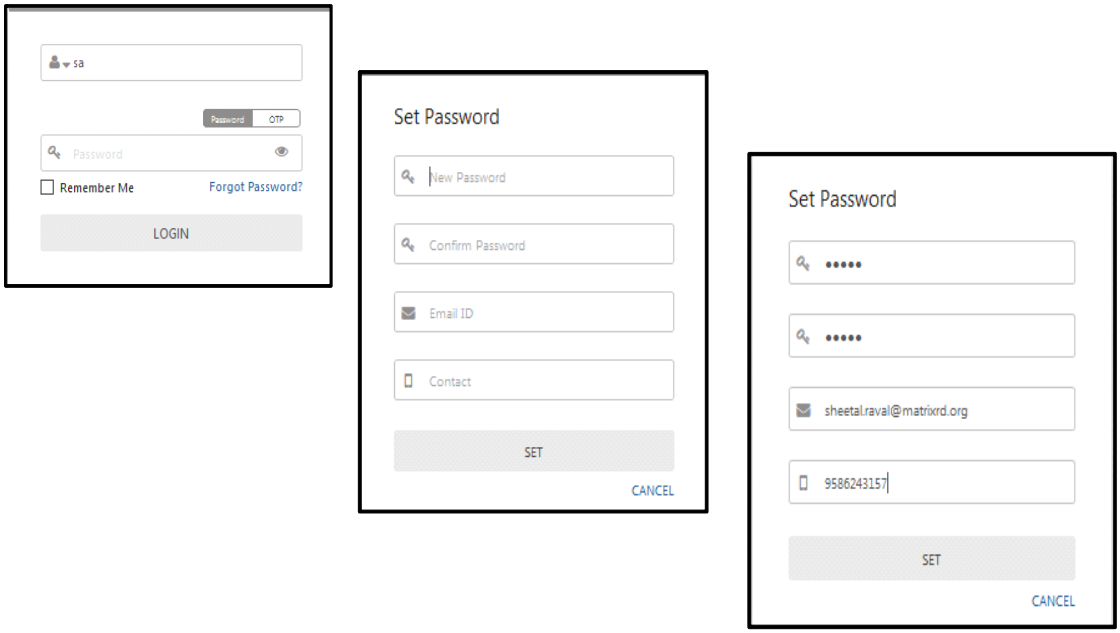


The Login page appears as shown below. Enter the Login ID and Password. When you are login for the first time, you will have to set the password.

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



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.



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 31.
You must ensure that the Login ID being used has the respective correct icon.See “Icon of Login ID” on page 30.

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.

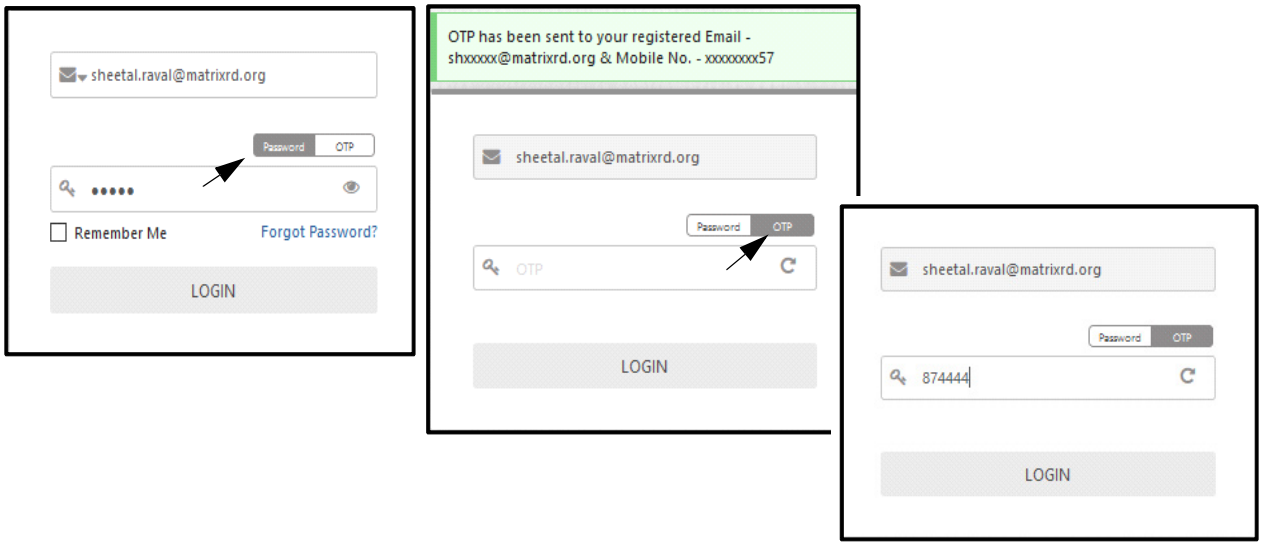
User ID with Password or OTP

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.

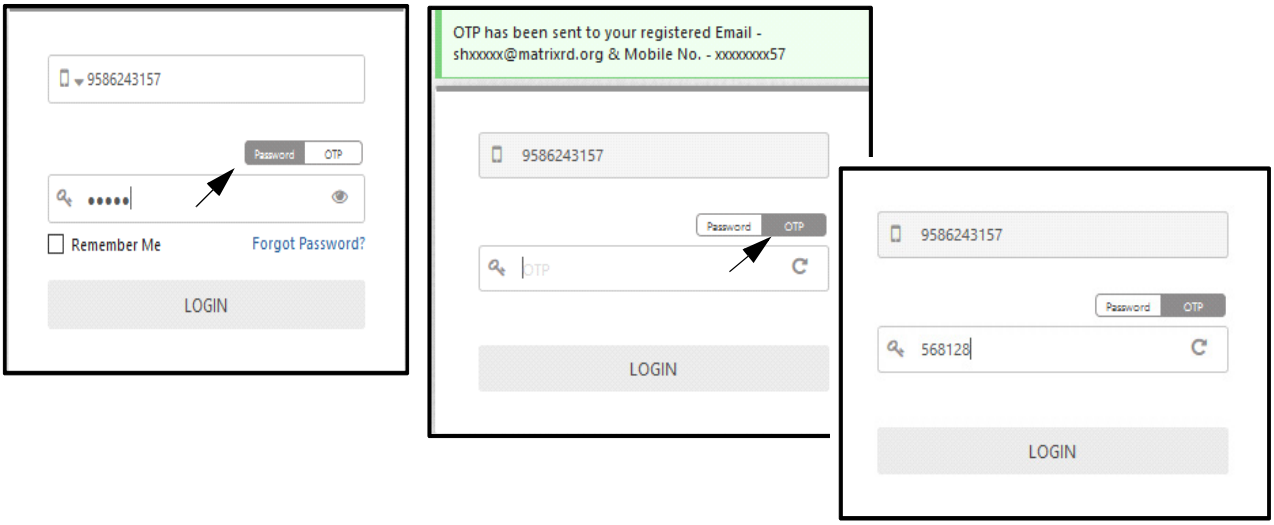
You can click on **Resend OTP** button if OTP is to be sent again.

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.



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.



Password Then OTP

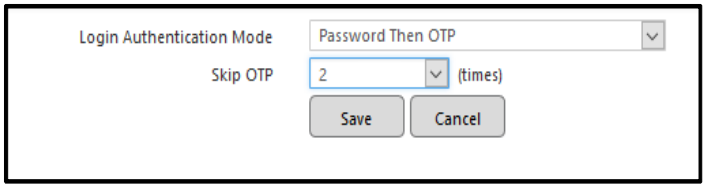
In this authentication you have to enter both Password and then OTP for accessing Admin Portal.

User ID with Password Then OTP

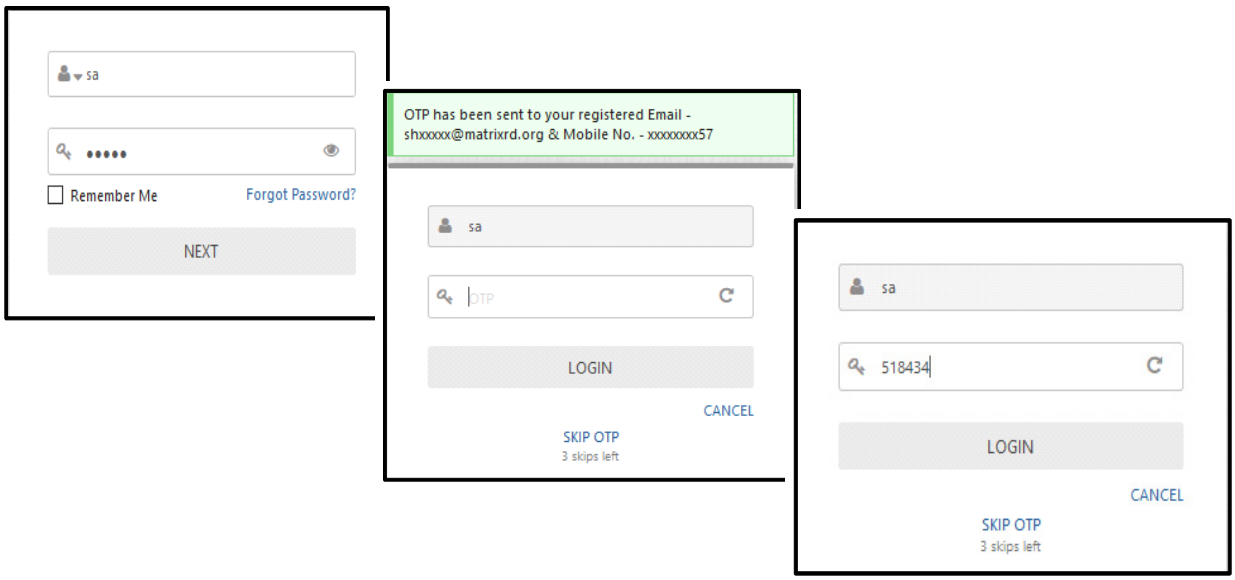
Enter the User ID of login user. Then enter the password and click **Next** button.

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.



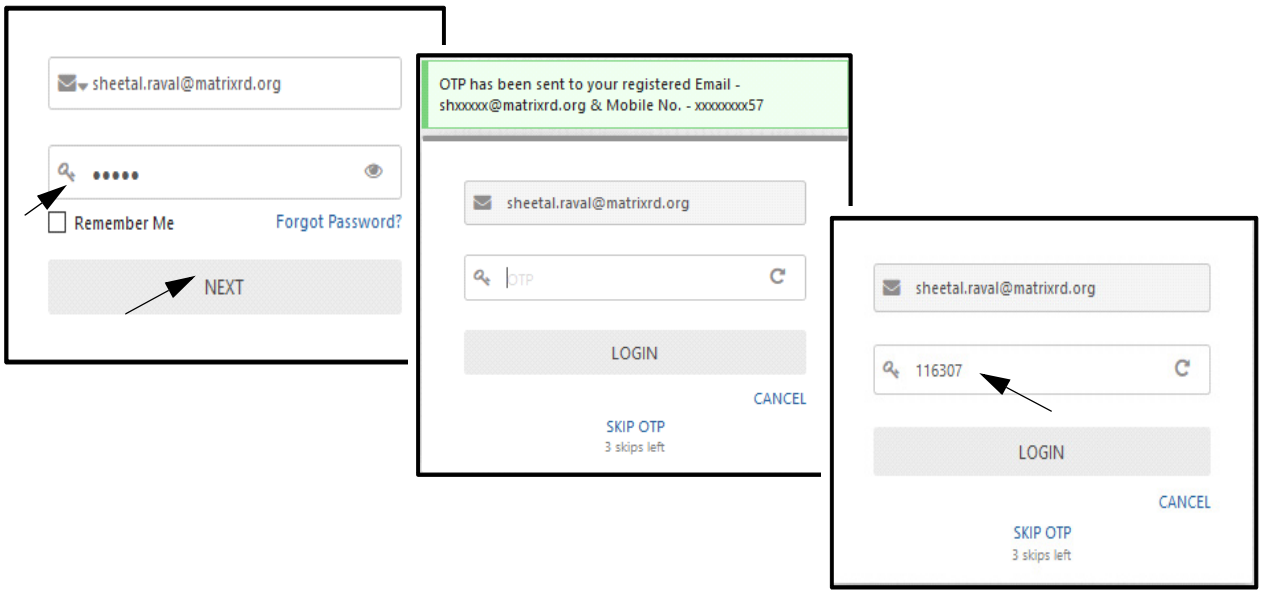
Eg: If Skip OTP is set as 2, the user can click on SKIP OTP for 2 times. When later if SKIP OTP in Login policy is changed to 5; then for 3 more times user can use SKIP OTP.



Email ID with Password Then OTP

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

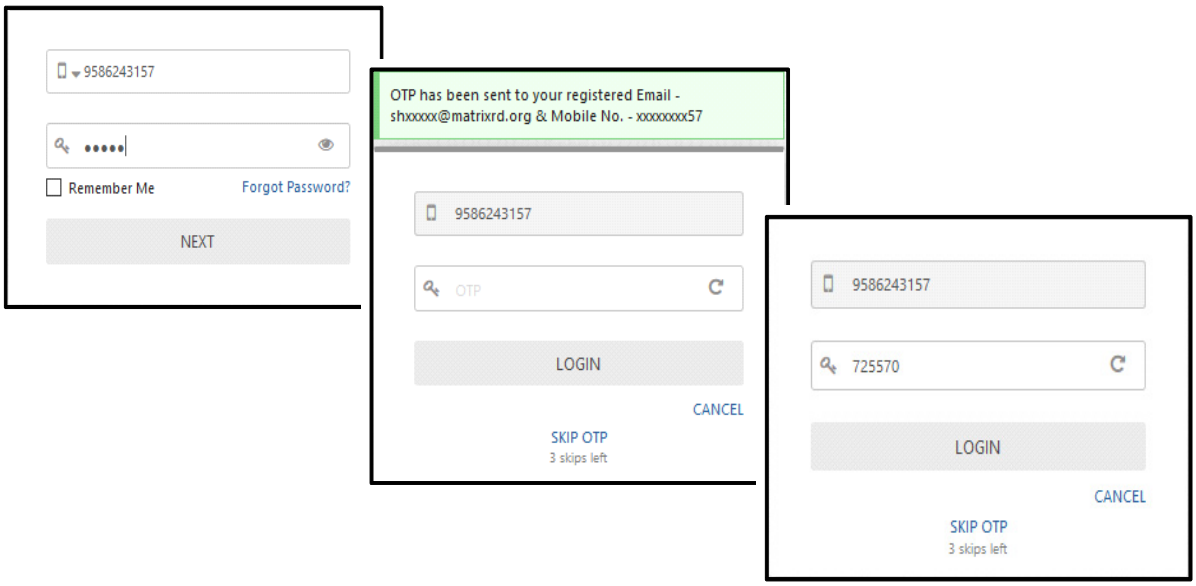
The OTP will be sent to the registered contact details of login user. Then enter the OTP and click **Login** button to login to Admin Portal. You can also skip entering OTP by clicking on **SKIP OTP** link.



Mobile Number with Password Then OTP

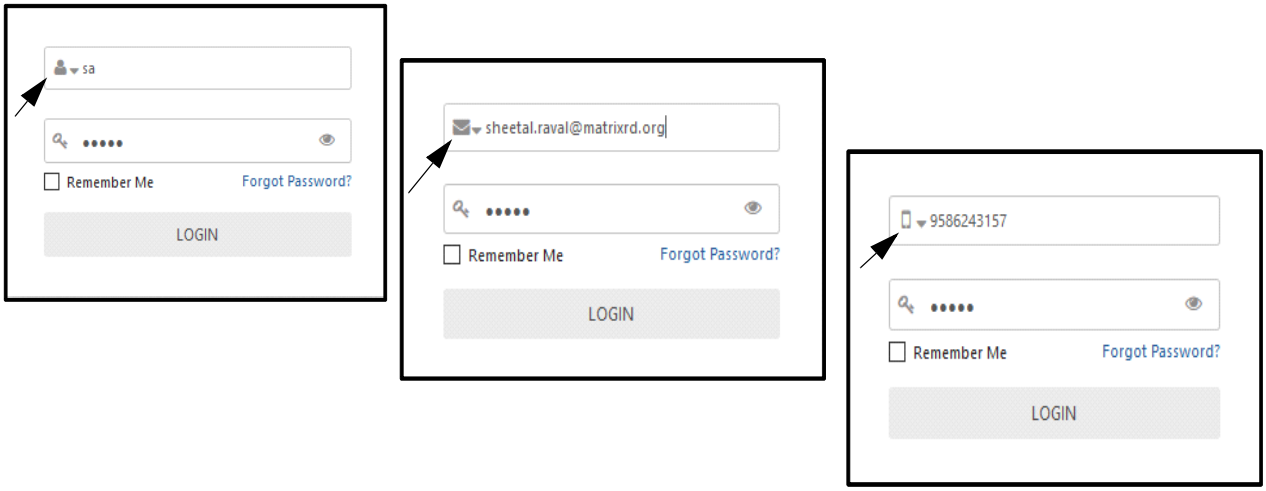
Enter the **Mobile number** of login user. Then enter the Password and click **Next** button.

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.



Password

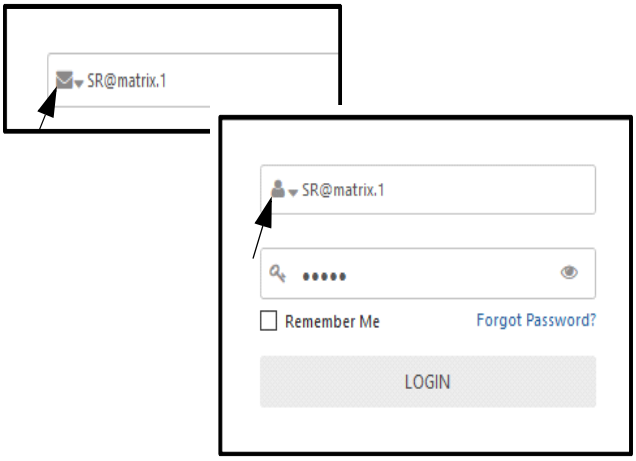
You can select Login Authentication mode as “Password”. This will require login ID with only password. Enter the login ID as User ID/ Email ID/ Mobile Number and the password. Then click Login to login into COSEC Web.



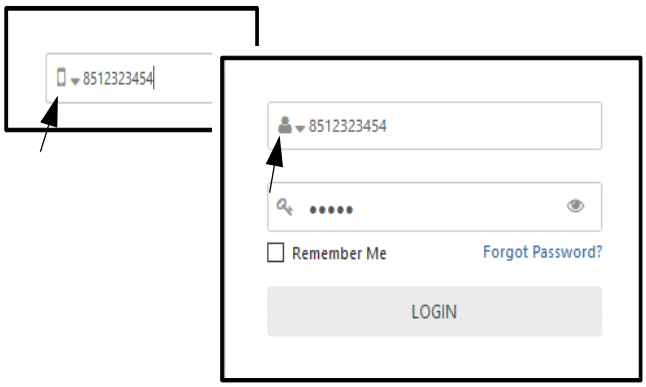
Icon of Login ID

Suppose you are logging into COSEC with your User ID which is similar to Email ID configuration eg: SR@matrix.1.

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

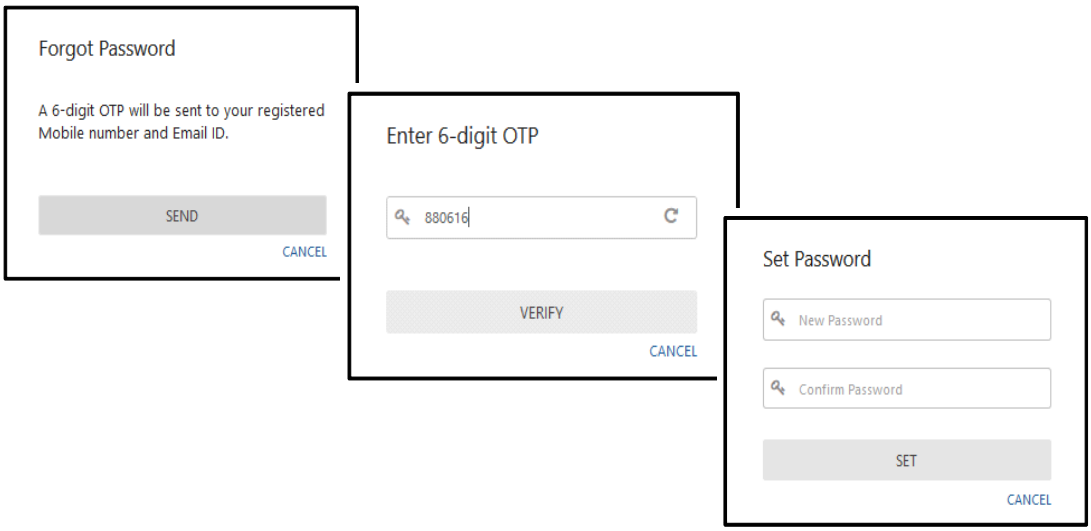


Suppose you are logging into COSEC with your User ID which is of 10 characters eg: 8532621525 so as there are 10 numeric characters; the icon will automatically change to Mobile number and it will try to login using Mobile number. As there is no such mobile number; you will not be able to login. Hence you should manually click on the icon to change from Mobile to User ID.



Forgot Password

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



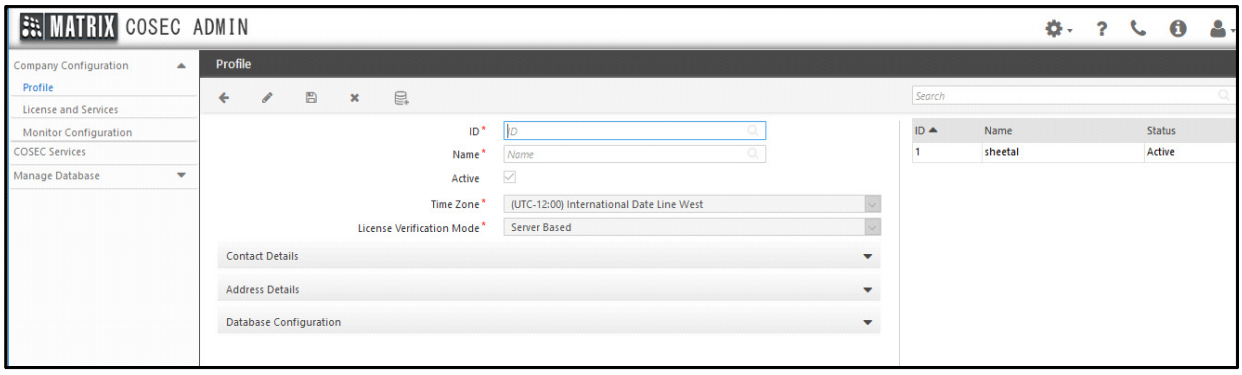
Now click **Send** button to get the password on registered Email ID and/or registered mobile number of the login user. Then Enter the 6-digit OTP and click **Verify.** After verification you can set your new password from Set Password window. Then you can login to Admin Portal using your login ID and 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 79.
See “Email Configuration” on page 84.

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



CHAPTER 4

Company Configuration

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:

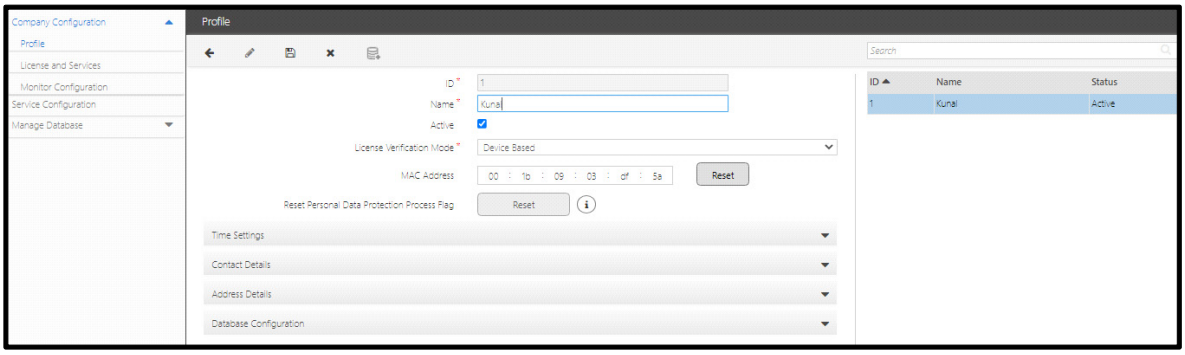
Profile

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.



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. It is the name as configured at the time of installing the Setup. You may modify it if required.

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

License Verification Mode: There are three modes for License Verification — Server Based, Device Based and Virtual License.

The option you select while installing the setup, appears here automatically. You can change the same if required.

- **Server Based:** If the licensing mode is set as Server Based, then Dongle must be inserted in the PC where Master service is installed.

  Click **Save**.

  The Dongle only has the GENERIC License. You need to purchase and update the licenses as per your requirement, click **Company Configuration > License and Services**. For details, refer to "Supported Licenses" and "License and Services".

- **Device Based:** If the licensing mode is set to Device Based, then license key shall be fetched from the Dongle connected to the desired device.

  Make sure the License Dongle is connected to the desired device. The **MAC Address** of the device with which the License Dongle is connected is displayed here.

  If you wish to change the device, click **Reset**.

  Click **Save**.

For Device Based License Verification, the devices — VEGA, ARGO, ARGO FACE Direct Doors and Panel lite V2/Panel200 in Server Mode — can be used.

*Make sure you have a **COSEC CENTRA** connection and the devices are configured in the same application.*

Once Dongle is connected to the desired device; enter the License Server URL (Default is 192.168.50.100) and License Server Port (Default is 15025) in Server Settings of the device from the device or its webpage.

The Dongle only has the GENERIC License. You need to purchase and update the licenses as per your requirement, click **Company Configuration > License and Services**. For details, refer to "Supported Licenses" and "License and Services".

- **Virtual License:** With the introduction of Virtual License, the need of a Dongle is eliminated, but you need to make sure you have:
  - Persistent Internet connection with good speed (where Master Service is running).
  - Received the MATRIX VIRTUAL DONGLE300 Key in PDF form.
  - Received the COSEC CENTRA PLATFORM Key in PDF form.
  - Received the desired module activation License Keys in PDF form.

  You need to purchase the keys. For details, refer to "Supported Licenses".

  Once the keys are received, you need to register/update the same. Click **Company Configuration > License and Services**. For details, refer to "License and Services".

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.

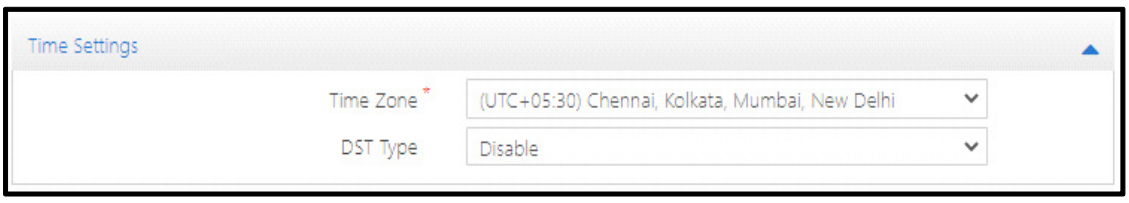
*The **Reset** functionality will reset the GDPR process status to its initial stage. If you desire, you may restart the GDPR process again.*

Select the respective link for further configuration:

- “Time Settings”
- “Contact Details”
- “Address Details”
- “Database Configuration”

Time Settings

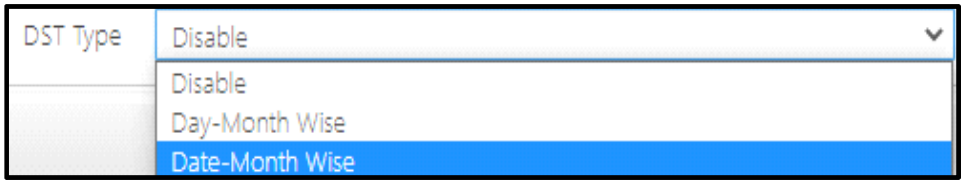
Click on the **Time Settings** collapsible panel to configure the time as per the company location.



