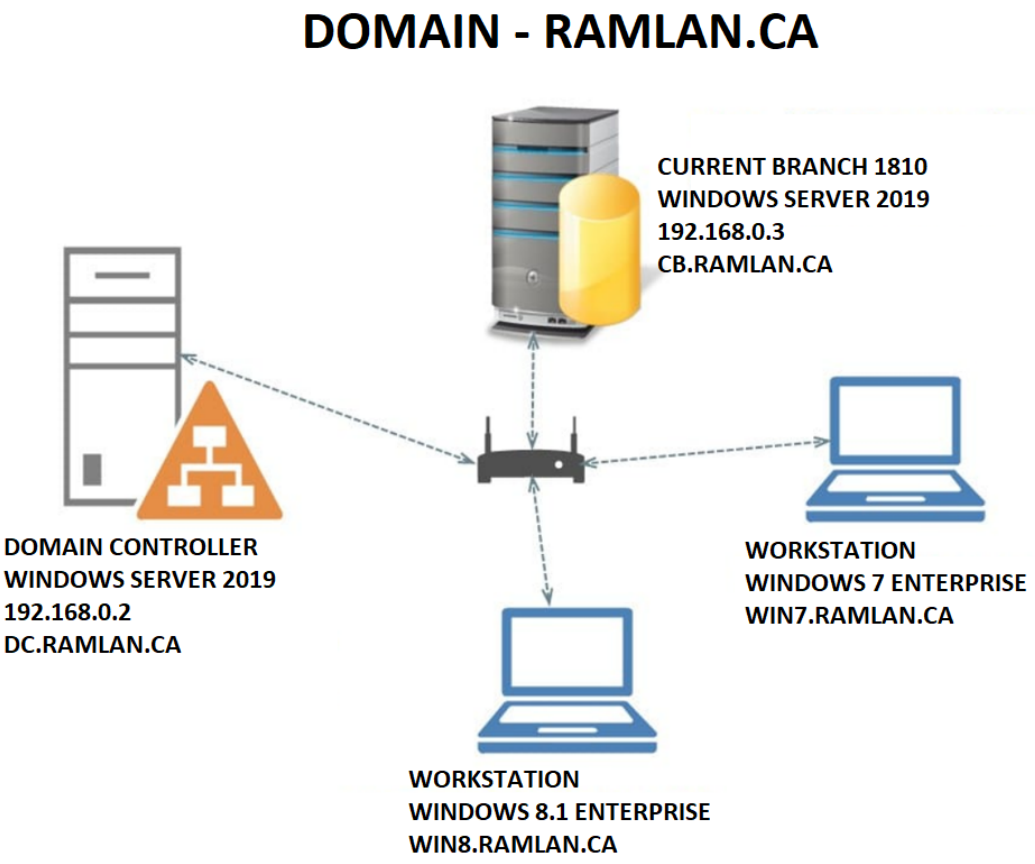
PKI (Public Key Infrastructure) Implementation for CB1810

In this post, I will show you how to deploy PKI for Current Branch 1810. PKI is being deployed in large organization to keep communication secured between clients and server.

An individual who intends to communicate securely with others can distribute the public key but must keep the private key secret. Content encrypted by using one of the keys can be decrypted by using the other. PKI can be used to secure e-mail, secure web communications, secure web sites, digital signing of software files etc.

When you use Active Directory Certificate Services and certificate templates, the Microsoft PKI solution can ease the management of the certificates. One thing to note here is template-based certificates can be issued only by an enterprise certification authority running on the Enterprise Edition or Datacenter Edition of the server operating system.

The HTTPS protocol provides client-to-server communications that are mutually authenticated, signed, and encrypted. Internet clients must use HTTPS, and all clients are more secure if configured to use HTTPS. You must deploy the required certificate to each client and site system that will use HTTPS.



PKI Requirements:

Certificate Requirement	Certificate Description
Web server certificate for site systems that run IIS	This certificate is used to encrypt data and authenticate the server to clients. It must be installed externally from Configuration Manager on site systems servers that run IIS and that are configured in Configuration Manager to use HTTPS.
Client certificate for Windows computers	This certificate is used to authenticate Configuration Manager client computers to site systems that are configured to use HTTPS. It can also be used for management points and state migration points to monitor their operational status when they are configured to use HTTPS. It must be installed externally from Configuration Manager on computers.
Client certificate for distribution points	The certificate is used to authenticate the distribution point to an HTTPS-enabled management point before the distribution point sends status messages. When the Enable PXE support for clients distribution point option is selected, the certificate is sent to computers that PXE boot so that they can connect to a HTTPS-enabled management point during the deployment of the operating system.
Client certificate for Mac computers	This certificate is used to authenticate Configuration Manager Mac computers to management points and distribution points that are configured to support HTTPS. You can request and install this certificate from a Mac computer when you use Configuration Manager enrollment and select the configured certificate template as a mobile device client setting.

A typical PKI consists of the following elements.

Element	Description
Certification Authority	Acts as the root of trust in a public key infrastructure and provides services that authenticate the identity of individuals, computers, and other entities in a network.
Registration Authority	Is certified by a root CA to issue certificates for specific uses permitted by the root. In a Microsoft PKI, a registration authority (RA) is usually called a subordinate CA.
Certificate Database	Saves certificate requests and issued and revoked certificates and certificate requests on the CA or RA.
Certificate Store	Saves issued certificates and pending or rejected certificate requests on the local computer.
Key Archival Server	Saves encrypted private keys in the certificate database for recovery after loss.

Deploying Web Server Certificate for Site Systems That Run IIS:

1) Creating and Issuing the Web Server Certificate Template on the Certification Authority

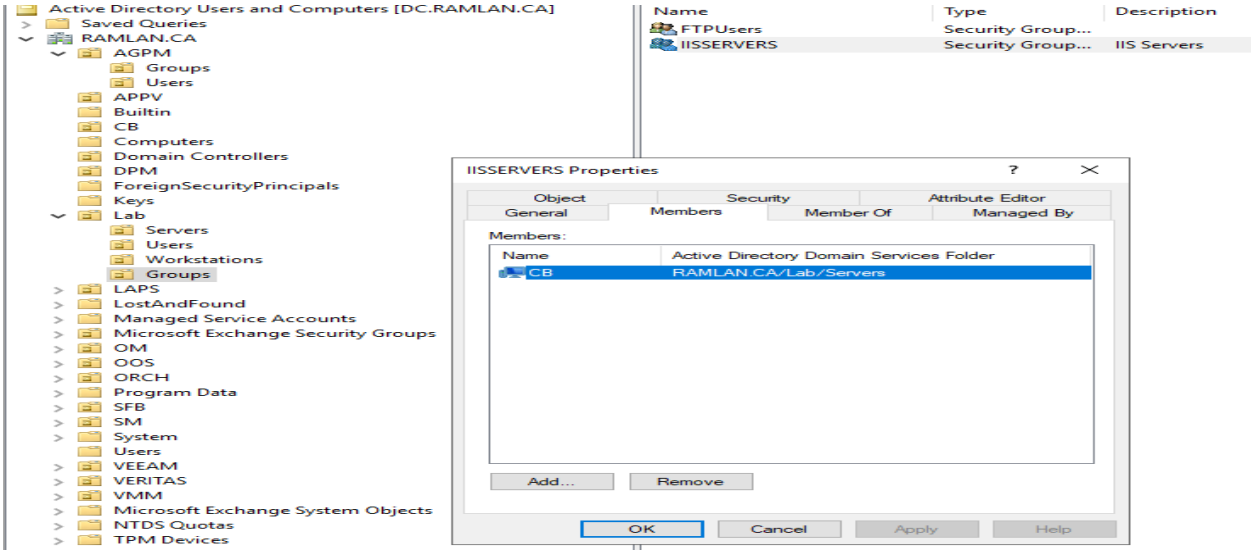
2) Requesting the Web Server Certificate

3) Configuring IIS to Use the Web Server Certificate

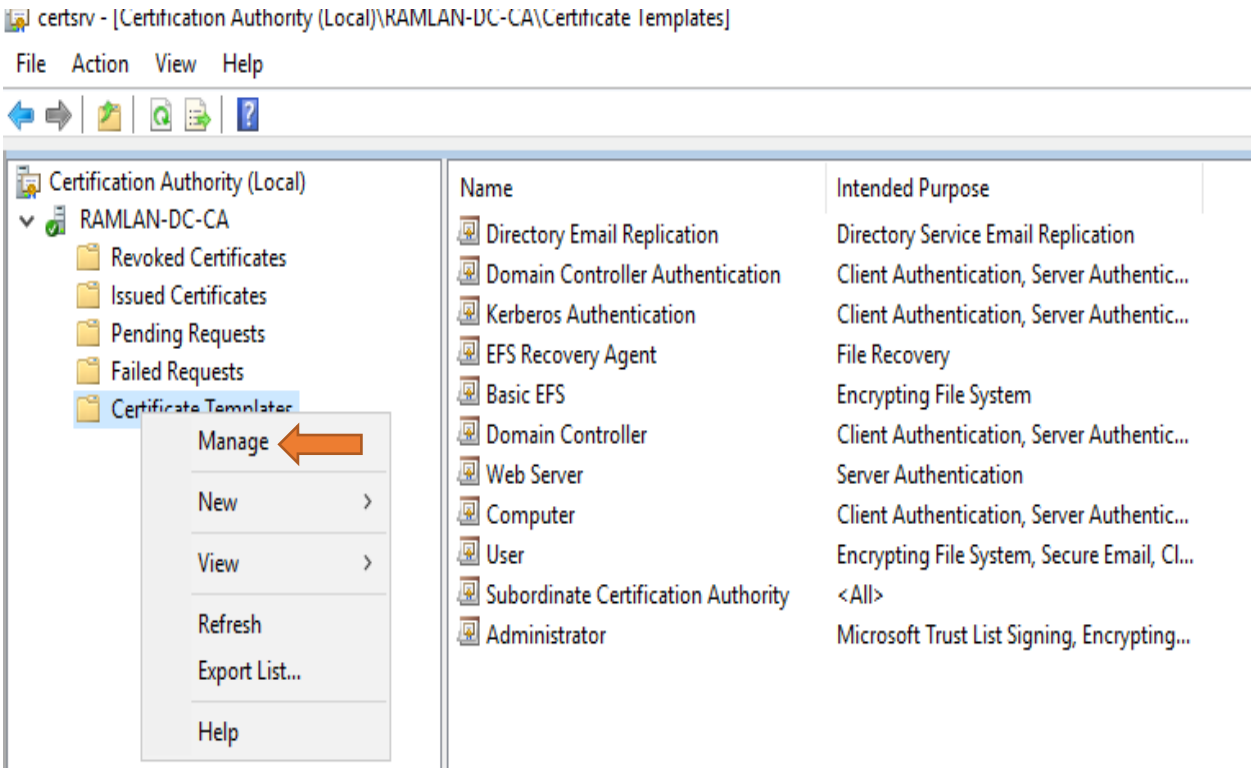
This certificate is used to encrypt data and authenticate the server to clients. It must be installed externally from Configuration Manager on site systems servers that run IIS and that are configured in Configuration Manager to use HTTPS.

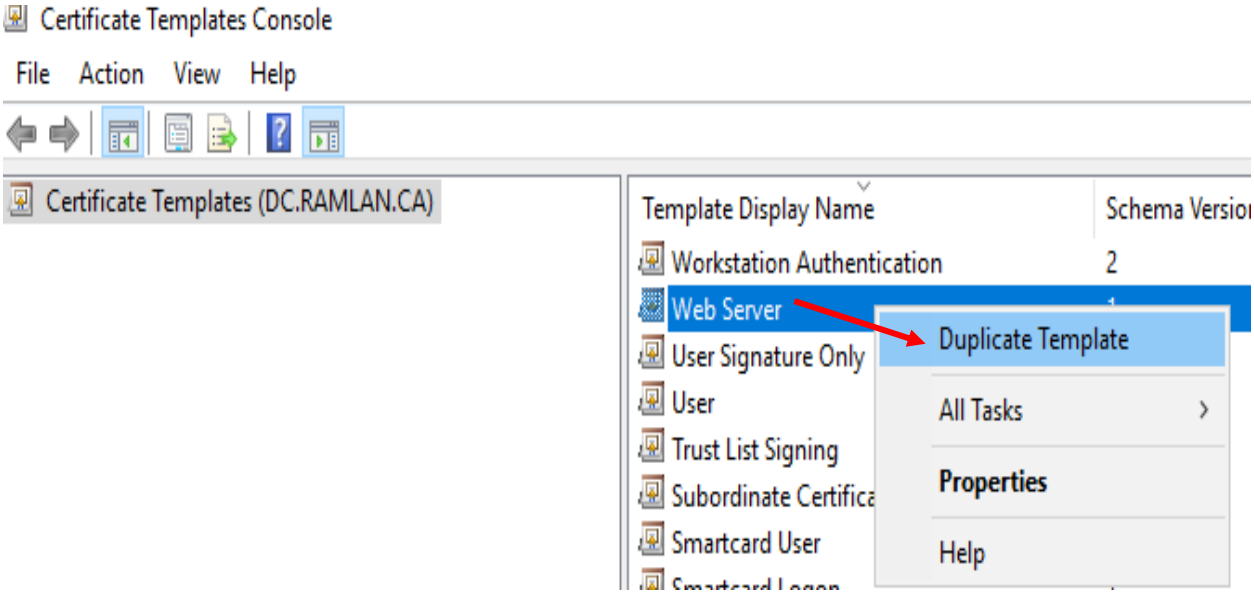
Security Group:

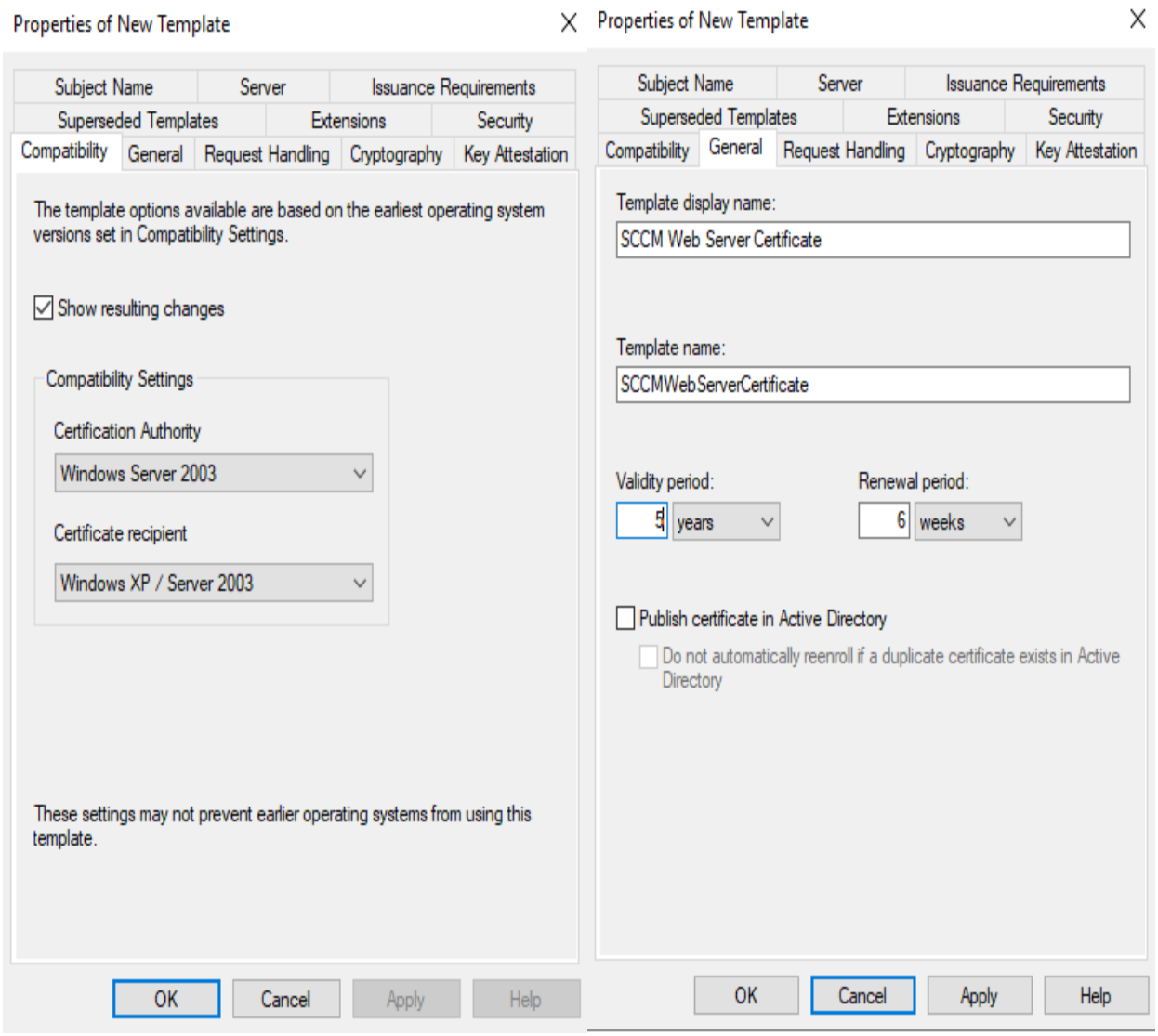
Before we start certificate configuration, I did create a security group called **IISSERVERS** and added CB to that group so we can target the certificate for this group later.

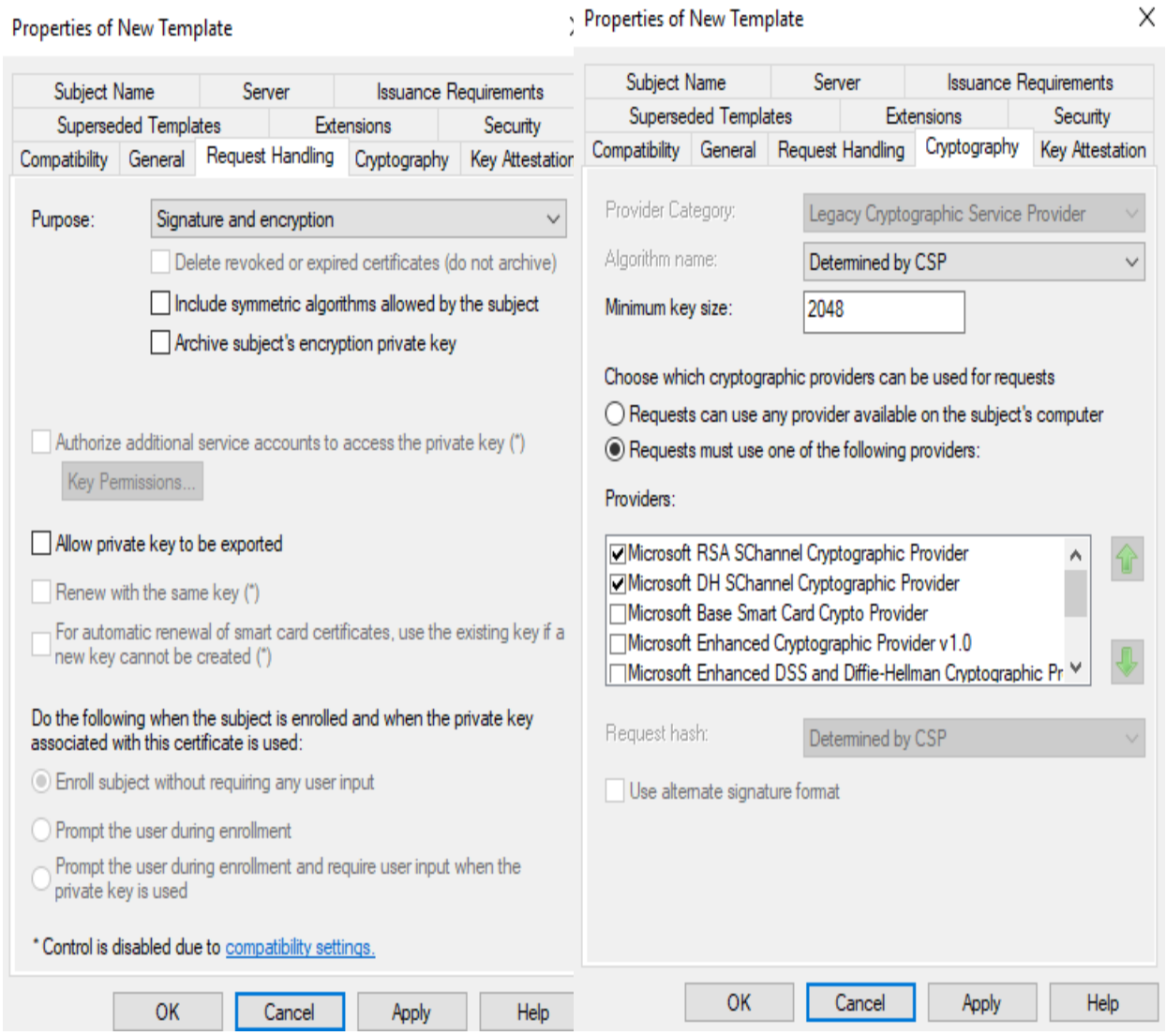


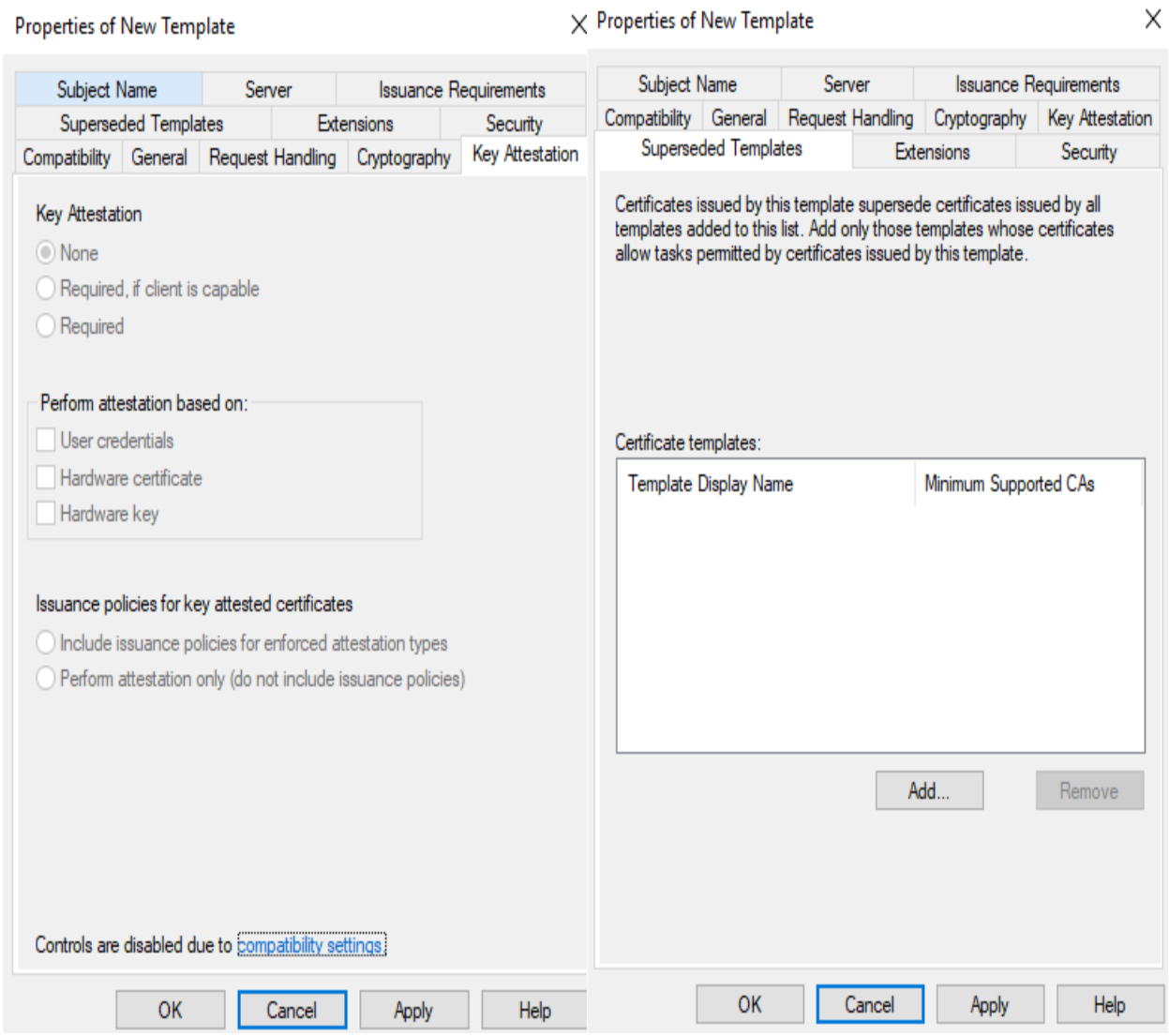
Open Certification Authority from Domain Controller to start **Web Server Certificate**.

