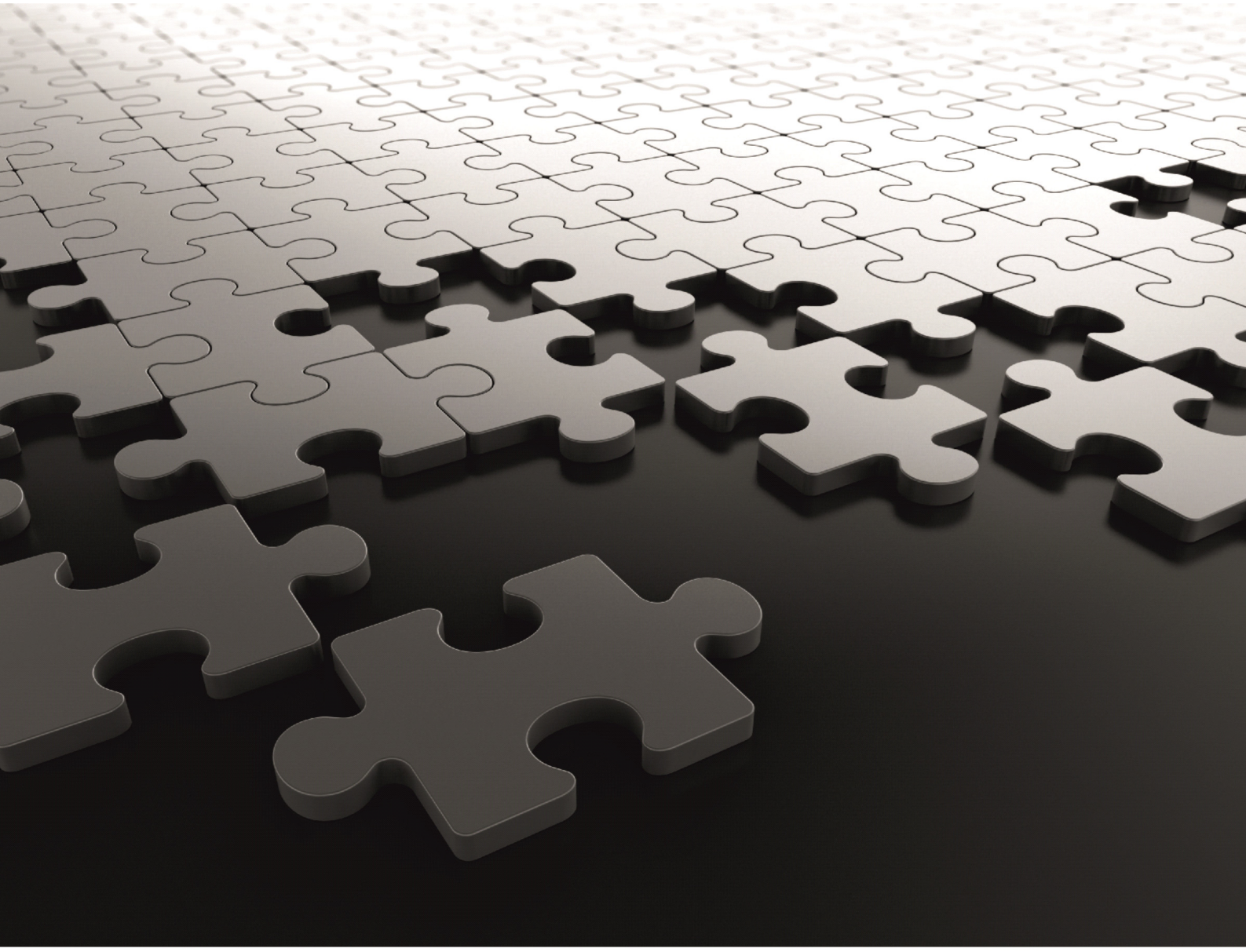
Matrix COSEC
Software Installation Guide



MATRIX
SECURITY SOLUTIONS

MATRIX
SECURITY SOLUTIONS

Matrix COSEC

Software Installation Guide

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 9
Release date: May 15, 2024

Contents

CHAPTER 1

COSEC Software Installation

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

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

System Requirements

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

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

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

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

Pre-Requisites for Face Recognition and Face Enrollment

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

Computer Hardware Platform

For Windows with CPU:

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

For Windows with GPU:

- Nvidia GeForce GTX 1050 Ti-4 GB onwards

Operating System

Microsoft Windows 10 64-bit

Recommendations for Liveness Verification

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

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

Recommendations for Face Recognition

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

Recommended Camera Settings for Liveness Verification

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

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

Security Setup for COSEC[1]

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

Step 1:

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

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

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

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

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

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

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

Step 2:

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

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

Step 3:

- Enable TLS1.2 in the Server.

Port Requirement

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

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

Installing Prerequisites

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

1. Install Internet Information Services (IIS).
   For Installing Internet Information Services (IIS) click on "Installing IIS on the Windows Operating System (Windows10)".

2. Install .Net Framework ver. 4.5 (mandatory).
   For Installing .Net Framework click on *".Net Framework Installation".*

3. Microsoft SQL Server 2008 R2 SP2 or above.
   For Starting Microsoft SQL Server click on *"Microsoft SQL Server".*

4. Oracle database server- upto version 19C. For Starting Oracle click on *"Oracle Installation".*

Installing IIS on the Windows Operating System (Windows10)

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

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

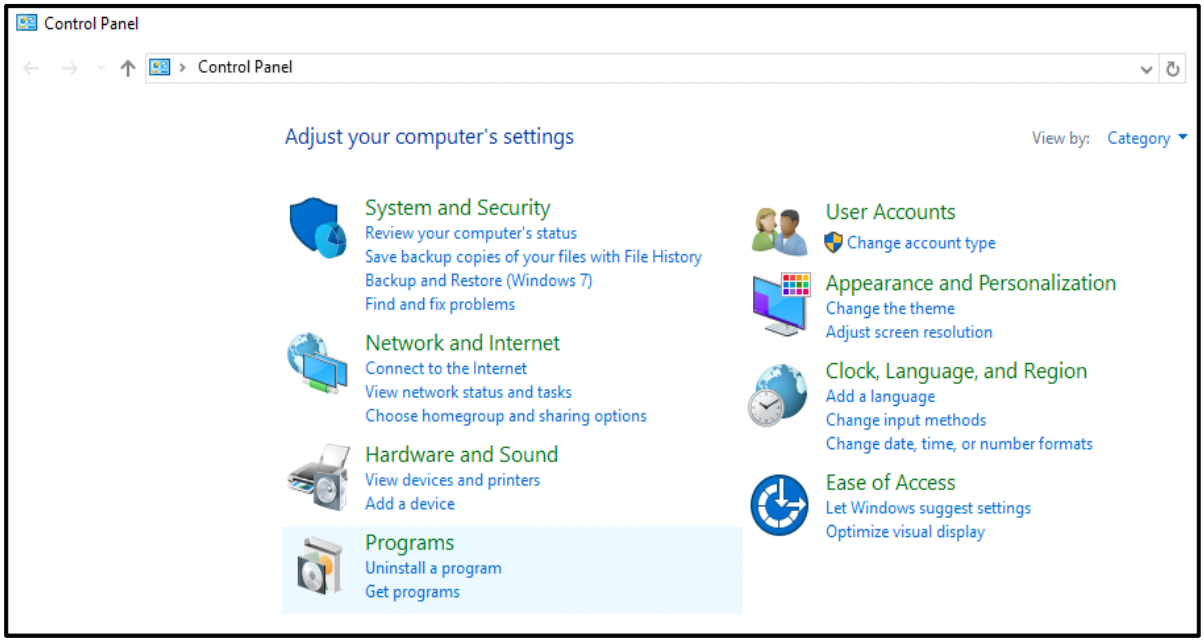
The following IIS components must be enabled for Windows 10 and above.

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

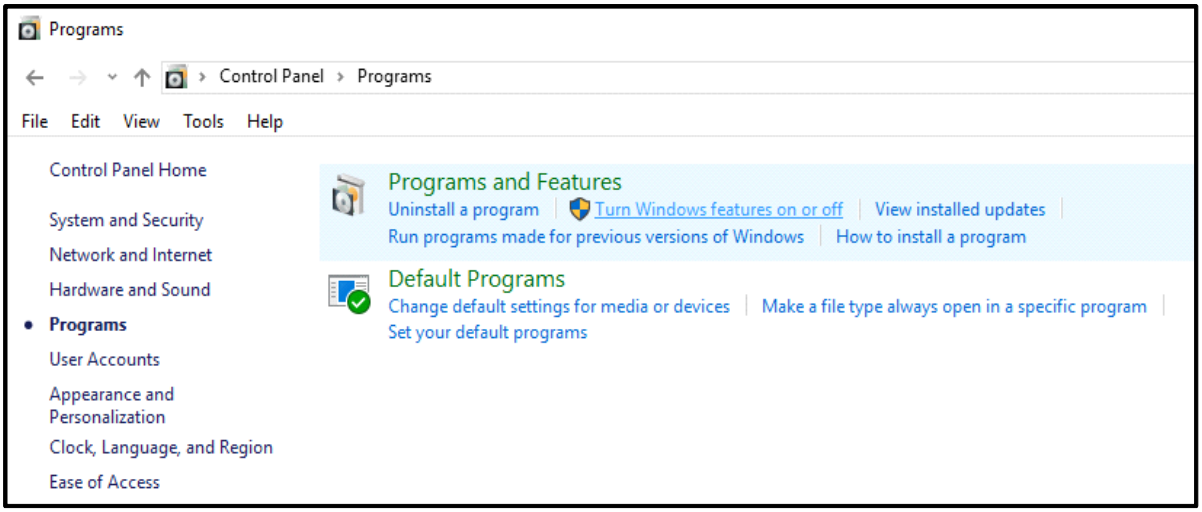
"IIS-LegacySnapIn"

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

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

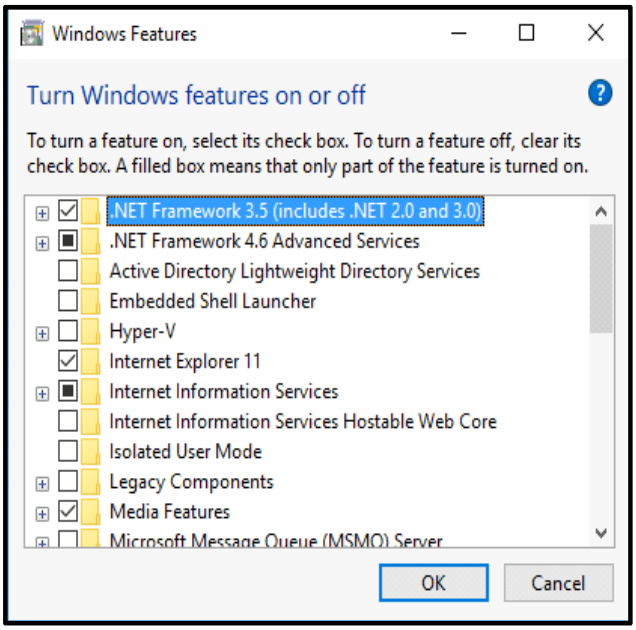


- The Control Panel **Programs and features** options are displayed.

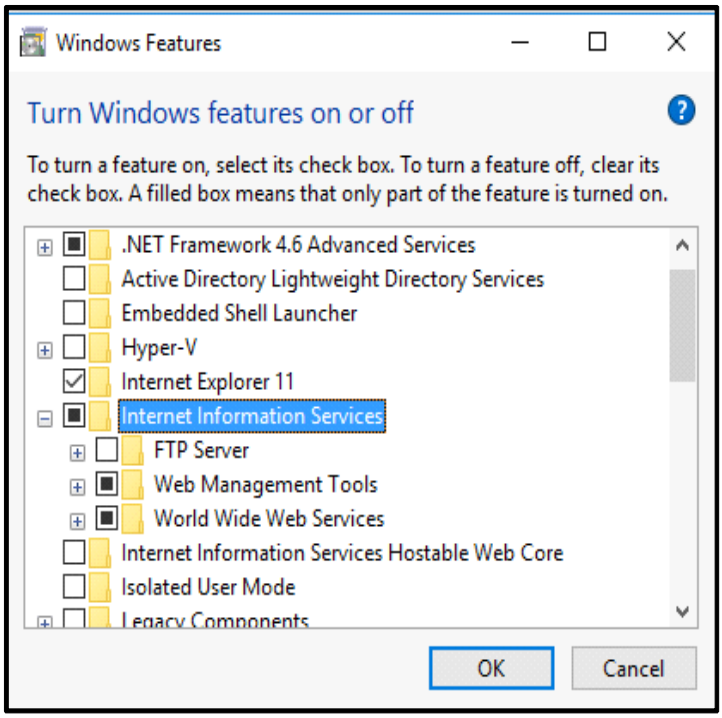


- Click, **Turn Windows features on or off**. You may receive the Windows Security warning at this point. Click **Continue** to continue.

