



# SSL Certificate Management for XenData Web services

## Table of Contents

XenData Web Services .....	<b>Error! Bookmark not defined.</b>
<b>1. Creating a Certificate Signing Request (CSR) .....</b>	<b>3</b>
<b>2. Submitting a Re-Key Request for an Existing SSL Cert .....</b>	<b>13</b>
<b>3. Installing the Certificate on the Server .....</b>	<b>15</b>

Note: Local **Administrators** is the minimum group membership required to complete these procedures.

## 1. Creating a Certificate Signing Request (CSR)

If you are ordering your SSL certificate from DigiCert, you can skip steps **1.1** through **1.22** and instead, follow the instructions found here: <https://www.digicert.com/kb/util/csr-creation-microsoft-servers-using-digicert-utility.htm>

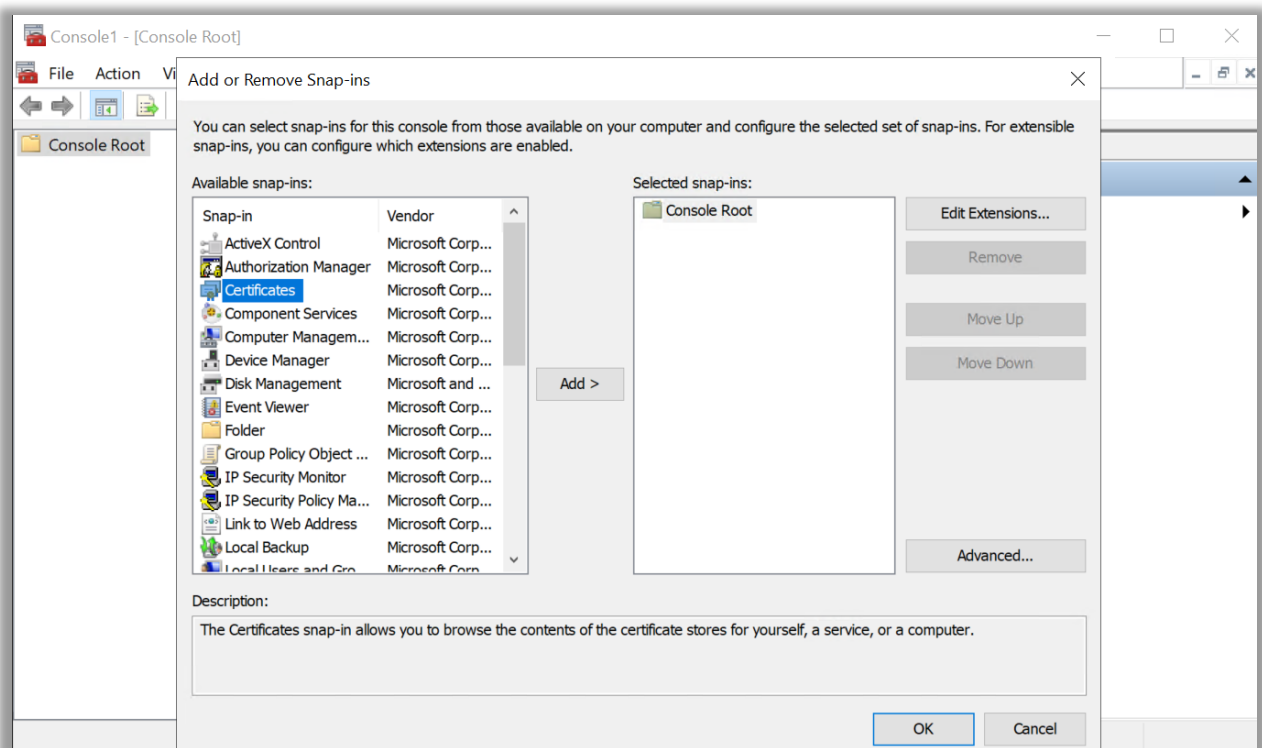
The following instructions will generate a Certificate Signing Request, *they should be followed on the server that the SSL certificate will be installed on*. The CSR can be submitted when requesting an SSL certificate, the Certificate Authority will create an SSL certificate based on the CSR. If an SSL certificate has already been requested and created, the same CSR can be used to request a 're-key', whereupon the Certificate Authority will provide a new SSL certificate based on the CSR.

**1.1** Right-Click Start, select Run

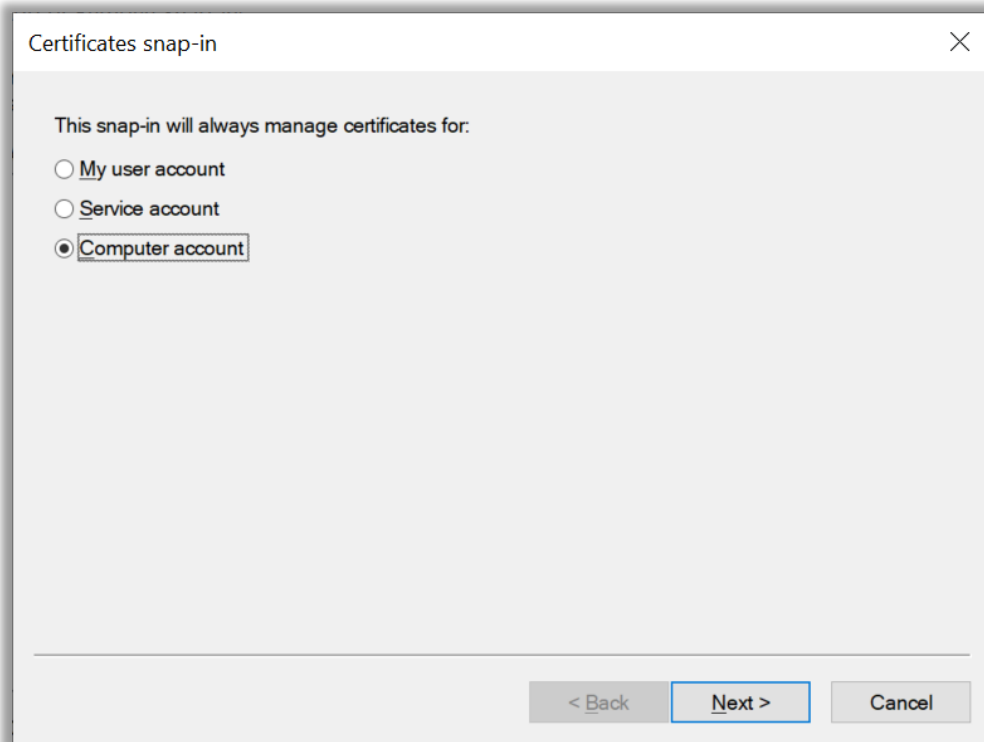
**1.2** Type MMC in the Run box and press Enter

**1.3** Click on the Files menu, then click Add/Remove Snap-in

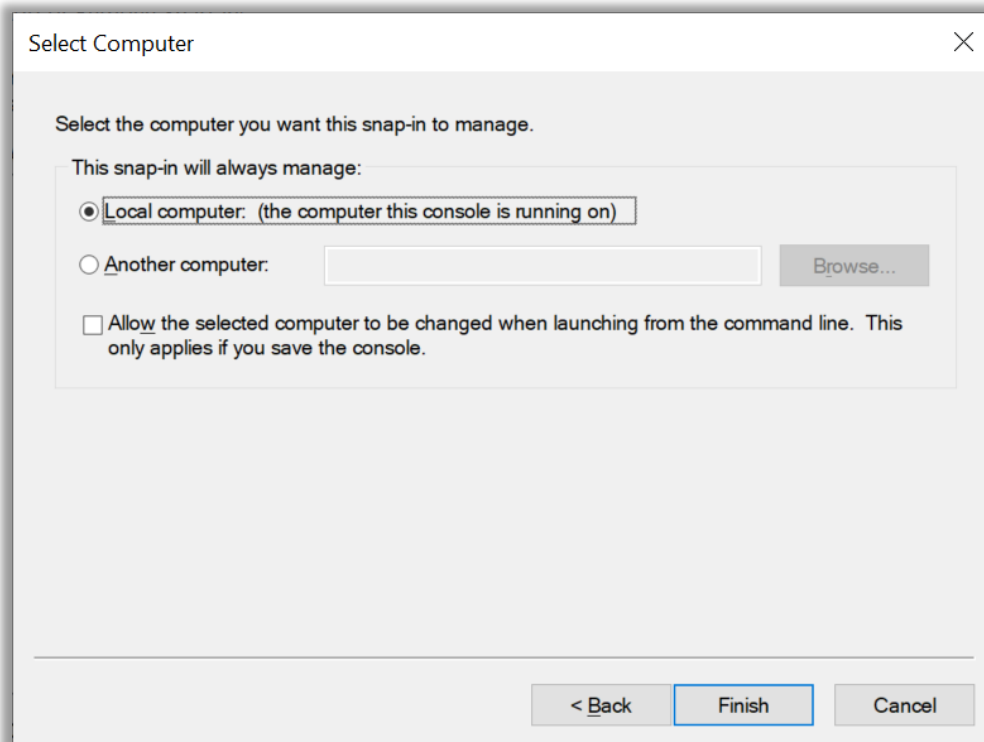
**1.4** From the available snap-ins list, click Certificates then click Add



