The objective of this lab is to manage a Certificate Authority (CA) Server in an Active Directory (AD) domain by issuing and managing certificates for various purposes.

Lab Assignment 3 (Part II) – Managing a Certificate Authority Server

Monica Perez

Table of Contents

Lab Assignment 3 (Part II) – Managing a Certificate Authority Server

1 Lab Objective

The objective of this lab is to manage a Certificate Authority (CA) Server in an Active Directory (AD) domain by issuing and managing certificates for various purposes.

You will configure certificate templates, enable automatic enrollment, and use certificates for securing documents and internal web servers.

By the end of this lab, you will:

- Issue and manage User Certificates for authentication and encryption.
- Enable Automatic Certificate Enrollment for users and computers in the domain.
- Issue certificates to digitally sign documents and files.
- Secure internal web servers with SSL/TLS certificates for encrypted communications.

2 Lab Environment Requirements

- **Enterprise CA and Domain Controller (DC101)** – Active Directory integrated Certificate Authority
- **Client1** – To test certificate issuance.

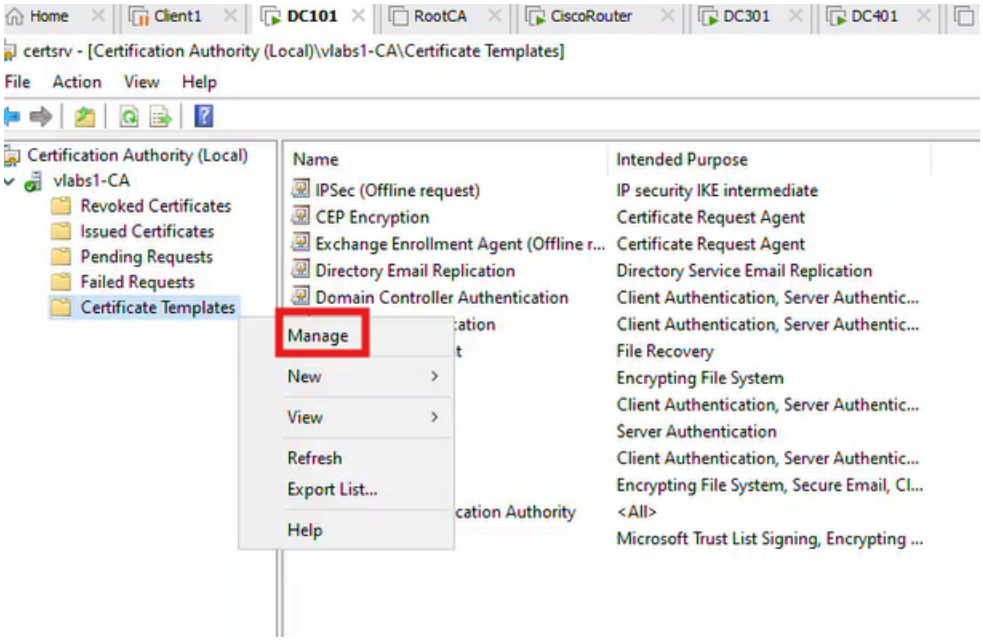
3 Task 1: Issue User Certificates in an AD Domain

3.1 Configure and publish User Certificates from Enterprise CA

1. **Log in to DC101** with an account that has Enterprise Admin or CA Administrator privileges.

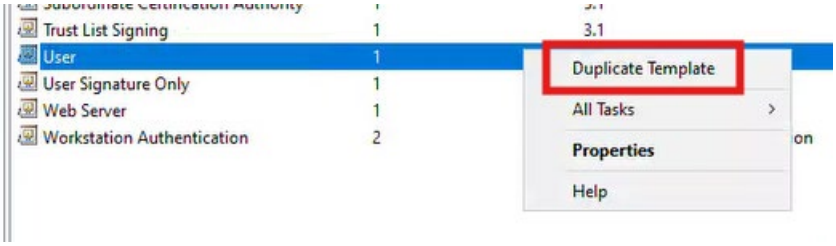
2. **Open Certification Authority Console:**
- Go to Server Manager.
- Click on Tools and then select Certification Authority.

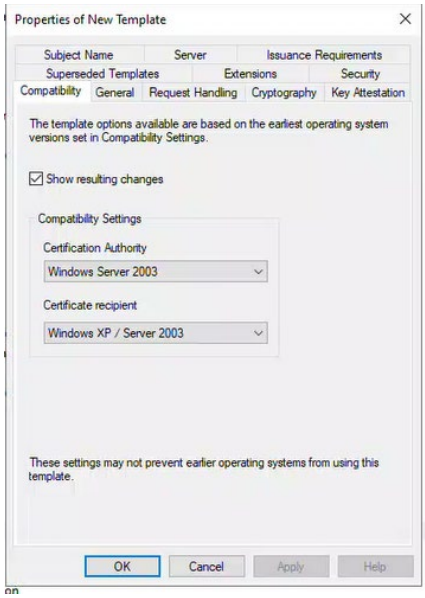
3. **Manage Certificate Templates:**
- In the Certification Authority console, expand your CA name.
- Right-click on Certificate Templates and select Manage. This will open the Certificate Templates Console.



4. **Duplicate the User Template:**

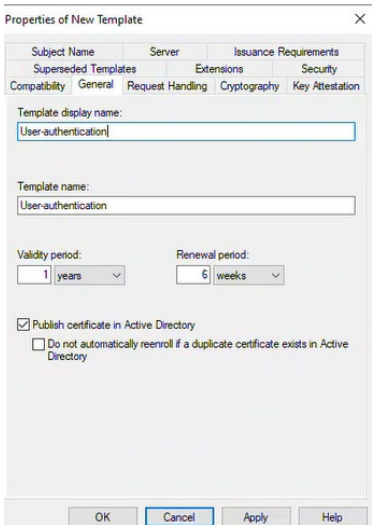
- In the Certificate Templates Console, locate the User template.
- Right-click on User and select Duplicate Template.



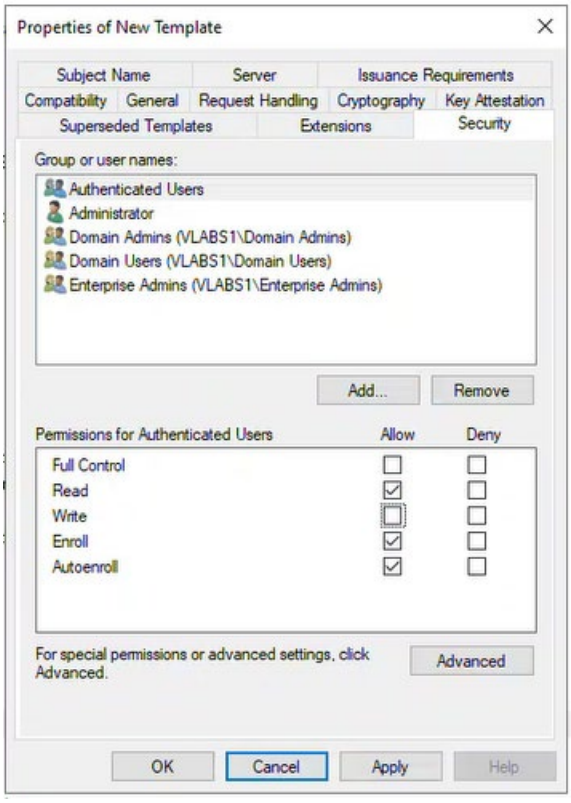


5. **Configure the New User Template:**

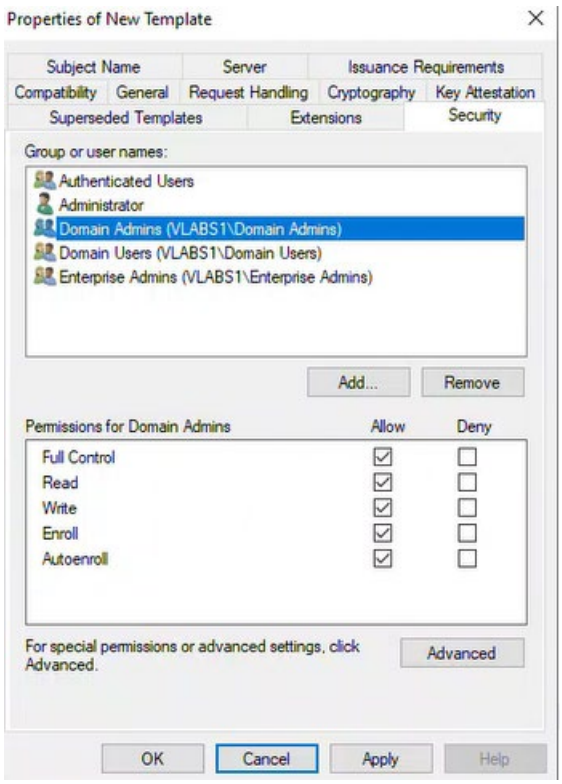
- **General Tab:**
    - Give it a descriptive Template display name.
    - Set the Validity period.

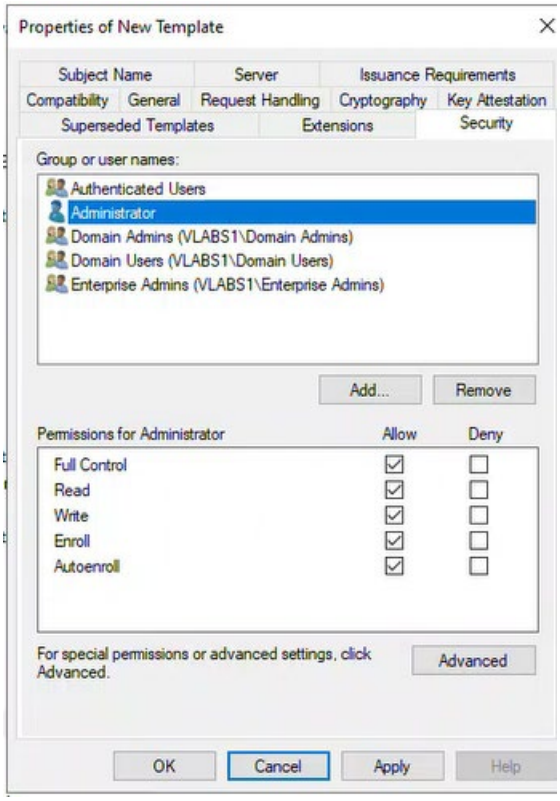


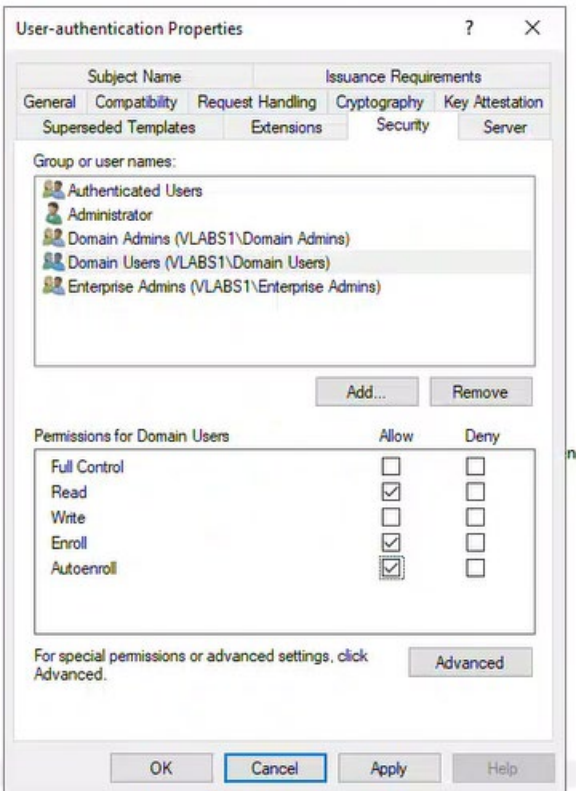
    - Verify that Domain Users have Read and Enroll permissions. If you want specific users or groups to be able to request this certificate, add them and grant Enroll permission.



- Ensure Domain Admins (or your administrative account) also has Full Control so you can manage the template.

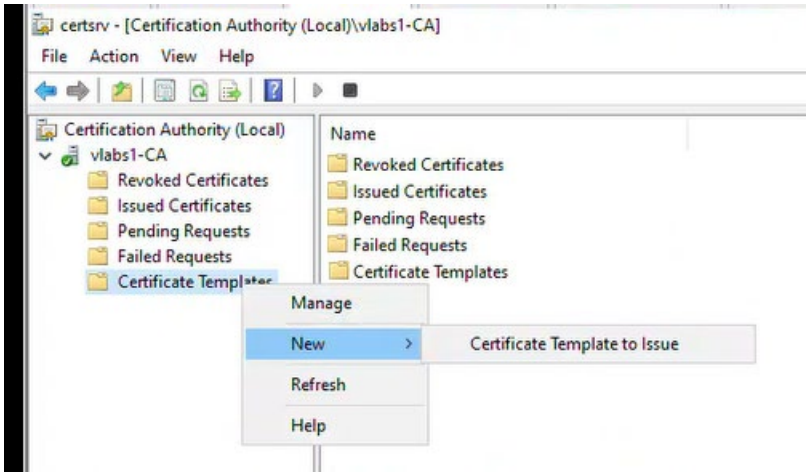




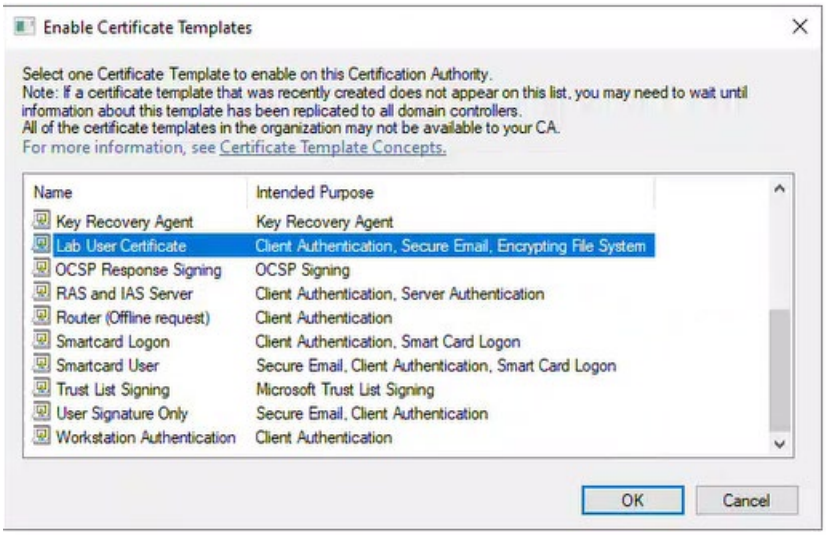


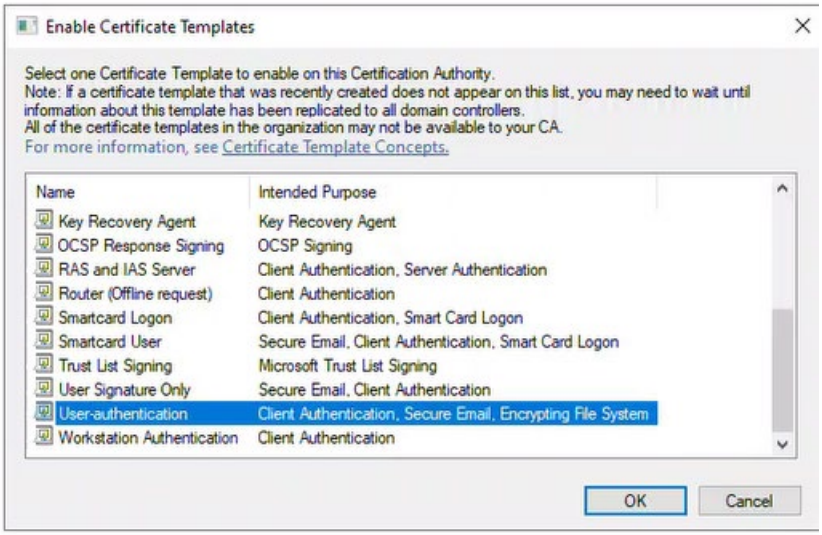
6. **Issue the New Certificate Template from the CA:**

- Back in the Certification Authority console (on DC101), right-click on Certificate Templates.
- Select New -> Certificate Template to Issue.

