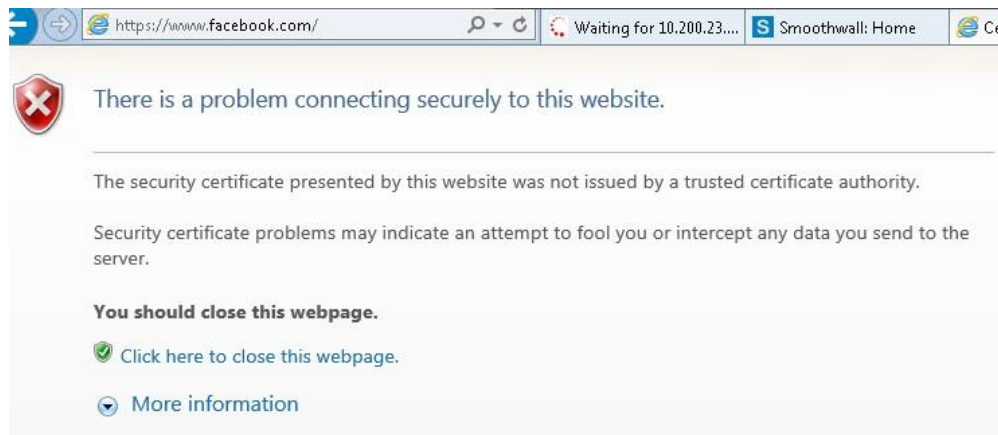


Smoothwall Certificate Guidance

A Smoothwall **root and intermediate** certificate must be installed on all devices requiring Internet access. If the Smoothwall certificates are not installed, users will receive an error/warning message similar to the one shown below when accessing content which is decrypted by Smoothwall. **This process is slightly different to previous years when only a root certificate was required.**



The Smoothwall certificates can be downloaded from the links below. Both certificates are in base64 format which can be opened and installed in most operating systems:

Schools Smoothwall root certificate 2025 – 2026

<https://sccwebassets.blob.core.windows.net/public/schools/smoothwall-2025-2027-root.cer>

Schools Smoothwall intermediate certificate 2025 – 2026

<https://sccwebassets.blob.core.windows.net/public/schools/smoothwall-2025-2027-intermediate.cer>

Note that the certificate is valid between Jan 2025 – Jan 2027 but due to Christmas we will need to replace again in December 2026. Two years is the maximum validity period recommended and officially supported by Smoothwall.

The following guidance to install the certificate in a Windows environment is provided as a supplement to information on the Smoothwall website.

Further links are available on the [Smoothwall site](#) for a variety of different web browsers and operating systems. If you require further assistance with installing the certificate, please contact your IT support company.

The instructions below include steps for:

- Page 2 - Installing the root and intermediate certificates on a standalone Windows computer
- Page 11 - Deploying the Smoothwall certificate to Windows computers via group policy
- Page 20 – Deploying the Smoothwall certificate to Windows computers using certutil dspublish

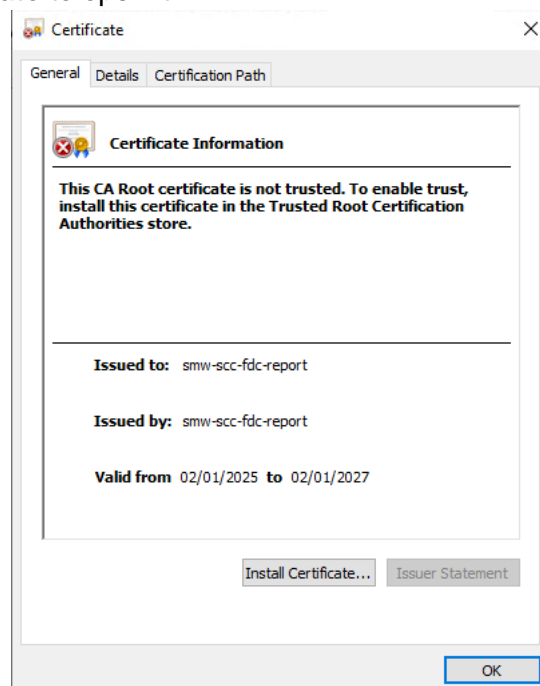
Installing the root and intermediate certificates on a standalone Windows computer

Note: the following steps must be performed by a user with Administrative rights, specifically the user must have permissions to add a certificate to the Trusted Root Certification Authorities store.

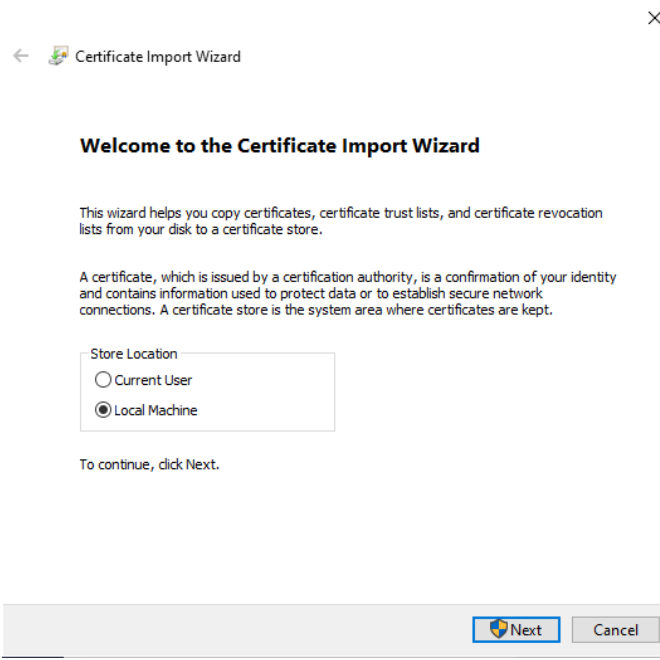
- 1) Download the Smoothwall root and intermediate certificates and save them to a suitable location. It is recommended that the file names are not changed as the root is required to be installed in the root store and the intermediate in the intermediate store (installing them in the wrong stores may result in SSL errors).

2) Installing the root certificate

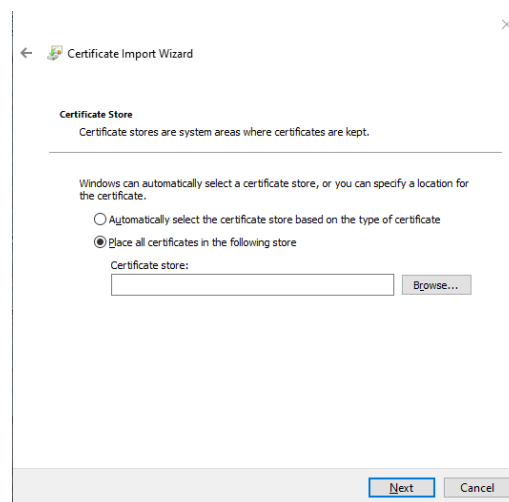
- a) Navigate to the location where you saved the Smoothwall certificates and double-click the **root certificate** to open it.



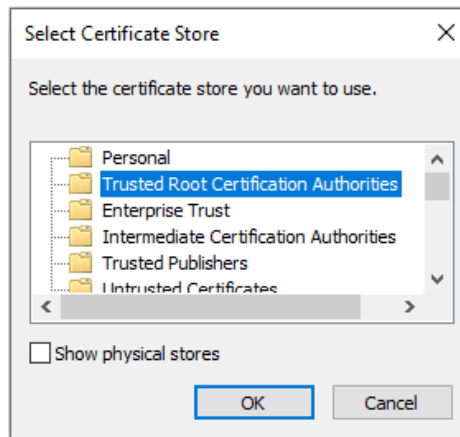
The certificate properties box will be displayed as shown above. Click on Install Certificate to start the Certificate Import Wizard.



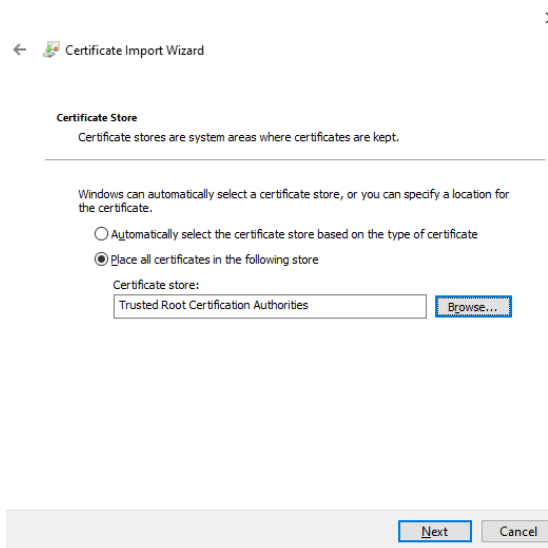
- b Select **Local Machine** and Click **Next**. You may need to enter a username and password which has permissions to add a certificate to the local machines certificate store.



- c Choose **Place the certificate in the following store** as shown above, then click **Browse**.



- d Choose the **Trusted Root Certification Authorities** folder. Click **OK**.



- e Ensure the Certificate store detailed in the **Completing the Certificate Import Wizard** is set to **Trusted Root Certification Authorities** as shown above, then click **Next**. *If not, click on **Browse** and review the selection, by repeating step 6. If you do not install the certificate in this certificate store, the Smoothwall Certificate will NOT function correctly.*

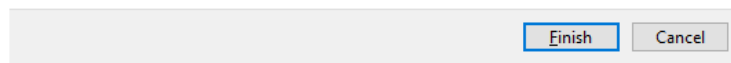


Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

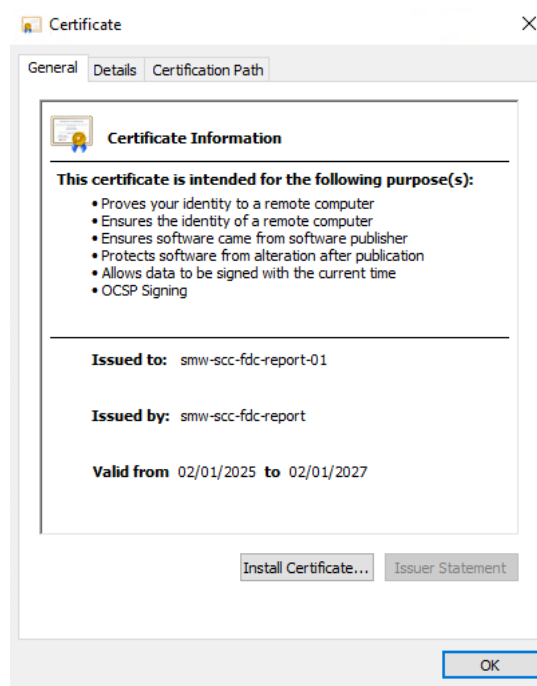
Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate



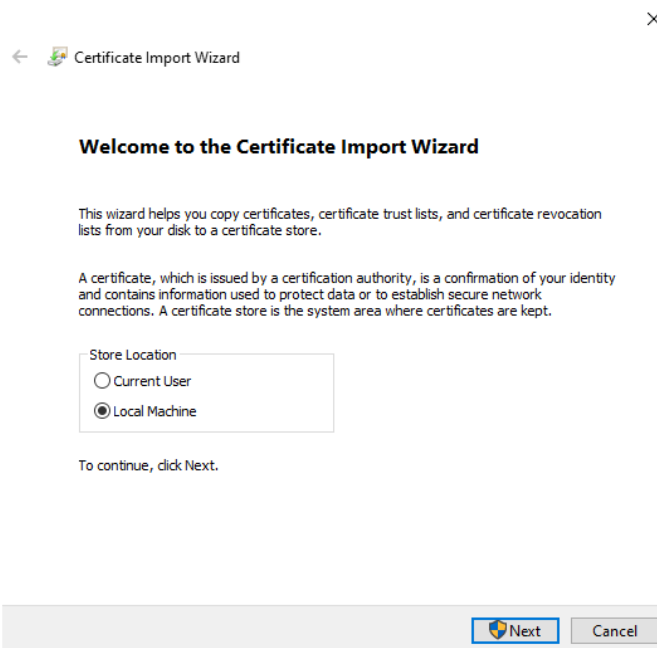
- f Click **Finish**.
- g On some older operating systems you may be prompted by a security warning. Click **Yes** to confirm you wish to install the certificate.
- h Click **OK** to close the Certificate Import Wizard.
- i Click **OK** to close the certificate.

