



# O-Insights Plugin 5.0 Installation Guide

## Table of Contents

Pre-Requisites .....	3
Minimum Server Requirements.....	3
Where to Install.....	3
Setup .....	4
O-Insights Query Engine.....	4
O-Insights Plugin.....	10
O-Insights Web.....	13
Manual Steps to create the Web App .....	16
Configuring SSL/Enabling HTTPS .....	17
O-Insights Query Engine Configuration Tool .....	19
O-Insights Plugin Configuration.....	24
Steps to create Self Sign Certificate .....	25
MongoDB Password Update Procedure .....	27
Upgrading from Versions Before v5.0 .....	29
Pre-Upgrade Recommendations .....	29

## Pre-Requisites

- **Milestone XProtect 2023 R2, or later.**
- **.Net Framework v 4.7.2 or later.**  
[Link to download .NET Framework](#)
- **Microsoft Visual C++ Redistributable 2019 Update 9 (Ver:14.27.29903) or later.**
- **IIS (Internet Information Services) for Web Setup.**
- **Required Ports:** 8096 and 9011 must be available

Port Number	Service	Source	Destination
8096	O-Insights Web	Clients accessing the O-Insights Web	Server running O-Insights Web Server
9011	O-Insights Query engine service	XProtect Smart Clients running O-Insights workspace, reporting	Server running O-Insights Query Engine

**Note:** During installation, follow this order:  
**Query Engine, Plugin, and the Web Component.**

## Minimum Server Requirements

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

## Where to Install

Application	Environment
-------------	-------------

<i>OInsights-QueryEngine-Setup.exe</i>	XProtect Management server or server that can connect to the Management Server.
<i>O-Insights for VMS.exe</i>	XProtect Smart Client, XProtect Management Client
<i>O-Insights Web.exe</i>	XProtect Management server or server that can connect to the Management Server. Should have IIS installed.

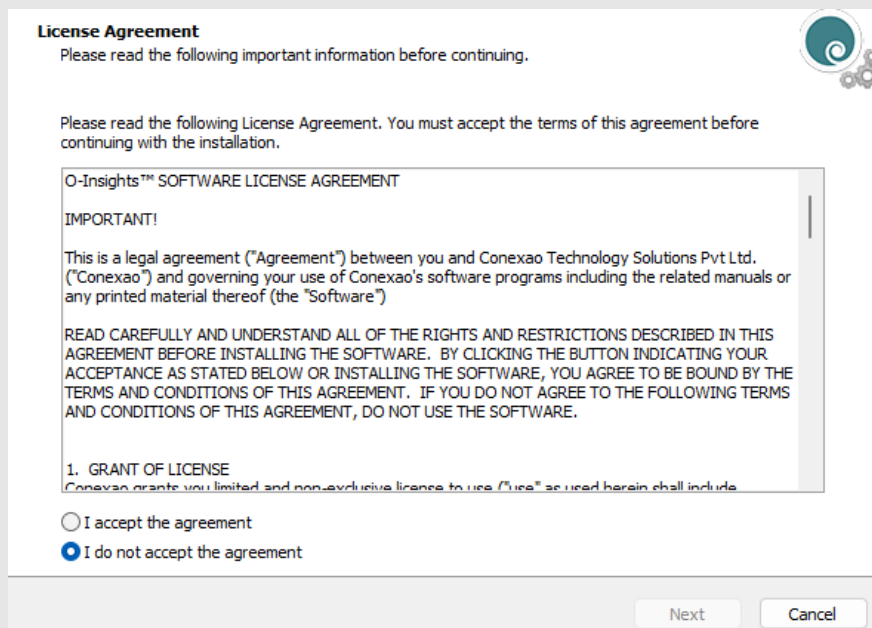
## Setup

### 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.

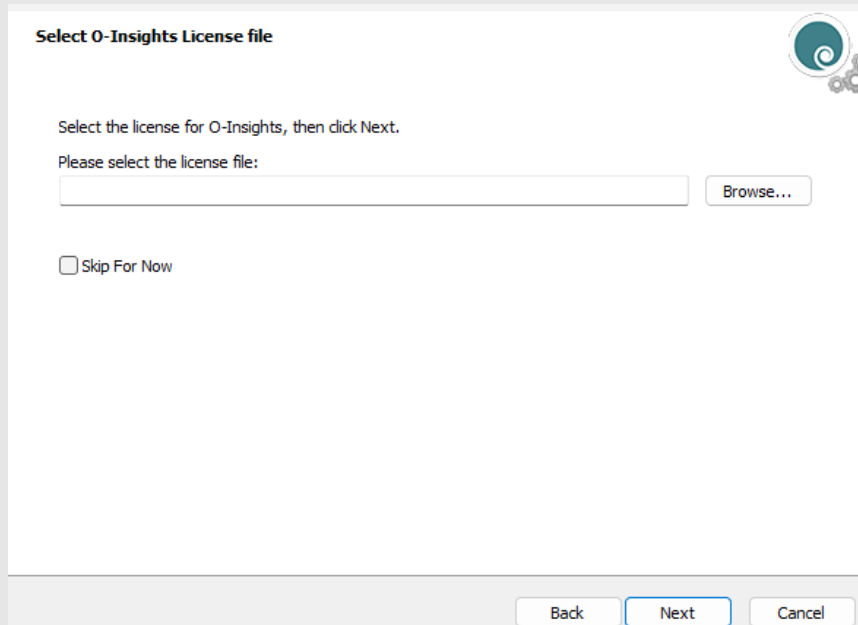
#### 1. Start the Installation

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



## 2. License File

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**.

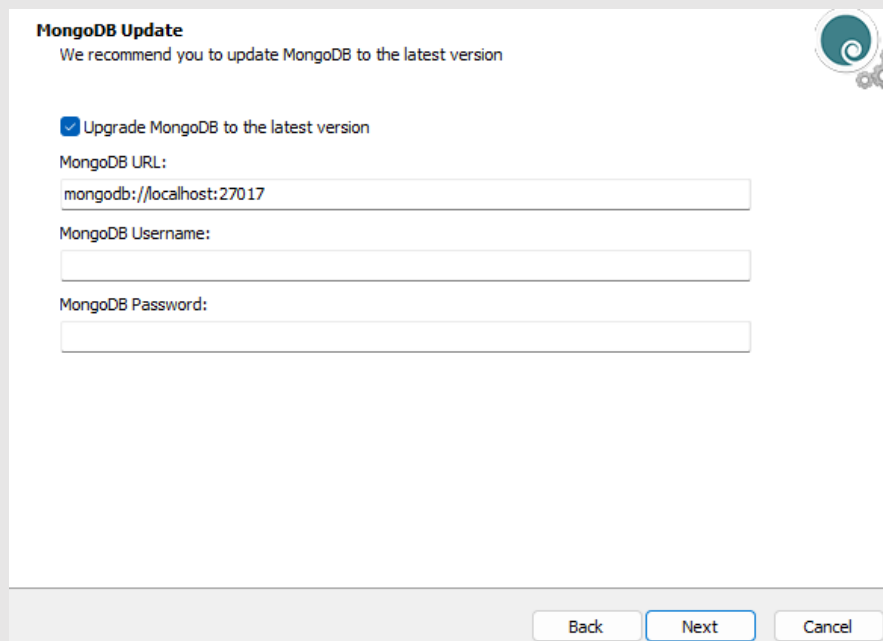


The screenshot shows a dialog box titled "Select O-Insights License file". In the top right corner is the O-Insights logo, which consists of a teal circle with a white swirl and three gray gears. The main text inside the dialog says "Select the license for O-Insights, then click Next." followed by "Please select the license file:". Below this text is a text input field and a "Browse..." button to its right. At the bottom left of the dialog is a checkbox labeled "Skip For Now". At the bottom right of the dialog are three buttons: "Back", "Next" (which is highlighted with a blue border), and "Cancel".

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

## 3. Upgrade MongoDB (Upgrade scenario)

If upgrading from O-Insights 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.



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

☒ Upgrade MongoDB to the latest version

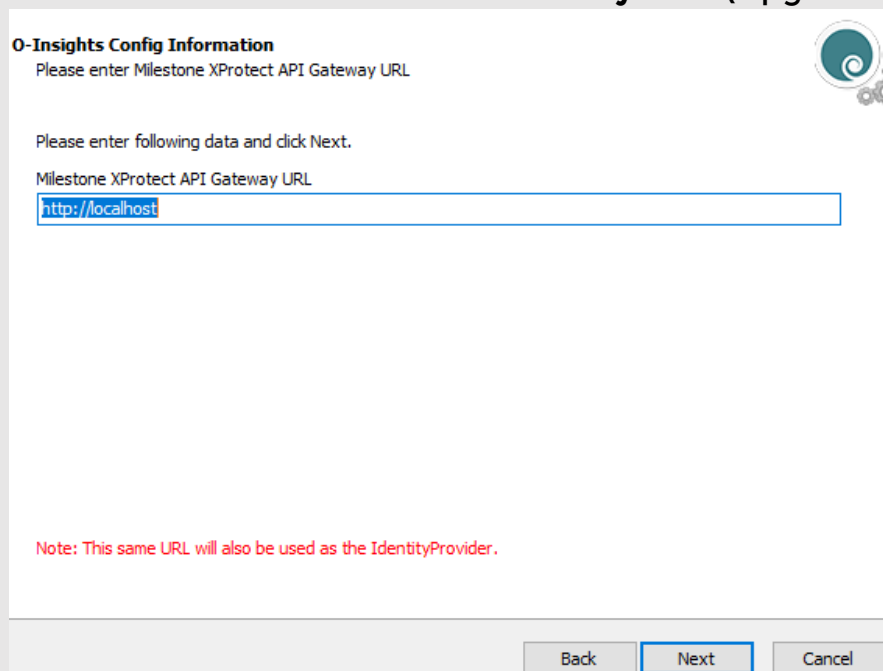
MongoDB URL:  
mongodb://localhost:27017

MongoDB Username:

MongoDB Password:

Back Next Cancel

#### 4. Enter Milestone XProtect API Gateway URL (Upgrade scenario)



**O-Insights Config Information**  
Please enter Milestone XProtect API Gateway URL

Please enter following data and click Next.