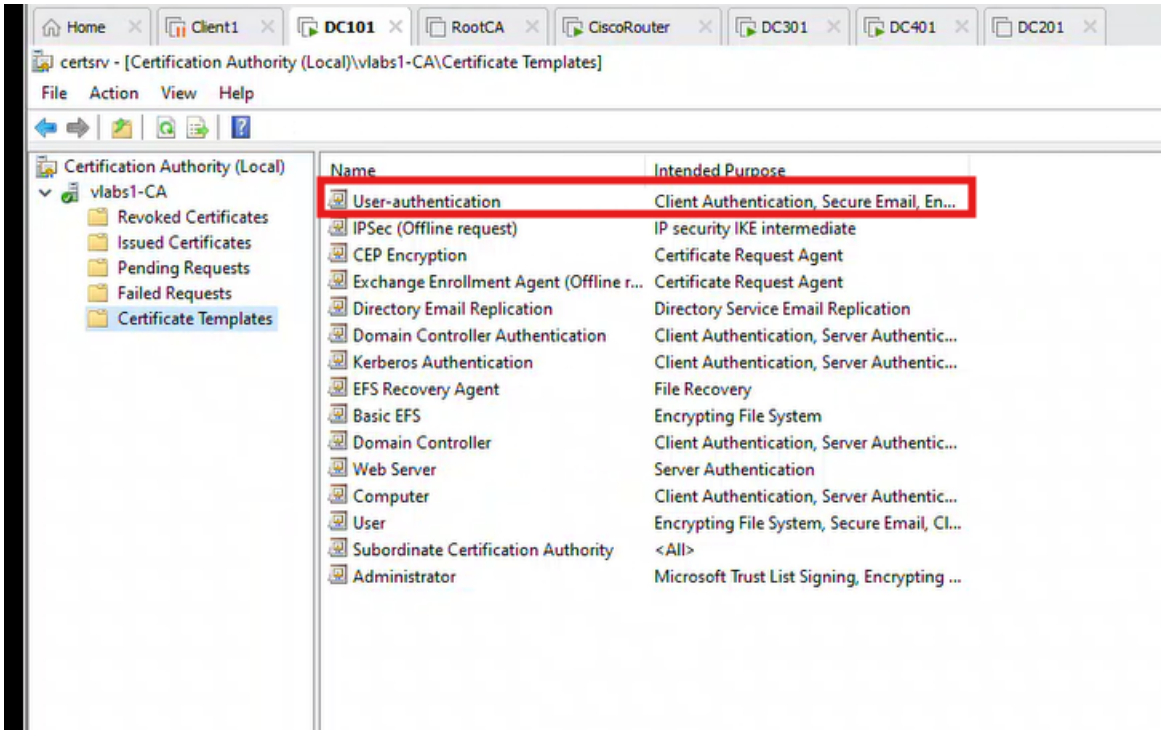


- From the list, select the new template you just created and click OK.



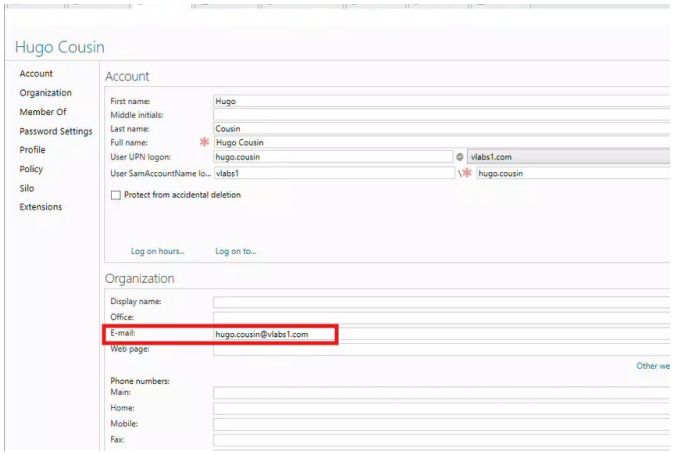


- The new template should now appear under Certificate Templates in the Certification Authority console.

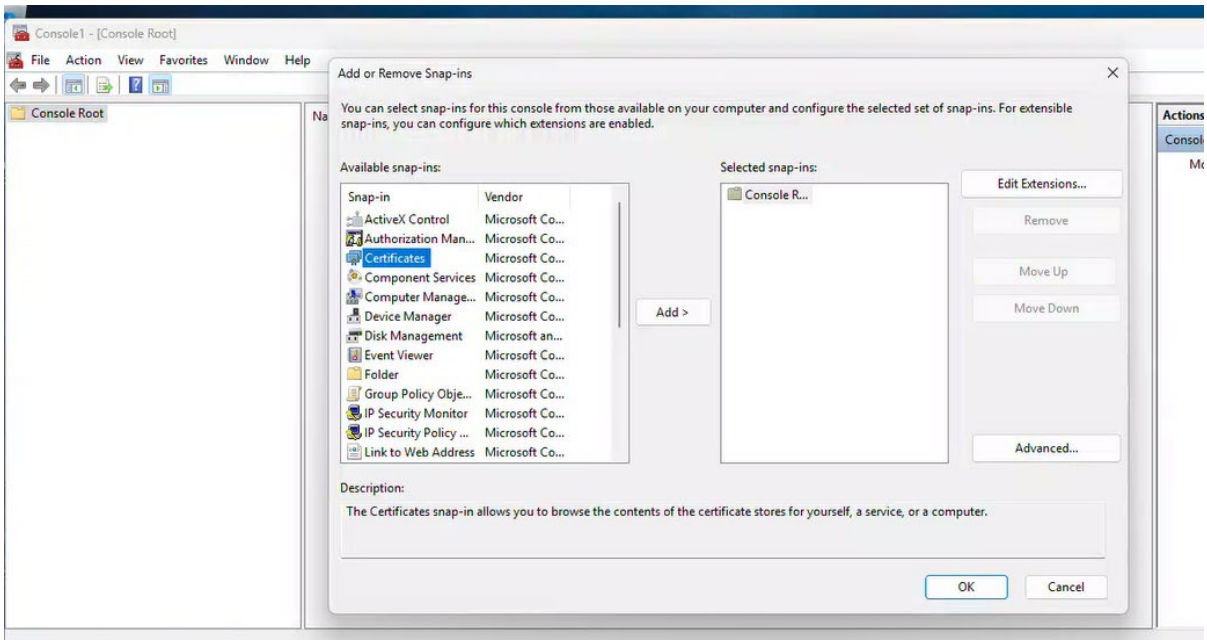


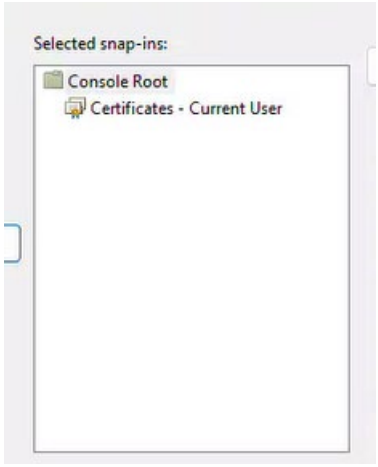
3.2 Open a session on Client1 with a user that has an email address and manually requests a user certificate.

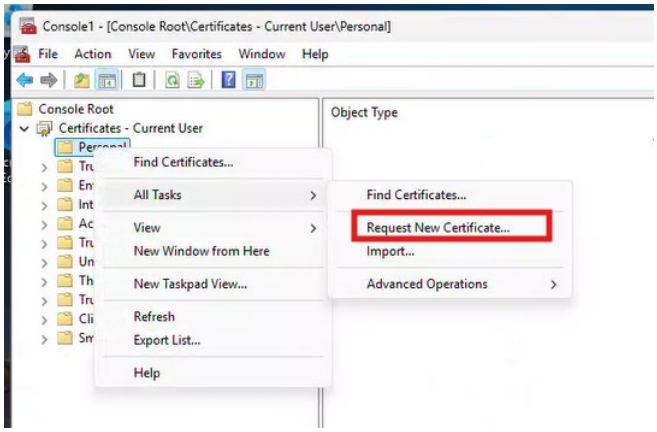
1. Open a session on ClientX using a user account that has an email address assigned to it.
2. Verify in DC101 that user has email

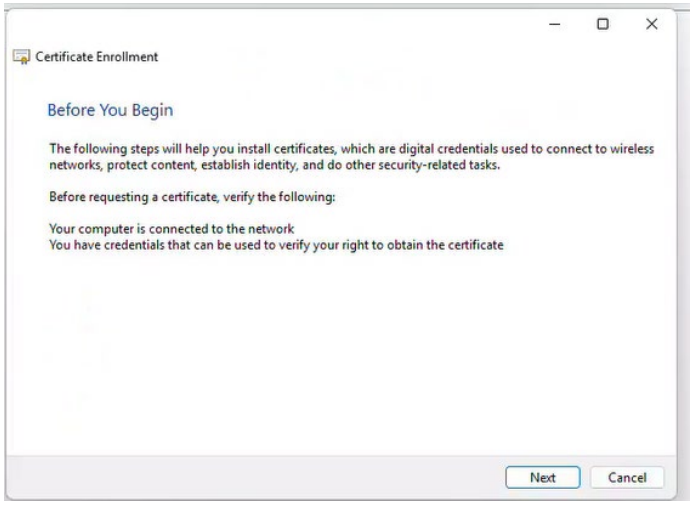


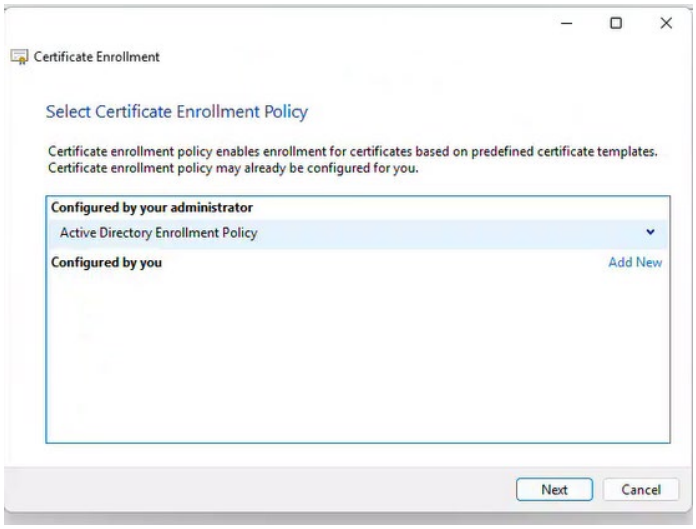
3. Open the Run dialog (Win + R), type mmc, and press Enter.
4. Click File → Add/Remove Snap-in.
5. Select Certificates → Add → My user account → Finish → OK.
6. Expand Certificates - Current User → Right-click Personal → All Tasks → Request New Certificate.
7. Click Next, select the Active Directory Enrollment Policy, then click Next again.
8. Select the newly published User Certificate Template, click Enroll, then Finish.

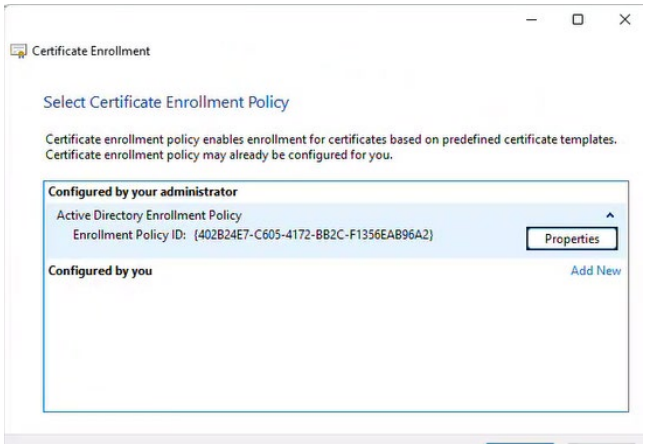


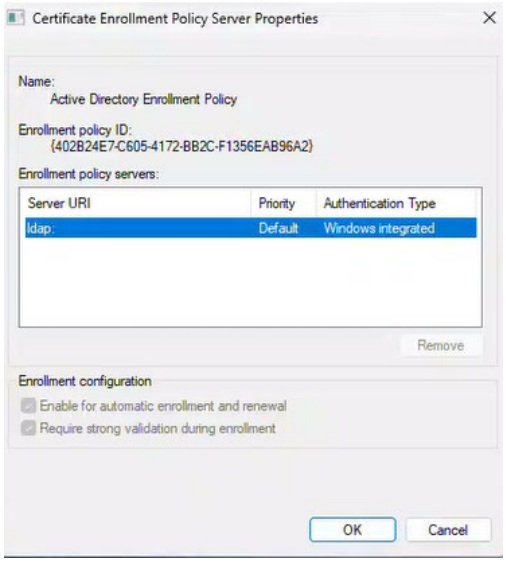

Selected snap-ins:
Console Root
Certificates - Current User

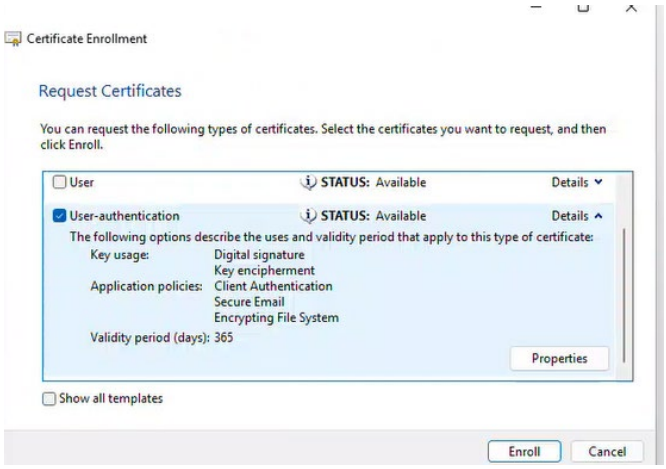

Console1 - [Console Root\Certificates - Current User\Personal]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Object Type
Find Certificates...
All Tasks
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help
Find Certificates...
Request New Certificate...
Import...
Advanced Operations

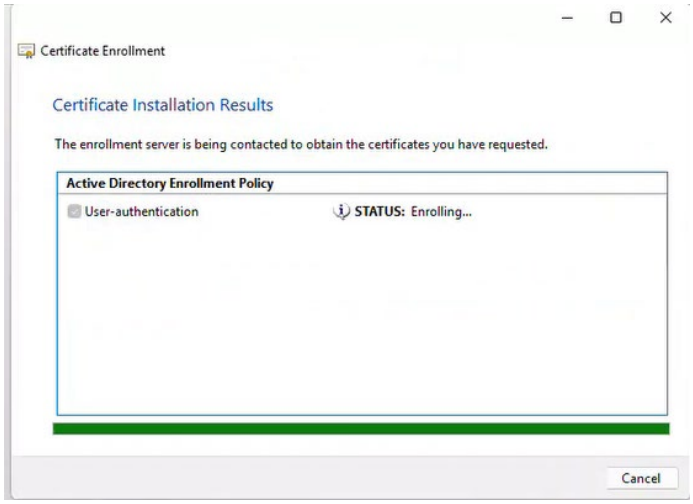

Certificate Enrollment
Before You Begin
The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.
Before requesting a certificate, verify the following:
Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate
Next
Cancel

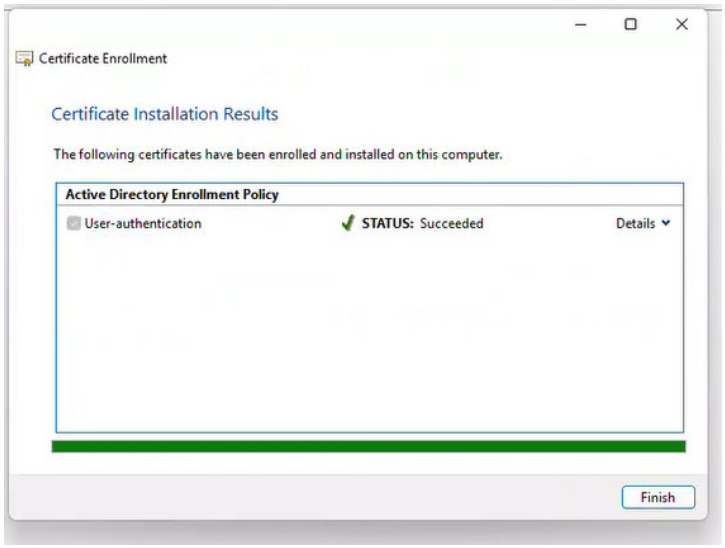

Certificate Enrollment
Select Certificate Enrollment Policy
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates.
Certificate enrollment policy may already be configured for you.
Configured by your administrator
Active Directory Enrollment Policy
Configured by you
Add New
Next
Cancel


Certificate Enrollment
Select Certificate Enrollment Policy
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates.
Certificate enrollment policy may already be configured for you.
Configured by your administrator
Active Directory Enrollment Policy
Enrollment Policy ID: {402B24E7-C605-4172-BB2C-F1356EAB96A2}
Properties
Configured by you
Add New


Certificate Enrollment Policy Server Properties
Name:
Active Directory Enrollment Policy
Enrollment policy ID:
{402B24E7-C605-4172-BB2C-F1356EAB96A2}
Enrollment policy servers:
Server URI
Priority
Authentication Type
ldap:
Default
Windows integrated
Remove
Enrollment configuration
Enable for automatic enrollment and renewal
Require strong validation during enrollment
OK
Cancel

