

---

# Setting up a Certificate Authority

Server Exploits - Module 2

---

# Overview

---

---

---

# What is a Certificate

HTTPS traffic is encrypted by a protocol (like TLS 1.2) and a cipher (like the 3DES cipher). In order to have full encrypted traffic over HTTPS, the server the client is connecting to will also need an SSL Certificate. This certificate is used to authenticate the identity of the server and encrypt the traffic between the server and the client. You can view an SSL Certificate in your browser by clicking on the lock icon next to a website's URL.

---

# What is a Certificate

Certificate Viewer: \*.nsc.ca

General

Details

Issued To

Common Name (CN)	*.nsc.ca
Organization (O)	Nova Scotia Community College
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	GlobalSign RSA OV SSL CA 2018
Organization (O)	GlobalSign nv-sa
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Thursday, November 24, 2022 at 9:51:02 AM
Expires On	Tuesday, December 26, 2023 at 9:51:01 AM

Fingerprints

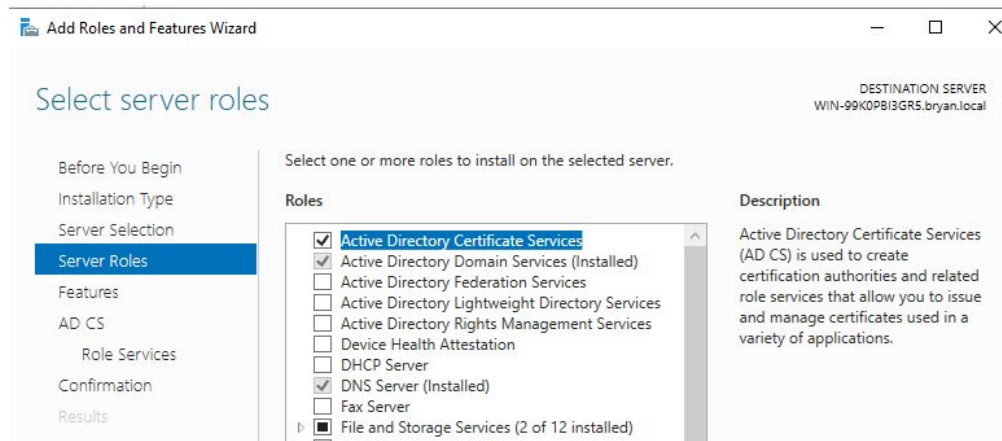
SHA-256 Fingerprint	A2 FB 45 FB EF 37 A3 61 0D 29 7C C9 12 85 F1 85 93 2C 45 AB 80 89 FE 57 8C EB E6 48 75 77 38 FD
SHA-1 Fingerprint	0F E8 39 40 E8 77 72 47 6D BB 9A 6D 5B AE BF 2B 67 FC 1E 51

# Setup

---

# Configuring a CA

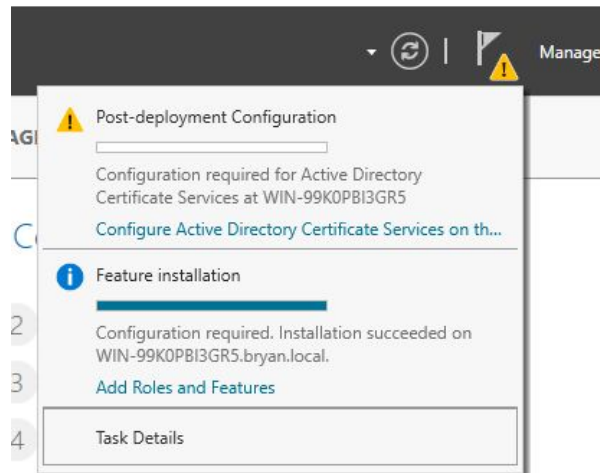
If we want to get Win-RM to communicate over HTTPS, we will have to create a certificate for the DC. Firstly, we will need to add the Active Directory Certificate Services feature. You can do this the same way you created the DC.



