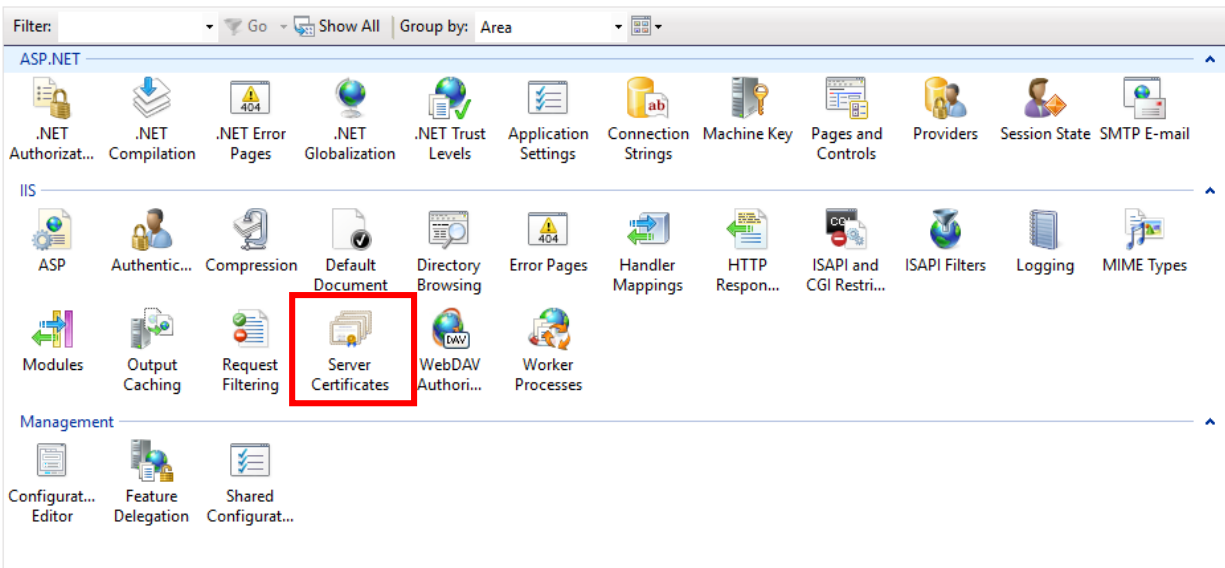


Request a Qlik Sense Certificate (CSR)

Requirements:

You must have a certificate with a **private key**.


Open IIS in any computer, go to “Server Certificates”:



In the right pane click in “Create Certificate Request”

Fill all the information to generate the CSR

Request Certificate ? X

 **Distinguished Name Properties**


Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	<input type="text" value="sense.example.com"/>
Organization:	<input type="text" value="Example Company"/>
Organizational unit:	<input type="text" value="IT"/>
City/locality:	<input type="text" value="Fort Collins"/>
State/province:	<input type="text" value="Colorado"/>
Country/region:	<input type="text" value="US"/>

Previous Next Finish Cancel

Change the bit length to 2048

Request Certificate ? X

 **Cryptographic Service Provider Properties**

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.


Cryptographic service provider:
Microsoft RSA SChannel Cryptographic Provider

Bit length:
2048

Previous Next Finish Cancel

Select the path to store the CSR

Request Certificate ? X

 **File Name**

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:
C:\Users\Example\Desktop\CSR.txt

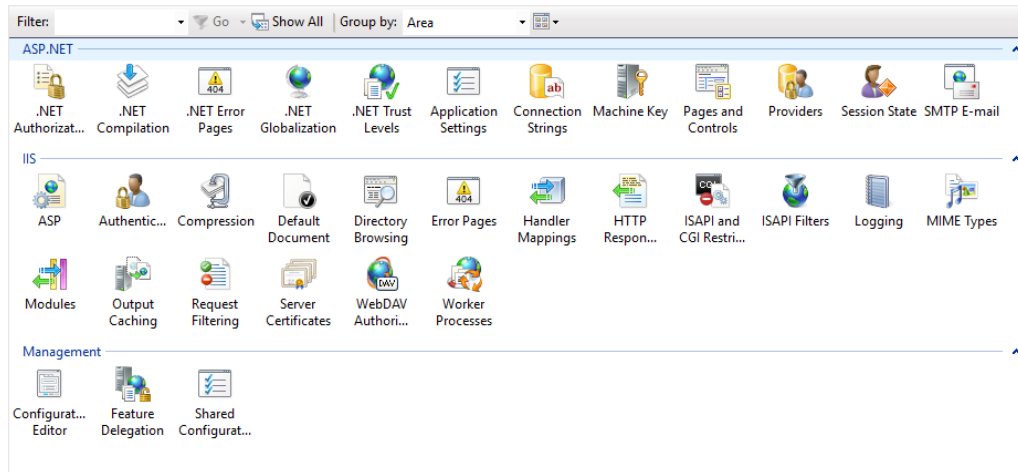
Previous Next Finish Cancel

Send the CSR to your CA.