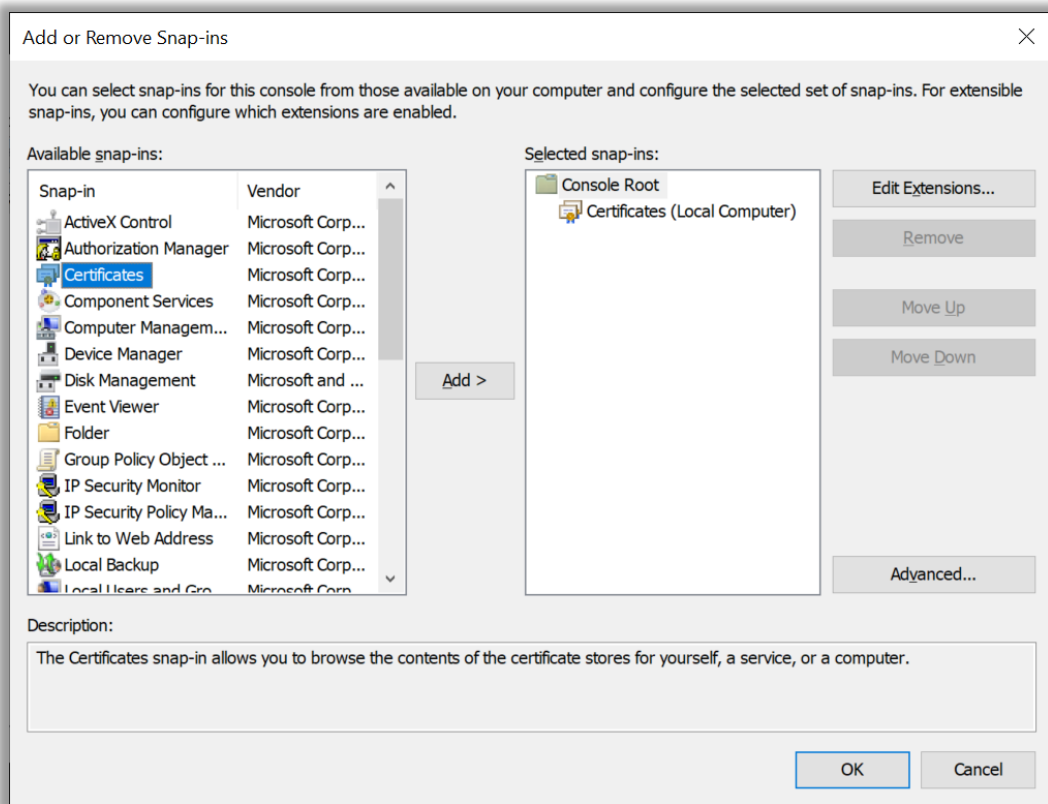
### 1.5 Select Computer account, then click Next



### 1.6 Select Local computer and click Finish

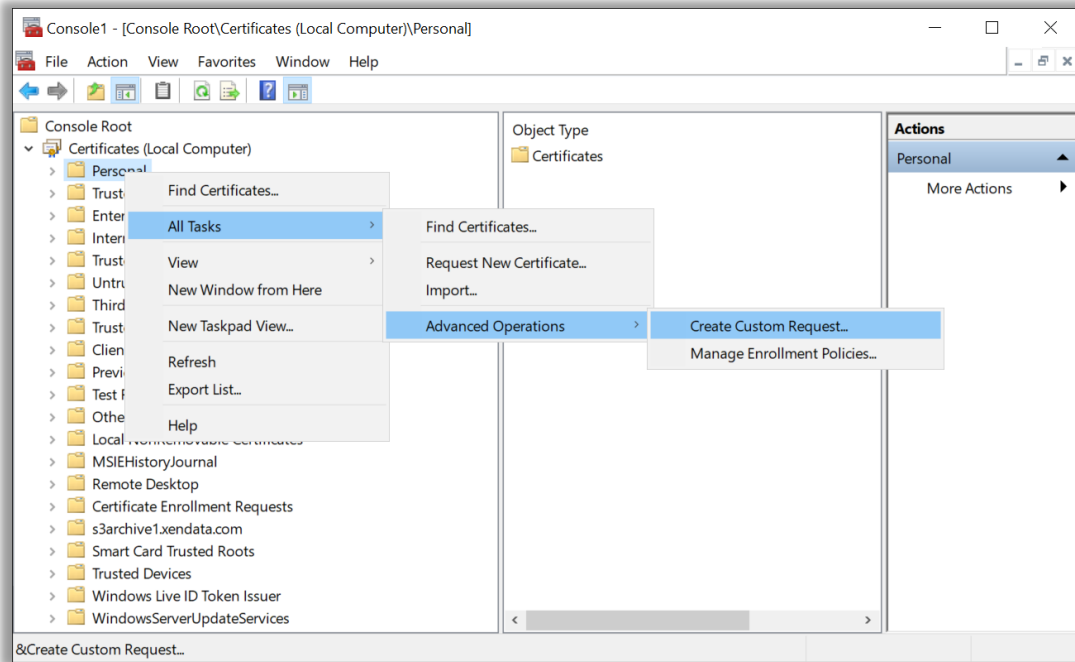


**1.7** On the Add or Remove Snap-ins dialog, click on OK



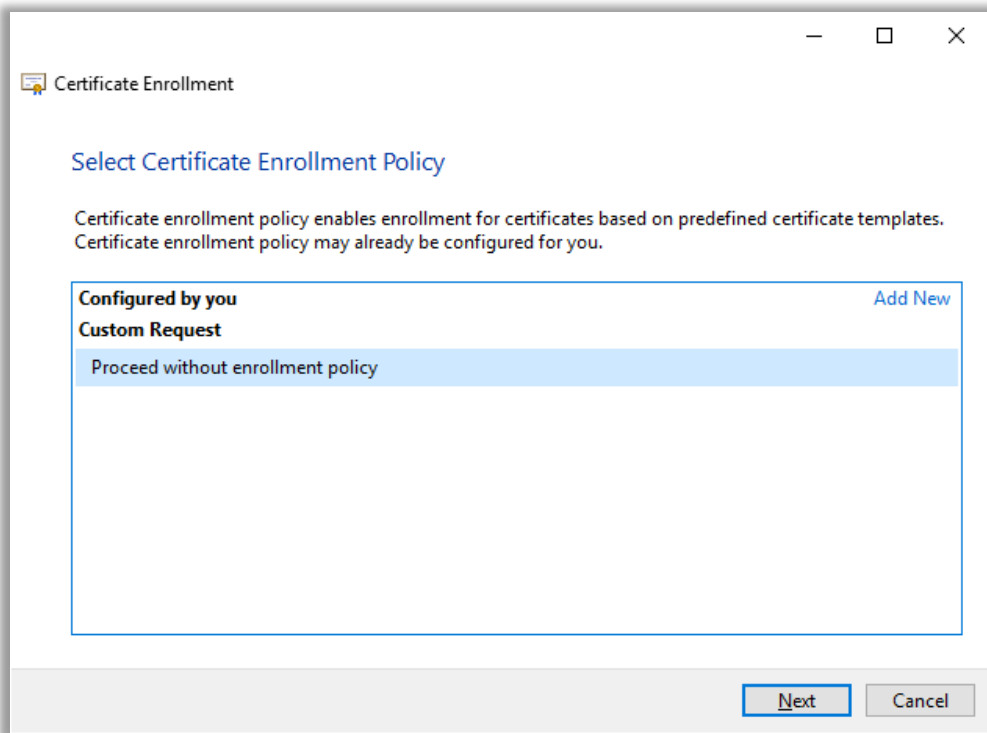
**1.8** Under the Console Root folder, expand Certificates (Local computer)

**1.9** Right-click the Personal folder and select: All Tasks, then Advanced Options, and click Create Custom Request

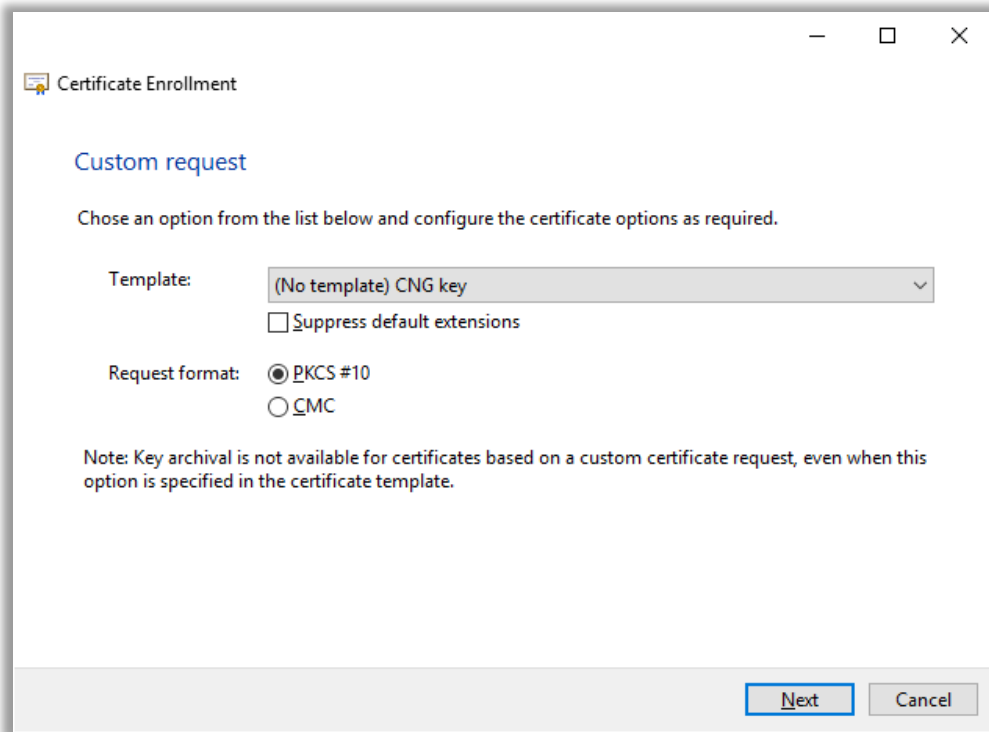


**1.10** On the Certificate Enrollment dialog, read Before you begin, click on Next

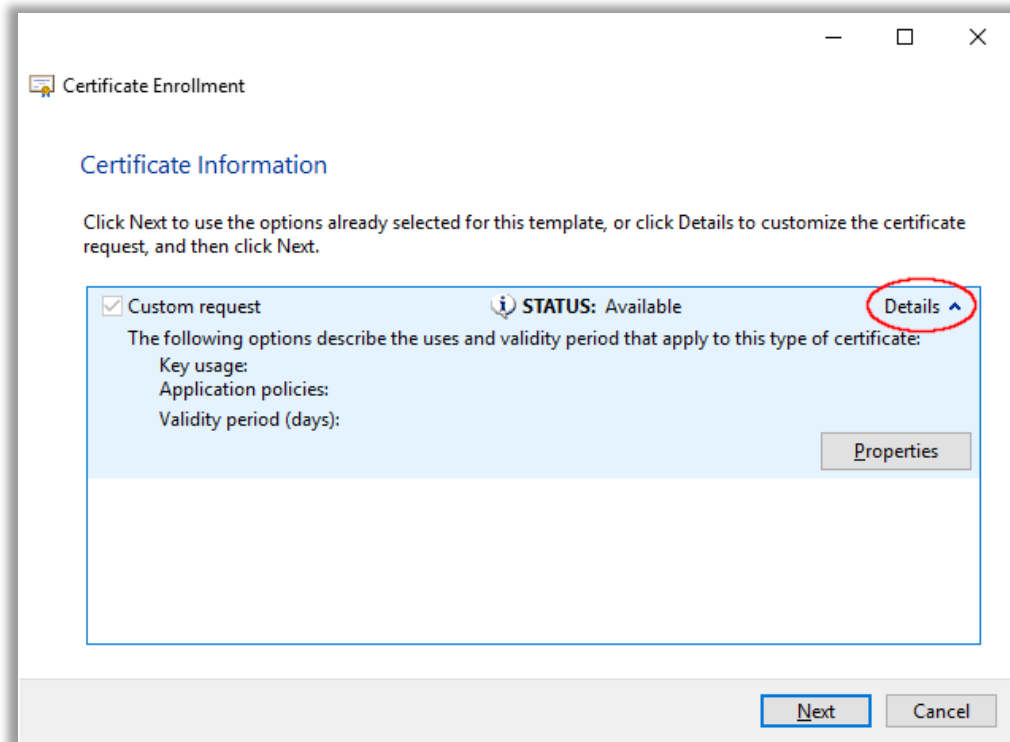
**1.11** On the Select Certificate Enrollment Policy dialog, select Proceed without enrollment policy, click on Next



