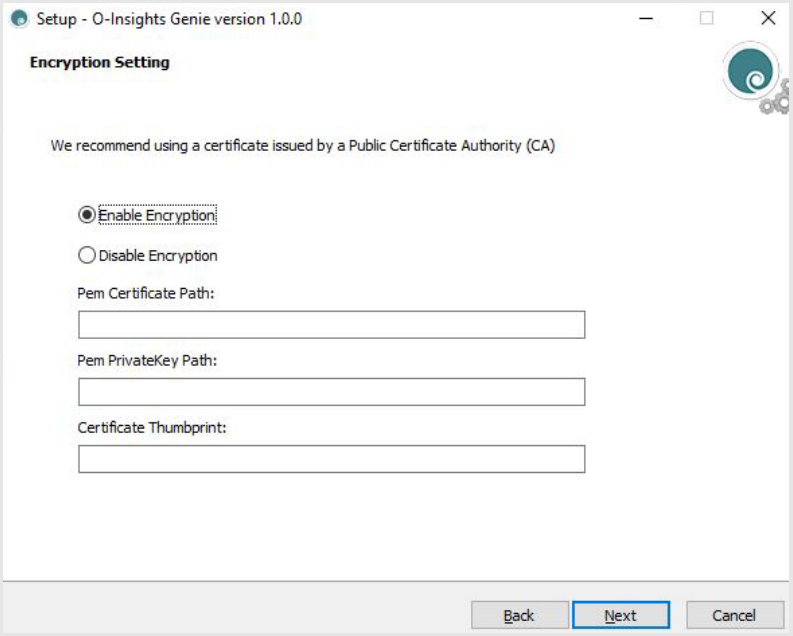
O-Insights Genie v1.0 – Installation Instructions

Pre-Requisites

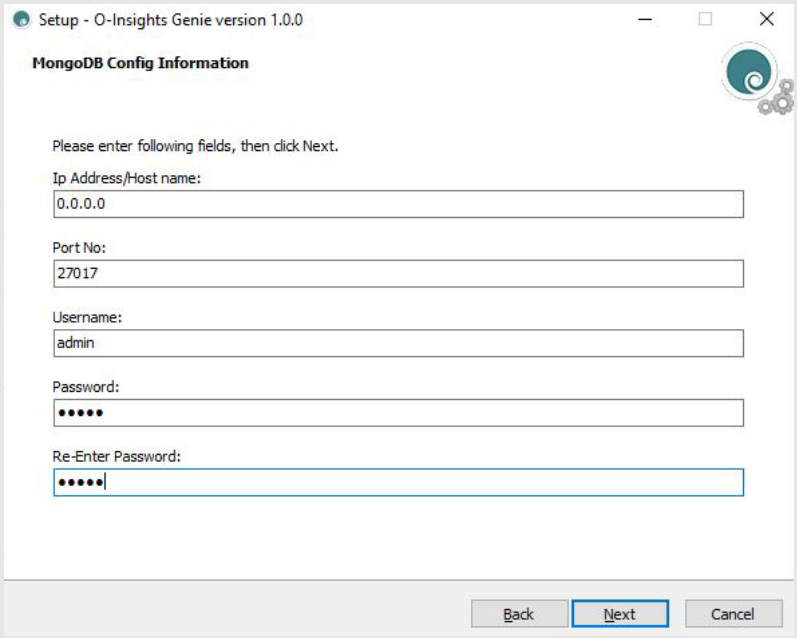
- O-Insights Query Engine 4.8 or later.
- XProtect Smart Client
- **Mongo DB** 6.0 and above

Setup (Genie Service)

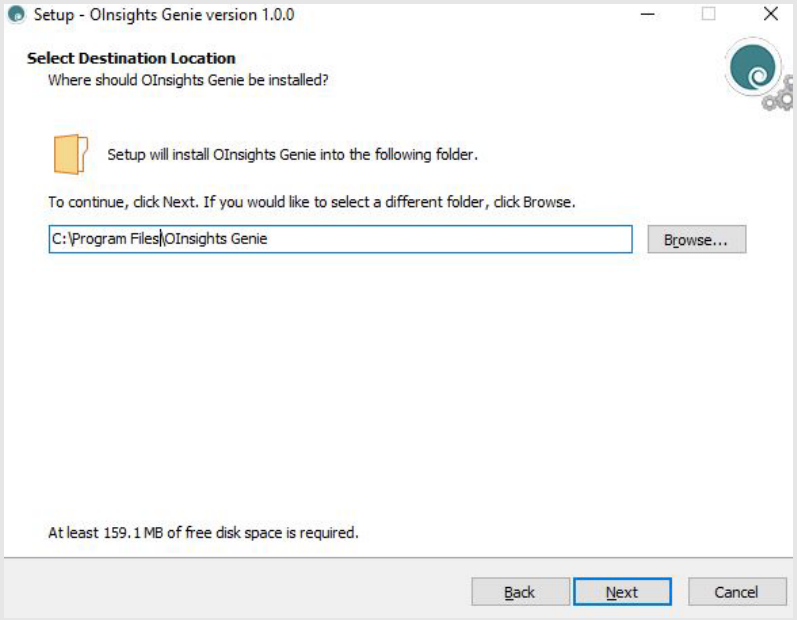
- Open the setup EXE file provided.
- Read the license agreement and click on *I accept the agreement and* click on *Next* to proceed.
- To use SSL Encryption with Genie, choose *Enable Encryption* and provide the paths for the PEM Certificate, PEM Private Key and Certificate in the respective fields. The process of generating the following files is detailed in the below section.