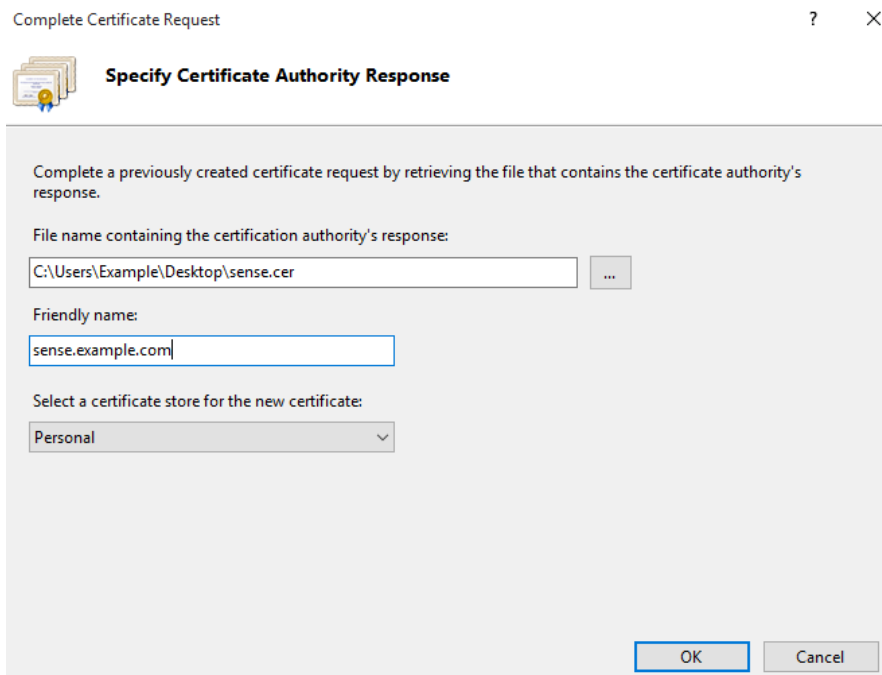
Import the private key

Go back to the same server that you generated the CSR and sign with the private key.

Open IIS, go to “Server Certificates”:



In the right pane click in “Complete Certificate Request”, select the .cer file that you received from your CA

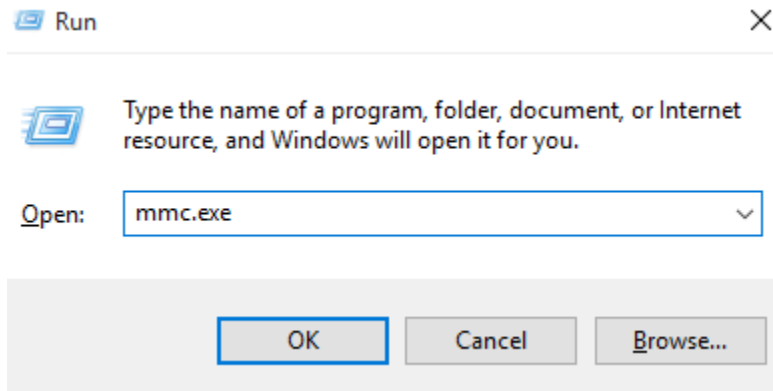


You'll have a signed certificate in that computer.