---

# Configuring a CA

For the roles, we just need a certificate authority. This will designate the DC as the authority to create and sign SSL Certificates for your domain. You will see an alert message to Configure AD Certificate Services.



---

# Configuring a CA

You will need to add your Domain Admin's credentials.

The screenshot shows the 'Credentials' step of the Windows Server Configuration Wizard. On the left is a navigation pane with the following items: 'Credentials' (highlighted in blue), 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main area is titled 'Specify credentials to configure role services'. In the top right corner, it says 'DESTINATION SEI WIN-99K0PB13GR5.bryan.'. Below the title, there are two sections of instructions. The first section states 'To install the following role services you must belong to the local Administrators group:' and lists three items: 'Standalone certification authority', 'Certification Authority Web Enrollment', and 'Online Responder'. The second section states 'To install the following role services you must belong to the Enterprise Admins group:' and lists four items: 'Enterprise certification authority', 'Certificate Enrollment Policy Web Service', 'Certificate Enrollment Web Service', and 'Network Device Enrollment Service'. At the bottom, there is a 'Credentials:' label followed by a text box containing 'BRYAN\beard' and a 'Change...' button.

Credentials

DESTINATION SEI  
WIN-99K0PB13GR5.bryan.

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: BRYAN\beard Change...

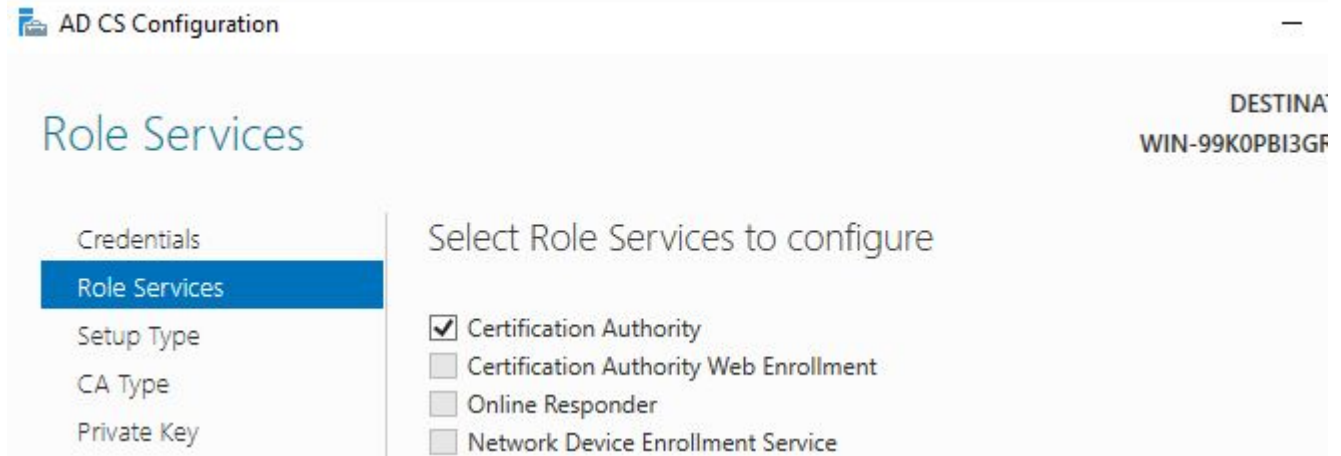


---

# Configuring a CA

Roll Services will just be Certificate Authority

---



The screenshot shows the 'AD CS Configuration' console window. The title bar reads 'AD CS Configuration'. The main area is titled 'Role Services'. On the right, the destination is listed as 'DESTINATION: WIN-99K0PBI3GF'. On the left, a navigation pane lists 'Credentials', 'Role Services' (which is selected and highlighted in blue), 'Setup Type', 'CA Type', and 'Private Key'. The main content area is titled 'Select Role Services to configure' and contains a list of services with checkboxes: 'Certification Authority' (checked), 'Certification Authority Web Enrollment' (unchecked), 'Online Responder' (unchecked), and 'Network Device Enrollment Service' (unchecked).

