



O-Insights™ Command Center– 1.0 Installation Guide

Contents

- Pre-Requisites3
- Minimum Server Requirements3
- Where to Install4
- Setup5
 - O-Insights Query Engine 5
 - Command Center Service.....10
- Enable SSL Encryption for Command Center 14
 - Using an Existing Certificate..... 14
 - Checking/ Verifying SSL Certificate.....16
- Command Center Plugin Installation 17

Pre-Requisites

- **XProtect 2023 R2**, or later.
- **.Net Framework v 4.7.2** or later.
- **Microsoft Visual C++ Redistributable 2019 Update 9 (Ver:14.27.29903)** or later
- **O-Insights Query Engine v 5.0**
- Following ports to be opened: **9011, 9026, 9027, 9028**

Port Number	Service	Source	Destination
9011	O-Insights Query engine service	O-Insights Command Center Service, XProtect Smart Clients running O-Insights Command Center	Server running O-Insights Query Engine
9026,9027,9028	O-Insights Command Center Service	XProtect Smart Clients running O-Insights Command Center	Server running Command Center

Minimum Server Requirements

CPU	<i>Quad-Core CPU with Hyper-Threading or better, 2.5 GHz or higher</i>
RAM	<i>8GB, 16GB or more for large systems</i>
Network	<i>Ethernet 100 Mbit or better</i>
Hard Disk	<i>8 GB or more free</i>

Where to Install

Application	Environment
<i>O-Insights Query Engine Setup.exe</i>	XProtect Management server or server that can connect to the Management Server.
<i>O-Insights Command Center Service Setup.exe</i>	XProtect Management server or server that can connect to the Management Server.
<i>O-Insights Command Center Plugins.exe</i>	XProtect Smart Client, XProtect Event Server

Setup

O-Insights Query Engine


O-Insights™ Query Engine is a powerful reporting engine designed to work natively with XProtect, enabling automated report generation. It is recommended to install it on the XProtect Management Server. Follow the steps below to install and configure the Query Engine.

1. Start the Installation

Open the setup file. After reviewing the License Agreement, click **Accept** and then **Next** to proceed.

License Agreement

Please read the following important information before continuing.



Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

O-Insights™ SOFTWARE LICENSE AGREEMENT

IMPORTANT!

This is a legal agreement ("Agreement") between you and Conexao Technology Solutions Pvt Ltd. ("Conexao") and governing your use of Conexao's software programs including the related manuals or any printed material thereof (the "Software")

READ CAREFULLY AND UNDERSTAND ALL OF THE RIGHTS AND RESTRICTIONS DESCRIBED IN THIS AGREEMENT BEFORE INSTALLING THE SOFTWARE. BY CLICKING THE BUTTON INDICATING YOUR ACCEPTANCE AS STATED BELOW OR INSTALLING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE FOLLOWING TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT USE THE SOFTWARE.

1. GRANT OF LICENSE

Conexao grants you limited and non-exclusive license to use. ("Use" as used herein shall include


☐ I accept the agreement

☒ I do not accept the agreement

Next

Cancel

2. License File

Select O-Insights License file

Select the license for O-Insights, then click Next.


Please select the license file:

☐ Skip For Now

Locate the license file by browsing the designated path or skip this step if the license file is already present (e.g., in an upgrade scenario). Alternatively, you can manually copy the license file into the License folder and then click **Next**.

Note: The license file can be found in the following directory:
'C:\Program Files\O-Insights Query Engine\License'.

