Creating Windows CA Code Signing Certificate for WSUS

Simon Edwards

Senior Technical Support Engineer

3th April 2020

Table of Contents

1.0 Code Signing Certificates.

The purpose of code signing is a method to prove the origin of an item of software that came from a trusted source and that it has not been tampered since it was released by applying a digital signing to the software package.

In the case of Windows updates, the update files that sync from Microsoft to your WSUS Server are already digitally signed by the vendor, as is all device drivers from hardware vendors, and all software that you may download from other trusted software vendors. The Windows operating requires that these items are all digitally signed before it will permit their installation.

How this applies to the Software Vulnerability Manager System is all patches that are delivered to your SVM console are delivered as an SPS Package ready to be created into an install package for deployment, with certain configuration options.

During the creation of an installation package that is to be deployed to your client machines, the WSUS Server digitally signs the packages that are created before publishing them to your WSUS server, ready for deployment using either WSUS or SCCM.

When an update or a patch is installed the client machine verifies that the software has come from a trusted source by checking its digital signature, if it isn't digitally signed or if the certificate to which a package was created using has expired the software will fail to install.

It is quite critical for the functionality of the SVM System that certificates are created and applied to the WSUS correctly to prevent publishing issues.

There are three ways of doing this, the first being is to obtain a code signing certificate from an external Trusted Certificate issuer, but this can be expensive, and this would only be required if you were wanting to make your WSUS Server public on the Internet. We will not cover this scenario in this document as it is a highly unlikely scenario.

The second is on Windows enterprise networks that run a root Certification Authority to request a code signing certificate from the Root CA. We will cover this scenario in this document.

The third method is to use a WSUS self-signed certificate generated by the WSUS server itself using the SVM connection tool contained in the console plugin.

Note: *If using a self-signed certificate, you will need to distribute the certificate to the client machines using a GPO, this is covered later in this document.*

Important Note:

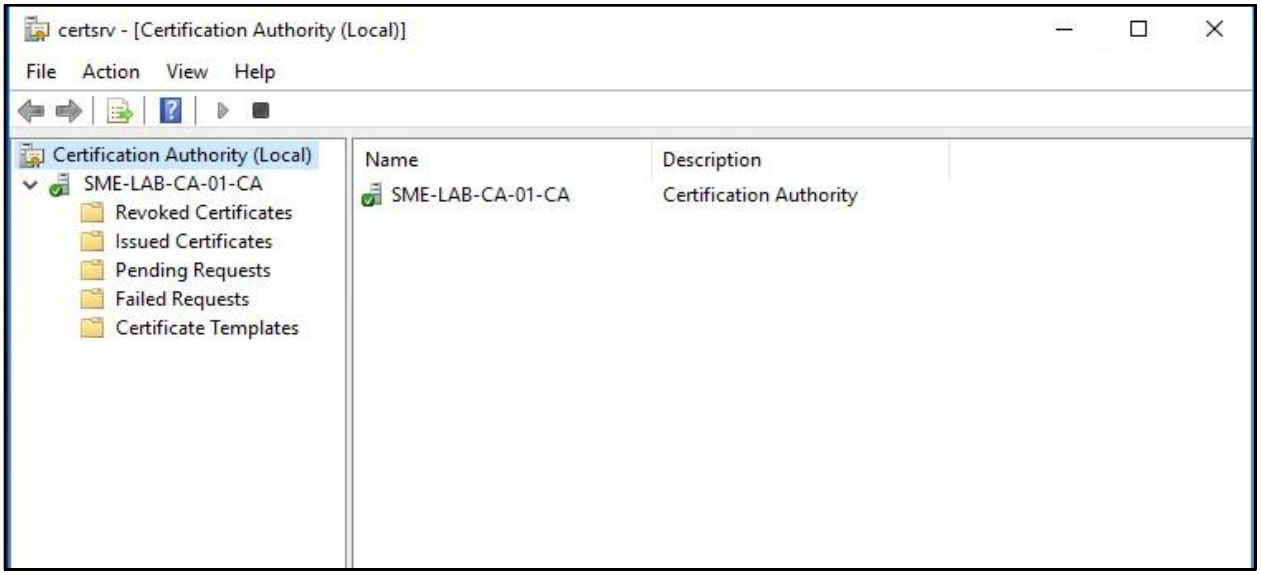
Creation and management of certificates will require a user with Administrative Privileges on the domain.

2.0 How to generate a Windows CA Code Signing Certificate for WSUS Code Signing Purposes.

The process of creating a Code Signing Certificate is in two parts, the first part is the configuration that will need to be undertaken is on the Windows RootCA Server, and the second part is the requesting of the certificate from the RootCA on the WSUS Server. Please ensure you have administrative access to both of these servers before continuing.

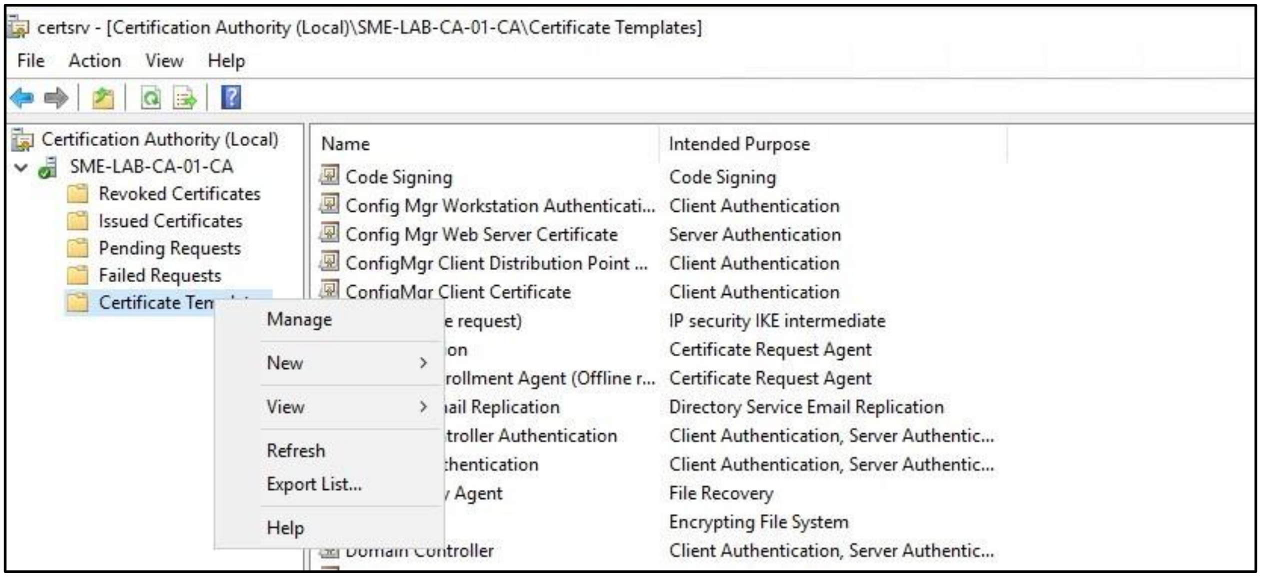
2.1 Windows Root CA Server

Connect to your Windows RootCA server and navigate to the Certificate Authority Console.



Name	Description
SME-LAB-CA-01-CA	Certification Authority

The first thing we need to do is to create a code signing certificate template, we achieve this by selecting certificate templates in the left-hand pane and right-clicking to bring up the menu.

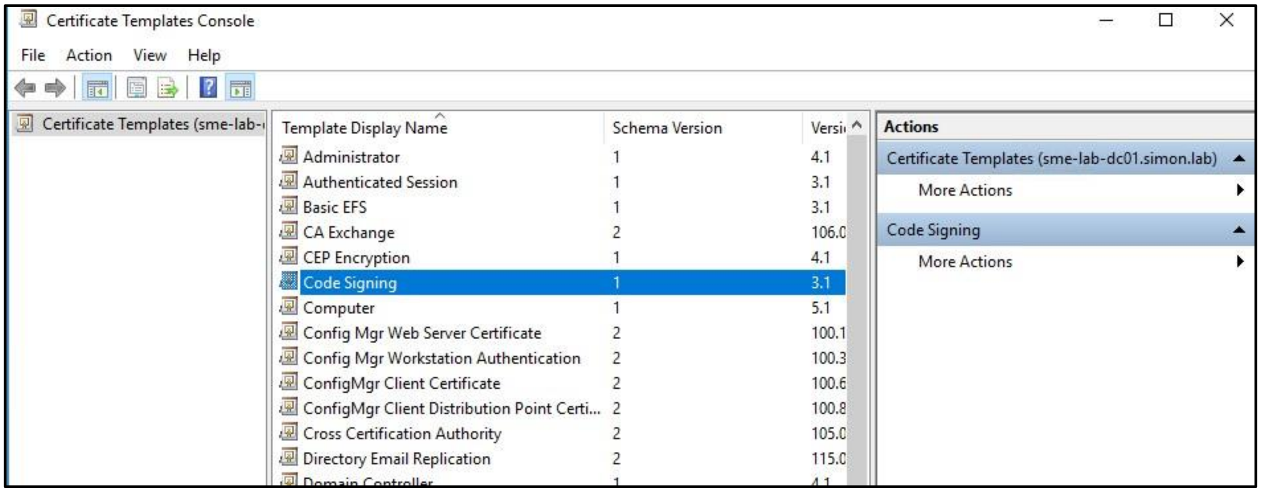


Name	Intended Purpose
Code Signing	Code Signing
Config Mgr Workstation Authenticati...	Client Authentication
Config Mgr Web Server Certificate	Server Authentication
ConfigMgr Client Distribution Point ...	Client Authentication
ConfigMgr Client Certificate	Client Authentication
e request)	IP security IKE intermediate
on	Certificate Request Agent
rollment Agent (Offline r...	Certificate Request Agent
ail Replication	Directory Service Email Replication
troller Authentication	Client Authentication, Server Authentic...
thentication	Client Authentication, Server Authentic...
Agent	File Recovery
	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...