AD CS Configuration

Role Services

DESTINATION: WIN-99K0PBI3GF

Credentials

**Role Services**

Setup Type

CA Type

Private Key

Select Role Services to configure

- ☒ Certification Authority
- ☐ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service

---

---

# Configuring a CA

Click Enterprise CA. This is for domain members.

Setup Type

DESTINATION SERVER  
WIN-99K0PBI3GR5.bryan.local

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

☒ Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

---

# Configuring a CA

Because this is our first Certificate Authority, click Root CA. Click Next and create a new private key.

DESTINATION SERVER  
WIN-99K0PBI3GR5.bryan.local

CA Type

Credentials

Role Services

Setup Type

**CA Type**

Private Key

Cryptography

CA Name

## Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

☒ Root CA

Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

# Configuring a CA

For your private key, there are some best practices. Nowadays, the private key should be at least RSA 2048 for its cryptographic provider and the signing algorithm must be at least SHA256 (do not use SHA1 or MD5 as these are weak encryption algorithms).

Cryptography for CA

DESTINATION SERVER  
WIN-99K0PBI3GR5.bryan.local

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
**Cryptography**  
CA Name  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512
- SHA1
- MD5

☐ Allow administrator interaction when the private key is accessed by the CA.

---

# Configuring a CA

Your CA Name details should be automatically filled out. This sets your DC as the CA.

CA Name

DESTINATION SERVER  
WIN-99K0PBI3GR5.bryan.local

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
Cryptography  
**CA Name**  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:

Distinguished name suffix:

Preview of distinguished name:

---

---

# Configuring a CA

You can set your validity period to be however long you want. 5 Years is good. This means you will have to redo your CA in 5 years time.

The default certificate database folder path is OK, so don't change that either.

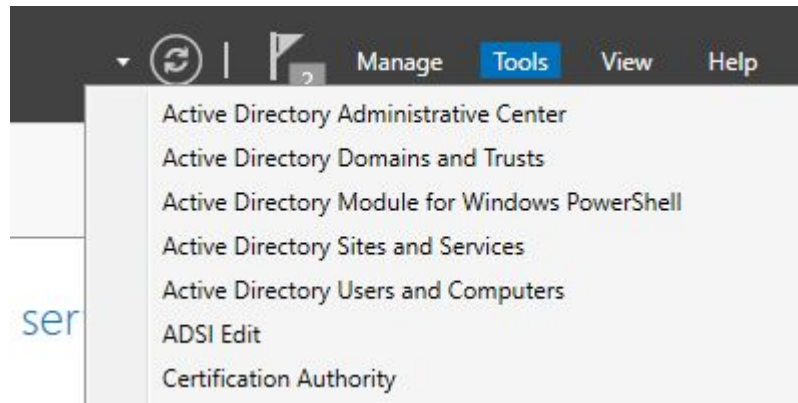
Click Configure when you are done.

---

---

# Configuring a CA

You should now see Certificate Authority under your Tools in Server Manager. Open it.



# Creating a Certificate

---



---

# Creating a Certificate

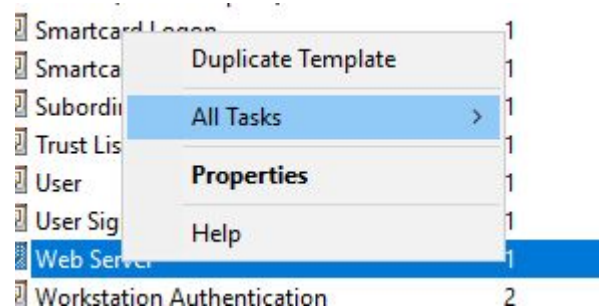
Right-Click Certificate Templates and hit Manage



---

# Creating a Certificate

Find the Web Server Template and right-click and select Duplicate Template



---

---

# Creating a Certificate

Under the General tab, you can name your new certificate template under the Template display name field. I have called mine WinRM.

