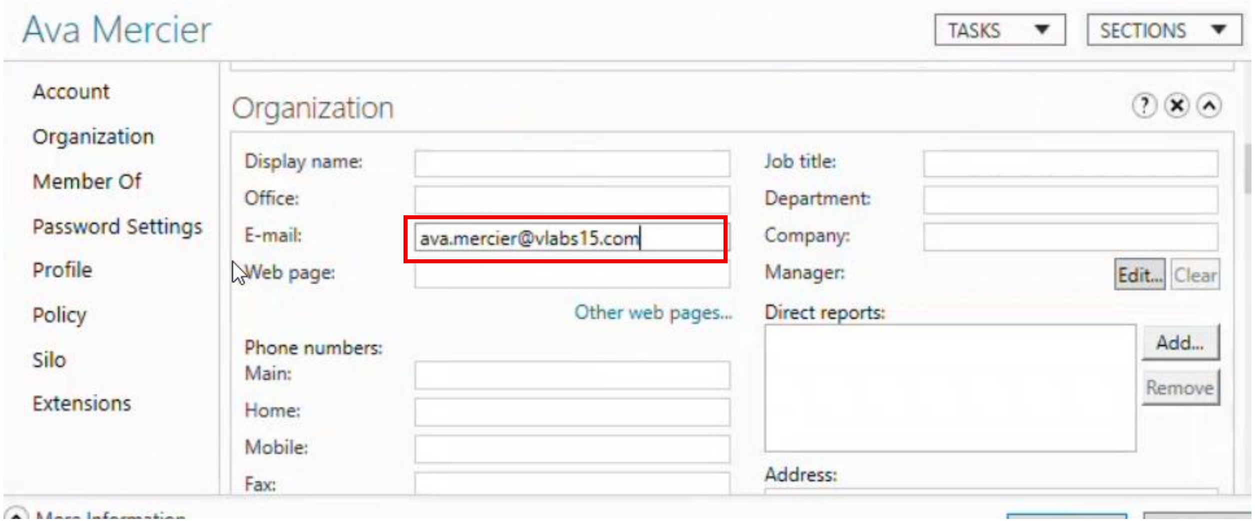
Lab - Managing a Certificate Authority Server in Active Directory

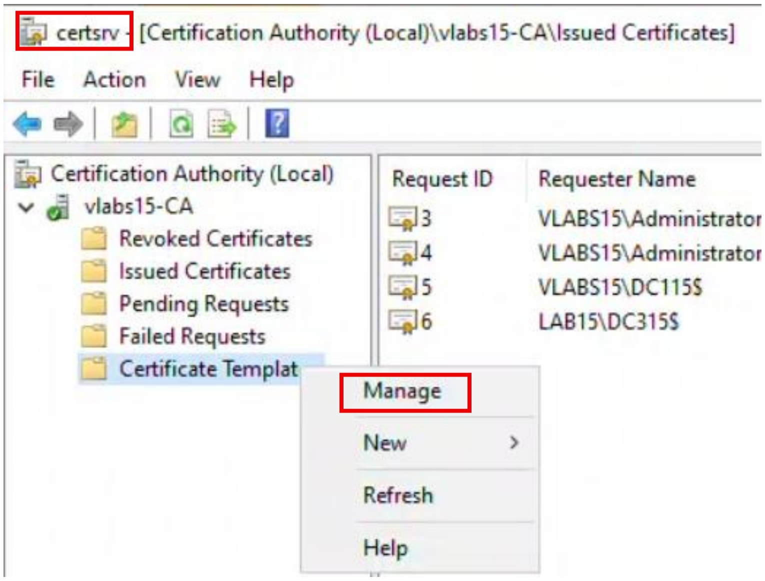
Task 1: Issue User Certificates in an AD Domain

- Configure and publish User Certificates from Enterprise CA.

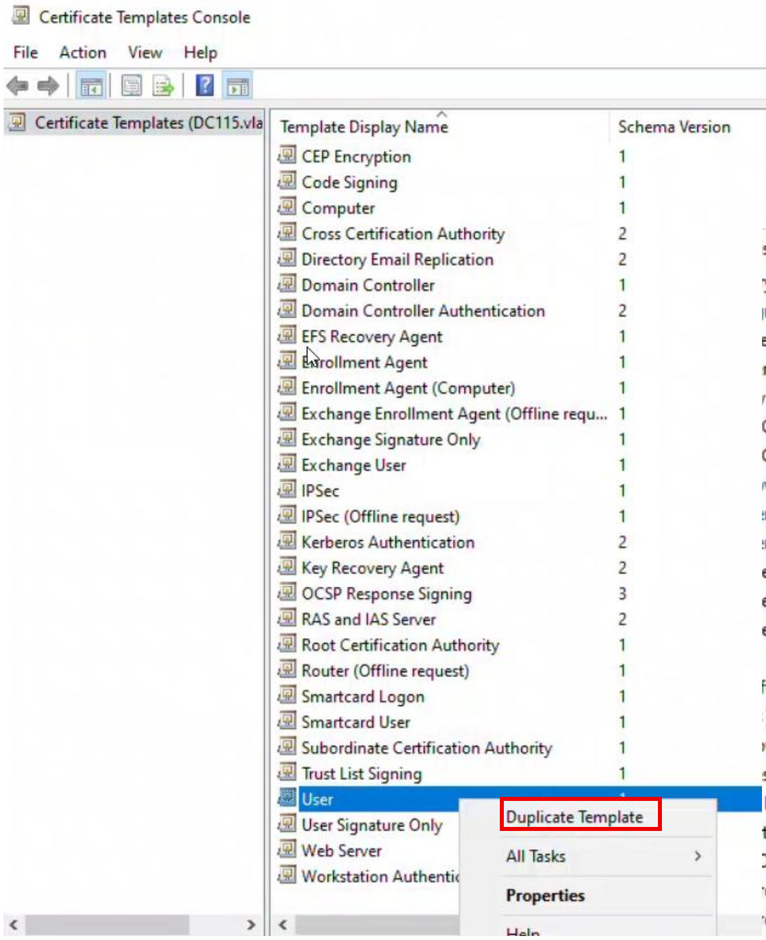
Make sure the user(s) have an email address assigned to their profile



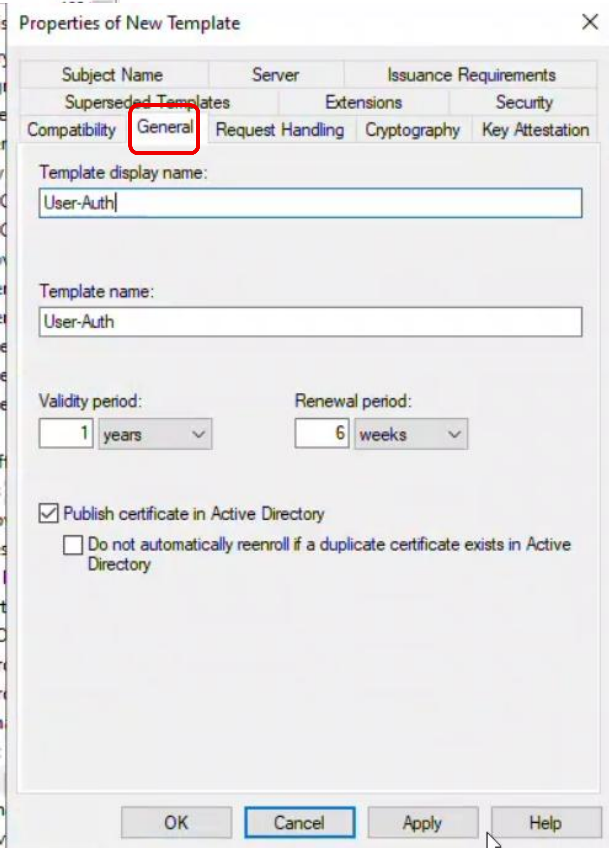
E-mail: ava.mercier@vlabs15.com


certsrv - [Certification Authority (Local)\vlabs15-CA\Issued Certificates]

Request ID	Requester Name
3	VLABS15\Administrator
4	VLABS15\Administrator
5	VLABS15\DC115$
6	LAB15\DC315$



Template Display Name	Schema Version	Versi
CEP Encryption	1	4.1
Code Signing	1	3.1
Computer	1	5.1
Cross Certification Authority	2	
Directory Email Replication	2	
Domain Controller	1	
Domain Controller Authentication	2	
EFS Recovery Agent	1	
Enrollment Agent	1	
Enrollment Agent (Computer)	1	
Exchange Enrollment Agent (Offline requ...	1	
Exchange Signature Only	1	
Exchange User	1	
IPSec	1	
IPSec (Offline request)	1	
Kerberos Authentication	2	
Key Recovery Agent	2	
OCSP Response Signing	3	
RAS and IAS Server	2	
Root Certification Authority	1	
Router (Offline request)	1	
Smartcard Logon	1	
Smartcard User	1	
Subordinate Certification Authority	1	
Trust List Signing	1	
User	1	
User Signature Only		
Web Server		
Workstation Authentic		



Template display name: User-Auth

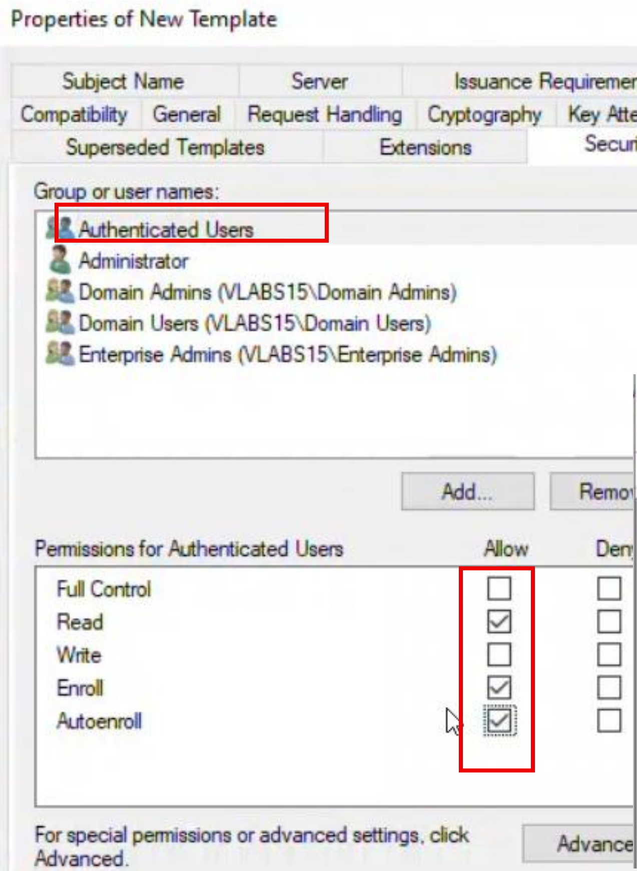
Template name: User-Auth

Validity period: 1 years

Renewal period: 6 weeks

☑ Publish certificate in Active Directory

☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

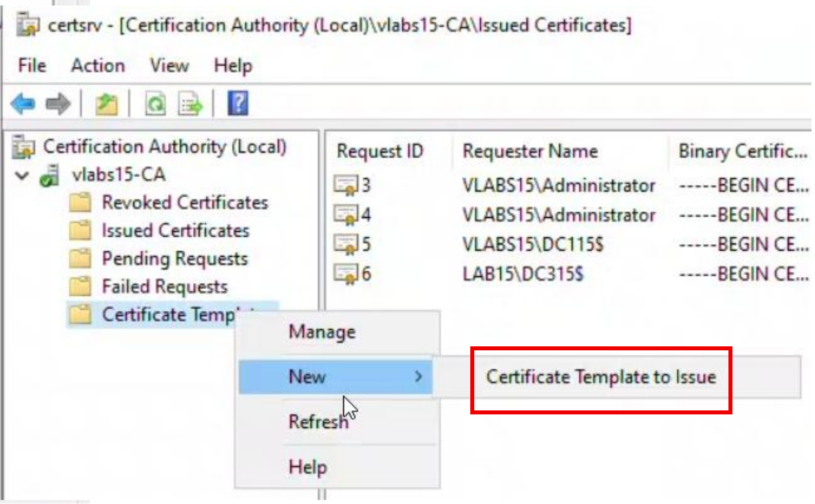


Group or user names:

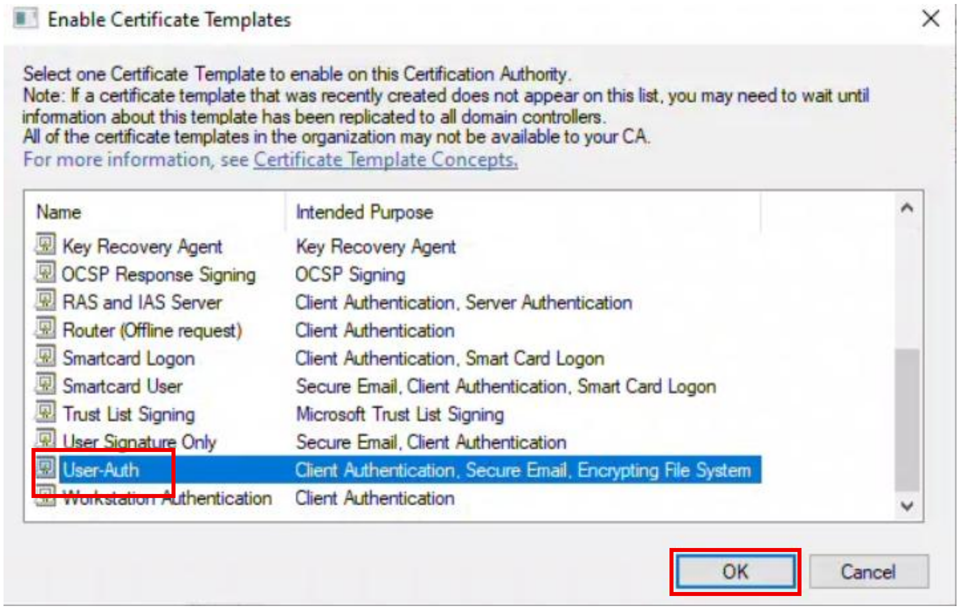
- Authenticated Users
- Administrator
- Domain Admins (VLABS15\Domain Admins)
- Domain Users (VLABS15\Domain Users)
- Enterprise Admins (VLABS15\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	☐	☐
Read	☑	☐
Write	☐	☐
Enroll	☑	☐
Autoenroll	☑	☐

For special permissions or advanced settings, click Advanced.



Request ID	Requester Name	Binary Certific...
3	VLABS15\Administrator	-----BEGIN CE...
4	VLABS15\Administrator	-----BEGIN CE...
5	VLABS15\DC115$	-----BEGIN CE...
6	LAB15\DC315$	-----BEGIN CE...