3. Upgrade MongoDB

MongoDB Update
We recommend you to update MongoDB to the latest version

☒ Upgrade MongoDB to the latest version

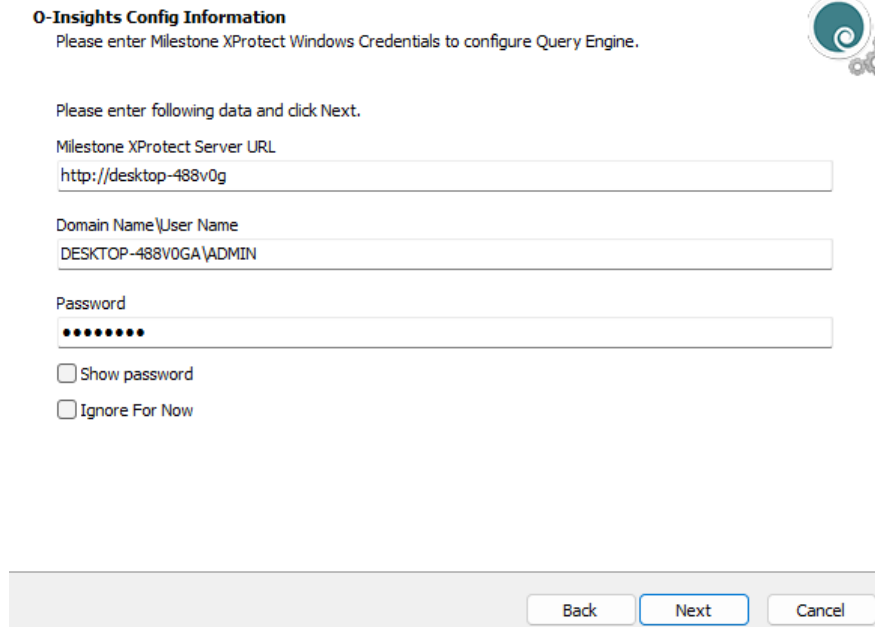
MongoDB URL:

MongoDB Username:

MongoDB Password:

If upgrading from version 4.8 to 5.0, you will be prompted to update MongoDB to the latest version. If you choose to proceed, check the corresponding box and provide the MongoDB username and password. This will migrate all databases to the latest version (7.0.12.0) upon successful installation.

4. Configure Query Engine



O-Insights Config Information
Please enter Milestone XProtect Windows Credentials to configure Query Engine.

Please enter following data and click Next.

Milestone XProtect Server URL

Domain Name\User Name

Password

☐ Show password
☐ Ignore For Now

Enter the Query Engine configuration details and click **Next**.

- a. **Milestone XProtect Server URL:** Obtain this from Milestone Server Configurator > Registering Servers > Management Server address.
- b. **Username and Password:** These credentials will be used to run the Query Engine Service. The account needs to have an administrator role in XProtect. If you skip this step, the service will run as “Local System,” requiring configuration with a XProtect Basic user with admin role using the Query Engine Configuration tool.

5. SSL Certificate (if applicable)

Enter the SSL certificate thumbprint, if encryption using SSL is configured on your system. If encryption is not configured, proceed without enabling it and click **Next**.

Encryption Setting

We recommend using a certificate issued by a Public Certificate Authority (CA)



☒ Enable encryption

Enter Certificate Thumbprint:

4a0416133ff1d3a907952d9463bc4b991d90f5ab

Back

Next

Cancel

6. Install or Use Existing MongoDB

- Install:** Select this option for a fresh installation of the Query Engine, including MongoDB configuration.
- Use Existing:** Choose this option if you have an existing MongoDB service. Enter the same MongoDB username and password used for other applications. Click **Next** to verify the credentials.

MongoDatabase Config Information



☒ Install

☐ Use Existing

Ip Address/Host name:

desktop-488v0g

Port No:

27017

Username:

admin

Password:

Re-Enter Password:

Back

Next

Cancel

7. Complete Installation

Click **Finish** to complete the installation. Ensure that the Query Engine has fetched all necessary data before starting the XProtect Smart Client.

☒ Install☐ Use Existing

Ip Address/Host name:

desktop-488v0g

Port No:

27017

Username:

admin

Password:

Re-Enter Password:

Back

Next

Cancel

Note: Please make sure to securely document and store the passwords as they will be required for any future upgrades or maintenance tasks. Losing access to these credentials may result in difficulties during the upgrade process.