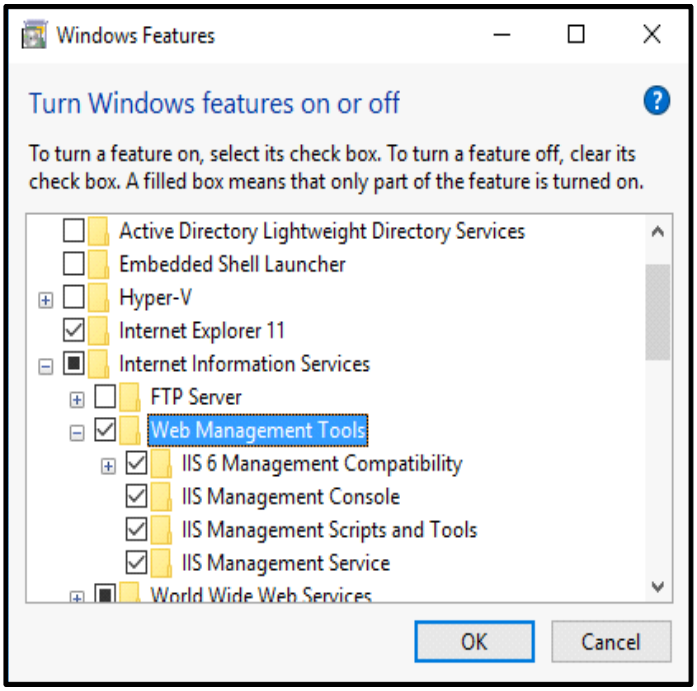
The Turn Windows Features on or off window will be displayed as shown below:



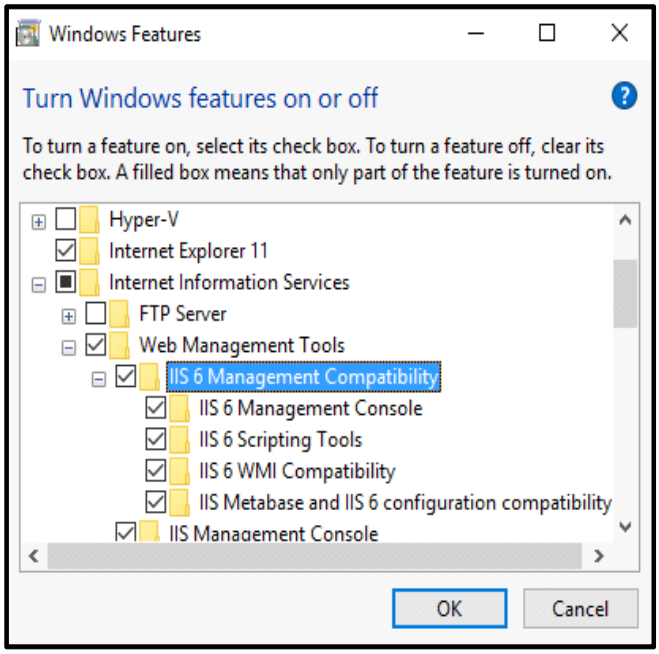
- The IIS default install features are shown as selected. Click on **Internet Information Services**. Additional IIS features will be displayed as shown.



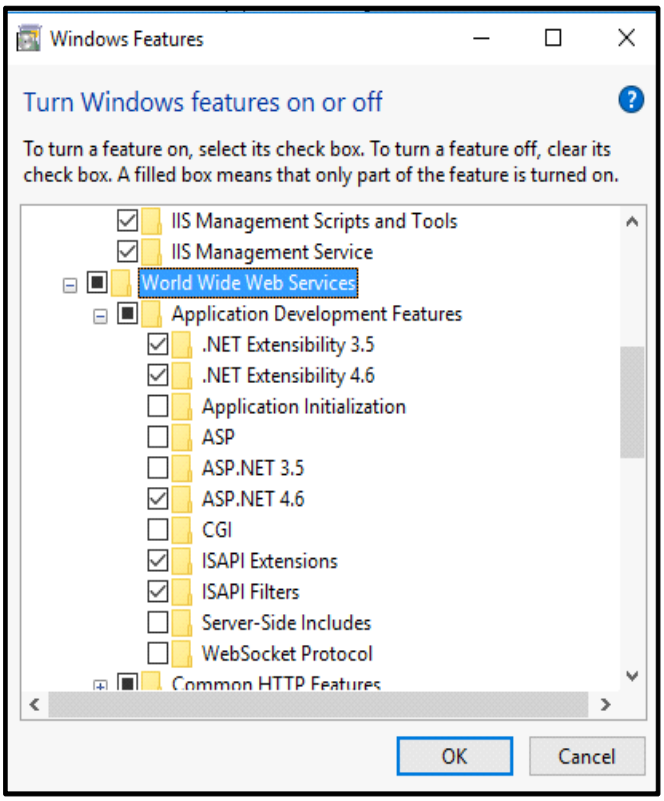
- Click on **Web Management Tools** to view the available features. Check the boxes against the features to be turned on as shown below.



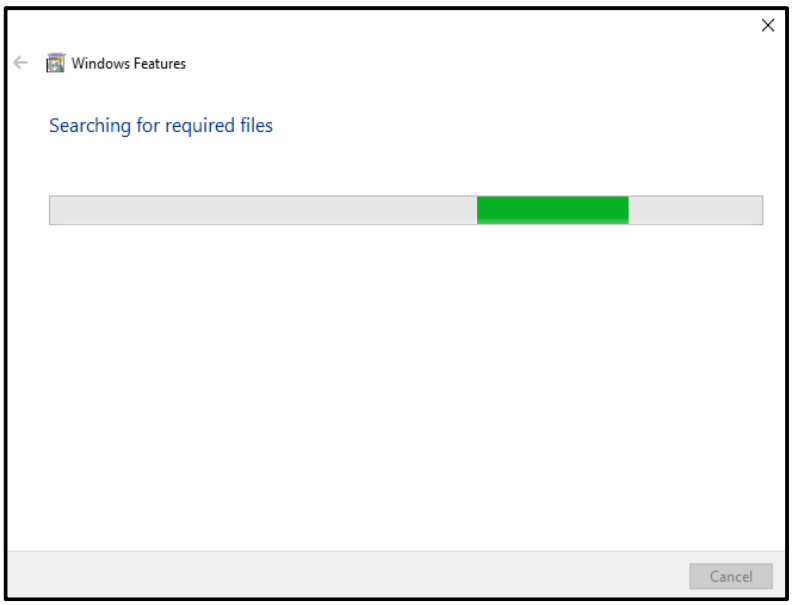
- Click on **the IIS 6 Management Compatibility** (Version depends on OS) and check the boxes against the features as shown.

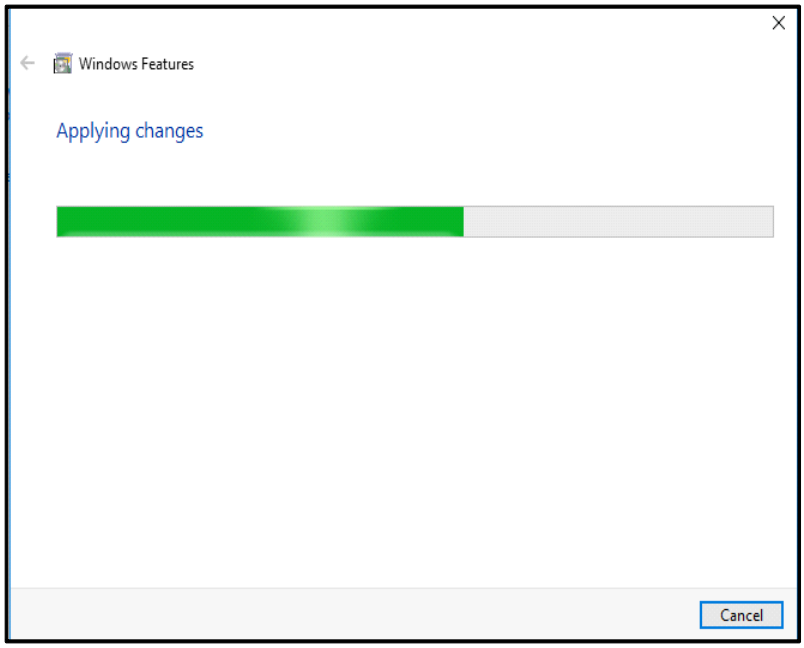


- Now click on **World Wide Web Services** and then on the **Application Development Features** option. Check the boxes against the features as shown.



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



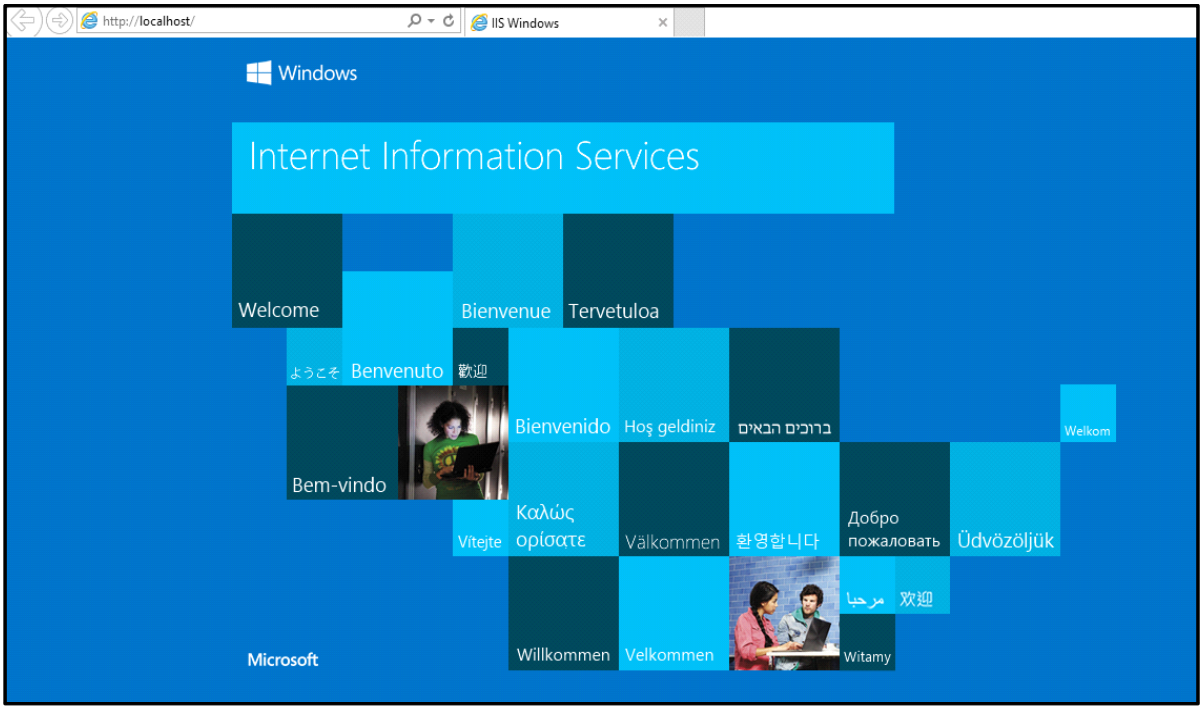


When the installation completes, the Windows Features dialog closes and you are returned to the Control Panel.

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

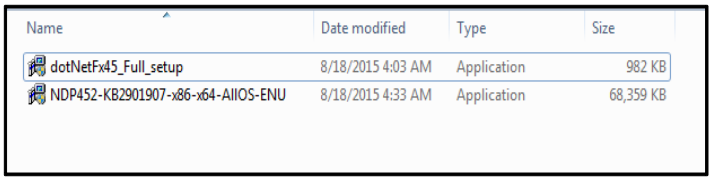
Start Internet Explorer web browser and enter the address http://localhost/
You should see the default IIS "Welcome" page.

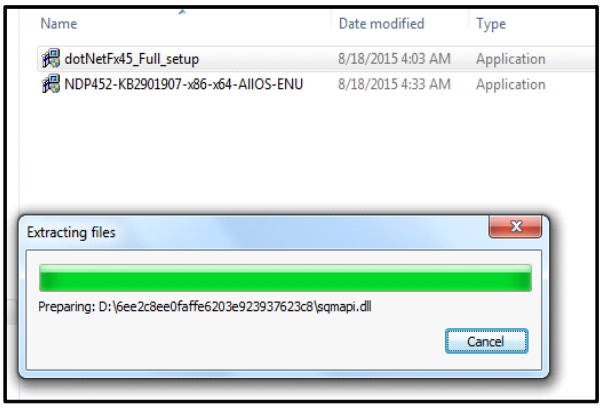
IIS version may change depending on the software updation and Windows in your Computer.