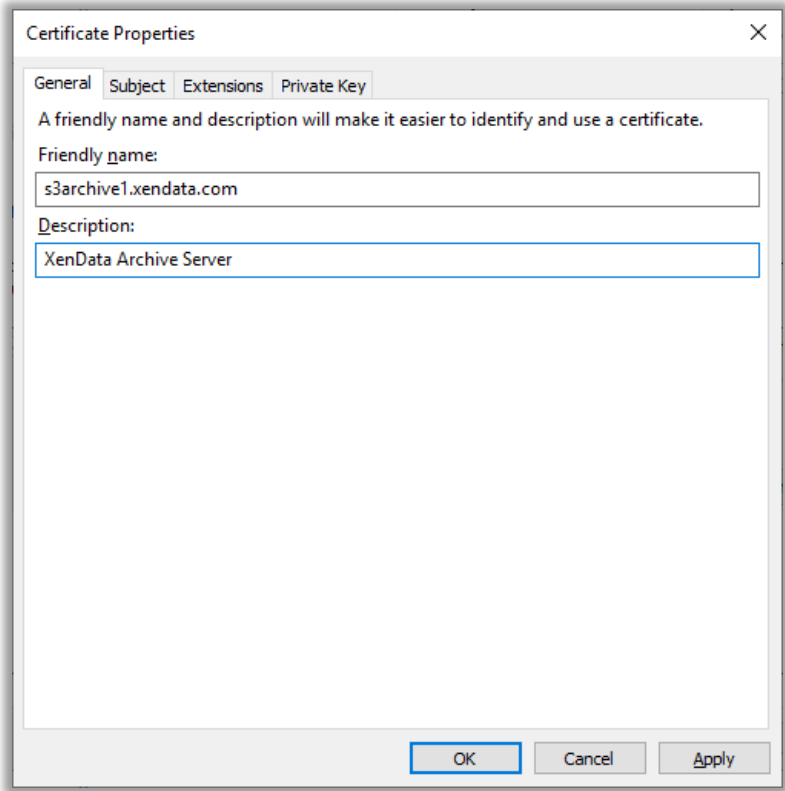
1.12 On the Custom Request dialog, leave the default values, then click Next



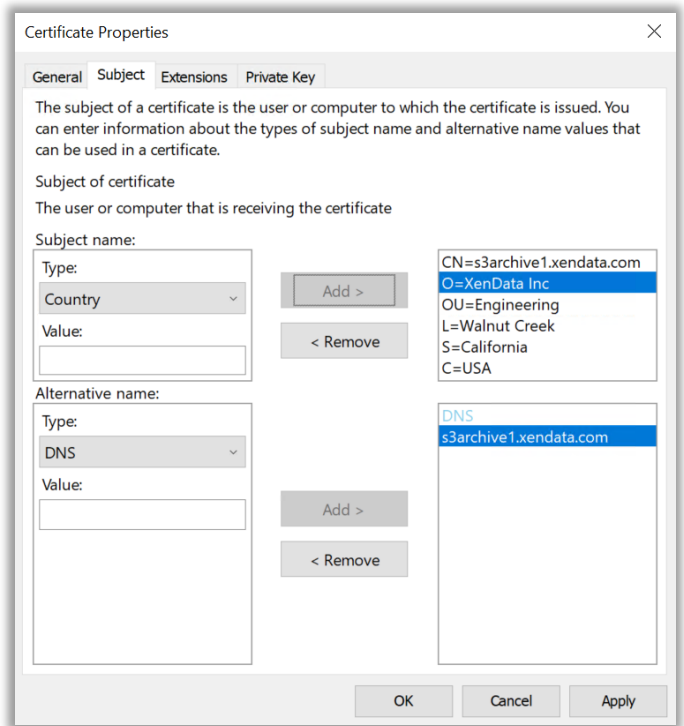
1.13 Expand the details pane and select Properties



1.14 Add a Friendly name and description for the certificate, then select the Subject tab

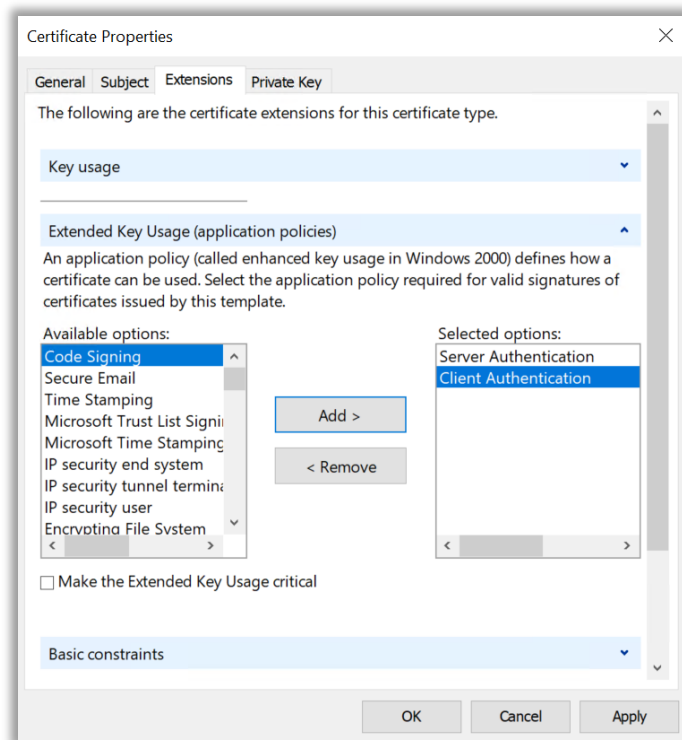


**1.15** Move to the Subject tab, and add certificate details, the ones we used were Common Name, Organization, Organization Unit, Location, County

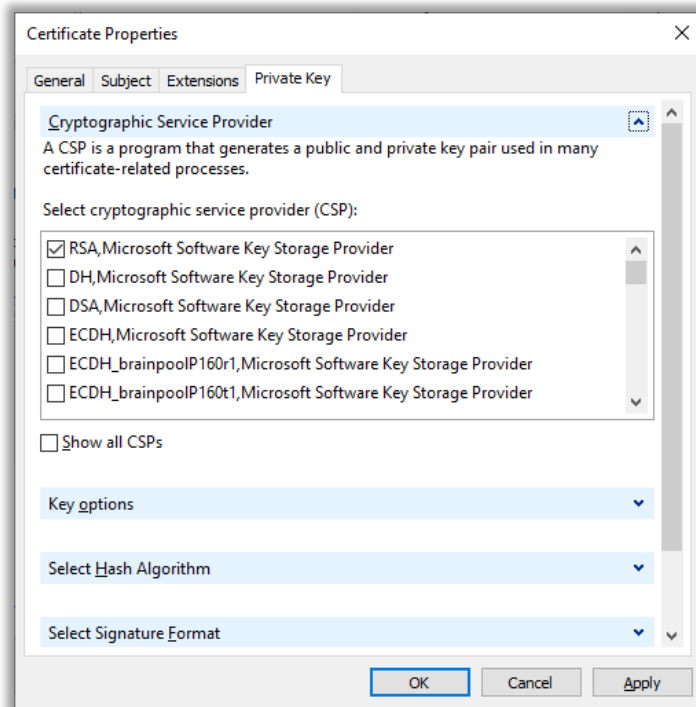




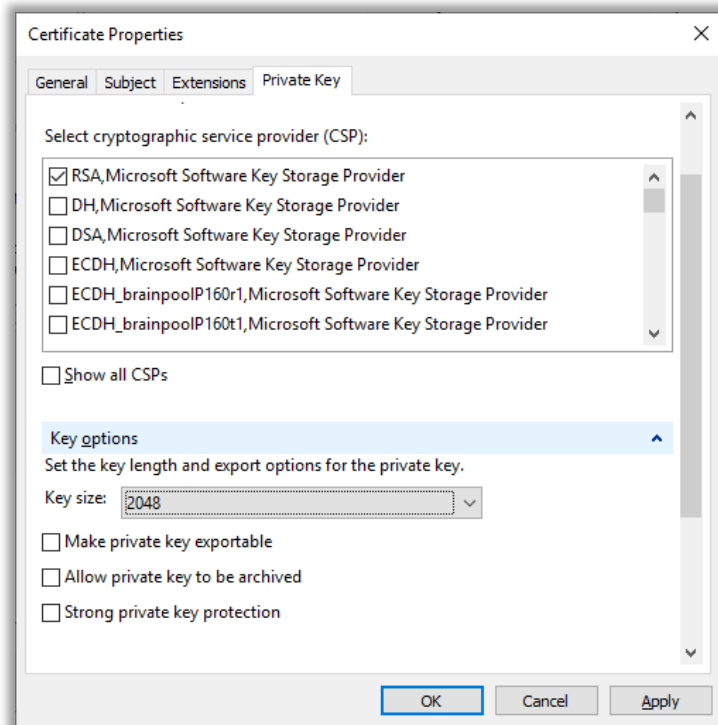
**1.16** Move to the Extensions tab, expand 'Extended Key Usage' and add Server Authentication, and Client Authentication



**1.17** Move to the Private Key tab and expand 'Cryptographic Service Provider'. Ensure that only RSA Microsoft Software Key Storage Provider is checked