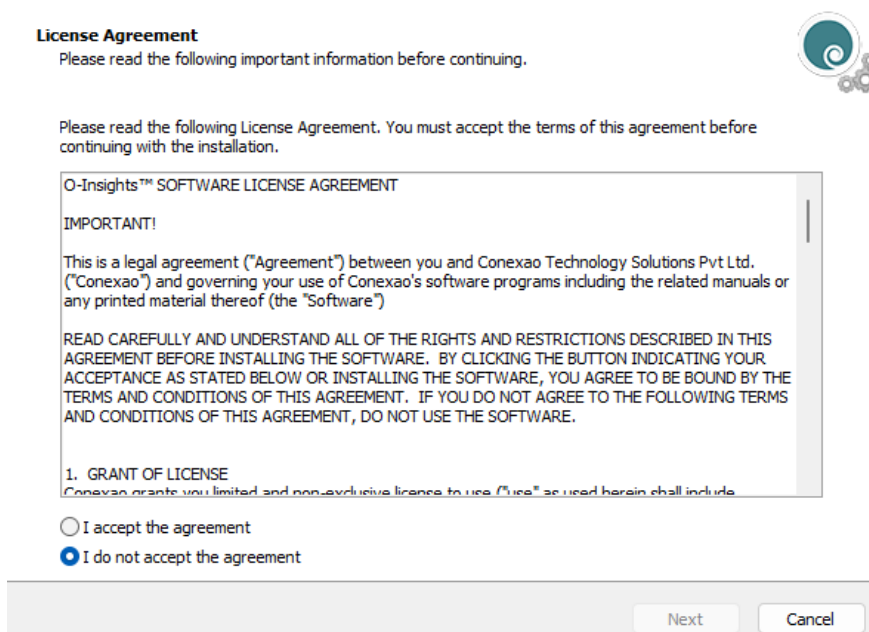
Command Center Service

The Command Center Service facilitates communication between XProtect and the Command Center application. The Command Center Service should be installed on the XProtect Management Server or any server machine that can connect to the XProtect Management Server for optimal performance.

Prerequisites:

- **Query Engine Installation:** It is mandatory to install the Query Engine before setting up the Command Center. If it is not already installed for O-Insights reporting, please proceed with its installation first, following the steps detailed above.

Installation Steps:



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

O-Insights™ SOFTWARE LICENSE AGREEMENT

IMPORTANT!

This is a legal agreement ("Agreement") between you and Conexao Technology Solutions Pvt Ltd. ("Conexao") and governing your use of Conexao's software programs including the related manuals or any printed material thereof (the "Software")

READ CAREFULLY AND UNDERSTAND ALL OF THE RIGHTS AND RESTRICTIONS DESCRIBED IN THIS AGREEMENT BEFORE INSTALLING THE SOFTWARE. BY CLICKING THE BUTTON INDICATING YOUR ACCEPTANCE AS STATED BELOW OR INSTALLING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE FOLLOWING TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT USE THE SOFTWARE.

1. GRANT OF LICENSE
Conexao grants you limited and non-exclusive licence to use ("Use" as used herein shall include

☐ I accept the agreement
☒ I do not accept the agreement

Next Cancel


1. Start the Installation

Open the setup file, *O-Insights Command Center Service Setup.exe*. After reviewing the License Agreement, click *Accept* and then *Next* to proceed.

2. License Agreement:

- Read the license agreement carefully.
- Select *I accept the agreement* and click *Next* to proceed.

3. Configuration Details:

Query Engine Config Information 

Please enter following fields, then click Next.


PROTOCOL:
☒ https ☐ http

SERVER:

PORT:

- **Protocol Selection:** Choose the appropriate protocol (HTTP or HTTPS).
- **Server Details:** Enter the hostname of the machine where the Query Engine is running in the *SERVER* field.
- **Port Configuration:** The default *PORT* is 9011. Click *Next* to continue.

4. Setting up MongoDB:

Config Information 

Please enter following fields, then click Next.

MongoDB Ip Address/Host name:

MongoDB Port No:

MongoDB Username:

MongoDB Password:

- The MongoDB v7.0 installs automatically with Query Engine 5.0. If MongoDB is already installed, ensure it is at least version 6.0 for compatibility.
- Leave the MongoDB IP Address/Hostname as default if the Query Engine and Command Center Service are on the same machine.
- **Default MongoDB Port No is 27017.**

- Enter the MongoDB password used during the Query Engine installation in the *MongoDB Username and MongoDB Password* fields.

Note: Please make sure to securely document and store the passwords as they will be required for any future upgrades or maintenance tasks. Losing access to these credentials may result in difficulties during the upgrade process.

5. SSL Encryption (Optional):

Encryption Setting



We recommend using a certificate issued by a Public Certificate Authority (CA)

- ☒ Enable Encryption
☐ Disable Encryption

Private Key Path:

Certificate Path:

Back

Next

Cancel

To enable the SSL Encryption, choose the *Enable Encryption* option.

- If using SSL Encryption, enable encryption and provide paths for the PEM Certificate and PEM Private Key in the *Certificate Path* and *Private Key Path* respectively.
- **Certificates used for XProtect, Query Engine, and Command Center Service should be consistent.**
- Once done, click *Next* to proceed.

6. Select Destination

Select Destination Location

Where should O-Insights Command Center be installed?