---

---

# Creating a Certificate

Under the Subject Name Tab, select “Build from AD Information”. Select Common name for the Subject Name Format, and include only DNS name as alternate subject name.

Properties of New Template ✕

Superseded Templates		Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name		Server	Issuance Requirements	

☐ 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

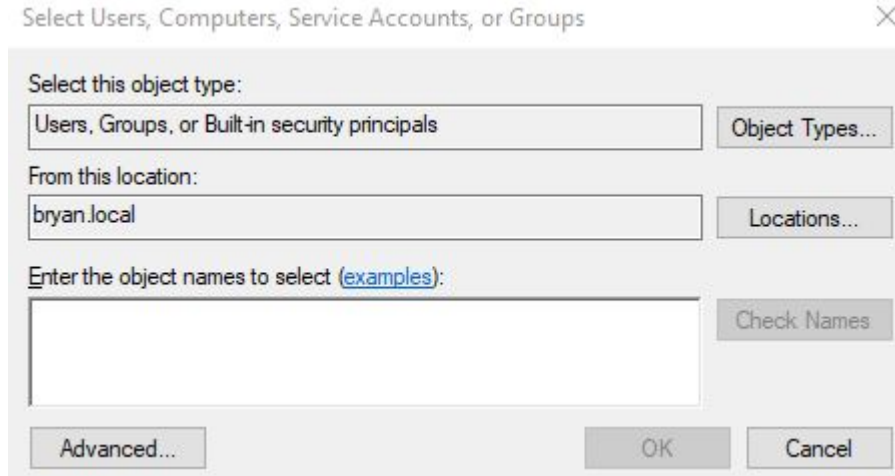
☐ User principal name (UPN)

☐ Service principal name (SPN)

---

# Creating a Certificate

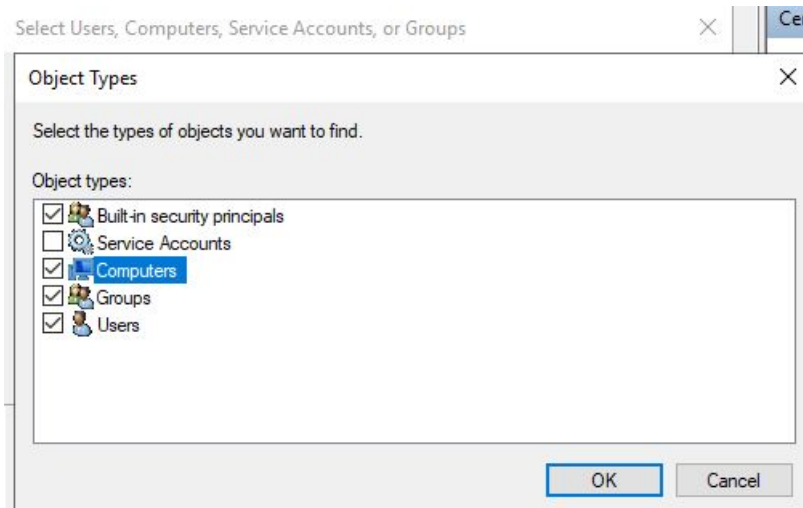
Under the Security tab, click Add to Add a group. You will see the following Window.