Configure the following parameters:

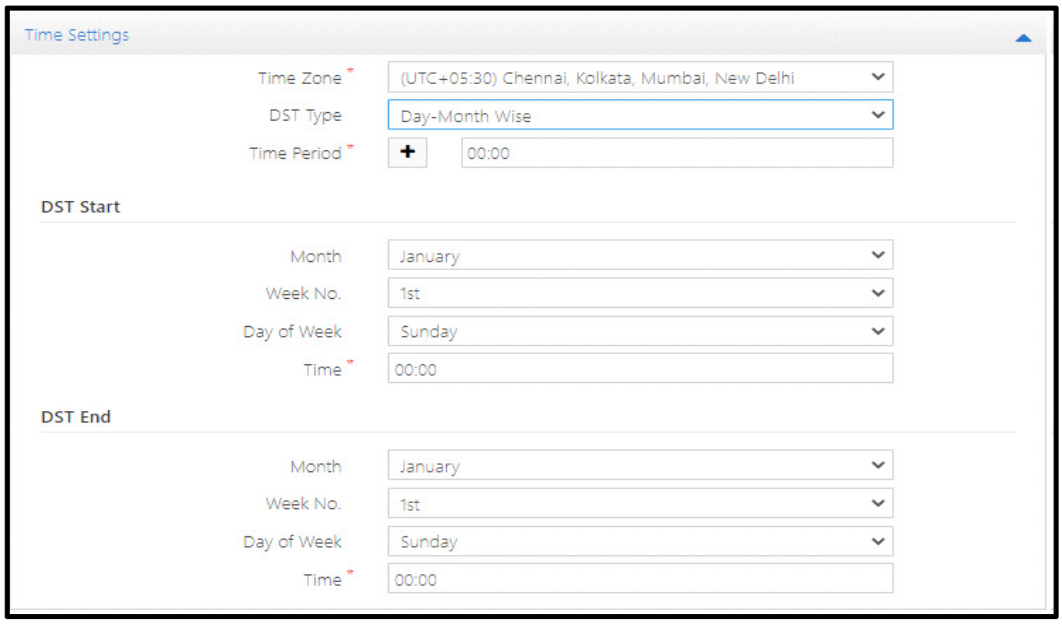
Time Zone: Select the desired time zone from the drop down list as per the location of your company.

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



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.



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

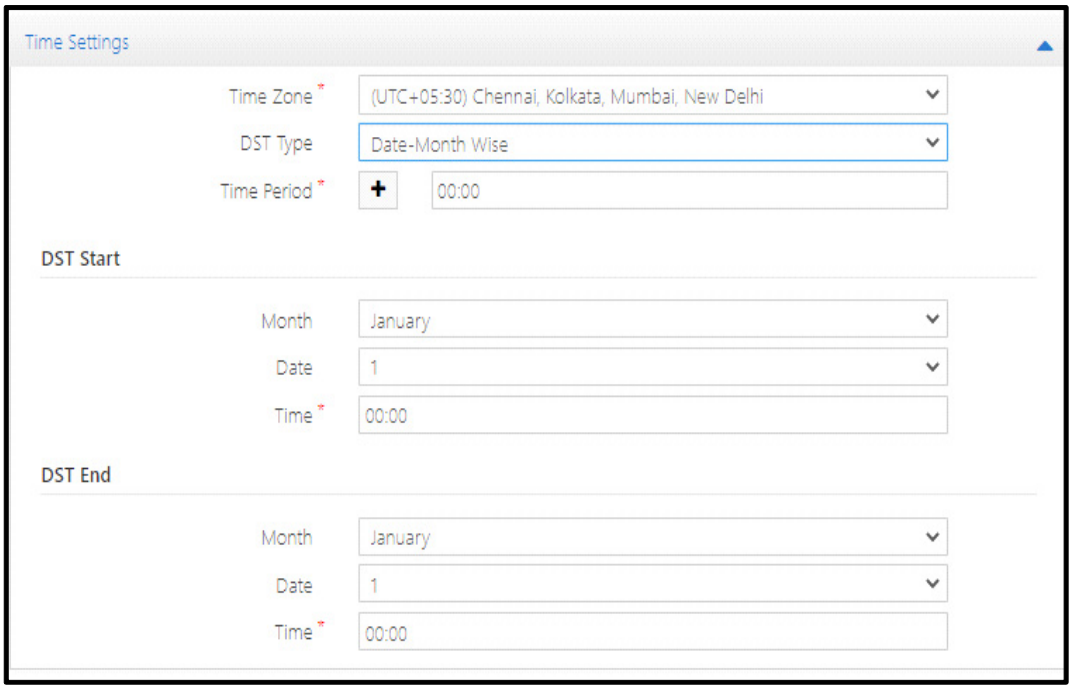
  - Select the **Month** when DST begins: January to December.
  - Select the **Week No**. when DST begins:1st Week,2nd Week,3rd Week,4th Week,5th Week.
  - Select the **Day** of the week when DST begins: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.
  - Set the **Time** when you want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



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

  DST Start

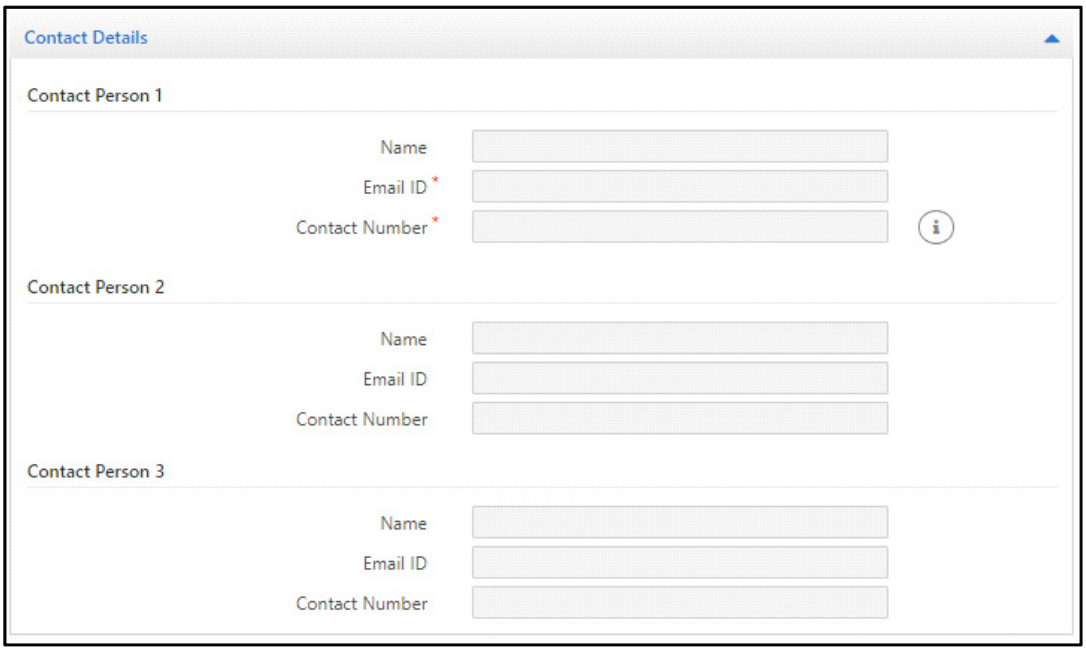
  - Select the **Month** when DST begins — January to December.
  - Select the **Date** on which DST begins — 1 to 31.
  - Set the **Time** when DST begins in 24 hours format.

  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.



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.

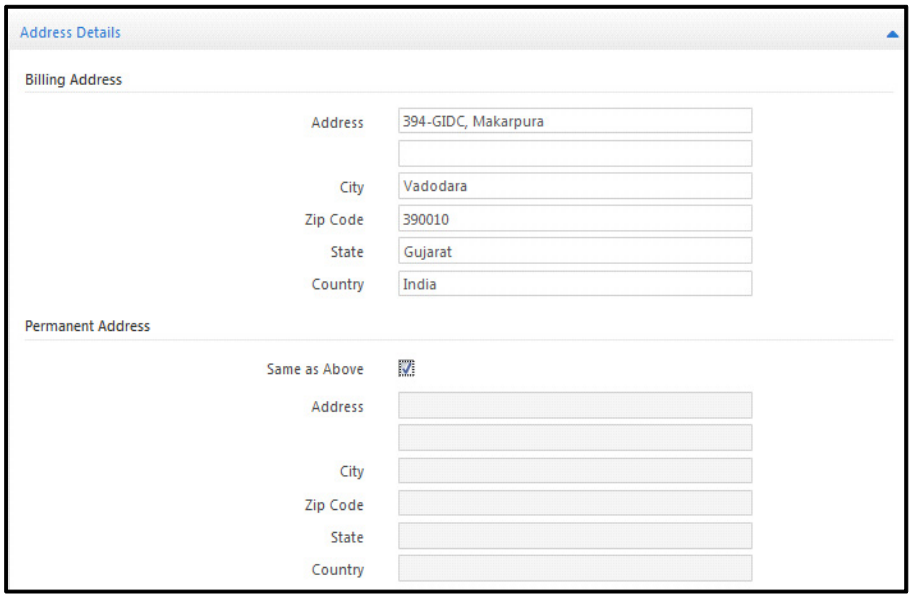
Contact Number: Enter the Contact number of the Company. This Contact Number will be used when the user (SA user) forgets password.

For COSEC VYOM Setup, the Alerts —SMS, WhatsApp and Email are sent on the Mobile Number and Email ID configured on Tenant Configuration > Tenants > Contact Details and on Business Partners page.

If the Contact Details — Email ID and Contact Number — is configured for all the 3 Contact Persons, then the Alerts — SMS, Email, Whats App — will be sent to the first contact only.

Address Details

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

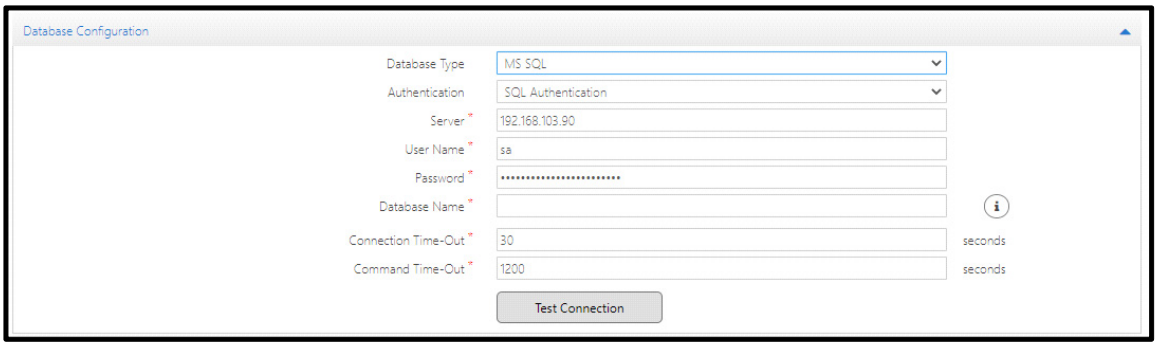


Billing Address: Enter the Address of the Company at which billing is to be done.

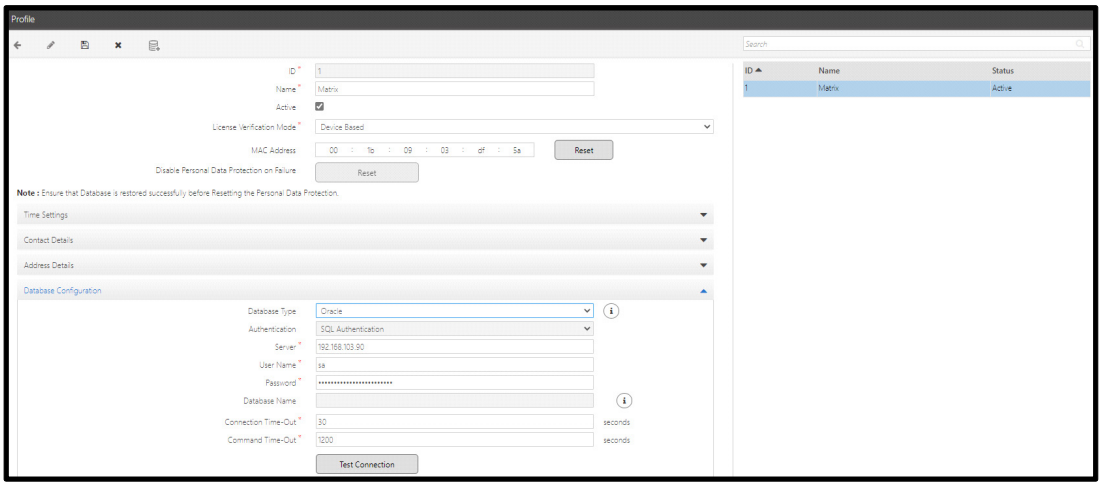
Permanent Address: If the permanent address is same as billing address, then select Same as Above or else enter the permanent address of the Company.

Database Configuration

Database Configuration for **MS SQL**



Database Configuration for **Oracle**



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\sqlexpress or localhost\sqlexpress
    - **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 Key may be a Virtual Key or Dongle Key. From the License and Services,

- you can manage the upgradation/registration of these keys.
- assign the COSEC Services to the Company.
- view the details of the license under Current License Profile.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.

If you have opted for Server Based/Device Based License Key, then the Dongle will have only the GENERIC license, all other license vouchers need to be purchased. These need to be purchased as per your requirement. Once ordered, you will receive keys in the form of a PDF file.

If you have opted for Virtual License then you need to purchase the MATRIX VIRTUAL DONGLE300 Key as well as other vouchers as per your requirement.

If you have opted to migrate from the Dongle License to Virtual License, then you need to contact Matrix Technical Support Team and get the new Virtual License Key (with all existing licenses of the Dongle incorporated in this key) PDF generated.

For the details regarding the various licenses that can be purchased, refer to “Supported Licenses”.

After you have received the License Key PDF as per your requirement, you need to register/update the same.

For details refer to “Virtual License Key” or “Dongle License Key”, “Services” and “Current License Profile”.

If you are migrating from the Dongle License to Virtual License and you have received the migrated License Key PDF as per your requirement, refer to “Virtual License Key” for details.

For additional security and privacy during Virtual License communication, COSEC supports Proxy Server Configuration. For more details, refer to “Proxy Server Configuration”.

Virtual License Key

If have opted for the Virtual License option for the first time, you need to make sure you have purchased the Licenses — MATRIX VIRTUAL DONGLE300 Key as well as the COSEC CENTRA PLATFORM Key (as well as the Module licenses need to be purchased as per your requirement). You will receive PDF’s for these keys.

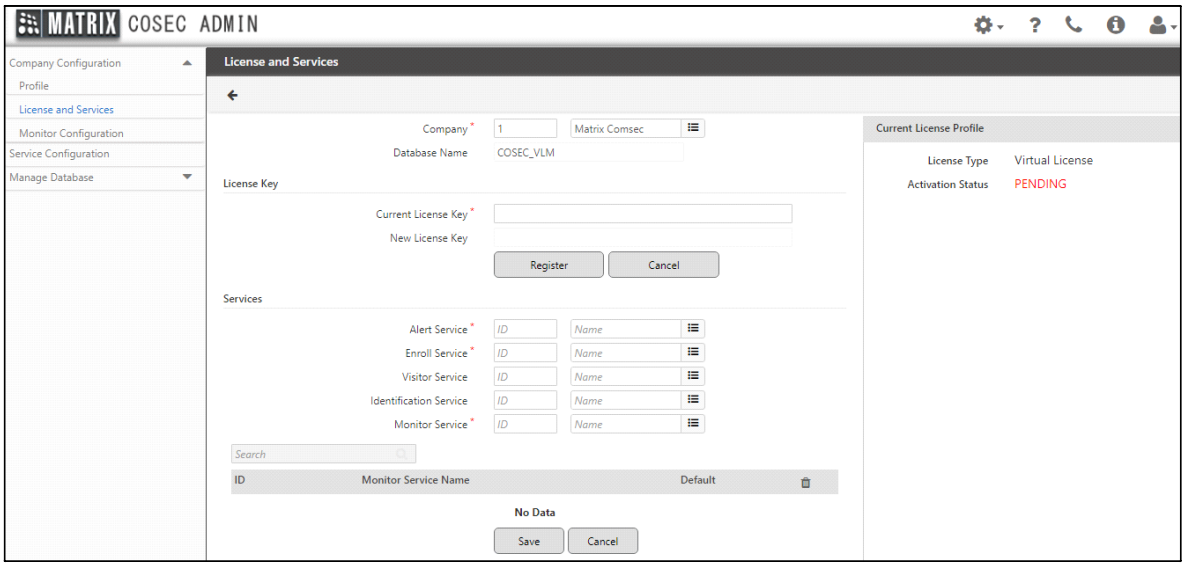
If you have opted to migrate from Dongle License to Virtual License, then make sure you have received the migrated Virtual License Key PDF.

For Virtual License, you need to have:

- a persistent internet connection with good speed (where Master Service is running).
- both these License Key PDF’s or the migrated License Key PDF are kept handy for activation.

The process for activating the newly purchased Virtual License Key or migrated Virtual License Key is the same.

Click **Company Configuration > License and Services.**



Company: Click the **Company** picklist. The **Select Company** pop--up appears. Click to select the desired company.

The picklist will display the Company Name as configured at the time of installing the Setup. This is also displayed in the Profile page. If you wish to edit the same, you can do so from the Profile page.

Database Name: It displays the COSEC Database Name of the company as configured at the time of installing the Setup. This is also displayed in the Profile page. If you wish to edit the same, you can do so from the Profile > Database Configuration.

License Key

The COSEC communicates with the Virtual License Manager (VLM) for registration, updation as well as re-registration. If the connectivity establishes the further process continues. For details refer to:

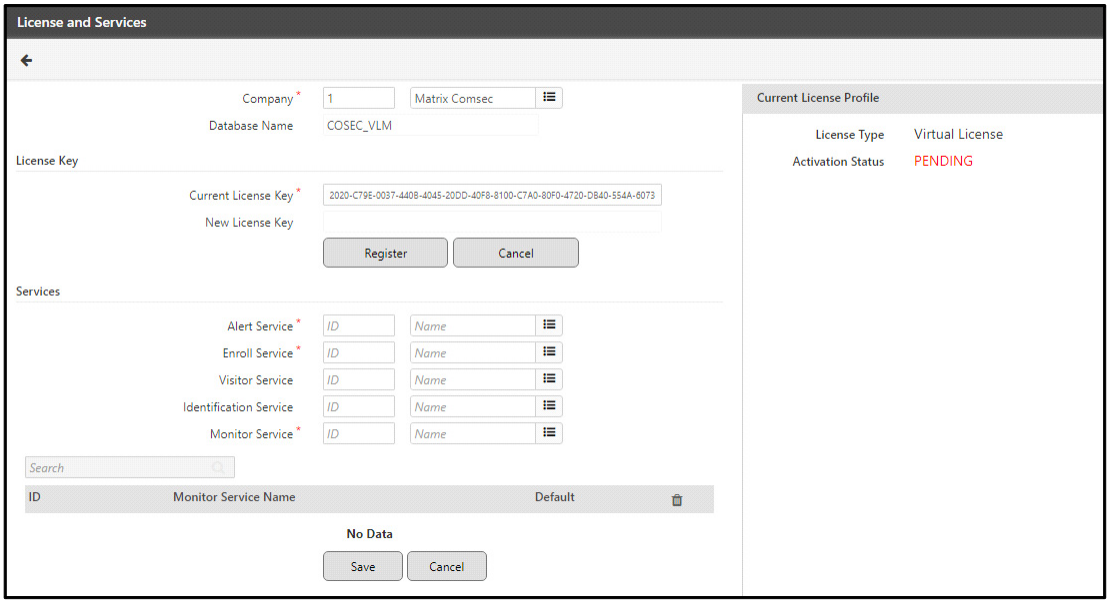
- “Registering the Virtual License Key”
- “Updating the Virtual License Key”
- “Updating the Contact Details”
- “Re-registering the Virtual License Key”

Registering the Virtual License Key

Current License Key: Enter the Generic Virtual License Key / migrated Virtual License Key received in the PDF here. To do so,

- Open the Generic Virtual License Key PDF / migrated Virtual License Key PDF file and select the key.

- Drag and drop the same onto this field.



Click **Register**.

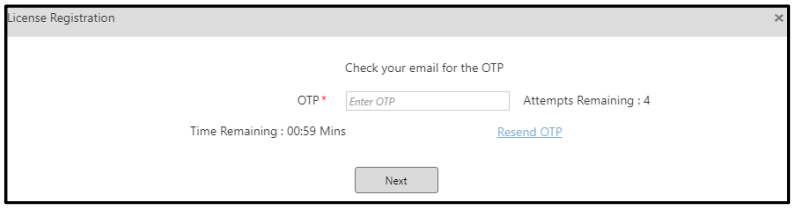
The **License Registration** pop-up appears.

Configure the following parameters:

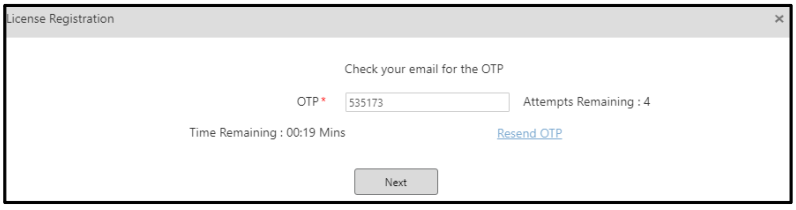
- **Email ID:** Enter the Email ID of the Client. Make sure it is genuine as the Alerts/Notifications as well as authentication OTP will be sent on this Email.
- **Mobile Number:** Enter the Mobile Number of the Client.
- **Name:** This displays the Company Name. It is fetched from Company Configuration > Profile.
- **SI Name:** Enter the name of the SI.

Click **Next**.

The OTP pop-up appears.



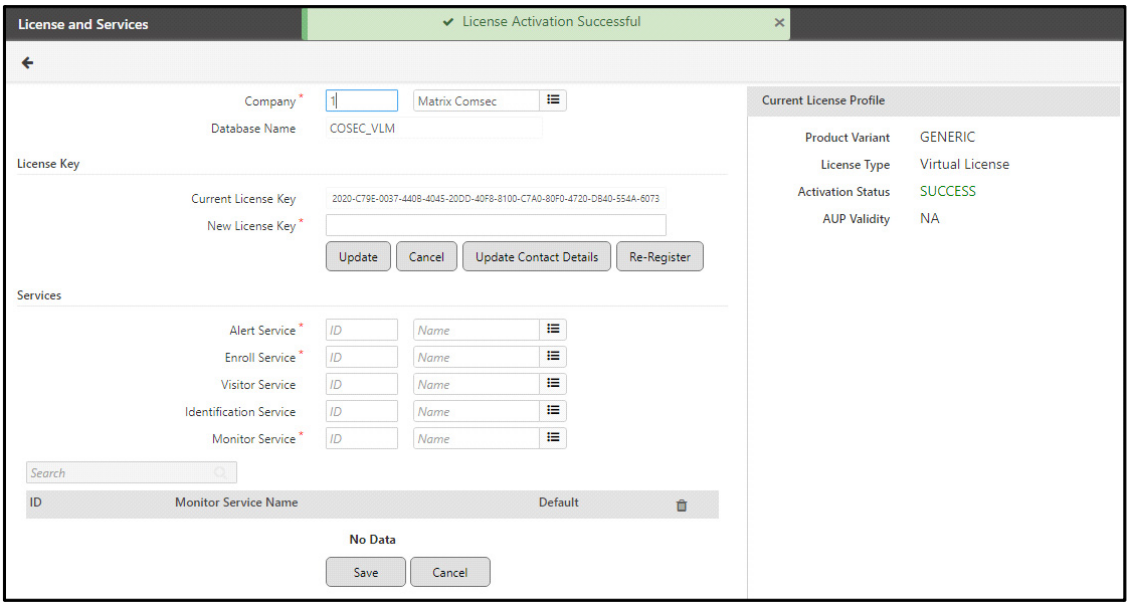
- **OTP:** Check your Email ID for the OTP and enter the same here.



As soon as the system sends the first OTP, the Time Remaining timer begins. The Attempts Remaining are displayed.
In case you do not receive the first OTP, you can click Resend OTP only after the Time Remaining timer expires.
When you click Resend OTP, the OTP is sent again to the Email ID and again the Time Remaining timer begins and number of Attempts Remaining is updated.

Once the Generic Virtual License Key/migrated Virtual License Key is authenticated and registered successfully, the successful message appears.

COSEC then checks the availability of the VLM server at regular internals (make sure you have a persistent internet connection where Master Service is running) and if it is unable to reach the VLM Server, then the alert — “Virtual License Validation Failed” — will be sent to the selected user’s Email ID and/or Mobile Number. To ensure the Alert is sent make sure you select Alert Filter as System and Event as Virtual License Validation Failed. For details, refer to *Admin Module > System Configuration > Alert Message Configuration* in the User Guide.



This registered Generic Virtual License Key is now displayed as the Current License Key and the License activation details are updated in the right grid under **Current License Profile** as per the key.

Updating the Virtual License Key

You need to Update the existing keys in the following scenarios:

- after registering the Generic Virtual License Key you need to update this key with the COSEC CENTRA PLATFORM Key.
- if you have purchased new vouchers to add on to your existing license, then you can update your existing key.

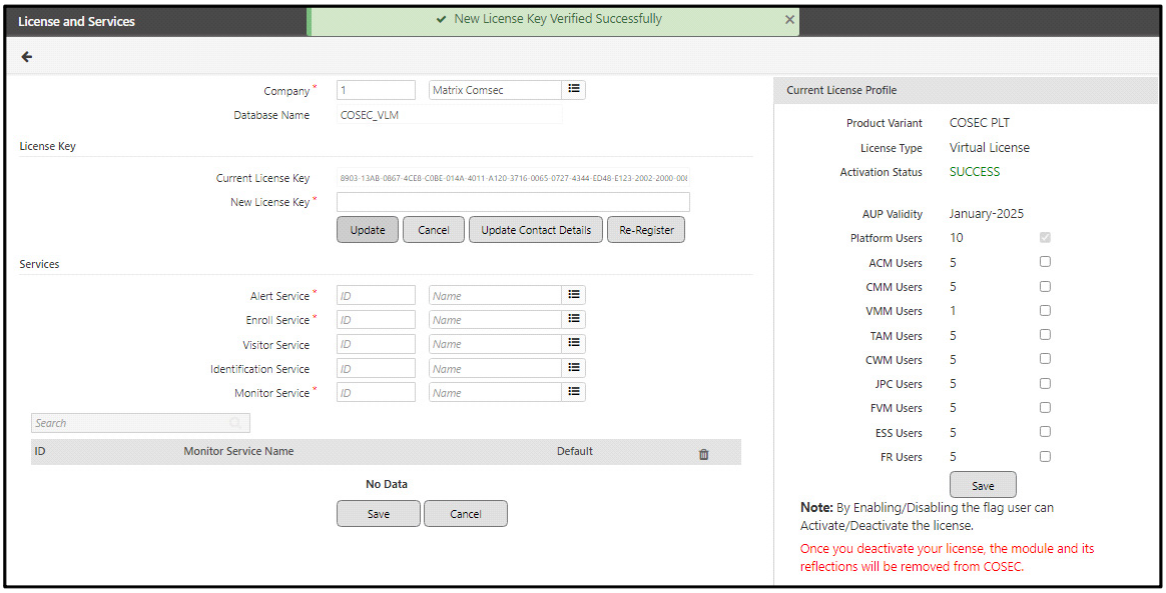
These keys are received in the form of PDF against your Purchase Order.

