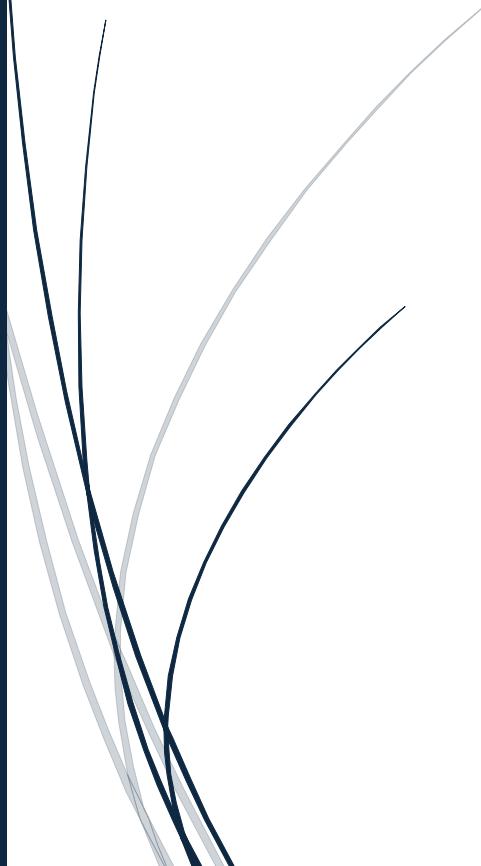


5/27/2025

Assignment 3

Part 1



Mohammed, Laetitia, 0931512
NETWORK INSTALLATION AND ADMINISTRATION II

Contents

Task 1: Deploy an Offline Standalone Root CA on DC212	1
Task 2: Deploy an Enterprise Subordinate CA on DC112.....	22

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

```
PS C:\Users\Administrator.VLABS12.000> Uninstall-ADDSDomainController -DemoteOperationMasterRole -Force  
LocalAdministratorPassword: *****  
  
Uninstall-ADDSDomainController  
  
    Validating environment and user input  
        All tests completed successfully  
        [ooooooooooooooooooooooo  
Uninstalling domain controller  
    Starting  
  
CONFIRM: LocalAdministratorPassword?  
  
Message           Context          RebootRequired  Status  
-----           -----          -----          -----  
Operation completed successfully DCPromo.General.1      False Success  
  
PS C:\Users\Administrator.VLABS12.000>
```

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

```
WARNING: To launch Server Configuration tool again, run "SConfig"  
PS C:\Users\Administrator.VLABS12.000> Remove-Computer -Restart -Force
```

```
WARNING: To stop SConfig from launching at sign-in, type "Set-SConfig -AutoLaunch $false"
```

```
-----  
Welcome to Windows Server 2025 Standard  
-----
```

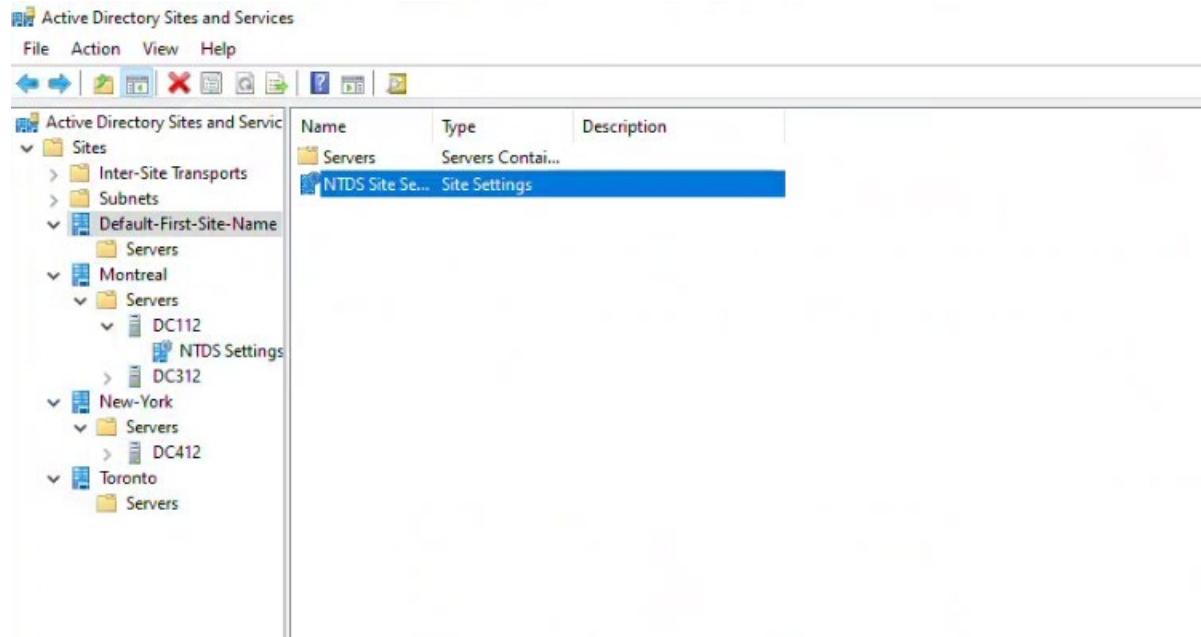
- | | |
|---------------------------------------|-------------------------------|
| 1) Domain/workgroup: | Workgroup: WORKGROUP |
| 2) Computer name: | DC212 |
| 3) Add local administrator | Enabled |
| 4) Remote management: | Download only |
| 5) Update setting: | Enabled (more secure clients) |
| 6) Install updates | |
| 7) Remote desktop: | |
| 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: -
```

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

```
PS C:\Users\Administrator.DC112> Get-ADComputer DC212 | Remove-ADObject -Recursive -Confirm:$false  
PS C:\Users\Administrator.DC112>
```

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

```
WARNING: To launch Server Configuration Tool again, run "Seconfig"
PS C:\Users\Administrator.DC212.000> Add-WindowsFeature Adcs-Cert-Authority
Collecting data...
10%
[oooooooooooo
```

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 4096 -HashAlgorithm SHA256 -CryptoProviderName "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 ErrorCode
-----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>
```

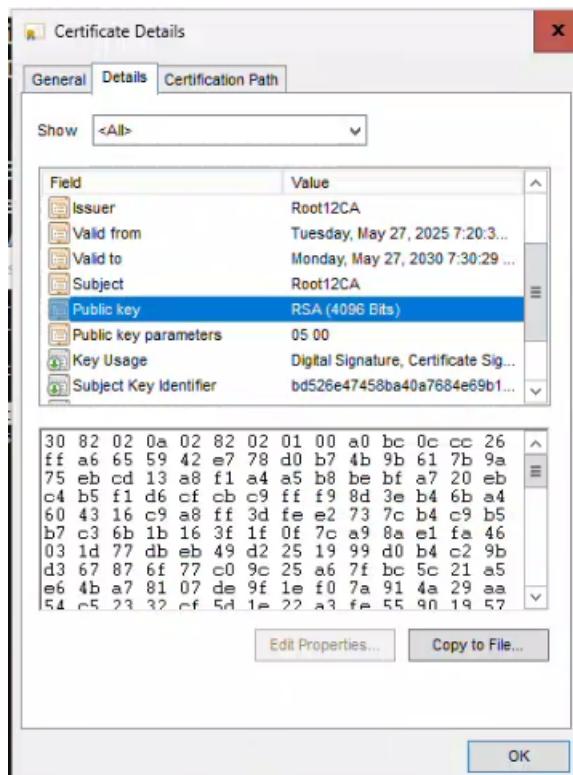
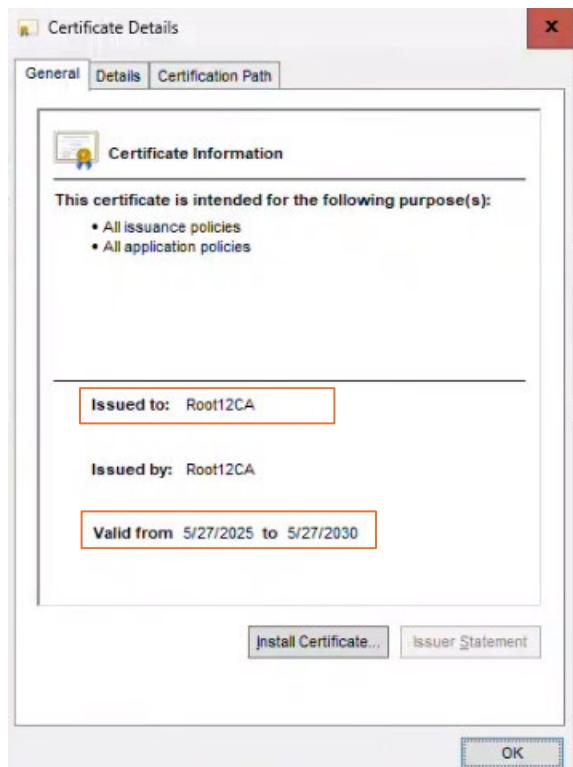
View the new Server Root12CA certificate:

certutil -viewstore CA

```
View Certificate Store
Select Certificate
Root Agency
Issuer: Root Agency
Valid From: 5/ 28/ 1996 to 12/ 31/ 2039
Click here to view certificate properties
More choices
OK
Cancel
```

```
Select a sign-in options or hit ESC to cancel
Root Agency
www.verisign.com/CPS Incorp. by Ref. LIABILITY LTD.(c)97 VeriSign
Root12CA
Microsoft Windows Hardware Compatibility
```

```
View Certificate Store
Select Certificate
Root12CA
Issuer: Root12CA
Valid From: 5/ 27/ 2025 to 5/ 27/ 2030
Click here to view certificate properties
More choices
OK
Cancel
```



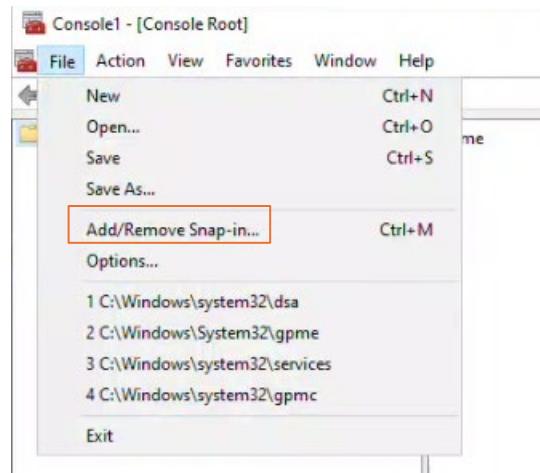
Modify the CRL Distribution Points (CDP) and Authority Information Access (AIA) settings from DC212 to DC112.

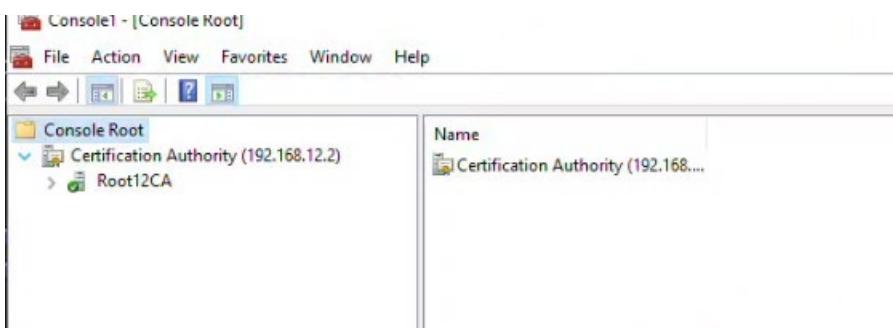
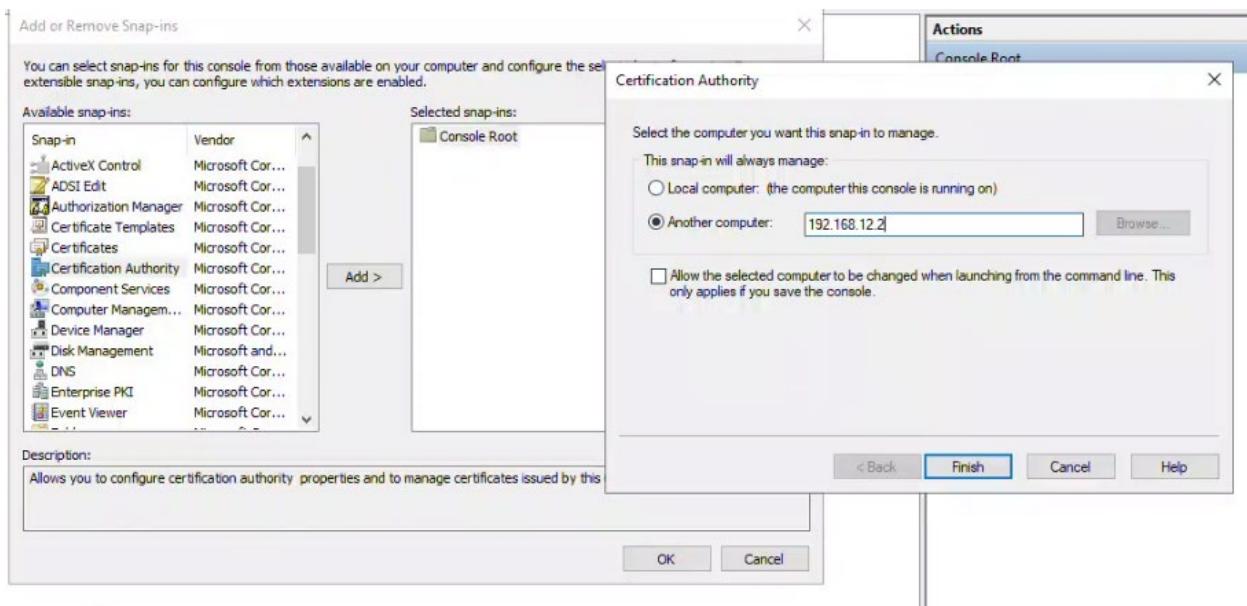
On DC112, install Active Directory Certificate Services (AD CS) and the management tools

```
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>
```

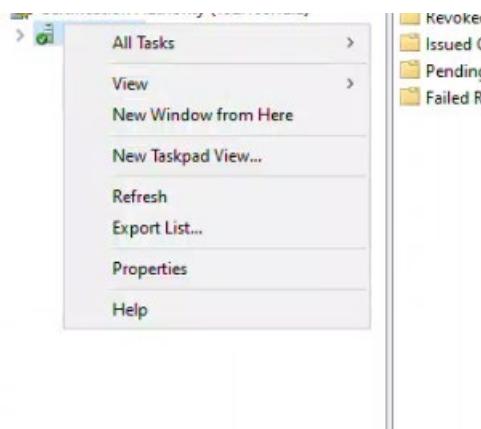
Define where CDP and AIA can be accessed

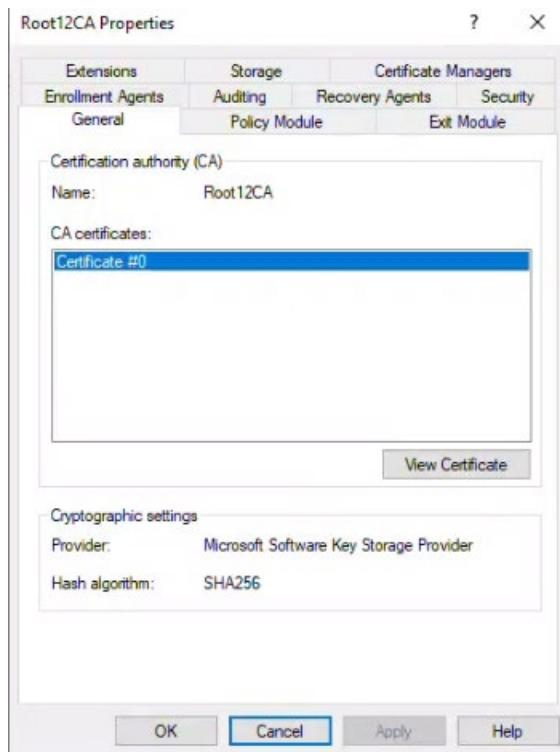
Use Certification Authority Snap-in using mmc.exe and connect Root12CA using it's IP address 192.168.12.2



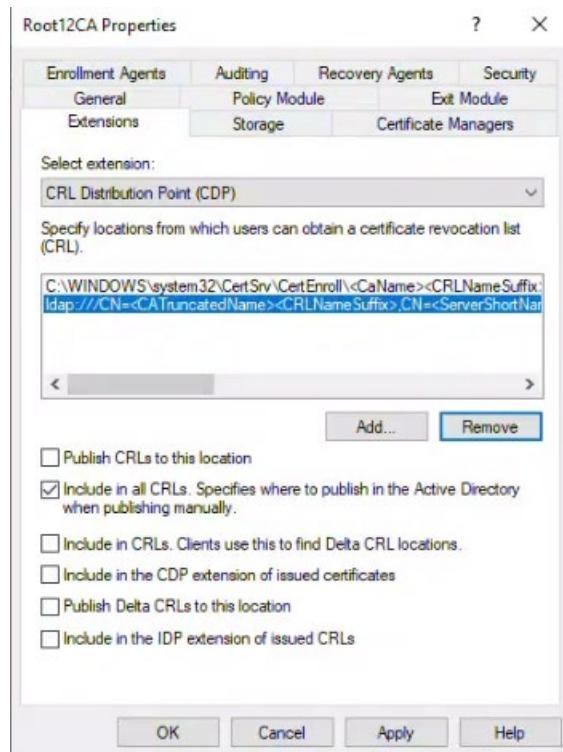
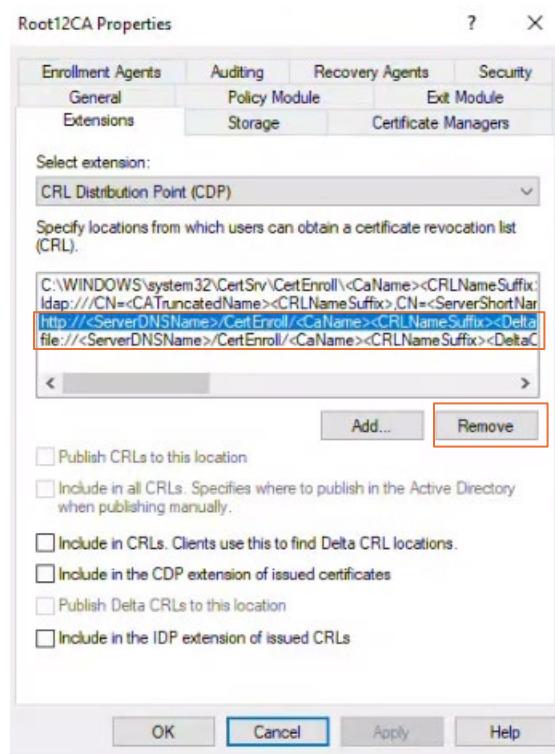


To define where CDP and AIA can be accessed, right-click on Root12CA → Properties

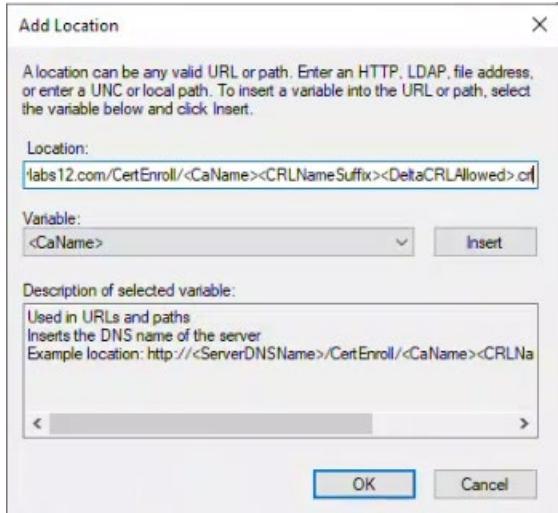




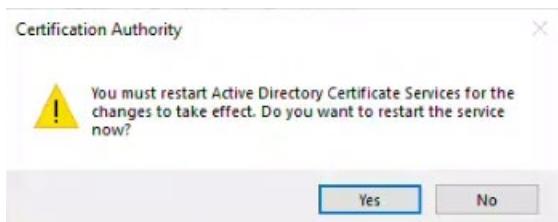
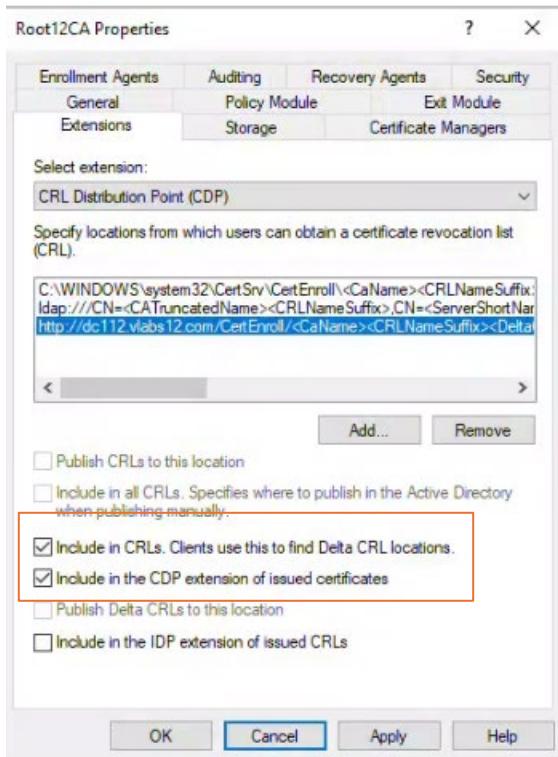
Go to the Extensions tab and remove the http and file entries.



