5/27/2025

Assignment 3

Part 1

Mohammed, Laetitia, 0931512

NETWORK INSTALLATION AND ADMINISTRATION II

Contents

Task 1: Deploy an Offline Standalone Root CA on DC212

Demote **DC212** and remove it from the domain

Rename DC212 to **Root12CA.**

Install **Active Directory Certificate Services (AD CS)** on Root12CA.

Configure **Root12CA** as a **Standalone Root CA**

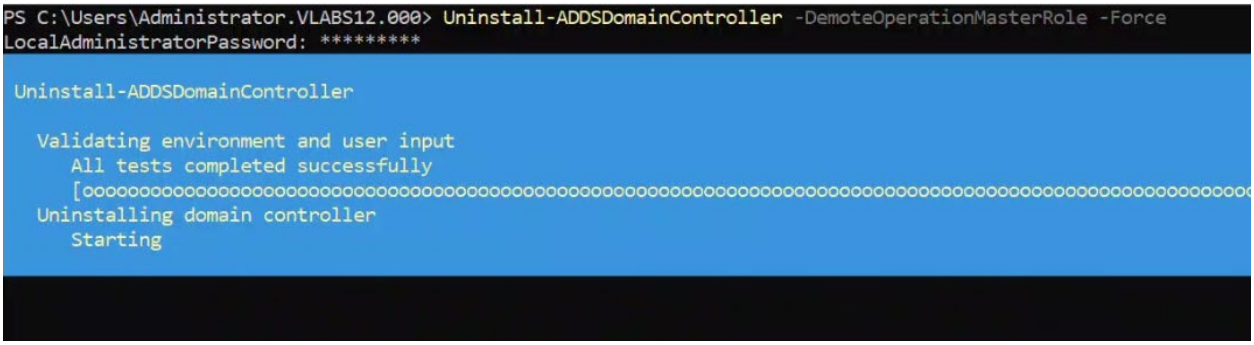
Configure the Server Registry keys

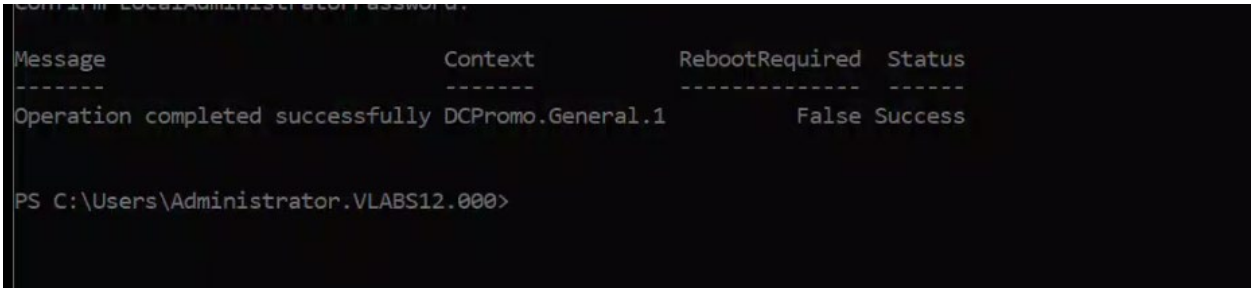
Modify the **CRL Distribution Points (CDP)** and **Authority Information Access (AIA)** settings from **DC212** to **DC112**

Copy the **Root CA Certificate, Certificate Revocation List (CRL)** and **CA private key** to **DC112**

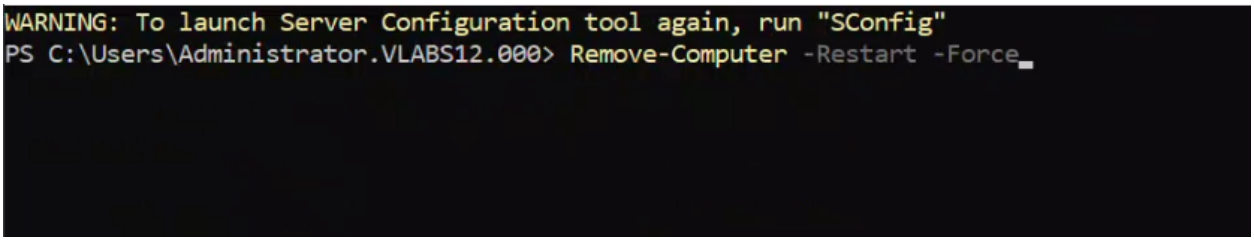
This task will set up a secure root certificate authority on server DC212 by removing it from the network domain, renaming it to Root12CA, and installing the necessary certificate services. It will configure the server to issue the main security certificates, adjust its settings, update where certificate information is stored, and share the certificates and security keys with another server, DC112.

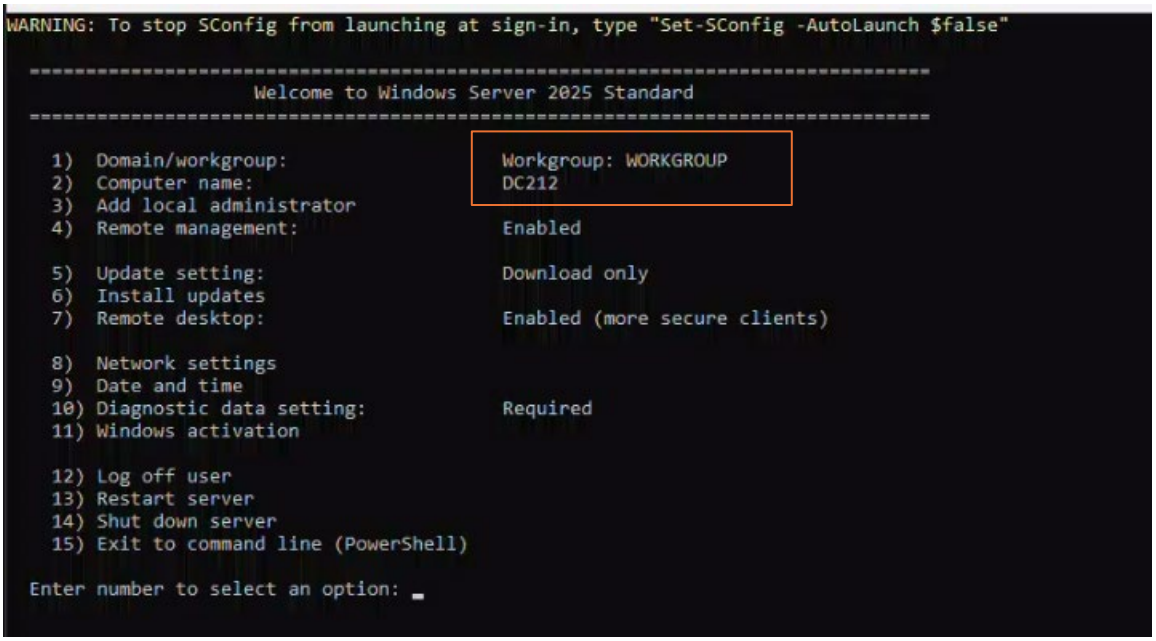
Demote DC212 and remove it from the domain using PowerShell



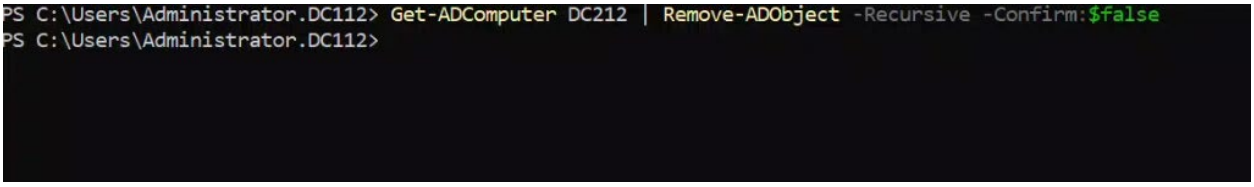


Wait for the server to reboot after demoting and then use this command to remove it from the domain vlabs12.com

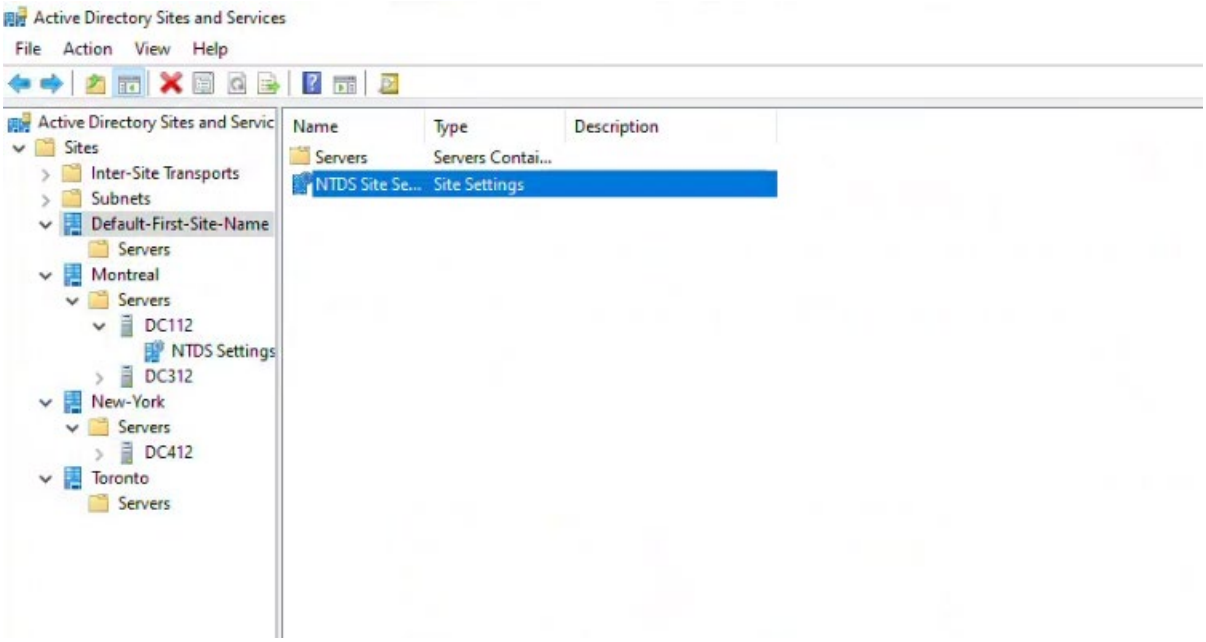




On DC112, use this command to remove the DC212 computer object from AD



To remove DC212 from AD sites and services, the powershell command was not working for me. So I did it graphically. Found DC212 in Montreal → right clicked → delete. Looked around in all other sites/servers/settings for remnants of DC212 and did not find any.



Rename DC212 to Root12CA

Run the following commands on DC212 to set up hostname:

```
WARNING: To launch Server Configuration tool again, run "SConfig"
PS C:\Users\Administrator.DC212.000> Rename-Computer -NewName "Root12CA"
WARNING: The changes will take effect after you restart the computer DC212.
PS C:\Users\Administrator.DC212.000> Restart-Computer
```

```
  1)  Domain/workgroup:                  Workgroup: WORKGROUP
  2)  Computer name:                     ROOT12CA
  3)  Add local administrator
  4)  Remote management:                 Enabled

  5)  Update setting:                    Download only
  6)  Install updates
  7)  Remote desktop:                    Enabled (more secure clients)

  8)  Network settings
  9)  Date and time
  10) Diagnostic data setting:           Required
  11) Windows activation

  12) Log off user
  13) Restart server
  14) Shut down server
  15) Exit to command line (PowerShell)

Enter number to select an option:
```

Install Active Directory Certificate Services (AD CS) on Root12CA

Add-WindowsFeature Adcs-Cert-Authority

```
PS C:\Users\Administrator.DC212.000> Add-WindowsFeature Adcs-Cert-Authority

Collecting data...
   10%
   [ooooooooo
```

```
Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Certificate Services, Ce...

PS C:\Users\Administrator.DC212.000>
```

Get-WindowsFeature AD-Certificate

```
PS C:\Users\Administrator.DC212.000> Get-WindowsFeature AD-Certificate

Display Name                                            Name                       Install State
------------                                            ----                       -------------
[X] Active Directory Certificate Services               AD-Certificate                 Installed


PS C:\Users\Administrator.DC212.000>
```

Configure Root12CA as a Standalone Root CA

Install-AdcsCertificationAuthority -CAType StandaloneRootCA -CACommonName "Root12CA" -KeyLength 4096 -HashAlgorithm SHA256 -CryptoProviderName "RSA#Microsoft Software Key Storage Provider"

Type: A (For Yes to all)

```
PS C:\Users\Administrator.DC212.000> Install-AdcsCertificationAuthority -CAType StandaloneRootCA -CACommonName "Root12CA" -KeyLength
derName "RSA#Microsoft Software Key Storage Provider"

Confirm
Are you sure you want to perform this action?
Performing the operation "Install-AdcsCertificationAuthority" on target "ROOT12CA".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A

ErrorId ErrorString
------- -----------
      0


PS C:\Users\Administrator.DC212.000>
```

```
PS C:\Users\Administrator> certutil
Entry 0: (Local)
  Name:                         "Root12CA"
  Organizational Unit:          ""
  Organization:                 ""
  Locality:                     ""
  State:                        ""
  Country/region:               ""
  Config:                       "Root12CA\Root12CA"
  Exchange Certificate:         ""
  Signature Certificate:        "Root12CA_Root12CA.crt"
  Description:                  ""
  Server:                       "Root12CA"
  Authority:                    "Root12CA"
  Sanitized Name:               "Root12CA"
  Short Name:                   "Root12CA"
  Sanitized Short Name:         "Root12CA"
  Flags:                        "12"
  Web Enrollment Servers:       ""
CertUtil: -dump command completed successfully.
```

Configure the Server Registry keys

certutil -setreg CA\ValidityPeriod "Years"

```
PS C:\Users\Administrator> certutil -setreg CA\ValidityPeriod "Years"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Root12CA\ValidityPeriod:

Old Value:
  ValidityPeriod REG_SZ = Years

New Value:
  ValidityPeriod REG_SZ = Years
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
PS C:\Users\Administrator>
```

certutil -setreg CA\ValidityPeriodUnits 5

```
PS C:\Users\Administrator> certutil -setreg CA\ValidityPeriodUnits 5
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Root12CA\ValidityPeriodUnits:

Old Value:
  ValidityPeriodUnits REG_DWORD = 1

New Value:
  ValidityPeriodUnits REG_DWORD = 5
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
PS C:\Users\Administrator>
```

certutil -setreg CA\DSConfigDN "CN=Configuration,DC=vlabs12,DC=com"

```
PS C:\Users\Administrator> certutil -setreg CA\DSConfigDN "CN=Configuration,DC=vlabs12,DC=com"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Root12CA\DSConfigDN:

New Value:
  DSConfigDN REG_SZ = CN=Configuration,DC=vlabs12,DC=com
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
PS C:\Users\Administrator>
```

certutil -setreg CA\DSDomainDN "DC=vlabs12,DC=com"

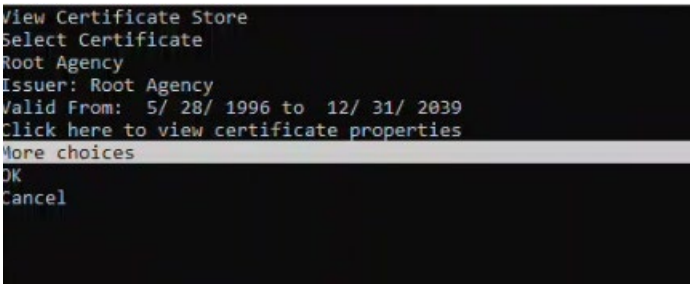
```
PS C:\Users\Administrator> certutil -setreg CA\DSDomainDN "DC=vlabs12,DC=com"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Root12CA\DSDomainDN:

New Value:
  DSDomainDN REG_SZ = DC=vlabs12,DC=com
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
PS C:\Users\Administrator>
```

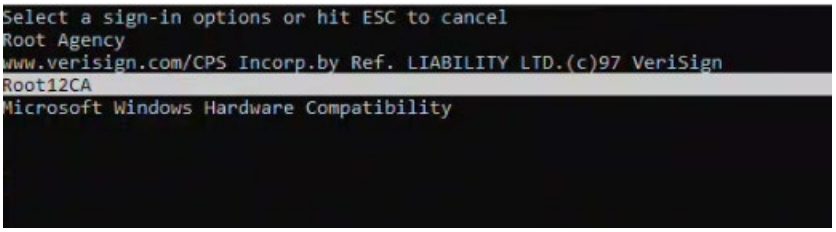
Restart-Service certsvc

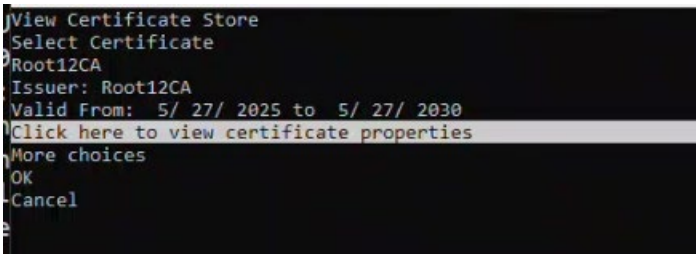
```
PS C:\Users\Administrator> Restart-Service certsvc
PS C:\Users\Administrator>
```

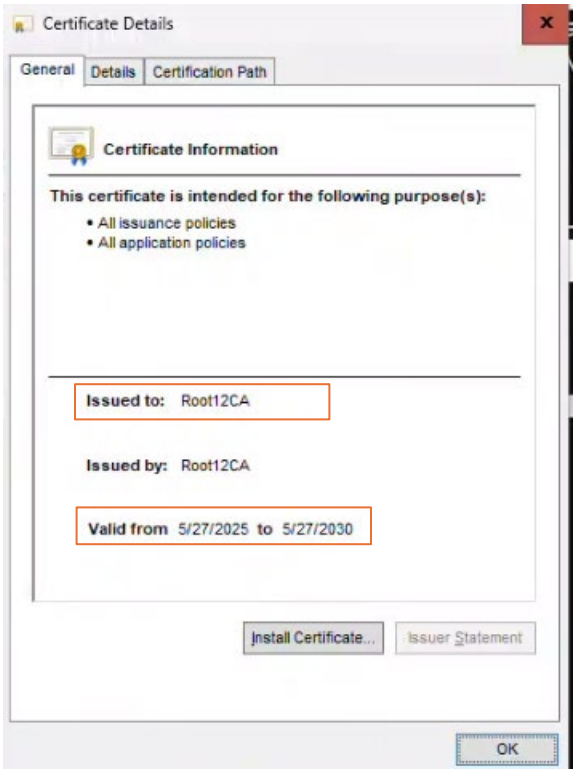
View the new Server Root12CA certificate:

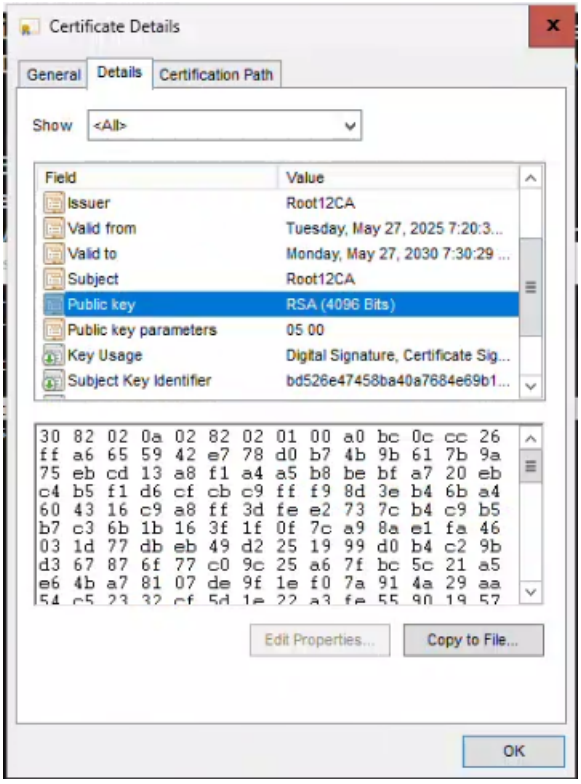
certutil -viewstore CA








Certificate Details
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Issued to: Root12CA
Issued by: Root12CA
Valid from 5/27/2025 to 5/27/2030
Install Certificate...
Issuer Statement
OK


Certificate Details
General
Details
Certification Path
Show
<All>
Field
Value
Issuer
Root12CA
Valid from
Tuesday, May 27, 2025 7:20:3...
Valid to
Monday, May 27, 2030 7:30:29 ...
Subject
Root12CA
Public key
RSA (4096 Bits)
Public key parameters
05 00
Key Usage
Digital Signature, Certificate Sig...
Subject Key Identifier
bd526e47458ba40a7684e69b1...
30 82 02 0a 02 82 02 01 00 a0 bc 0c cc 26
ff a6 65 59 42 e7 78 d0 b7 4b 9b 61 7b 9a
75 eb cd 13 a8 f1 a4 a5 b8 be bf a7 20 eb
c4 b5 f1 d6 cf cb c9 ff f9 8d 3e b4 6b a4
60 43 16 c9 a8 ff 3d fe e2 73 7c b4 c9 b5
b7 c3 6b 1b 16 3f 1f 0f 7c a9 8a e1 fa 46
03 1d 77 db eb 49 d2 25 19 99 d0 b4 c2 9b
d3 67 87 6f 77 c0 9c 25 a6 7f bc 5c 21 a5
e6 4b a7 81 07 de 9f 1e f0 7a 91 4a 29 aa
Edit Properties...
Copy to File...
OK

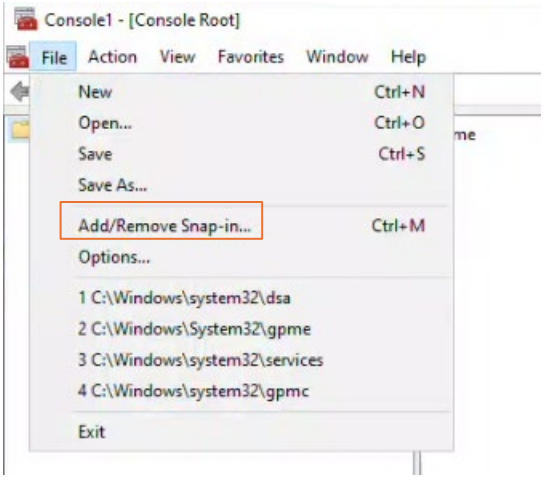
Modify the CRL Distribution Points (CDP) and Authority Information Access (AIA) settings from DC212 to DC112.

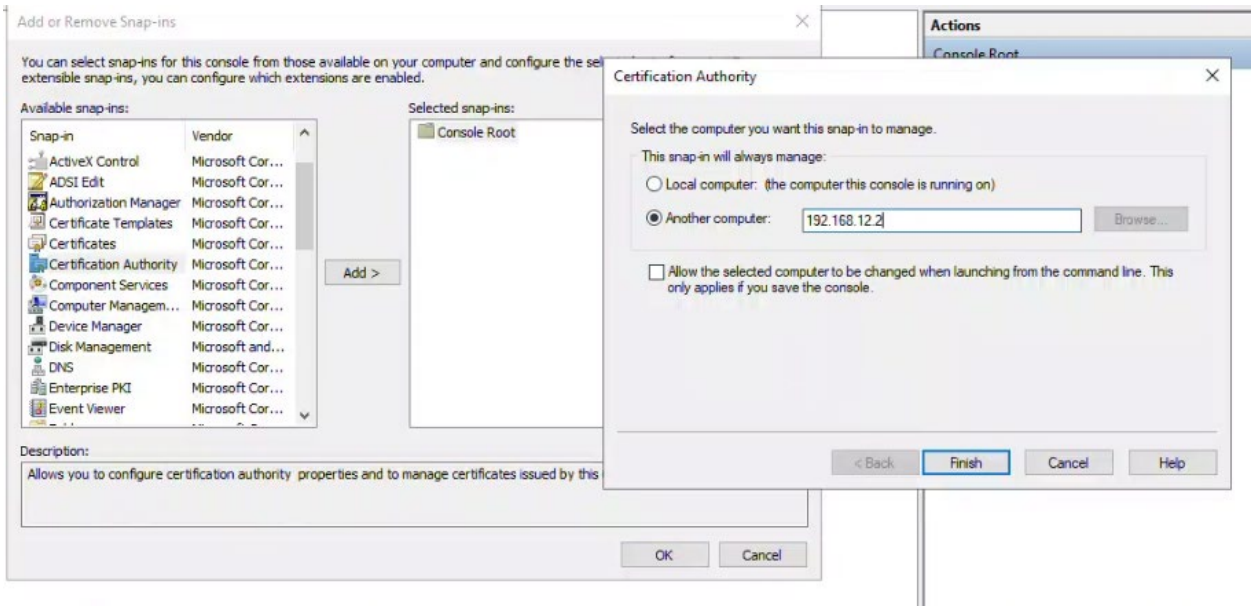
On DC112, install Active Directory Certificate Services (AD CS) and the management tools

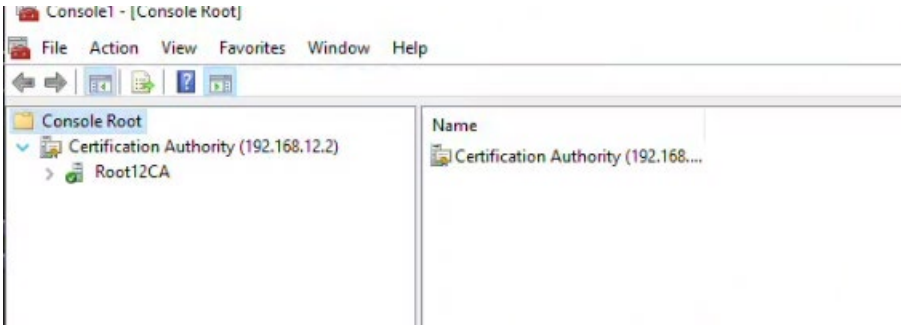
```
PS C:\Users\Administrator.DC112> Install-WindowsFeature -Name AD-Certificate -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Certificate Services, Ce...


PS C:\Users\Administrator.DC112>
```

Define where CDP and AIA can be accessed

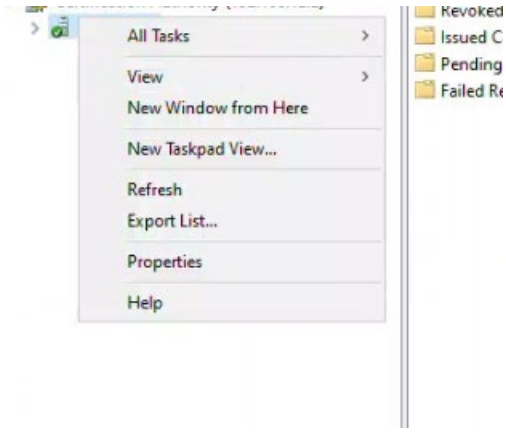
Use Certification Authority Snap-in using mmc.exe and connect Root12CA using it's IP address 192.168.12.2

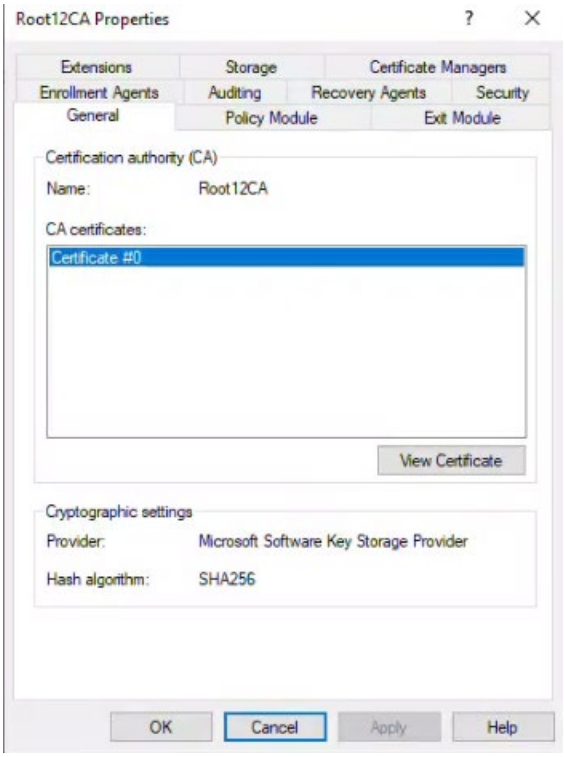




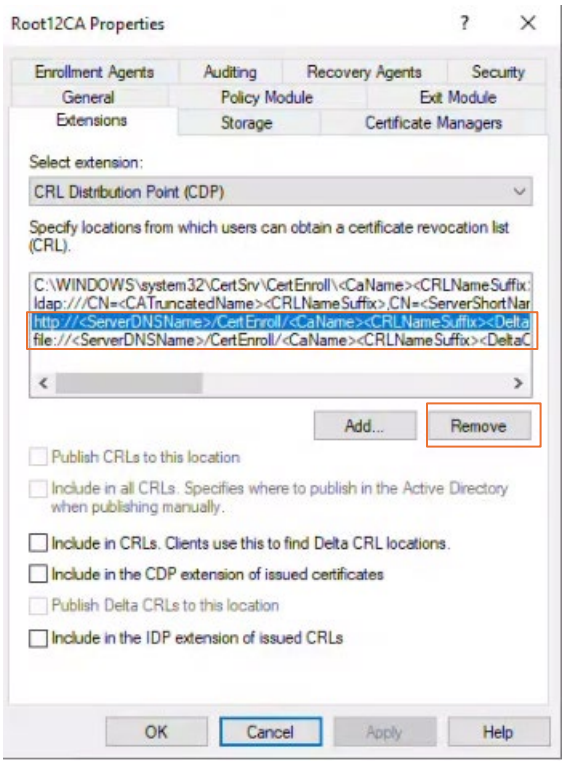


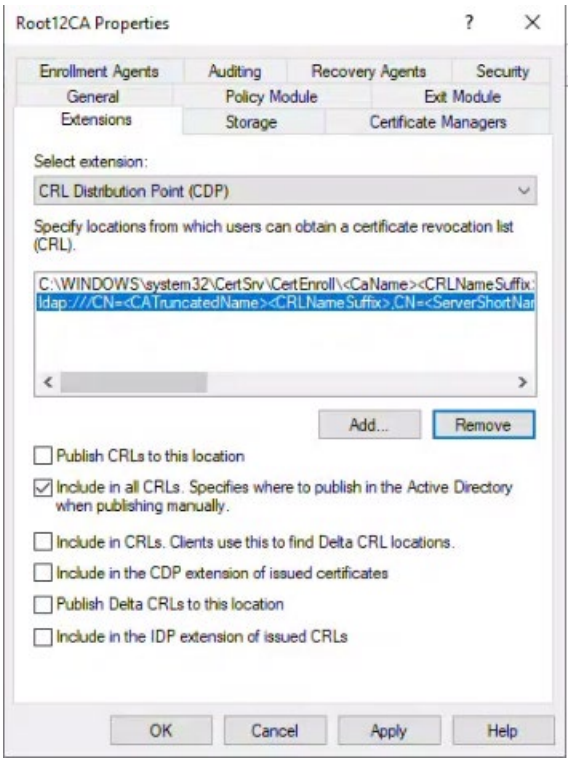
To define where CDP and AIA can be accessed, right-click on Root12CA → Properties



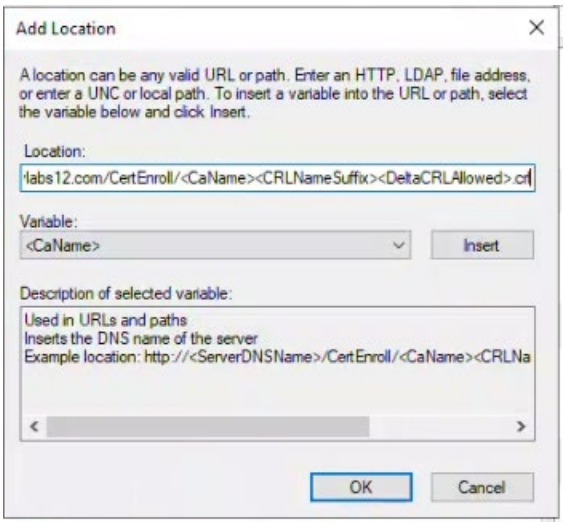


Go to the Extensions tab and remove the http and file entries.

