

# Setting up Certificate Authentication for SonicWall SRA / SMA 100 Series

---

**SonicWall SRA and SMA devices now have the option to authenticate using Client User Certificates.**

- This is a guide on how to implement this using a Domain CA Certificate along with User Certificates.
- This guide is based SMA Firmware 8.6.0.3-11sv and Microsoft Server 2008 R2.
- It is presumed that you have already set up an Authentication Domain using Active Directory for your Domain on the SRA/SMA Appliance as this will be needed for the Group Affinity Checking.

**There are two different options when setting up a SSL VPN domain requiring client certificates:**

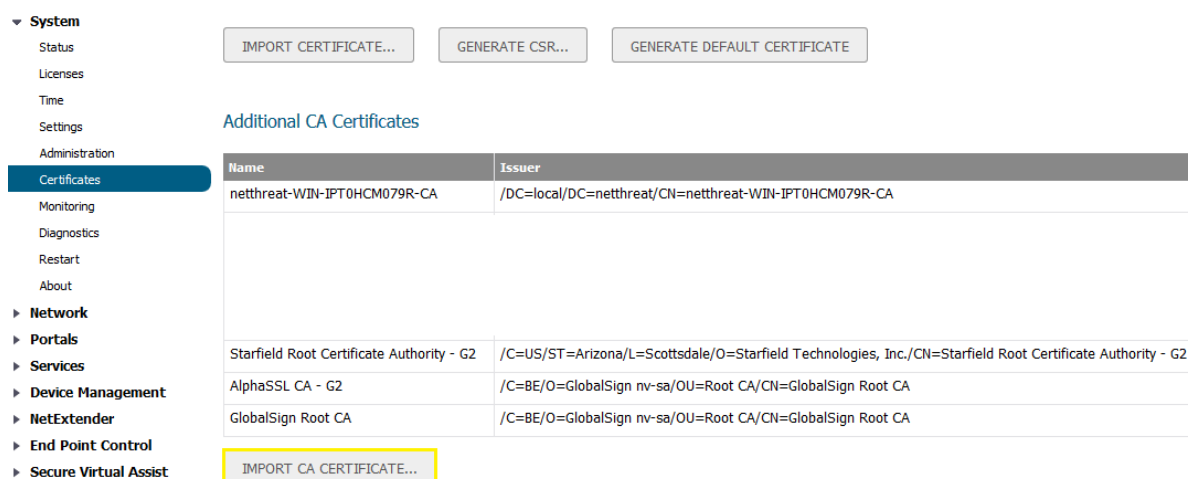
1. A standalone SSL-VPN domain which only uses Client Certificates (if using this method it is recommended to maybe restrict the expiry on the certificates or at least use a specific OU for Mobile users on the Group Policy rather than Issuing User Certificates to all the Domain Users).
2. On a new or already configured SSL-VPN Domain you can use the Enable Client Certificate Check enabled to provide further security.

- [Setting Up the SRA/SMA](#)
- [Setting up User Certificates on the Domain Controller](#)
- [Setting up the Group Policy](#)
- [Exporting and Importing the User Certificate](#)
- [Connecting to the SSL VPN Portal and NetExtender / Mobile Connect](#)

## Setting up the SRA / SMA

If you have not already set up User Certificates on your domain then go to the Section **Setting up User Certificates on the Domain Controller**.

1. In the SMA GUI, go to System/Certificates and import your domain CA certificate in the Additional CA Certificates section at the bottom.



**System**

- Status
- Licenses
- Time
- Settings
- Administration
- Certificates**
- Monitoring
- Diagnostics
- Restart
- About

**Network**

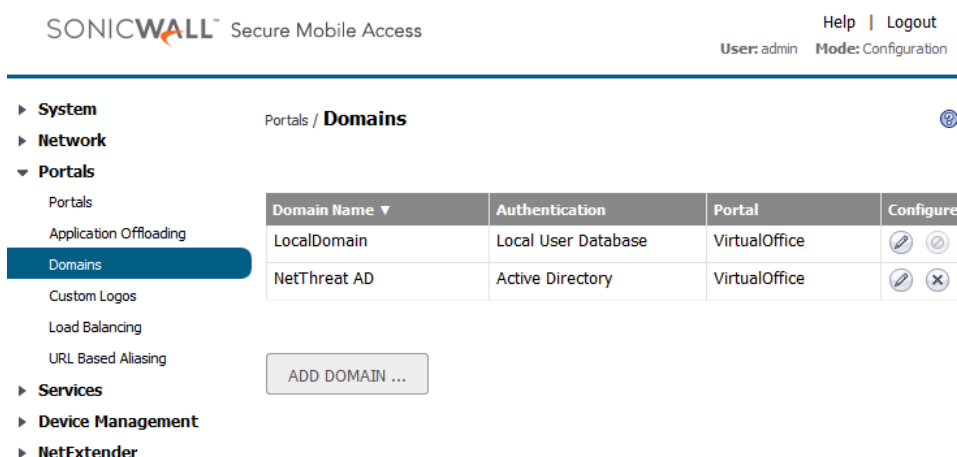
- Portals
- Services
- Device Management
- NetExtender
- End Point Control
- Secure Virtual Assist

**Additional CA Certificates**

Name	Issuer
netthreat-WIN-IPT0HCM079R-CA	/DC=local/DC=netthreat/CN=netthreat-WIN-IPT0HCM079R-CA
Starfield Root Certificate Authority - G2	/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Root Certificate Authority - G2
AlphaSSL CA - G2	/C=BE/O=GlobalSign nv-sa/OU=Root CA/CN=GlobalSign Root CA
GlobalSign Root CA	/C=BE/O=GlobalSign nv-sa/OU=Root CA/CN=GlobalSign Root CA