3) Installing the intermediate certificate

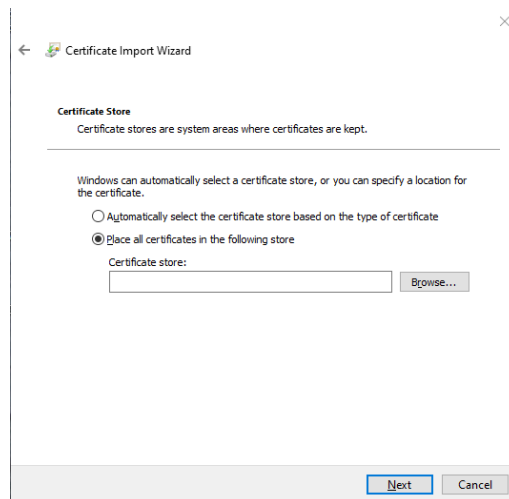
- a Navigate to the location where you saved the Smoothwall certificates and double-click the **intermediate certificate** to open it.



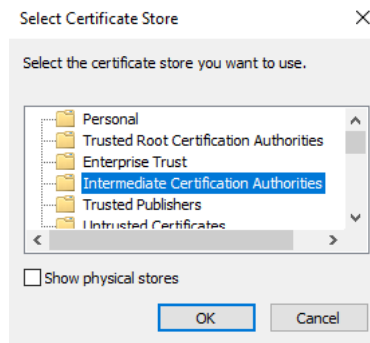
- b The certificate properties box will be displayed as shown above. Click on **Install Certificate** to start the **Certificate Import Wizard**.



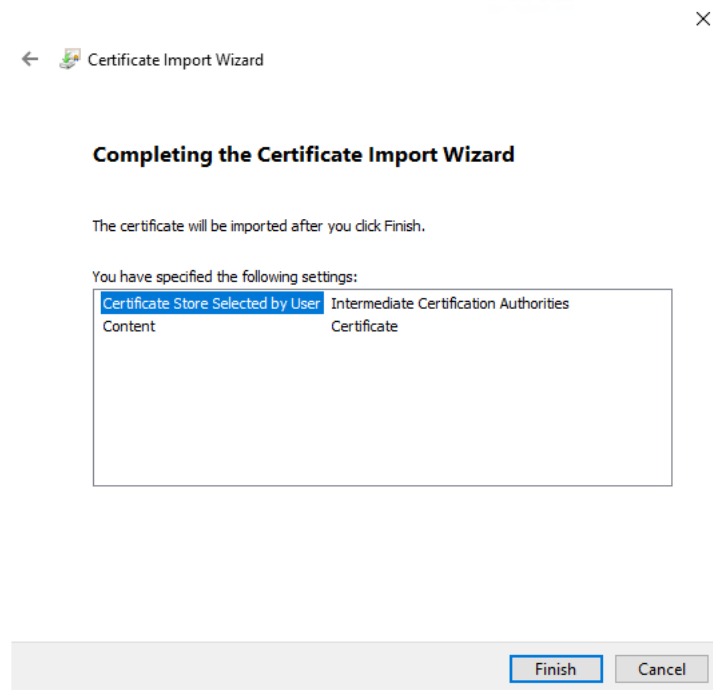
- c Select **Local Machine** and Click **Next**. You may need to enter a username and password which has permissions to add a certificate to the local machines certificate store.



- d Choose **Place the certificate in the following store** as shown above, then click **Browse**.



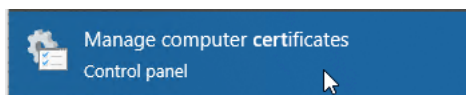
- e Choose the **Intermediate Certification Authorities** folder. Click **OK**.



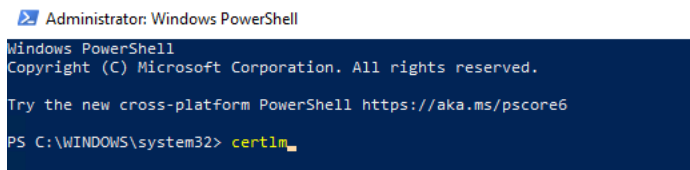
- f Ensure the Certificate store detailed in **Completing the Certificate Import Wizard** is set to **Intermediate Certification Authorities** as shown above, then click **Next**. *If not,*

click on **Browse** and review the selection, by repeating step 6. If you do not install the certificate in this certificate store, the Smoothwall Certificate will NOT function correctly.

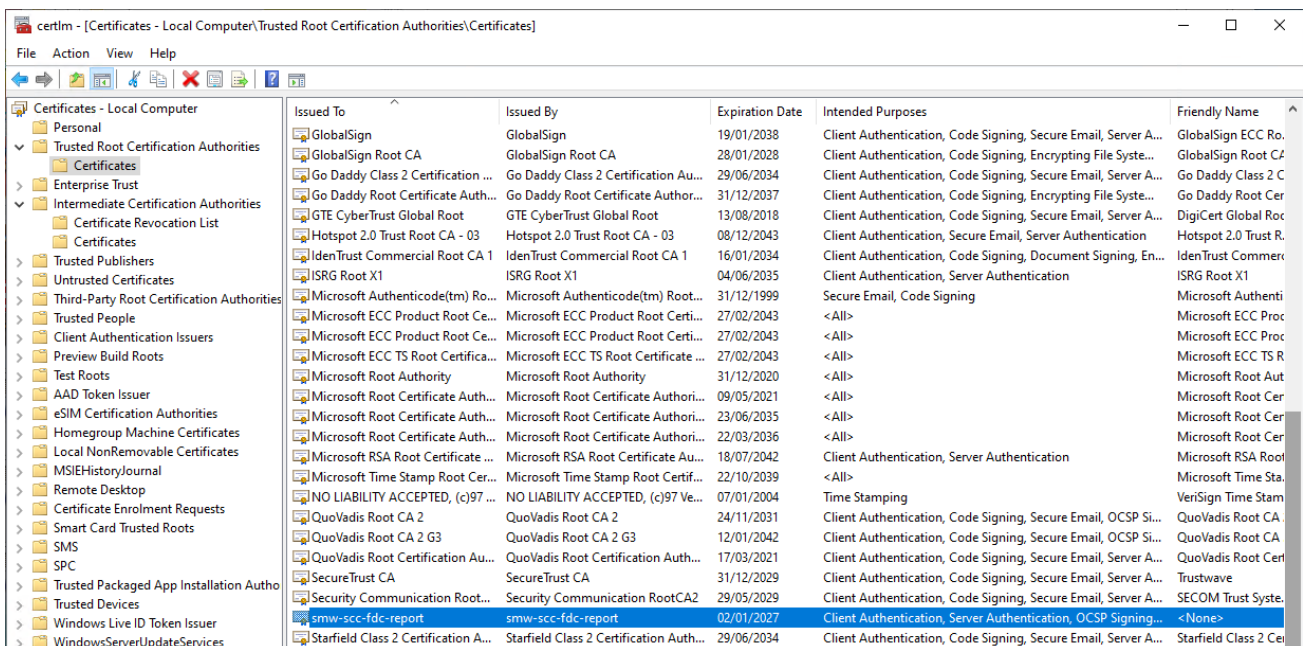
- g Click **Finish**.
 - h On some older operating systems you may be prompted by a security warning. Click **Yes** to confirm you wish to install the certificate.
 - i Click **OK** to close the Certificate Import Wizard.
 - j Click **OK** to close the certificate.
 - k The certificates will now be installed successfully.
- 4) **Verifying certificates are installed correctly:**
- a Open certificate management tool by searching for **manage computer certificates** or running **certlm** on a command prompt with administrative privileges.