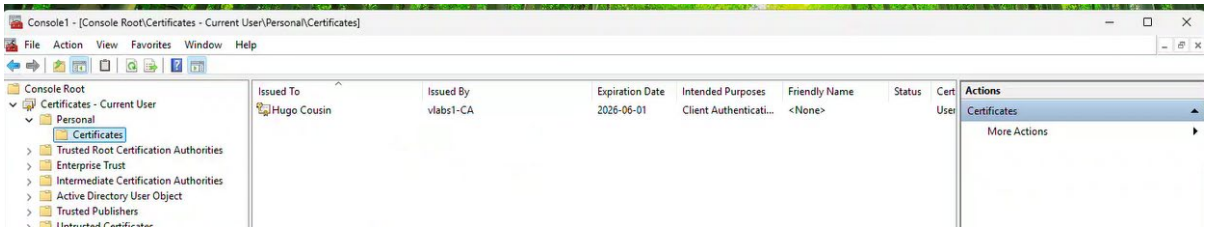

Certificate Enrollment
Request Certificates
You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.
User
STATUS: Available
Details
User-authentication
STATUS: Available
Details
The following options describe the uses and validity period that apply to this type of certificate:
Key usage:
Digital signature
Key encipherment
Application policies:
Client Authentication
Secure Email
Encrypting File System
Validity period (days): 365
Properties
Show all templates
Enroll
Cancel

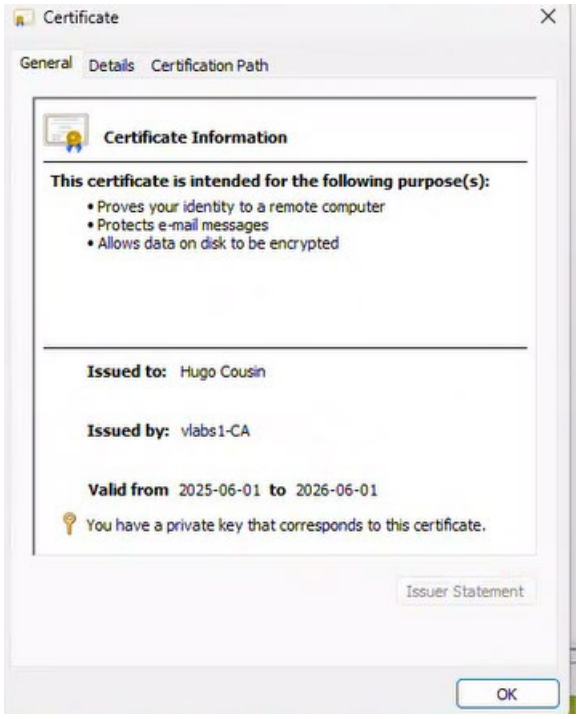


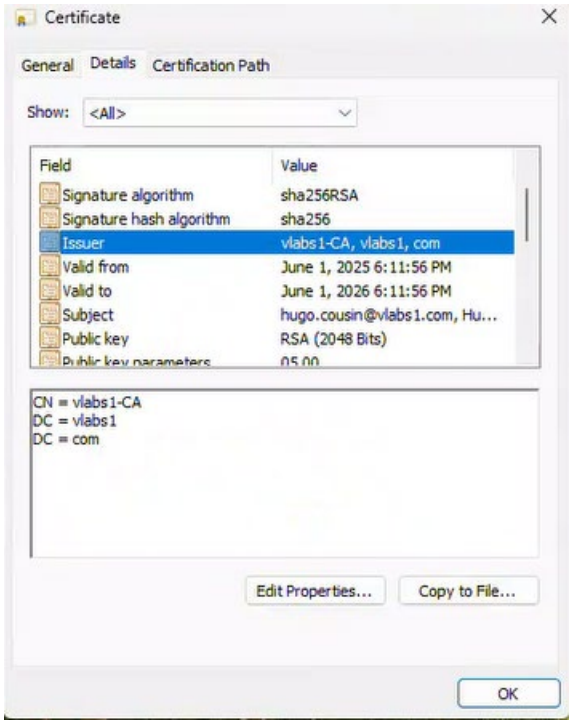


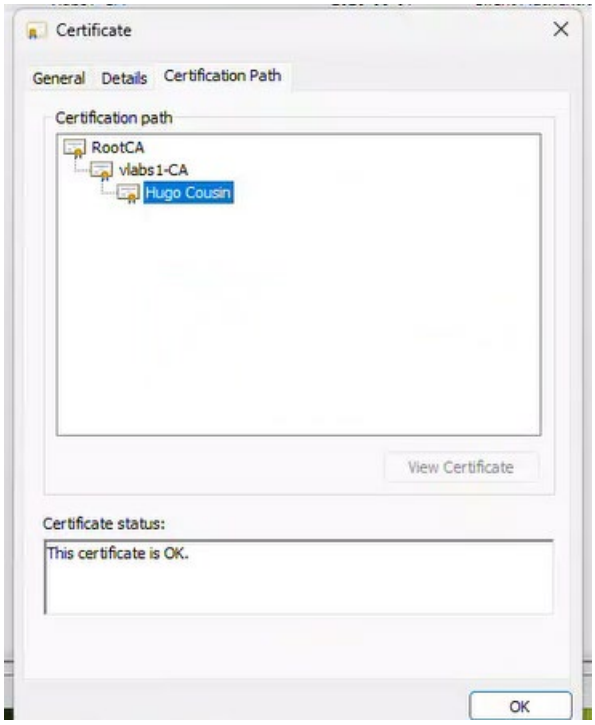
3.3 Verify that the user has obtain a valid certificate on the Client and on his account in the AD.

Navigate to **Personal → Certificates**.
Ensure the issued certificate appears in the list.
Double-click the certificate to verify details like the **Issuer** and **Valid From/To** dates.



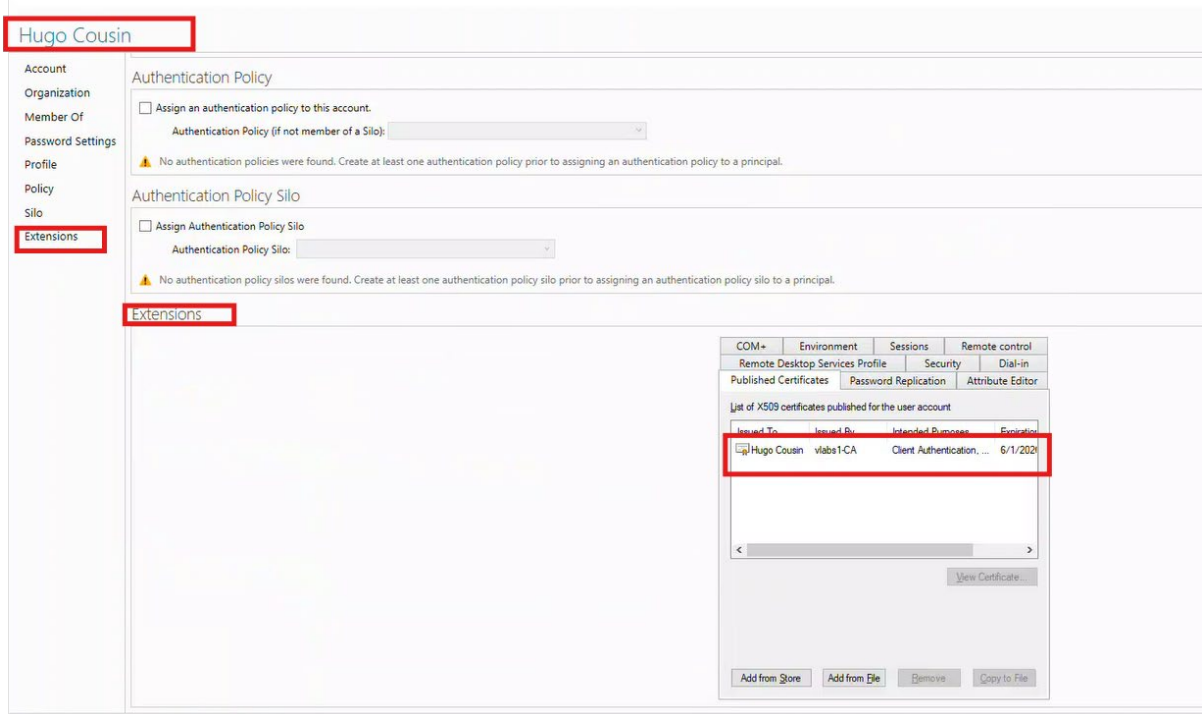

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Protects e-mail messages
• Allows data on disk to be encrypted
Issued to: Hugo Cousin
Issued by: vlabs1-CA
Valid from 2025-06-01 to 2026-06-01
You have a private key that corresponds to this certificate.
Issuer Statement
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
vlabs1-CA, vlabs1, com
Valid from
June 1, 2025 6:11:56 PM
Valid to
June 1, 2026 6:11:56 PM
Subject
hugo.cousin@vlabs1.com, Hu...
Public key
RSA (2048 Bits)
CN = vlabs1-CA
DC = vlabs1
DC = com
Edit Properties...
Copy to File...
OK

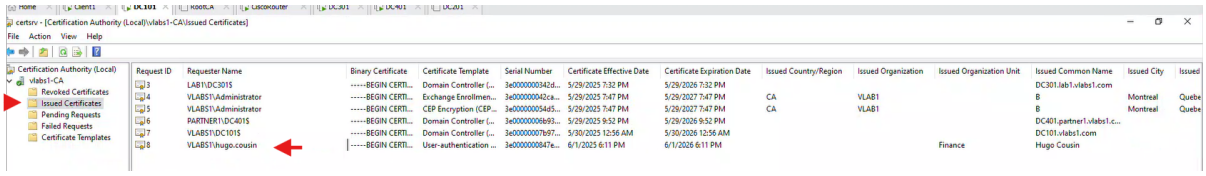


On DC101

See in Active directory the user in section Extensions.
Verify Published Certificates



Verify in Certification authority
See Issued certificates



4 Task 2: Enable Automatic Certificate Enrollment in AD

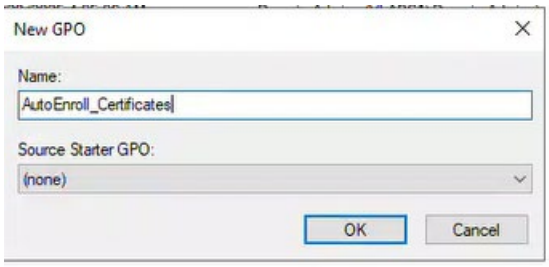
4.1 Configure Group Policy settings to allow automatic certificate enrollment.

1. **Open Group Policy Management (GPMC)**

2. **Create or Edit GPO**

a) Navigate to: **Forest: vlabs1.com** → **Domains** → **vlabs1.com** → **Group Policy Objects**

b) Right-click → **New GPO** (Name: AutoEnroll_Certificates)



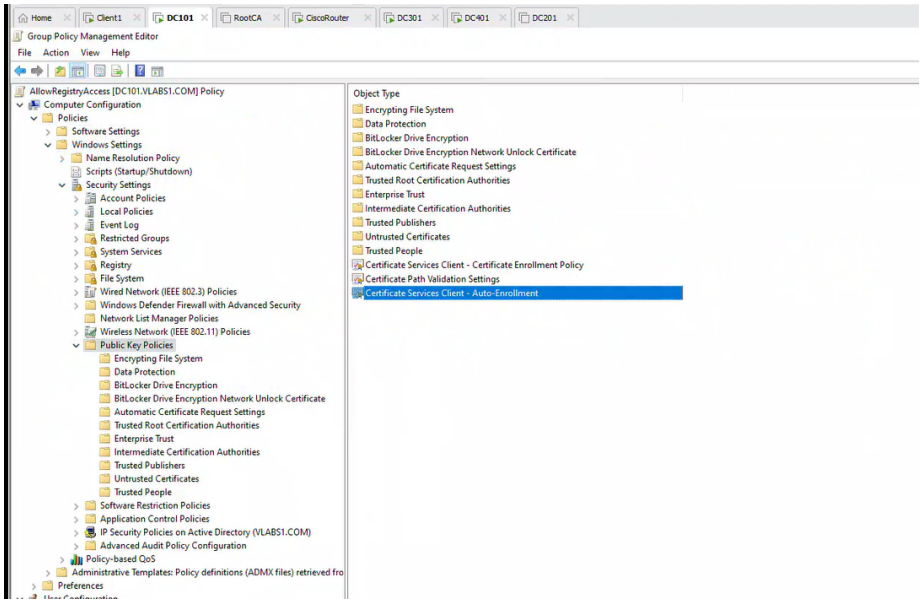
c) Right-click → **Edit**

3. **Navigate to Auto-Enrollment Settings**

a) Go to: **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Public Key Policies**

4. **Enable Automatic Certificate Enrollment**

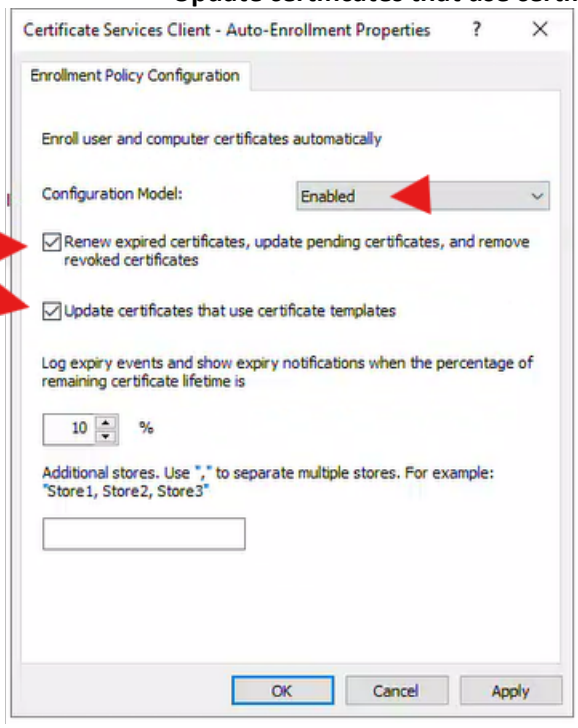
a) Click **Certificate Services Client - Auto-Enrollment**



b) Double click **Configuration Model** . Set to: **Enabled**

c) Check:

- **Renew expired certificates, update pending certificates, and remove revoked certificates**
- **Update certificates that use certificate template**



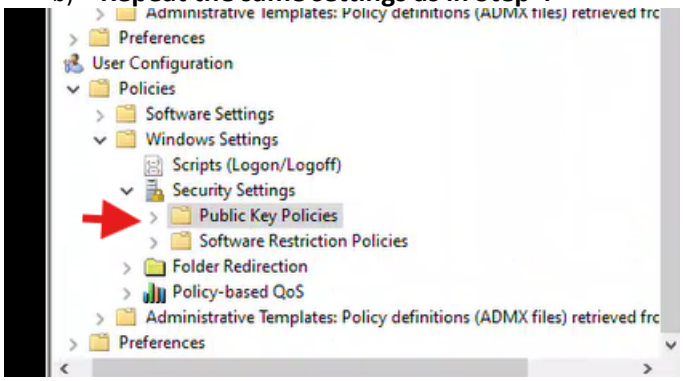
d) Click Apply , then **OK**

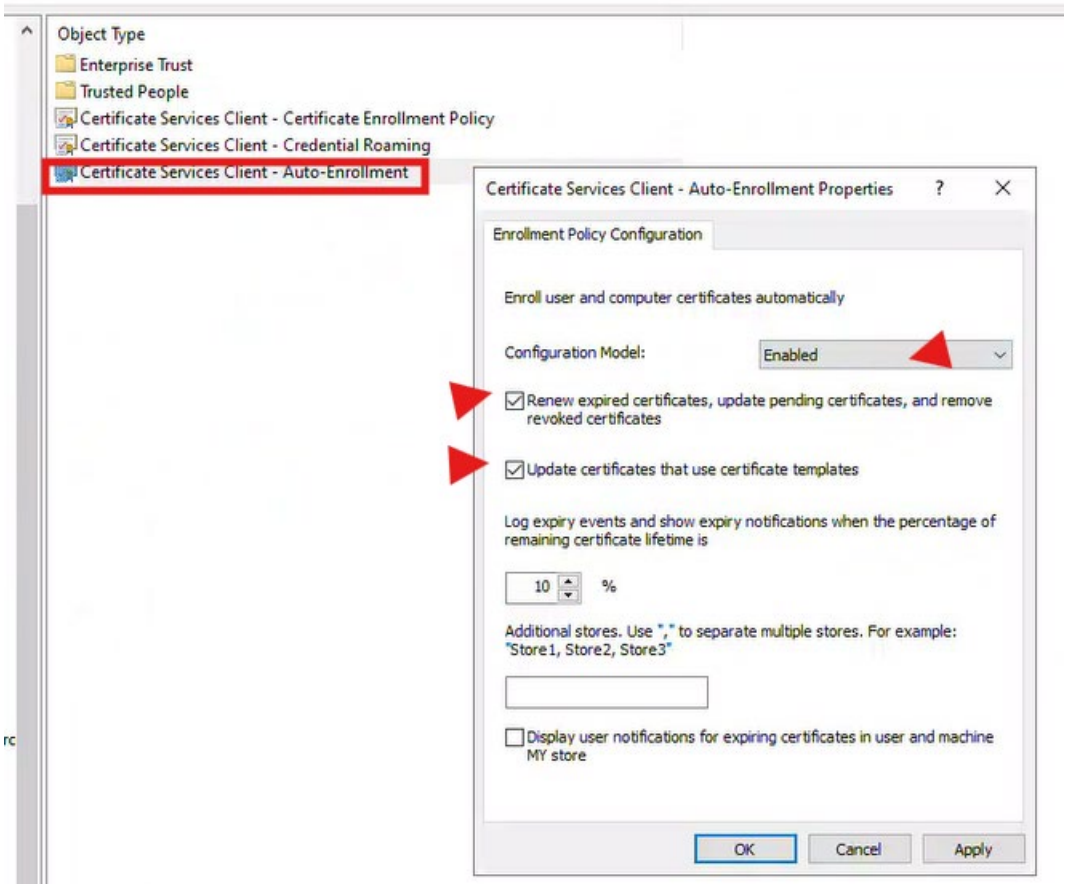
5. Enable certificate Auto-enrollment for users (Optional)

a) Expand : User Configuration -> Policies -> Windows Settings -> Security Settings -> Public

