

SHA256 Certificate Installation

How to migrate the server certificate for Secret Server to the new PKI Infra (SHA256)

Part I : Creating the CSR

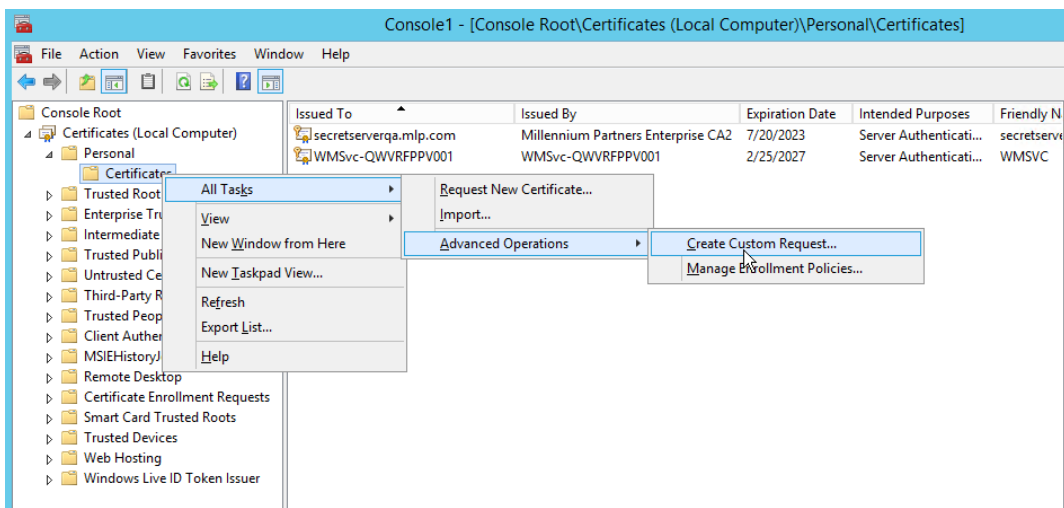
Log on to machine with administrative rights