Milestone XProtect API Gateway URL  
http://localhost

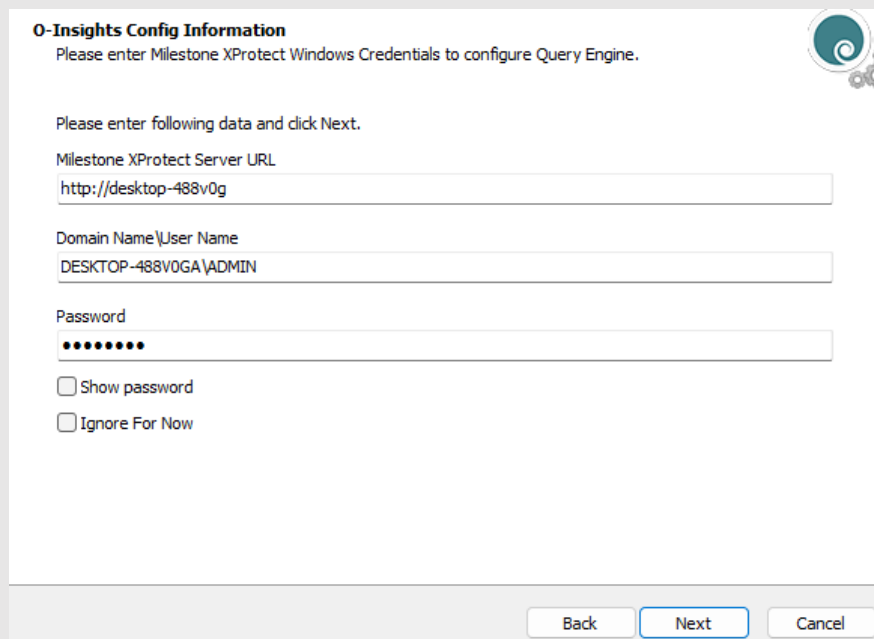
Note: This same URL will also be used as the IdentityProvider.

Back Next Cancel

#### 5. Configure Query Engine

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

- Milestone XProtect Server URL:** Obtain this from Milestone Server Configurator > Registering Servers > Management Server address.
- 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.



**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  
http://desktop-488v0g

Domain Name\User Name  
DESKTOP-488V0GA\ADMIN

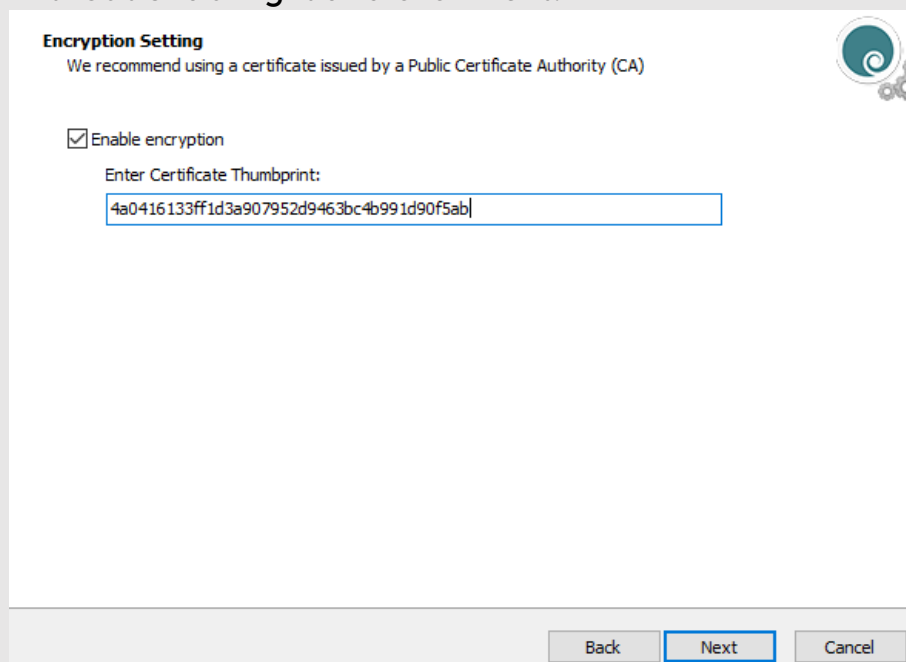
Password  
••••••••

☐ Show password  
☐ Ignore For Now

Back Next Cancel

## 6. 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)

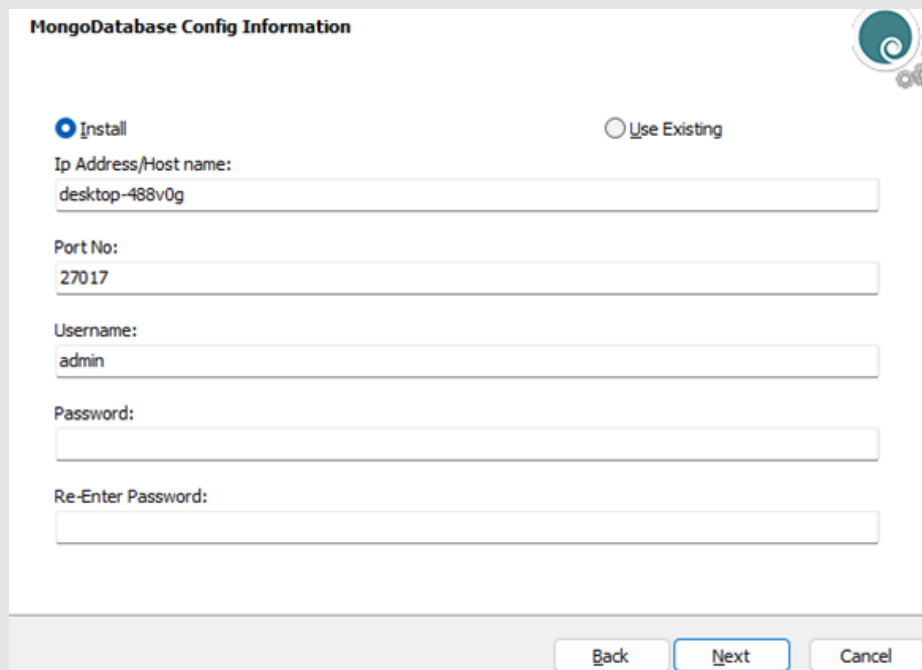
☒ Enable encryption

Enter Certificate Thumbprint:  
4a0416133ff1d3a907952d9463bc4b991d90f5ab

Back Next Cancel

## 7. 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

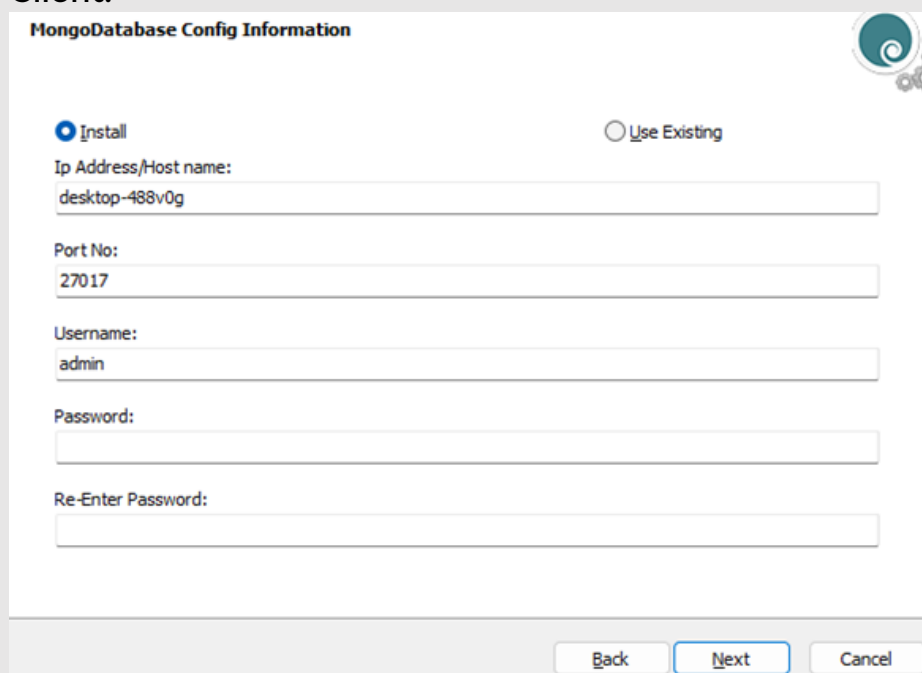
Password:

Re-Enter Password:

Back Next Cancel

## 8. Complete Installation

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



**MongoDatabase Config Information**

☒ Install ☐ Use Existing

Ip Address/Host name:  
desktop-488v0g

Port No:  
27017

Username:  
admin

Password:

Re-Enter Password:

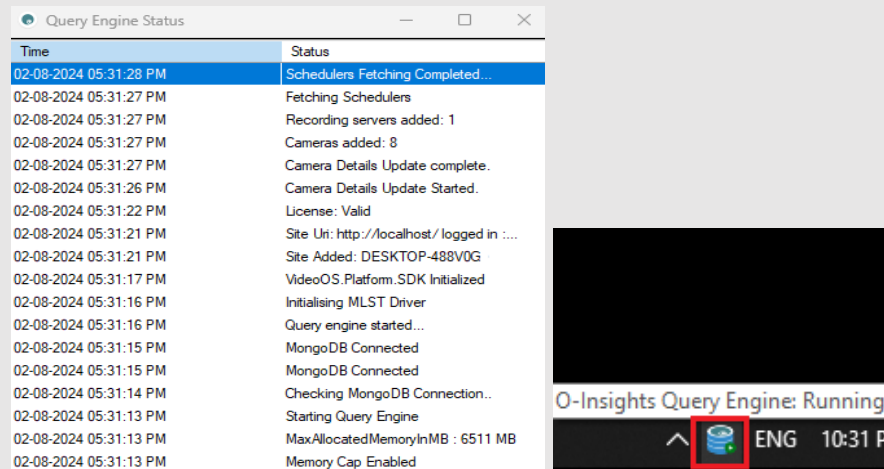
Back Next Cancel

**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.



## 9. Configuration Tray Application

After installation, a configuration tray application for the Query Engine will appear in the system tray. Double-click the icon to view the status.



For detailed information, refer to the O-Insights Query Engine Configuration Tool documentation.

## 10. Multisite Environment

If operating in a multi-server environment, utilize the Multisite feature.

**Note:** To bypass the Query engine address in the Query Engine Configuration Tool, uncomment the key below and add the required value

`<!-- <add key="QueryEngineAddress" value="" /> -->`

Path to locate the key : <Installation Directory>\O-Insights Query Engine\QEConfigurator.exe.config

## O-Insights Plugin

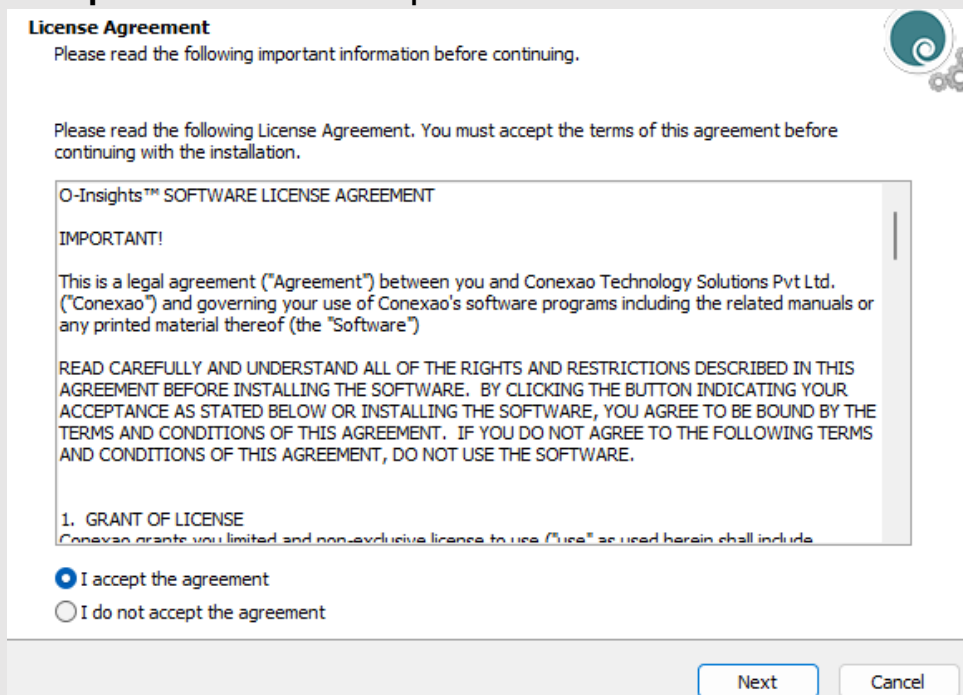
O-Insights™ is a dashboarding and analytics solution tailored for XProtect. It features an agile workspace allowing users to create and customize their dashboards. Once installed, an additional tab named “O-Insights” will appear in the XProtect Smart Client. Follow these steps for installation:

1. **Close All XProtect Components**

Ensure that all XProtect client components are closed before starting the installation.

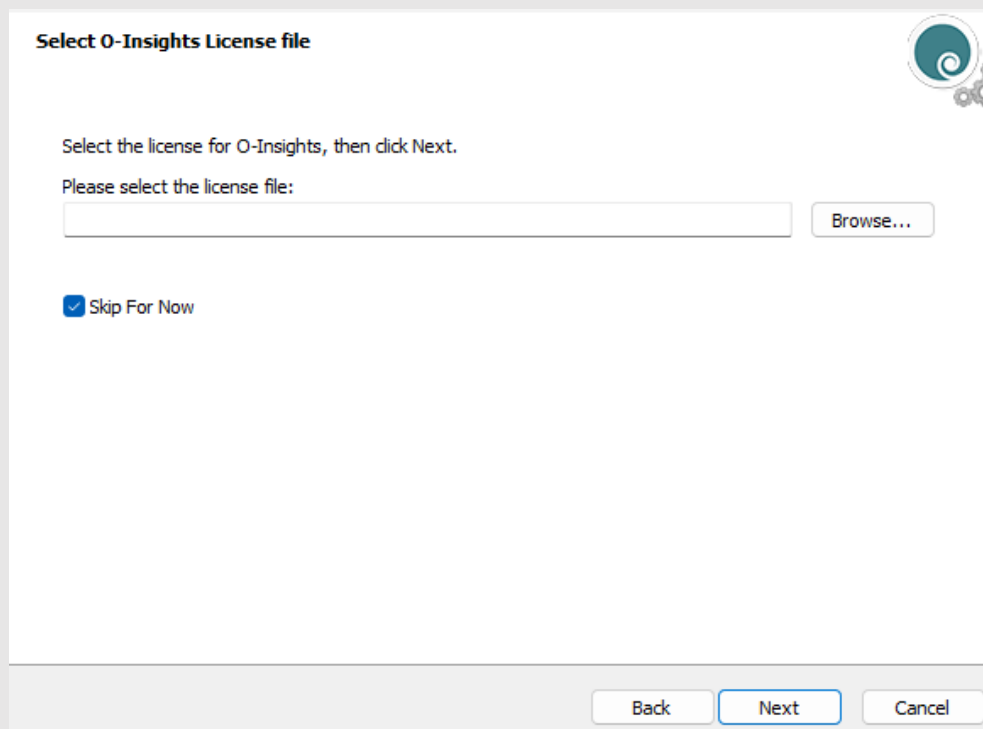
2. **Start the Installation**

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

The image shows a 'License Agreement' window for O-Insights. At the top, it says 'Please read the following important information before continuing.' Below this, it states 'Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.' The main text area contains the 'O-Insights™ SOFTWARE LICENSE AGREEMENT' and an 'IMPORTANT!' notice. The notice explains that this is a legal agreement between the user and Conexao Technology Solutions Pvt Ltd. It instructs the user to read carefully and understand all rights and restrictions before installing the software. It states that by clicking the button indicating acceptance, the user agrees to be bound by the terms and conditions. It also says that if the user does not agree, they should not use the software. Below the text, there are two radio buttons: 'I accept the agreement' (which is selected) and 'I do not accept the agreement'. At the bottom right, there are 'Next' and 'Cancel' buttons.

3. **License File**

Locate and select the license file by browsing the designated path or skip this step if the license file has already been placed in the License folder. Click **Next** to continue.



**Select O-Insights License file**

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

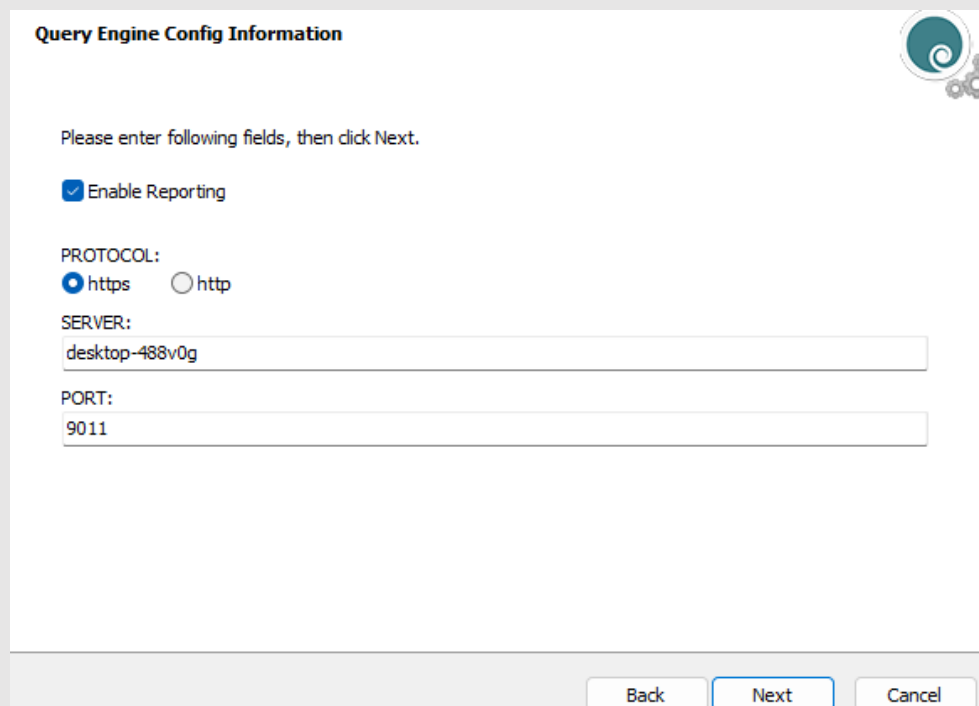
Please select the license file:

☒ Skip For Now

#### 4. Configure Reporting Settings

Enable reporting and provide the protocol, hostname/IP address, and port number of the machine where the Query Engine is installed. Click **Next**.