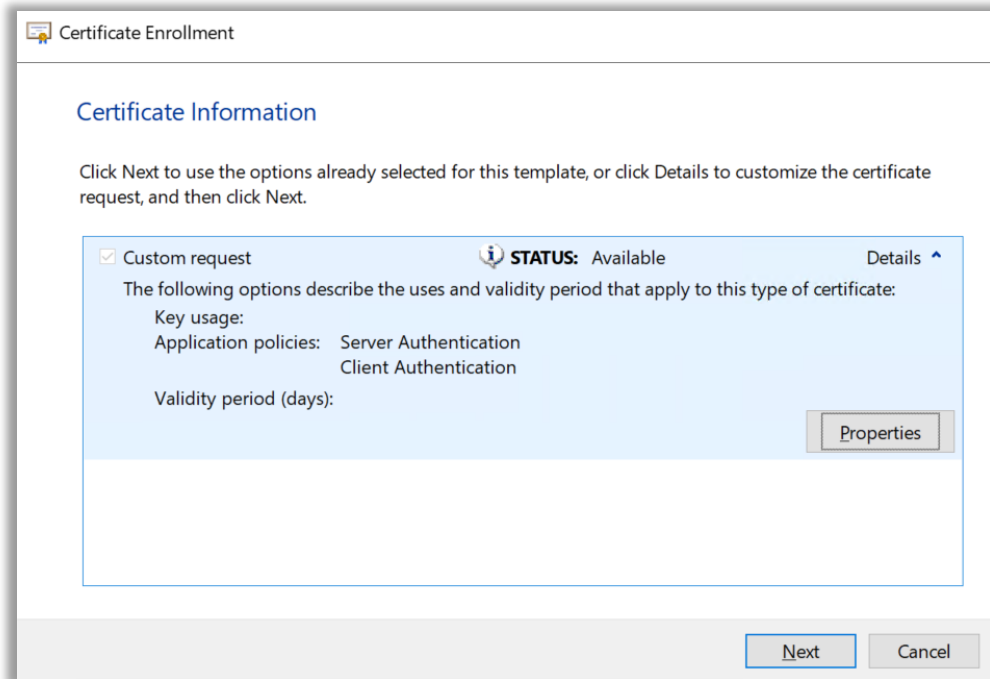


**1.18** Expand 'Key Options' and change the Key Size to 2048, and check 'Make Private Key Exportable'

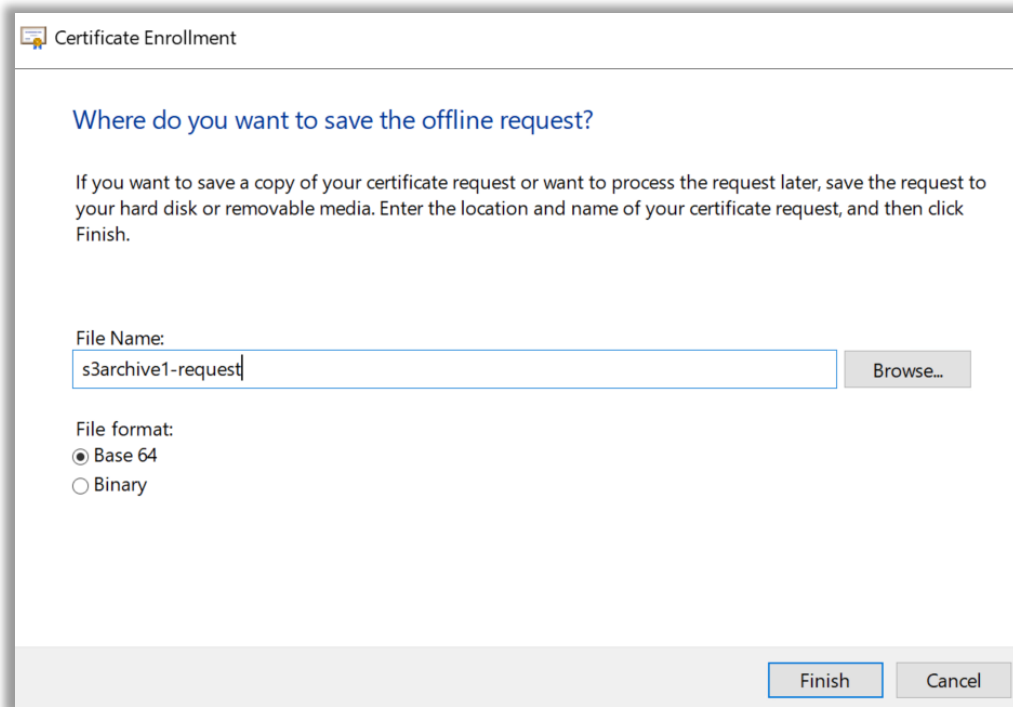


**1.19** Apply all these settings and click OK

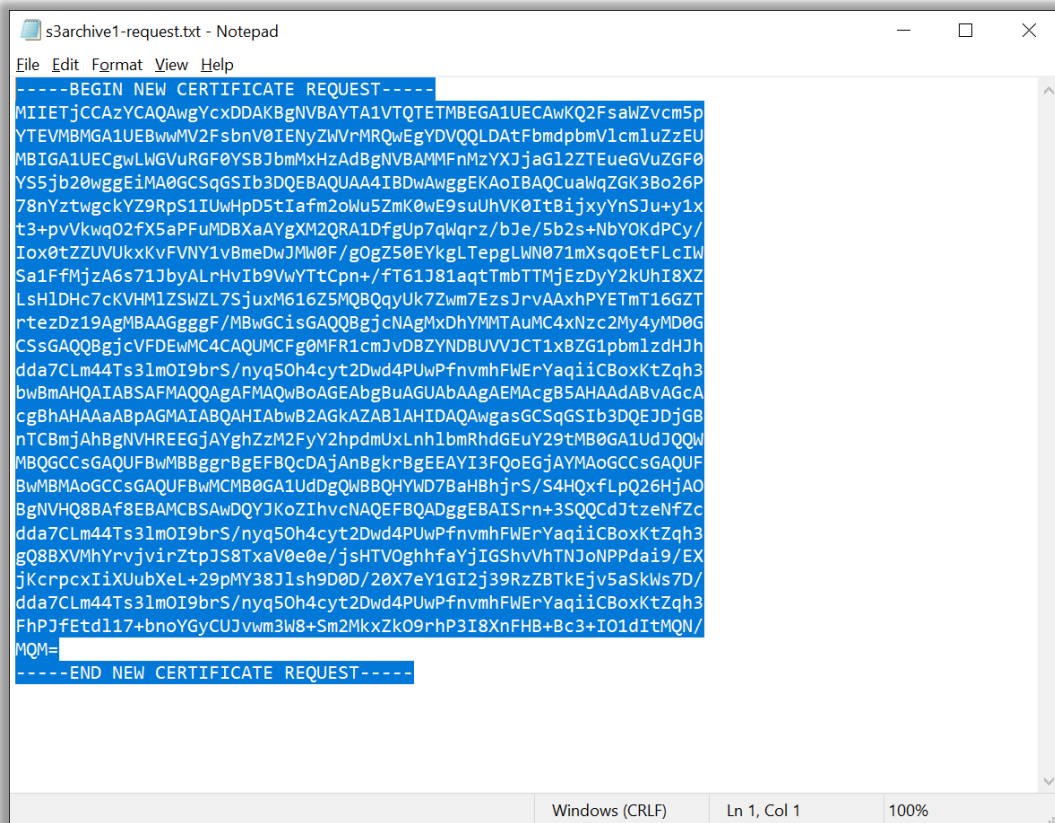
**1.20** On the Certificate Information dialog, click Next



1.21 Save the file in Base 64 file format with a .txt extension and select Finish



**1.22** Open the saved file, select all and copy, this is the CSR which can be used when requesting an SSL certificate from the Certificate Authority