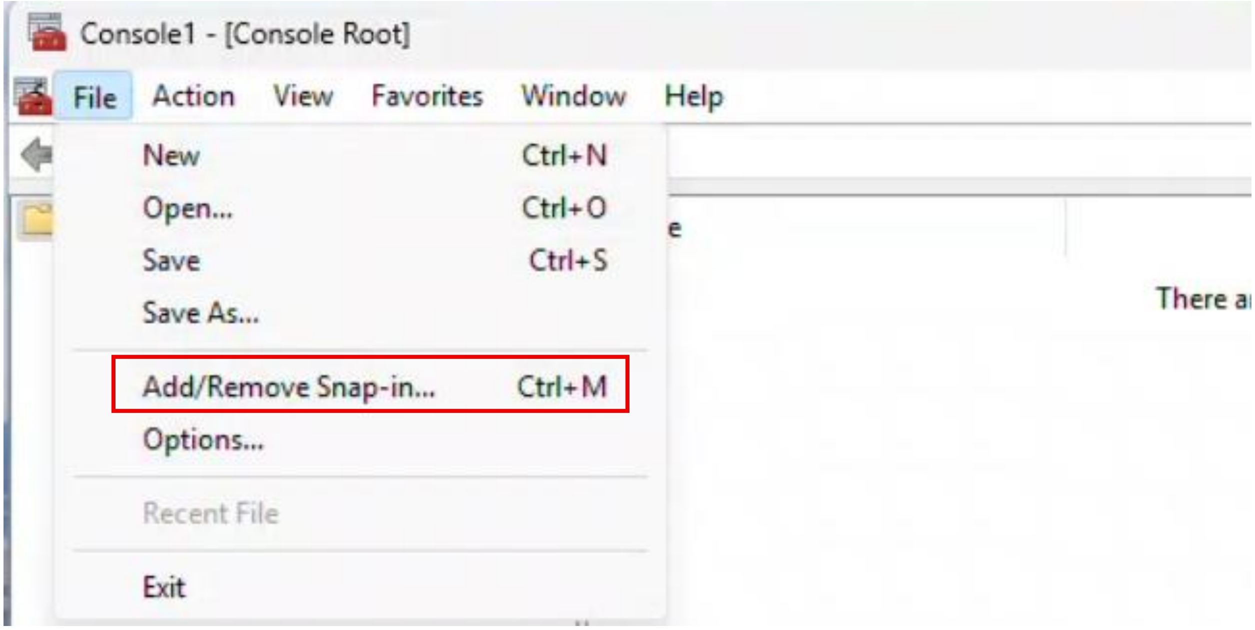


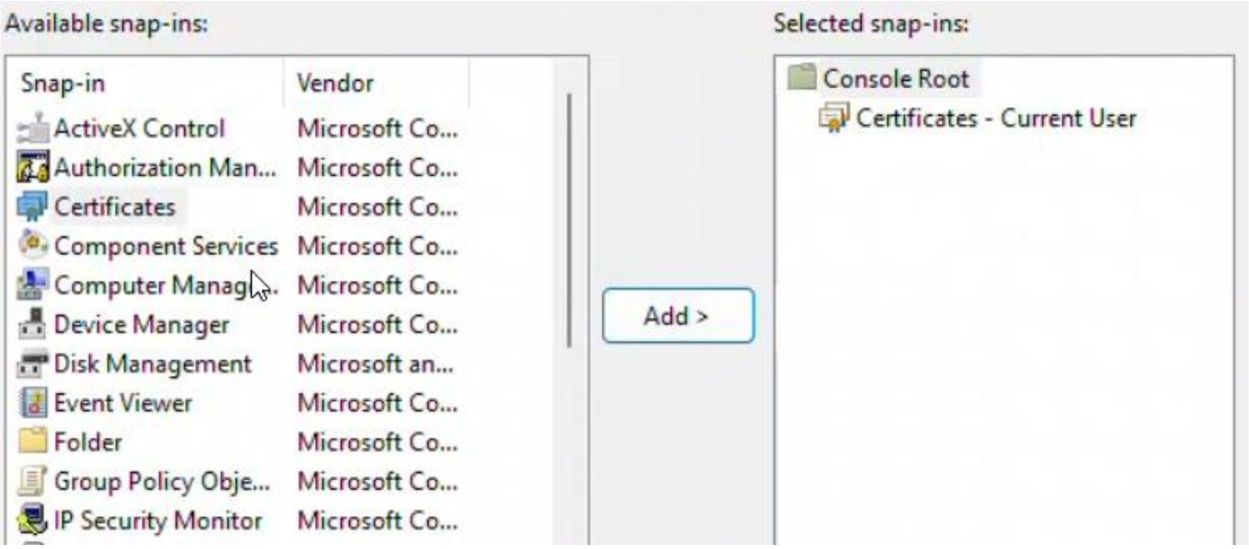
Enable Certificate Templates

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon
Trust List Signing	Microsoft Trust List Signing
User Signature Only	Secure Email, Client Authentication
User-Auth	Client Authentication, Secure Email, Encrypting File System
Workstation Authentication	Client Authentication

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



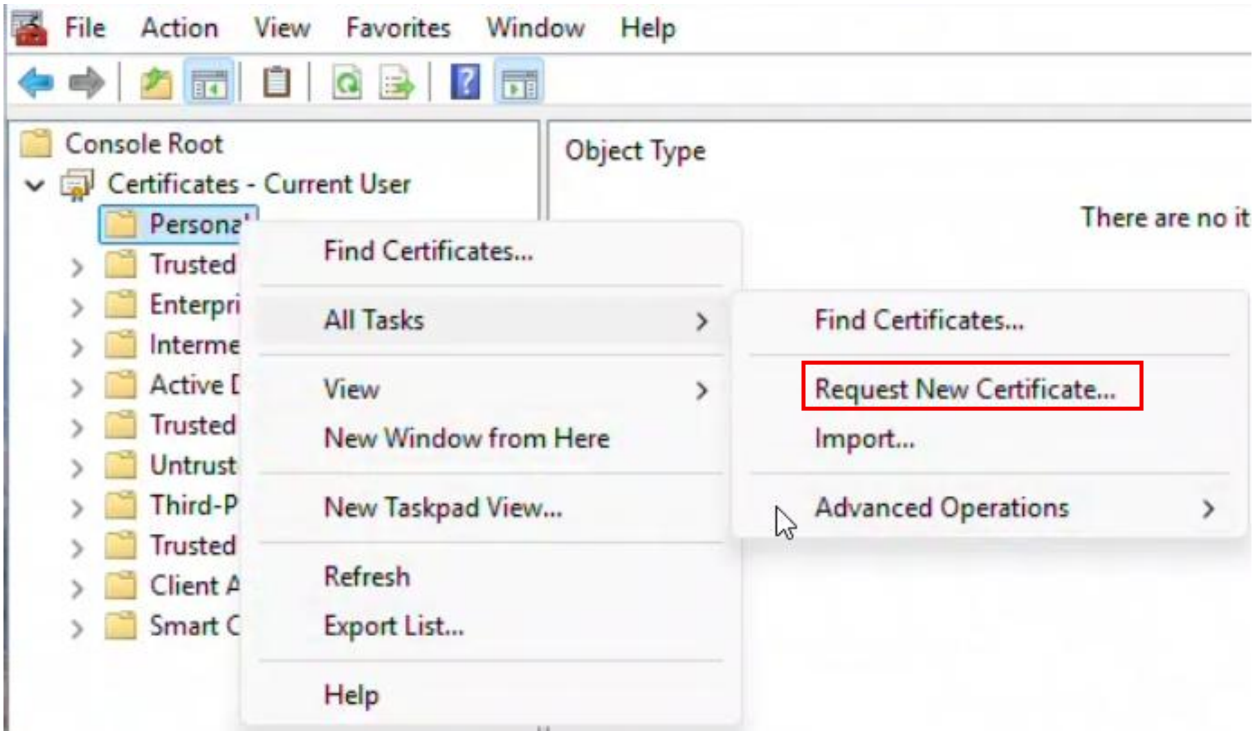


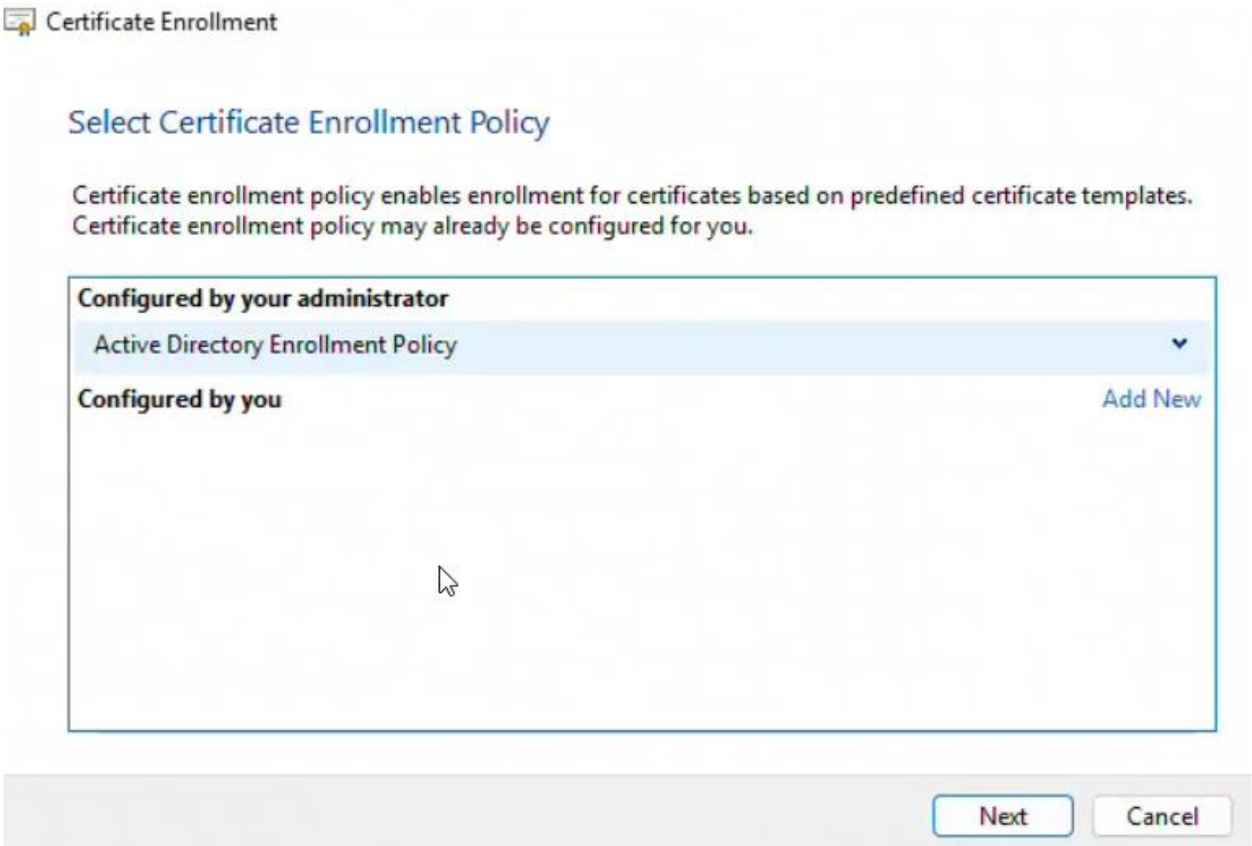
Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Co...
Authorization Man...	Microsoft Co...
Certificates	Microsoft Co...
Component Services	Microsoft Co...
Computer Manag...	Microsoft Co...
Device Manager	Microsoft Co...
Disk Management	Microsoft an...
Event Viewer	Microsoft Co...
Folder	Microsoft Co...
Group Policy Obje...	Microsoft Co...
IP Security Monitor	Microsoft Co...

Selected snap-ins:

Console Root
Certificates - Current User





Certificate Enrollment

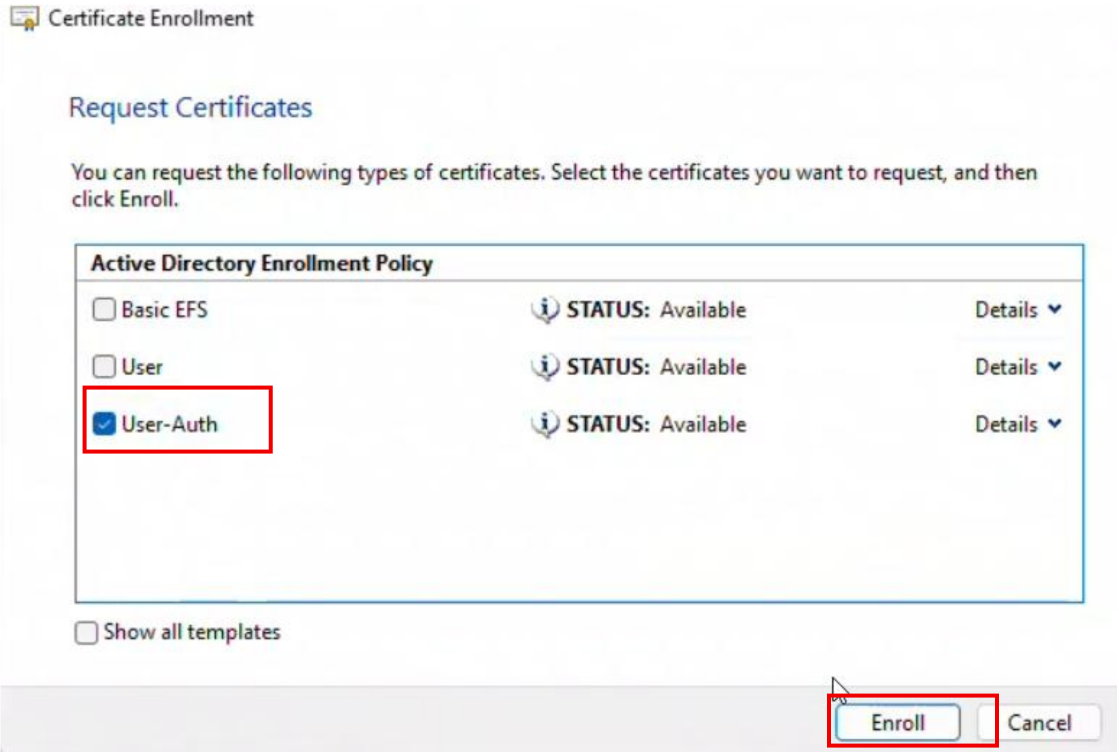
Select Certificate Enrollment Policy

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



Certificate Enrollment

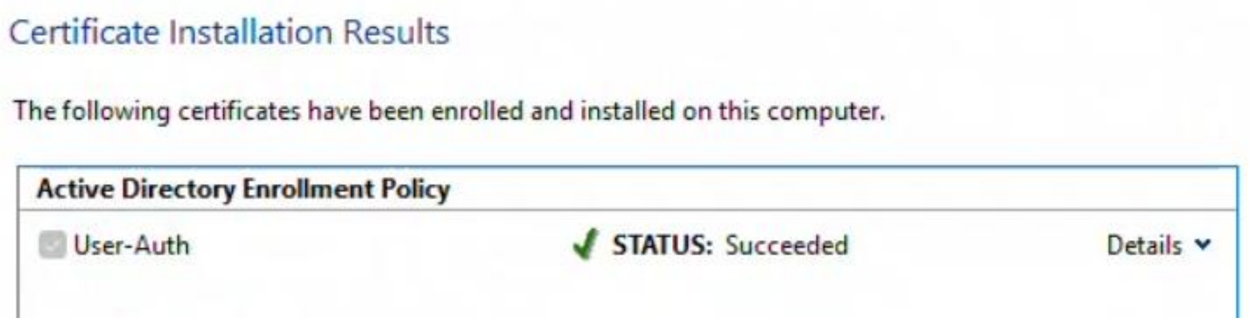
Request Certificates

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

Active Directory Enrollment Policy

□ Basic EFS	**STATUS:** Available	Details
□ User	**STATUS:** Available	Details
☑ User-Auth	**STATUS:** Available	Details

□ Show all templates



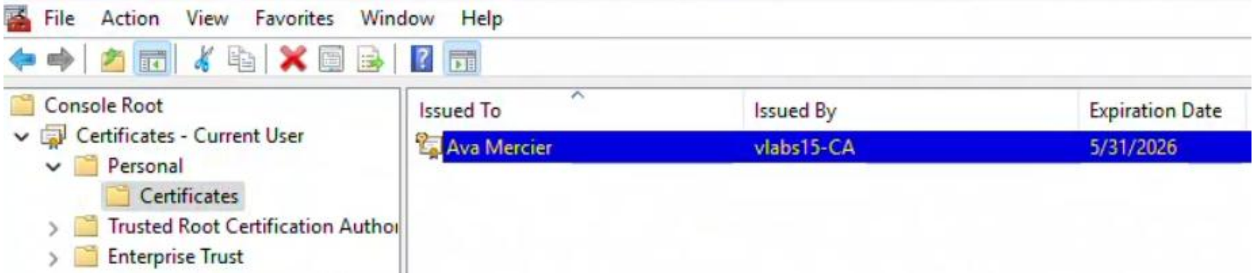
Certificate Installation Results

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

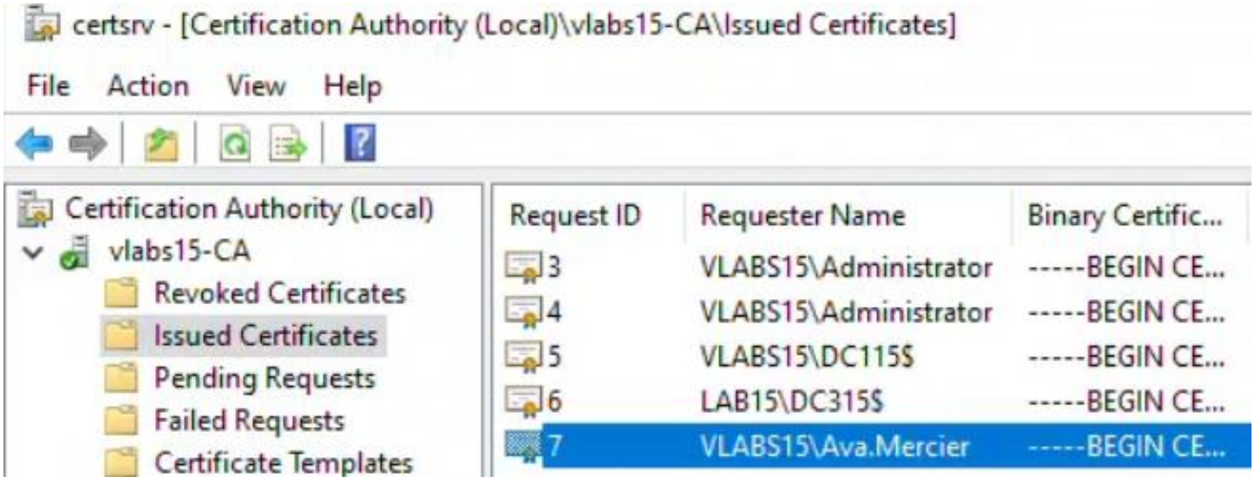
Active Directory Enrollment Policy

☑ User-Auth ✓ STATUS: Succeeded

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



Issued To	Issued By	Expiration Date
Ava Mercier	vlabs15-CA	5/31/2026



certsrv - [Certification Authority (Local)\vlabs15-CA\Issued Certificates]