- a. If the Query Engine and workspace are on separate machines, ensure that port **9011** is open on both machines.



**Query Engine Config Information**

Please enter following fields, then click Next.

☒ Enable Reporting

PROTOCOL:  
☒ https ☐ http

SERVER:

PORT:

## 5. Complete Installation

Click **Finish** to complete the installation process.

## 6. Verify Installation

Launch the XProtect Smart Client from the installed directory or desktop shortcut. You should see the additional “O-Insights” tab within the client.

**Ensure that CefSharp version 119.4.30 is installed. If another version of CefSharp is installed by a different plugin, the O-Insights Plugin may not load.**

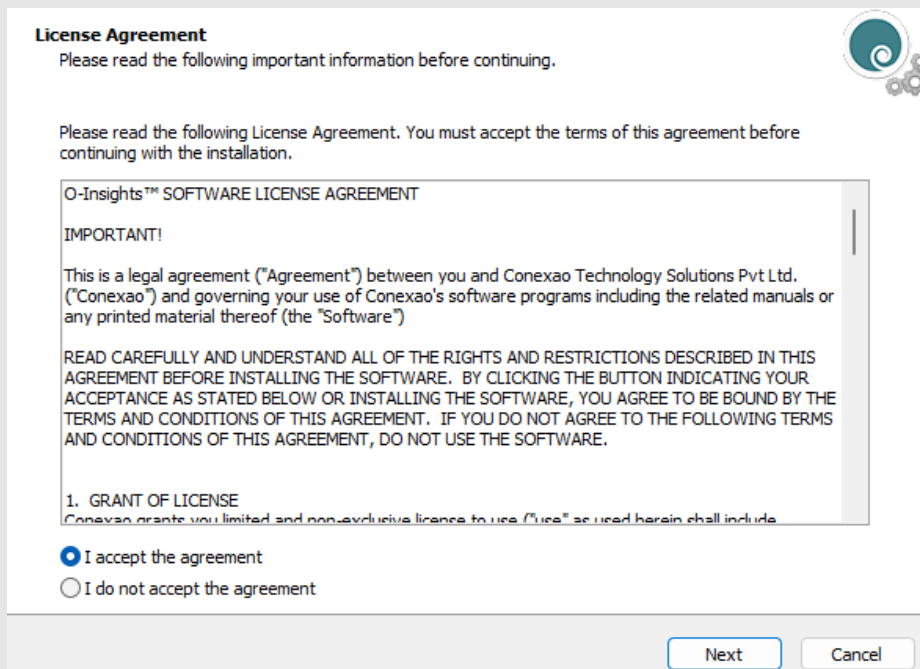
**Note:** Installation should be done in the MIP Plugin Directory. Default path “*C:\Program Files\Milestone\MIPPlugins\O-Insights for VMS*”

## O-Insights Web

**O-Insights™ Web** is a comprehensive dashboarding and analytics solution designed to integrate seamlessly with XProtect. It is compatible with standard browsers such as Google Chrome and Microsoft Edge, allowing users to create and customize their workspaces. Follow these steps to install and access O-Insights Web:

### 1. Start the Installation

Begin by launching the O-Insights Web setup. After reviewing the License Agreement, click **Accept** and then **Next** to proceed.



The screenshot shows a 'License Agreement' window with a title bar. Inside, there's a header 'License Agreement' and a sub-header 'Please read the following important information before continuing.' Below this, a paragraph states: 'Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.' A scrollable text area contains the 'O-Insights™ SOFTWARE LICENSE AGREEMENT'. The text starts with 'IMPORTANT!' and explains that this is a legal agreement between the user and Conexao Technology Solutions Pvt Ltd. It instructs the user to read carefully and understand all rights and restrictions before installing. Below the text area, there are two radio buttons: 'I accept the agreement' (which is selected) and 'I do not accept the agreement'. At the bottom right, there are 'Next' and 'Cancel' buttons.

**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

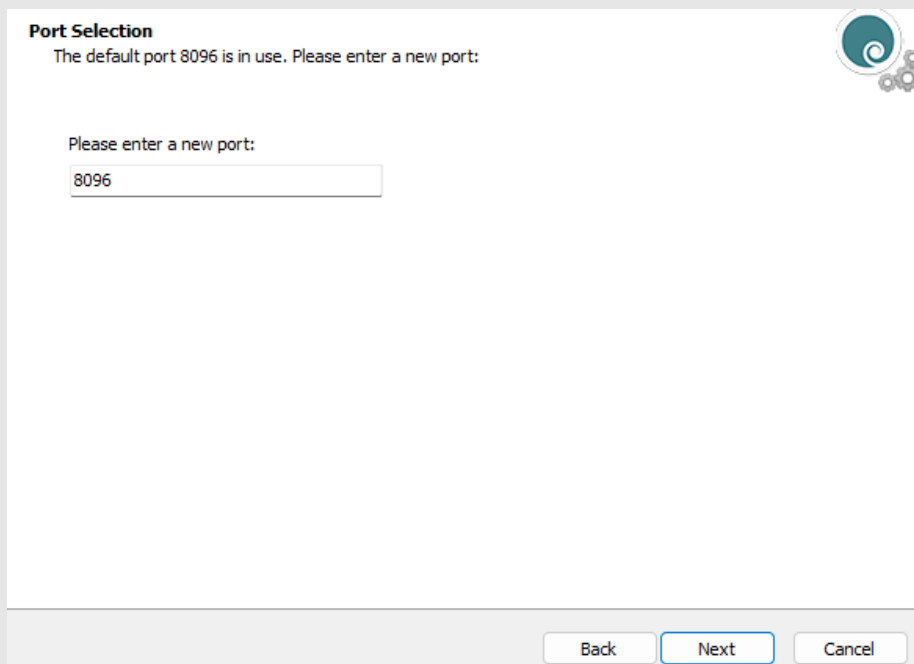
☒ I accept the agreement

☐ I do not accept the agreement

Next Cancel

### 2. Configure Port Number

Enter the port number for HTTP access. This port is used to access the O-Insights Web application.



**Port Selection**

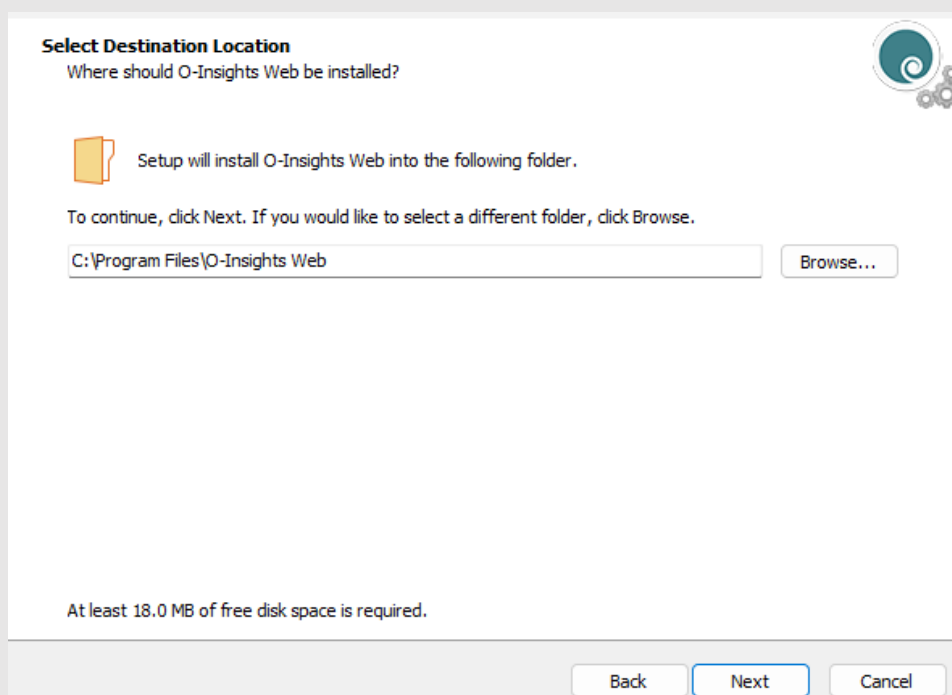
The default port 8096 is in use. Please enter a new port:

Please enter a new port:

Back Next Cancel


### 3. Select Installation Path

Choose the directory where O-Insights Web will be installed.