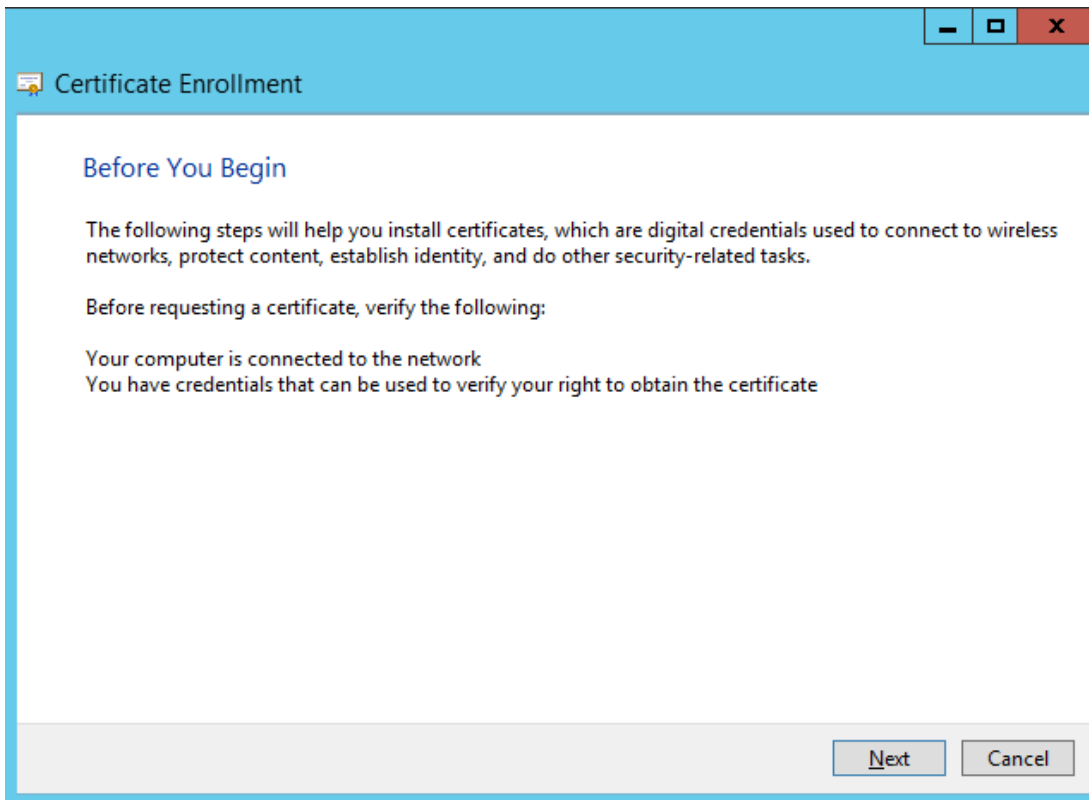
Run mmc

Add the Certificate (Local Computer) Snap-in

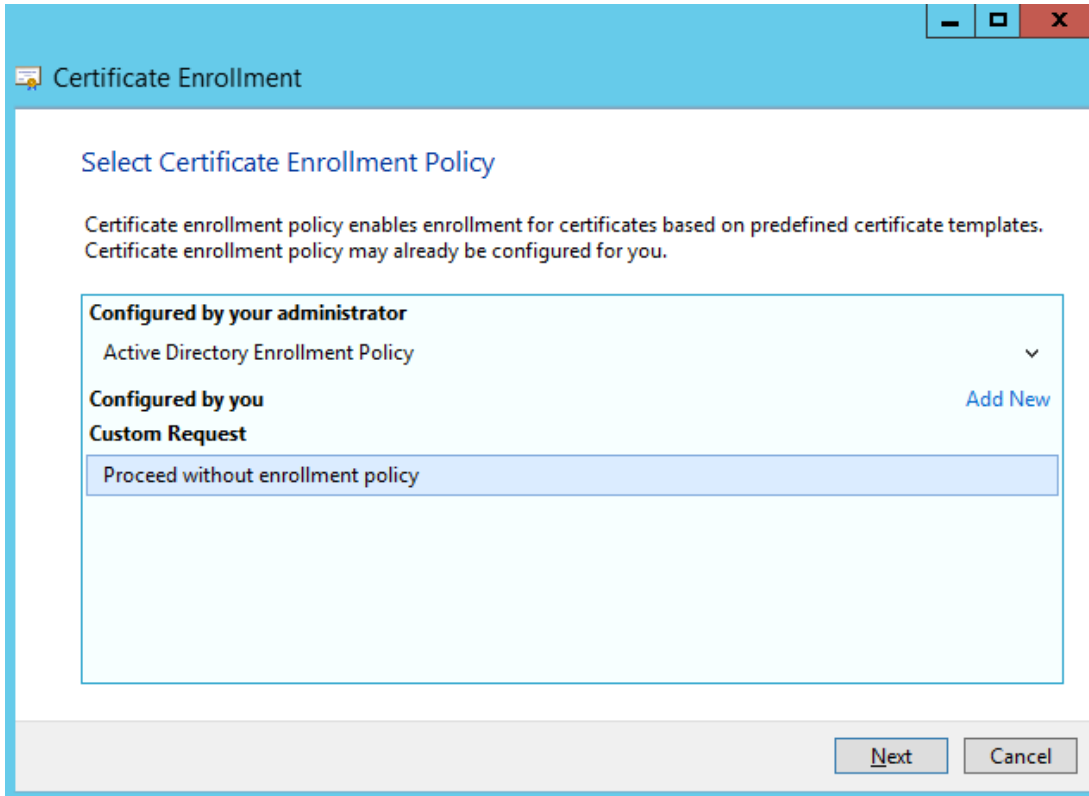
Expand Personal > Certificates Folder

Right Click > All Tasks > Advanced Operations > Create Custom Request

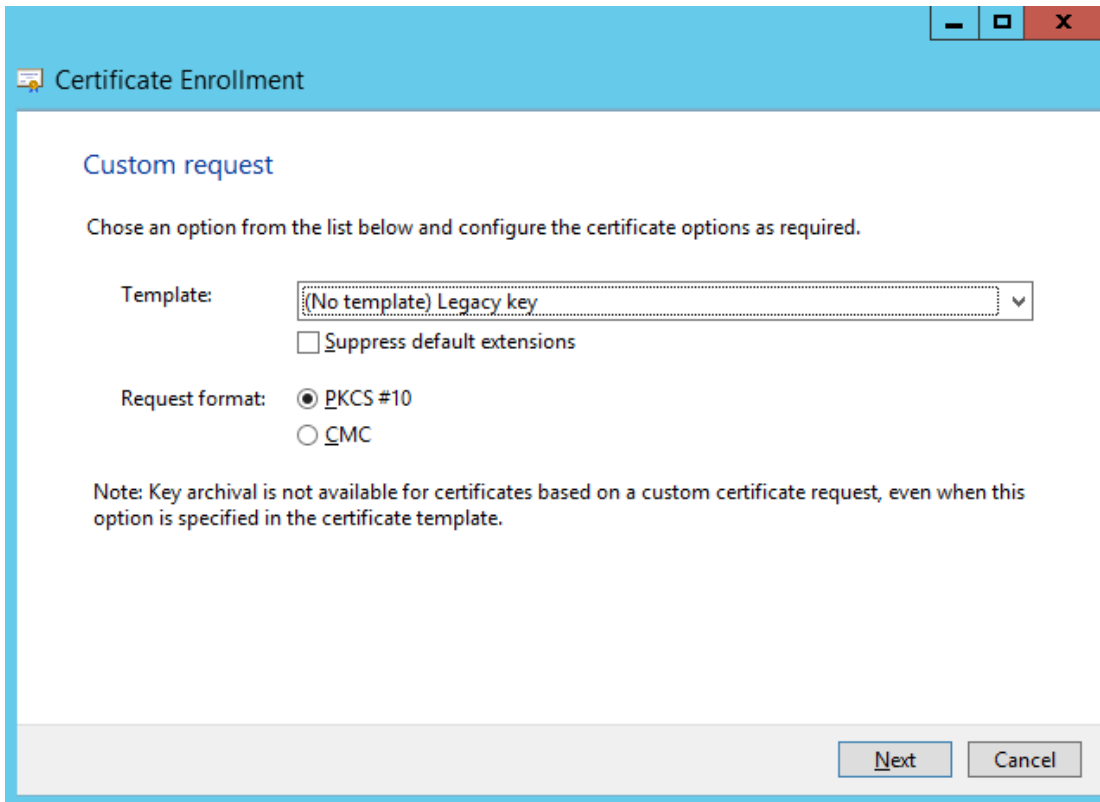




Click **Next**



Select **'Proceed without enrollment policy'**.