.Net Framework Installation

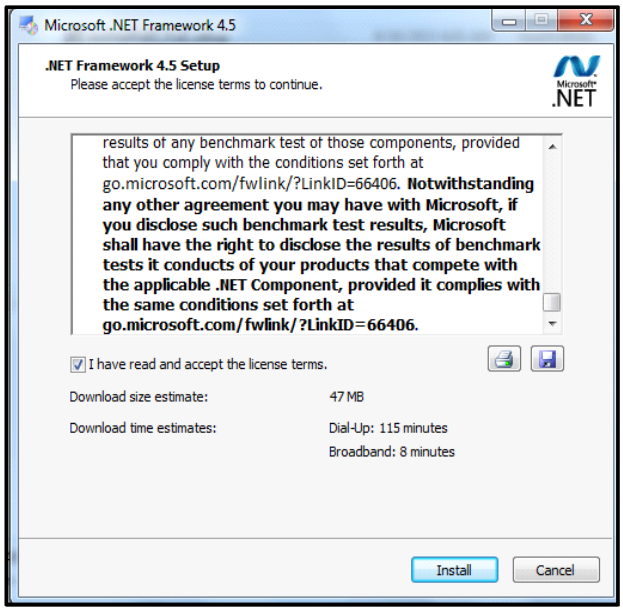
In the absence of the**.Net Framework**, user must install it before proceeding with COSEC installation.



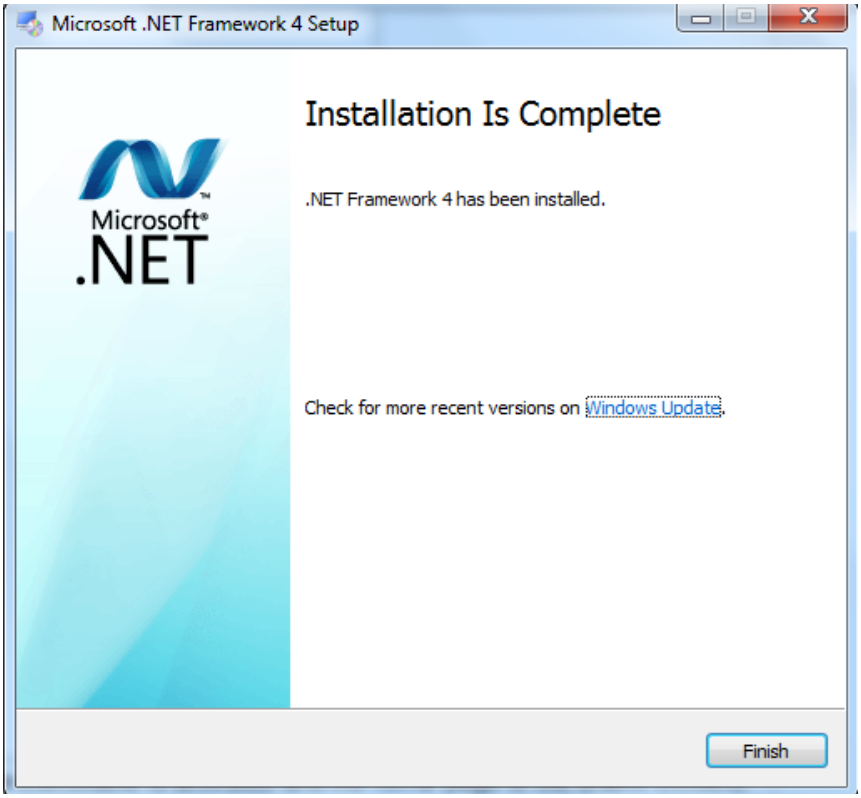


Browse the set and run the application.

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

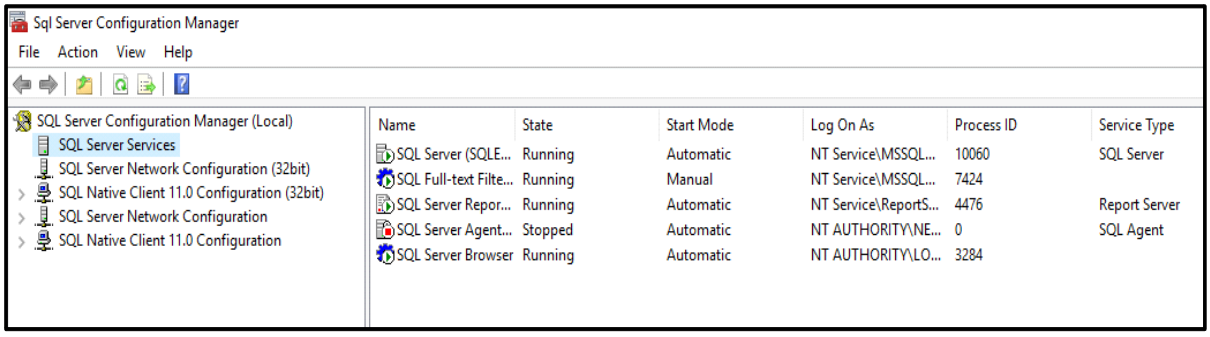


After installation is complete Click on **Finish** to exit the setup.

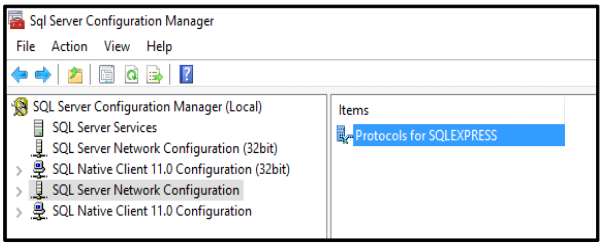


Microsoft SQL Server

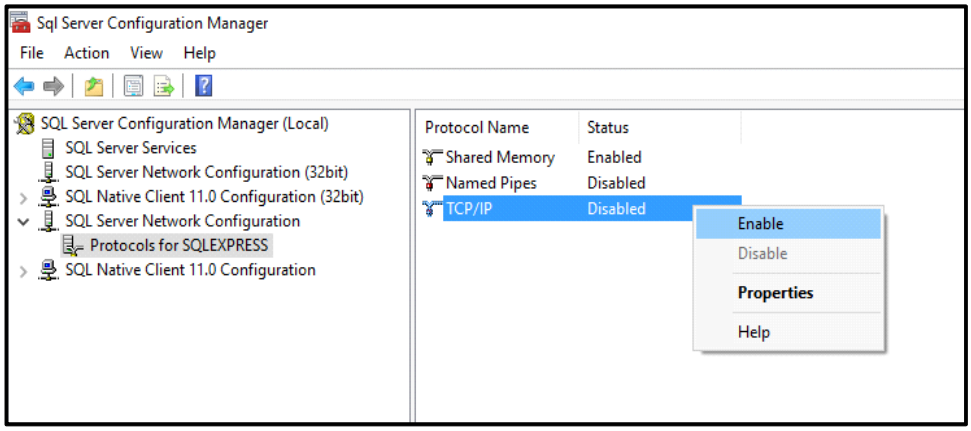
Now the installer needs to enable the appropriate protocols from the **SQL Server Configuration Manager** to allow the connectivity to the SQL server. For example; Navigate to the SQL Server 2014 Configuration Manager by typing it in “Search the web and Windows” option.



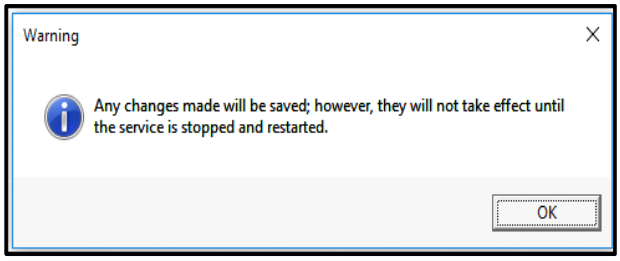
Go to **SQL Server Network Configuration > Protocols for SQLEXPRESS** option as shown in the figure.



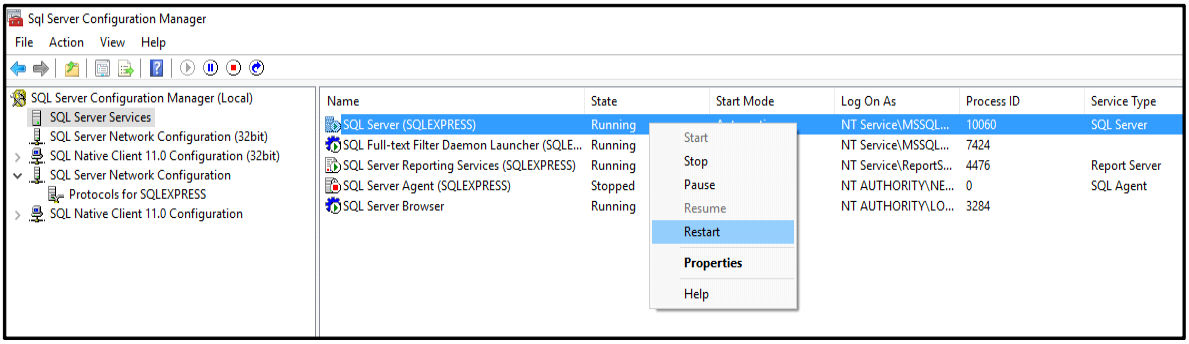
Click on the **Protocols for SQLEXPRESS** option in the left pane. The protocol options appear in the right pane as shown.

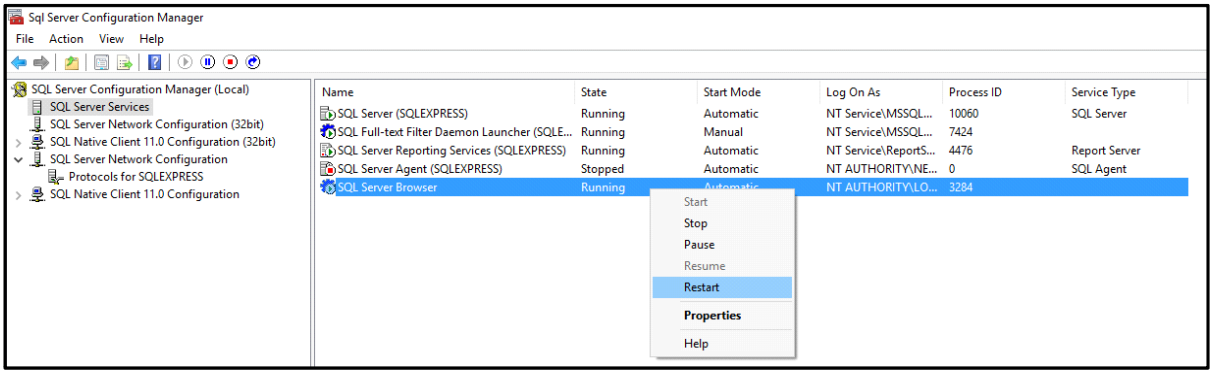


Right click on the **TCP/IP** option in the right pane and select the **Enable** option. The System will display the warning that the changes have been saved but it will take effect only after the service is restarted. Click OK to continue.