---

# Creating a Certificate

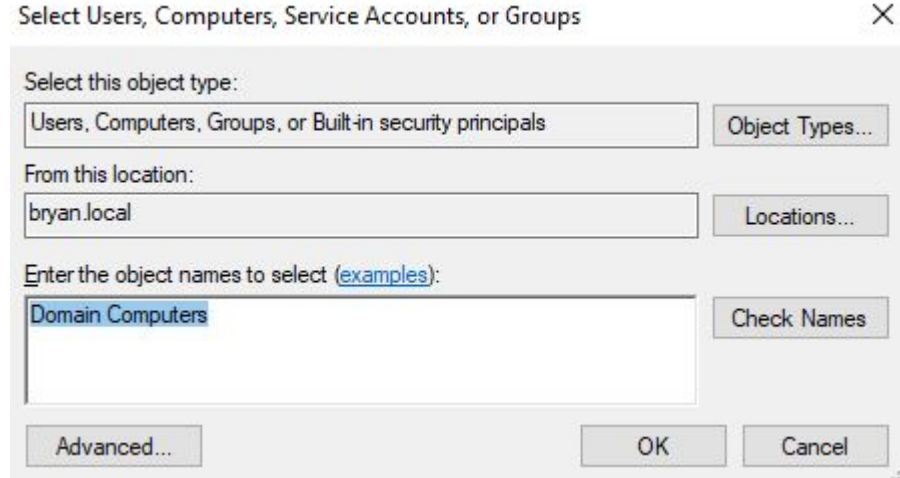
Click “Object Types and ensure the Computers box is checked. Hit OK when you are done.



---

# Creating a Certificate

Now Add the Domain Computers group and hit OK.



# Creating a Certificate

Give Read, Enroll and Autoenroll permissions to the Domain Computers group. The hit Apply.

The screenshot shows the 'Security' tab of the 'Certificate Template Properties' dialog box. The 'Group or user names' list contains five entries: 'Authenticated Users', 'Administrator', 'Domain Admins (BRYAN\Domain Admins)', 'Domain Computers (BRYAN\Domain Computers)' (which is selected), and 'Enterprise Admins (BRYAN\Enterprise Admins)'. Below this list are 'Add...' and 'Remove' buttons. The 'Permissions for Domain Computers' section contains a table with columns for 'Allow' and 'Deny'. The permissions listed are 'Full Control', 'Read', 'Write', 'Enroll', and 'Autoenroll'. The 'Read', 'Enroll', and 'Autoenroll' permissions are checked in the 'Allow' column. At the bottom, there is a note: 'For special permissions or advanced settings, click Advanced.' and an 'Advanced' button.

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security

Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (BRYAN\Domain Admins)
- Domain Computers (BRYAN\Domain Computers)**
- Enterprise Admins (BRYAN\Enterprise Admins)

Add... Remove

Permissions for Domain Computers	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