**IMPORT CA CERTIFICATE...**

2. Navigate to Portals/Domains and select Add Domain.







**SONICWALL** Secure Mobile Access

Help | Logout  
User: admin Mode: Configuration

**System**

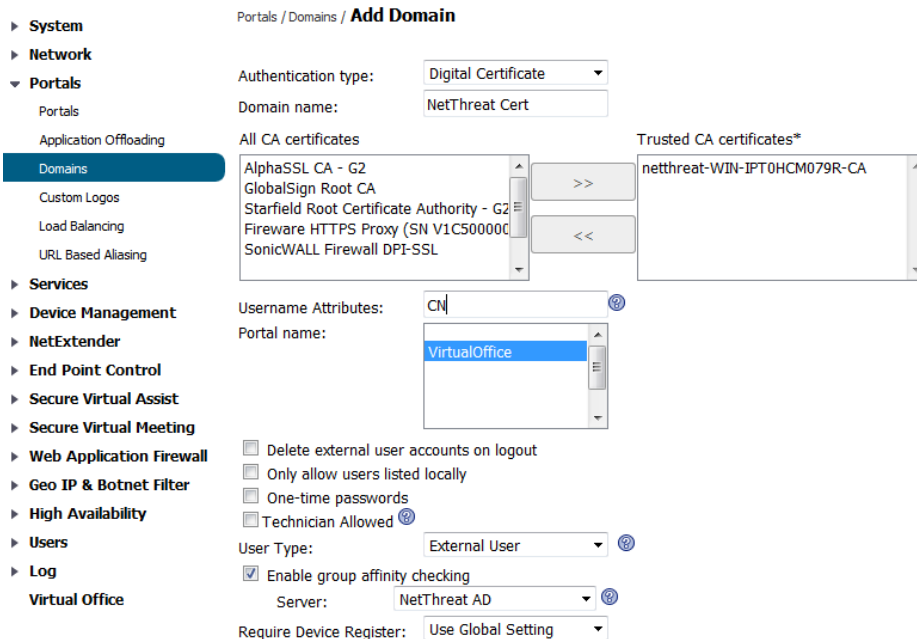
- Network
- Portals**
  - Portals
  - Application Offloading
  - Domains**
  - Custom Logos
  - Load Balancing
  - URL Based Aliasing
- Services
- Device Management
- NetExtender

**Portals / Domains**

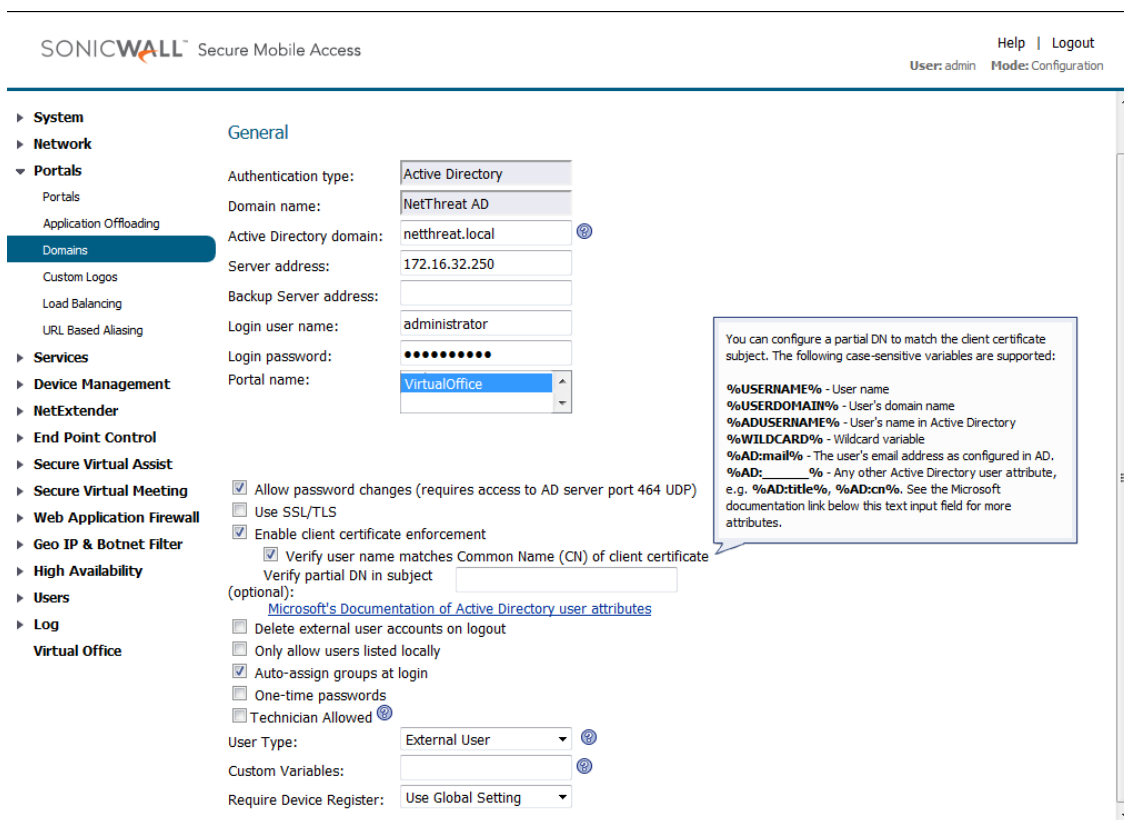
Domain Name	Authentication	Portal	Configure
LocalDomain	Local User Database	VirtualOffice	 
NetThreat AD	Active Directory	VirtualOffice	 

**ADD DOMAIN ...**

3. Select Authentication Type as **Digital Certificate**. Set the rest as below and add your Domain CA Certificate to the Trusted CA certificates.