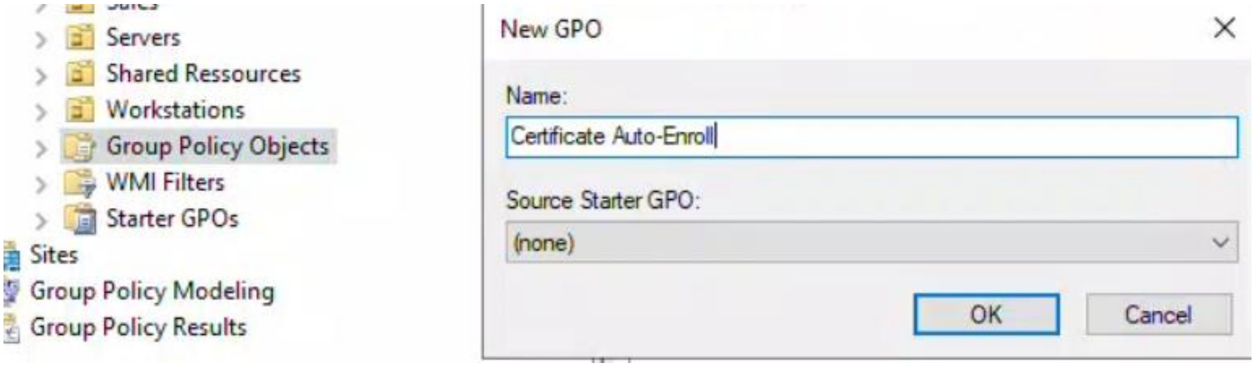
Request ID	Requester Name	Binary Certific...
3	VLABS15\Administrator	-----BEGIN CE...
4	VLABS15\Administrator	-----BEGIN CE...
5	VLABS15\DC115$	-----BEGIN CE...
6	LAB15\DC315$	-----BEGIN CE...
7	VLABS15\Ava.Mercier	-----BEGIN CE...

Task 2: Enable Automatic Certificate Enrollment in AD

- Configure Group Policy settings to allow automatic certificate

enrollment.

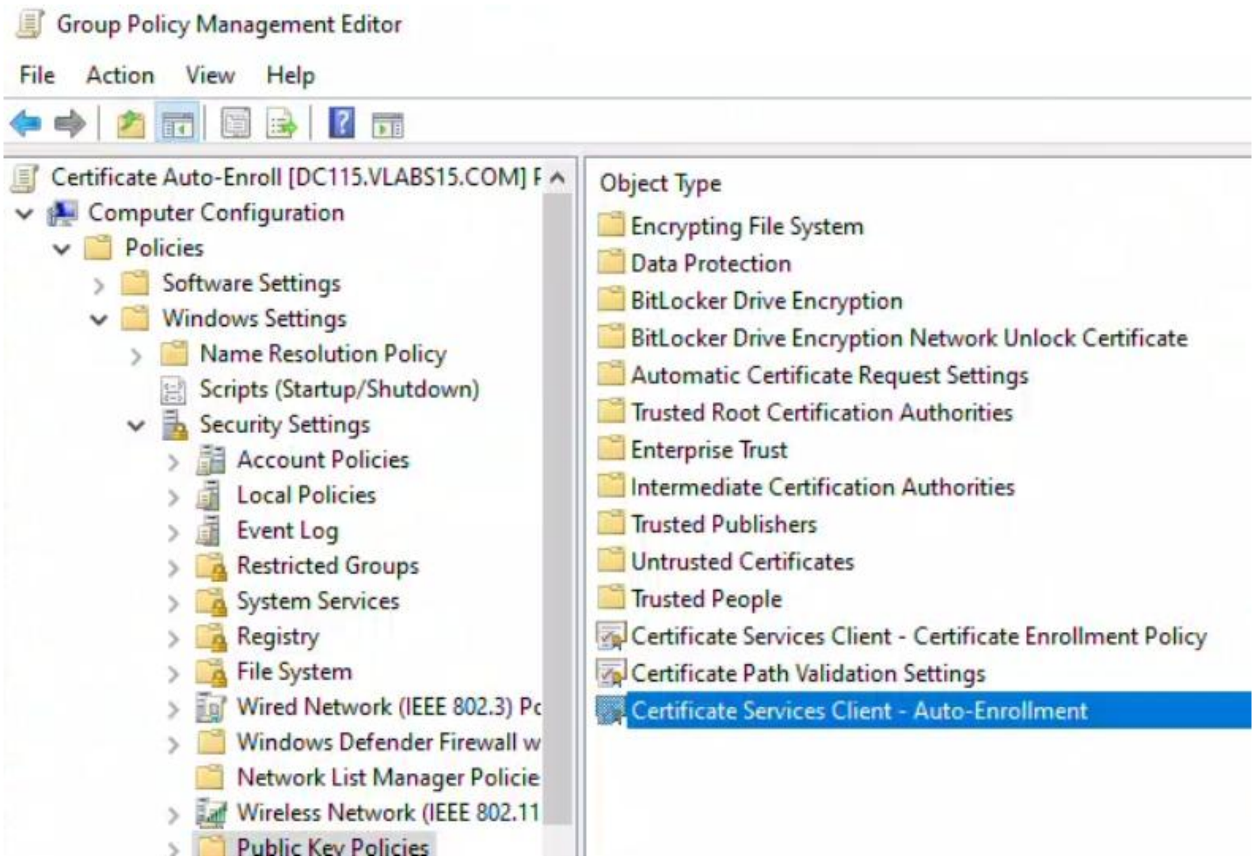
Computer Configuration →Policies →Windows Settings →Security →Public Key Policies



New GPO

Name: Certificate Auto-Enroll

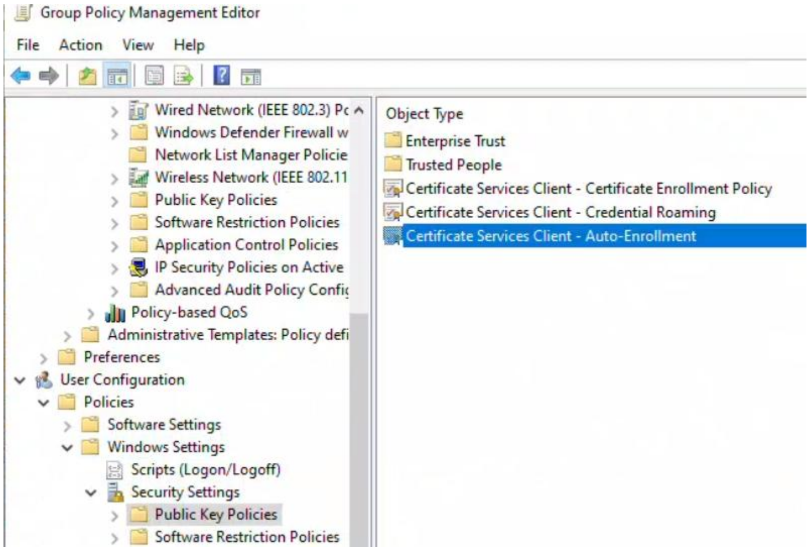
Source Starter GPO: (none)

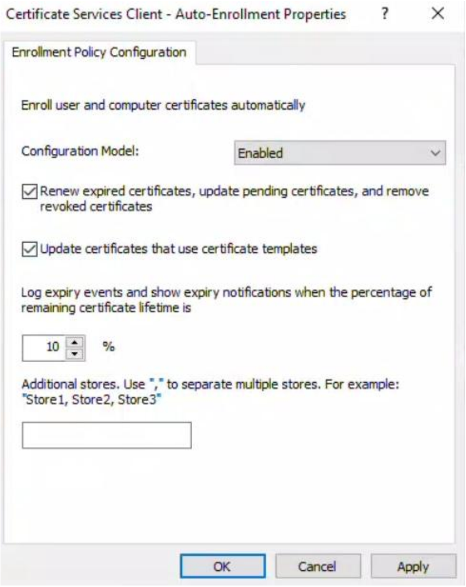

Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Pc
Windows Defender Firewall w
Network List Manager Policie
Wireless Network (IEEE 802.11
Public Key Policies
Object Type
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlock Certificate
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Services Client - Certificate Enrollment Policy
Certificate Path Validation Settings

Certificate Auto-Enroll [DC115.VLABS15.COM] P

Certificate Services Client - Auto-Enrollment

Now do the same in User Configuration


Group Policy Management Editor
File Action View Help
Wired Network (IEEE 802.3) Pc
Windows Defender Firewall w
Network List Manager Policie
Wireless Network (IEEE 802.11
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active
Advanced Audit Policy Config
Policy-based QoS
Administrative Templates: Policy defi
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Scripts (Logon/Logoff)
Security Settings
Public Key Policies
Software Restriction Policies
Object Type
Enterprise Trust
Trusted People
Certificate Services Client - Certificate Enrollment Policy
Certificate Services Client - Credential Roaming
Certificate Services Client - Auto-Enrollment


Certificate Services Client - Auto-Enrollment Properties ? ×
Enrollment Policy Configuration

Enroll user and computer certificates automatically

Configuration Model: Enabled

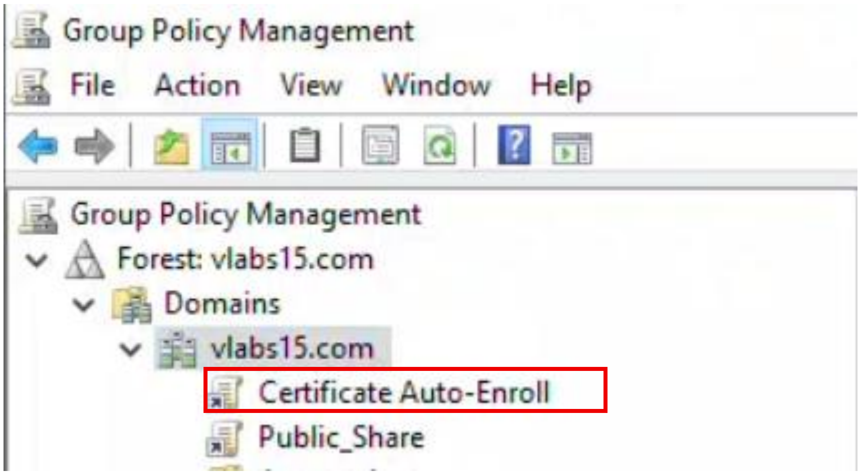
☑ Renew expired certificates, update pending certificates, and remove revoked certificates

☑ Update certificates that use certificate templates

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

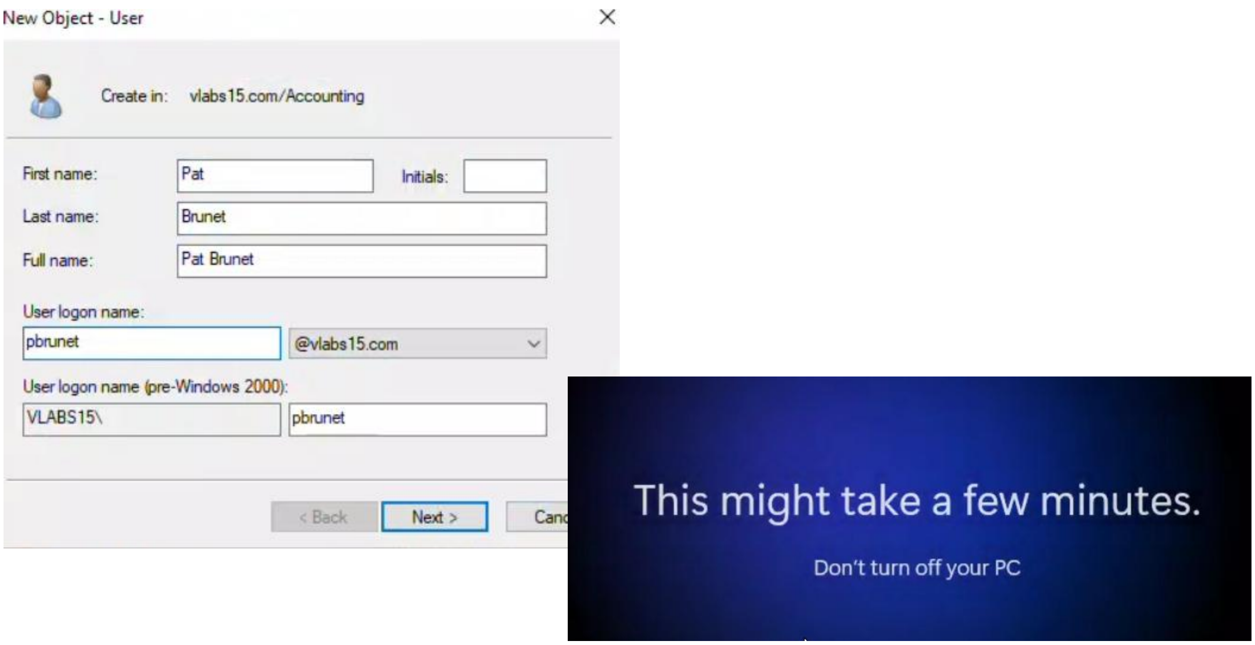
10 %

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



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

Let's create a new user Pat Brunet and test with him on the client(make sure they have an email address associated with the user)



New Object - User

Create in: vlabs15.com/Accounting

First name:	Pat	Initials:	
Last name:	Brunet		
Full name:	Pat Brunet		

User logon name:

pbrunet @vlabs15.com

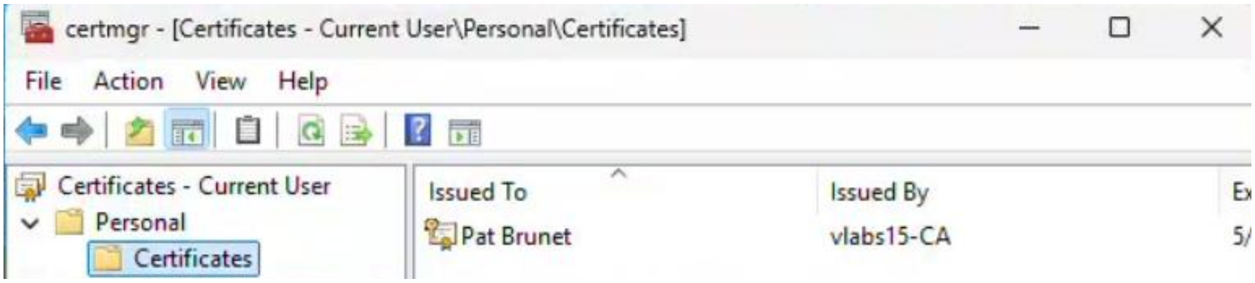
User logon name (pre-Windows 2000):

VLABS15\ pbrunet

This might take a few minutes.

Don't turn off your PC

The certificate was automatically assigned.

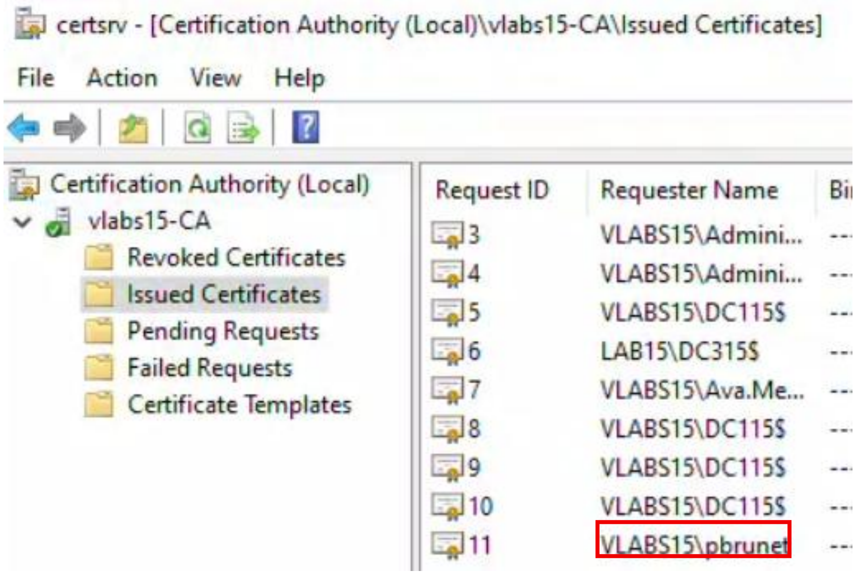


certmgr - [Certificates - Current User\Personal\Certificates]

Issued To	Issued By	Ex
Pat Brunet	vlabs15-CA	5/

- Check the user account in the AD to verify that he has a valid certificate.