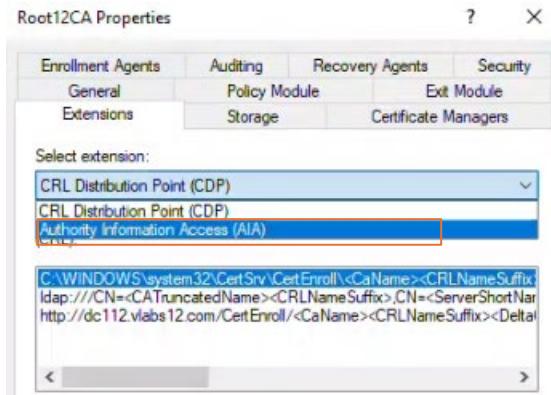
Add an entry with our Enterprise Subordinate CA server (DC112) URL:



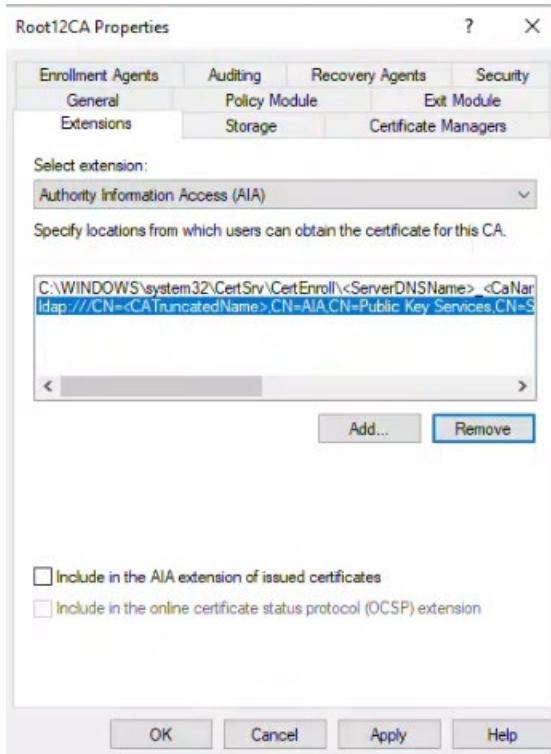
Make sure to tick the boxes “Include in CRLs” and “Include in the CDP”



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

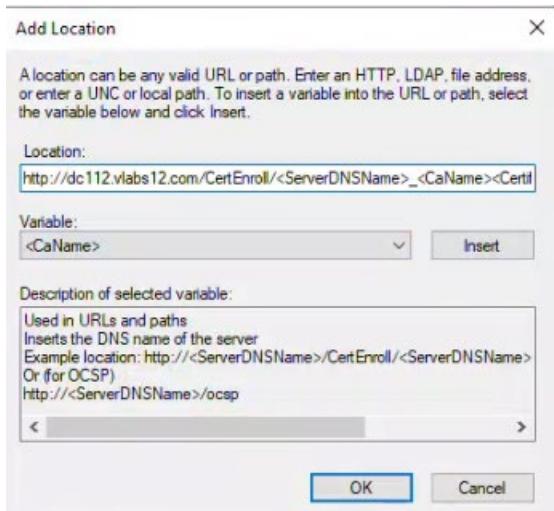


Like before, remove the http and file entries.

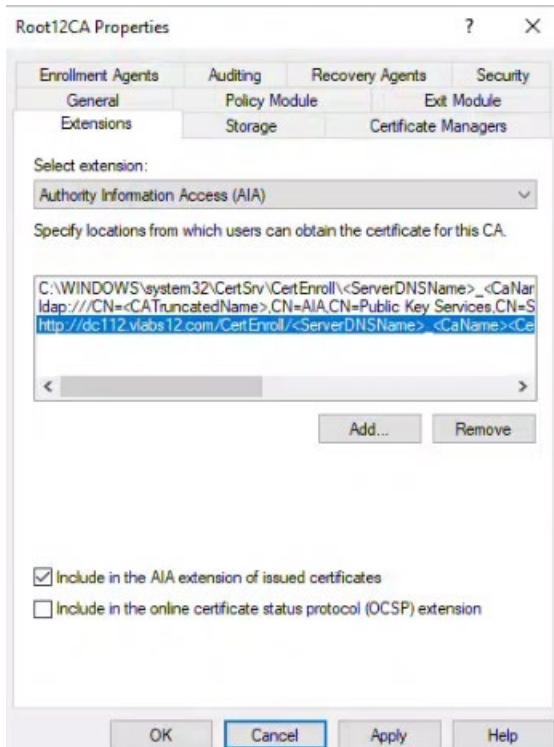


Create a new entry with our URL:

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

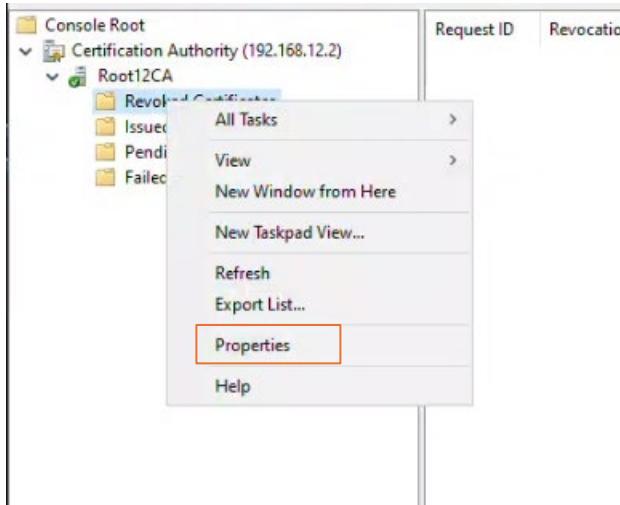


Click on “Include in the AIA extension of issued certificates” then click apply

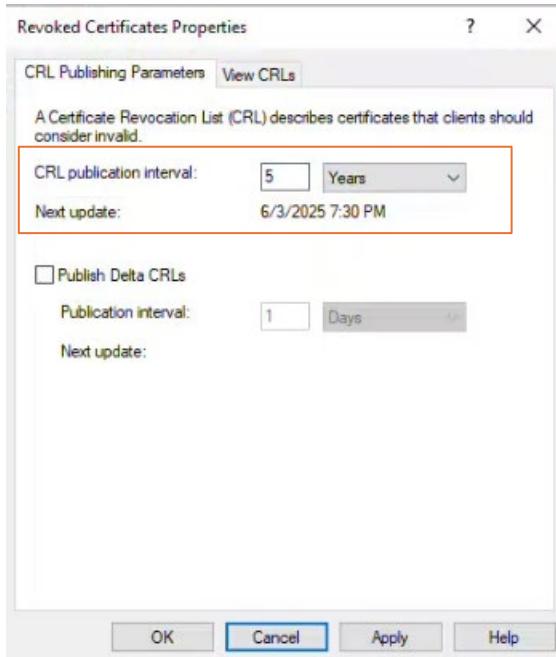


Restart the service when prompted.

Go to Root12CA → Revoked Certificates and select Properties

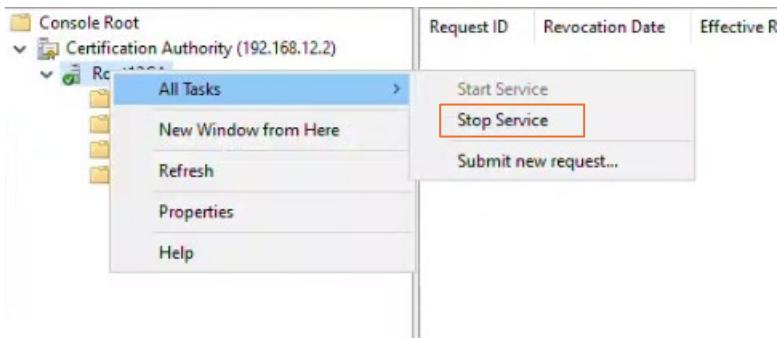


Since Root12CA was configured to be offline for 5 years, modify the CRL publication interval for 5 years so that Root12CA is not needed.

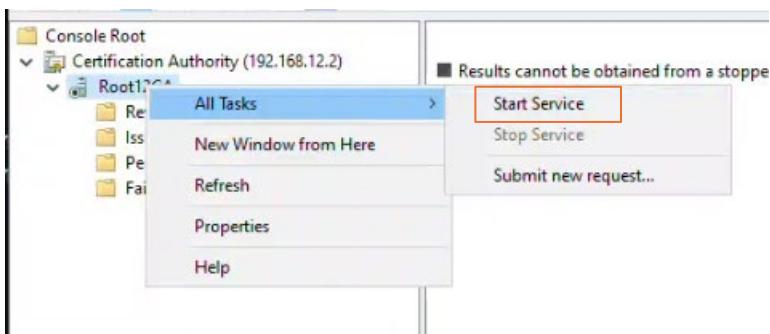


Restart Root12CA so that the changes are applied

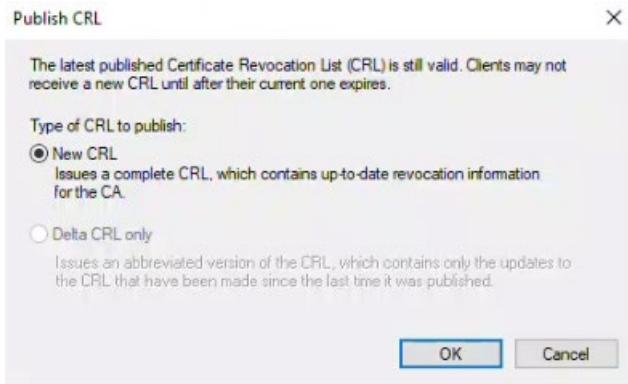
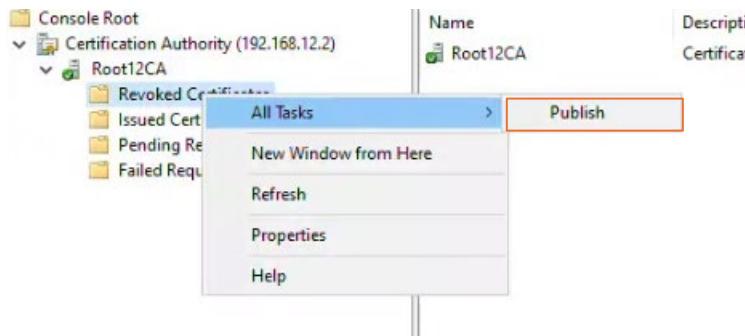
Right-click on Root12CA → All Tasks → Stop Service



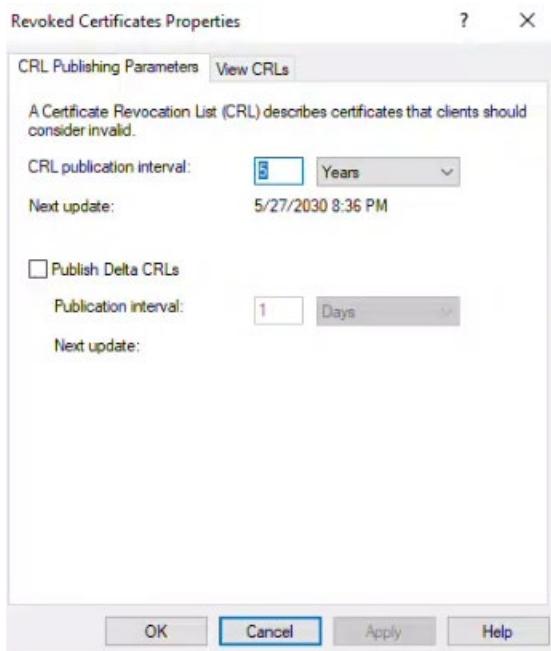
Start the service afterwards



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

This PC > Local Disk (C:) >				
	Name	Date modified	Type	Size
IS	└ DataBase	5/27/2025 9:01 PM	File folder	
S	└ GPOs	5/27/2025 1:48 PM	File folder	
IS	└ PerfLogs	5/8/2021 4:20 AM	File folder	
IS	└ Program Files	4/29/2025 2:16 PM	File folder	
IS	└ Program Files (x86)	5/8/2021 5:42 AM	File folder	
(C:)	└ Users	5/5/2025 3:48 PM	File folder	
nitions	└ Windows	5/13/2025 7:56 PM	File folder	
	└ addusers	5/10/2025 3:31 PM	Windows PowerS...	3 KB
	└ cleanAD	5/9/2025 1:58 PM	Windows PowerS...	2 KB
	└ replsummary	5/15/2025 5:36 PM	Text Document	2 KB
	└ Root12CA	5/27/2025 8:36 PM	Certificate Revoca...	1 KB
	└ Root12CA	5/27/2025 9:01 PM	Personal Informati...	5 KB
	└ Root12CA_Root12CA	5/27/2025 7:30 PM	Security Certificate	2 KB
	└ users	5/9/2025 10:42 AM	CSV File	5 KB

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

```
PS C:\Users\Administrator.DC112> Install-WindowsFeature -Name ADCS-Cert-Authority, ADCS-Web-Enrollment, ADCS-Enroll-Web-Svc, ADCS-Enroll-Web-Pol, ADCS-Online-Cert, ADCS-Device-Enrollment –IncludeManagementTools
Start Installation...
74%
[oooooooooooooooooooooooooooooooooooooooooooooooooooo] ]
```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{Network Device Enrollment Service, Certif...

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

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

```
PS C:\Users\Administrator.DC112> Get-WindowsFeature| Where-Object { $_.Name -like "ADCS*" } | Format-Table Name,InstallState
Name          InstallState
-----
ADCS-Cert-Authority  Installed
ADCS-Enroll-Web-Pol  Installed
ADCS-Enroll-Web-Svc   Installed
ADCS-Web-Enrollment   Installed
ADCS-Device-Enrollment Installed
ADCS-Online-Cert     Installed

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

Configure DC112 as an Enterprise Subordinate CA

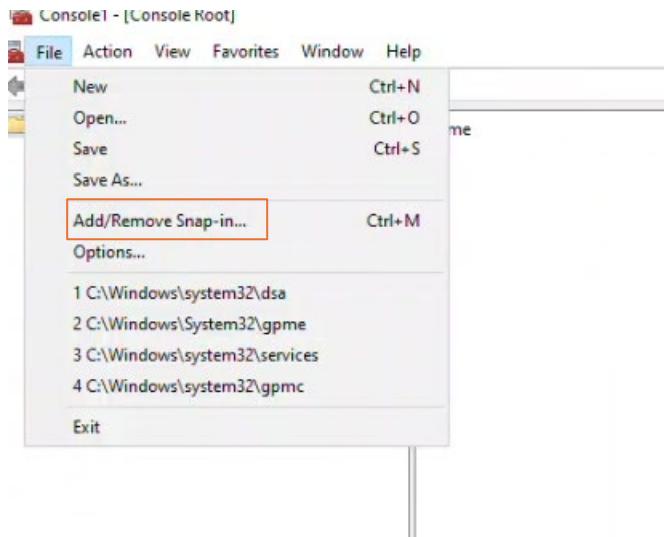
```
Install-AdcsCertificationAuthority -CAType EnterpriseSubordinateCa -  
CACCommonName vlabs12-CA -KeyLength 4096 -HashAlgorithm SHA256 -  
CryptoProviderName "RSA#Microsoft Software Key Storage Provider"
```

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

```
PS C:\Users\Administrator.DC112> Install-AdcsCertificationAuthority -CAType EnterpriseSubordinateCa -CACCommonName vlabs12-CA -KeyLength 4096 -HashAlgorithm SHA256 -CryptoProviderName "RSA#Microsoft Software Key Storage Provider"  
  
Confirm  
Are you sure you want to perform this action?  
Performing the operation "Install-AdcsCertificationAuthority" on target "DC112".  
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): A  
WARNING: The Active Directory Certificate Services installation is incomplete. To complete the installation, use the request file "C:\DC112.vlabs12.com_vlabs12-CA.req" to obtain a certificate from the parent CA. Then, use the Certification Authority snap-in to install the certificate. To complete this procedure, right-click the node with the name of the CA, and then click Install CA Certificate. The operation completed successfully. 0x0 (WIN32: 0)  
  