4. To enable client certificate enforcement on an already configured SSL-VPN Domain, set as below adding any partial DN required.

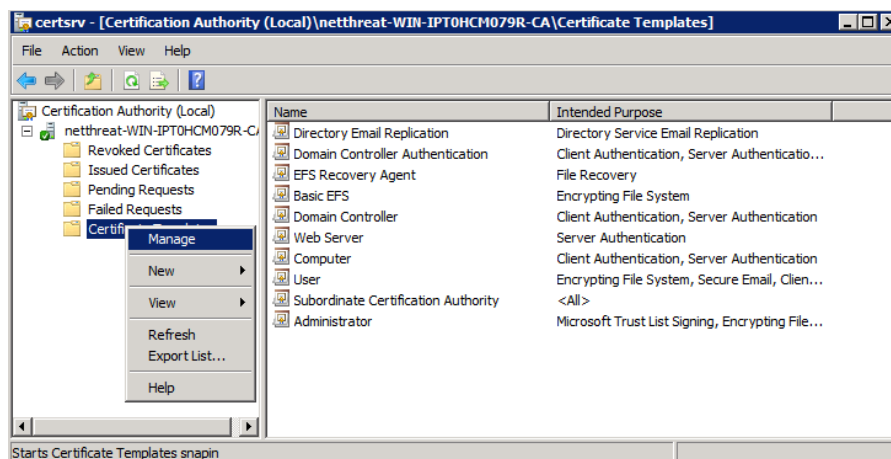


## Setting up User Certificates on the Domain Controller

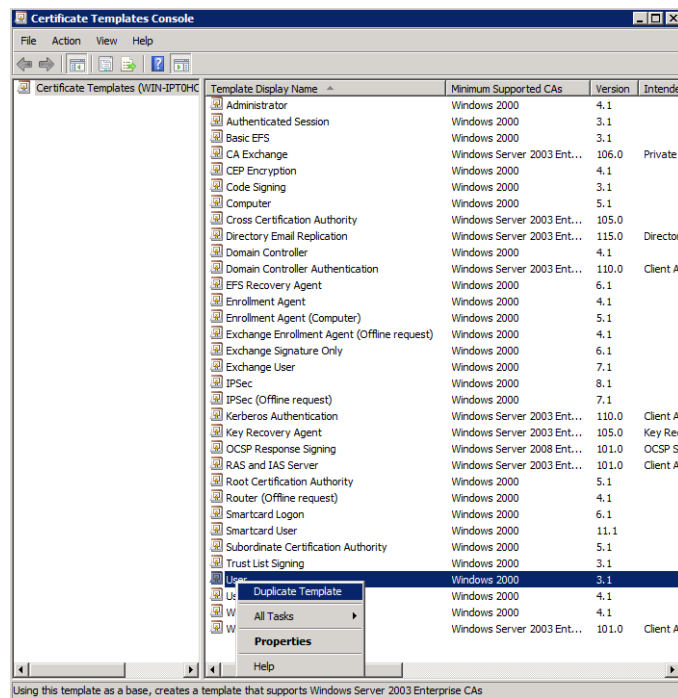
**N.B. Auto Enrol is only supported on the following Windows Server operating systems:**

**Server 2003 Enterprise, Server 2008 Enterprise, Server 2008 R2 and later on at least Standard version.**

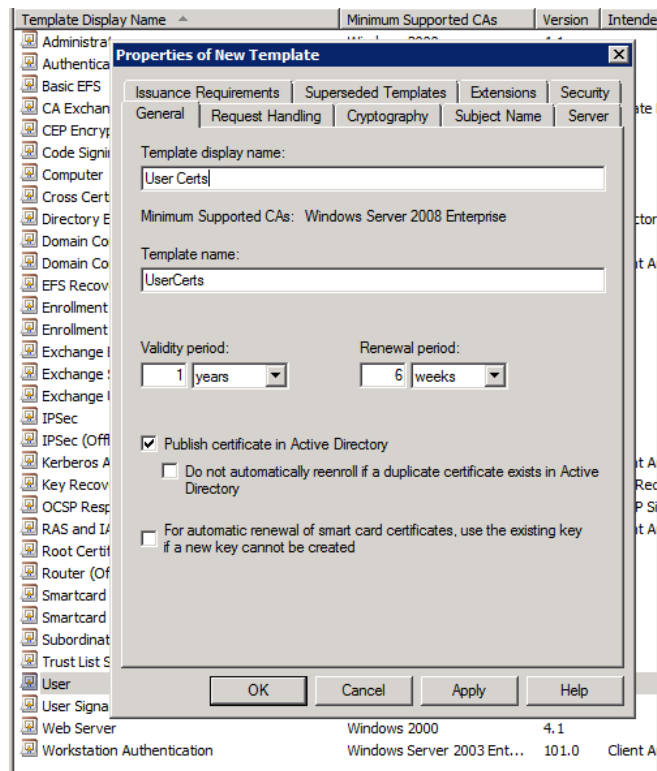
- Make sure you have the **Active Directory Certificate Services** Role Installed.
  - If you want users to request the Certificates Manually then also add the role **Certification Authority Web Enrollment** - not discussed in detail in this document. Please see here for further support on that feature [https://technet.microsoft.com/en-us/library/cc732895\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc732895(v=ws.11).aspx)
1. To start the Certification Authority either type in the run console **certsrv.msc** or go to Start/Administrative Tools/Certification Authority.
  2. Expand the Menu as below, Right Click on the Certificate Templates and select Manage.