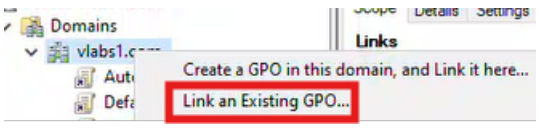
Key Policies

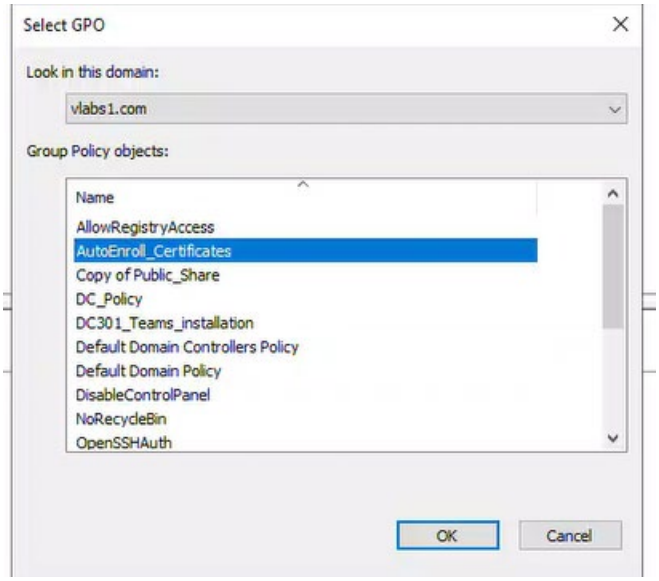
b) **Repeat the same settings as in Step 4**

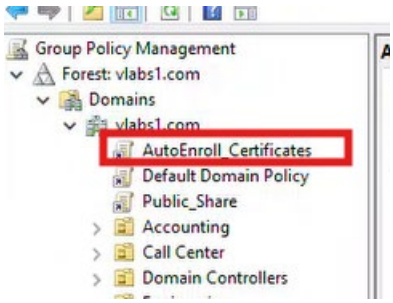


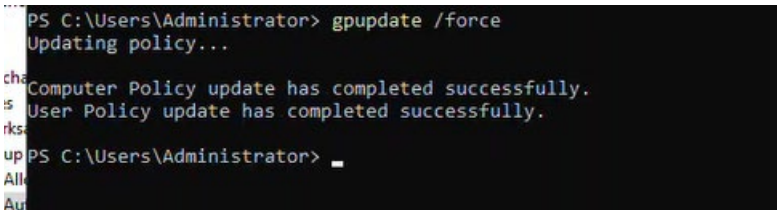


6. **Link GPO to the domain**









4.2 Open a session on Client1 using a different user from task 1, that has an email address. and verify if he has received automatically the necessary certificate.

1. Run this command on client machine

   gpupdate /force

2. Verify auto enrollment

a) Open certificates mmc

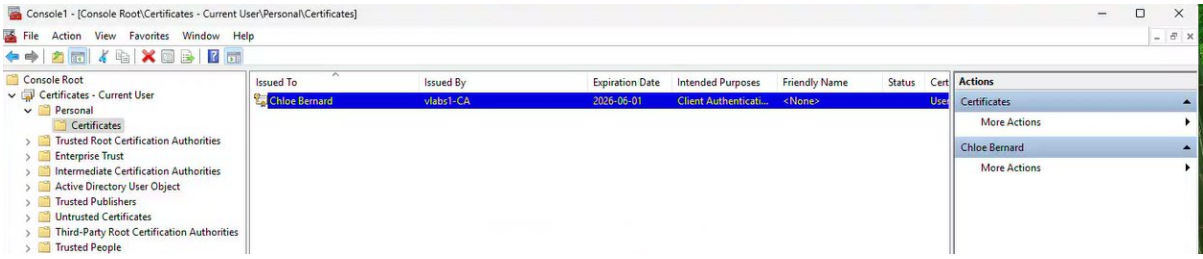
b) Click File -> add/Remove Snap-in

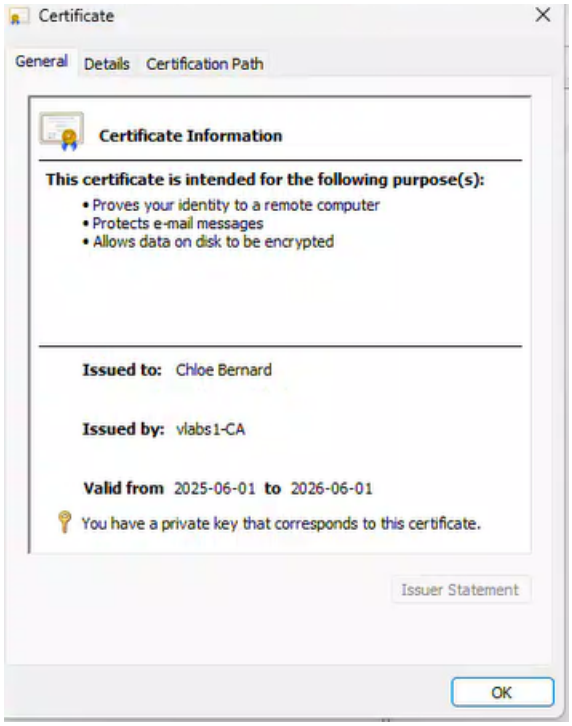
c) Select Certificates -> Add-> My user account -> Finish -> OK

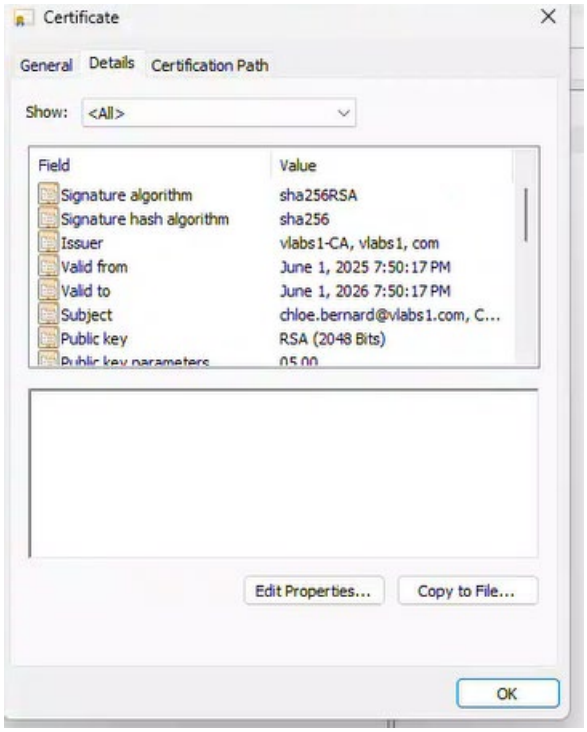
d) Navigate to :

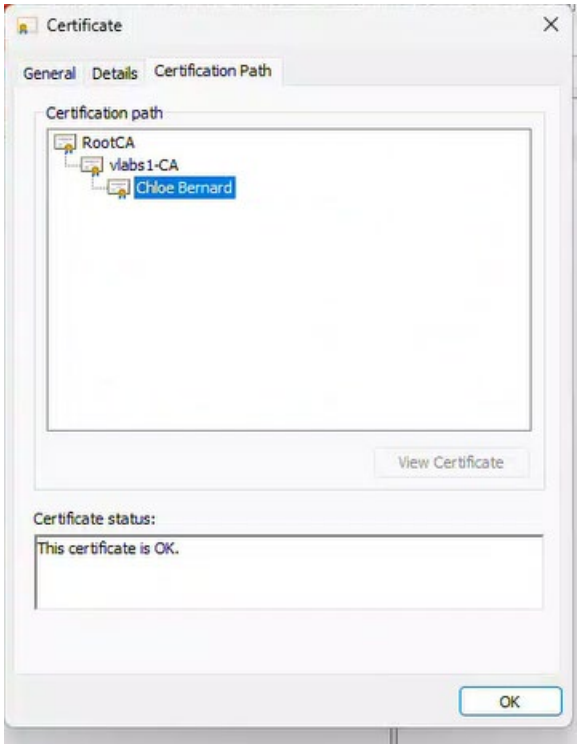
Certificates -> Personal -> Certificate

e) Verify that the newly issued certificates are present.



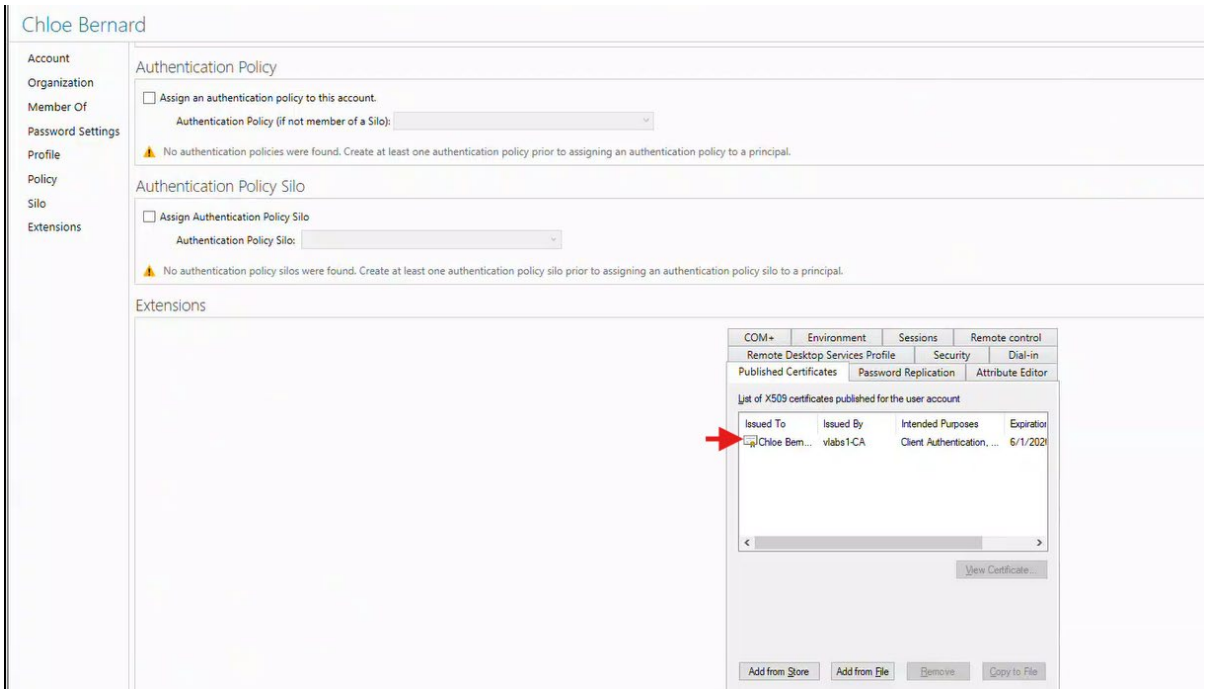


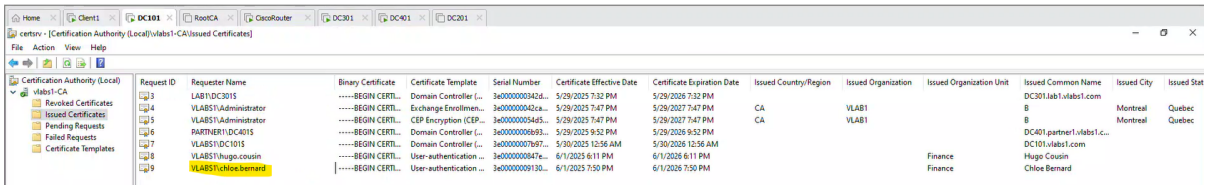




4.3 Check the user account in the AD to verify that he has a valid

certificate.





5 Task 3: Issue Digitally Signed Documents and Files

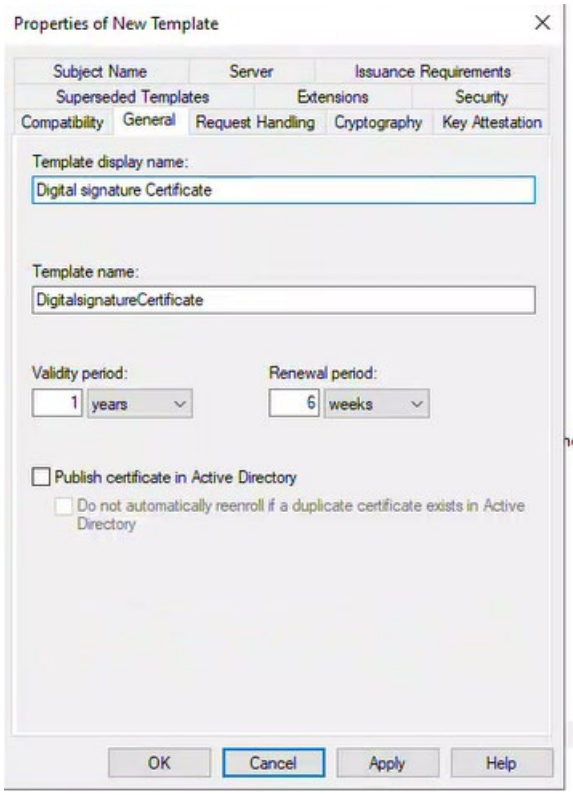
5.1 Issue Digital Signature Certificates from Enterprise CA.

1. **Open Certificate Authority Console** certmpl.msc

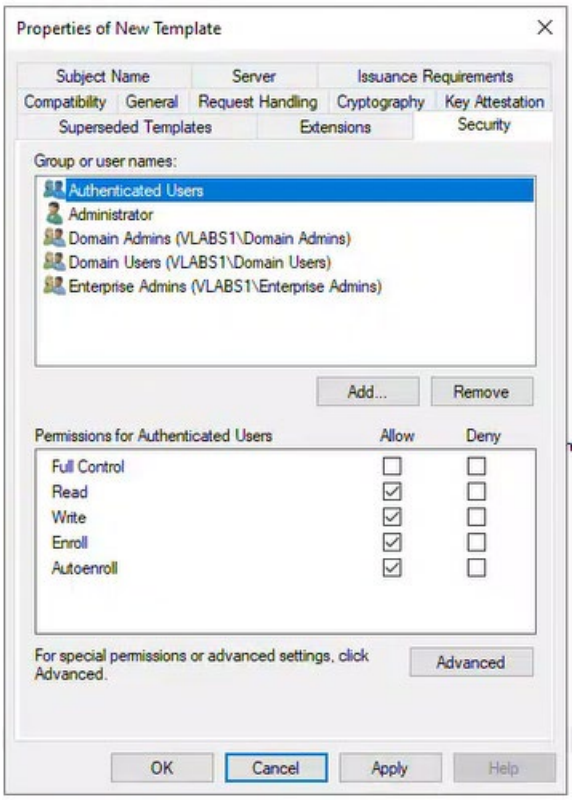
a) Locate the User signature Only template

b) Right-click → **Duplicate Template**

c) Name: **DigitalSignature_Certificate**

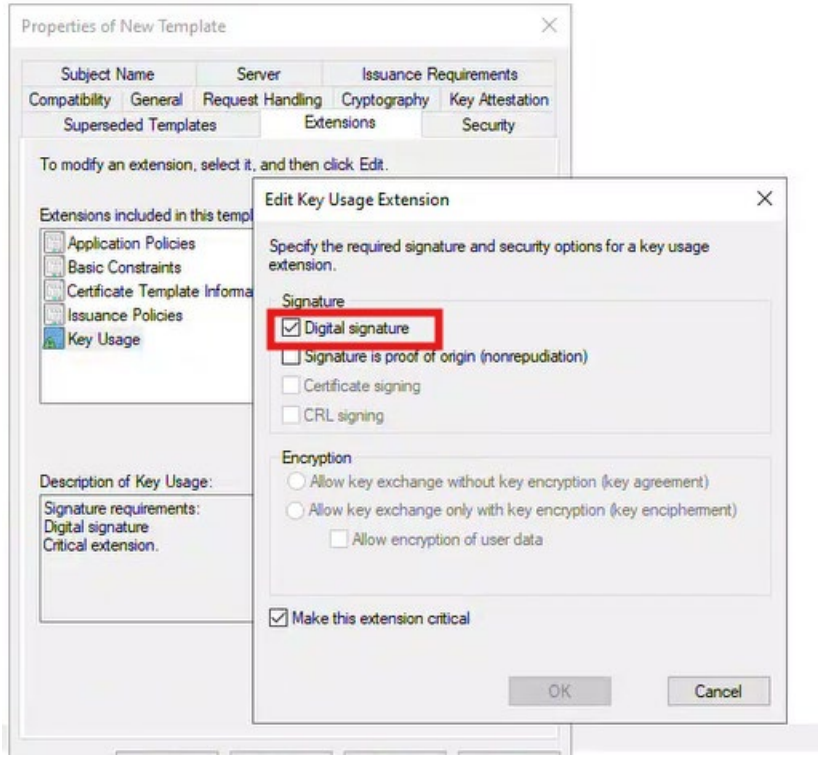


d) Add the authenticated Users Group or specific group
Assign Security -> Read / Enroll autoenroll



e) Enable certificate for digital Signin

Go to Extensions tab
Select Key usage - > Edit
Ensure this options are selected : Digital Signature