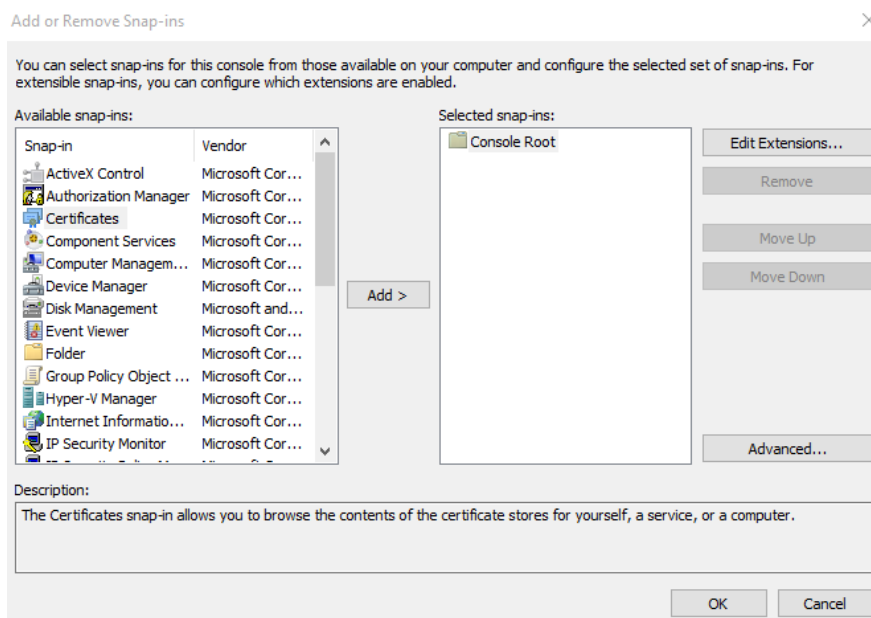
Export certificate with private key

Export certificate from the requestor server

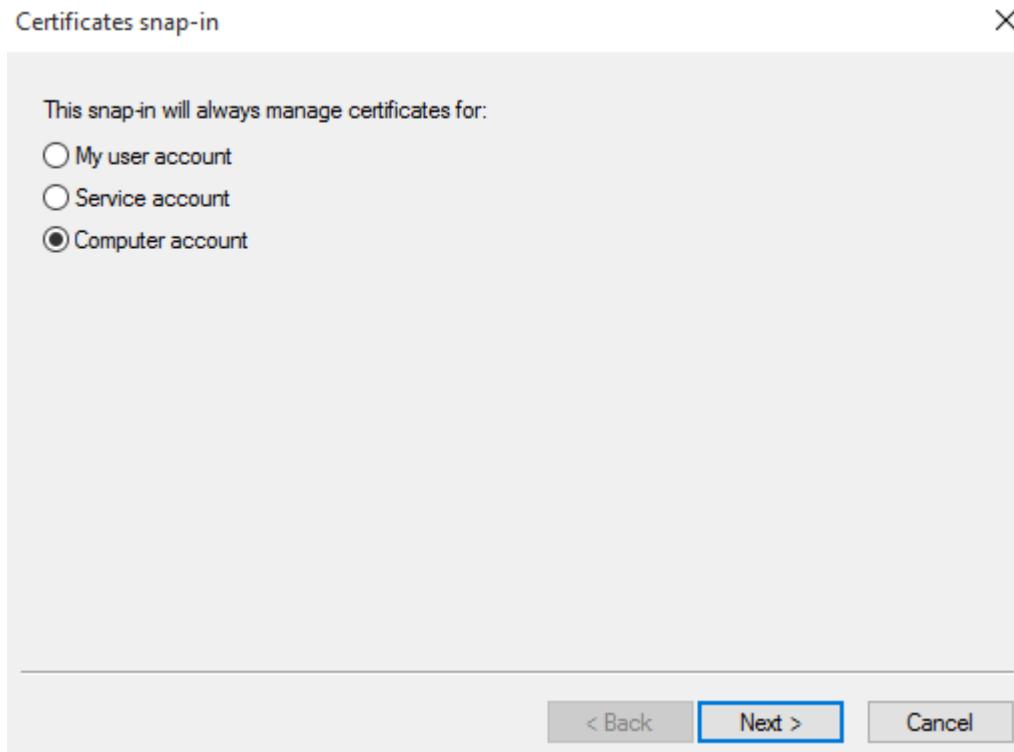
Open MMC.exe



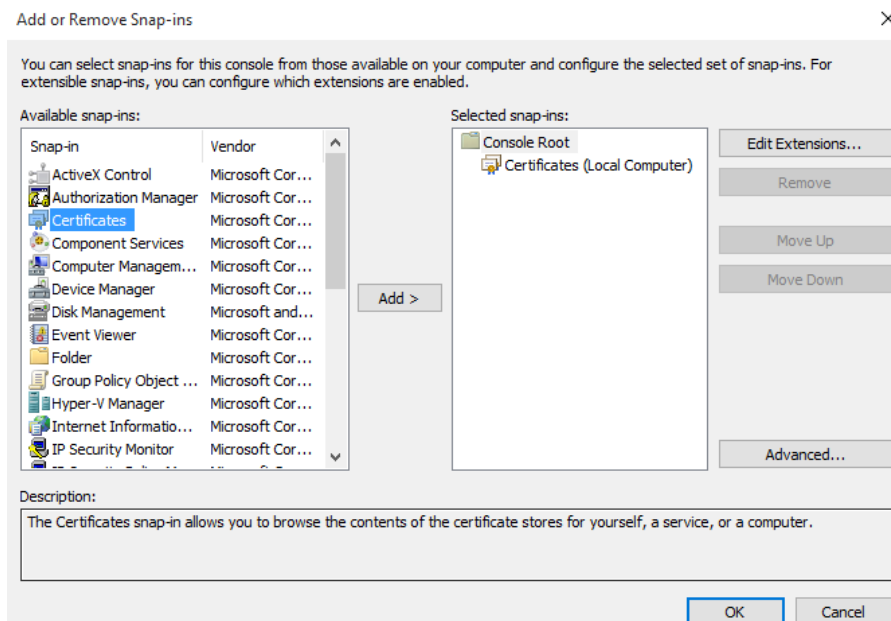
"File", "Add/Remove Snap-in...", "Certificates"