Current License Key: Displays the Generic Virtual License Key (in case you are activating the Virtual License for the first time).

New License Key: If you have purchased new vouchers for additional features, you will receive a new License PDF. You need to update the existing key with this new key.To do so,

- Open the License Key PDF file and select the key.
- Drag and drop the same onto this field.

Click **Update**.



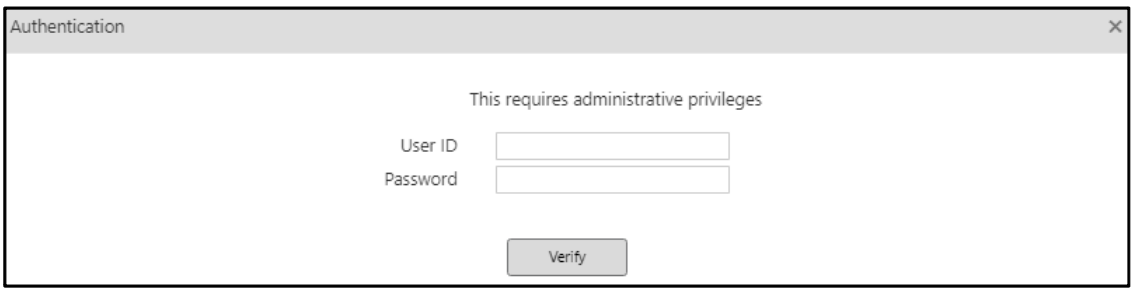
Now, this new key is displayed as the **Current License Key** and the License activation details are updated in the right grid under **Current License Profile** as per the key.

Updating the Contact Details

There may be certain instances — the personnel managing the IT may have left, Company changing it domain, Mobile Number is discontinued, etc — where-in you need to update the contact details so that you continue receiving the alerts/OTPs. To do so,

Click **Update Contact Details**.

The **Authentication** pop-up appears.



- **User ID:** Enter the User ID, for example sa.
- **Password:** Enter the Password, for example admin.

Click **Verify**.

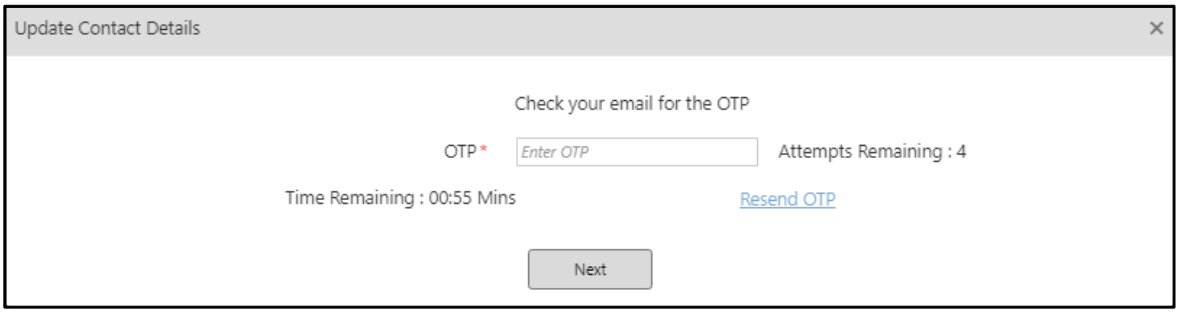
The **Update Contact Details** pop-up appears.

- Fill-in the updated details as per your requirement.

  The **Name** displayed here is fetched from Company Configuration > Profile. If you wish to edit the same post license registration you can do so from Profile page and then the same will be displayed here.

To update only Name in the VLM database, you need to change the same from Company Configuration > Profile, then click Update Contact Details. Enter the existing details in Email ID, Mobile Number and SI Name is you do not wish to change the same. Click Next and then enter the OTP. Click Next. The Name will be updated while other details remain same.

Click **Next**. The OTP pop-up appears. and an OTP is sent to your Email ID.



- **OTP:** Check your Email ID for the OTP and enter the same here.

Click **Next**.

The **Contact Details are Updated Successfully**, message appears.

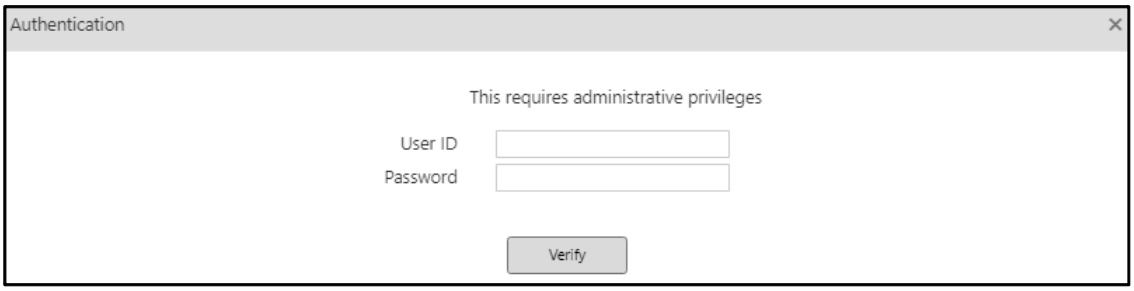
Re-registering the Virtual License Key

If you wish to migrate from a lower configuration COSEC Server PC to a higher configuration Server PC or your PC needs to undergo maintenance, that is you are changing your PC but the Admin database backup is available, then you need to Re-register the Virtual License Key, so that Virtual License validation can be re-initiated.

If your COSEC Server PC crashes and the Admin database backup is not available, then you need to contact the Technical Support Team for registering your Virtual License Key.

To Re-register the Virtual License Key,

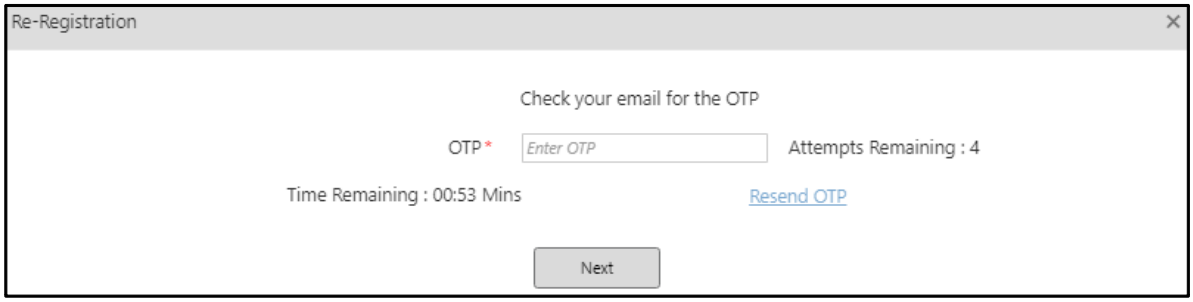
Click **Re-register**. The **Authentication** pop-up appears.



- **User ID:** Enter the User ID, for example sa.
- **Password:** Enter the Password, for example admin.

Click **Verify**.

The **Re-Registration** pop-up appears and an OTP is sent to your Email ID.



- **OTP:** Check your Email ID for the OTP and enter the same here.

Click **Next**.

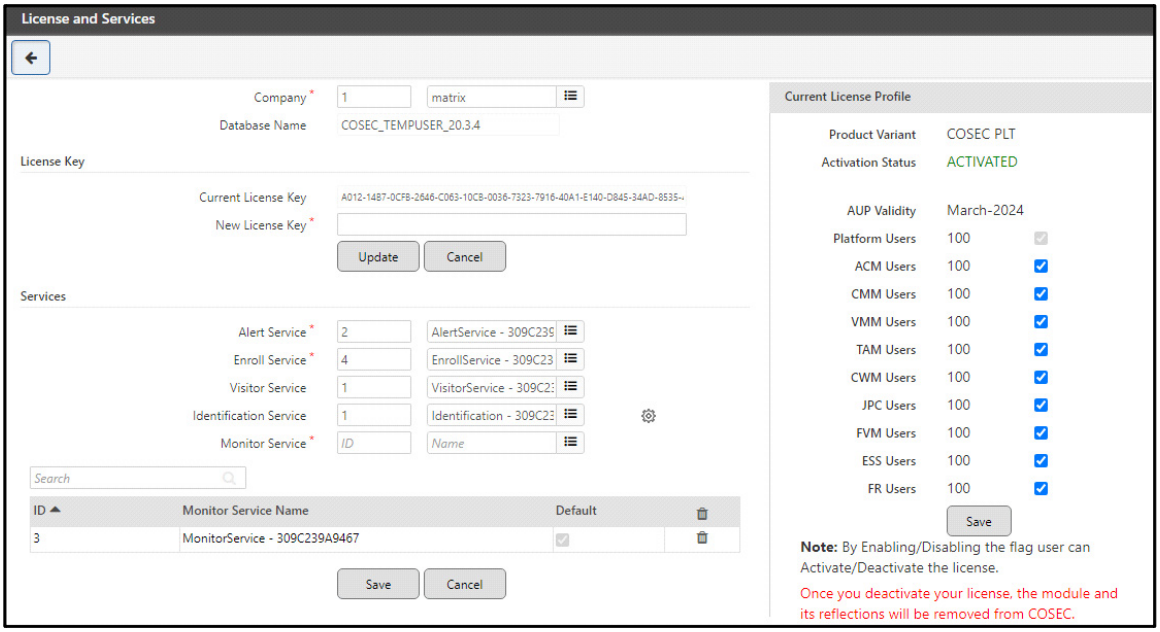
The **License Re-registered Successfully**, message appears.

- *If the internet connectivity is not available or lost at any given point COSEC will close any open popup and you will be re-directed to the Licenses and Services page. You need to restart the registration process.*
- *If you close the pop-up or the browser or your PC restarts or you refresh, then no previous request initiated information will be retained by COSEC.*
- *If at any point of time there exists any ongoing license registration/ verification/ new key updation or contact updatation process, then please wait for some time if you receive the same message again and again.Then retry after sometime.*

After successful registration of the license you need to upgrade the database. For details refer to “Database Upgrade”.

Dongle License Key

Click **Company Configuration > License and Services.**



Company: Click the **Company** picklist. The **Select Company** pop-up appears. Click to select the desired company.

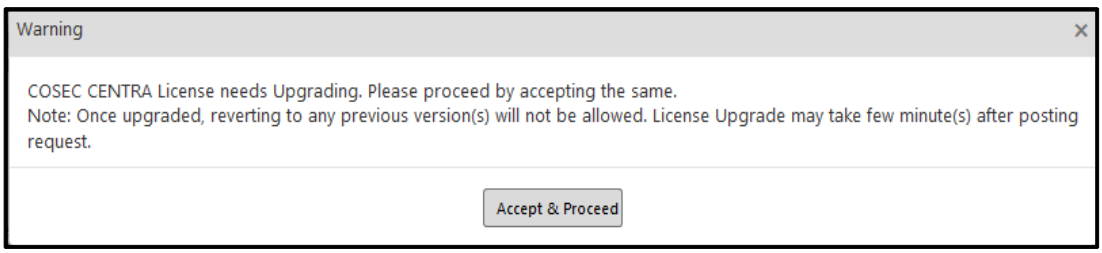
The picklist will display the Company Name as configured at the time of installing the Setup. This is also displayed in the Profile page. If you wish to edit the same, you can do so from the Profile page.

Database Name: It displays the COSEC Database Name of the Company as configured at the time of installing the Setup. This is also displayed in the Profile page. If you wish to edit the same, you can do so from the Company Configuration > Profile > Database Configuration.

Current License Key: It displays the current license key available in Dongle. This is the Generic Key.

Click **License Upgrade** for upgrading the License structure. A warning appears.

*The **License Upgrade** icon will appear only if you have the old License Keys — GE, PE, LE, ME, DEMO or LE MOI.*

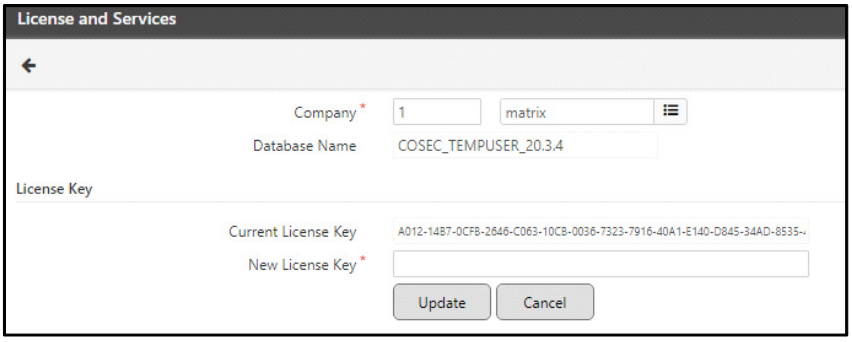


Only SA user can upgrade the license structure.

Click **Accept & Proceed.** The Master Service will upgrade the License Key to the new structure. This key appears as the Current License Key.

New License Key: If you have purchased new vouchers for additional features, you will receive a new License PDF. You need to update the existing key with this new key.To do so,

- Open the License Key PDF file and select the key.
- Drag and drop the same onto this field.
- Click **Update**.



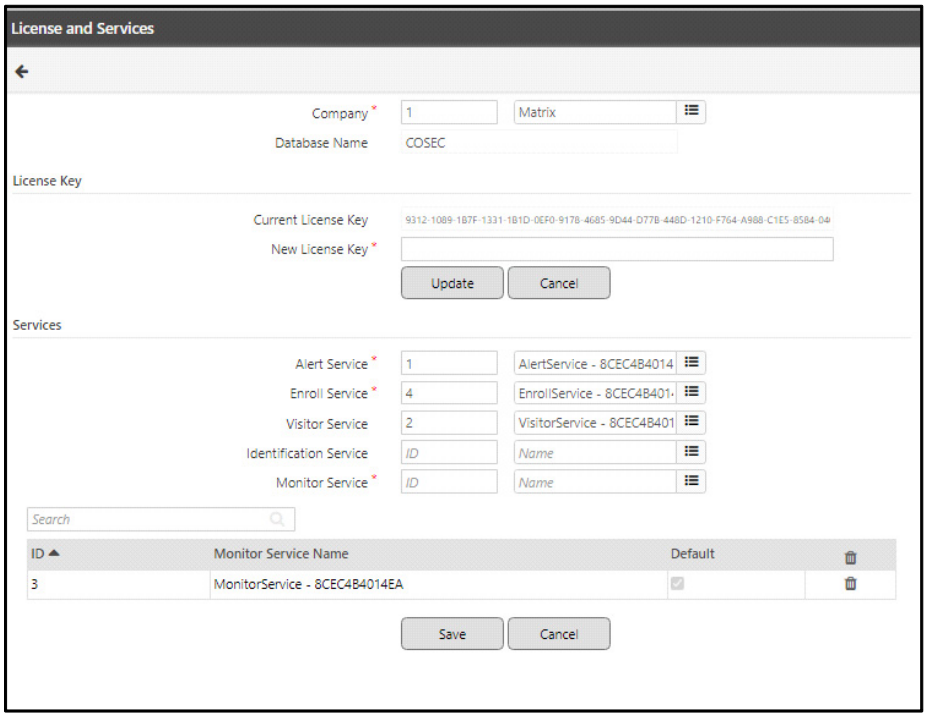
Now, this new key is displayed as the **Current License Key** and the License activation details are updated in the right grid under **Current License Profile** as per the key.

Updating the key will add new features to the existing license key by keeping the COSEC CENTRA PLATFORM Key (Serial No.) as it is.

After successful updation of the license you need to upgrade the database. For details refer to “Database Upgrade”.

Services

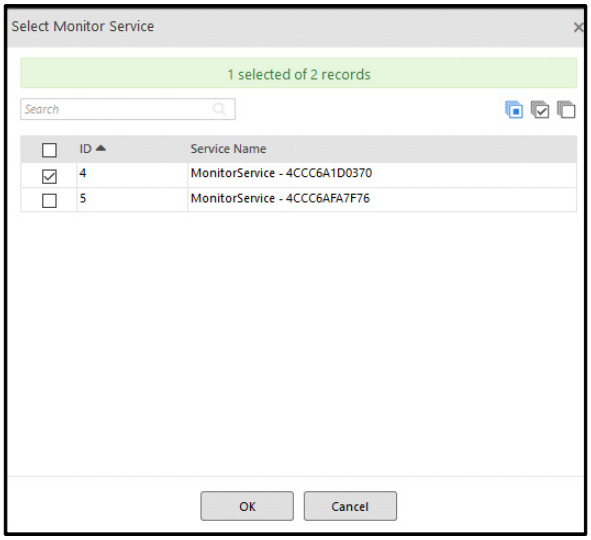
There is provision to assign Alert Service, Enroll Service, Visitor Service, Identification Service and multiple Monitor Services to the Company Profile. Once the services are installed, the default services will be assigned to the Company.



Multiple Monitor Service's can be assigned as per the Company's device requirements. By default the first Monitor Service will be considered as the default service.

The services (for example Monitor Service) running on one computer can access Master Service running on another computer. The Monitor Server will register by itself and will appear in the Monitor Service picklist.

- For Example: The Monitor Service on computer 192.168.104.24 is using Master Service running on computer 192.168.104.12 so picklist of Monitor Service will display this additional Monitor Service of 192.168.104.24 also.



Whenever any Monitor Service is deleted then on save, all the devices assigned to this service will be transfered to the default Monitor Service.

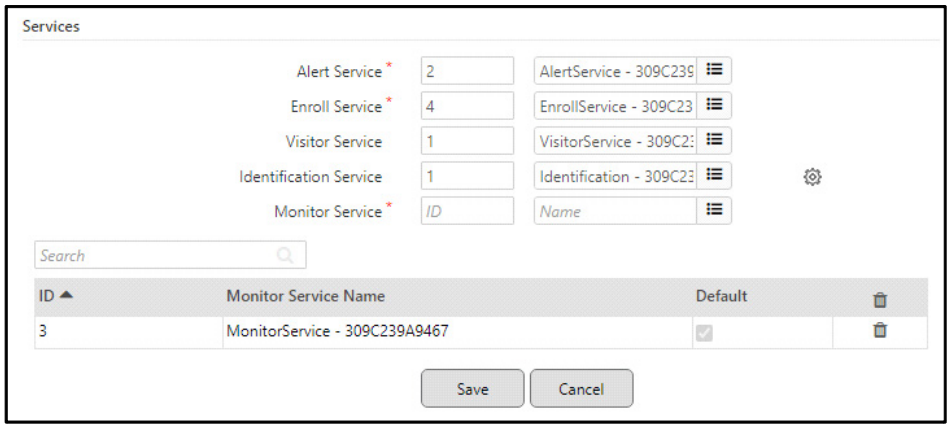
This change will be done in Company's COSEC DB.

Alert Service: Click the picklist and select the Alert Service you wish to assign to the selected Company.

Enroll Services: Click the picklist and select the Enroll Service you wish to assign to the selected Company.

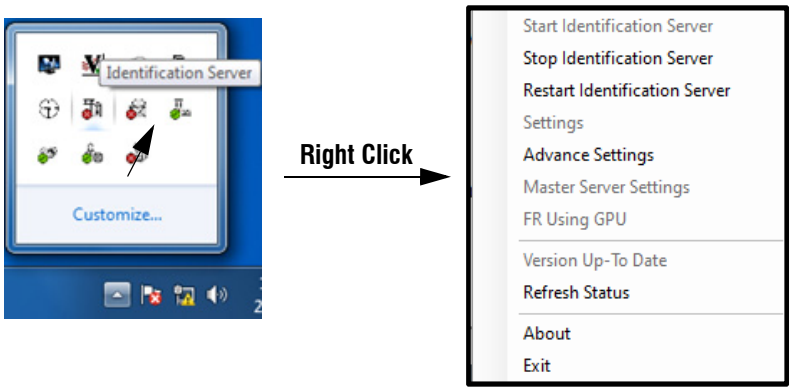
Visitor Service: Click the picklist and select the Visitor Service you wish to assign to the selected Company. This service will be required if you wish to use the Visitor Utility.

Identification Service: Click the picklist and select the Identification Service you wish to assign to the selected Company.



To make sure this service functions as the Centralized Identification Service, follow the steps as mentioned:

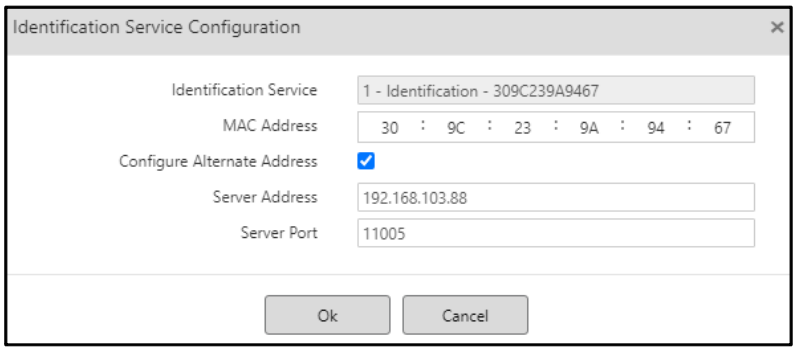
- Click **Save**.
- Right-click on the IDS Tray Service .



- Click **Restart Identification Server**.

The features — Group FR (Mark Group Attendance), Capture Face of Unidentified User, Manual Group Attendance 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 **Settings** . The **Identification Service Configuration** pop-up appears:



It displays the following details:

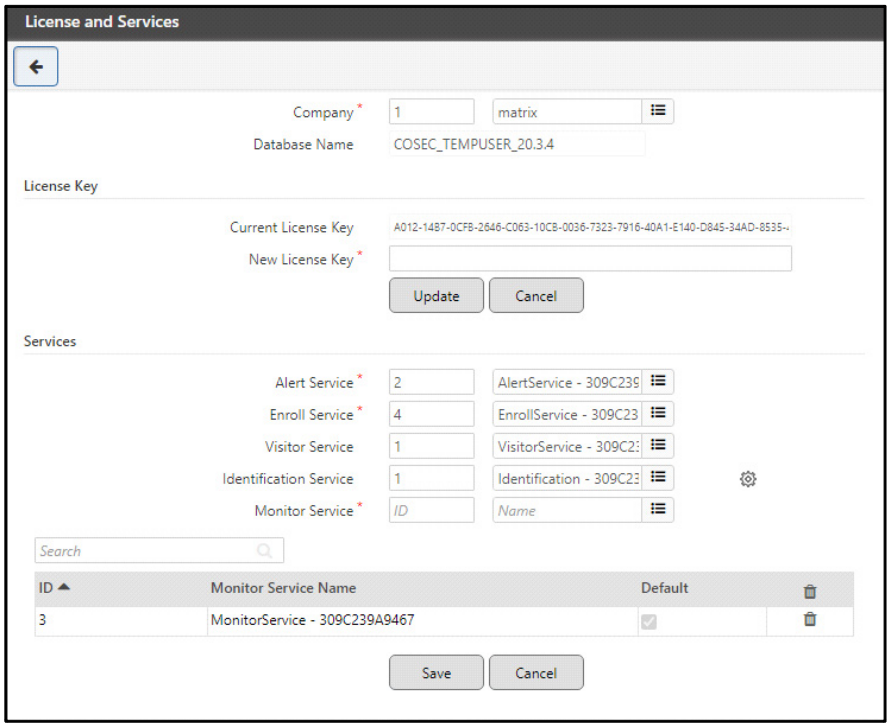
- **Identification Service:** Displays the name of the Identification Service.
- **MAC Address:** Displays the MAC Address of the computer where the Identification Service is running.
- **Configure Alternate Address:** By default this check box is enabled. The **Server Address** will be displayed automatically.

  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.

Monitor Service: Click the picklist and select the Monitor Service you wish to assign to the selected Company. You can select multiple Monitor Service's from the picklist to be assigned to the selected Company.

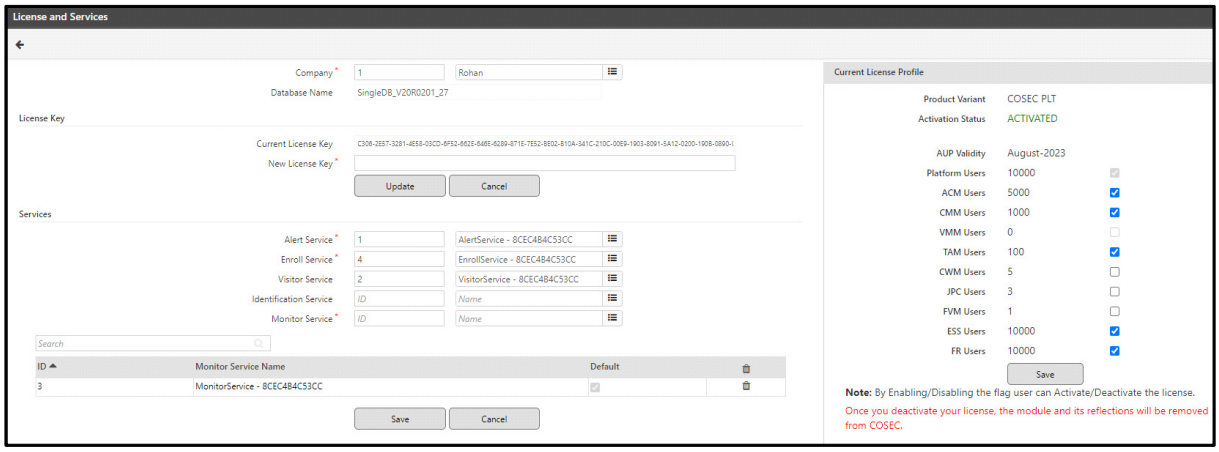
The assigned Monitor Service appears in the list as displayed below.



For more details regarding services, refer to “COSEC Services”.

Current License Profile

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



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 Platform User license will always be selected and un-editable.

By default the check box will be selected and editable for those modules whose license is activated and have more than 5 user license.These modules and their reflections will be visible in COSEC Web.

By default the check box will be clear and editable 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. If you want these modules and their reflections to appear, select their check boxes.