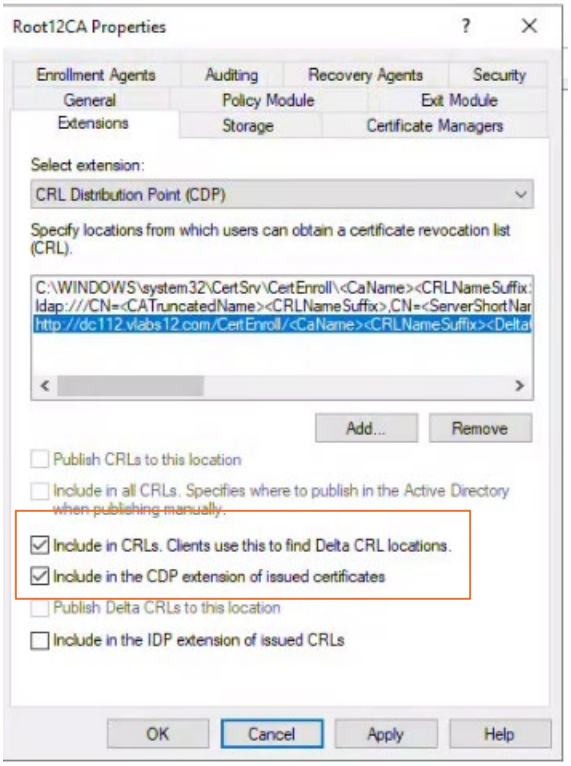


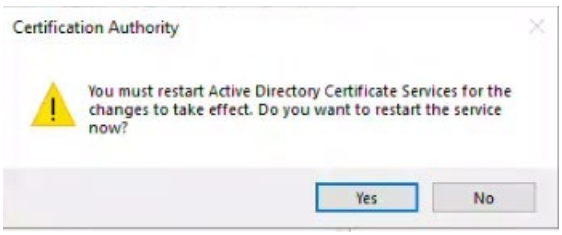


Add an entry with our Enterprise Subordinate CA server (DC112) URL:

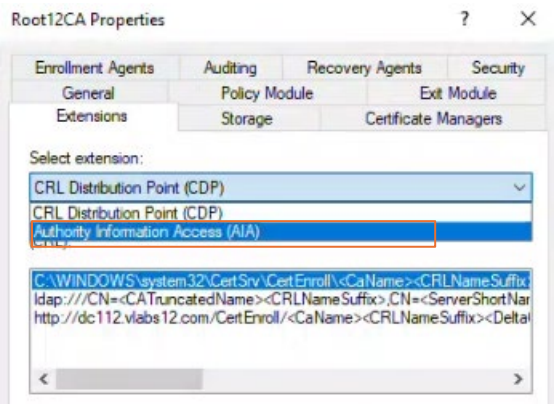


Make sure to tick the boxes “Include in CRLs” and “Include in the CDP”

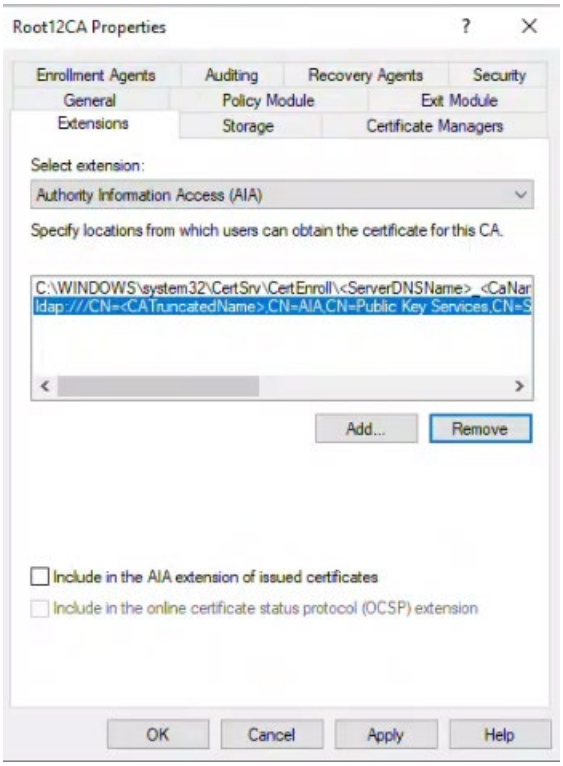




To define where AIA can be accessed, go back to Extensions and choose Authority Information Access from the dropdown menu

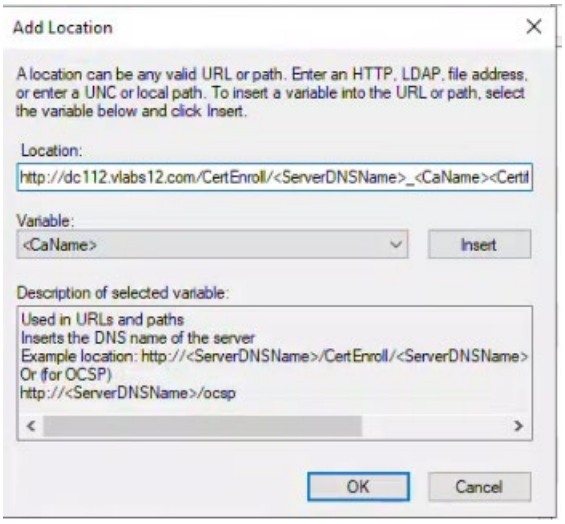


Like before, remove the http and file entries.

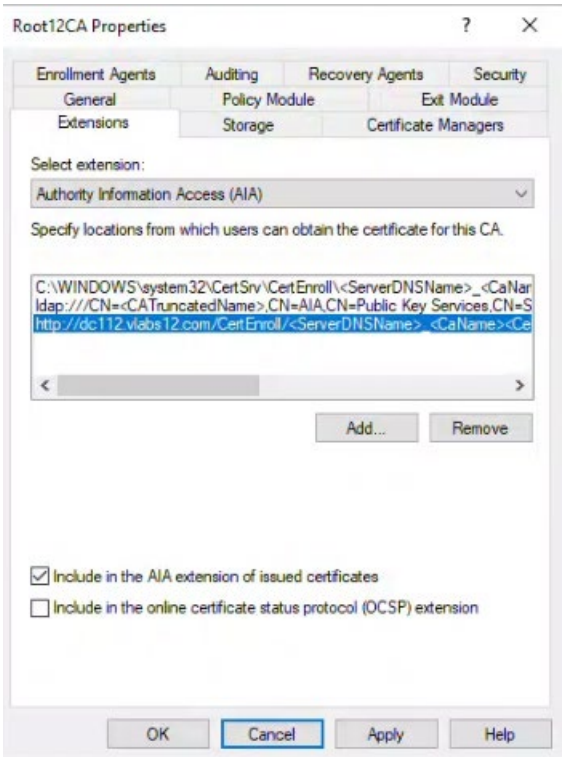


Create a new entry with our URL:

http://dc112.vlabs12.com/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt

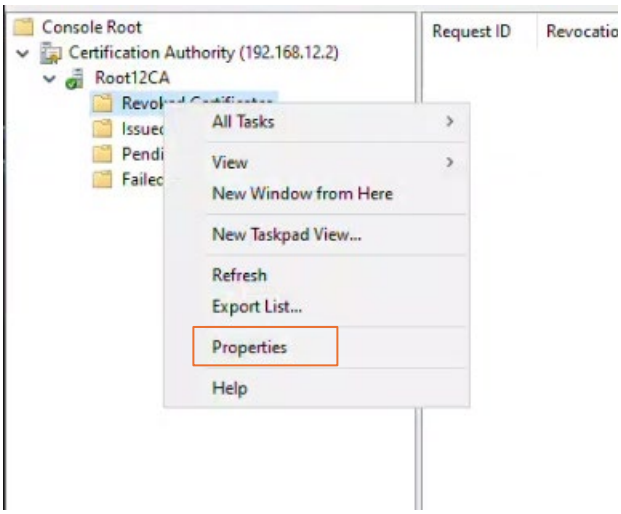


Click on “Include in the AIA extension of issues certificates” then click apply

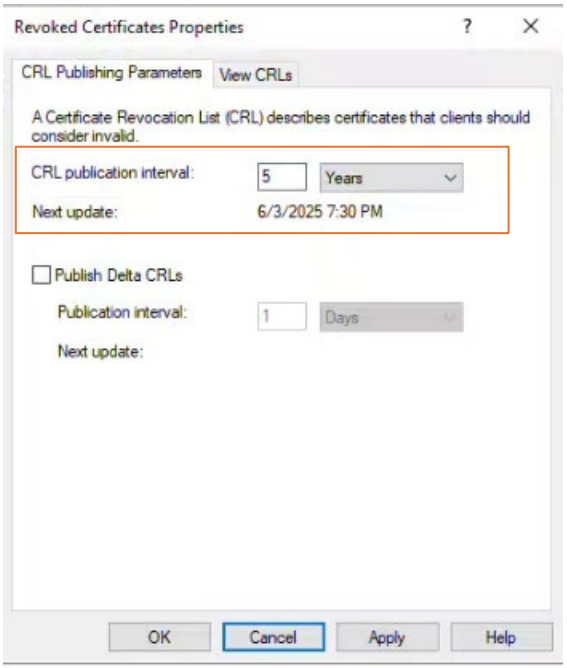


Restart the service when prompted.

Go to Root12CA → Revoked Certificates and select Properties

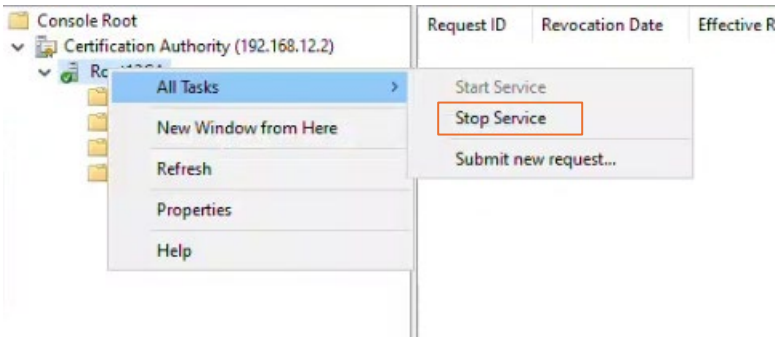


Since Root12CA was configured to be offline for 5 years, modify the CRL publication interval for 5 years so that Root12CA is not needed.

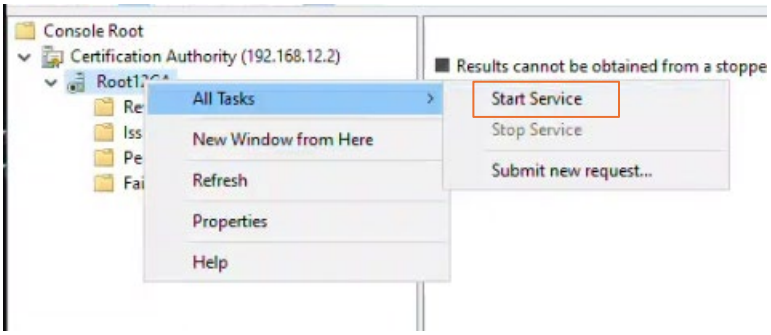


Restart Root12CA so that the changes are applied

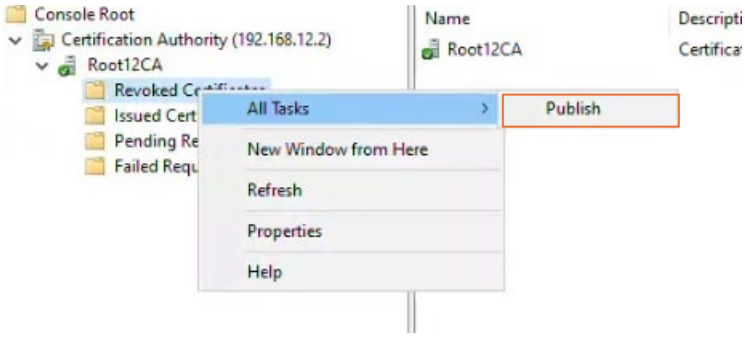
Right-click on Root12CA → All Tasks → Stop Service

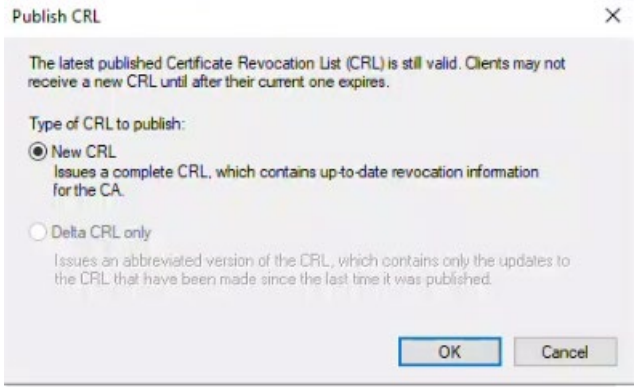


Start the service afterwards

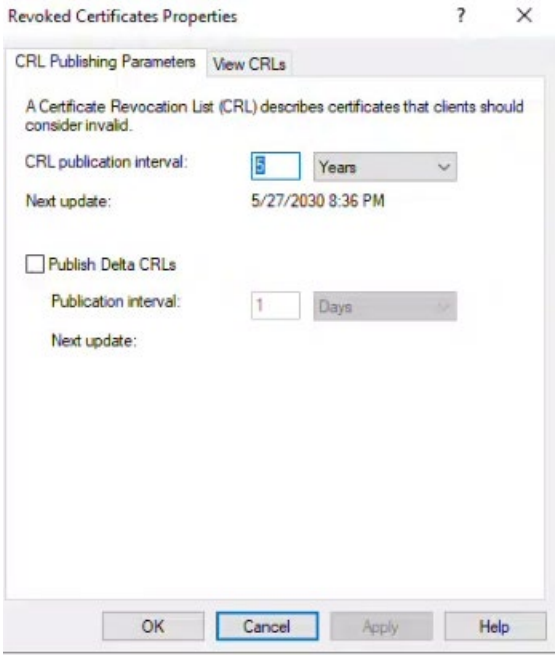


Publish the CRL by right-clicking on Revoked Certificates → All Tasks → Publish





You can view the CRL publication interval in Revoked Certificates → Properties. It's set to 5 years and next update in 2030



Copy the Root CA Certificate, Certificate Revocation List (CRL) and CA private key to DC112.

On DC212, copy the root certificate to DC112

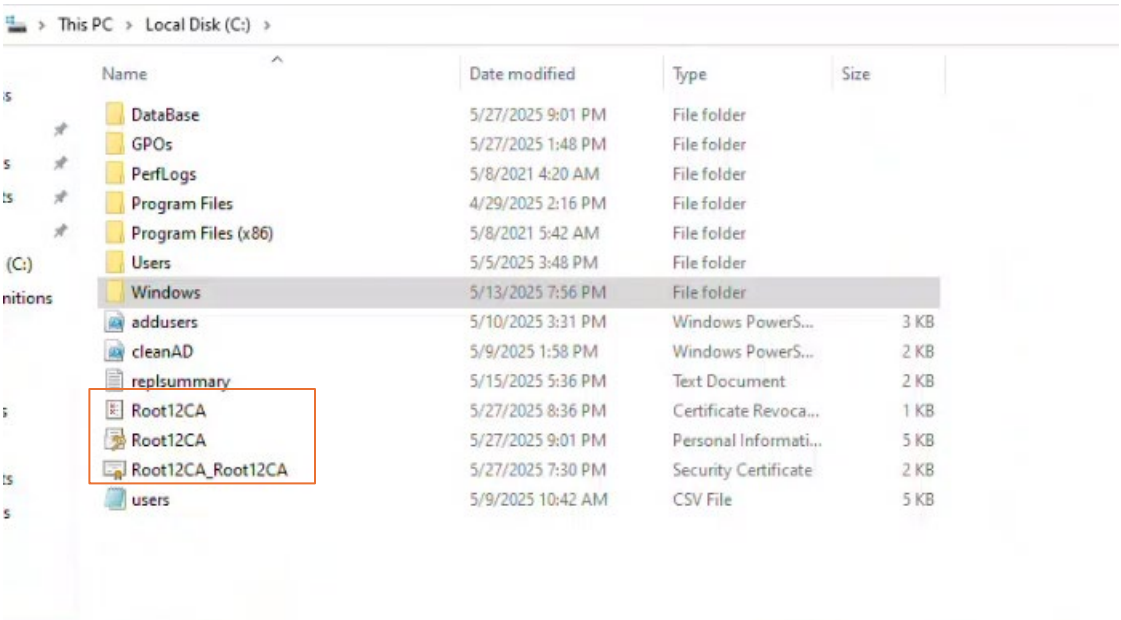
```
PS C:\Users\Administrator> Copy-Item "C:\Windows\System32\CertSrv\CertEnroll\*" \\192.168.12.1\C$
PS C:\Users\Administrator>
```

certutil -backup \\192.168.12.1\C$

Enter the password “Passw0rd$”

```
PS C:\Users\Administrator> certutil -backup \\192.168.12.1\C$
Enter new password:

Confirm new password:

Backed up keys and certificates for Root12CA\Root12CA to \\192.168.12.1\C$\Root12CA.p12.
Full database backup for Root12CA\Root12CA.
Backing up Database files: 100%
Backing up Log files: 100%
Truncating Logs: 100%
Backed up database to \\192.168.12.1\C$.
Database logs successfully truncated.
CertUtil: -backup command completed successfully.
PS C:\Users\Administrator>
```

Verify on DC112 that the keys have been copied over by looking on the C:\ drive



Task 2: Deploy an Enterprise Subordinate CA on DC112

Install Active Directory Certificate Services (AD CS) including all AD CS features on DC112.

Configure DC112 as an Enterprise Subordinate CA

Configure AD CS other roles on DC112

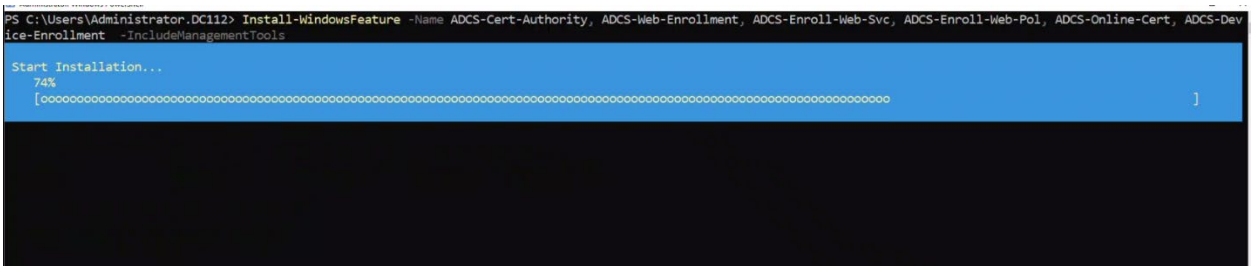
Secure Root CA and take it offline

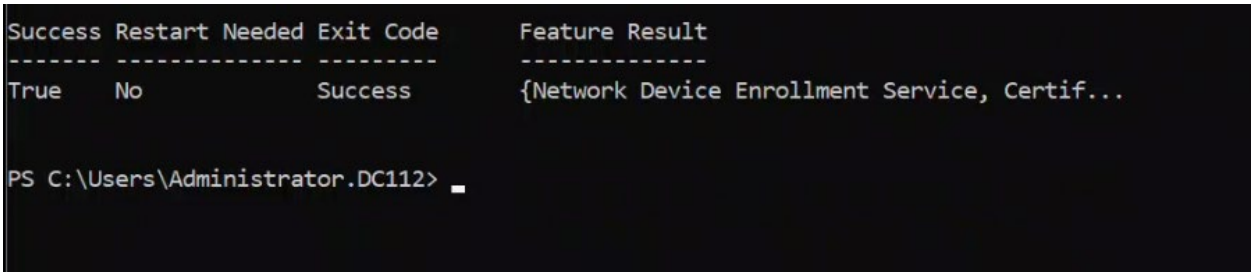
Verify that Enterprise Subordinate CA is working fine.

This task will set up a Enterprise Subordinate CA on DC112 that works under the main Root12CA. It involves installing all certificate service features, linking it to the root authority, setting up additional certificate roles, securing the main root server by taking it offline, and confirming the secondary server is working properly.

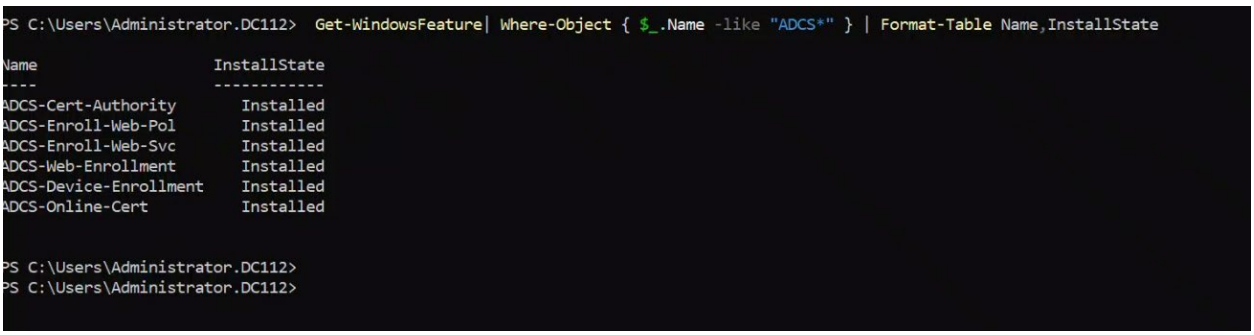
On DC112 using PowerShell, install AD CS and all features with the following:

Install-WindowsFeature -Name ADCS-Cert-Authority, ADCS-Web-Enrollment, ADCS-Enroll-Web-Svc, ADCS-Enroll-Web-Pol, ADCS-Online-Cert, ADCS-Device-Enrollment –IncludeManagementTools





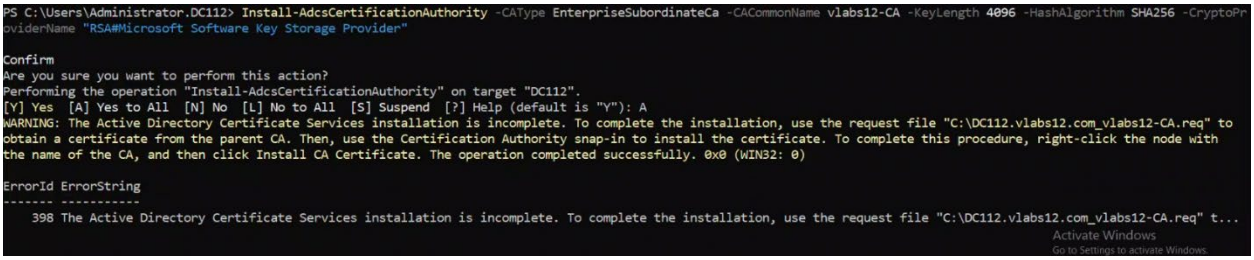
Get-WindowsFeature| Where-Object { $_.Name -like "ADCS*" } | Format-Table Name,InstallState



Configure DC112 as an Enterprise Subordinate CA

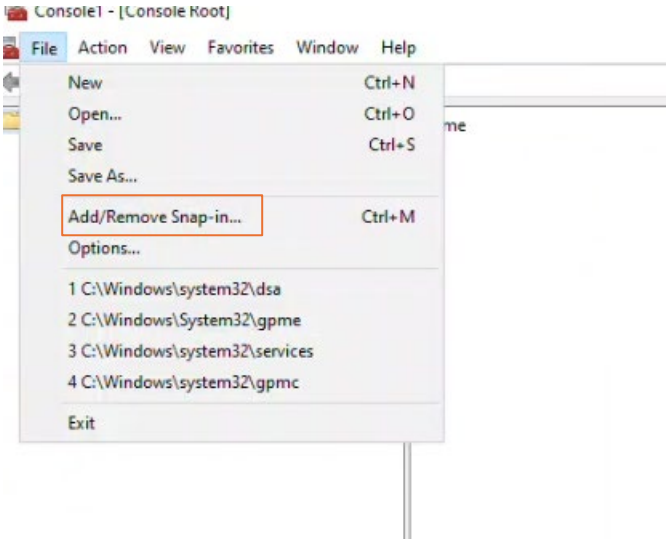
Install-AdcsCertificationAuthority -CAType EnterpriseSubordinateCa -CACommonName vlabs12-CA -KeyLength 4096 -HashAlgorithm SHA256 -CryptoProviderName "RSA#Microsoft Software Key Storage Provider"

Note: you will get a warning that the installation is incomplete. It's normal, due to the fact we have to request a certificate from the parent CA using Certificate Authority Snap-in



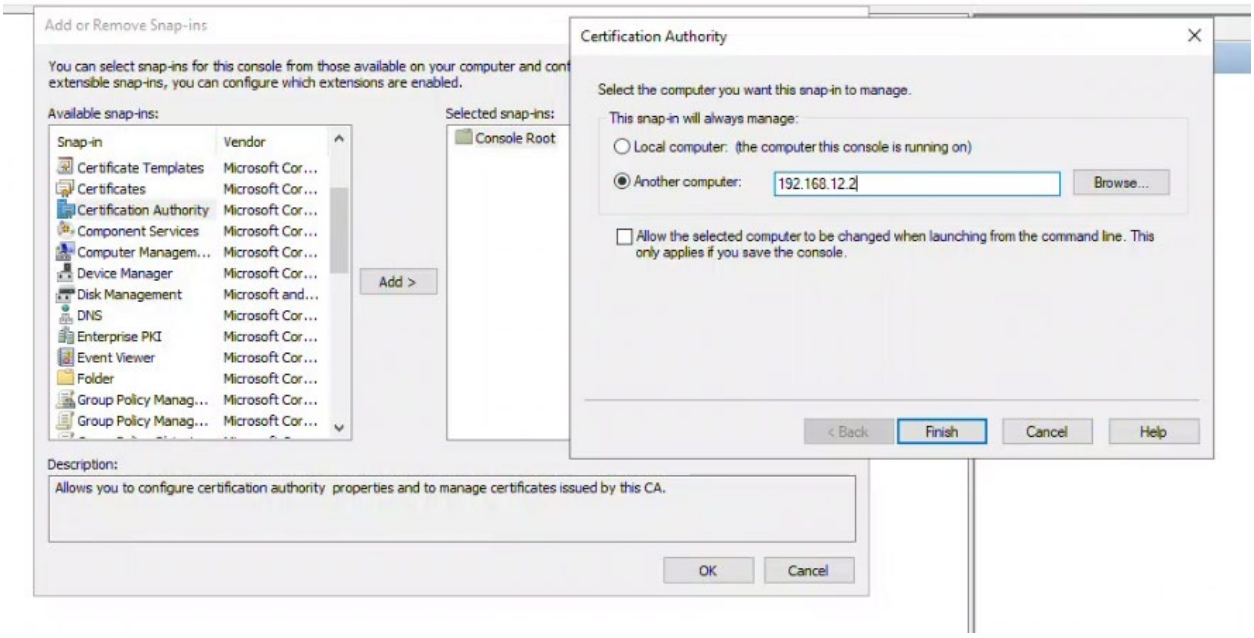
Go to Certificate Authority Snap-in using mmc.exe and connect Root12CA using it's ip address 192.168.12.2

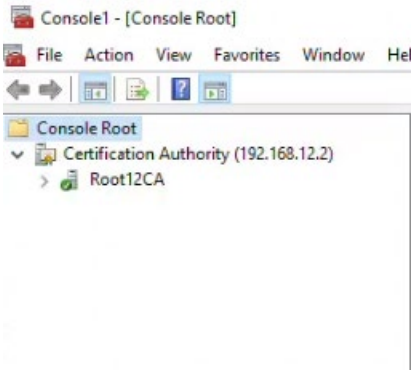
Click on File → Add/Remove Snap-in..