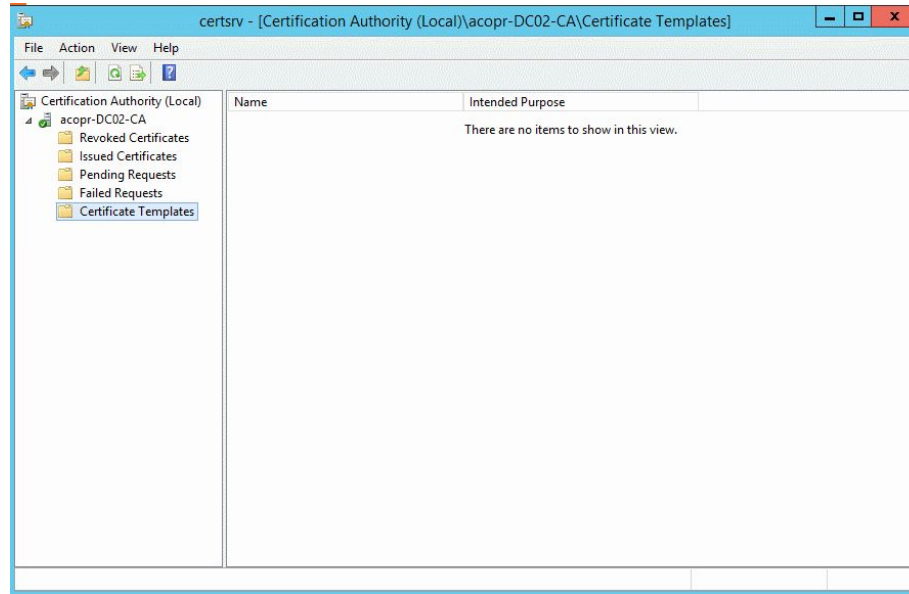
Advanced



---

# Creating a Certificate

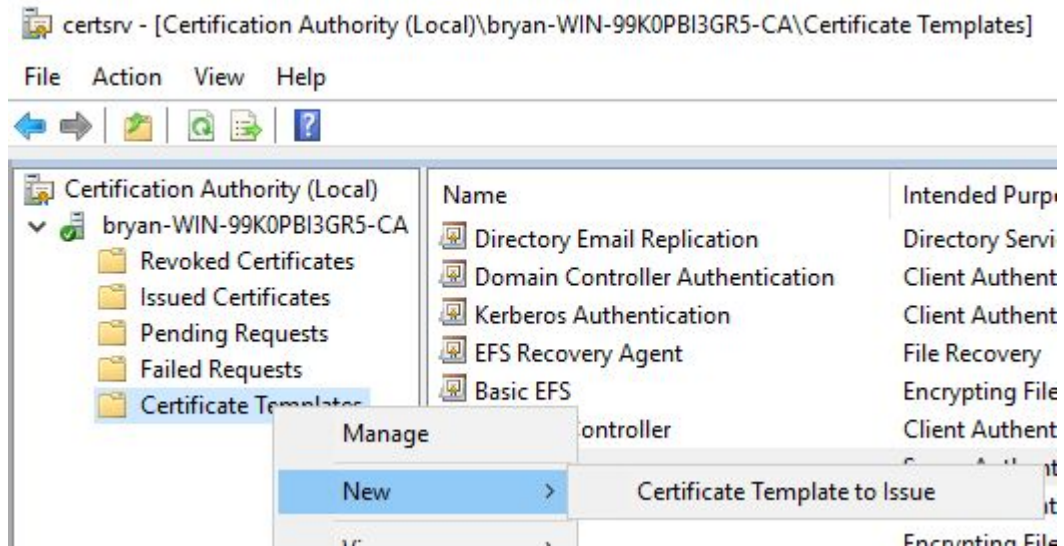
Here is an animation of the previous steps. This animation checks UPN under Subject Name, which is not required.



---

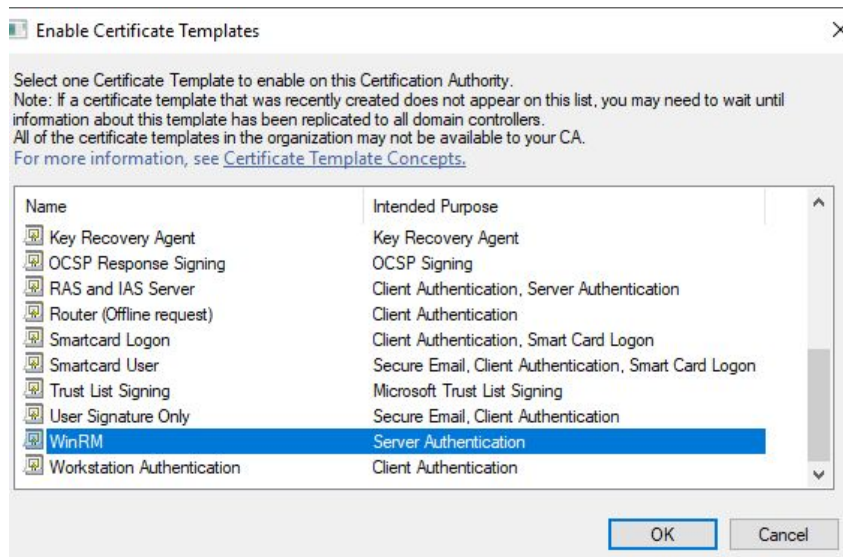
# Creating a Certificate

Go back to the certsrv window, right click Certificate Templates -> new -> Certificate Template to Issue



# Creating a Certificate

Find your WinRM certificate and Click OK.