Now click on “Manage” and this will bring up the Certificate Templates Console

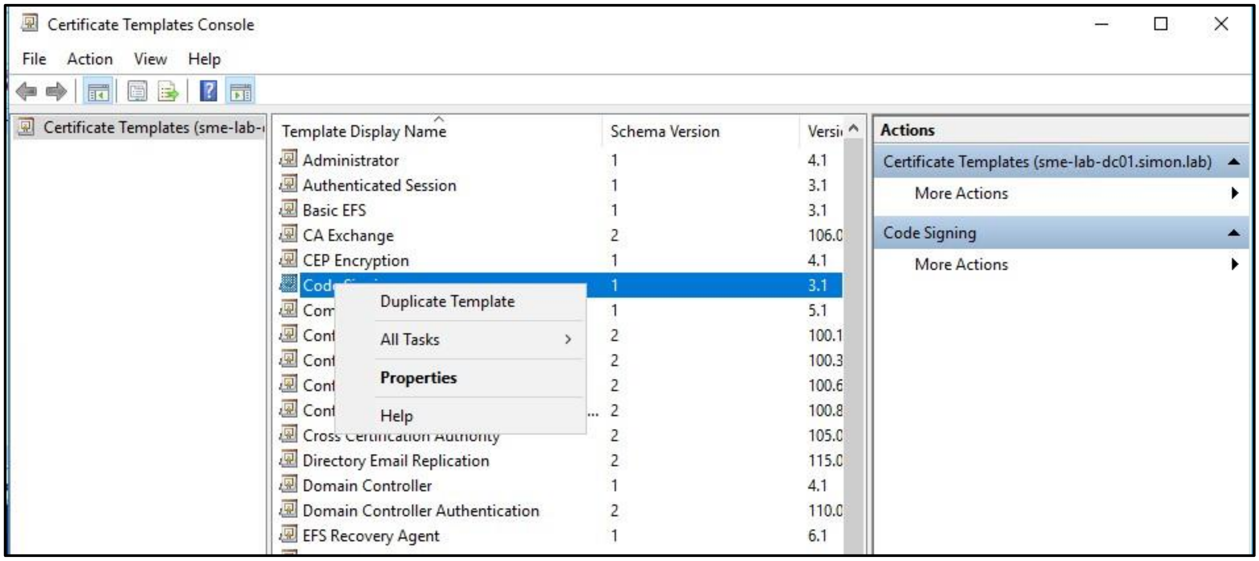
3.0 Certificate Template Console

Once the Template console has loaded look for the Code Signing template that is in the Templates list


Certificate Templates Console
File
Action
View
Help
Certificate Templates (sme-lab-
Actions
Certificate Templates (sme-lab-dc01.simon.lab)
More Actions
Code Signing
More Actions

Template Display Name	Schema Version	Versi
Administrator	1	4.1
Authenticated Session	1	3.1
Basic EFS	1	3.1
CA Exchange	2	106.0
CEP Encryption	1	4.1
Code Signing	1	3.1
Computer	1	5.1
Config Mgr Web Server Certificate	2	100.1
Config Mgr Workstation Authentication	2	100.3
ConfigMgr Client Certificate	2	100.6
ConfigMgr Client Distribution Point Certi...	2	100.8
Cross Certification Authority	2	105.0
Directory Email Replication	2	115.0
Domain Controller	1	4.1

Right Click on the Code Signing Template, and select “Duplicate Template” as shown below

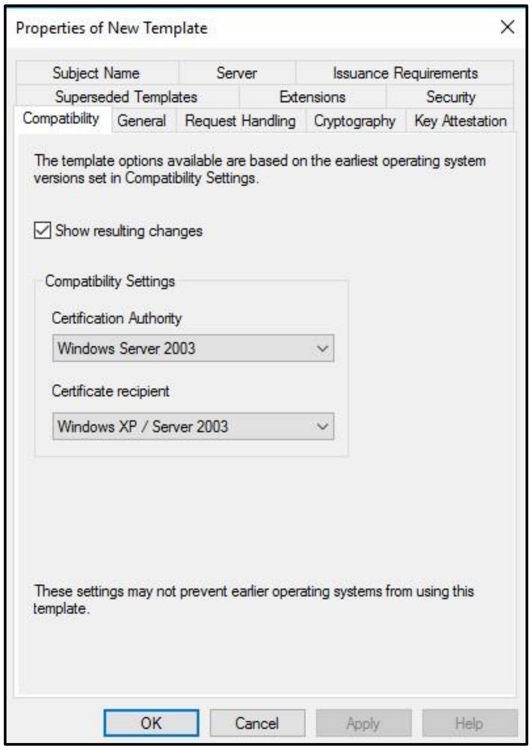

Certificate Templates Console
File
Action
View
Help
Certificate Templates (sme-lab-
Duplicate Template
All Tasks
Properties
Help
Actions
Certificate Templates (sme-lab-dc01.simon.lab)
More Actions
Code Signing
More Actions

Template Display Name	Schema Version	Versi
Administrator	1	4.1
Authenticated Session	1	3.1
Basic EFS	1	3.1
CA Exchange	2	106.0
CEP Encryption	1	4.1
Cod	1	3.1
Com	1	5.1
Conf	2	100.1
Conf	2	100.3
Conf	2	100.6
Conf	2	100.8
Cross Certification Authority	2	105.0
Directory Email Replication	2	115.0
Domain Controller	1	4.1
Domain Controller Authentication	2	110.0
EFS Recovery Agent	1	6.1

Once you click Duplicate Template, the template configuration will display.

3.1 Certificate Template Configuration

There are several tabs within the template configuration that you need to set the first tab to pop up will be the compatibility tab as below:-



The template options available are based on the earliest operating system versions set in Compatibility Settings.

☑ Show resulting changes

Compatibility Settings

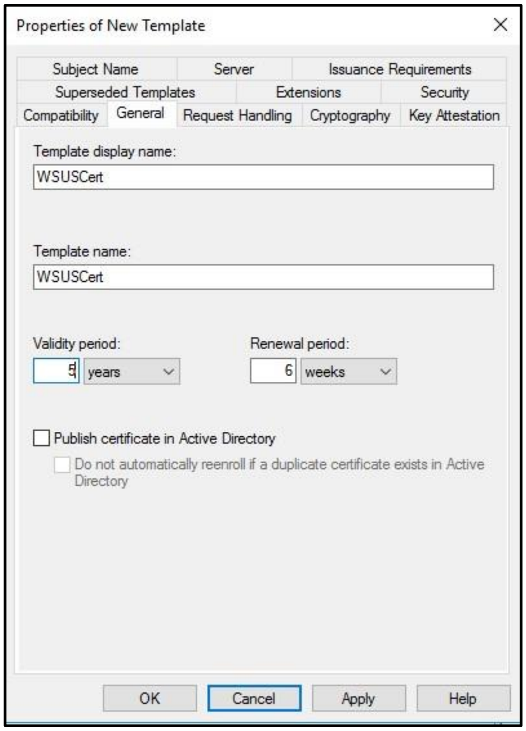
Certification Authority: Windows Server 2003

Certificate recipient: Windows XP / Server 2003

These settings may not prevent earlier operating systems from using this template.

Compatibility Tab

- No changes are required on this tab, please click on the general tab and see below
- Click on Apply



Template display name: WSUSCert

Template name: WSUSCert

Validity period: 5 years

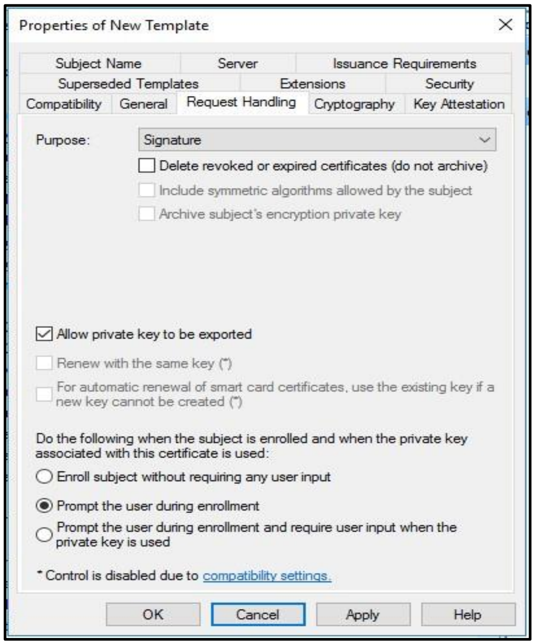
Renewal period: 6 weeks

☐ Publish certificate in Active Directory

☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

General Tab

- Give the certificate template a name, in this case, I have just used “WSUSCert” as the name.
- Set the validity period. I have used 5 years, but this can be set to a period of your choice, it makes sense to use a long validity time as this ensures all your published patches will continue to work for a long period.
- Click on Apply



Properties of New Template

Purpose: Signature

□ Delete revoked or expired certificates (do not archive)

□ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

☑ Allow private key to be exported

□ Renew with the same key (*)

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

○ Enroll subject without requiring any user input

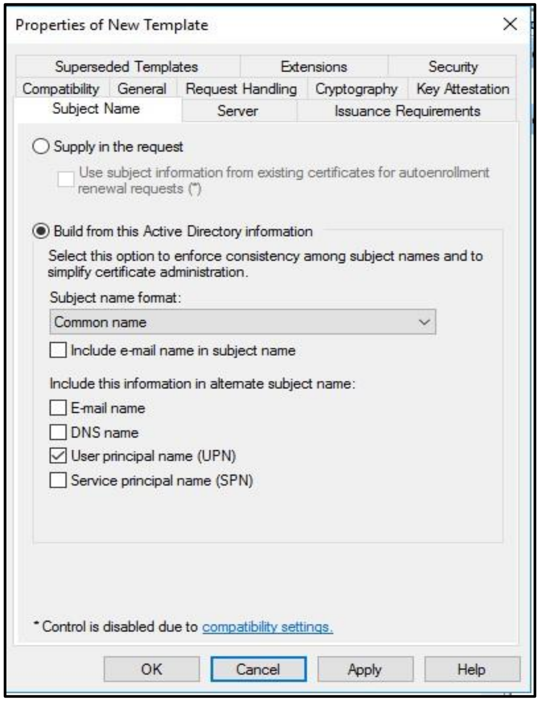
● Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to compatibility settings.