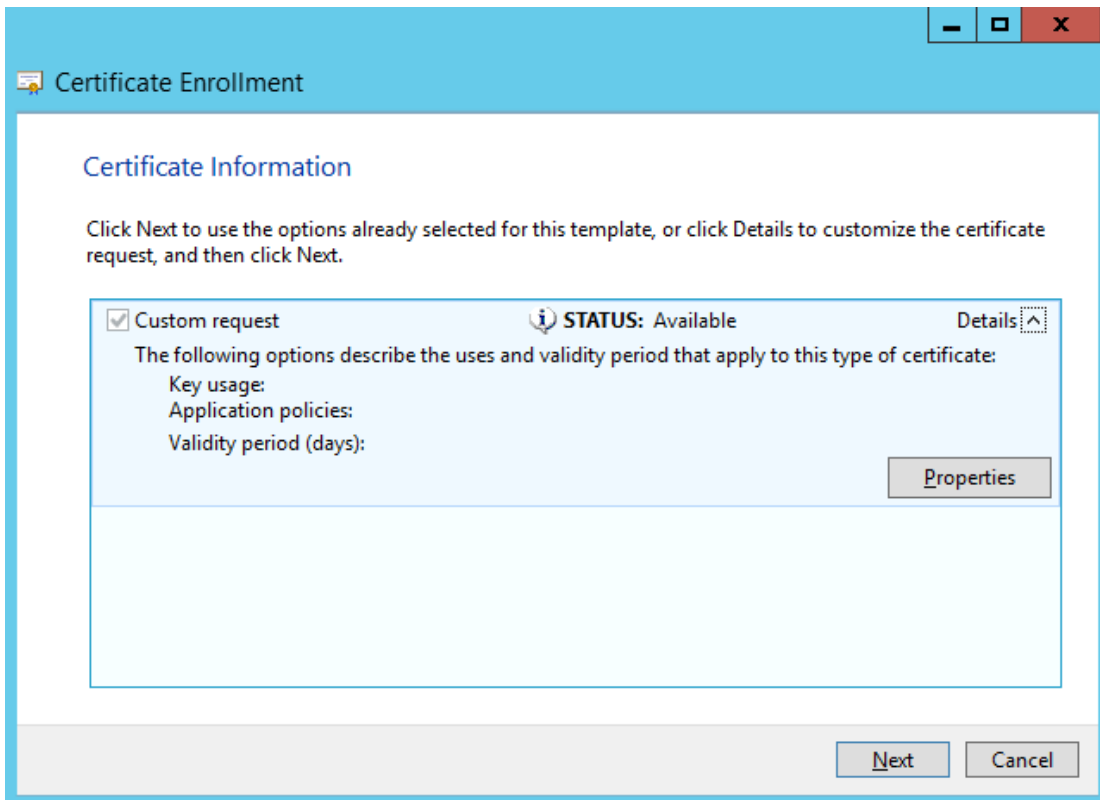
The image shows a Windows-style dialog box titled "Certificate Enrollment". It has a blue header bar with standard window controls (minimize, maximize, close) on the right. The main content area is white and contains the following elements:

- Custom request**: A section header in blue text.
- Chose an option from the list below and configure the certificate options as required.**: A line of instructional text.
- Template:**: A label followed by a dropdown menu showing "(No template) Legacy key".
- ☐ **Suppress default extensions**: A checkbox with a label.
- Request format:**: A label followed by two radio button options:
● **PKCS #10** (selected)
○ **CMC**
- Note:** Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.
- Next** and **Cancel**: Two buttons at the bottom right.

Change the Template to '**(No template) Legacy key**'

Click **Next**

Expand the Details under the Custom request and Click **Properties**.



The Certificate Enrollment dialog box has a blue title bar with standard window controls. The main area is white with a blue header 'Certificate Enrollment' and a sub-header 'Certificate Information'. Below this is a blue box containing a 'Custom request' checkbox (checked), a status indicator 'STATUS: Available', and a 'Details' link. The box also lists 'Key usage:', 'Application policies:', and 'Validity period (days):' with a 'Properties' button. At the bottom are 'Next' and 'Cancel' buttons.

Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

☒ Custom request **STATUS: Available** Details ^

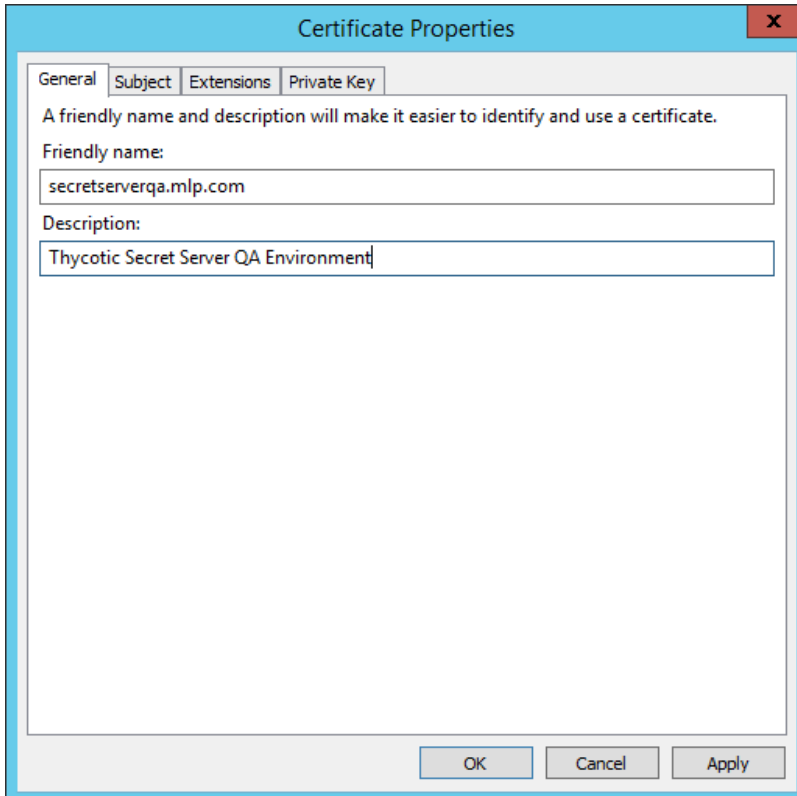
The following options describe the uses and validity period that apply to this type of certificate:

Key usage:
Application policies:
Validity period (days):

Properties

Next Cancel

Fill in the Friendly Name and Description fields



The Certificate Properties dialog box has a blue title bar. It features a tabbed interface with 'General', 'Subject', 'Extensions', and 'Private Key' tabs. The 'General' tab is active, showing a message about friendly names and descriptions. Below this are text boxes for 'Friendly name:' (containing 'secretserverqa.mlp.com') and 'Description:' (containing 'Thycotic Secret Server QA Environment'). At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Certificate Properties

General Subject Extensions Private Key

A friendly name and description will make it easier to identify and use a certificate.