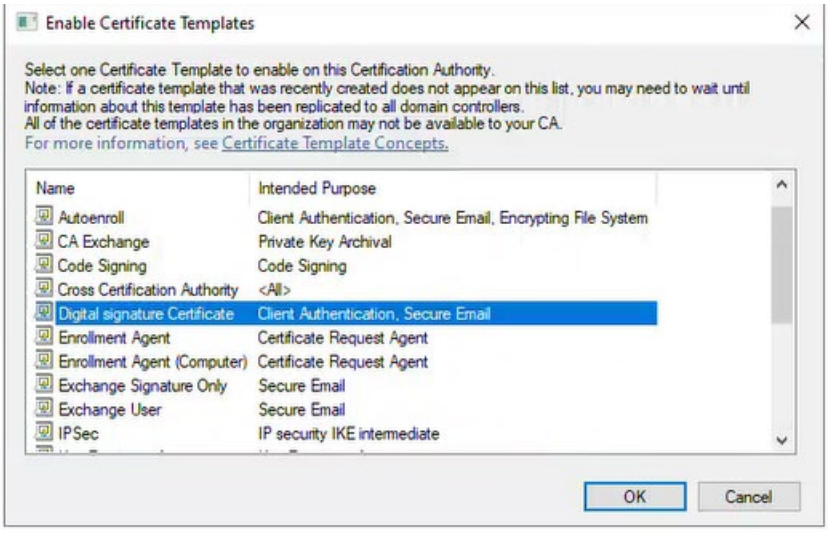
f) Click **OK**

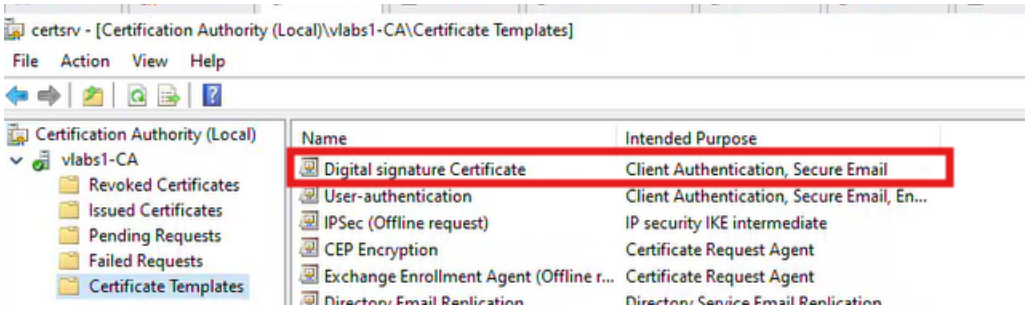
2. **Publish the Template in the CA**

a) **Open Certification Authority**

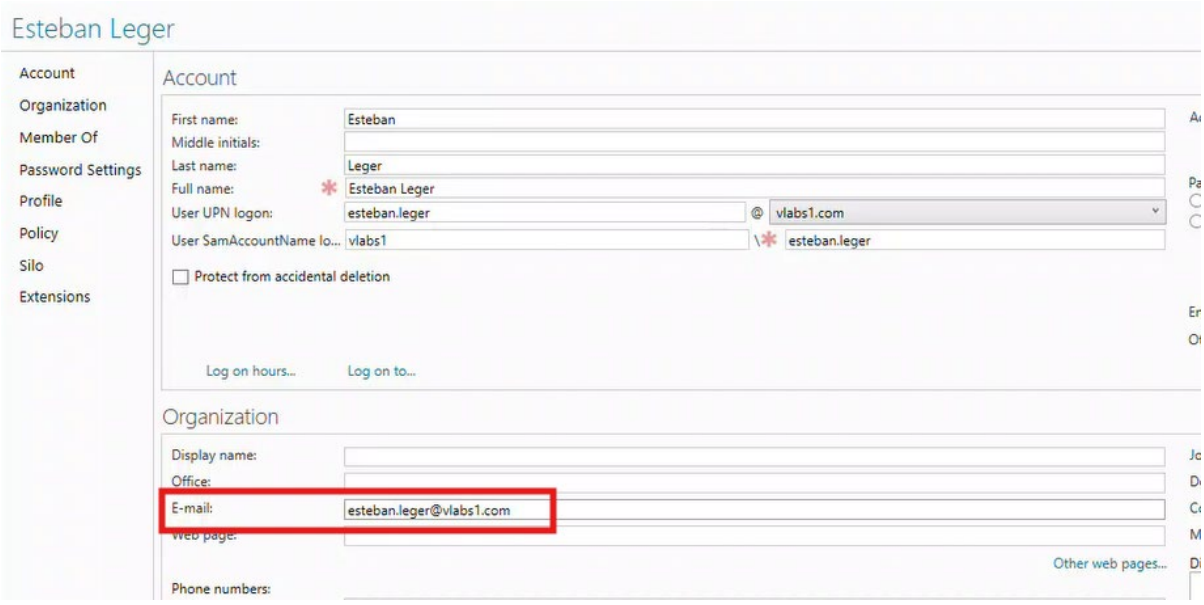
b) Right-click **Certificate Templates → New → Certificate Template to Issue**

c) Select **DigitalSignature_Certificate → OK**





5.2 Open a session on Client1 with a user and manually request a user certificate.



1. Open a session on Client1 using a user account that has an email address assigned to it.

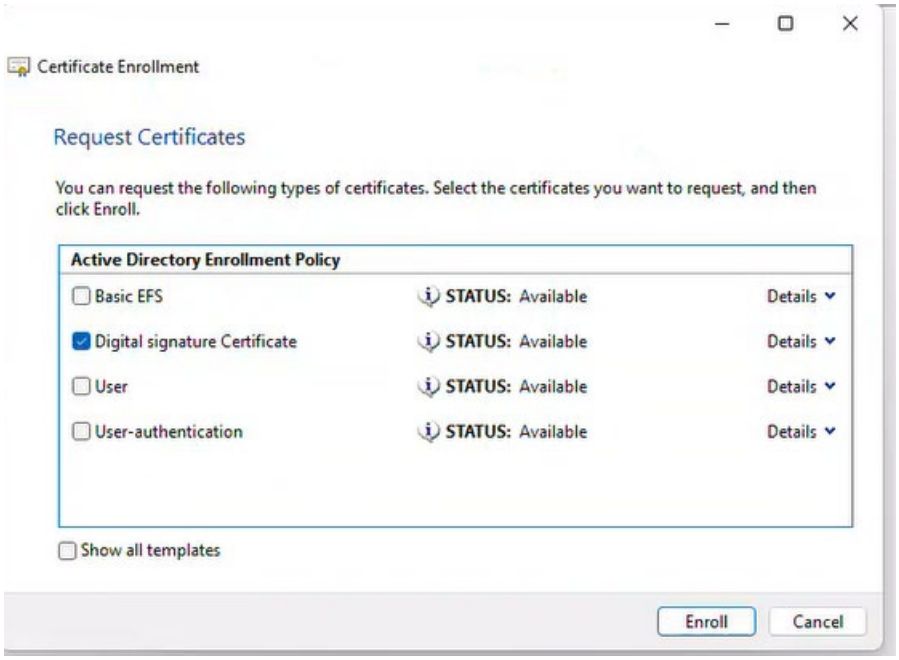
2. Open the Run dialog (Win + R), type mmc, and press Enter.

-3. Click File → Add/Remove Snap-in.

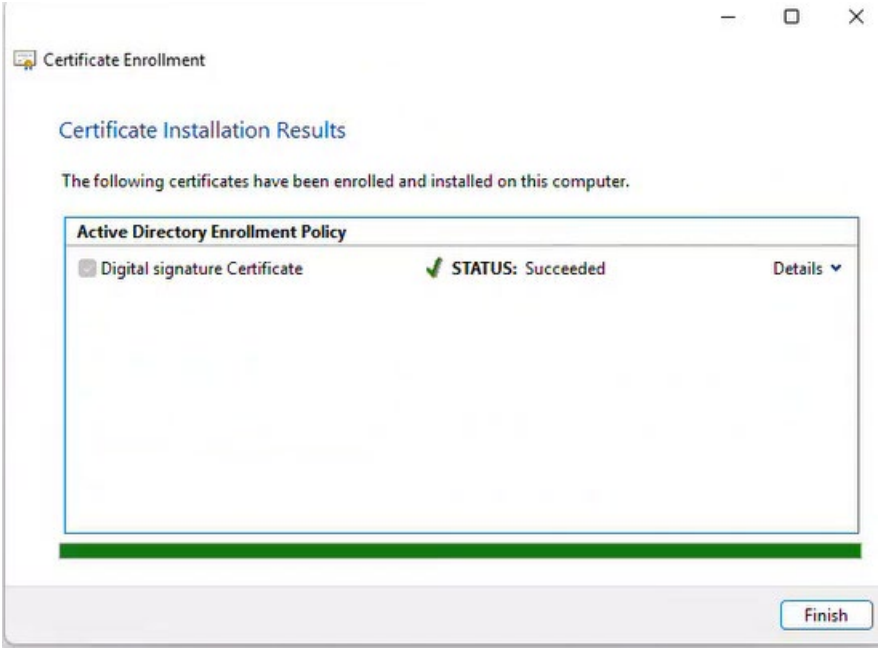
3. Select Certificates → Add → My user account → Finish → OK.

Extracted Text: Step 2: Request a New Certificate

- Expand **Certificates - Current User**, then **Right-click Personal → All Tasks → Request New Certificate**.
- Click **Next**, select **Active Directory Enrollment Policy**, then click **Next** again.
- Select the **Digital Signature Certificate** template.

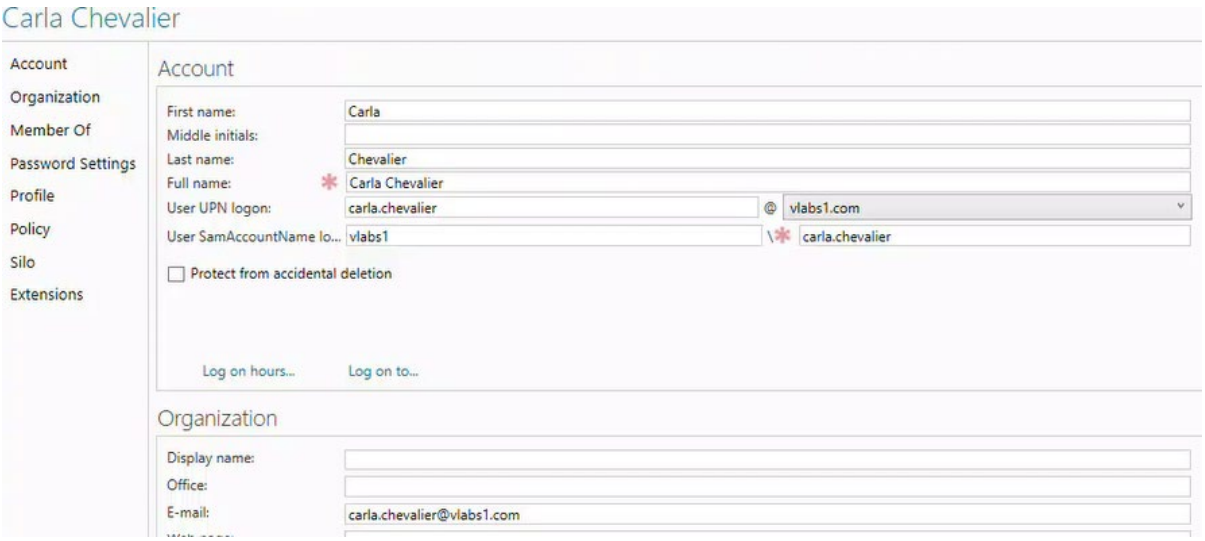


- Click **Enroll**, then **Finish**.



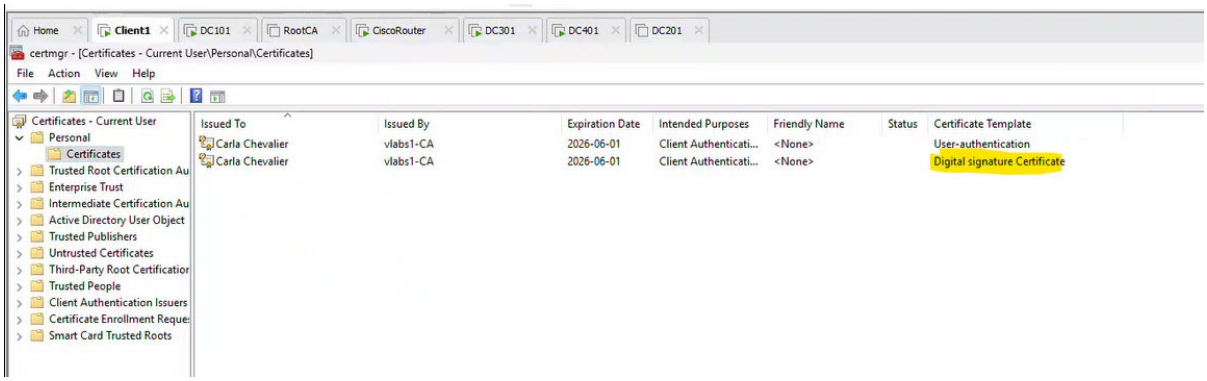
5.3 Verify that he has received this certificate.

Another user



Open client 1

Received automatically via auto enroll

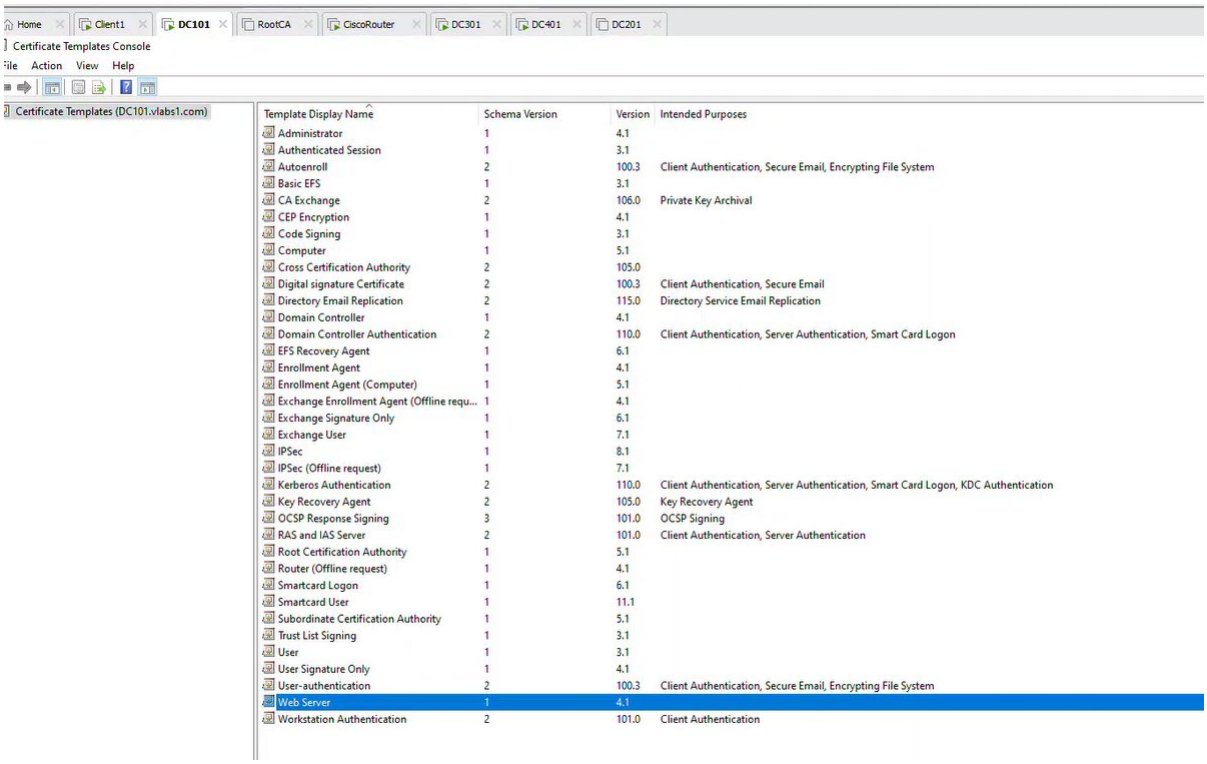


Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration D
3	LAB1\DC301$	-----BEGIN CERTI...	Domain Controller (DomainController)	3e0000000342d...	5/29/2025 7:32 PM	5/29/2026 7:32 PM
4	VLABS1\Administrator	-----BEGIN CERTI...	Exchange Enrollment Agent (Offline request) (EnrollmentAgen...	3e000000042ca...	5/29/2025 7:47 PM	5/29/2027 7:47 PM
5	VLABS1\Administrator	-----BEGIN CERTI...	CEP Encryption (CEPEncryption)	3e000000054d5...	5/29/2025 7:47 PM	5/29/2027 7:47 PM
6	PARTNER1\DC401$	-----BEGIN CERTI...	Domain Controller (DomainController)	3e00000006b93...	5/29/2025 9:52 PM	5/29/2026 9:52 PM
7	VLABS1\DC101$	-----BEGIN CERTI...	Domain Controller (DomainController)	3e00000007b97...	5/30/2025 12:56 AM	5/30/2026 12:56 AM
8	VLABS1\hugo.cousin	-----BEGIN CERTI...	User-authentication (1.3.6.1.4.1.311.21.8.3480757.9425196.8407...	3e0000000847e...	6/1/2025 6:11 PM	6/1/2026 6:11 PM
9	VLABS1\chloe.bernard	-----BEGIN CERTI...	User-authentication (1.3.6.1.4.1.311.21.8.3480757.9425196.8407...	3e00000009130...	6/1/2025 7:50 PM	6/1/2026 7:50 PM
11	VLABS1\chloe.bernard	-----BEGIN CERTI...	Digital signature Certificate (1.3.6.1.4.1.311.21.8.3480757.942519...	3e0000000bad...	6/1/2025 8:46 PM	6/1/2026 8:46 PM
16	VLABS1\esteban.leger	-----BEGIN CERTI...	Digital signature Certificate (1.3.6.1.4.1.311.21.8.3480757.942519...	3e000000109c0...	6/1/2025 8:53 PM	6/1/2026 8:53 PM
17	VLABS1\esteban.leger	-----BEGIN CERTI...	User-authentication (1.3.6.1.4.1.311.21.8.3480757.9425196.8407...	3e00000011163...	6/1/2025 8:55 PM	6/1/2026 8:55 PM
18	VLABS1\carla.chevalier	-----BEGIN CERTI...	Digital signature Certificate (1.3.6.1.4.1.311.21.8.3480757.942519...	3e000000126ee...	6/1/2025 9:00 PM	6/1/2026 9:00 PM
19	VLABS1\carla.chevalier	-----BEGIN CERTI...	User-authentication (1.3.6.1.4.1.311.21.8.3480757.9425196.8407...	3e00000013a5b...	6/1/2025 9:00 PM	6/1/2026 9:00 PM