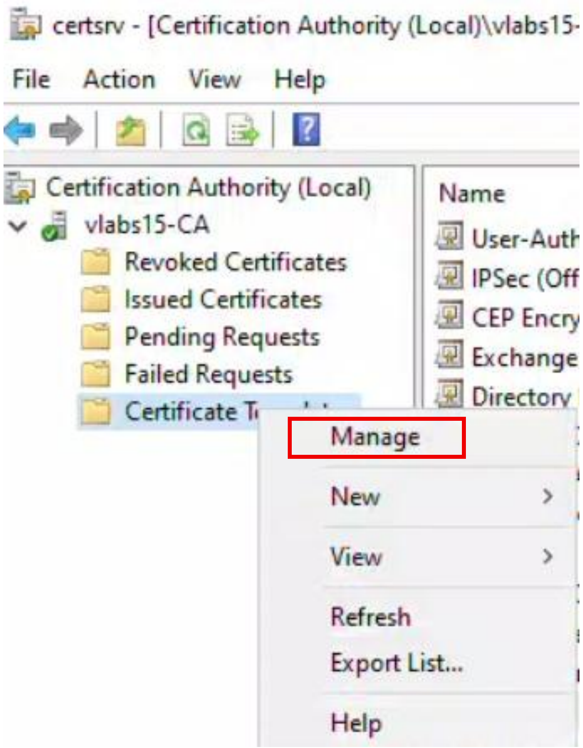
The certificate was automatically assigned.

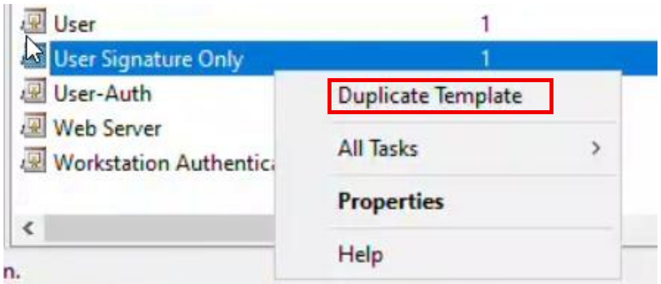


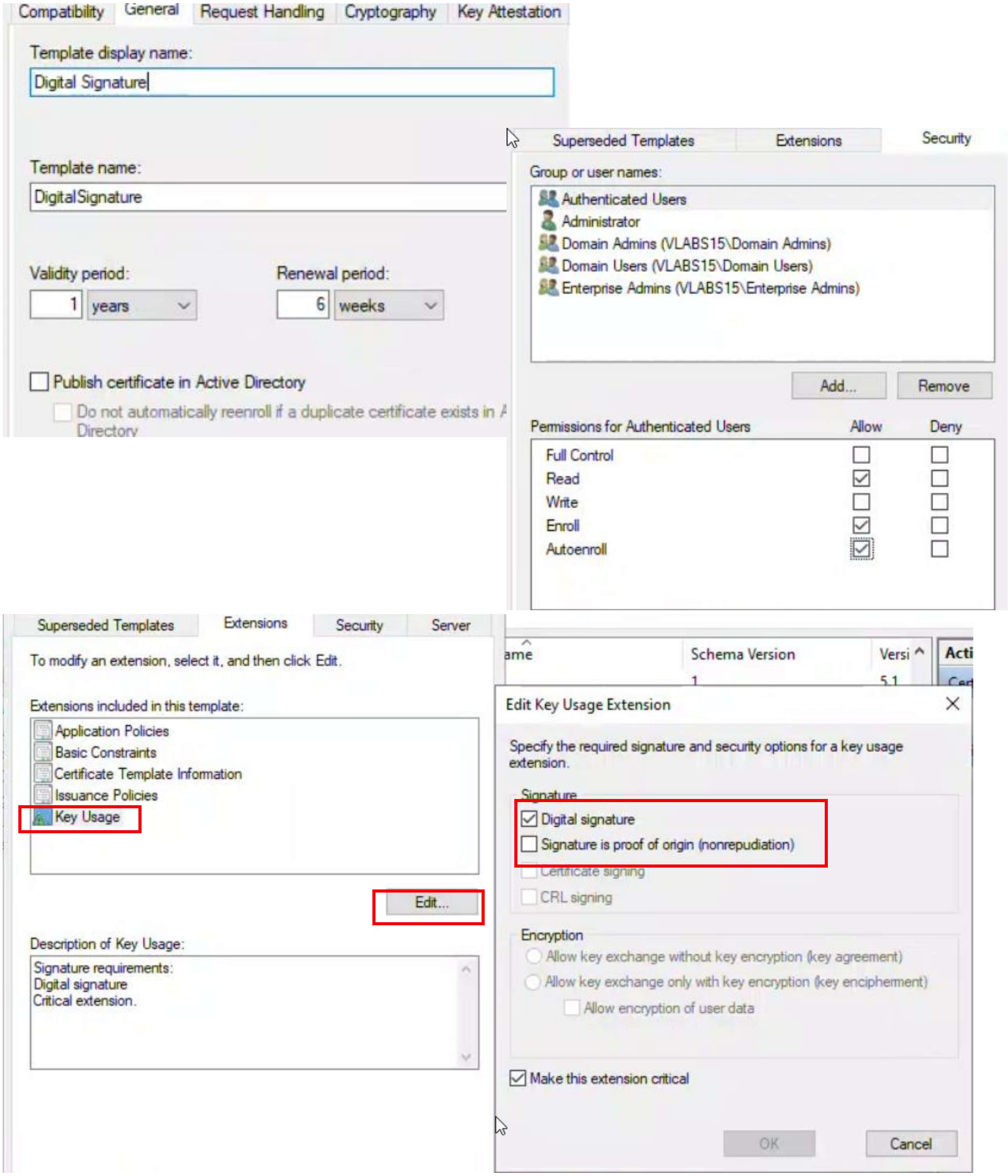
Request ID	Requester Name	Bi
3	VLABS15\Admini...	---
4	VLABS15\Admini...	---
5	VLABS15\DC115$	---
6	LAB15\DC315$	---
7	VLABS15\Ava.Me...	---
8	VLABS15\DC115$	---
9	VLABS15\DC115$	---
10	VLABS15\DC115$	---
11	VLABS15\pbrunet	---

Task 3: Issue Digitally Signed Documents and Files

- Issue Digital Signature Certificates from Enterprise CA.







Template display name: Digital Signature

Template name: DigitalSignature

Validity period: 1 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in A Directory

Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (VLABS15\Domain Admins)
- Domain Users (VLABS15\Domain Users)
- Enterprise Admins (VLABS15\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	☑	□

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

Description of Key Usage:

Signature requirements:
Digital signature
Critical extension.

Edit Key Usage Extension

Specify the required signature and security options for a key usage extension.

Signature

☑ Digital signature

□ Signature is proof of origin (nonrepudiation)

□ Certificate signing

□ CRL signing

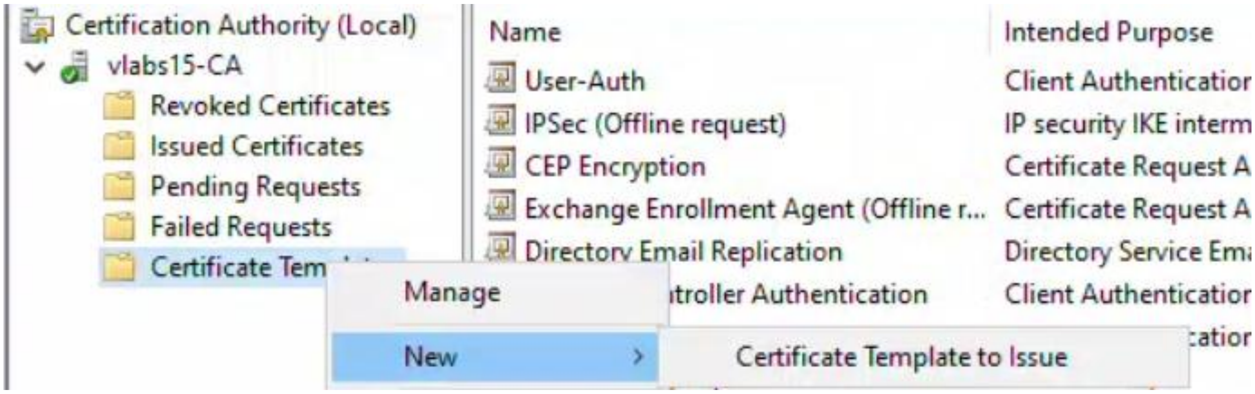
Encryption

○ Allow key exchange without key encryption (key agreement)

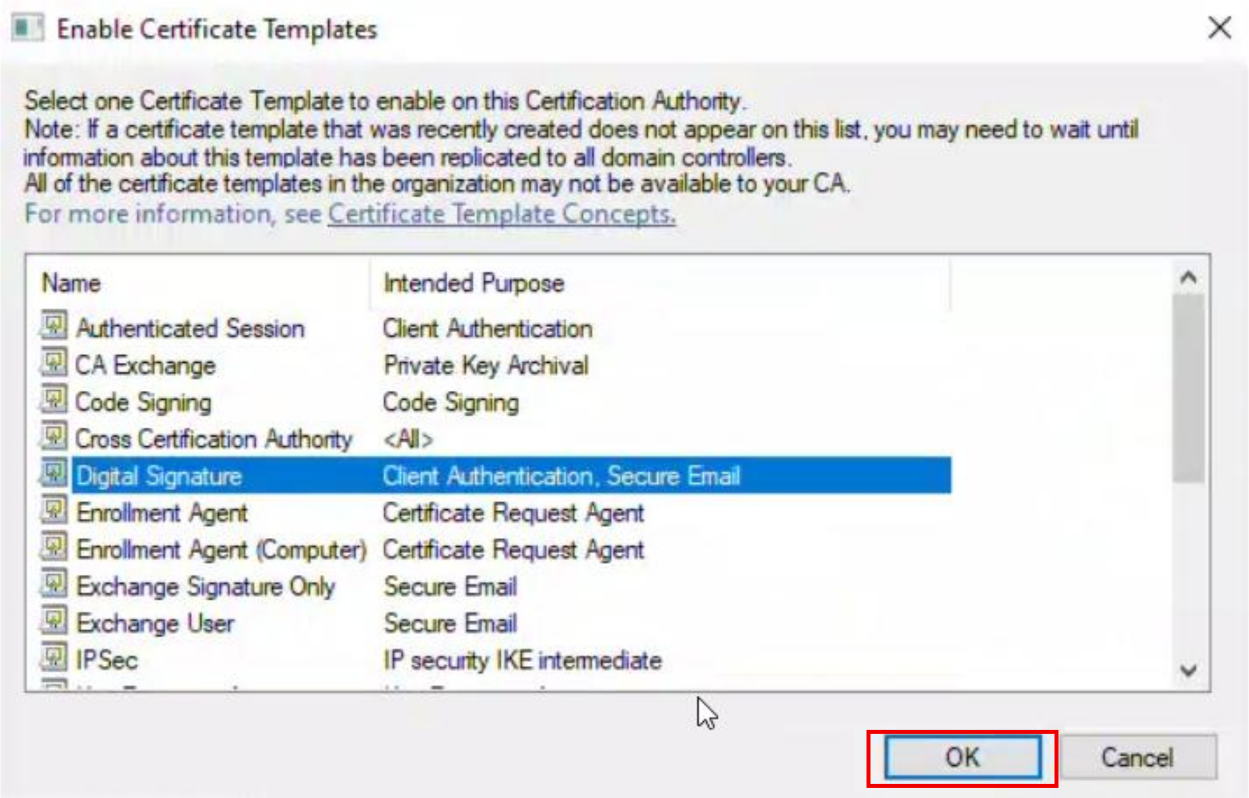
○ Allow key exchange only with key encryption (key encipherment)

□ Allow encryption of user data

☑ Make this extension critical



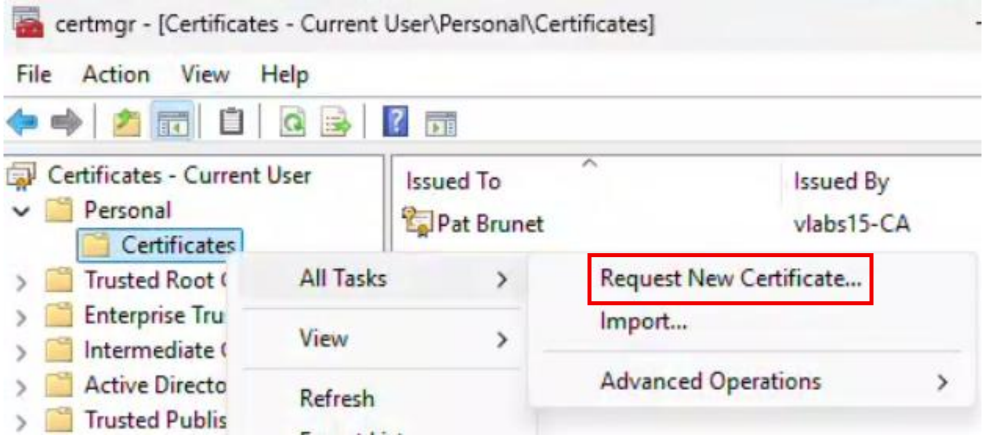
Name	Intended Purpose
User-Auth	Client Authenticatior
IPSec (Offline request)	IP security IKE interm
CEP Encryption	Certificate Request A
Exchange Enrollment Agent (Offline r...	Certificate Request A
Directory Email Replication	Directory Service Emi
ıtroller Authentication	Client Authenticatior
	:atior



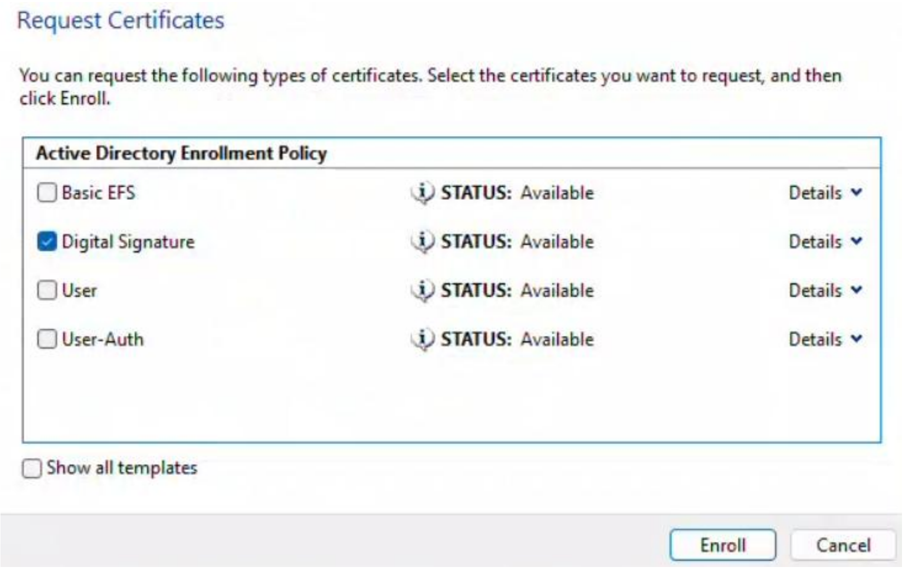
Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Authenticated Session	Client Authentication
CA Exchange	Private Key Archival
Code Signing	Code Signing
Cross Certification Authority	<All>
Digital Signature	Client Authentication, Secure Email
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Signature Only	Secure Email
Exchange User	Secure Email
IPSec	IP security IKE intermediate

- Open a session on ClientXX with a user and manually request a user certificate.