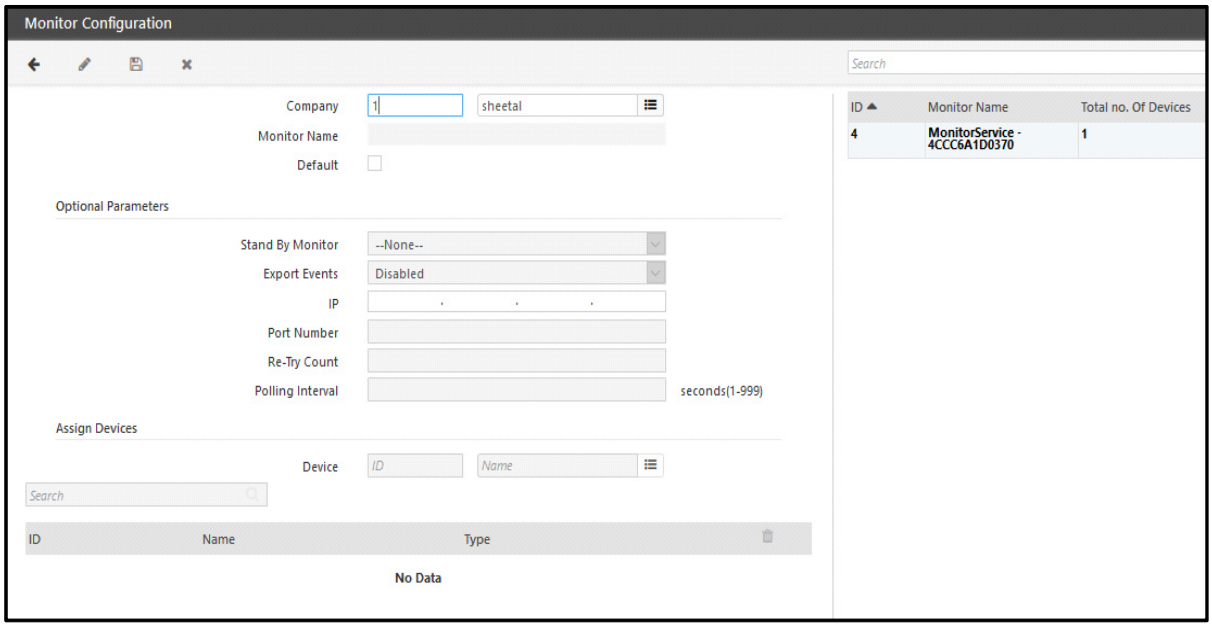
Similarly, by default the check box will be clear and un-editable for those modules whose license is not present and have 0 user license.Such modules and their reflections in other modules will be removed in COSEC Web. For example, there are 0 VMM Users and the check box is clear and un-editable, then 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

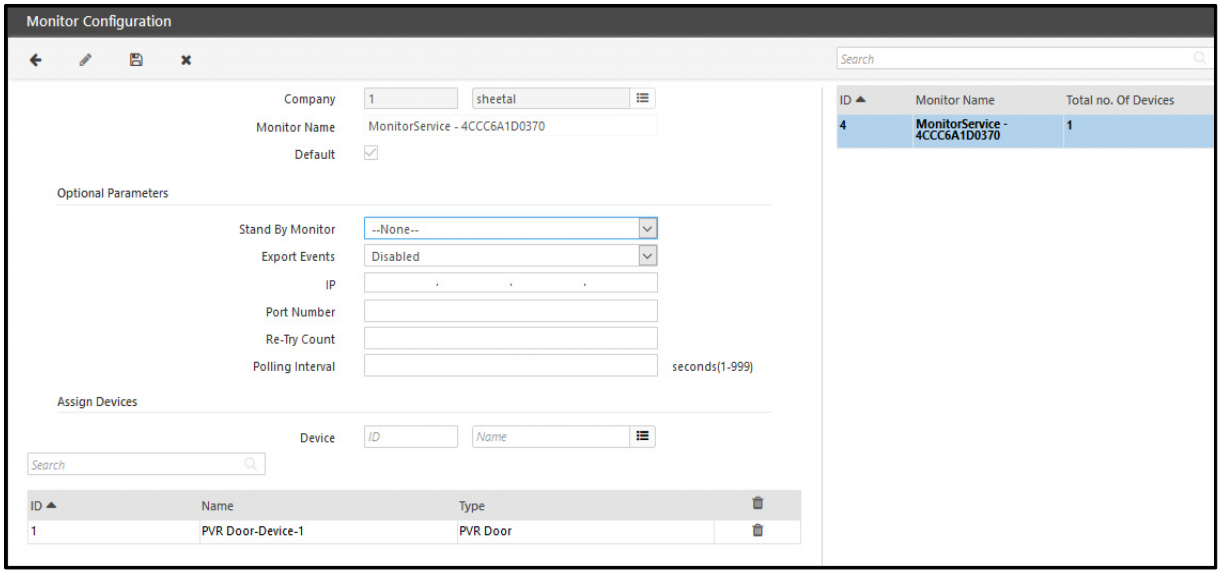
The Management team of the Company has to ensure the proper device assignment to Monitors. They can assign/ re-assign devices among the monitor services assigned to the Company.

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.



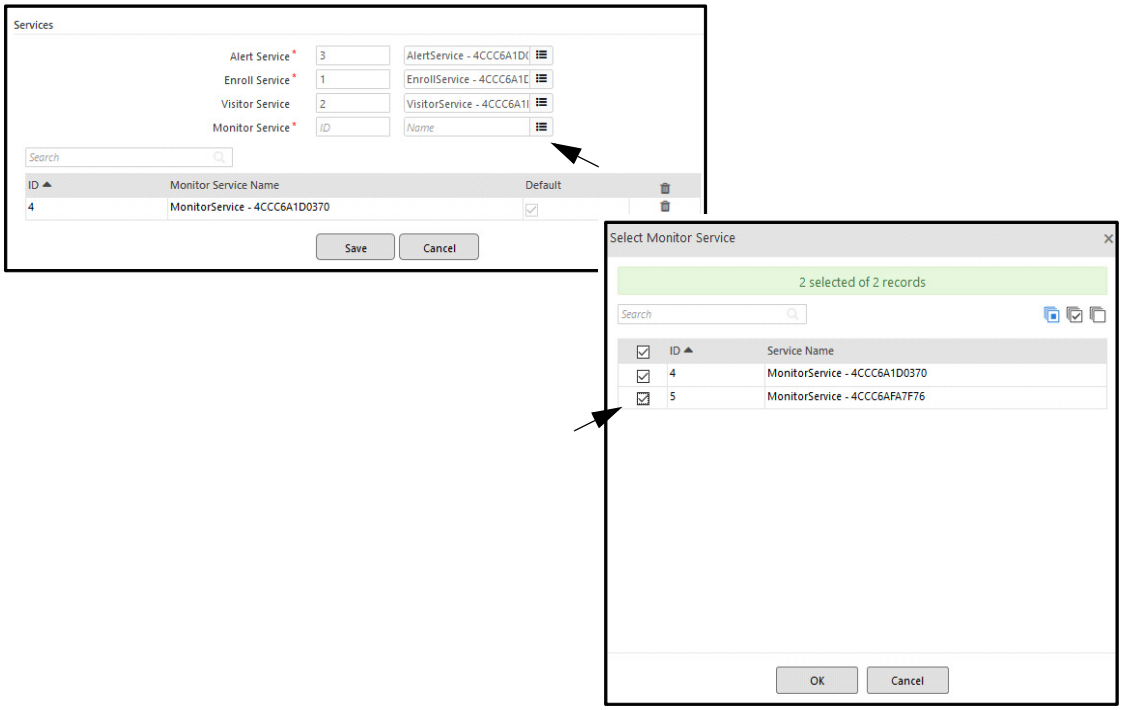
Company: It displays the company profile name. The monitor services assigned to the company will appear in the grid on right side. Select the Monitor service from the grid to view the assigned devices to the respective monitor service.



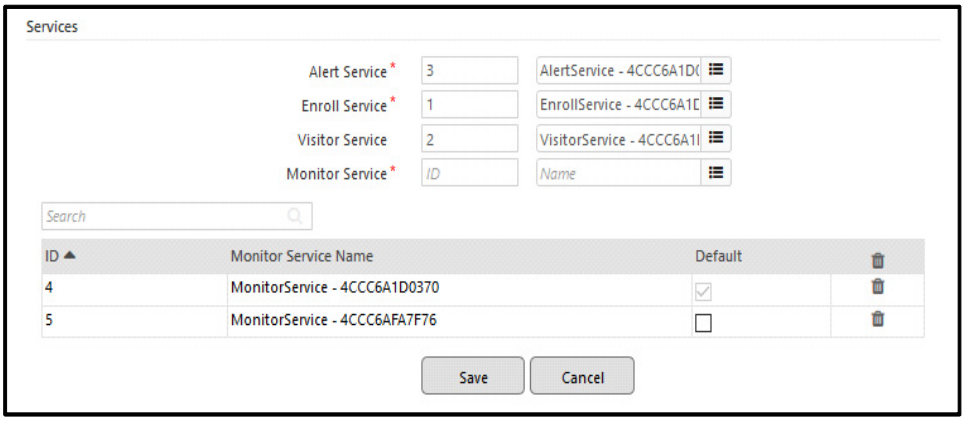
The Monitor Service is assigned to the company from “License and Services” page.

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

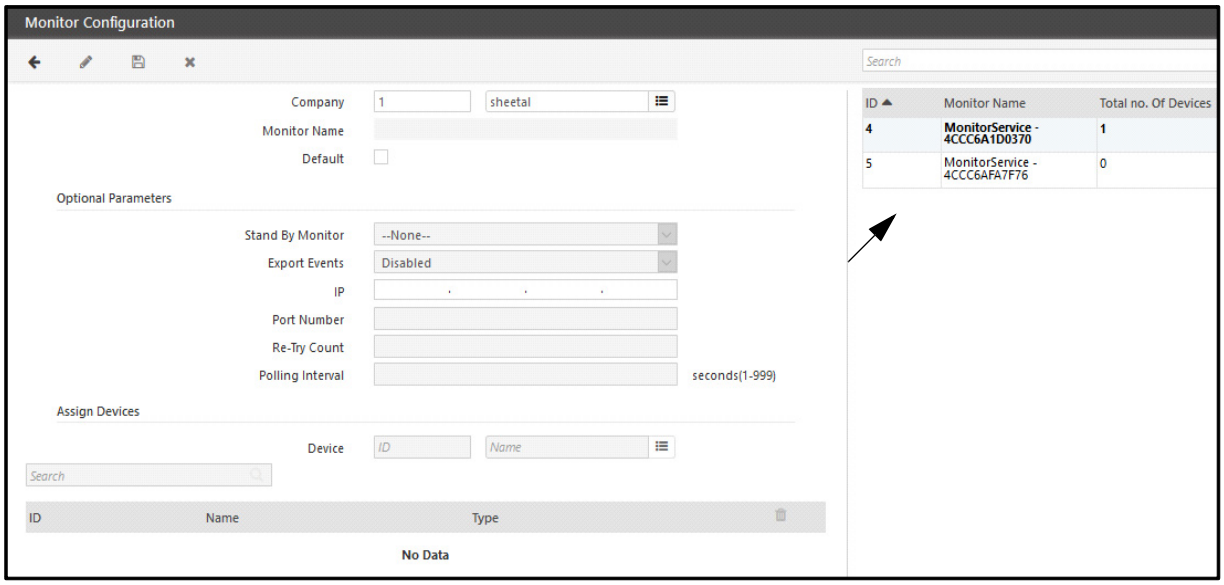
For assigning another monitor service click the Monitor Service pick-list on License and Services page. Then select the check-box for the monitor service which is to be assigned to the company. Then click OK and Save the settings.



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

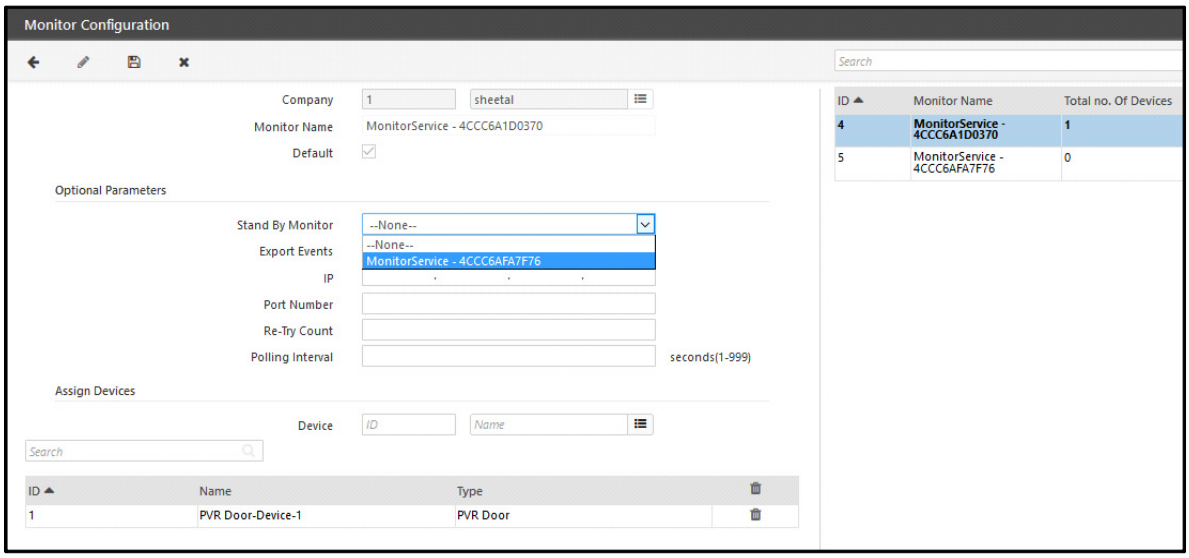


The new monitor service is now available in monitor configuration as well.



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.



- **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.

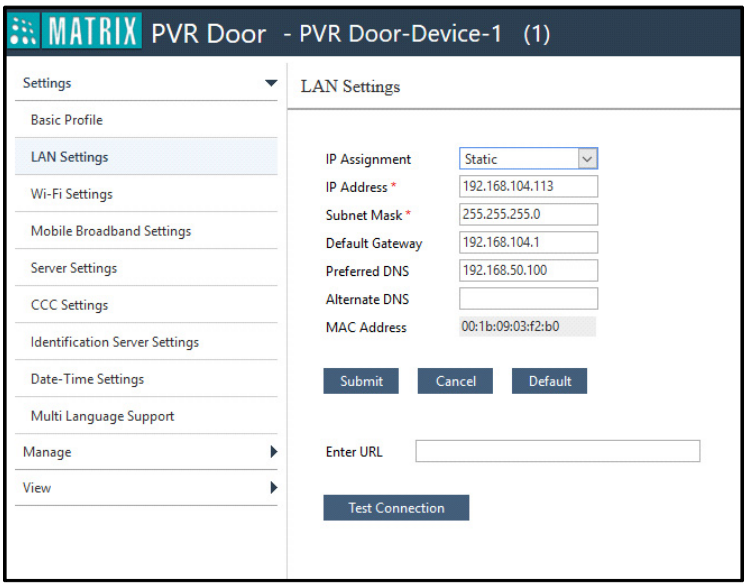
Assign Devices

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.

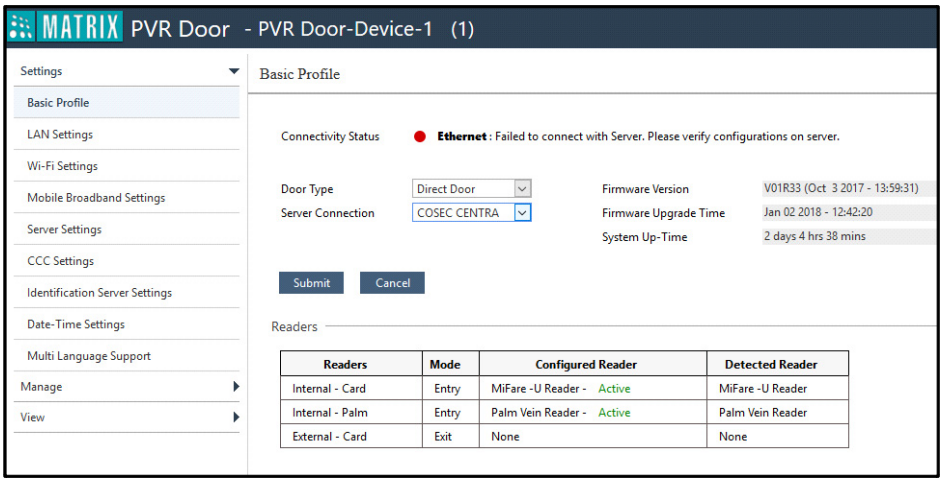
If this monitor service is set as **default** from “License and Services”, then newly added device will be directly added in the grid.

To add a device (PVR Door) to Monitor

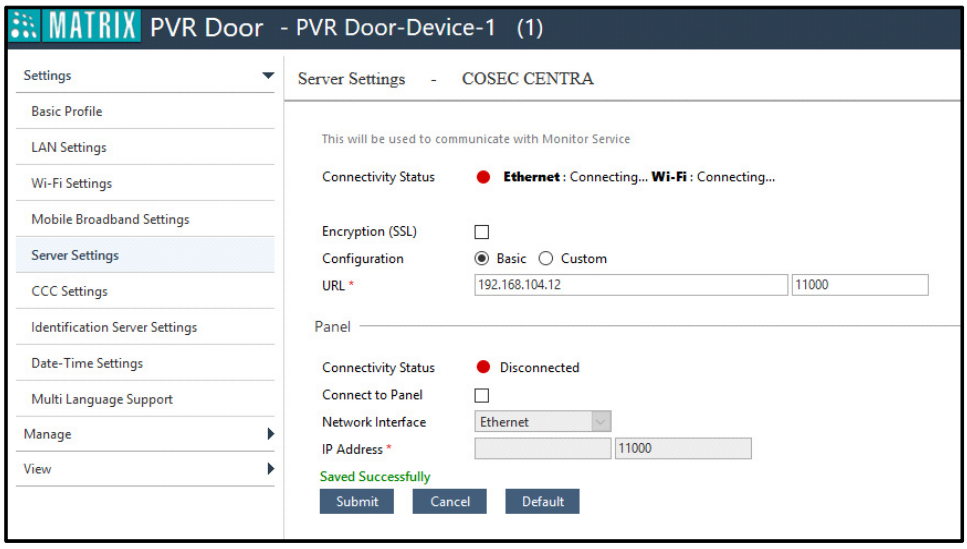
1. Open the Webpage of PVR Door by accessing Door’s IP address (192.168.104.113) in browser. Configure the Gateway and DNS settings as shown below.



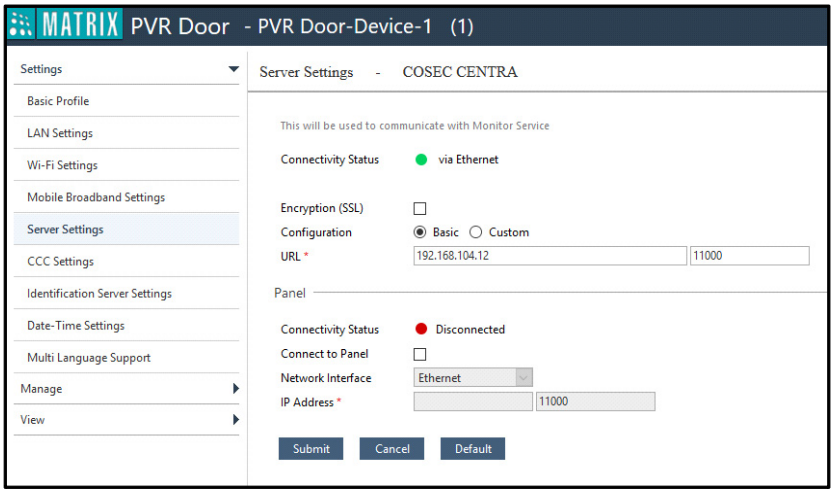
2. Configure the Basic Profile. Select the server connection as COSEC CENTRA.



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.

CHAPTER 5

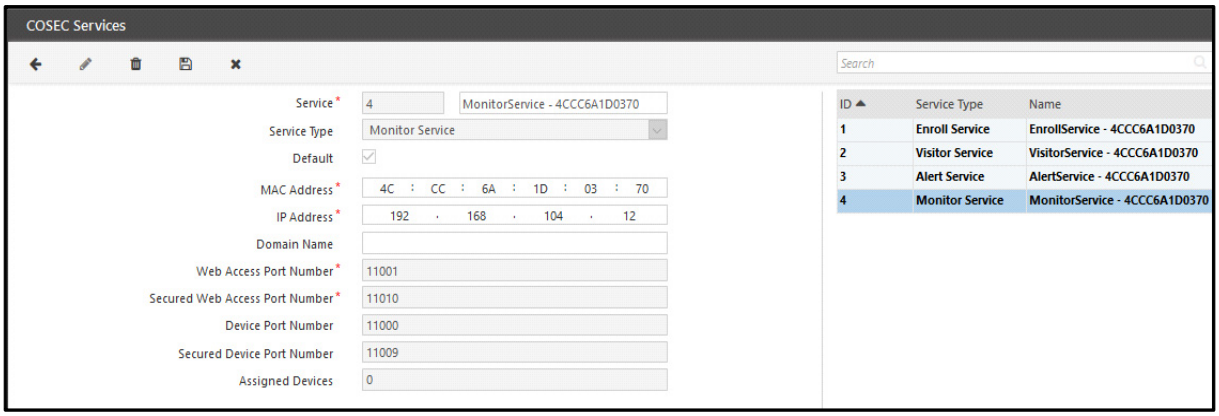
COSEC Services

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.

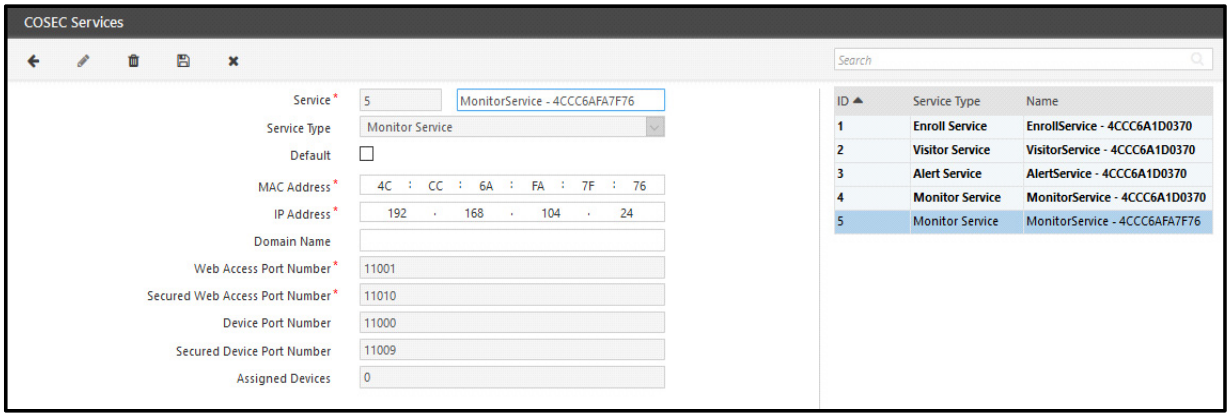
Once the services are started and running, it will automatically get assigned to the company.
By default following COSEC services can be managed:

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

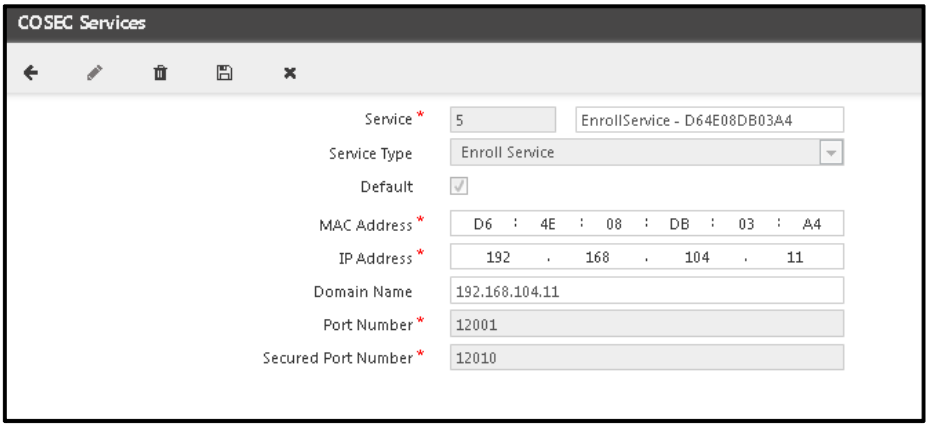


The new services cannot be configured here. But the services (Say Monitor Service) running on one computer can access Master service running on another computer. This will self-register the monitor service and will appear in the list shown on right side.

The Monitor Service on computer 192168.104.24 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
Search
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
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



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

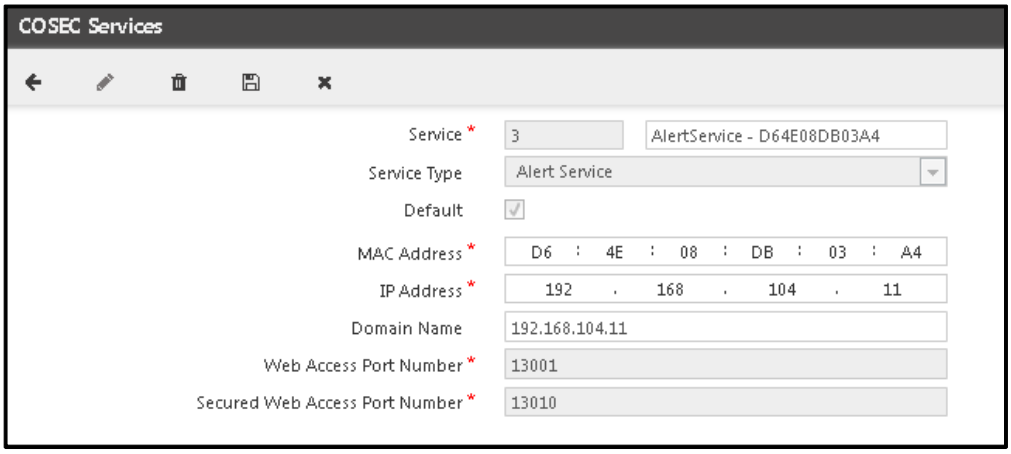
IP Address: Enter the IP address of the computer on which the Enroll service is accessible.

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



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

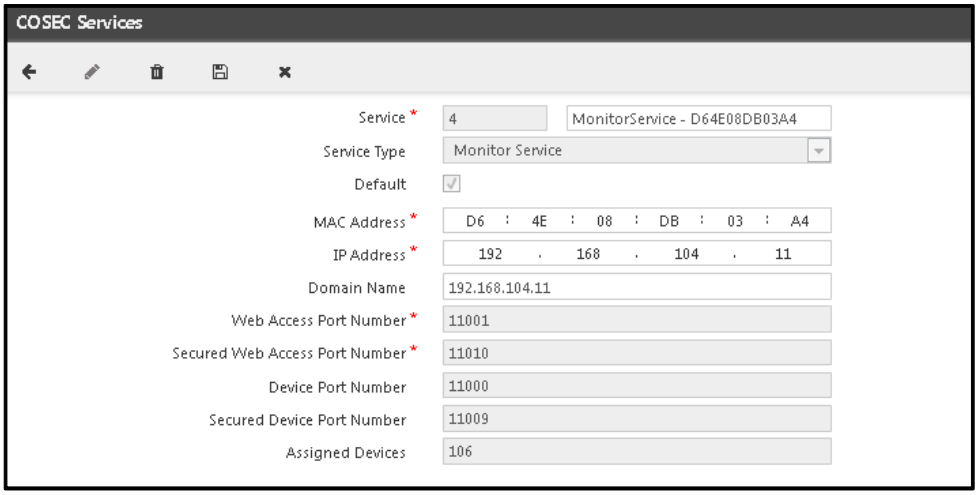
When client is situated in a time zone other than Alert Service's time zone; Alert Service will take company's time zone into consideration while processing scheduled tasks or generating scheduled reports.

“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



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.