Friendly name:
secretserverqa.mlp.com

Description:
Thycotic Secret Server QA Environment

OK Cancel Apply

Complete the required Subject and SAN information according to your application's requirements.

Certificate Properties

General Subject Extensions Private Key

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate
The user or computer that is receiving the certificate

Subject name:

Type: Country

Value:

Add >

< Remove

CN=secretserverqa.mlp.com
E=itseceng@mlp.com
O=Millennium Partners
OU=Information Security
L=Somerset

Alternative name:

Type: DNS

Value:

Add >

< Remove

DNS
secretserverqa.mlp.com
qwvrfppv001.ad.mlp.com
qwvrfppv001.mlp.com
qwvrfppv001
qwvrfppv002.ad.mlp.com
qwvrfppv002.mlp.com
qwvrfppv002

OK Cancel Apply

Select and Add the 'Server Authentication' option.

Certificate Properties

General Subject Extensions Private Key

The following are the certificate extensions for this certificate type.

Key usage

Extended Key Usage (application policies)

An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

Available options:

Client Authentication

Code Signing

Secure Email

Time Stamping

Microsoft Trust List Signing

Microsoft Time Stamping

IP security end system

IP security tunnel termination

IP security user

Add >

< Remove

Selected options:

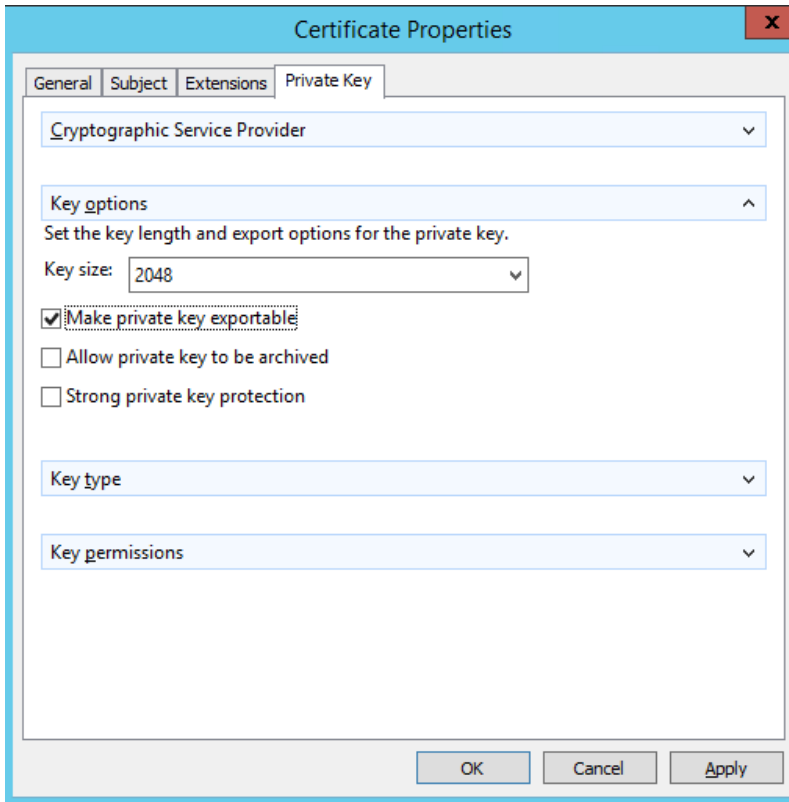
Server Authentication

☐ Make the Extended Key Usage critical

OK Cancel Apply

Choose a key size of **2048** or more

Select the option to 'Make private key exportable'



The image shows the 'Certificate Properties' dialog box with the 'Private Key' tab selected. The 'Cryptographic Service Provider' is set to 'Microsoft Cryptographic Base Provider'. Under 'Key options', the 'Key size' is set to '2048'. The checkbox 'Make private key exportable' is checked. Other options like 'Allow private key to be archived' and 'Strong private key protection' are unchecked. The 'Key type' is set to 'RSA' and 'Key permissions' are set to 'Full control'. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom.

Certificate Properties

General Subject Extensions Private Key

Cryptographic Service Provider

Key options

Set the key length and export options for the private key.