Issued To	Issued By
Pat Brunet	vlabs15-CA



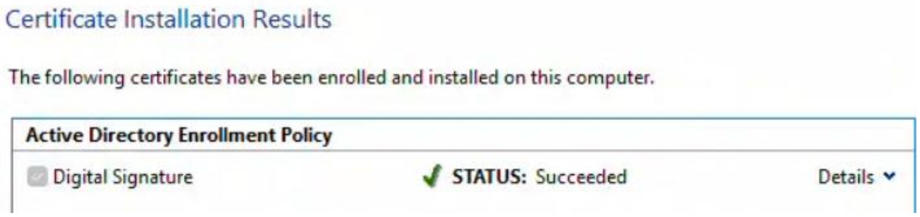
Request Certificates

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

Active Directory Enrollment Policy

☐ Basic EFS	**STATUS:** Available	Details
☑ Digital Signature	**STATUS:** Available	Details
☐ User	**STATUS:** Available	Details
☐ User-Auth	**STATUS:** Available	Details

☐ Show all templates

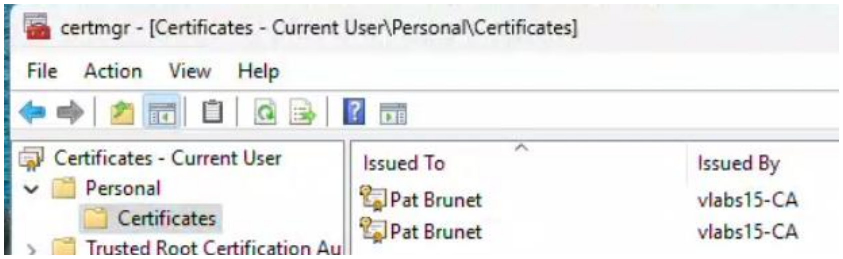


Certificate Installation Results

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

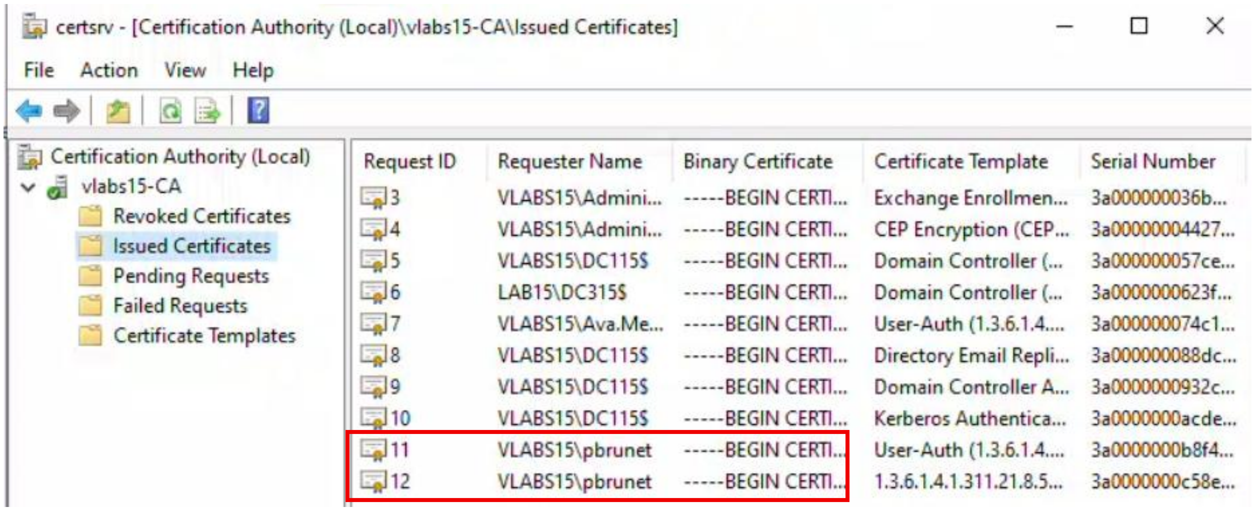
Active Directory Enrollment Policy

☑ Digital Signature	✓ **STATUS:** Succeeded	Details


certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au

Issued To	Issued By
Pat Brunet	vlabs15-CA
Pat Brunet	vlabs15-CA

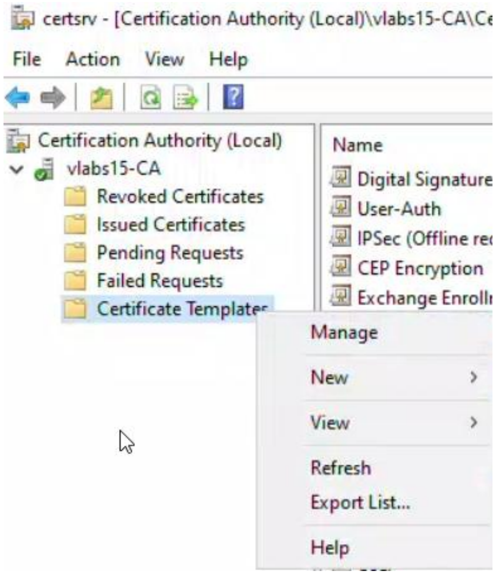
- Verify that he has received this certificate.

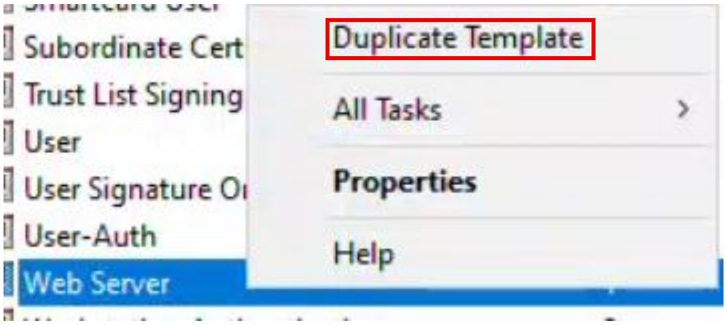


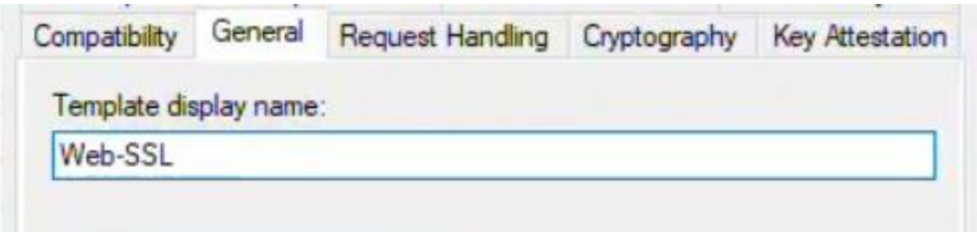
Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number
3	VLABS15\Admini...	-----BEGIN CERTI...	Exchange Enrollmen...	3a000000036b...
4	VLABS15\Admini...	-----BEGIN CERTI...	CEP Encryption (CEP...	3a00000004427...
5	VLABS15\DC115$	-----BEGIN CERTI...	Domain Controller (...	3a000000057ce...
6	LAB15\DC315$	-----BEGIN CERTI...	Domain Controller (...	3a0000000623f...
7	VLABS15\Ava.Me...	-----BEGIN CERTI...	User-Auth (1.3.6.1.4....	3a000000074c1...
8	VLABS15\DC115$	-----BEGIN CERTI...	Directory Email Repli...	3a000000088dc...
9	VLABS15\DC115$	-----BEGIN CERTI...	Domain Controller A...	3a0000000932c...
10	VLABS15\DC115$	-----BEGIN CERTI...	Kerberos Authentica...	3a0000000acde...
11	VLABS15\pbrunet	-----BEGIN CERTI...	User-Auth (1.3.6.1.4....	3a0000000b8f4...
12	VLABS15\pbrunet	-----BEGIN CERTI...	1.3.6.1.4.1.311.21.8.5...	3a0000000c58e...

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

- Create an SSL certificate on the Enterprise CA.

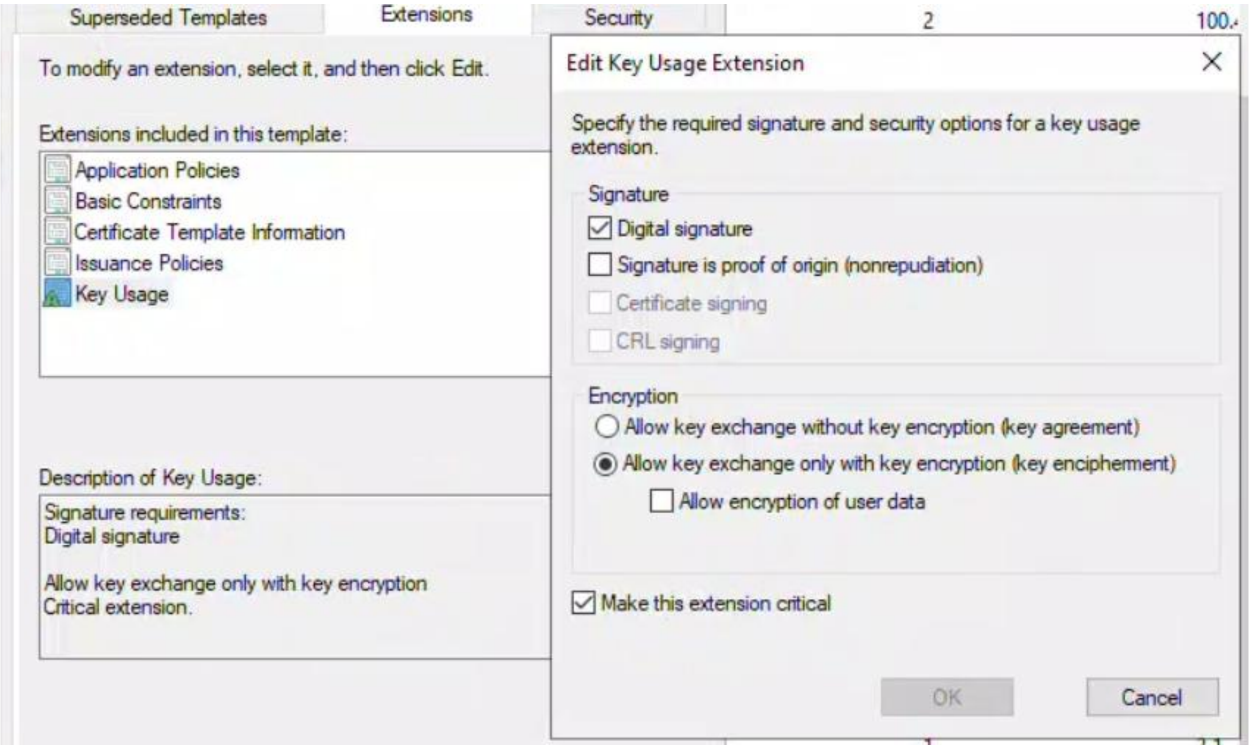






Template display name:

Web-SSL



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

Description of Key Usage:

Signature requirements:
Digital signature

Allow key exchange only with key encryption
Critical extension.

Edit Key Usage Extension

Specify the required signature and security options for a key usage extension.

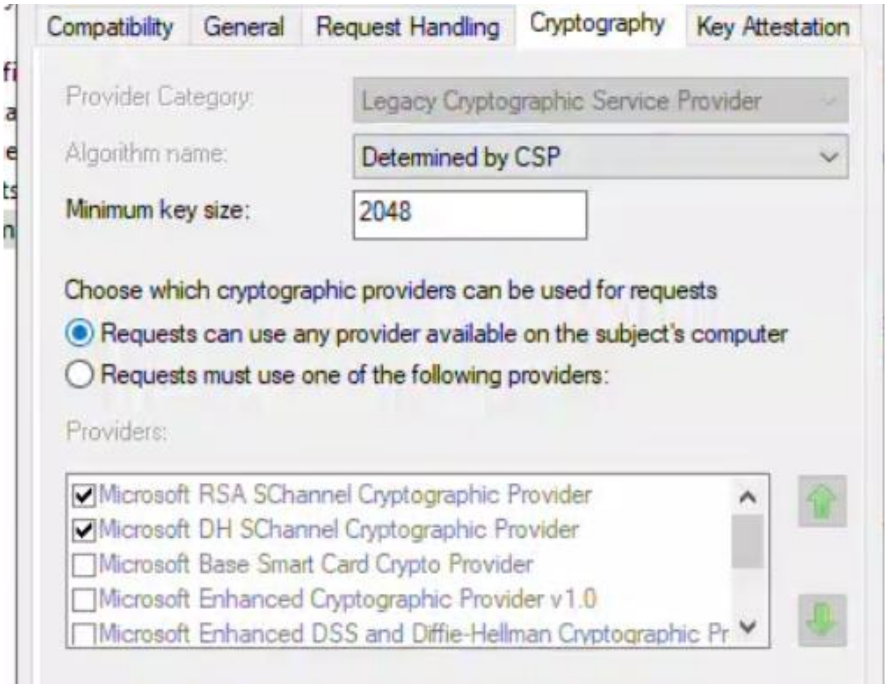
Signature

☑ Digital signature
□ Signature is proof of origin (nonrepudiation)
□ Certificate signing
□ CRL signing

Encryption

○ Allow key exchange without key encryption (key agreement)
● Allow key exchange only with key encryption (key encipherment)
□ Allow encryption of user data

☑ Make this extension critical



Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

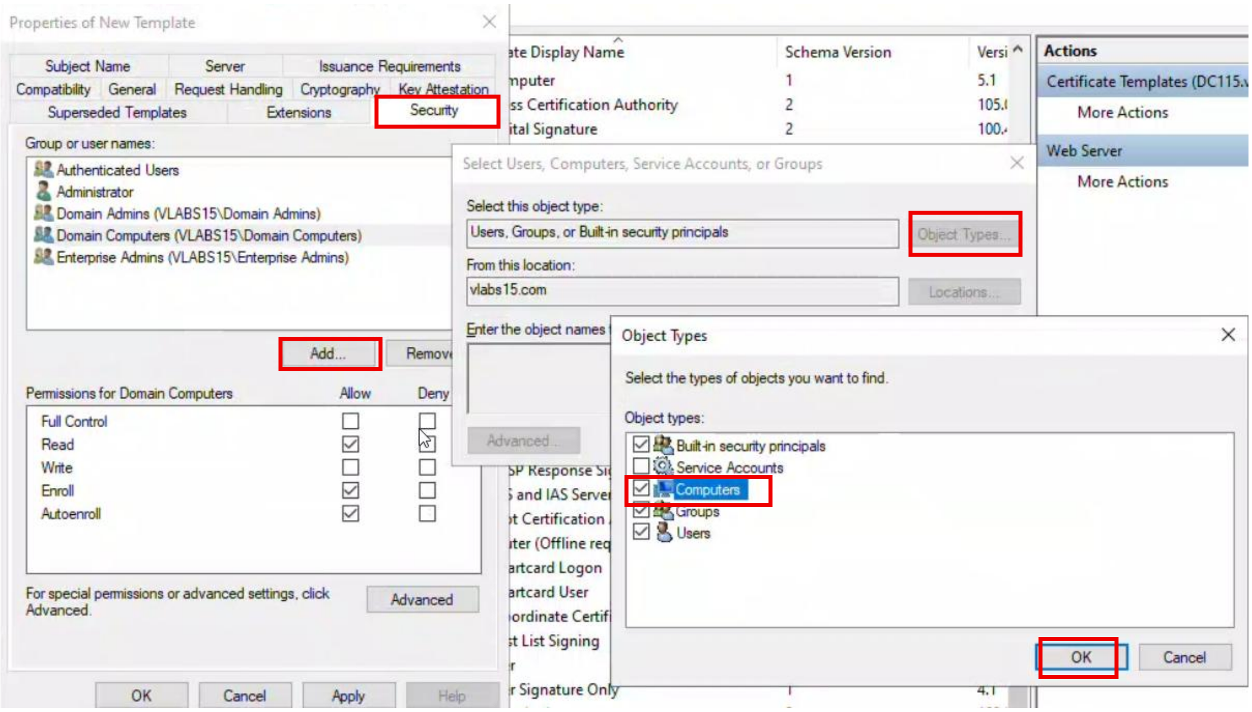
Minimum key size: 2048

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



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
- Domain Admins (VLABS15\Domain Admins)
- Domain Computers (VLABS15\Domain Computers)
- Enterprise Admins (VLABS15\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

ate Display Name	Schema Version	Versi
nputer	1	5.1
ss Certification Authority	2	105.(
ital Signature	2	100.4
SP Response Si		
S and IAS Server		
ot Certification		
iter (Offline req		
artcard Logon		
artcard User		
ordinate Certifi		
st List Signing		
r		
r Signature Only	1	4.1

Actions

Certificate Templates (DC115.v

More Actions

Web Server

More Actions

Select Users, Computers, Service Accounts, or Groups

Select this object type:

Users, Groups, or Built-in security principals

Object Types...