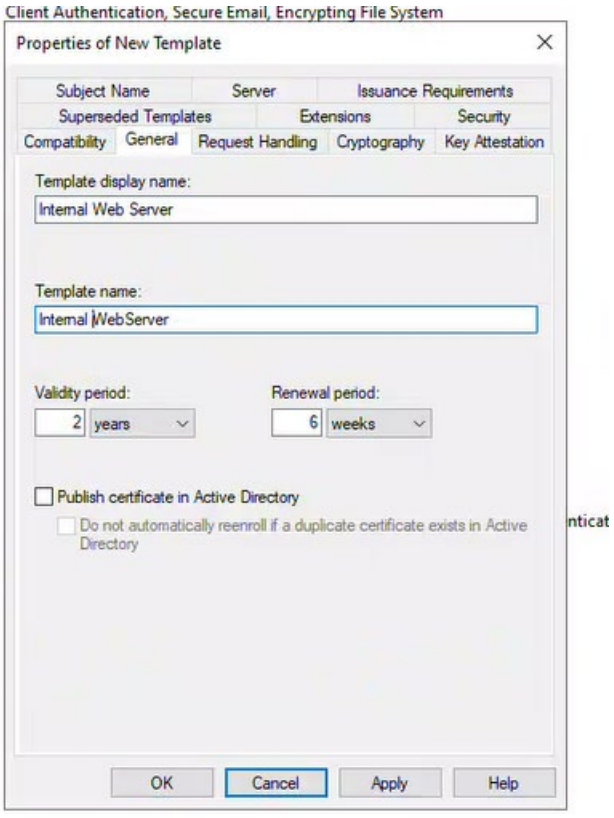
6 Task 4: Secure Internal Web Servers with SSL/TLS Certificates

6.1 Create an SSL certificate on the Enterprise CA.

1. Open Certificate Templates Console
    - Run `certtmpl.msc` on your Enterprise CA.
2. Duplicate an Existing Web Server Template
    - Find Web Server → Right-click → Duplicate Template.
    - Go to the General tab → Set a new Template Display Name (e.g., Internal Web Server).



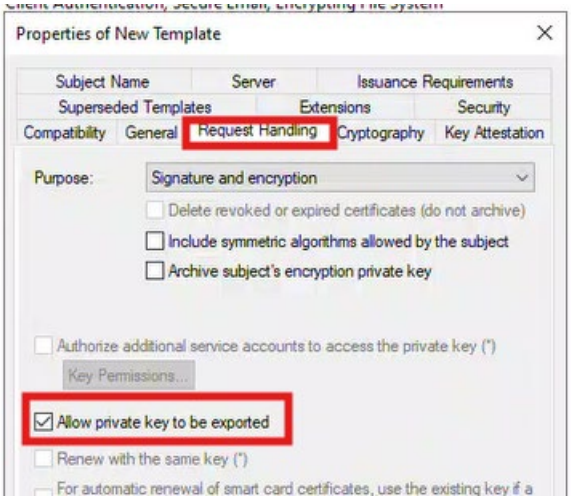
Template Display Name	Schema Version	Version	Intended Purposes
Administrator	1	4.1	
Authenticated Session	1	3.1	
Autoenroll	2	100.3	Client Authentication, Secure Email, Encrypting File System
Basic EFS	1	3.1	
CA Exchange	2	106.0	Private Key Archival
CEP Encryption	1	4.1	
Code Signing	1	3.1	
Computer	1	5.1	
Cross Certification Authority	2	105.0	
Digital signature Certificate	2	100.3	Client Authentication, Secure Email
Directory Email Replication	2	115.0	Directory Service Email Replication
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon
EFS Recovery Agent	1	6.1	
Enrollment Agent	1	4.1	
Enrollment Agent (Computer)	1	5.1	
Exchange Enrollment Agent (Offline requ...	1	4.1	
Exchange Signature Only	1	6.1	
Exchange User	1	7.1	
IPSec	1	8.1	
IPSec (Offline request)	1	7.1	
Kerberos Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon, KDC Authentication
Key Recovery Agent	2	105.0	Key Recovery Agent
OCSP Response Signing	3	101.0	OCSP Signing
RAS and IAS Server	2	101.0	Client Authentication, Server Authentication
Root Certification Authority	1	5.1	
Router (Offline request)	1	4.1	
Smartcard Logon	1	6.1	
Smartcard User	1	11.1	
Subordinate Certification Authority	1	5.1	
Trust List Signing	1	3.1	
User	1	3.1	
User Signature Only	1	4.1	
User-authentication	2	100.3	Client Authentication, Secure Email, Encrypting File System
Web Server	1	4.1	
Workstation Authentication	2	101.0	Client Authentication



nticat

3. Enable Private Key Export

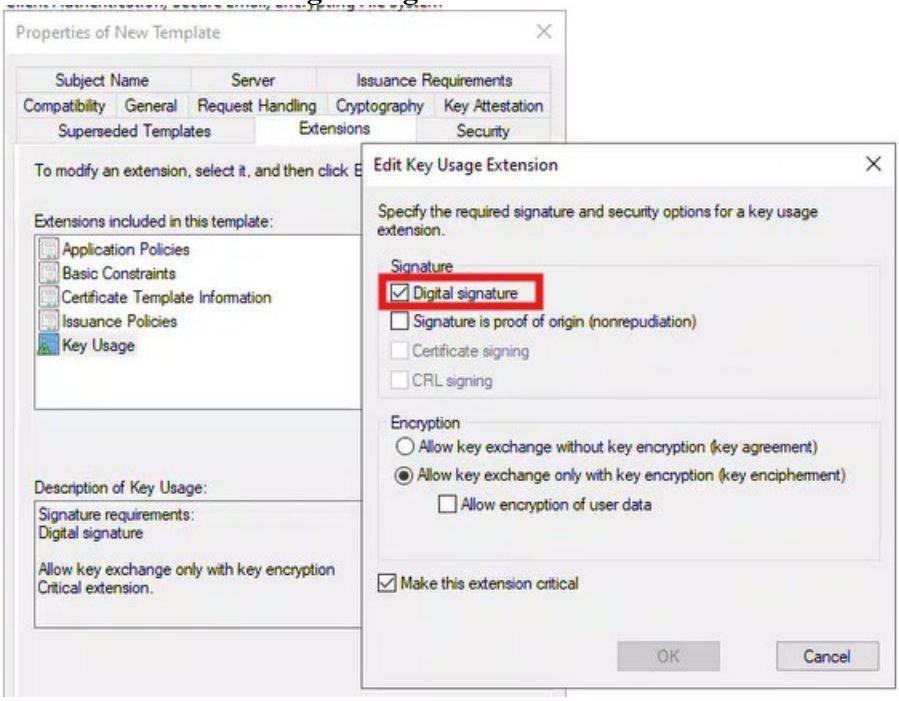
    - Go to Request Handling tab → Check **Allow private key to be exported**.



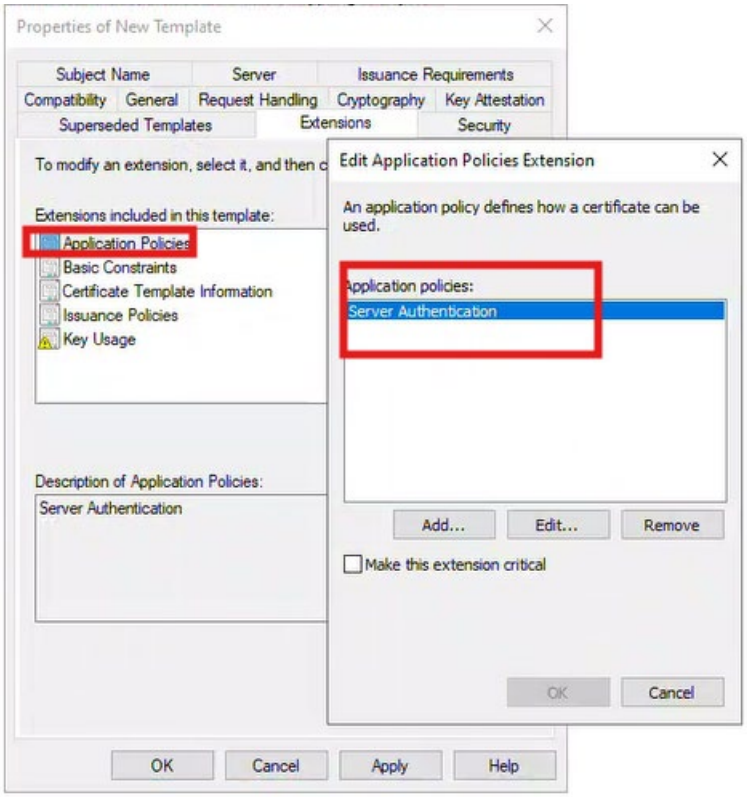
4. Enable Server Authentication Usage

a) Navigate to **Extensions** → Select **Key Usage** → Click **Edit**.

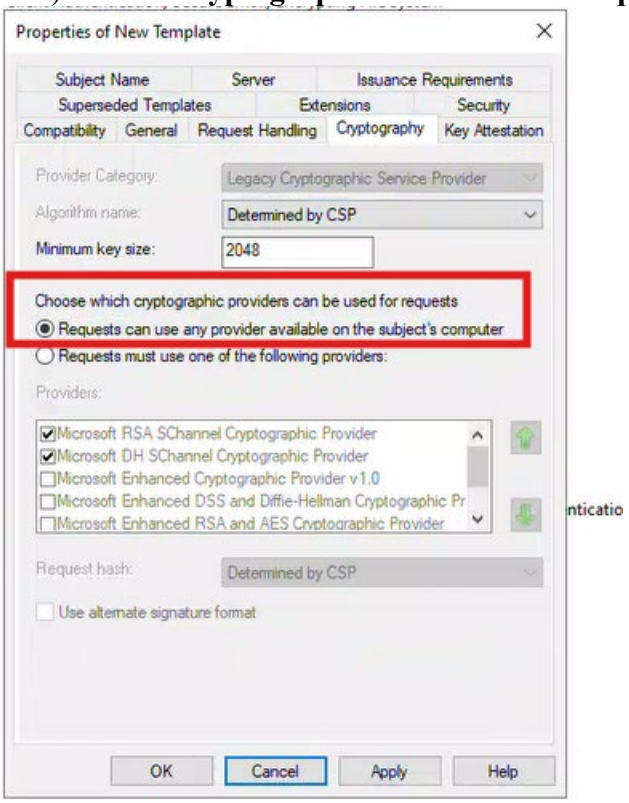
    - Check: **Digital Signature**



b) Select **Application Policies** → Ensure **Server Authentication** is present.



c) Select **Cryptographie and** → Check **Requests can use any provider**.

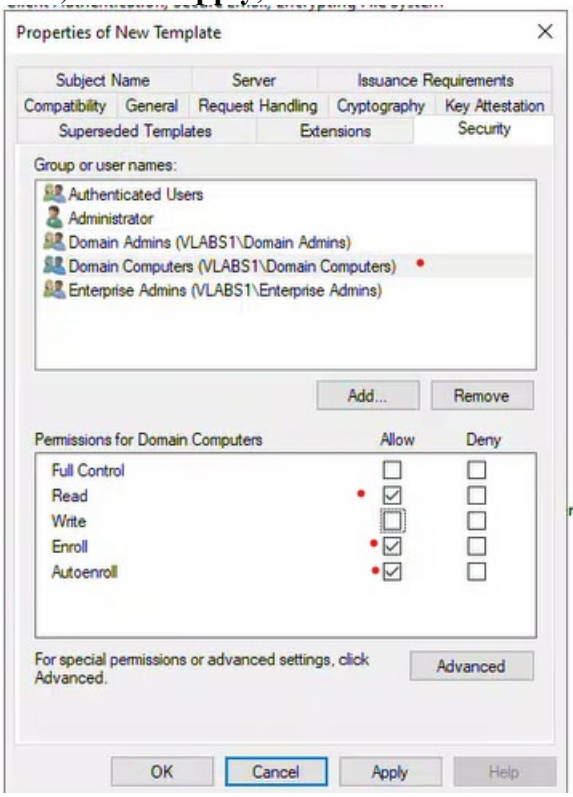


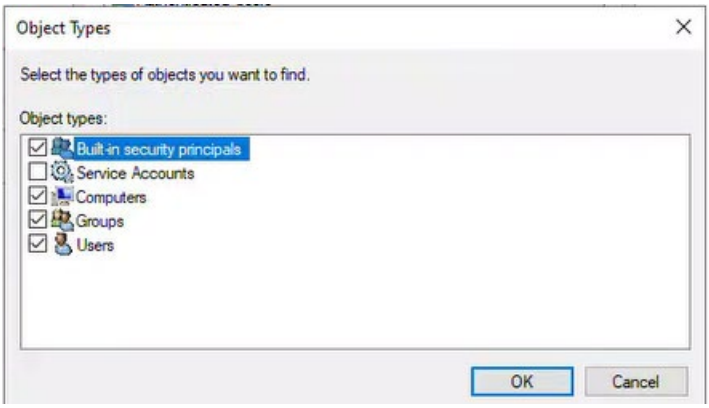
5. Configure Security Permissions

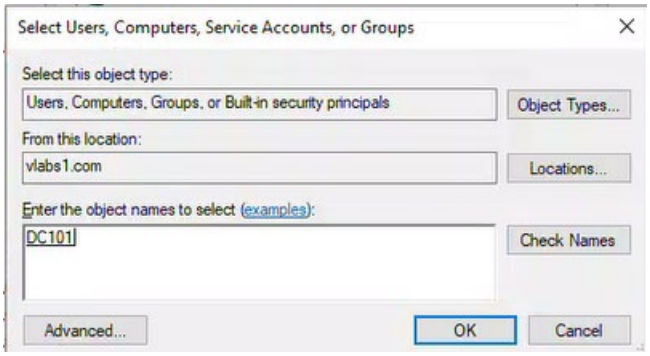
a) Go to the **Security** tab.

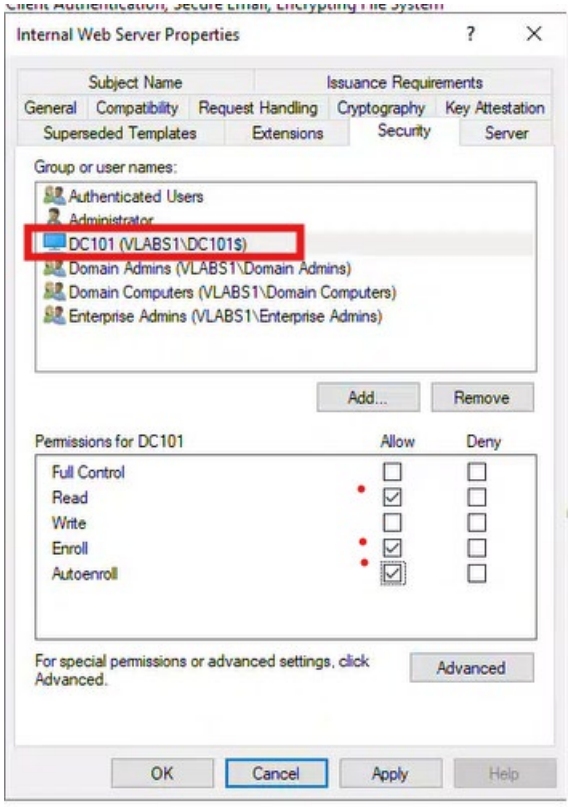
b) Add **Domain Computers** or the specific server (e.g., **DC101$**).
c) Assign:
   - **Read**
   - **Enroll**
   - **Autoenroll** (Optional)

d) Click **Apply**, then **OK**.