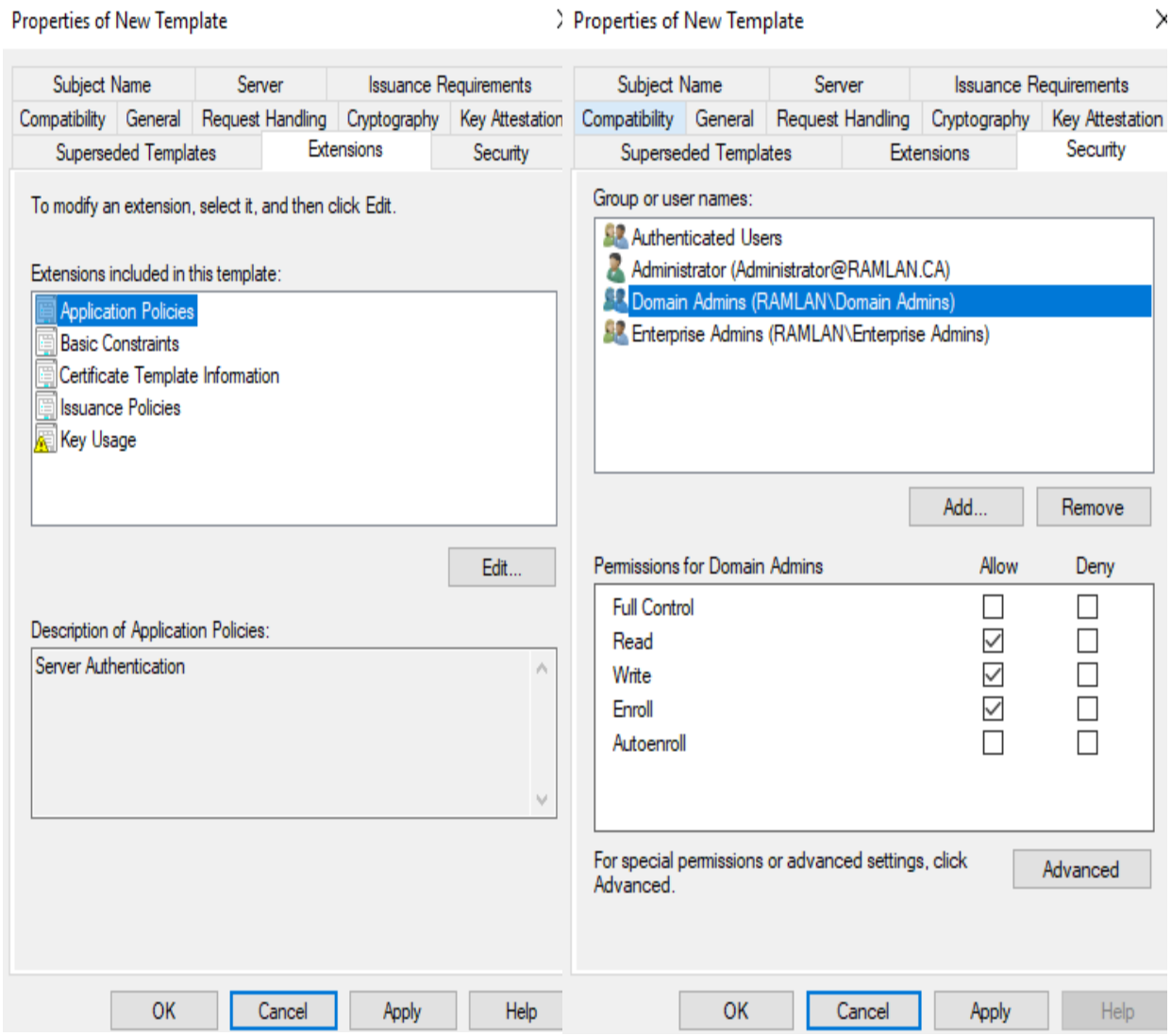


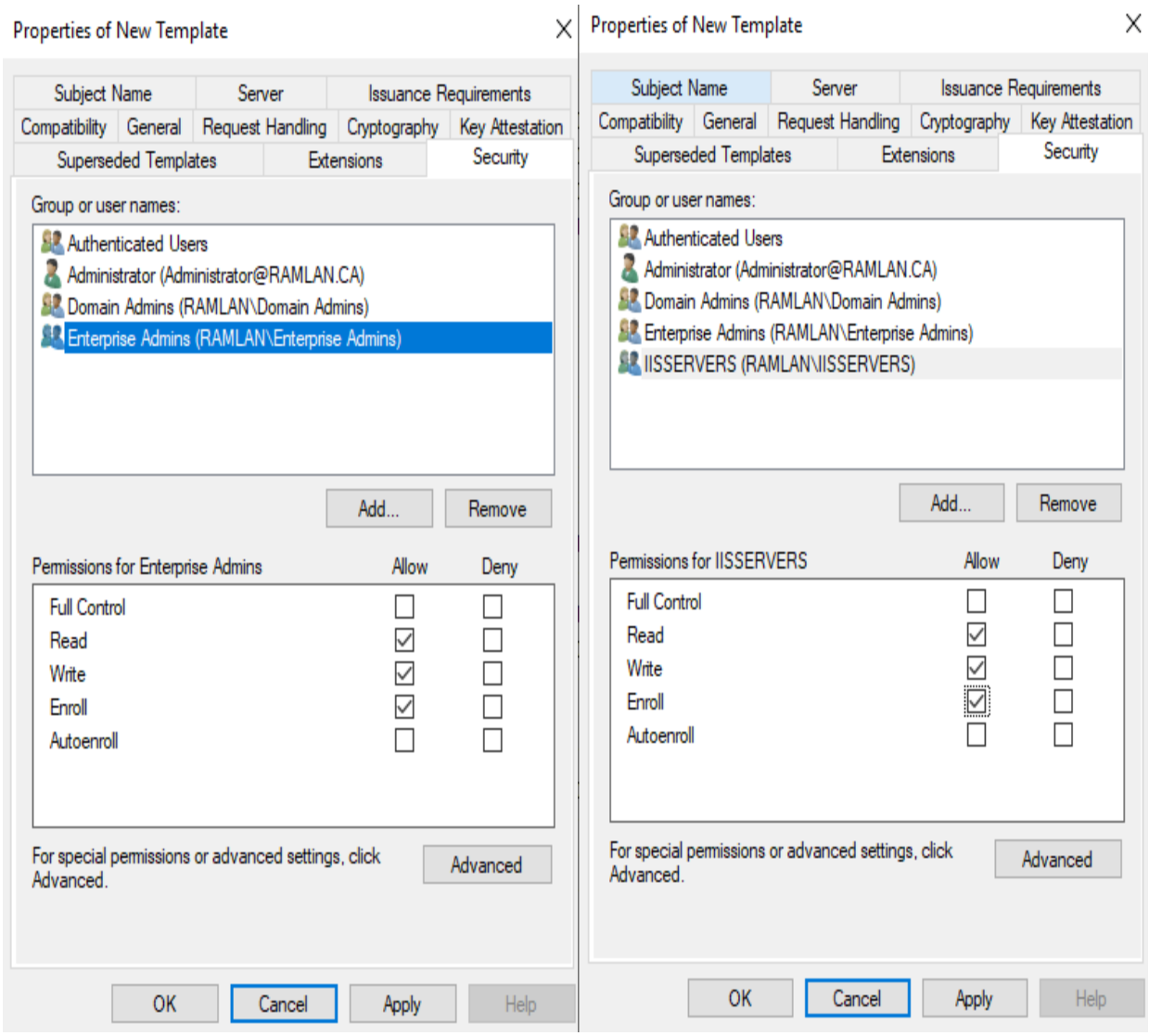


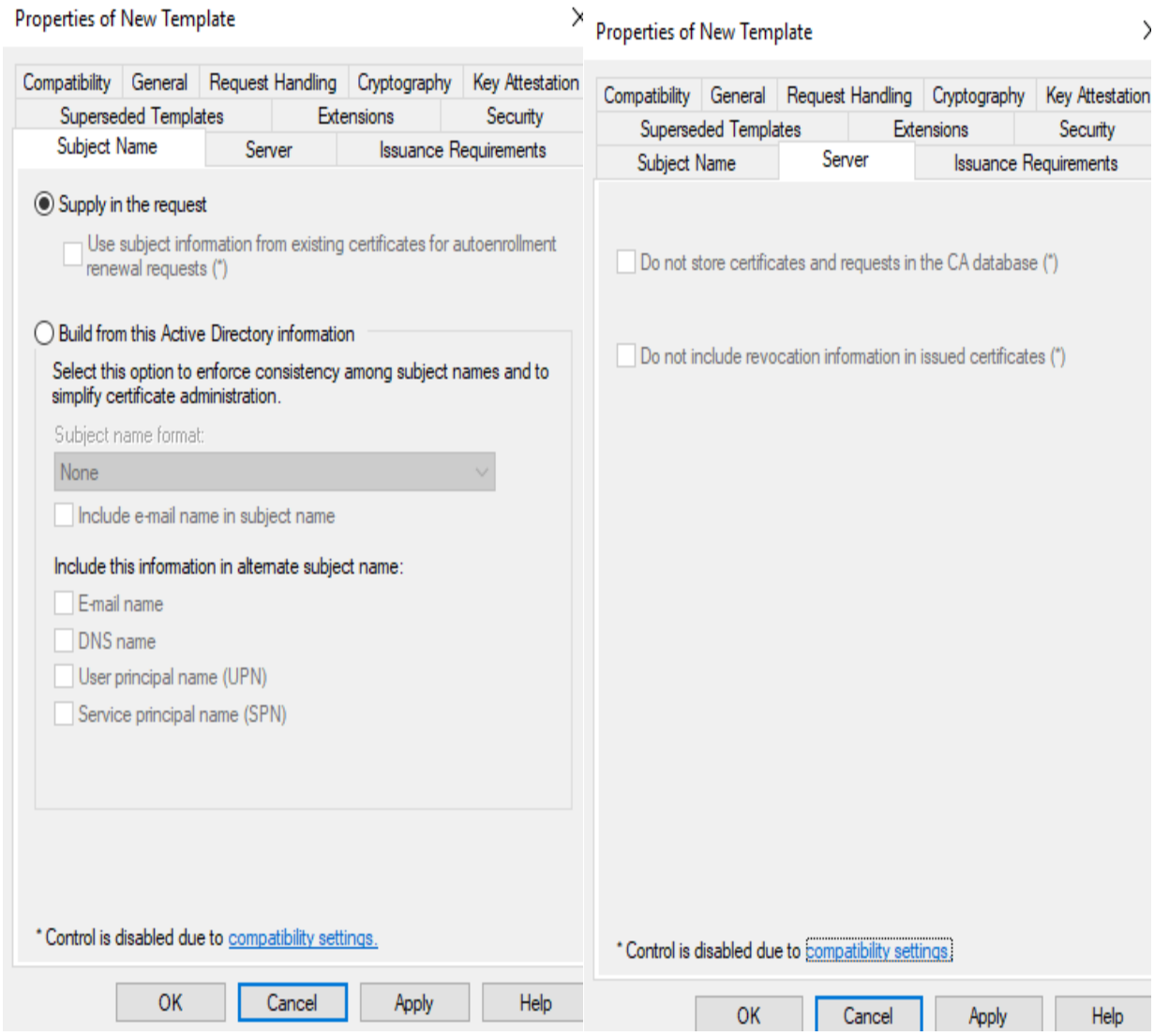

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
The template options available are based on the earliest operating system versions set in Compatibility Settings.
Show resulting 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.
OK
Cancel
Apply
Help
Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Template display name:
SCCM Web Server Certificate
Template name:
SCCMWebServerCertificate
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
OK
Cancel
Apply
Help

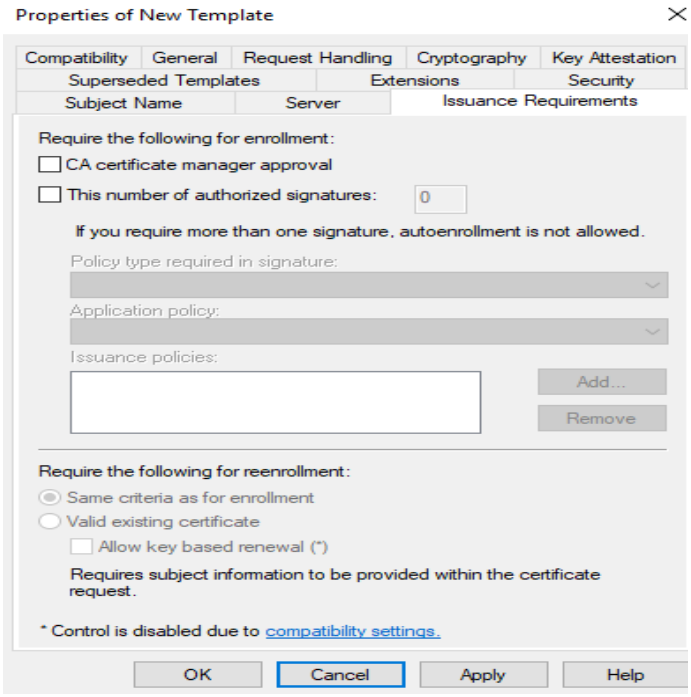

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Purpose:
Signature and encryption
Delete revoked or expired certificates (do not archive)
Include symmetric algorithms allowed by the subject
Archive subject's encryption private key
Authorize additional service accounts to access the private key (*)
Key Permissions...
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.
OK
Cancel
Apply
Help
Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Provider Category:
Legacy Cryptographic Service Provider
Algorithm name:
Determined by CSP
Minimum key size:
2048
Choose which cryptographic providers can be used for requests
Requests can use any provider available on the subject's computer
Requests must use one of the following providers:
Providers:
Microsoft RSA SChannel Cryptographic Provider
Microsoft DH SChannel Cryptographic Provider
Microsoft Base Smart Card Crypto Provider
Microsoft Enhanced Cryptographic Provider v1.0
Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr
Request hash:
Determined by CSP
Use alternate signature format
OK
Cancel
Apply
Help

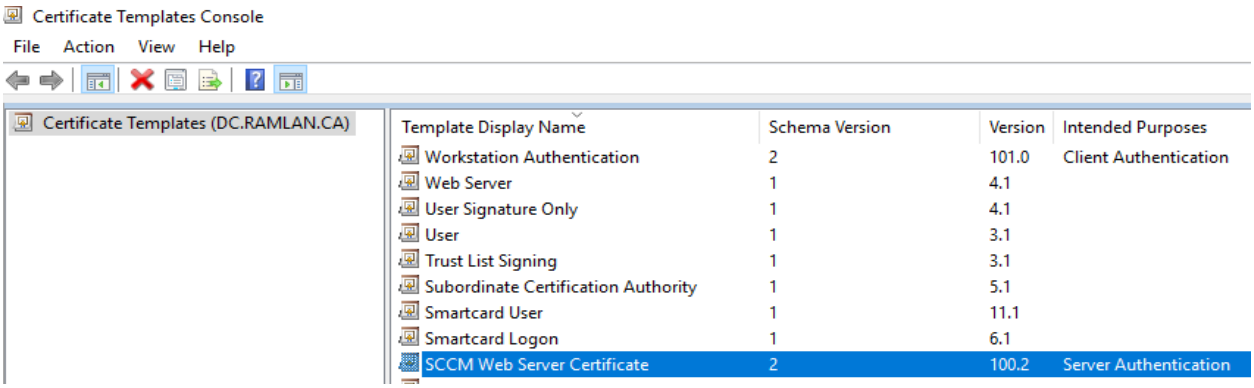

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Key Attestation
None
Required, if client is capable
Required
Perform attestation based on:
User credentials
Hardware certificate
Hardware key
Issuance policies for key attested certificates
Include issuance policies for enforced attestation types
Perform attestation only (do not include issuance policies)
Controls are disabled due to compatibility settings
OK
Cancel
Apply
Help
Properties of New Template
Subject Name
Server
Issuance Requirements
Compatibility
General
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Certificates issued by this template supersede certificates issued by all templates added to this list. Add only those templates whose certificates allow tasks permitted by certificates issued by this template.
Certificate templates:
Template Display Name
Minimum Supported CAs
Add...
Remove
OK
Cancel
Apply
Help


Properties of New Template
Subject Name
Server
Issuance Requirements
Compatibility
General
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
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
Edit...
Description of Application Policies:
Server Authentication
OK
Cancel
Apply
Help
Properties of New Template
Subject Name
Server
Issuance Requirements
Compatibility
General
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Group or user names:
Authenticated Users
Administrator (Administrator@RAMLAN.CA)
Domain Admins (RAMLAN\Domain Admins)
Enterprise Admins (RAMLAN\Enterprise Admins)
Add...
Remove
Permissions for Domain Admins
Allow
Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

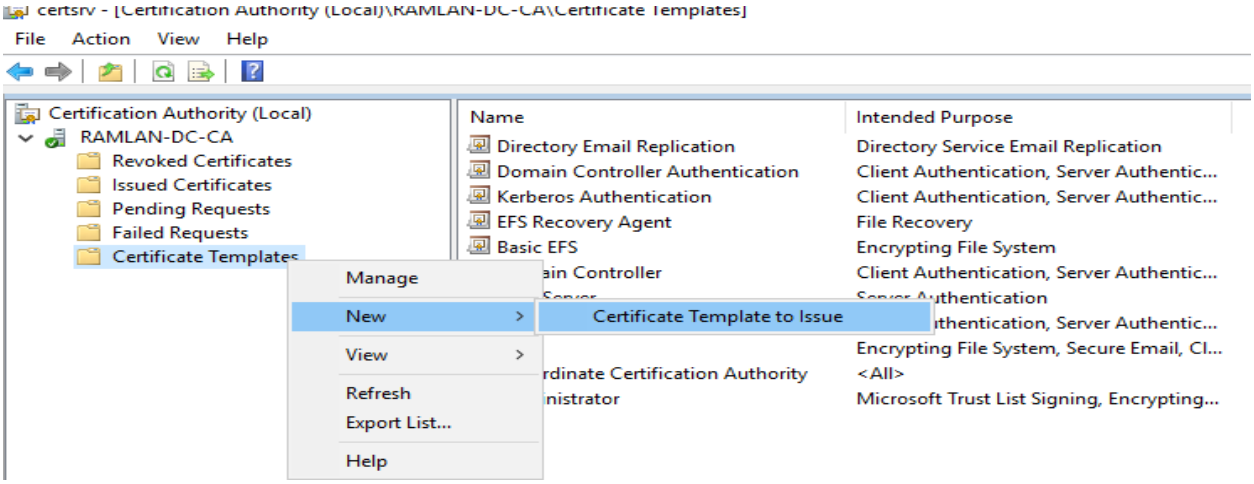

Properties of New Template
Subject Name
Server
Issuance Requirements
Compatibility
General
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Group or user names:
Authenticated Users
Administrator (Administrator@RAMLAN.CA)
Domain Admins (RAMLAN\Domain Admins)
Enterprise Admins (RAMLAN\Enterprise Admins)
Add...
Remove
Permissions for Enterprise Admins
Allow
Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help
Properties of New Template
Subject Name
Server
Issuance Requirements
Compatibility
General
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Group or user names:
Authenticated Users
Administrator (Administrator@RAMLAN.CA)
Domain Admins (RAMLAN\Domain Admins)
Enterprise Admins (RAMLAN\Enterprise Admins)
IISSERVERS (RAMLAN\IISSERVERS)
Add...
Remove
Permissions for IISSERVERS
Allow
Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

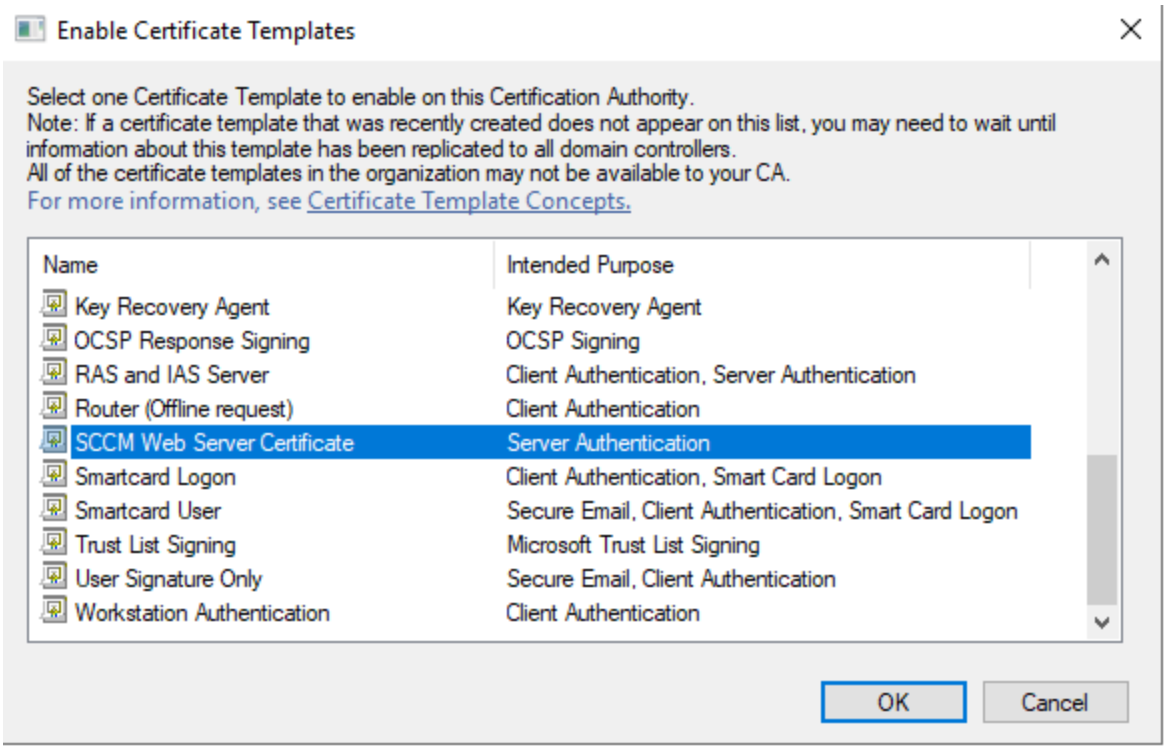

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Subject Name
Server
Issuance Requirements
Supply in the request
Use subject information from existing certificates for autoenrollment renewal requests (*)
Build from this Active Directory information
Select this option to enforce consistency among subject names and to simplify certificate administration.
Subject name format:
None
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.
OK
Cancel
Apply
Help
Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Subject Name
Server
Issuance Requirements
Do not store certificates and requests in the CA database (*)
Do not include revocation information in issued certificates (*)
* Control is disabled due to compatibility settings.
OK
Cancel
Apply
Help





Now we will issue the certificate

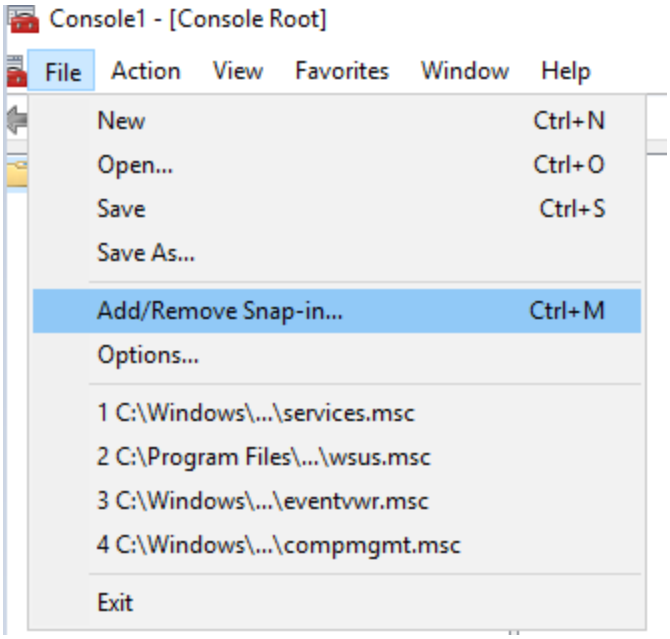


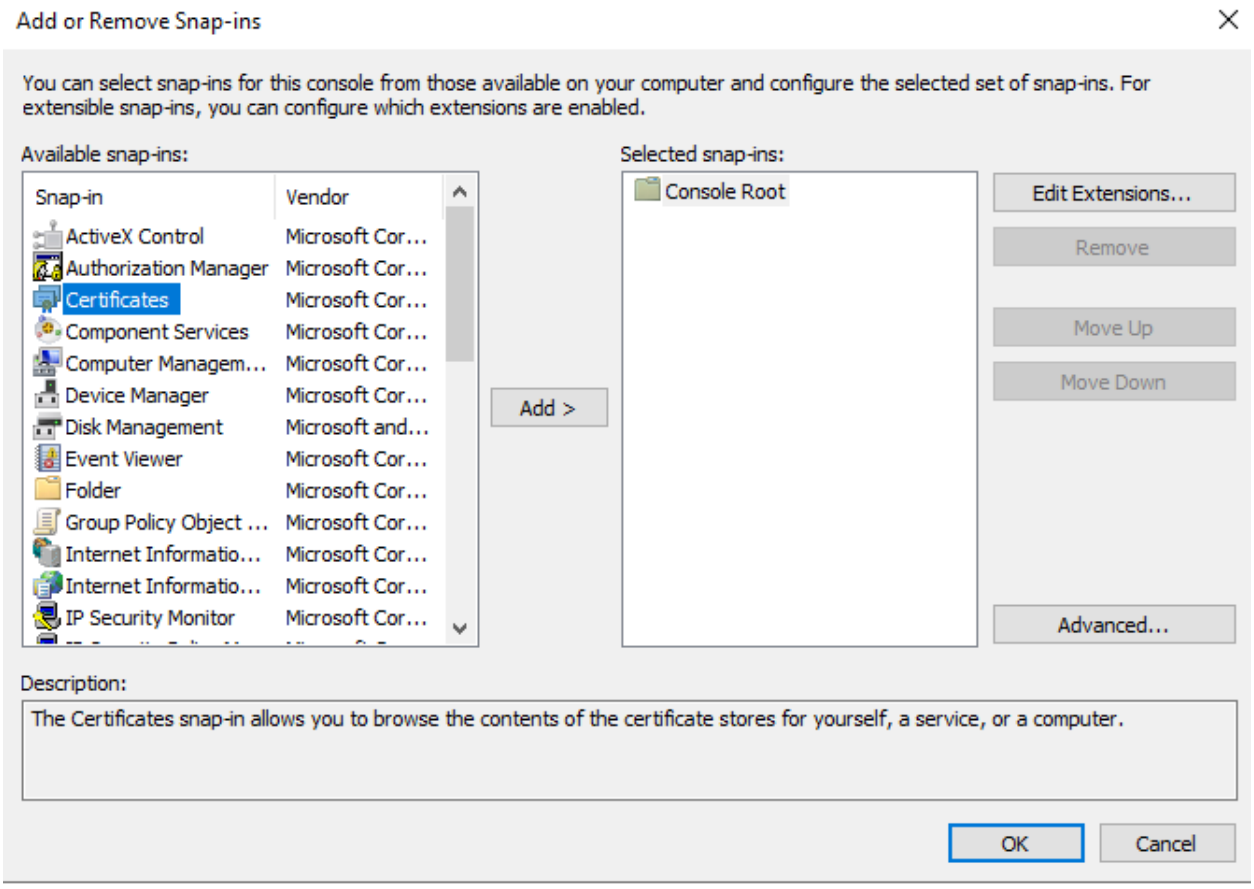


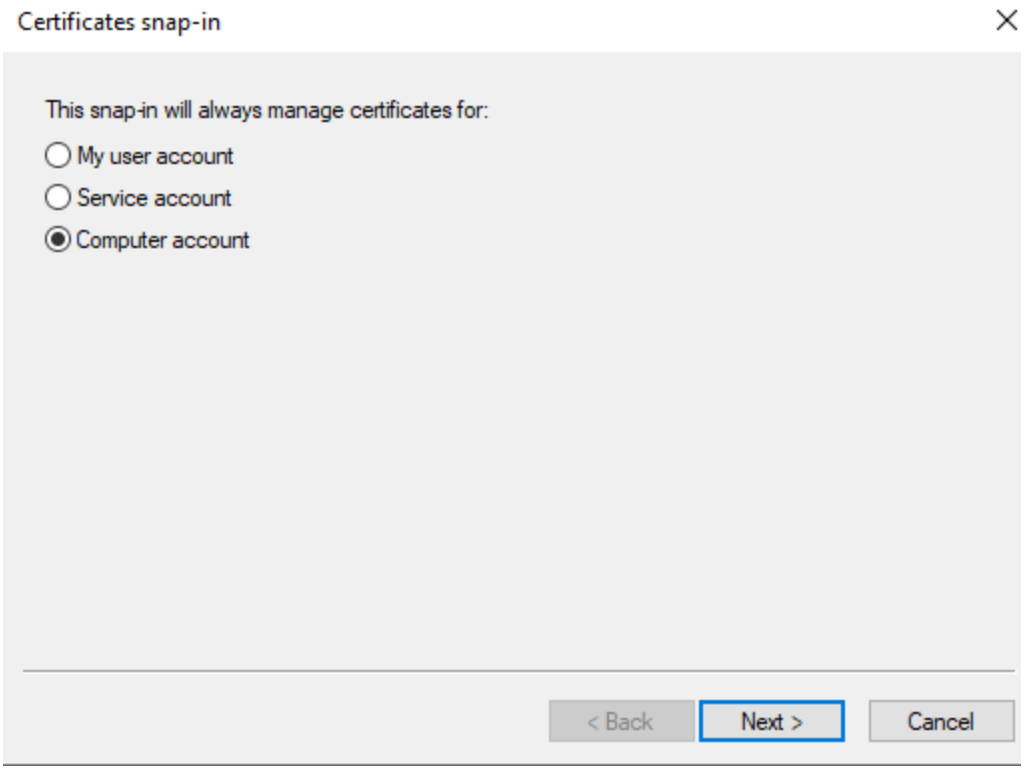
Request the Certificate:

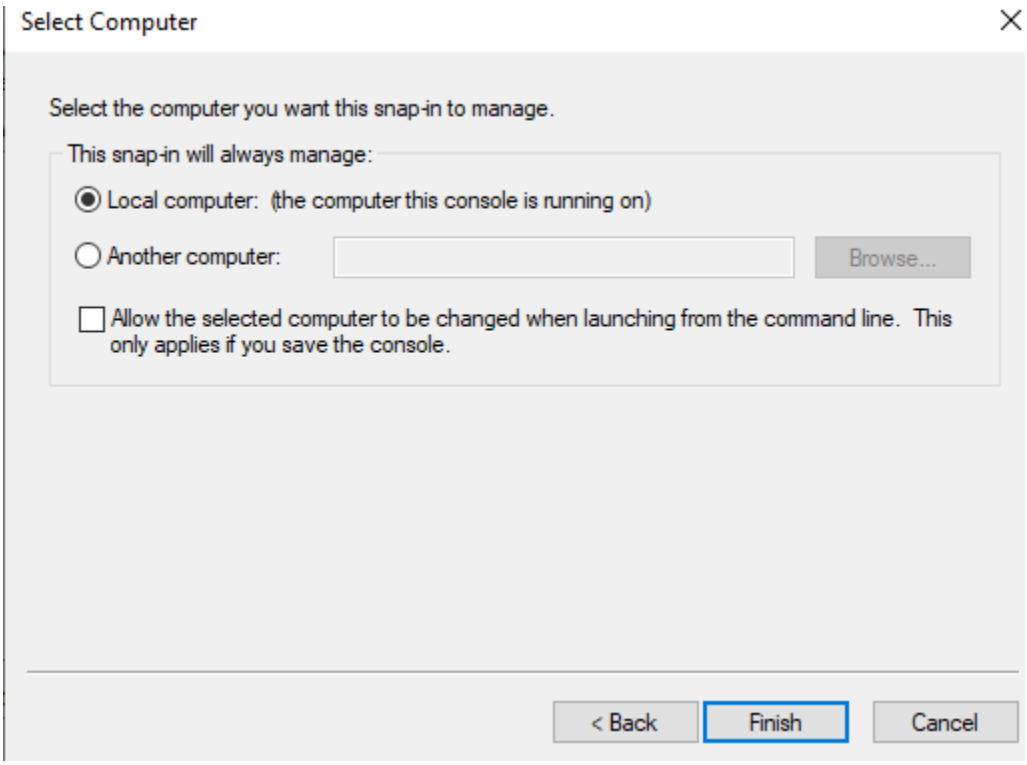
The steps should be performed on Configuration Manager Server (**CB.RAMLAN.CA**) to install the web server certificate that runs IIS. Microsoft recommends you to restart the member server that runs IIS. This is just to ensure that the computer can access the certificate template that you created.

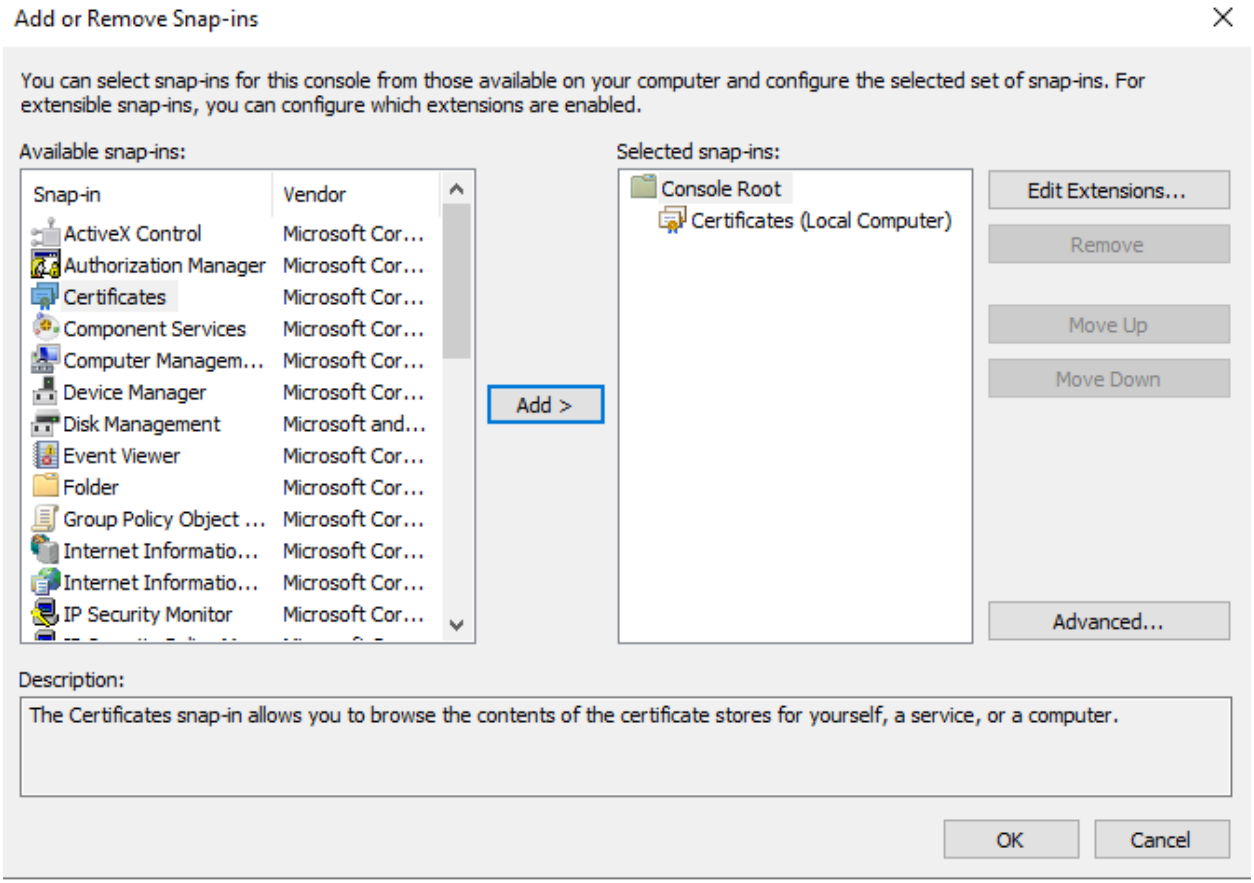
Run the mmc.exe command. In the empty console, click File, and then click Add/Remove Snap-in. In the Add or Remove Snap-ins dialog box, select Certificates from the list of Available snap-ins, and then click Add. In the Certificate snap-in dialog box, select Computer account, and then click Next. In the Select Computer dialog box, ensure Local computer: (the computer this console is running on) is selected, and then click Finish. In the Add or Remove Snap-ins dialog box, click OK. In the console, expand Certificates (Local Computer), and then click Personal. Right-click Certificates, click All Tasks, and then click Request New Certificate.