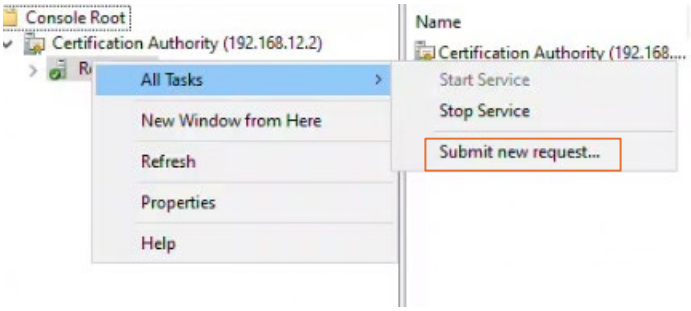
Certification Authority → Add → Another computer → 192.168.12.2

Wait for it to connect

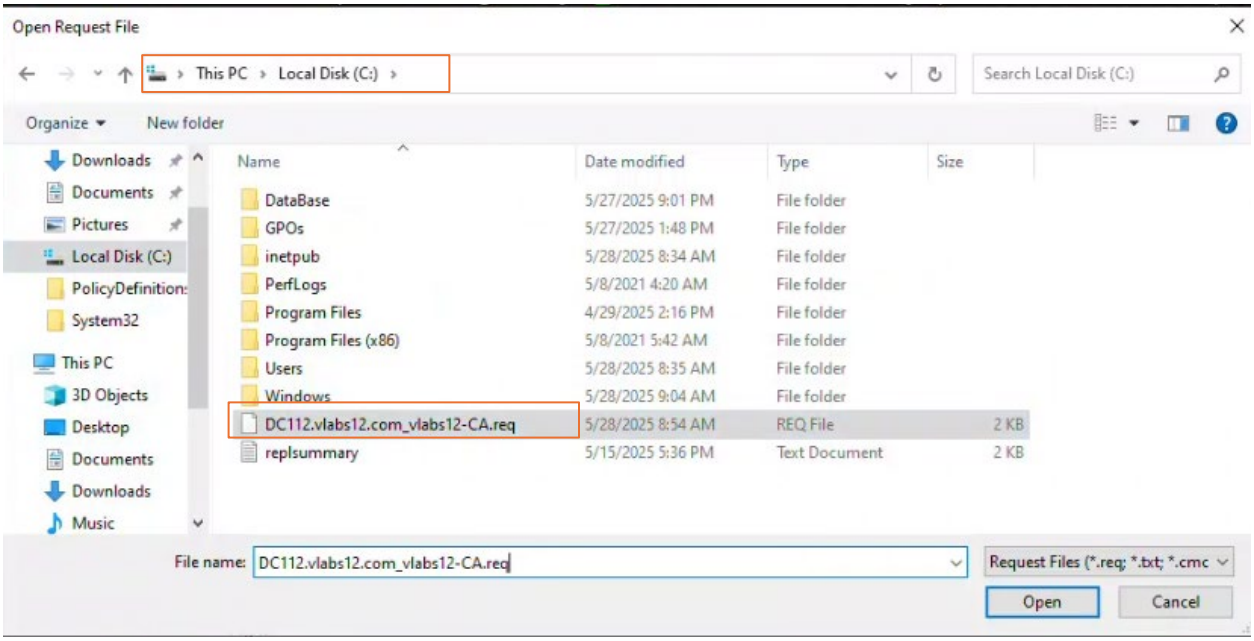




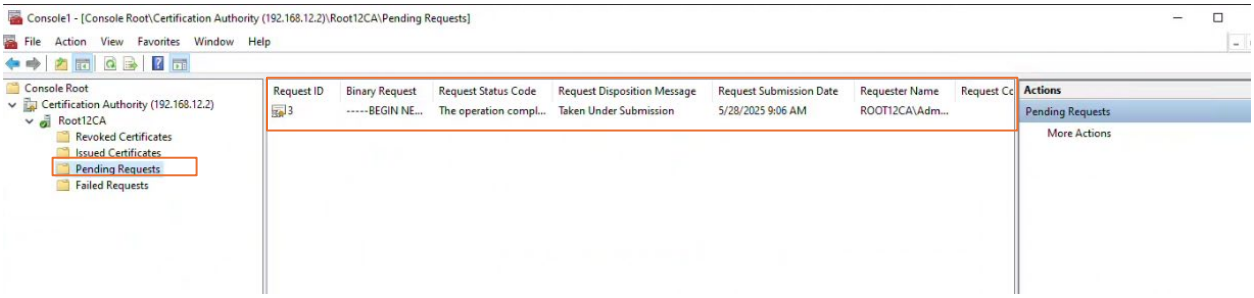
Right-click on Root12CA → All tasks → Submit new request

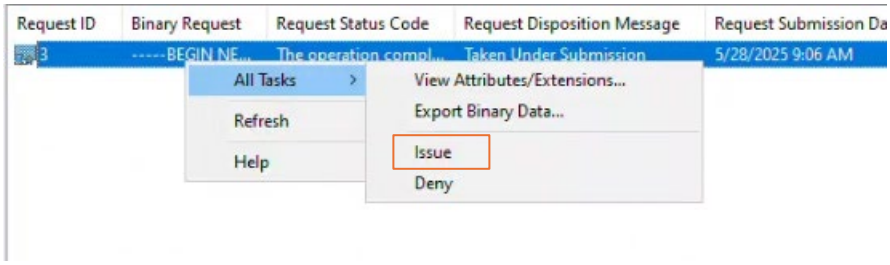


On your C:\ drive, you'll find the request file **DC112.vlabs12.com_vlabs12-CA.req.** Select it and click open

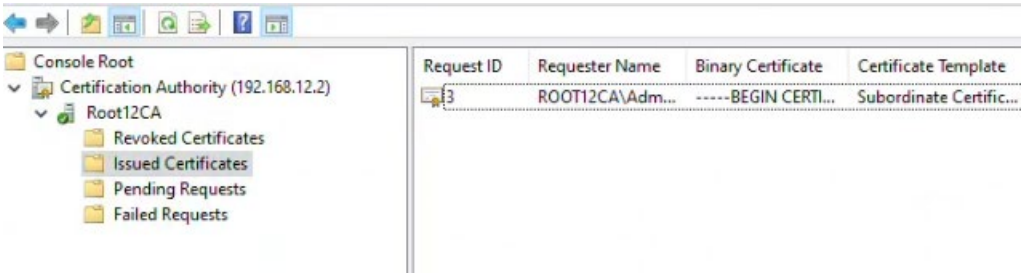


You'll find the file under Pending Requests. Right-click it → All tasks → Issue

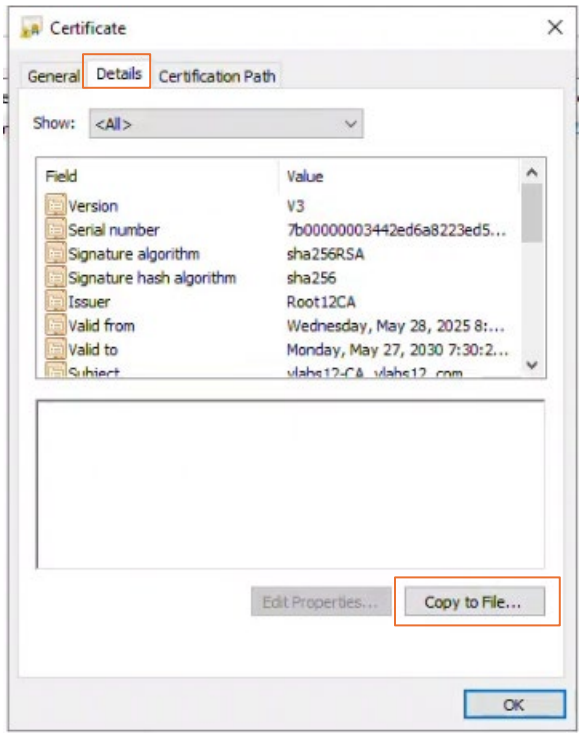




You'll see the file is now gone from Pending Requests and has been moved to Issued Certificates

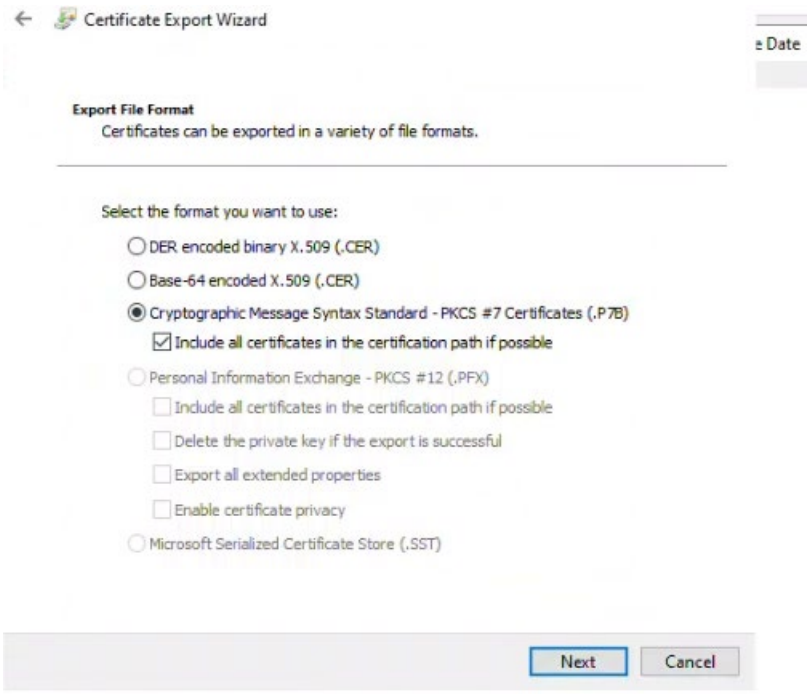


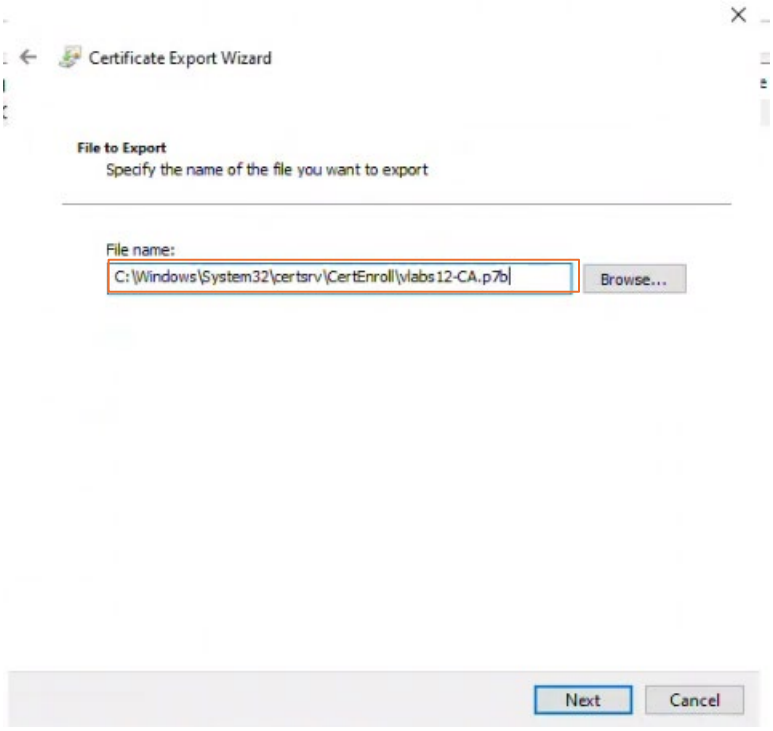
Double click on the issued certificate, go to Details tab and click Copy to File…



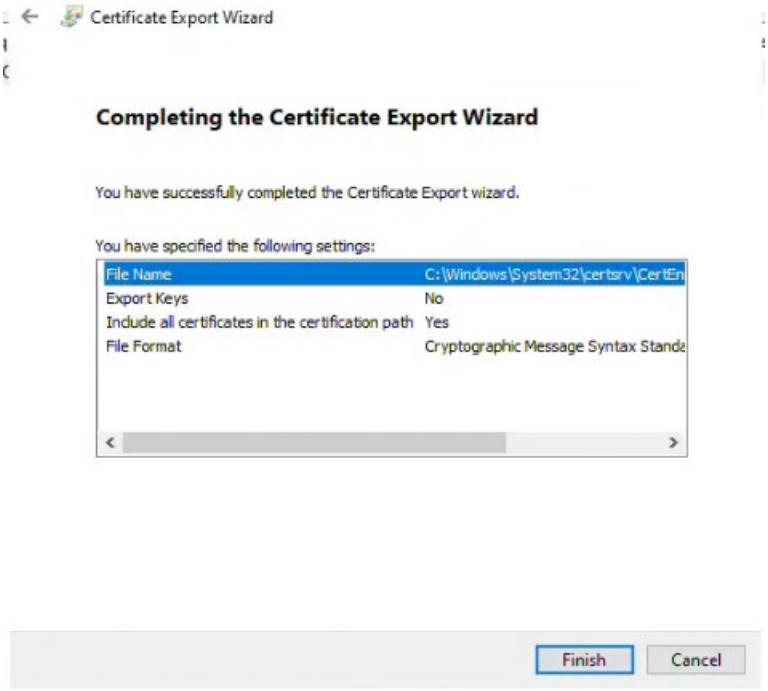
The Certificate Export Wizard will now open. Click on next on the welcome page

Select the **Cryptographic Message Syntax Standard - PKCS #7** type and select “Include all certificates in the certification path” click next and save the file under: **C:\Windows\System32\certsrv\CertEnroll\vlabs12-CA.p7b**





Review the selections and then click on Finish

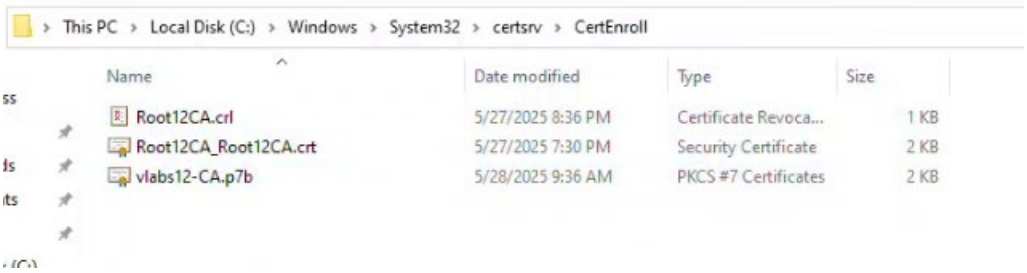


Next we need to copy the Root12CA certificate and CRL to the Enterprise Subordinate CA certificate Enroll folder using PowerShell:

Copy-Item -Path C:*.crt -Destination C:\Windows\System32\certsrv\CertEnroll

Copy-Item -Path C:*.crl -Destination C:\Windows\System32\certsrv\CertEnroll

```
PS C:\Users\Administrator.DC112> Copy-Item -Path C:\*.crt -Destination C:\Windows\System32\certsrv\CertEnroll\
PS C:\Users\Administrator.DC112>  Copy-Item -Path C:\*.crl -Destination C:\Windows\System32\certsrv\CertEnroll\
PS C:\Users\Administrator.DC112>
PS C:\Users\Administrator.DC112>
```



We need to publish the Certificate and CRL to AD. Use the following:

certutil -dspublish -f C:\Windows\System32\certsrv\CertEnroll\Root12CA_Root12CA.crt

```
PS C:\Users\Administrator.DC112> certutil -dspublish -f C:\Windows\System32\certsrv\CertEnroll\Root12CA_Root12CA.crt
ldap:///CN=Root12CA,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=vlabs12,DC=com?cACertificate

Certificate added to DS store.

ldap:///CN=Root12CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=vlabs12,DC=com?cACertificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.
PS C:\Users\Administrator.DC112>
```

certutil -dspublish -f C:\Windows\System32\certsrv\CertEnroll\Root12CA.crl

```
PS C:\Users\Administrator.DC112> certutil -dspublish -f C:\Windows\System32\certsrv\CertEnroll\Root12CA.crl
ldap:///CN=Root12CA,CN=Root12CA,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=vlabs12,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
?certificateRevocationList

Base CRL added to DS store.

CertUtil: -dsPublish command completed successfully.
```


Now we need to install the Root12CA certificate using the following:

certutil -addstore Root C:\Windows\System32\certsrv\CertEnroll\Root12CA_Root12CA.crt

```
PS C:\Users\Administrator.DC112>  certutil -addstore Root C:\Windows\System32\certsrv\CertEnroll\Root12CA_Root12CA.crt
Root "Trusted Root Certification Authorities"
Signature matches Public Key
Certificate "Root12CA" added to store.
CertUtil: -addstore command completed successfully.
PS C:\Users\Administrator.DC112>
```

Next is to install the Root12CA CRL

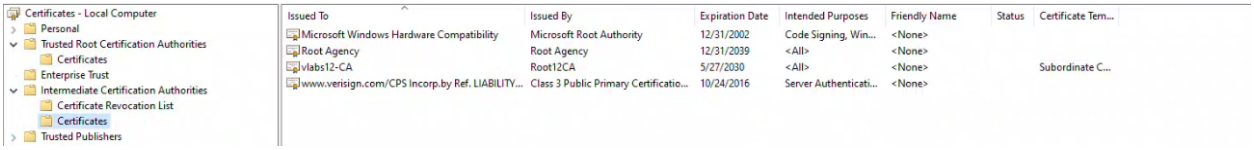
Certutil -addstore CA C:\Windows\System32\certsrv\CertEnroll\Root12CA.crl

```
PS C:\Users\Administrator.DC112> certutil -addstore CA C:\Windows\System32\certsrv\CertEnroll\Root12CA.crl
CA "Intermediate Certification Authorities"
CRL "CN=Root12CA" added to store.
CertUtil: -addstore command completed successfully.
PS C:\Users\Administrator.DC112>
```

Install the Subordinate CA certificate:

certutil -installCert C:\Windows\System32\certsrv\CertEnroll\vlabs12-CA.p7b

```
PS C:\Users\Administrator.DC112>  certutil -installCert C:\Windows\System32\certsrv\CertEnroll\vlabs12-CA.p7b
CertUtil: -installCert command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
PS C:\Users\Administrator.DC112>
```



Once that's done, start the CA service on the subordinate CA Certificate:

Start-Service certsvc

```
PS C:\Users\Administrator.DC112> Start-Service certsvc
PS C:\Users\Administrator.DC112>
```

We're ready to install the AD CS roles on DC112

CA Web Enrollment

The Certification Authority (CA) Web Enrollment role service provides a set of web pages that allow users to perform certificate tasks, such as requesting and renewing certificates, retrieving certificate revocation lists (CRLs), and enrolling for smart card certificates. It allows interaction with the Certification Authority role service.

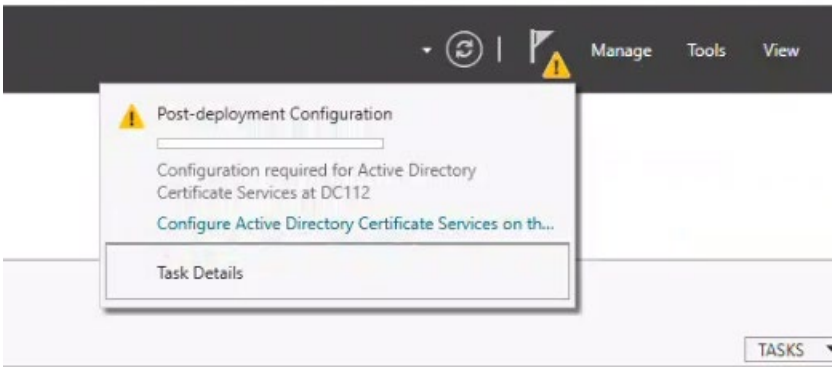
CEP and CES Certificate Enrollment Policy Web Services

The Certificate Enrollment Web Services (CEP and CES) enable the automatic request and renewal of certificates from a certification authority via a Web-based interface. CES enables policy-based certificate enrollment when the client computer is not a member of a domain or when a domain member is not connected to the domain. The Certificate Enrollment Policy Web Service lets users and computers obtain certificate enrollment policy information even when the computer isn't a member of a domain or if a domain-joined computer is temporarily outside the security boundary of the corporate network

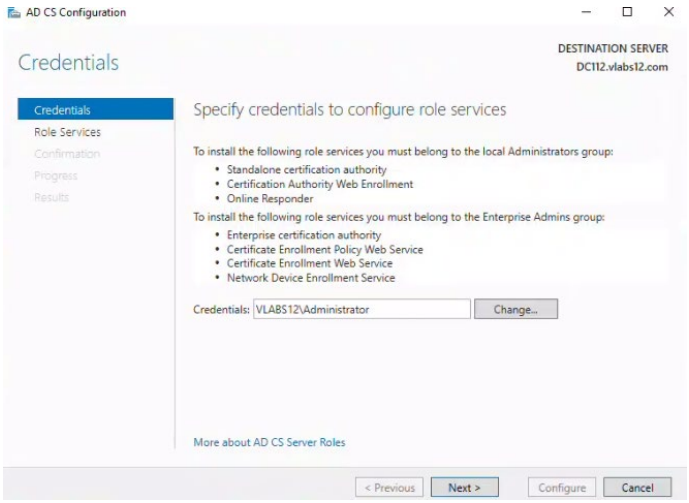
NDES performs the following functions:

Generates and provides one-time enrollment passwords to administrators.
Submits enrollment requests to the CA.
Retrieves enrolled certificates from the CA and forwards them to the network device.