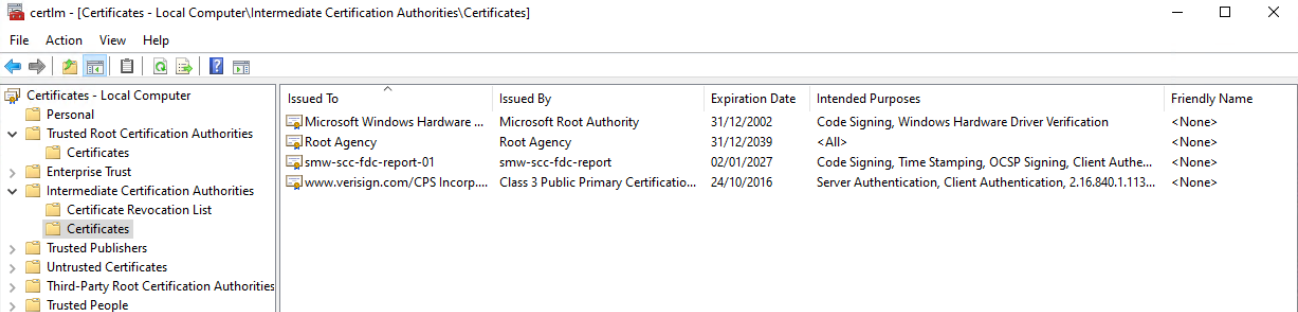
OR



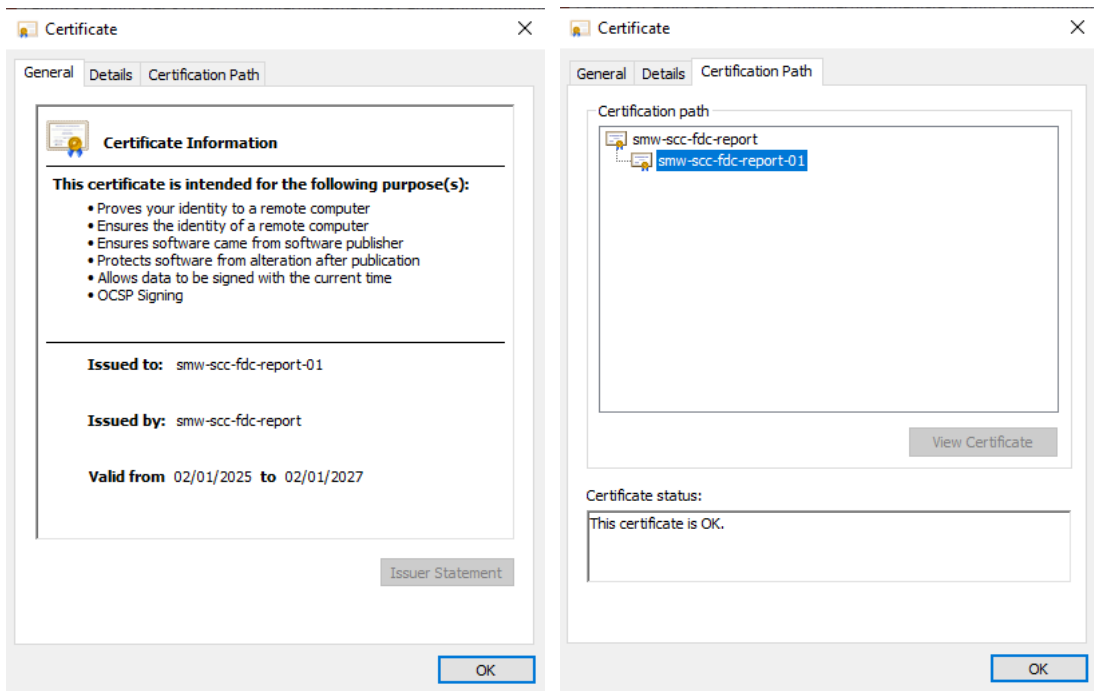
- b Expand the **Trusted Root Certification Authorities** store on the left hand side. Verify the certificate is present as follows. The issued to name should be **smw-scc-fdc-report**.



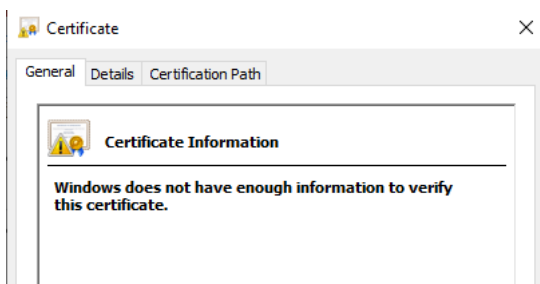
- c Next expand the **Intermediate Certification Authorities** store on the left hand side. Verify the certificate is present as follows. The issued to name should be **smw-scc-fdc-report-01**.

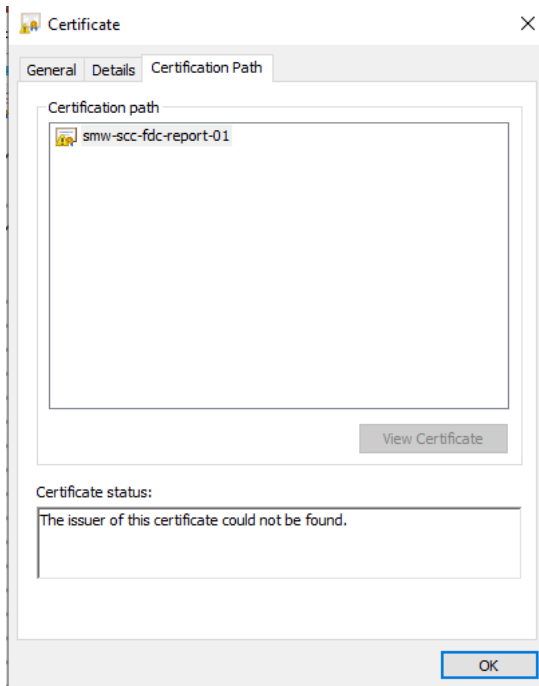


- d Next double click the certificate **smw-scc-fdc-report-01** to open it. Click on the Certification Path. You should see the certificate chain as shown below and the certificate status as OK.



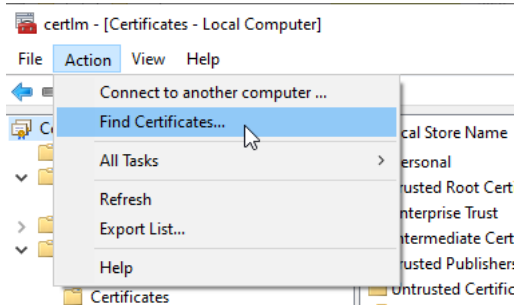
Note: if the root has not been installed correctly you will observe the following errors.



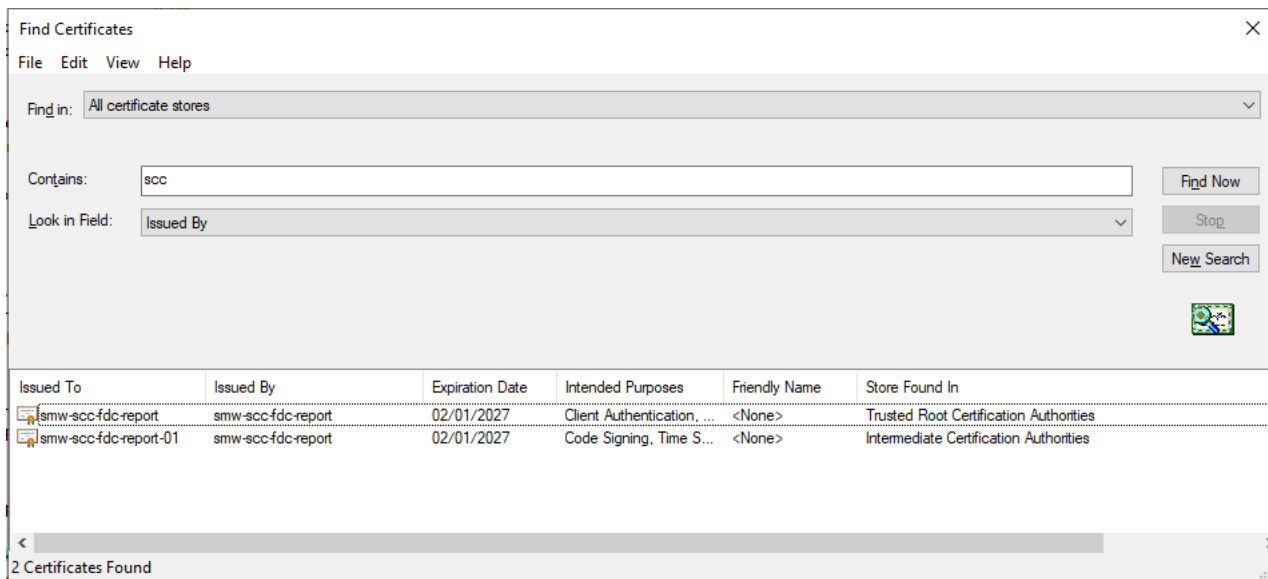


Alternatively you can also search as follows:

Click Action > Find Certificates



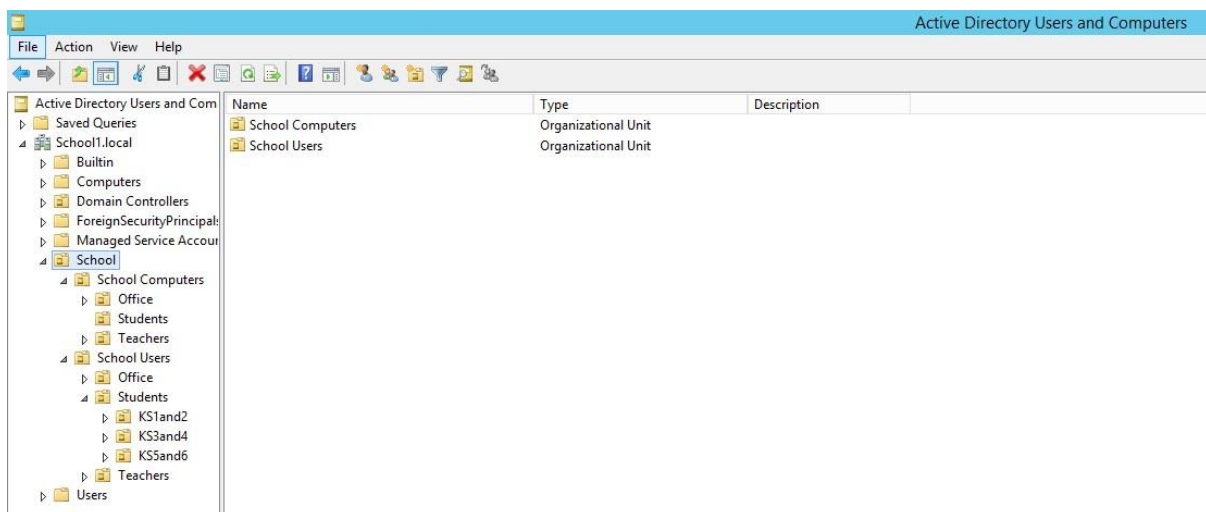
Enter scc in the contains field and select Find Now:



Deploying the Smoothwall certificate to Windows computers via group policy

If your school has a Microsoft Windows Server managing your computer accounts, and if an appropriate organisational structure in your Active Directory has been configured, you may be able to deploy the Smoothwall certificates to all Windows computers in your domain using group policy.

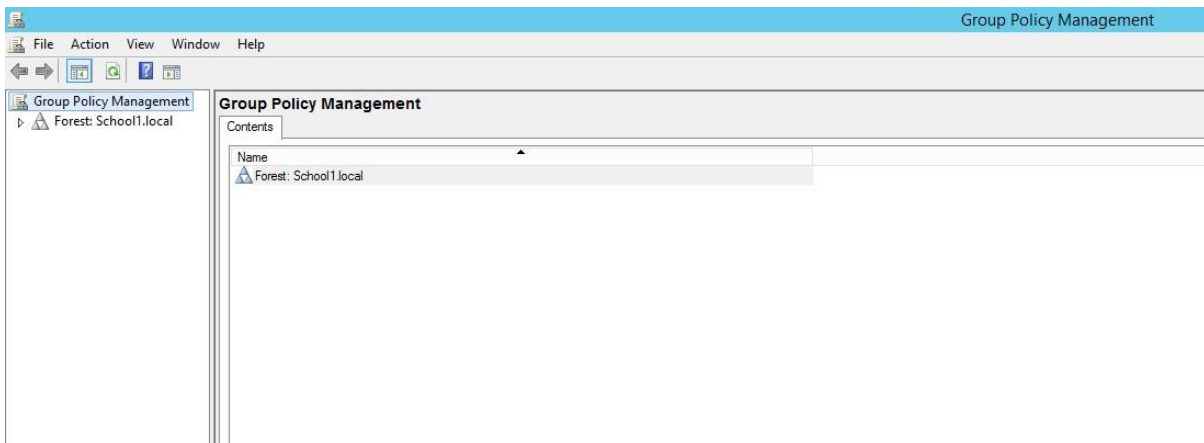
For the purposes of this guide, a domain called **School1.local** has been created with an organisational unit structure that contains a top level organisational unit called **School**. Within the **School** organisational unit there are further organisational units for managing either school computers, or school users. These are further broken down into office, student and teacher computer organisational units, and office, student and teacher user organisational units. The student users are further organised into organisational units of **KS1and2**, **KS3and4**, and **KS5and16**.