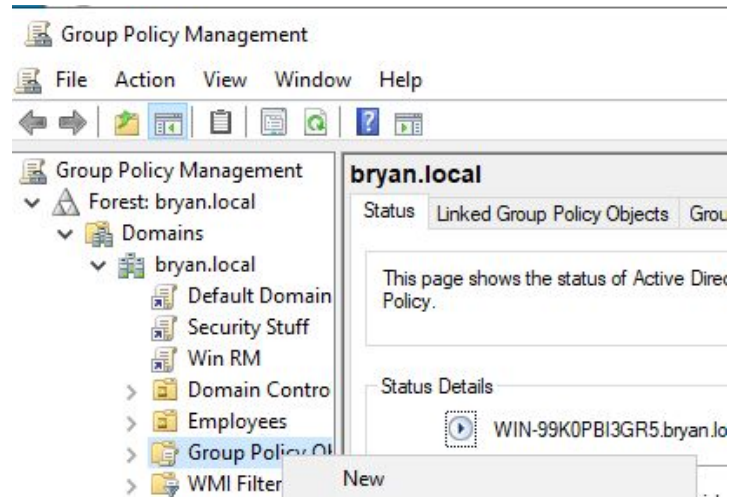
# Pushing Out the Certificate

---

---

# Creating a Certificate

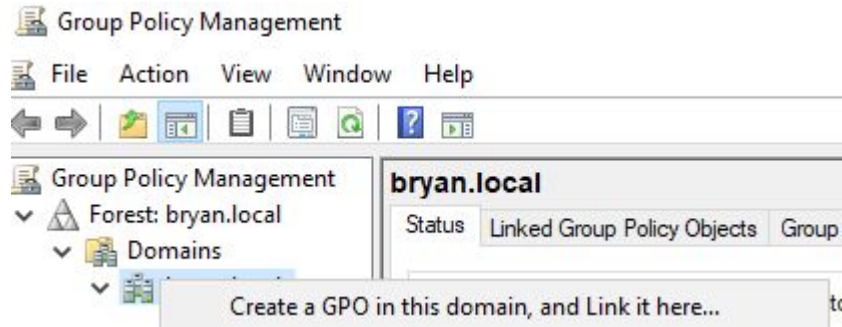
With the certificate created, we can now use a GPO to push it out to all machines in your domain. Open up GPMC and create a new GPO. You can call it whatever you'd like.



---

# Creating a Certificate

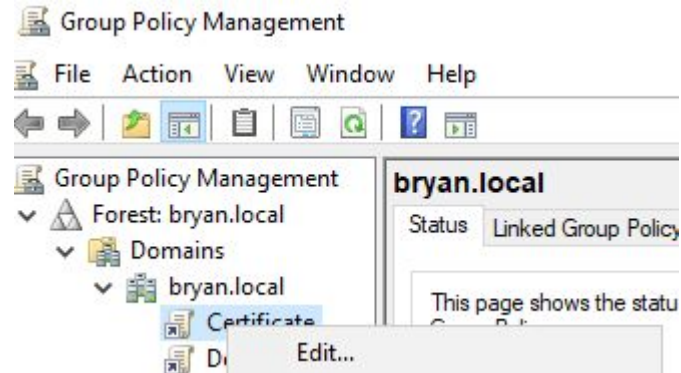
With the certificate created, we can now use a GPO to push it out to all machines in your domain. Open up GPMC and create a new GPO by right-clicking your domain and clicking Create a GPO in this domain and Link it here. You can call it whatever you'd like, I have called mine "Certificate".