Setup will install O-Insights Command Center into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\O-Insights Command Center

Browse...

At least 245.6 MB of free disk space is required.

Back

Next

Cancel

On the **Select Destination Location** page, you can change the installation path of the service if necessary. The default installation path is *C:\Program Files\O-Insights Command Center*. Click *Next* to proceed.

7. Complete Installation

Click on *Install*. Once installation is done, click *Finish* to complete the installation and exit the setup.

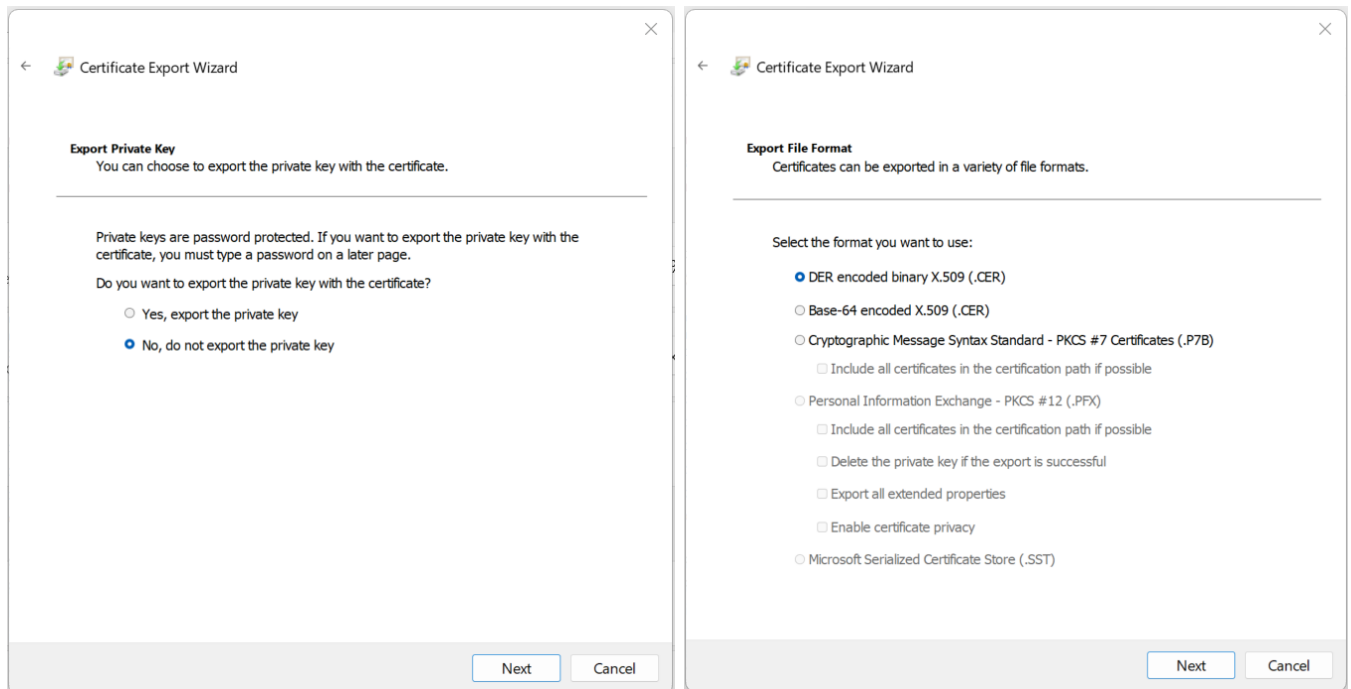
Enable SSL Encryption for Command Center

For enabling SSL with the Command Center over HTTPS, follow these detailed steps. We recommend obtaining a certificate from a trusted certificate authority for security reasons.

Using an Existing Certificate

To utilize an existing certificate, it needs to be converted to .pem format. Follow these steps to convert a certificate to .pem files:

1. **Open MMC:** Run *mmc.exe* and access the certificates folder.
2. **Export to .cer File:**



- Right-click on the required certificate.
- Navigate to All Tasks -> Export.
- Save the file as .cer in a desired location. Click *Next* and once done, click *Finish*.

3. Export to .pfx File:

The first screenshot shows the 'Export Private Key' step of the Certificate Export Wizard. It asks if the user wants to export the private key with the certificate. The user has selected 'Yes, export the private key'.