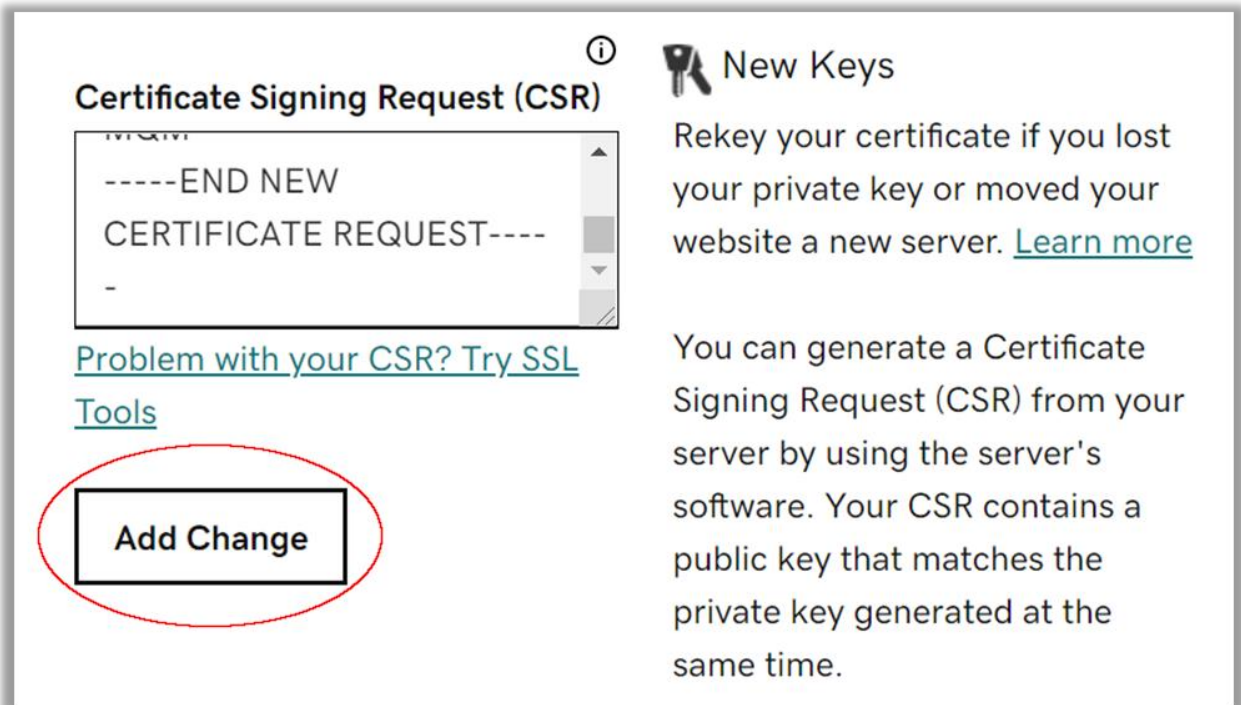
```
s3archive1-request.txt - Notepad
File Edit Format View Help
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEtjCCAzYCAQAwwYcxDDAKBgNVBAYTA1VTQETMBEGA1UECAwKQ2FsawZvcM5p
YTEVMBMGA1UEBwwMV2FsbnV0IENyZWVrMRQwEgYDVQQLDAtFbmdpbmV1cm1uZzEU
MBIGA1UECgwLWGVuRGF0YS8JbmMxHzAdBgNVBAMFNmZyXjJaG1Z2TEueGVuZGF0
YS5jb20wgGE1MA0GCsqGSIB3DQEBAQUAA4IBDwAwggEKAoIBAQCuaWqZGK3Bo26P
78nYztwgckYZ9RpS1IUwHpD5tIafm2oWu5ZmK0wE9suUHVk0ItBijxyYnSJu+y1x
t3+pvVkwqO2fX5aPFuMdBXaAYgXM2QRA1DfgUp7qWqrz/bJe/5b2s+NbYOKdPCy/
Iox0tZUVUkxKvFVNY1vBmeDwJMw0F/gOgZ50EYkgLTepgLN071mXsqoEtFLcIW
Sa1FfMjzA6s71JbyALrhVib9VwYtTcPn+/FT61J81aqTmbTTMjEzDyV2kUhI8XZ
LsHIDhc7cKVHM1ZSWZL7SjuxM616Z5MQBQqyUk7Zwm7EzsJrvAAxhPYETmT16GZT
rtezDz19AgMBAAGgggF/MBwGCisGAQQBggjcnAgMx0hYMMTAuMC4xNzc2My4yMD0G
CSsGAQQBggjcvFDEwMC4CAQUMCFg0MFR1cmJvDBZYNDUUVJCT1xBZG1pbm1zdHJh
dda7CLm44Ts31m0I9brS/nyq50h4cyt2Dwd4PUwPfnvmhFWErYaqiiCBoxKtZqh3
bwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAgAEMAcb5AHAADABVAGcA
cgBhAHAaAbpAGMAIABQAHIAbwB2AGkAZAB1AHIDAQAwwGASqGSIB3DQEJJDjGB
nTCBmJAhBgNVHREEGjAYghZz2M2FyY2hpdMuxLnh1bmRhdGEuY29tMB0GA1UdJQQW
MQBQCCsGAQUFBwMBBggrBgEFBQcDAjAnBgkrBgEEAYI3FQoEGjAYMAoGCCsGAQUF
BwMBMAoGCCsGAQUFBwMCMCB0GA1UdDgQWBQBQHYWd7BaHBhjrS/S4HQxfLpQ26HjAO
BgNVHQ8BAf8EBAMCBSAwDQYJKoZIhvcNAQEFBQADggEBAISrn+3SQQcdJtzeNfZc
dda7CLm44Ts31m0I9brS/nyq50h4cyt2Dwd4PUwPfnvmhFWErYaqiiCBoxKtZqh3
gQ8BXVMhYrvjvirZtpJS8TxaV0e0e/jSHTV0ghhfaYjIGShvVhTNJoNPPdai9/EX
jKcrpcxIiXUubXeL+29pMY38J1sh9D0D/20X7eY1GI2j39RzZBTkEjv5aSkws7D/
dda7CLm44Ts31m0I9brS/nyq50h4cyt2Dwd4PUwPfnvmhFWErYaqiiCBoxKtZqh3
FhPjFetd117+bnoYgCUJvwm3W8+Sm2MkxZk09rhP3I8XnFHB+Bc3+IO1dItMQN/
MQM=
-----END NEW CERTIFICATE REQUEST-----
Windows (CRLF) Ln 1, Col 1 100%
```

**1.23** Download your SSL certificate. If prompted for Server type, choose “IIS” and download the Zip file. After saving the Zip file, copy it to the server and extract it to a known location

## 2. Submitting a Re-Key Request for an Existing SSL Cert

If an SSL certificate has already been purchased, the CSR can be used to request a re-key for the server on which you want to install the certificate. The following instructions describe the process used to re-key a certificate where the Certificate Authority is GoDaddy; equivalent functionality should be found on the websites of other Certificate Authorities.

- 2.1 Navigate to the SSL Cert management console
- 2.2 Paste the CSR content into the SSL certificate providers SSL Certificate Signing Request (CSR) tool and click 'Add Change'



**Certificate Signing Request (CSR)** ⓘ

```
-----END NEW  
CERTIFICATE REQUEST-----  
-
```

[Problem with your CSR? Try SSL Tools](#)

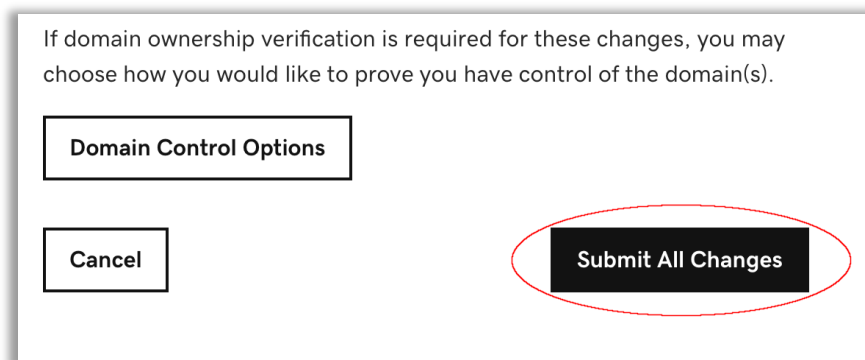
**Add Change**

### 🔑 New Keys

Rekey your certificate if you lost your private key or moved your website a new server. [Learn more](#)

You can generate a Certificate Signing Request (CSR) from your server by using the server's software. Your CSR contains a public key that matches the private key generated at the same time.

- 2.3 Submit the certificate request (response times vary from a few minutes to a week or more, depending on the certificate type)

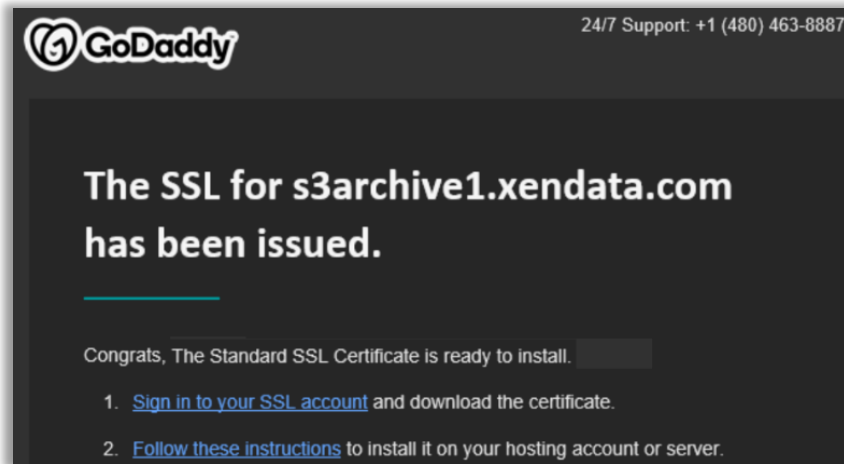


If domain ownership verification is required for these changes, you may choose how you would like to prove you have control of the domain(s).

**Domain Control Options**

**Cancel** **Submit All Changes**

## 2.4 Your Certificate Authority should email you once the certificate is ready



## 2.5 Download your SSL certificate. If prompted for Server type, choose "IIS" and download the Zip file. After saving the Zip file, copy it to the server and extract it to a known location

Certificate Details	
Type	Standard SSL Certificate
Status	Certificate issued ( <a href="#">Revoke</a> )
Domain name	s3archive1.xendata.com
Certificate Issuer	GoDaddy SHA-2
Request Date	7/12/2021 10:13
Request Submission Type	Rekey
Current Certificate Validity Period	7/12/2021 - 4/8/2022
Subscription Period	4/8/2021 - 4/8/2022
Serial Number	c6:25:f2:1f:b3:9a:26:17

### Download Certificate

To secure your site that's hosted elsewhere, download the Zip file that matches your hosting server type. Then, install all of the certificates in the Zip file on your hosting server, including any intermediate certificates that might be needed for older browsers or servers.

First time installing a certificate?  
[View Installation Instructions for the selected server.](#)

Server type

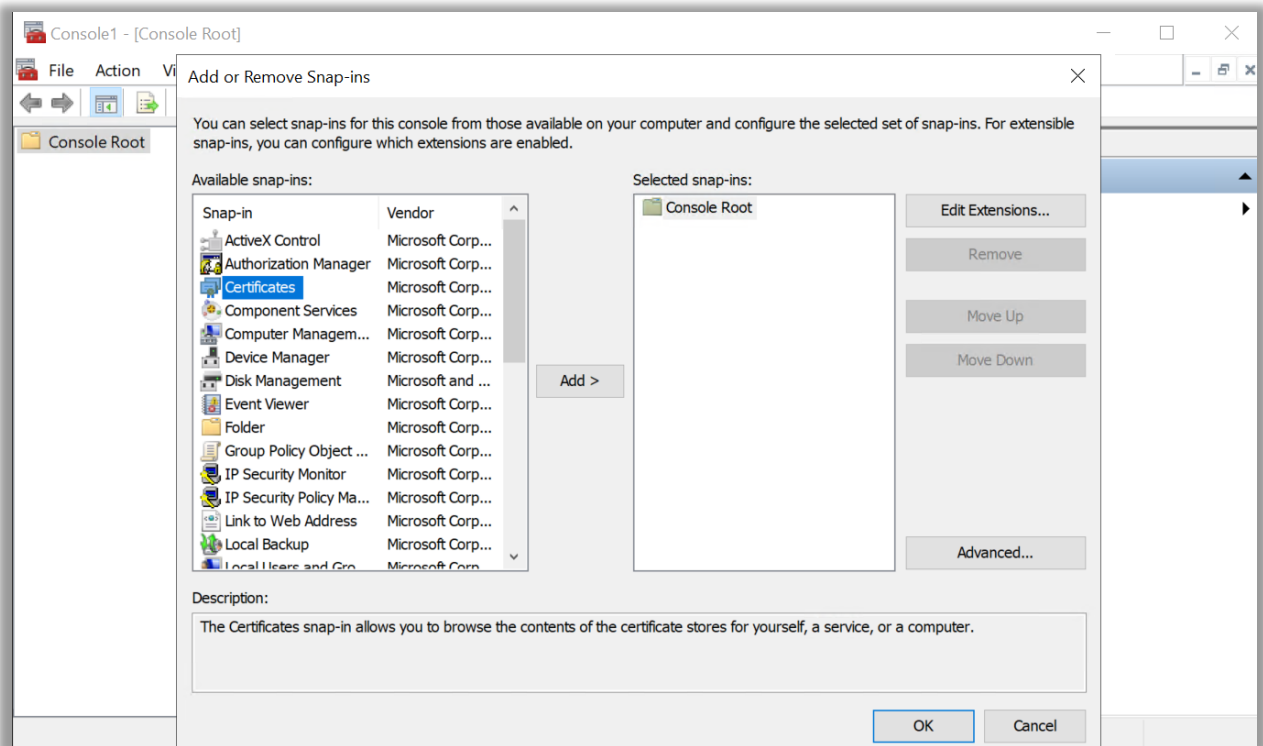
## 3. Installing the Certificate on the Server