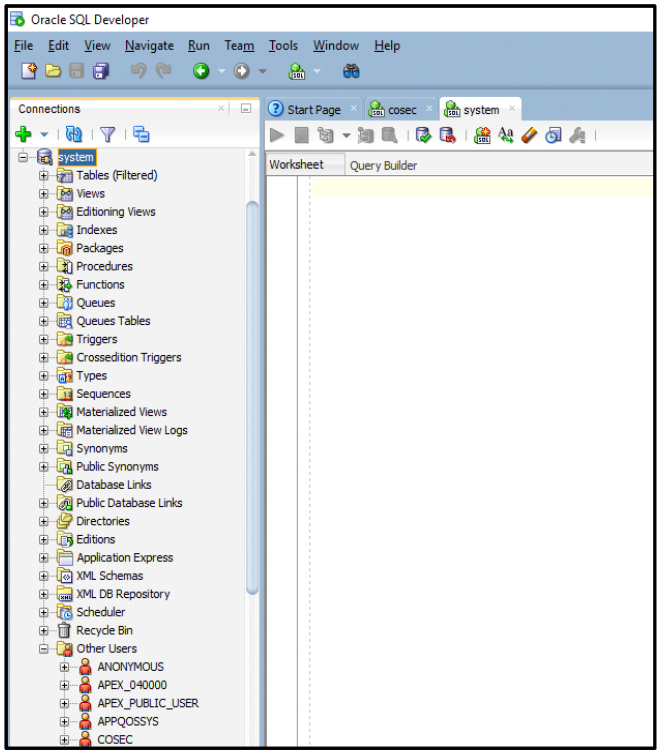
Select the **SQL Server Services** in the left pane. Restart the **SQL Server** and the **SQL Server Browser** services by right clicking on the options and selecting the **Restart** option as shown below:



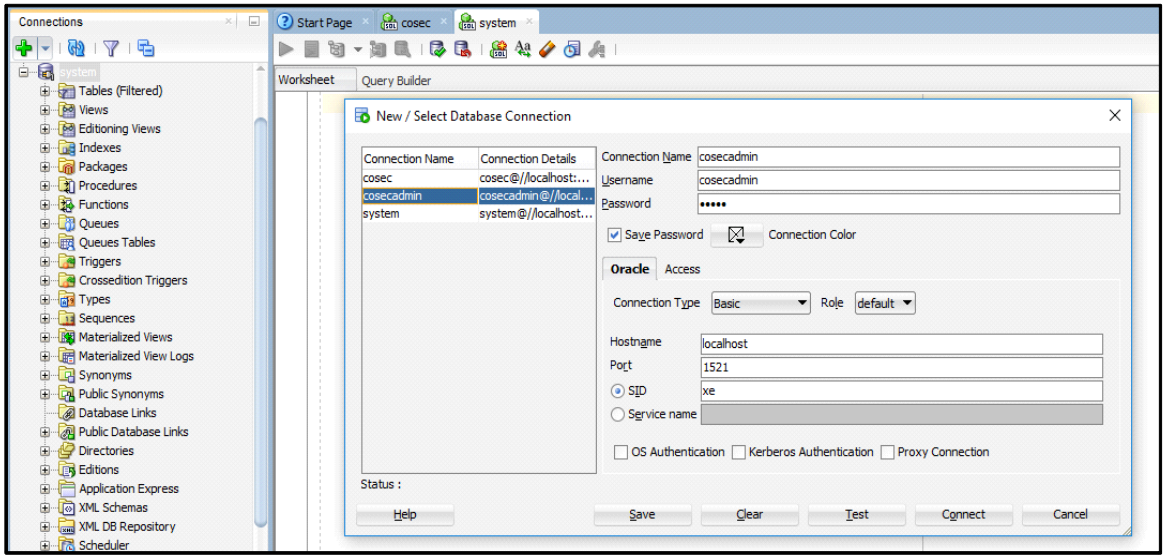


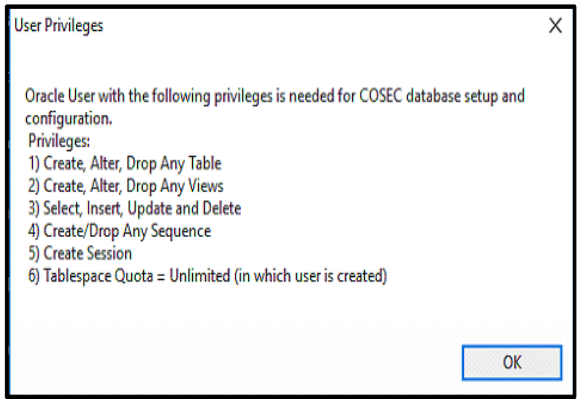
Oracle Installation

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



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



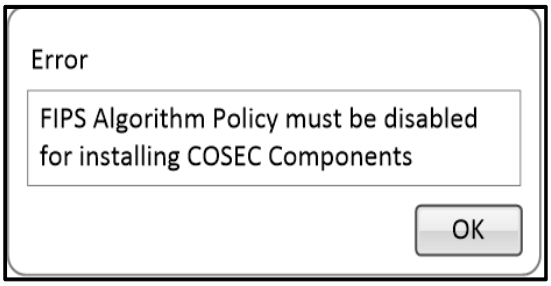


From PC where COSEC Web is installed - Execute msi file available at following path of Setup folder: Setup\Prerequisites\SqlLocalDB\x64 OR x86 (as per 64-bit OR 32-bit system respectively)

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

FIPS Algorithm Policy Check

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



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

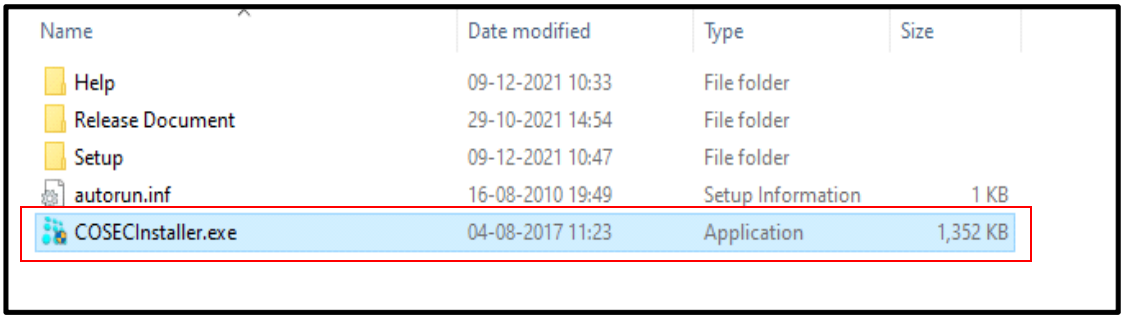
Then go to the path:
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy.

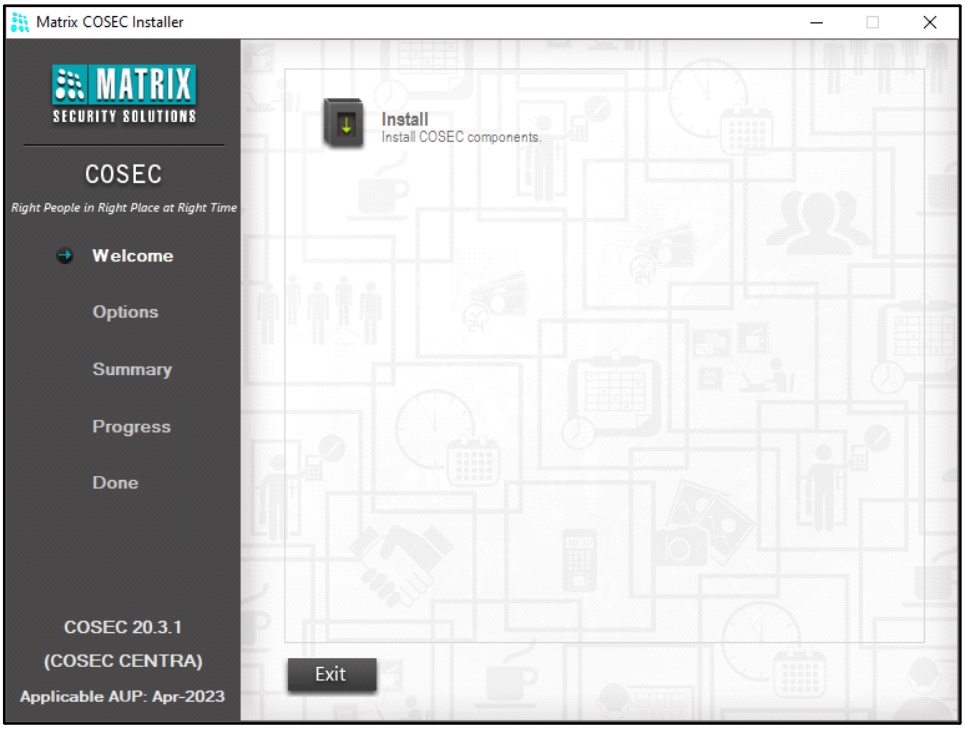
Now you can disable the FIPS Algorithm policy. Then Reset IIS Server and install the setup.

Installing COSEC

In order to install the COSEC application:

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





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.

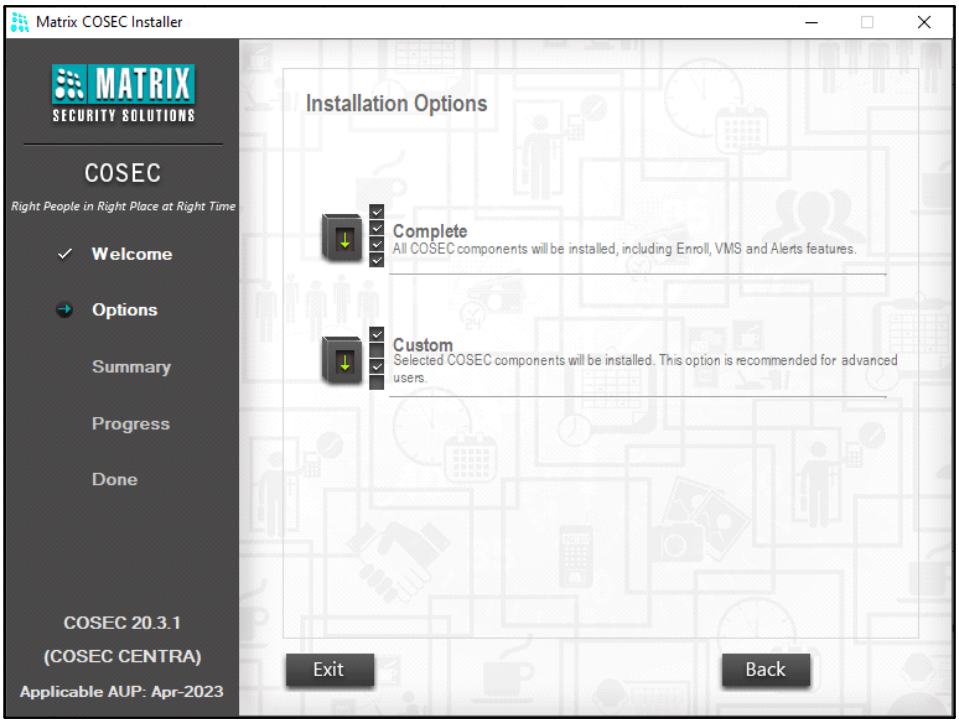
The COSEC application requires the Microsoft. Net Framework ver 4.0 to be installed prior to its installation on the application server. The COSEC Installer utility automatically detects the presence or absence of this component and the same must be installed in its absence.

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

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

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

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



Complete: Select this option if you wish to install all the components of the COSEC application. For details, refer to "Complete Installation".

Custom: Select this option if you wish to install the components of the COSEC application selectively. For details, refer to "Custom Installation".

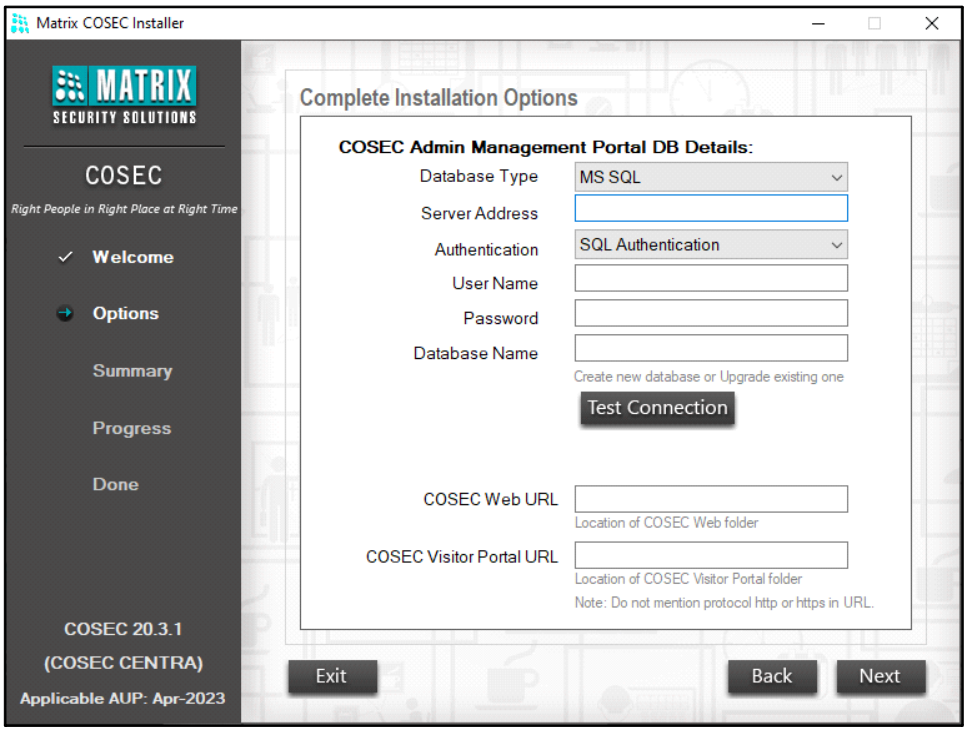
Select the appropriate installation option to continue.