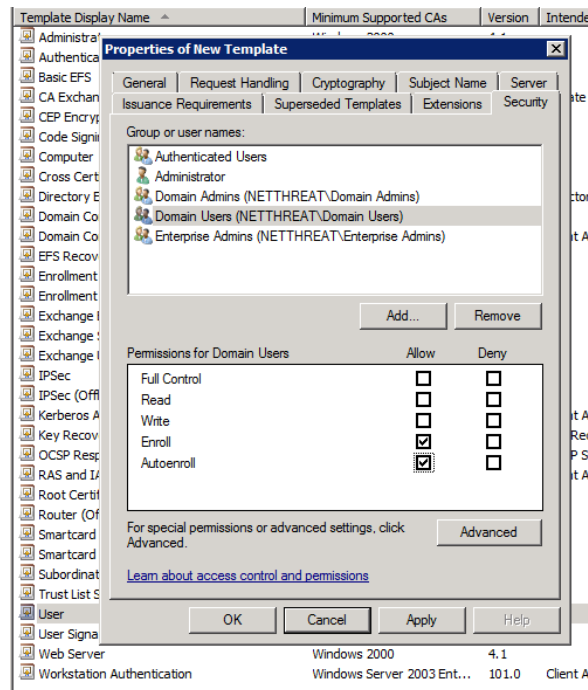
3. Select the **User** Template. Right click and Select Duplicate Template. Next, select the option Windows Server 2008 Enterprise and select ok.



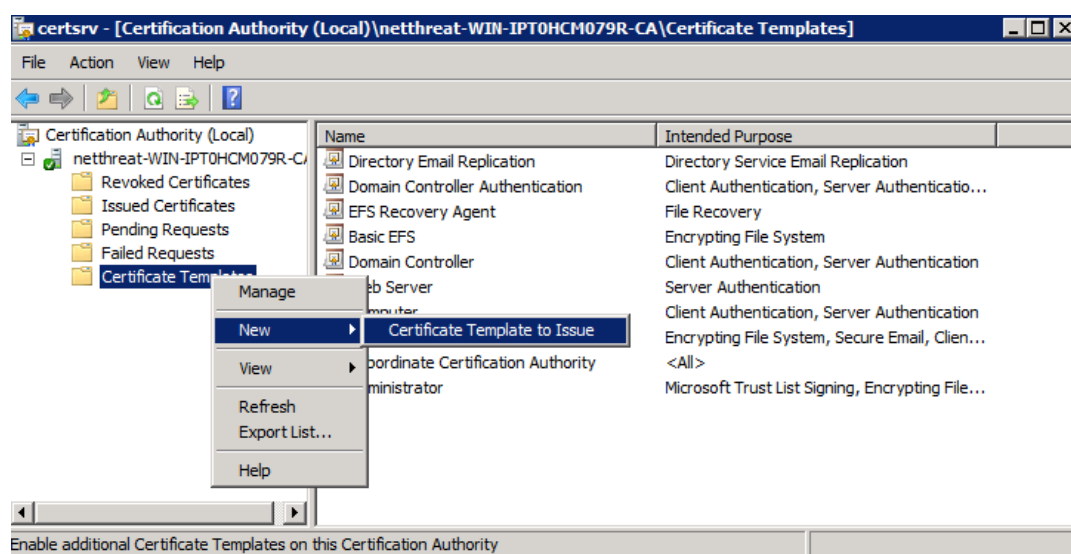
4. Give the new Template a relevant name and select the Validity and Renewal Periods as required.



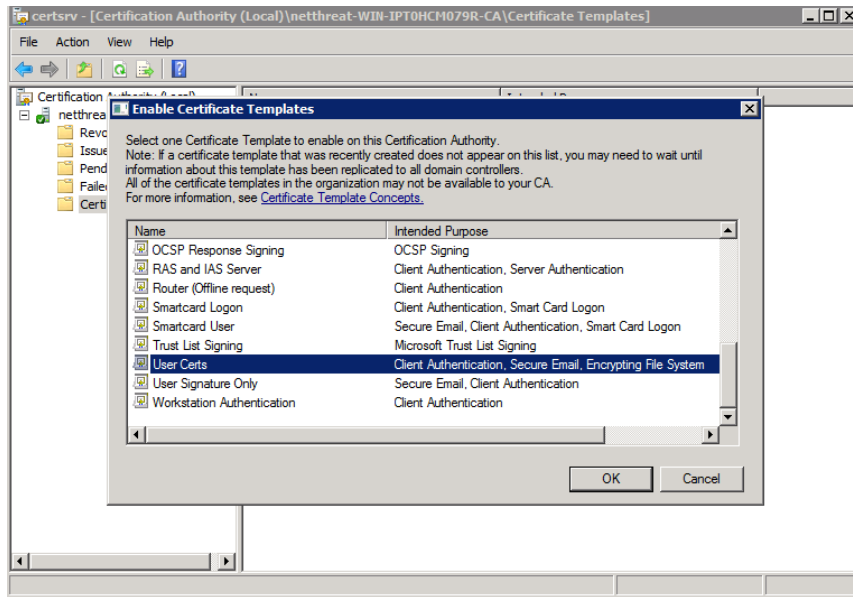
5. Under the Security Tab you need to make the following changes to the Domain Users permissions:



6. **Important** : unless all users that you wish to have a User Certificate deployed, have email address entered in to their account under the general settings menu on AD, you will need to un-tick the 'Include e-mail name' in the subject name under the Subject Name menu.
7. Once the new Template has been saved, you can now select it to be used to issue User Certificates. To do this, right click on the Certificates Templates and select New/Certificate Template to Use.