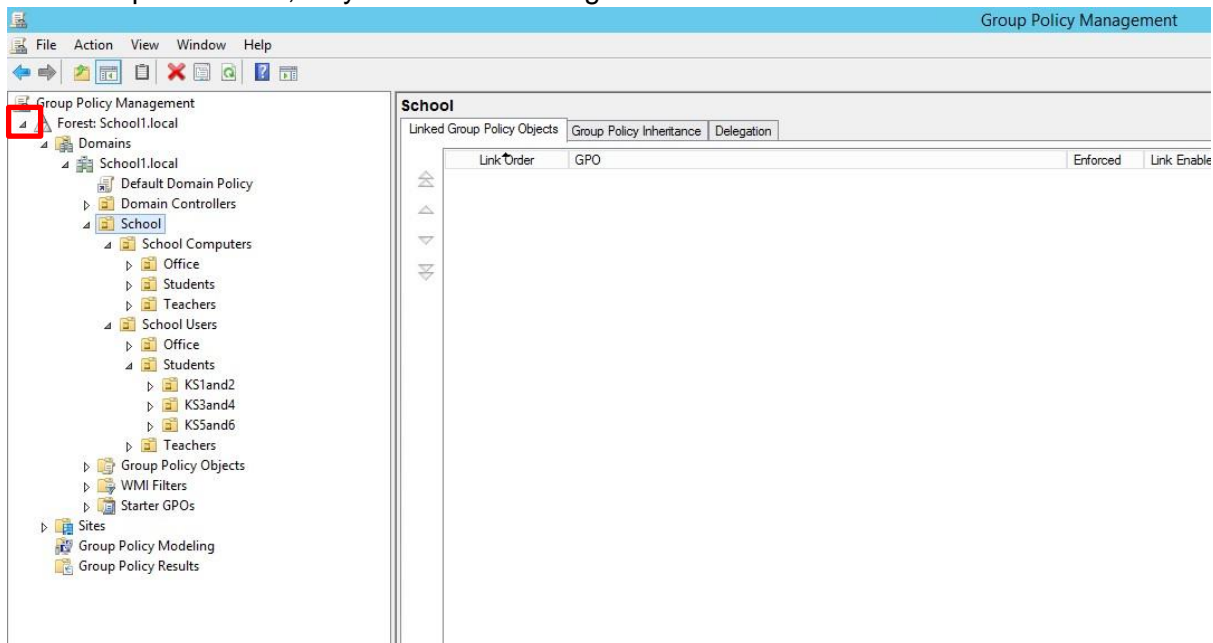
The following guidance is provided as a supplement to the guidance on the Smoothwall website and has been tested on Windows computers using Internet Explorer 11.

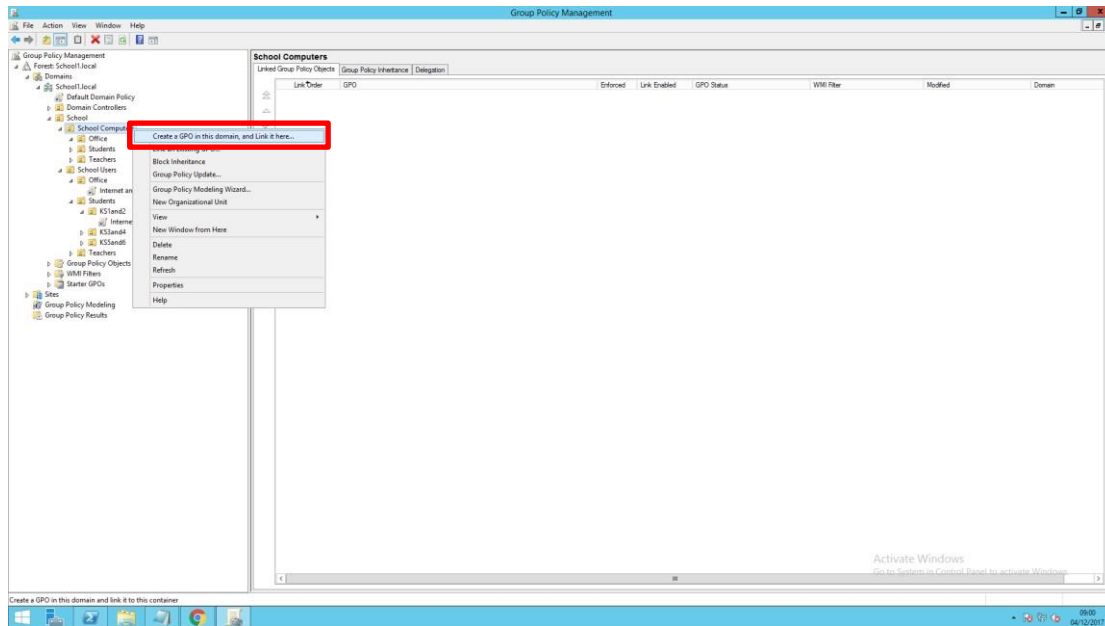
NOTE: This guide was conducted on a server running Microsoft Windows Server 2012 R2, thus some of the screenshot images in this guide may differ from what you see on your server.

- 1) Download the Smoothwall certificate and save it to a suitable location.
- 2) Open the **Group Management Console** on your server. You can search for this if required, as shown below.
- 3) The **Group Management Console** will be displayed, as shown below.

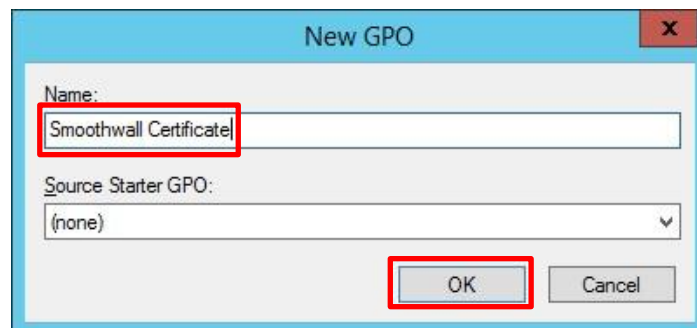


- 4) If required, click the arrow next to the Forest in the left-hand pane, so that it expands as shown below. Our primary organisational unit is called **School**, so we've selected and expanded that, so you can see the organisational units beneath.

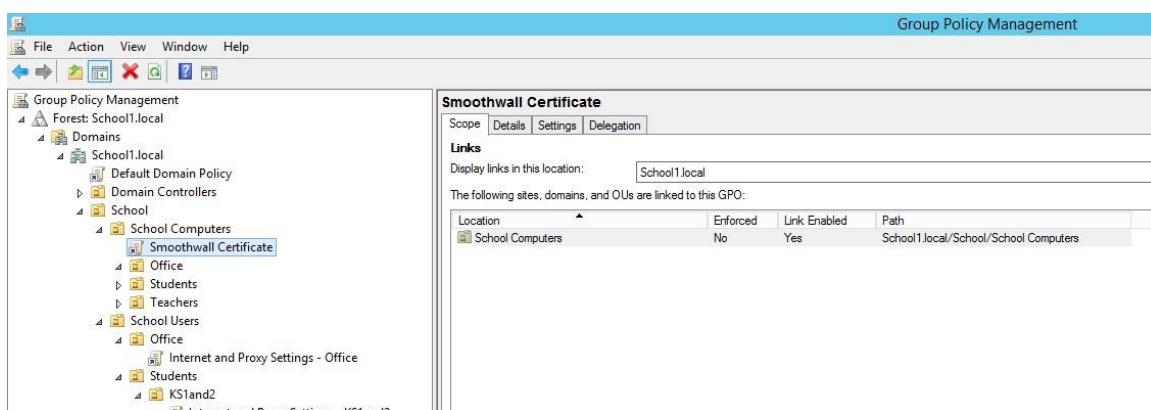


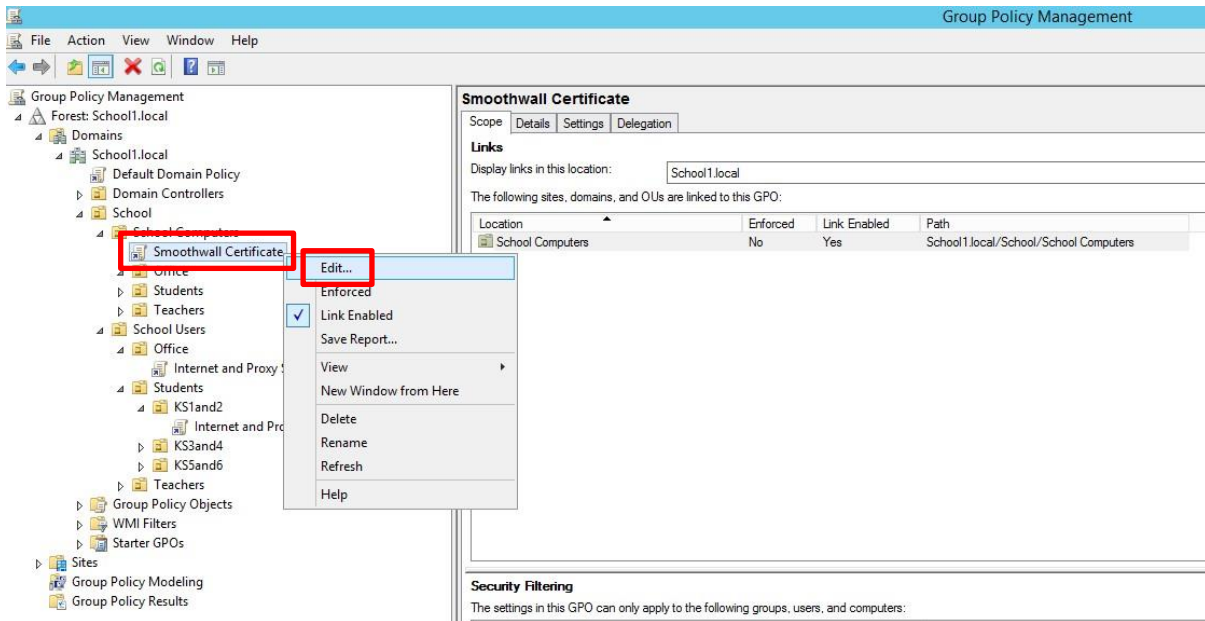


- 5) As the certificate will be required on all computers, it should be applied to computer organisational units, rather than user organisational units. In this example, we'll create a GPO (Group Policy Object) which will be used to apply the certificate to the School Computers organisational unit. Right-click the **School Computers** organisational unit and choose **Create a GPO in this domain, and Link it here...**