Complete Installation

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

COSEC Admin Management Portal DB Details

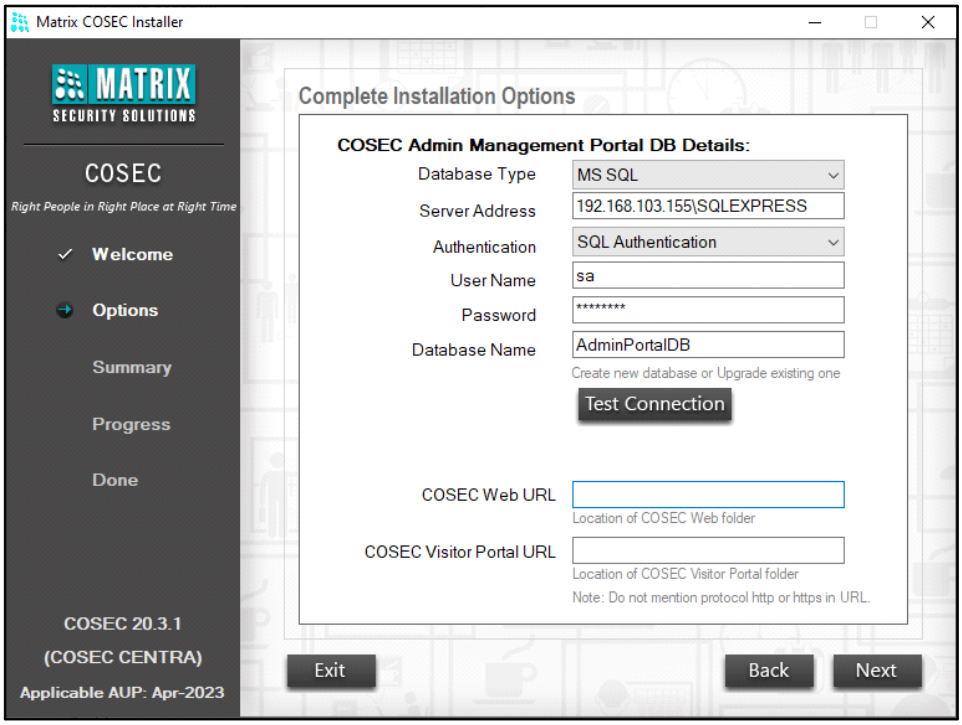
Enter the details to configure Admin Management Portal Database.



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.

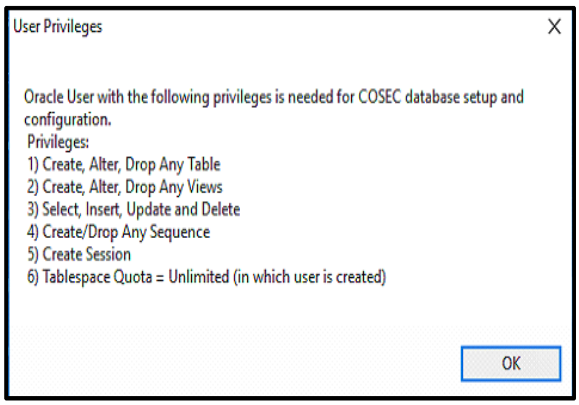
- If you select Authentication Type as **SQL Authentication**, configure the following:
  - **User Name:** Specify the user name as created during SQL server instance. For example: sa
  - **Password:** Specify the password as created during SQL server instance. For example: matrix_1
- If you select Authentication 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.

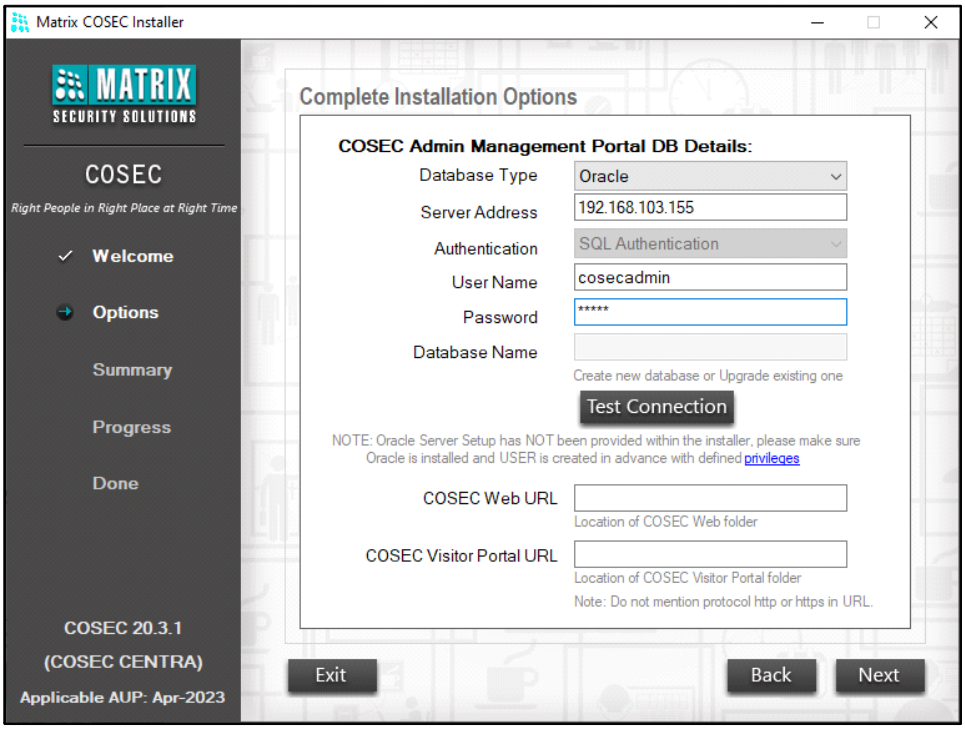
Oracle Database Type

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



For details, refer to "Oracle Installation".

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



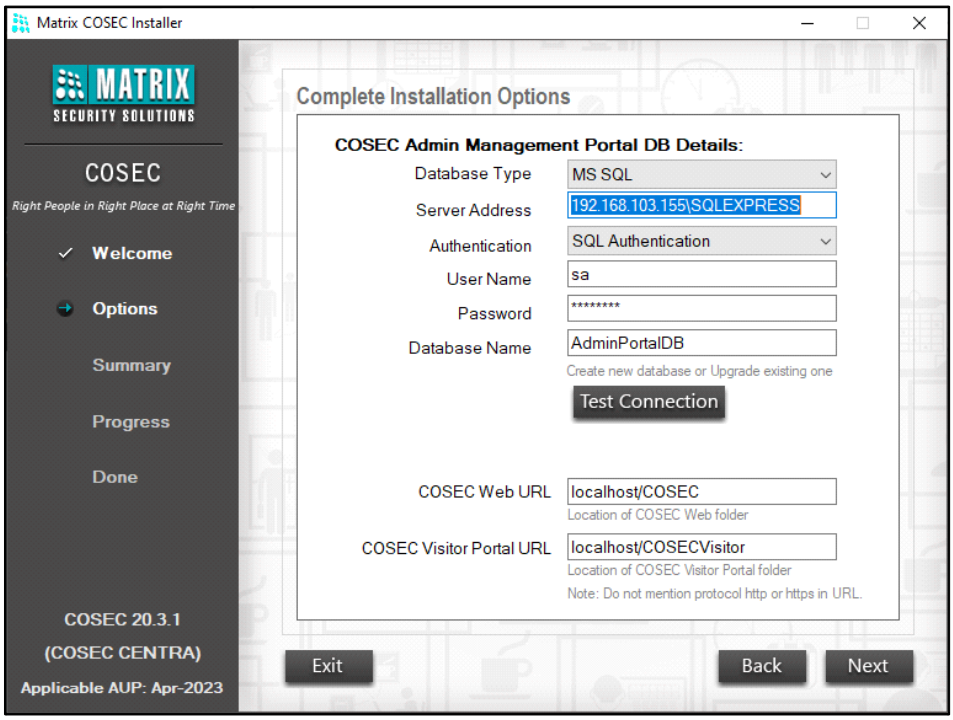
Server Address: Enter the Server Address where the database of Admin Management Portal is to be created. For example: 192.168.103.155.

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.

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



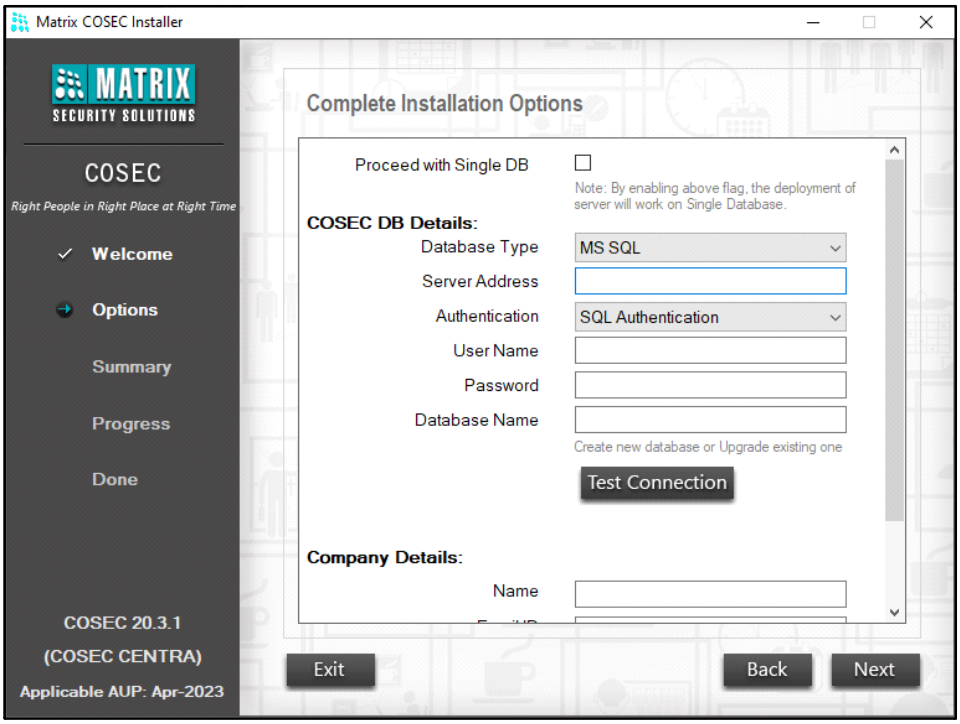
COSEC Web URL: Enter the URL through which COSEC Web is to be accessed. If you are installing COSEC Web in PC2 and accessing from PC1; then enter IP of PC2 where Web is installed. If Web is to be accessed locally then IP or localhost can be entered in URL.

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 enter IP of PC2 where Visitor Portal is installed. If Visitor Portal is to be accessed locally then IP or localhost can be entered in URL.

Now click on **Next** button.

COSEC DB Details

Configure the parameters for COSEC Database.



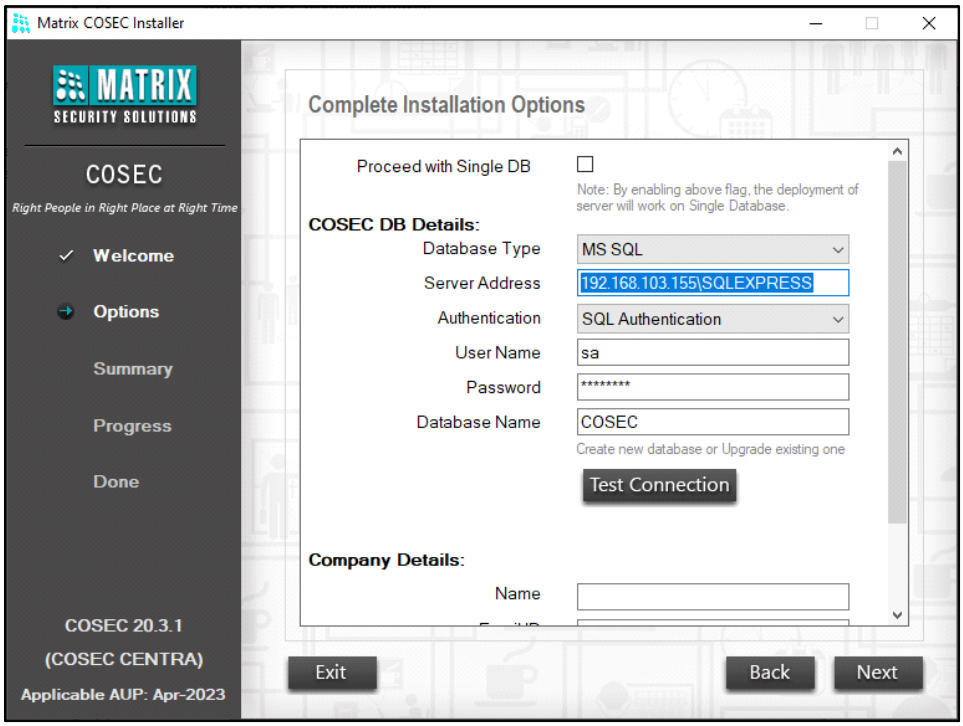
Proceed with Single DB: Select this check box to complete the installation with creation of single database for Admin Portal and COSEC. The details will be auto-filled as configured under **COSEC Admin Management Portal DB Details**.