ErrorId ErrorString  
-----  
398 The Active Directory Certificate Services installation is incomplete. To complete the installation, use the request file "C:\DC112.vlabs12.com_vlabs12-CA.req" t...  
Activate Windows  
Go to Settings to activate Windows.
```

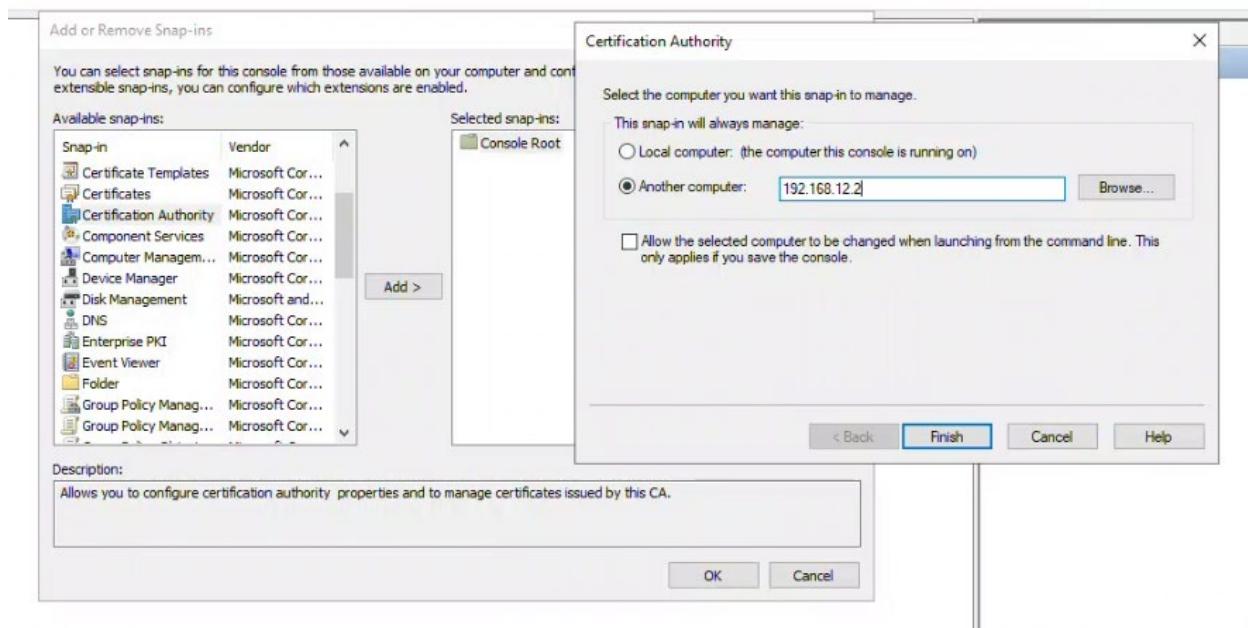
Go to Certificate Authority Snap-in using mmc.exe and connect Root12CA using it's ip address 192.168.12.2

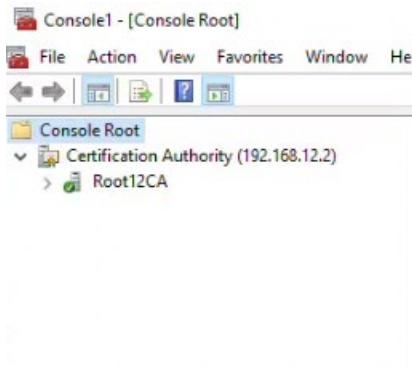
Click on File → Add/Remove Snap-in..



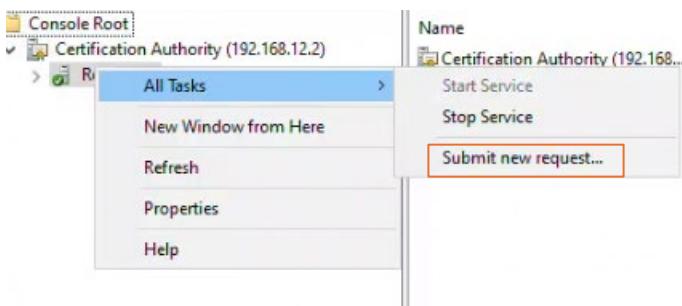
Certification Authority → Add → Another computer → 192.168.12.2

Wait for it to connect

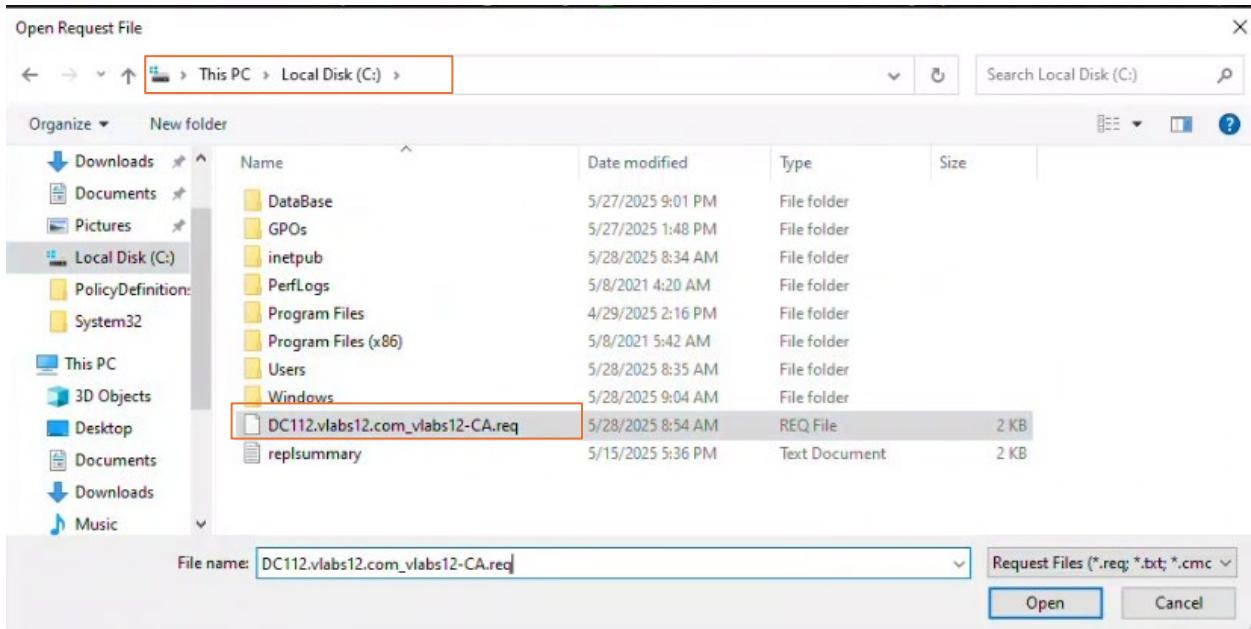




Right-click on Root12CA → All tasks → Submit new request



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

The screenshot shows the MMC interface for a Certification Authority. On the left, a navigation pane lists 'Console Root' and 'Certification Authority (192.168.12.2)'. Under the CA node, 'Root12CA' is expanded, showing 'Revoked Certificates', 'Issued Certificates', 'Pending Requests' (which is selected and highlighted with a red box), and 'Failed Requests'. The main pane displays a table of pending requests:

Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Co.
3	-----BEGIN NE...	The operation compl...	Taken Under Submission	5/28/2025 9:06 AM	ROOT12CA\Admin...	

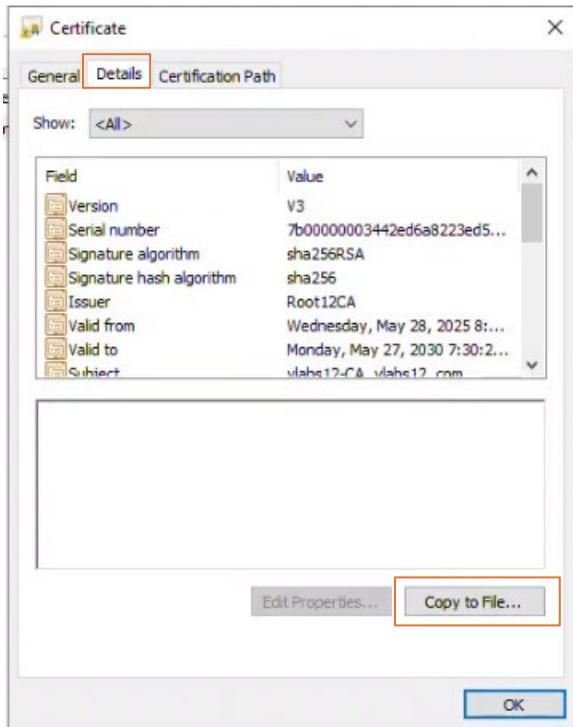
A context menu is open over the row for Request ID 3. The menu items are: All Tasks, View Attributes/Extensions..., Refresh, Help, Issue (which is highlighted with a red box), and Deny.

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

The screenshot shows the MMC interface after the certificate has been issued. The navigation pane remains the same. The main pane now displays the 'Issued Certificates' section for the 'Root12CA' node, showing a single issued certificate:

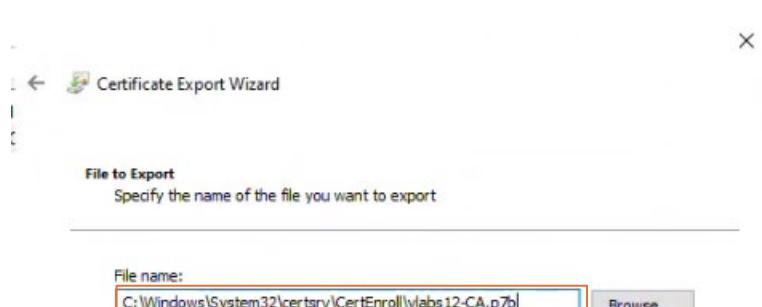
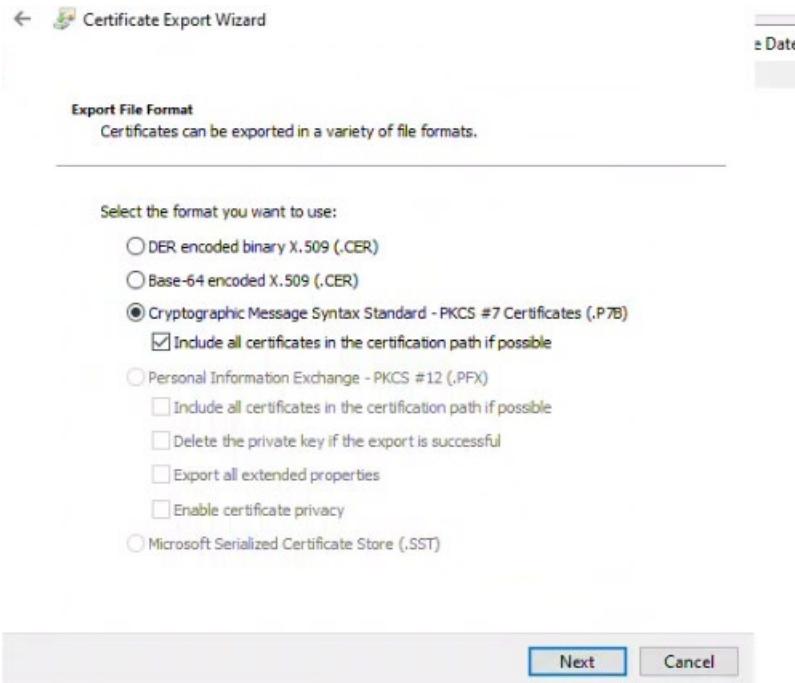
Request ID	Requester Name	Binary Certificate	Certificate Template
3	ROOT12CA\Admin...	-----BEGIN CERTI...	Subordinate Certific...

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

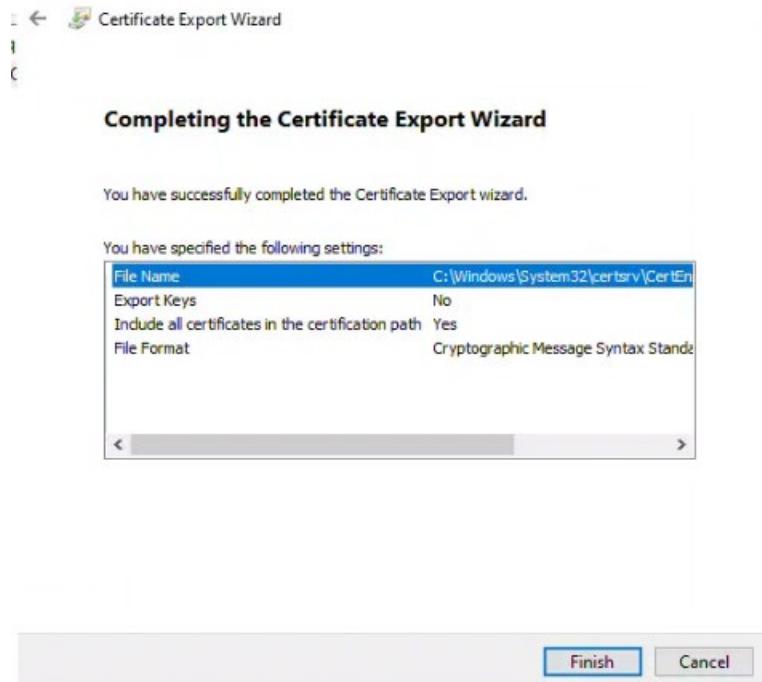


The Certificate Export Wizard will now open. Click on next on the welcome page

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\vlab12-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>
```

This PC > Local Disk (C:) > Windows > System32 > certsrv > CertEnroll				
	Name	Date modified	Type	Size
ss	Root12CA.crl	5/27/2025 8:36 PM	Certificate Revoca...	1 KB
ls	Root12CA_Root12CA.crt	5/27/2025 7:30 PM	Security Certificate	2 KB
its	vlabs12-CA.p7b	5/28/2025 9:36 AM	PKCS #7 Certificates	2 KB

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=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=vlabs12,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
Base CRL added to DS store.

CertUtil: -dsPublish command completed successfully.
```

Activate Windows
Go to Settings to activate Windows.

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>
```

Certificates - Local Computer	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Term...
> Personal	[Class 3 Public Primary Certification Authority]	Class 3 Public Primary Certification Authority	8/1/2028	Client Authentication...	VenSign Class 3 Pu...		
✓ Trusted Root Certification Authorities	[Copyright (c) 1997 Microsoft Corp.]	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...		
Certificates	[DigiCert Assured ID Root CA]	DigiCert Assured ID Root CA	11/9/2031	Client Authentication...	DigiCert		
> Enterprise Trust	[DigiCert Global Root CA]	DigiCert Global Root CA	11/9/2031	Client Authentication...	DigiCert		
> Intermediate Certification Authorities	[DigiCert Global Root G2]	DigiCert Global Root G2	1/15/2038	Client Authentication...	DigiCert Global Roo...		
> Trusted Publishers	[DigiCert Global Root G3]	DigiCert Global Root G3	1/15/2038	Client Authentication...	DigiCert Global Roo...		
> Untrusted Certificates	[Microsoft Authenticode(tm) Root Authority]	Microsoft Authenticode(tm) Root Authority	12/31/1999	Secure Email, Code...	Microsoft Authenti...		
> Third-Party Root Certification Authorities	[Microsoft ECC Product Root Certificate Authority]	Microsoft ECC Product Root Certificate Authority	2/27/2043	<All>	Microsoft ECC Prod...		
> Trusted People	[Microsoft ECC TS Root Certificate Authority 2018]	Microsoft ECC TS Root Certificate Authority	2/27/2043	<All>	Microsoft ECC TS R...		
> Client Authentication Issuers	[Microsoft Root Authority]	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
> Preview Build Roots	[Microsoft Root Certificate Authority]	Microsoft Root Certificate Authority	5/9/2021	<All>	Microsoft Root Cert...		
> Test Roots	[Microsoft Root Certificate Authority 2010]	Microsoft Root Certificate Authority	6/23/2035	<All>	Microsoft Root Cert...		
> Remote Desktop	[Microsoft Root Certificate Authority 2011]	Microsoft Root Certificate Authority	3/22/2036	<All>	Microsoft Root Cert...		
> Certificate Enrollment Requests	[Microsoft Time Stamp Root Certificate Authority]	Microsoft Time Stamp Root Certificate Authority	10/22/2039	<All>	Microsoft Time Sta...		
> Smart Card Trusted Roots	[NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.]	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	1/7/2004	Time Stamping	VenSign Time Stam...		
> Trusted Packaged App Installation Authorities	[Root12CA]	Root12CA	5/27/2030	<All>	<None>		
> Trusted Devices	[Symantec Enterprise Mobile Root for Microsoft]	Symantec Enterprise Mobile Root for Microsoft	3/14/2032	Code Signing	<None>		
> Web Hosting	[Thawte Timestamping CA]	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestampi...		
> Windows Live ID Token Issuer							
> WindowsServerUpdateServices							