Key size: 2048

☒ Make private key exportable

☐ Allow private key to be archived

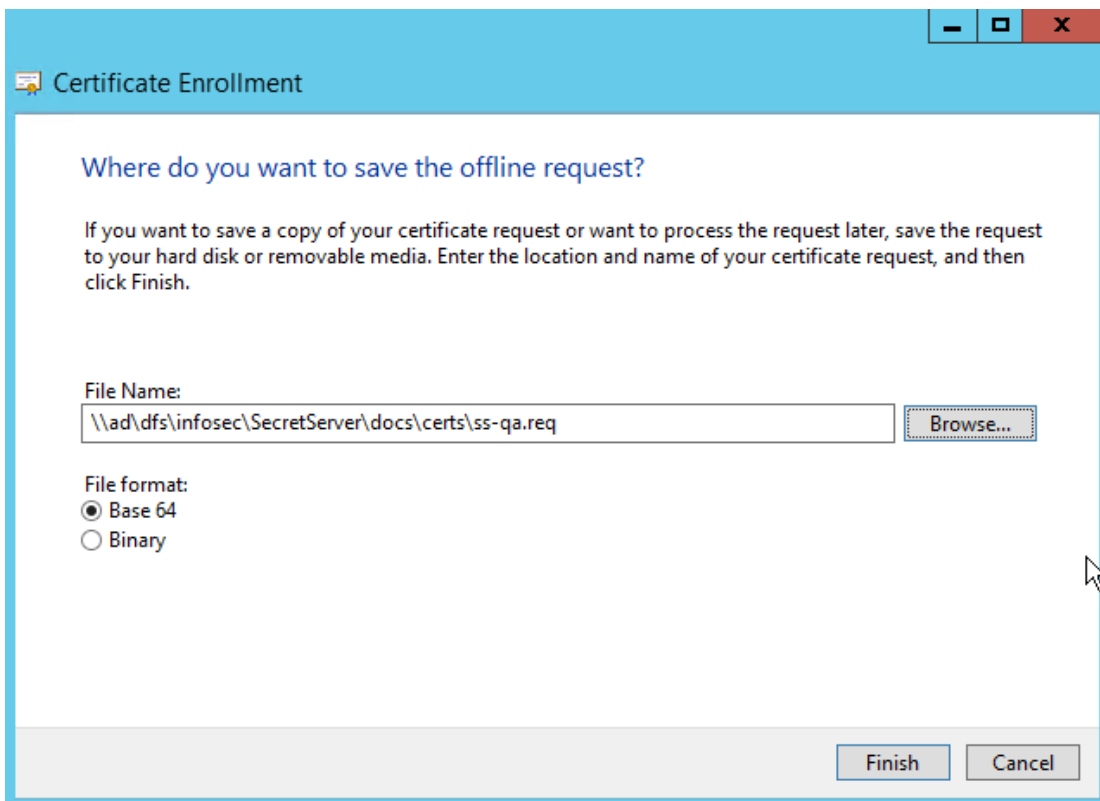
☐ Strong private key protection

Key type

Key permissions

OK Cancel Apply

Save the Certificate Request to a file.



The image shows the 'Certificate Enrollment' dialog box. It asks 'Where do you want to save the offline request?'. It provides instructions: 'If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.' The 'File Name' field contains '\\ad\dfs\infosec\SecretServer\docs\certs\ss-qa.req'. There is a 'Browse...' button next to it. The 'File format' section has 'Base 64' selected with a radio button, and 'Binary' is unselected. The 'Finish' and 'Cancel' buttons are at the bottom.

Certificate Enrollment

Where do you want to save the offline request?

If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.

File Name:

\\ad\dfs\infosec\SecretServer\docs\certs\ss-qa.req Browse...

File format:

☒ Base 64

☐ Binary

Finish Cancel

Send the CSR to request-infosec@mlp.com for signing.