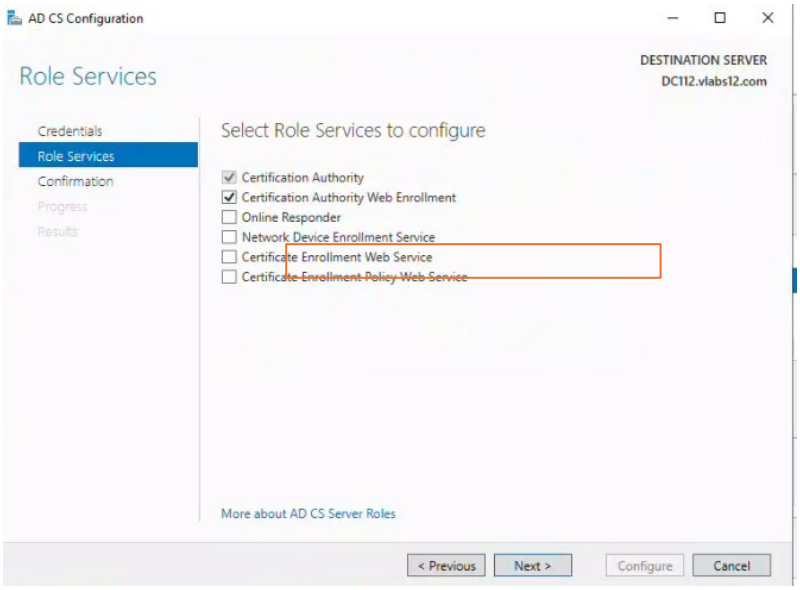
On DC112 server manager, click the exclamation mark at the top and select Configure AD CS on the destination server



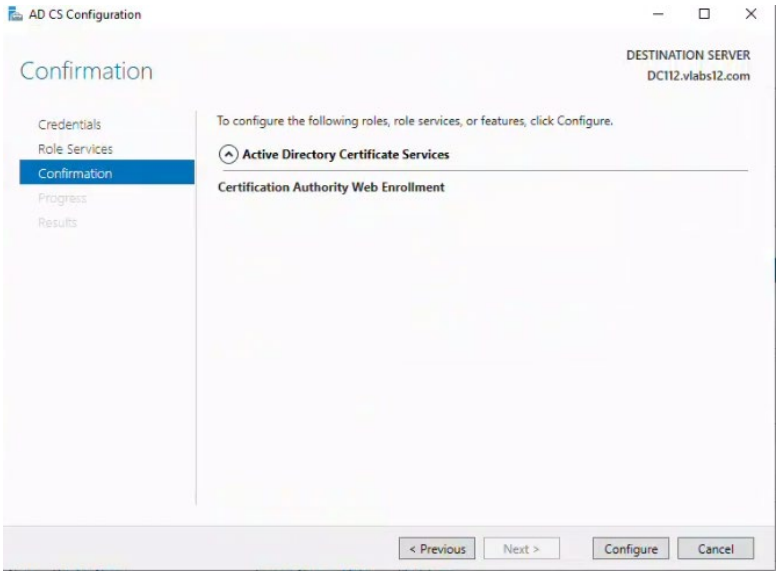
Confirm the credentials → Next

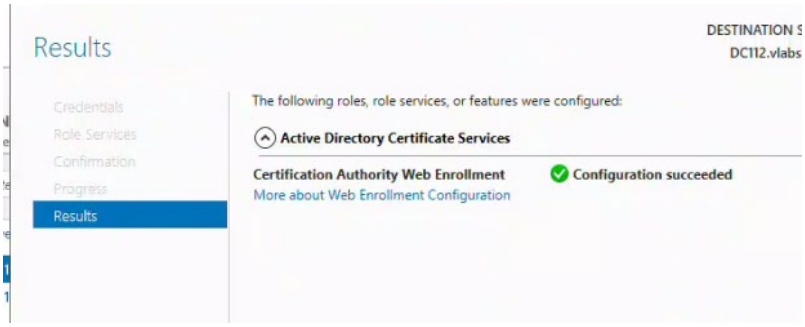


Tick the box “CA Web Enrollment” → Next

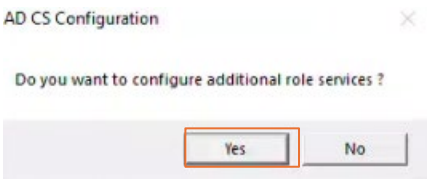


Click on **Configure**

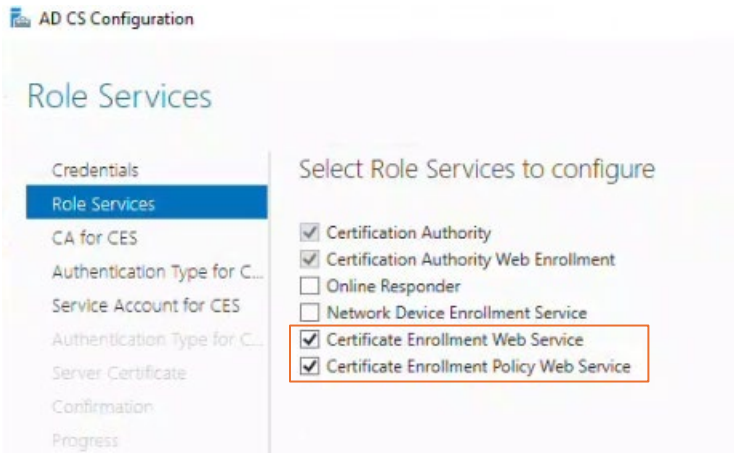




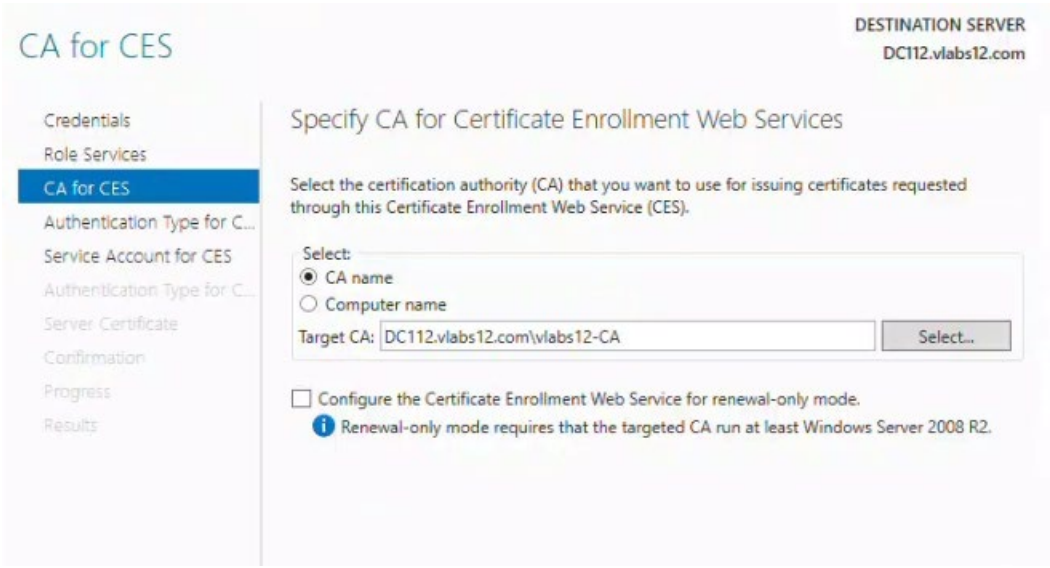
Click close and then Yes at this prompt to install additional roles



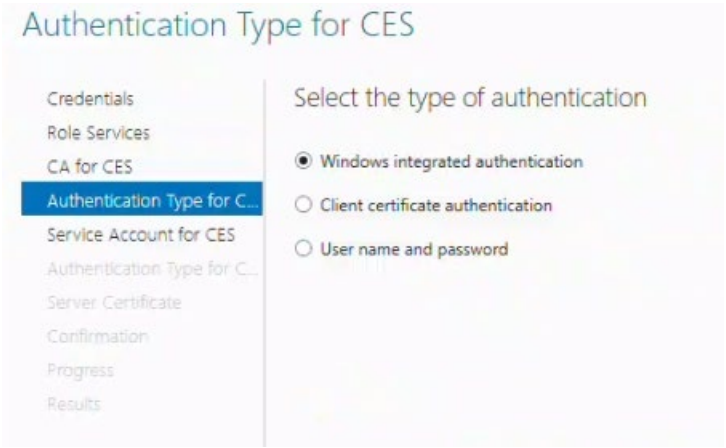
Now we'll install CES and CEP. Select both roles → Next



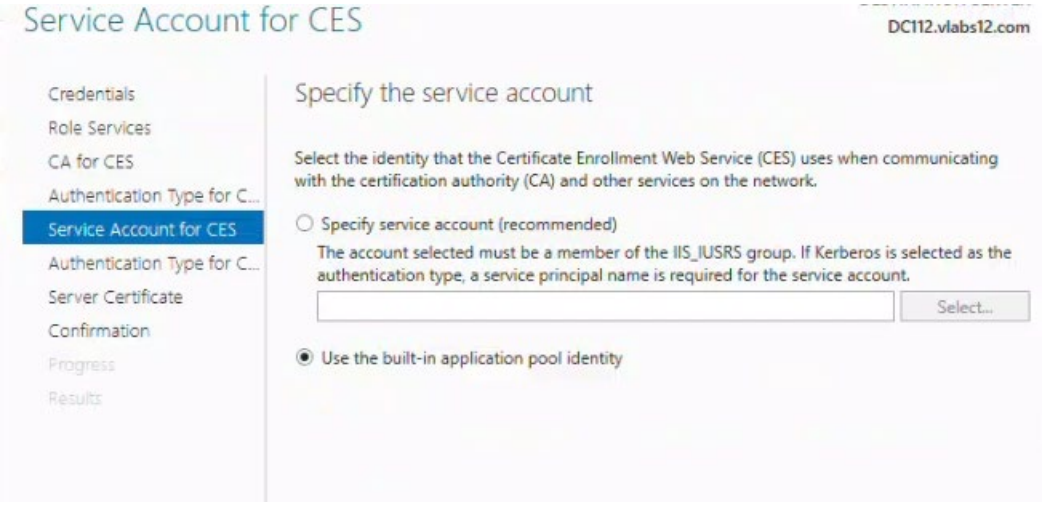
Confirm the target CA is our DC112 CA

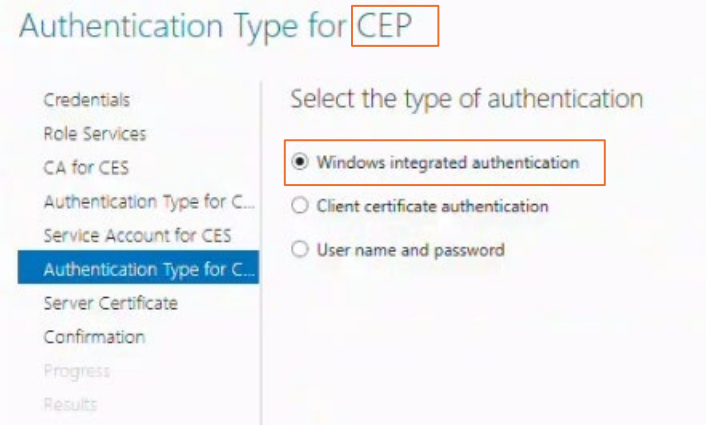


For both CES and CEP, select “Windows integrated authentication”



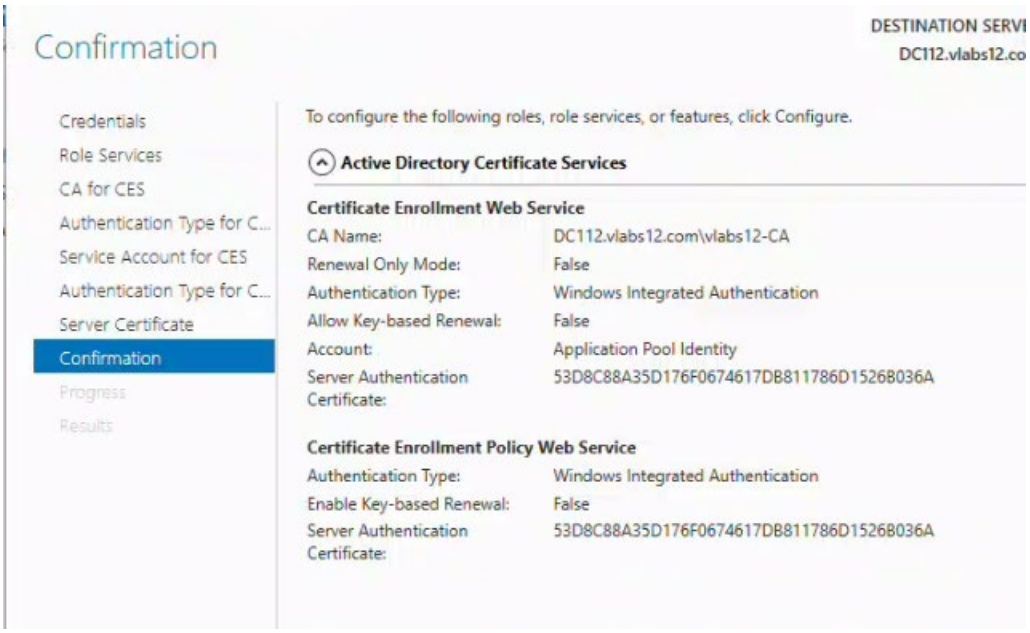
For the service account, select “use the built-in application pool identity”

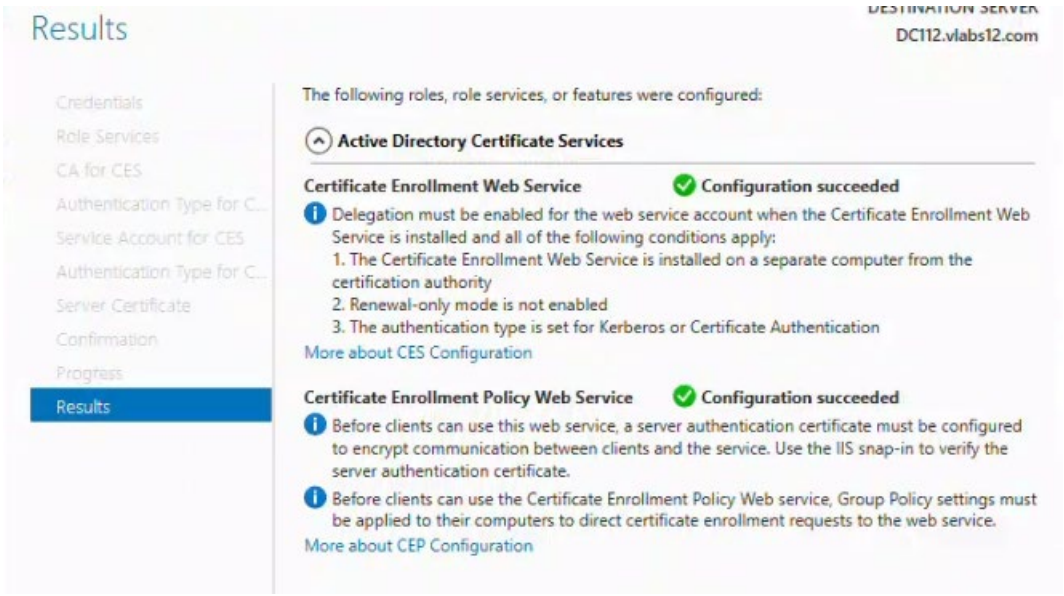




Select “vlabs12-CA” for SSL encryption and click on Next

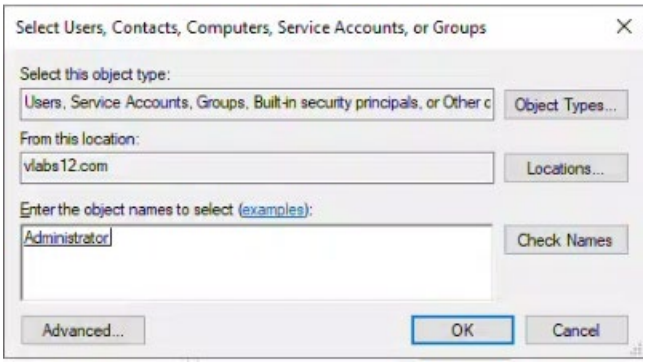
Confirm all the selections and then click on configure

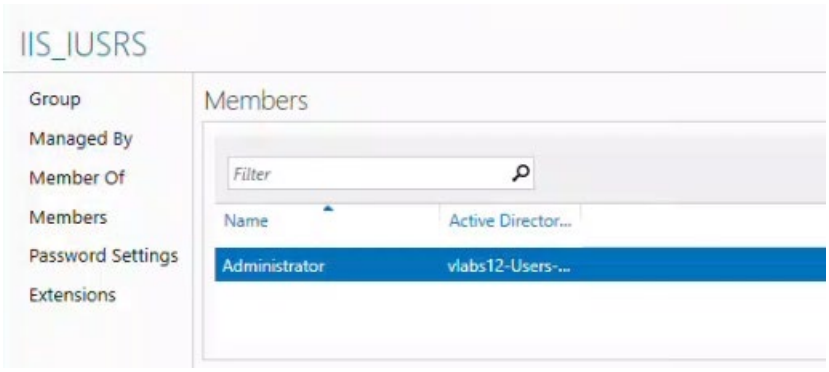




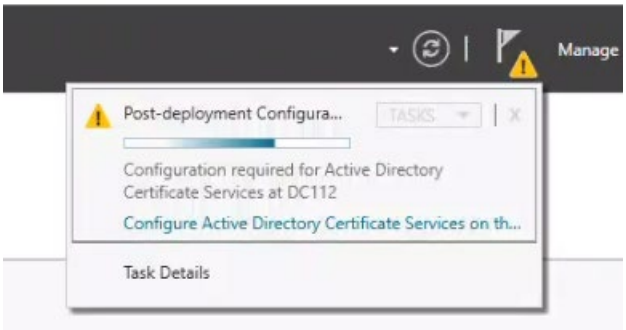
Before we configure the Network Device Enrollment Service, we need to add Administrator to the **IIS_IUSRS group** using ADAC

IIS_IUSRS is under Bulletin

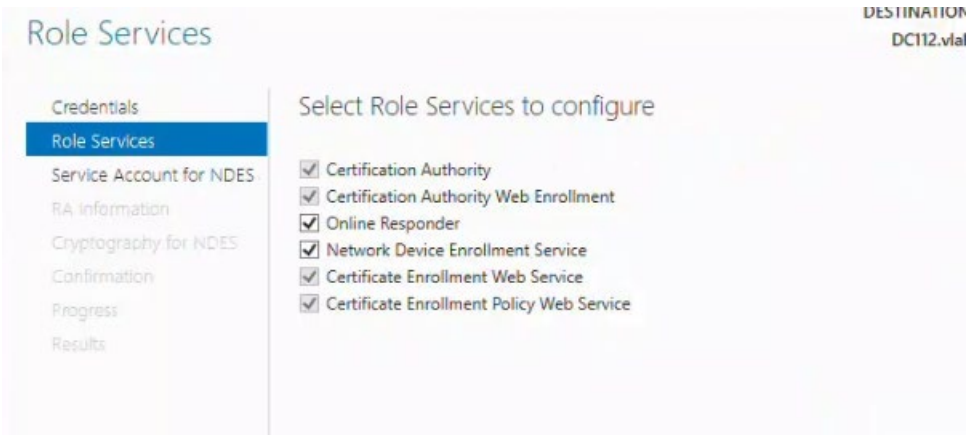




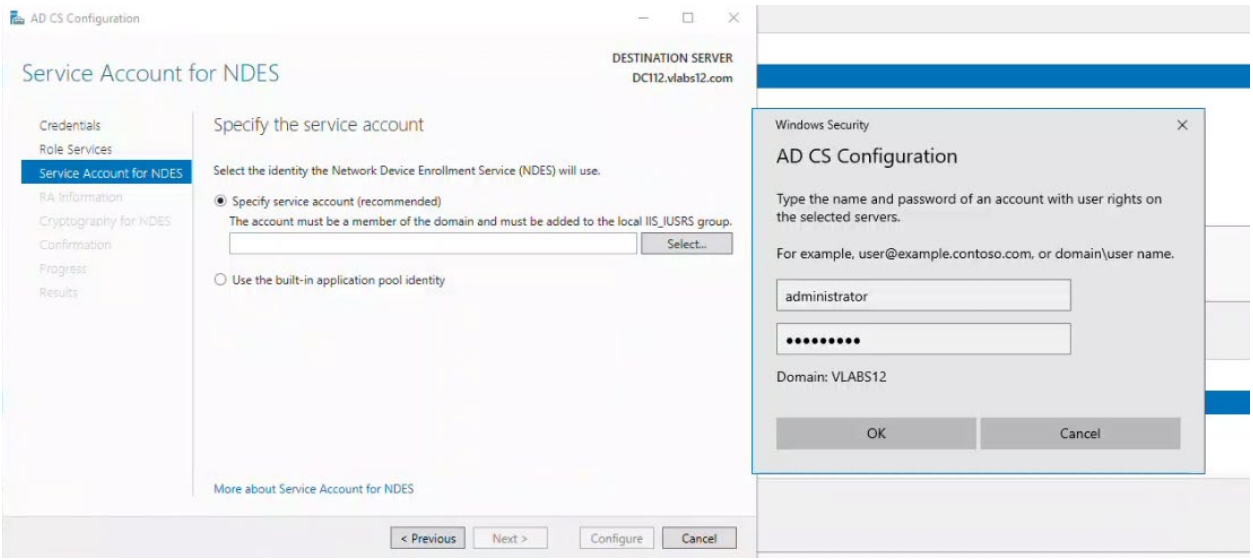
Now we can proceed with NDES

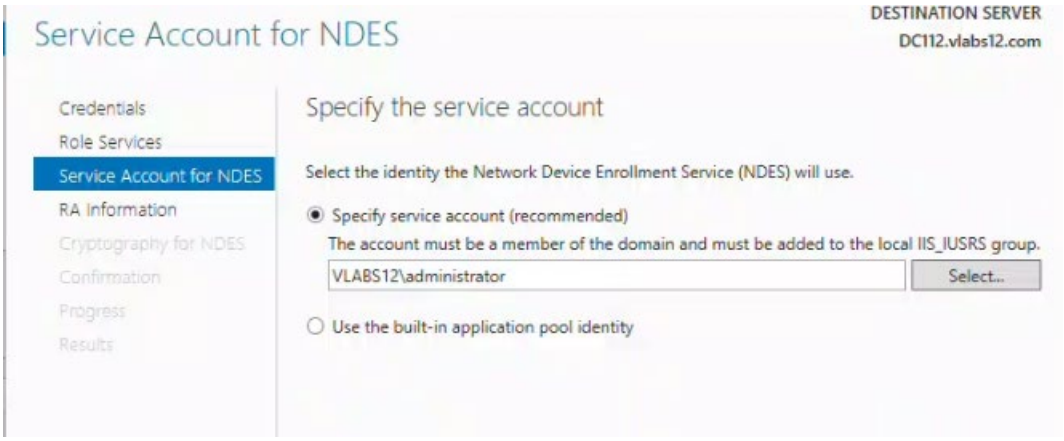


Tick the box “Network Device Enrollment Service”

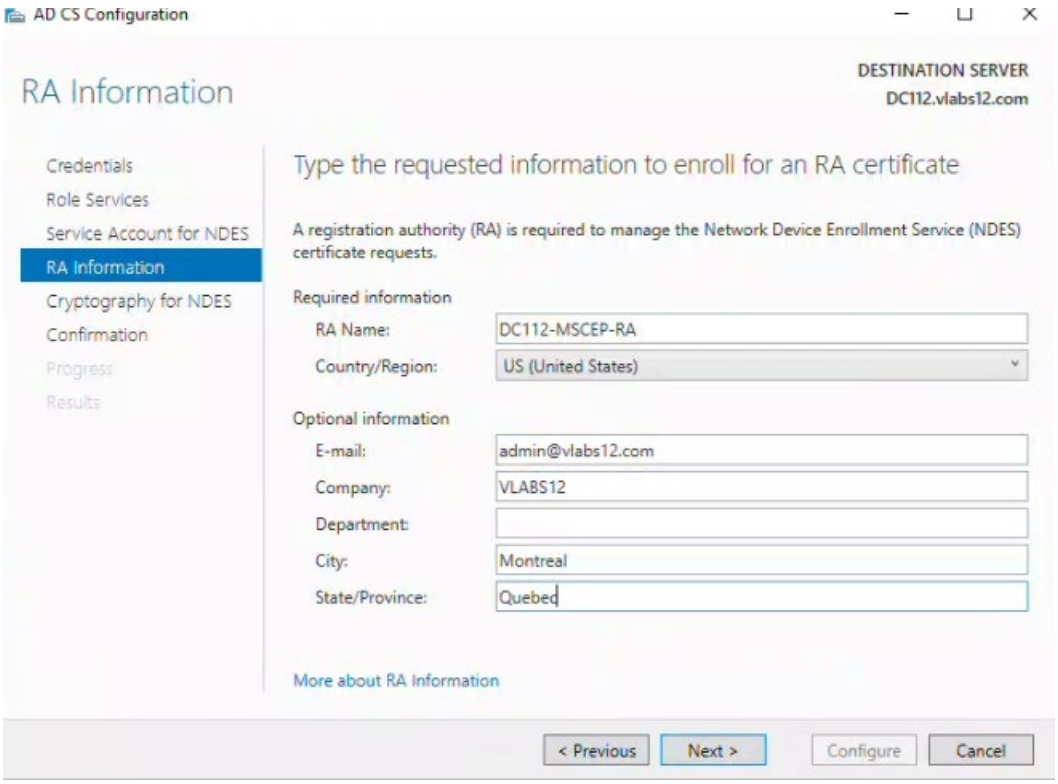


Select “specify service account” → Select and then add your administrator credentials

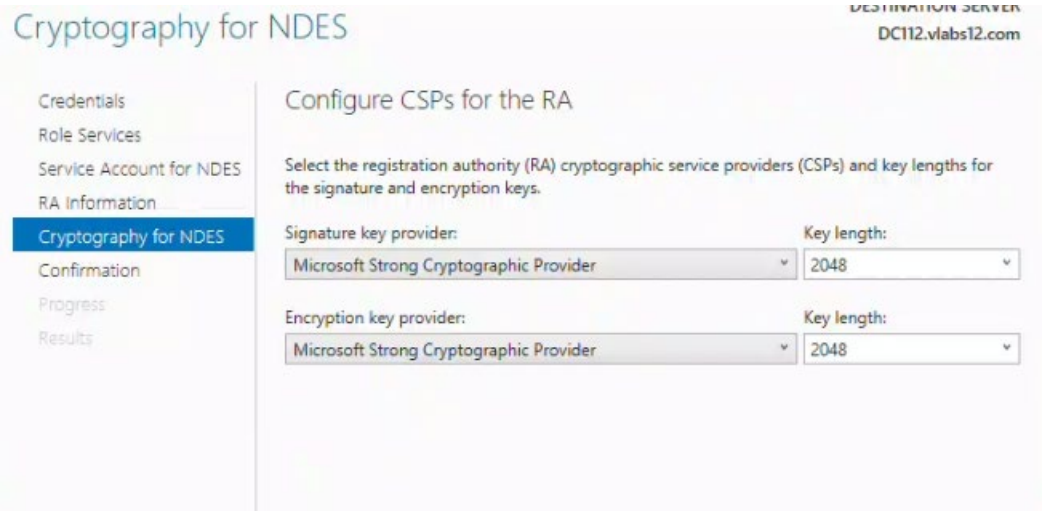




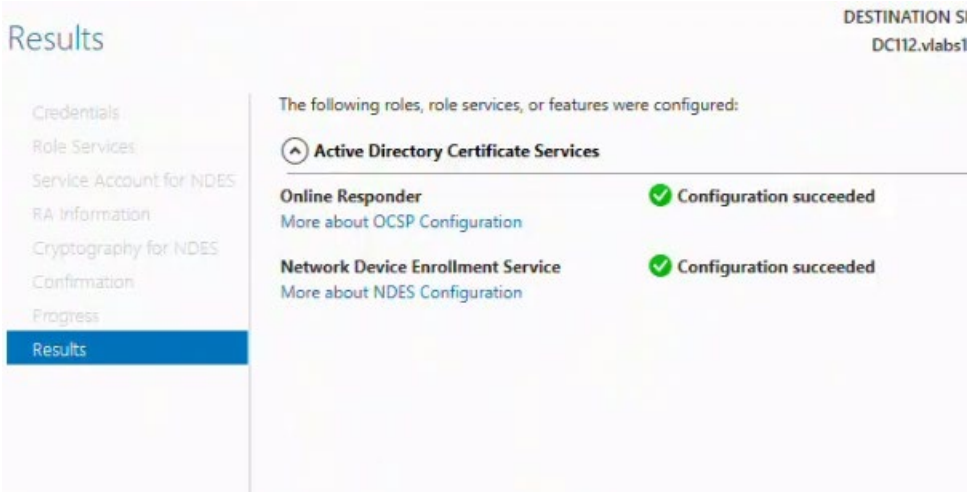
Add an email, company name, city and province



Confirm the key length for both is 2048



Click on Configure when complete and wait for the role services to install



Configuration of DC112 for AD CS complete.

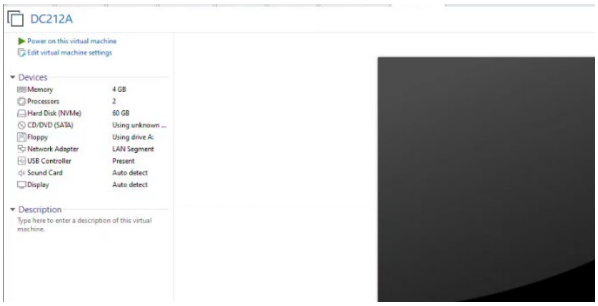
Now we have to take DC112 (Root12CA) offline for security reasons.

Use the following:

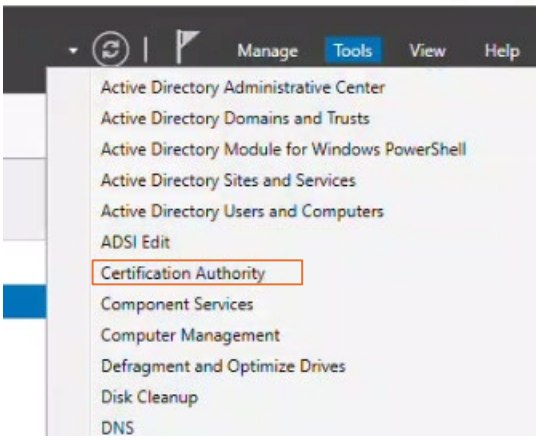
net stop certsvc

```
PS C:\Users\Administrator>  net stop certsvc
The Active Directory Certificate Services service is stopping.
The Active Directory Certificate Services service was stopped successfully.

PS C:\Users\Administrator>
```

Stop-Computer

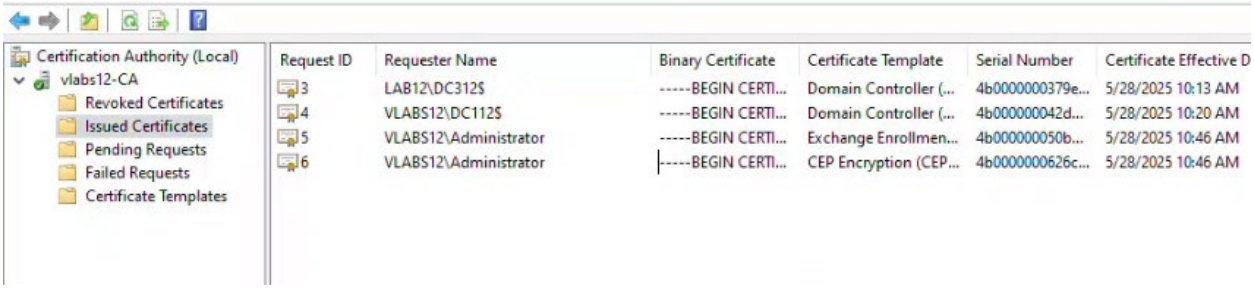


We can see on DC112 the certificates we've already issued. Go to Tools → Certification Authority

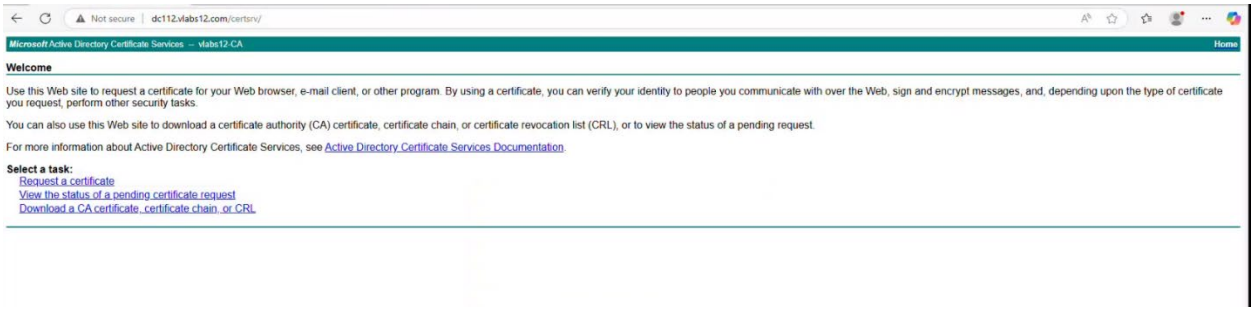


Under vlabs12-CA → Issued Certificates.