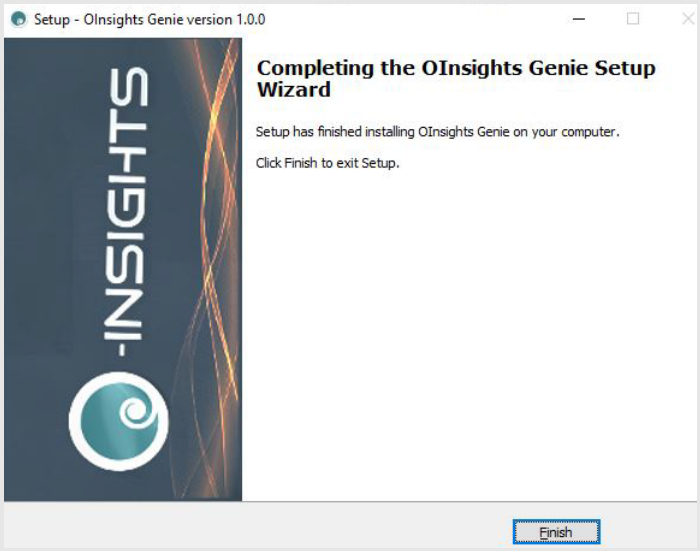
- *IP Address/Host name:* IP address/host name on which the database is to be installed.
- *Port No:* Open port number for database
- *Username* and *Password:* Username and password for the database. The username/password must be remembered in the unlikely event of needing to recover the database.



- Select the destination location and Click *Next*.

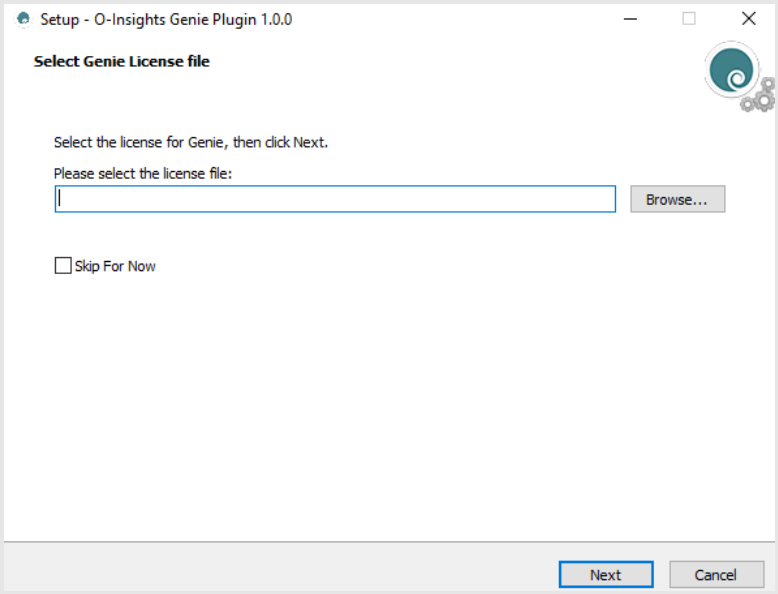


- Click on *Install*, then click on *Finish* to complete the installation and exit setup.