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

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**.**

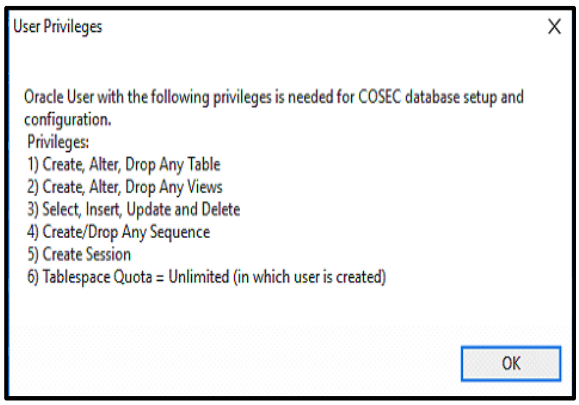
- If you select Authentication Type as **SQL Authentication**, configure the following:
  - **User Name:** Specify the user name as created during SQL server instance. For example: sa
  - **Password:** Specify the password as created during SQL server instance. For example: matrix_1
- If you select Authentication 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.

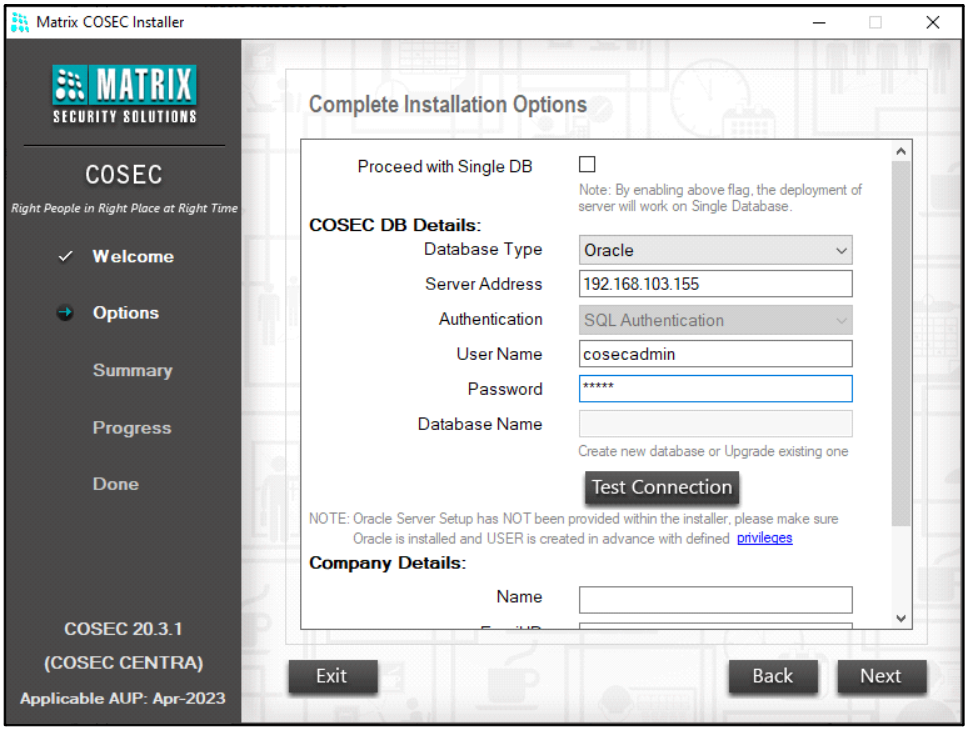
Oracle Database Type

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



For details, refer to "Oracle Installation".

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.

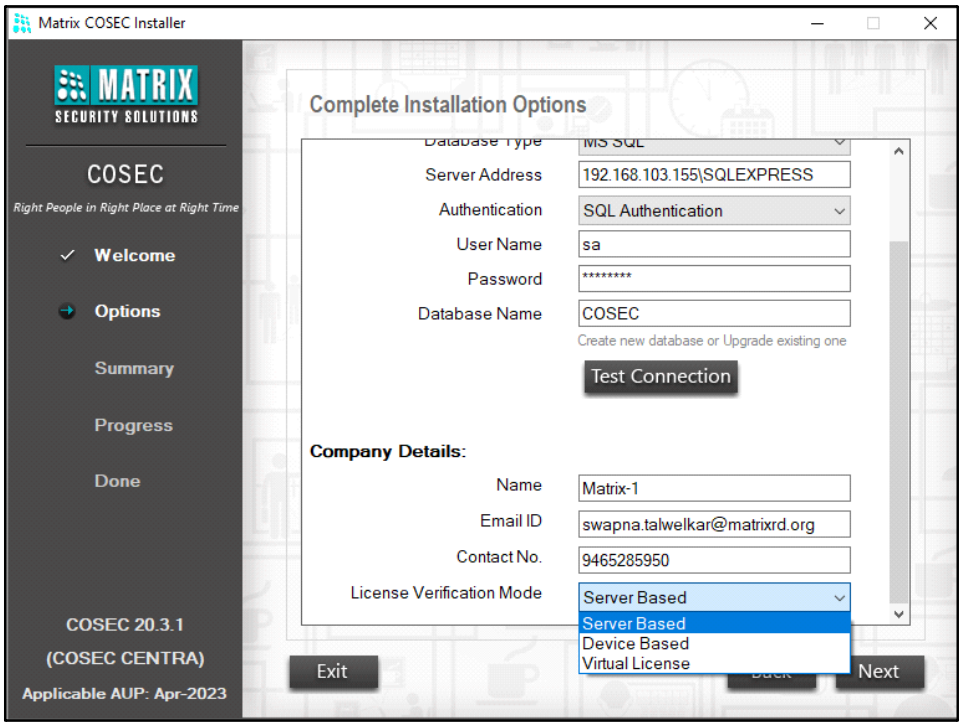
User Name: Specify the user name as the name of the user created from Oracle system. For example: cosecadmin

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 option as **Server Based, Device Based** or **Virtual License** for verifying the license.

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

- 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.*

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

- 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 the Matrix Support Team.*

Server Based

Make sure the License Dongle is connected to 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.

The Dongle only has the Generic Key, you need to purchase other licenses as per your requirement and update the new license key. For details, refer to Admin Management Portal > Company Configuration > **License and Services** and in the Admin Management Portal User Guide, Appendix > **Supported Licenses**.

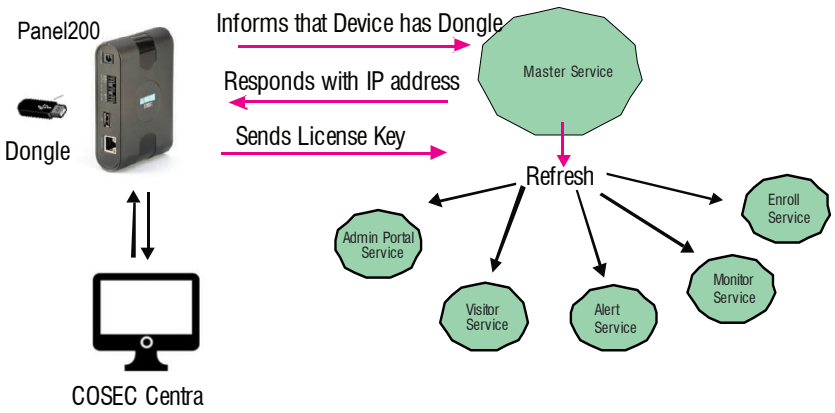
Device Based

In Device Based licensing VEGA, ARGO, ARGO FACE Direct Doors or Panel200 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 Admin Management Portal > Company Configuration > **Profile.**

The Dongle only has the Generic Key, you need to purchase other licenses as per your requirement and update the new license key. For details, refer to Admin Management Portal > Company Configuration > **License and Services** and in the Admin Management Portal User Guide, Appendix > **Supported Licenses**.

Now,
- 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 the 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.
- 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.

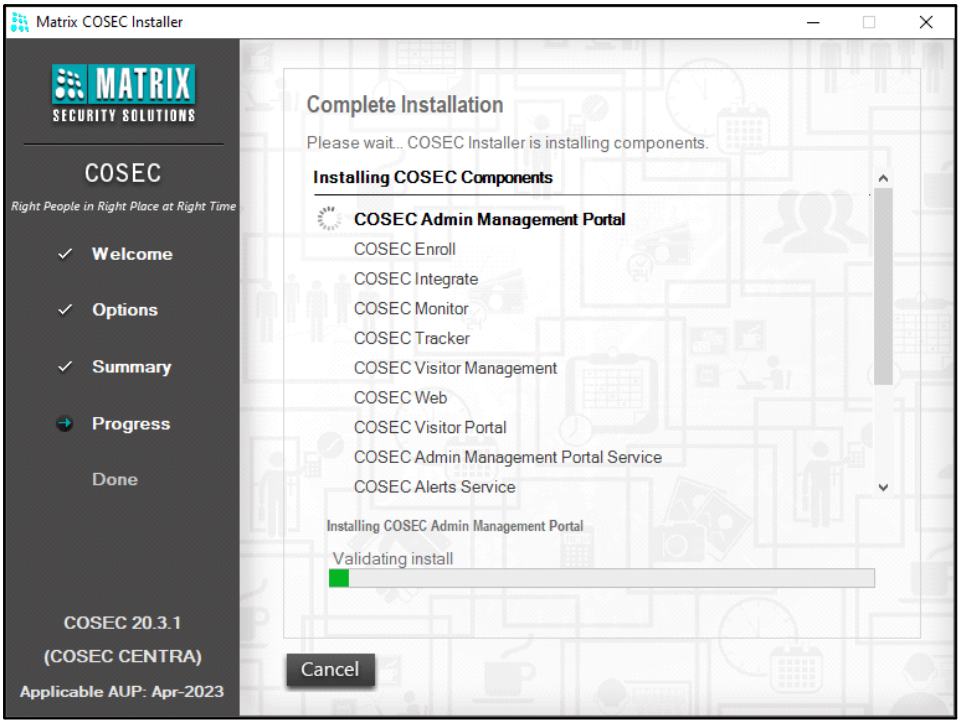
The licenses need to be purchased as per your requirement. For details, refer to **Supported Licenses** in the Admin Management Portal User Guide

Once the keys are received you need to Register/Update the same. For details, refer to **License and Services** in the Admin Management Portal User Guide.

The registration request is sent to the Virtual License Manager. The Virtual License Manager checks for the authenticity of the key as well as it communicates with the Matrix License Manager. Thereafter the request is served.

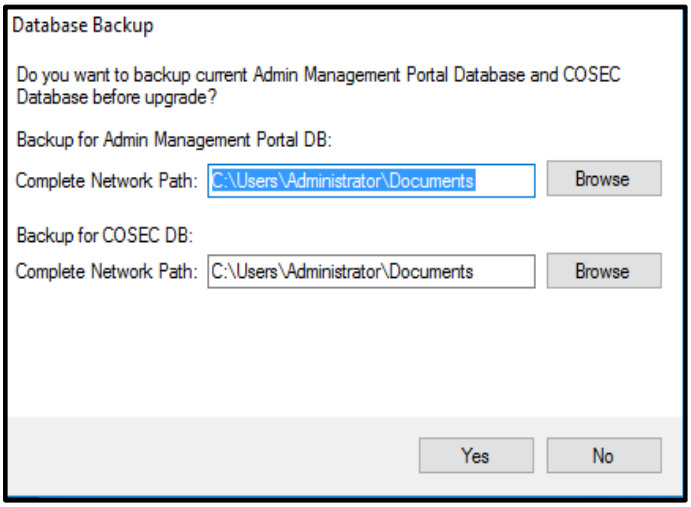
Once the License Verification Mode is selected and test connection is successful, click **Next** to proceed with the installation.

The Installation process of the various components begins.