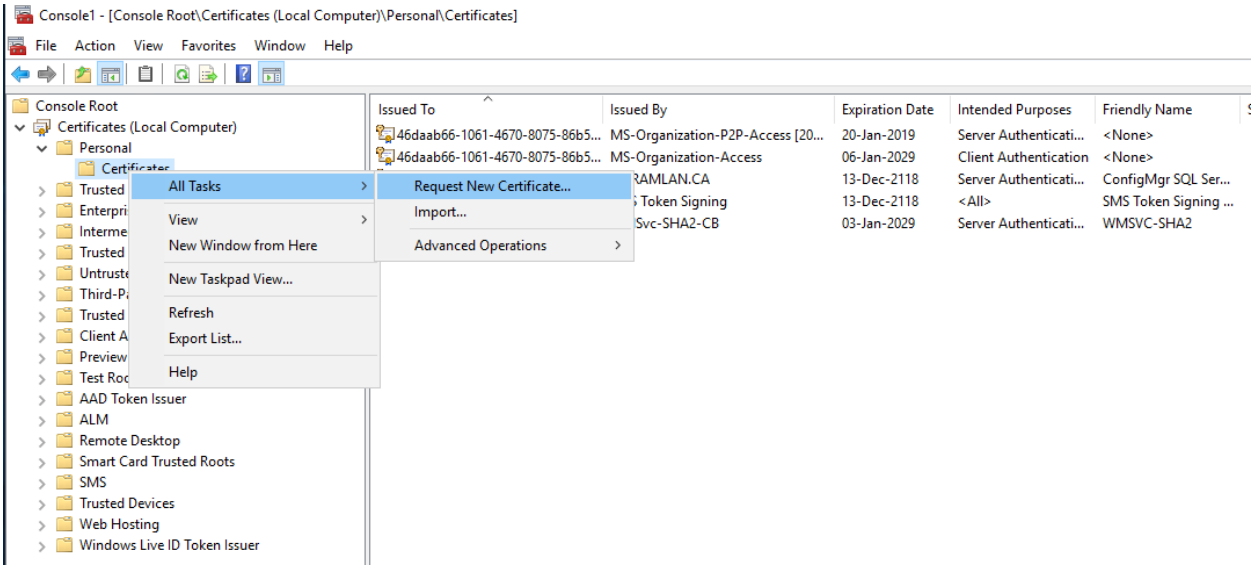

Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\...\services.msc
2 C:\Program Files\...\wsus.msc
3 C:\Windows\...\eventvwr.msc
4 C:\Windows\...\compmgmt.msc
Exit


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
ActiveX Control Microsoft Cor...
Authorization Manager Microsoft Cor...
Certificates Microsoft Cor...
Component Services Microsoft Cor...
Computer Managem... Microsoft Cor...
Device Manager Microsoft Cor...
Disk Management Microsoft and...
Event Viewer Microsoft Cor...
Folder Microsoft Cor...
Group Policy Object ... Microsoft Cor...
Internet Informatio... Microsoft Cor...
Internet Informatio... Microsoft Cor...
IP Security Monitor Microsoft Cor...
Add >
Selected snap-ins:
Console Root
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
Description:
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.
OK
Cancel


Certificates snap-in
This snap-in will always manage certificates for:
My user account
Service account
Computer account
< Back
Next >
Cancel


Select Computer
Select the computer you want this snap-in to manage.
This snap-in will always manage:
Local computer: (the computer this console is running on)
Another computer:
Browse...
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.
< Back
Finish
Cancel


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
ActiveX Control
Microsoft Cor...
Authorization Manager
Microsoft Cor...
Certificates
Microsoft Cor...
Component Services
Microsoft Cor...
Computer Managem...
Microsoft Cor...
Device Manager
Microsoft Cor...
Disk Management
Microsoft and...
Event Viewer
Microsoft Cor...
Folder
Microsoft Cor...
Group Policy Object ...
Microsoft Cor...
Internet Informatio...
Microsoft Cor...
Internet Informatio...
Microsoft Cor...
IP Security Monitor
Microsoft Cor...
Add >
Selected snap-ins:
Console Root
Certificates (Local Computer)
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
Description:
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.
OK
Cancel


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted
Enterpri
Interme
Trusted
Untruste
Third-P
Trusted
Client A
Preview
Test Roo
AAD Token Issuer
ALM
Remote Desktop
Smart Card Trusted Roots
SMS
Trusted Devices
Web Hosting
Windows Live ID Token Issuer
All Tasks
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help
Request New Certificate...
Import...
Advanced Operations
Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
46daab66-1061-4670-8075-86b5...
MS-Organization-P2P-Access [20...
20-Jan-2019
Server Authenticati...
<None>
46daab66-1061-4670-8075-86b5...
MS-Organization-Access
06-Jan-2029
Client Authentication
<None>
RAMLAN.CA
13-Dec-2118
Server Authenticati...
ConfigMgr SQL Ser...
Token Signing
13-Dec-2118
<All>
SMS Token Signing ...
Svc-SHA2-CB
03-Jan-2029
Server Authenticati...
WMSVC-SHA2

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

Next Cancel

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

Enrollment Policy ID: {344C808C-D718-4B47-A80E-9CE5D2179167}

Properties

Configured by you

Add New

Next Cancel

Request Certificates

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

Active Directory Enrollment Policy

☐ Computer	**STATUS:** Available	Details
☐ SCCM Web Server Certificate	**STATUS:** Available	Details

More information is required to enroll for this certificate. Click here to configure settings.

☐ Show all templates

Enroll | Cancel

Certificate Properties

Subject | General | Extensions | Private Key | Certification Authority | Signature

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Full DN

Value:

Add > | < Remove

Alternative name:

Type: DNS

Value:

Add > | < Remove

DNS
CB.RAMLAN.CA

OK | Cancel | Apply

Request Certificates

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

Active Directory Enrollment Policy

☐ Computer	**STATUS:** Available	Details
☑ SCCM Web Server Certificate	**STATUS:** Available	Details

☐ Show all templates

Enroll Cancel

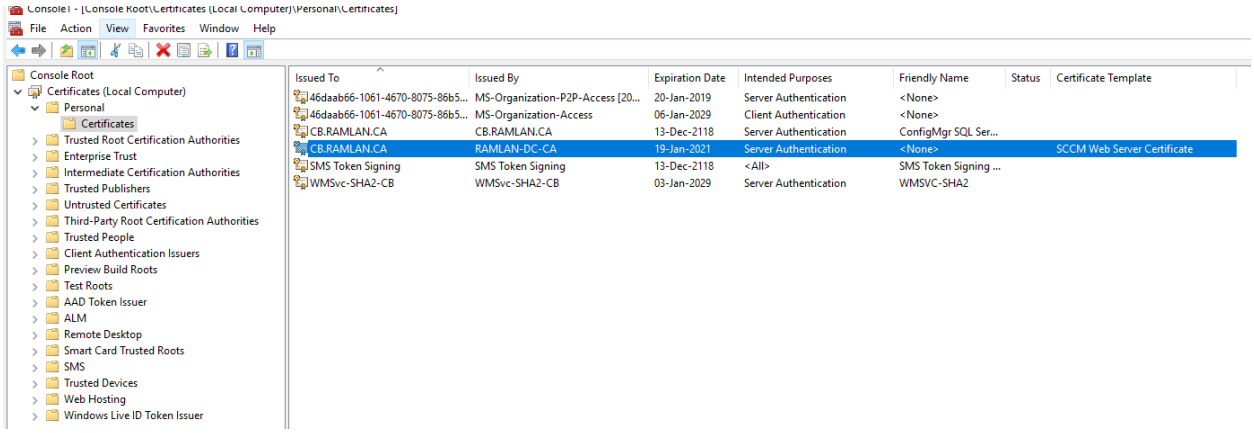
Certificate Installation Results

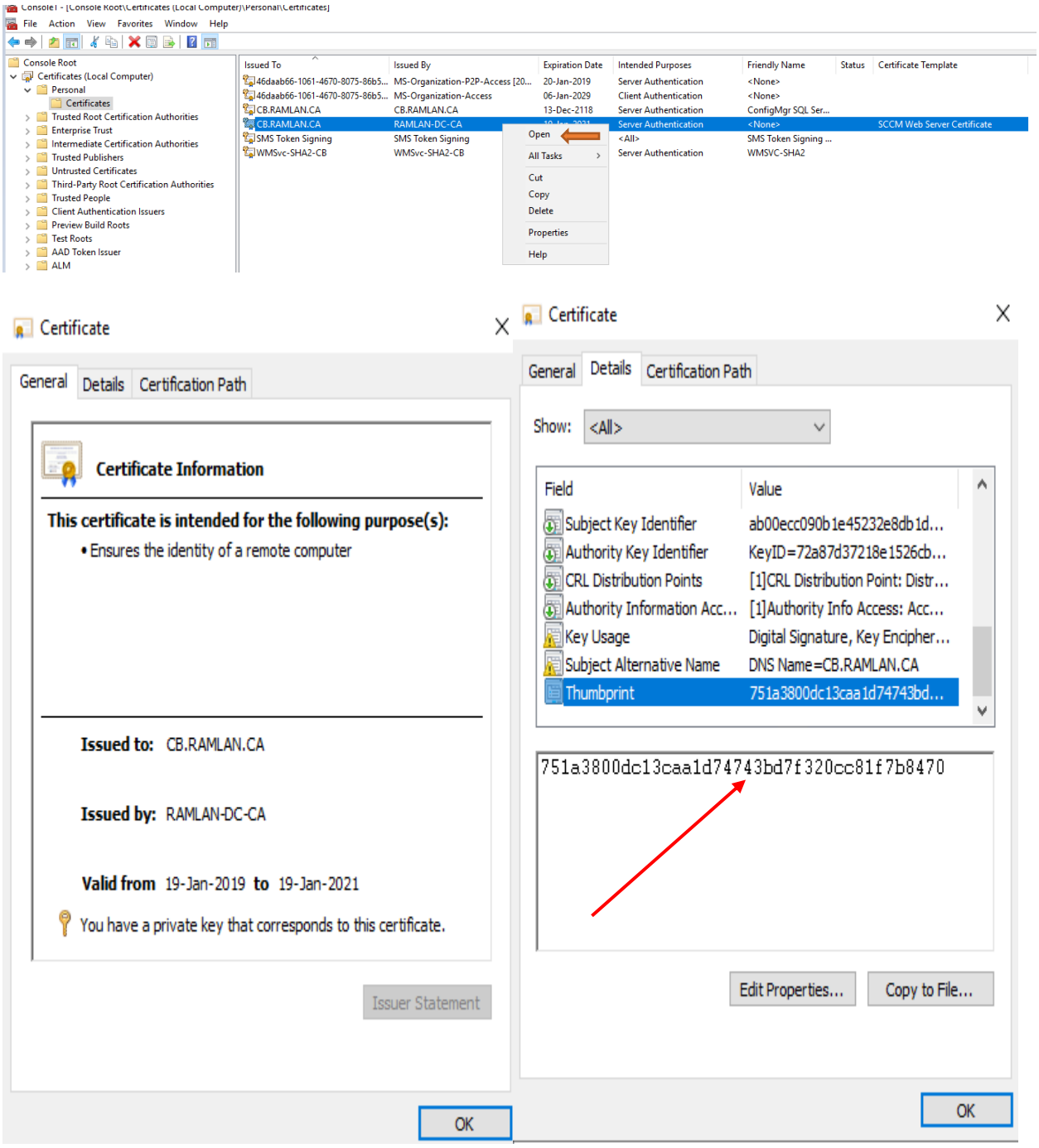
The following certificates have been enrolled and installed on this computer.

Active Directory Enrollment Policy

☑ SCCM Web Server Certificate	**STATUS:** Succeeded	Details

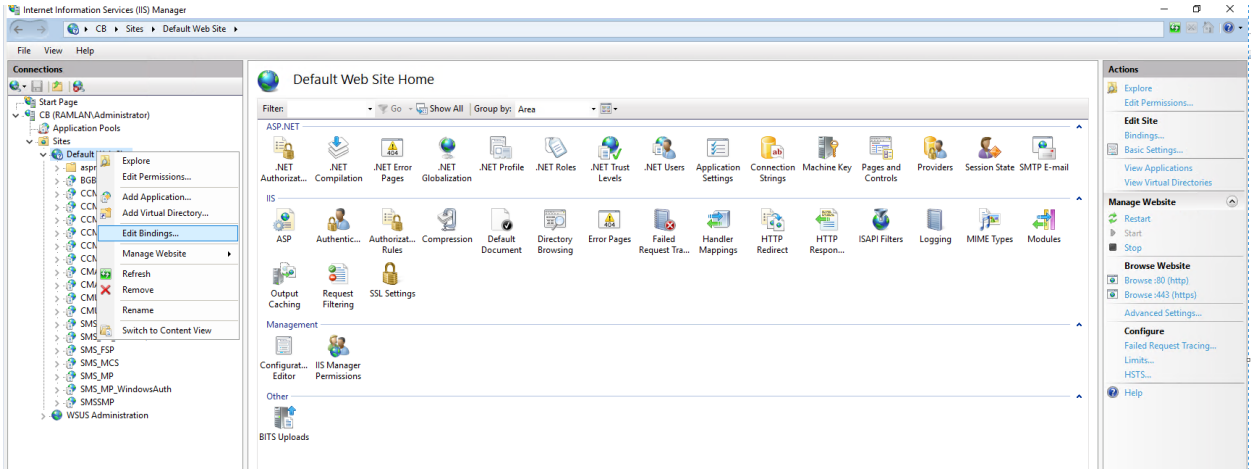
Finish

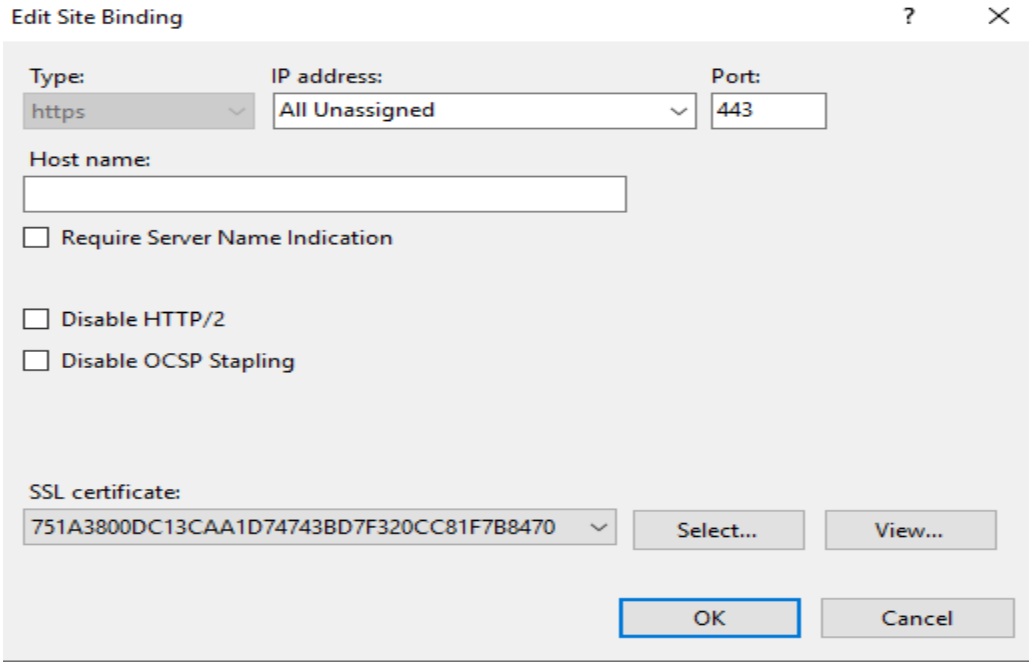


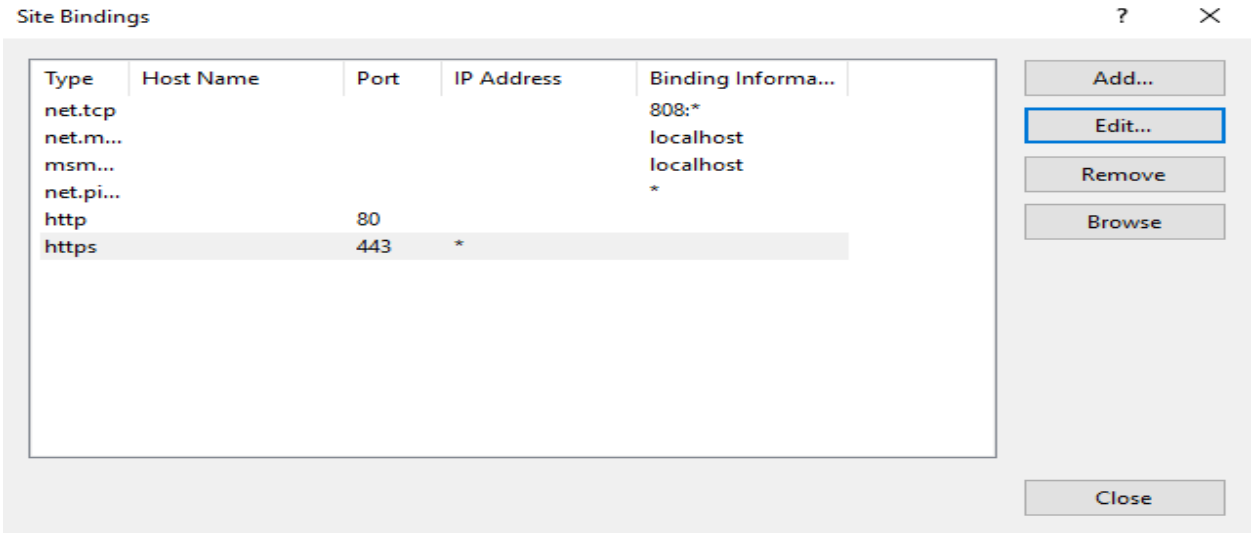


Configuring IIS to Use the Web Server Certificate

The steps that we perform now will configure IIS to use the web server certificate that we had configured in the above steps. On the configuration manager server that has IIS installed, launch the Internet Information Services (IIS) Manager. Expand Sites, right-click Default Web Site, and then select Edit Bindings.

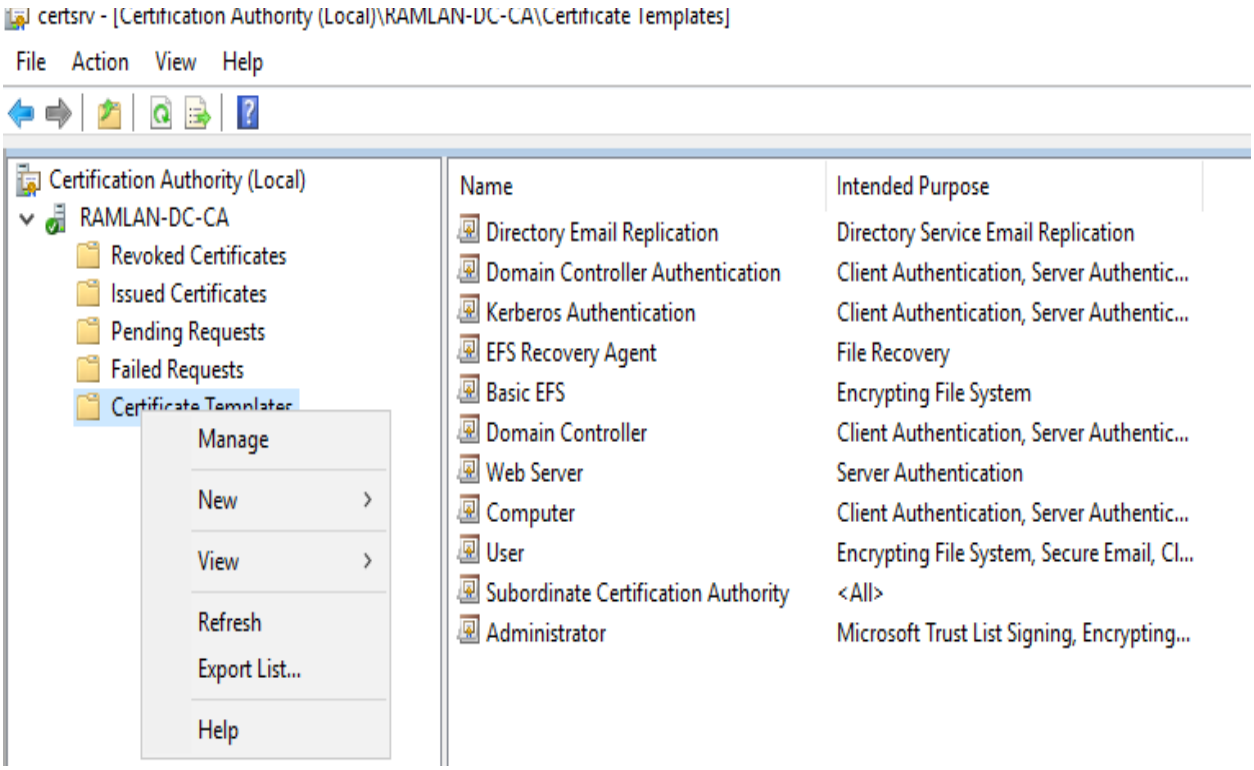

Internet Information Services (IIS) Manager
CB ▸ Sites ▸ Default Web Site ▸
File View Help
Connections
Start Page
CB (RAMLAN\Administrator)
Application Pools
Sites
Default Web Site
Explore
Edit Permissions...
Add Application...
Add Virtual Directory...
Edit Bindings...
Manage Website
Refresh
Remove
Rename
Switch to Content View
SMS_FSP
SMS_MCS
SMS_MP
SMS_MP_WindowsAuth
SMSSMP
WSUS Administration
Default Web Site Home
Filter:
Go
Show All
Group by: Area
ASP.NET
.NET Authorizat...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Profile
.NET Roles
.NET Trust Levels
.NET Users
Application Settings
Connection Strings
Machine Key
Pages and Controls
Providers
Session State
SMTP E-mail
IIS
ASP
Authentic...
Authorizat... Rules
Compression
Default Document
Directory Browsing
Error Pages
Failed Request Tra...
Handler Mappings
HTTP Redirect
HTTP Respon...
ISAPI Filters
Logging
MIME Types
Modules
Output Caching
Request Filtering
SSL Settings
Management
Configurat... Editor
IIS Manager Permissions
Other
BITS Uploads
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse :80 (http)
Browse :443 (https)
Advanced Settings...
Configure
Failed Request Tracing...
Limits...
HSTS...
Help

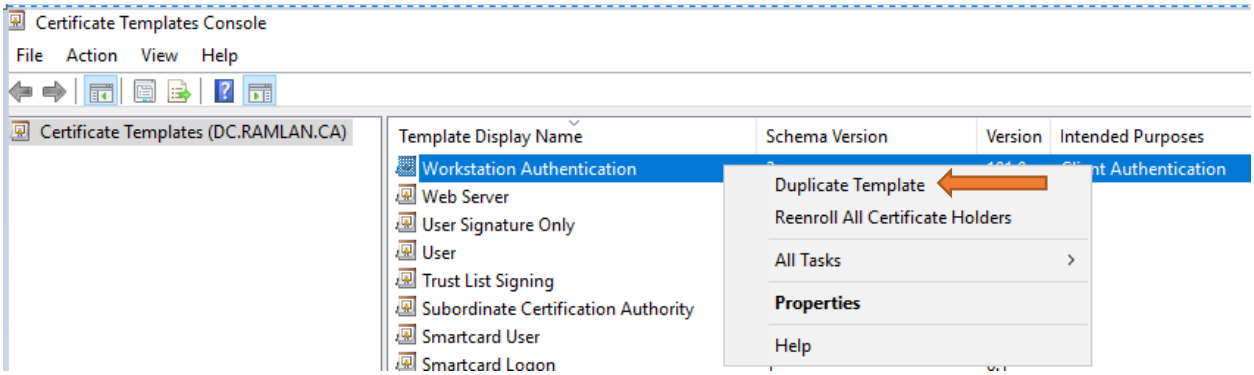

Edit Site Binding
Type:
https
IP address:
All Unassigned
Port:
443
Host name:
Require Server Name Indication
Disable HTTP/2
Disable OCSP Stapling
SSL certificate:
751A3800DC13CAA1D74743BD7F320CC81F7B8470
Select...
View...
OK
Cancel

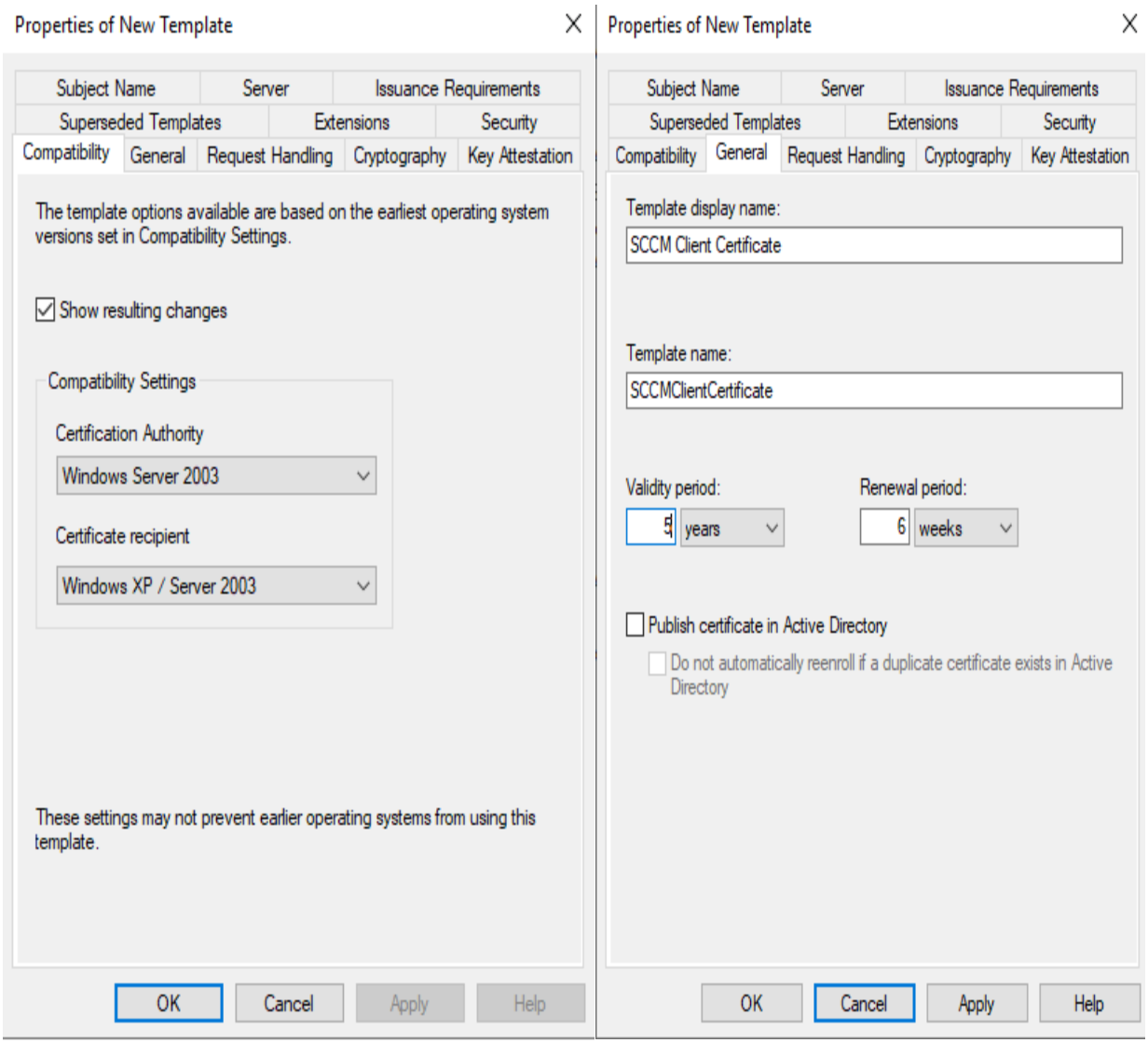

Site Bindings
Type
Host Name
Port
IP Address
Binding Informa...
net.tcp
808:*
net.m...
localhost
msm...
localhost
net.pi...
*
http
80
https
443
*
Add...
Edit...
Remove
Browse
Close