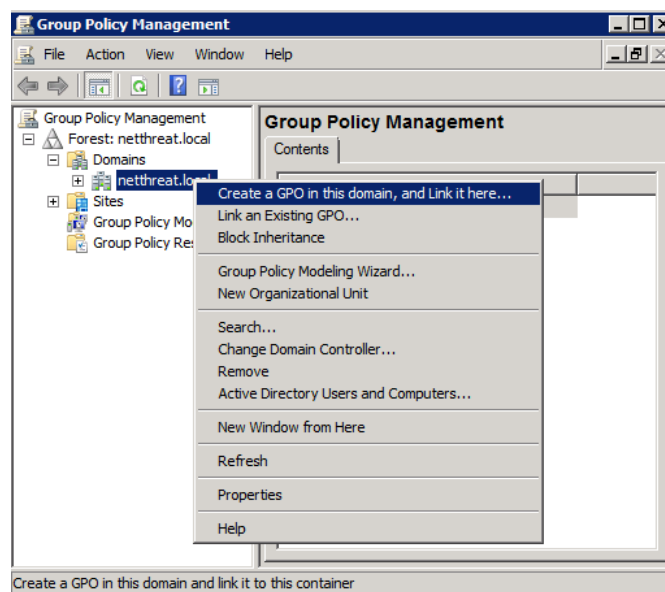


8. Select your new Template from the list and select ok then exit the console.

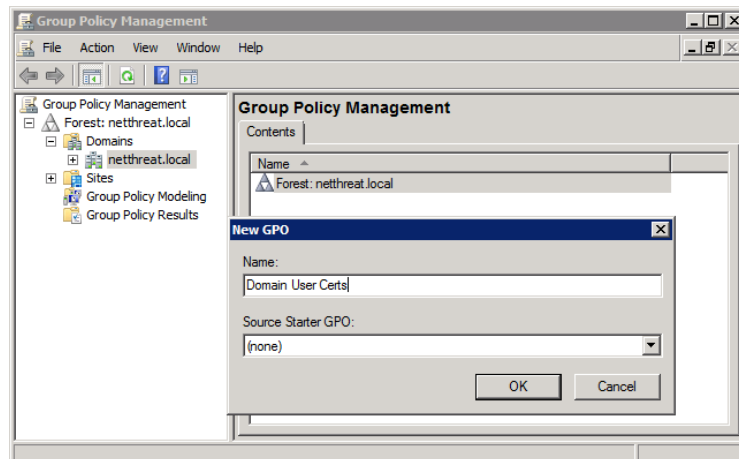


## Setting up the Group Policy

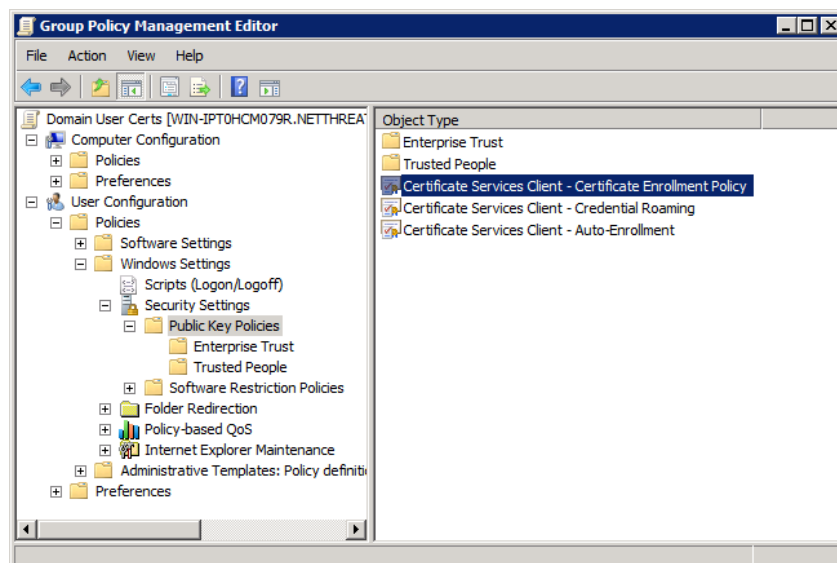
1. To start the Group Policy Manager Console either type in the run console **gpmc.msc** or go to Start/Administrative Tool/Group Policy Management.
2. Expand the Domains, then right click and select Create a GPO in this domain as below.  
**If you only want to auto enrol User Certificates for a specific AD group then you will need to create a New Organizational Unit and make sure the Users are moved to that OU in Active Directory.**



3. Name the GPO as below.

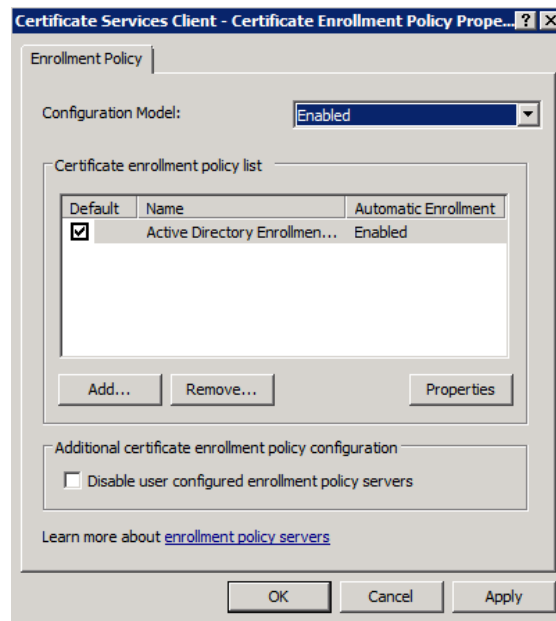


4. Once created, right click and select Edit, then browse to User Configuration/Windows Settings/Security Settings/Public Key Policies