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>
```

The screenshot shows the Windows Certificates snap-in. On the left, there's a tree view with nodes like 'Certificates - Local Computer', 'Personal', 'Trusted Root Certification Authorities', 'Enterprise Trust', 'Intermediate Certification Authorities', 'Certificate Revocation List', and 'Trusted Publishers'. On the right, a detailed table lists certificates with columns for Issued To, Issued By, Expiration Date, Intended Purposes, Friendly Name, Status, and Certificate Type. The table includes entries for 'Microsoft Windows Hardware Compatibility' (Issued By: Microsoft Root Authority, Expiry: 12/31/2002), 'Root Agency' (Issued By: Root Agency, Expiry: 12/31/2039), 'vLabs12-CA' (Issued By: RootI2CA, Expiry: 5/27/2030), and 'www.verisign.com/CPS Incorp. by Ref. LIABILITY...' (Issued By: Class 3 Public Primary Certification Authority, Expiry: 10/24/2016).

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Type
Microsoft Windows Hardware Compatibility	Microsoft Root Authority	12/31/2002	Code Signing, Win...	<None>		
Root Agency	Root Agency	12/31/2039	<All>	<None>		
vLabs12-CA	RootI2CA	5/27/2030	<All>	<None>		Subordinate C...
www.verisign.com/CPS Incorp. by Ref. LIABILITY...	Class 3 Public Primary Certification Authority	10/24/2016	Server Authentication	<None>		

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.

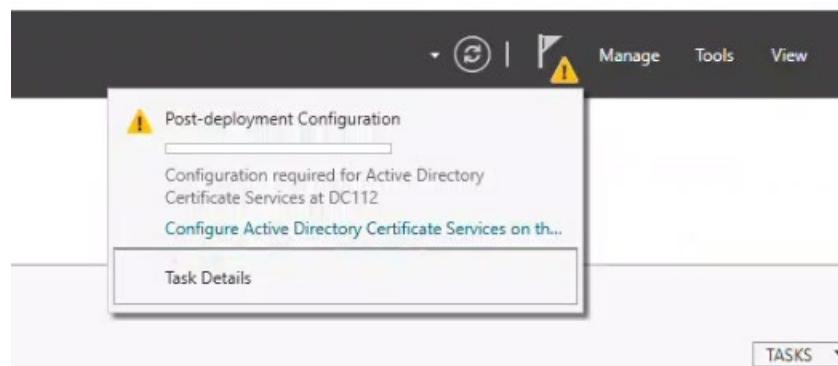
CEP and CES Certificate Enrollment Policy Web Services

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

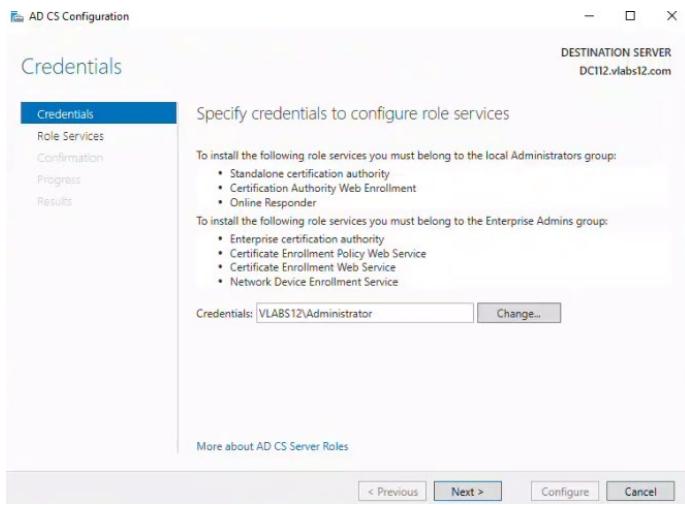
NDES performs the following functions:

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.

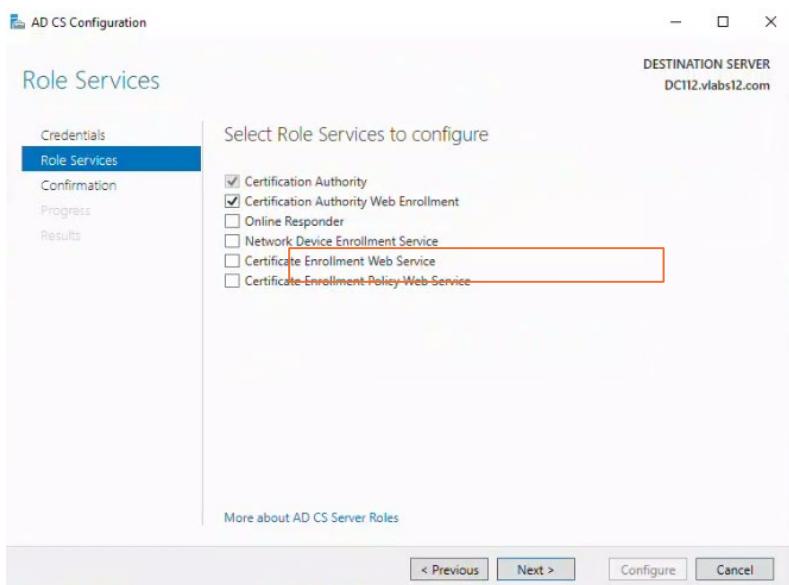
On DC112 server manager, click the exclamation mark at the top and select Configure AD CS on the destination server



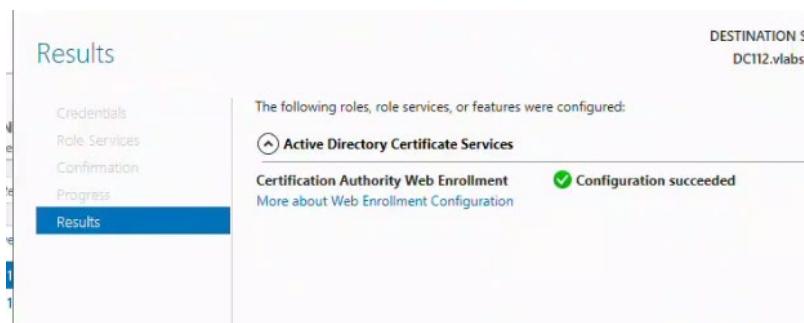
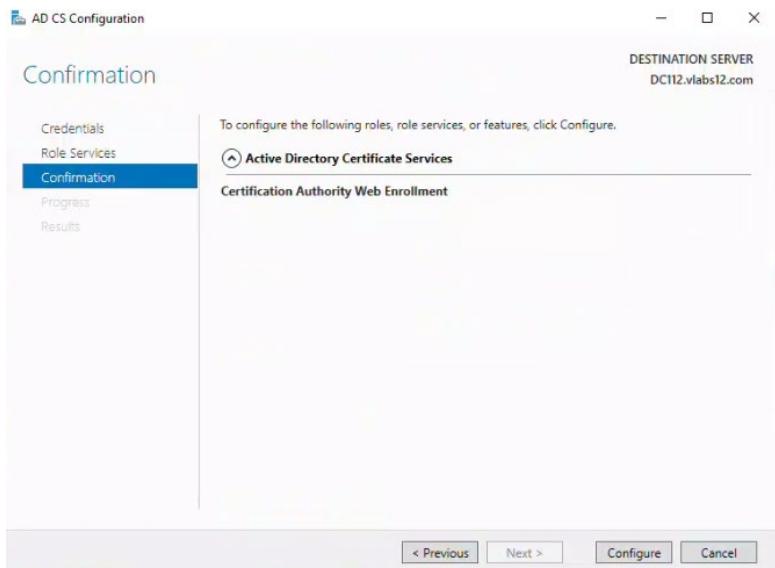
Confirm the credentials → Next



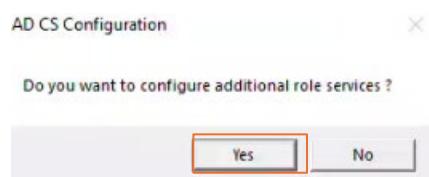
Tick the box “CA Web Enrollment” → Next



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

AD CS Configuration

Role Services

Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results

Select Role Services to configure

Certification Authority
 Certification Authority Web Enrollment
 Online Responder
 Network Device Enrollment Service
 Certificate Enrollment Web Service
 Certificate Enrollment Policy Web Service

Confirm the target CA is our DC112 CA

CA for CES

DESTINATION SERVER
DC112.vlabs12.com

Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results

Specify CA for Certificate Enrollment Web Services

Select the certification authority (CA) that you want to use for issuing certificates requested through this Certificate Enrollment Web Service (CES).

Select:
 CA name
 Computer name
Target CA: DC112.vlabs12.com\vlabs12-CA

Configure the Certificate Enrollment Web Service for renewal-only mode.
i Renewal-only mode requires that the targeted CA run at least Windows Server 2008 R2.

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

Authentication Type for CES

Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results

Select the type of authentication

Windows integrated authentication
 Client certificate authentication
 User name and password

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

Service Account for CES DC112.vlabs12.com

Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results

Specify the service account

Select the identity that the Certificate Enrollment Web Service (CES) uses when communicating with the certification authority (CA) and other services on the network.

Specify service account (recommended)
The account selected must be a member of the IIS_IUSRS group. If Kerberos is selected as the authentication type, a service principal name is required for the service account.
 Use the built-in application pool identity

Authentication Type for CEP

Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results

Select the type of authentication

Windows integrated authentication
 Client certificate authentication
 User name and password

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

Specify a Server Authentication Certificate

When communicating with clients, the web service(s) uses Secure Sockets Layer (SSL) protocol to encrypt network traffic.

Choose an existing certificate for SSL encryption (recommended)

Issued To	Issued By	Expiration Date
vlabs12-CA	Root12CA	5/27/2030

Confirm all the selections and then click on configure

Confirmation

DESTINATION SERVER
DC112.vlabs12.co

Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results

To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certificate Enrollment Web Service

CA Name:	DC112.vlabs12.com\vlabs12-CA
Renewal Only Mode:	False
Authentication Type:	Windows Integrated Authentication
Allow Key-based Renewal:	False
Account:	Application Pool Identity
Server Authentication	53D8C88A35D176F0674617DB811786D1526B036A
Certificate:	

Certificate Enrollment Policy Web Service

Authentication Type:	Windows Integrated Authentication
Enable Key-based Renewal:	False
Server Authentication	53D8C88A35D176F0674617DB811786D1526B036A
Certificate:	

Results

DESTINATION SERVER
DC112.vlabs12.com

Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results

The following roles, role services, or features were configured:

Active Directory Certificate Services

Certificate Enrollment Web Service  Configuration succeeded

i Delegation must be enabled for the web service account when the Certificate Enrollment Web Service is installed and all of the following conditions apply:
 1. The Certificate Enrollment Web Service is installed on a separate computer from the certification authority
 2. Renewal-only mode is not enabled
 3. The authentication type is set for Kerberos or Certificate Authentication
[More about CES Configuration](#)

Certificate Enrollment Policy Web Service  Configuration succeeded

i Before clients can use this web service, a server authentication certificate must be configured to encrypt communication between clients and the service. Use the IIS snap-in to verify the server authentication certificate.
i Before clients can use the Certificate Enrollment Policy Web service, Group Policy settings must be applied to their computers to direct certificate enrollment requests to the web service.
[More about CEP Configuration](#)

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

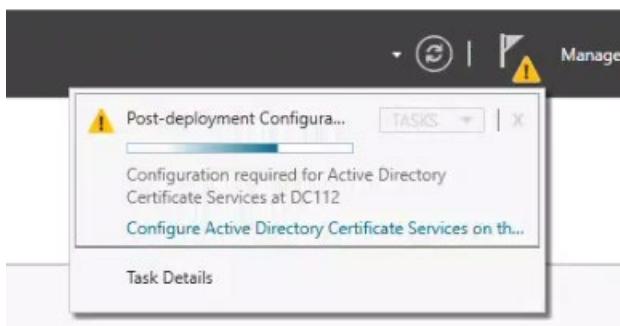
IIS_IUSRS is under Bulletin

The screenshot shows the 'Members' tab for the 'IIS_IUSRS' group. On the right, there's a table with columns for 'Name' and 'Active Director...'. A single row is selected, showing 'Administrator' and 'vlabs12-Users-...'. On the far right of the table, there are 'Add...' and 'Remove' buttons. The left sidebar lists 'Group', 'Managed By', 'Member Of', 'Members', 'Password Settings', and 'Extensions'.



The screenshot shows the 'Members' tab for the 'IIS_IUSRS' group. The 'Administrator' user is now listed in the table under 'Name' and 'Active Director...'. The rest of the interface is identical to the first screenshot.

Now we can proceed with NDES



Tick the box “Network Device Enrollment Service”

The screenshot shows the 'Role Services' configuration window. On the left, under 'Service Account for NDES', the 'Role Services' tab is selected. In the main pane, titled 'Select Role Services to configure', several checkboxes are checked, including 'Certification Authority', 'Certification Authority Web Enrollment', 'Online Responder', 'Network Device Enrollment Service', 'Certificate Enrollment Web Service', and 'Certificate Enrollment Policy Web Service'. The destination server is set to 'DC112.vlal'.

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

The screenshot shows the 'AD CS Configuration' window with the 'Service Account for NDES' step selected. In the 'Specify the service account' sub-dialog, it asks to select the identity for the Network Device Enrollment Service. The 'Specify service account (recommended)' option is selected, with a note that the account must be a member of the domain and added to the local IIS_IUSRS group. Below it, there's an option to 'Use the built-in application pool identity'. A 'Windows Security' dialog is overlaid, prompting for a user name ('administrator') and password ('*****'). The domain is listed as 'VLABS12'. At the bottom of the main window, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

Service Account for NDES

DESTINATION SERVER
DC112.vlabs12.com

Credentials
Role Services
Service Account for NDES
RA Information
Cryptography for NDES
Confirmation
Progress
Results

Specify the service account

Select the identity the Network Device Enrollment Service (NDES) will use.

Specify service account (recommended)
The account must be a member of the domain and must be added to the local IIS_IUSRS group.
VLABS12\administrator

Use the built-in application pool identity

Add an email, company name, city and province

AD CS Configuration

RA Information

DESTINATION SERVER
DC112.vlabs12.com

Credentials
Role Services
Service Account for NDES
RA Information
Cryptography for NDES
Confirmation
Progress
Results

Type the requested information to enroll for an RA certificate

A registration authority (RA) is required to manage the Network Device Enrollment Service (NDES) certificate requests.

Required information

RA Name: DC112-MSCEP-RA
Country/Region: US (United States)

Optional information

E-mail: admin@vlabs12.com
Company: VLABS12
Department:
City: Montreal
State/Province: Quebec

More about RA Information

< Previous

Confirm the key length for both is 2048

Cryptography for NDES

DESTINATION SERVER
DC112.vlabs12.com

Credentials
Role Services
Service Account for NDES
RA Information
Cryptography for NDES
Confirmation
Progress
Results

Configure CSPs for the RA

Select the registration authority (RA) cryptographic service providers (CSPs) and key lengths for the signature and encryption keys.

Signature key provider: Microsoft Strong Cryptographic Provider Key length: 2048

Encryption key provider: Microsoft Strong Cryptographic Provider Key length: 2048

(Active Directory Certificate Services

Online Responder

Network Device Enrollment Service

Account:	VLABS12\administrator
RA Information:	
Name:	DC112-MSCEP-RA
Country/Region:	US
Email:	admin@vlabs12.com
Company:	VLABS12
Department:	<None>
City:	Montreal
State/Province:	Quebec
Signature Key Provider:	Microsoft Strong Cryptographic Provider
Signature Key Length:	2048
Exchange Key Provider:	Microsoft Strong Cryptographic Provider
Exchange Key Length:	2048

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

Results

DESTINATION SITE
DC112.vlabs1

The following roles, role services, or features were configured:

Active Directory Certificate Services

Online Responder More about OCSP Configuration	Configuration succeeded
Network Device Enrollment Service More about NDES Configuration	Configuration succeeded

Credentials
Role Services
Service Account for NDES
RA Information
Cryptography for NDES
Confirmation
Progress
Results

Configuration of DC112 for AD CS complete.

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

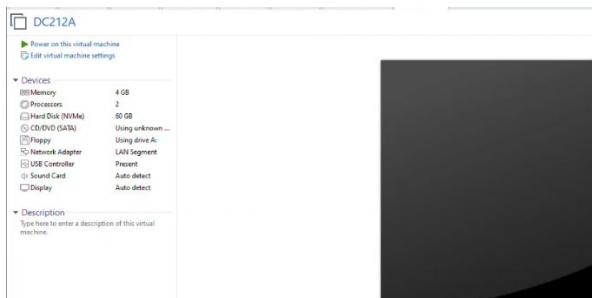
Use the following:

net stop certsvc

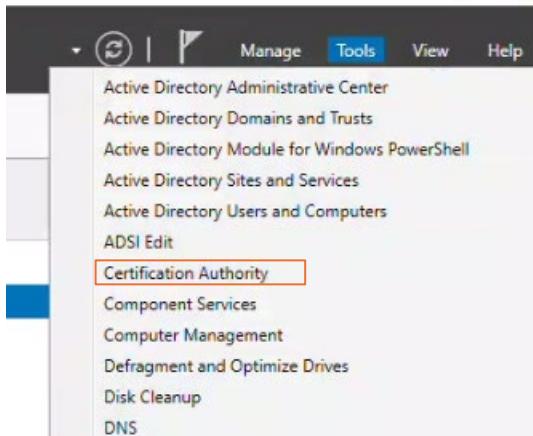
```
PS C:\Users\Administrator> net stop certsvc
The Active Directory Certificate Services service is stopping.
The Active Directory Certificate Services service was stopped successfully.
```

```
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.

A screenshot of the 'Issued Certificates' list in the Certification Authority interface. The left pane shows a tree view with 'vlabs12-CA' expanded, showing 'Revoked Certificates', 'Issued Certificates' (selected), 'Pending Requests', 'Failed Requests', and 'Certificate Templates'. The right pane displays a table with the following data:

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

A screenshot of the Microsoft Active Directory Certificate Services - vlabs12-CA website. The URL is dc112.vlabs12.com/certsrv/. The page has a header 'Welcome' and a paragraph about the service. Below it is a 'Select a task:' section with three options: 'Request a certificate', 'View the status of a pending certificate request', and 'Download a CA certificate, certificate chain, or CRL'. The page is mostly empty content.

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

The screenshot shows the MMC interface for managing certificates. The left pane displays a tree structure with 'Certification Authority (Local)' expanded, showing 'vlabs12-CA' as a child node. Under 'vlabs12-CA', there are several sub-nodes: 'Revoked Certificates', 'Issued Certificates', 'Pending Requests', 'Failed Requests', and 'Certificate Templates'. The 'Certificate Templates' node is selected. The right pane lists the available certificate templates with their names and intended purposes:

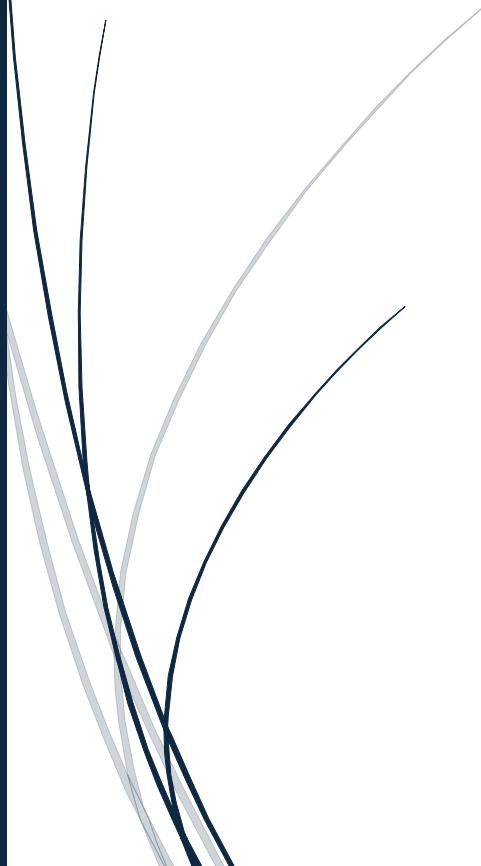
Name	Intended Purpose
IPSec (Offline request)	IP security IKE intermediate
CEP Encryption	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, 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 ...

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	1
Task 2: Enable Automatic Certificate Enrollment in AD.....	10
Task 3: Issue Digitally Signed Documents and Files.....	17
Task 4: Secure Internal Web Servers with SSL/TLS Certificates	26

Task 1: Issue User Certificates in an AD Domain

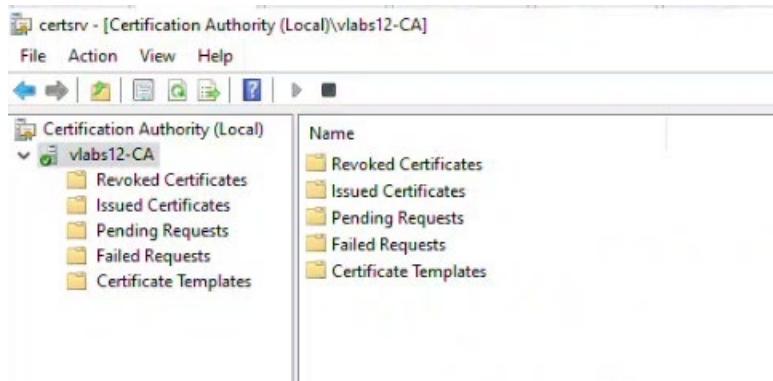
Configure and publish User Certificates from Enterprise CA

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

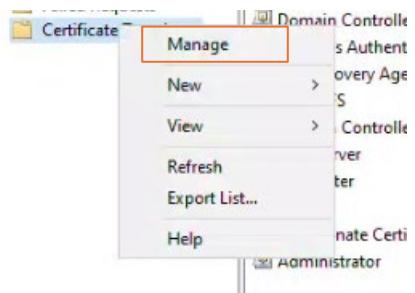
Verify that the user has obtain a valid certificate on the Client and on his account in the AD.

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.

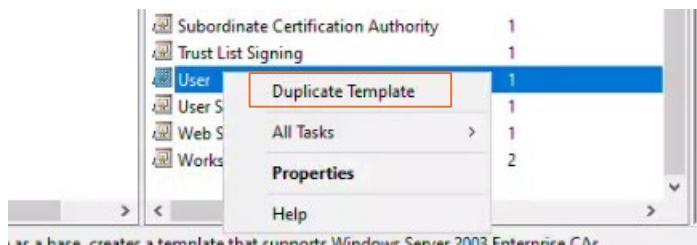
We need to configure and publish Certificate Templates in order to issue user certificates, so start by going to the Certification Authority console (certsrv.msc)



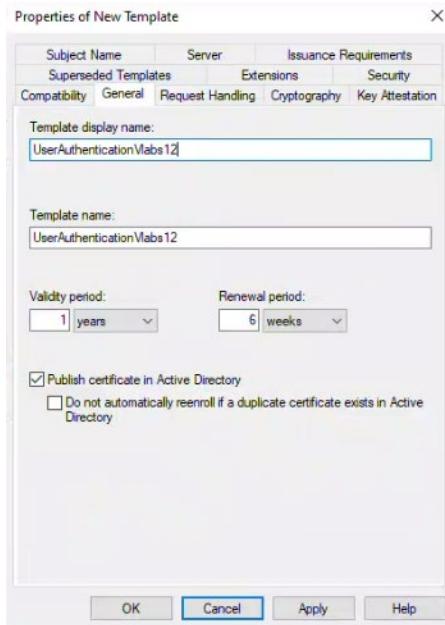
Expand your CA name and right-click on Certificate Templates → Manage



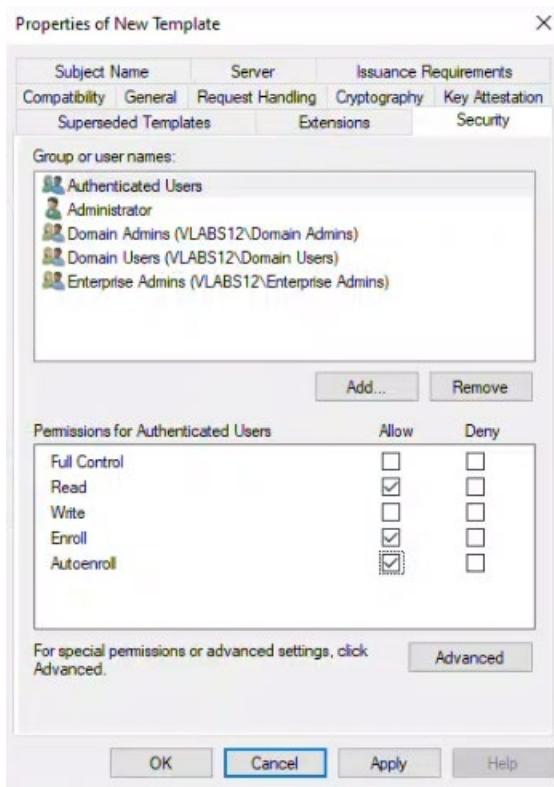
Scroll down to find User, right-click and select duplicate template



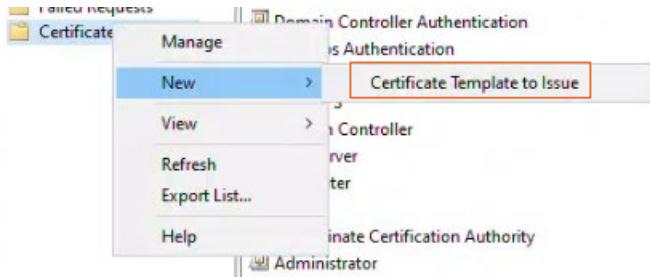
Go to the General tab and set a template display name



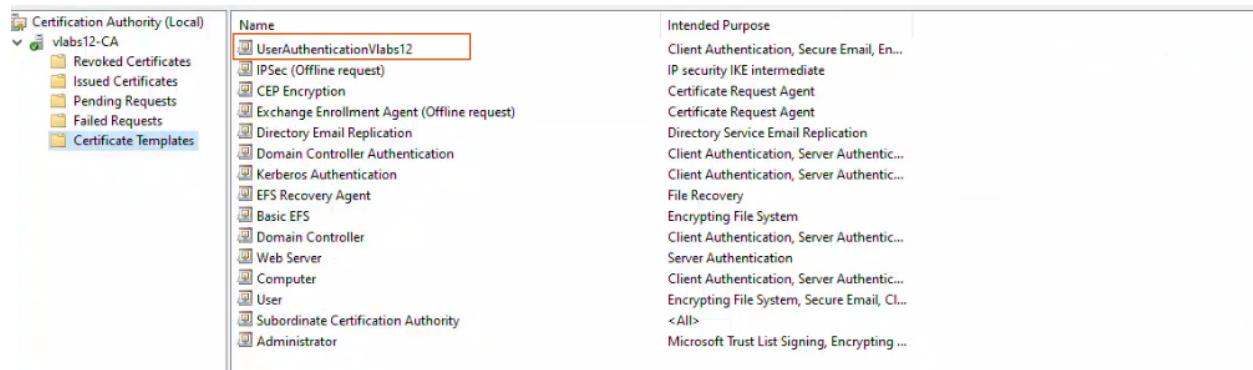
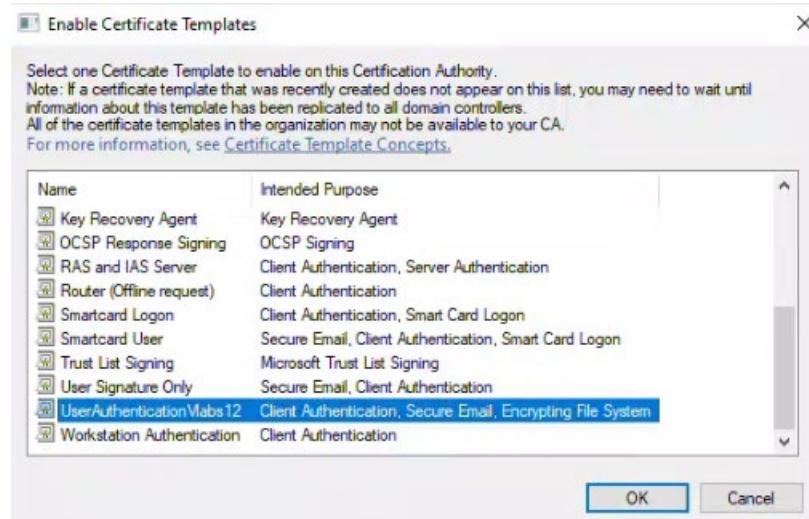
Next go to the Security tab and make sure to grant Authenticated Users enroll and autoenroll permissions. Autoenroll permissions will be used later when setting up a GPO to automatically grant certificates to authenticated users on the domain.