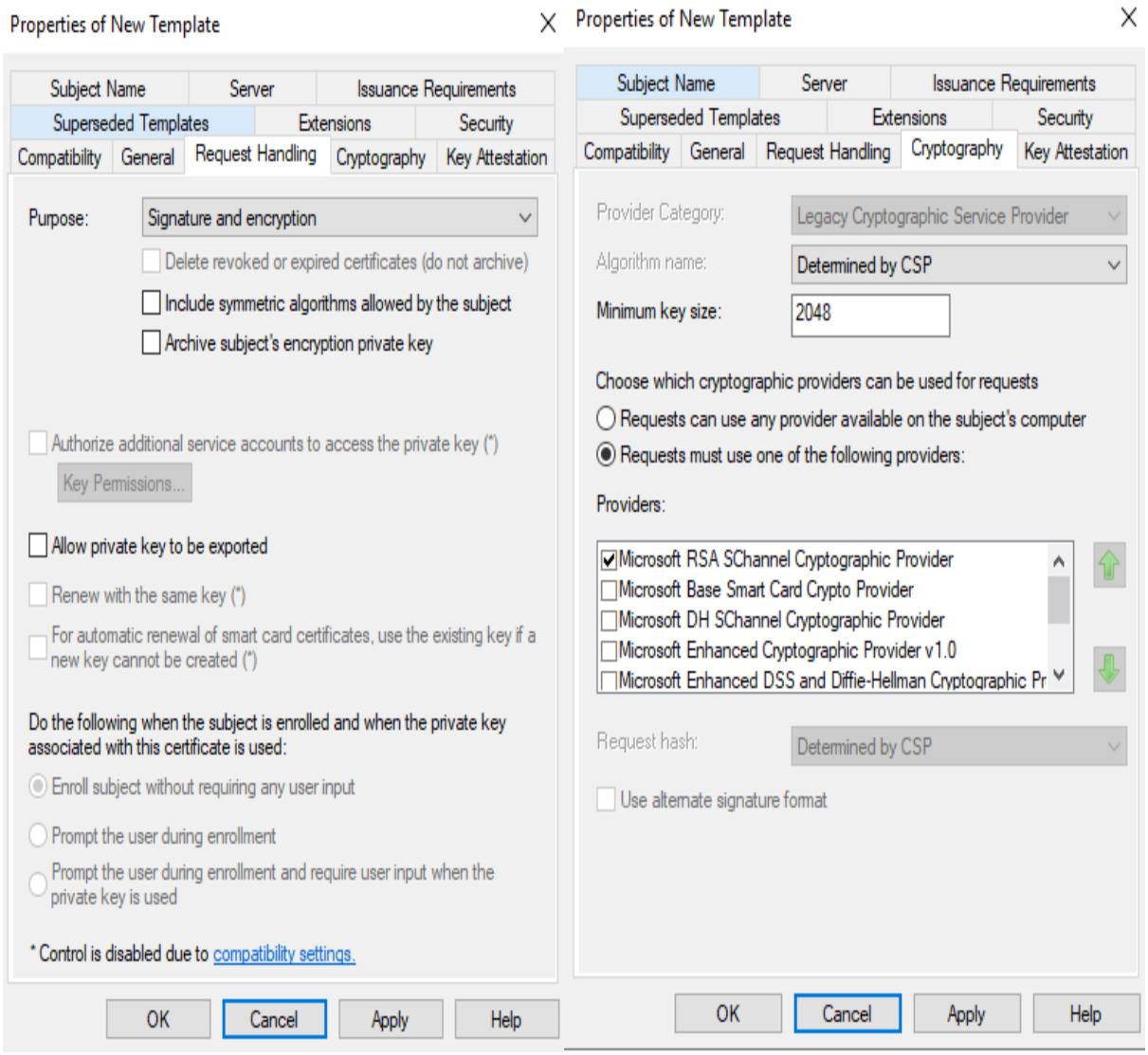
Deploying the Client Certificate for Windows Computers:

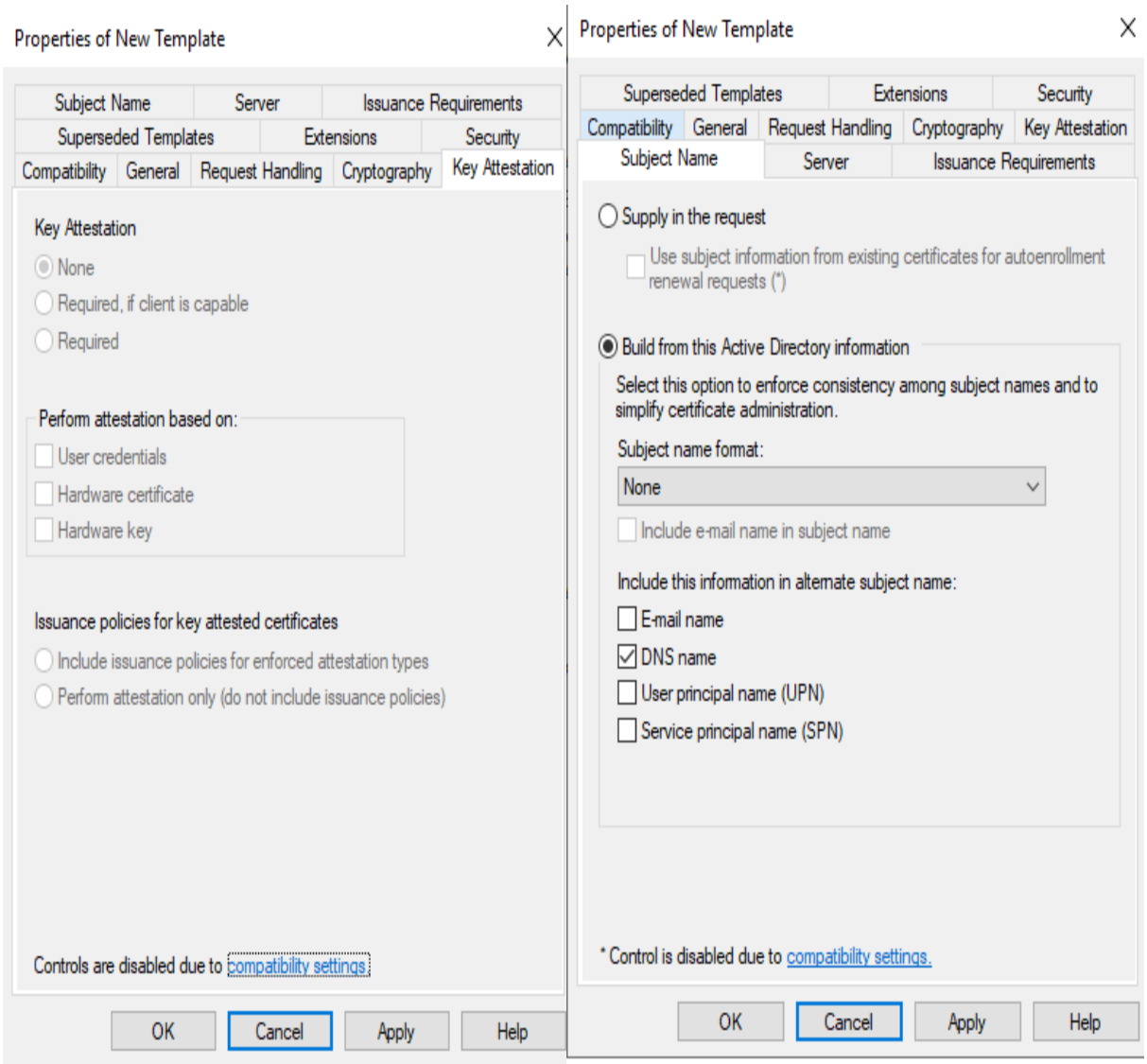
Open Certification Authority from Domain Controller to start **Workstation Authentication Certificate**.

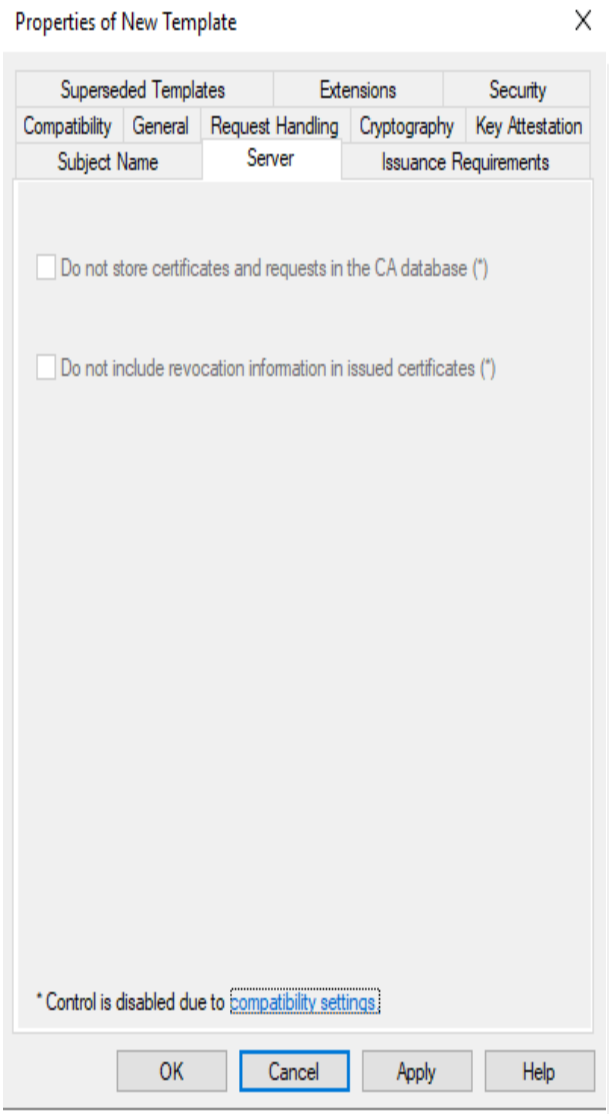


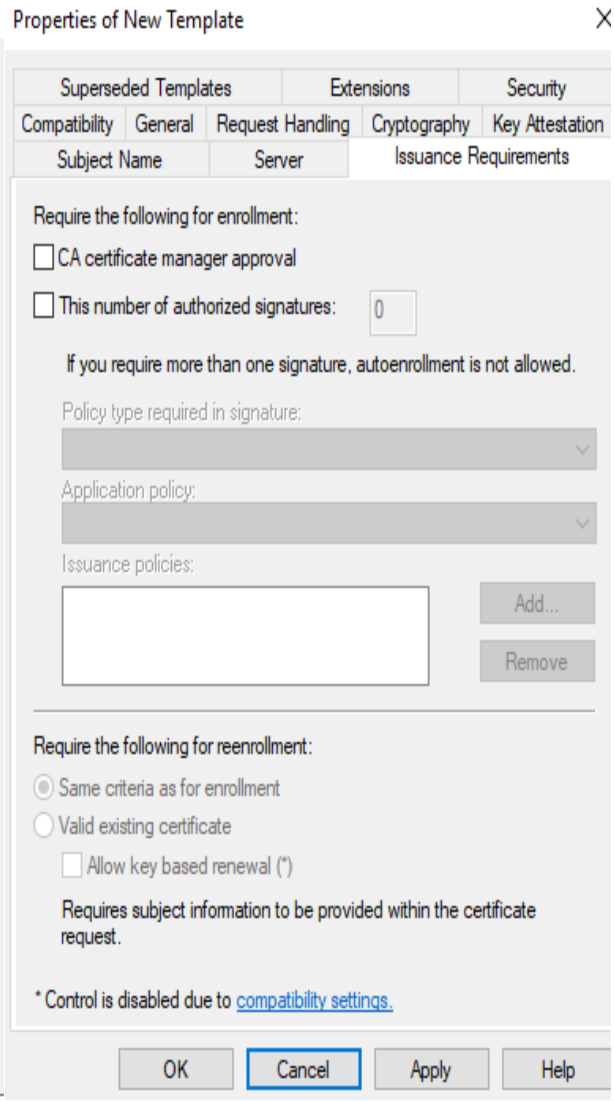


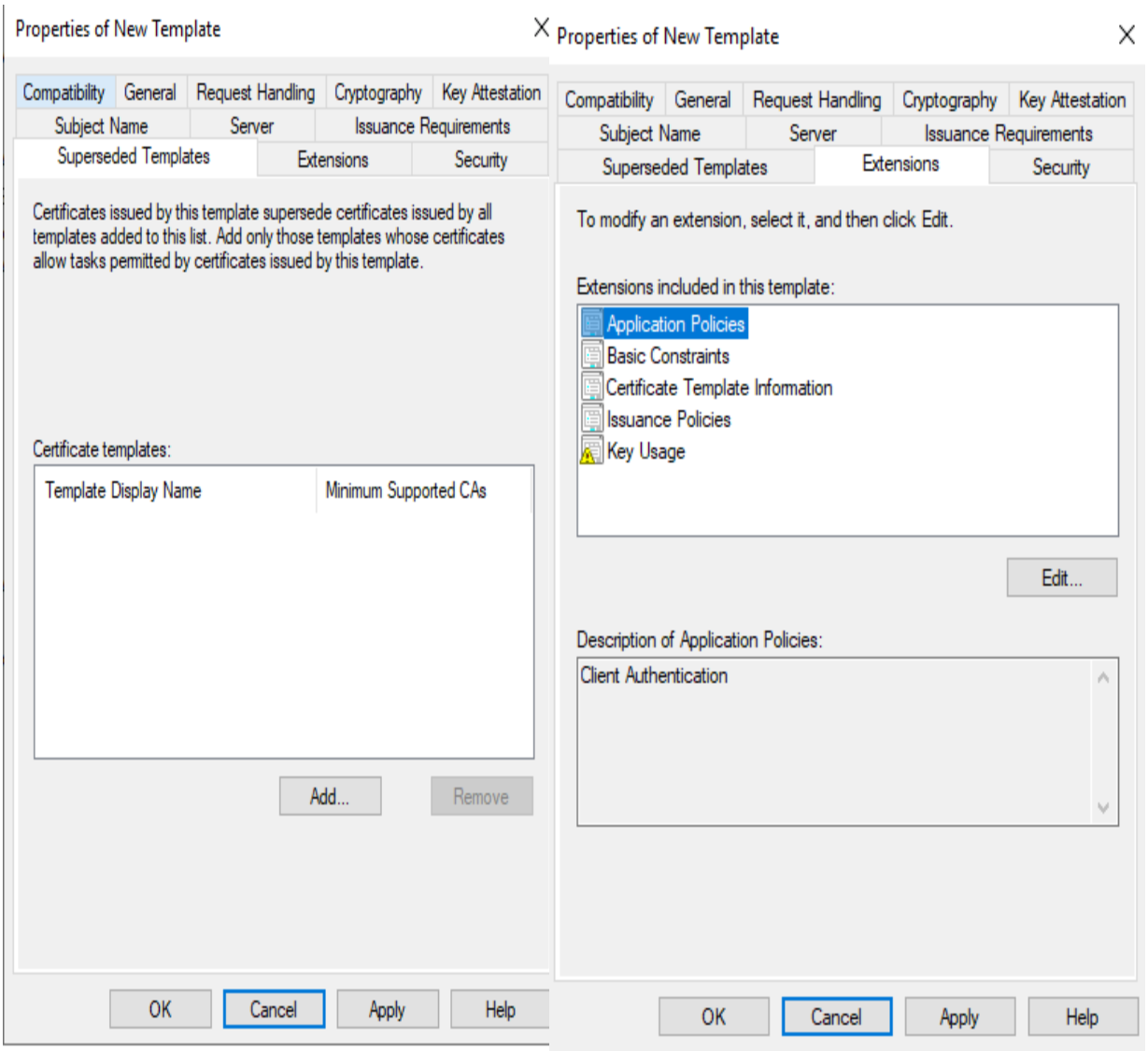

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
The template options available are based on the earliest operating system versions set in Compatibility Settings.
Show resulting 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.
OK
Cancel
Apply
Help
Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Template display name:
SCCM Client Certificate
Template name:
SCCMClientCertificate
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
OK
Cancel
Apply
Help

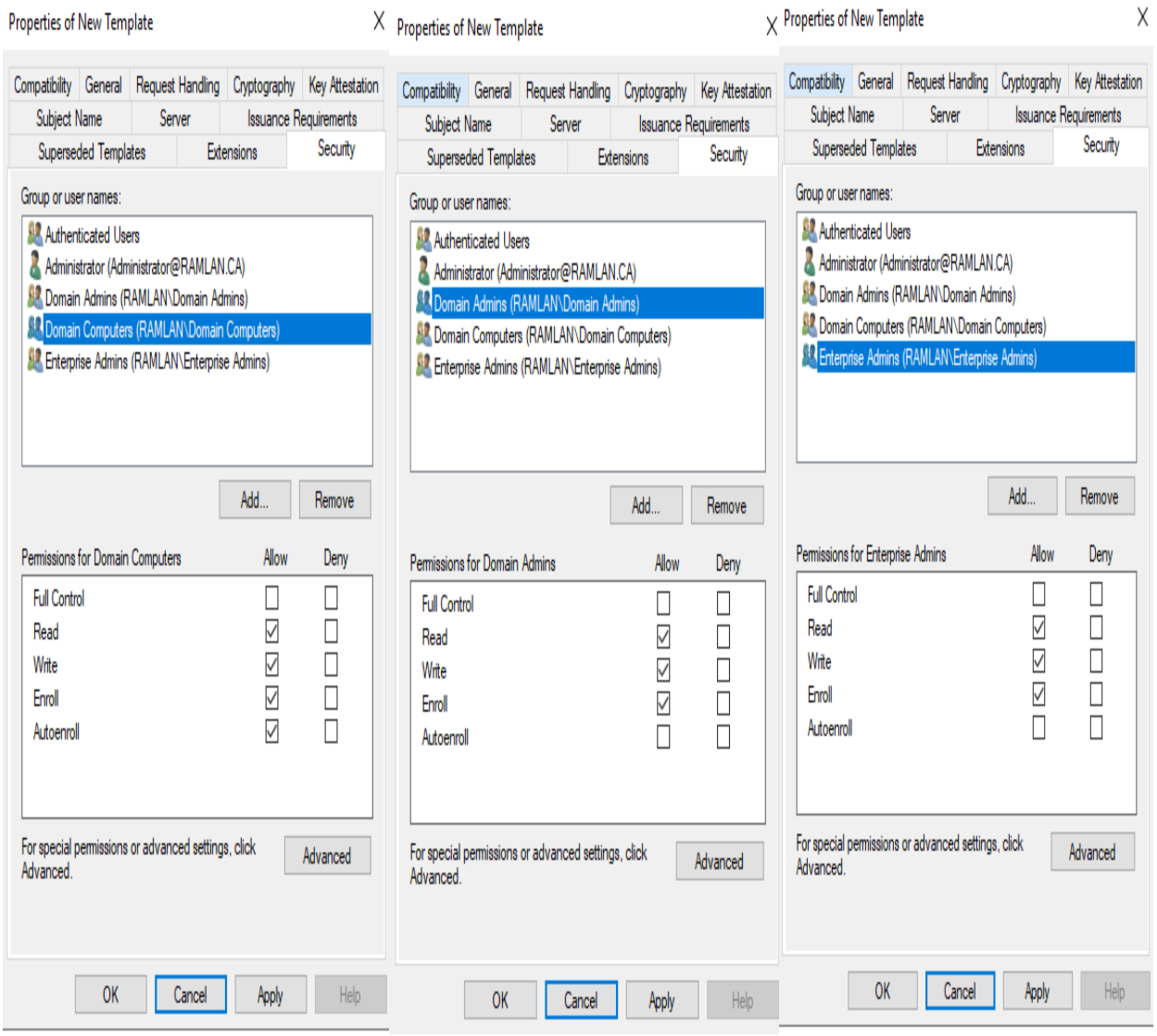

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Purpose:
Signature and encryption
Delete revoked or expired certificates (do not archive)
Include symmetric algorithms allowed by the subject
Archive subject's encryption private key
Authorize additional service accounts to access the private key (*)
Key Permissions...
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.
OK
Cancel
Apply
Help
Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Provider Category:
Legacy Cryptographic Service Provider
Algorithm name:
Determined by CSP
Minimum key size:
2048
Choose which cryptographic providers can be used for requests
Requests can use any provider available on the subject's computer
Requests must use one of the following providers:
Providers:
Microsoft RSA SChannel Cryptographic Provider
Microsoft Base Smart Card Crypto Provider
Microsoft DH SChannel Cryptographic Provider
Microsoft Enhanced Cryptographic Provider v1.0
Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr
Request hash:
Determined by CSP
Use alternate signature format
OK
Cancel
Apply
Help

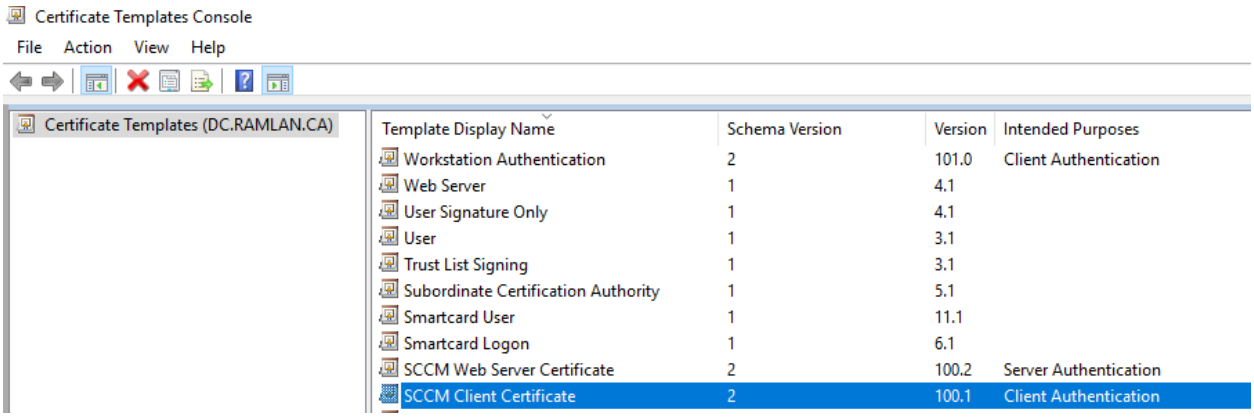

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Key Attestation
None
Required, if client is capable
Required
Perform attestation based on:
User credentials
Hardware certificate
Hardware key
Issuance policies for key attested certificates
Include issuance policies for enforced attestation types
Perform attestation only (do not include issuance policies)
Controls are disabled due to compatibility settings
OK
Cancel
Apply
Help
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:
None
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.
OK
Cancel
Apply
Help


Properties of New Template
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Do not store certificates and requests in the CA database (*)
Do not include revocation information in issued certificates (*)
* Control is disabled due to compatibility settings
OK
Cancel
Apply
Help

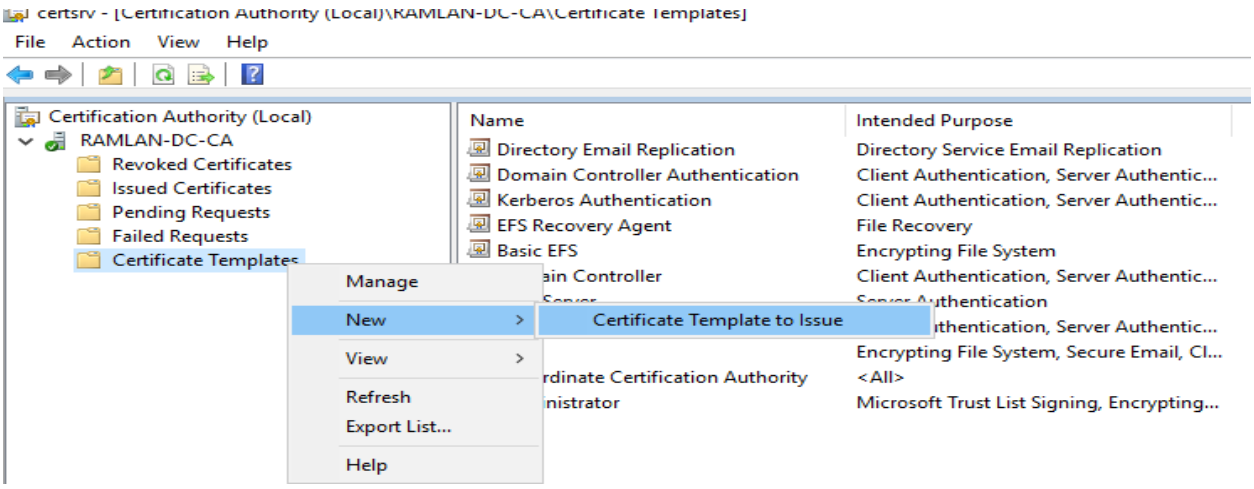

Properties of New Template
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Require the following for enrollment:
CA certificate manager approval
This number of authorized signatures:
0
If you require more than one signature, autoenrollment is not allowed.
Policy type required in signature:
Application policy:
Issuance policies:
Add...
Remove
Require the following for reenrollment:
Same criteria as for enrollment
Valid existing certificate
Allow key based renewal (*)
Requires subject information to be provided within the certificate request.
* Control is disabled due to compatibility settings.
OK
Cancel
Apply
Help

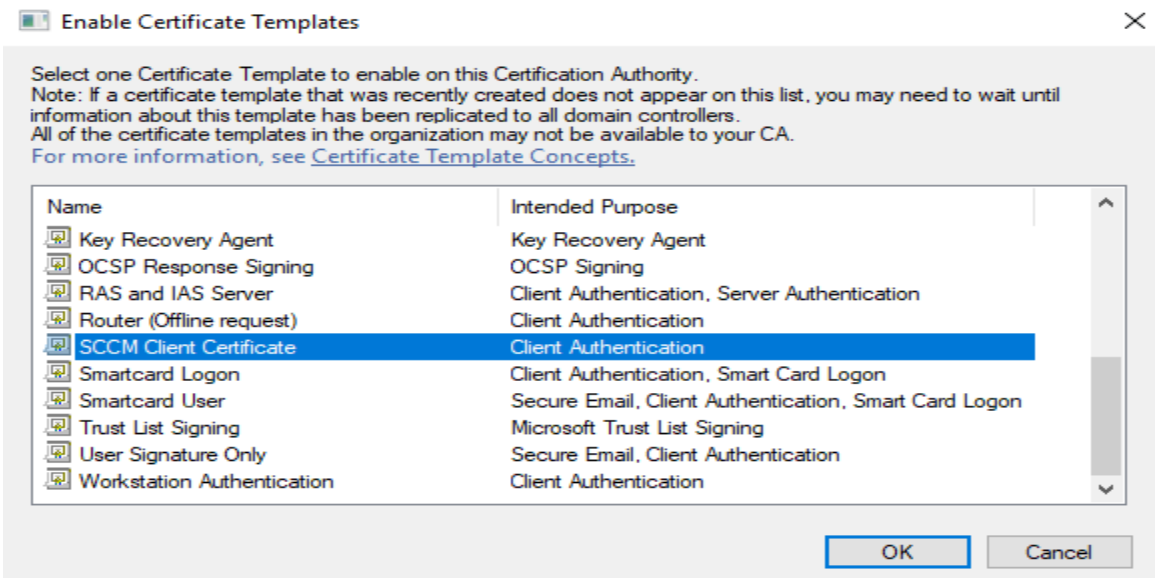

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Certificates issued by this template supersede certificates issued by all templates added to this list. Add only those templates whose certificates allow tasks permitted by certificates issued by this template.
Certificate templates:
Template Display Name
Minimum Supported CAs
Add...
Remove
OK
Cancel
Apply
Help
Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
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
Edit...
Description of Application Policies:
Client Authentication
OK
Cancel
Apply
Help

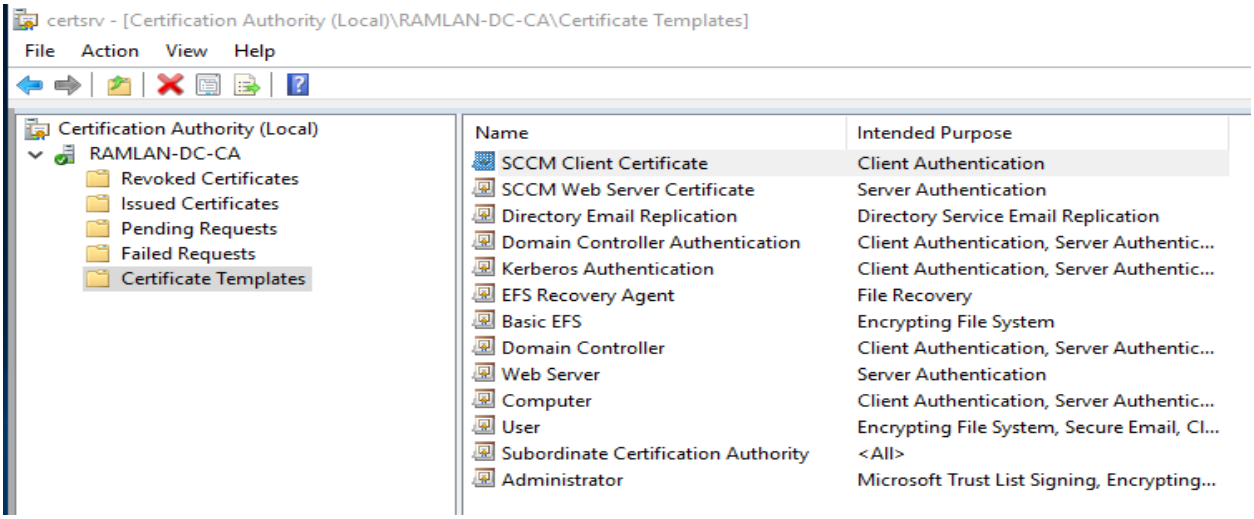

Properties of New Template
Compatibility General Request Handling Cryptography Key Attestation
Subject Name Server Issuance Requirements
Superseded Templates Extensions Security
Group or user names:
Authenticated Users
Administrator (Administrator@RAMLAN.CA)
Domain Admins (RAMLAN\Domain Admins)
Domain Computers (RAMLAN\Domain Computers)
Enterprise Admins (RAMLAN\Enterprise Admins)
Add... Remove
Permissions for Domain Computers Allow Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply Help
Properties of New Template
Compatibility General Request Handling Cryptography Key Attestation
Subject Name Server Issuance Requirements
Superseded Templates Extensions Security
Group or user names:
Authenticated Users
Administrator (Administrator@RAMLAN.CA)
Domain Admins (RAMLAN\Domain Admins)
Domain Computers (RAMLAN\Domain Computers)
Enterprise Admins (RAMLAN\Enterprise Admins)
Add... Remove
Permissions for Domain Admins Allow Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply Help
Properties of New Template
Compatibility General Request Handling Cryptography Key Attestation
Subject Name Server Issuance Requirements
Superseded Templates Extensions Security
Group or user names:
Authenticated Users
Administrator (Administrator@RAMLAN.CA)
Domain Admins (RAMLAN\Domain Admins)
Domain Computers (RAMLAN\Domain Computers)
Enterprise Admins (RAMLAN\Enterprise Admins)
Add... Remove
Permissions for Enterprise Admins Allow Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply Help


Certificate Templates Console
File Action View Help
Certificate Templates (DC.RAMLAN.CA)
Template Display Name Schema Version Version Intended Purposes
Workstation Authentication 2 101.0 Client Authentication
Web Server 1 4.1
User Signature Only 1 4.1
User 1 3.1
Trust List Signing 1 3.1
Subordinate Certification Authority 1 5.1
Smartcard User 1 11.1
Smartcard Logon 1 6.1
SCCM Web Server Certificate 2 100.2 Server Authentication
SCCM Client Certificate 2 100.1 Client Authentication

Now we will issue the certificate.