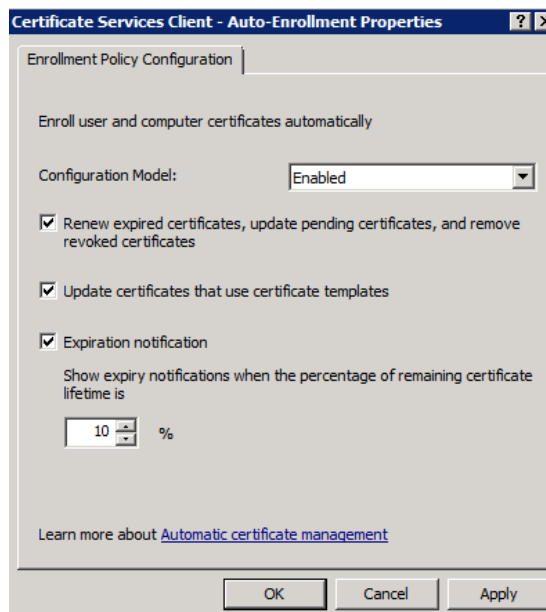




5. On the Certificate Services Client – Certificate Enrollment Policy right click and select Properties, and set to Enabled then apply and ok.



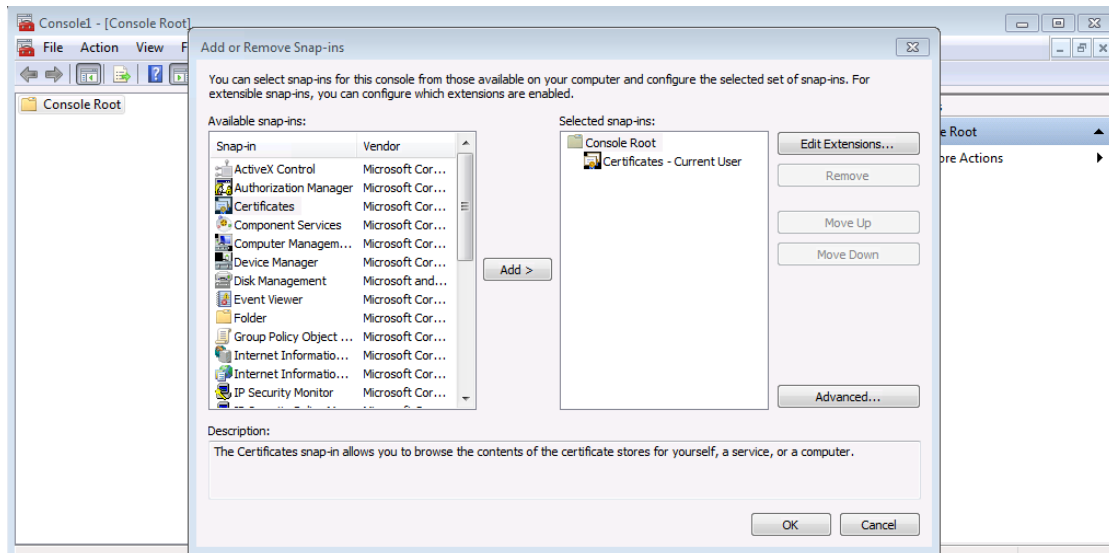
6. Now do the same for Certificate Services Client – Auto- Enrollment and set as below:



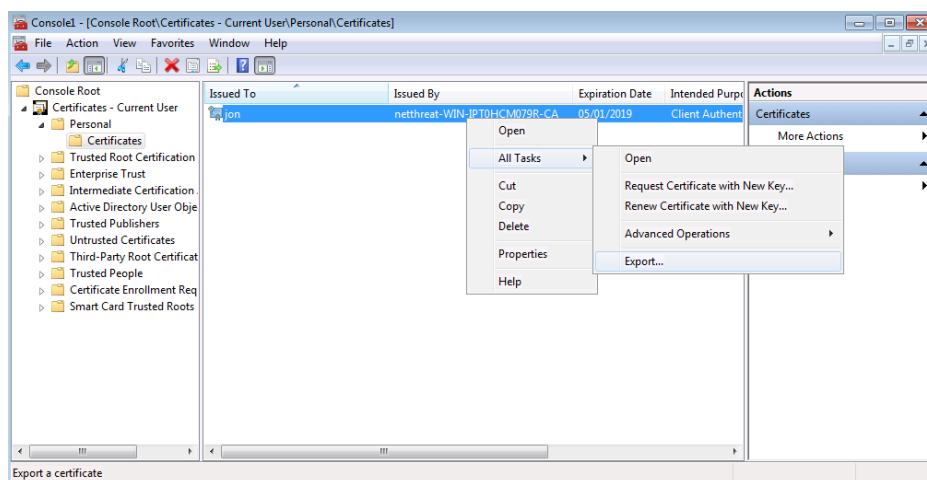
7. Once configured apply and exit the Group Policy Management console,
8. To push the policy out to the Domain Users, run the **gpupdate /force** command from the command prompt. They will then be issued their User Certificate next time they log on to the Domain.