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



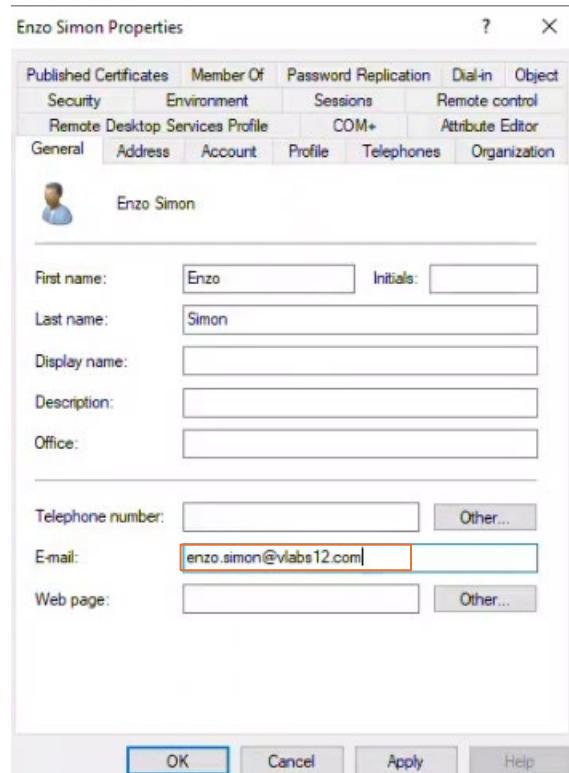
Select the new template we just created and click OK



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.

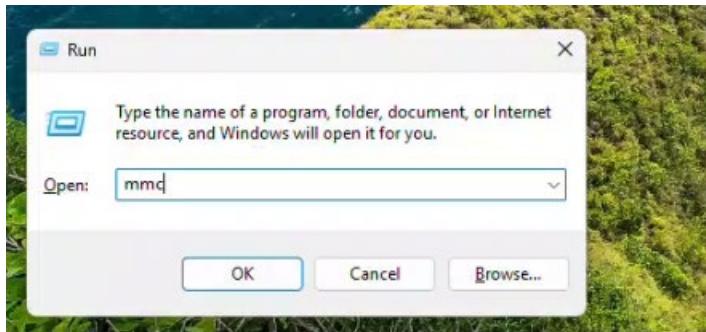
Go to AD Users and Computers, choose a user, right-click and select Properties.

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

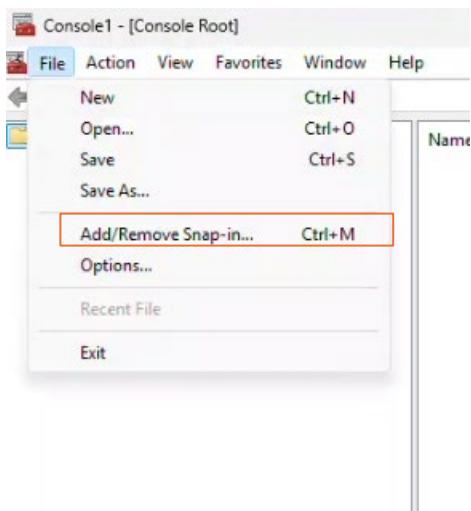


Now sign-in as Enzo on Client12

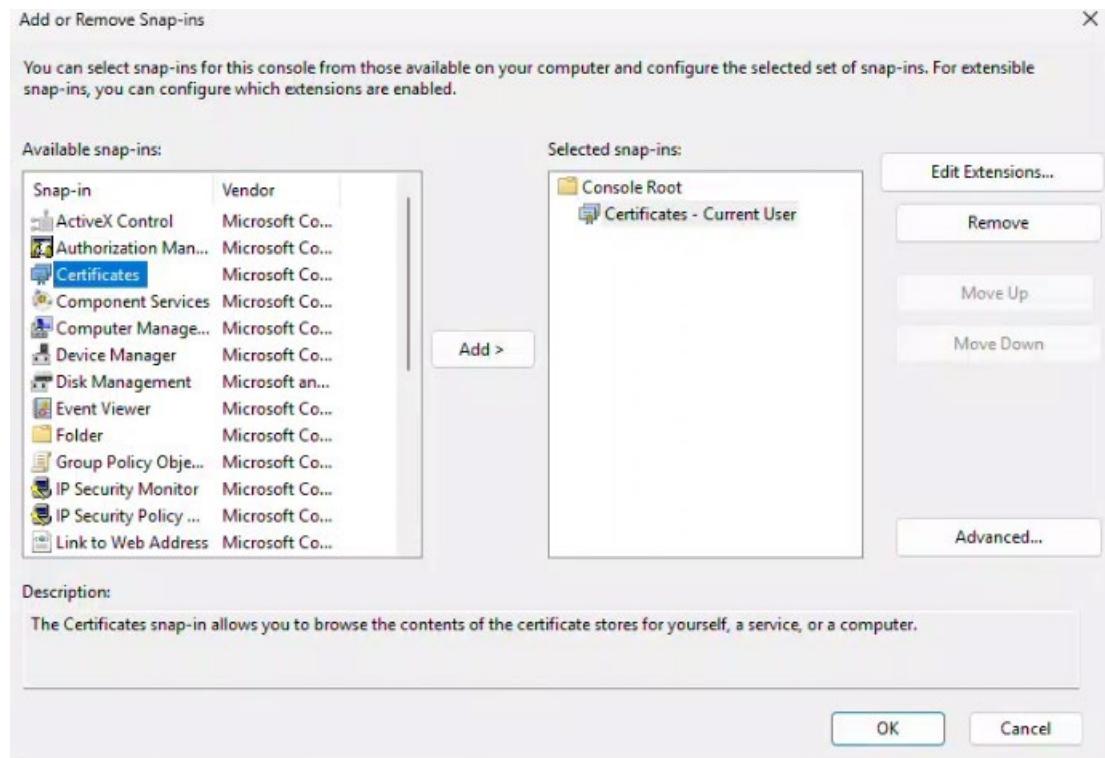
Once signed in, click Win+R for Run and enter mmc



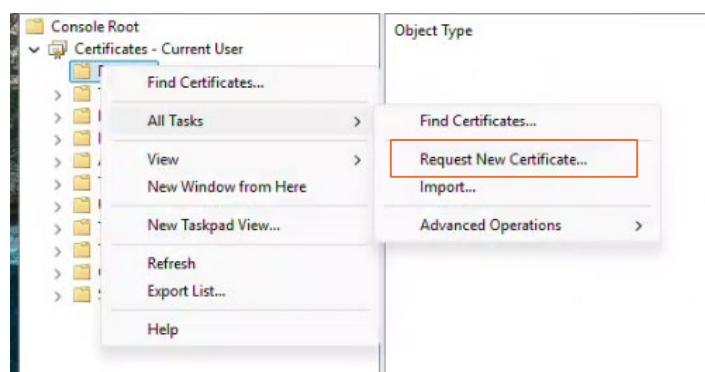
Click on File → Add/Remove Snap-in



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



Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network

You have credentials that can be used to verify your right to obtain the certificate

[Next](#) [Cancel](#)



Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy
Enrollment Policy ID: {8302C4B3-399C-45A3-BC29-228834DB712A} [Properties](#)

Configured by you [Add New](#)



Select the UserAuthenticationVlabs12 certificate and then click Enroll



Request Certificates

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

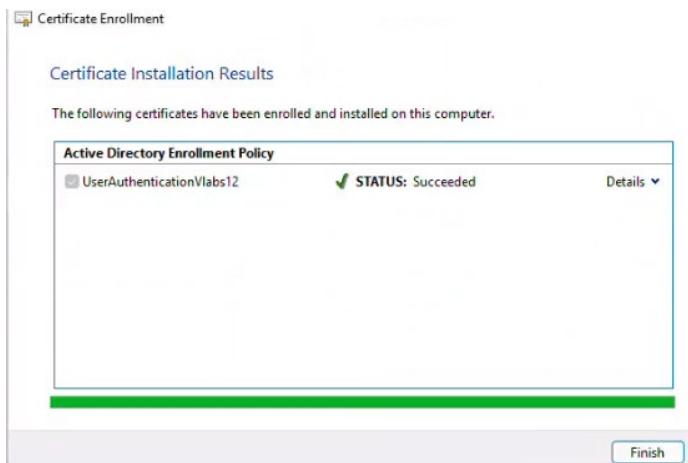
Active Directory Enrollment Policy

	STATUS:	Available	Details
<input type="checkbox"/> Basic EFS		Available	Details
<input type="checkbox"/> User		Available	Details
<input checked="" type="checkbox"/> UserAuthenticationVlabs12		Available	Details

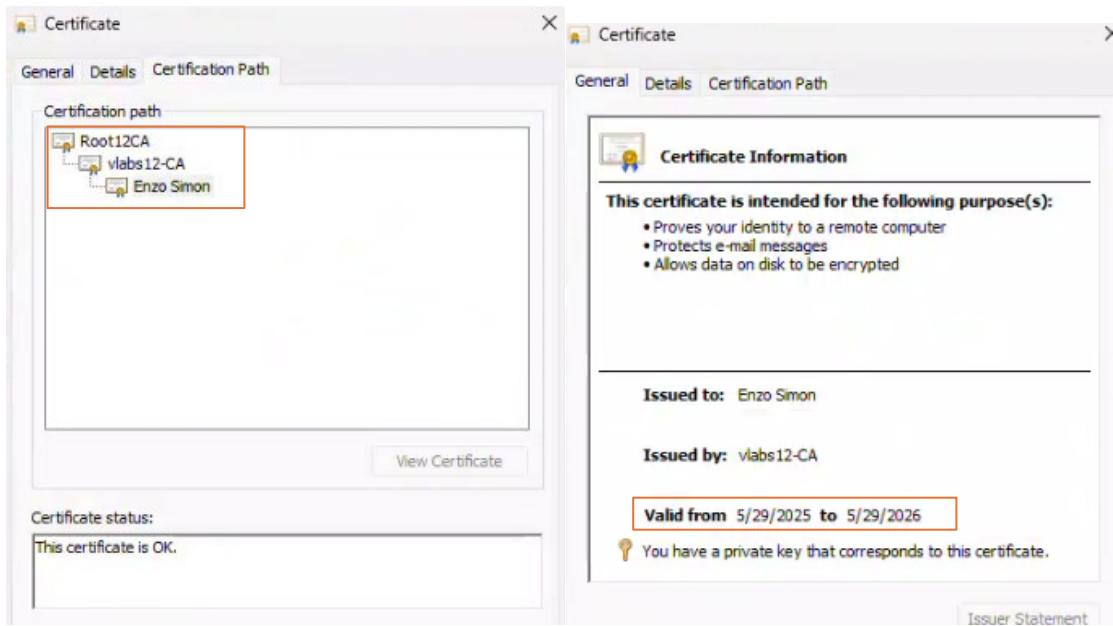


Show all templates

[Enroll](#) [Cancel](#)



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

Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Numl
3	LAB12\DC312\$	-----BEGIN CERTI...	Domain Controller (...	4b00000003
4	VLABS12\DC112\$	-----BEGIN CERTI...	Domain Controller (...	4b00000004
5	VLABS12\Administrator	-----BEGIN CERTI...	Exchange Enrollment...	4b00000005
6	VLABS12\Administrator	-----BEGIN CERTI...	CEP Encryption (CEP...	4b00000006
7	PARTNER12\DC412\$	-----BEGIN CERTI...	Domain Controller (...	4b00000007
8	VLABS12\esimon	-----BEGIN CERTI...	1.3.6.1.4.1.311.21.8.1...	4b00000008

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

Issued To	Issued By	Intended Purposes	Expiration
Enzo Simon	vlab12-CA	Client Authentication, ...	5/29/20...

Task 2: Enable Automatic Certificate Enrollment in AD

Configure Group Policy settings to allow automatic certificate enrollment

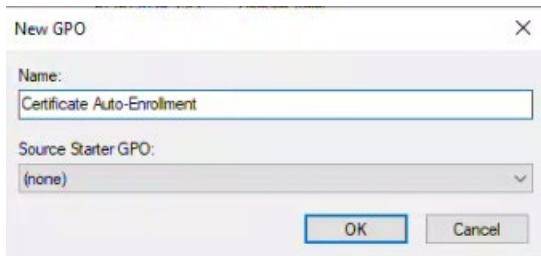
Open a session on Client12 using a different user from task 1, that has an email address. and verify if he has received automatically the necessary certificate

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

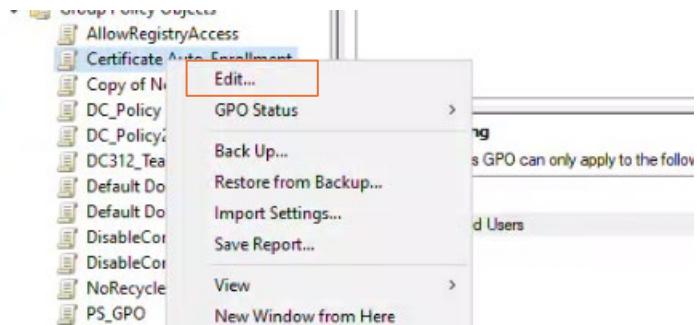
In this task, we'll create a GPO and edit it to allow automatic certificate enrollment. Meaning any user within the domain with an email address will automatically receive a certificate without manually requesting it. We'll test the new GPO by signing into Client12 as any other user and verify that we've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



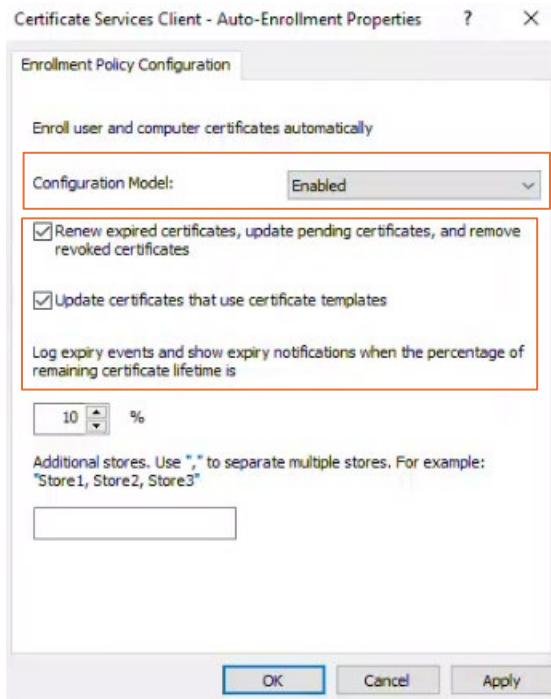
Under Computer Configuration → Policies → Windows Settings → Security Settings, click on Public Key Policies

A screenshot of the Group Policy Management Editor. The left pane shows a tree structure under 'Computer Configuration' → 'Policies' → 'Windows Settings' → 'Security Settings'. The 'Public Key Policies' node is selected and highlighted with a red box. The right pane, titled 'Object Type', lists various certificate-related objects, with 'Certificate Services Client - Auto-Enrollment' also highlighted with a red box.

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 Services Client - Auto-Enrollment

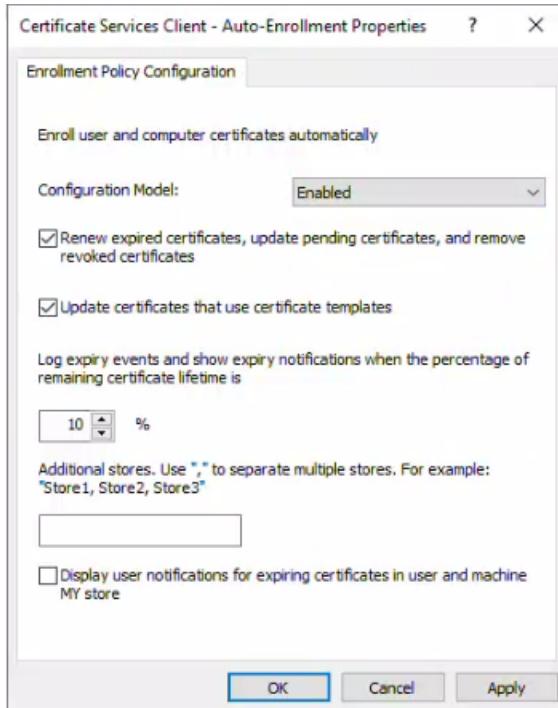
Click on Certificate services client – auto enrollment

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

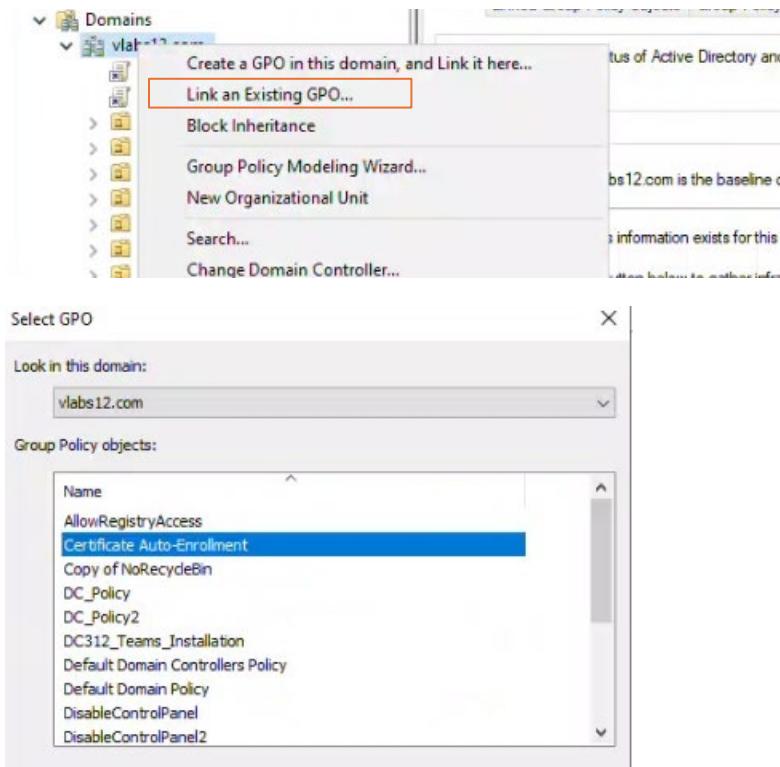


Repeat the process under User Configuration

The screenshot shows the 'Certificate Auto-Enrollment [DC112.VLABS12.COM] Policy' node in the left navigation pane of the Group Policy Management Editor. In the 'Object Type' pane on the right, 'Enterprise Trust' and 'Trusted People' are listed and highlighted with a red rectangle. Other items include 'Certificate Services Client - Certificate Enrollment Policy', 'Certificate Services Client - Credential Roaming', and 'Certificate Services Client - Auto-Enrollment'. The 'Software Settings' node under 'Policies' is also highlighted with a red rectangle.