We can see that we've issued certificates to Administrator and also DC312 (Lab12.vlabs12.com) who is our child domain.

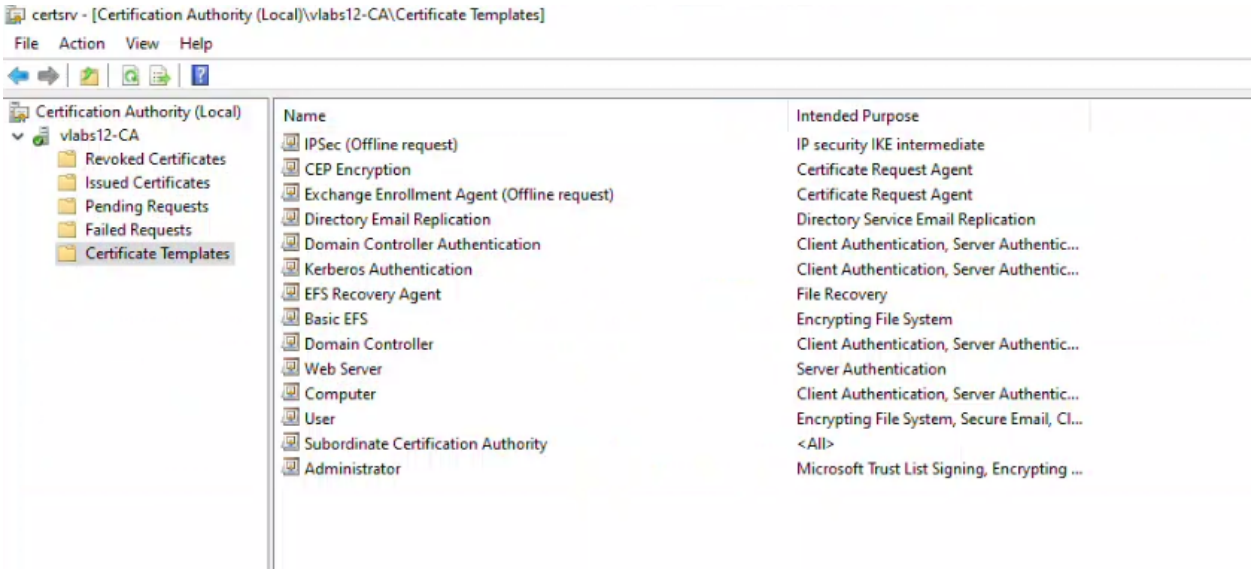


We also have a website at **dc112.vlabs12.com/certsrv/**



The website is not really used anymore since everything can be done through Active Directory but it can be used for others to request a certificate.

You can also view the Certificate Templates under vlabs12-CA



That's it. We've successfully configured DC212 (Root12CA) as a Offline Standalone Root CA, and DC112 as an Enterprise Subordinate CA with the capabilities of issuing certificates.

5/29/2025

Assignment 3

Part 2

Mohammed, Laetitia, 0931512

NETWORK INSTALLATION AND ADMINISTRATION II

Contents

Task 1: Issue User Certificates in an AD Domain

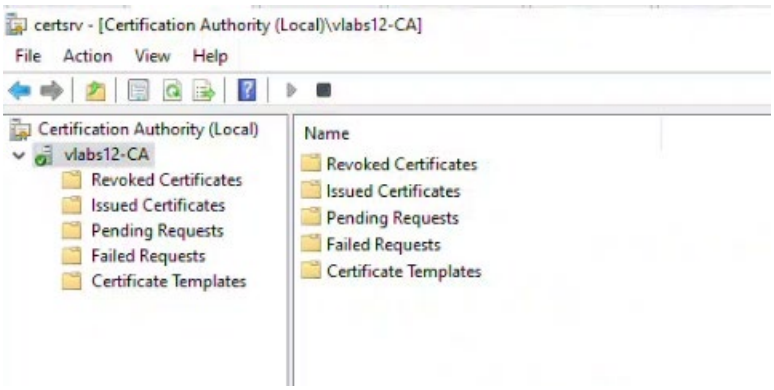
Configure and publish User Certificates from Enterprise CA

Open a session on Client12 with a user that has an email address and manually requests a user certificate

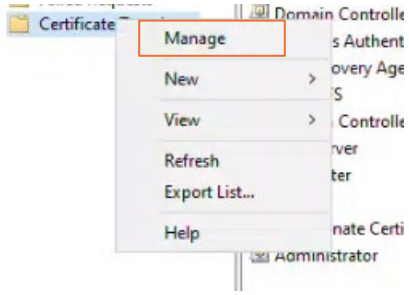
Verify that the user has obtain a valid certificate on the Client and on his account in the AD.

In this task, we'll create a user template and publish it to issue certificates to users with an email address within the domain who manually request it. We'll verify by signing into Client12 as a user and request a certificate from vlabs12-CA, and then verify on DC112 that the issued certificate is shown.

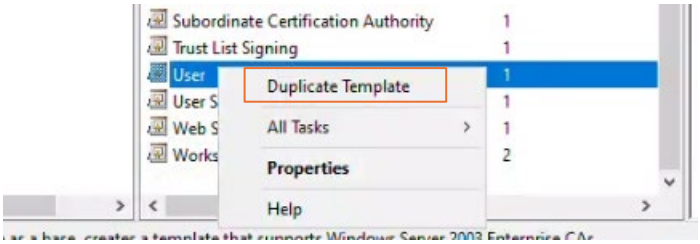
We need to configure and publish Certificate Templates in order to issue user certificates, so start by going to the Certification Authority console (certsrv.msc)



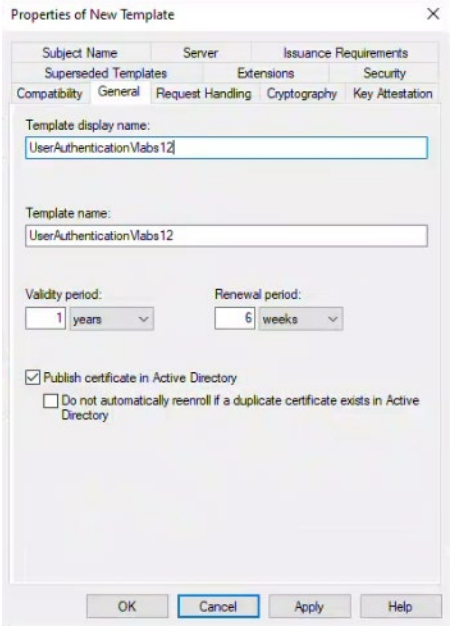
Expand your CA name and right-click on Certificate Templates → Manage



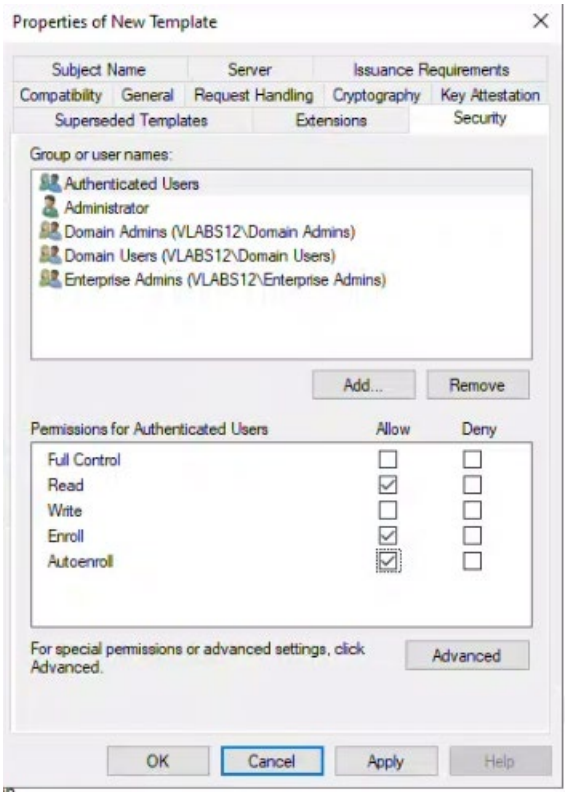
Scroll down to find User, right-click and select duplicate template



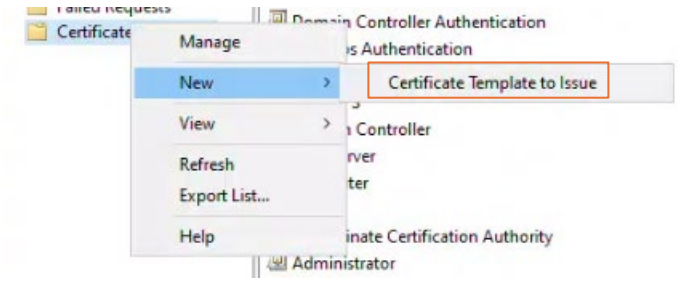
Go to the General tab and set a template display name



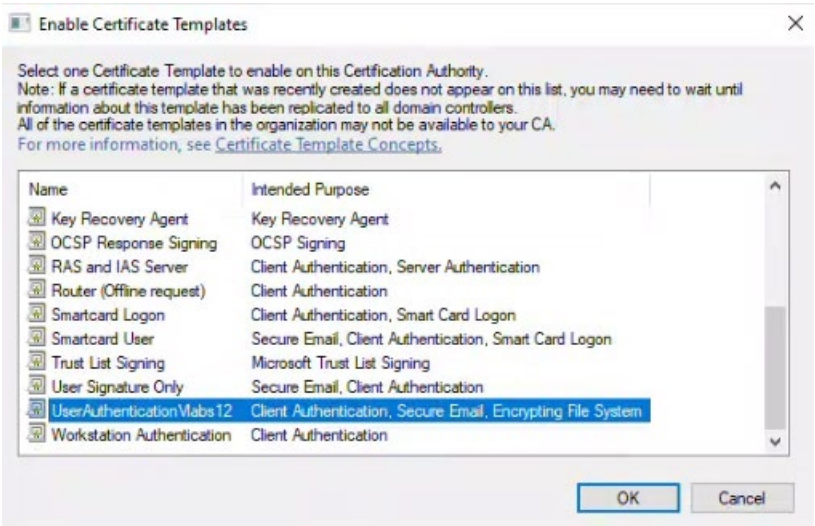
Next go to the Security tab and make sure to grant Authenticated Users enroll and autoenroll permissions. Autoenroll permissions will be used later when setting up a GPO to automatically grant certificates to authenticated users on the domain.

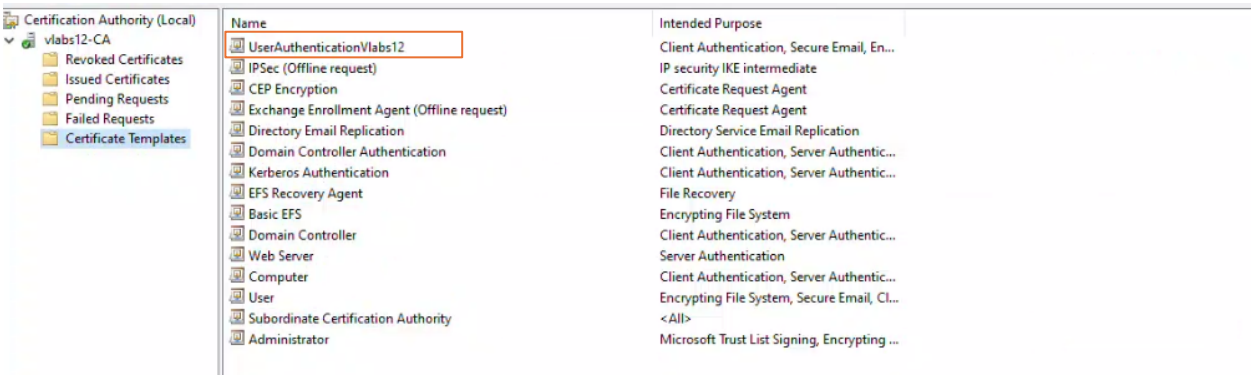


Back in Certification Authority, right-click on Certificate Templates → New → Certificate Templates to Issue



Select the new template we just created and click OK

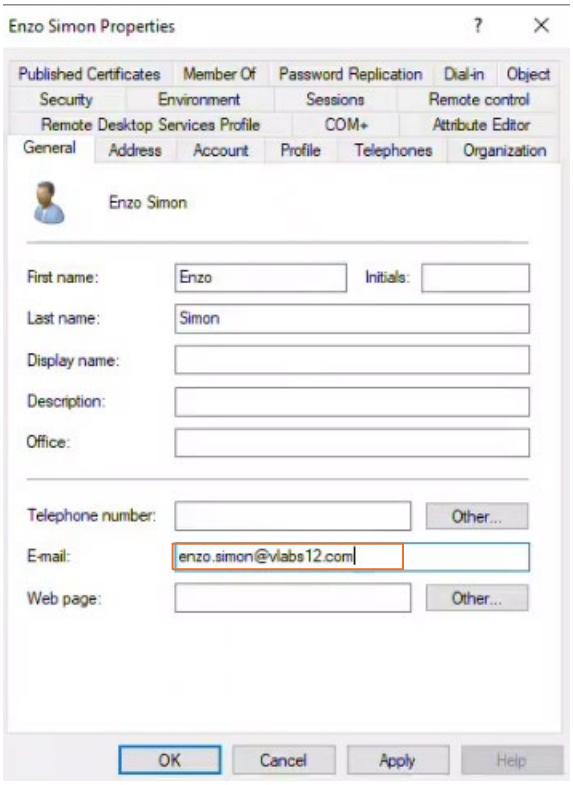




Before we sign in with a user on Client12, we have to first make sure they have an email address or assign one to them.

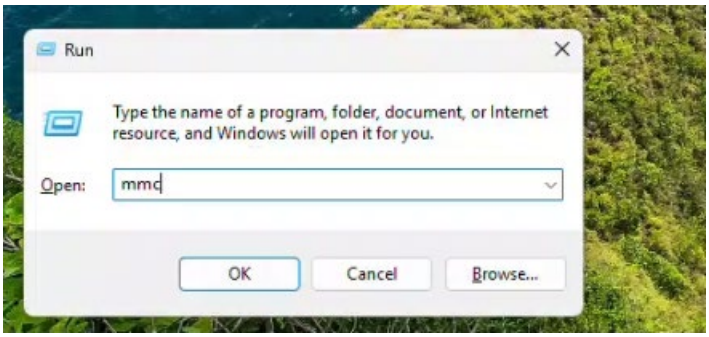
Go to AD Users and Computers, choose a user, right-click and select Properties.

I'll use Enzo Simon from Accounting and give him the email enzo.simon@vlabs12.com

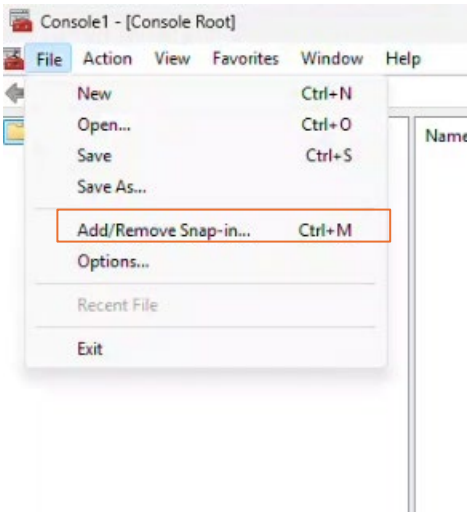


Now sign-in as Enzo on Client12

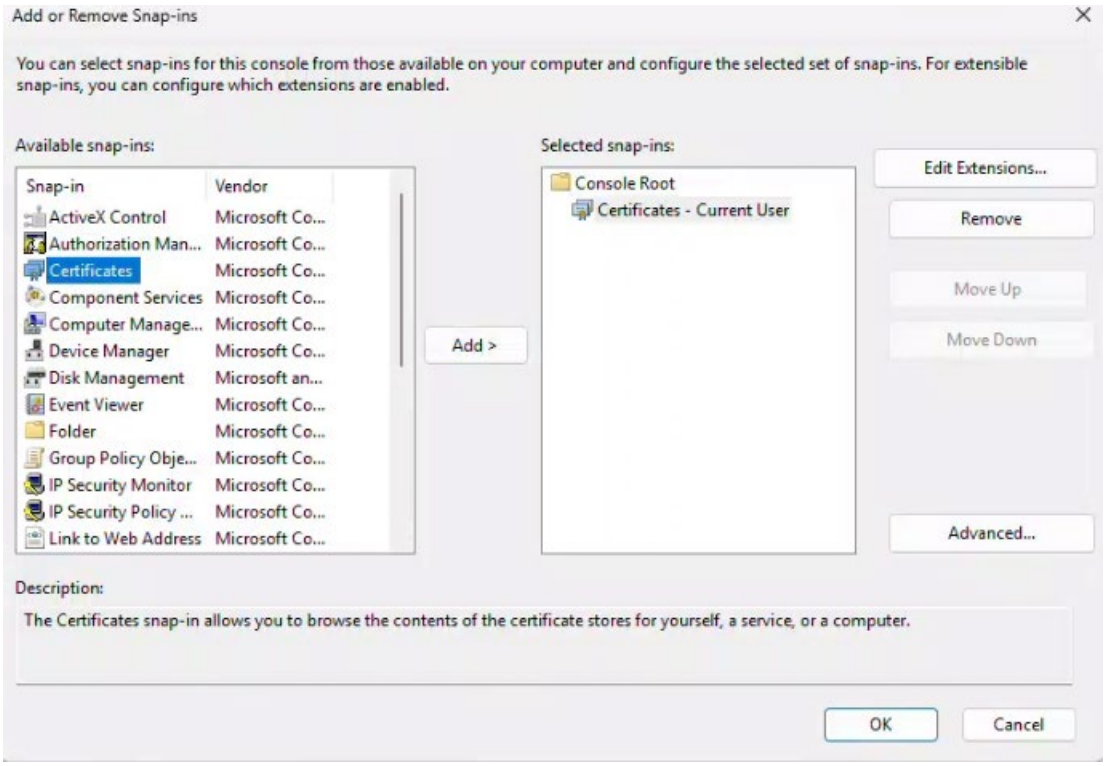
Once signed in, click Win+R for Run and enter mmc



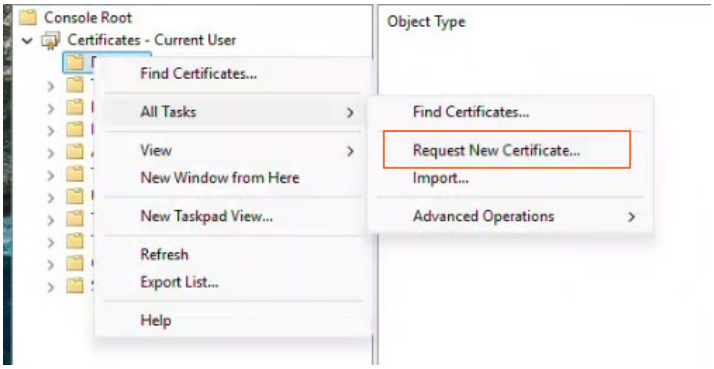
Click on File → Add/Remove Snap-in



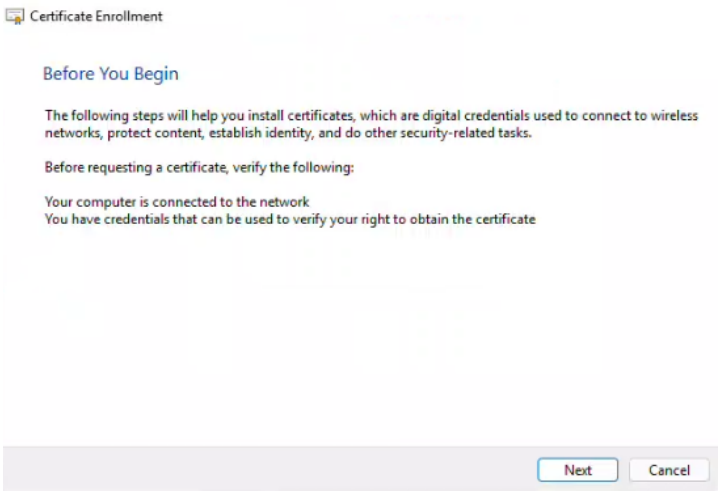
Select Certificates → Add. It'll add current user. Click ok.

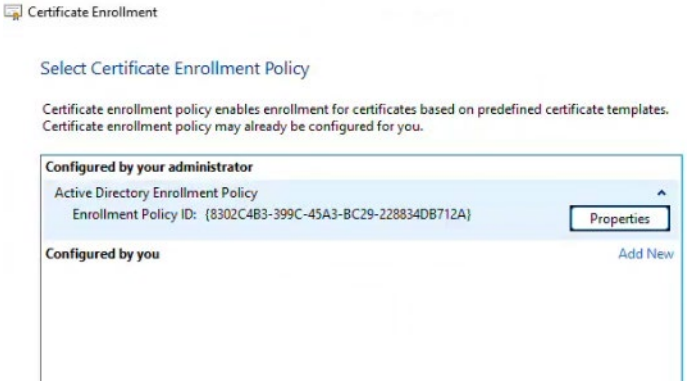


Expand Certificates – Current User, right-click on Personal → Request New Certificate

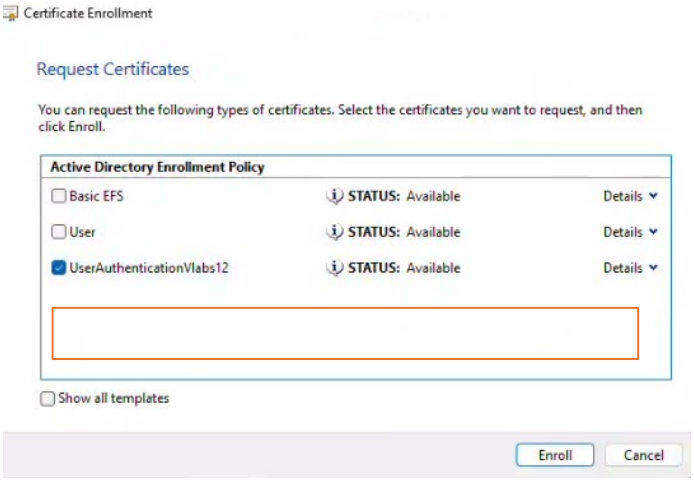


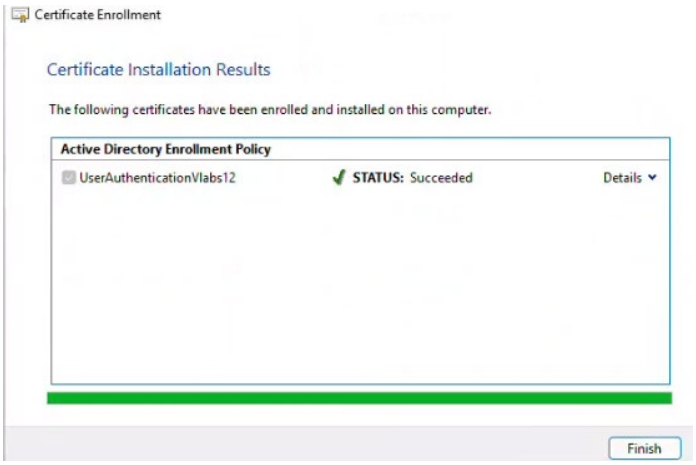
Click next and next



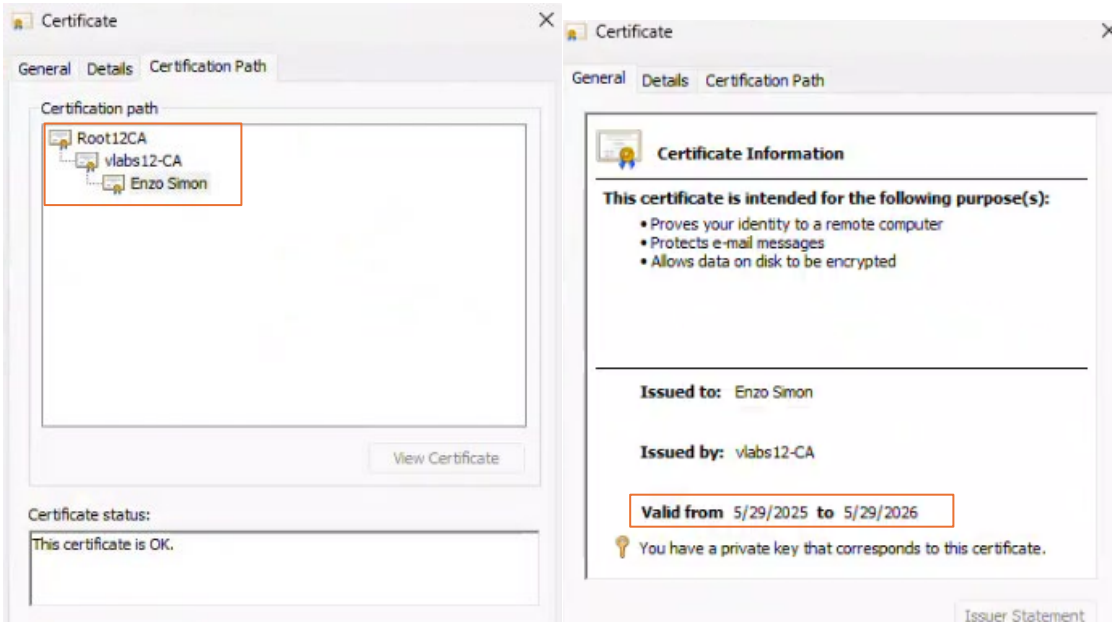


Select the UserAuthenticationVlabs12 certificate and then click Enroll



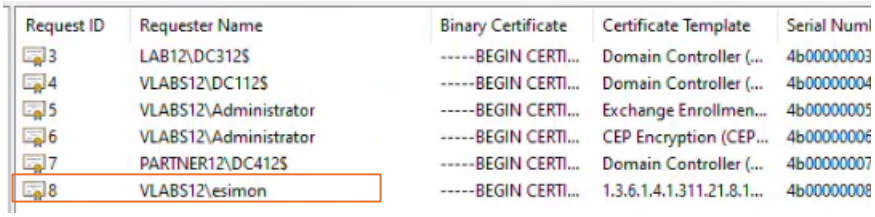


You can see the newly issued certificate for Enzo Simon, the date issued, who it was issued by, etc. under certificates and if you double click on it, you can see the expiration date along with the certification path

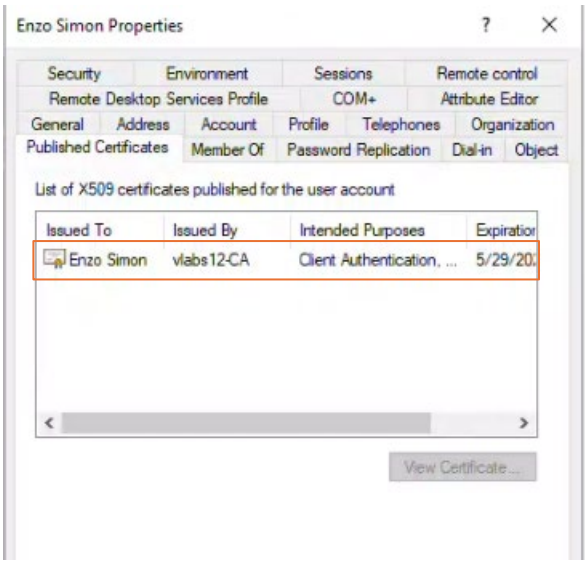


Verify that the user has obtained a valid certificate on the Client and on his account in the AD.