## Exporting and Importing the User Certificate

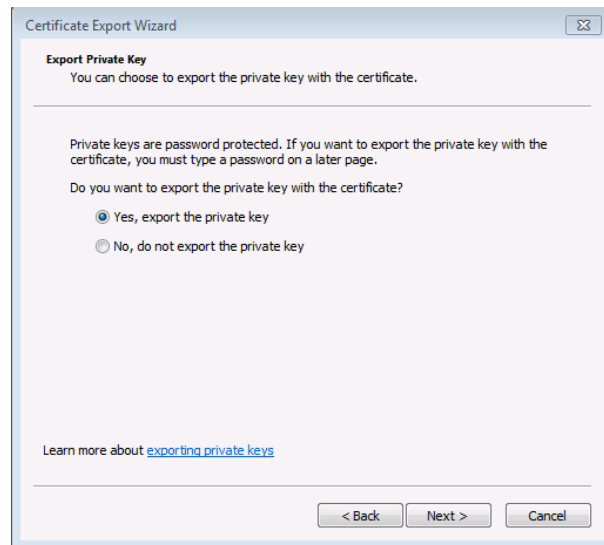
1. To Export the User Certificate go to MMC and add the snap-in for Certificates and select ok.



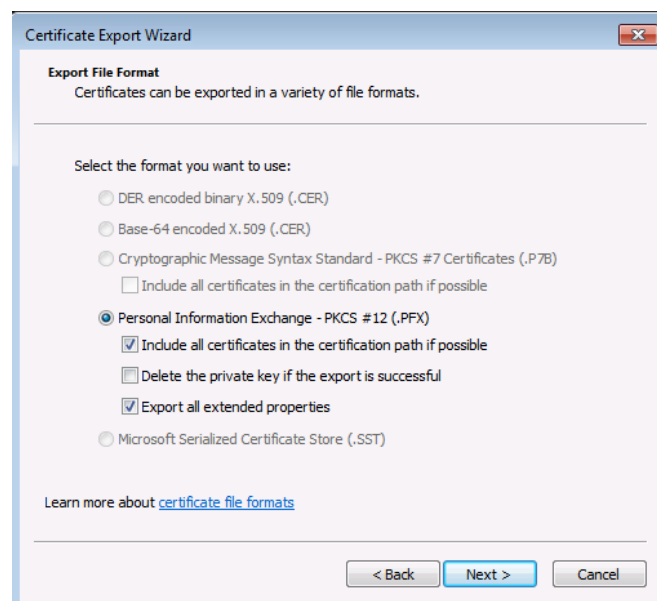
2. Browse to Personal and right click on your Certificate and choose export.



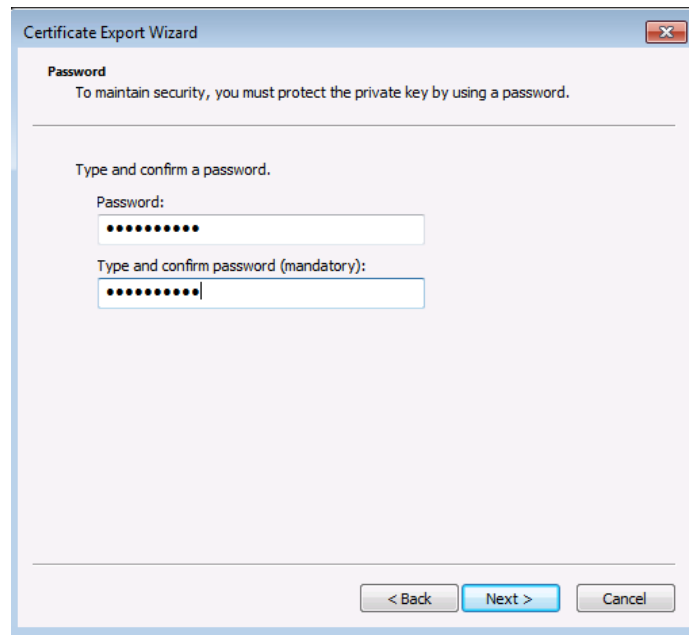
3. Choose Yes export the Private Key:



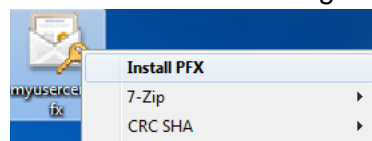
4. Select the Include all Certificates in the certification path and Export all extended properties.



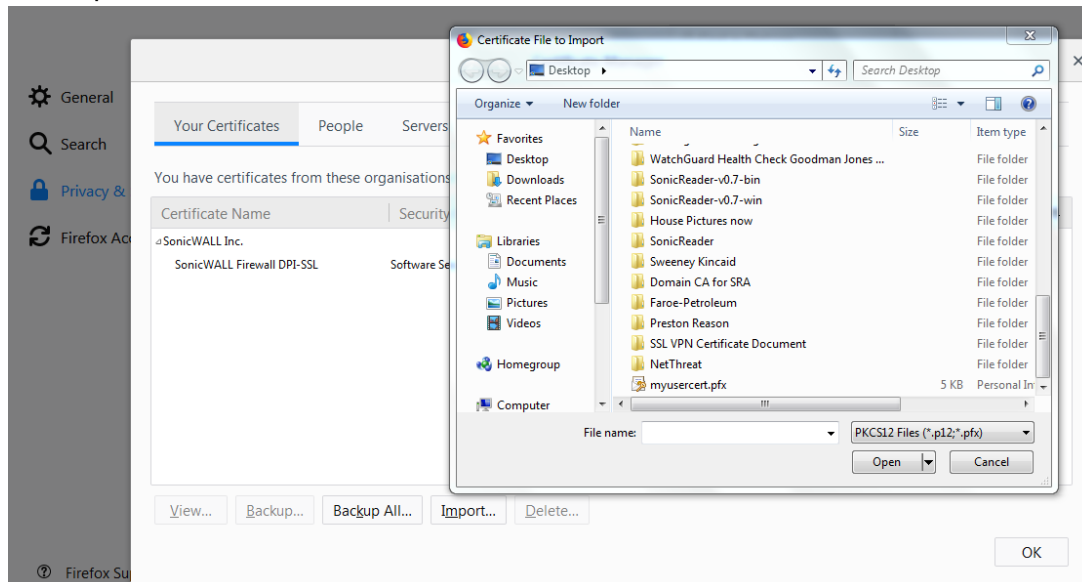
5. Give the Certificate a password and then save to a relevant folder.