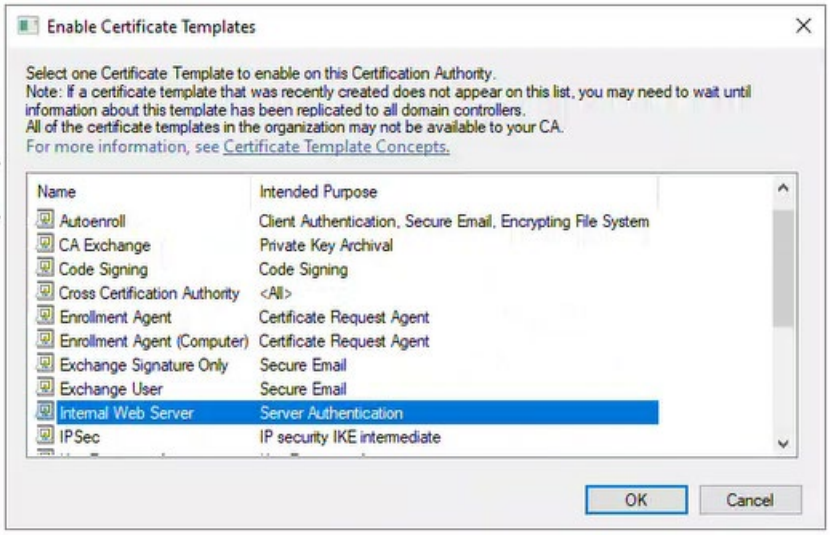






6. Publish the Template

a) Open Certification Authority Console (certsrv.msc).
b) Right-click **Certificate Templates to Issue → New → Certificate Template to issue**
c) Select **Internal Web Server SSL** and click **OK**.
d) Restart the CA service: **Restart-Service** certsvc.

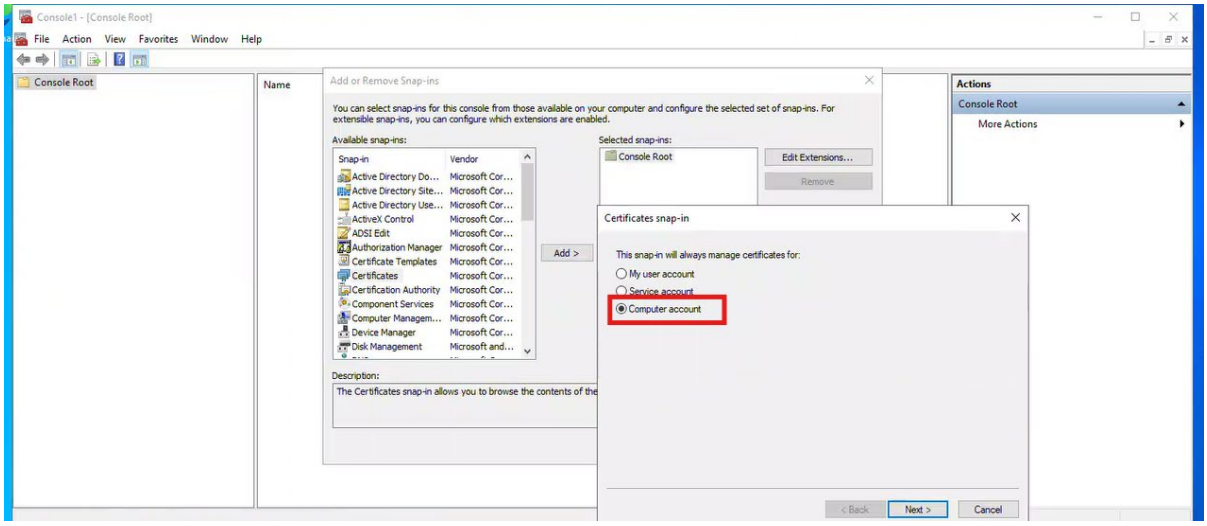


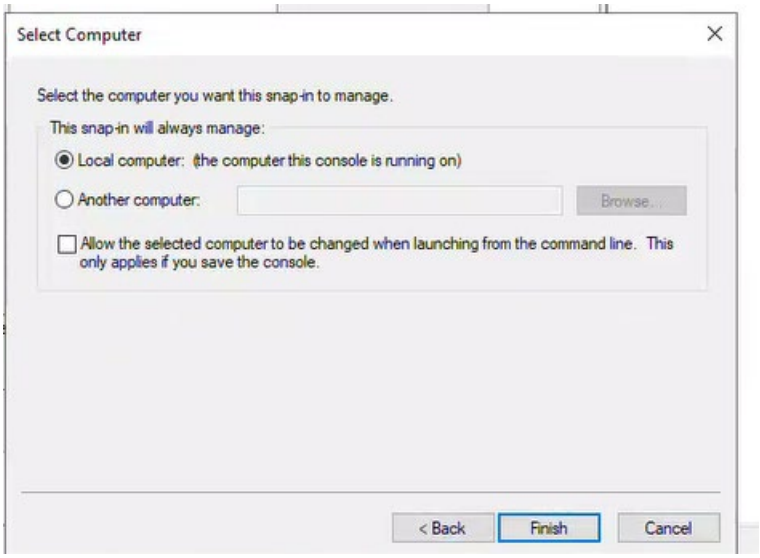

```
PS C:\Users\Administrator> Restart-Service certsvc
PS C:\Users\Administrator> _
```

6.2 Request and issue an SSL/TLS Certificate for dc101.vlabs1.com.

1. Open MMC on DC101

a) Press **Win + R**, type mmc, and press **Enter**.
b) Click **File → Add/Remove Snap-in**.
c) Select **Certificates → Add →** Choose **Computer Account → Next → Finish → OK**.





2. Request a New Certificate

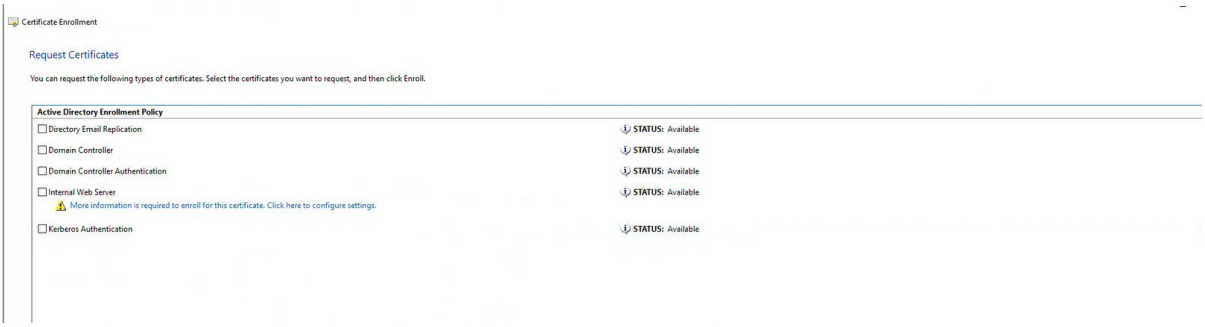
a) Expand Certificates (Local Computer) → Personal.

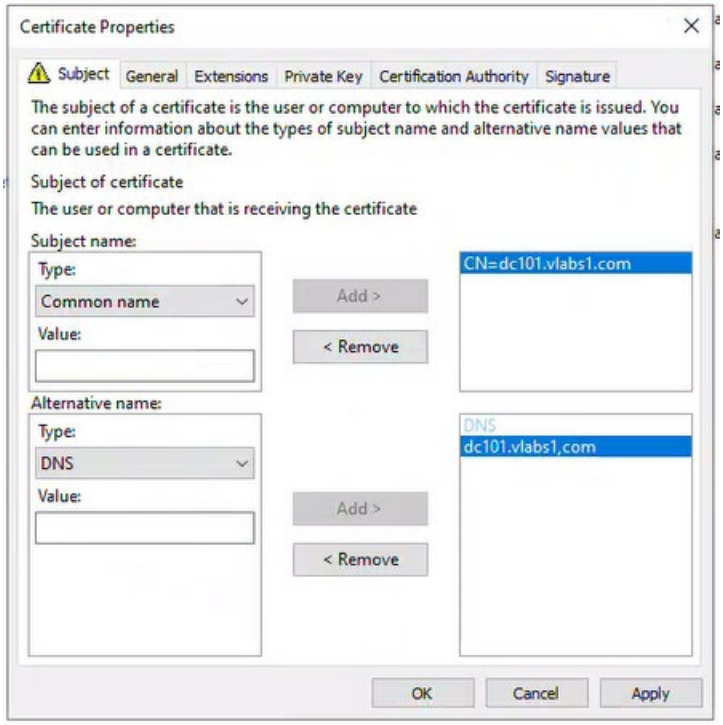
b) Right-click Certificates → All Tasks → Request New Certificate.

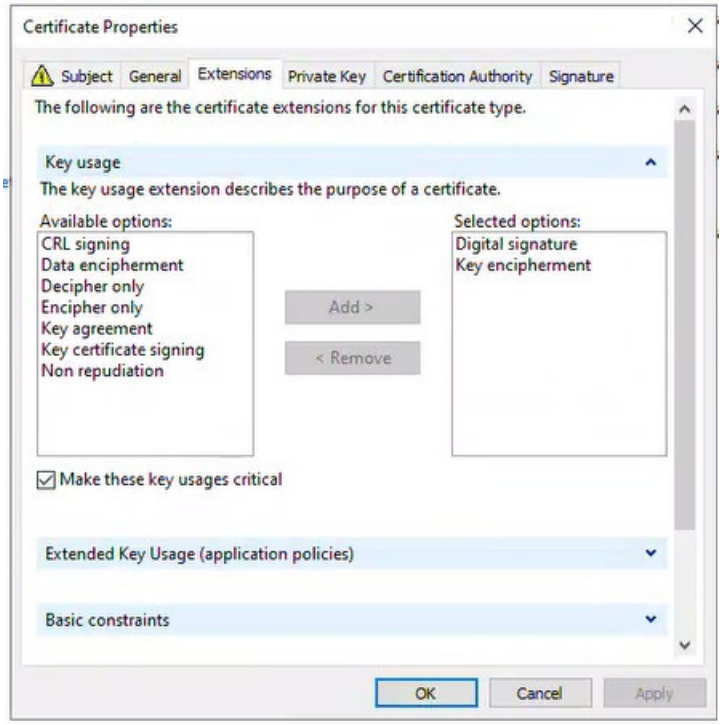
c) Click Next, select Active Directory Enrollment Policy, then click Next again.

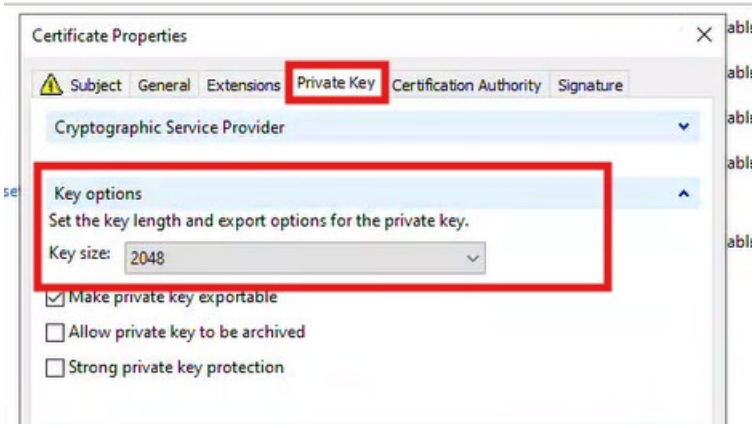
d) Select the Internal Web Server SSL template.

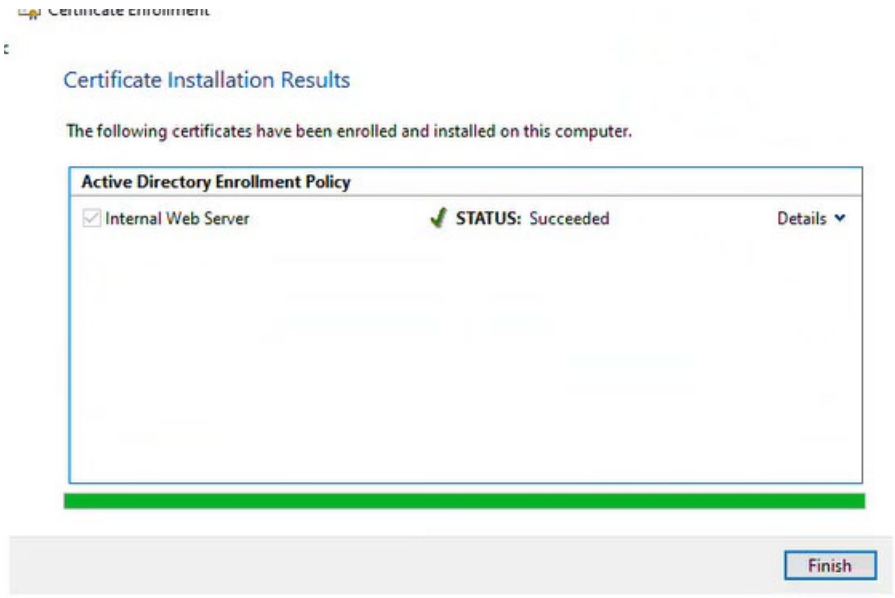
e) Click on More Information is required ...

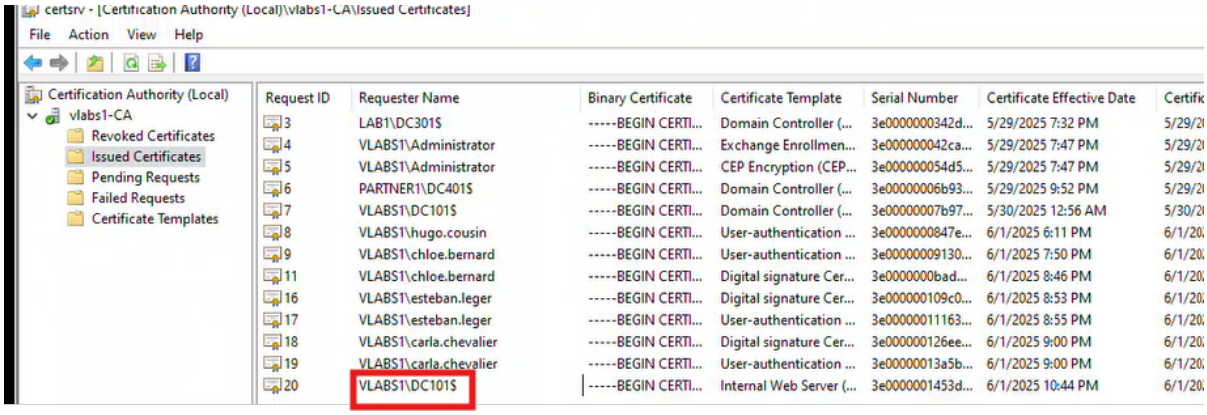



Certificate Properties
Subject
General
Extensions
Private Key
Certification Authority
Signature
The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.
Subject of certificate
The user or computer that is receiving the certificate
Subject name:
Type:
Common name
Value:
Add >
< Remove
CN=dc101.vlabs1.com
Alternative name:
Type:
DNS
Value:
Add >
< Remove
DNS
dc101.vlabs1,com
OK
Cancel
Apply


Certificate Properties
Subject
General
Extensions
Private Key
Certification Authority
Signature
The following are the certificate extensions for this certificate type.
Key usage
The key usage extension describes the purpose of a certificate.
Available options:
CRL signing
Data encipherment
Decipher only
Encipher only
Key agreement
Key certificate signing
Non repudiation
Add >
< Remove
Selected options:
Digital signature
Key encipherment
Make these key usages critical
Extended Key Usage (application policies)
Basic constraints
OK
Cancel
Apply







6.3 Bind the certificate to the local web server (IIS).

1. Install IIS (If Not Installed)

- Run the following command:

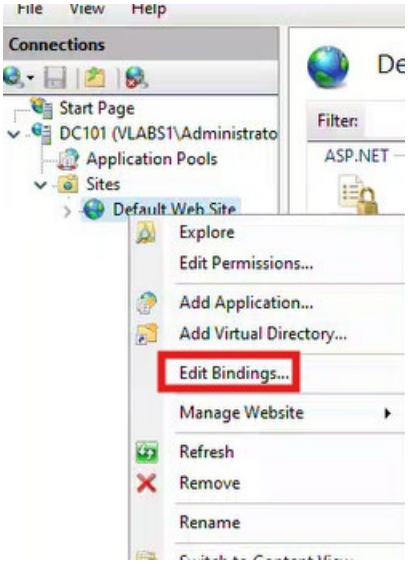
Install-WindowsFeature -Name Web-Server -IncludeManagementTools

2. Open IIS Manager

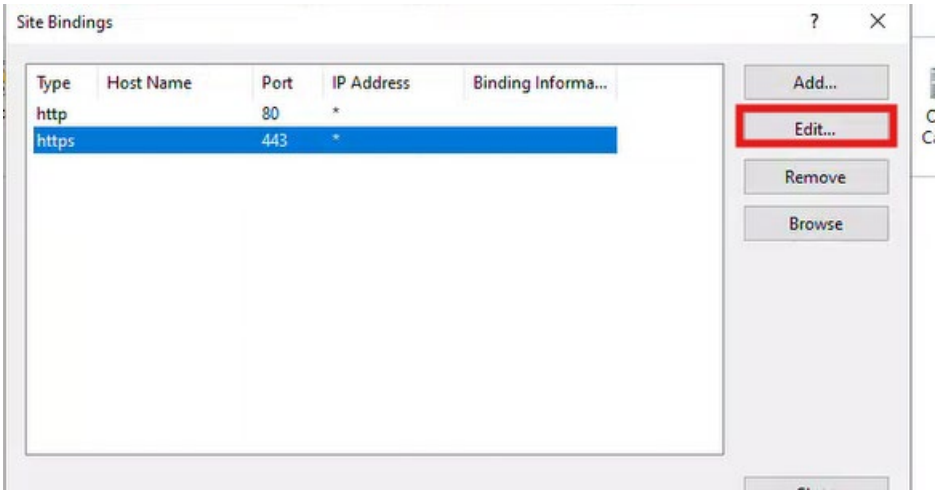
- Run inetmgr.