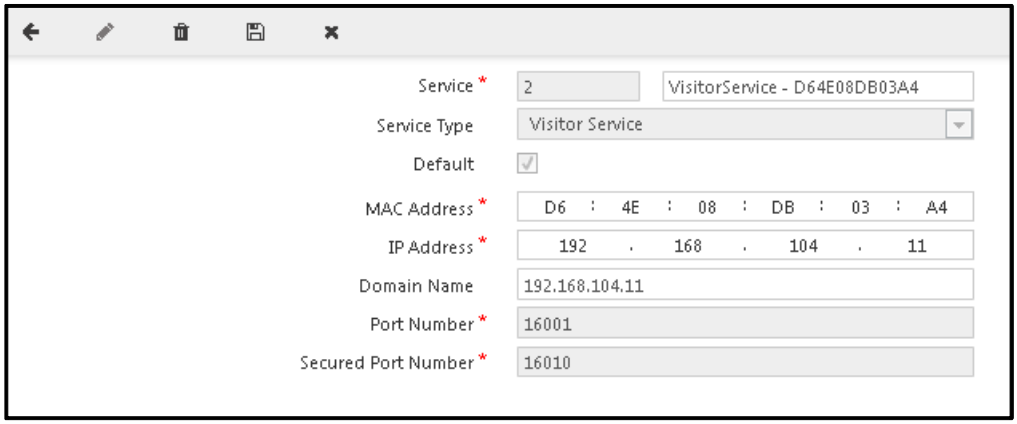
Secured Web Access Port Number: This shows the port number of the computer at which COSEC Web can access the Monitor Service on SSL mode. This port number is entered from Monitor Service Settings.

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



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.

CHAPTER 6

Manage Database

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.

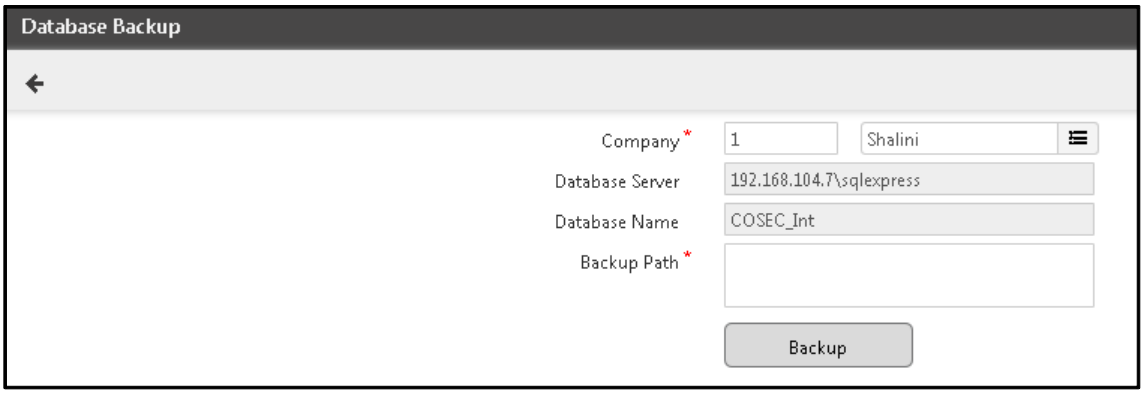
The Company administrator can take backup of company’s database. See“Database Backup”.

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.

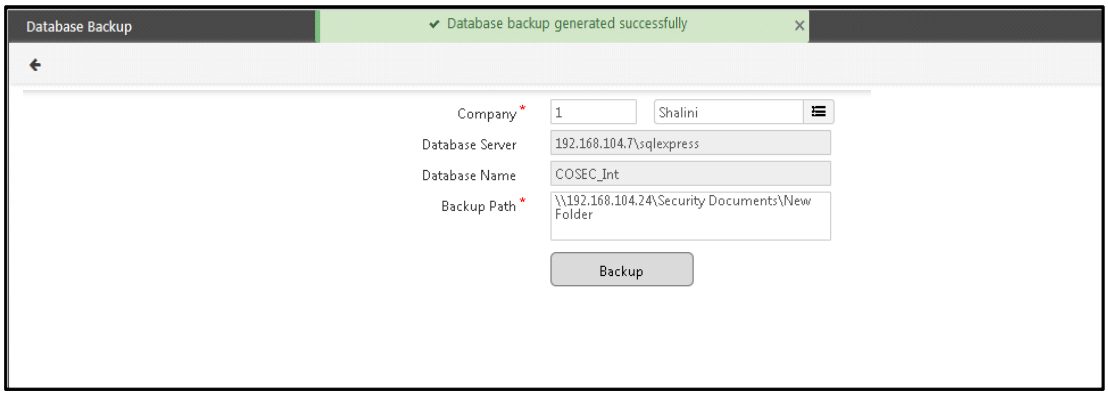
To take backup of database; go to **Manage Database > Database Backup**.



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.



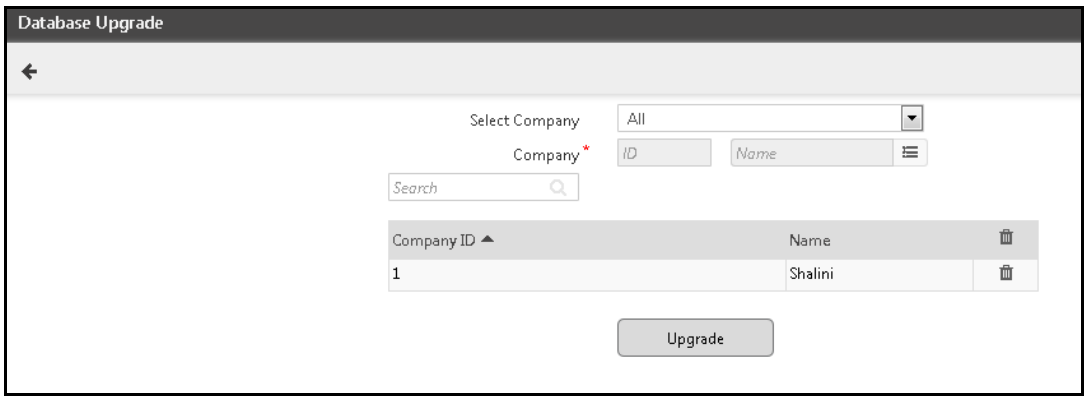
Database Upgrade

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**.

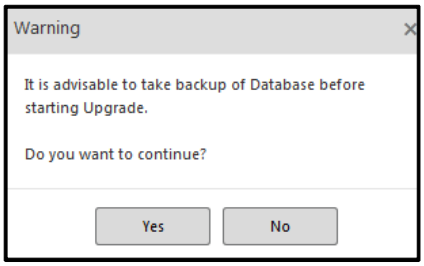
Select Company: You can select the option as **All** or **Select Randomly** depending on the upgradation required.

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

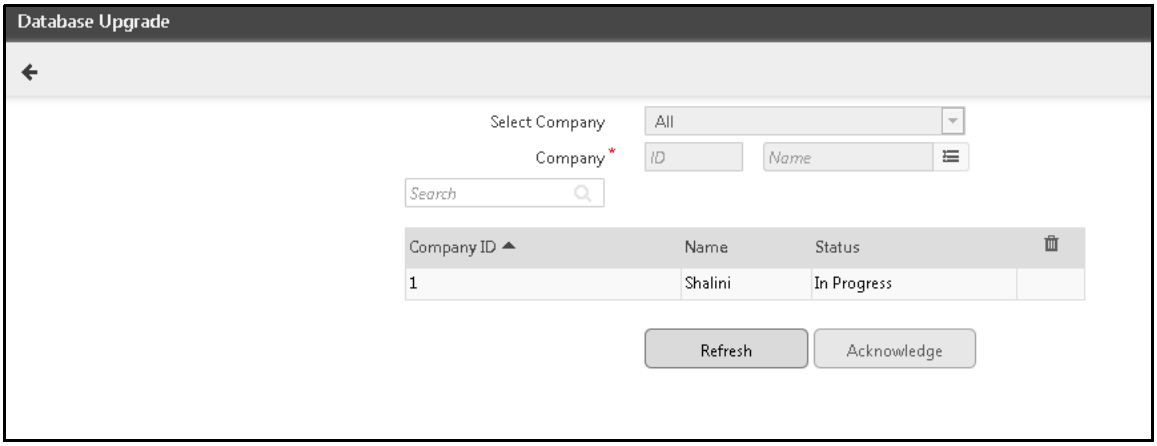


After selecting the company, the profile will be displayed in the grid. Click on **Upgrade** button.

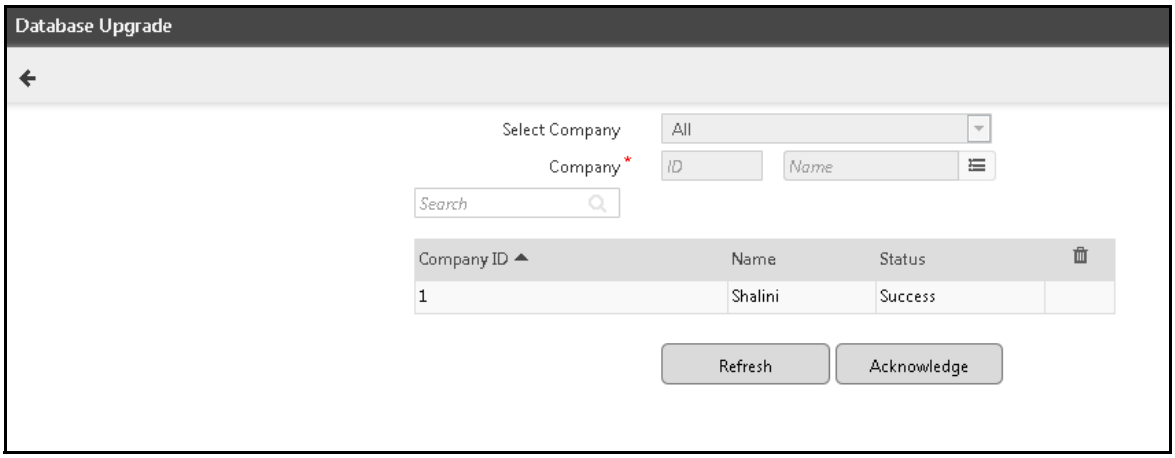
A Warning appears as shown below.You can take backup of database before upgrading. Click **No** and take the backup of existing database from “Database Backup”. If backup is not required; then click **Yes** to continue upgrade.



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



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



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

CHAPTER 7

System Configuration

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

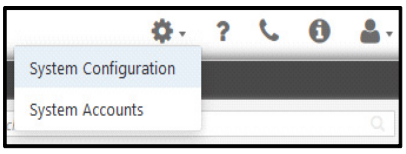
The Secured connection can be established between the Company and the Server after configuring Security settings.

The SMS, Email, WhatsApp notifications can be sent after configuring the SMS, Email as well as WhatsApp Configuration parameters.

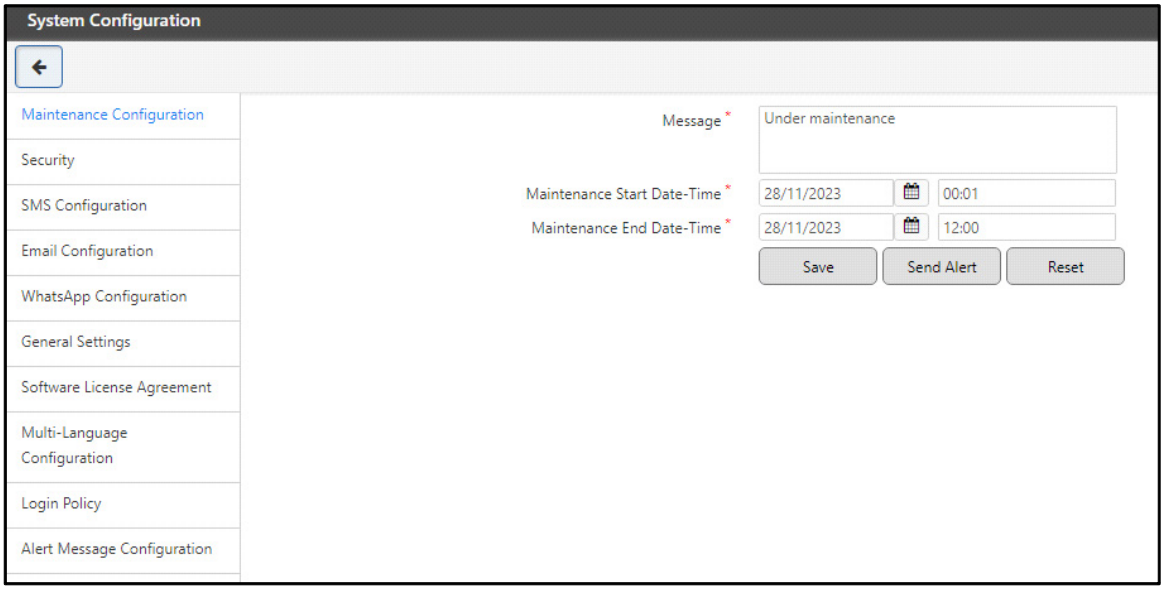
You can also configure the alerts that can be using SMS, Email or WhatsApp by configuring the Alert Message Configurations.

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.

- Click **Setting** and click **System Configuration**



Click on the links for various configurations:



“Maintenance Configuration”
“Security”
“SMS Configuration”
“Email Configuration”
“WhatsApp Integration”
“General Settings”
“Multi-language Configuration”
“Login Policy”
“Alert Message Configuration”

Maintenance Configuration

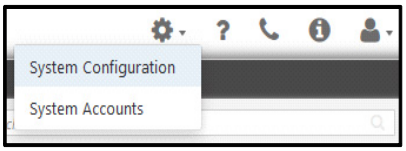
The COSEC System requires maintenance time during up-gradation of versions. During this time the company may not access COSEC application so the Maintenance duration can be configured from here which can be informed to the company.

Make sure you have configured:

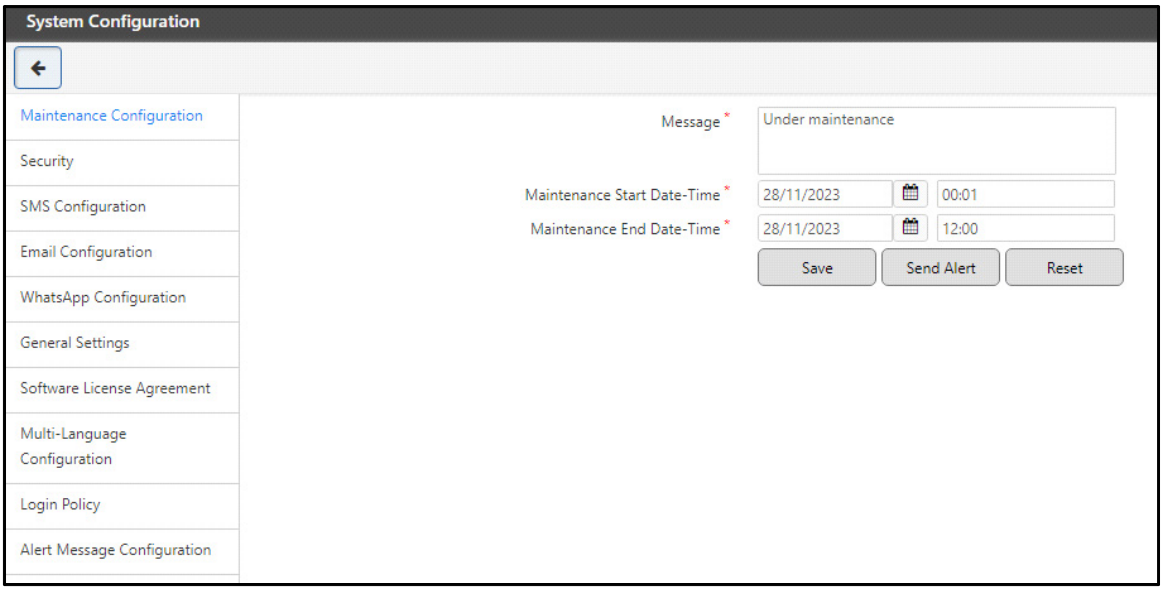
- the Mobile Number and Email ID in the contact details. Refer to “Contact Details” in “Profile” for details.
- the Maintenance Configuration alert, for details refer to “Alert Message Configuration”.

To configure the maintenance information,

- Click **Setting** and click **System Configuration**.



- Click **Maintenance Configuration.**



- **Message:** Enter a message that you wish to display. This message appears in the Maintenance Alert. For details refer to “Alert Message Configuration”.
- **Maintenance Start Date-Time:** Select the start date and specify the time at which maintenance start is planned.
- **Maintenance End Date-Time:** Select the end date and specify the time at which maintenance end is planned.

Click **Save** to save the configuration.

Click **Send Alert** to send the alert immediately.

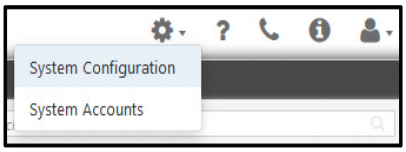
The company/user will get scheduled maintenance message on login page two days prior to Schedule Start Date.

Click **Reset** to clear all the configurations.

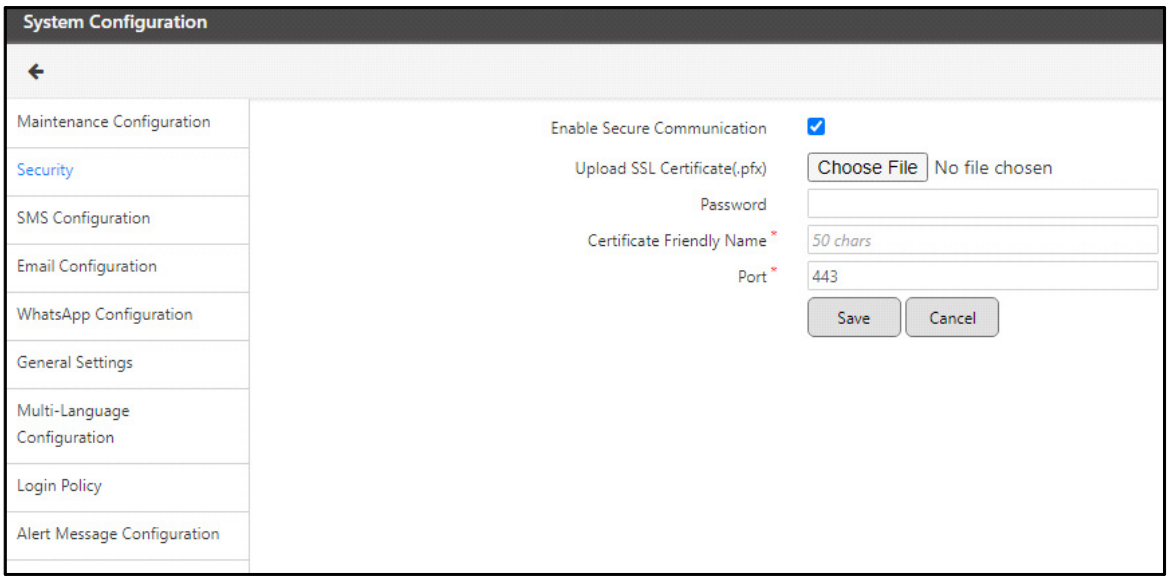
Security

To configure the Secure Communication settings.

Click **Setting** and then click **System Configuration**.



Click **Security.** The page appears as shown below.

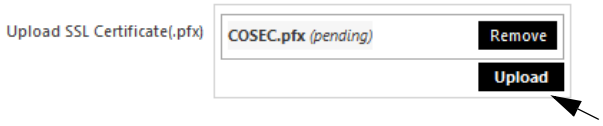


***SSL** or **Secure Sockets Layer** is a security protocol that enables to have secured communication between Client and Server by making use of asymmetric keys. These keys are defined in pairs of public-private key. Public key is available to all clients while private key is only available with the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

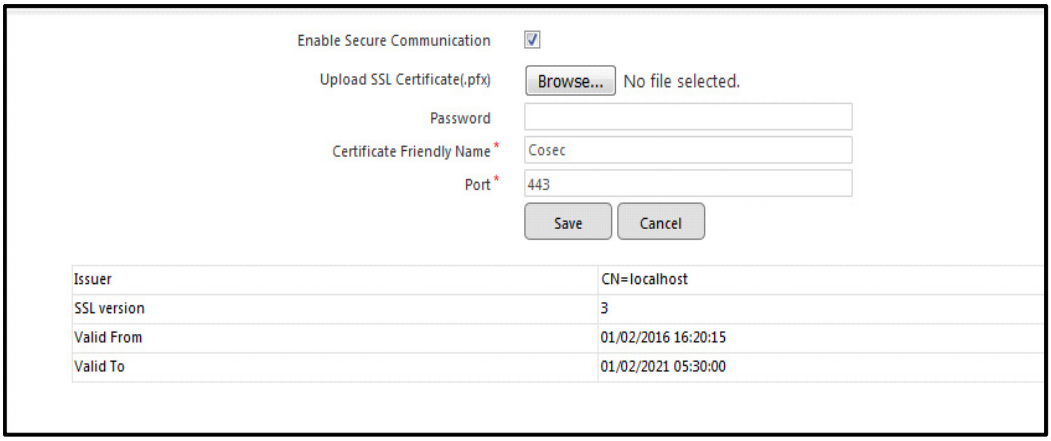
- **Enable Secure Communication**: Select to enable secure communication using SSL encryption.
- **Upload SSL Certificate(.pfx)**: Click to browse the file through your system and select the SSL certificate to be uploaded as a *.pfx file. Click **Upload**.



- **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.



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

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.

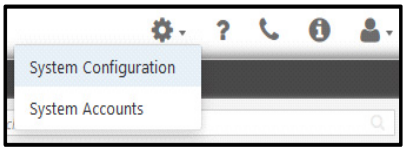
Restarting any COSEC Service will only be possible when it is accessible from Master Service. If not then user has to restart it manually.

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.

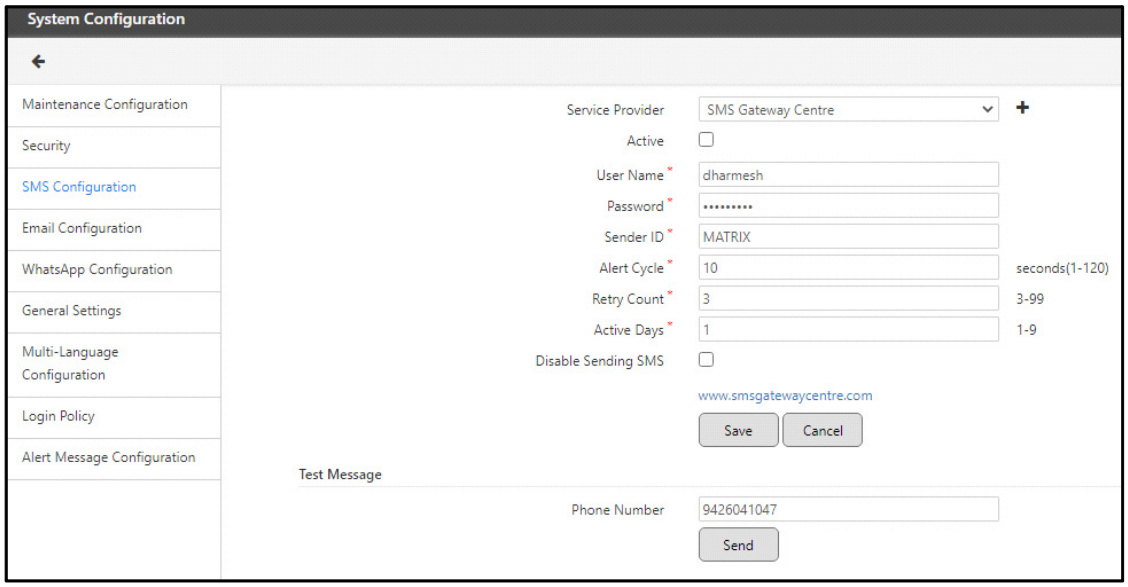
SMS Configuration

For SMS configuration settings,

Click **Setting** and then click **System Configuration**.



Click **SMS Configuration.** The page appears as shown below.



For additional security and privacy while sending SMS, COSEC supports Proxy Server Configuration. For more details, refer to "Proxy Server Configuration".

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.

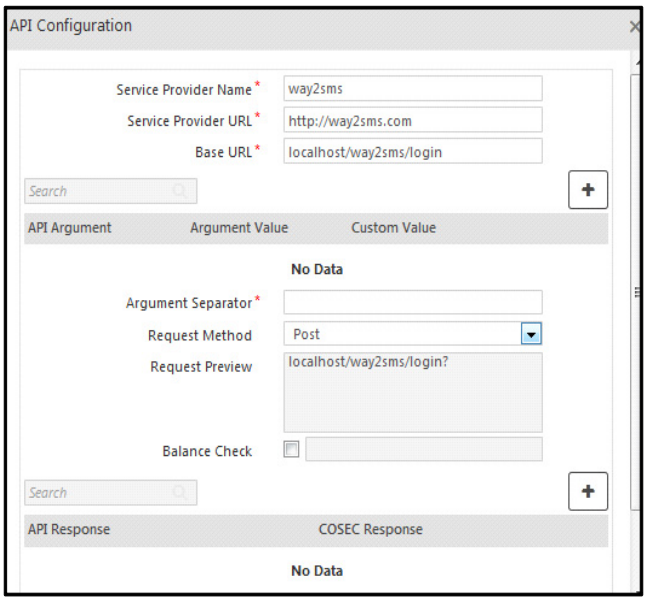
Disable Sending SMS: Check this box for temporarily disabling the SMS sending functionality.

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

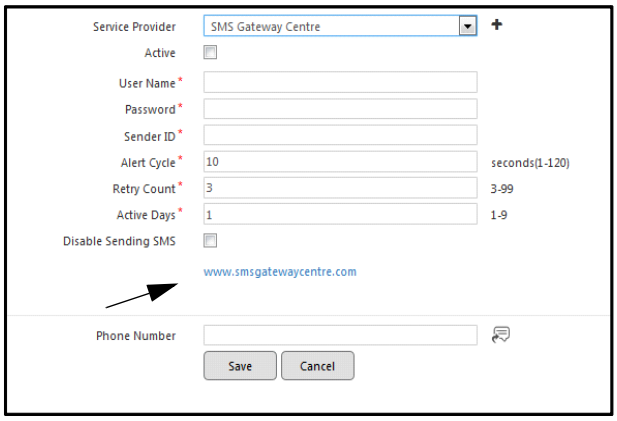
To add a new service provider, click the + button. The **API Configuration** window appears on your screen.



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”)

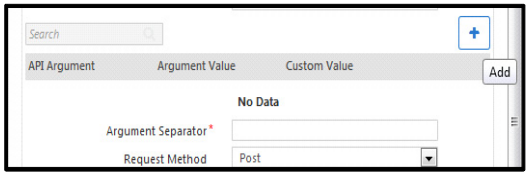
Service Provider URL: Enter the URL of the service provider.This url is displayed on the main SMS Setting page as shown in the screen below.

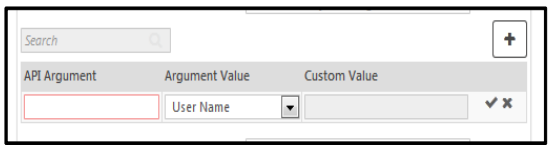


Base URL: Enter the base url of the service provider as given in the API document. This is used for sending the message through SMS.