Part II : Importing and Configuring the CSR

Save the certificate (CER) to a location accessible by the server

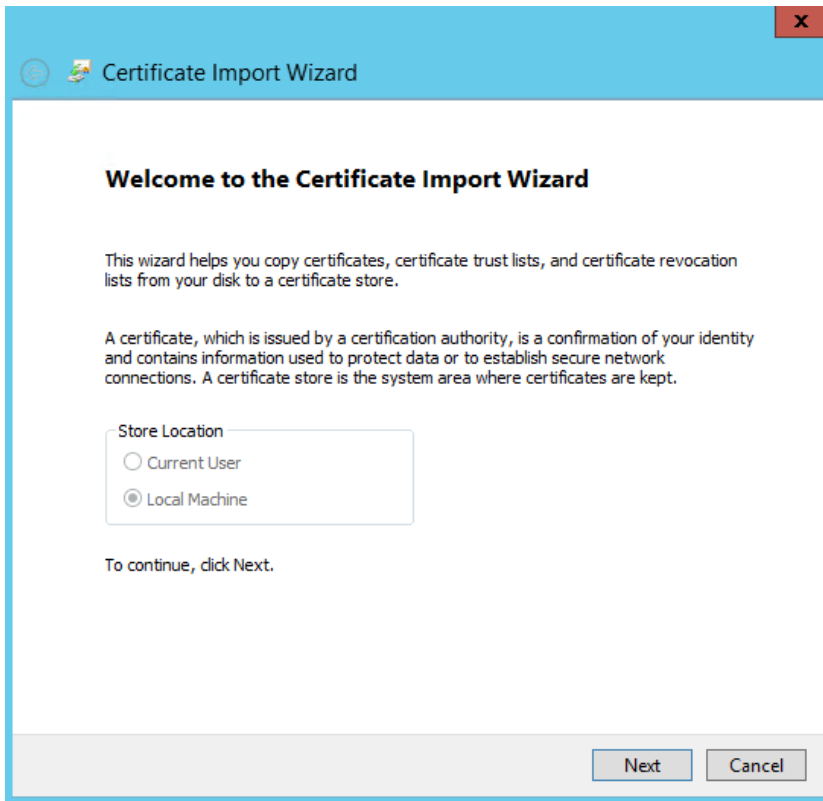
Import the certificate

Open MMC

Load the Certificates (Local Computer) Snap-In

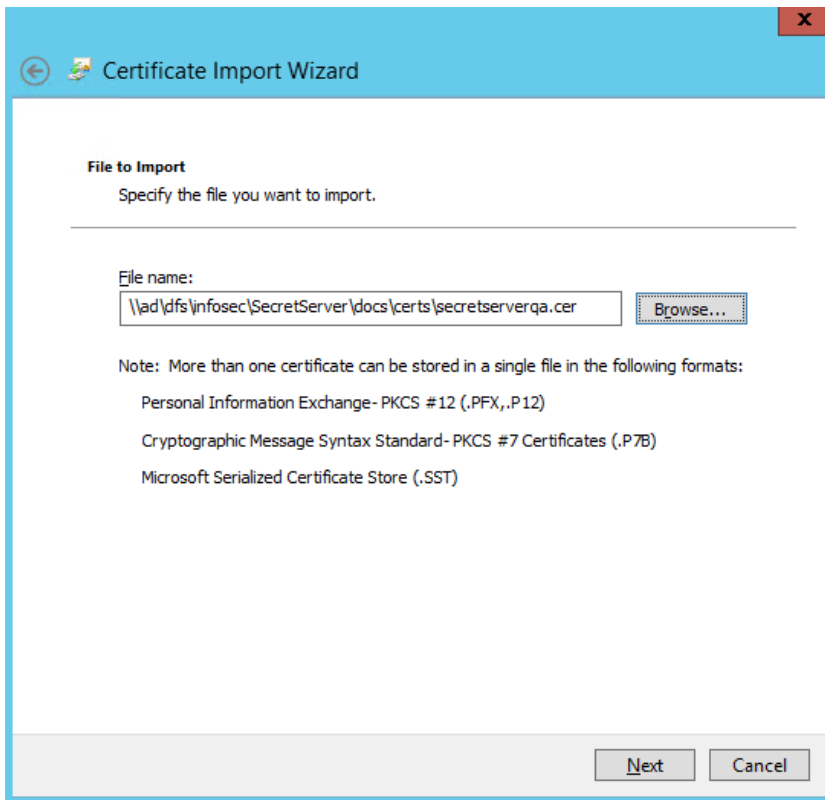
Navigate to the Personal > Certificates Folder

Right-Click and Choose Import



Click **Next**.

Browse to the location of the certificate file



The screenshot shows the 'File to Import' step of the Certificate Import Wizard. The window has a blue title bar with a back arrow, a forward arrow, and a close button. The main area is white with a blue border. The title 'Certificate Import Wizard' is in the top left. Below it, the section 'File to Import' is followed by the instruction 'Specify the file you want to import.' A horizontal line separates this from the input area. The 'File name:' label is above a text box containing the path '\\ad\dfs\infosec\SecretServer\docs\certs\secretserverqa.cer'. To the right of the text box is a 'Browse...' button. Below the text box, a 'Note' states: 'More than one certificate can be stored in a single file in the following formats:'. This is followed by three bullet points: 'Personal Information Exchange- PKCS #12 (.PFX,.P12)', 'Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)', and 'Microsoft Serialized Certificate Store (.SST)'. At the bottom right, there are 'Next' and 'Cancel' buttons.

File to Import
Specify the file you want to import.

File name:
\\ad\dfs\infosec\SecretServer\docs\certs\secretserverqa.cer Browse...

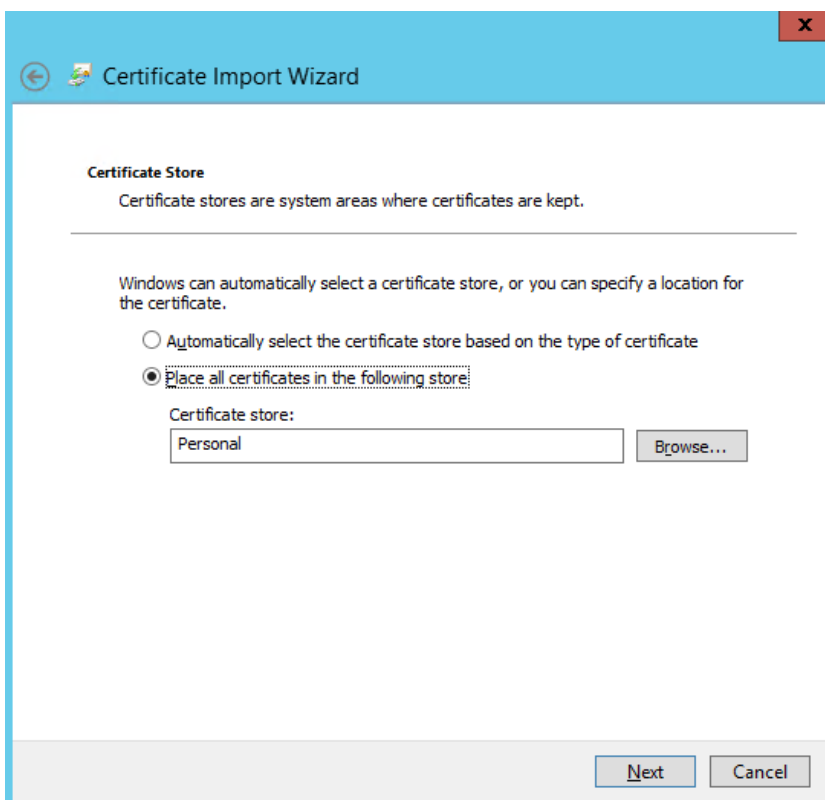
Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

Next Cancel

Click **Next**.

Place all certificates in the following store: Personal



The screenshot shows the 'Certificate Store' step of the Certificate Import Wizard. The window has a blue title bar with a back arrow, a forward arrow, and a close button. The main area is white with a blue border. The title 'Certificate Import Wizard' is in the top left. Below it, the section 'Certificate Store' is followed by the instruction 'Certificate stores are system areas where certificates are kept.' A horizontal line separates this from the input area. The text 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' is followed by two radio button options: 'Automatically select the certificate store based on the type of certificate' and 'Place all certificates in the following store'. The second option is selected. Below the selected option, the 'Certificate store:' label is above a text box containing the word 'Personal'. To the right of the text box is a 'Browse...' button. At the bottom right, there are 'Next' and 'Cancel' buttons.