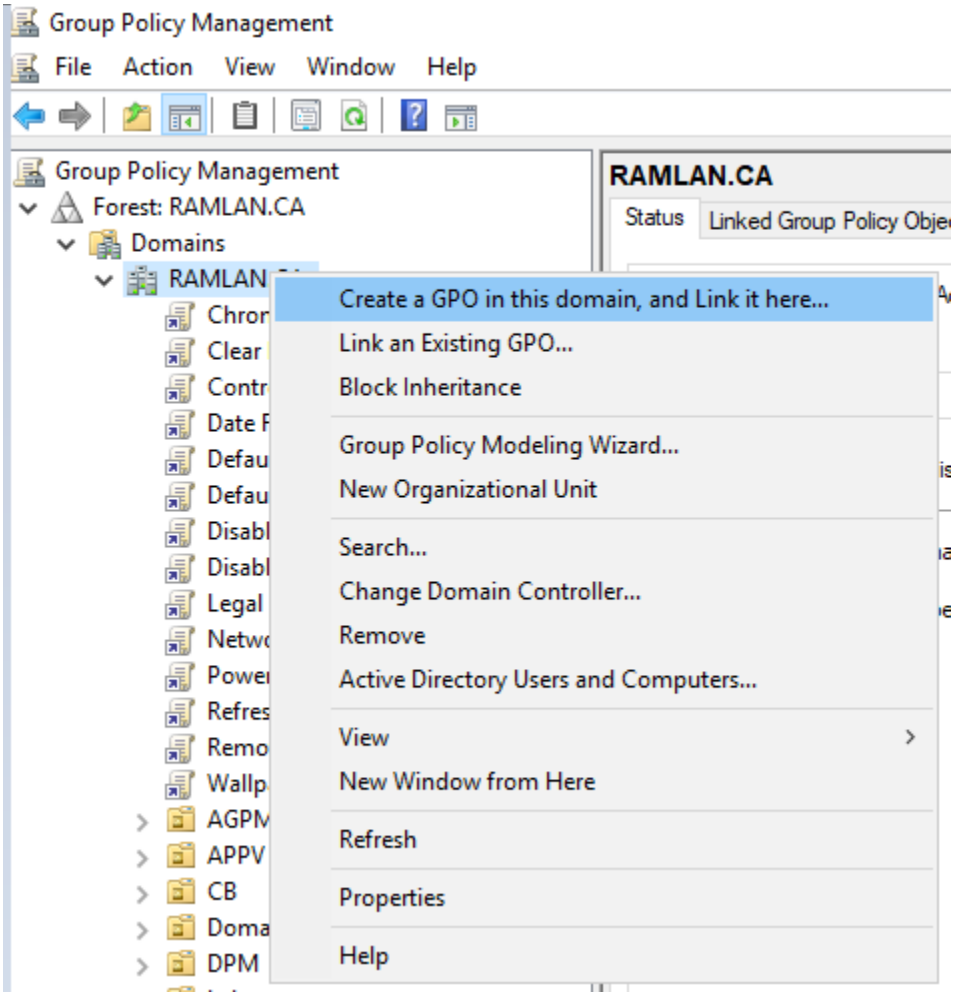


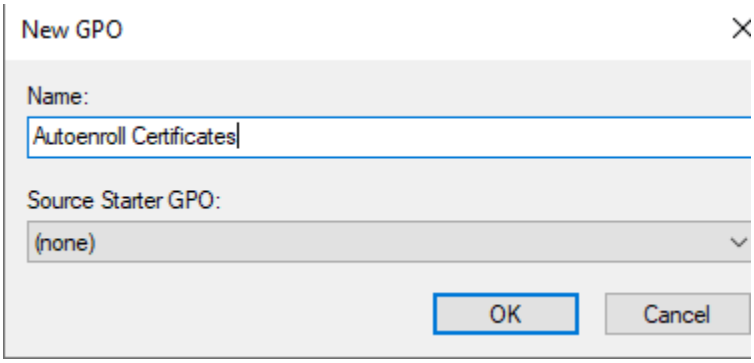


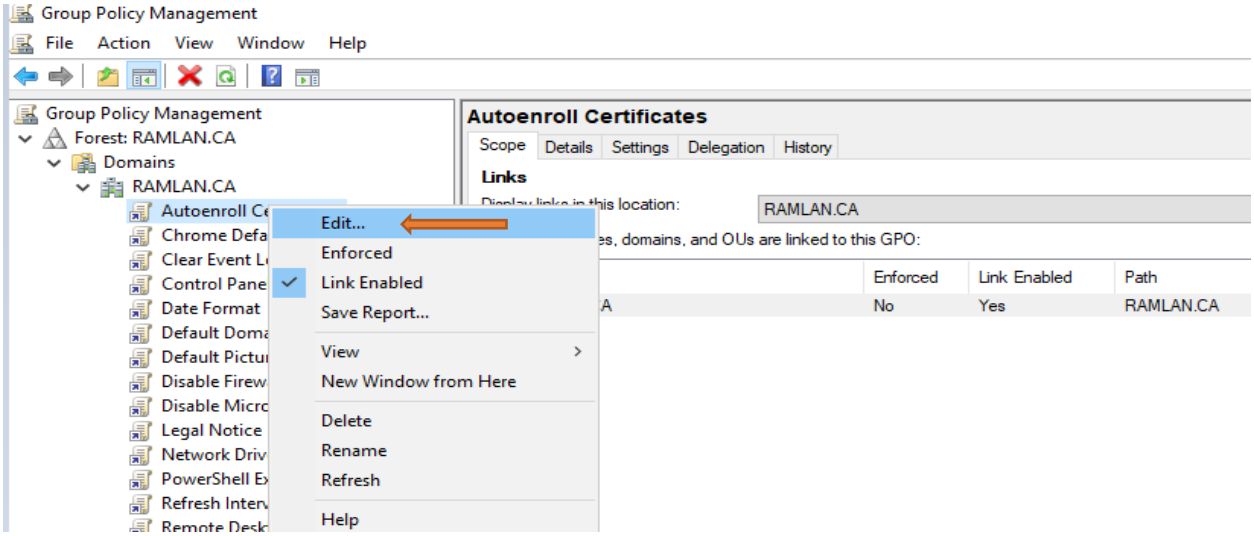


Configuring Auto enrollment of the Workstation Authentication Template by Using Group Policy:

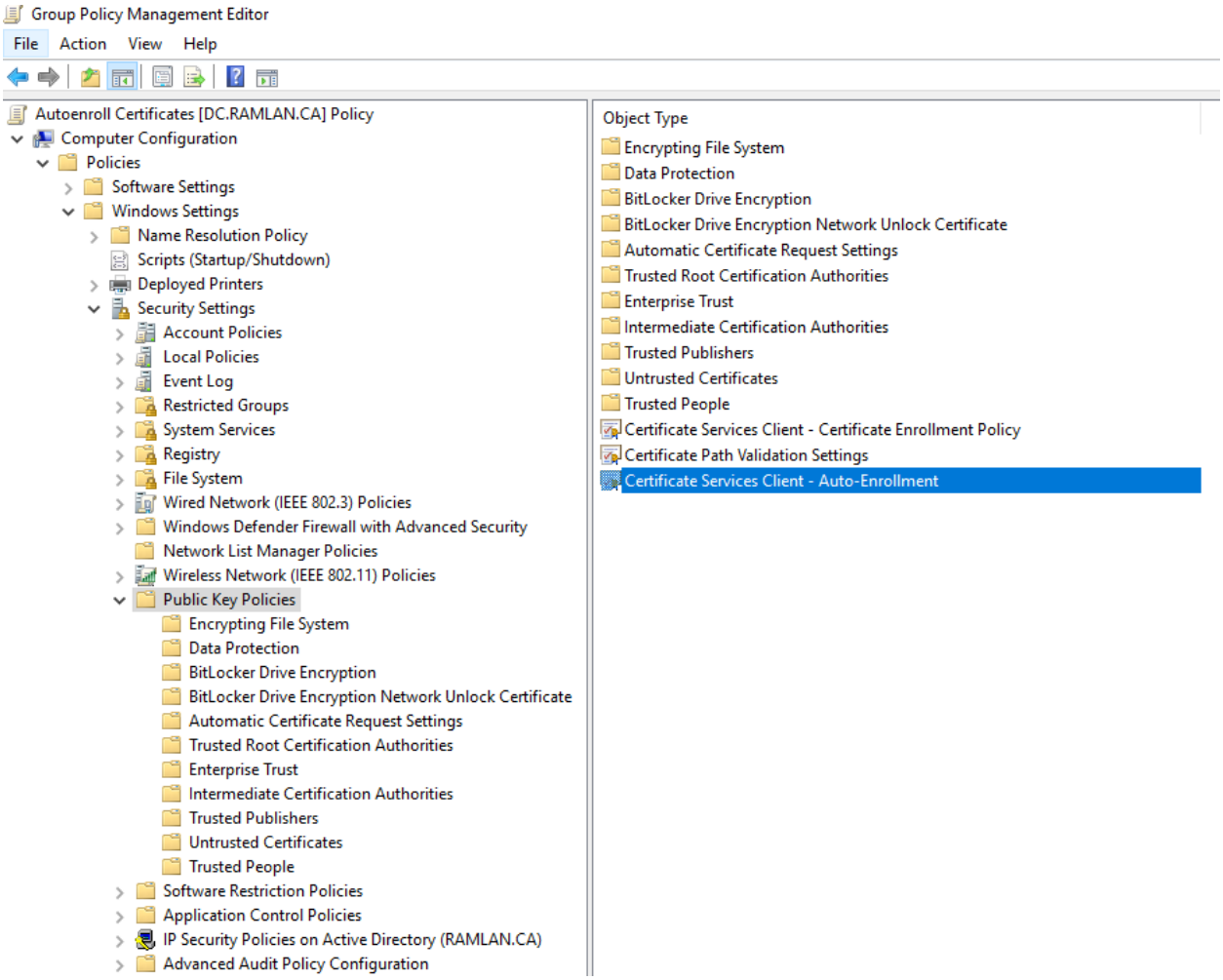
Open GPMC

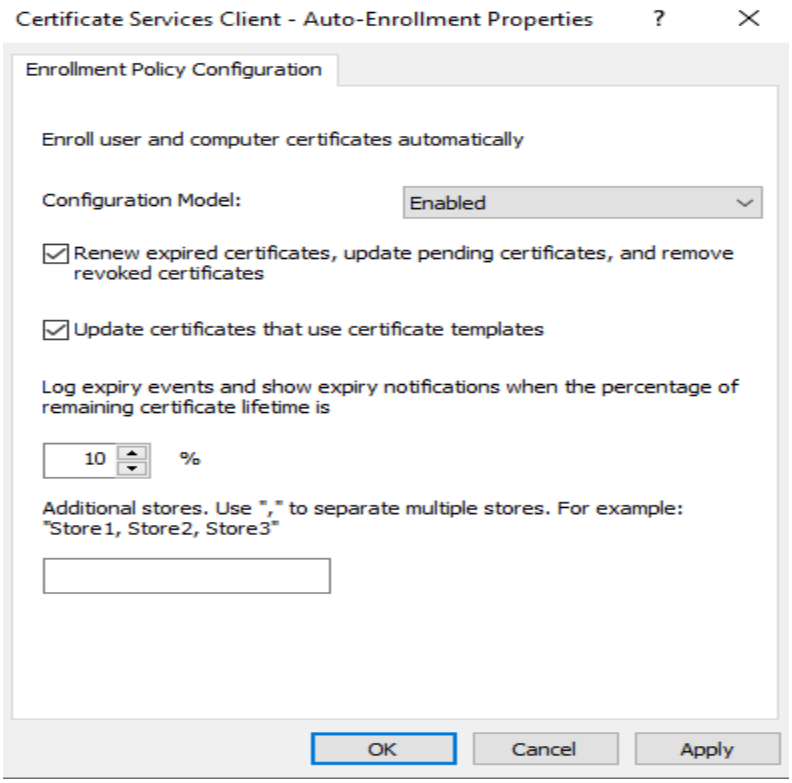






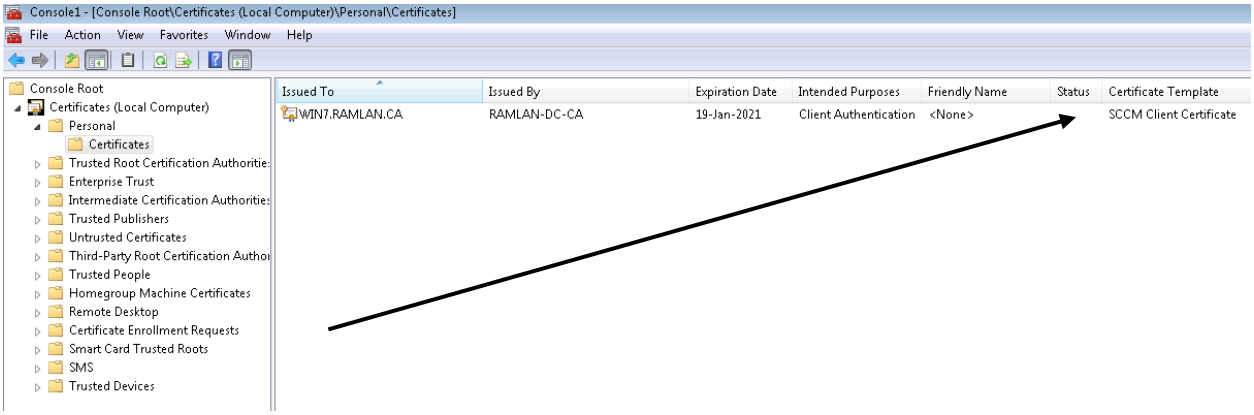
In the Group Policy Management Editor, expand Policies under Computer Configuration, and then navigate to Windows Settings > Security Settings > Public Key Policies. Right-click the object type named Certificate Services Client – Auto-enrollment, and then click Properties





Automatically Enrolling the Workstation Authentication Certificate and Verifying Its Installation on Computers:

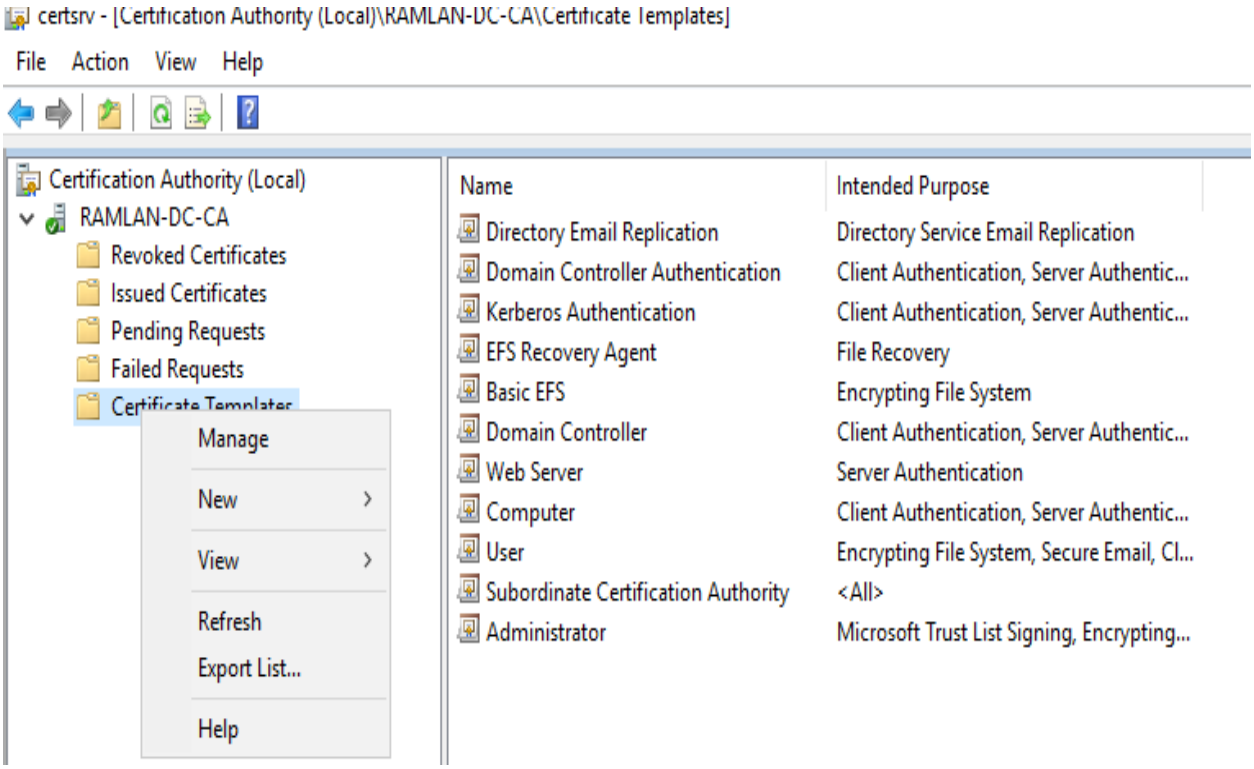
In the above steps we have configured auto enrollment of the workstation authentication template by using group policy. This procedure installs the client certificate on computers and verifies the installation. Restart the workstation computer, and wait a few minutes before logging on. Using the mmc command open the Certificate snap-in dialog box, select Computer account, and then click Next. In the Select Computer dialog box, ensure that Local computer: (the computer this console is running on) is selected, and then click Finish. In the console, expand Certificates (Local Computer), expand Personal, and then click Certificates. In the results pane, confirm that a certificate is displayed that has Client Authentication displayed in the Intended Purpose column, and that SCCM Client Certificate is displayed in the Certificate Template column. Close the console.

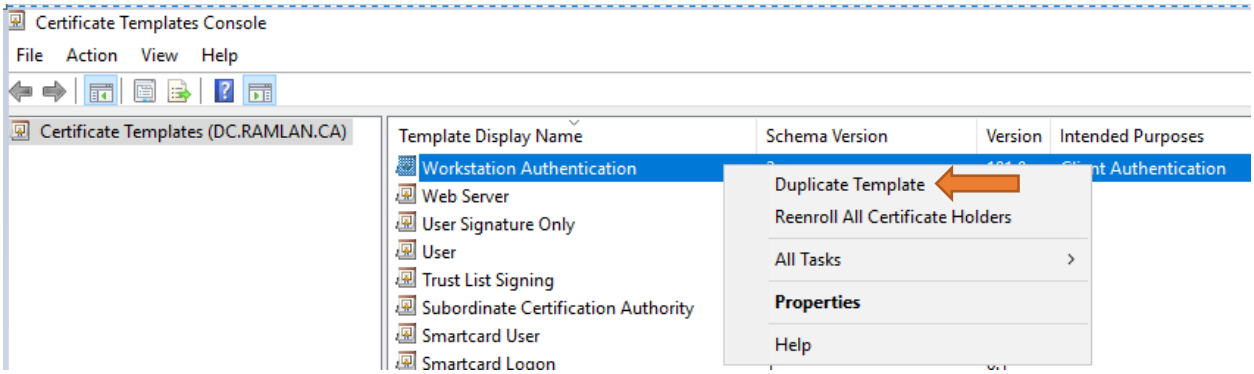


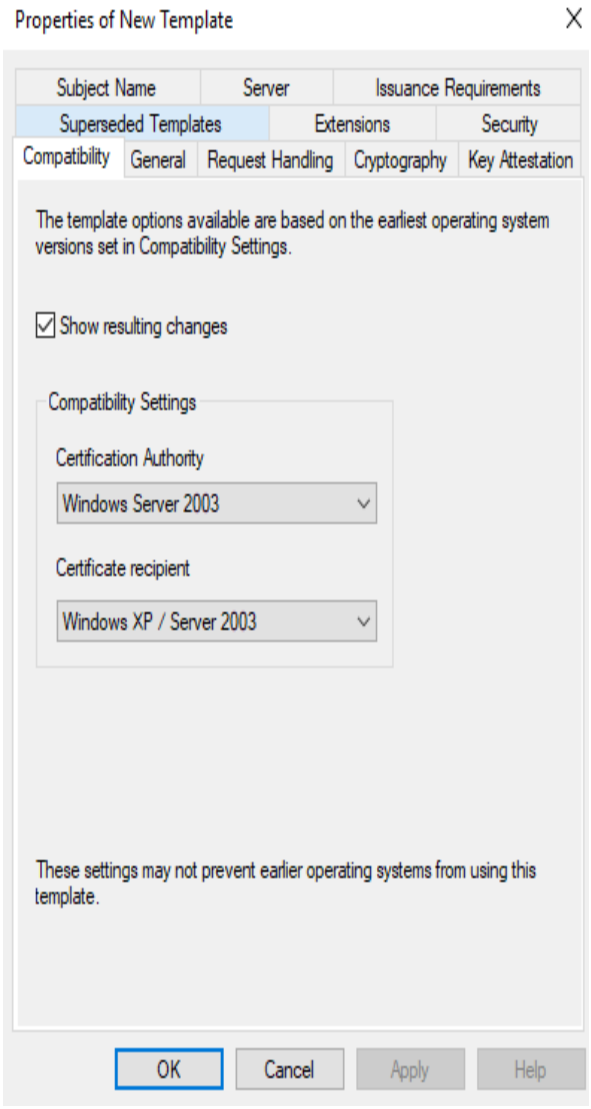
Deploying the Client Certificate for Distribution Points:

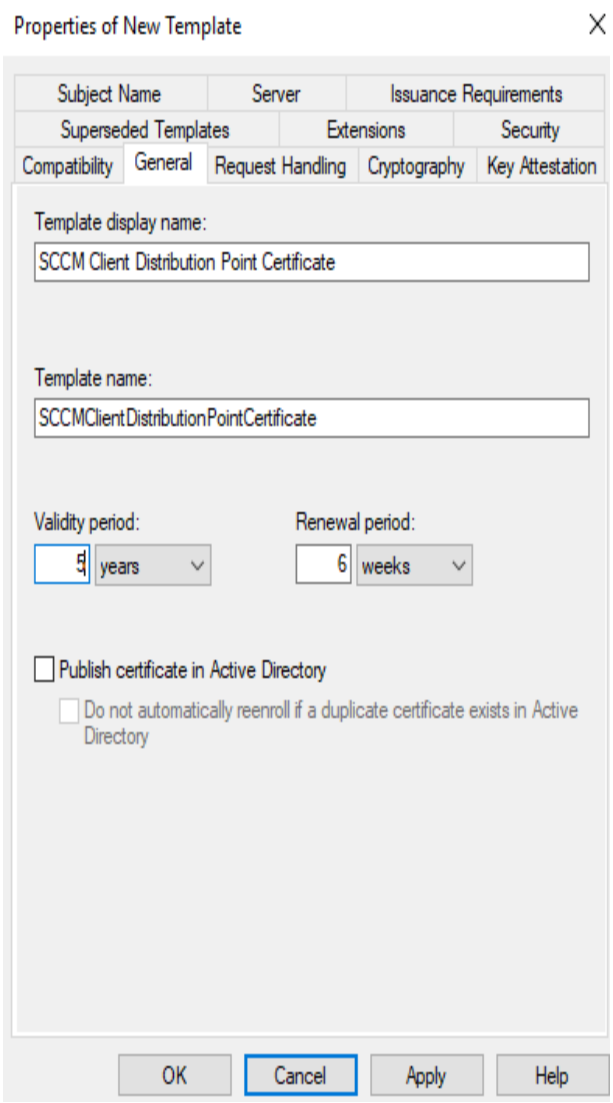
This certificate server two purposes. The certificate is used to authenticate the distribution point to an HTTPS-enabled management point before the distribution point sends status messages. When the Enable PXE support for client's distribution point option is selected, the certificate is sent to computers that PXE boot so that they can connect to a HTTPS-enabled management point during the deployment of the operating system.

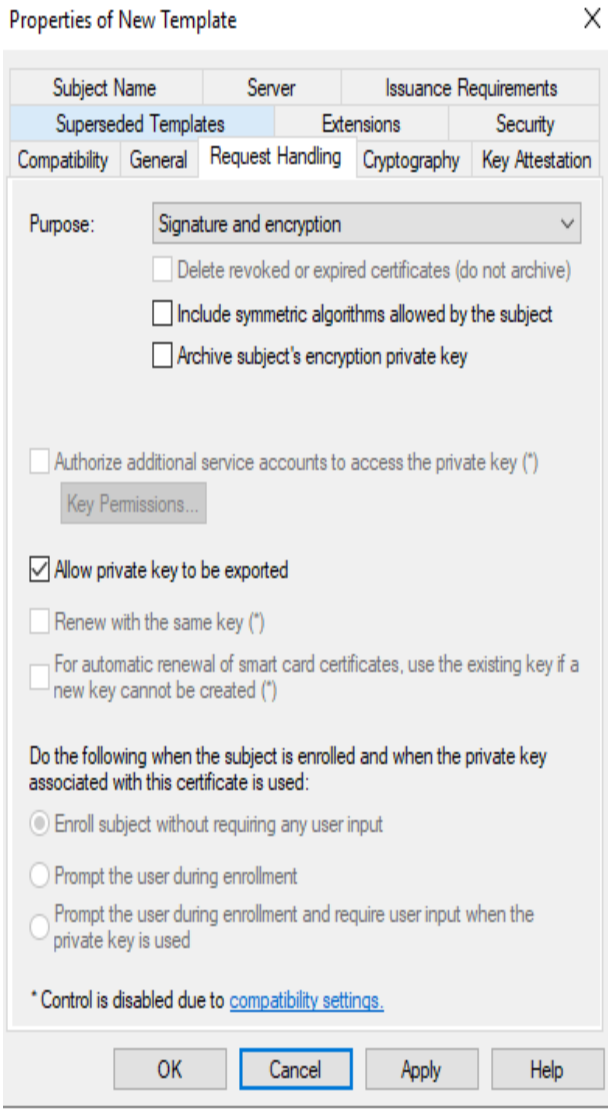
Open Certification Authority from Domain Controller to start **Workstation Authentication Certificate**.