**Select Destination Location**

Where should O-Insights Web be installed?

 Setup will install O-Insights Web into the following folder.

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

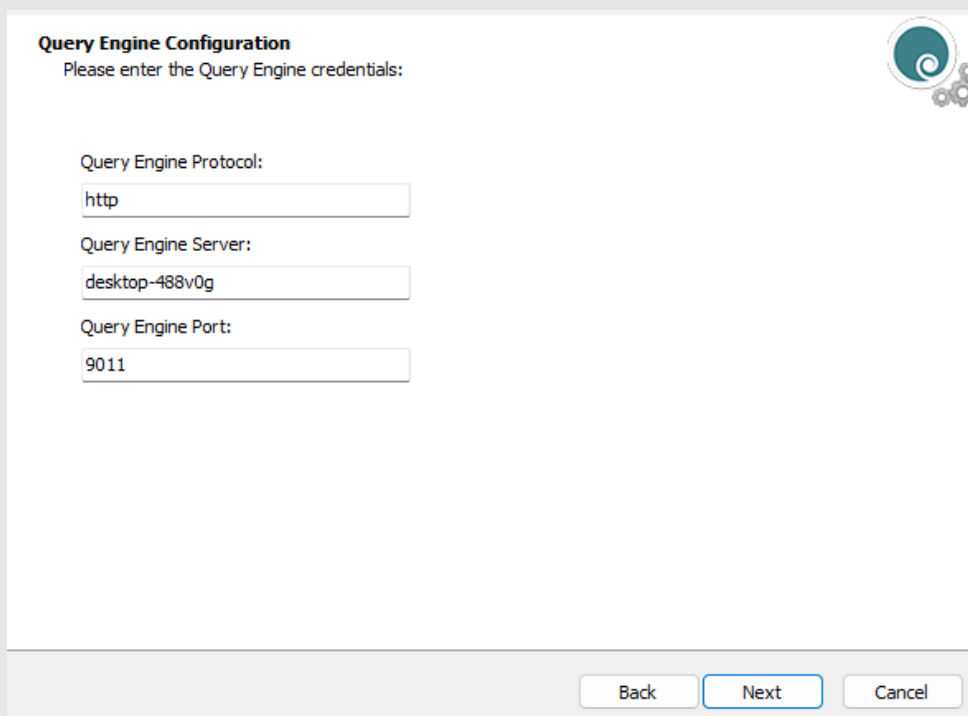
At least 18.0 MB of free disk space is required.

Back Next Cancel

### 4. Configure Query Engine Settings

Provide the Query Engine protocol, the hostname or IP address of the machine where the Query Engine is installed, and the port number. Click **Next** to continue.

**Note:** If you configured the query engine using a hostname or domain, you must use the same hostname or domain for both configuring and accessing the web interface.

A screenshot of a 'Query Engine Configuration' dialog box. The title bar says 'Query Engine Configuration'. Below the title, it says 'Please enter the Query Engine credentials:'. There are three text input fields: 'Query Engine Protocol:' with 'http' entered, 'Query Engine Server:' with 'desktop-488v0g' entered, and 'Query Engine Port:' with '9011' entered. At the bottom right, there are three buttons: 'Back', 'Next' (which is highlighted with a blue border), and 'Cancel'. In the top right corner, there is a logo consisting of a teal circle with a white swirl and three grey gears.

**Query Engine Configuration**  
Please enter the Query Engine credentials:

Query Engine Protocol:

Query Engine Server:

Query Engine Port:

Back Next Cancel

## 5. Complete Installation

After the installation is complete, click **Finish** to exit the setup wizard.

**Note:** To use the Live Camera widget, you need to make additional CORS configuration adjustments in the XProtect API Gateway.

## 6. Access the O-Insights Dashboard

To open the O-Insights Web dashboard, use the following URL in your browser:

*http://[hostname]:8096*

Replace [hostname] with the actual hostname of the machine where O-Insights Web is installed.

These steps will set up O-Insights Web, allowing you to start using its powerful dashboard and analytics features.

**Note:** If the Web app does not get published, please do it manually using the IIS Manager

## Manual Steps to create the Web App

### 1. Open IIS Manager

- Press Windows + R, type 'inetmgr', and hit Enter. This opens IIS Manager.

### 2. Add a New Website

- Right-click on 'Sites' in the Connections pane.
- Select 'Add Website...' from the context menu.

### 3. Configure the New Website

- **Site Name:** Enter a name for your site (e.g., O-Insights Web).
- **Physical Path:** Click the ... button next to the Physical path field, browse to the folder where you installed O-Insights Web earlier, and select it.
- **Binding Settings:**
  - **IP Address:** Select the appropriate IP address or leave it as 'All Unassigned' if you want the site to respond to all IP addresses on the server.
  - **Port:** Enter the port number.
  - **Host Name:** Enter the domain name if your site will respond to a specific domain or leave this blank if not applicable.
- **Host Header (optional):** If you're using host headers to host multiple websites on the same IP and port, enter the domain name here.
- **SSL Settings (if using HTTPS):** Choose an SSL certificate if you have one configured for HTTPS.

### 4. Complete the Setup

- After configuring the website, click OK to create the site.

### 5. Start the Web App

- Select your new web app in the Sites list.
- Click 'Start' in the Actions pane on the right-hand side.

### 6. Test Your Web App

- Open a web browser and enter the site's URL or IP address to verify that the site is up and running.

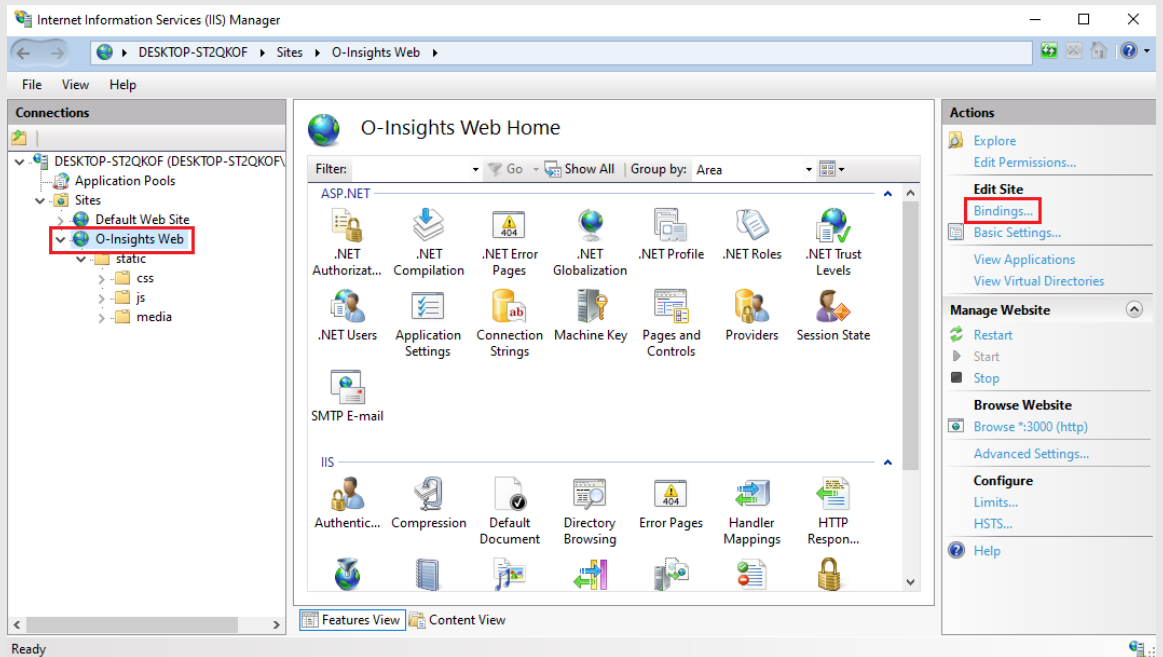


# Configuring SSL/Enabling HTTPS

To enable HTTPS for the O-Insights web application, follow these steps to configure it in IIS:

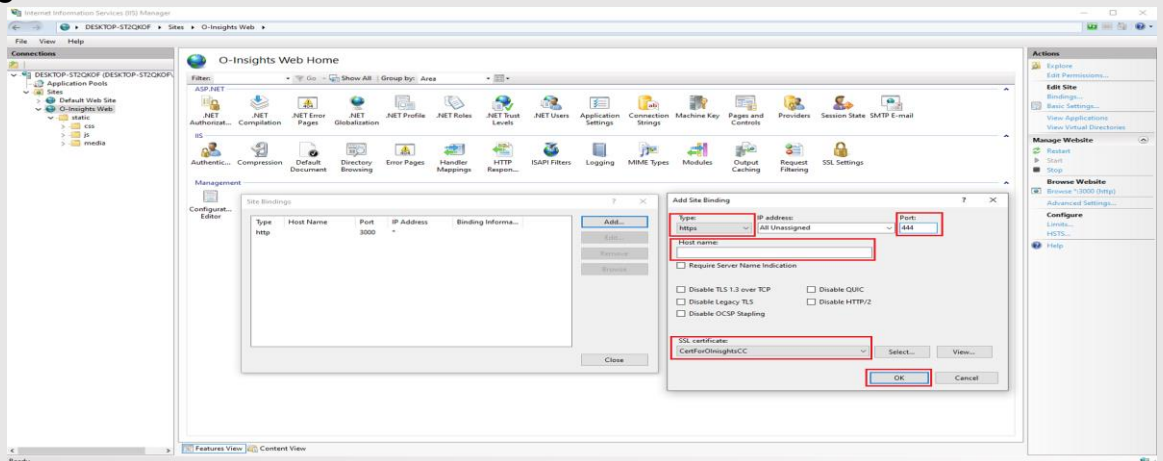
## 1. Open IIS Manager

On the machine where the O-Insights web app is installed, open IIS Manager. Locate and select **O-Insights Web** from the list of sites.