3.1 Right-Click Start, select Run

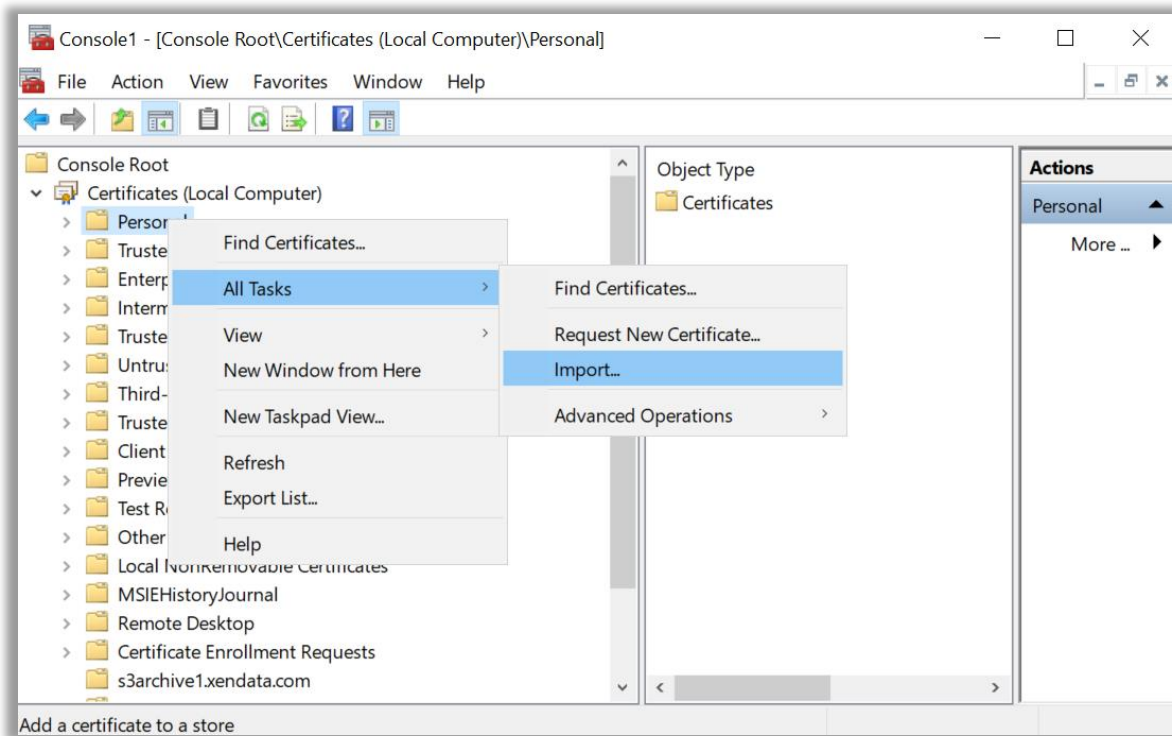
3.2 Type MMC in the Run box and press Enter

3.3 Click on the Files menu, then click Add/Remove Snap-in

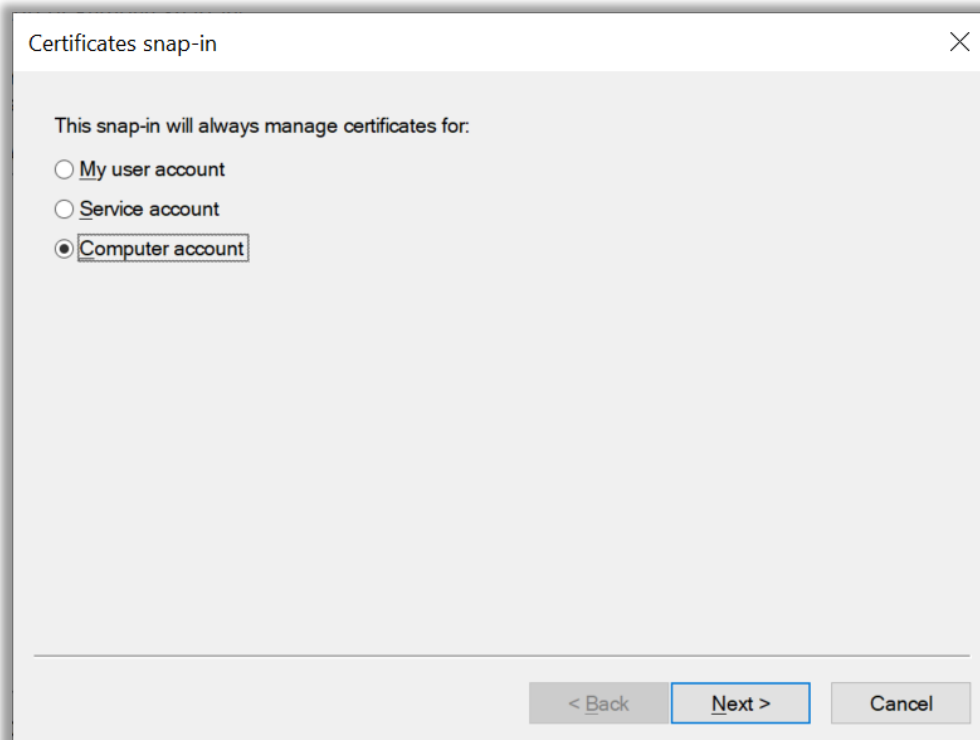
3.4 From the available snap-ins list, click Certificates then click Add



3.5 Under the Certificates – Local Computer Section, Select Personal, then right-click and select and expand All Tasks, then select Import