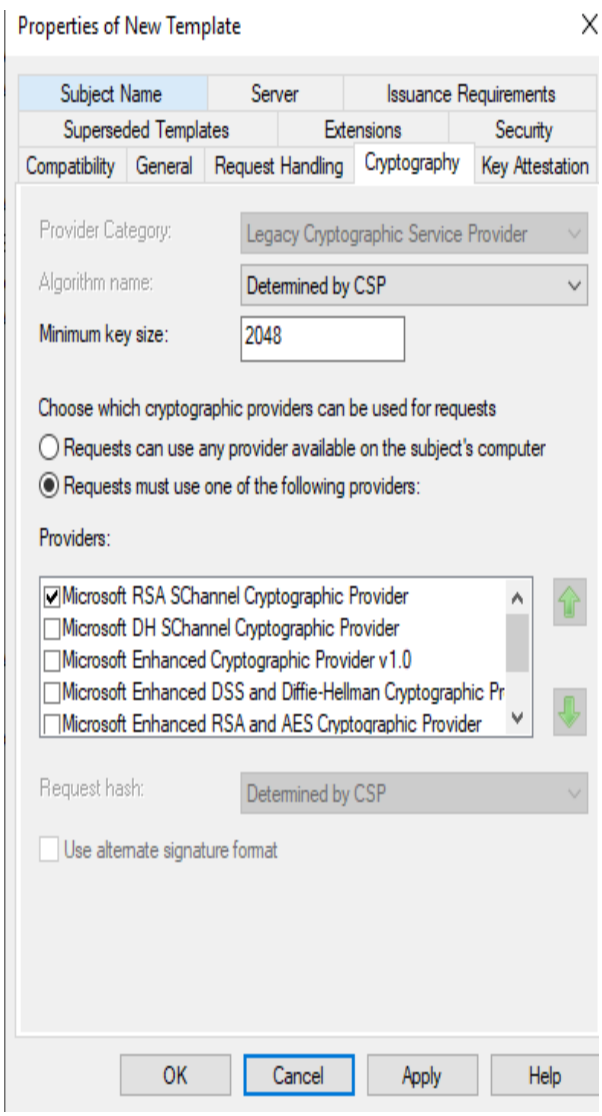


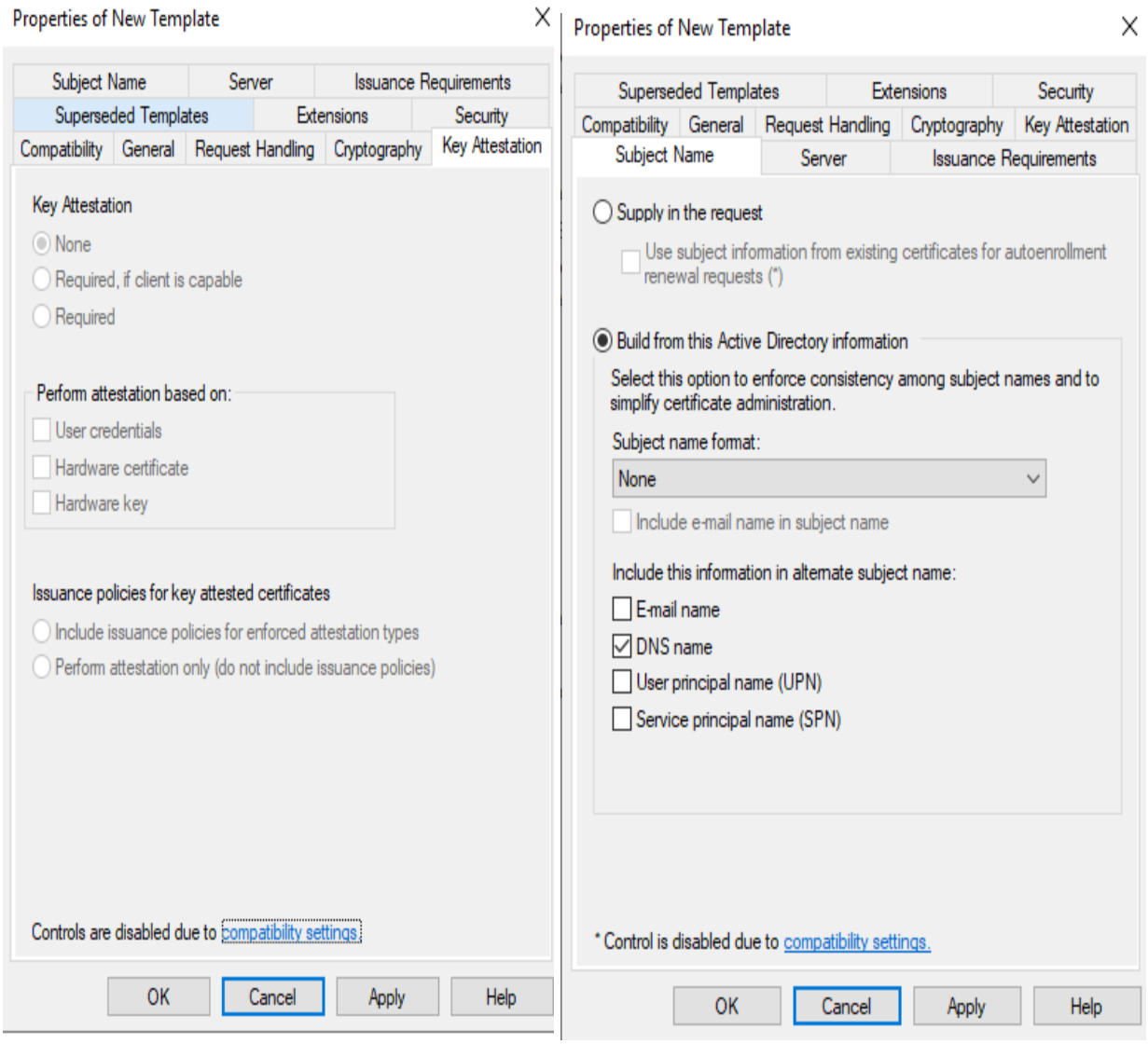


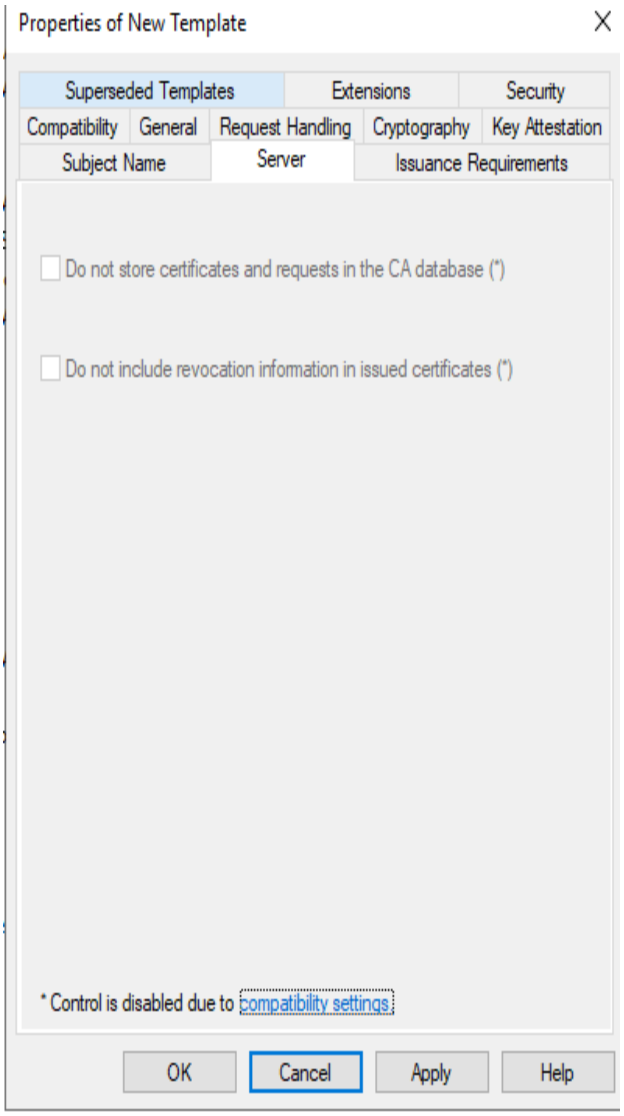

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
The template options available are based on the earliest operating system versions set in Compatibility Settings.
Show resulting 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.
OK
Cancel
Apply
Help

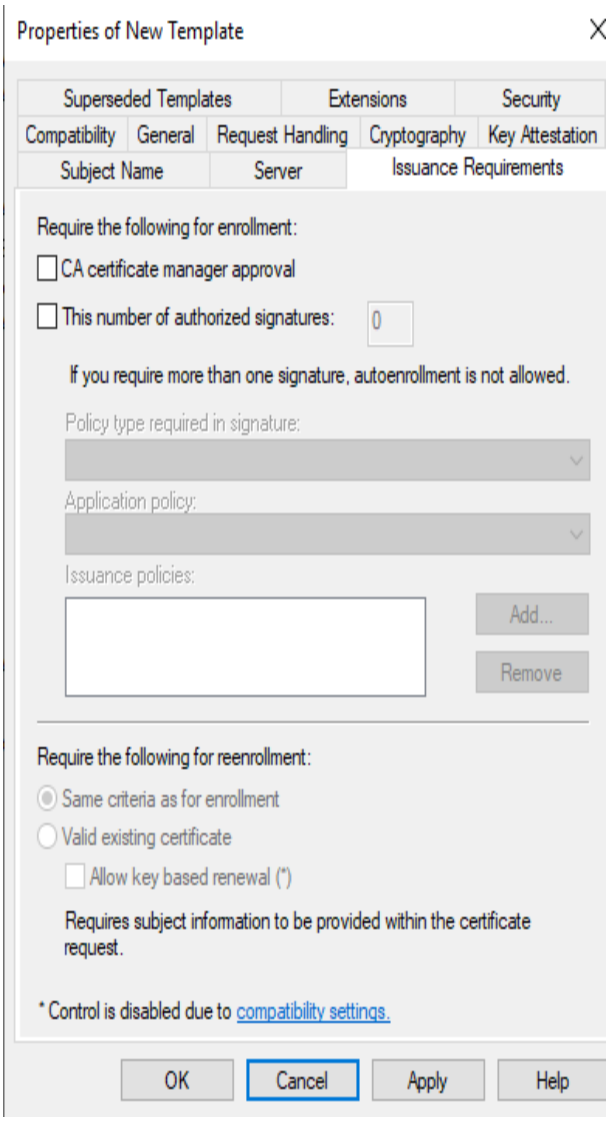

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Template display name:
SCCM Client Distribution Point Certificate
Template name:
SCCMClientDistributionPointCertificate
Validity period:
5
years
Renewal period:
6
weeks
Publish certificate in Active Directory
Do not automatically reenroll if a duplicate certificate exists in Active Directory
OK
Cancel
Apply
Help

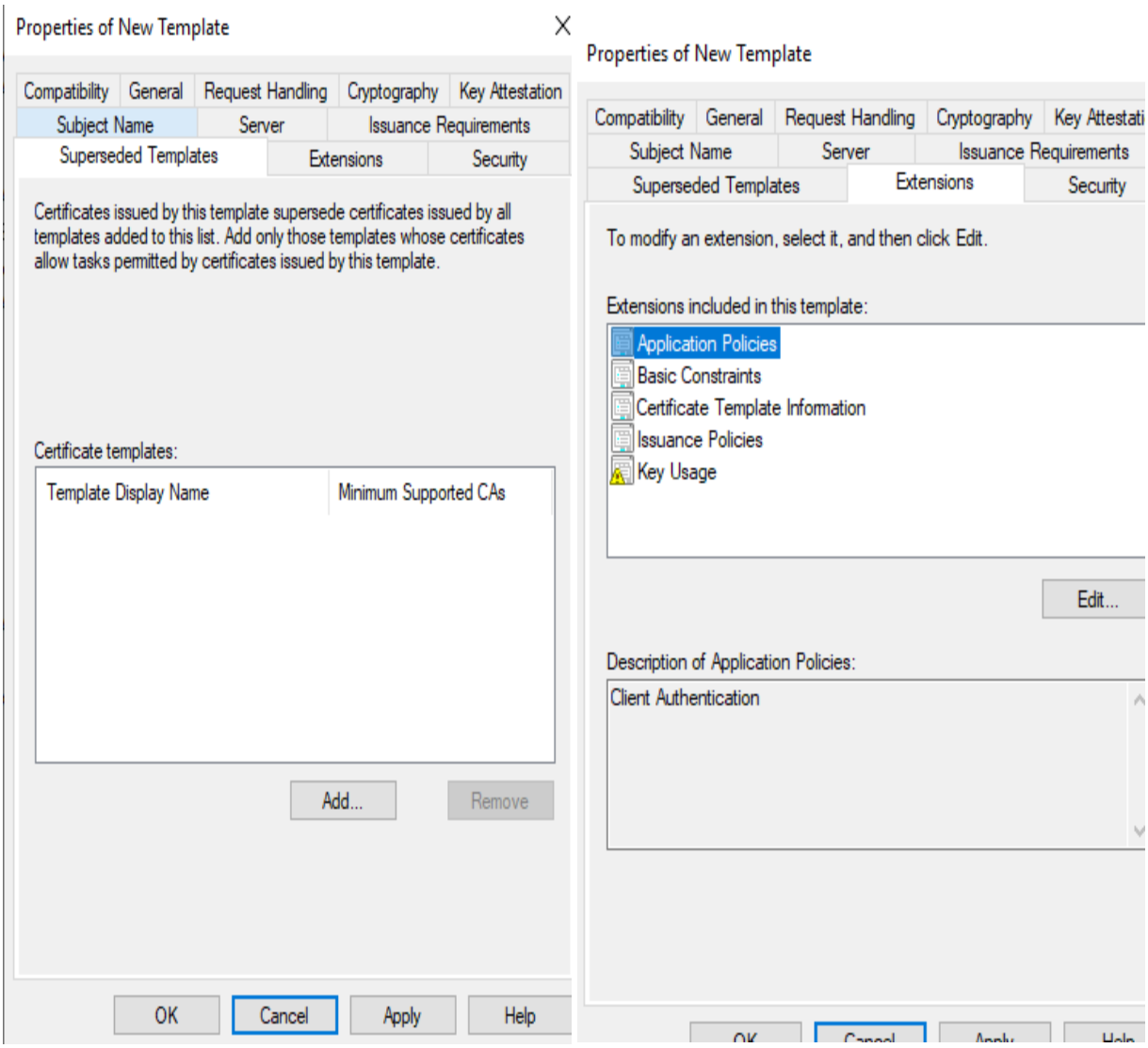

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Purpose:
Signature and encryption
Delete revoked or expired certificates (do not archive)
Include symmetric algorithms allowed by the subject
Archive subject's encryption private key
Authorize additional service accounts to access the private key (*)
Key Permissions...
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.
OK
Cancel
Apply
Help

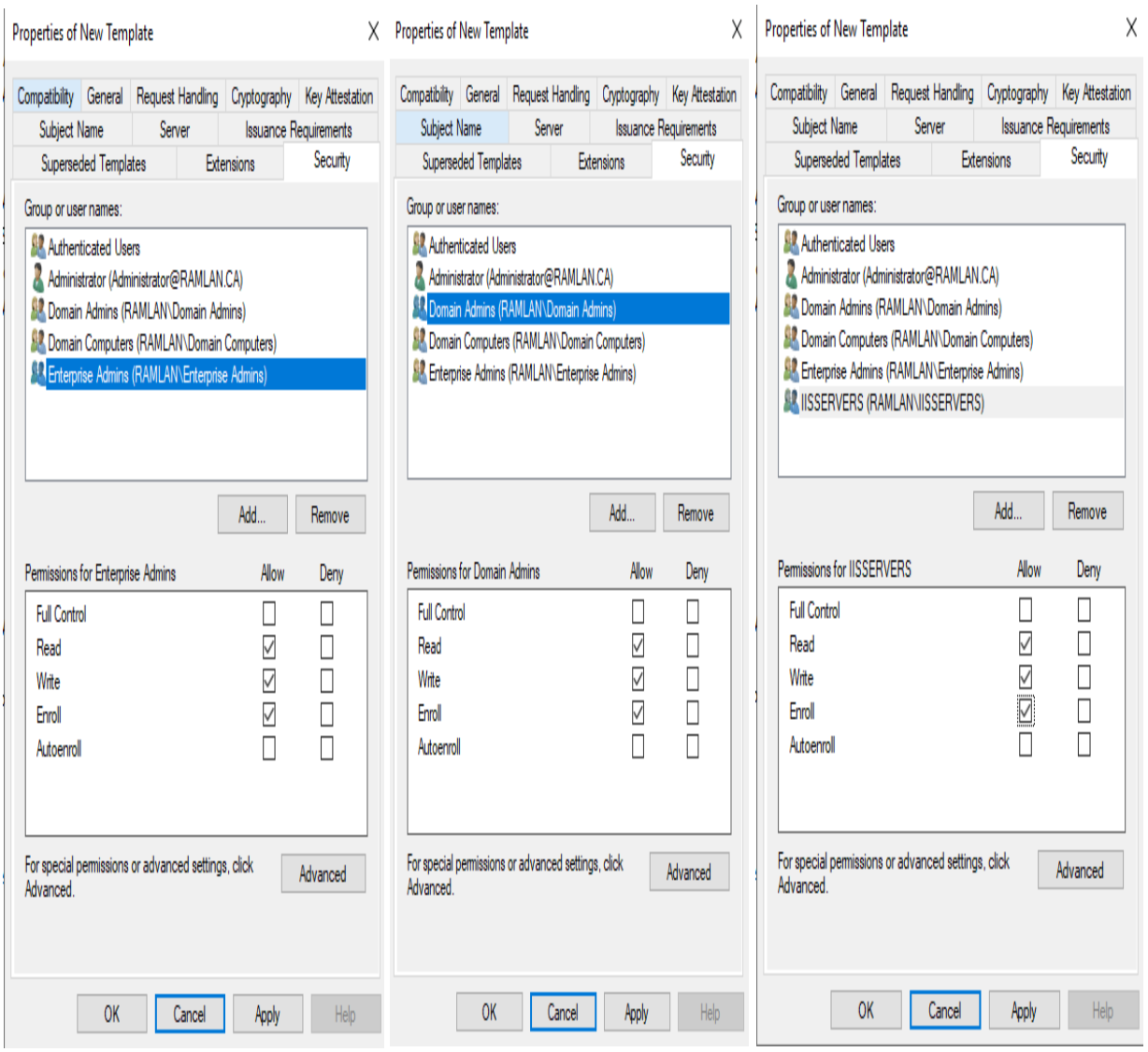

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Provider Category:
Legacy Cryptographic Service Provider
Algorithm name:
Determined by CSP
Minimum key size:
2048
Choose which cryptographic providers can be used for requests
Requests can use any provider available on the subject's computer
Requests must use one of the following providers:
Providers:
Microsoft RSA SChannel Cryptographic Provider
Microsoft DH SChannel Cryptographic Provider
Microsoft Enhanced Cryptographic Provider v1.0
Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr
Microsoft Enhanced RSA and AES Cryptographic Provider
Request hash:
Determined by CSP
Use alternate signature format
OK
Cancel
Apply
Help

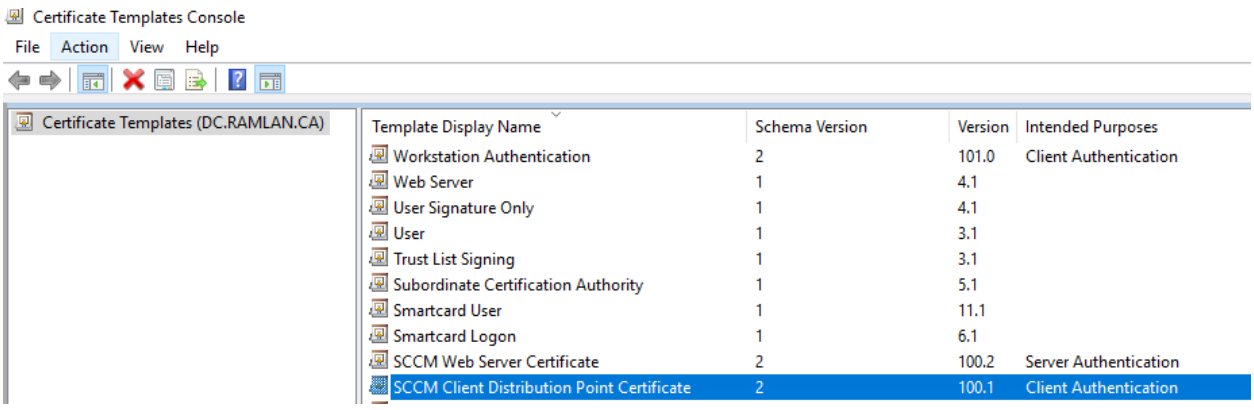

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Key Attestation
None
Required, if client is capable
Required
Perform attestation based on:
User credentials
Hardware certificate
Hardware key
Issuance policies for key attested certificates
Include issuance policies for enforced attestation types
Perform attestation only (do not include issuance policies)
Controls are disabled due to compatibility settings
OK
Cancel
Apply
Help
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:
None
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.
OK
Cancel
Apply
Help


Properties of New Template
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Do not store certificates and requests in the CA database (*)
Do not include revocation information in issued certificates (*)
* Control is disabled due to compatibility settings
OK
Cancel
Apply
Help

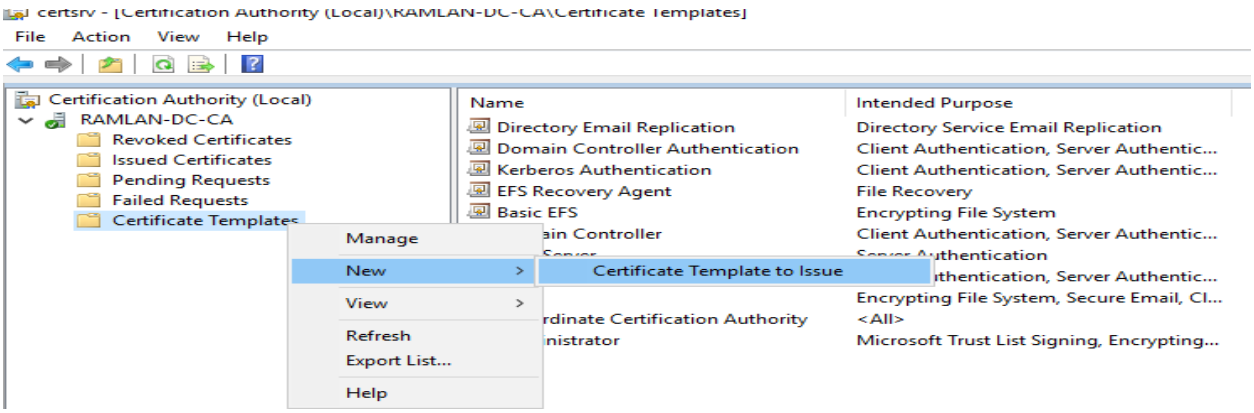

Properties of New Template
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Require the following for enrollment:
CA certificate manager approval
This number of authorized signatures:
0
If you require more than one signature, autoenrollment is not allowed.
Policy type required in signature:
Application policy:
Issuance policies:
Add...
Remove
Require the following for reenrollment:
Same criteria as for enrollment
Valid existing certificate
Allow key based renewal (*)
Requires subject information to be provided within the certificate request.
* Control is disabled due to compatibility settings.
OK
Cancel
Apply
Help

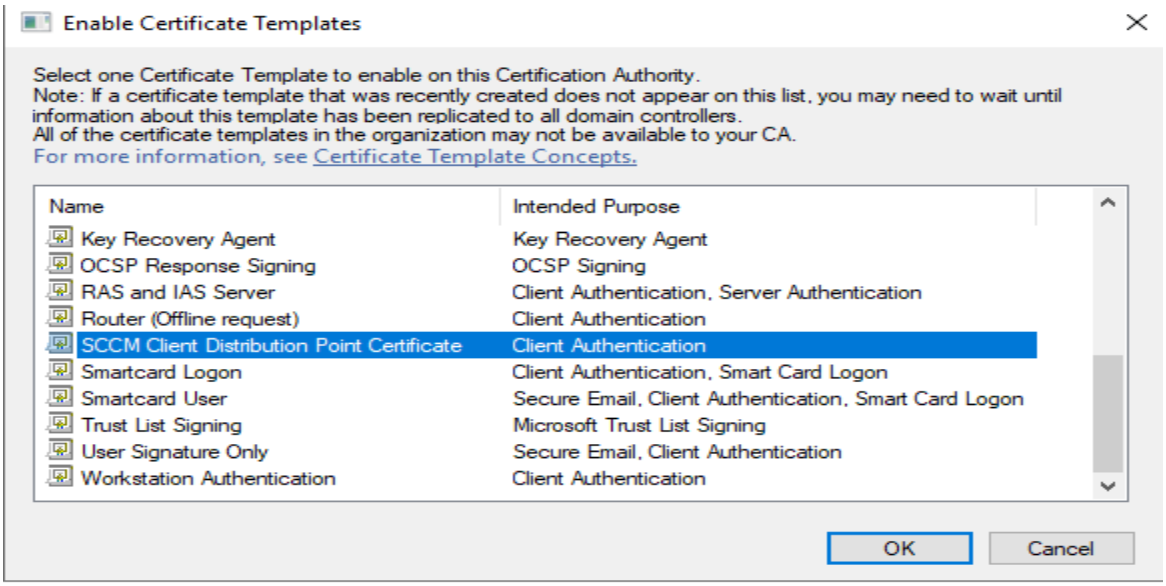

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Certificates issued by this template supersede certificates issued by all templates added to this list. Add only those templates whose certificates allow tasks permitted by certificates issued by this template.
Certificate templates:
Template Display Name
Minimum Supported CAs
Add...
Remove
OK
Cancel
Apply
Help
Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestati
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
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
Edit...
Description of Application Policies:
Client Authentication

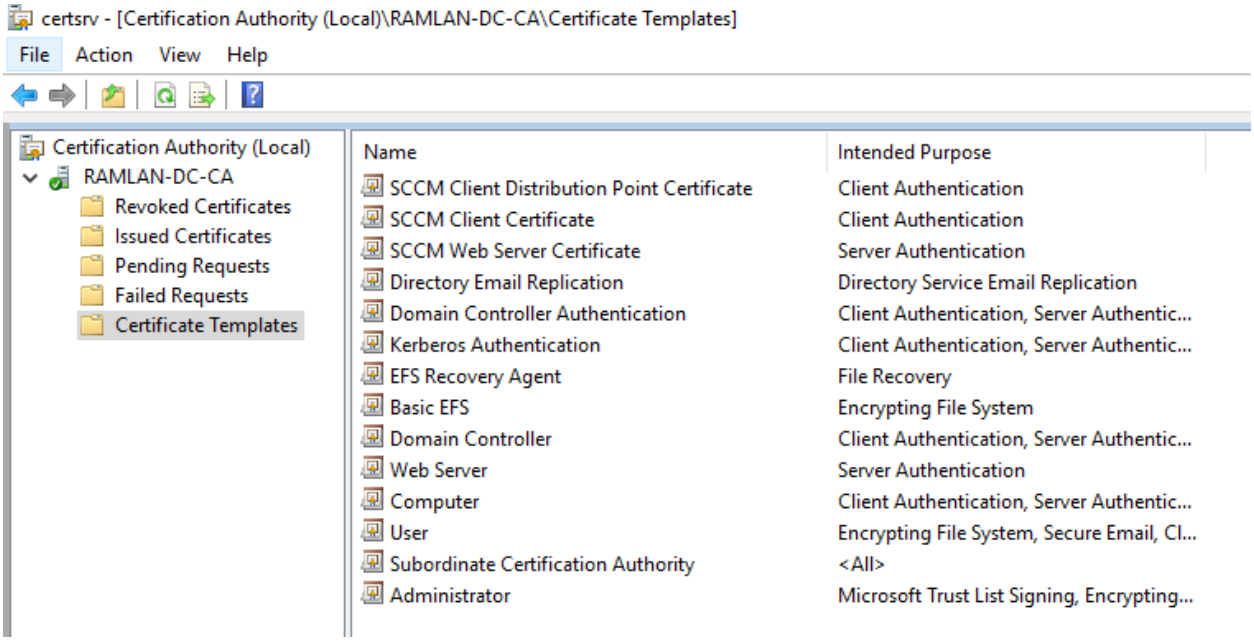

Properties of New Template
Compatibility General Request Handling Cryptography Key Attestation
Subject Name Server Issuance Requirements
Superseded Templates Extensions Security
Group or user names:
Authenticated Users
Administrator (Administrator@RAMLAN.CA)
Domain Admins (RAMLAN\Domain Admins)
Domain Computers (RAMLAN\Domain Computers)
Enterprise Admins (RAMLAN\Enterprise Admins)
Add... Remove
Permissions for Enterprise Admins Allow Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply Help
Properties of New Template
Compatibility General Request Handling Cryptography Key Attestation
Subject Name Server Issuance Requirements
Superseded Templates Extensions Security
Group or user names:
Authenticated Users
Administrator (Administrator@RAMLAN.CA)
Domain Admins (RAMLAN\Domain Admins)
Domain Computers (RAMLAN\Domain Computers)
Enterprise Admins (RAMLAN\Enterprise Admins)
Add... Remove
Permissions for Domain Admins Allow Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply Help
Properties of New Template
Compatibility General Request Handling Cryptography Key Attestation
Subject Name Server Issuance Requirements
Superseded Templates Extensions Security
Group or user names:
Authenticated Users
Administrator (Administrator@RAMLAN.CA)
Domain Admins (RAMLAN\Domain Admins)
Domain Computers (RAMLAN\Domain Computers)
Enterprise Admins (RAMLAN\Enterprise Admins)
IISSERVERS (RAMLAN\IISSERVERS)
Add... Remove
Permissions for IISSERVERS Allow Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply Help


Certificate Templates Console
File Action View Help
Certificate Templates (DC.RAMLAN.CA)
Template Display Name Schema Version Version Intended Purposes
Workstation Authentication 2 101.0 Client Authentication
Web Server 1 4.1
User Signature Only 1 4.1
User 1 3.1
Trust List Signing 1 3.1
Subordinate Certification Authority 1 5.1
Smartcard User 1 11.1
Smartcard Logon 1 6.1
SCCM Web Server Certificate 2 100.2 Server Authentication
SCCM Client Distribution Point Certificate 2 100.1 Client Authentication

Now we will issue the certificate.