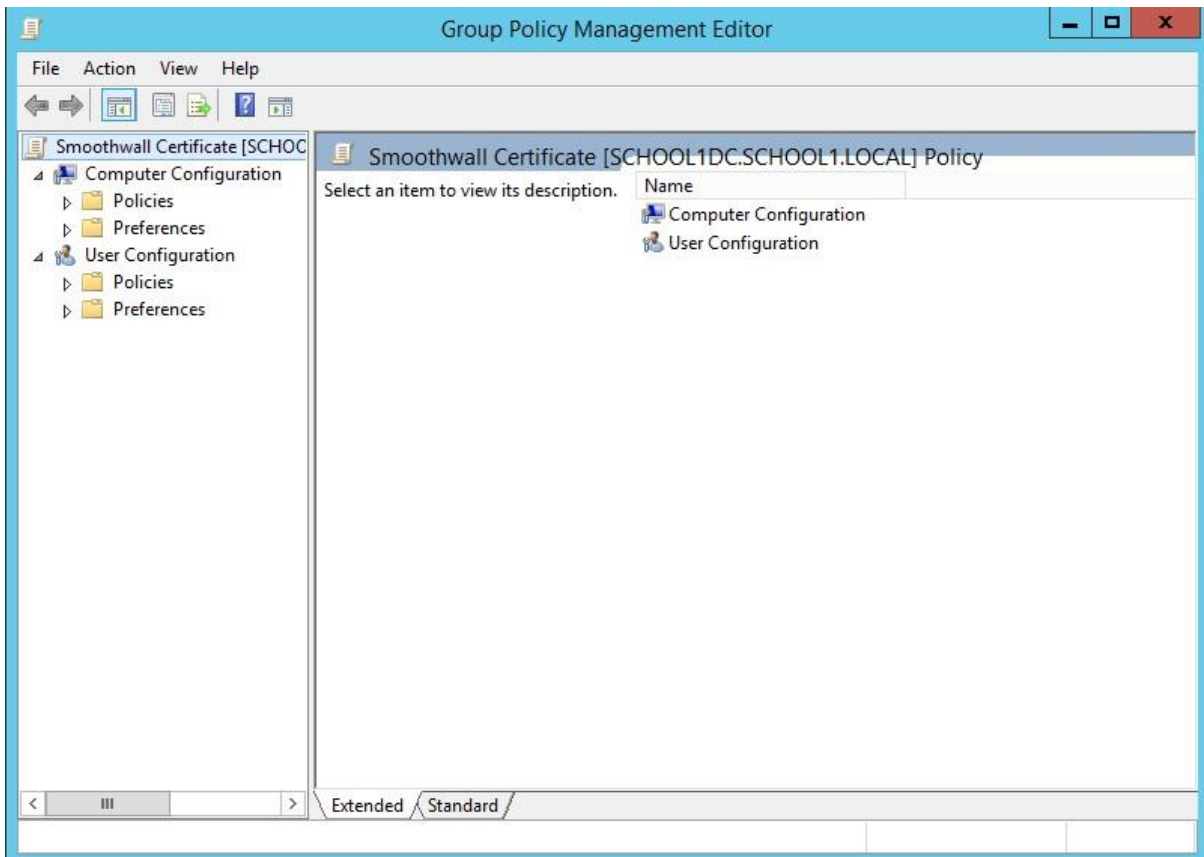


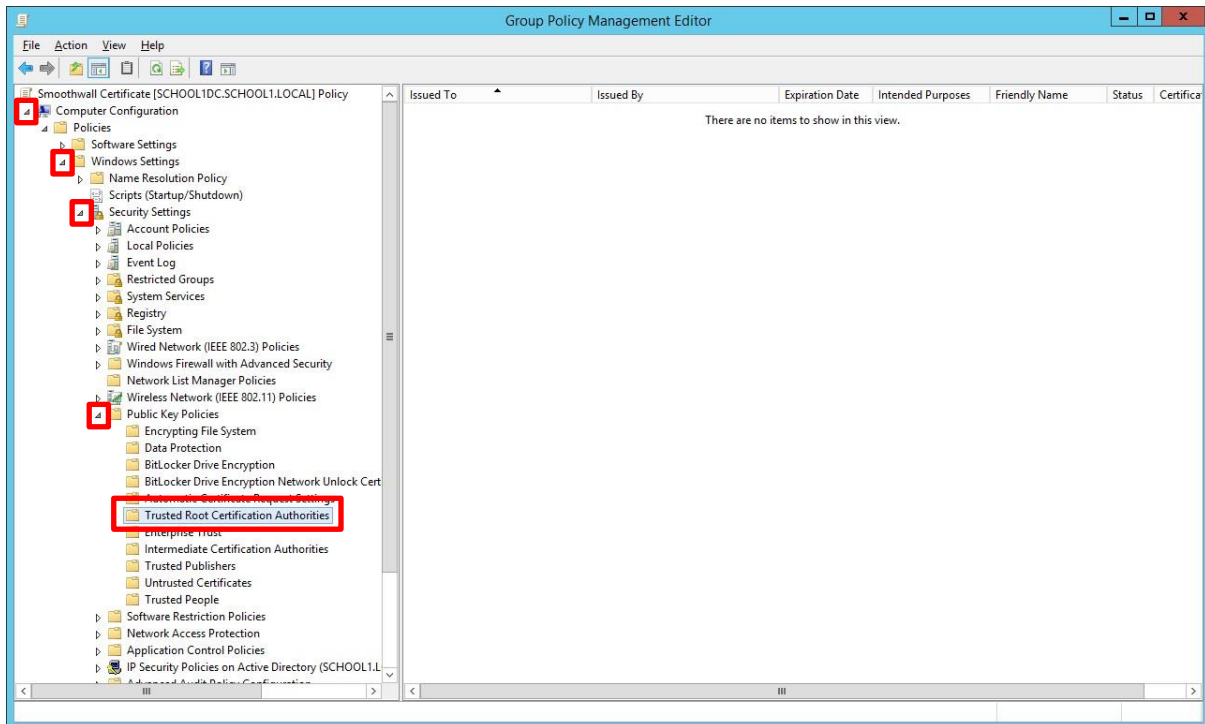
- 6) A **New GPO** box will appear. Type a name for the GPO, for example **Smoothwall Certificate** as shown above, then click **OK**. The new policy will appear under the **School Computers** organisational unit as shown below.





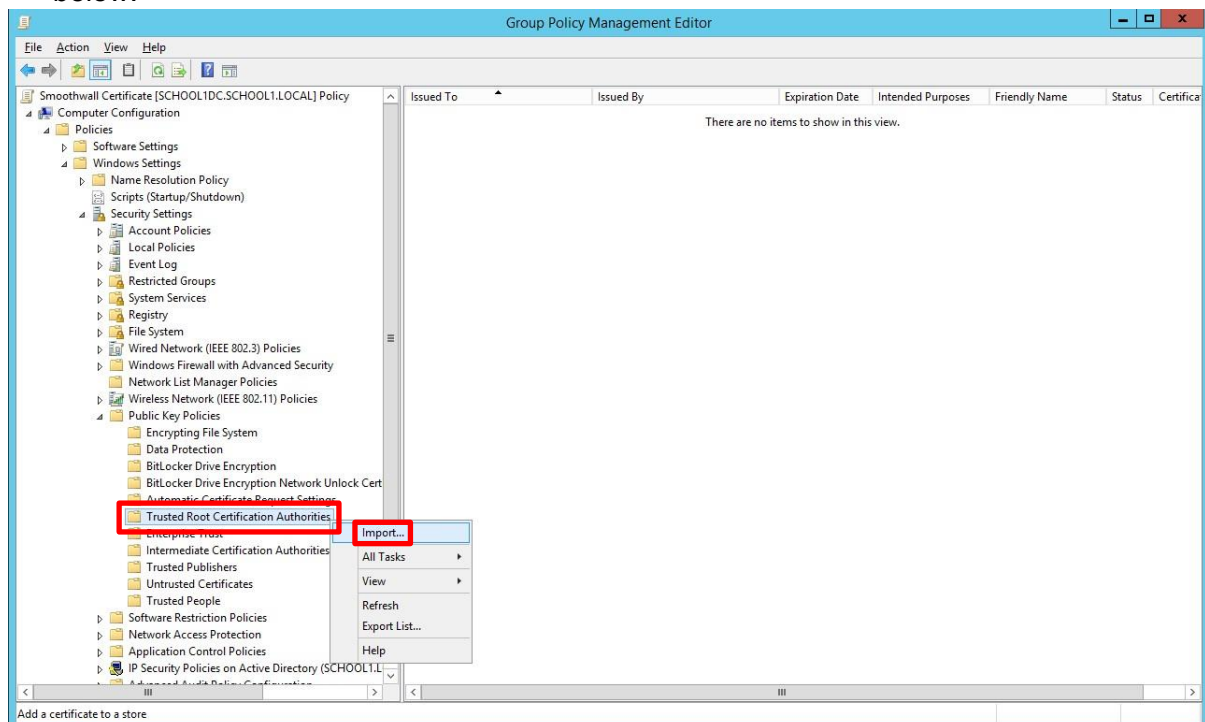
7) Right-click on the policy and choose **Edit**, as shown above. This will open the **Group Policy Management Editor**, as shown below.