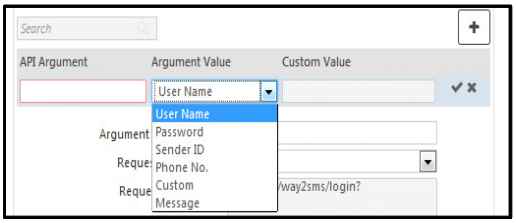
> **Example:** In the following url: “localhost/way2sms.com?uname=test;pwd=test;number=test;sid=test”, the url before the question mark is the base url and the remaining part is the argument and its value as shown in the screen below.

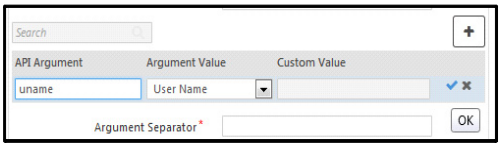
Now add the **API arguments** by clicking on **Add** icon as shown below.



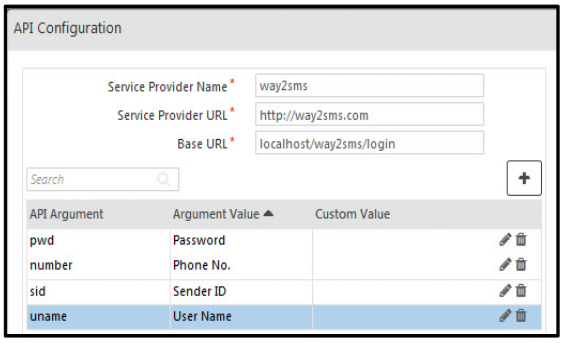


- **API Argument**: Enter the API argument name specified in the API document of the service provider.
- **Argument Value**: Select the argument value from the dropdown list which is to be associated with the API argument. Eg: Select the Argument value one by one from the drop down options. Eg: Select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



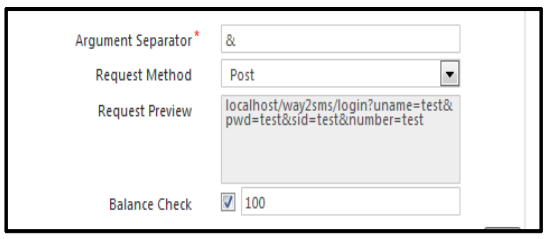


Click **Add** icon to associate **API Arguments** with the **Argument value**. These API arguments are available in the API document of the service provider. The added arguments get displayed in the grid below.



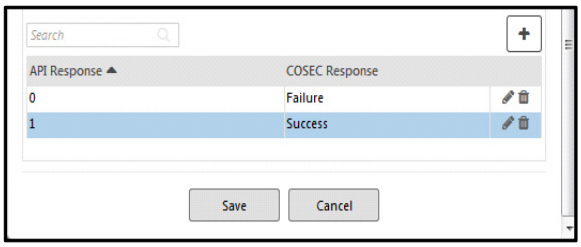
One can also click **Delete** icon, if any argument is to be removed. Further, one can also edit any argument by clicking on it, editing the argument and then clicking **Update**.

- **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.

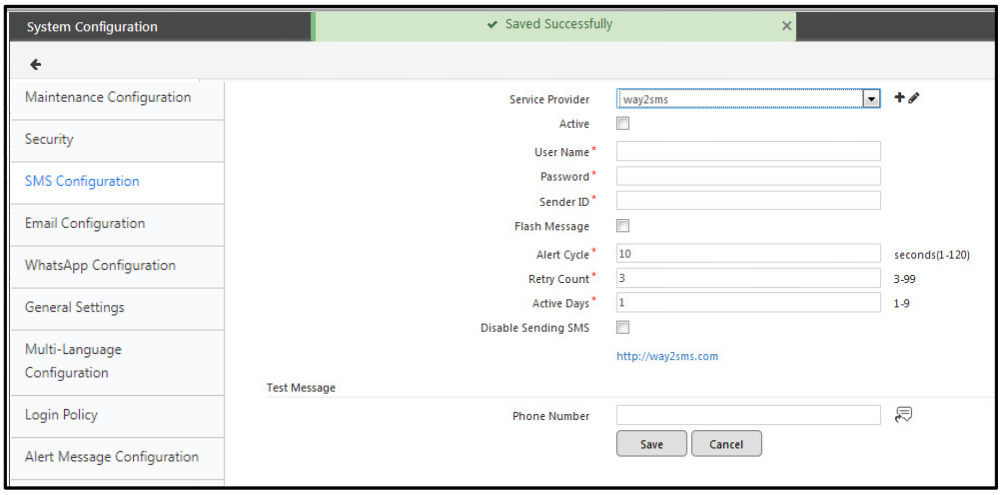


- **API Response**: Enter the API Response to be used for the selected **COSEC Response** from the dropdown list. Click **Add** button and the response gets displayed in the grid.

  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 withe value success.



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.

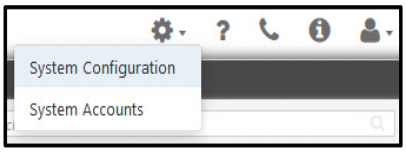


*To edit API configuration for a user-defined service provider, on the **SMS Setting** page, select a service provider and click the Edit button.*

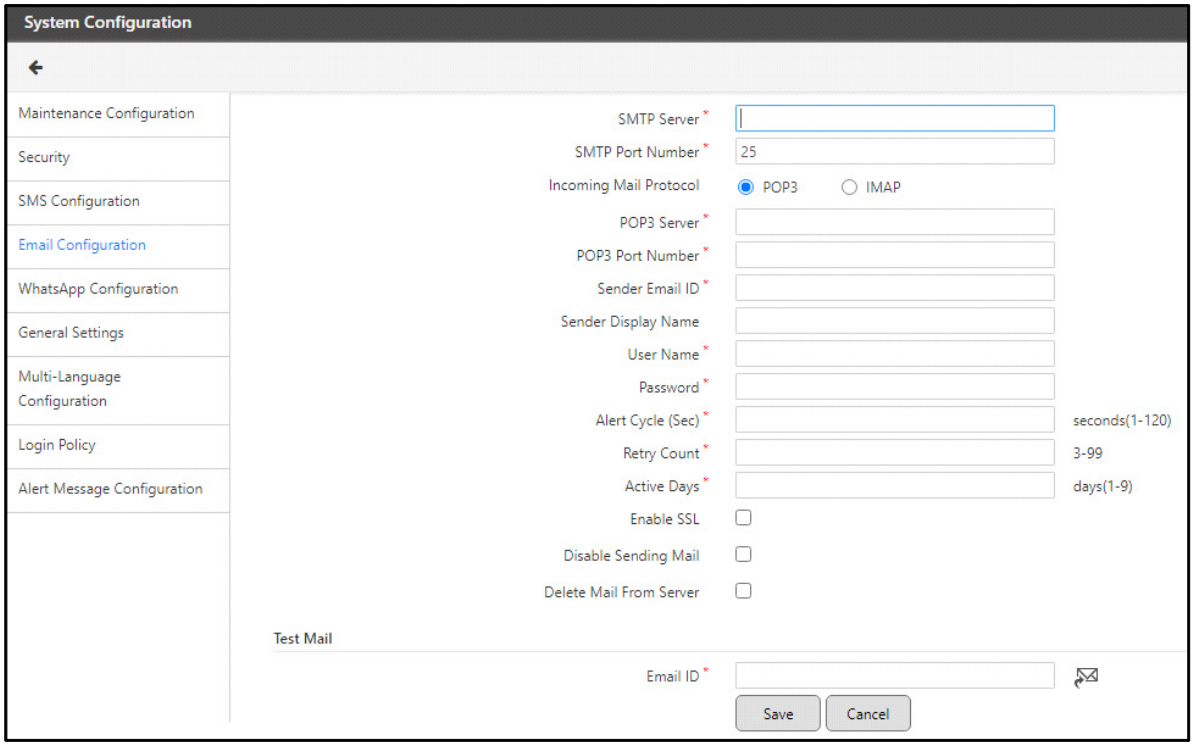
Email Configuration

For Email configuration settings.

Click **Setting** and then click **System Configuration**.



Click **Email Configuration.** The page appears as shown below.



For additional security and privacy while sending Emails, COSEC supports Proxy Server Configuration. For more details, refer to "Proxy Server Configuration".

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.

WhatsApp Integration

In today's world as we move ahead with technology, WhatsApp has become an integral part of businesses and hence its integration with COSEC is the need of the hour.

Integrating WhatsApp with COSEC will enable you to send/receive messages on WhatsApp.

To integrate WhatsApp with COSEC, you need to:

- Configure the WhatsApp parameters, refer to "WhatsApp Configuration" for details.
- Enable WhatsApp in Alert Message Configuration. refer to "Alert Message Configuration" for details.
- Make sure the contact details have been configured. Refer to "Contact Details" in "Profile" for details.

For additional security and privacy while sending WhatsApp messages, COSEC supports Proxy Server Configuration. For more details, refer to "Proxy Server Configuration".

WhatsApp Configuration

The WhatsApp Configuration includes two steps:

- Fulfilling the Pre-requite requirements, for details refer to "Pre-requisites".
- Configuring the WhatsApp parameters, for details refer to "Configuring WhatsApp Parameters".

Pre-requisites

To use WhatsApp for sending and receiving messages make sure you have completed the following:

Make sure you have persistent Internet connectivity.

The details mentioned below are as per the current (Oct, 2023) updates available on the official website of Meta.These are subject to change. To know more visit their official website: ***https://developers.facebook.com.***

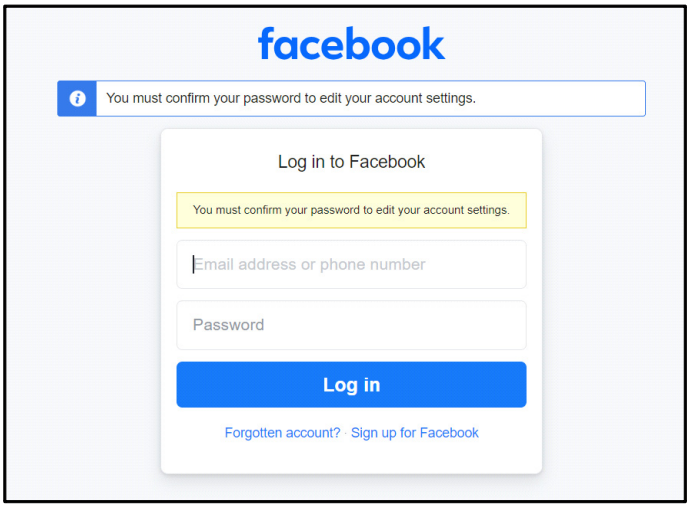
- Registered as a Meta Developer, refer to "Register as a Meta (Facebook) Developer".
- Enabled Two- Factor Authentication for your account, refer to "Enable Two-Factor Authentication".
- Created a Meta App, refer to "Create an App".
- Added a Phone Number in the Meta App, refer to "Add a Phone Number".
- Made the payment as per your requirement, refer to "Add Payment Method".
- Created a Permanent Toke for usage, refer to "Creating a Permanent Access Token".

Register as a Meta (Facebook) Developer

To register as a Meta Developer, following the steps given below:

- To start the registration process

  Login into your Facebook Account.



Make sure your Facebook Account is Meta verified and complies to all the Terms and Conditions of Meta. To do so, access your Facebook Account Setting & privacy > Meta Account Center > Meta Verified. Make sure you follow the instructions and fulfill all the necessary Meta requirements for the same.

- Agree to the Terms and Policies.

  Click **Next** to agree to the Platform Terms and Developer Policies.

- Verify your account

  A confirmation code will be send to the phone number and email address that you provide in order to confirm that you have access to them. Your number and email will be used for important developer notifications of any changes that may impact to your app.

- Select your occupation

  Select an occupation that most closely describes what you do for a living.

  The registration process is completed.

Enable Two-Factor Authentication

Two-factor authentication is a security feature that helps protect your Facebook account in addition to your password. If you set up two-factor authentication, you will be asked to enter a special login code or confirm your login attempt each time someone tries accessing Facebook from a browser or mobile device that Facebook does not recognize. You can also get alerts when someone tries logging in from a browser or mobile device that Facebook does not recognize.

Turning-on/managing two-factor authentication:

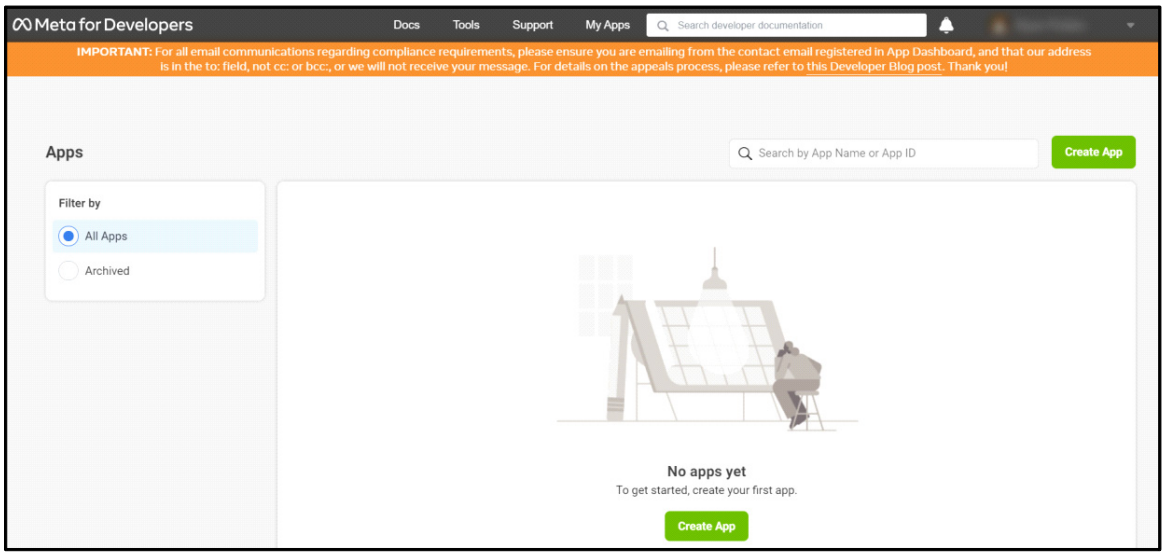
- Go to your **Security and Login Settings**.
- Scroll down to **Use two-factor authentication** and click **Edit**.
- Choose the any one of the three security method that you wish to add and follow the on-screen instructions.
    - Tapping your security key on a compatible device.
    - Login codes from a third-party authentication app.
    - Text Message (SMS) codes from your mobile phone.

Create an App

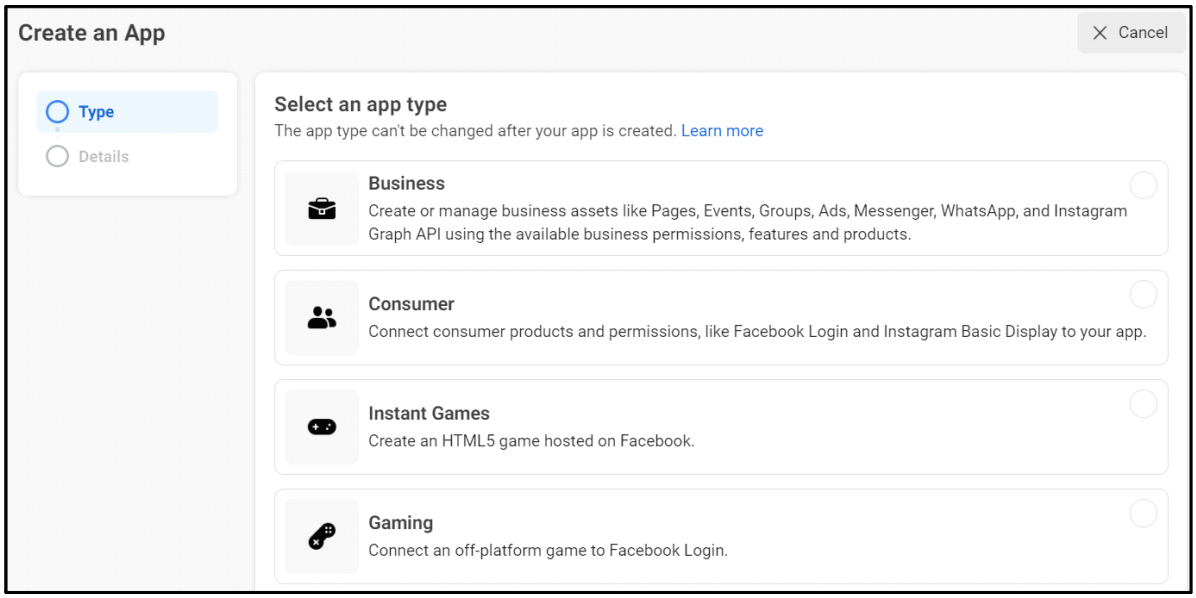
Making sure you have a developer account on Meta for Developers. You also need WhatsApp installed on a mobile device to send test message.

To create the App, following the steps mentioned below:

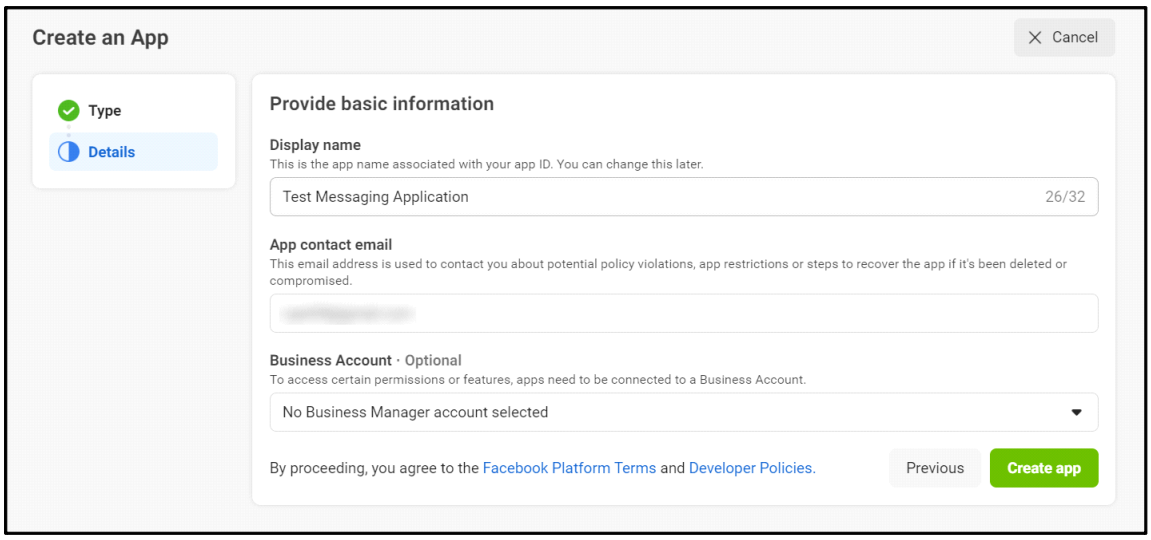
- Once you are signed in, you see the Meta for Developers App Dashboard. Click **Create App** to get started.



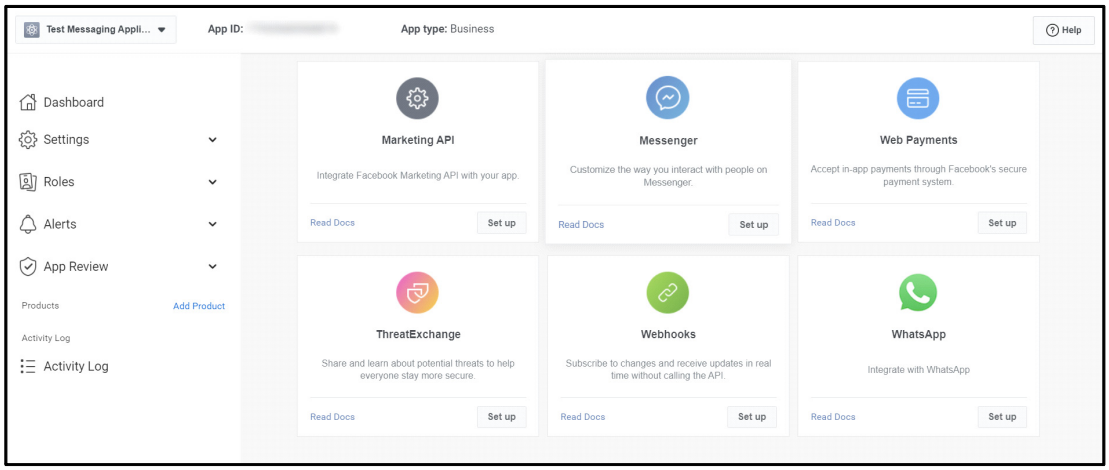
- Select **Business** as the **App Type**.



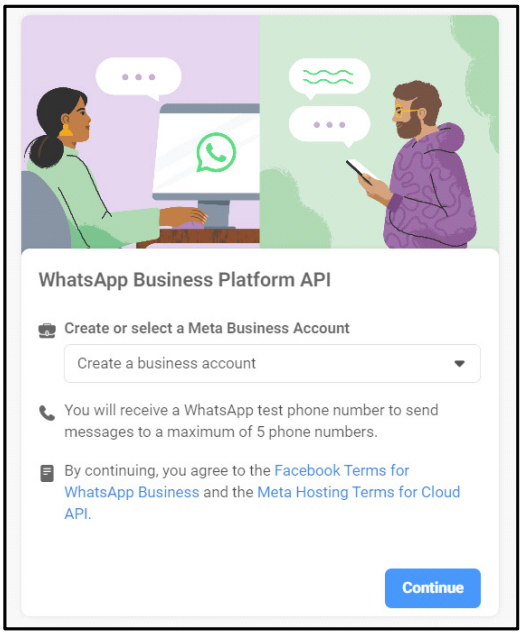
- Enter the **Display Name** for your App and an **Email Address** where you wish to receive any important developer notifications. The email address can be different from the email address associated with your Facebook account, just make sure it is valid and that you monitor it, since all important developer notifications will be sent there.



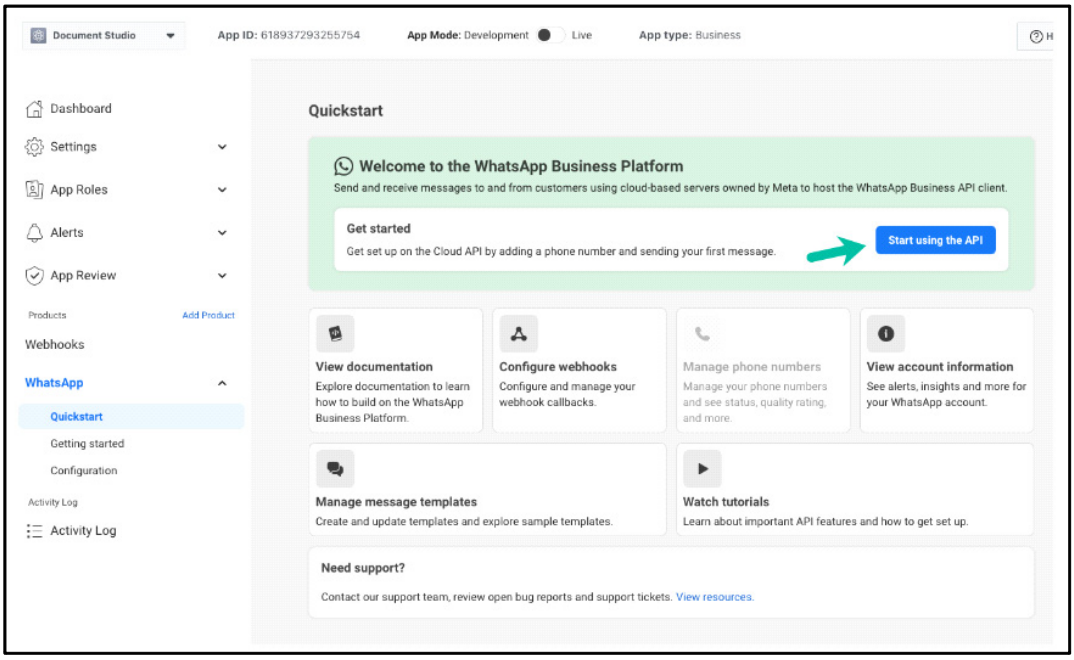
- You need to add products to your App. Scroll down until you see **WhatsApp** and click the **Set up**.



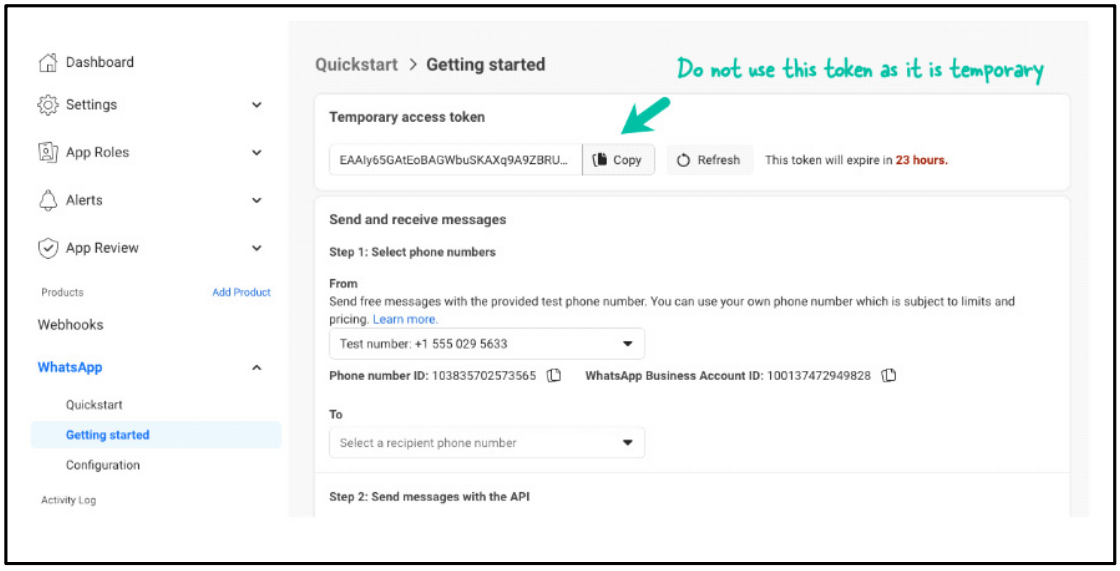
- Finally, choose an existing Meta Business Account or ask the platform to create a new one and click **Continue.**



- Click on **Start using the API** on the next screen.



Facebook will now generate a temporary access token that allows you to test your WhatsApp Cloud API integration. However, we will not use this token since it expires after 24 hours. So instead, we will generate a permanent access token. For details, refer to “Creating a Permanent Access Token”.