From this location:

vlabs15.com

Locations...

Enter the object names t

Advanced...

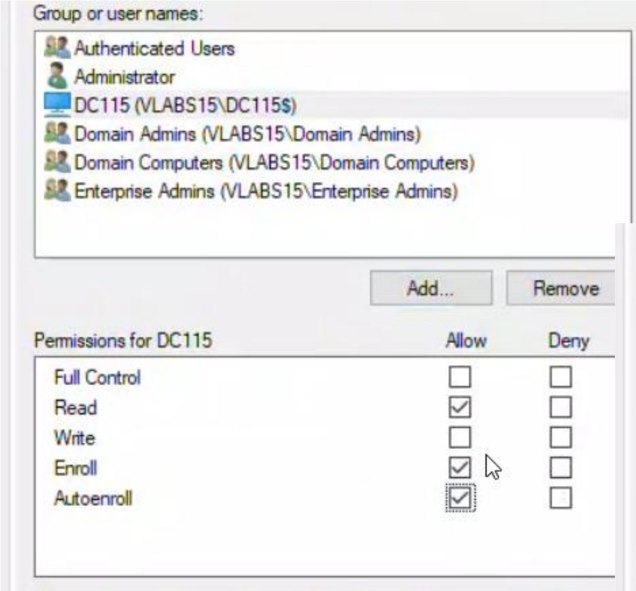
Object Types

Select the types of objects you want to find.

Object types:

- ☑ Built-in security principals
- □ Service Accounts
- ☑ Computers
- ☑ Groups
- ☑ Users

OK | Cancel

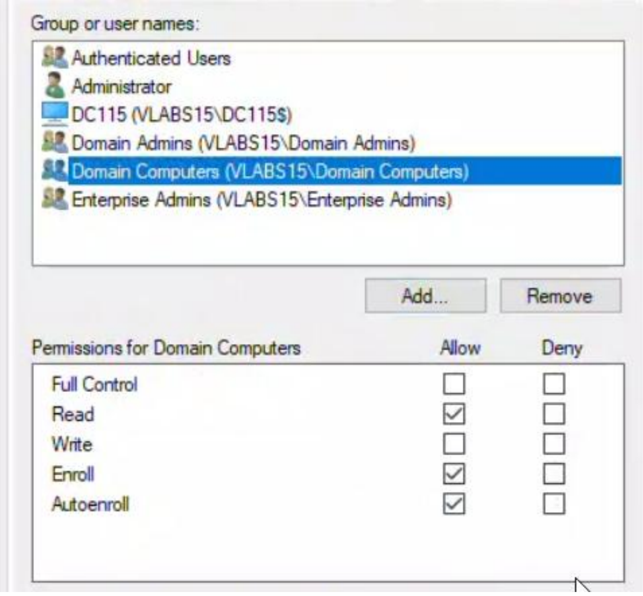


Group or user names:

- Authenticated Users
- Administrator
- DC115 (VLABS15\DC115$)
- Domain Admins (VLABS15\Domain Admins)
- Domain Computers (VLABS15\Domain Computers)
- Enterprise Admins (VLABS15\Enterprise Admins)

Add... | Remove

Permissions for DC115	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	☑	□

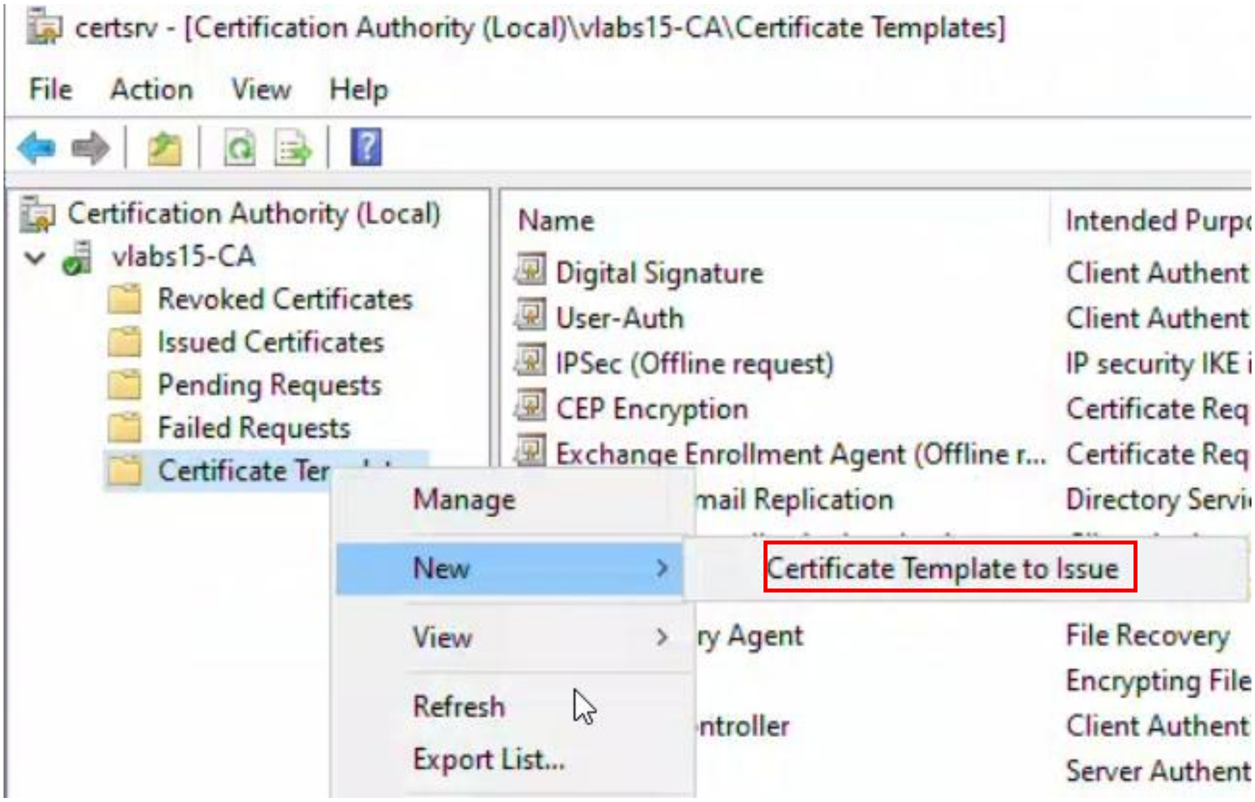


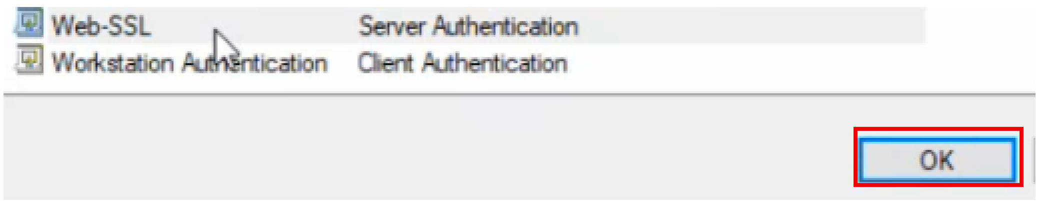
Group or user names:

- Authenticated Users
- Administrator
- DC115 (VLABS15\DC115$)
- Domain Admins (VLABS15\Domain Admins)
- Domain Computers (VLABS15\Domain Computers)
- Enterprise Admins (VLABS15\Enterprise Admins)

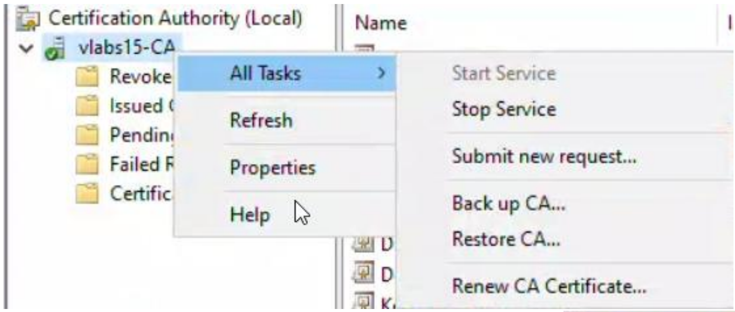
Add... | Remove

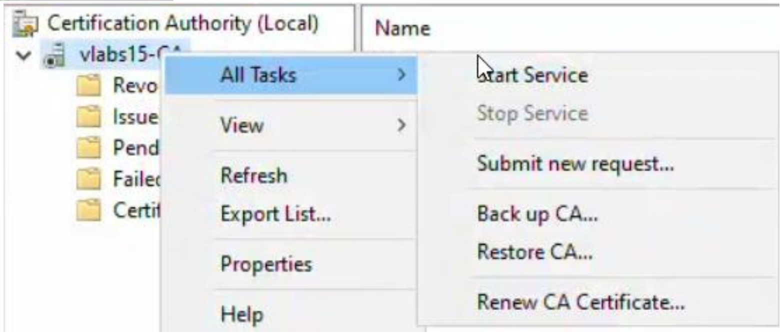
Permissions for Domain Computers	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	☑	□





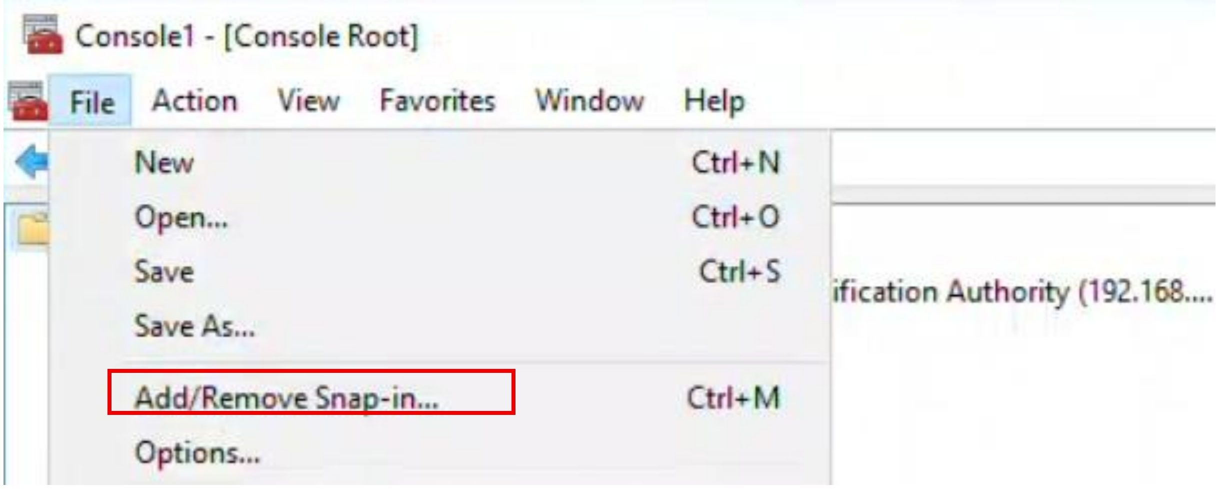
Restart the CA service (Stop / Start)

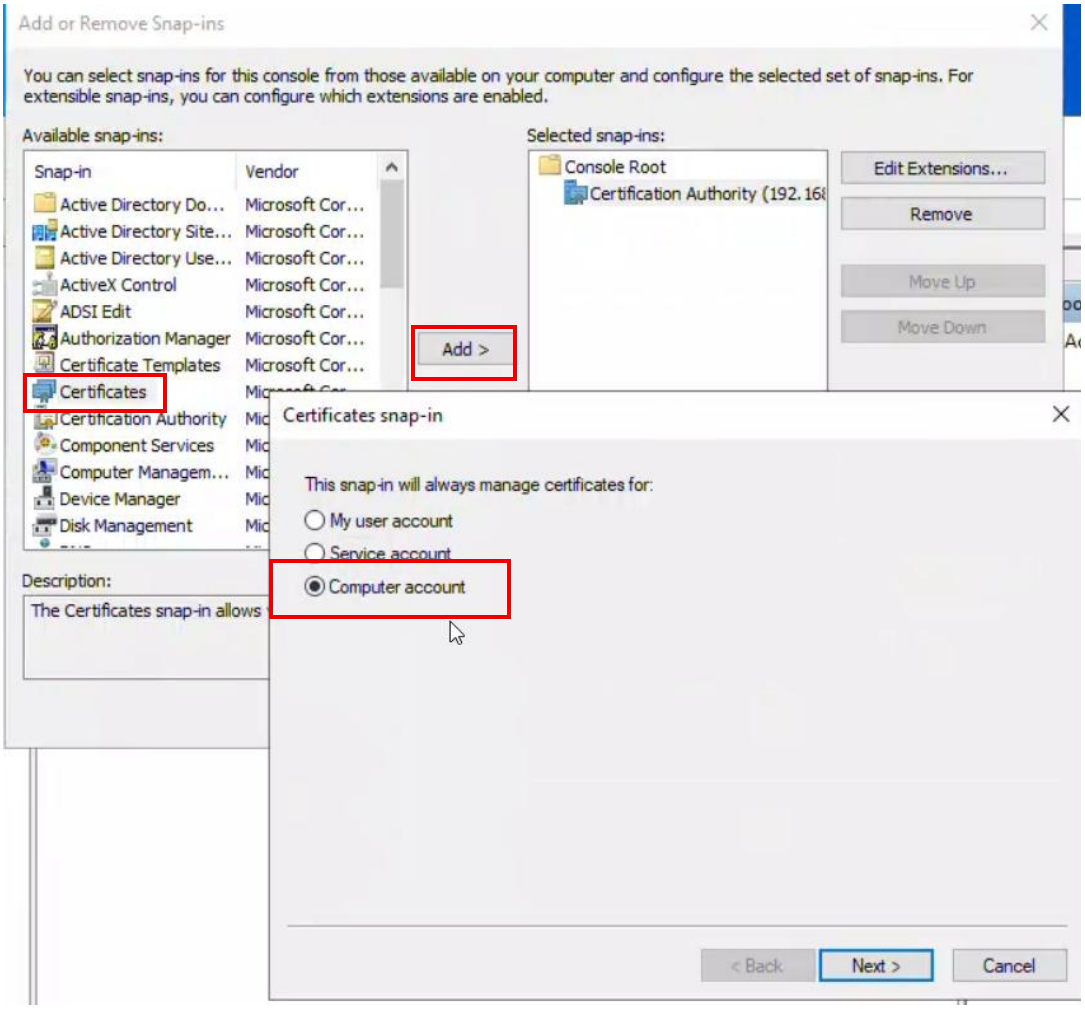




- Request and issue an SSL/TLS Certificate for dc1XX.vlabsXX.com.