## 2. Access Site Bindings

Click on **Bindings** in the right-hand Actions pane to open the Site Bindings dialog.



## 3. Add HTTPS Binding

- Click **ADD** to create a new site binding.
- From the **Type** dropdown menu, select **https**.
- Enter the appropriate **Port Number** (typically 443 for HTTPS or any other port configured for your site).

- Enter the **Domain Host Name** of the machine where O-Insights web is installed.
- Select the appropriate **Certificate** from the dropdown (refer to the Self-Signed Certificate section for details).
- Click **OK** to save the binding.

#### 4. Ensure Consistent Certificate Usage

The certificate used for XProtect, O-Insights Query Engine, and the O-Insights web app should be the same to maintain consistency across services.

#### 5. Verify URL Configuration

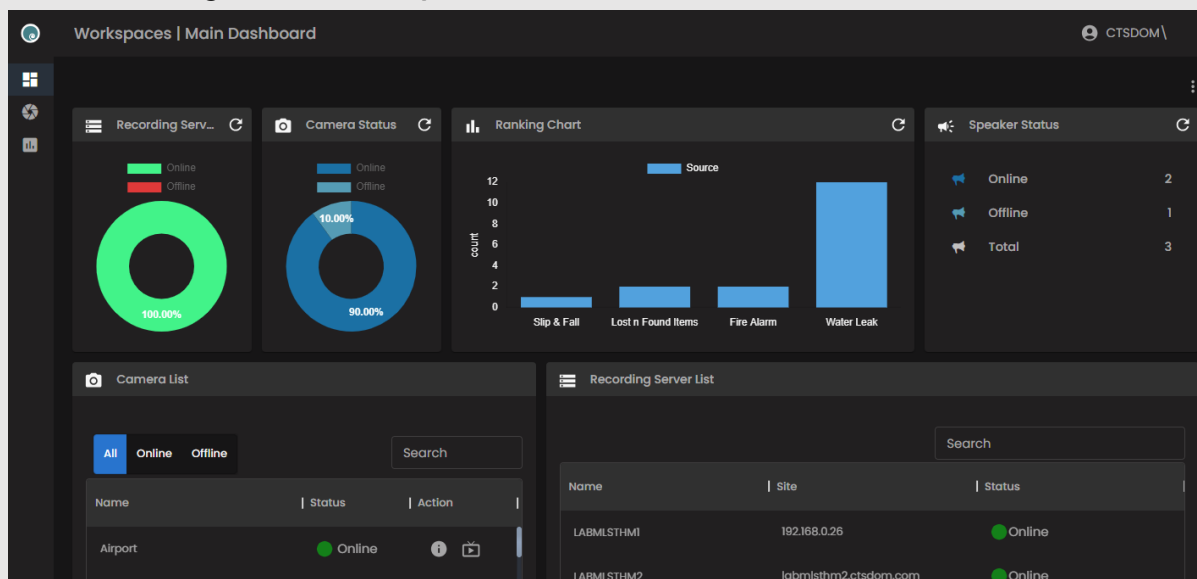
The configured URL will appear under **Browse Website** in the right-hand Actions pane.

#### 6. Access the Dashboard

You can now access the dashboard by navigating to the URL in your browser. For example:

*https://[Server Name]:444/*

Replace [Server Name] with the domain name of the machine and 444 with the configured HTTPS port number.



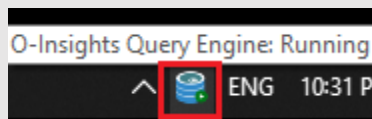
#### 7. Custom Dashboard Configuration

For additional customization of the dashboard, refer to the O-Insights web manual for detailed instructions.

Following these steps ensures that your O-Insights web app is properly configured to use HTTPS, enhancing security and accessibility.

## O-Insights Query Engine Configuration Tool

The O-Insights Query Engine Configuration Tool provides a range of options for managing and configuring the Query Engine from the system tray.

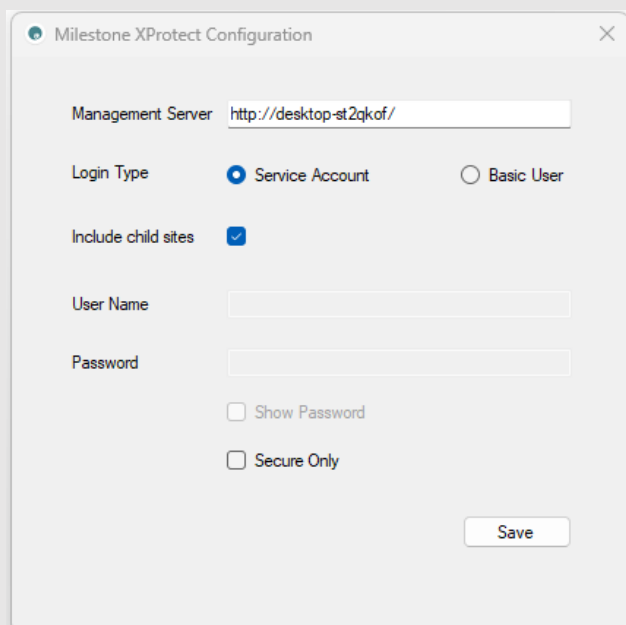


To use these options, right-click on the QE Configuration Tool icon in the system tray and select the desired option. Here's an overview of the available options:

Status: Running
Restart
Start
Stop
Site
Camera
Event Server
Running Job
Milestone XProtect Configuration
Multisite Configuration
Query Engine Configuration
MongoDB Credentials
Reset Credentials
Test Connection
Logs
Version: 5.0.15.0
Exit

1. **Status:** Displays the current status of the Query Engine service.
2. **Restart:** Restarts the Query Engine service.
3. **Start:** Starts the Query Engine service.
4. **Stop:** Stops the Query Engine service.
5. **Sites:** Lists all added sites.
6. **Camera:** Displays all cameras with server names and IP addresses and allows exporting this information to CSV.
7. **Event Servers:** Shows the connection status of event servers; If event server is not connected the dashboard will not display data correctly.
8. **Running Jobs:** Lists any running reports or user jobs.

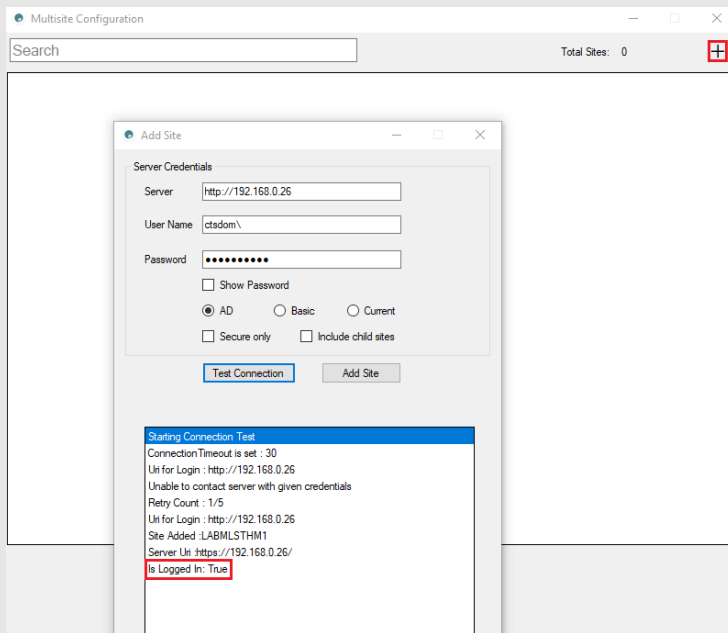
9. **Milestone XProtect Configuration:** Enter XProtect Management Server credentials for communication with the Query Engine. You can select either a Service Account or Basic Admin User for running the QE service. Check the "Include Child Sites" option to include data from child sites of a federated or interconnected master site; uncheck this option to include only parent site data. Click "Save" to apply changes.



The screenshot shows a dialog box titled "Milestone XProtect Configuration" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Management Server:** A text field containing the URL "http://desktop-st2qkof/".
- Login Type:** Two radio buttons: "Service Account" (selected) and "Basic User".
- Include child sites:** A checkbox that is checked.
- User Name:** An empty text field.
- Password:** An empty text field.
- Show Password:** An unchecked checkbox.
- Secure Only:** An unchecked checkbox.
- Save:** A button at the bottom right.