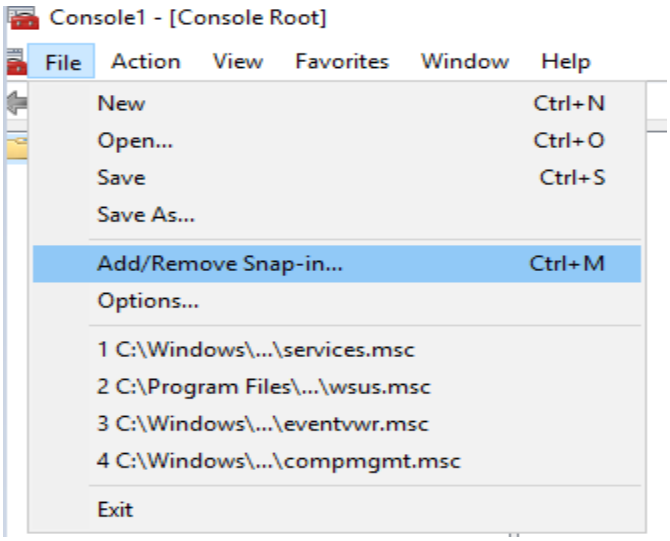


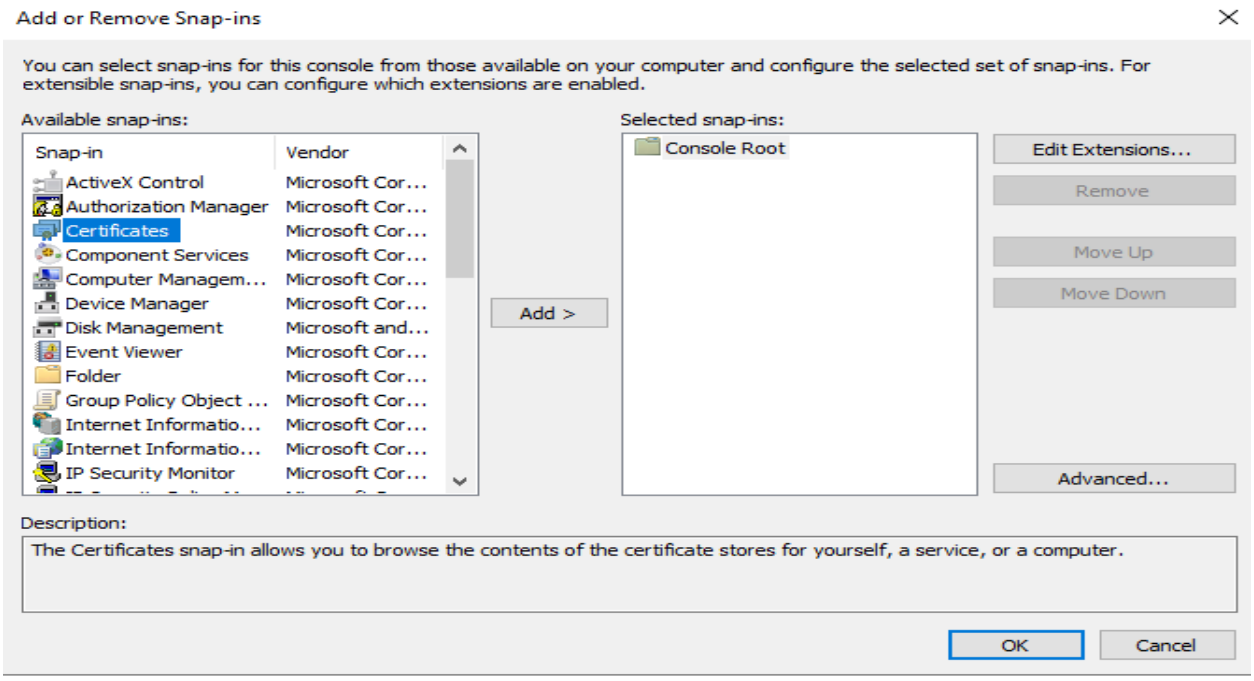


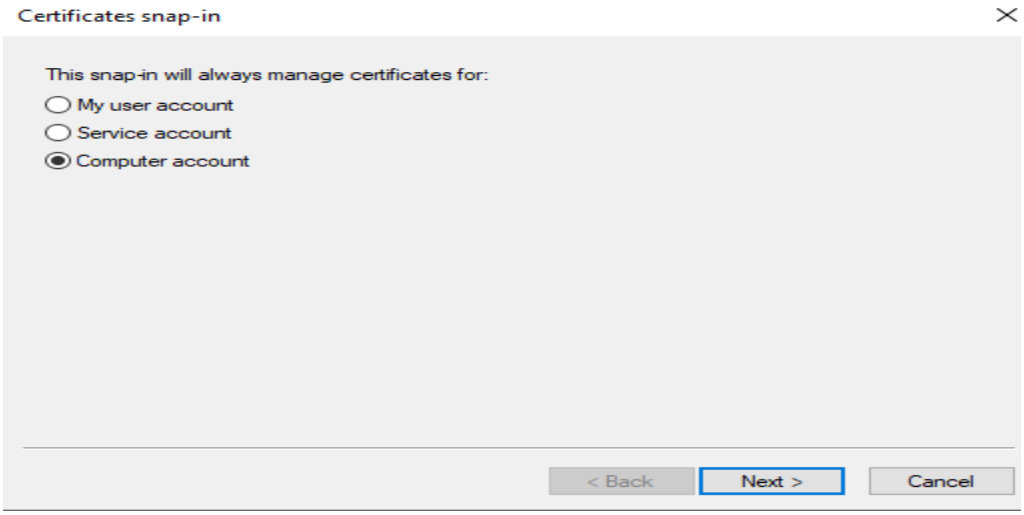
Request the Certificate:

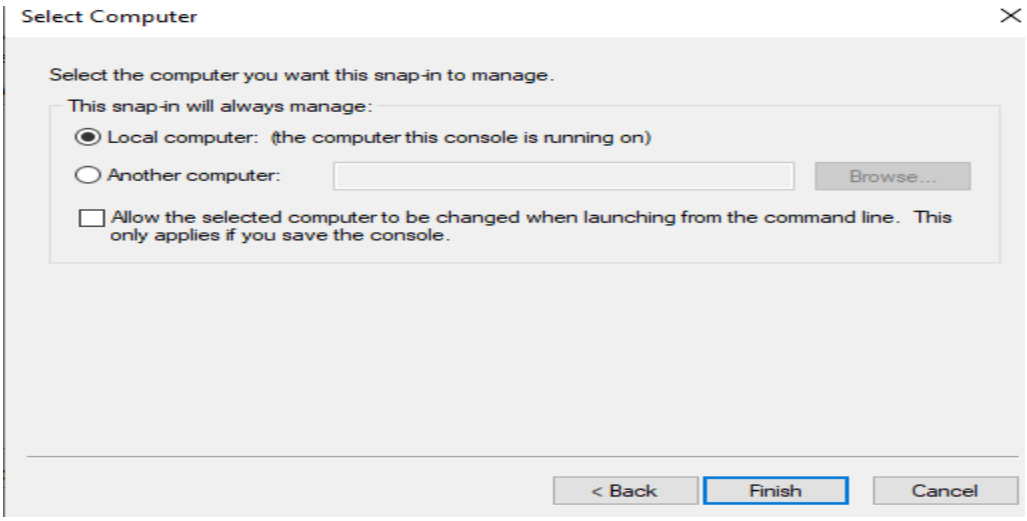
The steps should be performed on Configuration Manager Server (**CB.RAMLAN.CA**) to install the web server certificate that runs IIS. Microsoft recommends you to restart the member server that runs IIS. This is just to ensure that the computer can access the certificate template that you created.

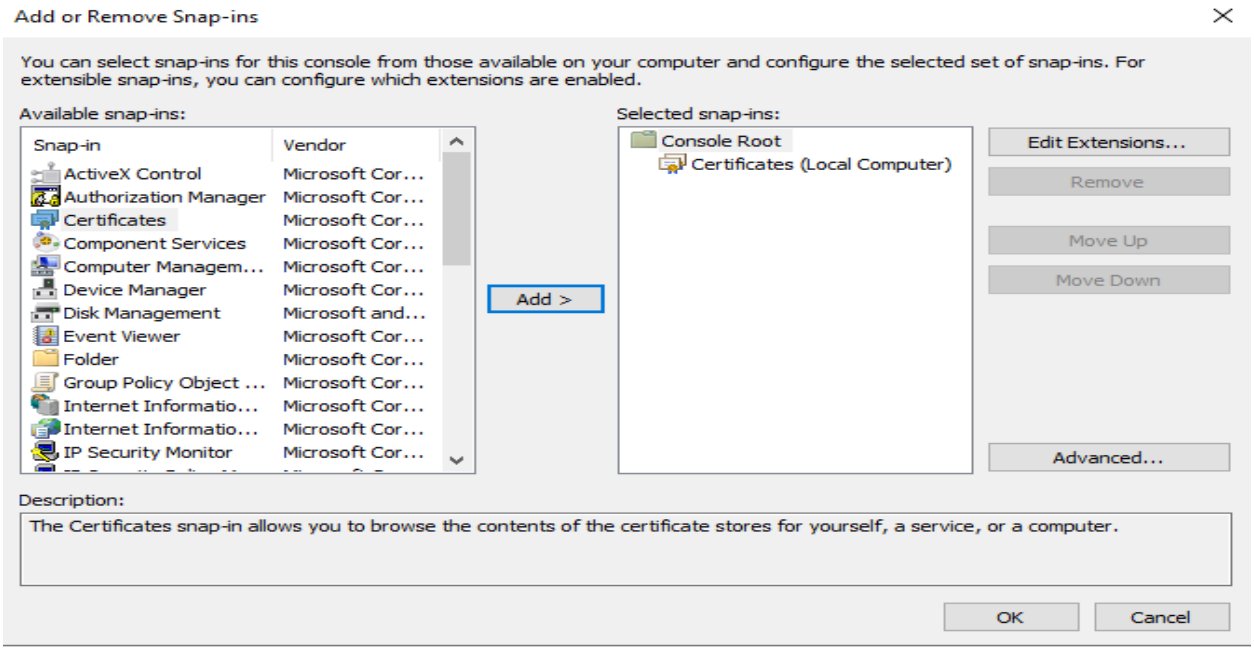
Run the mmc.exe command. In the empty console, click File, and then click Add/Remove Snap-in. In the Add or Remove Snap-ins dialog box, select Certificates from the list of Available snap-ins, and then click Add. In the Certificate snap-in dialog box, select Computer account, and then click Next. In the Select Computer dialog box, ensure Local computer: (the computer this console is running on) is selected, and then click Finish. In the Add or Remove Snap-ins dialog box, click OK. In the console, expand Certificates (Local Computer), and then click Personal. Right-click Certificates, click All Tasks, and then click Request New Certificate.

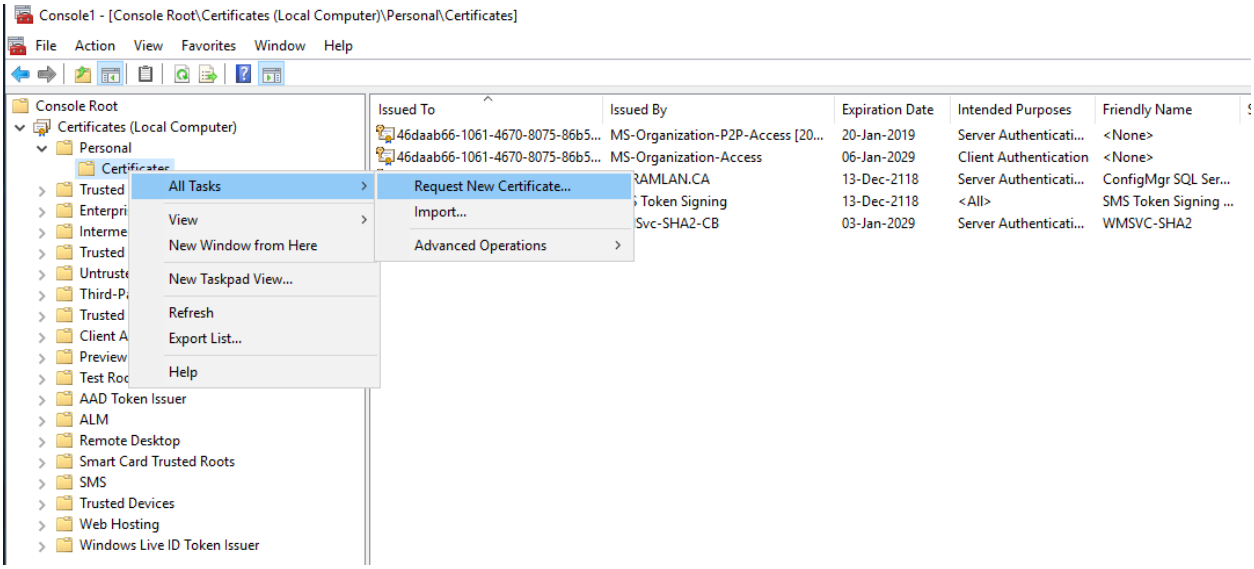





Certificates snap-in
This snap-in will always manage certificates for:
My user account
Service account
Computer account
< Back
Next >
Cancel


Select Computer
Select the computer you want this snap-in to manage.
This snap-in will always manage:
Local computer: (the computer this console is running on)
Another computer:
Browse...
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.
< Back
Finish
Cancel


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
ActiveX Control
Microsoft Cor...
Authorization Manager
Microsoft Cor...
Certificates
Microsoft Cor...
Component Services
Microsoft Cor...
Computer Managem...
Microsoft Cor...
Device Manager
Microsoft Cor...
Disk Management
Microsoft and...
Event Viewer
Microsoft Cor...
Folder
Microsoft Cor...
Group Policy Object ...
Microsoft Cor...
Internet Informatio...
Microsoft Cor...
Internet Informatio...
Microsoft Cor...
IP Security Monitor
Microsoft Cor...
Add >
Selected snap-ins:
Console Root
Certificates (Local Computer)
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
Description:
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.
OK
Cancel



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

Next Cancel

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

Enrollment Policy ID: {344C808C-D718-4B47-A80E-9CE5D2179167}

Properties

Configured by you Add New

Next Cancel

Certificate Enrollment

Request Certificates

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

Active Directory Enrollment Policy

☐ Computer	**STATUS:** Available	Details
☐ SCCM Client Certificate	**STATUS:** Available	Details
☑ SCCM Client Distribution Point Certificate	**STATUS:** Available	Details
☐ SCCM Web Server Certificate	**STATUS:** Available	Details

More information is required to enroll for this certificate. Click here to configure settings.

☐ Show all templates

Enroll Cancel

Certificate Enrollment

Certificate Installation Results

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

Active Directory Enrollment Policy

SCCM Client Distribution Point Certificate	**STATUS:** Succeeded	Details

Finish

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

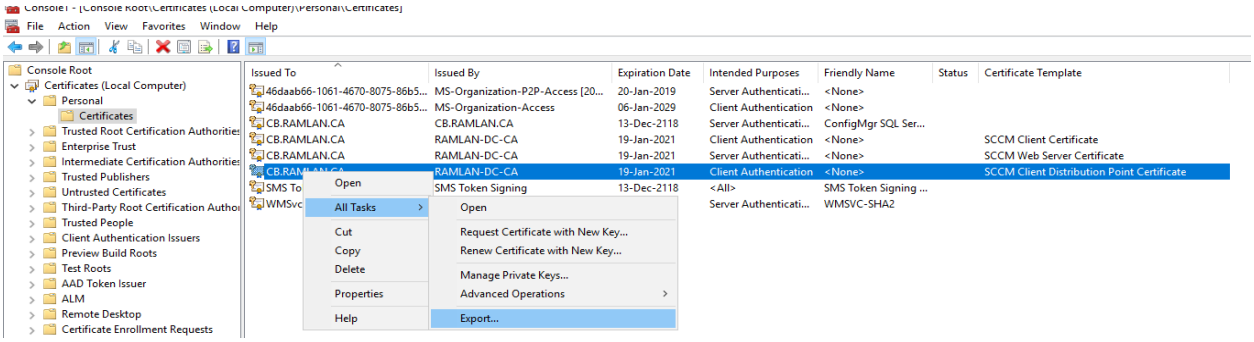
File Action View Favorites Window Help

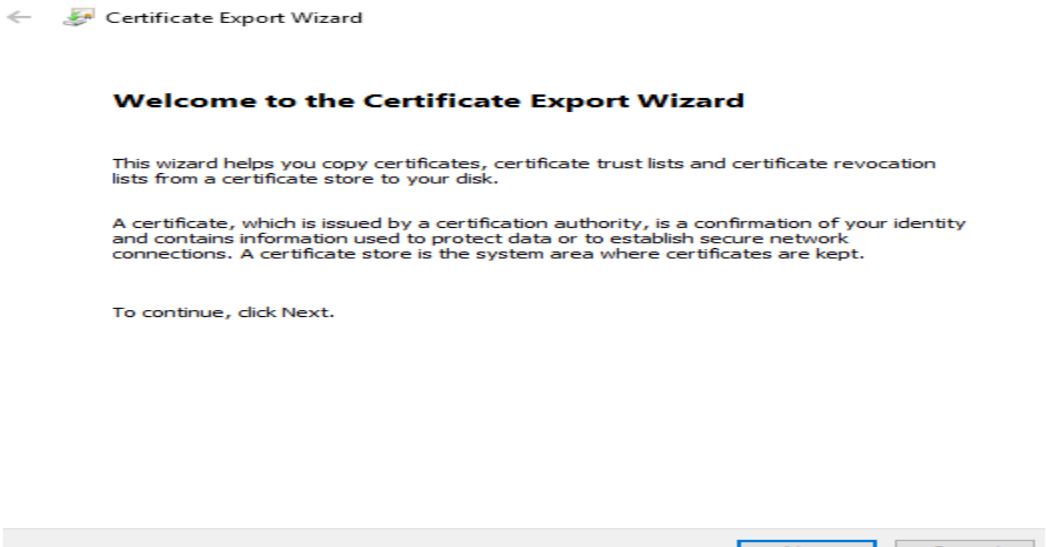
Console Root
- Certificates (Local Computer)
  - Personal
    - Certificates
  - Trusted Root Certification Authorities
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Trusted Publishers

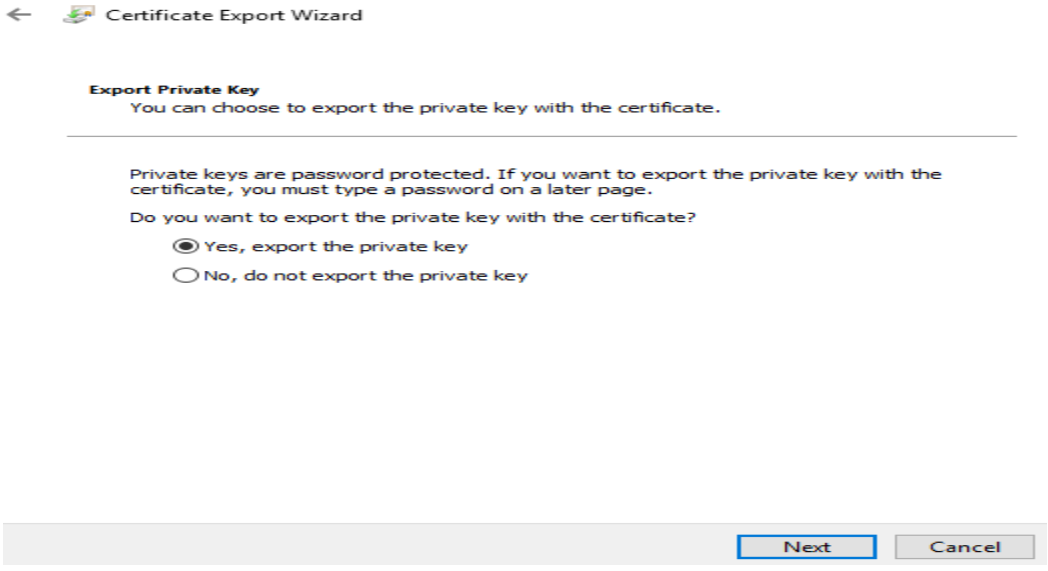
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Template
46daab66-1061-4670-8075-86b5...	MS-Organization-P2P-Access [20...	20-Jan-2019	Server Authenticati...	<None>		
46daab66-1061-4670-8075-86b5...	MS-Organization-Access	06-Jan-2029	Client Authentication	<None>		
CB.RAMLAN.CA	CB.RAMLAN.CA	13-Dec-2118	Server Authenticati...	ConfigMgr SQL Ser...		
CB.RAMLAN.CA	RAMLAN-DC-CA	19-Jan-2021	Client Authentication	<None>		SCCM Client Certificate
CB.RAMLAN.CA	RAMLAN-DC-CA	19-Jan-2021	Server Authenticati...	<None>		SCCM Web Server Certificate
CB.RAMLAN.CA	RAMLAN-DC-CA	19-Jan-2021	Client Authentication	<None>		SCCM Client Distribution Point Certificate

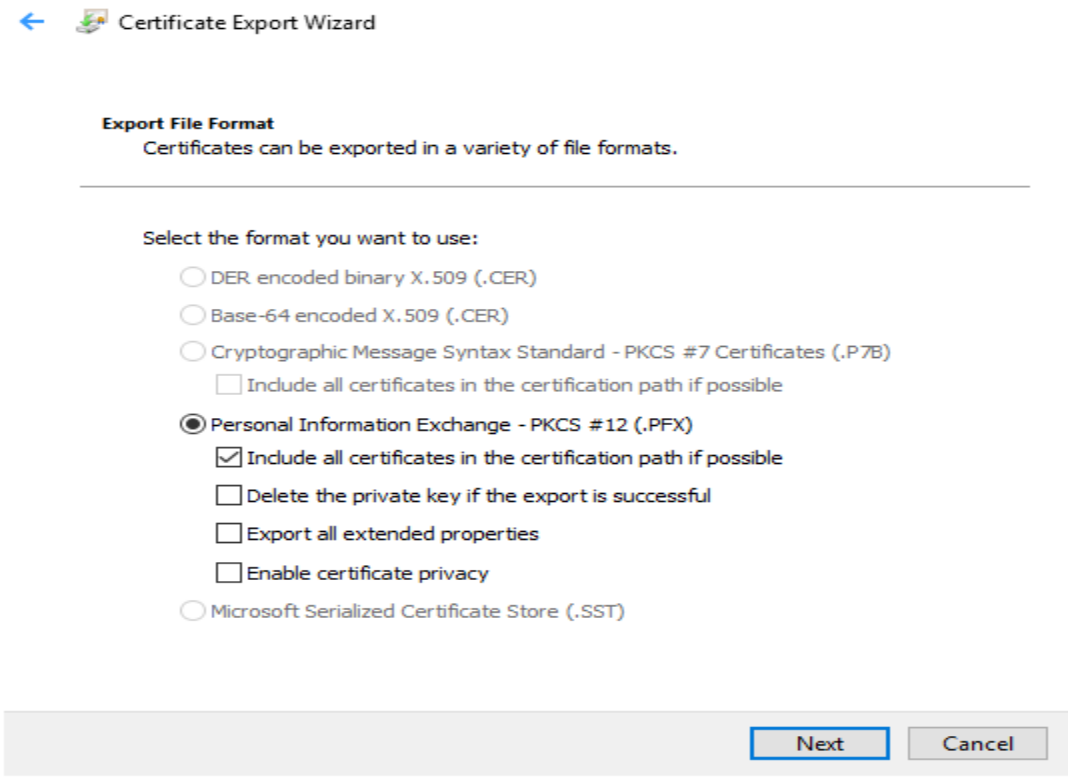
Exporting the Client Certificate for Distribution Points:

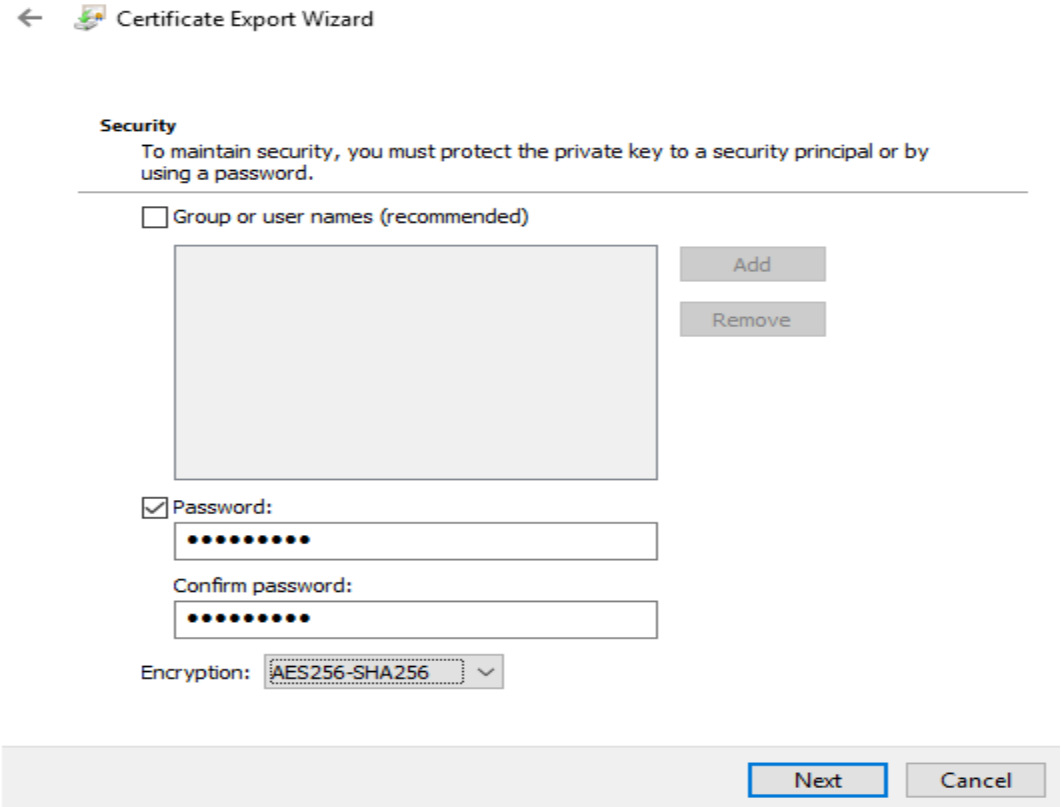
In the Certificates (Local Computer) console, right-click the certificate that you have just installed, select All Tasks, and then click Export.