Request Handling

- Check Allow Private Key to be exported, **this is very important that it is ticked.**
- And select "Prompt the user during enrollment"
- Click on Apply



Properties of New Template

○ Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests (*)

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format: Common name

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

□ DNS name

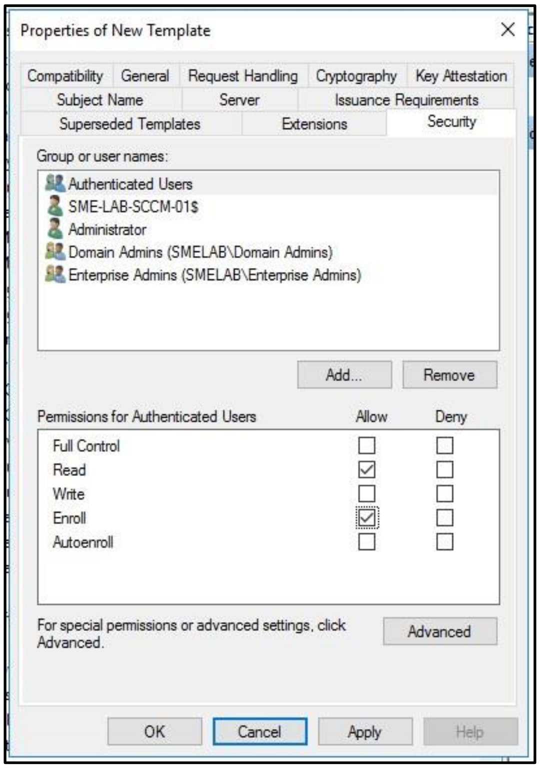
☑ User principal name (UPN)

□ Service principal name (SPN)

* Control is disabled due to compatibility settings.

Subject Name

- Select "Common Name" in "Subject name format"
- Only select UPN in the checkboxes below
- Click on Apply



Group or user names:

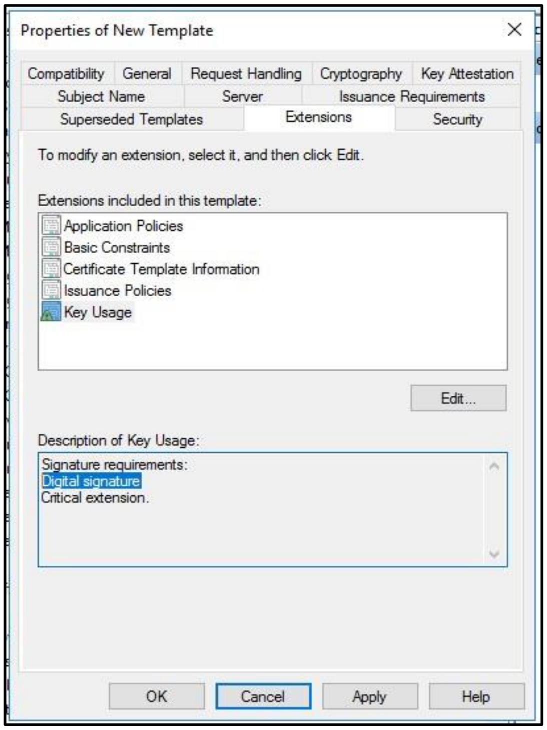
- Authenticated Users
- SME-LAB-SCCM-01$
- Administrator
- Domain Admins (SMELAB\Domain Admins)
- Enterprise Admins (SMELAB\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

For special permissions or advanced settings, click Advanced.

Security Tab

- Make sure you allocate permissions for a specific user or user group to be able to Read & Enroll, this example shows authenticated users with these permissions
- Click Apply



To modify an extension, select it, and then click Edit.

Extensions included in this template:

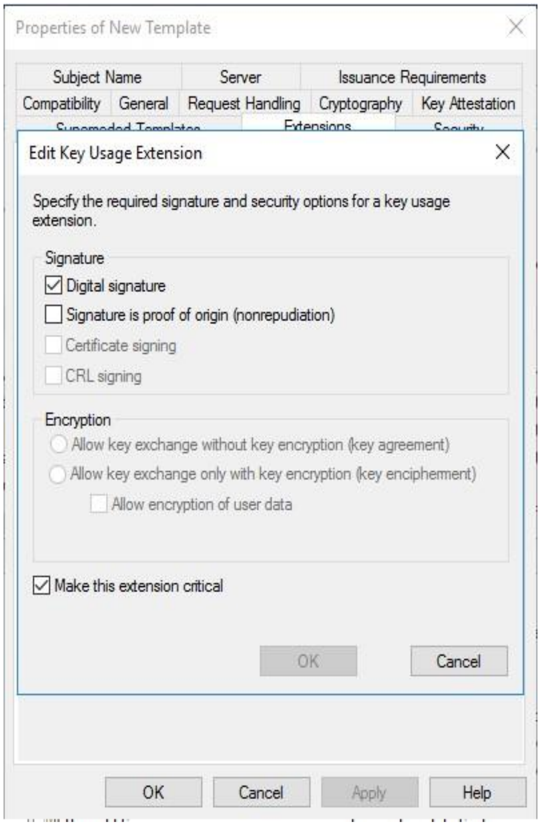
- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Key Usage:

Signature requirements:
Digital signature
Critical extension.

Extensions Tab

- Select Key Usage and then edit and see the next screen.



Edit Key Usage Extension

Specify the required signature and security options for a key usage extension.

Signature

☑ Digital signature

□ Signature is proof of origin (nonrepudiation)

□ Certificate signing

□ CRL signing

Encryption

○ Allow key exchange without key encryption (key agreement)

○ Allow key exchange only with key encryption (key encipherment)

□ Allow encryption of user data

☑ Make this extension critical

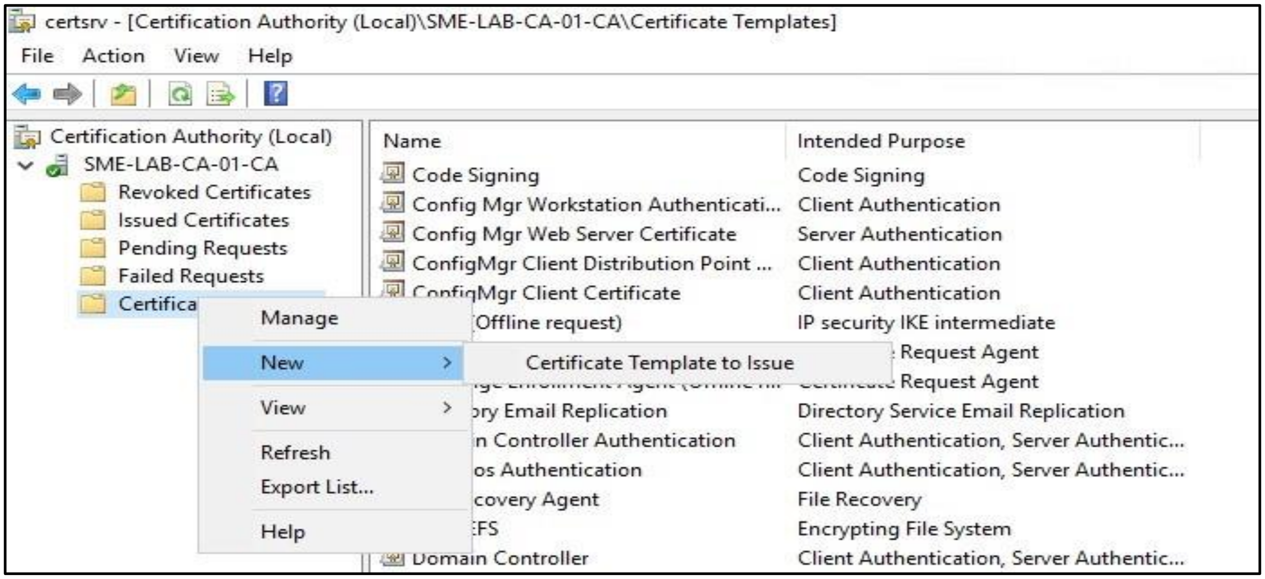
Edit Key Usage

- Make sure that “Digital Signature” & “Make this Extension Critical” are both checked
- Click Ok on the box, or cancel if no changes need to be made.
- Click on Apply on the Extensions Tab

Once this part is complete you can now close the Certificate Templates console, and return to the CA Console, the next part is we need to issue the template so that it becomes available to the users to be able to request a certificate.