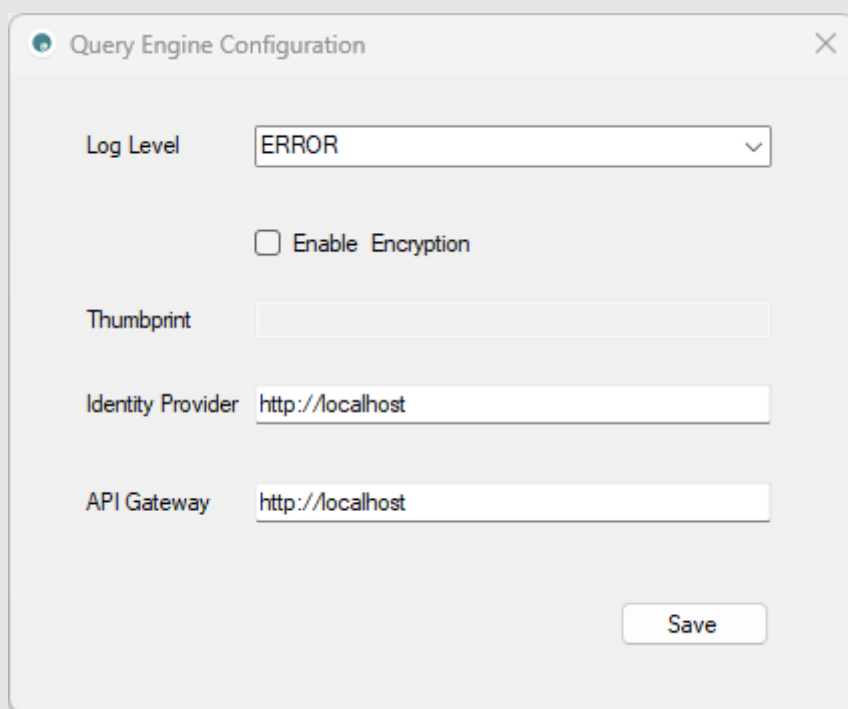
10. **Multisite Configuration:** This option allows users to add standalone XProtect servers that are not federated or use interconnect with the master site. You can view camera and recording server status and generate reports for devices of these standalone servers(aka sites). To add a site, click the "+" button, enter the XProtect Management Server details and credentials on the Add Site screen, and click "Test Connection" to ensure the site is reachable and the login is successful. Once verified, click "Add Site" to include it. You can use either a Windows User or Basic User to add the site.



Added sites will appear in the list, and you can edit or delete sites as needed.

Multisite Configuration									
Search									
Total Sites: 1									
Sl.No	URL	Username	Password	Secure Only	Include Child Sites	Authorization	Edit	Delete	
1	http://192.168...	ctadom\	*****	No	No	AD	Edit	Delete	

**11. Query Engine Configuration:** Configure settings for the O-Insights Query Engine. In the Log Level dropdown, select what information should be logged in the Query Engine log; “ERROR” is typically used to log only errors. Enter the addresses for the *Identity Provider* (XProtect IDP server) and *API Gateway* (XProtect API server).



Query Engine Configuration

Log Level: ERROR

☐ Enable Encryption

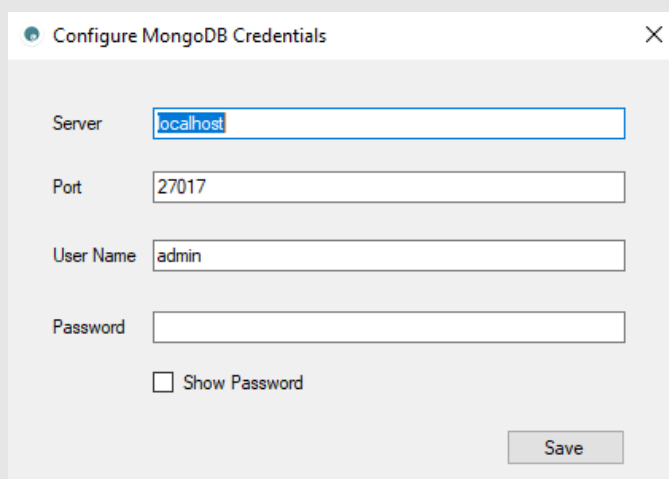
Thumbprint:

Identity Provider: http://localhost

API Gateway: http://localhost

Save

- 12. MongoDB Credentials:** Manage the database credentials used by the O-Insights Query Engine to connect to MongoDB. Enter the Server Address, Port Number, Username, and Password as configured. If you manually change the MongoDB password, update it here. If the MongoDB service is not running, you can enter the password used during the initial installation and save it before restarting the MongoDB service.



Configure MongoDB Credentials

Server: localhost

Port: 27017

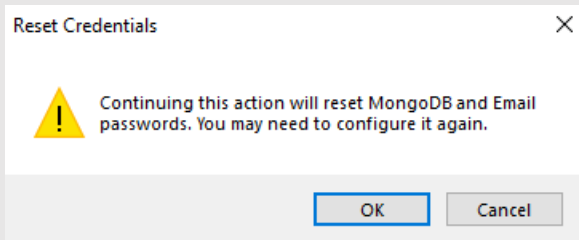
User Name: admin

Password:

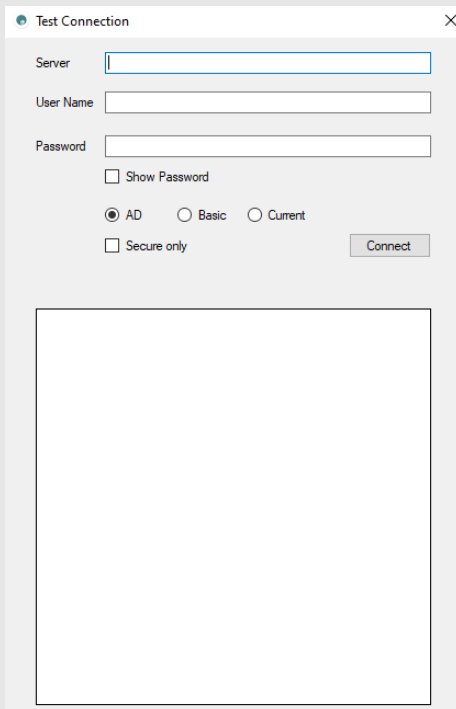
☐ Show Password

Save

- 13. Reset Credentials:** Clears the MongoDB password saved in the Query Engine and the email password configured for Query Engine (Reporting).



**14. Test Connection:** Tests the connection between the Query Engine and the XProtect Management Server.



**15. Logs:** Displays event logs for the Query Engine, based on the configuration.

**Note:** If you cannot access the logs from the Query Engine Configuration Tool, do exit the tool and rerun as administrator

**16. Exit:** Exits the Query Engine Configuration Tool. To reopen the tool, navigate to the installation directory and run *QEConfigurator.exe* (default path: *C:\Program Files\O-Insights Query Engine\QEConfigurator*).

After configuring, reopen the XProtect Smart Client to ensure that the Reports Tab within the O-Insights Plugin is visible.

## O-Insights Plugin Configuration

The O-Insights Plugin Configuration tool allows you to view and modify settings for installed O-Insights plugins. To access this tool:

1. Navigate to the application at *C:\Program Files\Milestone\MIPPlugins\O-Insights for VMS\O-Insights Plugin Configuration*.
2. Enter the required key value into the text field and click "Update" to apply the changes.

**Note:** Make sure to run the application as an administrator for full access and functionality.

O-Insights Plugin Configuration					
Sl.No	Plugin Name	Description	Key	Value	
1	O-Insights Plugin	Smart client plugin for Dashboard.	QueryEngineProtocol	https	Update
2	O-Insights Plugin	Smart client plugin for Dashboard.	QueryEngineServer	DESKTOP-MID9F07	Update
3	O-Insights Plugin	Smart client plugin for Dashboard.	QueryEnginePort	9011	Update
4	O-Insights Custom Camera Properties Plugin	Management client plugin for adding custom properties to camera.	QueryEngineProtocol	http	Update
5	O-Insights Custom Camera Properties Plugin	Management client plugin for adding custom properties to camera.	QueryEngineServer	DESKTOP-MID9F07	Update
6	O-Insights Custom Camera Properties Plugin	Management client plugin for adding custom properties to camera.	QueryEnginePort	9011	Update

For example, if you need to update the protocol of an O-Insights module from HTTP to HTTPS, you can make the necessary adjustments using this tool. After making changes, restart the XProtect Smart Client/Management client to ensure that updates are applied.