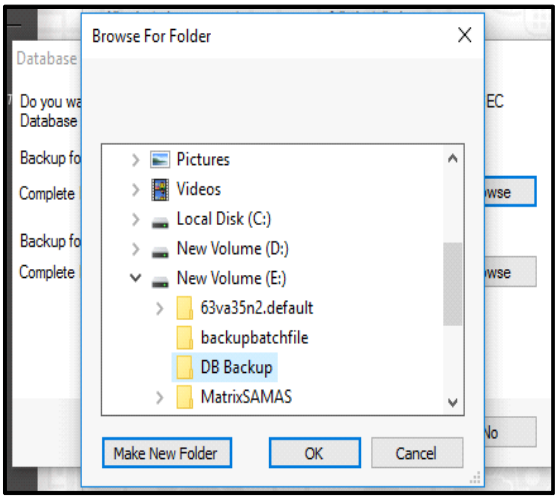


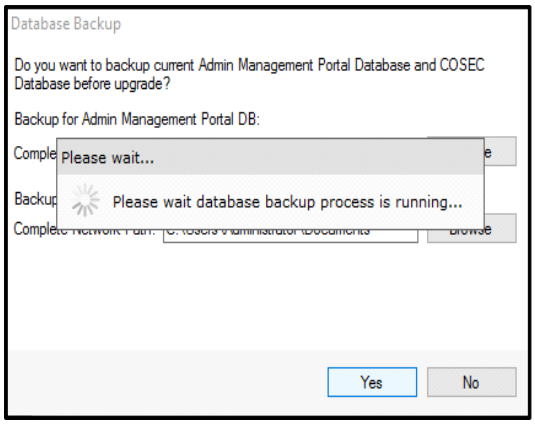
After the Installation is successful, the **Database Backup** pop-up appears.

- You can take the backup of the Admin Portal Database as well as COSEC Database.
- By default, the **Complete Network Path** is set as C:\Users\Administrator\Documents. You can also change this path as per your requirement. To do so,



- Click **Browse** and select the desired path where backup is to be taken.





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

After taking the backup, the following services will start automatically.

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

Once all the services are running, they appear in the tray.

The Master Service will only function when it gets the relevant license information. Hence, if you have opted for Dongle - Server Based or Device Based, make sure the Dongle is connected and if you have opted for Virtual License, you need to register the license key.

For more details related to License updation or registration of Server Based license or Device Based license or Virtual License, refer to the Admin Management Portal User Guide.

Now, you can login into the Admin Portal and COSEC Web.

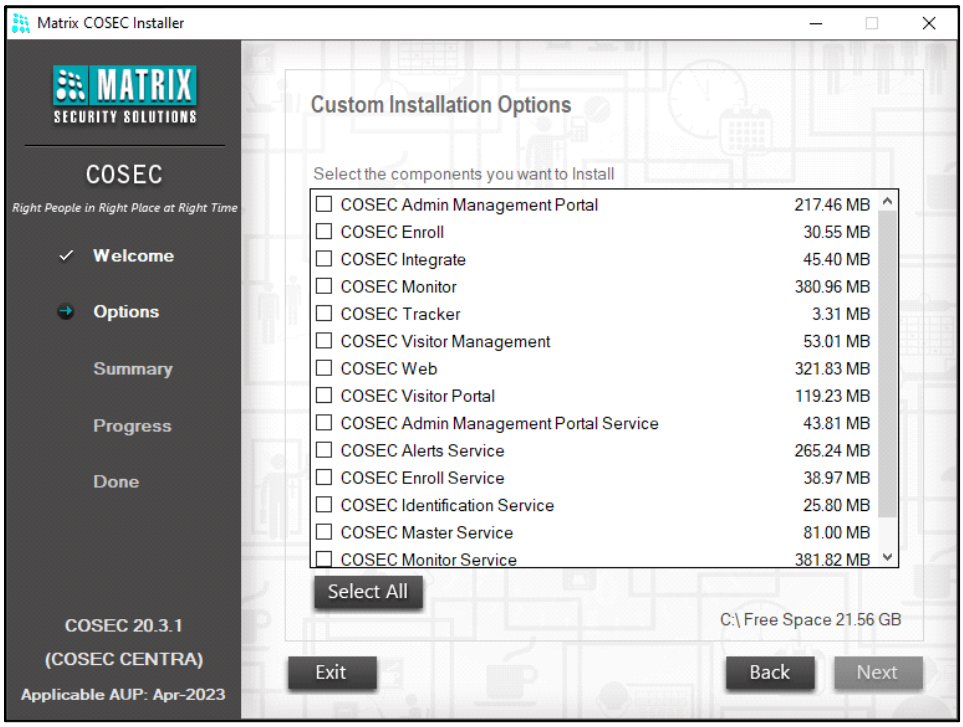
For more information regarding the above services refer, ***COSEC Services User Manual.***

Custom Installation

The **Custom Installation** option will install the selected COSEC components. Click on **Custom** option.

Make sure you install the following services for basic usage of COSEC Application —COSEC Admin Management Portal, COSEC Web, COSEC Admin Management Portal Service and COSEC Master Service. You can install other components as per your requirement.

- Select check boxes of the desired components from the list that you wish to install.



- Click **Next** to proceed. The remaining steps of installation are similar to **Complete Installation**. For details, refer to “Complete Installation”.

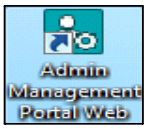
CHAPTER 2

Login to Admin Portal & COSEC Web

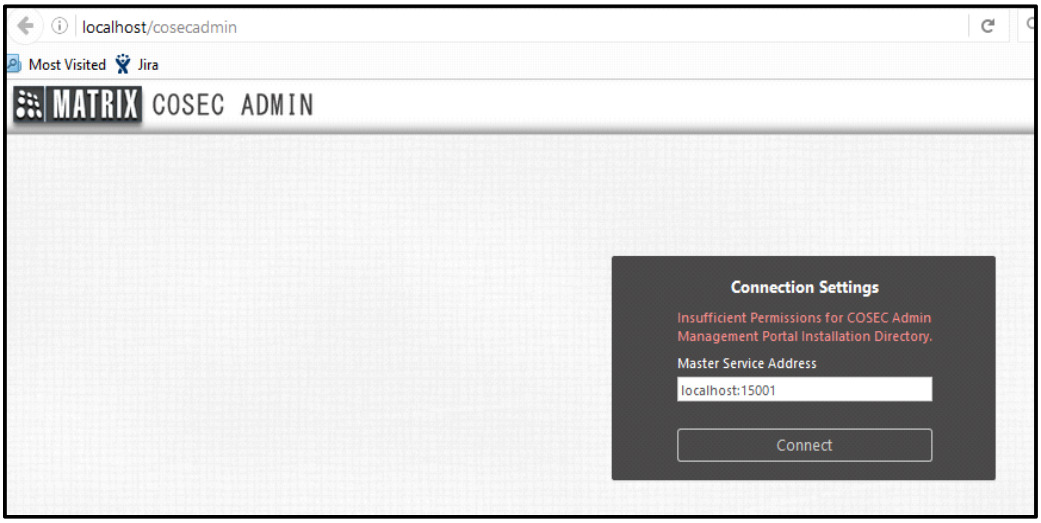
To login into the **Admin Portal** and **COSEC Web,** click the respective link for details.

- "Login to Admin Portal"
- "Login to COSEC Web"

Login to Admin Portal

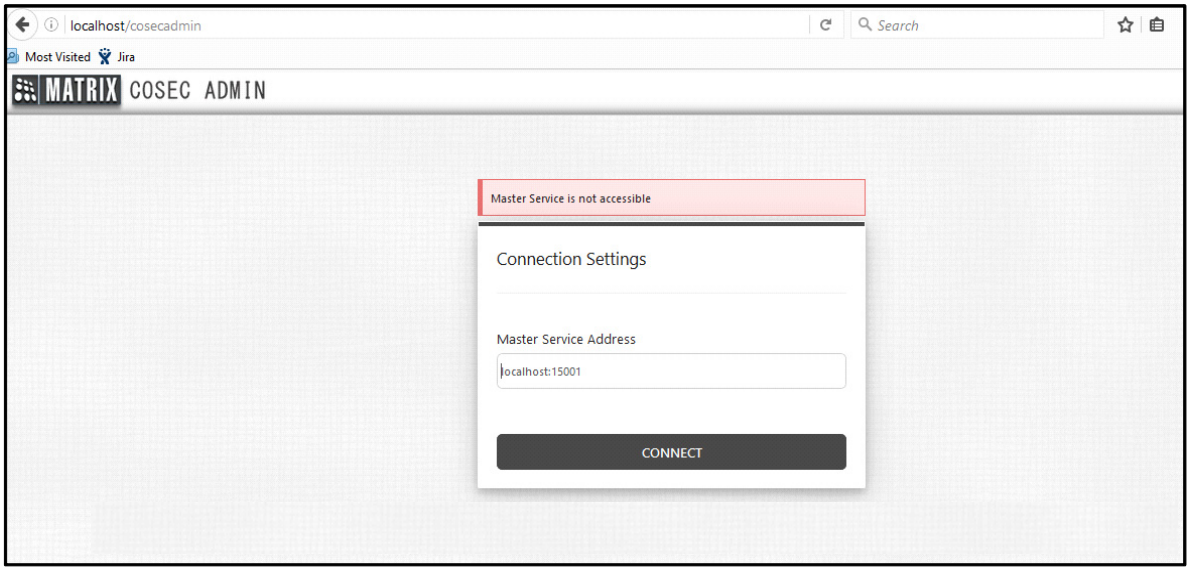
To access the Admin Management Portal, login to the Tenant Admin Portal with the URL localhost/cosecadmin on your browser or 192.168.104.12/cosecadmin or double-click on 

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



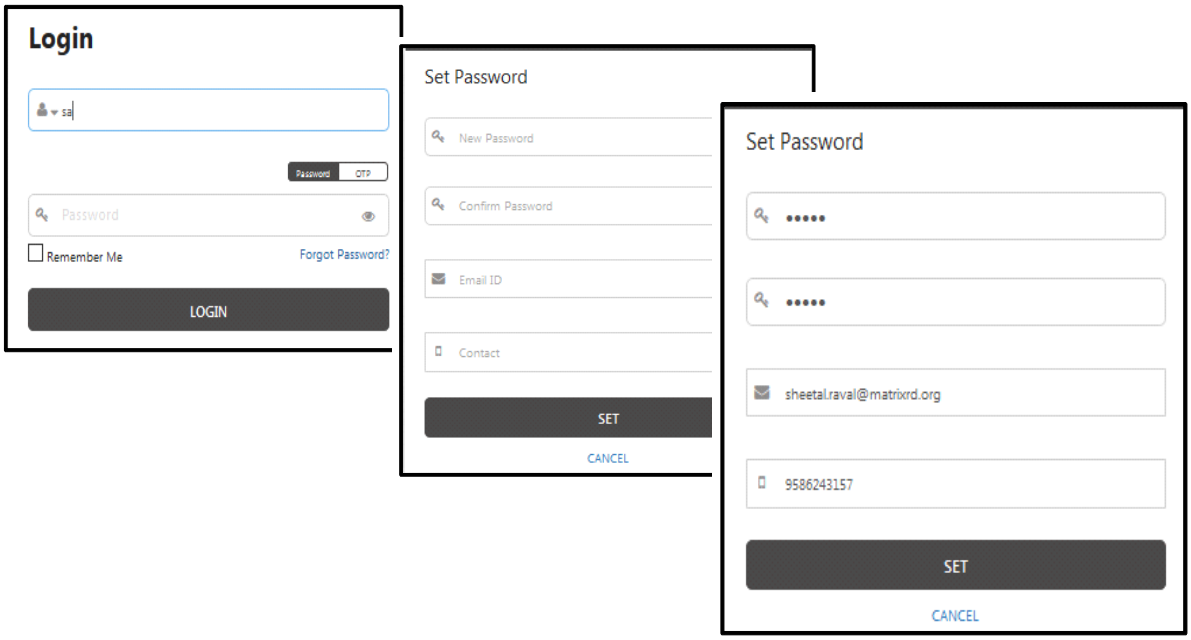
Check the rights on COSECADMIN folder. For this go to path C:\inetpub\wwwroot. The IIS user must be given full control rights. So click Edit and enable Full control checkbox. Then apply the changes. Now you can login to Admin Portal.