Exit the Editor and link the GPO to the domain



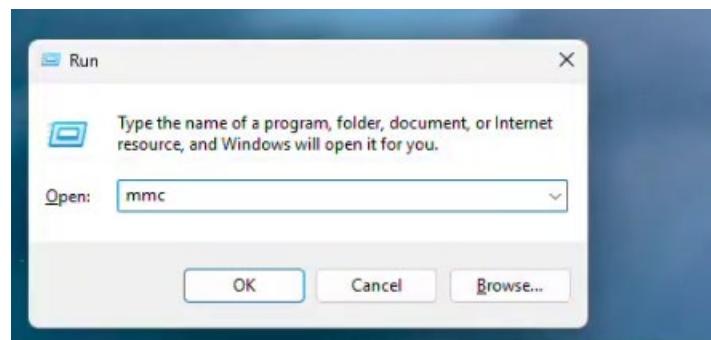
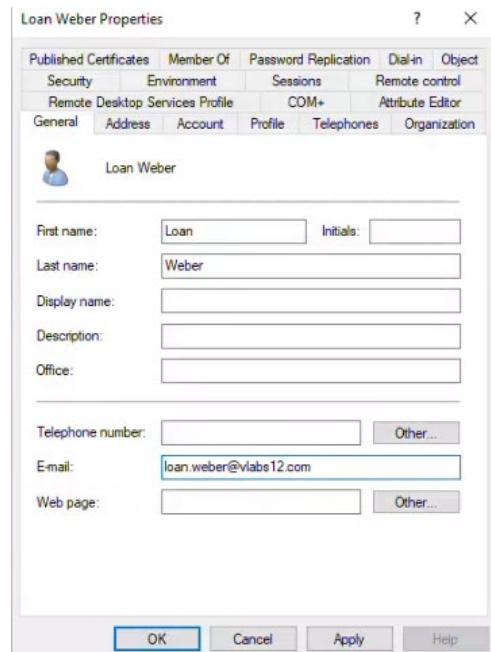
Always do a gpupdate /force after having made changes to a GPO

```
PS C:\Users\Administrator.DC112> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

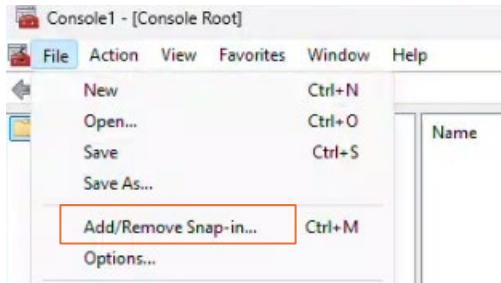
PS C:\Users\Administrator.DC112>
```

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

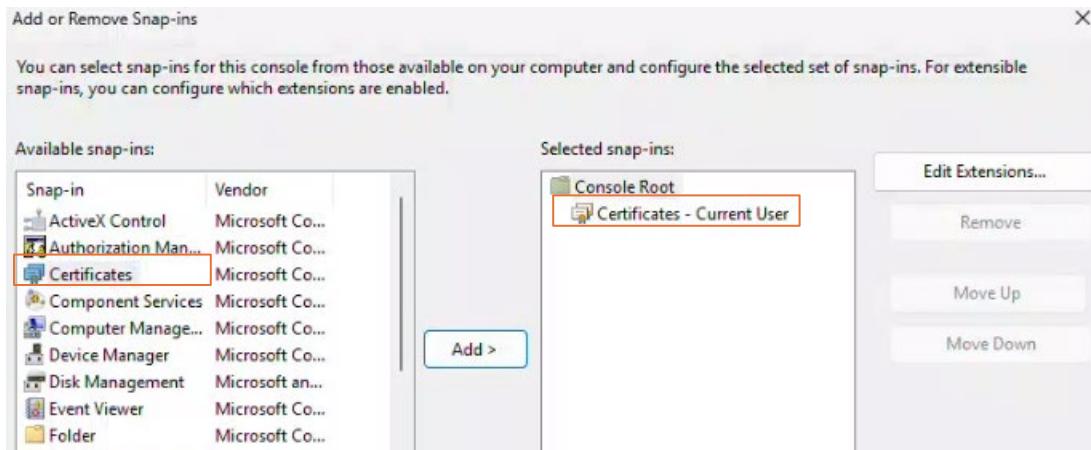
I'll give Loan Weber the email loan.weber@vlabs12.com and then sign in to Client12



Go to File → Add/Remove Snap-in..

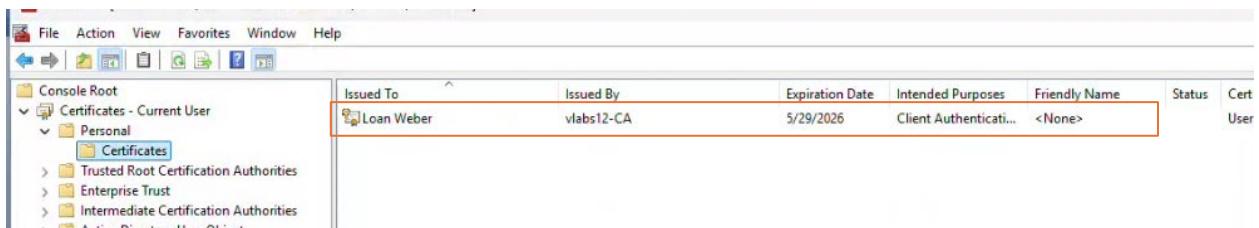


Certificates → Add



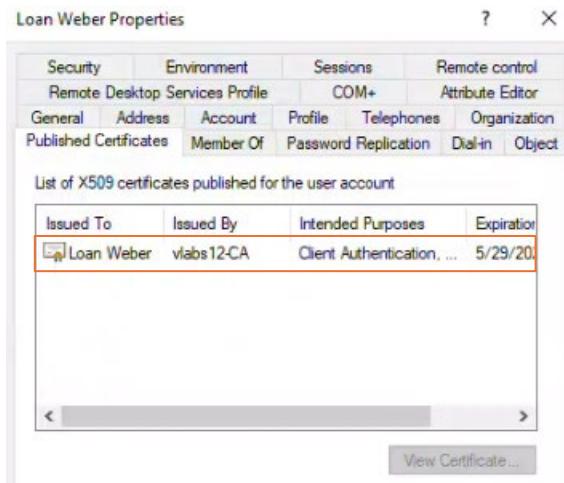
Expand Certificates – Current User

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

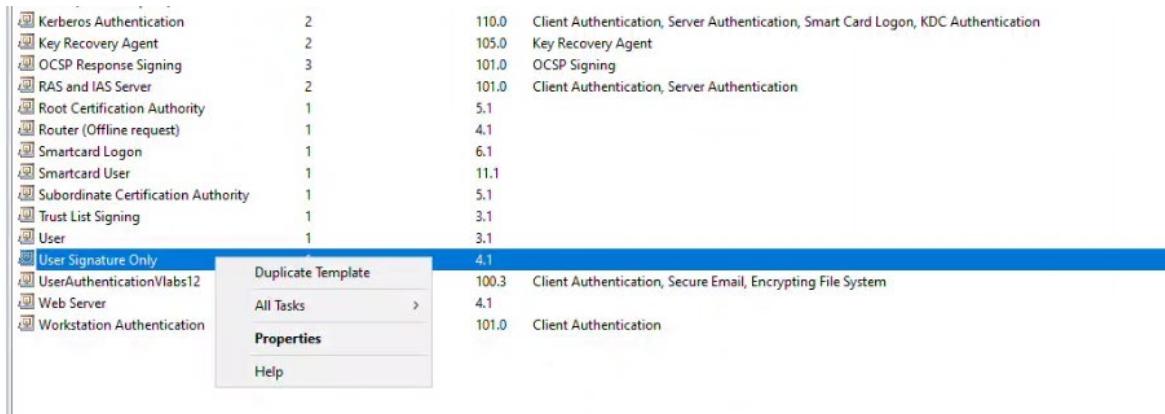
Verify that he has received this certificate.

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.

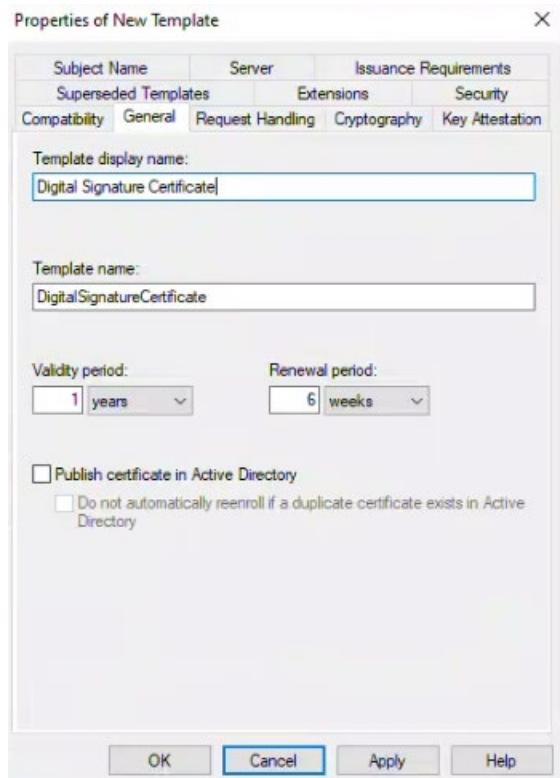
We need to configure a Digital Signing Certificate Template using certificate template console

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

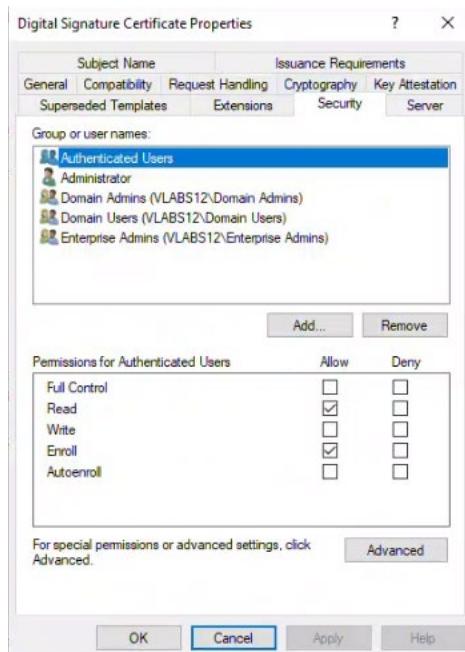
Right click on User Signature Only template and select Duplicate Template



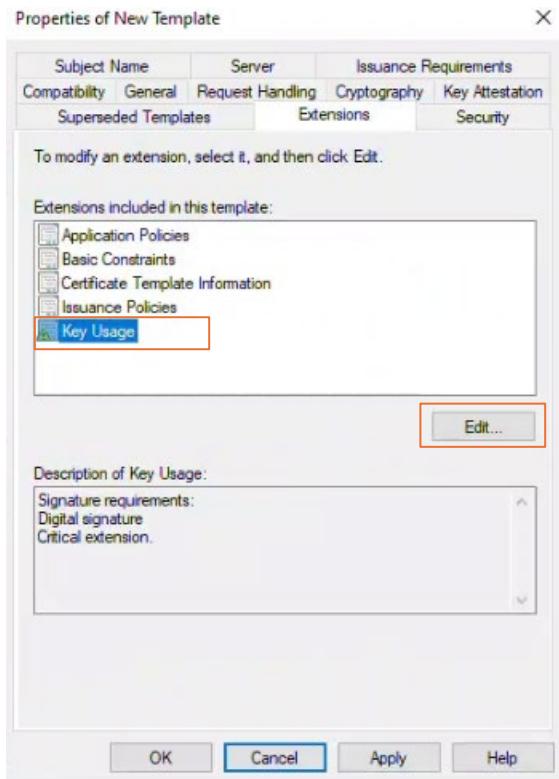
Go to the General tab and set a display name



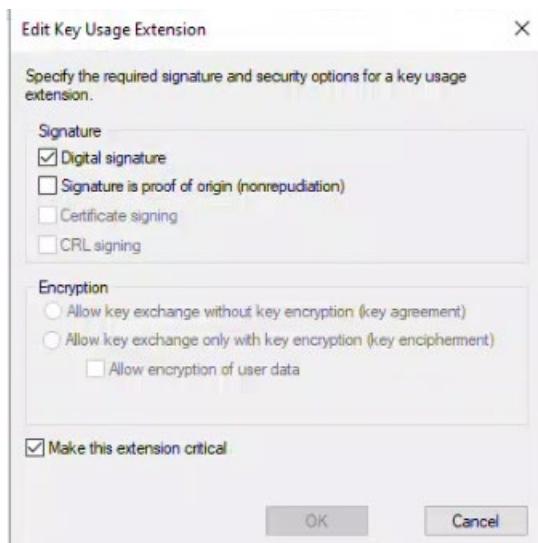
Go to the Security tab and give Authenticated Users the permissions Read, Enroll (we won't be adding Autoenroll this time since we need to test by manually requesting the certificate and we have a GPO specifically for autoenroll)



In the Extensions tab, click on Key Usage → Edit



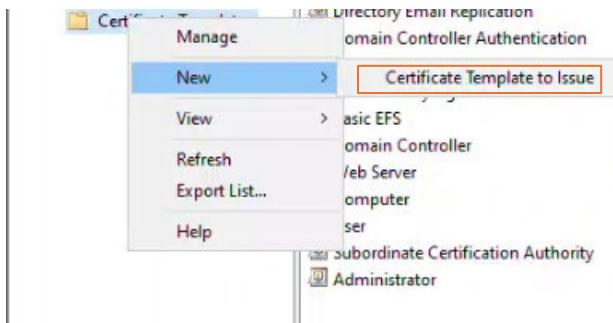
Verify that Digital signature is checked



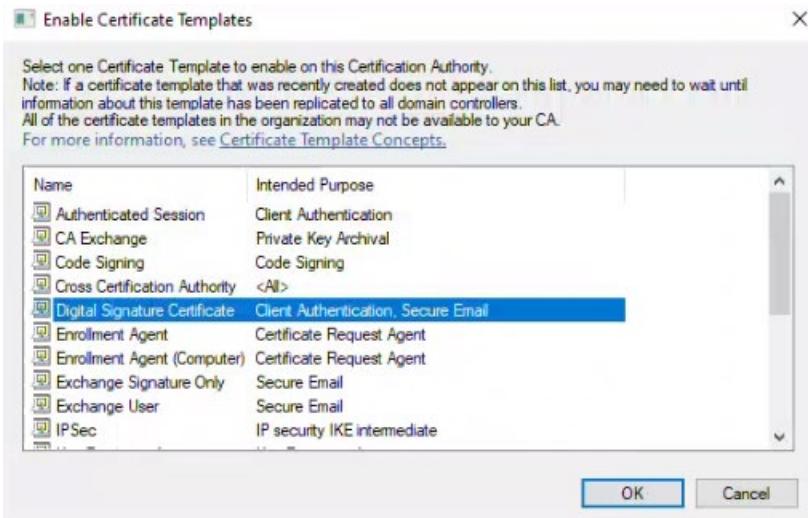
Now we need to publish the template to the CA

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.



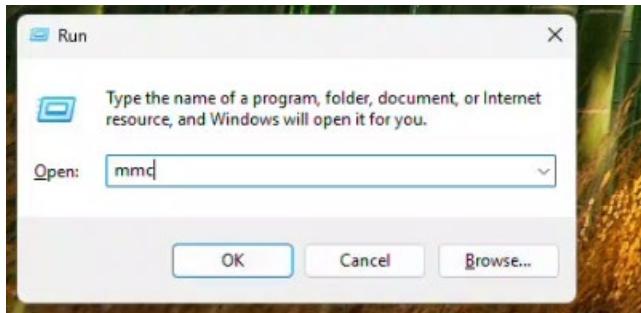
Name	Intended Purpose
Digital Signature Certificate	Client Authentication, Secure Email
UserAuthenticationVlabs12	Client Authentication, Secure Email, En...
IPSec (Offline request)	IP security IKE intermediate
CEP Encryption	Certificate Request Agent
Exchange Enrollment Agent (Offline r...	Certificate 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...

Double-click it to see its purposes.

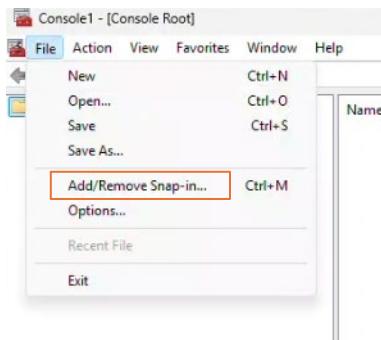


Now we need to test with a user on Client12. I'll use Louis Roux this time.

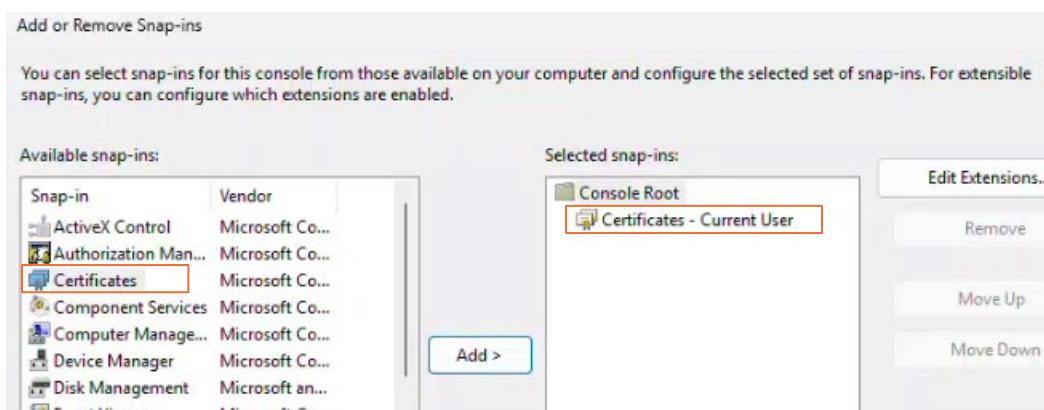
Use Run and type mmc



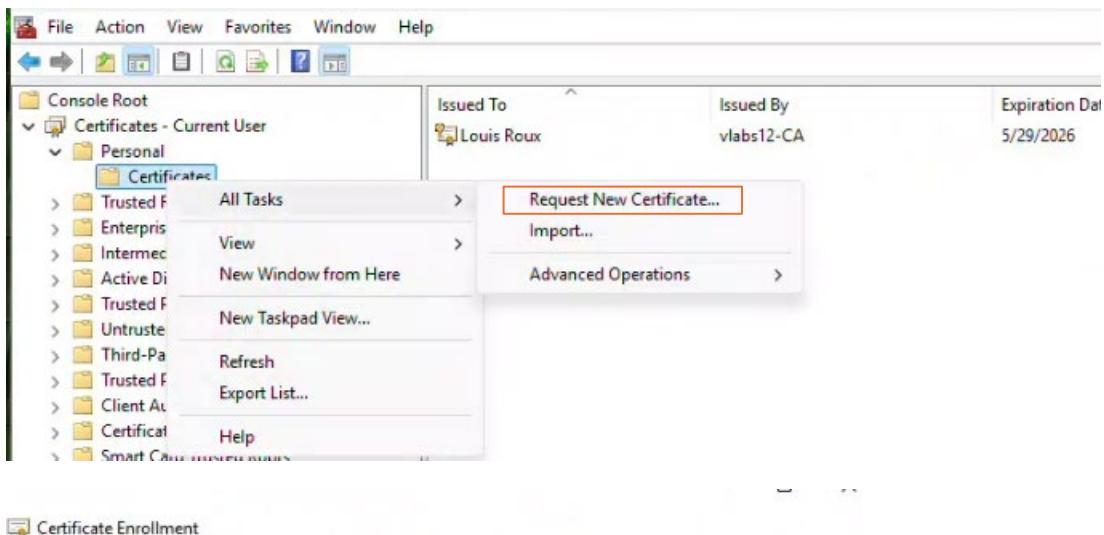
Go to File → Add/Remove Snap-in..