# Steps to create Self Sign Certificate

## 1. Create the Self-Signed Certificate

Open PowerShell in Administrator mode and run the following command:

```
$selfSignedRootCA = New-SelfSignedCertificate -Subject CertForOlnisghts -  
DnsName "MACHINE-DNS-NAME" -notafter (Get-Date).AddMonths(36) -  
CertStoreLocation Cert:\LocalMachine\My\ -KeyExportPolicy Exportable -  
KeyUsage CertSign,CRLSign,DigitalSignature -KeySpec KeyExchange -  
KeyLength 2048 -KeyUsageProperty All -KeyAlgorithm 'RSA' -HashAlgorithm  
'SHA256' -Provider 'Microsoft Enhanced RSA and AES Cryptographic  
Provider'
```

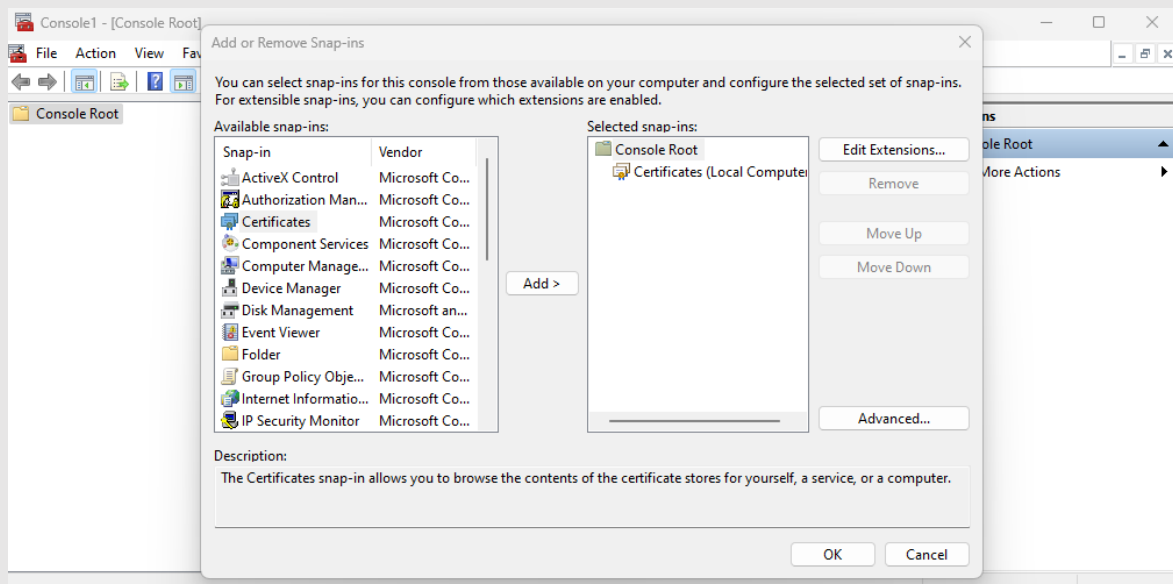
Replace "**MACHINE-DNS-NAME**" with the machine DNS name in above step.

## 2. Access the Certificates Management Console

Open the Run dialog by pressing Win + R, then type mmc.exe and press Enter.

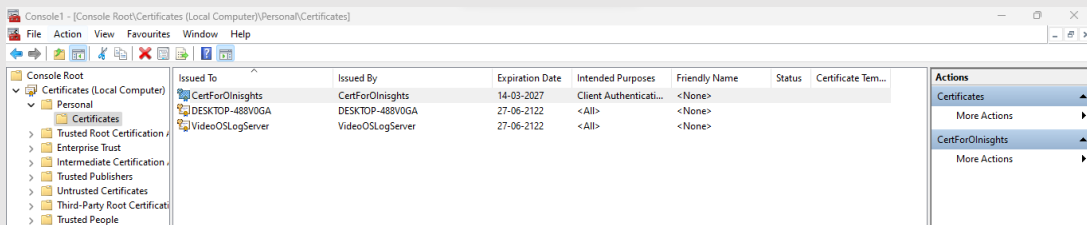
## 3. Add the Certificates Snap-in

In the MMC window, go to **File -> Add or Remove Snap-ins -> Certificates -> Add -> Computer account -> Local computer**. Click **Finish**, then **OK**.



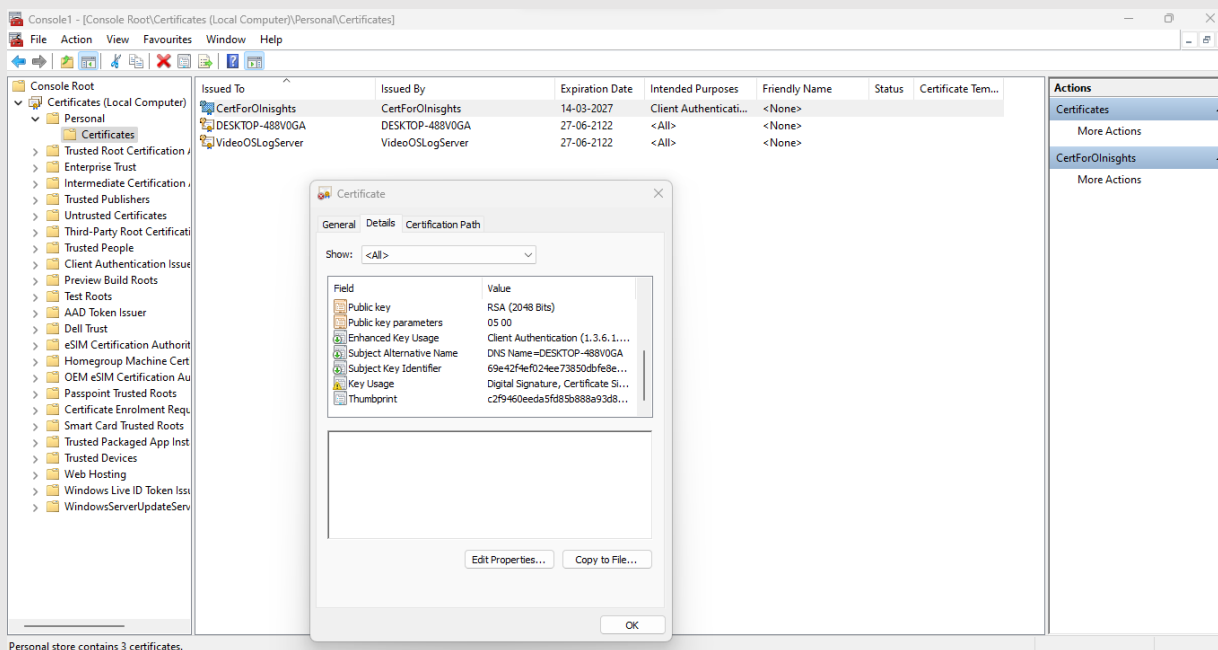
## 4. Move the Certificate to Trusted Root Certification Authorities

- Expand the **Personal** folder under **Certificates (Local Computer)**.
- Locate the CertForOlnisghts certificate you just created.
- Right-click on the certificate, select **Copy**, and then paste it into the **Trusted Root Certification Authorities - Certificates** folder.



## 5. Note the Certificate Thumbprint

- Double-click the CertForOlnisghts certificate in the **Trusted Root Certification Authorities** folder.
- Go to the **Details** tab and find the **Thumbprint**. This thumbprint will be used for the installation process.



## MongoDB Password Update Procedure

1. Navigate to the MongoDB installation directory and open `mongod.cfg` in Notepad++ (typically located in `C:\Program Files\MongoDB\Server\X.X\bin`).

2. Disable security by adding a `#` before the following lines:

```
#security:
```

```
#authorization: "enabled"
```

3. Restart the MongoDB service.

4. Open `mongosh.exe` in admin mode from the MongoDB installation directory.

5. Connect to the MongoDB server by either pressing Enter for default credentials or providing the connection string.

6. Update the password by running the following commands:

- Use the admin database:

```
use admin
```

- Update the password for the admin user:

```
db.updateUser("<username>", { pwd: "<new password>", roles: [{ role: "root", db: "admin" }] })
```

Replace `<username>` with the actual username and `<new password>` with the new password.

- Switch to the MLSTQueryDB database:

```
use MLSTQueryDB
```

- Update the password for the user in MLSTQueryDB:

```
db.updateUser("<username>", { pwd: "<new password>", roles: [{ role: "dbAdmin", db: "MLSTQueryDB" }, { role: "dbOwner", db: "MLSTQueryDB" }] })
```

Replace `<username>` with the actual username and `<new password>` with the new password.

7. In the Query Engine Configuration tool, select “Reset Credentials” to delete the existing credentials from the Query Engine.

8. Update the MongoDB credentials in the Query Engine Configuration tool with the new password.

9. Re-enable security in `mongod.cfg` by removing the `#` added in step 2. Restart the MongoDB service.

10. Restart the OInsightsMLSTQueryEngine service.

11. Verify the connection status by checking the system tray status. The Query Engine should now connect using the new password.

## Upgrading from Versions Before v5.0

Upgrading to version 5.0 is not compatible with direct upgrades from versions earlier than 4.7. If you are upgrading from versions 4.7 or 4.8 to 5.0, follow these steps when updating the Query Engine (QE):

1. Stop the Query Engine service.
2. Exit the Query Engine Configuration Tool.
3. Proceed with the update after completing these actions.

## Pre-Upgrade Recommendations

### *Taking Backup*

Before starting the installation, ensure you back up the following folders and files:

- C:\ProgramData\CTS
- C:\Program Files\Milestone\MIPPlugins\O-Insights for VMS\License\License.lic
- C:\Program Files\O-Insights Query Engine\Config
- C:\Program Files\O-Insights Query Engine\Templates
- Exported Workspaces

### *Taking MongoDB Dump:*

While the installer can handle MongoDB upgrade (backup and restore) from versions 4.7 or 4.8 to 5.0, it is recommended to manually back up MongoDB as follows:

1. Open the mongod.cfg file in a text editor like Notepad.
2. Temporarily disable security by commenting out the security lines:  
*# security*  
*# authorization: "enabled"*

If security is not disabled, ensure you provide the password:

```
mongodump --uri="mongodb://myUser:myPassword@localhost:27017"
```

3. Restart the MongoDB service to apply changes. Re-enable security by removing the # symbols from the security section.
4. Navigate to the old installation directory: C:\Program Files\MongoDB\Server\6.0\bin\  
*mongodump.exe*
5. Double-click *mongodump.exe* to generate a backup. This will create a Dump folder in the MongoDB installation directory.
6. This backup can be restored if needed after installing O-Insights 5.0, which involves updating MongoDB from version 6.0 to 7.0.