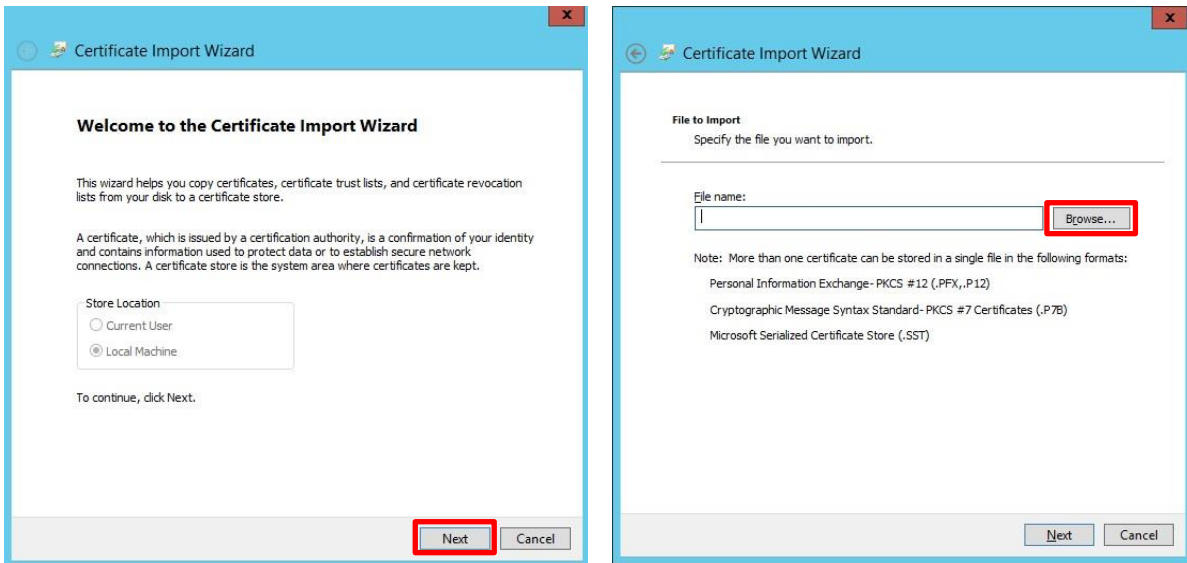




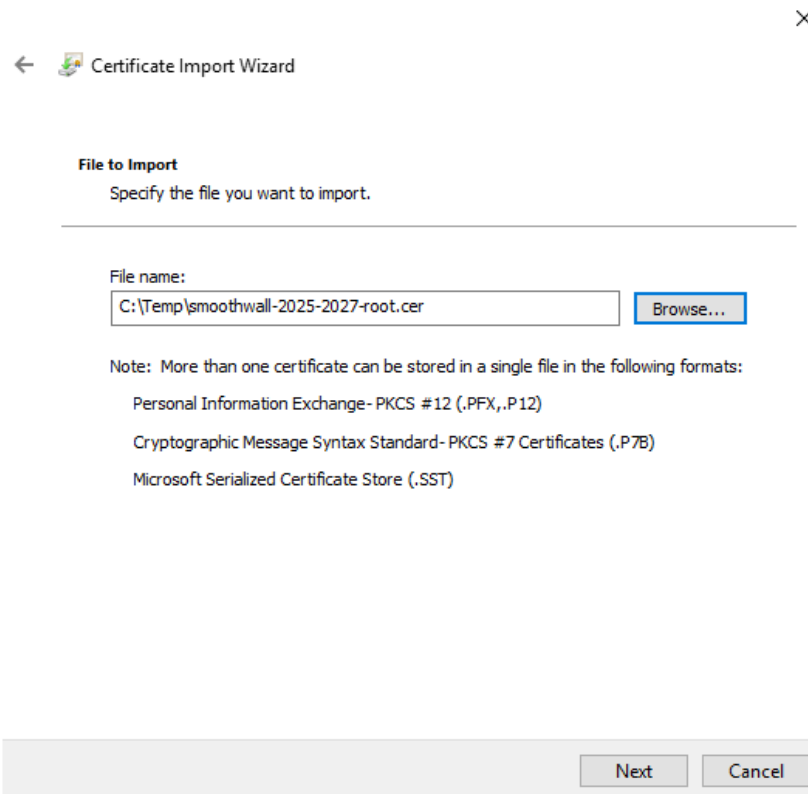
8) Under **Computer Configuration**, expand **Windows Settings**, **Security Settings**, **Public Key Policies** and choose **Trusted Root Certification Authorities**, as shown above.

9) Right-click on **Trusted Root Certification Authorities** and choose **Import...** as shown below.

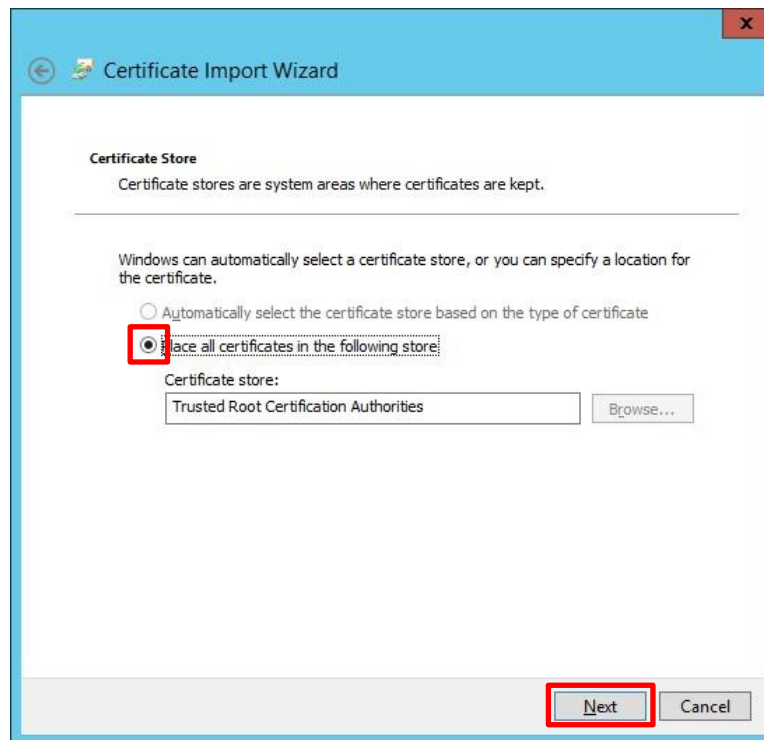




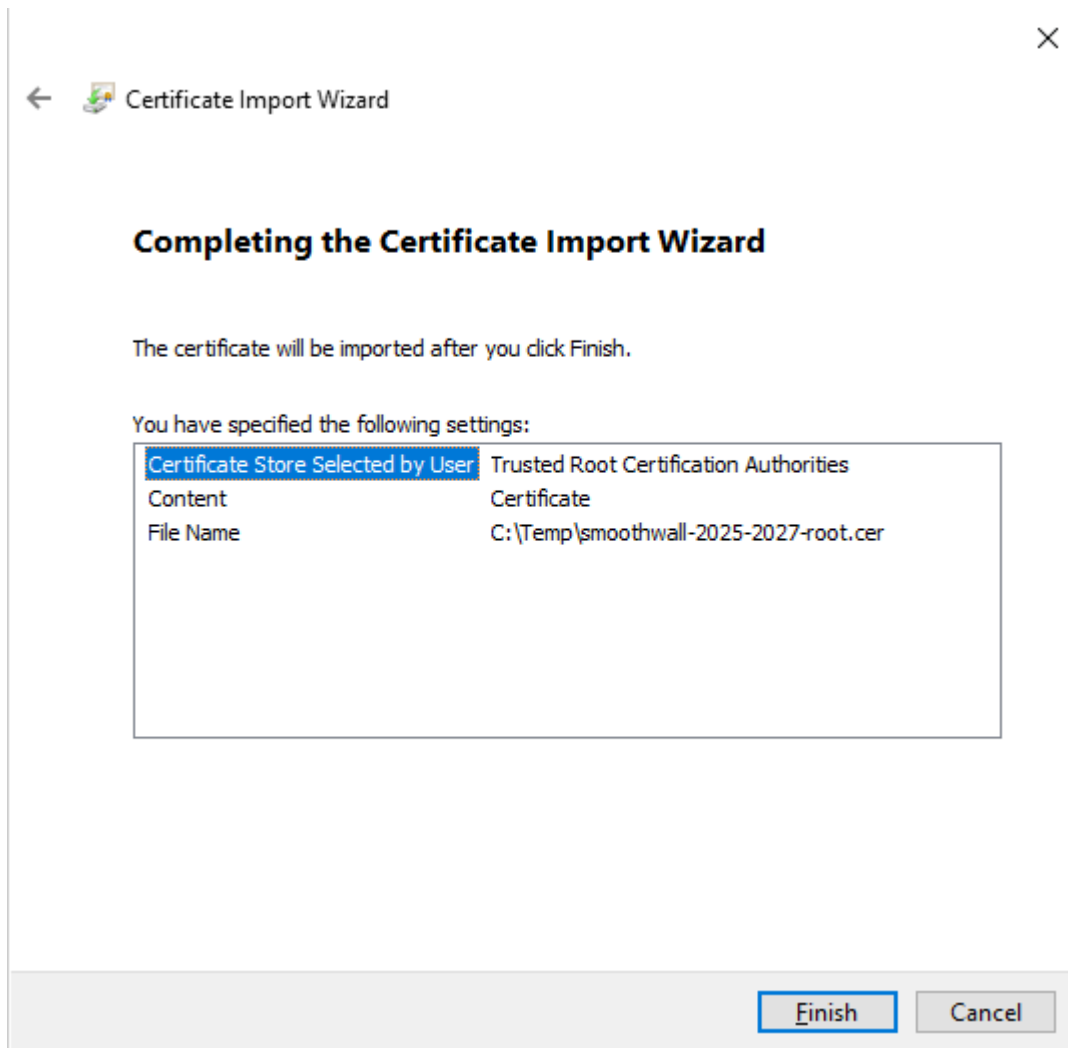
- 10) The **Certificate Import Wizard** will open as shown above on the left. Click **Next** to continue, then click **Browse** as shown above on the right. Navigate to the location where you saved the certificate. Select the certificate, as shown below, then click **Open**.



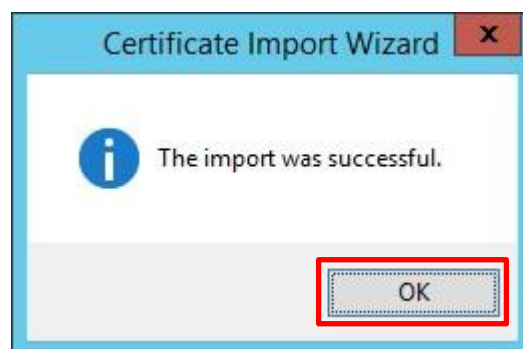
- 11) Click **Next**.