---

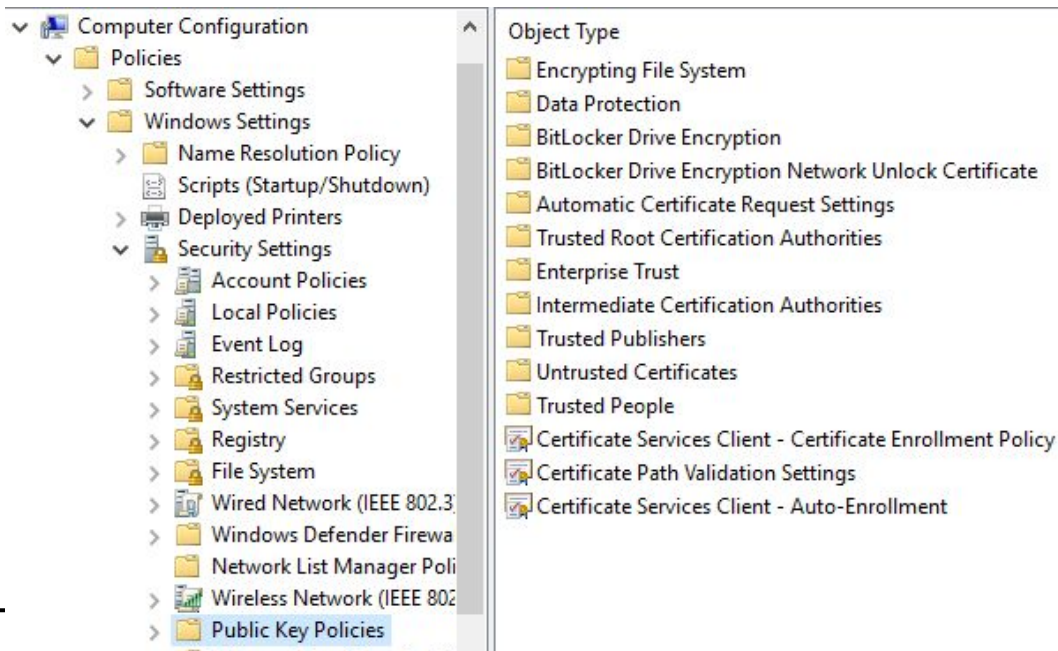
# Creating a Certificate

Right-click your new GPO and click Edit.



# Creating a Certificate

Go to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Public Key Policies

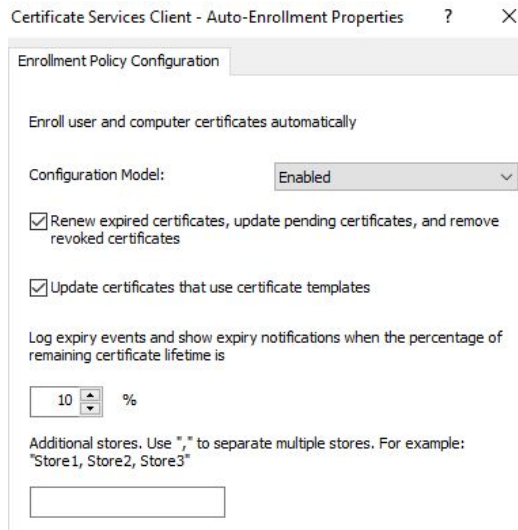




---

# Creating a Certificate

Double click Certificate Services Client - Auto Enrollment and set the configuration model to enable. Check both boxes.



The screenshot shows the 'Certificate Services Client - Auto-Enrollment Properties' dialog box with the 'Enrollment Policy Configuration' tab selected. The 'Enroll user and computer certificates automatically' section is active. The 'Configuration Model' is set to 'Enabled'. Two checkboxes are checked: 'Renew expired certificates, update pending certificates, and remove revoked certificates' and 'Update certificates that use certificate templates'. Below these, there is a section for logging expiry events with a percentage spinner set to 10%. At the bottom, there is a text field for 'Additional stores' with a placeholder example: 'Store1, Store2, Store3'.

Certificate Services Client - Auto-Enrollment Properties ? X

Enrollment Policy Configuration

Enroll user and computer certificates automatically

Configuration Model: Enabled

☒ Renew expired certificates, update pending certificates, and remove revoked certificates

☒ Update certificates that use certificate templates

Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is

10 %

Additional stores. Use ", " to separate multiple stores. For example: "Store1, Store2, Store3"

# Creating a Certificate

Hit apply and run `gpupdate /force` on your workstation and DC. If you go back to your Certificate Authority under Tools in Server Manager, then go to Issues Certificates, you should see your certificates issued to your workstation and DC.