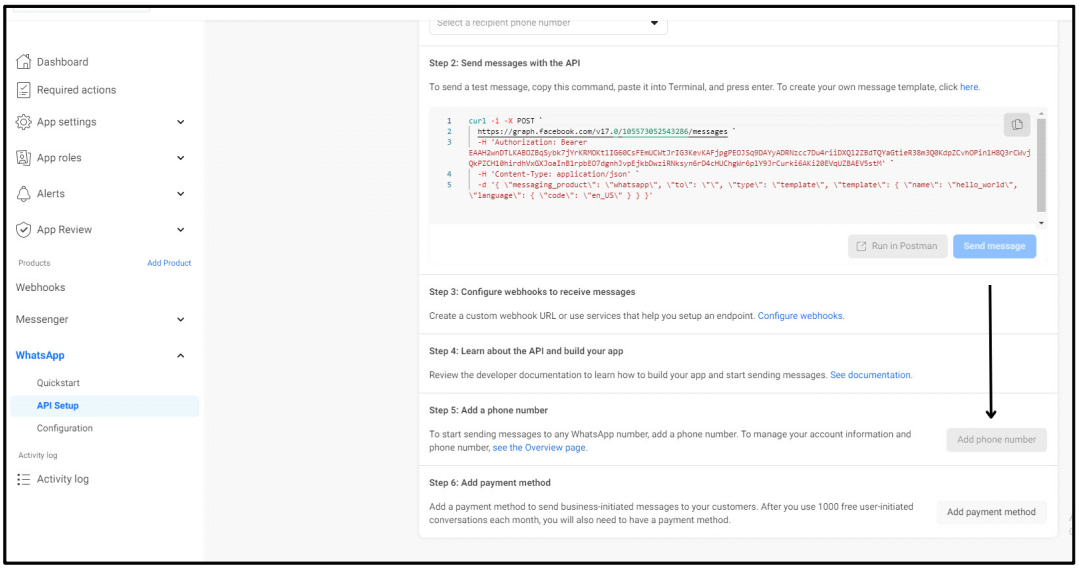


Send a message with the test number generated by WhatsApp to your Business WhatsApp number to test if your integration is a success.

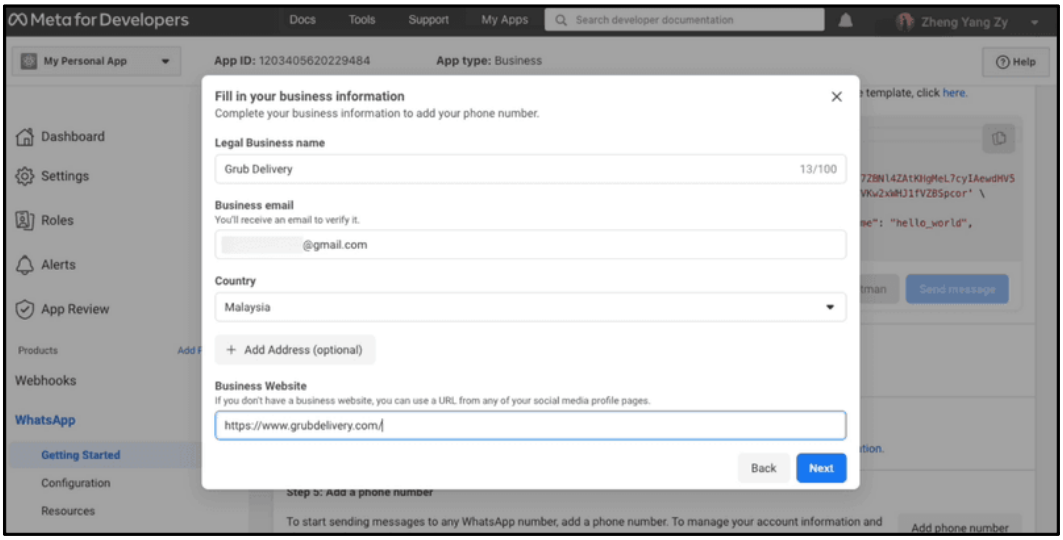
Next, you need to add your phone number to your WhatsApp Cloud API account.

Add a Phone Number

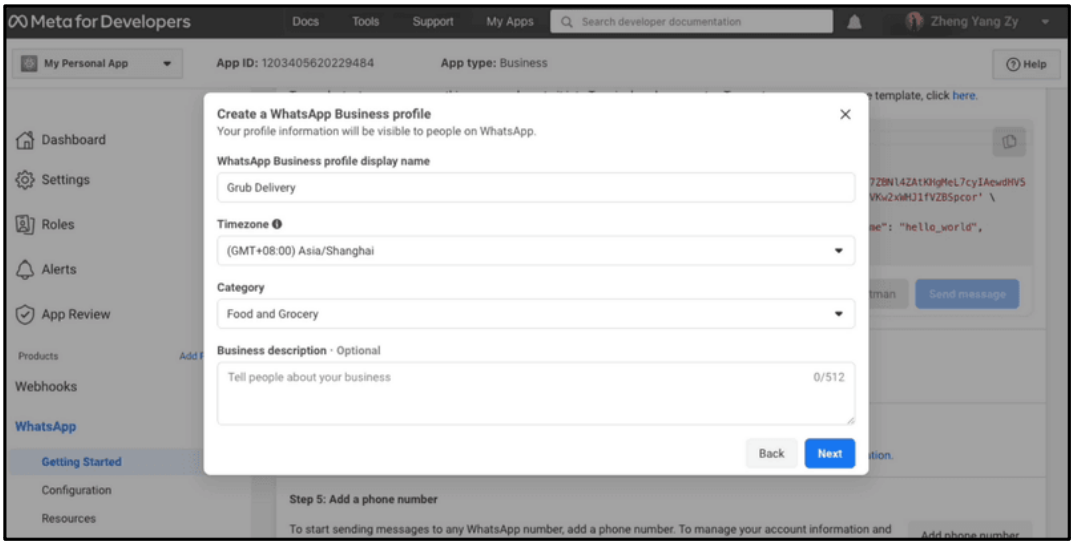
- Scroll down on the page and click **Add phone number**. You need to associate a phone number with the WhatsApp API to send messages to any WhatsApp number.



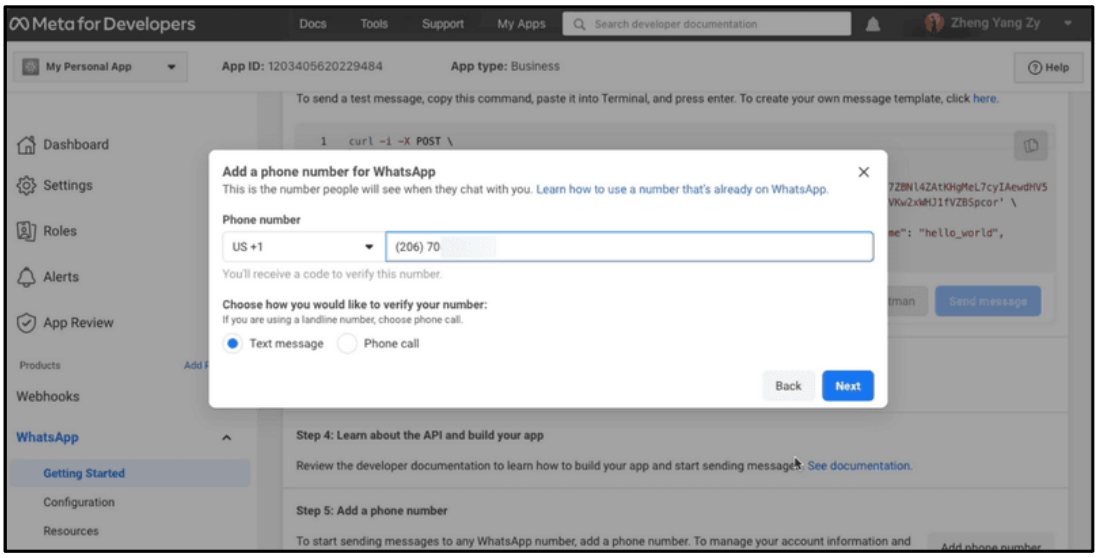
- Fill in your business information and click **Next**.



- Fill in your WhatsApp Business profile information and click **Next**.



- Add a phone number for your WhatsApp Cloud API.

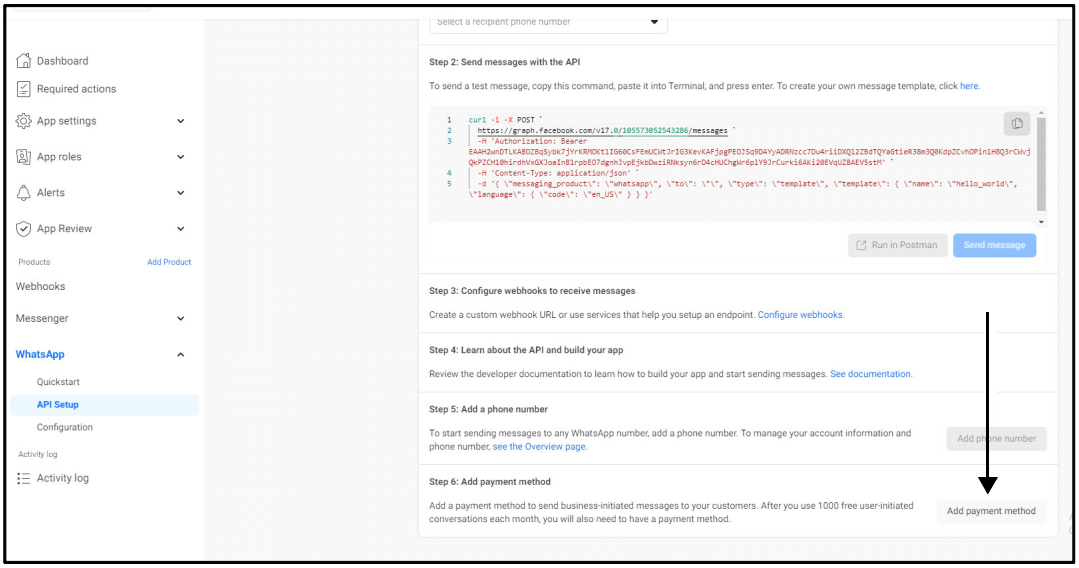


Make sure that when you are adding a number it is a new number and has never been used in WhatsApp.

- To verify the phone number you added, a 6-digit verification code will be sent to the number. Enter the verification code once you receive it.

Add Payment Method

- Click **Add payment method**.



Follow the steps and complete the payment.

Next, copy and save the **WhatsApp Business Account ID** for this phone number.

Creating a Permanent Access Token

Knowing that you need to use a bearer token in the Authorization Header of an HTTP request is helpful, but it is not enough. The only access token you have seen so far is temporary. Chances are that you want your App to access the API for more than 24 hours, so you need to generate a longer-lasting access token.

The Meta for Developers platform makes this easy. All you need to do is add a System User to your business account to obtain an access token that you can use to continue accessing the API.

To create a system user, following the steps:

- Go to **Business Settings**.
- Select the business account your app is associated with.
- Select **Users > System Users**.
- Click **Add**.
- Configure a **Name** for the system user, choose **Admin** as the user role, and click **Create System User** to continue.
- Select the **whatsapp_business_messaging** and **whatsapp_business_management** permission.
- Click **Generate New Token** to generate a permanent access token.
- Please copy the access token and save it in your notepad as it will not be visible again on your Facebook Dashboard.

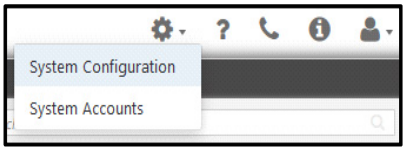
Configuring WhatsApp Parameters

WhatsApp configuration includes the following:

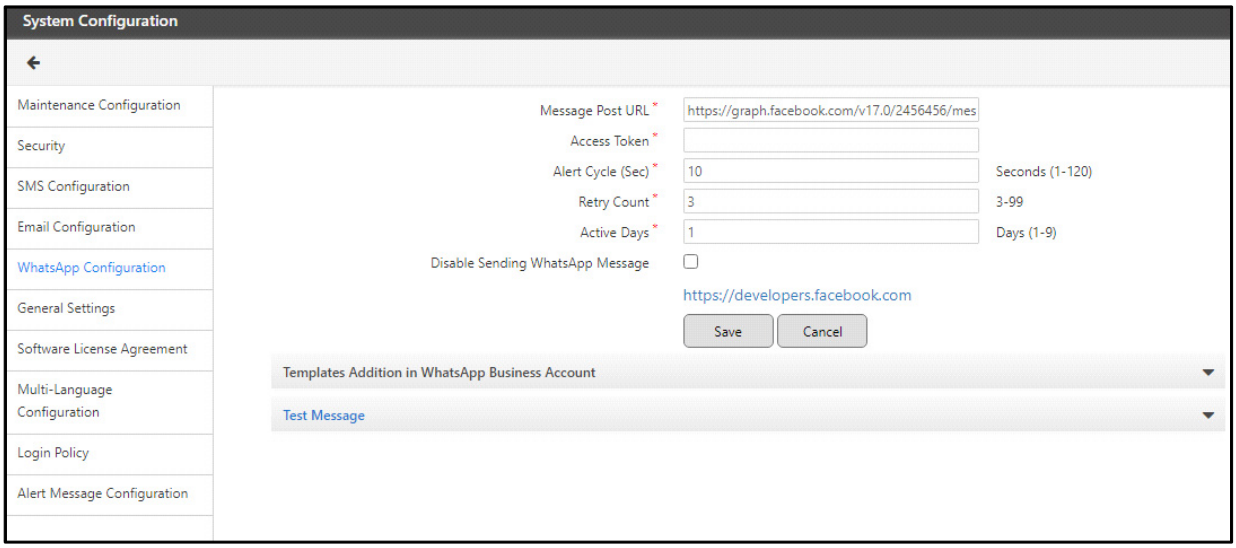
- "WhatsApp Parameters"
- "Templates Addition in WhatsApp Business Account"
- "Test Message"

WhatsApp Parameters

- Click **Setting** and then click **System Configuration**.



- Click **WhatsApp Configuration** and the following screen appears.



Configure the following parameters:

- **Message Port URL:** This is the URL that will be used for sending WhatsApp Messages.

  Default: https://graph.facebook.com/v17.0/{Phone_Number_ID}/messages

  You only need to change the {Phone_Number_ID} in the URL, with your actual Phone Number ID. The Phone Number ID can be taken from the WhatsApp Business Account you created.

  You also need to check if the version mentioned in the URI, that is v17.0, is the same as your WhatsApp Business Account Version. If not, change it as per your account version.

  For example, if your Phone Number ID is 123115956238956 and version is 18, then the URL will be: https://graph.facebook.com/v18.0/123115956238956/messages.

The system will only consider the configured URL for sending messages. Make sure it is configured correctly.

- **Access Token**: Enter the token number received after you have successfully created the WhatsApp Business Account.
- **Alert Cycle (Sec)**: Specify the time in seconds between successive send attempts when the system tries to send the pending messages. Valid Range: 1 to 120.
- **Retry Count**: Specify the number of times the system needs to retry to send the same message in the event of an unsuccessful attempt. Valid Range: 3 to 99.
- **Active Days**: Specify the number of days the system needs to keep the unsent messages active in the event of the service being stopped. Valid Range: 1 to 9.
- **Disable Sending WhatsApp Message:** Select the check box if you do not wish to send WhatsApp messages.

Click **Save** to save the configurations.

Templates Addition in WhatsApp Business Account

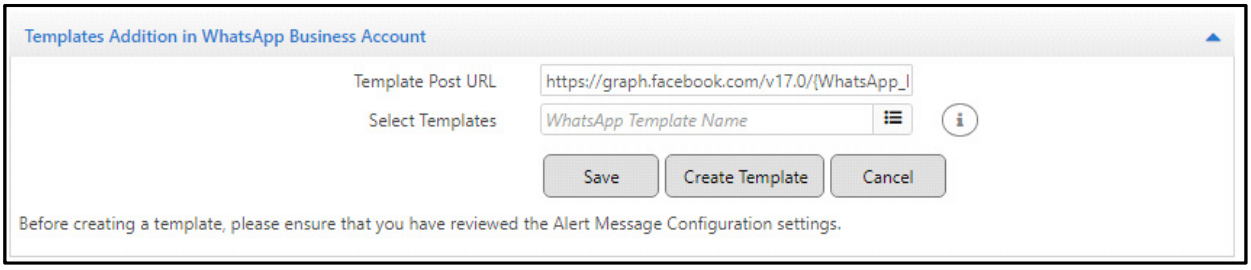
*Make sure you have visited their official website:**https://developers.facebook.com** and read the guidelines provided for the Templates.*

Before you add any template to your WhatsApp Business Account make sure:

- *you have updated/edited the templates as per your requirement from Alert Messages. For details, refer to "Alert Message Configuration". If you have sent the template/s to your WhatsApp Account and then modify the same from Alert Messages, you will have to manually update/edit/delete the templates from your WhatsApp Account..For smooth functioning of WhatsApp, make sure the content of the Alert Templates and the WhatsApp Templates are identical.*
- *you do not have any template/s with the same name/s already created in your WhatsApp Account. If same name template/s are found in your WhatsApp Account and you select the same here, then these templates will not be sent to your WhatsApp Account.*
- *you have checked the WhatsApp Busines Policy. As per the WhatsApp Business Policy, you can create 100 templates per hour. The policies are frequently updated, hence refer to the policy details once before you move further.*
- *you have noted your WhatsApp Business Account ID. To check your WhatsApp Business Account ID, navigate to Business Manager > Business Settings > Accounts > WhatsApp Business Accounts.Click on the your account. A panel opens with the information of your account as well as ID.*
- *you have noted the App ID of your WhatsApp Business Account.To check your WhatsApp Business Account ID, navigate to Business Manager > Business Settings > Accounts > WhatsApp Business Accounts.Click on the your account. A panel opens with the information of your account as well as ID.*

You can select the Templates that you wish to add in your WhatsApp Business Account. To do so,

- Click the **Templates Addition in WhatsApp Business Account** collapsible panel and configure the following:



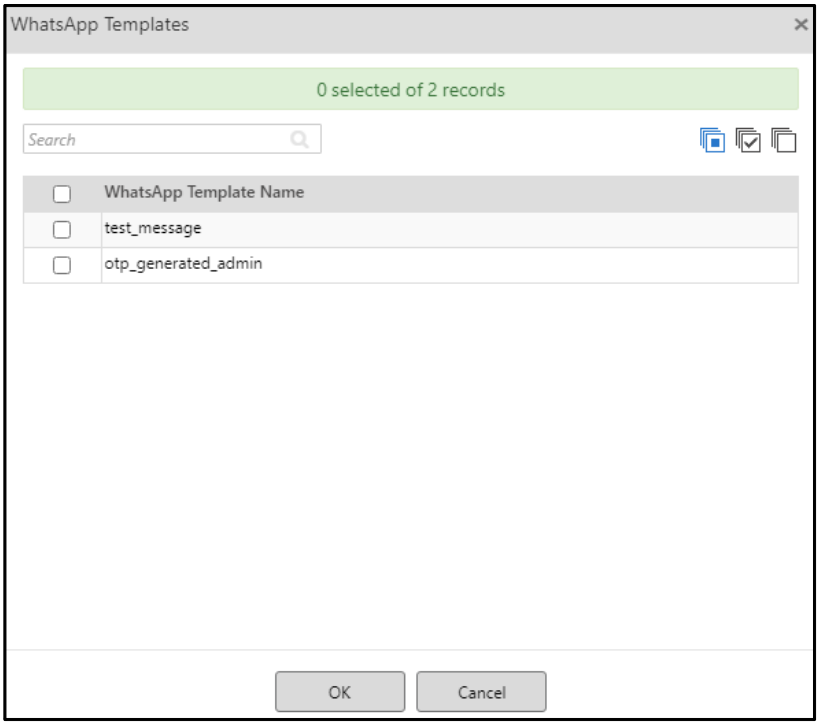
- **Template Post URL:** The default value is :https://graph.facebook.com/v17.0/{WhatsApp_Business_Account_ID}/message_templates.

  You need to replace the {WhatsApp_Business_Account_ID} with your WhatsApp Business Account ID. While replacing the text make sure you remove the brackets and do not change the format. For example: https://graph.facebook.com/v17.0/111000111100/message_templates

- **App ID**: Enter the App ID of your WhatsApp Business Account.

- Click **Save** to save the configurations.

- **Select Templates:** Click the picklist. The **WhatsApp Templates** pop-up appears.



The names of the WhatsApp Templates appear as configured in Alert Messages. The Templates will be added to your WhatsApp Business Account in the language that you have selected in Alert Messages. For details refer to "Alert Message Configuration".

The Maintenance Template is as per the user requirement, hence this needs to be created manually in your WhatsApp Business Account. Alert will be sent only after the same is approved by WhatsApp.

After the Templates are sent to you WhatsApp Business Account, Alerts will be sent only after these templates are approved by WhatsApp.

To select the desired templates, select the check boxes of the desired templates.

- Click **OK**. Hover-over the **Info** icon. It displays the number of selected templates.

- Click **Create Template** to create the templates in your WhatsApp Business Account. The templates will appear in your WhatsApp Account once these are approved by WhatsApp.

If you wish to abort, click **Cancel**.

To save the configurations, click **Save**.

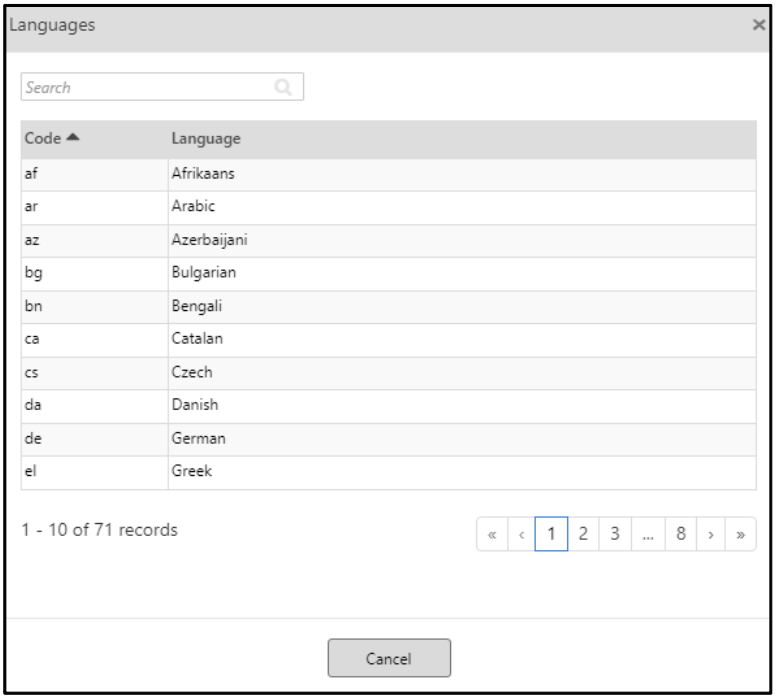
If the template/s creation fails, the reasons for failure will be displayed under the **Error List** collapsible panel. For details, refer to "Error List".

Test Message

You can send a test message to check if your WhatsApp integration is successfully.To do so,

- Click the **Test Message** collapsible panel and configure the following:

- **Template Language:** Click the picklist. The **Languages** pop-up appears.



  Select the language in which you wish to send the test message.

- **Template Name:** Enter the name of the template that you wish to send as the test message. The content of the template will be content of the test message.

Make sure:
- *the template you selected as the test message has only plain text and no variables.*
- *the template is registered and approved by WhatsApp.*

- **Phone Number:** Enter the phone number to which you wish to send the test WhatsApp message.

Click **Send**, to send the test message.

Error List

Click the **Error List** collapsible panel to view the reason for the failure in sending the templates to your WhatsApp Business Account.

The name of the template/s along with the reason for failure are displayed.

Proxy Server Configuration

COSEC provides the provision for configuring the Proxy Server. A Proxy Server acts as a gateway between the end user and the internet. All the outbound internet traffic will flow through the Proxy Server on its way to the address requested. Proxy Servers encrypt the outbound web requests as well as the destination server would not know who actually made the original request. Hence using Proxy Servers enhances security as well as privacy.

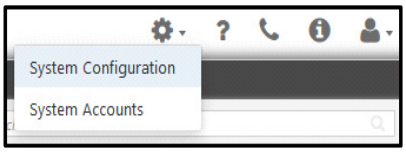
COSEC provides the provision to select the services — SMS, Email, WhatsApp, Virtual License — for which you wish to use Proxy Server for outbound requests.

Proxy Server Configuration is applicable to COSEC Centra and OEM.

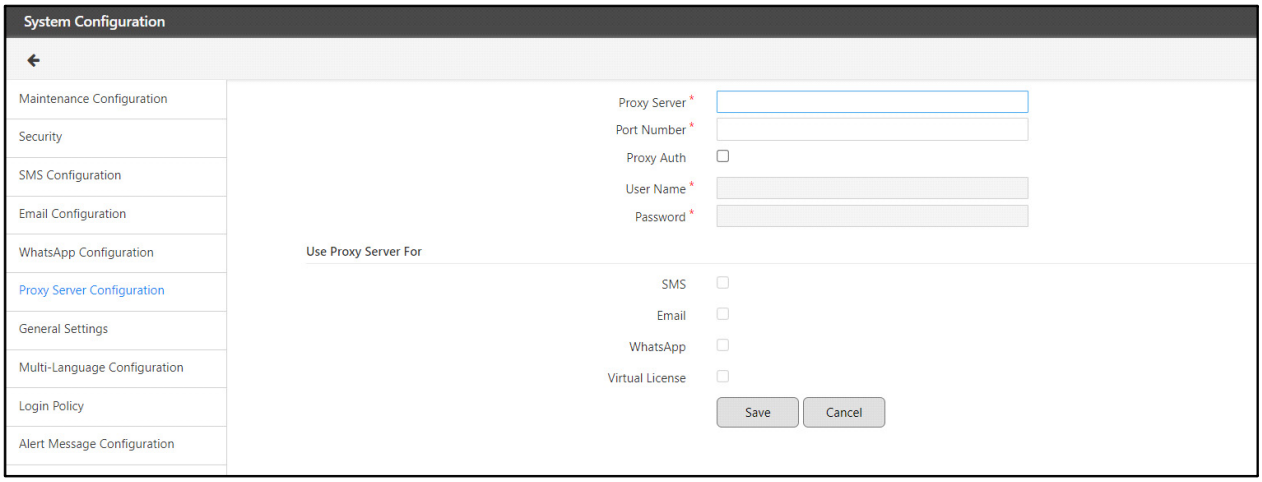
Make sure there is persistent internet connection where the Proxy Server is installed.

To configure the Proxy Server parameters,

Click **Setting** and then click **System Configuration**.



Click **Proxy Server Configuration** and the following screen appears.



Configure the following parameters:

- **Proxy Server:** Configure the IP Address of your Proxy Server. It can be a maximum of upto 50 characters. Default: Blank.
- **Proxy Port:** Configure the Port of your Proxy Server. It can be a maximum of upto 5 characters. Valid Characters: 0 to 9 and Valid Range: 1 to 65535. Default: Blank.
- **Proxy Auth:** By default, the Proxy Auth check box is selected, that is authentication is enabled and you need to configure the User Name and Password for the same. Clear the check box to disable.

- **User Name:** Configure the User Name that is to be used for logging into the Proxy Server. It can be a maximum of upto 50 characters.

  Valid characters are ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 1234567890/_\\.@:

- **Password:** Configure the Password that is to be used for logging into the Proxy Server. It can be a maximum of upto 128 characters.

  Valid characters are !\"#$%&'()*+,- 0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\\]^_`abcdefghijklmnopqrstuvwxyz{|}~

Use Proxy Server For

If you have configured the Proxy Server and Proxy Port, then you can select the services for which you wish to use the Proxy Server for outbound requests. To do so, configure the following:

- **SMS:** Select the check box to enable. Default: Disabled.
- **Email:** Select the check box to enable. Default: Disabled.
- **WhatsApp:** Select the check box to enable. Default: Disabled.
- **Virtual License:** Select the check box to enable. Default: Disabled.

Click **Save** to save the configurations.