Open mmc




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
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Mic
Component Services	Mic
Computer Managem...	Mic
Device Manager	Mic
Disk Management	Mic

Selected snap-ins:

Console Root
Certification Authority (192.168

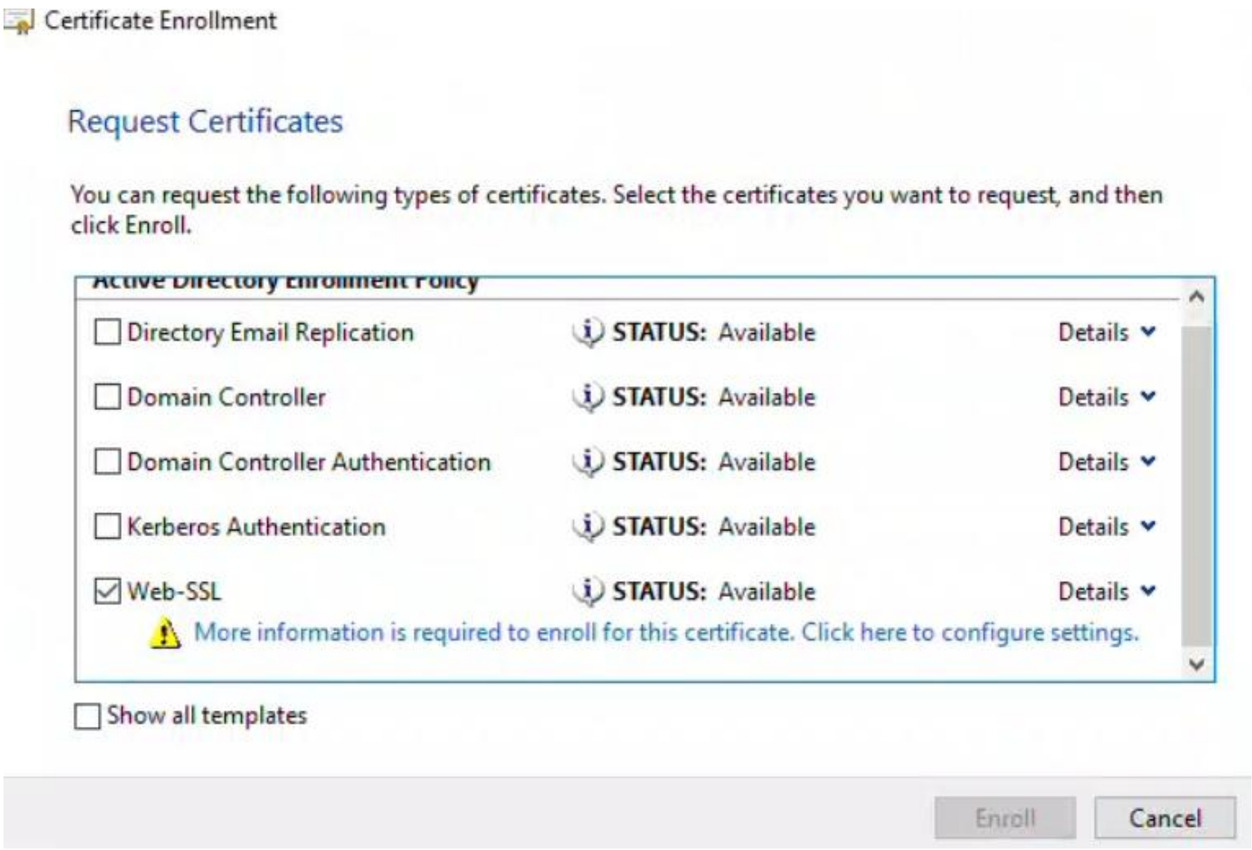
Description:

The Certificates snap-in allows

Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account



Certificate Enrollment

Request Certificates

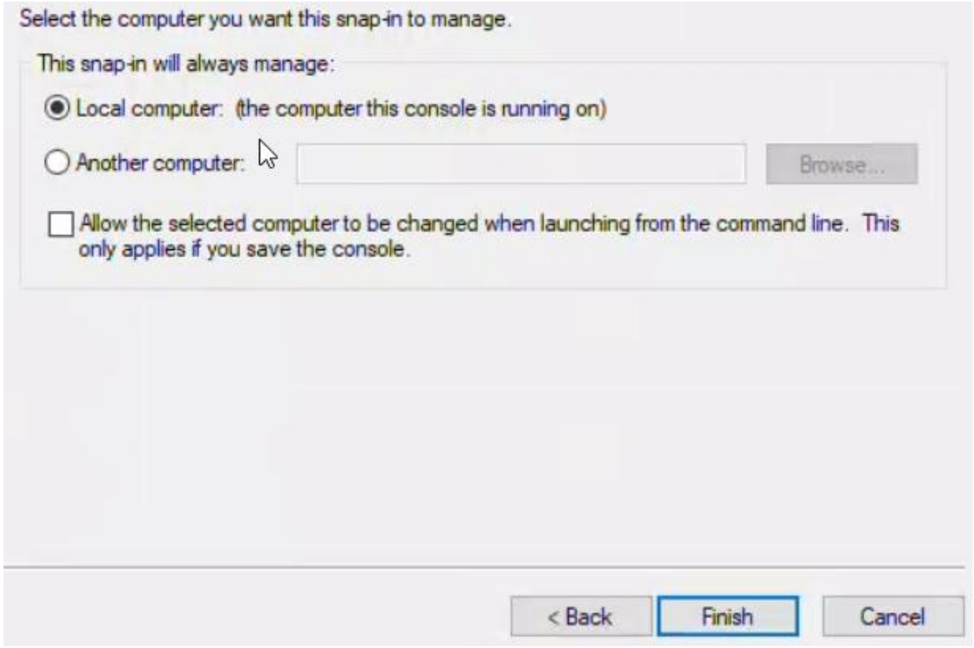
You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

□ Directory Email Replication	**STATUS:** Available	Details
□ Domain Controller	**STATUS:** Available	Details
□ Domain Controller Authentication	**STATUS:** Available	Details
□ Kerberos Authentication	**STATUS:** Available	Details
☑ Web-SSL	**STATUS:** Available	Details

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

□ Show all templates



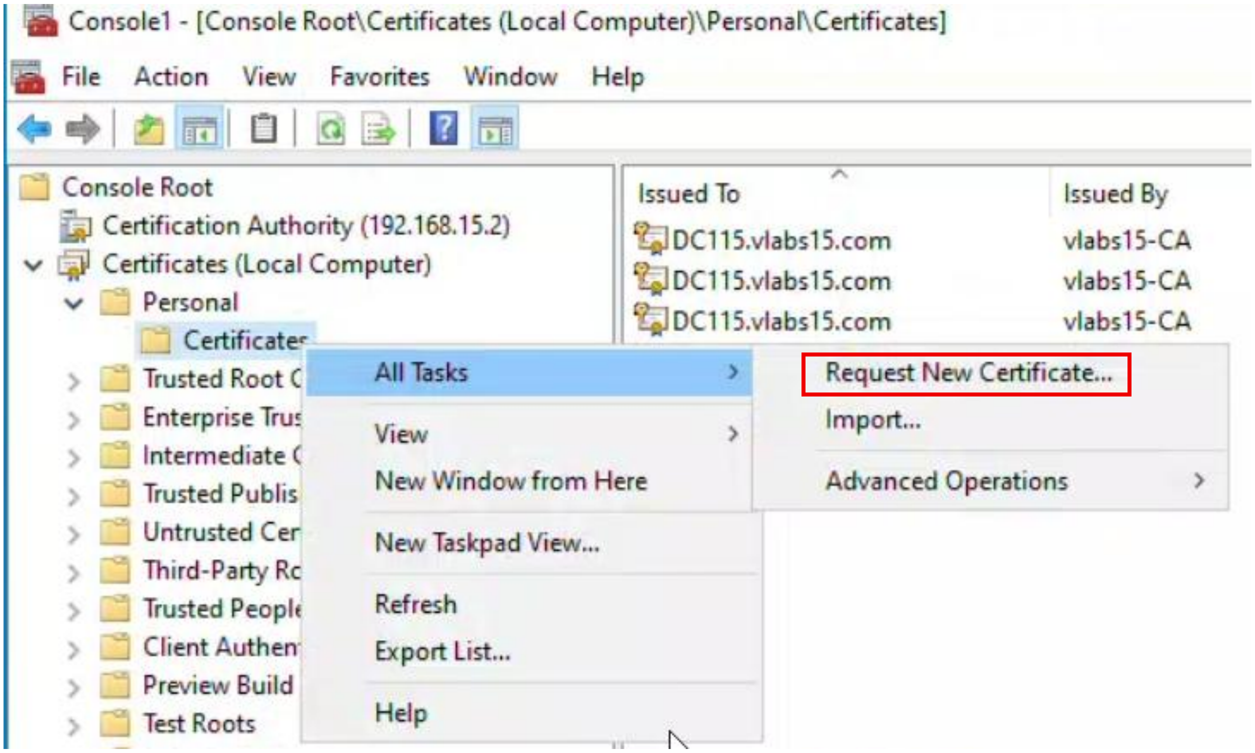
Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

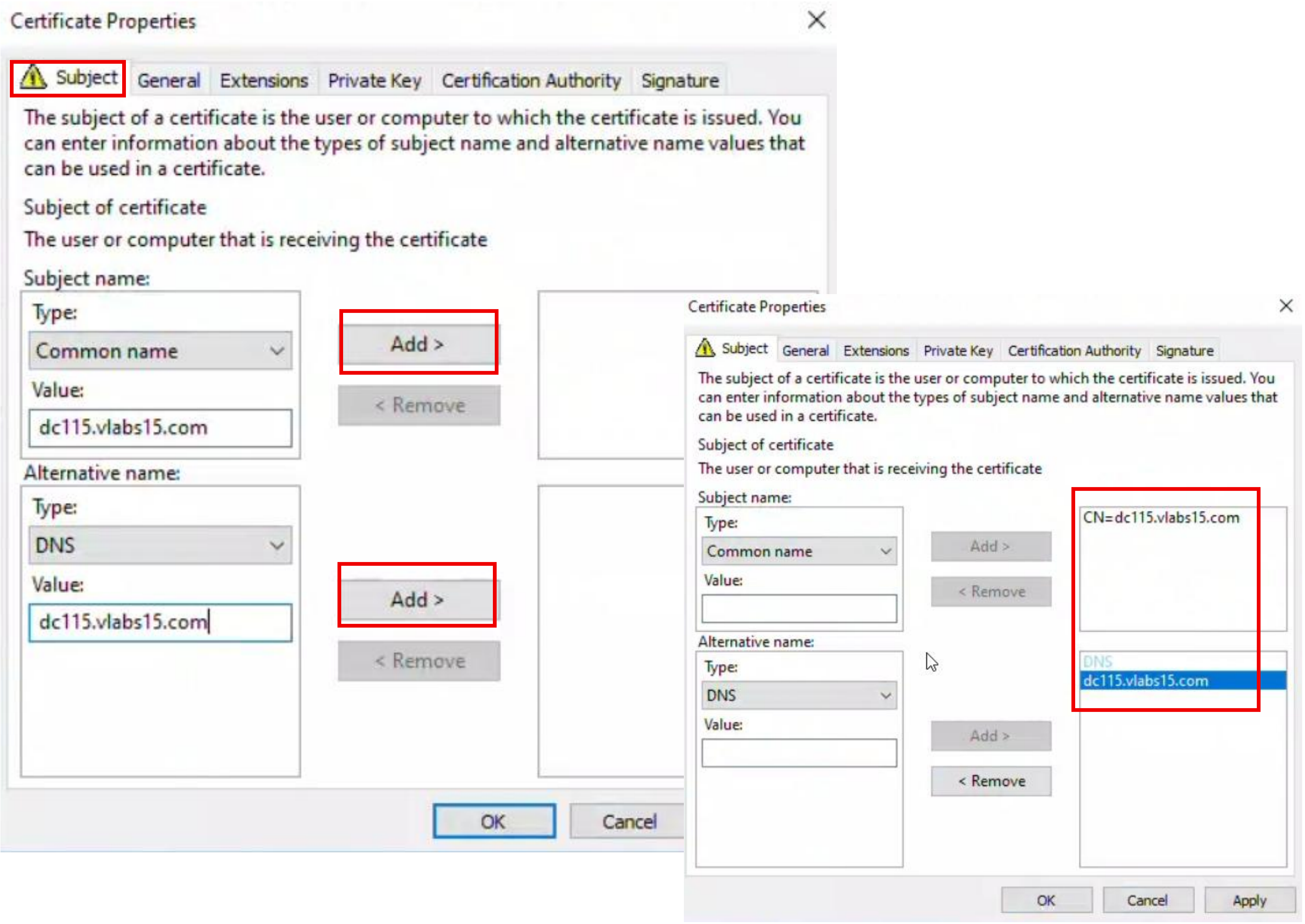
○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.



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

Issued To	Issued By
DC115.vlabs15.com	vlabs15-CA
DC115.vlabs15.com	vlabs15-CA
DC115.vlabs15.com	vlabs15-CA



Certificate Properties

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: dc115.vlabs15.com

Alternative name:

Type: DNS

Value: dc115.vlabs15.com

Certificate Properties

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:

Alternative name:

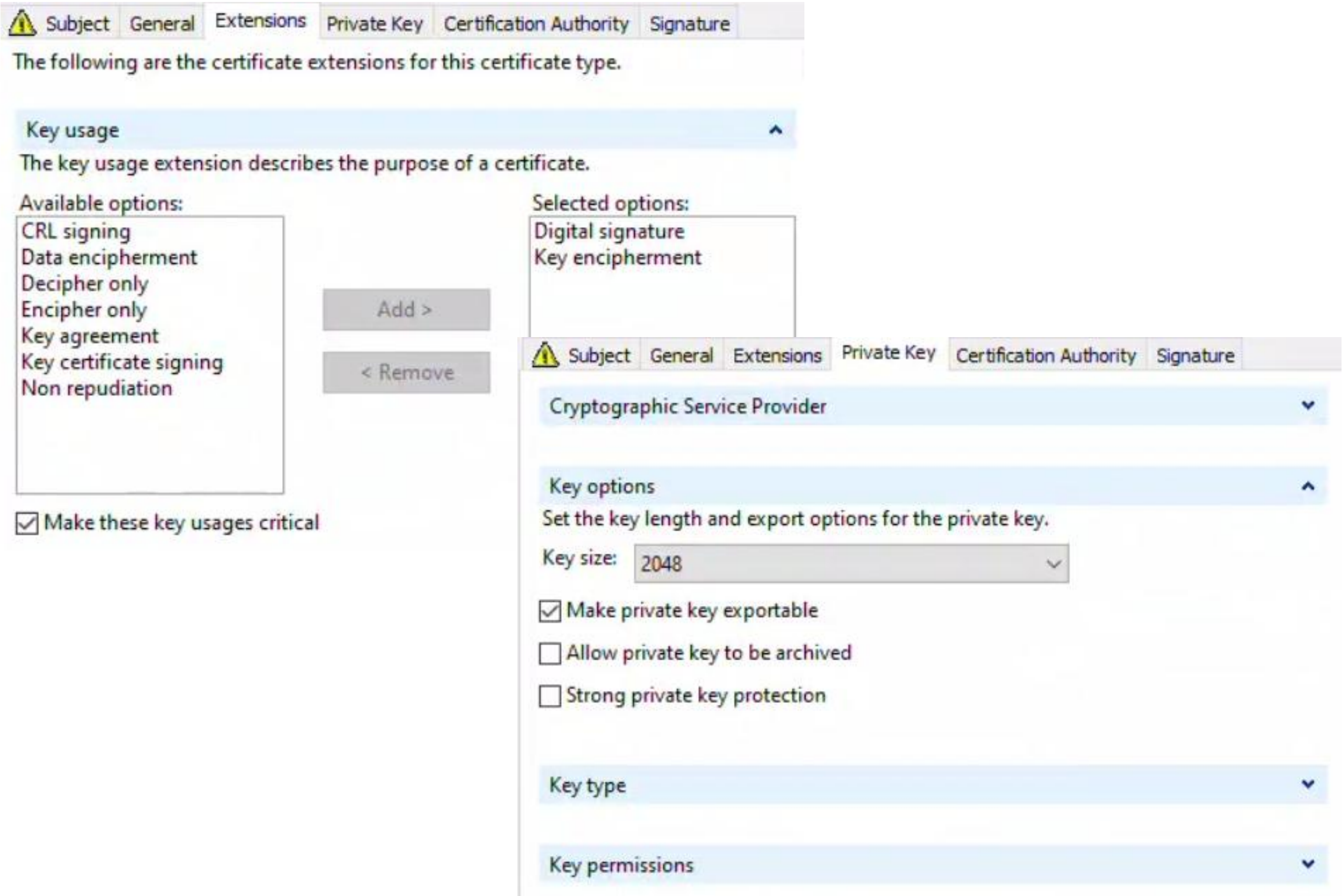
Type: DNS

Value:

CN=dc115.vlabs15.com

DNS
dc115.vlabs15.com

Make sure these tabs are correctly filled, then OK and Enroll.



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

Selected options:

- Digital signature
- Key encipherment

☑ Make these key usages critical

Key options

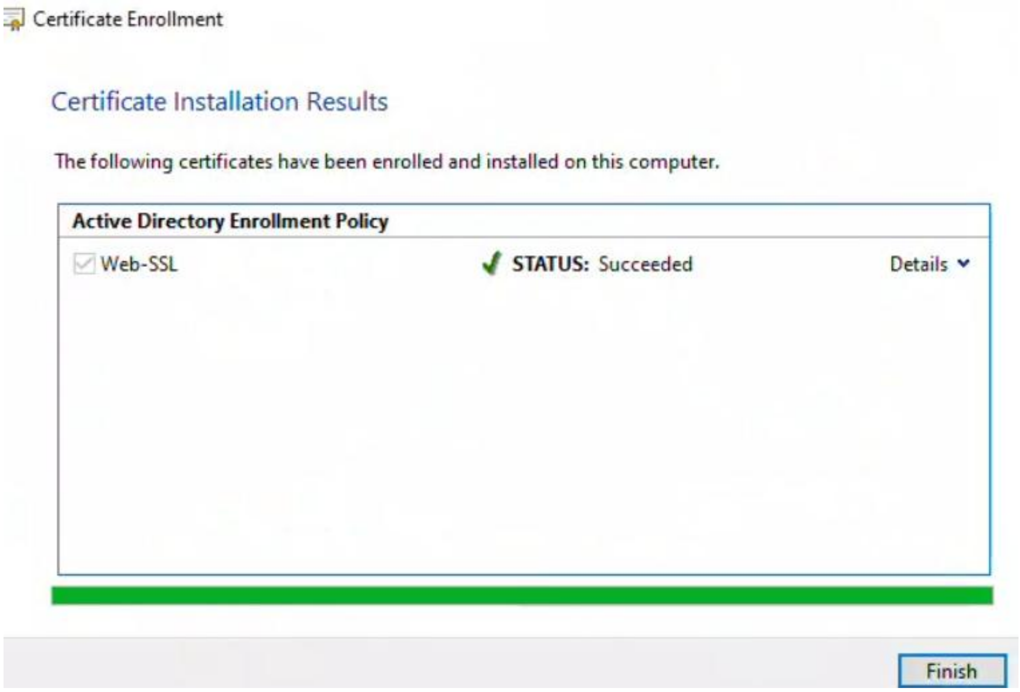
Set the key length and export options for the private key.