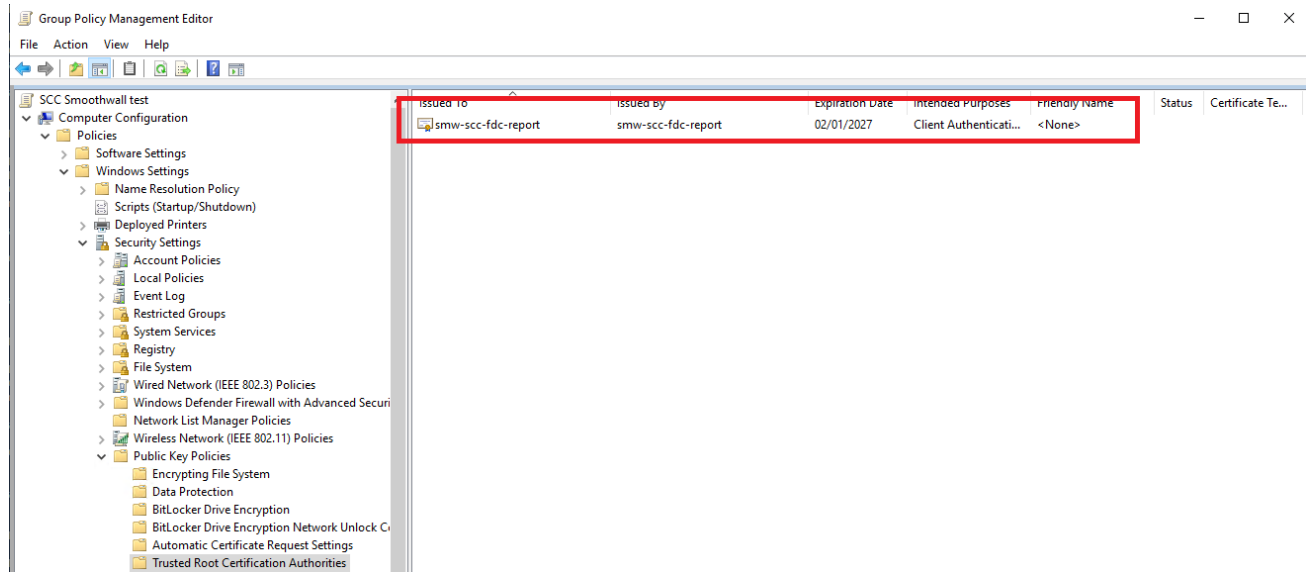
- 12) Ensure that the **Place all certificates in the following store** button is selected, and that the Certificate store is set as **Trusted Root Certification Authorities**, then click **Next**. *If not, cancel and return to step 8. If you do not install the certificate in this certificate store, the Smoothwall Certificate will NOT function correctly.*



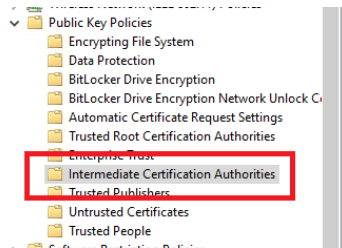
13) Click Finish



14) Click **OK** to close the Certificate Import Wizard. You should see the new certificate present.



15) Repeat the process and under step 8 install the intermediate certificate under **Computer Configuration**, expand **Windows Settings**, **Security Settings**, **Public Key Policies** and choose **Intermediate Certification Authorities**



Select the correct certificate:

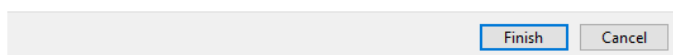


Completing the Certificate Import Wizard

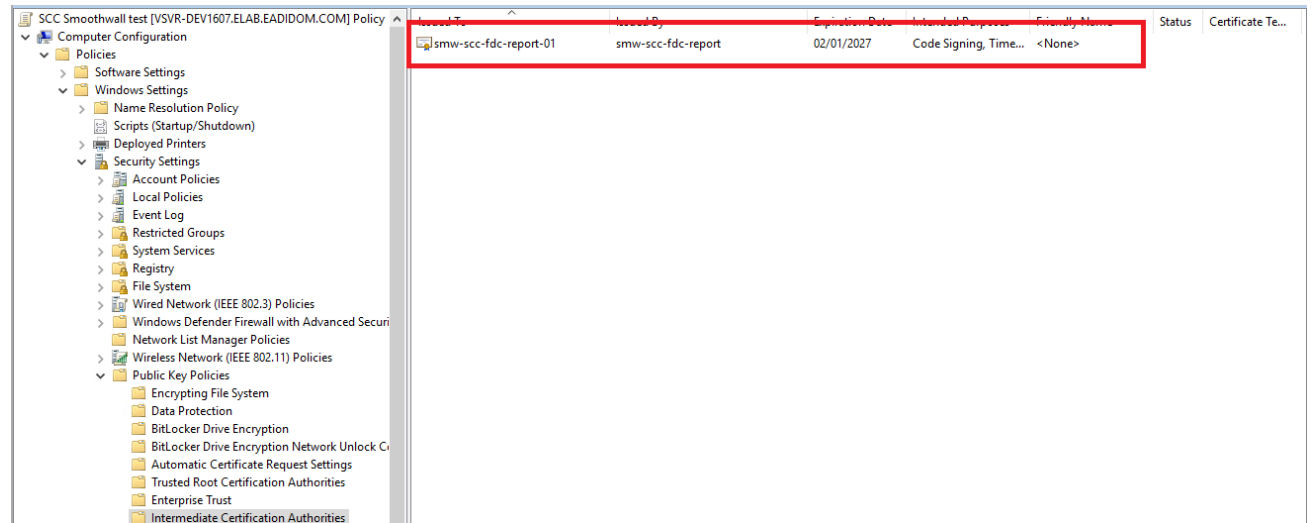
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Intermediate Certification Authorities
Content	Certificate
File Name	C:\Temp\smoothwall-2025-2027-intermediate.cer



Verify it is installed:



- 16) Back at the **Group Policy Management Editor** screen, you will see that the new policy has been created and is displayed in the right-hand pane, as shown above. Close the **Group Policy Management Editor**.

The certificate will be deployed to all computers in the target organisational units, and any subfolder organisational units you have below the target organisational unit. Computers will need to be rebooted at least twice. Alternatively, you can apply the settings to an individual computer in the target organisational unit by typing **gpupdate /force** from a command prompt on that computer, then rebooting the computer when prompted.

Always verify that the certificate is installed in the target computers local certificate stores.

Deploying the Smoothwall certificate to Windows computers using certutil dspublish

To publish root and intermediate certificates to Active Directory using certutil, you can use the -dspublish option. Here are the steps.

1. Save the Smoothwall root and intermediate certificates to your local computer, in the following steps it is assumed you have saved them as C:\temp\smoothwall-2025-2027-root.cer and C:\temp\smoothwall-2025-2027-intermediate.cer
2. Open a command prompt (or PowerShell) as an administrator. The following command must be run with an account that is a member of either Domain Admins or Enterprise Admins group.
3. Open ADSI edit by running the command. This will open in a new window:
`adsiedit`
4. Open Local machine certificates by running the command. This will also open in a new window:
`certlm`
5. Publish the root certificate. Enter the following command:
`certutil -dspublish -f "C:\temp\smoothwall-2025-2027-root.cer" RootCA`

The expected output is as follows:

```
PS C:\WINDOWS\system32> certutil -dspublish -f "C:\temp\smoothwall-2025-2027-root.cer"
RootCA

ldap:///CN=smw-scc-fdc-report,CN=Certification Authorities,CN=Public Key
Services,CN=Services,CN=Configuration,DC=YOUR,DC=DOMAIN,DC=com?cACertificate

Certificate added to DS store.

ldap:///CN=smw-scc-fdc-report,CN=AIA,CN=Public Key
Services,CN=Services,CN=Configuration,DC= YOUR,DC=DOMAIN,DC=com?cACertificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.
```

6. Publish the intermediate certificate. Enter the following command:
`certutil -dspublish -f "C:\temp\smoothwall-2025-2027-intermediate.cer" SubCA`

The expected output is as follows:

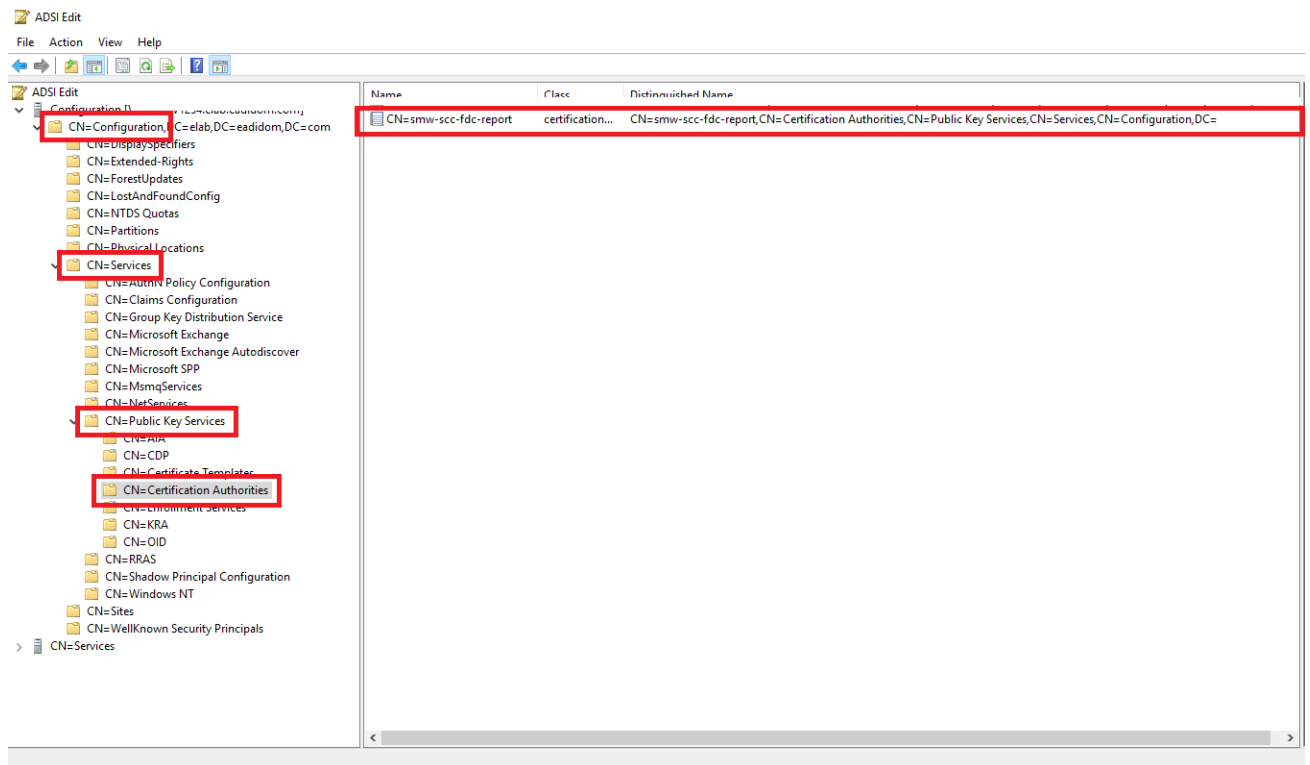
```
PS C:\WINDOWS\system32> certutil -dspublish -f "C:\temp\smoothwall-2025-2027-
intermediate.cer" SubCA

ldap:///CN=smw-scc-fdc-report-01,CN=AIA,CN=Public Key
Services,CN=Services,CN=Configuration,DC=YOUR,DC=DOMAIN,DC=com?cACertificate

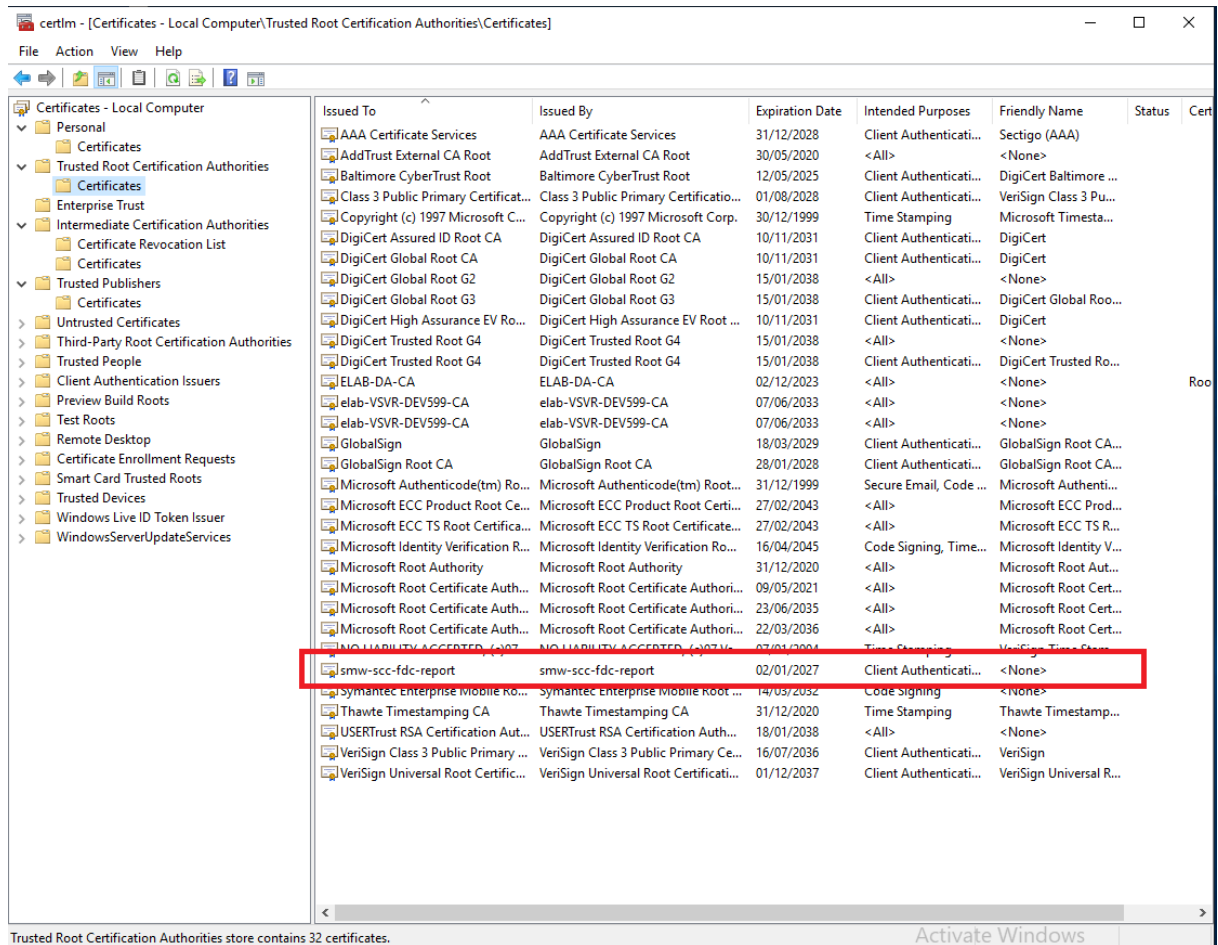
Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.
```