The second screenshot shows the 'Export File Format' step. It lists several formats: DER encoded binary X.509 (.CER), Base-64 encoded X.509 (.CER), Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B), Personal Information Exchange - PKCS #12 (.PFX), and Microsoft Serialized Certificate Store (.SST). The user has selected 'Personal Information Exchange - PKCS #12 (.PFX)' and 'Enable certificate privacy'.

- Repeat the export process for the same certificate (Right click -> All Tasks -> Export).
- This time, save as a .pfx file.

The screenshot shows the 'Security' step of the Certificate Export Wizard. It asks how to protect the private key. The user has selected 'Password'. A password field is shown with a masked password (seven dots). Below it is a 'Confirm password' field, also masked. The 'Encryption' dropdown is set to 'TripleDES-SHA1'.

- Enter a password for the file, which will be needed for the .pem conversion. Once done click *Next*.
- Save the file as .pem in a desired location. Click *Next* and once done, click *Finish*.

4. **Copy to OpenSSL Folder:** Move the `.cer` and `.pfx` files to the OpenSSL directory included with the Command Center setup.

5. **Convert to .pem:**

- Open a command line interface and navigate to the OpenSSL directory.
- Execute the following commands to convert files:

Convert `.cer` to `.pem`: `.\openssl x509 -inform DER -in yourcerfilename.cer -out cert.pem`

Convert `.pfx` to `.pem`: `.\openssl pkcs12 -in yourpfxfile.pfx -out key.pem -nocerts -nodes`

- Use the password from step 3 when prompted.

Note: When SSL is active for the Query Engine or Command Center Service using a self-signed certificate, adjust the `.env` file of the Command Center Service. By default, secure SSL certificate validation is enforced (value set to 1). For self-signed certificates, you need to modify the following line in the `.env` file located in `Install Directory>\O-Insights Command Center\Services\.env` to disable strict validation:

- `# Set to 0 if the SSL certificate is self-signed; setting it to 0 may compromise security`

`NODE_TLS_REJECT_UNAUTHORIZED=0`

Checking/ Verifying SSL Certificate

Here's the guide for checking and verifying the SSL certificate using the SSL Checker tool provided in the setup:

1. **Access Configuration File:** Open the `.env` file included with the SSL Checker tool.
2. **Update Certificate Paths**
 - Modify the following lines in the `.env` file to point to your certificate paths, then save the changes:
 - `SSL_CERTIFICATE_PATH=*C:\SSLCertificate\cert.pem*`
 - `SSL_PRIVATE_KEY_PATH=*C:\SSLCertificate\key.pem*`
3. **Run SSL Checker:** Execute the `ssl-cert-check.exe` tool to start the SSL verification process.
4. **Verify Certificate:** Once the application window provides a URL, copy and paste it into any web browser to check the certificate's functionality and ensure it is working correctly.

Command Center Plugin Installation

1. Prerequisites:

- Ensure that the Command Center Plugin is installed on all machines running XProtect Smart Client.
- If the event server is located on a different machine than the XProtect Smart Client machine, copy the *OInsights Incident Creator - Rule* folder to the MIP plugin folder of the event server. This folder can be found at:
 - *C:\Program Files\Milestone\MIPPlugins\O-Insights Command Center* on XProtect Smart Client machines where the Command Center plugin is installed.
- **Before starting the installation, ensure that all XProtect Client components are closed and the XProtect Event Server is stopped.**

Note: Installation should be done in the MIP Plugin Directory. Typically, this should be: *C:\Program Files\Milestone\MIPPlugins\O-Insights Command Center*

2. Installation Process:

- Open the setup EXE file provided.
- Read the license agreement, select *I accept the agreement*, and click *Next* to proceed.

Select Command Center License file



Select the license for O-Insights Command Center, then click Next.

Please select the license file:

Browse...

☐ Skip For Now

Back

Next

Cancel

- Choose the license file by clicking on *Browse* and then click *Next* to proceed.



Please enter following fields, then click Next.

PROTOCOL:

☒ https ☐ http

SERVER:

DESKTOP-ST2QKOF

PORT:

9026

Back

Next

Cancel

- Configure the Command Center Service details such as protocol, server, and port. Provide the DNS Host name of the machine running the Command Center Service in the *SERVER* field.

Note: Use the ping command to obtain the full DNS name.

3. Completing Installation:

- After completing the setup, click *Finish* to conclude the installation process.
- Restart the XProtect Event server.

You can start XProtect Smart Client from the installed directory or use the desktop shortcut.