Back on DC112, go back to Certification Authority and verify the issued certificate to Enzo Simon in Issued Certificates



Also check in AD Users and Computers (or ADAC). Right-click on Enzo Simon → Properties → Published Certificates



Task 2: Enable Automatic Certificate Enrollment in AD

Configure Group Policy settings to allow automatic certificate enrollment

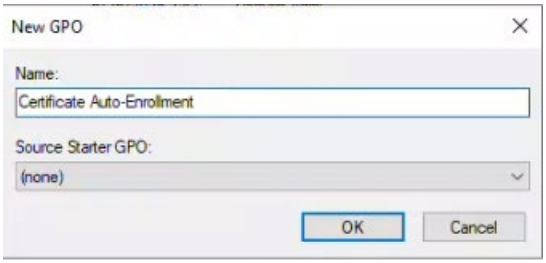
Open a session on Client12 using a different user from task 1, that has an email address. and verify if he has received automatically the necessary certificate

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

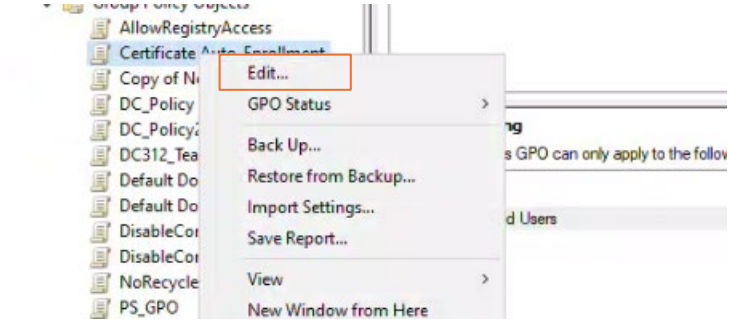
In this task, we'll create a GPO and edit it to allow automatic certificate enrollment. Meaning any user within the domain with an email address will automatically receive a certificate without manually requesting it. We'll test the new GPO by signing into Client12 as any other user and verify that we've received their certificate. Finally, we'll verify in DC112 that the issued certificate to that user is present.

Start by creating the new GPO in Group Policy Management. Right-click on Group Policy Objects → New

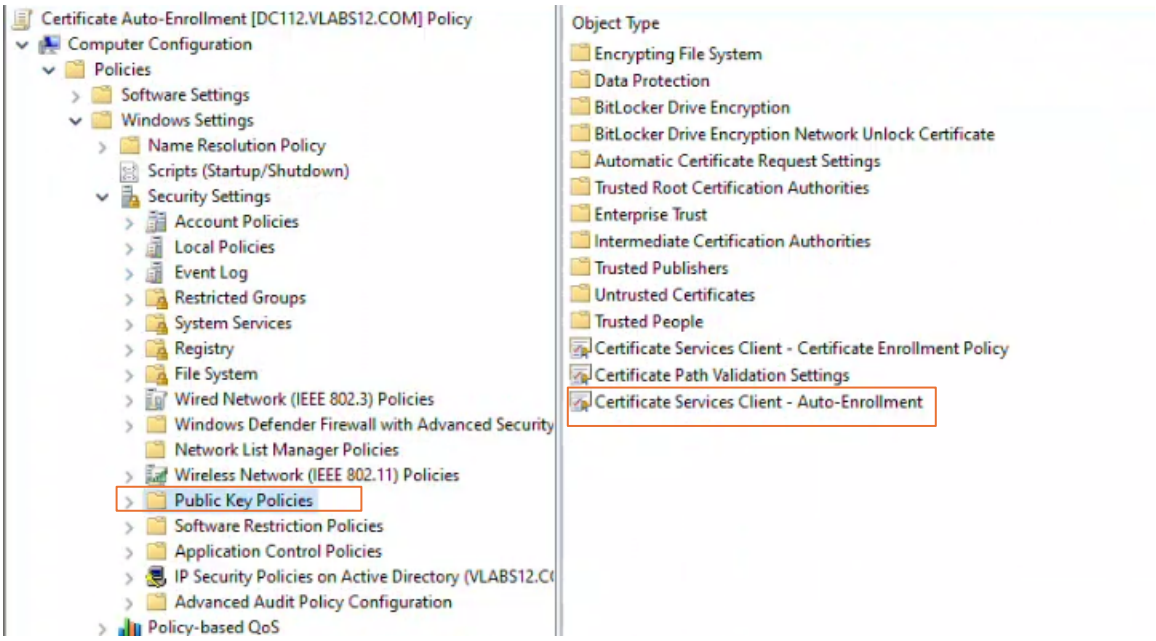
Name it Certificate Auto-Enrollment



Right-click on the GPO → Edit

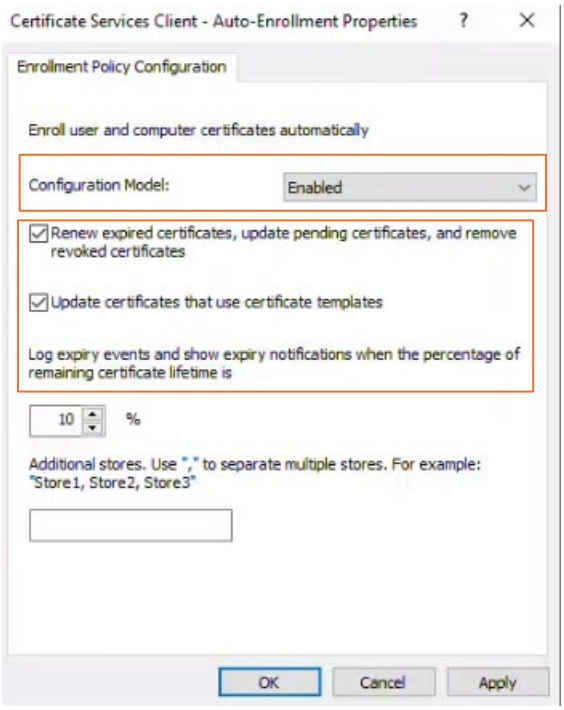


Under Computer Configuration → Policies → Windows Settings → Security Settings, click on Public Key Policies

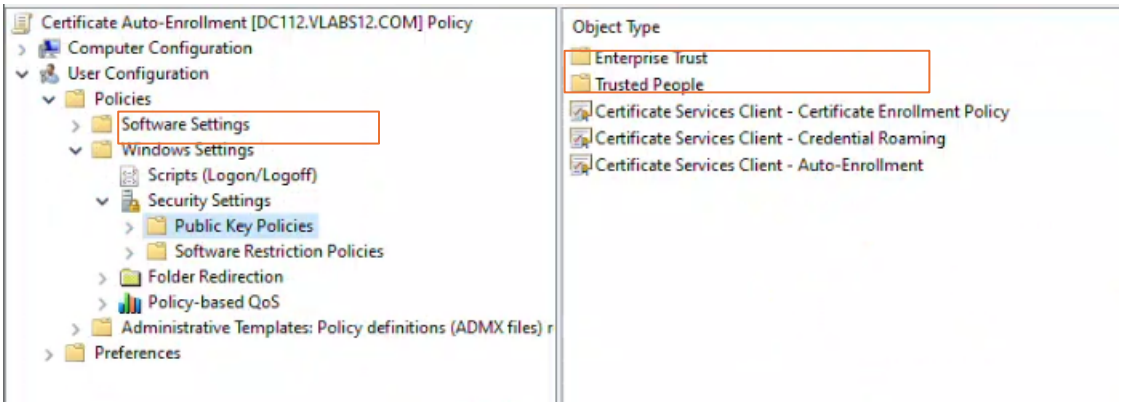


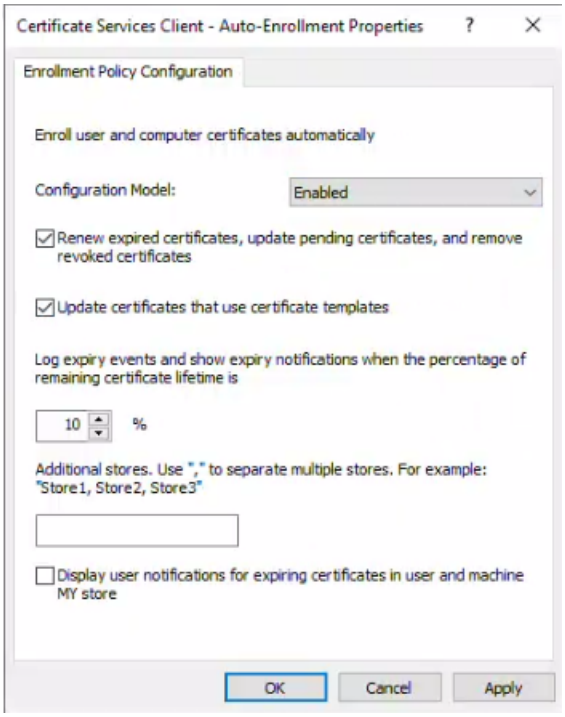
Click on Certificate services client – auto enrollment

Change the configuration model to Enabled, and tick the two boxes Renew expired certificates and update certificates using templates. Click Apply

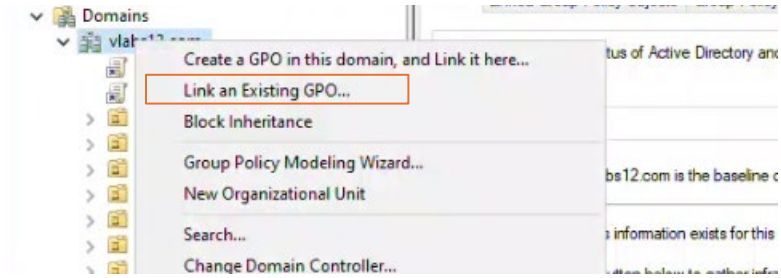


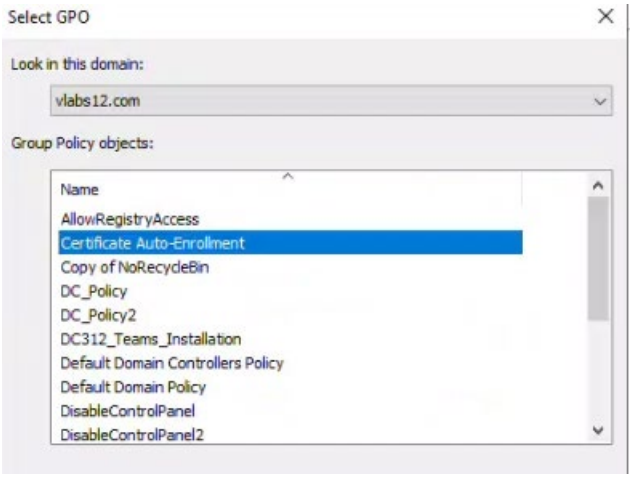
Repeat the process under User Configuration





Exit the Editor and link the GPO to the domain



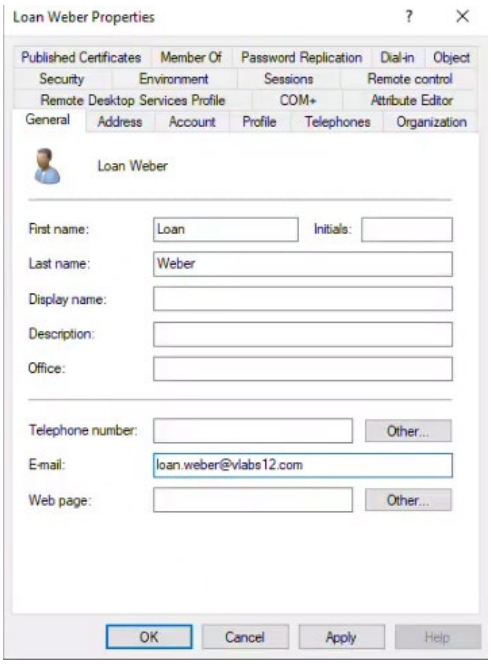


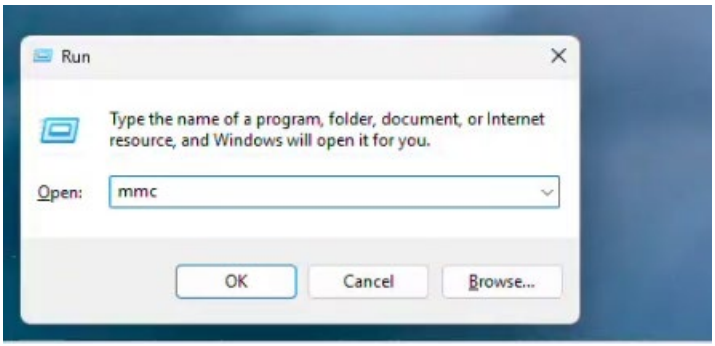
Always do a gpupdate /force after having made changes to a GPO

```
PS C:\Users\Administrator.DC112> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator.DC112>
```

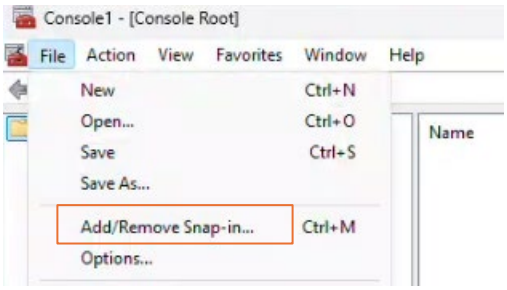
Now sign-in to Client12 with a user who has an email address.

I'll give Loan Weber the email loan.weber@vlabs12.com and then sign in to Client12

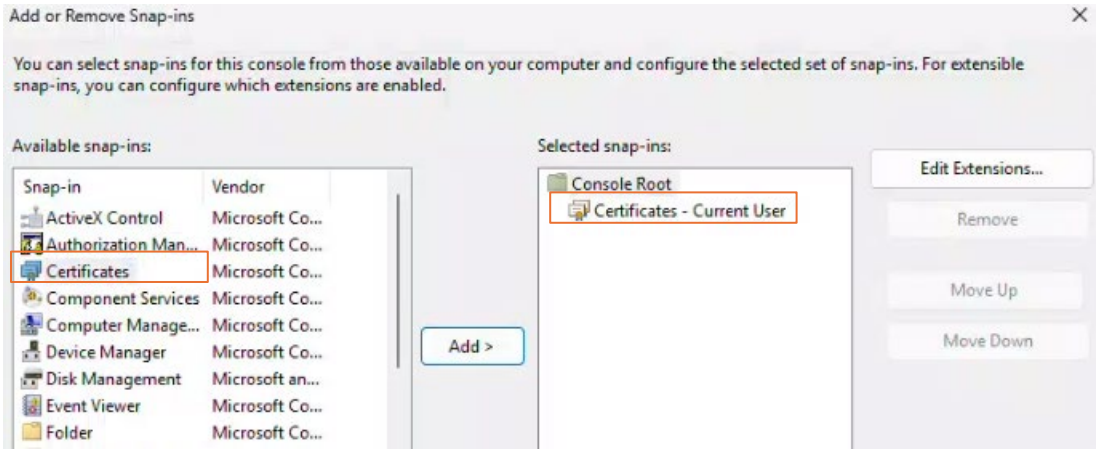




Go to File → Add/Remove Snap-in..

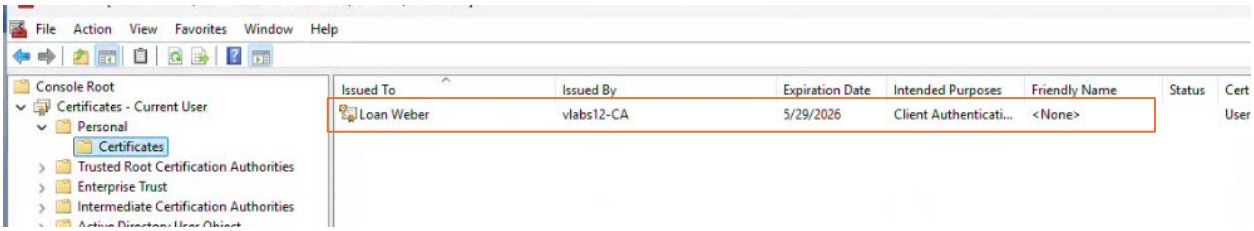


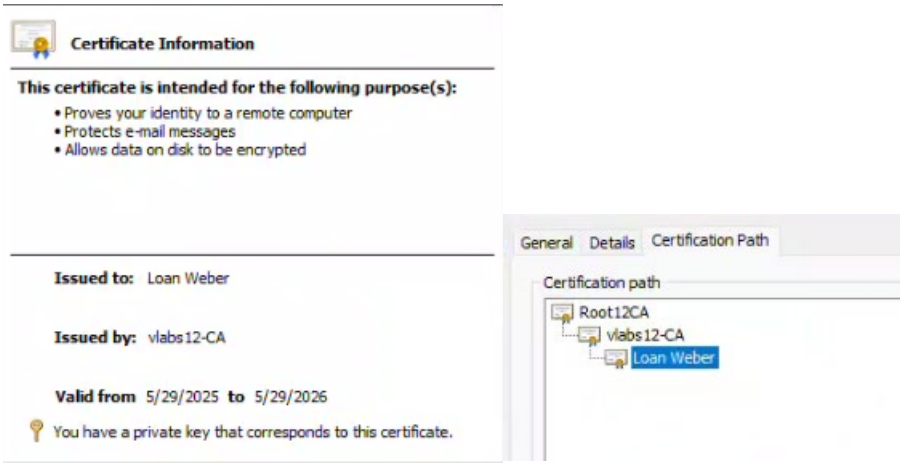
Certificates → Add



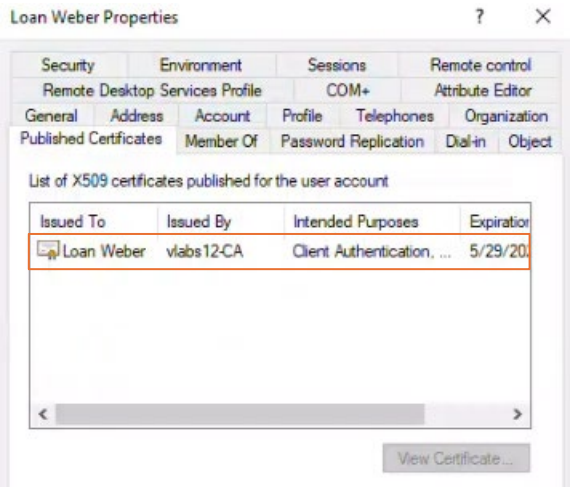
Expand Certificates – Current User

In Personal, click on certificates and you'll see the automatically issued certificate to Loan Weber





Back on DC112, go to AD Users and Computers (or ADAC) and verify that he has a valid certificate in Properties → Published Certificates



Task 3: Issue Digitally Signed Documents and Files

Issue Digital Signature Certificates from Enterprise CA

Open a session on Client12 with a user and manually request a user certificate

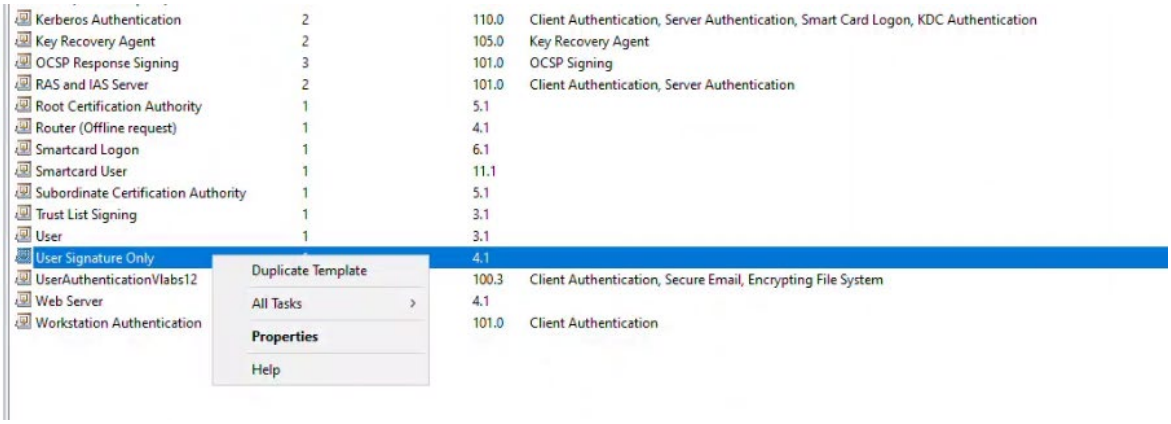
Verify that he has received this certificate.

Digitally signing documents and files in Active Directory ensures authenticity, integrity, and security. It verifies the signer's identity, prevents unauthorized modifications, and provides non-repudiation, meaning the signer cannot deny their involvement. In AD, these signatures often leverage Public Key Infrastructure (PKI) for encryption, making transactions and document management more secure and efficient. In this task, we'll set up digital signing of documents and files, and then verify like in the previous tasks using a user on Client12.

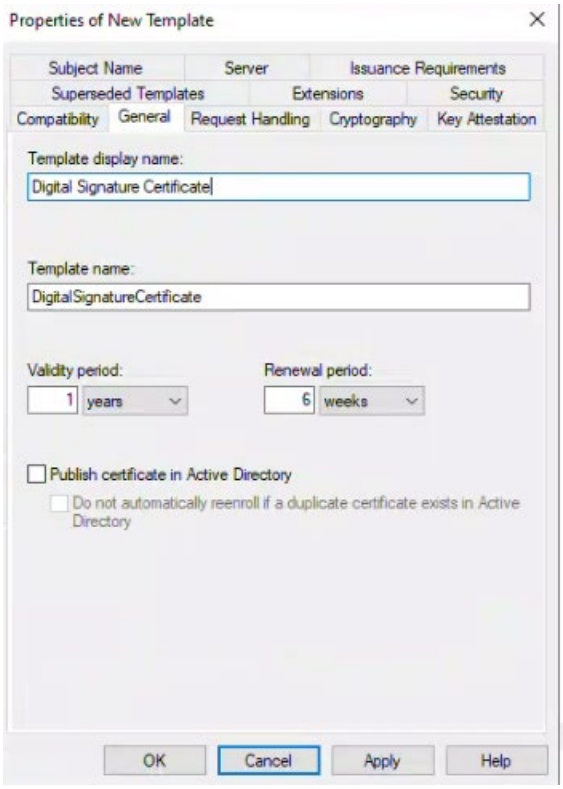
We need to configure a Digital Signing Certificate Template using certificate template console

Press on Win+R and type certtmpl.msc to open the console

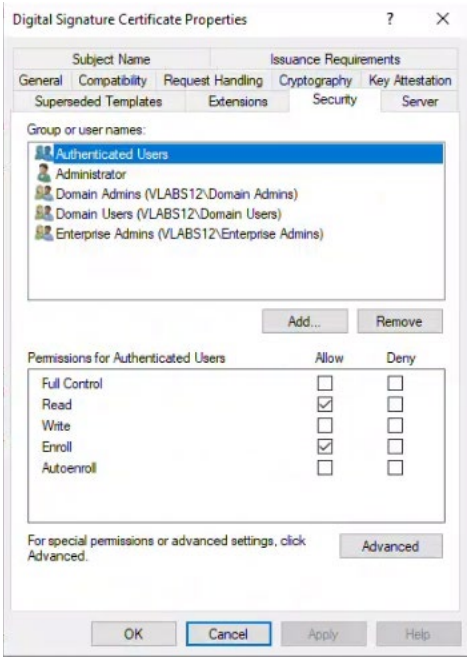
Right click on User Signature Only template and select Duplicate Template



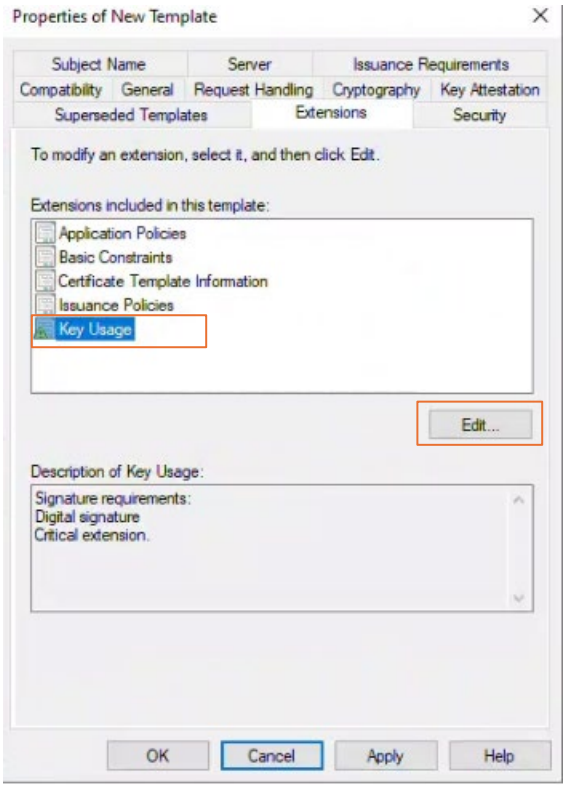
Go to the General tab and set a display name



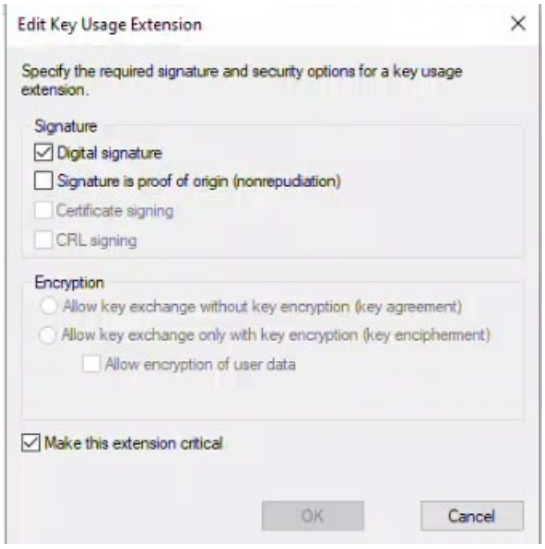
Go to the Security tab and give Authenticated Users the permissions Read, Enroll (we won't be adding Autoenroll this time since we need to test by manually requesting the certificate and we have a GPO specifically for autoenroll)



In the Extensions tab, click on Key Usage → Edit



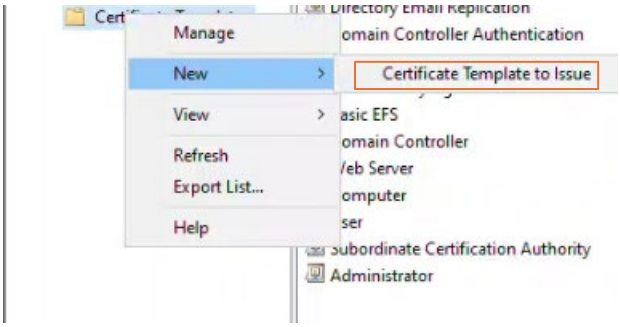
Verify that Digital signature is checked



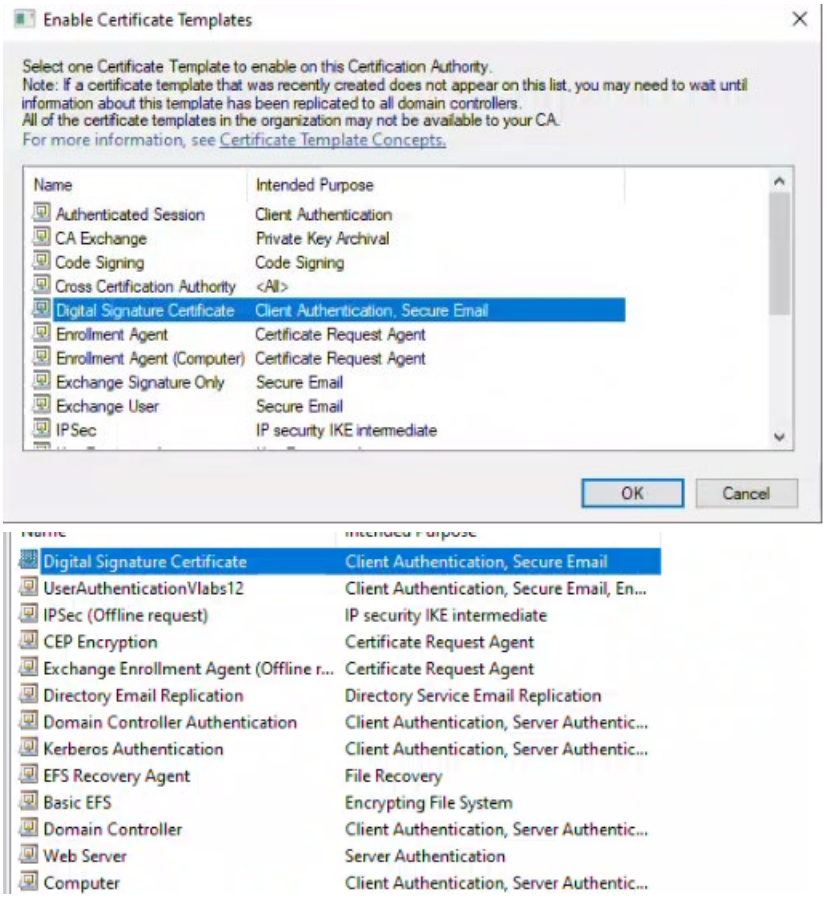
Now we need to publish the template to the CA

Open Run (Win+R) and type certsrv.msc

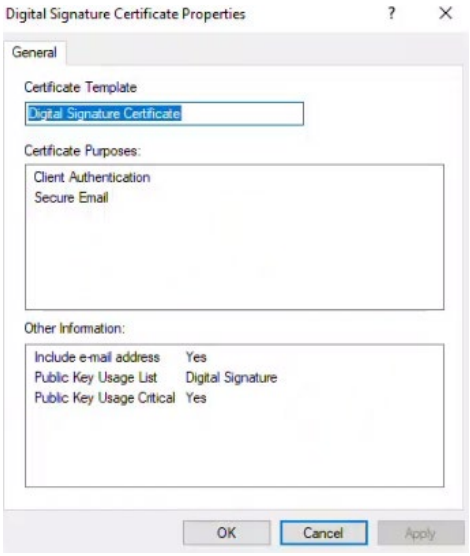
Right-click on Certificate Templates → New → Certificate Template to Issue



Select the Digital Signature Certificate we just created. Click OK.

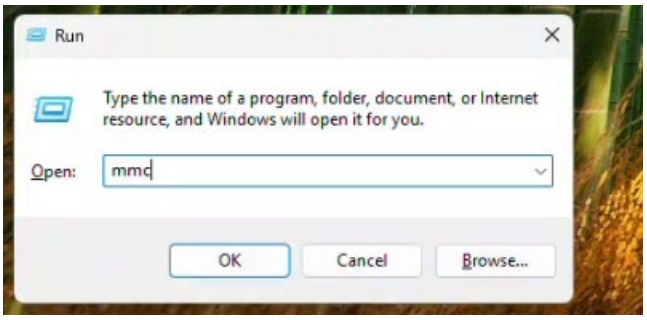


Double-click it to see it’s purposes.

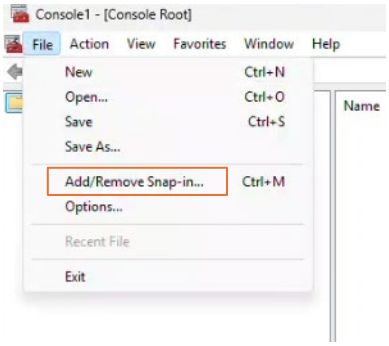


Now we need to test with a user on Client12. I'll use Louis Roux this time.

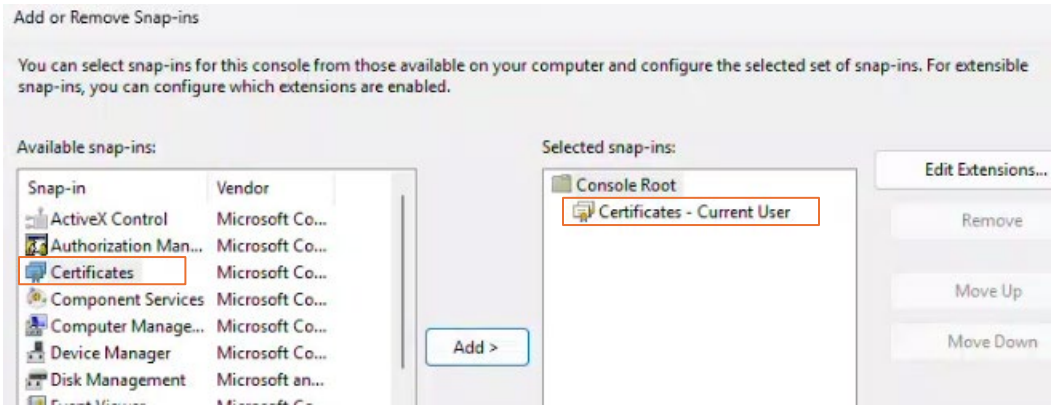
Use Run and type mmc



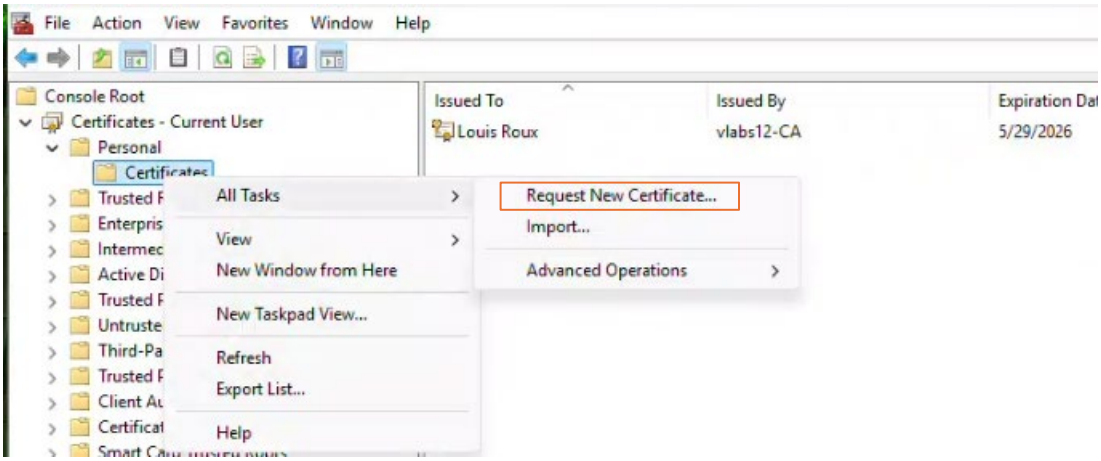
Go to File → Add/Remove Snap-in..

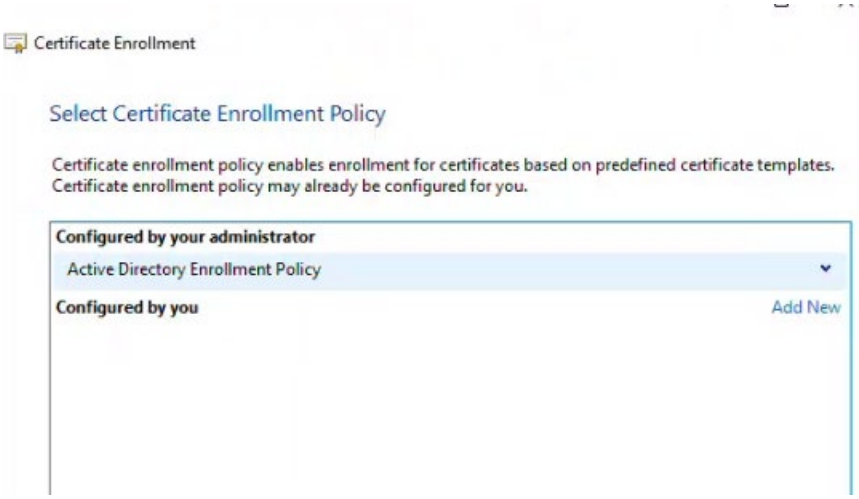


Go to Certificates → Add

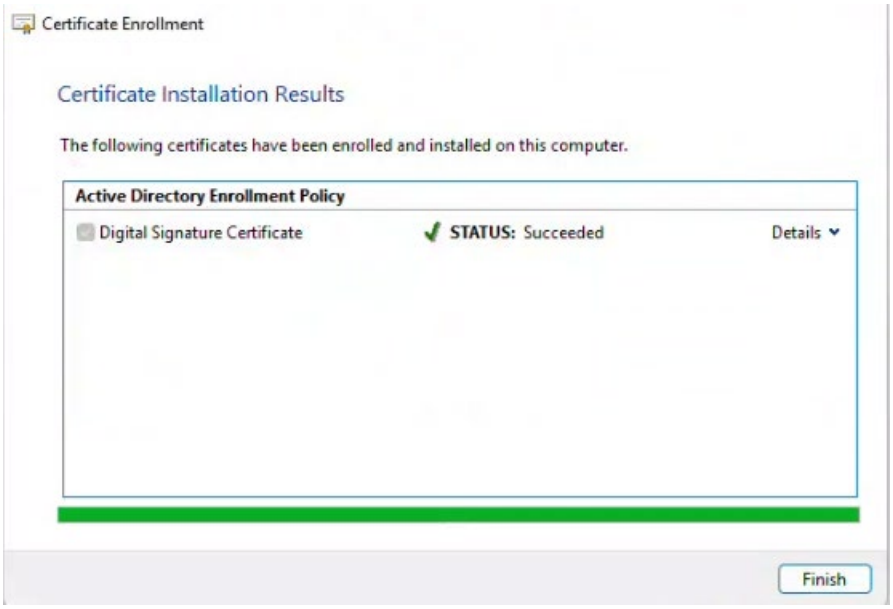


Expans Certificares – Current User, pull down Personal and right click on Certificates → All Tasks → Request New Certificate



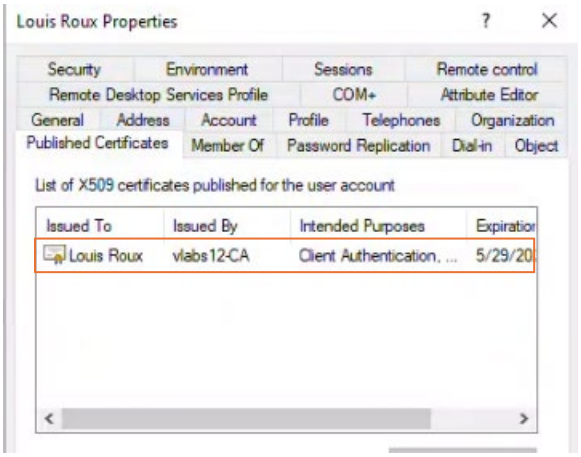


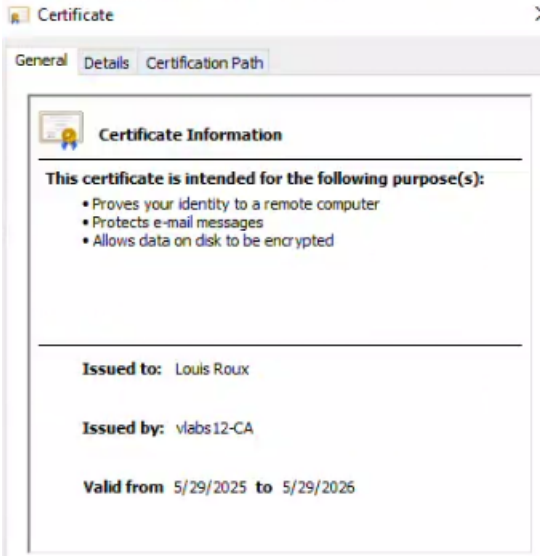
Select the Digital Signature Certificate and then click Enroll



Now the new certificate will be shown along with the user authentication autoenroll one from the GPO

Back in AD Users and Computers, go to Louis Roux's properties and verify he's received his new certificate under Published Certificates





Not part of the task, but to see how this certificate would be used to digitally sign a document, you would open Word, PDF or Excel, go to File → Info → Protect Document. You'd then click on Add a Digital Signature and then select the issued certificate and click Sign.

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

Create an SSL certificate on the Enterprise CA

Request and issue an SSL/TLS Certificate for dc112.vlabs12.com

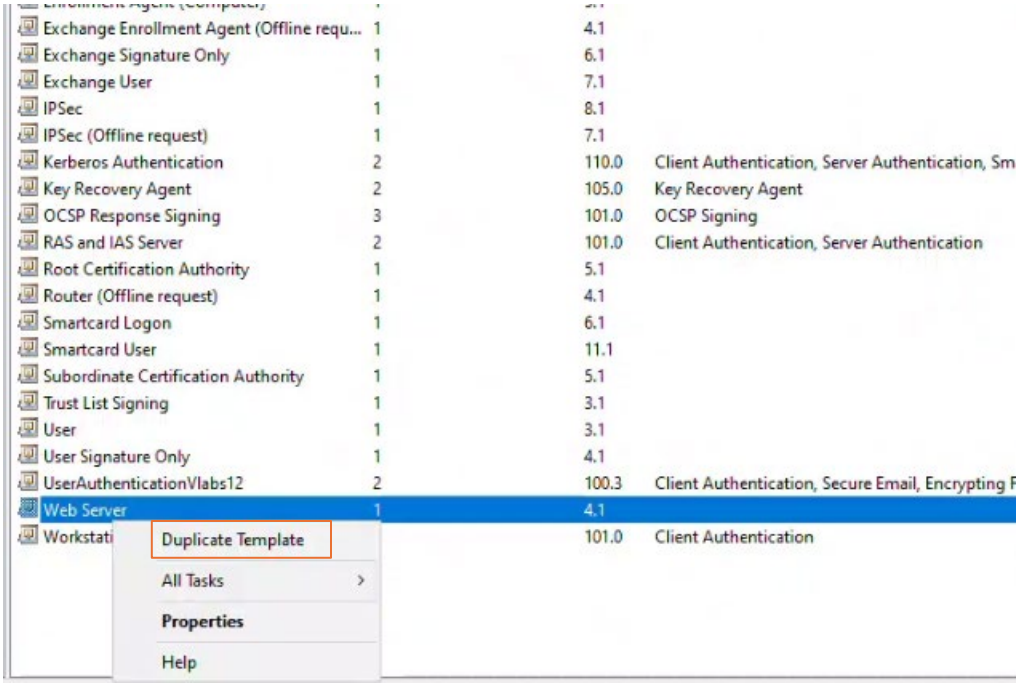
Bind the certificate to the local web server (IIS)

Test and verify HTTPS access to dc112.vlabs12.com

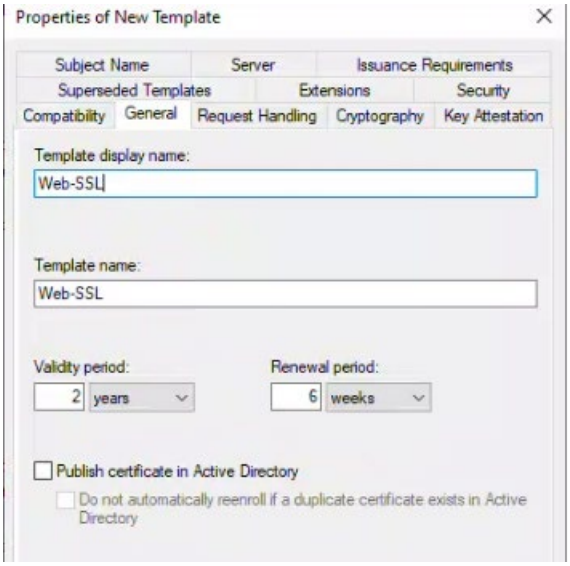
During this task, the internal web server will be secured using SSL/TLS certificates to ensure encrypted and safe communication. A trusted SSL certificate will be created on the Enterprise CA and issued for the designated server, allowing it to authenticate securely. The certificate will then be bound to the local web server, enabling HTTPS access and ensuring data exchanged between users and the server remains private. Finally, the setup will be tested on Client12 to verify that secure connections are functioning properly, enhancing overall security and trust in the internal network

On DC112, open Certification Authority. Right click on Certificate Templates and click on Manage

Right click on Web Server → Duplicate Template

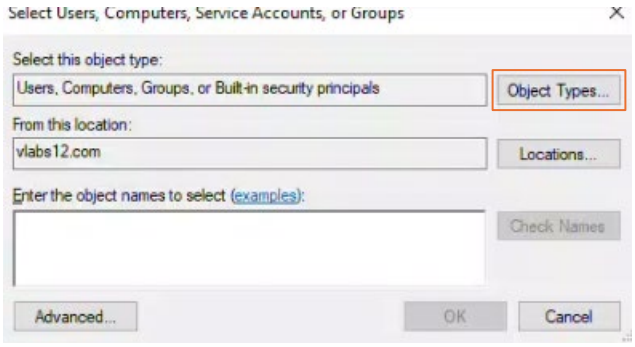


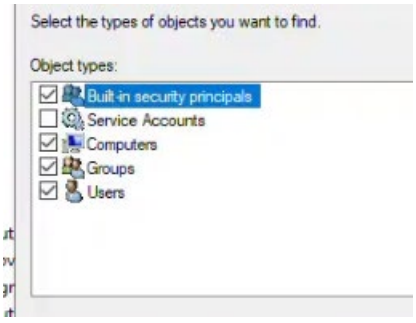
In the General tab, set a display name



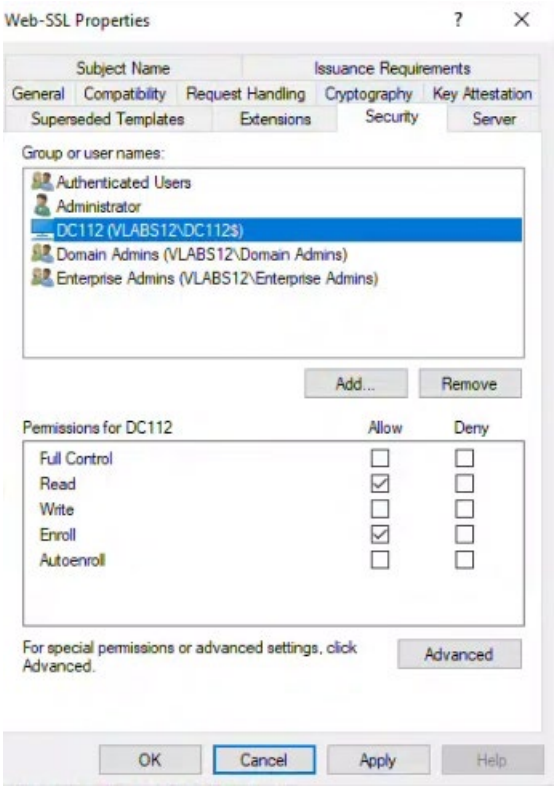
Go to Security and click Add

Click on Object Types and select Computers



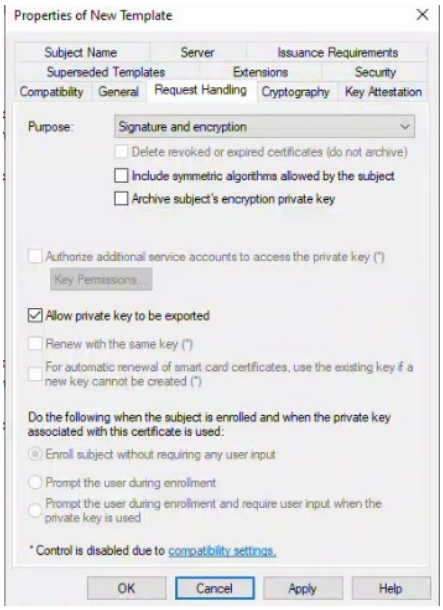


Add DC112

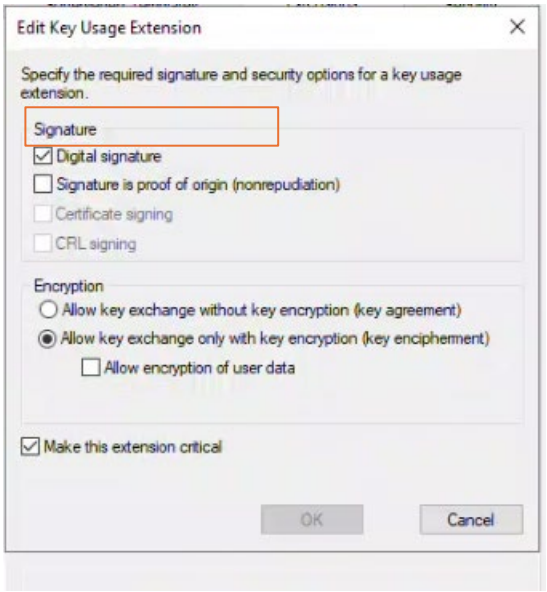


I'm just adding Enroll permissions this time but you can add autoenroll also

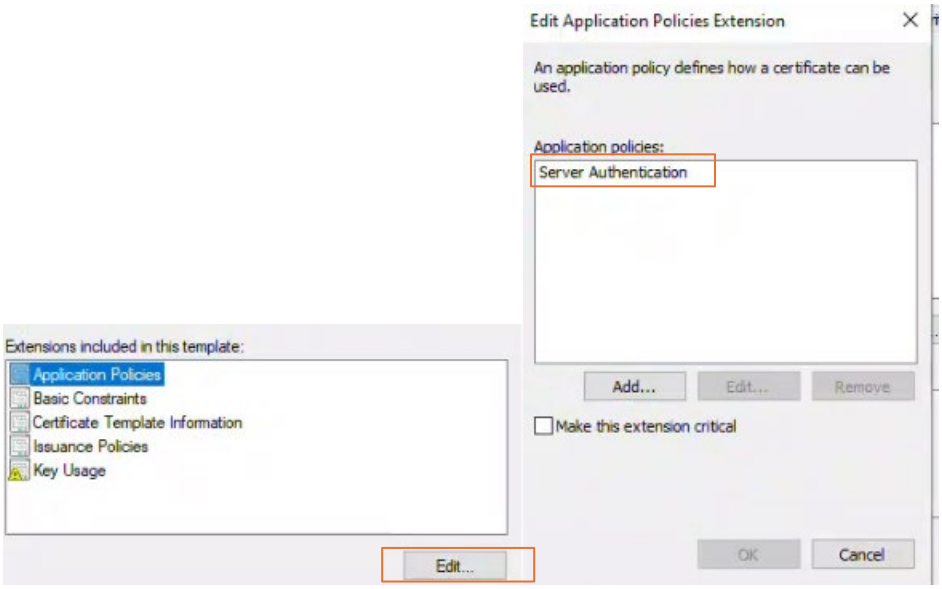
Next, go to Request Handling and check the box Allow private key to be exported



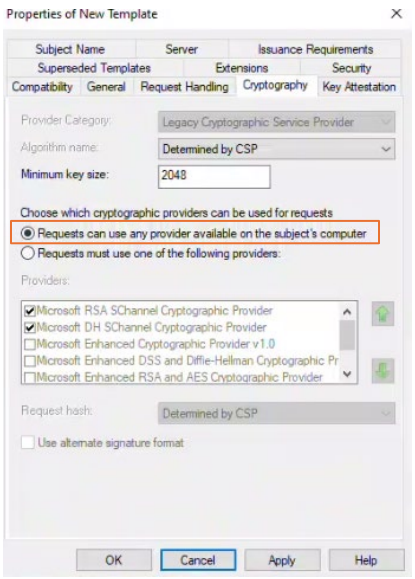
Enable the server authentication usage by going to Extensions → Key usage → Edit and make sure that Digital signature is checked



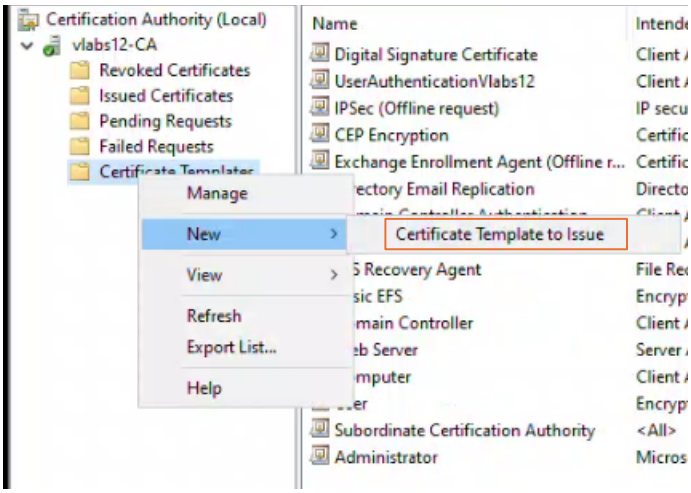
Click on Application Policies and ensure that Server Authentication is present



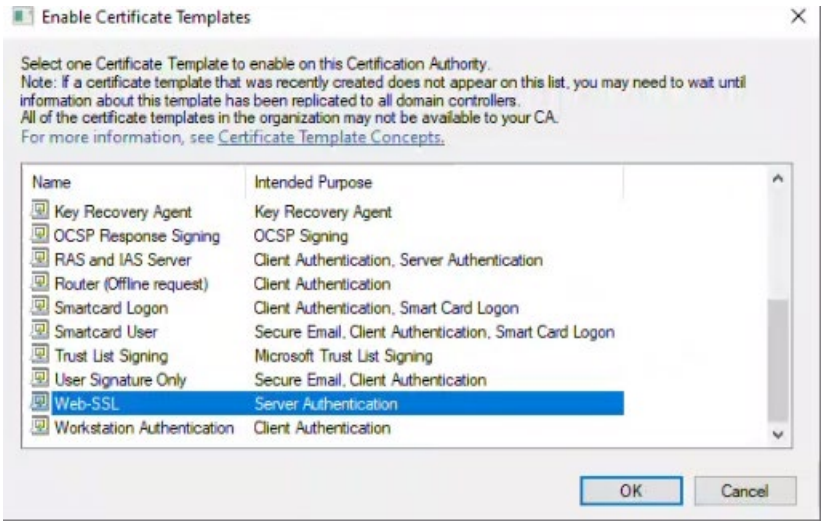
Now go to the Cryptography tab and make sure that “Requests can use any provider …” is checked



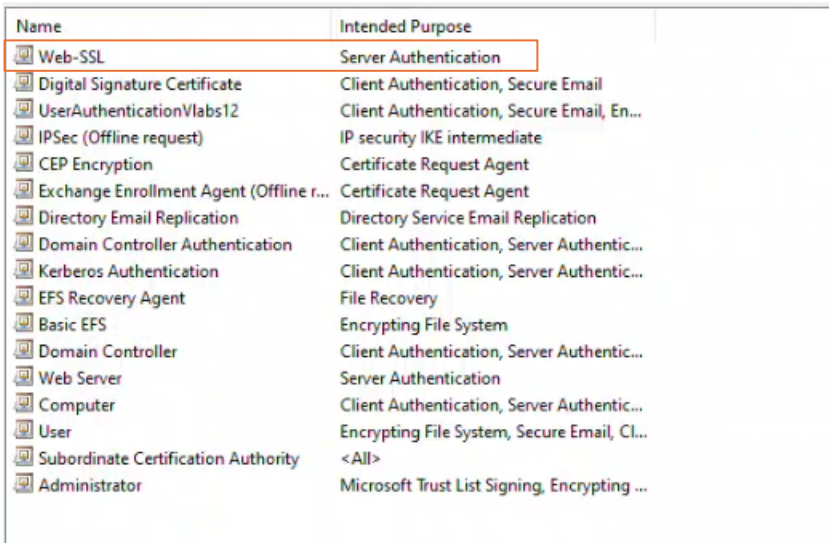
Next we need to publish the template. Go to Certification Authority Console, right click on Certificate Template → New → Certificate Template to Issue



Select Web-SSL and click OK



Now you'll see it published in Certificate Templates



Name	Intended Purpose
Web-SSL	Server Authentication
Digital Signature Certificate	Client Authentication, Secure Email
UserAuthenticationVlabs12	Client Authentication, Secure Email, En...
IPSec (Offline request)	IP security IKE intermediate
CEP Encryption	Certificate Request Agent
Exchange Enrollment Agent (Offline r...	Certificate Request Agent
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting ...