- Navigate to ADSI Edit and expand CN=Configuration, CN=Services, CN=Public Key Services and CN=Certificate Authorities. You should expect to see the certificate present as follows:



- Navigate to Certificate Management (certlm) tool and Browse to Trusted Root Certification Authorities. You should expect to see the root certificate present as follows:



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Cert
AAA Certificate Services	AAA Certificate Services	31/12/2028	Client Authenticati...	Sectigo (AAA)		
AddTrust External CA Root	AddTrust External CA Root	30/05/2020	<All>	<None>		
Baltimore CyberTrust Root	Baltimore CyberTrust Root	12/05/2025	Client Authenticati...	DigiCert Baltimore ...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	01/08/2028	Client Authenticati...	VeriSign Class 3 Pu...		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	30/12/1999	Time Stamping	Microsoft Timesta...		
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10/11/2031	Client Authenticati...	DigiCert		
DigiCert Global Root CA	DigiCert Global Root CA	10/11/2031	Client Authenticati...	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	15/01/2038	<All>	<None>		
DigiCert Global Root G3	DigiCert Global Root G3	15/01/2038	Client Authenticati...	DigiCert Global Roo...		
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	10/11/2031	Client Authenticati...	DigiCert		
DigiCert Trusted Root G4	DigiCert Trusted Root G4	15/01/2038	<All>	<None>		
DigiCert Trusted Root G4	DigiCert Trusted Root G4	15/01/2038	Client Authenticati...	DigiCert Trusted Ro...		
ELAB-DA-CA	ELAB-DA-CA	02/12/2023	<All>	<None>		Root
elab-VSVR-DEV599-CA	elab-VSVR-DEV599-CA	07/06/2033	<All>	<None>		
elab-VSVR-DEV599-CA	elab-VSVR-DEV599-CA	07/06/2033	<All>	<None>		
GlobalSign	GlobalSign	18/03/2029	Client Authenticati...	GlobalSign Root CA...		
GlobalSign Root CA	GlobalSign Root CA	28/01/2028	Client Authenticati...	GlobalSign Root CA...		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	31/12/1999	Secure Email, Code ...	Microsoft Authenti...		
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	27/02/2043	<All>	Microsoft ECC Prod...		
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate...	27/02/2043	<All>	Microsoft ECC TS R...		
Microsoft Identity Verification R...	Microsoft Identity Verification Ro...	16/04/2045	Code Signing, Time...	Microsoft Identity V...		
Microsoft Root Authority	Microsoft Root Authority	31/12/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	09/05/2021	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	23/06/2035	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	22/03/2036	<All>	Microsoft Root Cert...		
NO LIABILITY ACCEPTED (-)07...	NO LIABILITY ACCEPTED (-)07...	07/01/2001	Time Stamping	VeriSign Time Stamp...		
smw-scc-fdc-report	smw-scc-fdc-report	02/01/2027	Client Authenticati...	<None>		
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile root ...	14/05/2052	Code Signing	<None>		
Thawte Timestamping CA	Thawte Timestamping CA	31/12/2020	Time Stamping	Thawte Timestamp...		
USERTrust RSA Certification Aut...	USERTrust RSA Certification Auth...	18/01/2038	<All>	<None>		
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	16/07/2036	Client Authenticati...	VeriSign		
VeriSign Universal Root Certific...	VeriSign Universal Root Certificati...	01/12/2037	Client Authenticati...	VeriSign Universal R...		

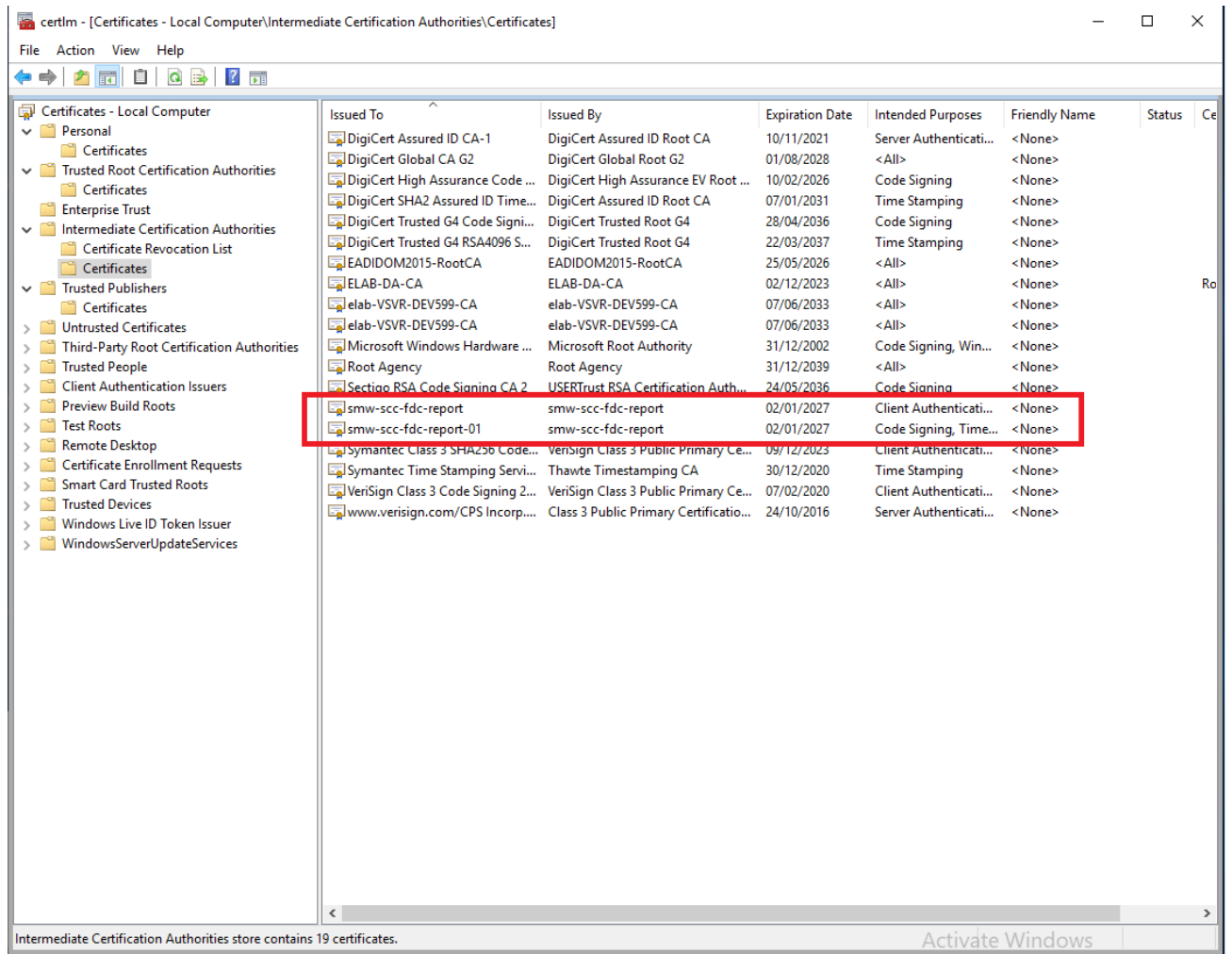
Trusted Root Certification Authorities store contains 32 certificates.

If this is not present yet you can pull down the certificate from AD by issuing the command:

```
PS C:\WINDOWS\system32> certutil -pulse
CertUtil: -pulse command completed successfully.
```

Refresh the certificate store and it should be present.

- Still in Certificate Management navigate to Intermediate Certification Authorities and you should expect to see both the intermediate and root certificate present:



10. If you now open the intermediate certificate (smw-scc-fdc-report-01) and click the Certification Path tab you should see the certificate nested and status is OK as below.