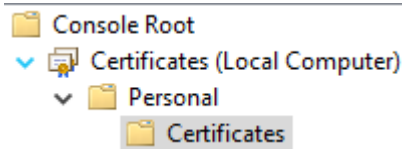
Select "Computer account", "Next", "Finish"



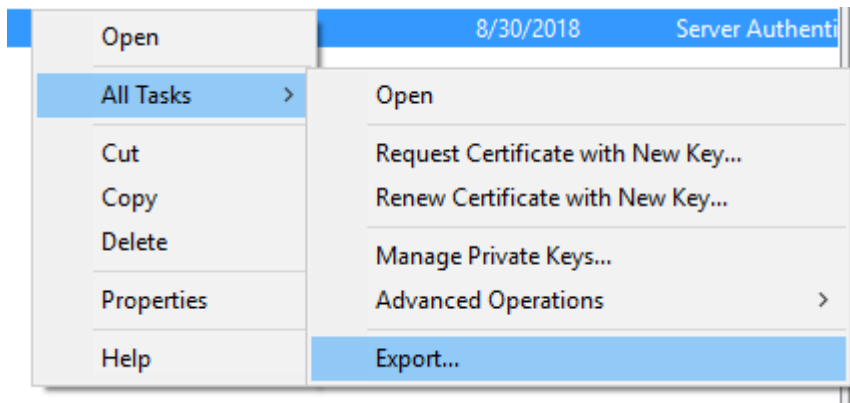
Press "OK"



Go to “Personal”, “Certificates”



Click with the right button in the certificate and “Export”



Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

- Yes, export the private key
- No, do not export the private key

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 - Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)
 - Include all certificates in the certification path if possible
 - Delete the private key if the export is successful
 - Export all extended properties
 - Enable certificate privacy
- Microsoft Serialized Certificate Store (.SST)

Create a password.

Security

To maintain security, you must protect the private key to a security principal or by using a password.

Group or user names (recommended)

Add

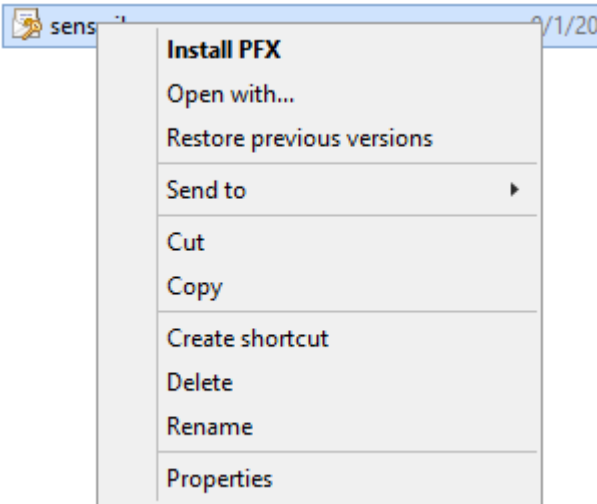
Remove

Password:

Confirm password:

Import Certificate

Copy the certificate (.pfx) to Sense Server, right click on it and click in "Install PFX"



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

Current User

Local Machine

To continue, click Next.

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

 Display Password

Import options:

- Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- Include all extended properties.

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

- Automatically select the certificate store based on the type of certificate
- Place all certificates in the following store

Certificate store:

Personal

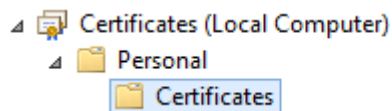
Browse...

Repeat the same steps again for "Current User".

Open MMC.exe

"File", "Add/Remove Snap-in...", "Certificates"
"Computer Account"

Browse to the certificate:



Double click in the certificate and go to the "Details" tab, copy the thumbprint and paste into Qlik Sense Proxy configuration.

(<http://help.qlik.com/en-US/sense/3.0/Subsystems/ManagementConsole/Content/change-proxy-certificate.htm>)