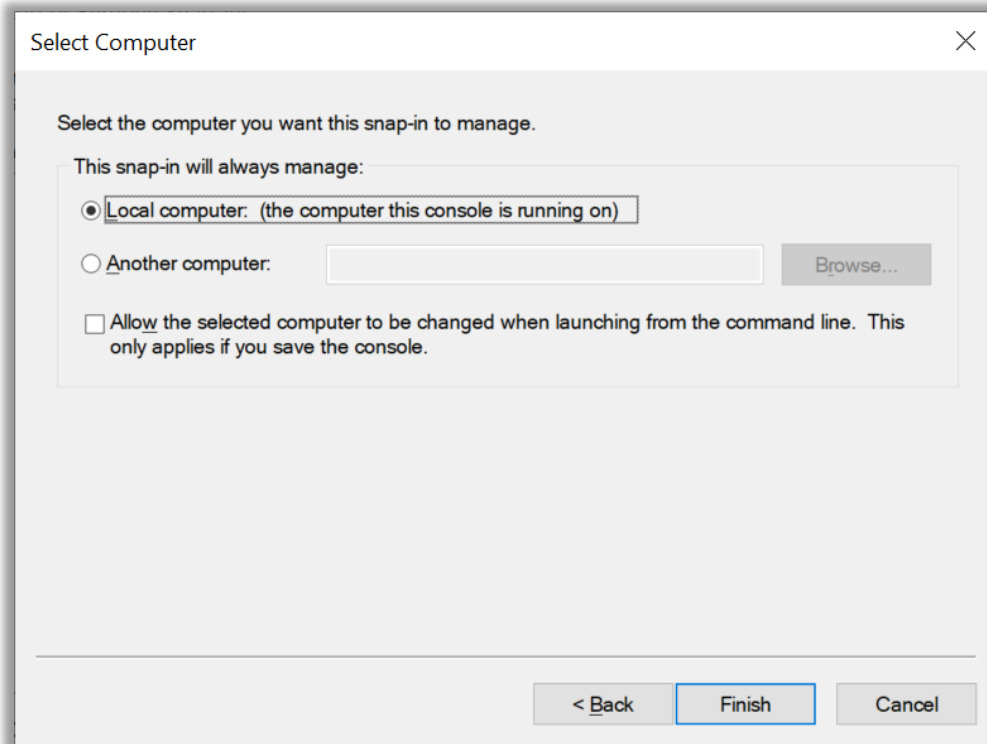


3.6 Select Computer account, then click Next

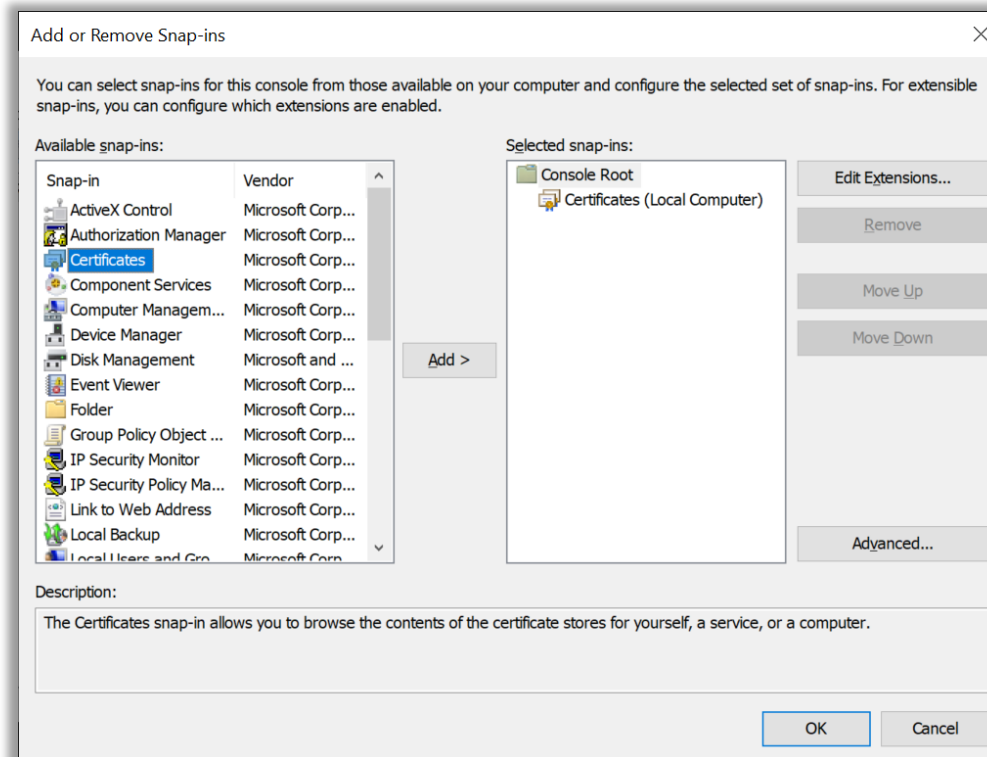




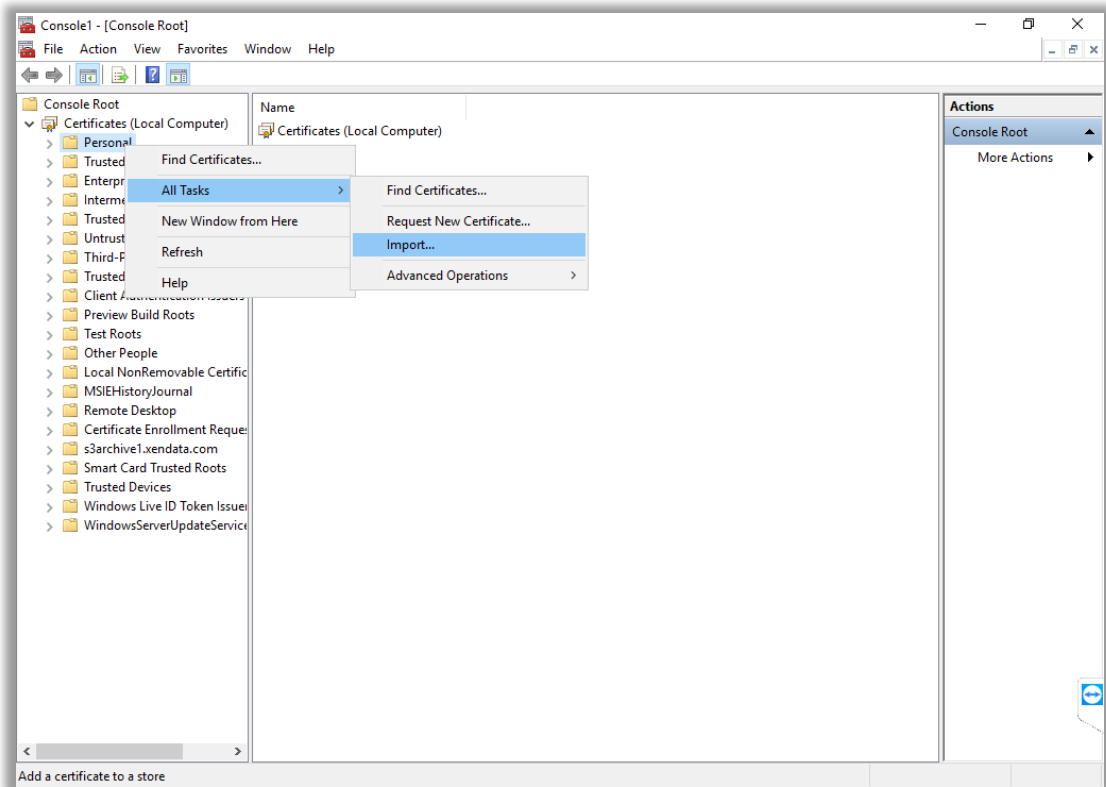
### 3.7 Select Local computer and click Finish



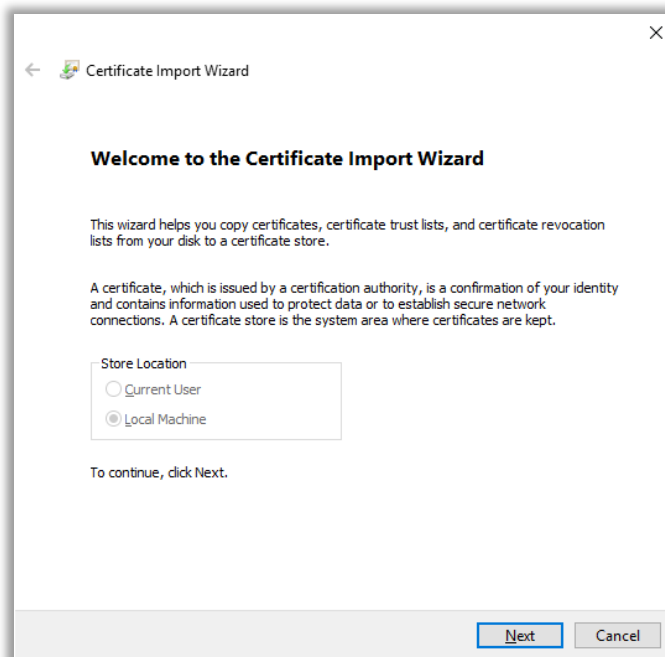
### 3.8 On the Add or Remove Snap-ins dialog, click on OK



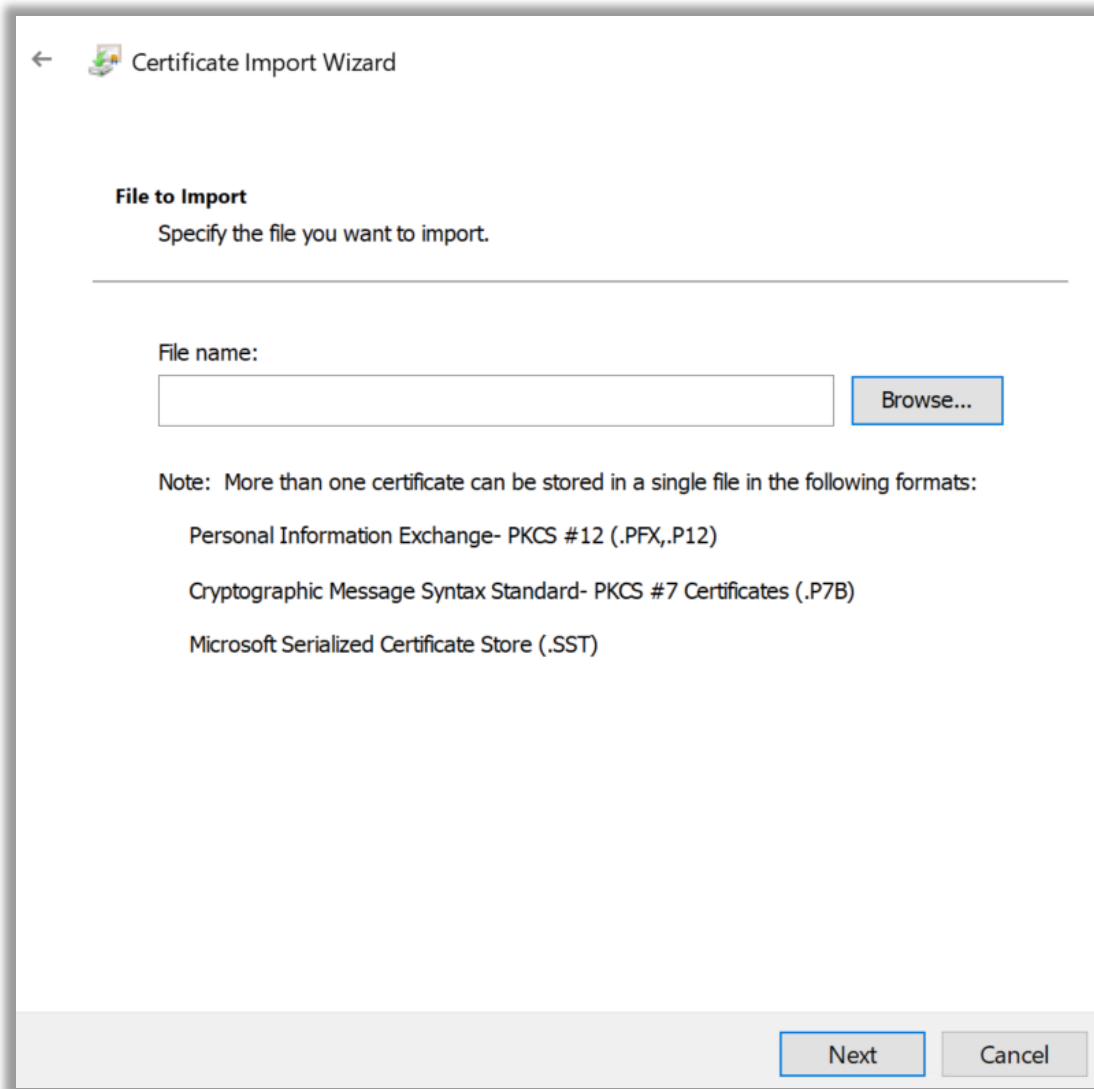
3.9 Under the Console Root folder, expand Certificates (Local computer). Right-click the Personal folder and select All Tasks - Import