3.2 Certificate Authority Console – Issuing Template.

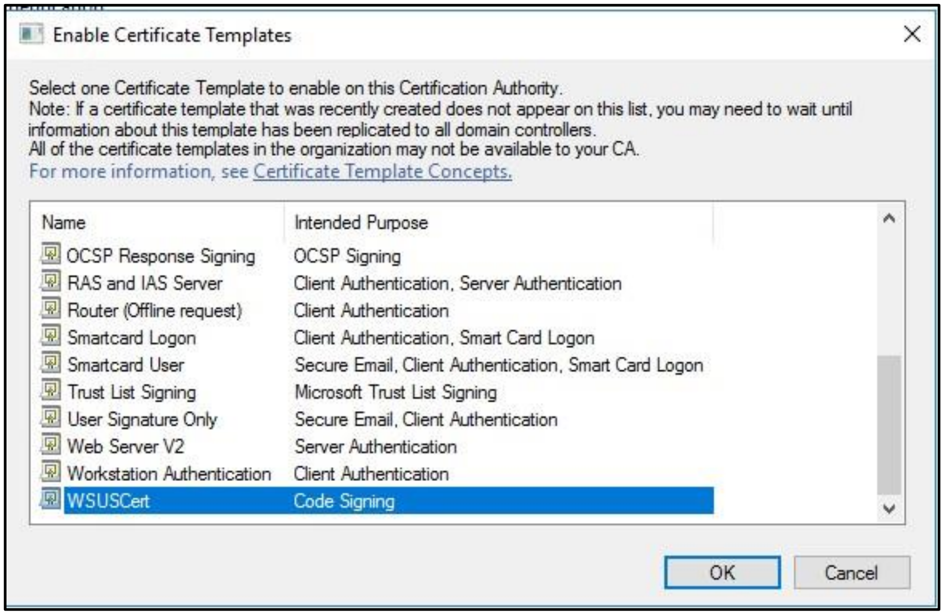
Right click on the Certificate Templates, Select New then select Certificate Template to Issue



Name	Intended Purpose
Code Signing	Code Signing
Config Mgr Workstation Authenticati...	Client Authentication
Config Mgr Web Server Certificate	Server Authentication
ConfigMgr Client Distribution Point ...	Client Authentication
ConfigMgr Client Certificate	Client Authentication
(Offline request)	IP security IKE intermediate
	: Request Agent
...ge Enrollment Agent (Offline ...	Certificate Request Agent
...ory Email Replication	Directory Service Email Replication
...n Controller Authentication	Client Authentication, Server Authentic...
...os Authentication	Client Authentication, Server Authentic...
...covery Agent	File Recovery
...FS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...

3.2 Certificate Templates - Issuing Template

Once you have selected New Certificate Template to Issue, the list of available templates will be displayed as per below, in the list find the name of the template you have just created, select it and click ok.

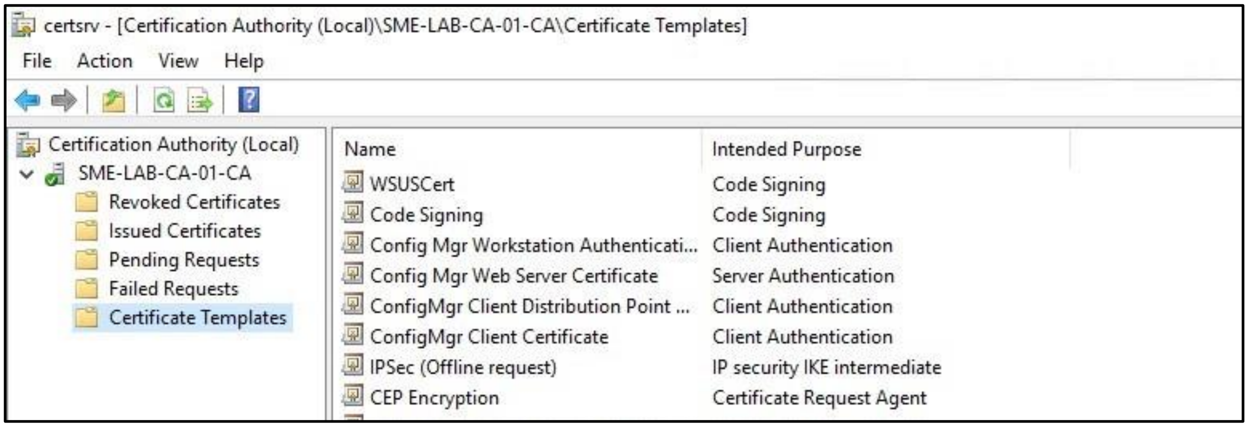


Enable Certificate Templates

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon
Trust List Signing	Microsoft Trust List Signing
User Signature Only	Secure Email, Client Authentication
Web Server V2	Server Authentication
Workstation Authentication	Client Authentication
WSUSCert	Code Signing

Your new template will now appear in the Certificate Templates container in the main Certification Authority Console



certsrv - [Certification Authority (Local)\SME-LAB-CA-01-CA\Certificate Templates]

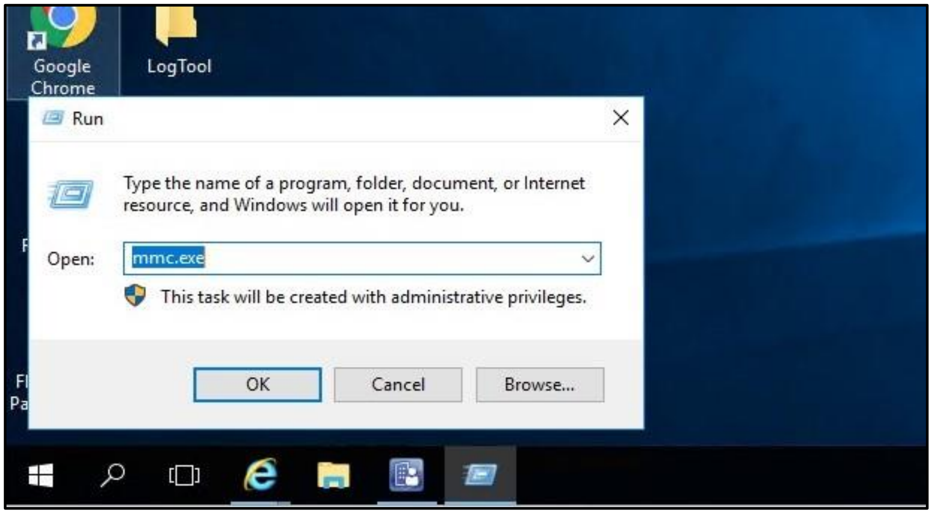
Name	Intended Purpose
WSUSCert	Code Signing
Code Signing	Code Signing
Config Mgr Workstation Authenticati...	Client Authentication
Config Mgr Web Server Certificate	Server Authentication
ConfigMgr Client Distribution Point ...	Client Authentication
ConfigMgr Client Certificate	Client Authentication
IPSec (Offline request)	IP security IKE intermediate
CEP Encryption	Certificate Request Agent

This completes what needs to be done on the CA, you can now log off your CA Server as you should not need to connect to it again during this process unless you have a domain certificate policy that requires Certificates to be approved on the CA.

4.0 Requesting a WSUS Code Signing Certificate

The next part needs you to log on to your WSUS Server, the first thing that we need to do is to open an MMC Console.

Right Click on the Start menu and select run

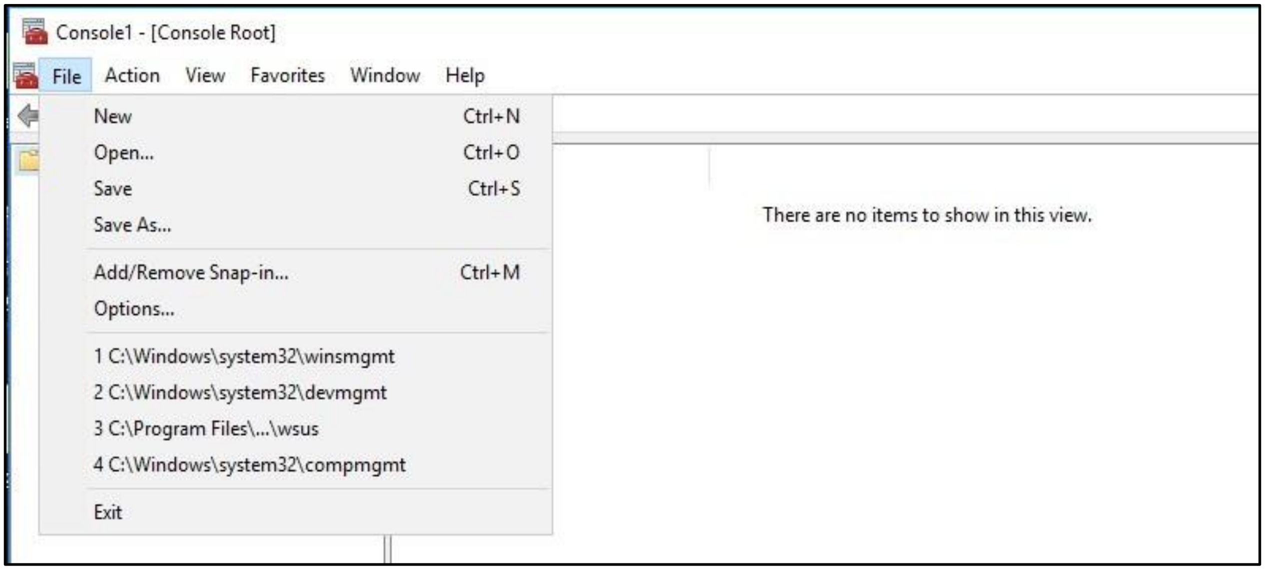


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc.exe

This task will be created with administrative privileges.

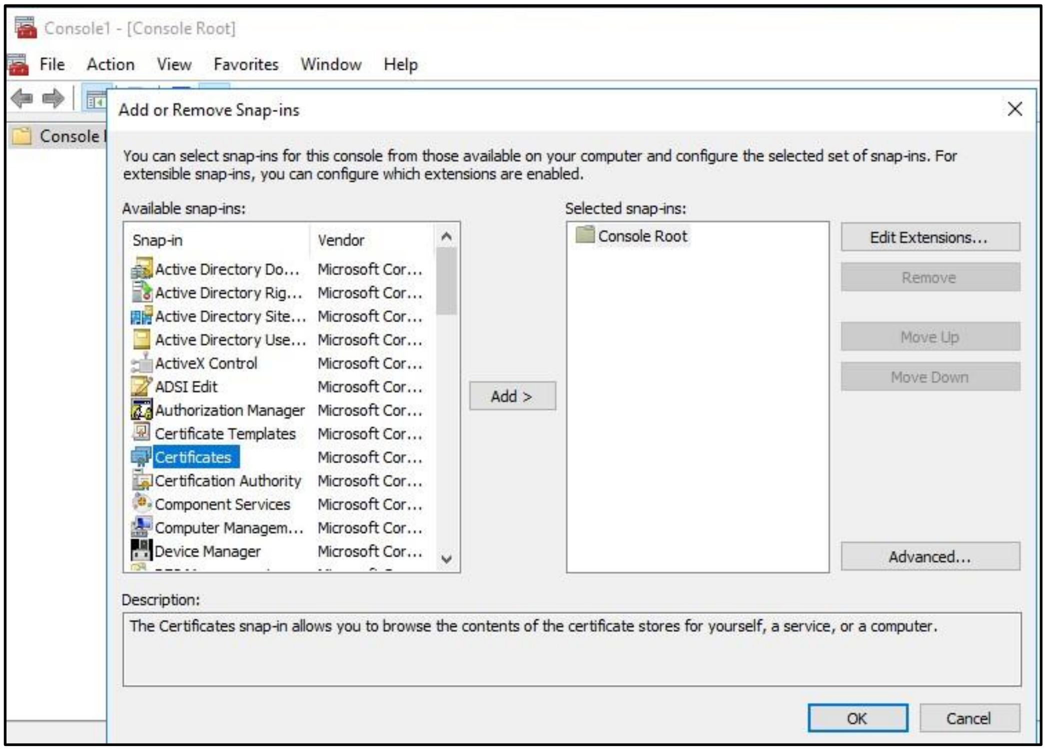
When the MMC Console has started, select File then Add/Remove Snap-in


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\system32\winsmgmt
2 C:\Windows\system32\devmgmt
3 C:\Program Files\...\wsus
4 C:\Windows\system32\compmgmt
Exit

There are no items to show in this view.

4.1 Adding the certificates Snap-in

Add the Certificates snap-in



Console1 - [Console Root]
File Action View Favorites Window Help
Console I
Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Rig...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...

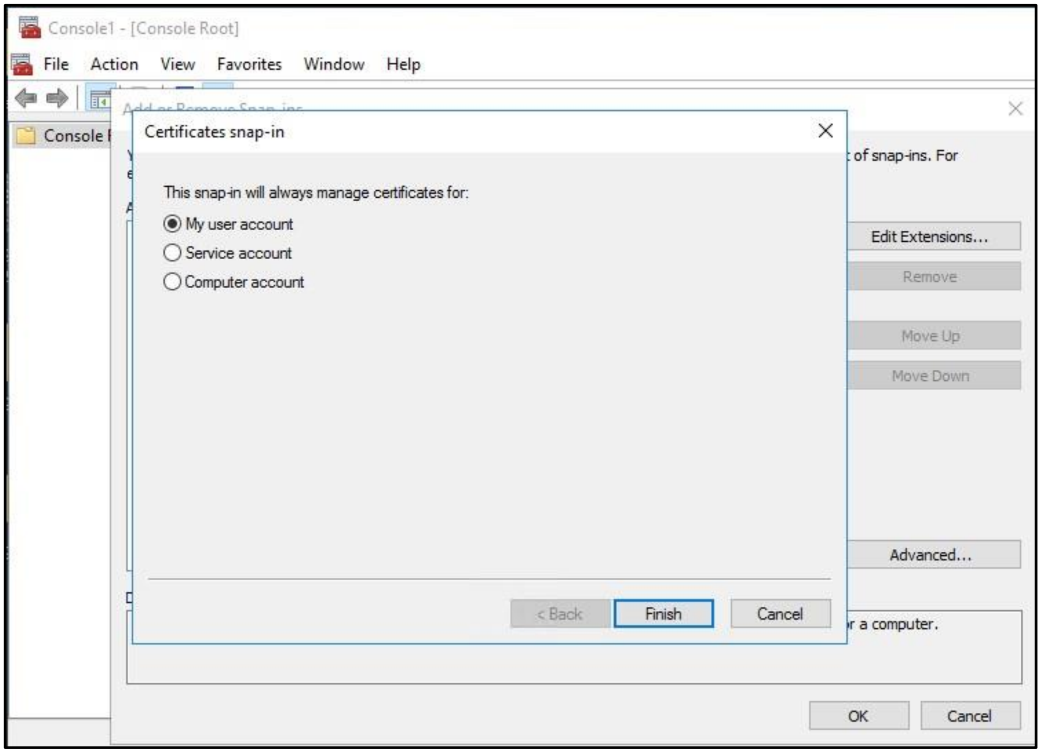
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Check “My User Account” and click “Finish”



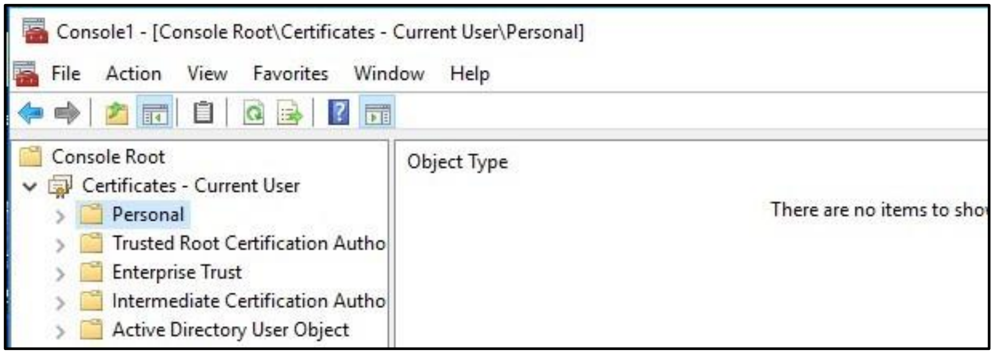
Console1 - [Console Root]
File Action View Favorites Window Help
Console I
Add or Remove Snap-ins
Certificates snap-in

This snap-in will always manage certificates for:

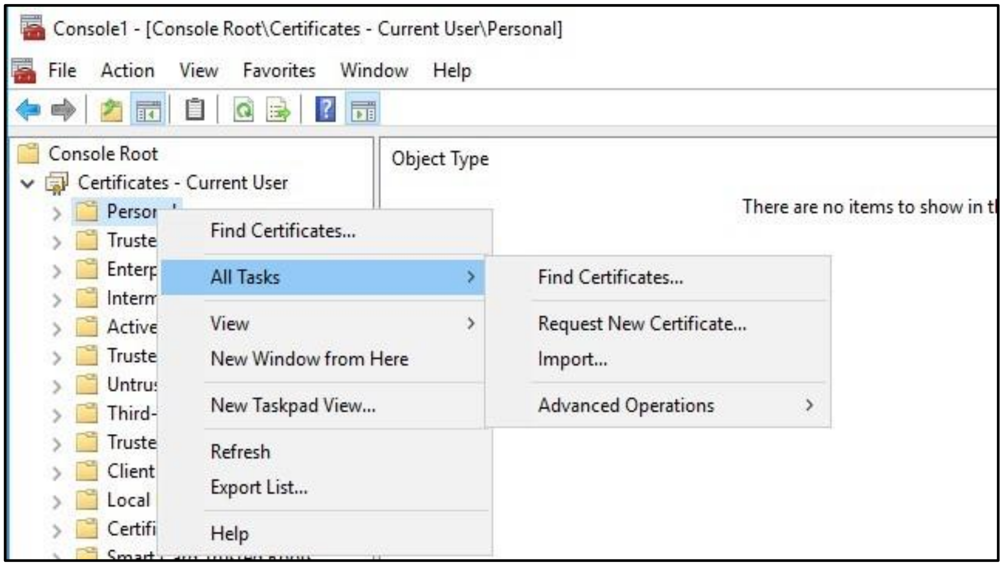
● My user account
○ Service account
○ Computer account

4.2 Requesting the Code Signing Certificate

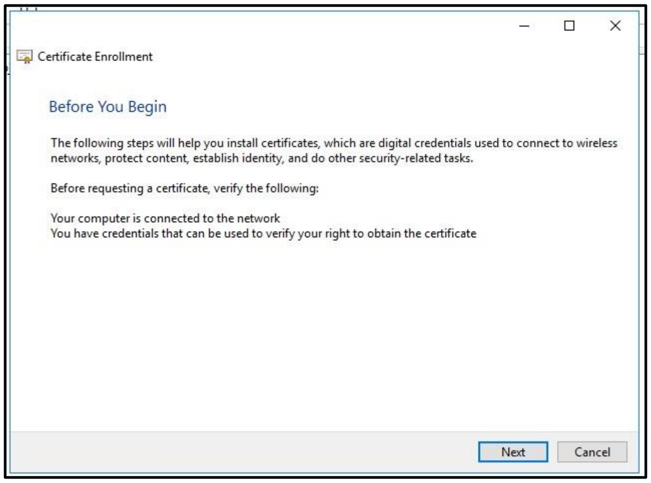
To request the certificate, first select the “Personal” folder in the left-hand pane of the Certificates console.


Console1 - [Console Root\Certificates - Current User\Personal]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification Autho
Enterprise Trust
Intermediate Certification Autho
Active Directory User Object
Object Type
There are no items to sho

Right click on the “Personal” folder and select “Request New Certificate”



The certificate enrollment Wizard will now start, once the following screen appears click “Next”



Before You Begin

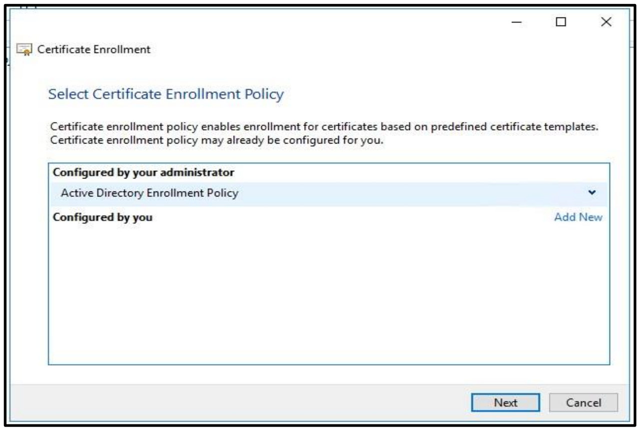
The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate

4.2 Requesting the Code Signing Certificate

By default the Active Directory Enrollment Policy is present, you should not need to make any changes on this section, please click “Next


Certificate Enrollment

Select Certificate Enrollment Policy

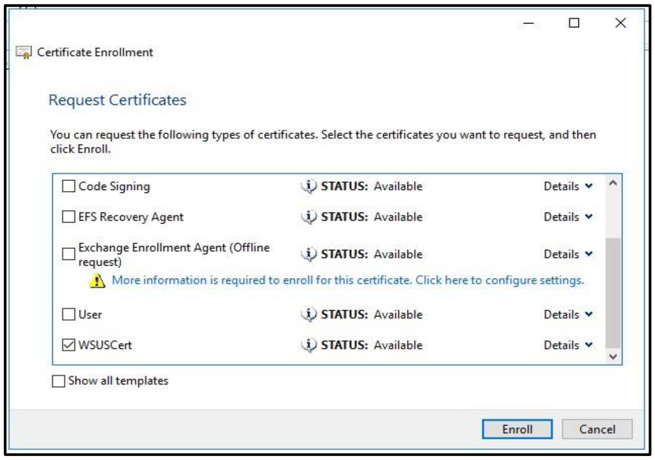
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy

Configured by you

When the types of certificates box appear, look for the Certificate Template you created earlier on the CA, and Check the Template, it should be showing as per the box below. Click on “Enroll”


Certificate Enrollment

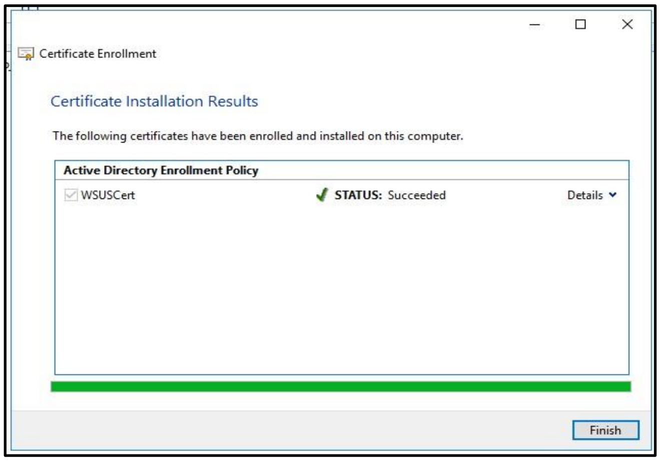
Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

- □ Code Signing — **STATUS:** Available — Details
- □ EFS Recovery Agent — **STATUS:** Available — Details
- □ Exchange Enrollment Agent (Offline request) — **STATUS:** Available — Details
  - More information is required to enroll for this certificate. Click here to configure settings.
- □ User — **STATUS:** Available — Details
- ☑ WSUSCert — **STATUS:** Available — Details

□ Show all templates

When you have clicked Enroll you will be shown the results of your request, it should show succeeded.


Certificate Enrollment

Certificate Installation Results

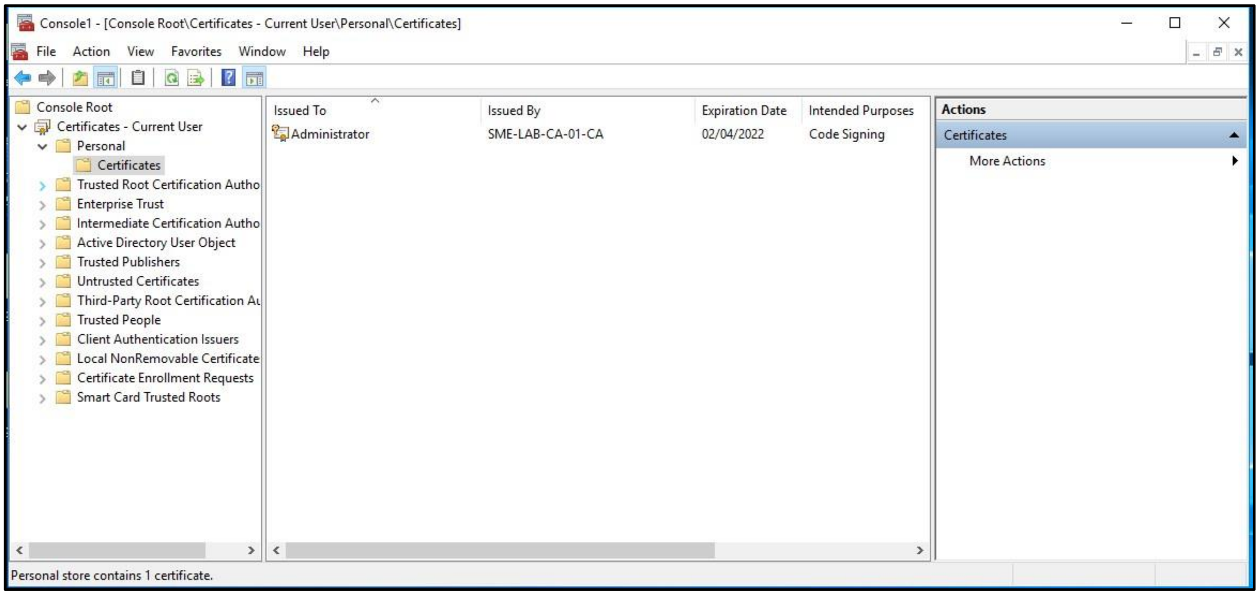
The following certificates have been enrolled and installed on this computer.

Active Directory Enrollment Policy

☑ WSUSCert — ✓ **STATUS:** Succeeded — Details

4.2 Requesting the Code Signing Certificate

Your new Code Signing Certificate will now appear in the “Personal\Certificates” folder as below



Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

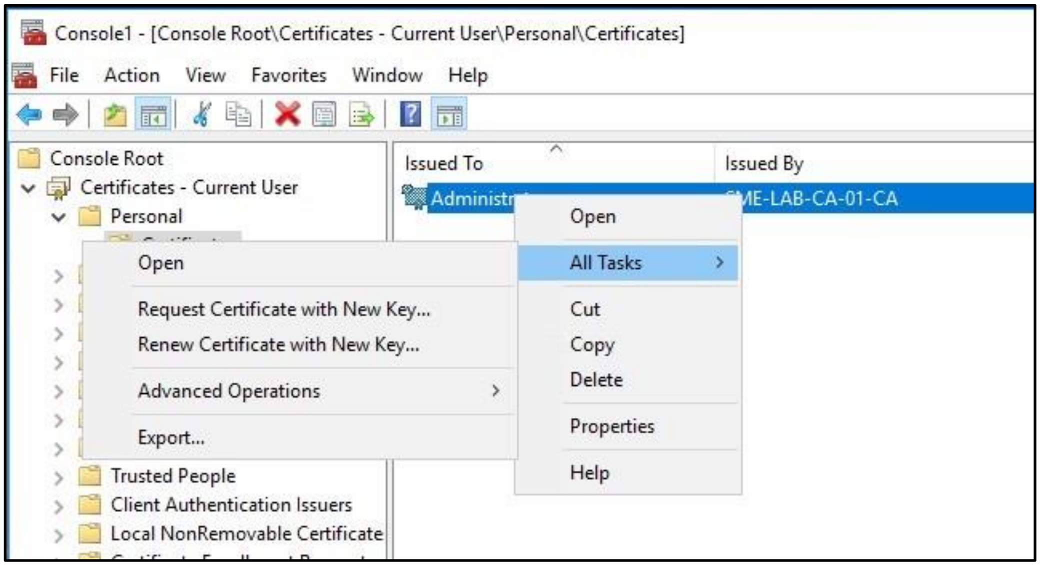
Issued To	Issued By	Expiration Date	Intended Purposes
Administrator	SME-LAB-CA-01-CA	02/04/2022	Code Signing

Personal store contains 1 certificate.

File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Autho
Enterprise Trust
Intermediate Certification Autho
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Client Authentication Issuers
Local NonRemovable Certificate
Certificate Enrollment Requests
Smart Card Trusted Roots
Actions
Certificates
More Actions

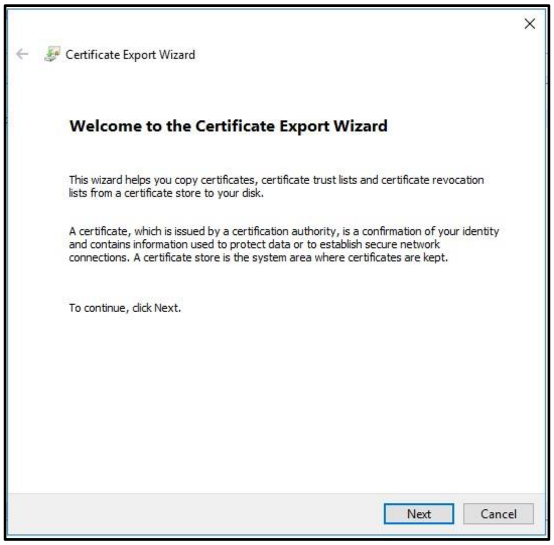
5.0 Exporting the Certificate.

The next part of the process we need to export the certificate to a file along with its private key, click on certificate to select it then right click, and select “All Tasks” then “Export”



Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

5.1 Certificate Export Wizard.



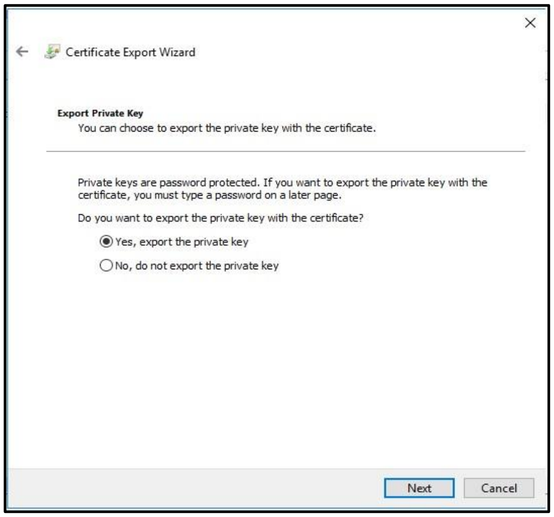
Welcome to the Certificate Export Wizard

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

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.

To continue, click Next.

- To continue, click “Next”



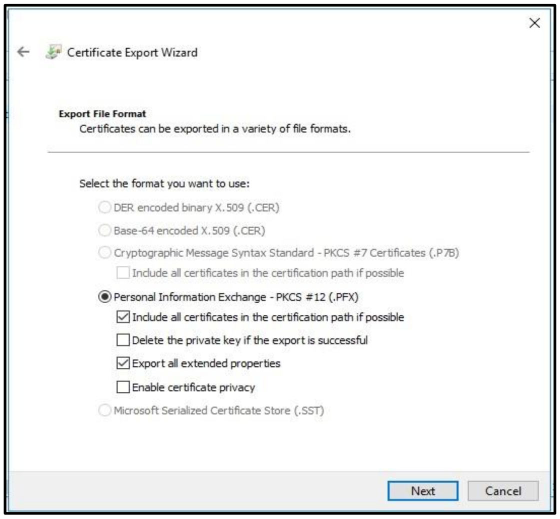
Export Private Key
You can choose to export the private key with the certificate.

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

- Select “Yes, export the Private Key”
- Click “Next”



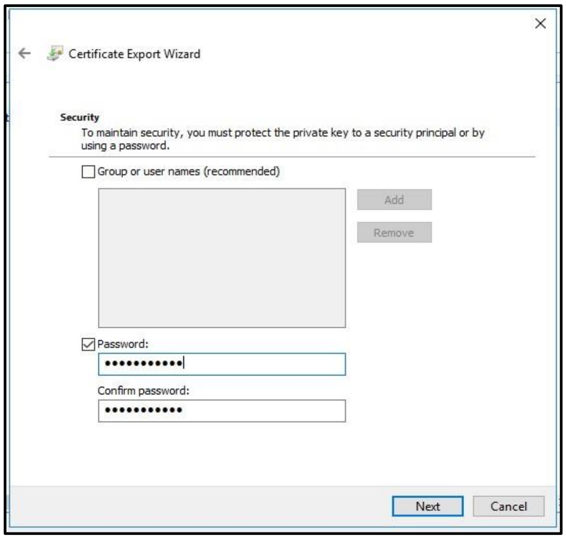
Export File Format
Certificates can be exported in a variety of file formats.

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)

- Make sure “Include all certificates in the certification path” is selected.
- Make sure “Export all Extended Properties is selected.

5.1 Certificate Export Wizard.



Security

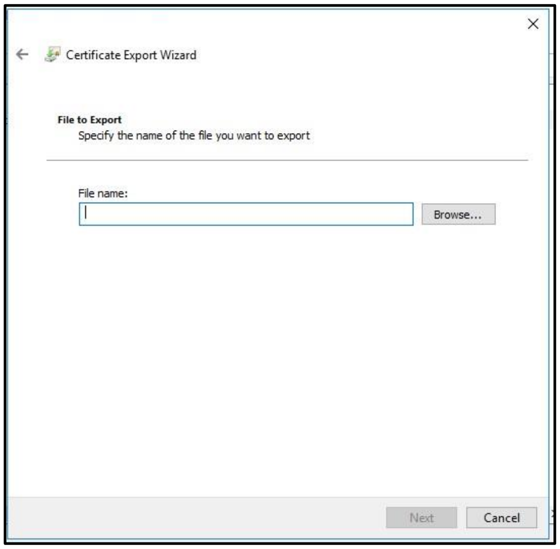
To maintain security, you must protect the private key to a security principal or by using a password.

☐ Group or user names (recommended)

☑ Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

- Type a password and confirm it and Click “Next”

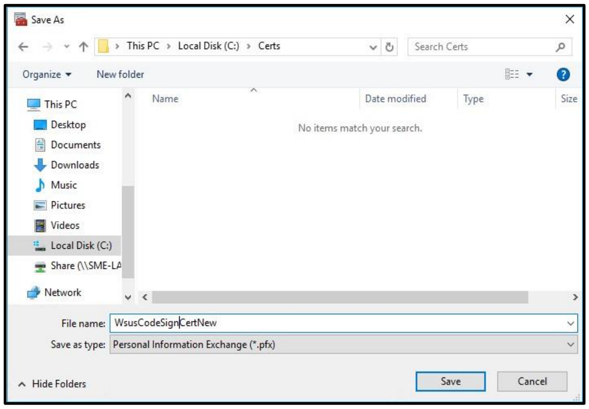


File to Export

Specify the name of the file you want to export

File name:

- Click “Browse”



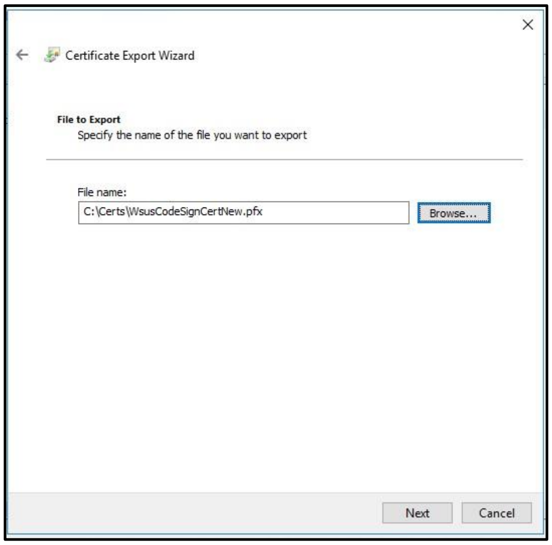
No items match your search.

File name: WsusCodeSignCertNew

Save as type: Personal Information Exchange (*.pfx)

- Select a location to save the certificate, I would suggest creating a folder on C:\ and saving it there.

5.1 Certificate Export Wizard.



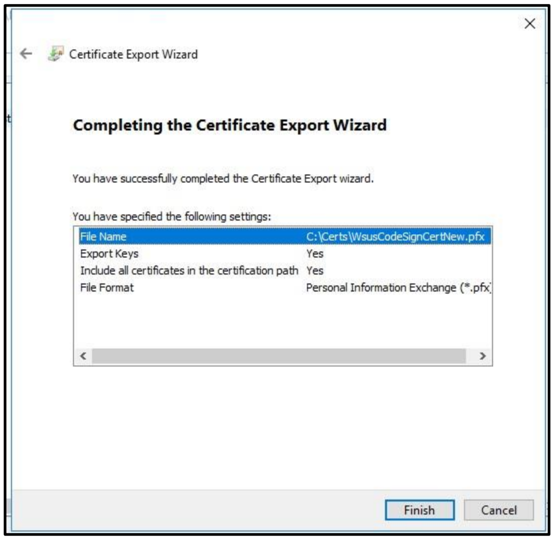
File to Export

Specify the name of the file you want to export

File name:

C:\Certs\WsusCodeSignCertNew.pfx

With the filename and path completed click "Next"



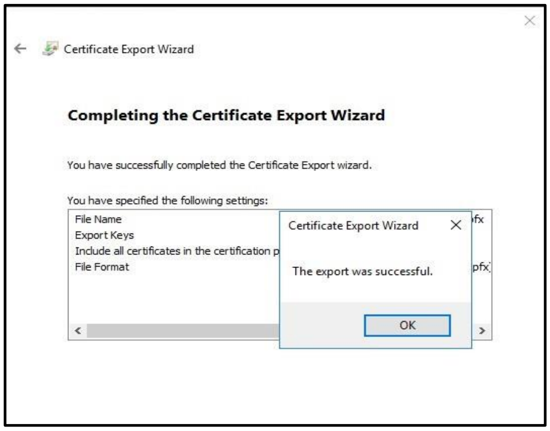
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Certs\WsusCodeSignCertNew.pfx
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Personal Information Exchange (*.pfx)

Check what is displayed looks ok and click "Finish"



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name

Export Keys

Include all certificates in the certification p

File Format

The export was successful.

- You should now get a message saying that your Certificate Export was successful

6.0 Importing Certificate into WSUS / SCUP

PKI generated certificates can only be imported into WSUS using a PowerShell Script

Open up Powershell as Administrator on your WSUS Server.

1. Open up PowerShell as Administrator on your WSUS server, or Software Update Point of SCCM.
2. Run the following to set the WSUS server and its configuration to an object.

```
[Reflection.Assembly]::LoadWithPartialName("Microsoft.UpdateServices.Administration")

$updateServer = [Microsoft.UpdateServices.Administration.AdminProxy]::GetUpdateServer()

$config = $updateServer.GetConfiguration()
```

3. Next, run this snippet to set the new code signing certificate.

```
$config.SetSigningCertificate("<Path to pfxFile>", "<PFX file password>")
```

Bear in mind, this will be a file with both the public and private keys (pfx usually). You'll need to replace the path and private key password within the placeholder values in quotes.

4. Now save the changes.

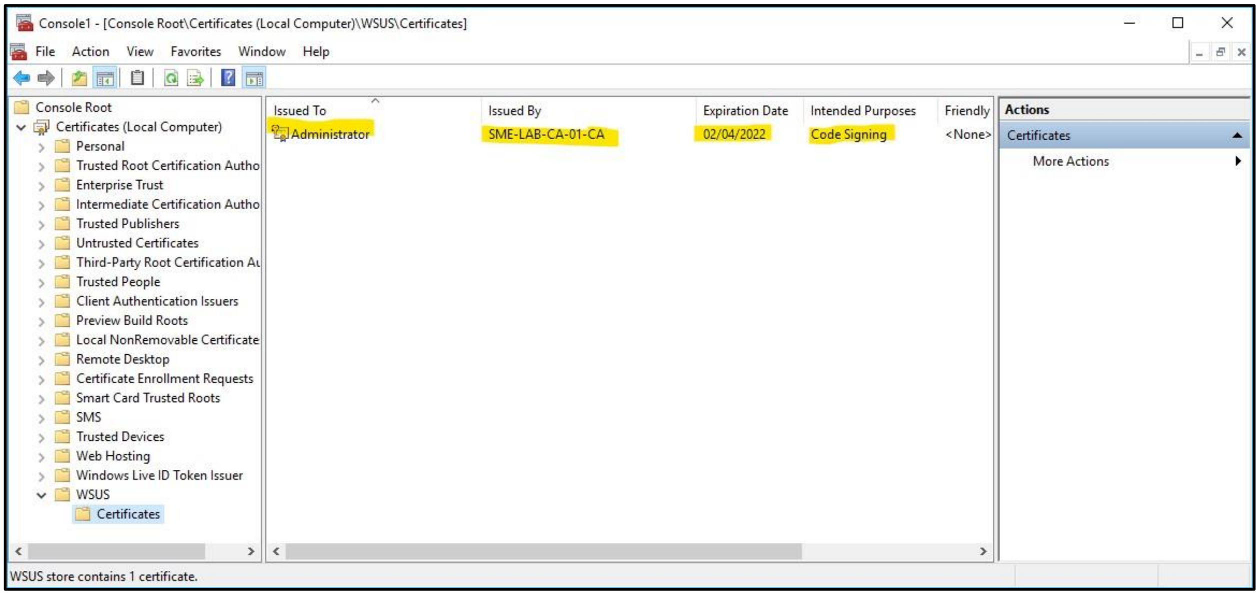
```
$config.Save()
```

You will need to resync your Software Update Point to make the certificate display in the SCUP Configuration.

7.0 Troubleshooting

Certificate Stores (WSUS Server)

If you have been running with a WSUS Self Signed Certificate and are looking to move to using a PKI Certificate generated from your Enterprise Windows CA, once you have installed the certificate as above, please check the WSUS Certificate Store for the Local Computer Account, to make sure you are only showing the one certificate in the WSUS Certificate in this store and this should be the Certificate you have generated from your CA this Certificate should should show you have the Private Key that corresponds to the certificate, there should be no other certificates in this store, also check that the certificate is appearing in Trusted Publishers without the Private Key.

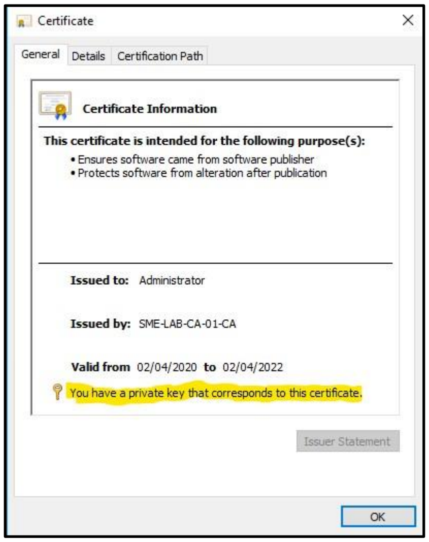


Console1 - [Console Root\Certificates (Local Computer)\WSUS\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly
Administrator	SME-LAB-CA-01-CA	02/04/2022	Code Signing	<None>

WSUS store contains 1 certificate.

WSUS Certificate store for Local Computer Account



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

Issued to: Administrator

Issued by: SME-LAB-CA-01-CA

Valid from 02/04/2020 **to** 02/04/2022

You have a private key that corresponds to this certificate.

Showing Private Key

7.0 Troubleshooting.

Software Update Point

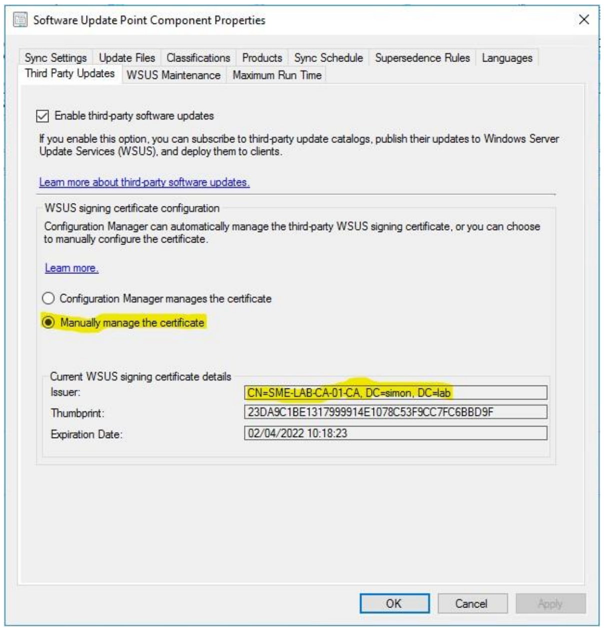
If you are having difficulties with syncronisation, sometimes this can be caused by the software update point not importing the certificate into the SCUP which it does during syncronisation.

To resolve this you need to open the SUP and remove all the classifications, then resync the SUP it might take a couple of goes to get it to work, it will start a sync import the certificate as there are no classifications to sync.

You can check that the certificate is the correct one by checking the Third Party Updates tab in the SCUP configuration to see if the certificate has changed to the correct one.

Once it appears re-enable your classification and resync the SCUP.

The two logs to check for the above issues are “wsyncmgr.log” and “wcm.log”



☑ Enable third-party software updates

If you enable this option, you can subscribe to third-party update catalogs, publish their updates to Windows Server Update Services (WSUS), and deploy them to clients.

WSUS signing certificate configuration

Configuration Manager can automatically manage the third-party WSUS signing certificate, or you can choose to manually configure the certificate.

○ Configuration Manager manages the certificate

● Manually manage the certificate

Current WSUS signing certificate details

Issuer:	CN=SME-LAB-CA-01-CA, DC=simon, DC=lab
Thumbprint:	23DA9C1BE1317999914E1078C53F9CC7FC6BBD9F
Expiration Date:	02/04/2022 10:18:23

SCUP Showing PKI Certificate after Software Update Syncronisation