Go to Certificates → Add



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



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.

The screenshot shows a configuration dialog for certificate enrollment policies. It has two main sections: 'Configured by your administrator' and 'Configured by you'. The 'Configured by your administrator' section contains a dropdown menu set to 'Active Directory Enrollment Policy'. The 'Configured by you' section is currently empty and has a blue 'Add New' button next to it. A vertical blue line highlights the 'Configured by you' section.

Select the Digital Signature Certificate and then click Enroll

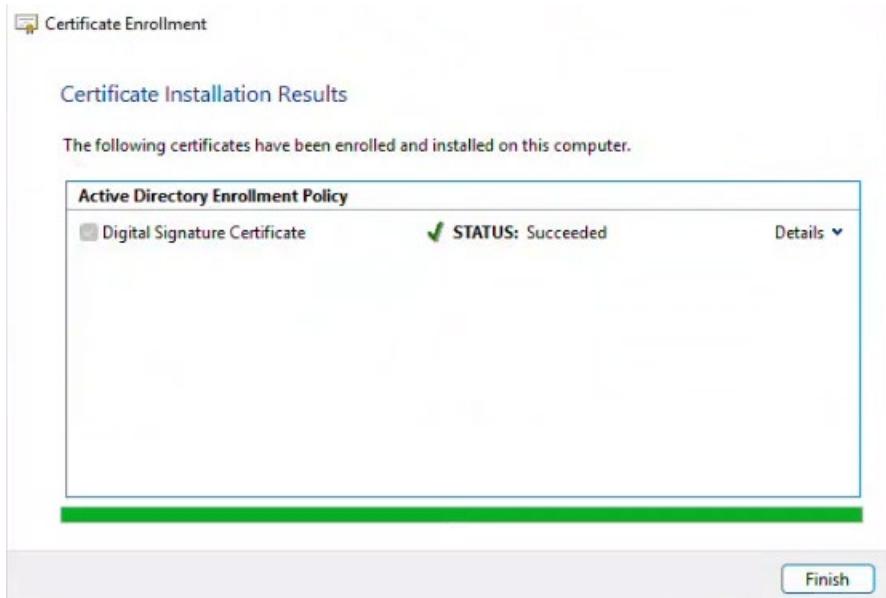
Certificate Enrollment

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		
<input type="checkbox"/> Basic EFS	STATUS: Available	Details ▾
<input checked="" type="checkbox"/> Digital Signature Certificate	STATUS: Available	Details ▾
<input type="checkbox"/> User	STATUS: Available	Details ▾
<input type="checkbox"/> UserAuthenticationVlabs12	STATUS: Available	Details ▾

Show all templates



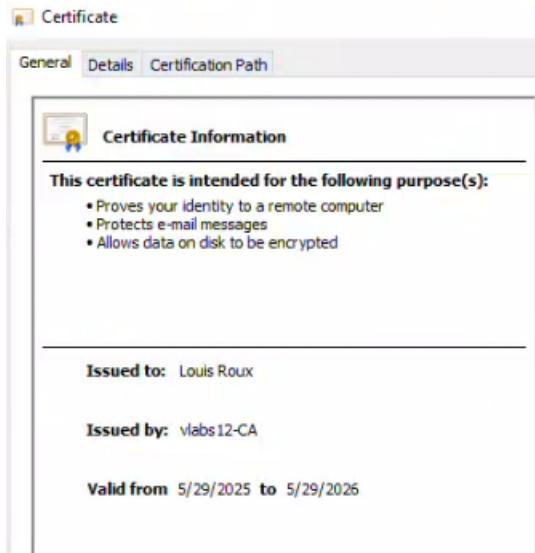
Now the new certificate will be shown along with the user authentication autoenroll one from the GPO

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Template
Louis Roux	vlabs12-CA	5/29/2026	Client Authentication	<None>		UserAuthenticationVlabs12
Louis Roux	vlabs12-CA	5/29/2026	Client Authentication	<None>		Digital Signature Certificate

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

The screenshot shows the 'Louis Roux Properties' dialog box. The 'Published Certificates' tab is selected. Below it, a table lists the X509 certificates published for the user account. The first entry is highlighted with a red border.

Issued To	Issued By	Intended Purposes	Expiration
Louis Roux	vlabs12-CA	Client Authentication, ...	5/29/2020



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

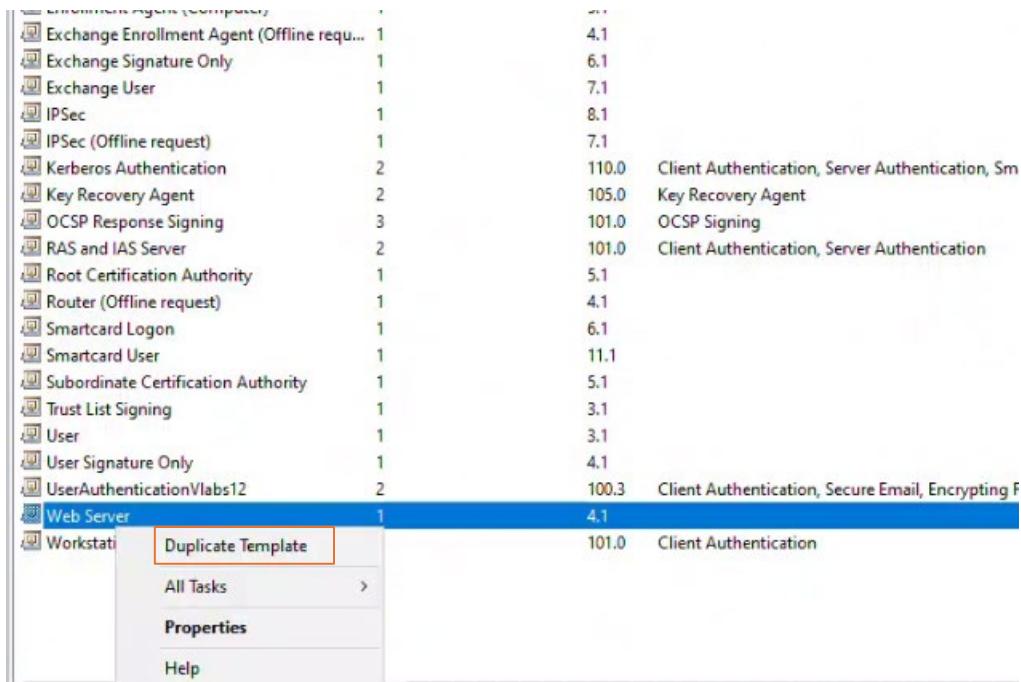
Bind the certificate to the local web server (IIS)

Test and verify HTTPS access to dc112.vlabs12.com

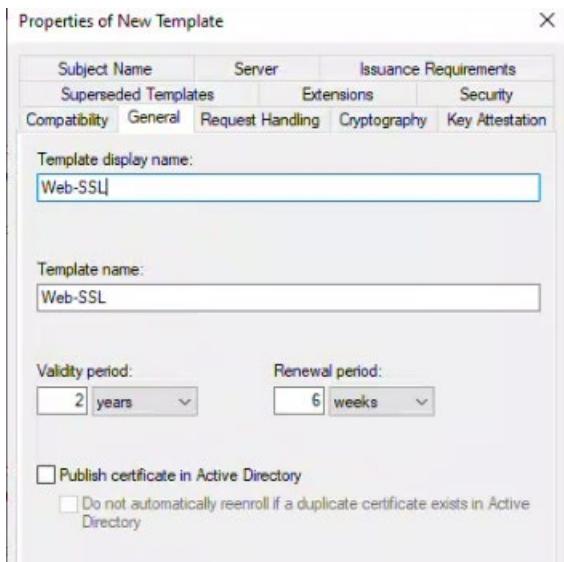
During this task, the internal web server will be secured using SSL/TLS certificates to ensure encrypted and safe communication. A trusted SSL certificate will be created on the Enterprise CA and issued for the designated server, allowing it to authenticate securely. The certificate will then be bound 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

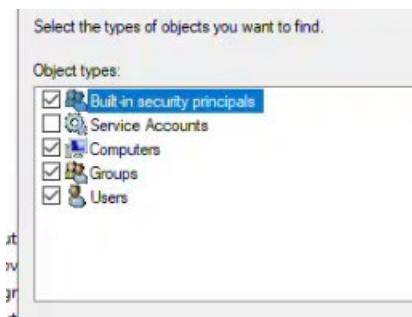
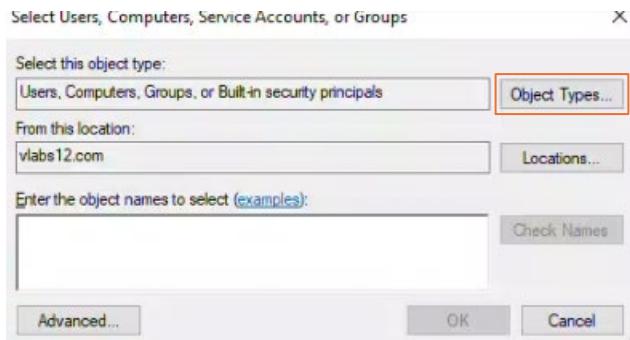


In the General tab, set a display name

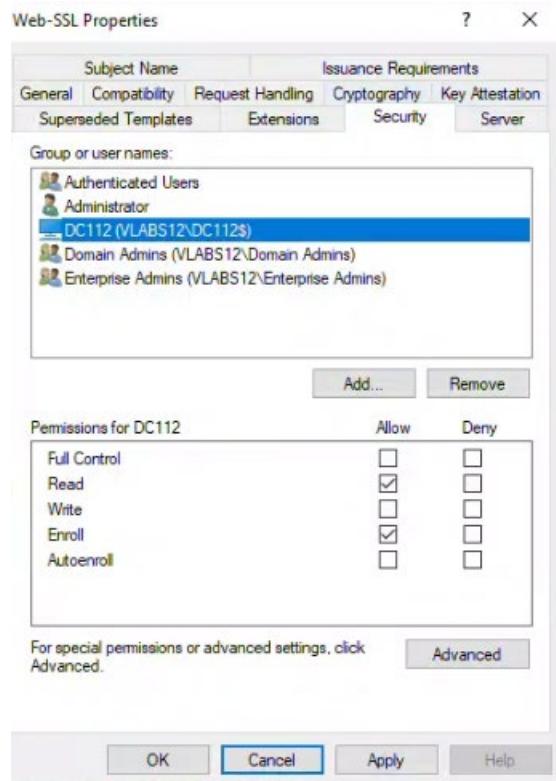


Go to Security and click Add

Click on Object Types and select Computers

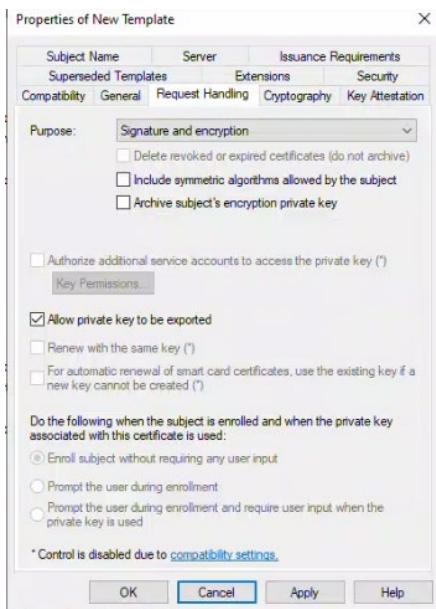


Add DC112

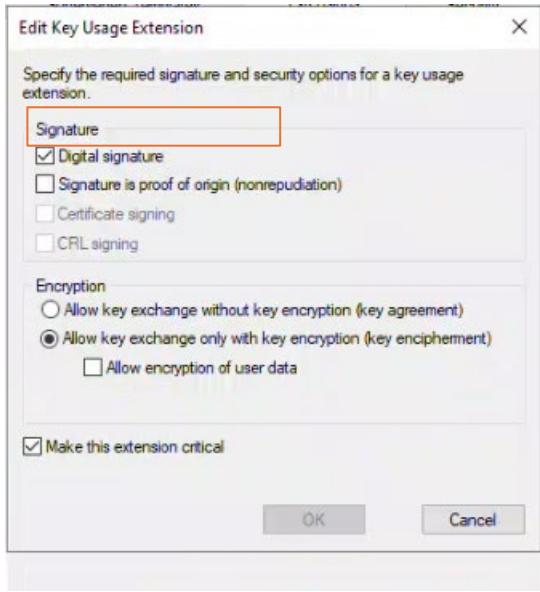


I'm just adding Enroll permissions this time but you can add autoenroll also

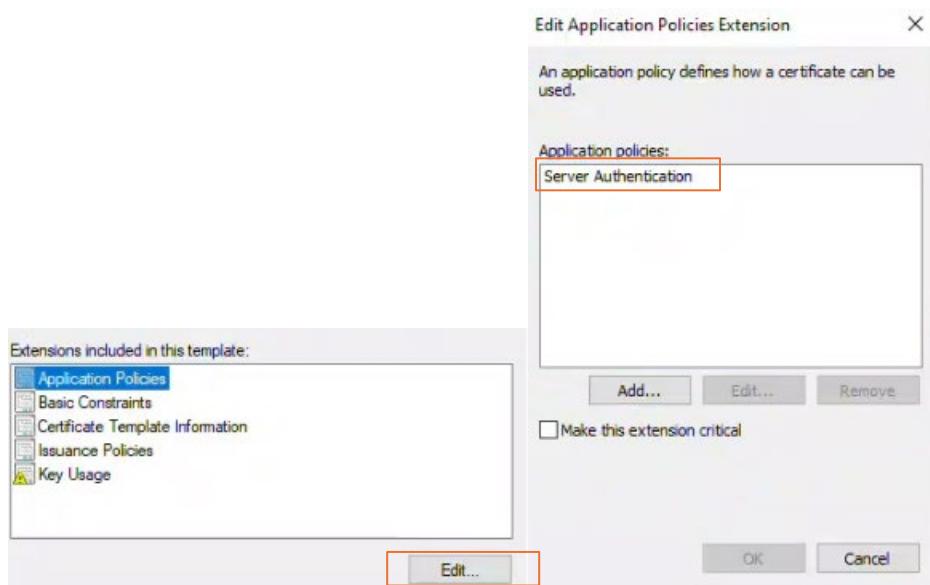
Next, go to Request Handling and check the box Allow private key to be exported



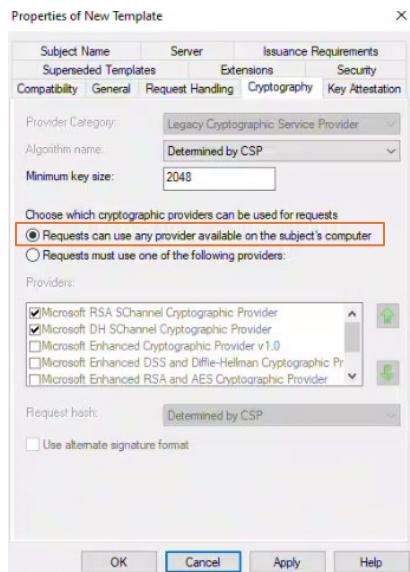
Enable the server authentication usage by going to Extensions → Key usage → Edit and make sure that Digital signature is checked



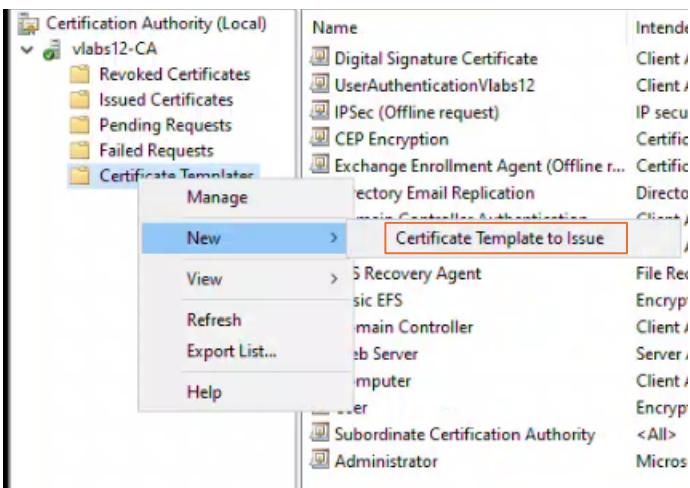
Click on Application Policies and ensure that Server Authentication is present



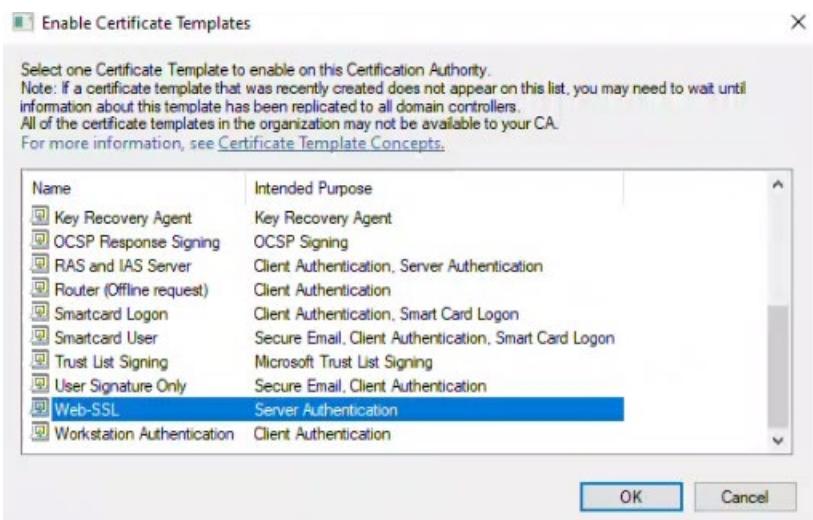
Now go to the Cryptography tab and make sure that “Requests can use any provider ...” is checked



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

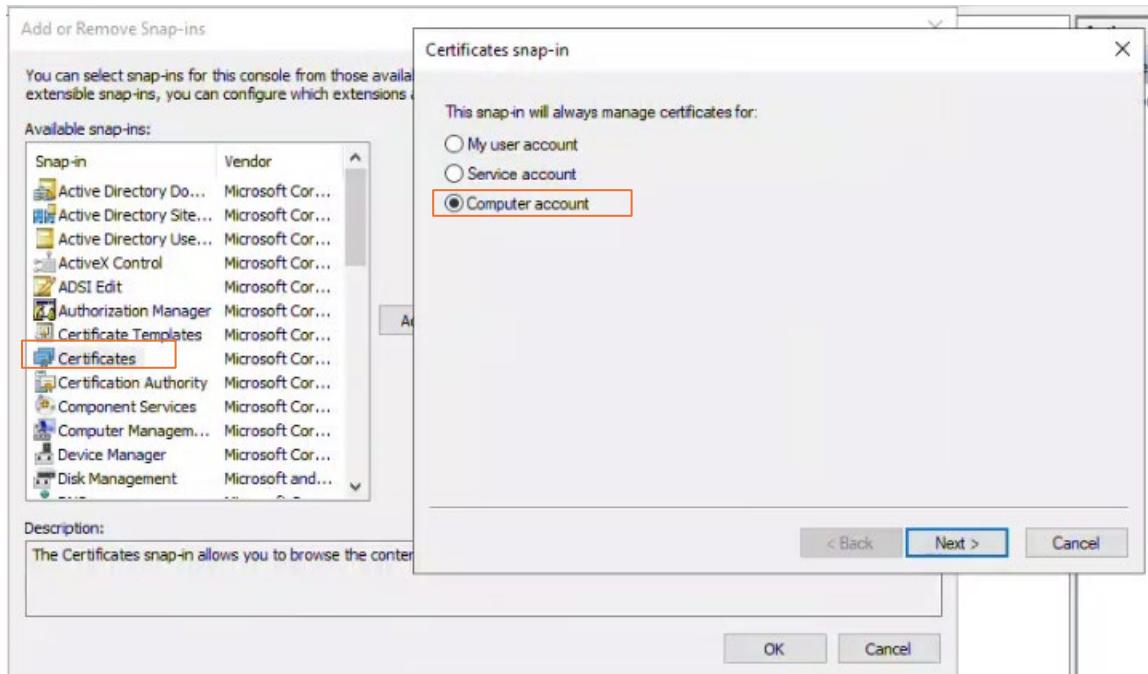
```
PS C:\Users\Administrator.DC112> Restart-Service certsvc
PS C:\Users\Administrator.DC112> ■
```

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

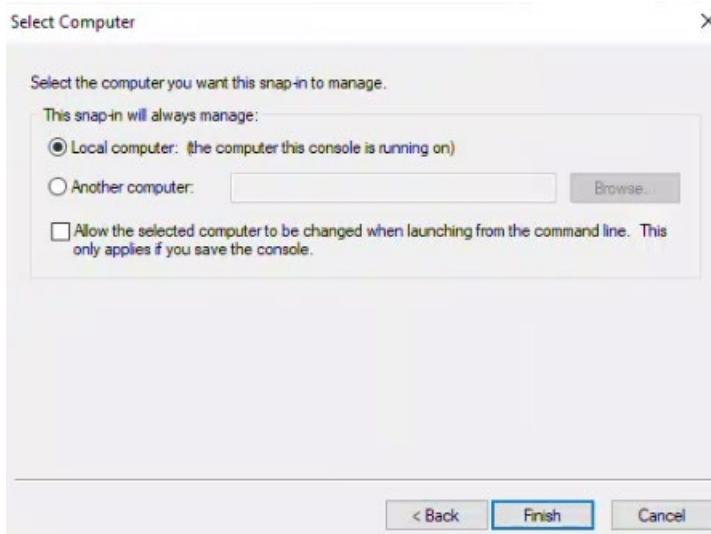
Open mmc on DC112 (Win+R, type mmc)

Go to File → Add/Remove Snap-in..