6. To Import the Certificate, this may be different depending on the browser used. For I.E and Chrome you can right click the certificate and select Install PFX and go through the wizard.



7. For Firefox go to Options /Privacy and security/View Certificates and select the Your Certificates tab and Import.



## Connecting to the SSL VPN Portal and NetExtender / Mobile Connect

1. Browse to the SSL VPN Portal from your browser. Select the domain created earlier and select Login.

SONICWALL™ Virtual Office

Welcome to the SonicWall Virtual Office

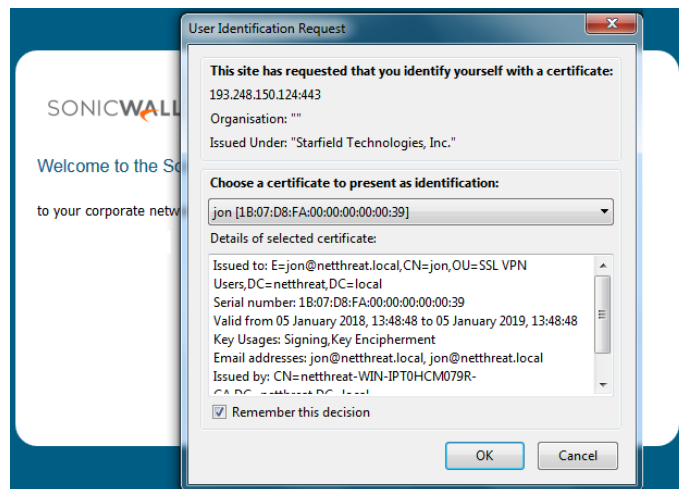
to your corporate network from anywhere on the Internet.

Username:

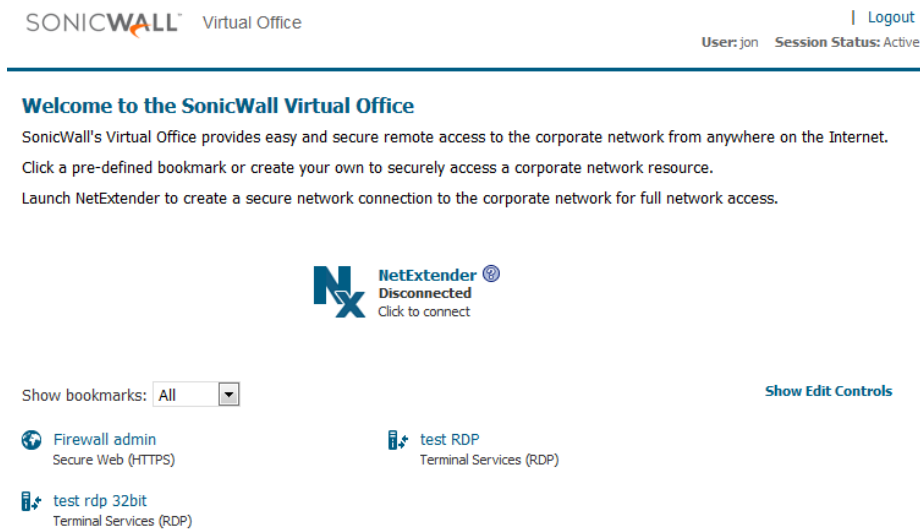
Password:

Domain:

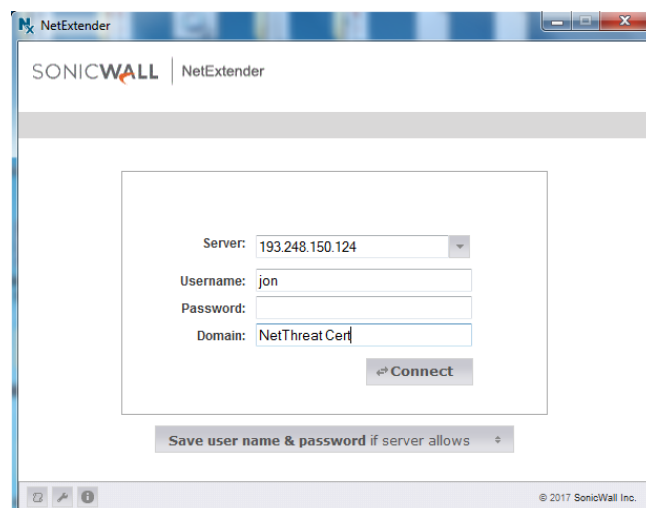
2. You will now be prompted to select the Users Certificate, choose the Certificate and ok.



- You will now be successfully logged in to the SSL VPN Portal as below.



- Using NetExtender or Mobile Connect, enter your Public IP address or FQDN in to the Server entry. Add your username and the Domain (this is case sensitive). There is no need to enter anything in the password details (unless using with another Domain that has Enable Client Certificate Check enabled).



5. You will be prompted for the Certificate to use, select and click ok.



6. You will now be connected to NetExtender.