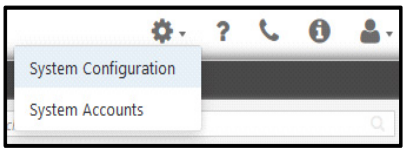
General Settings

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

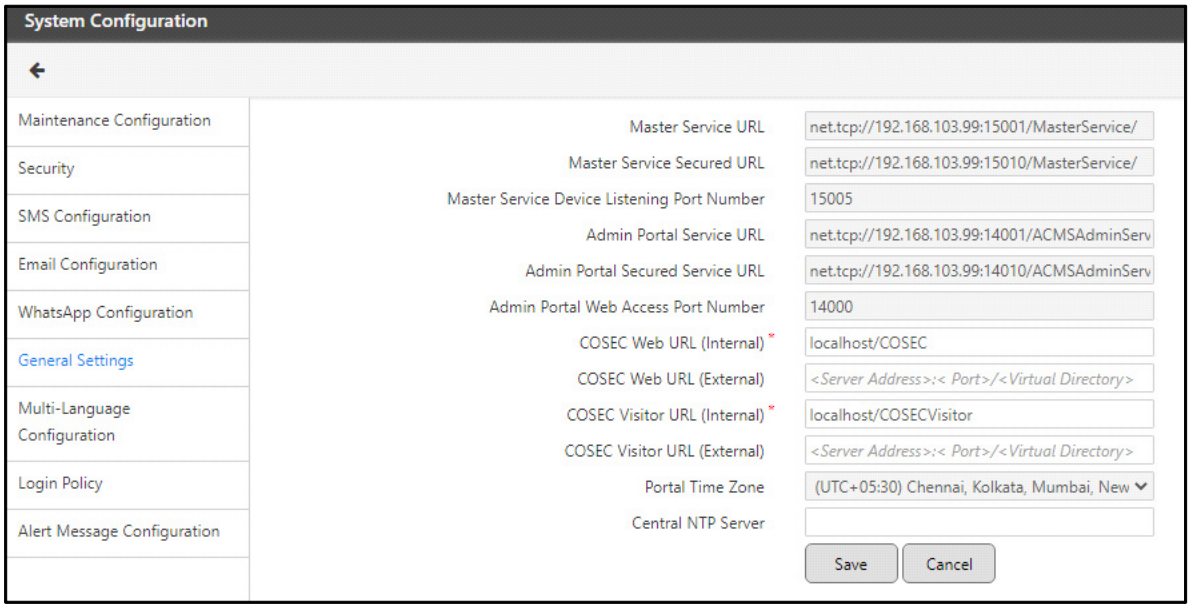
Once the service URLs are entered, then the fields shown below will be non-editable.

For General settings,

Click **Setting** and then click **System Configuration**.



Click **General Settings.** The page appears as shown below.



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.

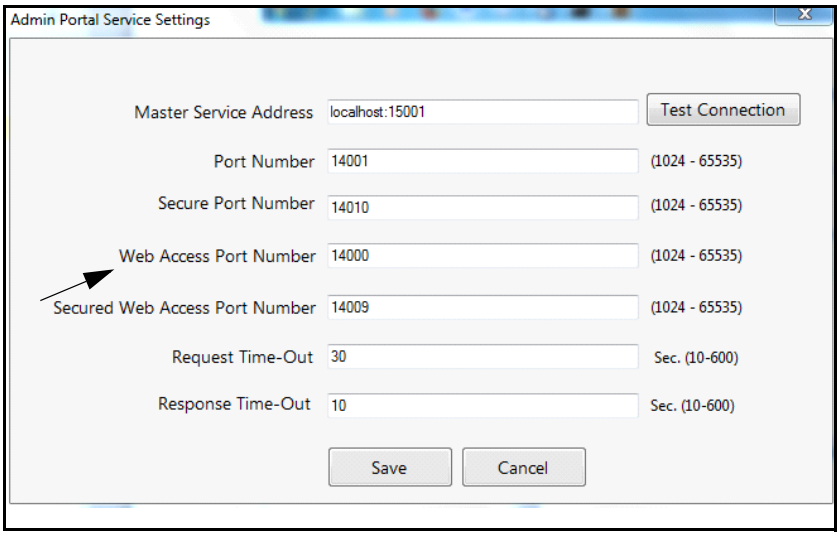
Admin Portal Secured Service URL: This is the secured URL where the Admin portal service is installed/hosted.

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.

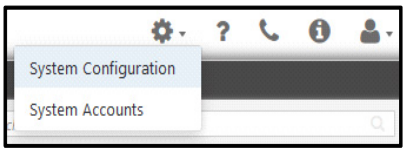
Multi-language Configuration

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

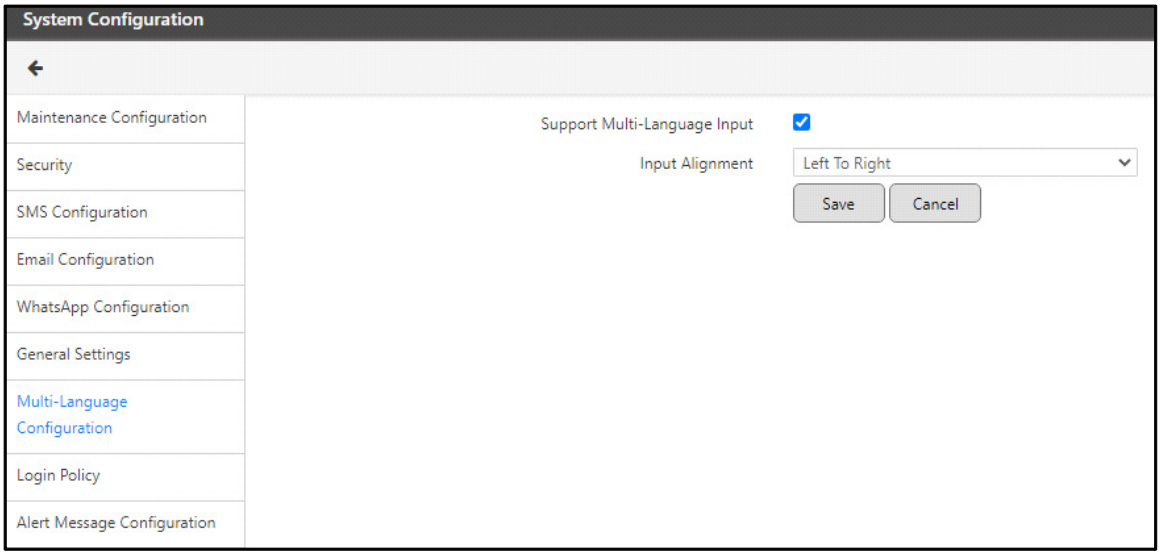
Once the service URLs are entered, then the fields shown below will be non-editable.

For configuration of Multi-language,

Click **Setting** and then click **System Configuration**.



Click **Multi-language Configuration.** The page appears as shown below.



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.

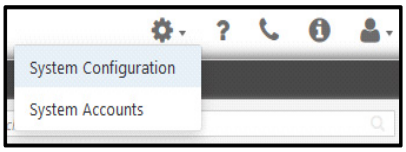
Data input and storing the same in database will support UTF-8 characters.

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

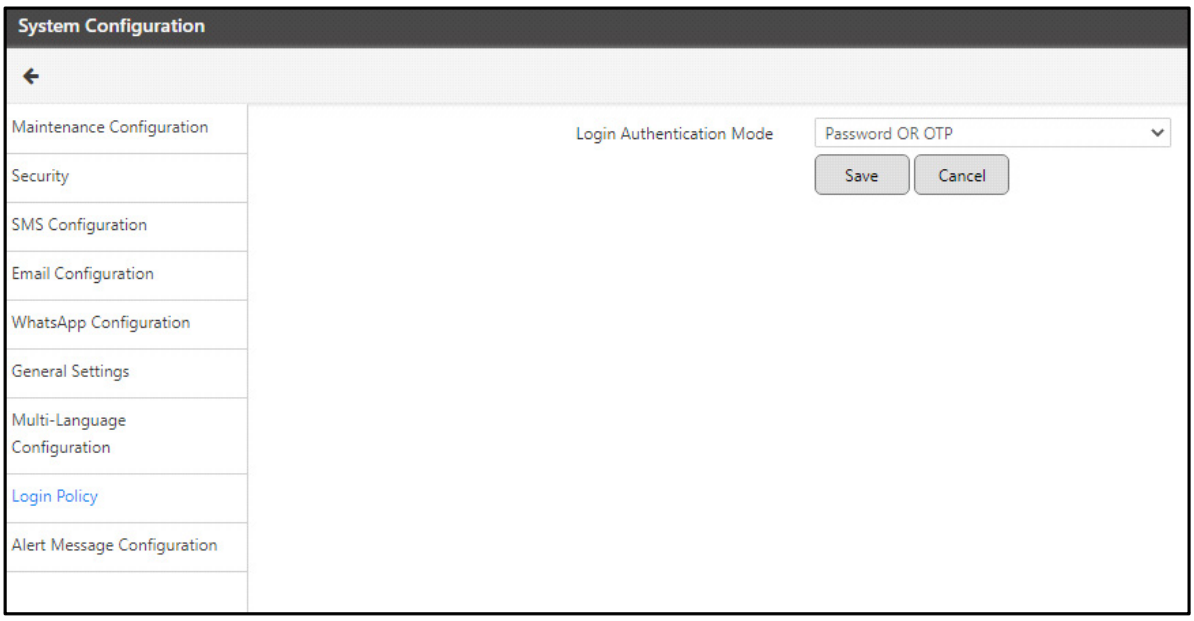
Login Policy

For configuration of Login Policy,

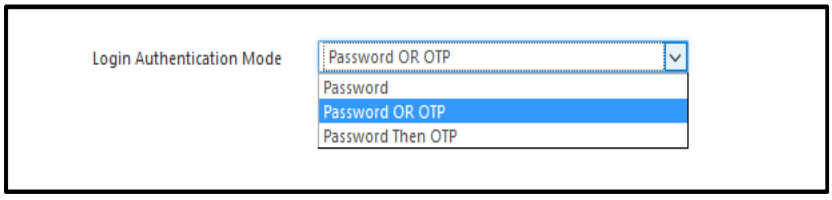
Click **Setting** and then click **System Configuration**.



Click **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.

Alert Message Configuration

Alerts can be sent as SMS, Emails as well as WhatsApp messages.

Make sure the pre-requisites are configured to ensure that the Alerts are sent. Refer to “Pre-requisites”.

For sending Alert Messages, each Alert Message Template has a default content that will be sent. You can edit this content if required.

For SMS Alerts, make sure the desired Alert Message Templates are registered with your Service Provider, who will verify the contents and then provide a Template ID for the same.Prepare the list of registered Alert Messages with their respective Template IDs as these are required while configuring the Alert Message parameters.

Each Alert Message Template is assigned a unique WhatsApp Template Name so that the templates can be added to your WhatsApp Business Account. If you wish to edit the Alert Message Templates, it should be done before sending the templates to your WhatsApp Business Account, else you will have to manually edit the templates from your Whats App Business Account. If you edit the name of the template, make sure it is unique, as same name templates cannot be added to your WhatsApp Business Account. For adding the Templates to your Whats App Business Account, refer to “Templates Addition in WhatsApp Business Account”.

Pre-requisites

Before you configure the Alert parameters, make sure:

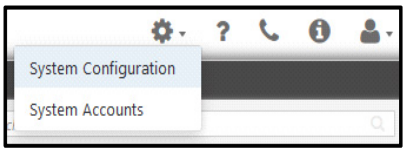
- you have configured the SMS parameters, refer to “SMS Configuration”.
- you have configured the Email parameters, refer to “Email Configuration”.
- you have configured the WhatsApp parameters, refer to “WhatsApp Integration”.
- you have configured the Mobile number and Email ID in the contact details. Refer to “Contact Details” in “Profile” for details. The Maintenance Alert will sent to this Mobile/Email ID.
- you have configured the Mobile number and Email ID in the System Accounts. Refer to “System Accounts” for details. The OTP Generated Alert will sent to this Mobile/Email ID. If you have configured multiple SA logins then it will be sent to the respective SA’s Email ID/Mobile as per the login. For Example if you have two SA login, SA and SA1, then when you login using SA the OTP will be sent to the Email/SMS as configured in System Accounts for this login.
- ensure Alert Service is running so that alert messages can be sent to the assigned users.

To configure an Alert Message, you need to configure the following

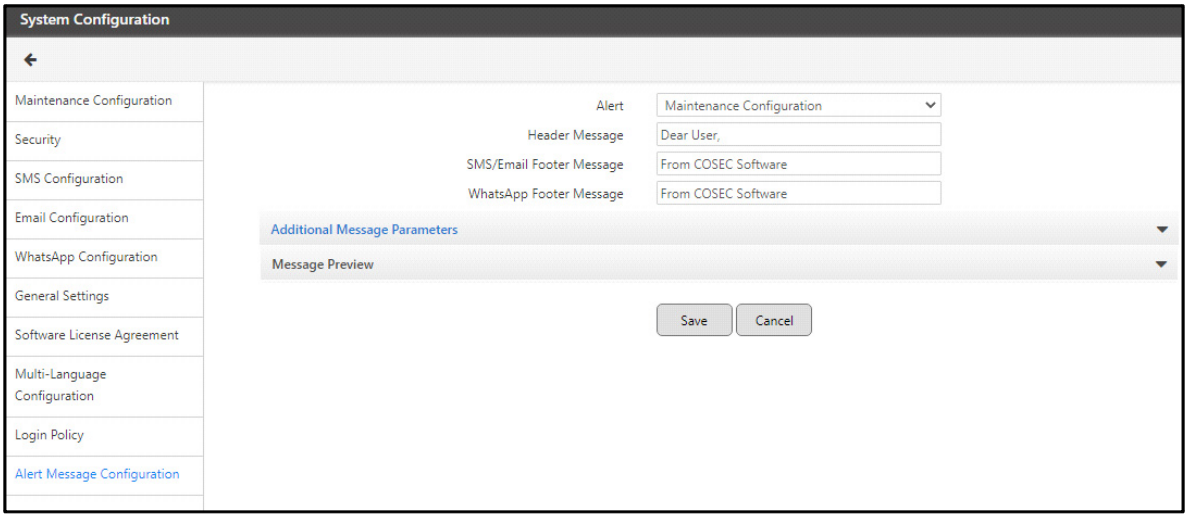
- “Alert Message Parameters”
- “Additional Message Parameters”
- “Message Preview”

Alert Message Parameters

- Click **Setting** and then click **System Configuration**.



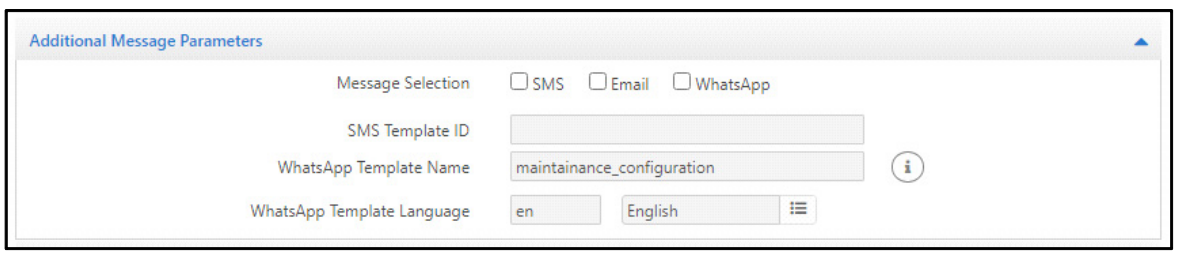
- Click **Alert Message Configuration**.



- **Alert:** Select the desired Alert that you wish to send from the drop-down list.
- **Header Message:** Enter the required text to be displayed in the header of the message, for example: Dear User.
- **SMS/Email Footer Message:** Enter the required text to be displayed in the footer of the SMS/Email message, for example: From COSEC Software.
- **WhatsApp Footer Message:** Enter the required text to be displayed in the footer of the WhatsApp message, for example: From COSEC Software.

Additional Message Parameters

Click the **Additional Message Parameters** collapsible panel and configure the following parameters:



The following Additional Parameters are common for all the Alerts.

- **Message Selection**: Select the desired check boxes **— SMS**, **Email, WhatsApp —** to determine the type of message/s to be sent.

- **SMS Template ID:** As per TRAI Regulation, an enterprise which sends messages to customers like OTP, communication message, promotional messages via SMS, have to register their entity and the content template to avoid spam, fake and fraudulent communication through SMS.

  It is mandatory for an Admin to register the SMS content template beforehand with their Service Provider which will be verified before it is delivered to the users.

  Once registered, the Service Provider will provide a Template ID against the registered SMS content. For every different Alert messages, a unique Template ID will be provided by the Service Provider.

  Make sure **SMS** check box is enabled in **Message Selection** to configure SMS Template ID. Enter the respective Template ID for the configured Alert message which is to be send to users via SMS.

If you have multiple Service Providers, then make sure the required templates are registered with all the desired Service Providers. Hence for each template you will have multiple Templates IDs. Also make sure you maintain a record of all the registered Message Templates with their respective Template IDs for reference.

- **WhatsApp Template Name:** Make sure **WhatsApp** check box is enabled in **Message Selection**. The default name assigned to this alert template is displayed. You can change the same if required. If you opt to add the alert templates to your WhatsApp Business Account then this same name will be displayed in the WhatsApp **Select Templates** picklist. Make sure you have checked the contents of the template before the same are added to your WhatsApp Business Account. For details, refer to "Templates Addition in WhatsApp Business Account".

- **WhatsApp Template Language:** Click the picklist. The **Language** pop-up appears. Select the desired language in which you wish to send the WhatsApp message. When you add the templates to your WhatsApp Business Account these will be added in the selected language. For details, refer to "Templates Addition in WhatsApp Business Account".

Message Preview

You can preview the alert message content as per the selected Alert — Maintenance Configuration, OTP Generated.

For the Message Preview of the Maintenance Alert make sure you have configured the desired message and dates in Maintenance Configuration. For details refer to "Maintenance Configuration".

To view the preview,

- Click the **Message Preview** collapsible panel.

The message details that will be sent to the recipient — SMS, Email, WhatsApp — appear.

You can copy the content of the message — SMS, WhatsApp — if required. To do so, click **Copy** .

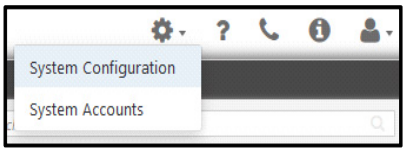
- Click **Save** to save the configurations.

Similarly, the OTP Generated Alert parameters can be configured.

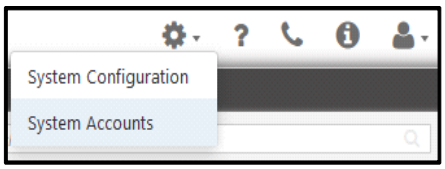
System Accounts

To create the system account users,

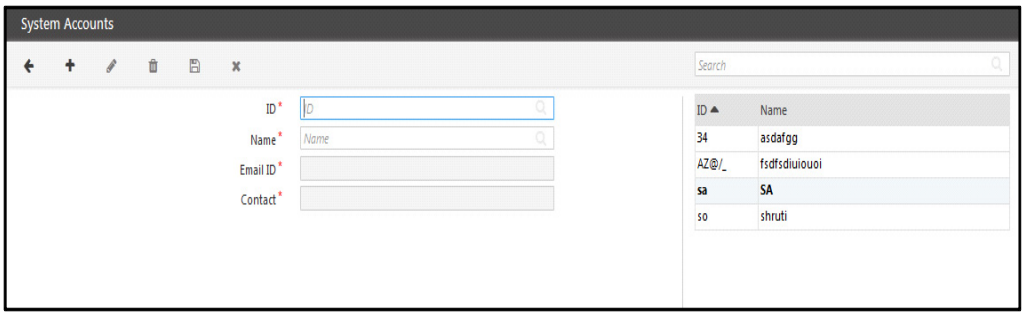
Click **Setting** .



Click **System Accounts**.

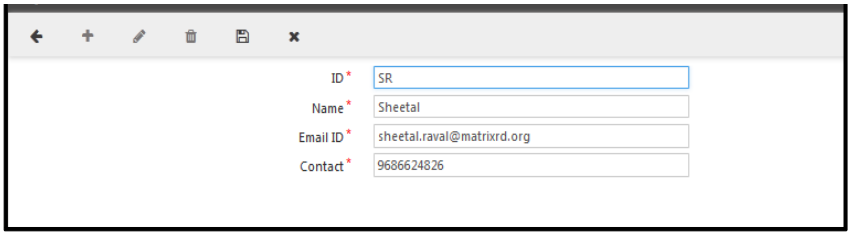


The System Accounts page appears as shown below.

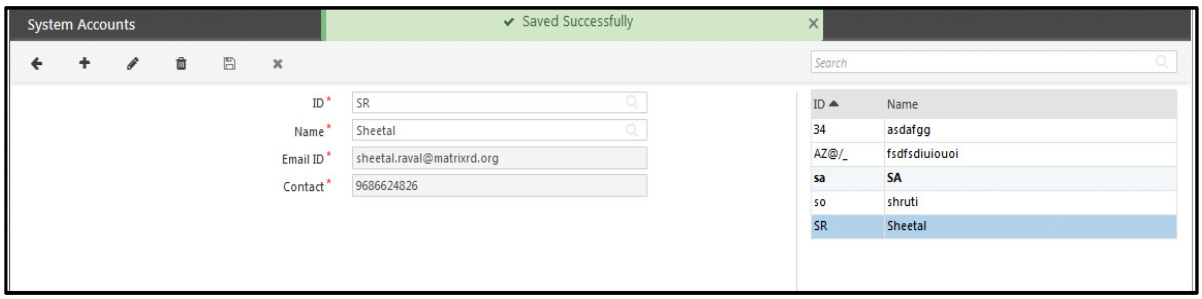


Click on **New** to create new system account user.

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.



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



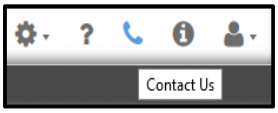
Help, Contact, About Us

Help

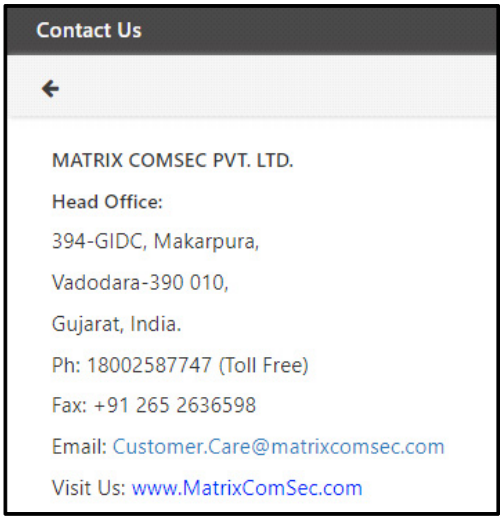
To view the Help manual of Admin Portal; click on the **Help** option from the admin menu. The pdf manual will open which will guide you for the management of portal.

Contact Us

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



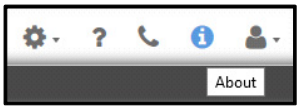
The Contact Us page appears as shown below.



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

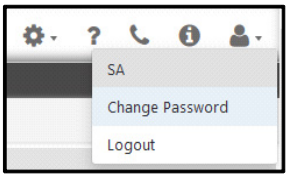
About

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

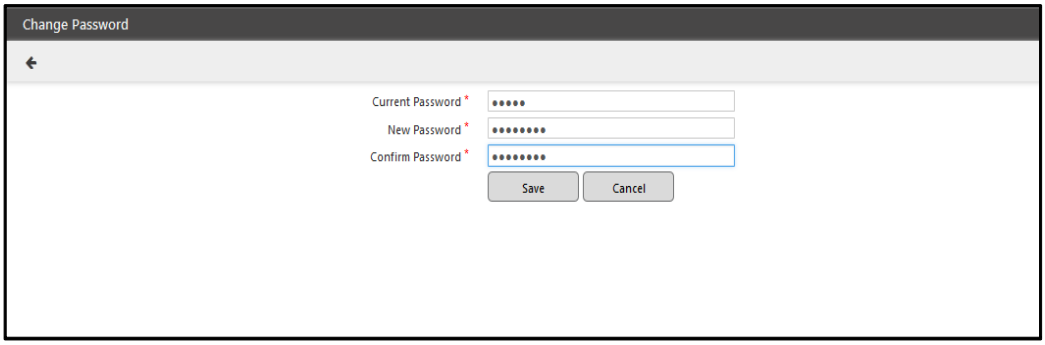


Change Password

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.



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.

Appendix

Supported Licenses

COSEC CENTRA LICENSES	Basic Platform License
MATRIX VIRTUAL DONGLE300	Generic key for Virtual License
MATRIX LICENSE DONGLE200	Generic key for Dongle License
COSEC CENTRA PLATFORM	This includes activation of: Platform Users - 10, ACM Users - 5, CMM Users - 5, VMM Users - 1, TAM Users - 5, CWM Users - 5, JPC Users - 5, FVM Users - 5, ESS Users - 5, FR Users - 5 , AUP Validity of 15 months
COSEC PLT USER10	10 Platform Users License
COSEC PLT USER100	100 Platform Users License
COSEC PLT USER1000	1000 Platform Users License
COSEC CENTRA TAM10	10 Time-Attendance Users License
COSEC CENTRA TAM100	100 Time-Attendance Users License
COSEC CENTRA TAM1000	1000 Time-Attendance Users License
COSEC CENTRA ACM10	10 Access Control Users License
COSEC CENTRA ACM100	100 Access Control Users License
COSEC CENTRA ACM1000	1000 Access Control Users License
COSEC CENTRA ESS10	10 Employee Self Service Portal Users License
COSEC CENTRA ESS100	100 Employee Self Service Portal Users License
COSEC CENTRA ESS1000	1000 Employee Self Service Portal Users License
COSEC CENTRA VMM10	10 Visitor Management Users License
COSEC CENTRA VMM100	100 Visitor Management Users License
COSEC CENTRA VMM1000	1000 Visitor Management Users License
COSEC CENTRA CMM10	10 Cafeteria Management Users License
COSEC CENTRA CMM100	100 Cafeteria Management Users License
COSEC CENTRA CMM1000	1000 Cafeteria Management Users License
COSEC CENTRA CWM10	10 Contract Workers Management Users License
COSEC CENTRA CWM100	100 Contract Workers Management Users License

COSEC CENTRA CWM1000	1000 Contract Workers Management Users License
COSEC CENTRA JPC10	10 Job Processing and Costing Users License
COSEC CENTRA JPC100	100 Job Processing and Costing Users License
COSEC CENTRA JPC1000	1000 Job Processing and Costing Users License
COSEC CENTRA FVM10	10 Field Visit Management Users License
COSEC CENTRA FVM100	100 Field Visit Management Users License
COSEC CENTRA FVM1000	1000 Field Visit Management Users License
COSEC CENTRA FR10	10 Facial Recognition Users License
COSEC CENTRA FR100	100 Facial Recognition Users License
COSEC CENTRA FR1000	1000 Facial Recognition Users License
COSEC CENTRA AUP10	10 Annual Upgrade Users License
COSEC CENTRA AUP100	100 Annual Upgrade Users License
COSEC CENTRA AUP1000	1000 Annual Upgrade Users License
You need to purchase the Dongle/Virtual Generic Key, then the Platform License. There after the you can purchase the Module Licenses as per your requirement.	

MATRIX COMSEC

Head Office:
394-GIDC, Makarpura, Vadodara - 390010, India.
Ph: (+91)18002587747
E-mail: Tech.Support@MatrixComSec.com

www.matrixcomsec.com