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.

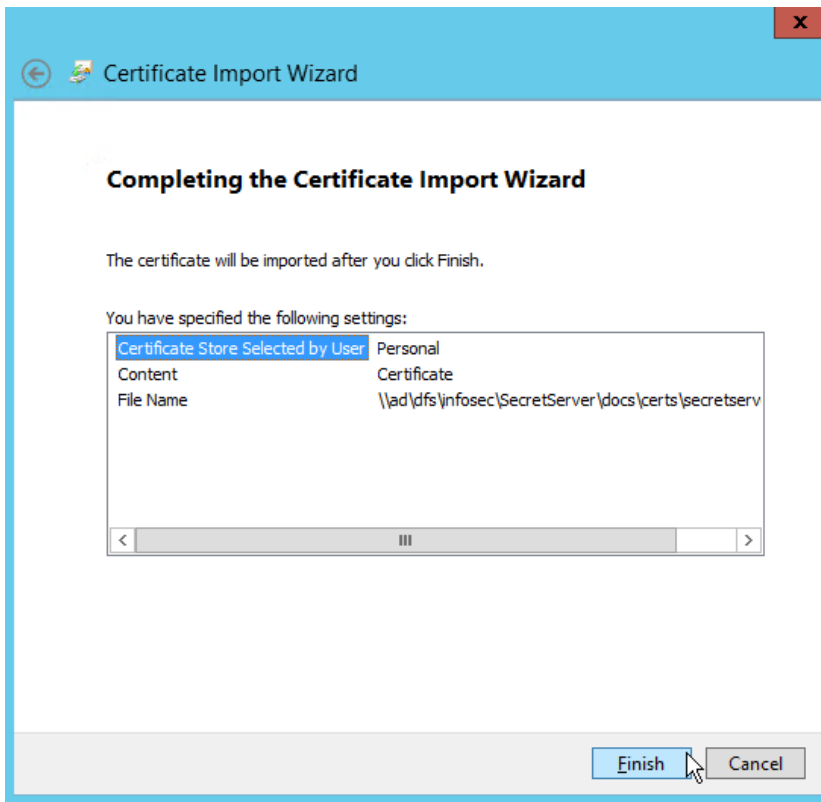
☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

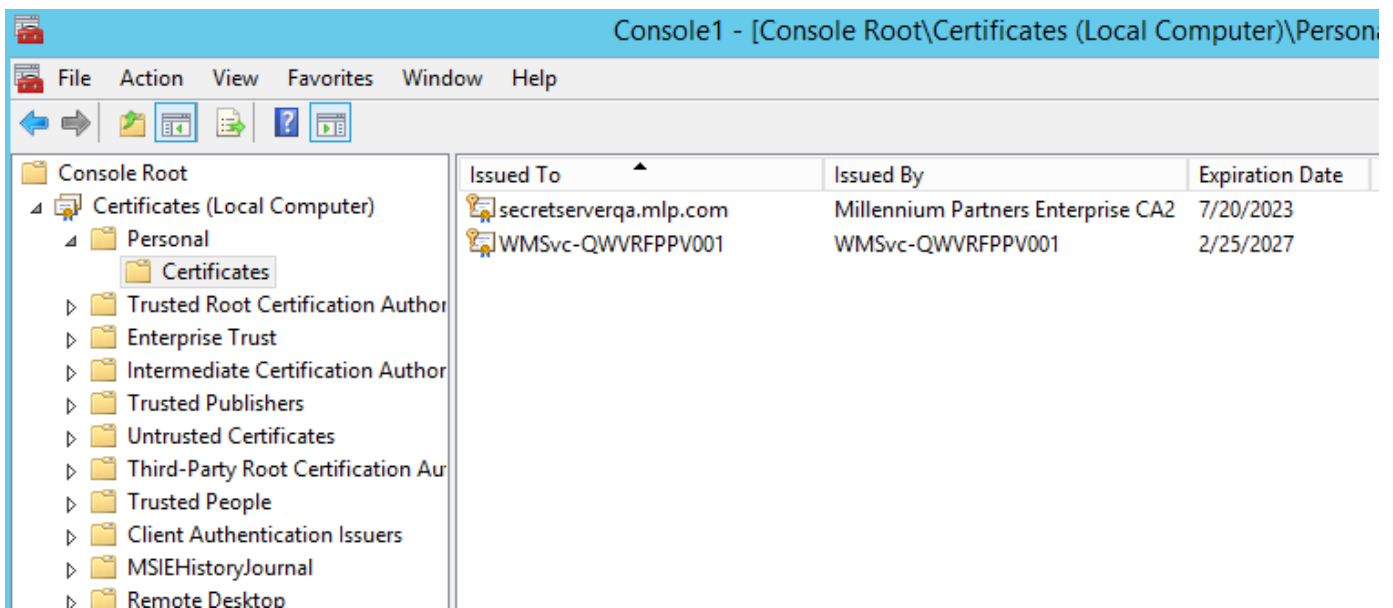
Certificate store:
Personal Browse...

Next Cancel

Click **Next**



Click **Finish**.