Key size: 2048

☑ Make private key exportable

☐ Allow private key to be archived

☐ Strong private key protection



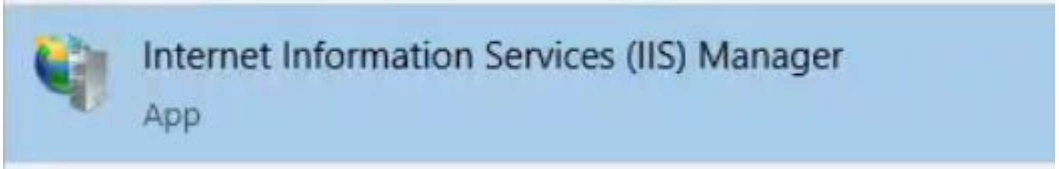
Certificate Installation Results

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

Active Directory Enrollment Policy

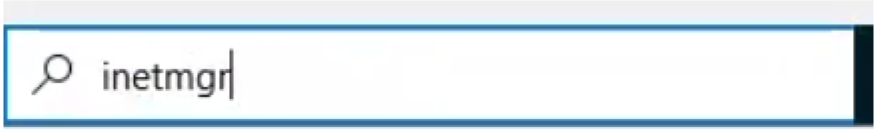
☑ Web-SSL ✓ **STATUS:** Succeeded

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

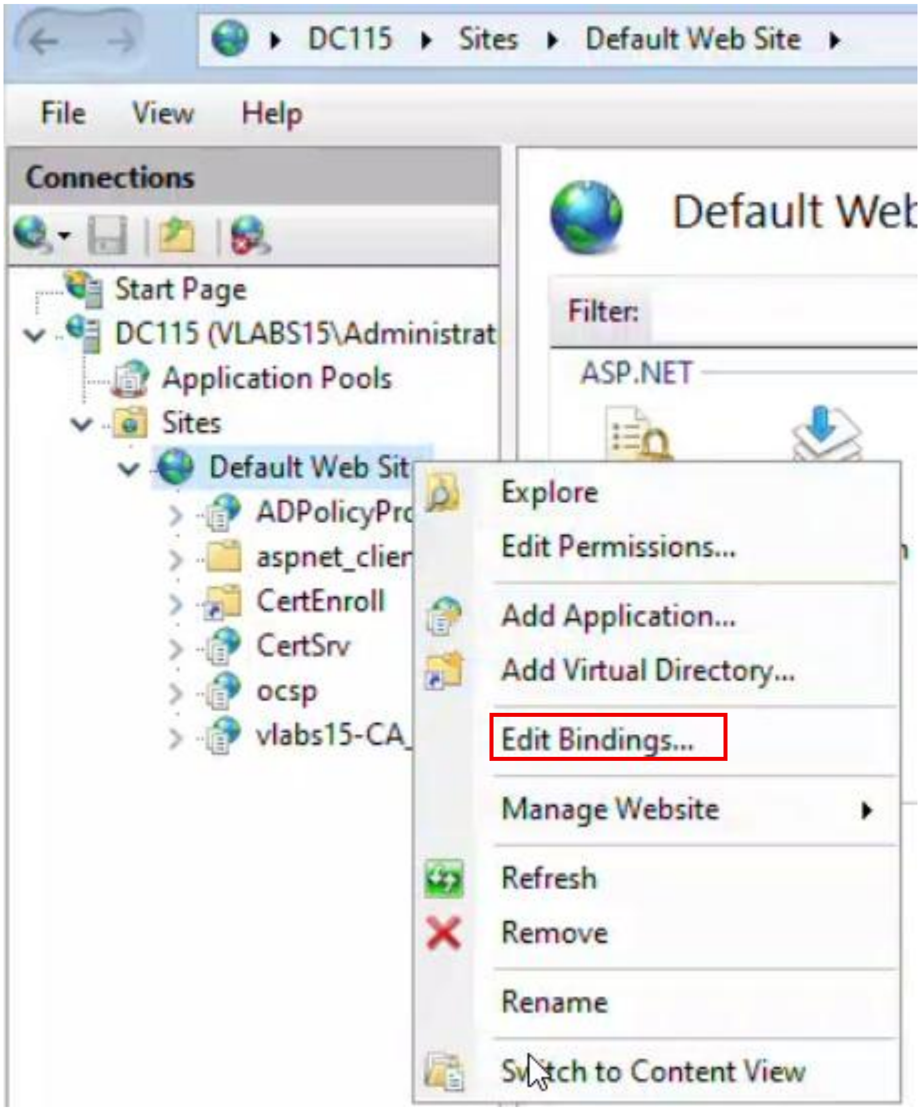


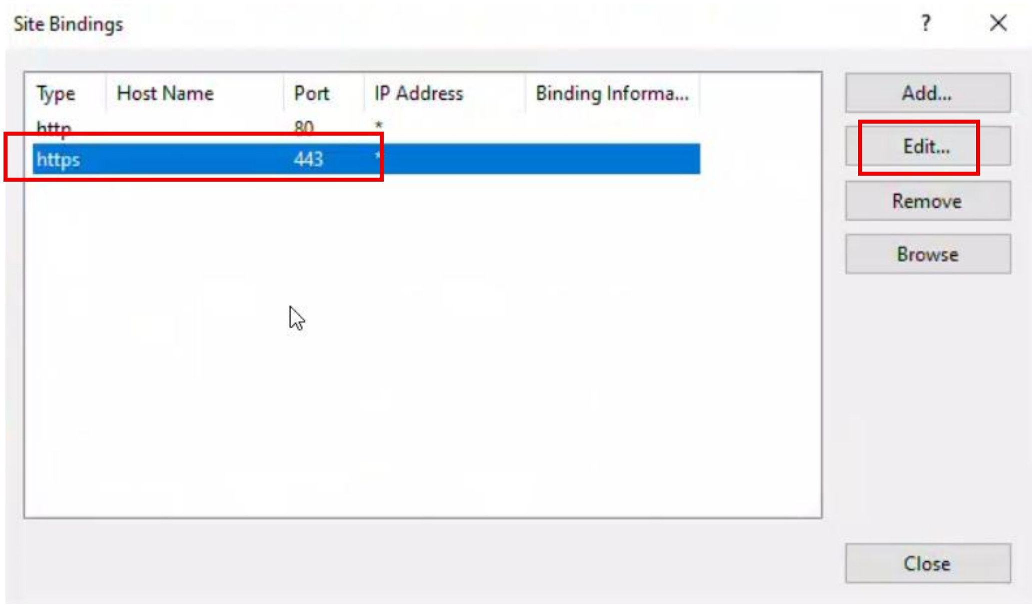
Internet Information Services (IIS) Manager

App



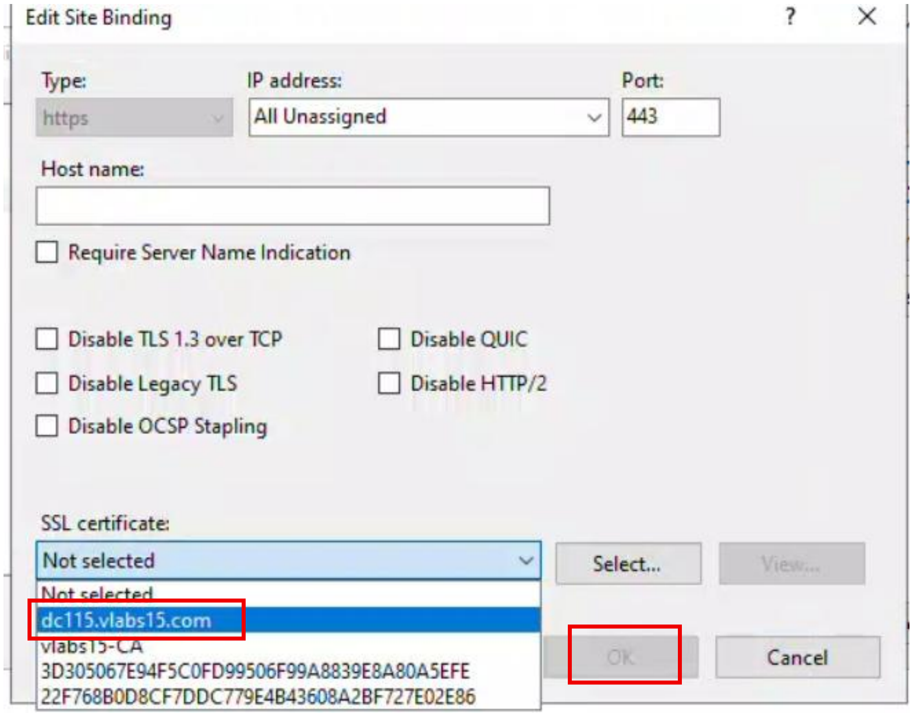
inetmgr





Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	



Edit Site Binding

Type: https

IP address: All Unassigned

Port: 443

Host name:

□ Require Server Name Indication

□ Disable TLS 1.3 over TCP

□ Disable QUIC

□ Disable Legacy TLS

□ Disable HTTP/2

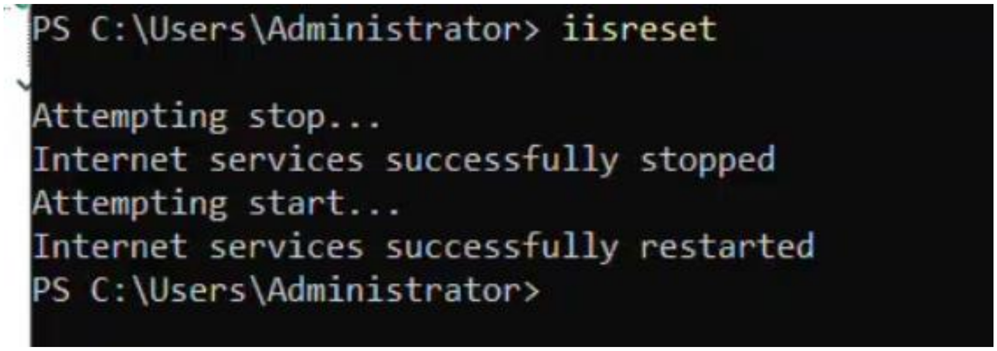
□ Disable OCSP Stapling

SSL certificate: Not selected

- Not selected
- dc115.vlabs15.com
- vlabs15-CA
- 3D305067E94F5C0FD99506F99A8839E8A80A5EFE
- 22F768B0D8CF7DDC779E4B43608A2BF727E02E86

Reset the service

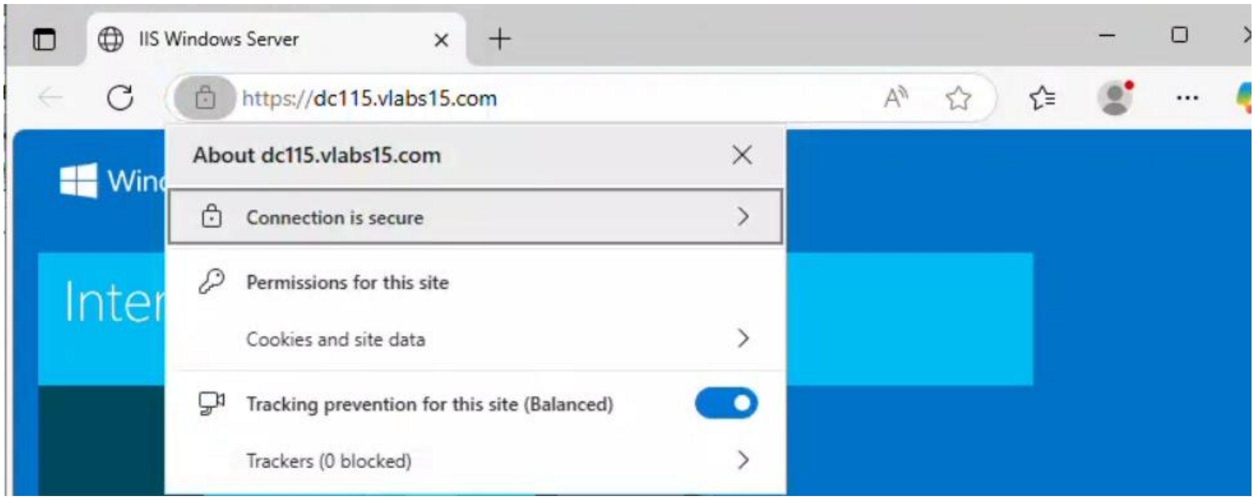
iireset



```
PS C:\Users\Administrator> iisreset

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
PS C:\Users\Administrator>
```

- Test and verify HTTPS access to dc1XX.vlabsXX.com.



About dc115.vlabs15.com

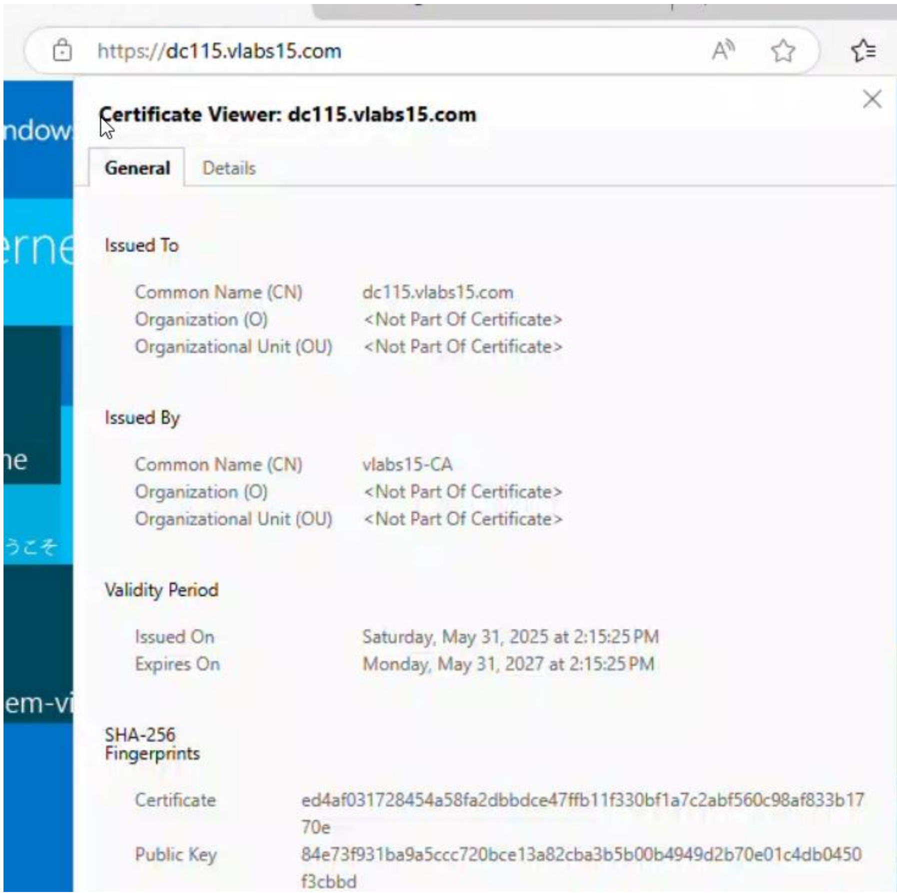
Connection is secure

Permissions for this site

Cookies and site data

Tracking prevention for this site (Balanced)

Trackers (0 blocked)



Certificate Viewer: dc115.vlabs15.com

General Details

Issued To

Common Name (CN)	dc115.vlabs15.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	vlabs15-CA
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Saturday, May 31, 2025 at 2:15:25 PM
Expires On	Monday, May 31, 2027 at 2:15:25 PM

SHA-256 Fingerprints

Certificate	ed4af031728454a58fa2dbbdce47ffb11f330bf1a7c2abf560c98af833b1770e
Public Key	84e73f931ba9a5ccc720bce13a82cba3b5b00b4949d2b70e01c4db0450f3cbbd