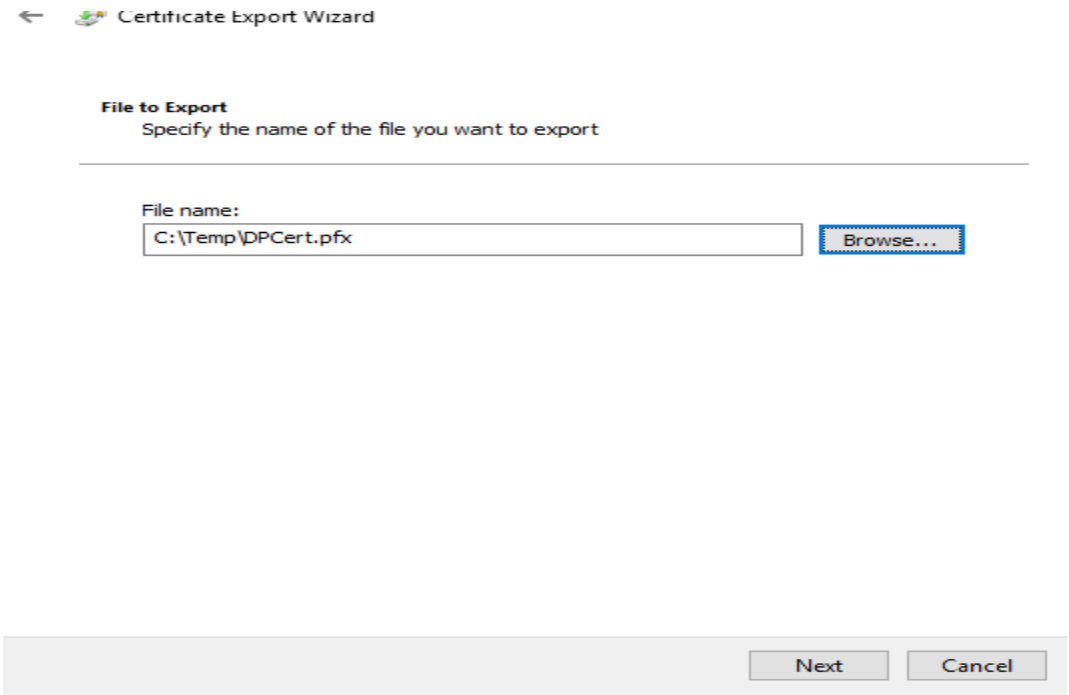


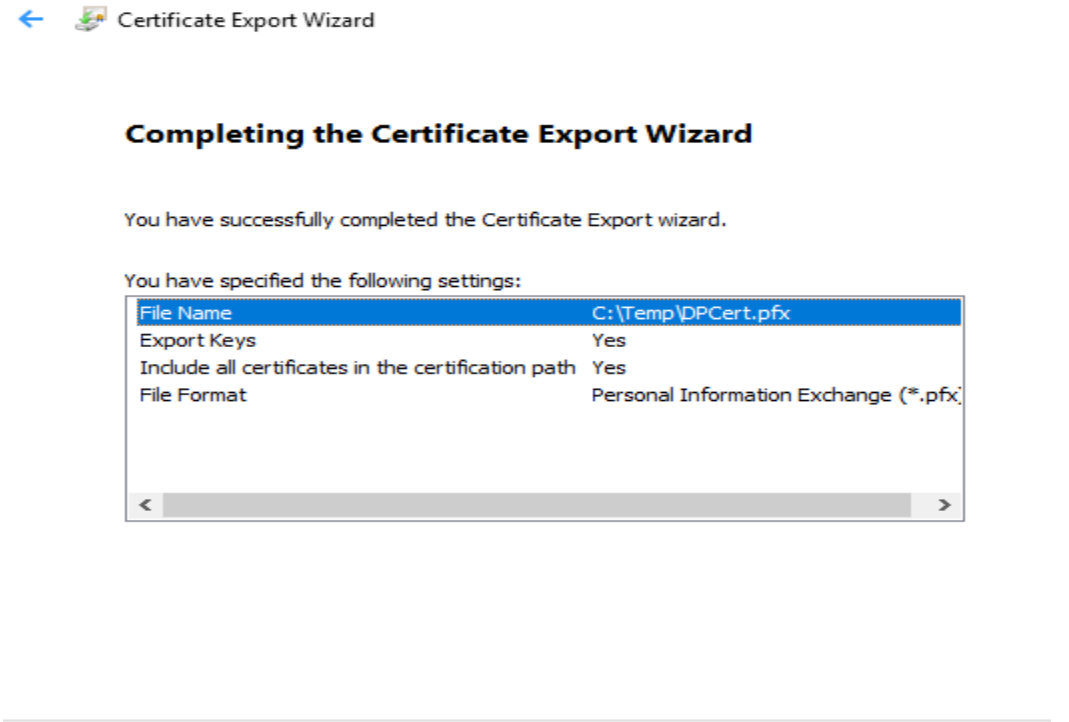


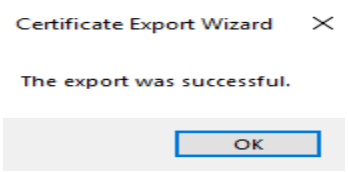



Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification 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)
Next
Cancel


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)
Add
Remove
Password:
Confirm password:
Encryption:
AES256-SHA256
Next
Cancel

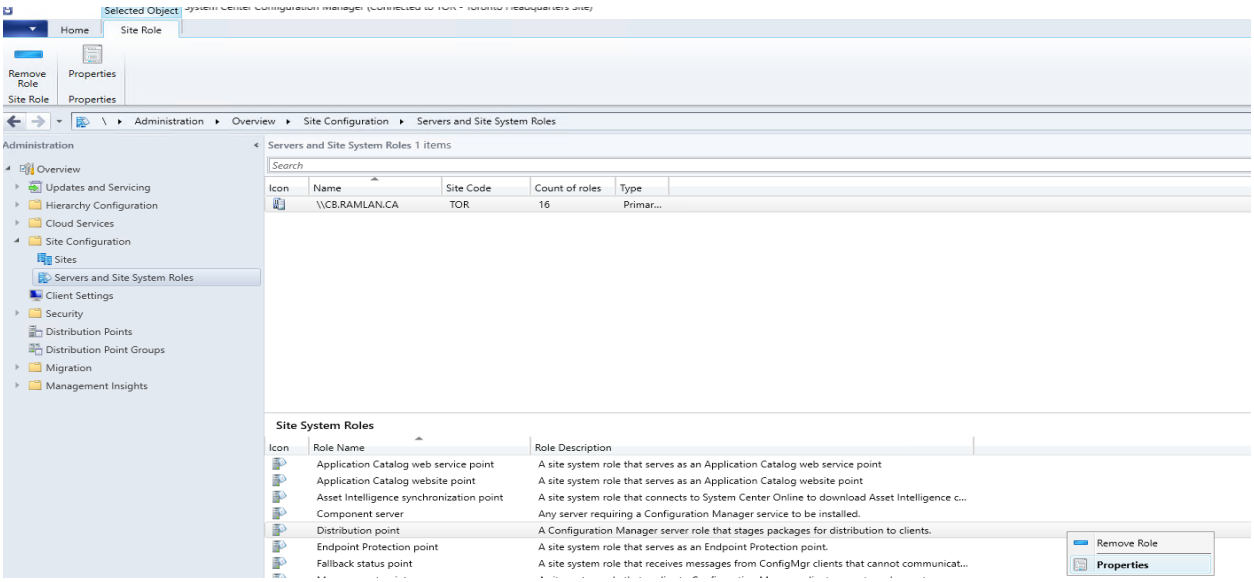

Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
C:\Temp\DPCert.pfx
Browse...
Next
Cancel

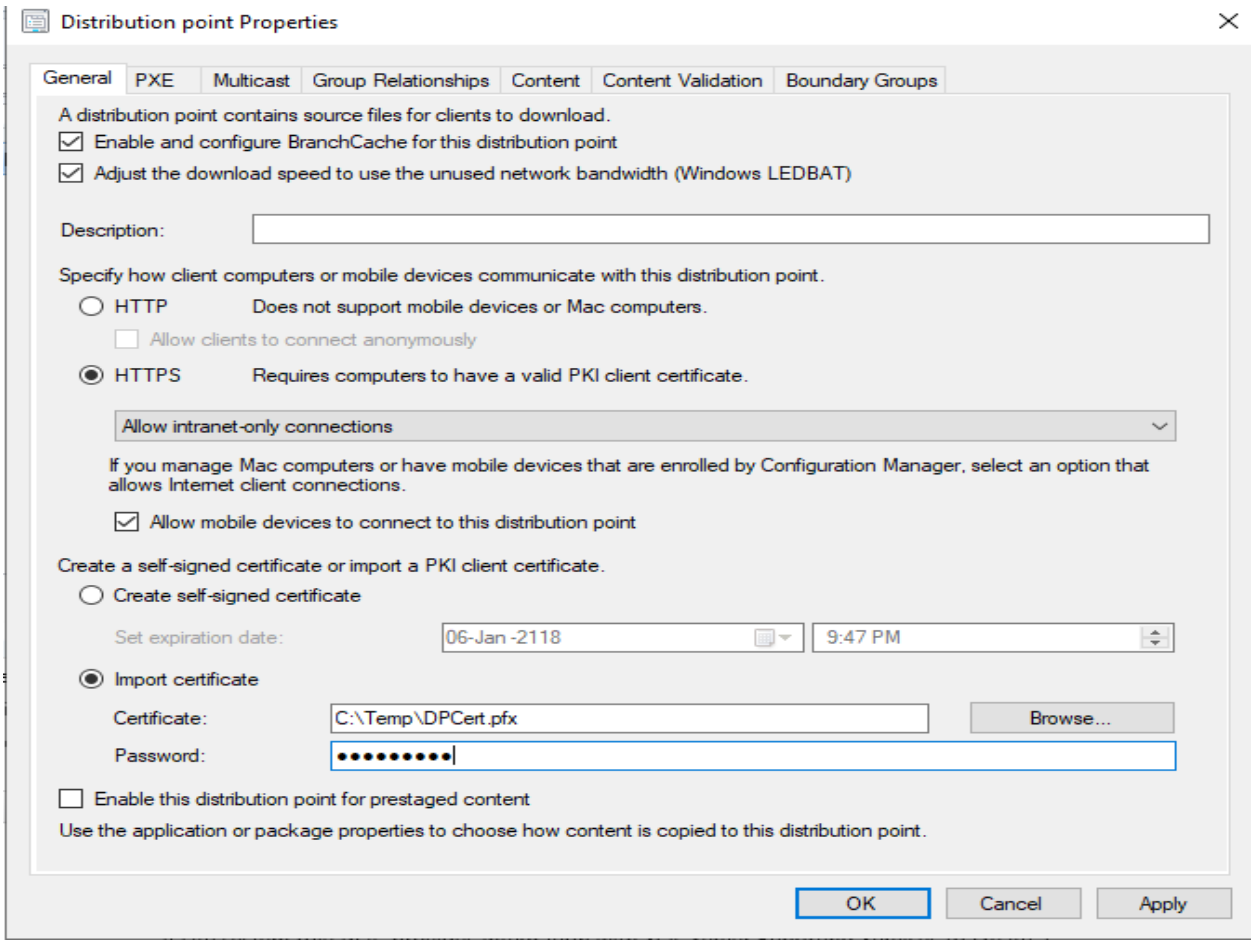

Certificate Export Wizard
Completing the Certificate Export Wizard
You have successfully completed the Certificate Export wizard.
You have specified the following settings:
File Name C:\Temp\DPCert.pfx
Export Keys Yes
Include all certificates in the certification path Yes
File Format Personal Information Exchange (*.pfx)
Finish
Cancel


Certificate Export Wizard
The export was successful.
OK

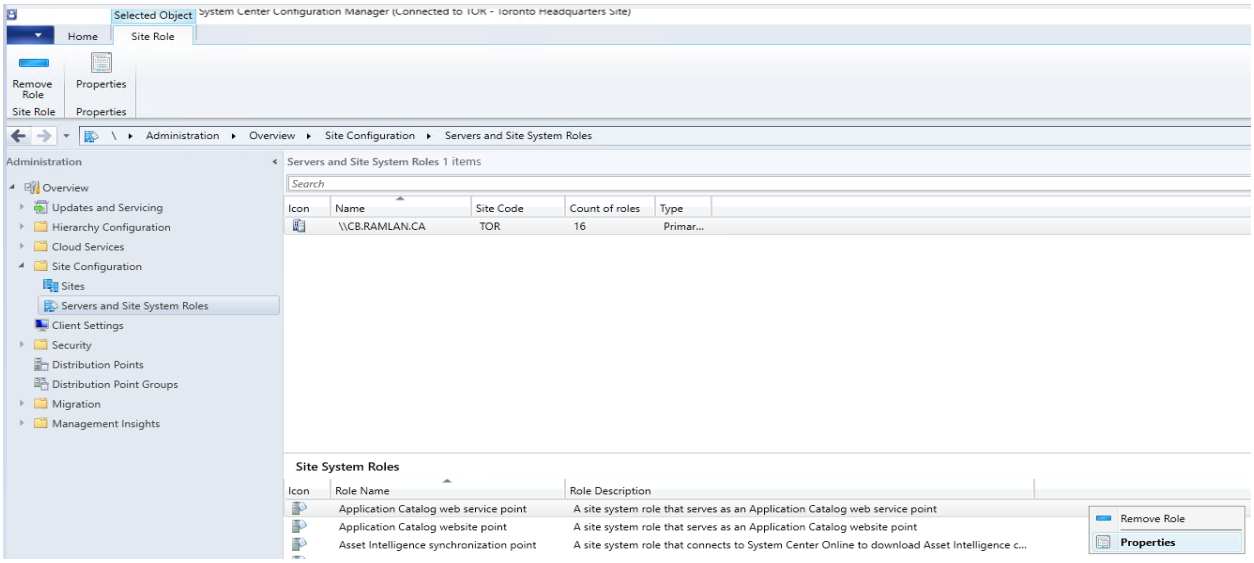
Deploying the Client Certificate for Distribution Points:

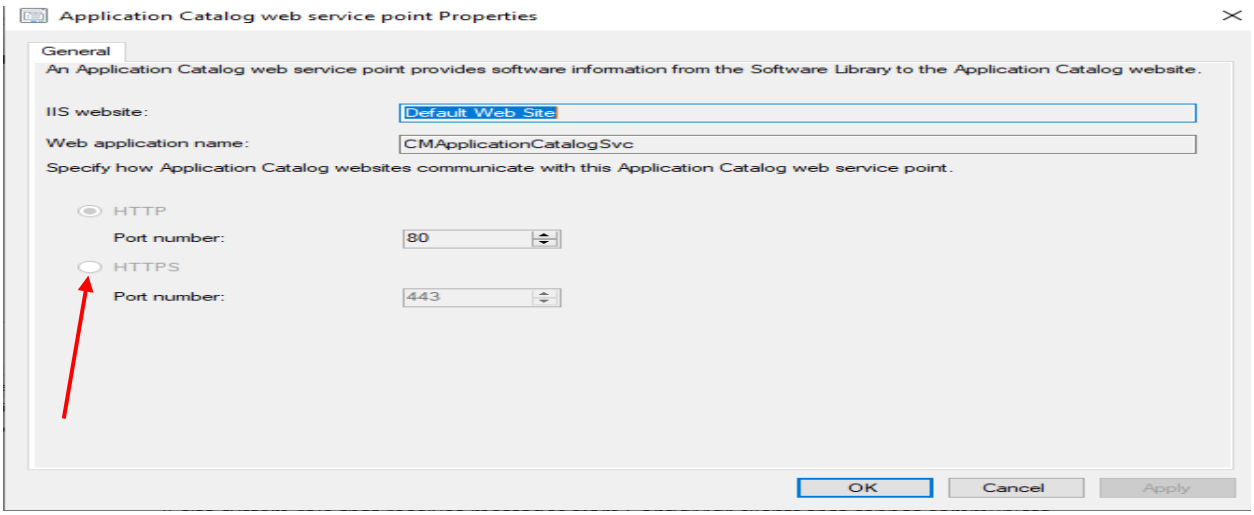
Now that we have got the client certificate for distribution points, let's assign them to the DP's. Right click on the DP and under General tab, choose HTTPS and to import the certificate click on Browse. Import the certificate that you have exported in the above steps, provide the password and click OK.

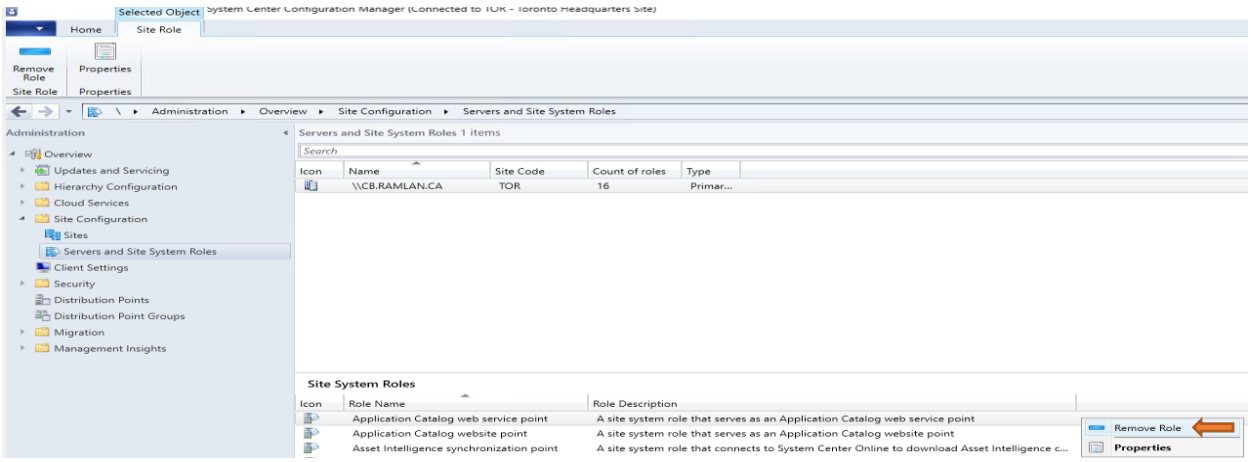


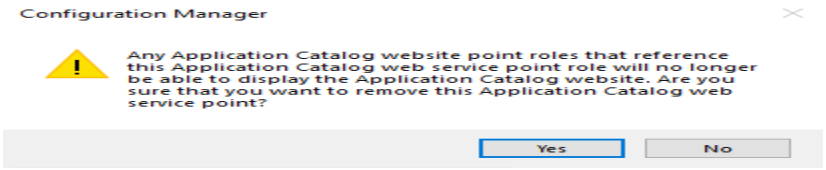


For other roles, you may not be able to switch from HTTP to HTTPS as the options are greyed out. For example, on Application catalog web service point, the options are greyed out. You have to uninstall both App catalog website point and App catalog web service point role and install the roles again.

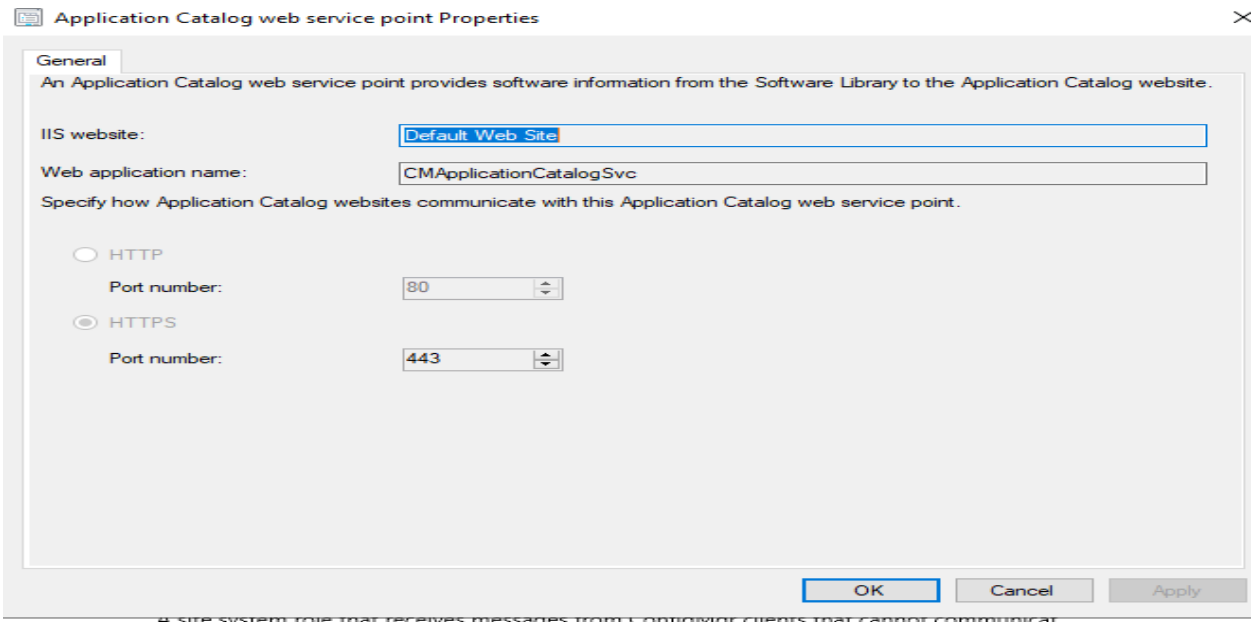


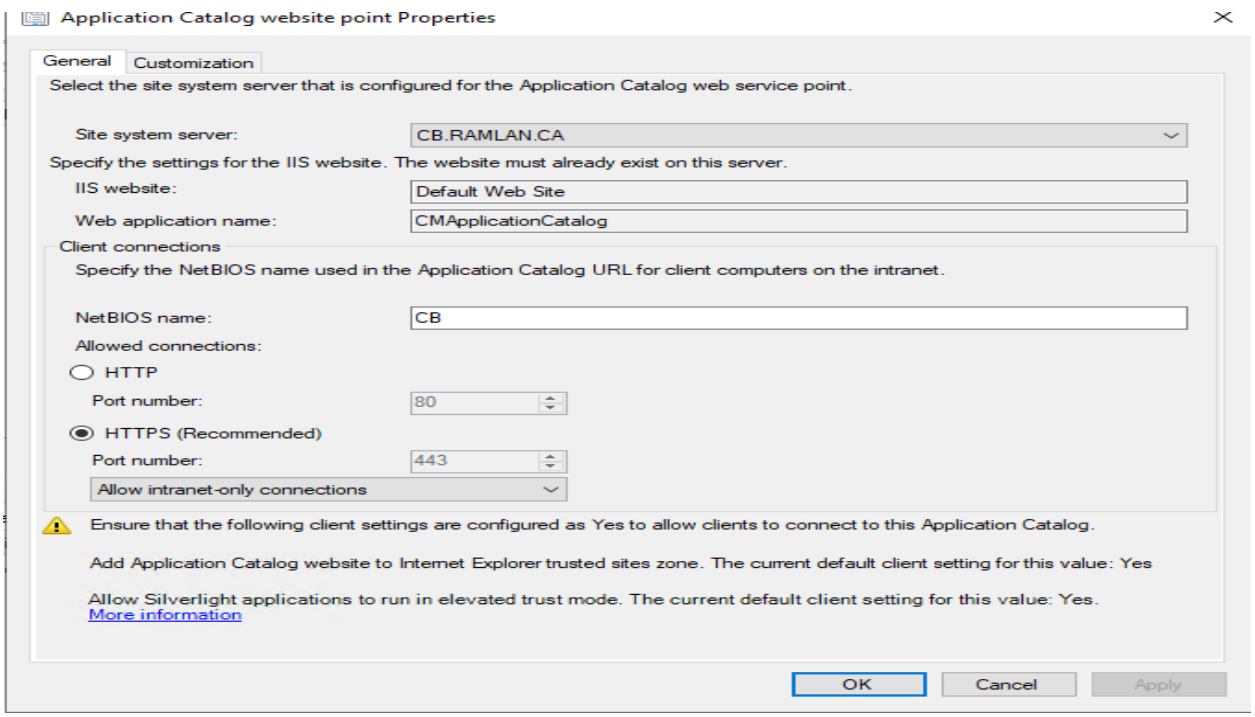




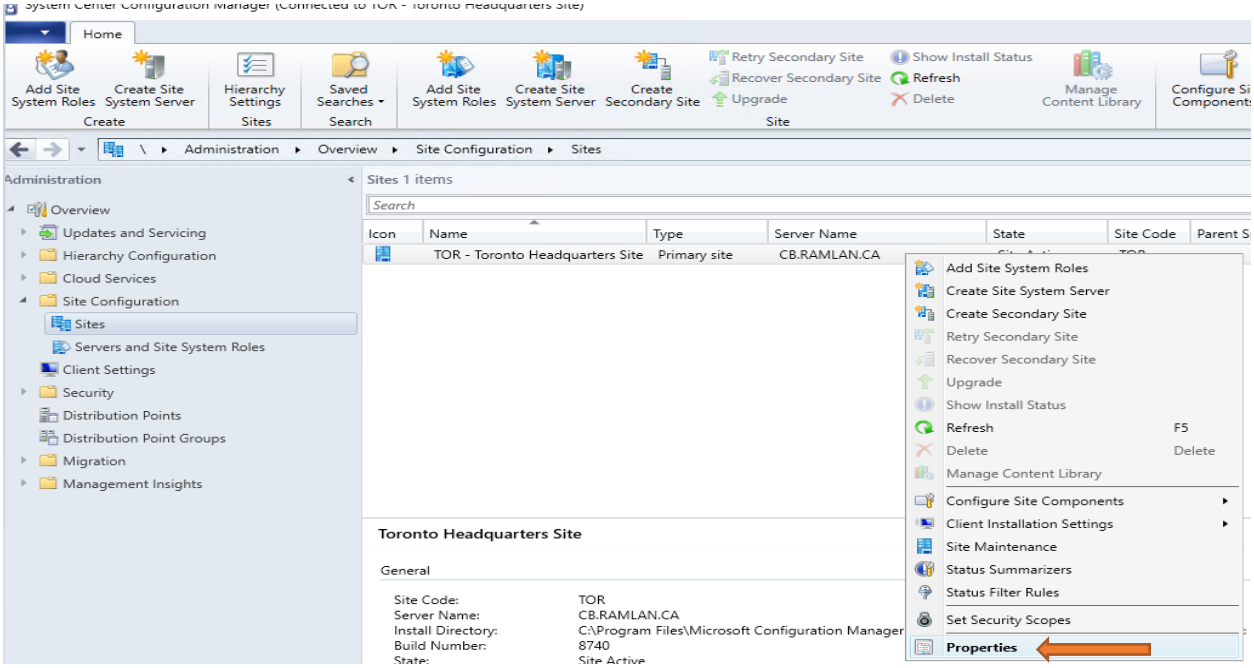


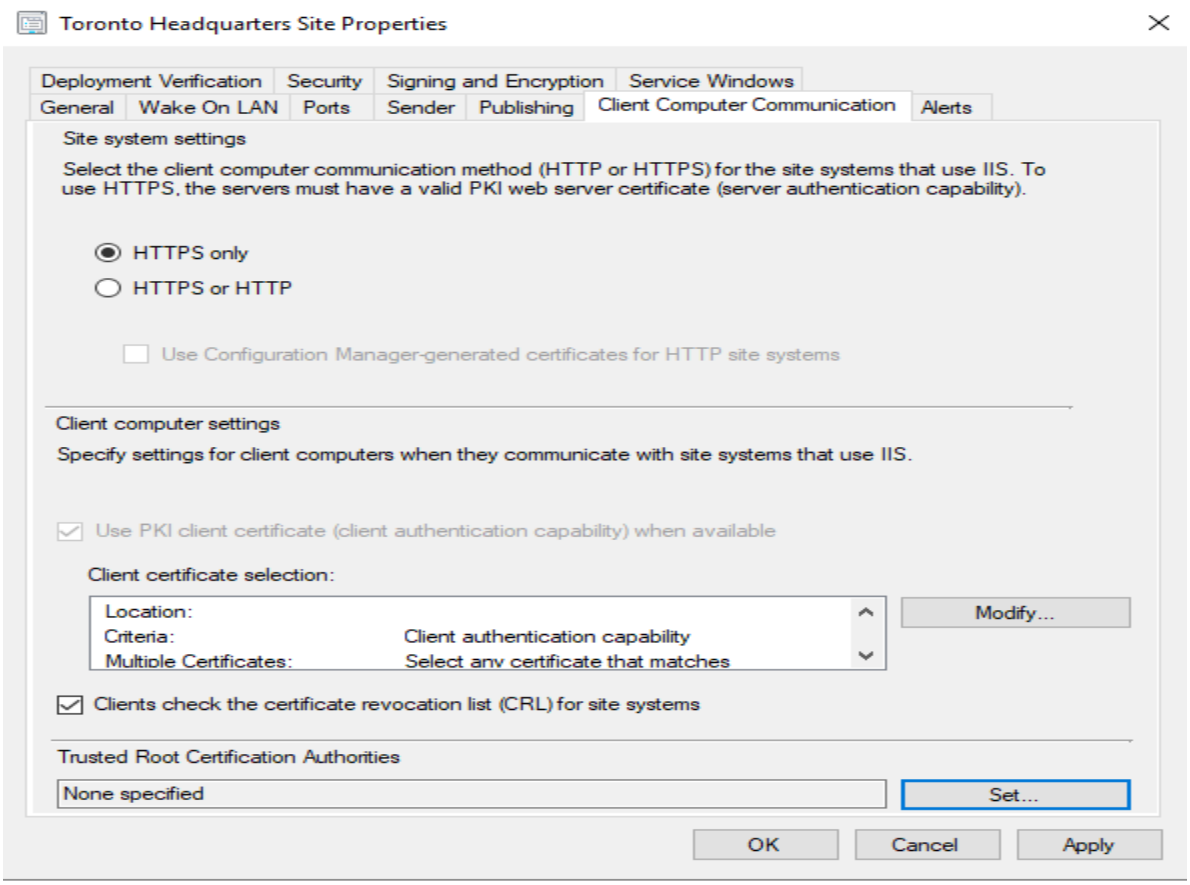
After reinstalling the roles, I am able to select HTTPS.

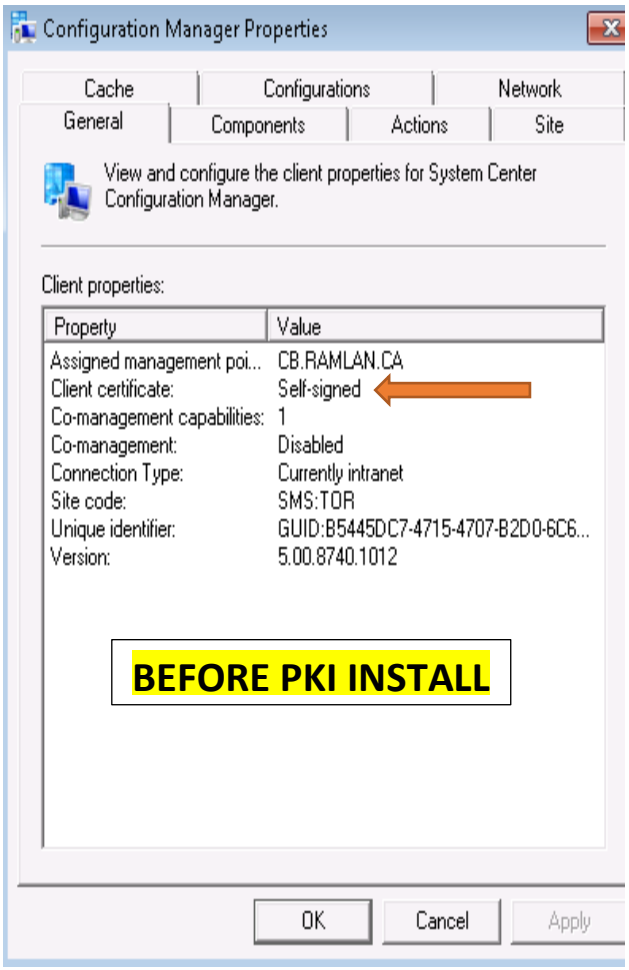


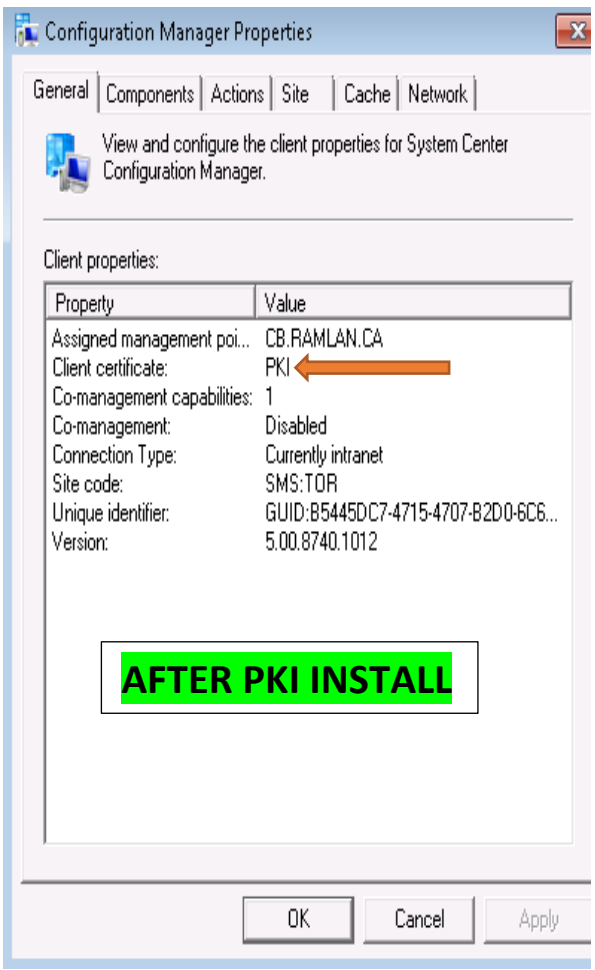


In the Configuration Manger console, navigate to Administration > Overview > Site Configuration > Sites. Right click on the site server and click Properties. Under site system settings, choose HTTPS only and click OK









This concludes the PKI setup for Current Branch 1810.

Thanks

Ram Lan
19th Jan 2019