3.10 Click Next on the Welcome to the Certificate Import Wizard dialog



**3.11** Browse to the location you extracted the SSL certs ZIP file and select the .CRT file and click Next



← Certificate Import Wizard

**File to Import**  
Specify the file you want to import.

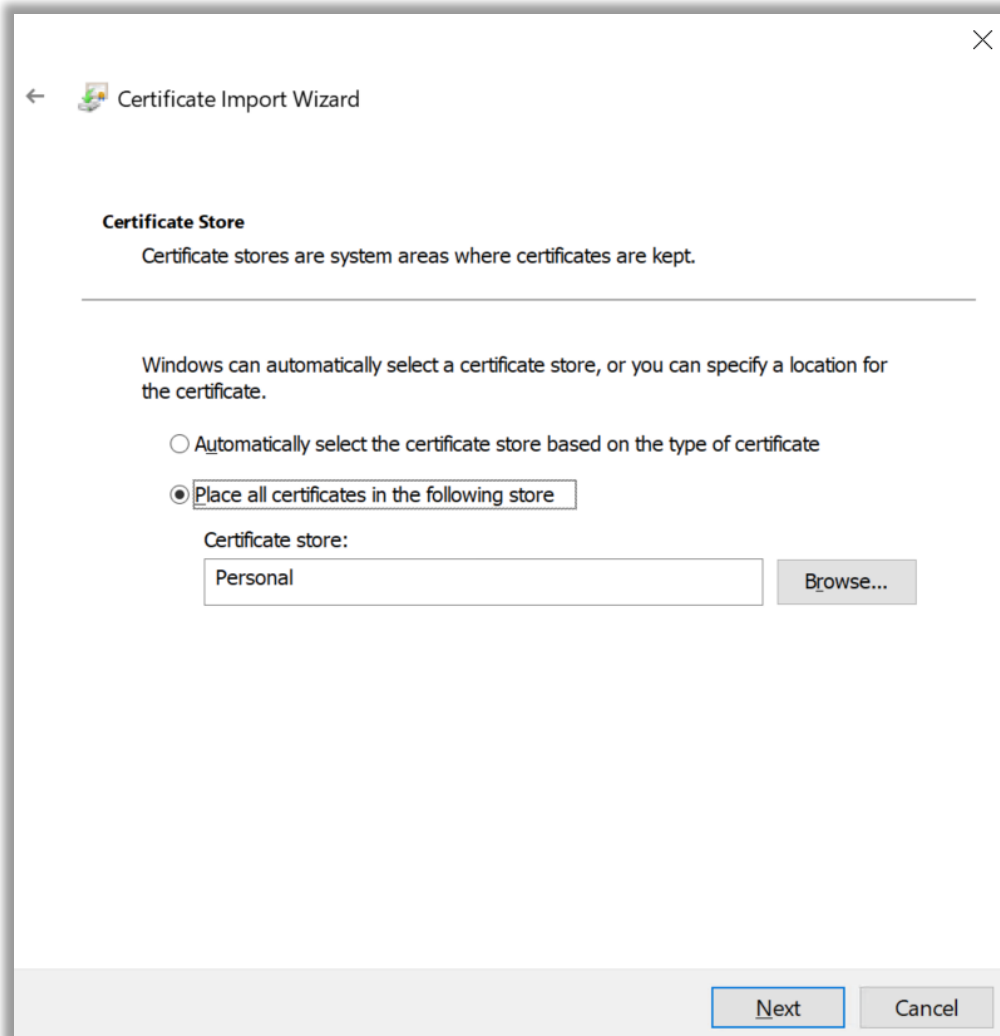
---

File name:

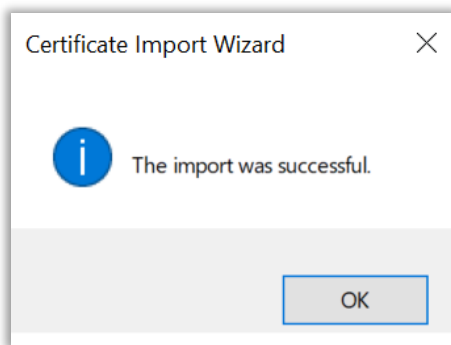
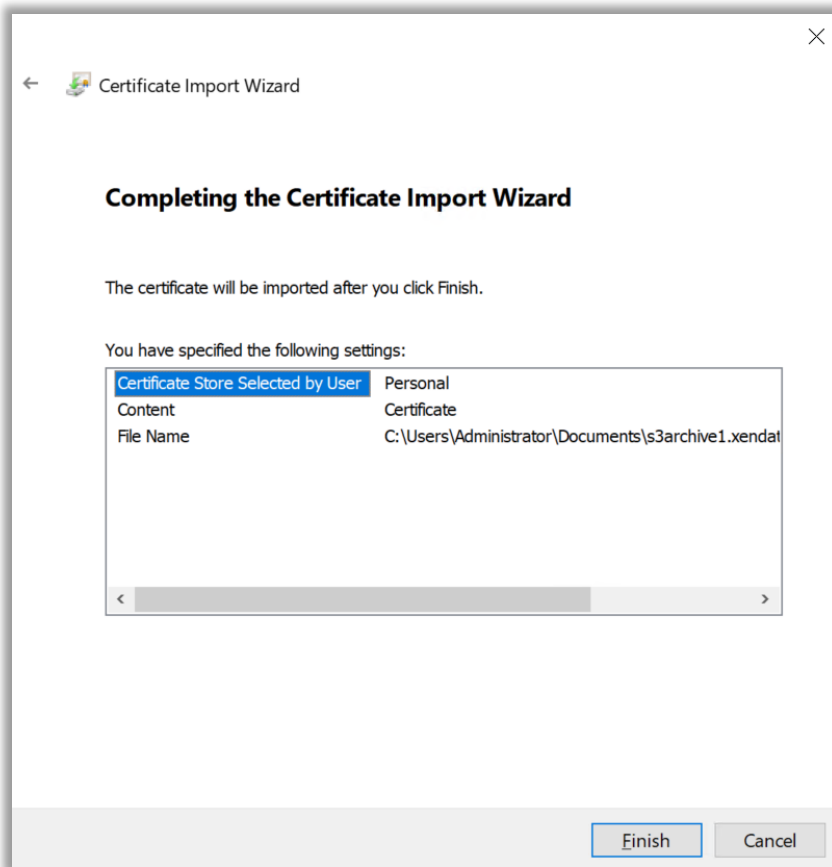
Note: More than one certificate can be stored in a single file in the following formats:

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

### 3.12 Choose to place all certificates into the Personal Certificate store and click Next

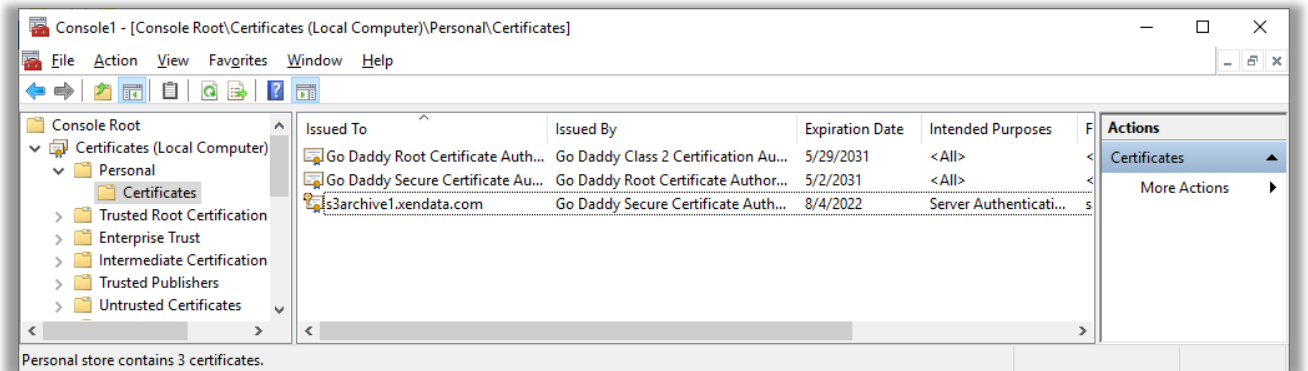


### 3.13 Click on Finish

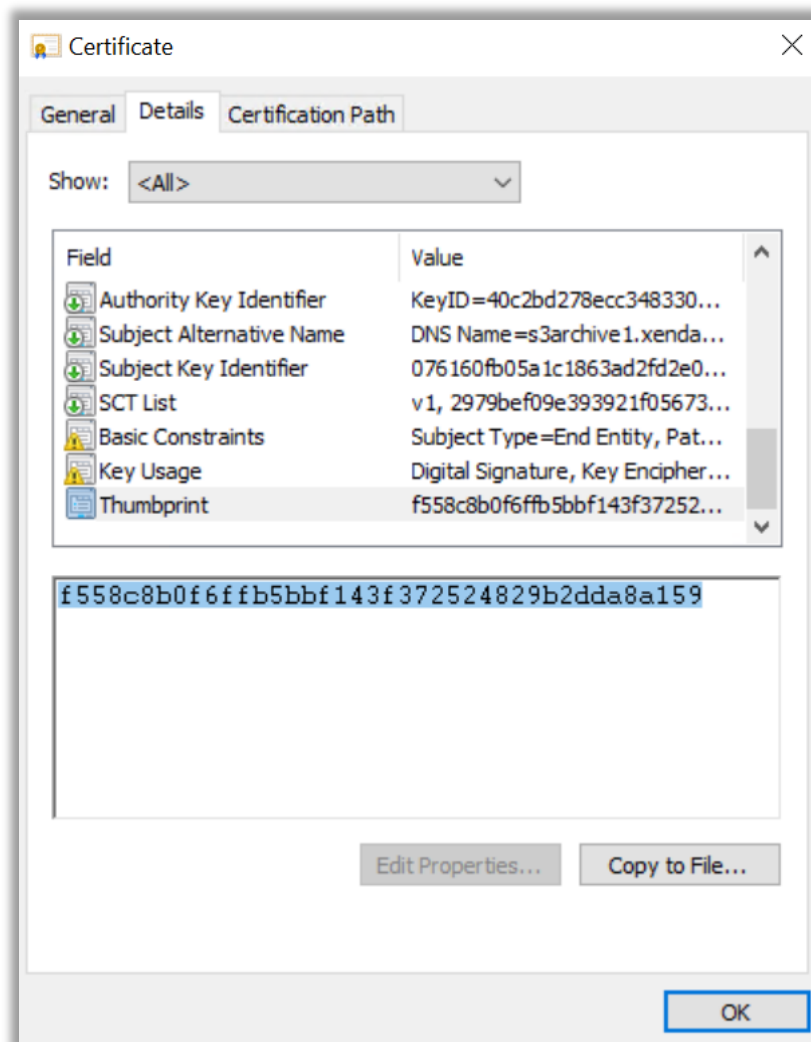


### 3.14 Repeat steps 3.9 through 3.13 for the .P7B file

**3.15** After importing the CRT and P7B files, the certificate should be visible in the Personal Certificate store



**3.16** Double click on the imported certificate and open the Details tab. Scroll to the bottom and then select and copy the contents of the 'Thumbprint' field



**3.17** Open a PowerShell session with the “Run as Administrator” option

**3.18** Generate a GUID using the following command:

```
[guid]::NewGuid().ToString("B")
```

**3.19** To add the SSL cert to the DNS name, enter the following **netsh** command, replacing:

**YOUR\_DNS\_NAME** with your DNS name

**THUMBPRINT** with the thumbprint acquired in step **3.16**\*

\*Remove any spaces and/or any strange characters in the copied thumbprint.

**GUID** with the GUID created in step **3.18**

```
netsh http add sslcert certstorename=MY hostnameport=YOUR_DNS_NAME:443  
certhash=THUMBPRINT appid='{GUID}'
```

Example:

```
netsh http add sslcert certstorename=MY hostnameport=archive1.xendata.com:443  
certhash=f558c8b0f6ffb5bbf143f372524829b2dda8a159 appid='{6dd8738a-b7b1-46af-a184-  
24cde77be7b2}'
```

If successful, the command will return the following message:

**SSL Certificate successfully added**

**3.20** Add the chosen DNS to your hosts file in windows, the file is located in:

C:\Windows\System32\drivers\etc\hosts and can be opened with Notepad

**3.21** Open a web browser and point to the DNS. You should be able to access it