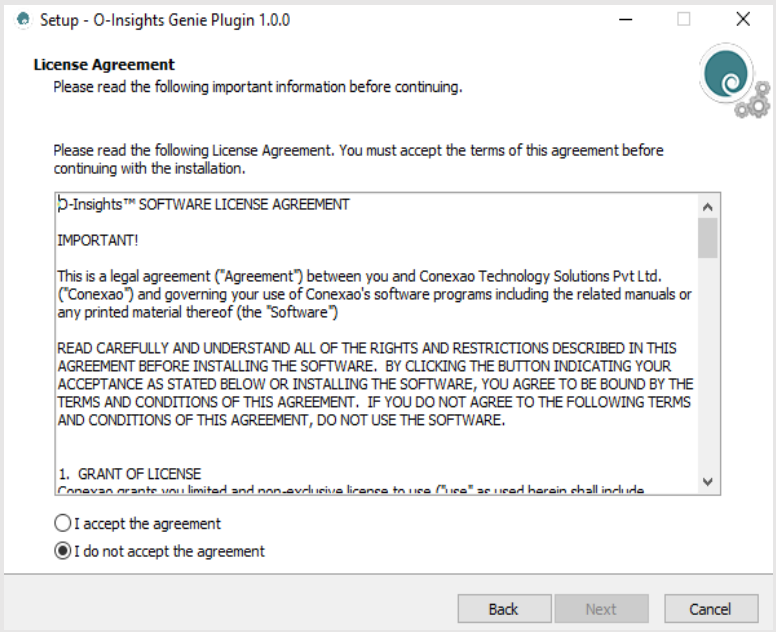


Setup (Genie Plugin)

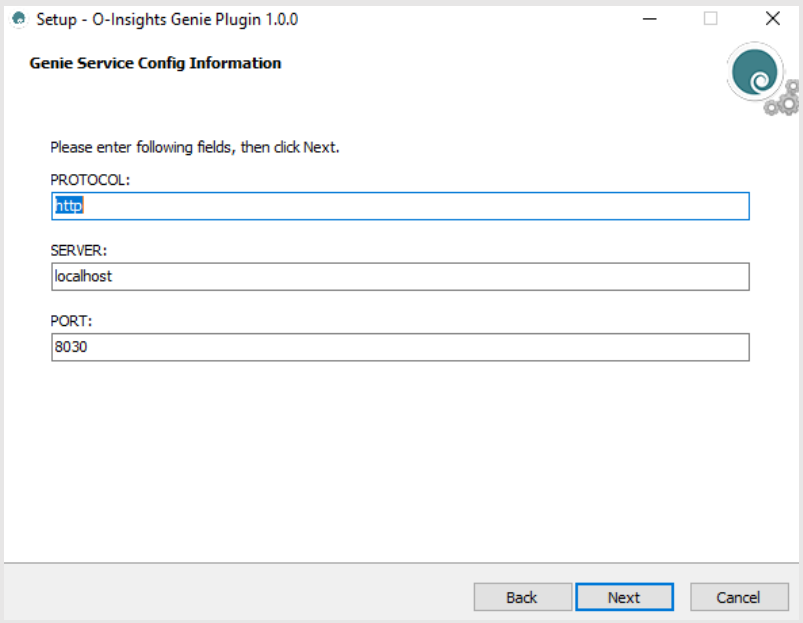
- Open the setup and either locate the license file by browsing the designated path or simply skip this step if you've already placed it in the License folder and click next.



- After reading the License Agreement, click accept and click next.



- Set Genie Service Config Information and click next.



- Post installation click *Finish* to exit the setup.
- You may start XProtect Smart Client from the installed directory or the desktop shortcut.

Note: The plugin should be installed in the in the MIP Plugin Directory. The default installation directory is *C:\Program Files\Milestone\MIPPlugins*.

Enable SSL Encryption

For SSL to be used with Genie (over HTTPS), follow the steps detailed below. We recommend having a certificate from a trusted authority. Alternatively, you may follow the steps in the below section to create self-signed certificates. The below steps require OpenSSL to be installed on your PC, in case a self-signed certificate is to be generated.

Creating a Self-Signed Certificate and Exporting Certificate and Key as PEM Files

- **Run the following command in Windows PowerShell (Admin mode), which can be accessed by typing** *PowerShell* **in the Start menu. You can replace "localhost" with your machine name for production:**

  $selfSignedRootCA = New-SelfSignedCertificate -DnsName "localhost" -notafter (Get-Date).AddMonths(6) -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'

- **Create .cer and .pfx files using the following command. Change the path and password as required.**

  $certBytes = $selfSignedRootCA.Export("Cert")

  $certPath = "C:\cert.cer"

  $certBytes | Set-Content -Path $certPath -Encoding Byte

  $privateKeyPath = "C:\private_key.pfx"

  $selfSignedRootCA | Export-PfxCertificate -FilePath $privateKeyPath -Password (ConvertTo-SecureString -String "YourPasswordHere" -Force -AsPlainText)

- **Go to the directory where OpenSSL is installed and navigate to the** *bin* **directory. From the directory, right click and choose** *Open from Terminal.* **Use the following commands in Terminal (Command Prompt) to convert these two files into PEM files:**

  openssl x509 -inform DER -in cert.cer -out cert.pem

  openssl pkcs12 -in private_key.pfx -out key.pem -nocerts -nodes

Adding Certificates to Certificate Store

- Follow all the steps outlined in the procedure and navigate to the certificate store.
- Go to the intermediate store, copy the newly created certificate, and paste it into the root trusted store.
- Use the paths of cert.pem and key.pem in the installer to use *SSL* with Genie.