3. Create a Local Website (If Not Already Available)

- Navigate to Sites → Right-click Default Web Site → Edit Bindings.



- Select https then Edit

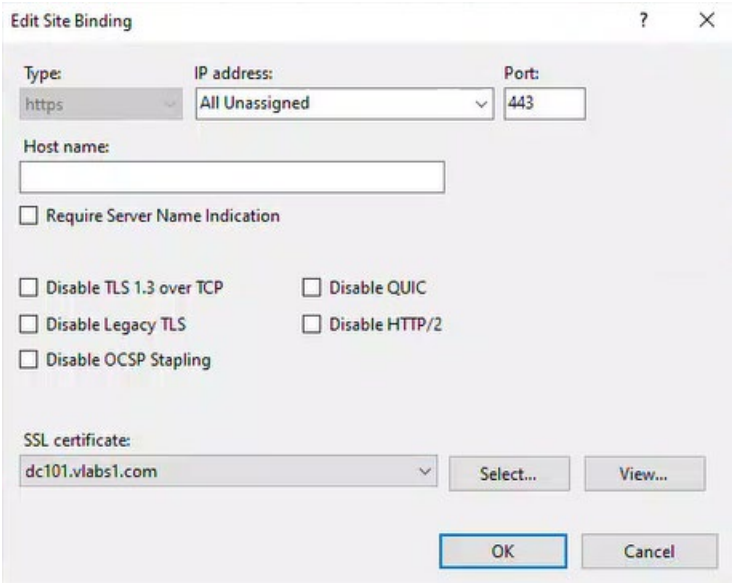


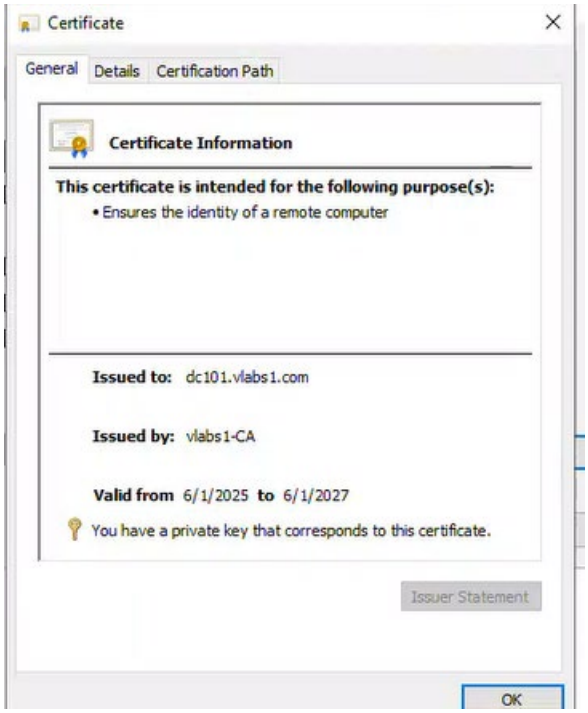
- Type: HTTPS

- IP Address: All Unassigned

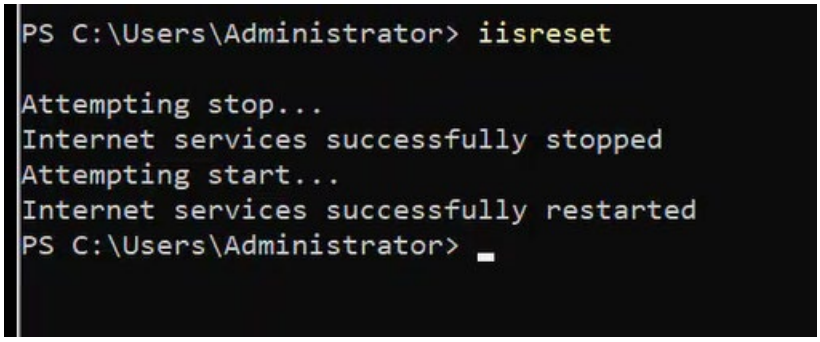
- Port: 443

- SSL Certificate: Select the issued certificate.

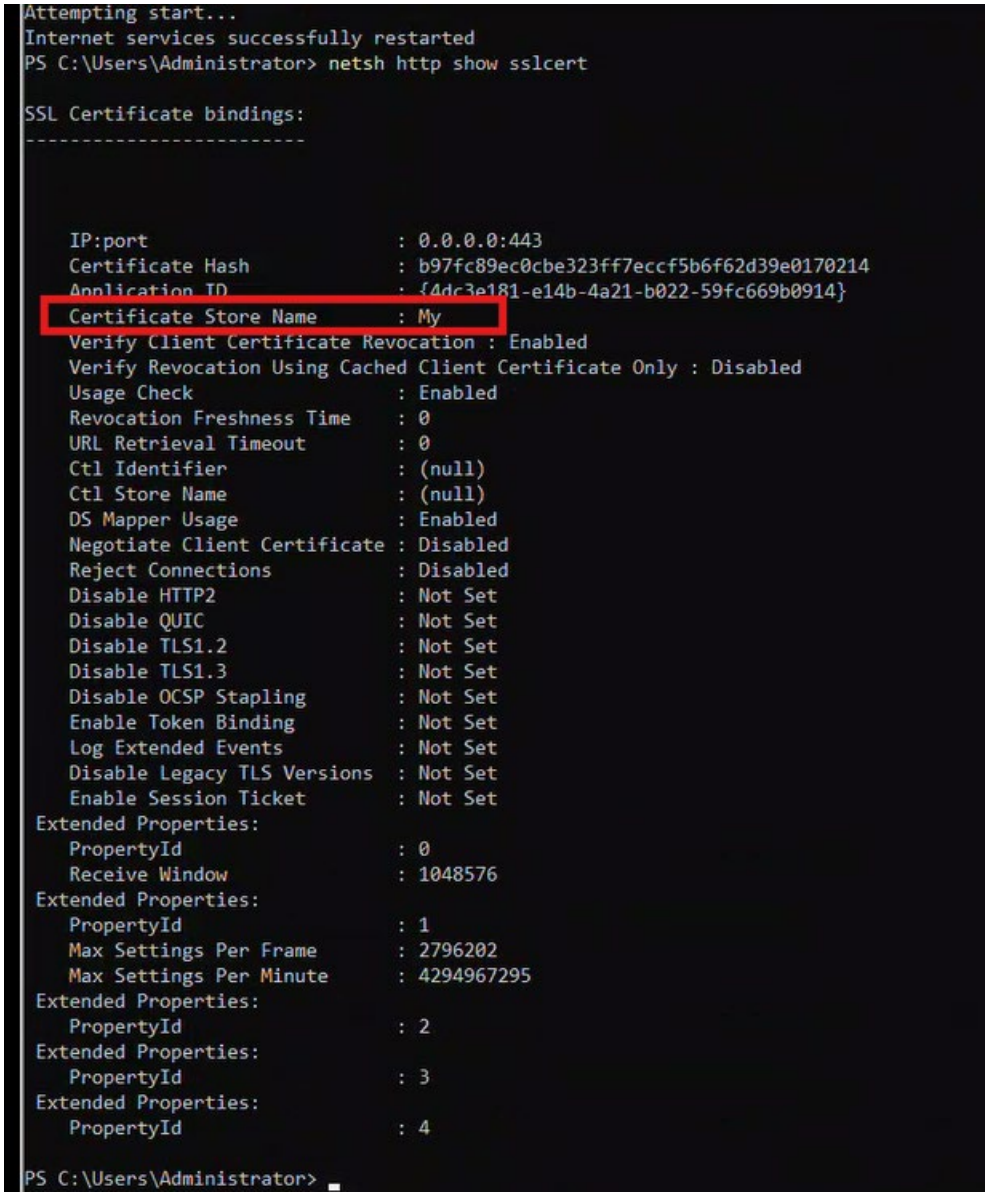




4. Apply and Restart IIS
   - Click OK → Close.
   - Restart IIS with: iisreset



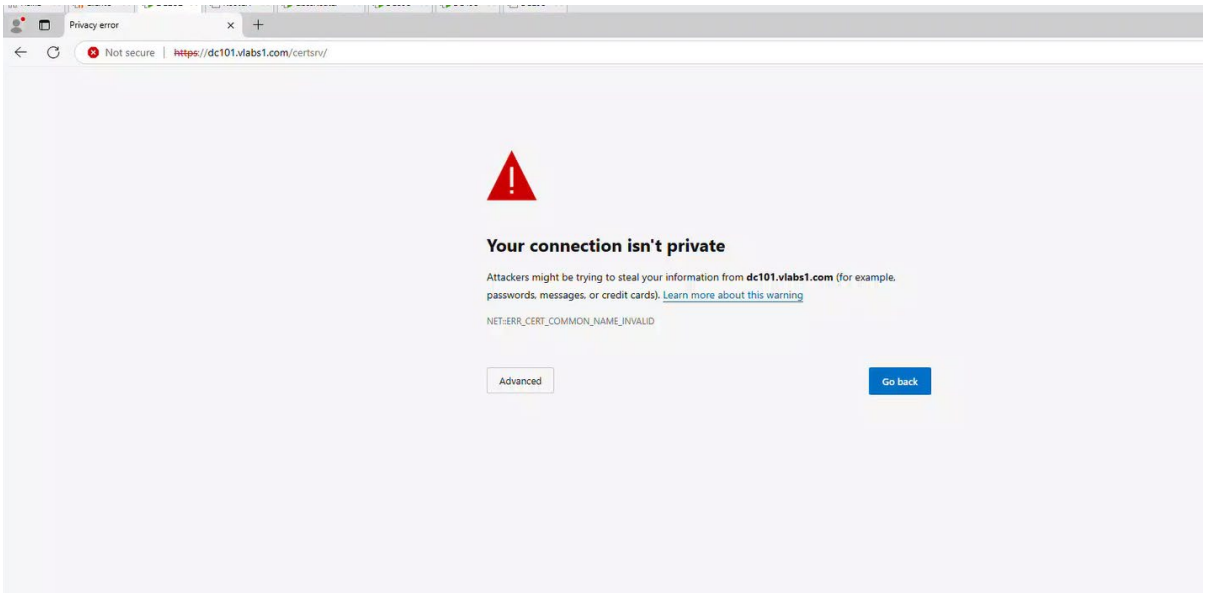
- Confirm That IIS is serving the correct certificate:
  netsh http show sslcert

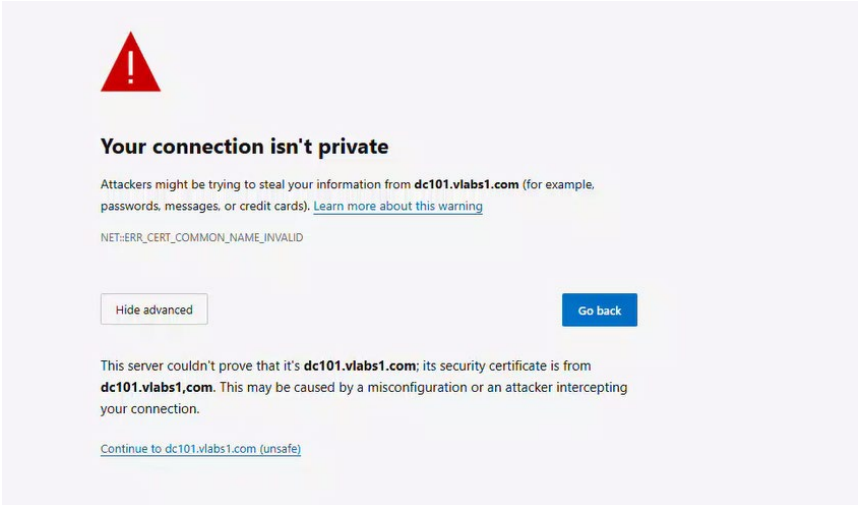


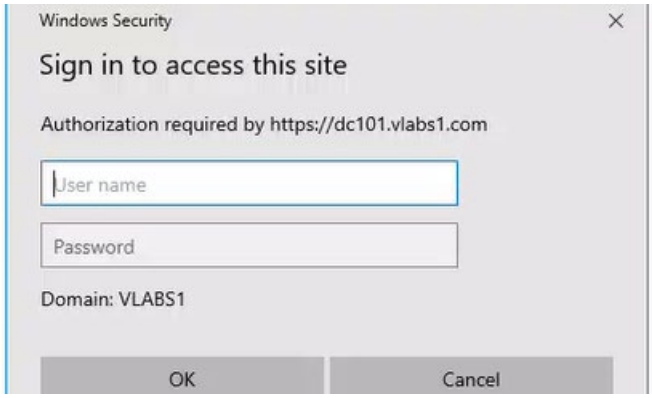
- Verify certificate details using this command:
  Get-ChildItem -Path Cert:\LocalMachine\My

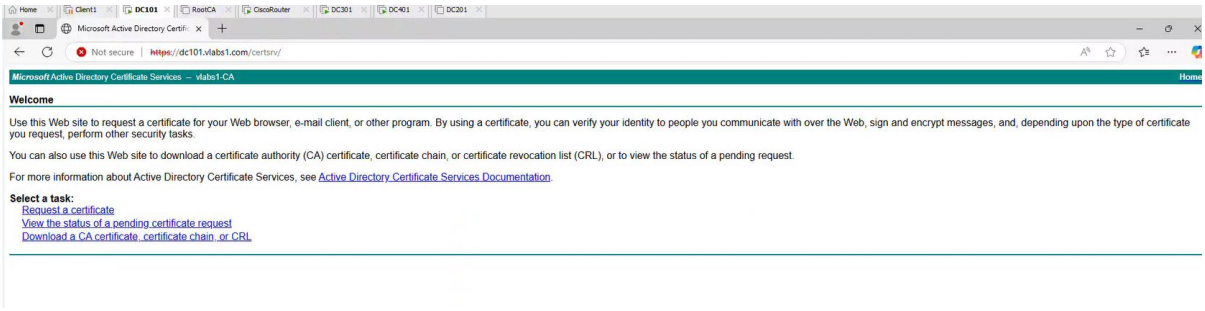
```
PS C:\Users\Administrator> Get-ChildItem -Path Cert:\LocalMachine\My


   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                                Subject
----------                                -------
ECA34B7E2935853DD42DE8CAE0E154504B610C70  CN=vlabs1-CA, DC=vlabs1, DC=com
B97FC89EC0CBE323FF7ECCF5B6F62D39E0170214  CN=dc101.vlabs1.com
96704B3DC64D8525A4AFBAC549F73661856A19E2  CN=DC101.vlabs1.com
3474A390B02D54557C4113318C3F2A8EA7A38E75  E=administartor@vlabs1.com, CN=B, O=VLAB1, L=Montreal, S=Quebec, C=CA
2A346023A0AAEC4ECF348168383C7DE55F9508CE  E=administartor@vlabs1.com, CN=B, O=VLAB1, L=Montreal, S=Quebec, C=CA


PS C:\Users\Administrator>
```

6.4 Test and verify HTTPS access to dc101.vlabs1.com.

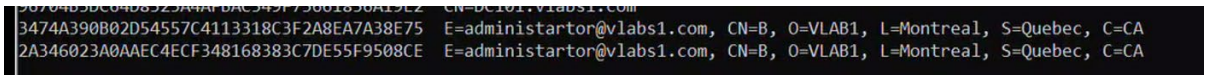








Certificate does not seem to work because maybe a typo



Email typo is administrator…. Should be administrator. Could not correct it