Restart the certsvc service using PowerShell:

Restart-Service certsvc

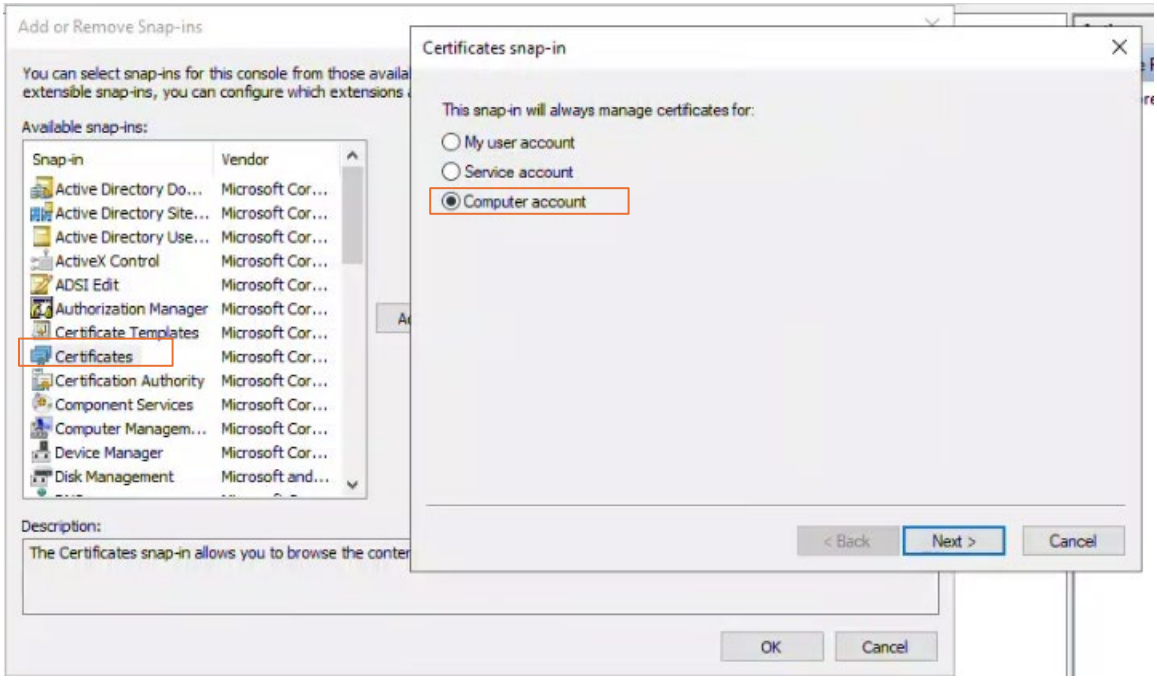
```
PS C:\Users\Administrator.DC112> Restart-Service certsvc
PS C:\Users\Administrator.DC112>
```

Request and issue an SSL/TLS Certificate for dc112.vlabs12.com

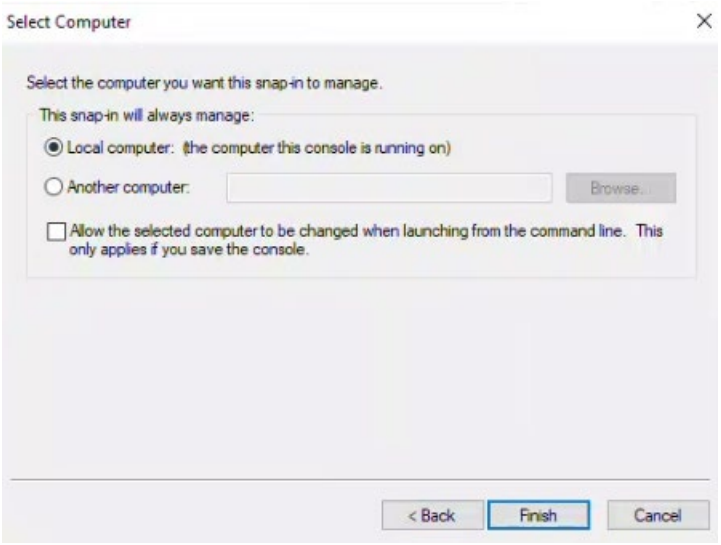
Open mmc on DC112 (Win+R, type mmc)

Go to File → Add/Remove Snap-in..

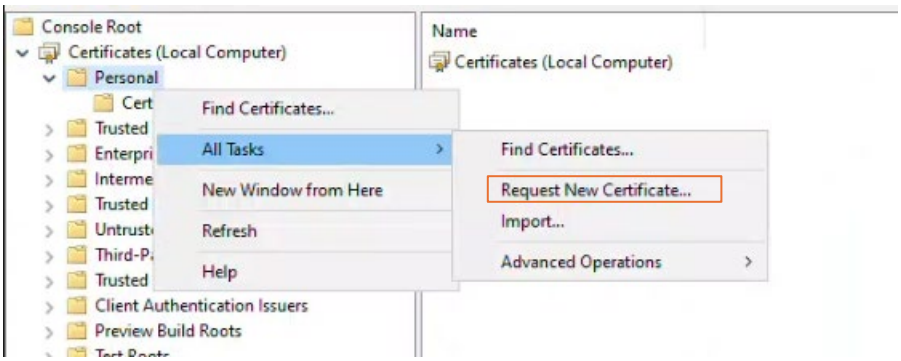
Select “Certificates” → Add and choose Computer account



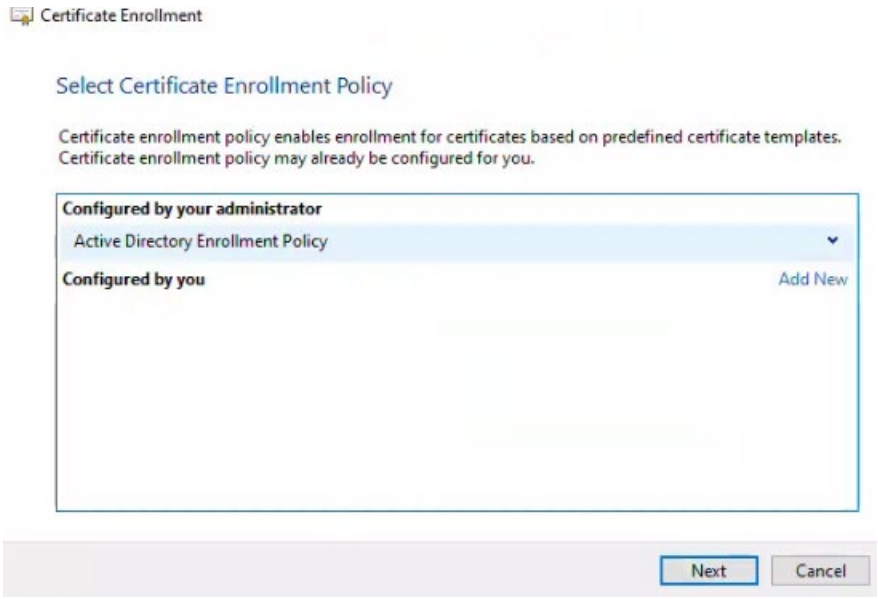
Keep this at Local computer. Click finish.



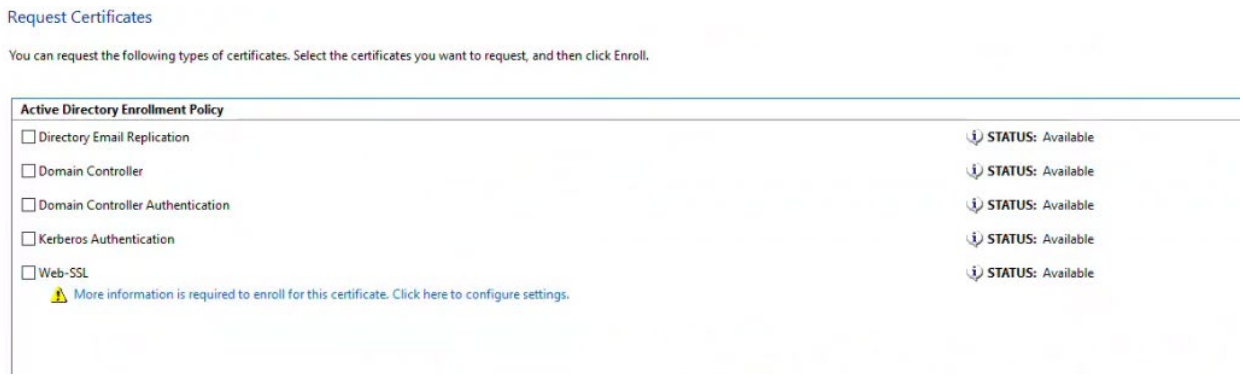
Expand Certificates → Personal → right click on Certificates → All Tasks → Request New Certificate



Click next and select AD Enrollment Policy → Next



Under Web-SSL, click the yellow exclamation triangle thing to input additional information to complete enrollment

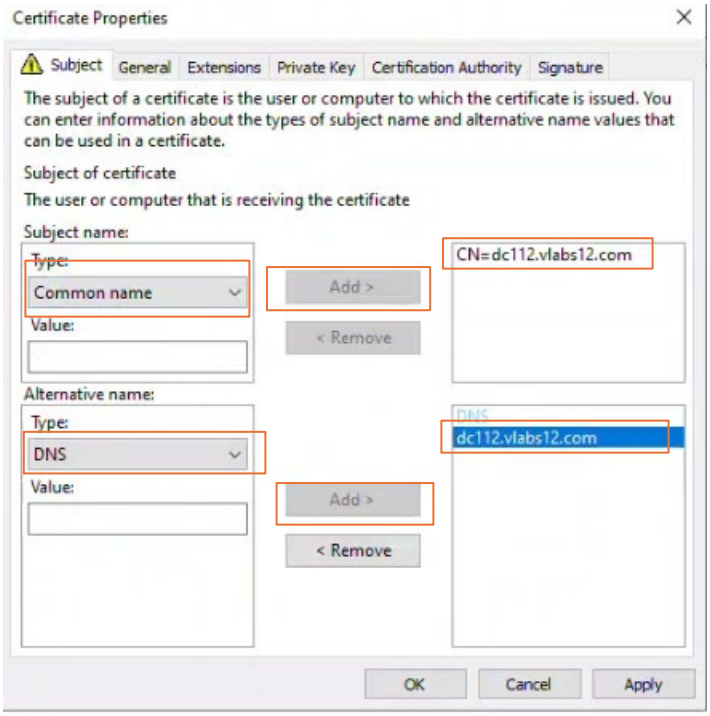


Use the dropdown menu for Type and select Common name

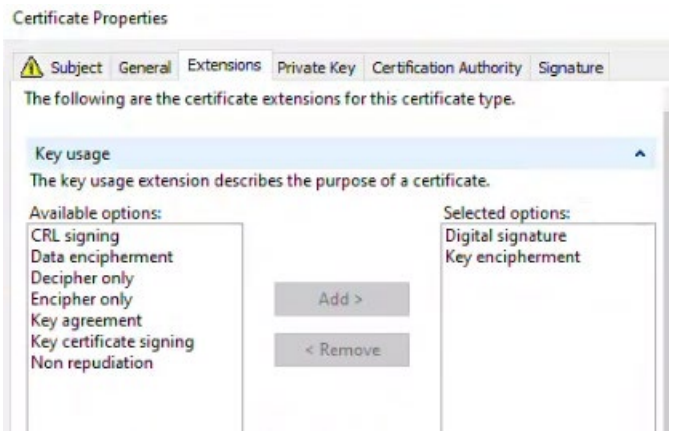
Put dc112.vlabs12.com

Do the same for Alternate name, using the dropdown menu for DNS and putting dc112.vlabs12.com

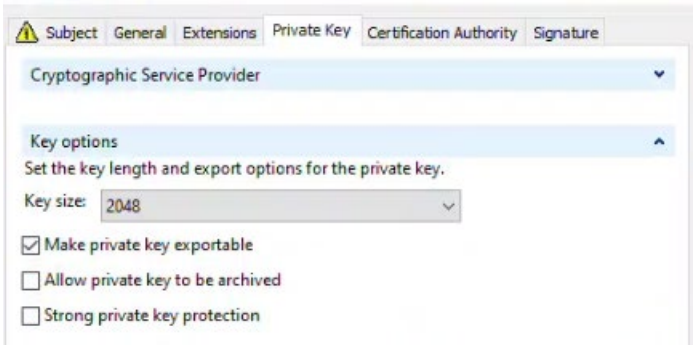
Click Add on both

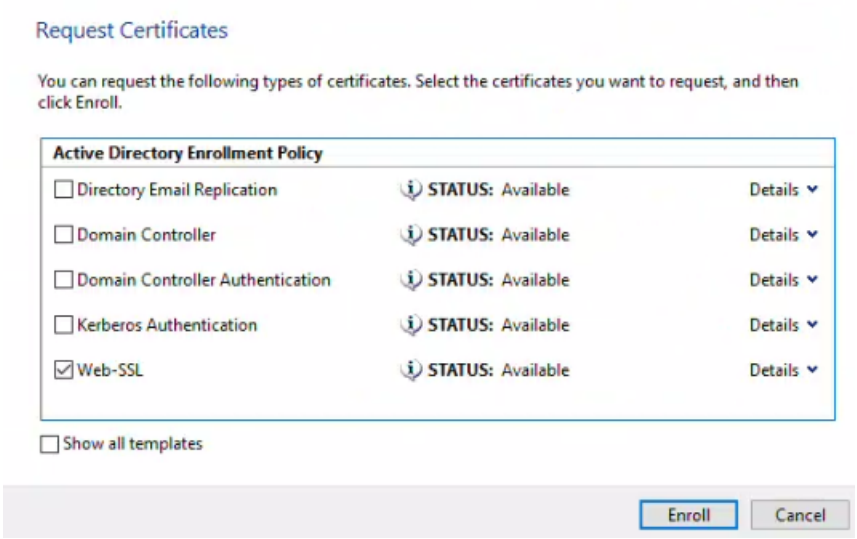


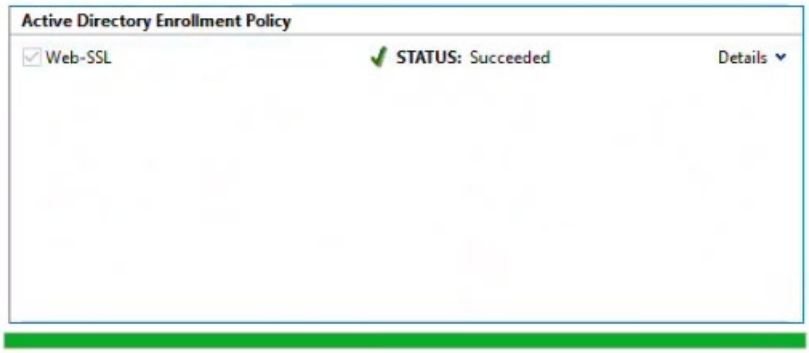
Click Apply and then go to Extensions. Pull down Key usage and make sure that Digital signature and Key encipherment is selected in the options box



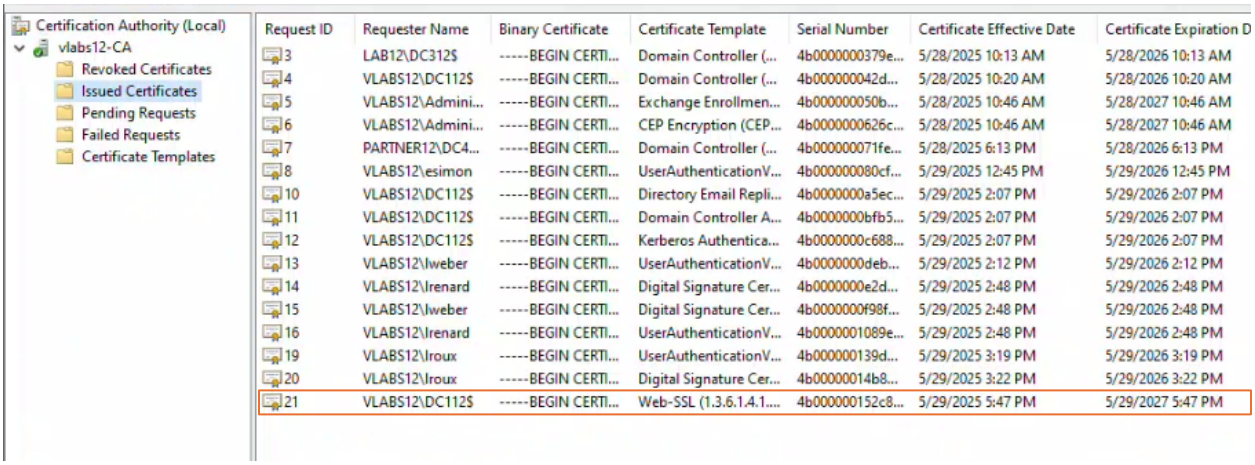
Next click on Private key, pull down the Key options and verify that the Key size is 2048 and the box for Make private key exportable is checked. Click ok, select Web-SSL (the exclamation mark will be gone) and click Enroll.







Verify using Certification Authority that the certificate has been issued



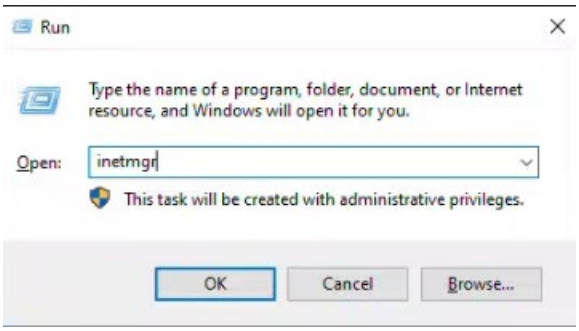
Next we need to bind the certificate to the local web server (IIS)

Using PowerShell, run the following command to install IIS

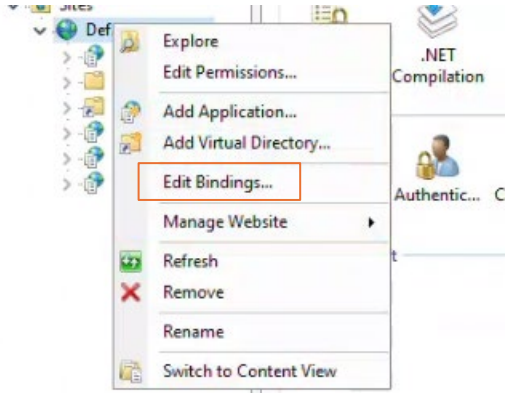
```
PS C:\Users\Administrator.DC112> Install-WindowsFeature -Name Web-Server -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             NoChangeNeeded {}


PS C:\Users\Administrator.DC112>
```

Use Run to open IIS Manager

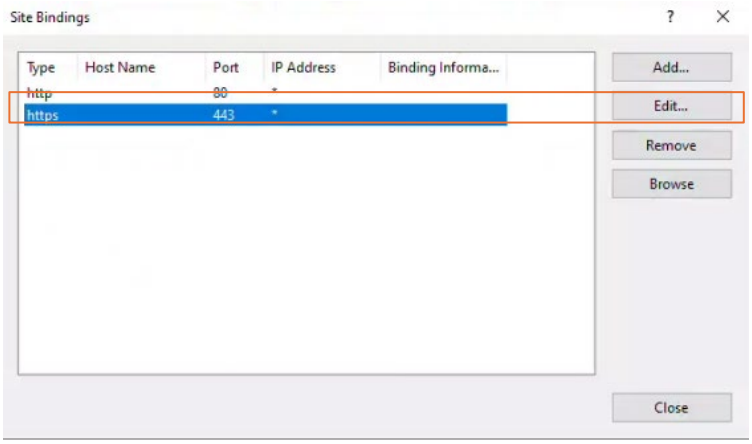
Type inetmgr



Expand DC112, drop down Sites, right-click on Default Web Site and click Edit Bindings



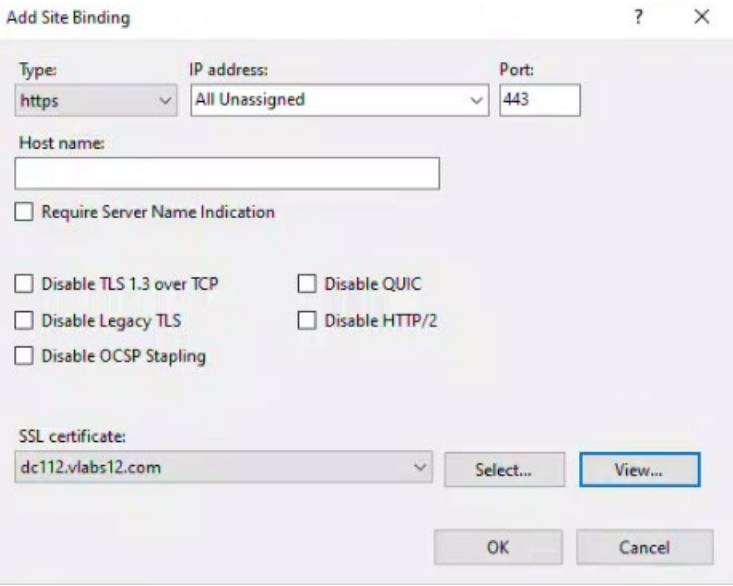
Select https and click on edit



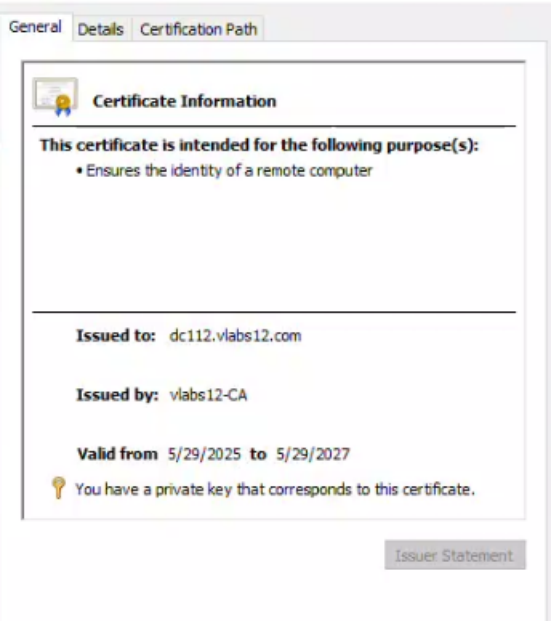
Leave IP address as **All Unassigned**

Leave port **443**

For SSL certificates, use the dropdown menu and select **dc112.vlabs12.com**



You can view the certificate by clicking on view. Click OK.

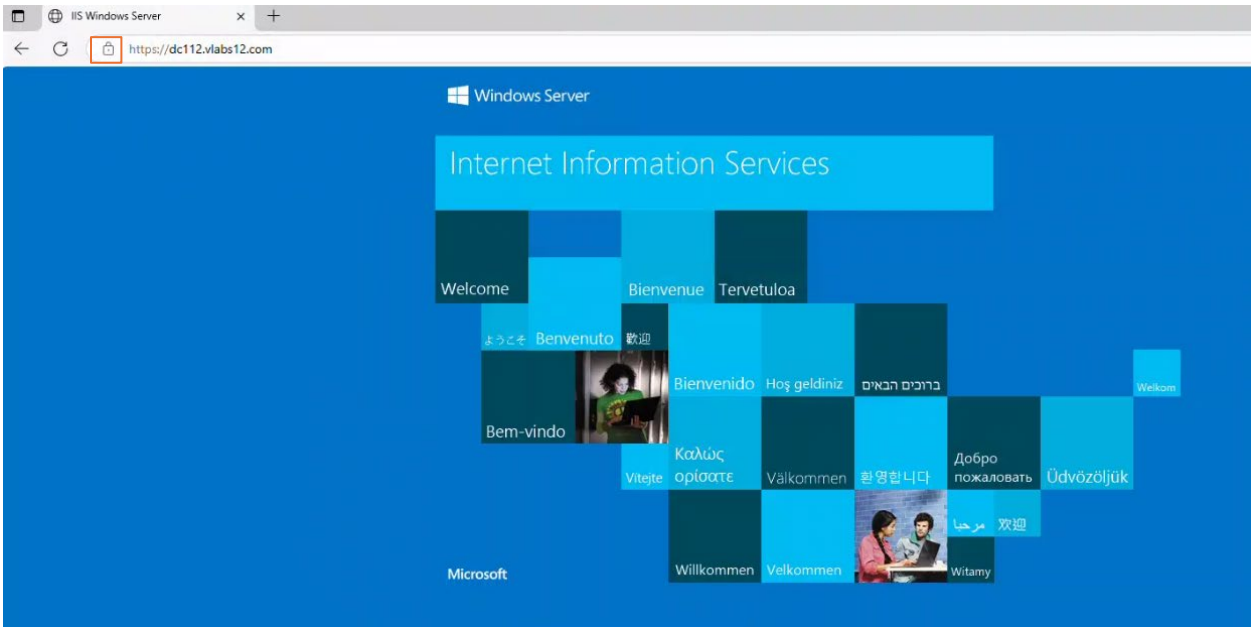


Restart IIS using PowerShell and the following command:

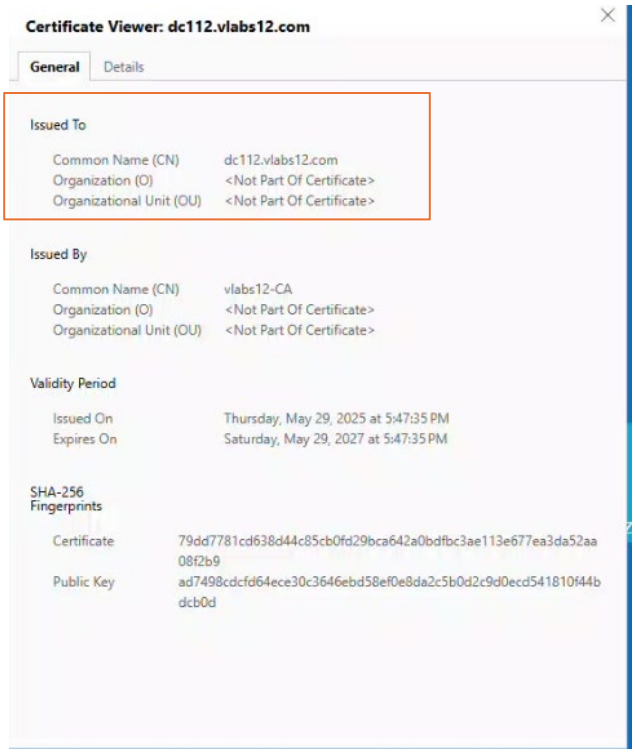
iisreset

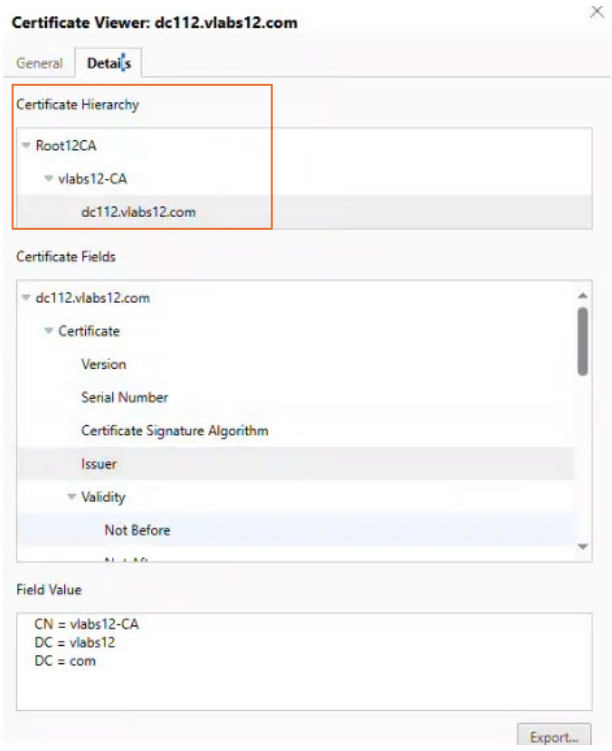
```
PS C:\Users\Administrator.DC112> iisreset

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
PS C:\Users\Administrator.DC112>
```

Test SSL certificate by visiting https://dc112.vlabs12.com on a browser



Click the padlock on the browser and confirm it shows a valid certificate issued by our Enterprise CA.


Certificate Viewer: dc112.vlabs12.com
General
Details
Issued To
Common Name (CN) dc112.vlabs12.com
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) vlabs12-CA
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Thursday, May 29, 2025 at 5:47:35 PM
Expires On Saturday, May 29, 2027 at 5:47:35 PM
SHA-256 Fingerprints
Certificate 79dd7781cd638d44c85cb0fd29bca642a0bdfbc3ae113e677ea3da52aa08f2b9
Public Key ad7498cdcfd64ece30c3646ebd58ef0e8da2c5b0d2c9d0ecd541810f44bdcb0d


Certificate Viewer: dc112.vlabs12.com
General
Details
Certificate Hierarchy
Root12CA
vlabs12-CA
dc112.vlabs12.com
Certificate Fields
dc112.vlabs12.com
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Field Value
CN = vlabs12-CA
DC = vlabs12
DC = com
Export...