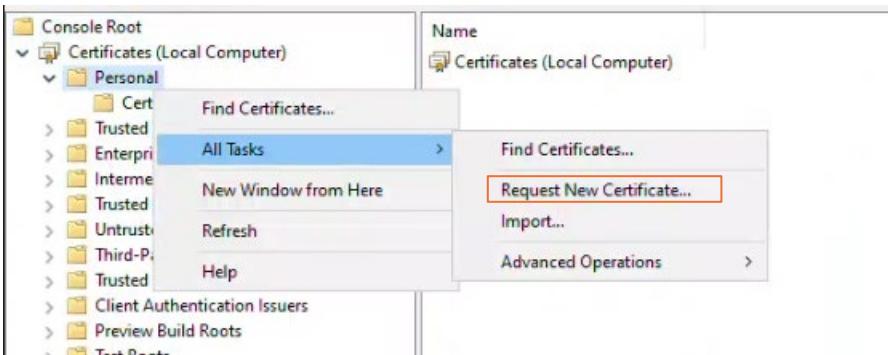
Select “Certificates” → Add and choose Computer account



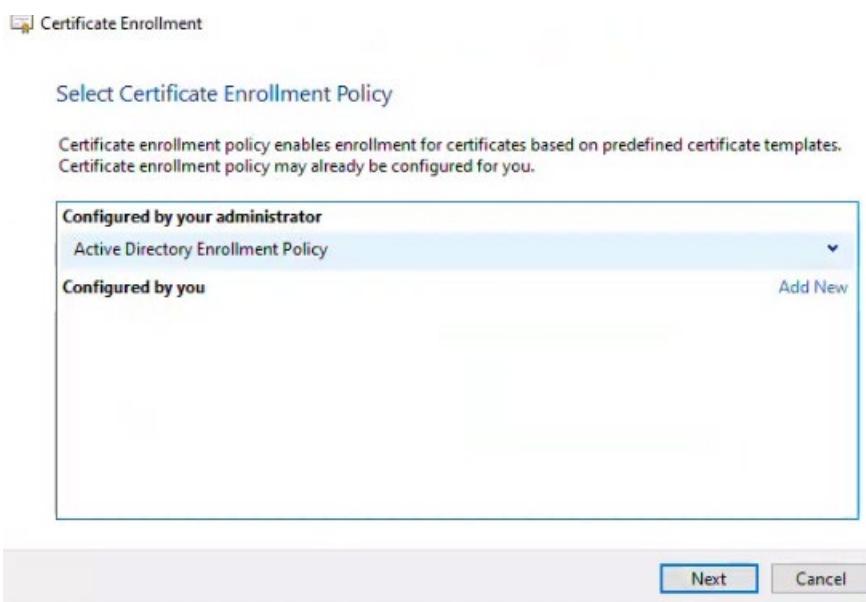
Keep this at Local computer. Click finish.



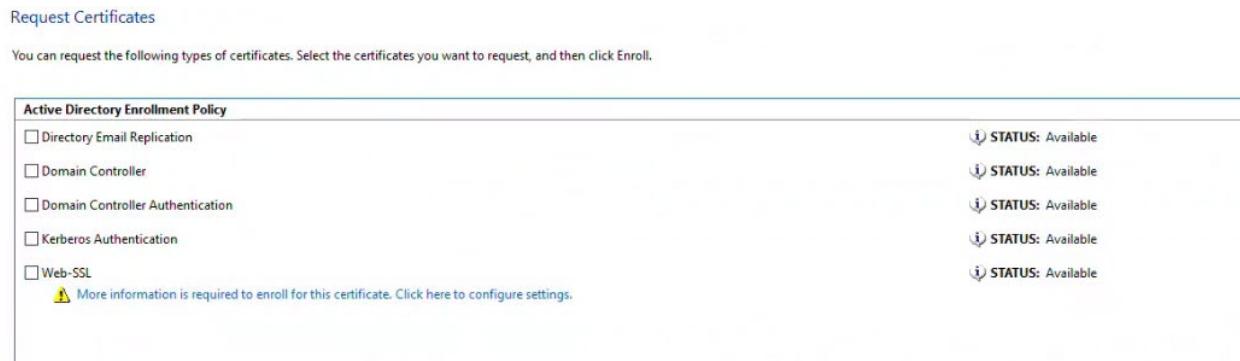
Expand Certificates → Personal → right click on Certificates → All Tasks → Request New Certificate



Click next and select AD Enrollment Policy → Next



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

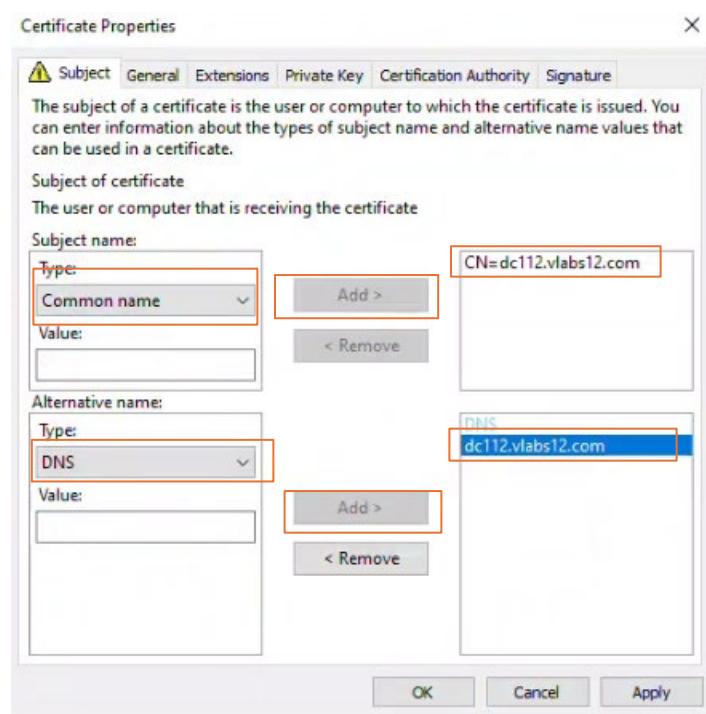


Use the dropdown menu for Type and select Common name

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

Certificate Properties

The following are the certificate extensions for this certificate type.

Key usage

The key usage extension describes the purpose of a certificate.

Available options:	Selected options:
CRL signing Data encipherment Decipher only Encipher only Key agreement Key certificate signing Non repudiation	Digital signature Key encipherment

Add > < Remove

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.

Subject General Extensions Private Key Certification Authority Signature

Cryptographic Service Provider

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

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

<input type="checkbox"/> Directory Email Replication	<i>STATUS: Available</i>	Details ▾
<input type="checkbox"/> Domain Controller	<i>STATUS: Available</i>	Details ▾
<input type="checkbox"/> Domain Controller Authentication	<i>STATUS: Available</i>	Details ▾
<input type="checkbox"/> Kerberos Authentication	<i>STATUS: Available</i>	Details ▾
<input checked="" type="checkbox"/> Web-SSL	<i>STATUS: Available</i>	Details ▾

Show all templates

Enroll **Cancel**

The screenshot shows the 'Active Directory Enrollment Policy' interface. At the top, there is a green checkmark icon next to 'Web-SSL' and the text 'STATUS: Succeeded'. Below this, there is a large, empty white area representing the policy details.

Verify using Certification Authority that the certificate has been issued

The screenshot shows the 'Certification Authority (Local)' interface. On the left, there is a navigation tree with 'vlab12-CA' expanded, showing 'Revoked Certificates', 'Issued Certificates' (which is selected), 'Pending Requests', 'Failed Requests', and 'Certificate Templates'. On the right, a table lists 21 issued certificates, each with columns for Request ID, Requester Name, Binary Certificate, Certificate Template, Serial Number, Certificate Effective Date, and Certificate Expiration Date. The table is sorted by Request ID.

Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration Date
3	LAB12\DC312\$	-----BEGIN CERT...	Domain Controller (...)	4b0000000379e...	5/28/2025 10:13 AM	5/28/2026 10:13 AM
4	VLABS12\DC112\$	-----BEGIN CERT...	Domain Controller (...)	4b000000042d...	5/28/2025 10:20 AM	5/28/2026 10:20 AM
5	VLABS12\Admini...	-----BEGIN CERT...	Exchange Enrollmen...	4b000000050b...	5/28/2025 10:46 AM	5/28/2027 10:46 AM
6	VLABS12\Admini...	-----BEGIN CERT...	CEP Encryption (CEP...)	4b0000000626c...	5/28/2025 10:46 AM	5/28/2027 10:46 AM
7	PARTNER12\DC4...	-----BEGIN CERT...	Domain Controller (...)	4b00000007fe...	5/28/2025 6:13 PM	5/28/2026 6:13 PM
8	VLABS12\esimon	-----BEGIN CERT...	UserAuthenticationV...	4b000000080cf...	5/29/2025 12:45 PM	5/29/2026 12:45 PM
10	VLABS12\DC112\$	-----BEGIN CERT...	Directory Email Repli...	4b0000000a5ec...	5/29/2025 2:07 PM	5/29/2026 2:07 PM
11	VLABS12\DC112\$	-----BEGIN CERT...	Domain Controller A...	4b0000000fbf5...	5/29/2025 2:07 PM	5/29/2026 2:07 PM
12	VLABS12\DC112\$	-----BEGIN CERT...	Kerberos Authentica...	4b0000000c688...	5/29/2025 2:07 PM	5/29/2026 2:07 PM
13	VLABS12\lweber	-----BEGIN CERT...	UserAuthenticationV...	4b0000000deb...	5/29/2025 2:12 PM	5/29/2026 2:12 PM
14	VLABS12\lrenard	-----BEGIN CERT...	Digital Signature Cer...	4b0000000e2d...	5/29/2025 2:48 PM	5/29/2026 2:48 PM
15	VLABS12\lweber	-----BEGIN CERT...	Digital Signature Cer...	4b0000000f90f...	5/29/2025 2:48 PM	5/29/2026 2:48 PM
16	VLABS12\lrenard	-----BEGIN CERT...	UserAuthenticationV...	4b0000001089e...	5/29/2025 2:48 PM	5/29/2026 2:48 PM
19	VLABS12\lroux	-----BEGIN CERT...	UserAuthenticationV...	4b000000139d...	5/29/2025 3:19 PM	5/29/2026 3:19 PM
20	VLABS12\lroux	-----BEGIN CERT...	Digital Signature Cer...	4b00000014b8...	5/29/2025 3:22 PM	5/29/2026 3:22 PM
21	VLABS12\DC112\$	-----BEGIN CERT...	Web-SSL (1.3.6.1.4.1...)	4b000000152c8...	5/29/2025 5:47 PM	5/29/2027 5:47 PM

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

Using PowerShell, run the following command to install IIS

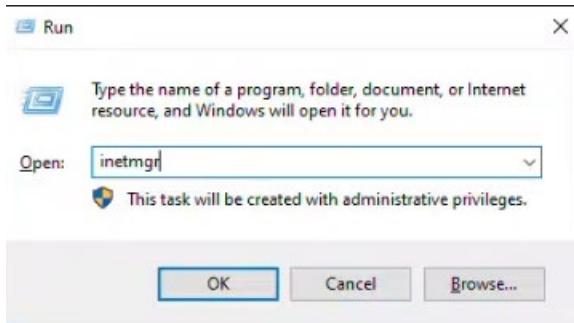
```
PS C:\Users\Administrator.DC112> Install-WindowsFeature -Name Web-Server -IncludeManagementTools

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

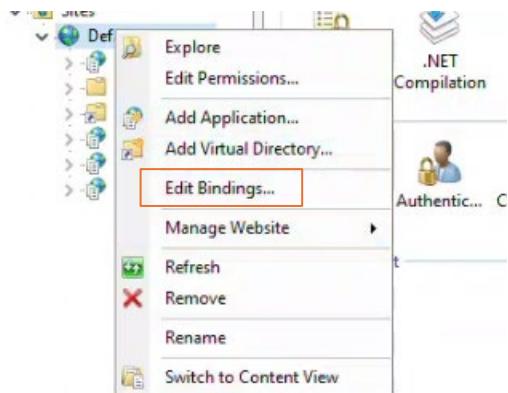
PS C:\Users\Administrator.DC112>
```

Use Run to open IIS Manager

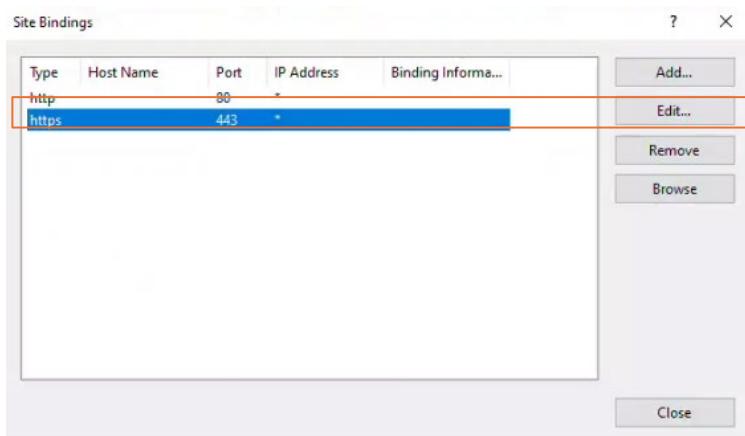
Type inetmgr



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



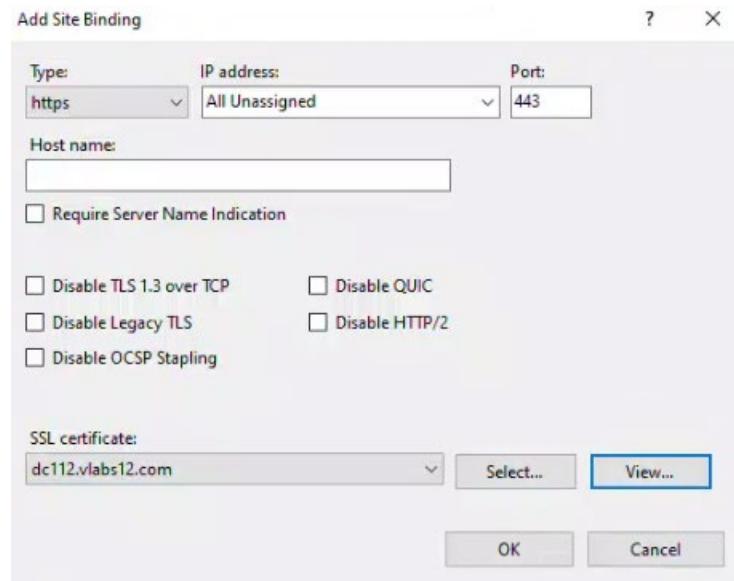
Select https and click on edit



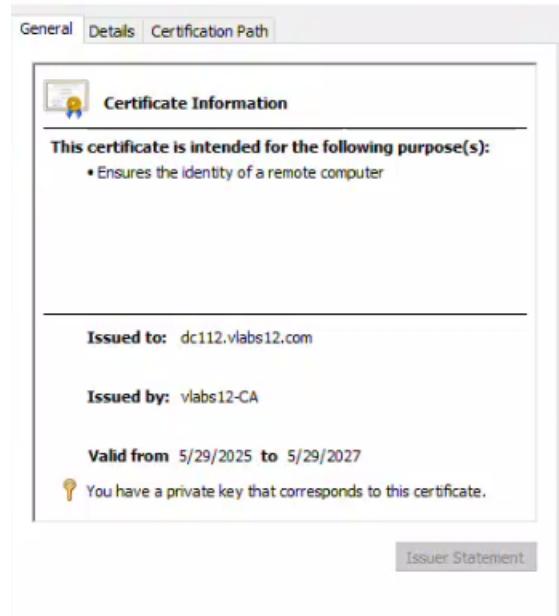
Leave IP address as **All Unassigned**

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.

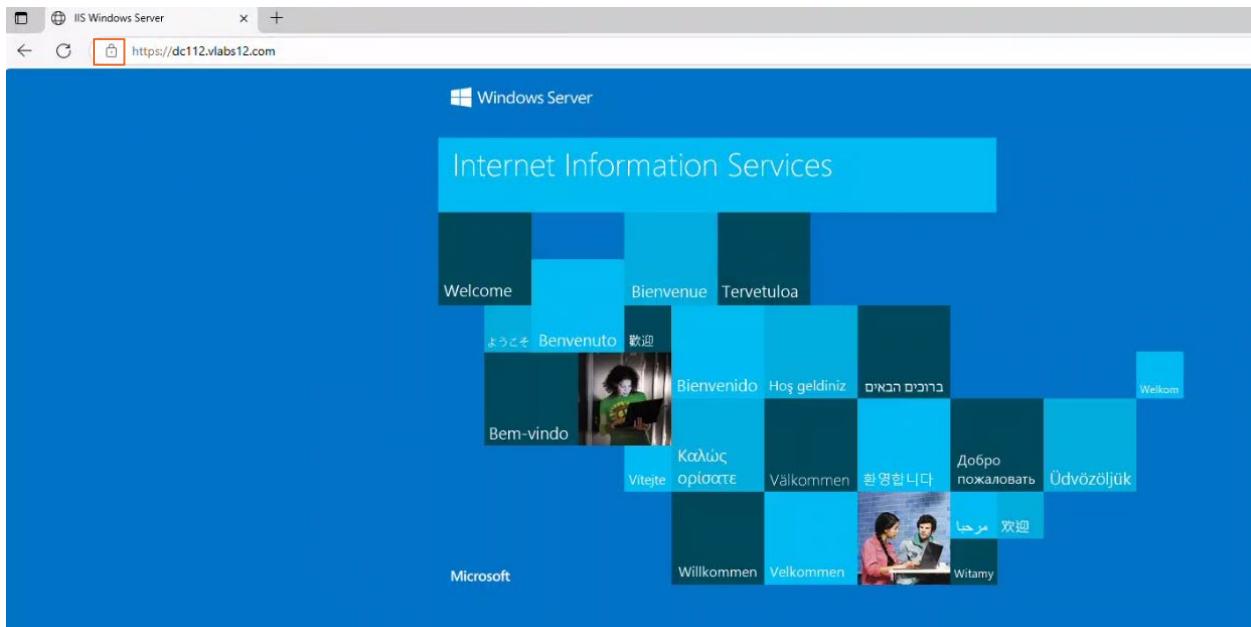


Restart IIS using PowerShell and the following command:

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	ad7498cdcf64ece30c3646ebd58ef0e8da2c5b0d2c9d0ecd541810f44bdcb0d

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...