The Connection Settings page will appear as shown below:

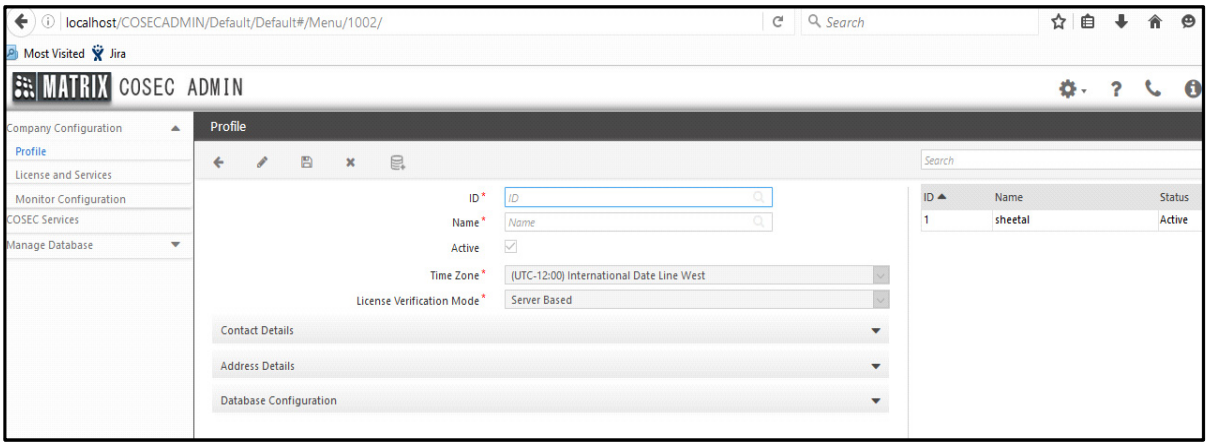


Enter the **Master Service Address** to connect with the database and click **Connect.** The Admin Portal will get connected with its database through the Master service. Ensure that Master service is running.

Then login with default login ID “sa” and set the desired password. You can use Login ID as **User ID/Mobile Number/Email ID** and login using OTP which is received on the Email ID and Contact number as specified while setting the password.



The Admin Portal page will open as shown below.



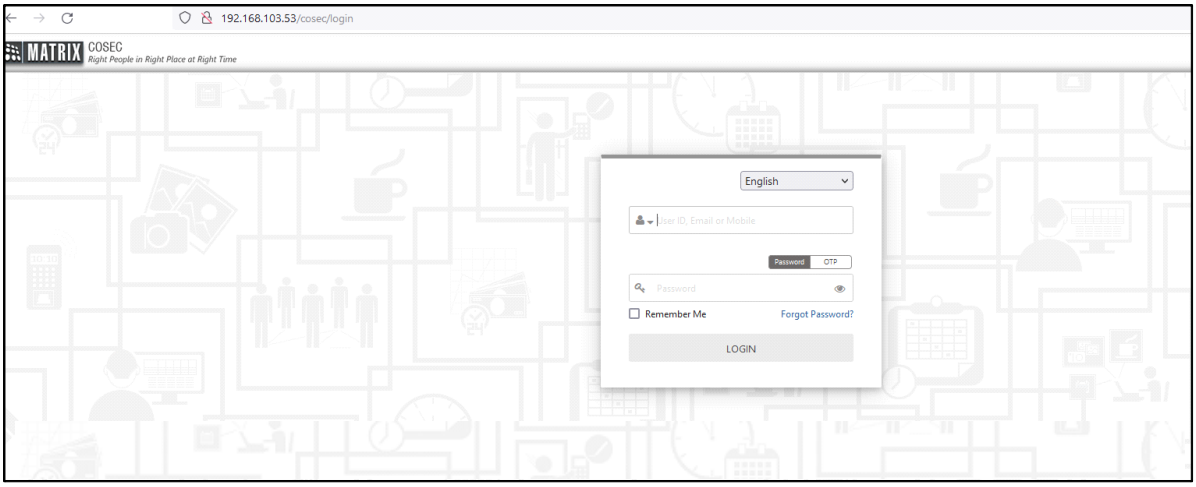
*For detailed information regarding Admin Portal refer **Admin Management Portal User Manual** from the setup.*

Login to COSEC Web

You can login to the COSEC Web using the Web URL **localhost/cosec** or say **192.168.104.12/cosec** in your browser or double-click on 

.

The login page appears as shown below.



You can select the desired language in which you wish to view the login page. To do so,

- Select the desired language from the dropdown list. The default language is English.

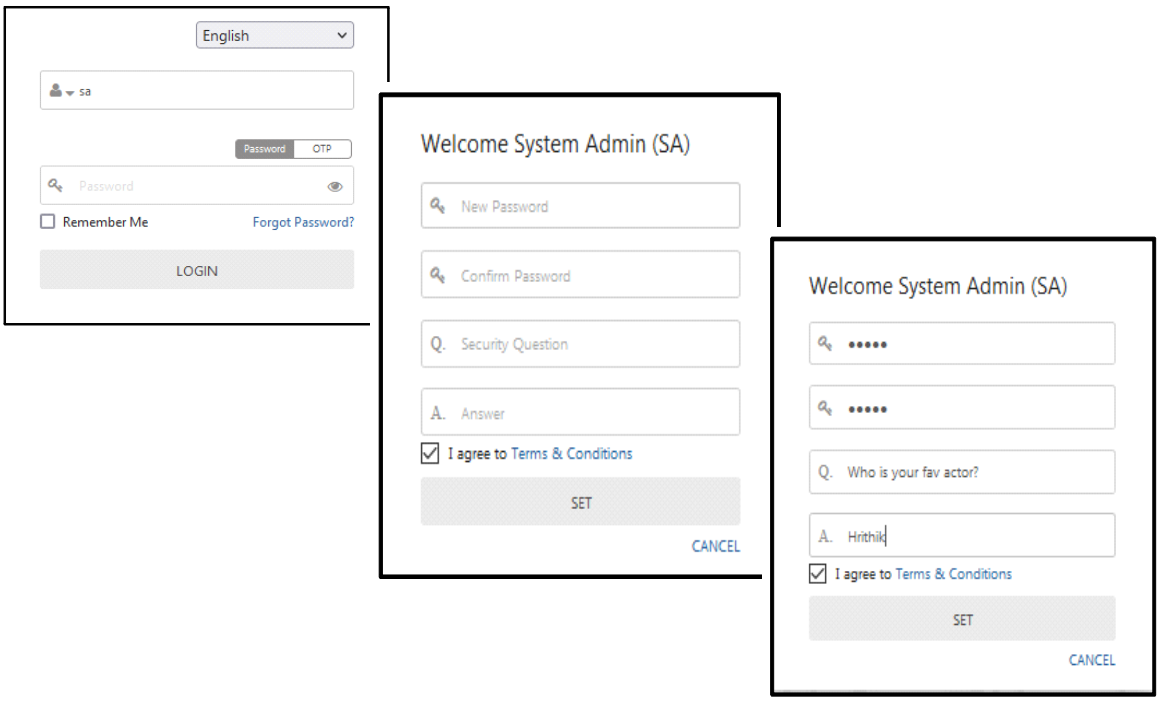
*The options for languages appear as per the language files available in the **Language Resource** folder at the following path: **C:\inetpub\wwwroot\COSEC\Language Resource.***

You can add language files to this folder via Language translation using the Multi-Language Utility. To know more, refer to the Multi Language Utility User Guide.

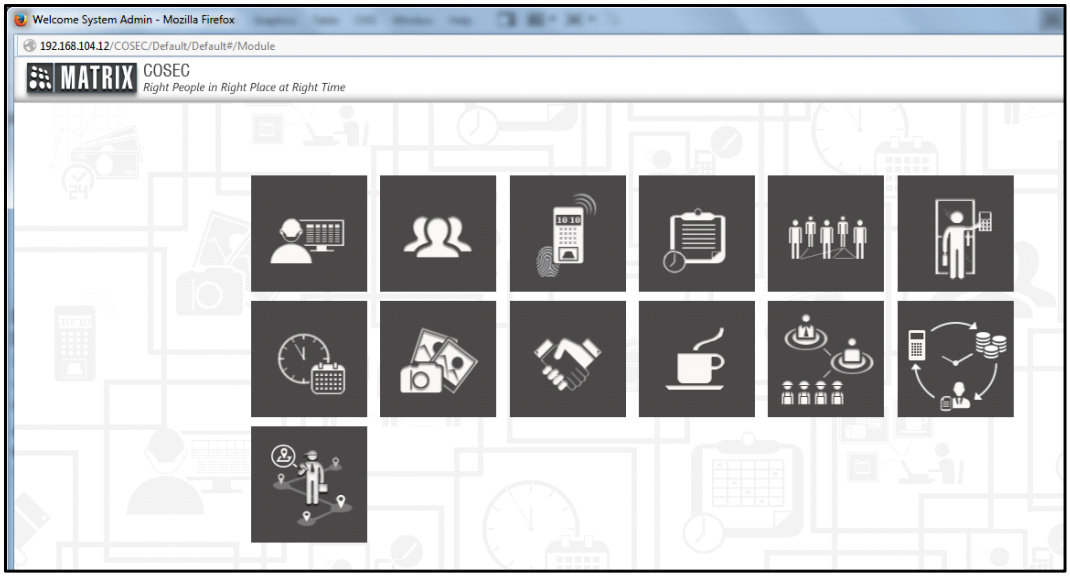
*The language set from **Global Language For Login** will be applicable to the login page. For more information refer **Global Language For Login** in User Guide, **Admin Module> System Configuration> Global Policy> Basic Policy> Global Language For Login.** If you wish to view the pages in another language post login, click **Account Settings > Set Language> Preferred Language** and select the desired language.*

- The login page will appear in the selected language for the current session.

When any of the system account user (sa, so, se) logins for the first time, they need to enter just the Login ID and directly click on Login and set the password.



You can also use **Login ID** as **User ID/Mobile Number/Email ID** to login into COSEC using the newly created password or the OTP once Alert configurations are done.



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

CHAPTER 3

Login to Visitor Portal

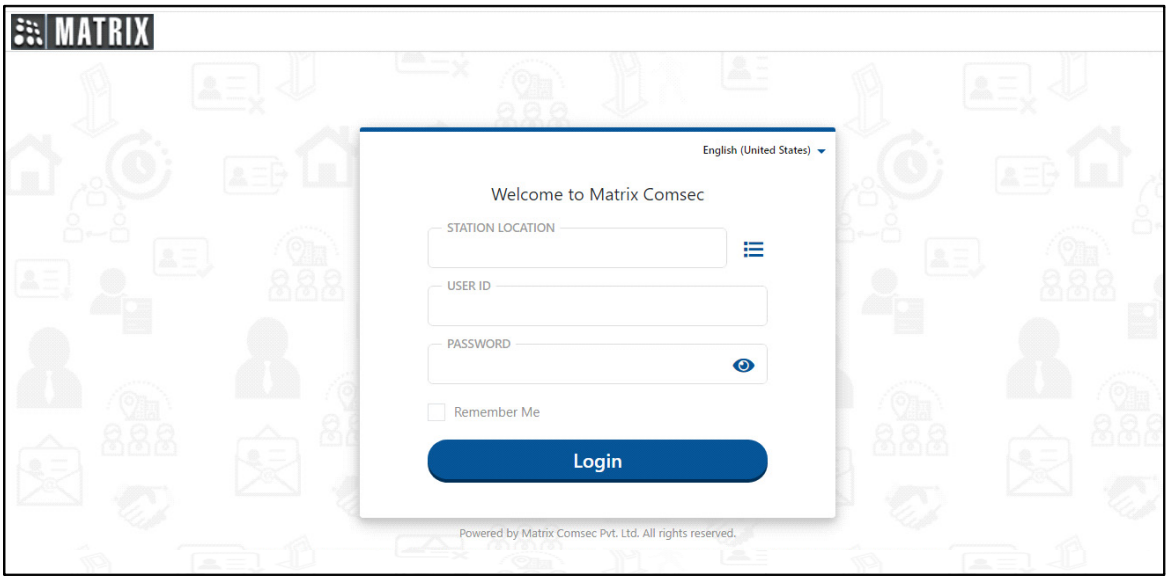
To access Visitor Portal, type the following link in the address bar of your browser: https://localhost/COSECVisitor/Login

or double-click on COSEC Visitor Portal 

.

To access Visitor Portal, VMS service should be running.

The login page will appear as shown below:



To view the login page in the desired language, click the Language dropdown list and select the desired language.

*By default, the login page appears in the language as set by the System Administrator in **Global Language For Login**. For more information refer **Global Language For Login** in User Guide, **Admin Module> System Configuration> Global Policy> Basic Policy> Global Language For Login.***

Click the picklist and select the desired **Station Location**.

Enter the **User ID** (default:sa) and **Password** (default:admin) as set for the COSEC Web Application. To view the password click icon.

Click the **Remember Me** check box to remember the User ID and Password automatically for the next login.

Click **Login.**

MATRIX COMSEC

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

www.matrixcomsec.com