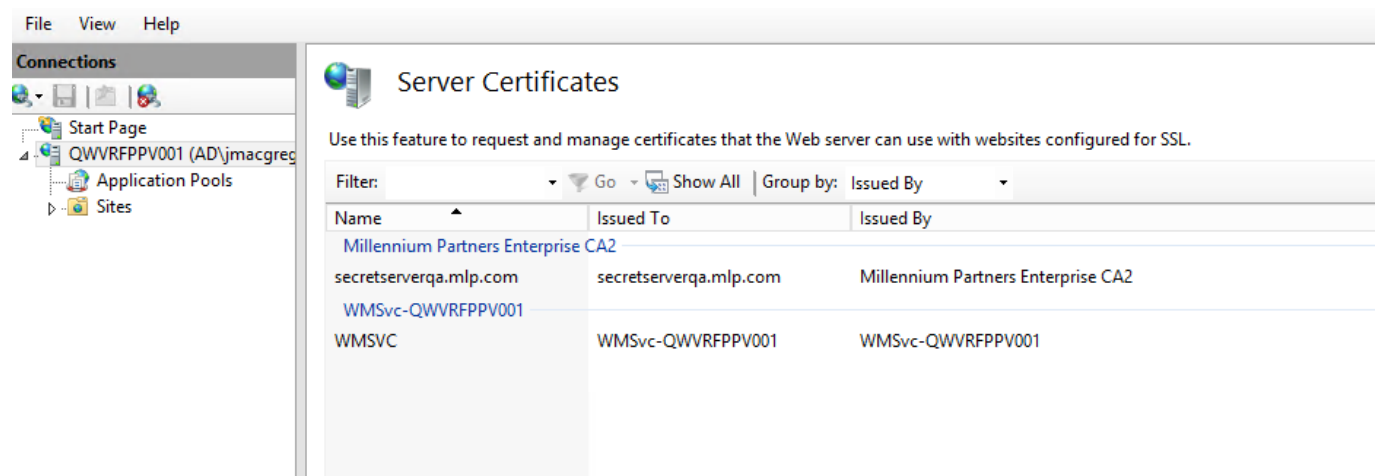
Confirm the certificate has been successfully imported into the certificate store

Open IIS Manager

Select the Web Server

Select Server Certificates

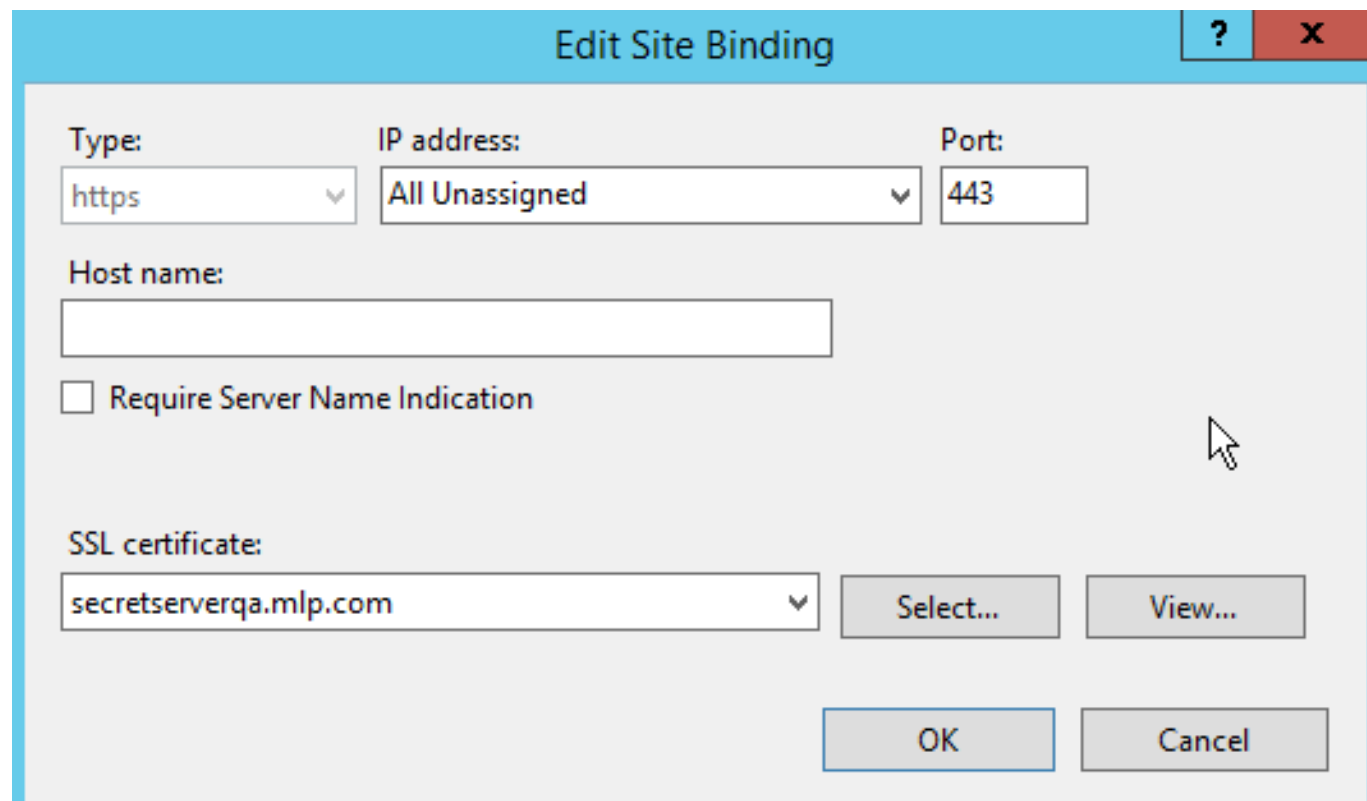
Confirm the certificate from the sequence above is visible



Select the Web Site under which the Application is deployed

Select **Bindings...**

Select **https > Edit**



Select the previously imported certificate

Click **OK**

Run IISRESET

Part III : Convert the PFX cert bundle file to KS file for JAVA API Usage

1. Export the PFX file from the Secret Server host which the original CSR was generated on
2. Convert the PFX backup file to Java KeyStore format using the command below: