Setup Server 2019 Enterprise CA 2/5: Offline Root CA

vmlabblog.com/2019/09/setup-server-2019-enterprise-ca-2-5-offline-root-ca

Aad Lutgert September 25, 2019

Previous: Overview

Updated 06-08-2020: Fixed typo CAPolicy.inf and removed incorrect screenshot.

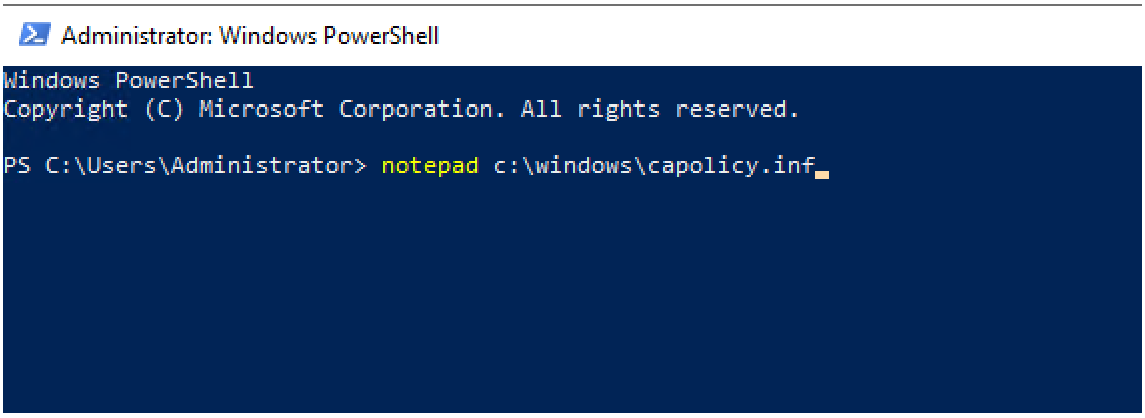
The Setup will start with the Offline Root CA server. This server will only be used to authorize the Subordinate Server and after that it will be turned off and only turned on to create and renew Subordinate CA Certificates. The offline CA Server is the OFFENT-CA01 and is a non-domainjoined server.

Setup Offline Root CA

First we will create the CApolicy.inf. This is a configuration file that defines multiple settings that are applied to the root CA certificate and all other certificates issued by the root CA. This file needs to be created before the ADCS is installed on the root CA. For more information about the Syntax go here.

1. Start powershell and type the following line and press “enter”:

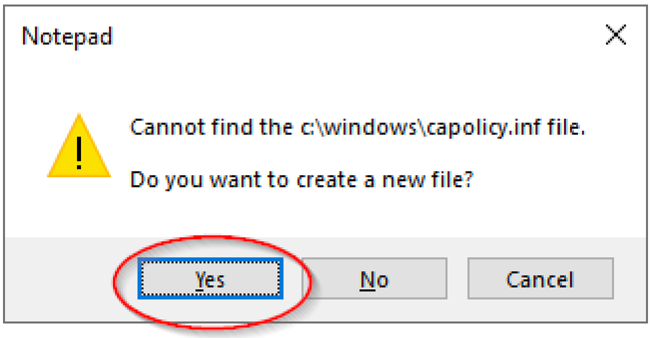
```
notepad c:\windows\capolicy.inf
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> notepad c:\windows\capolicy.inf
```

2. Select “yes” to create the new file



Notepad

Cannot find the c:\windows\capolicy.inf file.

Do you want to create a new file?

3. Because this is a lab setup I will only setup some basic settings for the Root CA. I will configure the following settings:

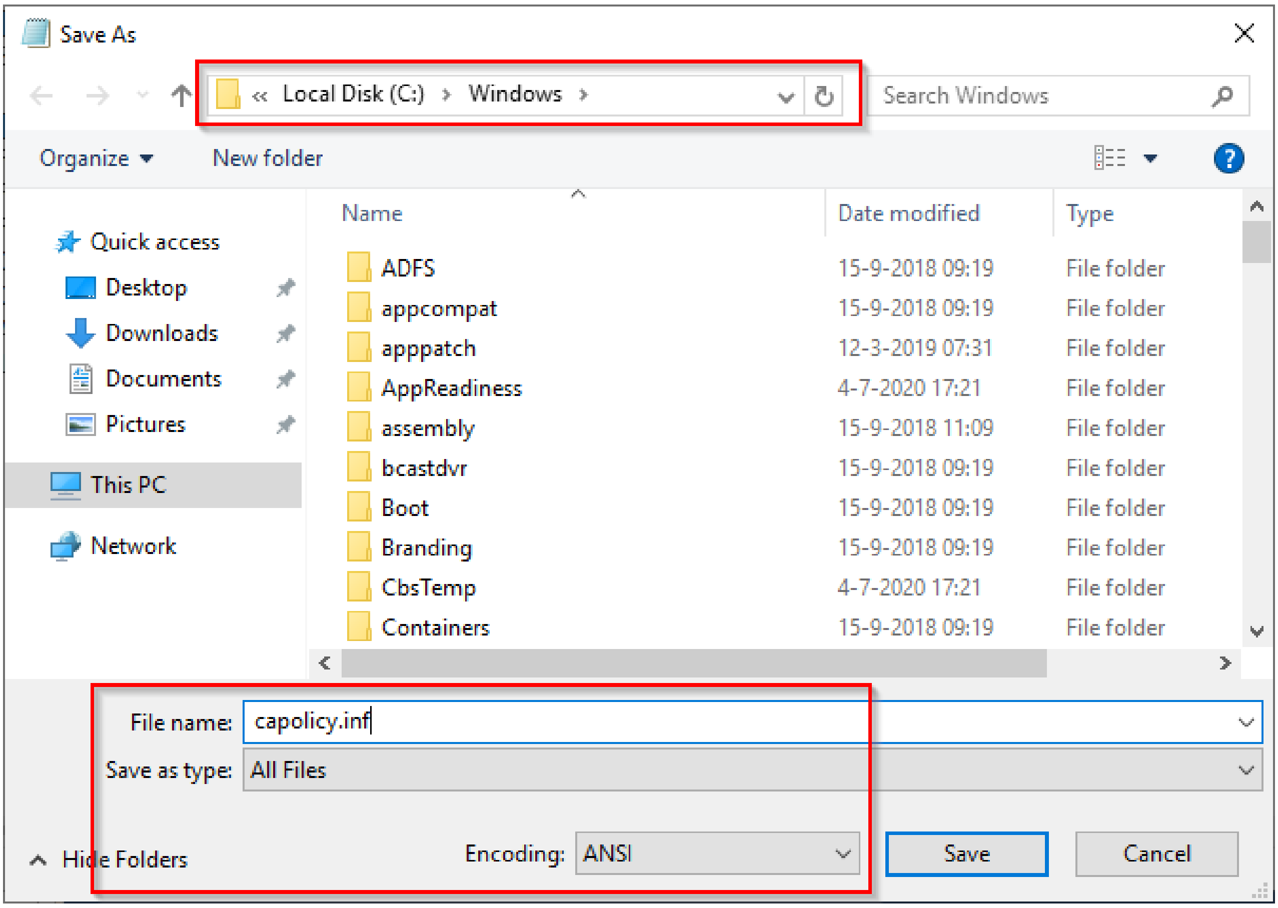
- Renewalinformation for the CA certificate.
- The validity period for the base CRL.
- Disable the AlternateSignatureAlgorithm (more info on why can be found here).
- Disable the DefaultTemplates, these are not used because this is an offline CA.

For this lab I will use a random generated OID which is based on the Microsoft OID. Because these generated OID may not be unique you should request a private enterprise number at IANA (link). This number can be added to the CAPolicy.inf.

```
[Version]
Signature="$Windows NT$"

[Certsrv_Server]
RenewalKeyLength=4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
CRLPeriod=Years
CRLPeriodUnits=1
AlternateSignatureAlgorithm=0
LoadDefaultTemplates=0
```

4. Save the file as “capolicy.inf” using “All files” and “ANSI” Encoding.



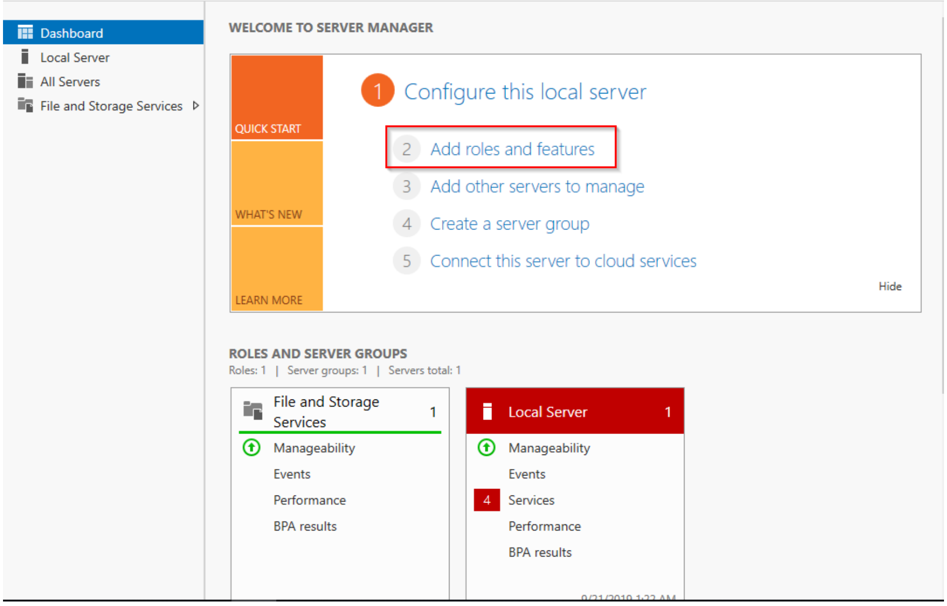
Name	Date modified	Type
ADFS	15-9-2018 09:19	File folder
appcompat	15-9-2018 09:19	File folder
apppatch	12-3-2019 07:31	File folder
AppReadiness	4-7-2020 17:21	File folder
assembly	15-9-2018 11:09	File folder
bcastdvr	15-9-2018 09:19	File folder
Boot	15-9-2018 09:19	File folder
Branding	15-9-2018 09:19	File folder
CbsTemp	4-7-2020 17:21	File folder
Containers	15-9-2018 09:19	File folder

File name: capolicy.inf

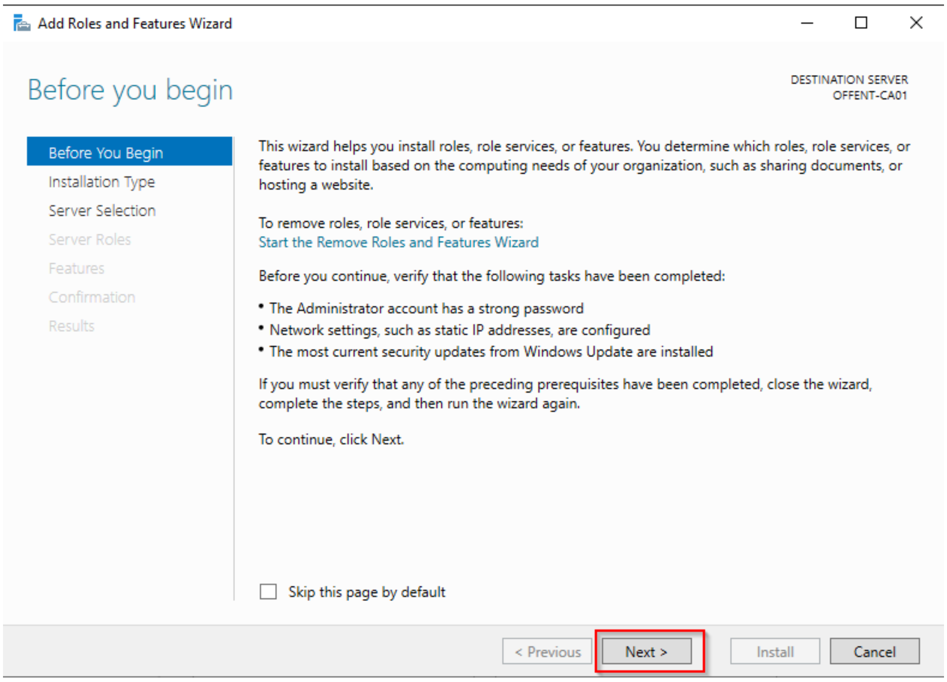
Save as type: All Files

Encoding: ANSI

5. Now we the role can be added and configured. Start the Server manager and select “Add roles and features”



6. The “Add Roles and Features Wizard” will start, press “Next” to continue.



Add Roles and Features Wizard

Before you begin

DESTINATION SERVER
OFFENT-CA01

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

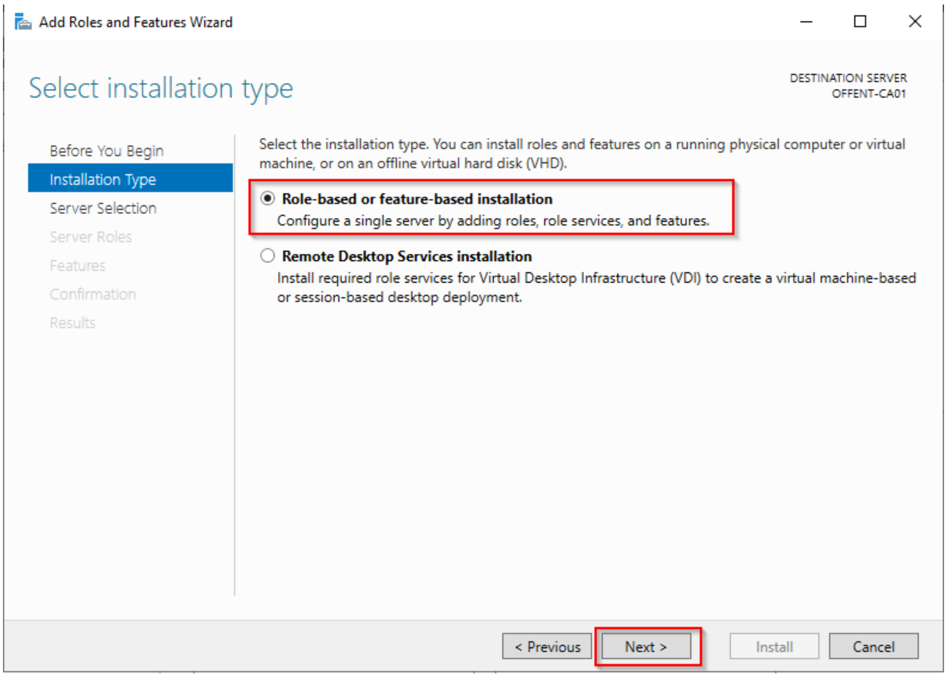
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

7. Select “Role-based or feature-based installation” and press “Next”



Add Roles and Features Wizard

Select installation type

DESTINATION SERVER
OFFENT-CA01

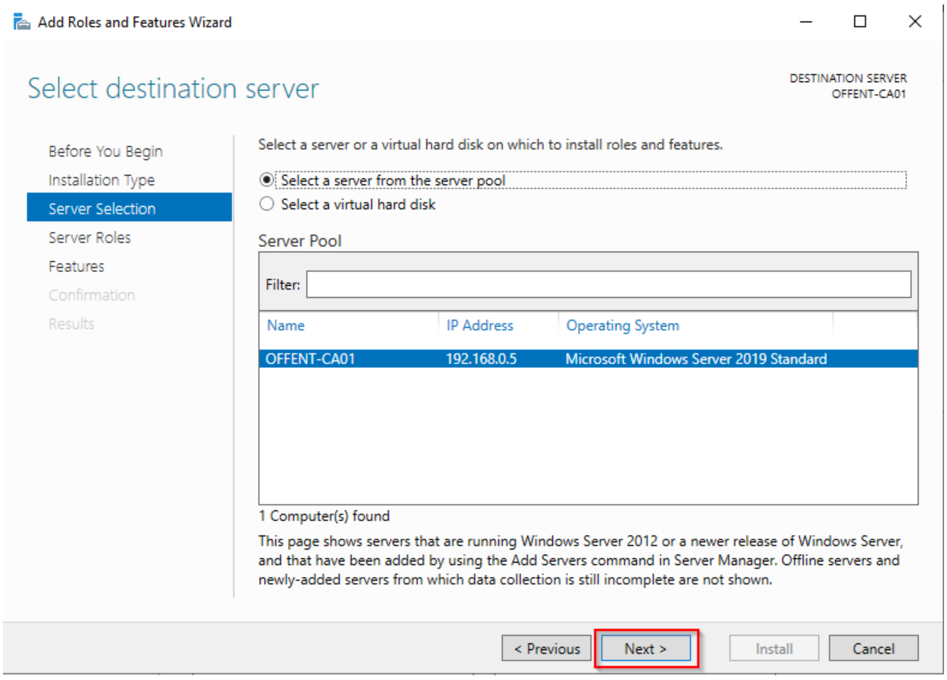
- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

8. Use the default settings and press “Next” to continue.



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
OFFENT-CA01

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

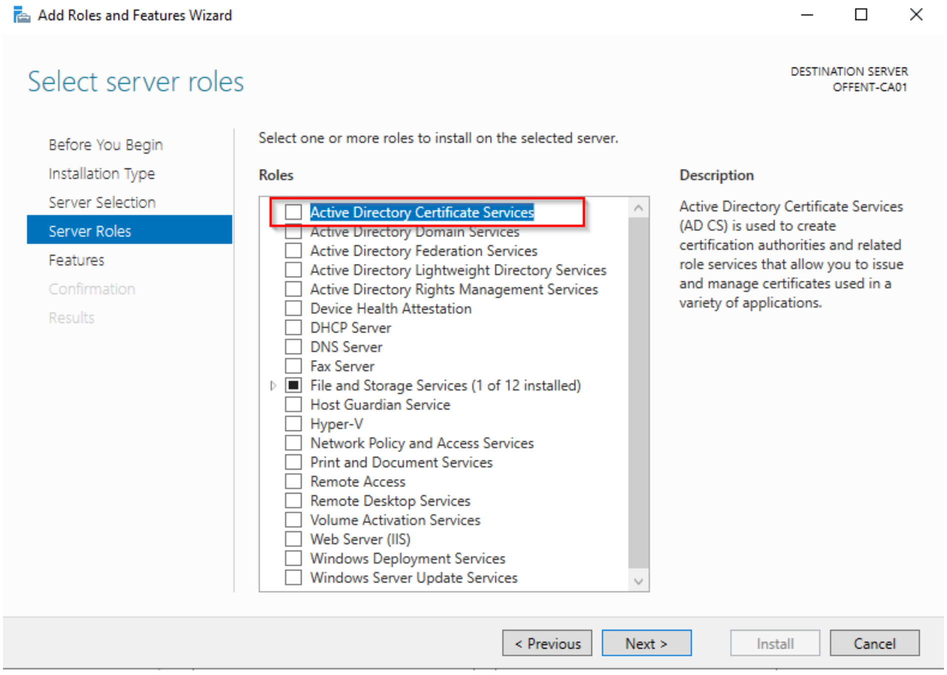
Filter:

Name	IP Address	Operating System
OFFENT-CA01	192.168.0.5	Microsoft Windows Server 2019 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

9. Select “Active Directory Certificate Services”



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
OFFENT-CA01

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more roles to install on the selected server.

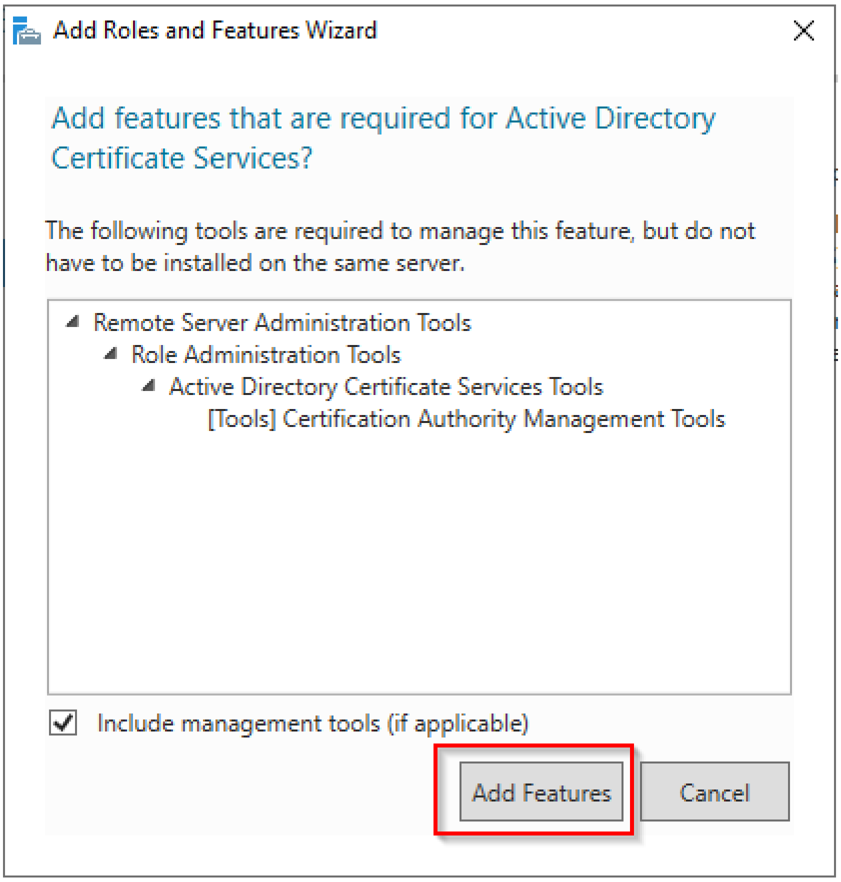
Roles

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

10. A pop-up will appear, press “Add Features” to continue.



Add Roles and Features Wizard

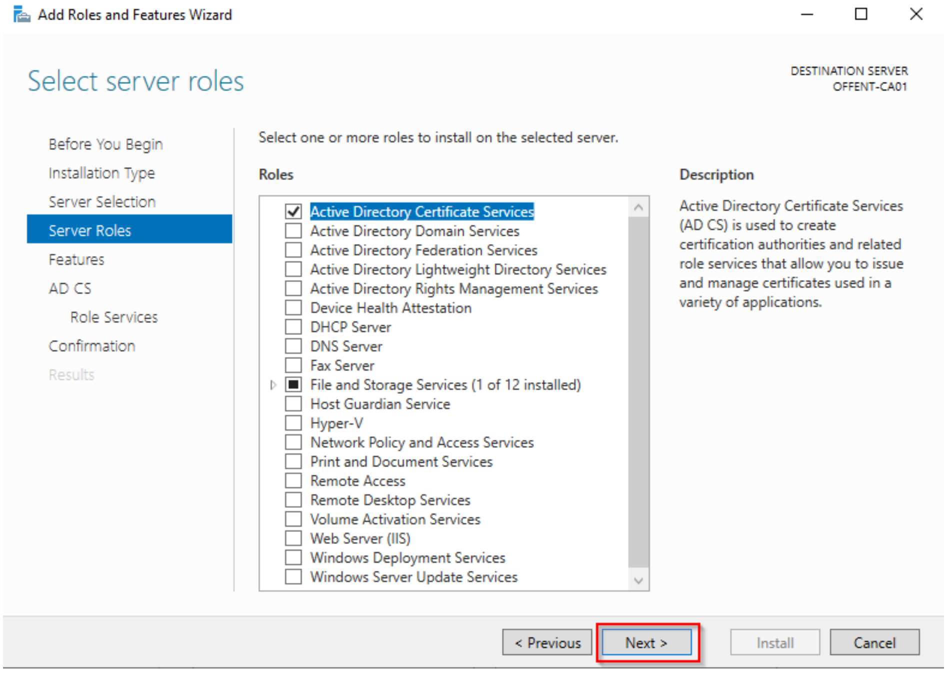
Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - Active Directory Certificate Services Tools
      - [Tools] Certification Authority Management Tools

☑ Include management tools (if applicable)

11. Press “Next” to continue



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
OFFENT-CA01

Select one or more roles to install on the selected server.

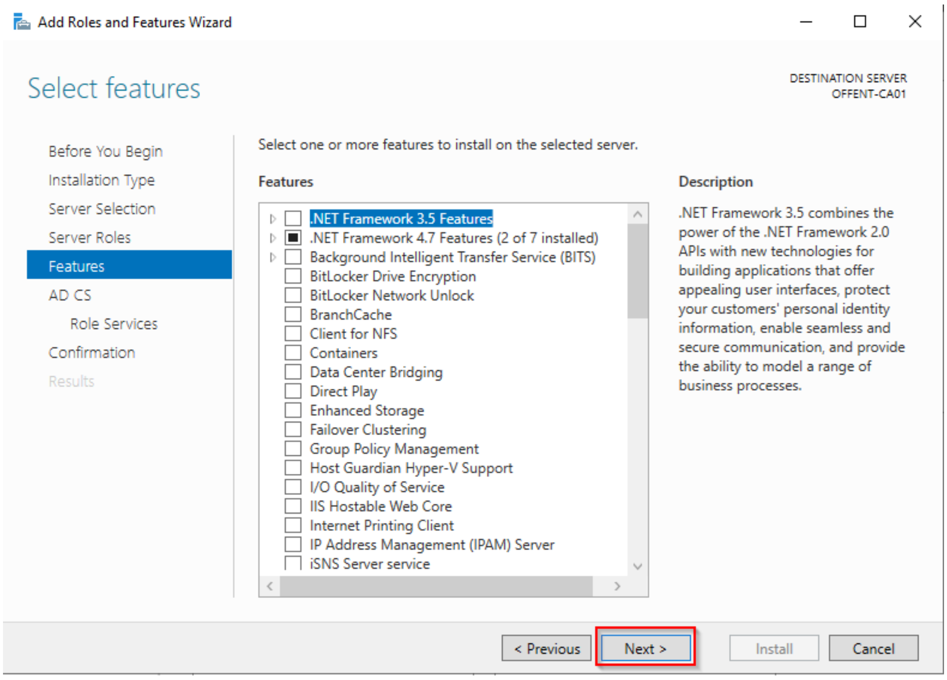
Roles

☑ Active Directory Certificate Services
☐ Active Directory Domain Services
☐ Active Directory Federation Services
☐ Active Directory Lightweight Directory Services
☐ Active Directory Rights Management Services
☐ Device Health Attestation
☐ DHCP Server
☐ DNS Server
☐ Fax Server
■ File and Storage Services (1 of 12 installed)
☐ Host Guardian Service
☐ Hyper-V
☐ Network Policy and Access Services
☐ Print and Document Services
☐ Remote Access
☐ Remote Desktop Services
☐ Volume Activation Services
☐ Web Server (IIS)
☐ Windows Deployment Services
☐ Windows Server Update Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

12. Press “Next” to continue.



Select features

Select one or more features to install on the selected server.

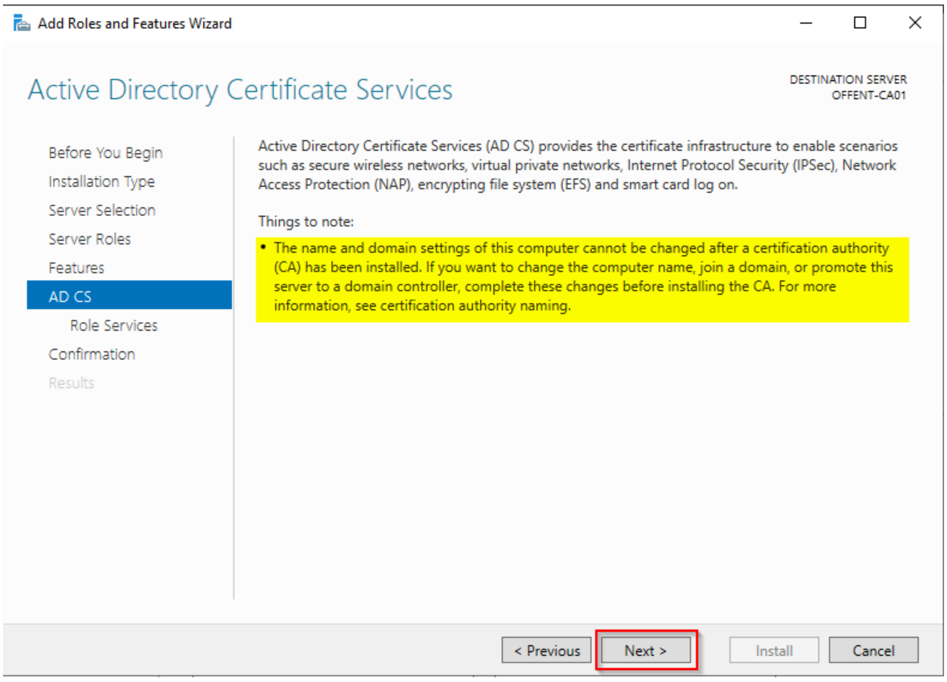
Features

- □ .NET Framework 3.5 Features
- ■ .NET Framework 4.7 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- □ Group Policy Management
- □ Host Guardian Hyper-V Support
- □ I/O Quality of Service
- □ IIS Hostable Web Core
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server
- □ iSNS Server service

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

13. Check if the Servername is correct and press “Next” to continue.



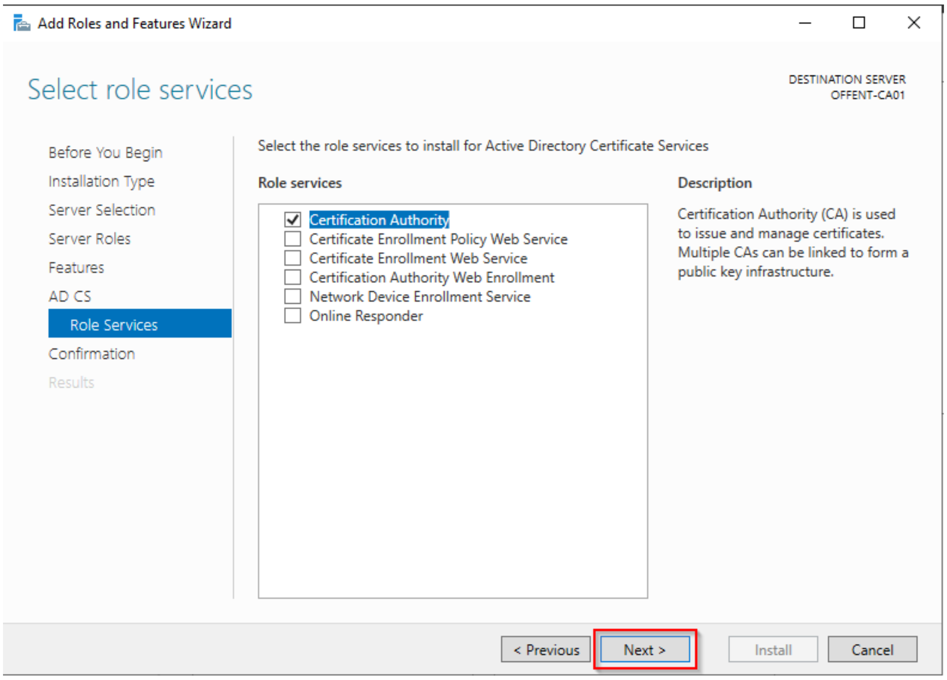
Active Directory Certificate Services

Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card log on.

Things to note:

- The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

14. Use the default settings, for the Root CA only the “Certification Authority” role is needed.


Add Roles and Features Wizard

Select role services

DESTINATION SERVER
OFFENT-CA01

Select the role services to install for Active Directory Certificate Services

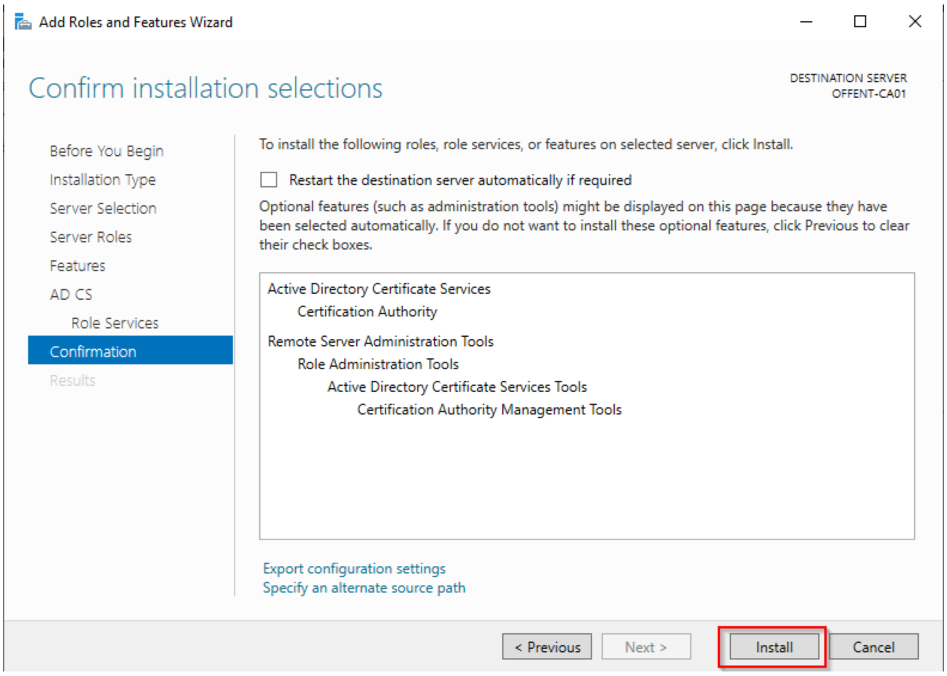
Role services

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

Description

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

15. Press “install” to add the Active Directory Certificate Services to the server.


Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
OFFENT-CA01

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

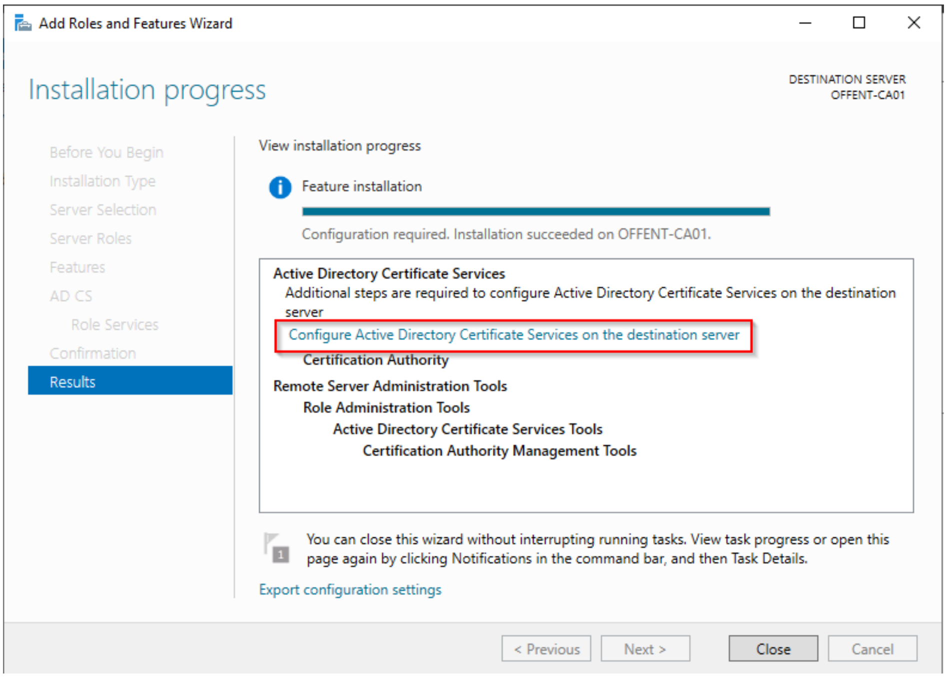
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Certificate Services
    Certification Authority

Remote Server Administration Tools
    Role Administration Tools
        Active Directory Certificate Services Tools
            Certification Authority Management Tools

Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

16. When the installation has completed, press the link “Configure Active Directory Certificate Services on the destination server”



Installation progress

DESTINATION SERVER
OFFENT-CA01

View installation progress

Feature installation

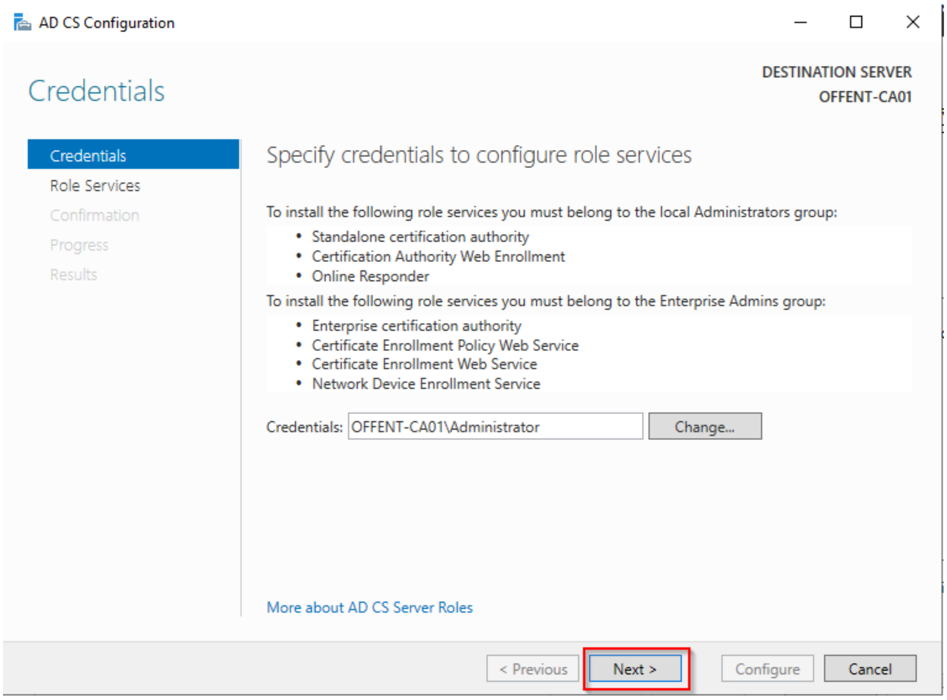
Configuration required. Installation succeeded on OFFENT-CA01.

Active Directory Certificate Services
Additional steps are required to configure Active Directory Certificate Services on the destination server
Configure Active Directory Certificate Services on the destination server
Certification Authority
Remote Server Administration Tools
Role Administration Tools
Active Directory Certificate Services Tools
Certification Authority Management Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

17. Use the default settings and press “Next”



Credentials

DESTINATION SERVER
OFFENT-CA01

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

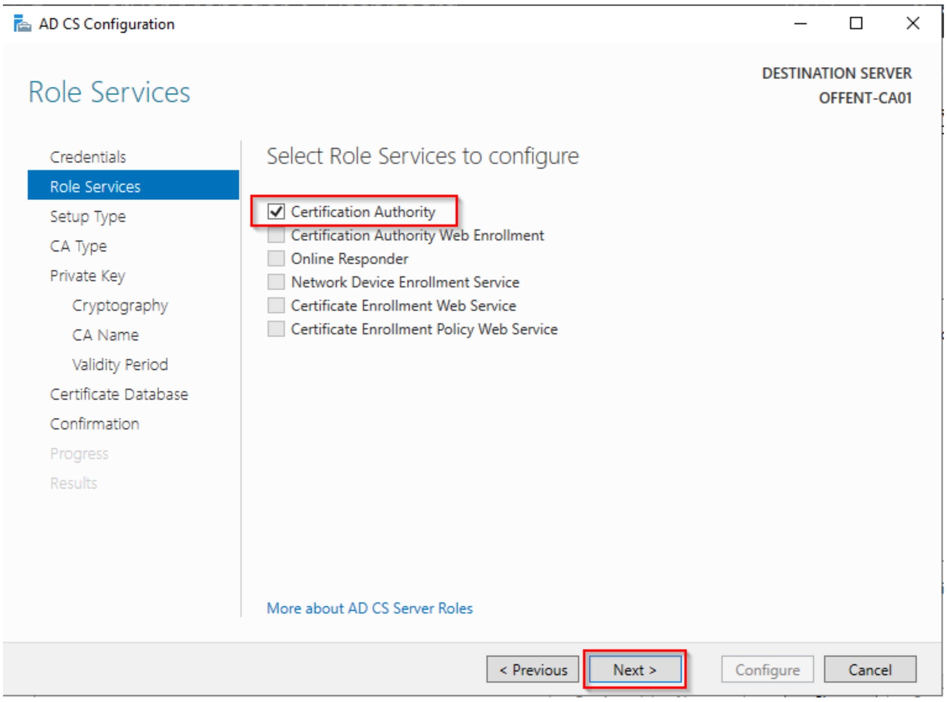
To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: OFFENT-CA01\Administrator

More about AD CS Server Roles

18. Select “Certification Authority” and press “Next”



AD CS Configuration

DESTINATION SERVER
OFFENT-CA01

Role Services

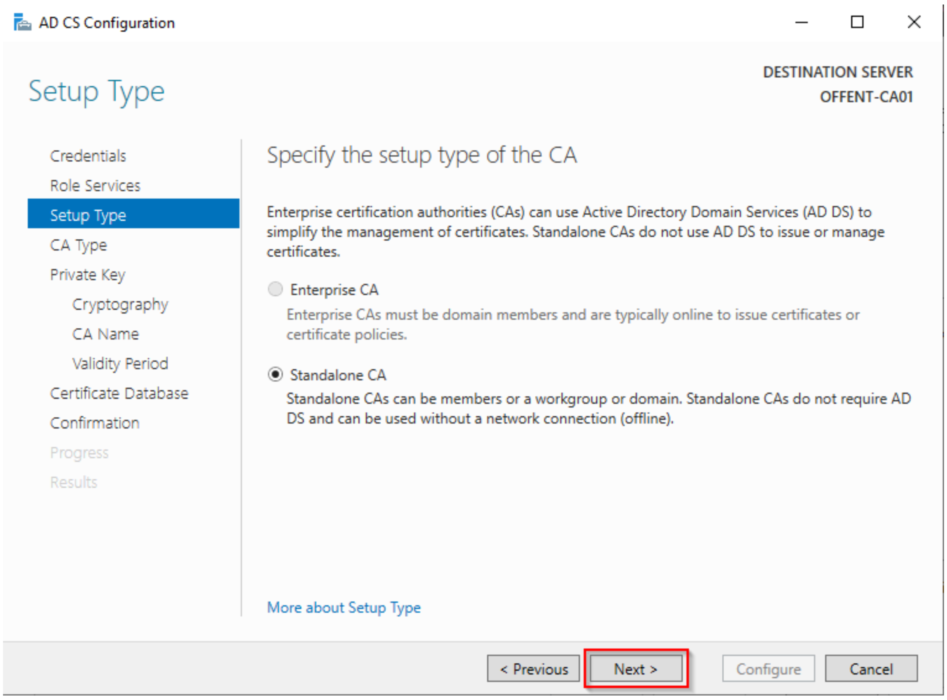
- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

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

More about AD CS Server Roles

19. Because this server is non-domain joined only Standalone CA can be selected. Press “Next” to continue.



AD CS Configuration

DESTINATION SERVER
OFFENT-CA01

Setup Type

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the setup type of the CA

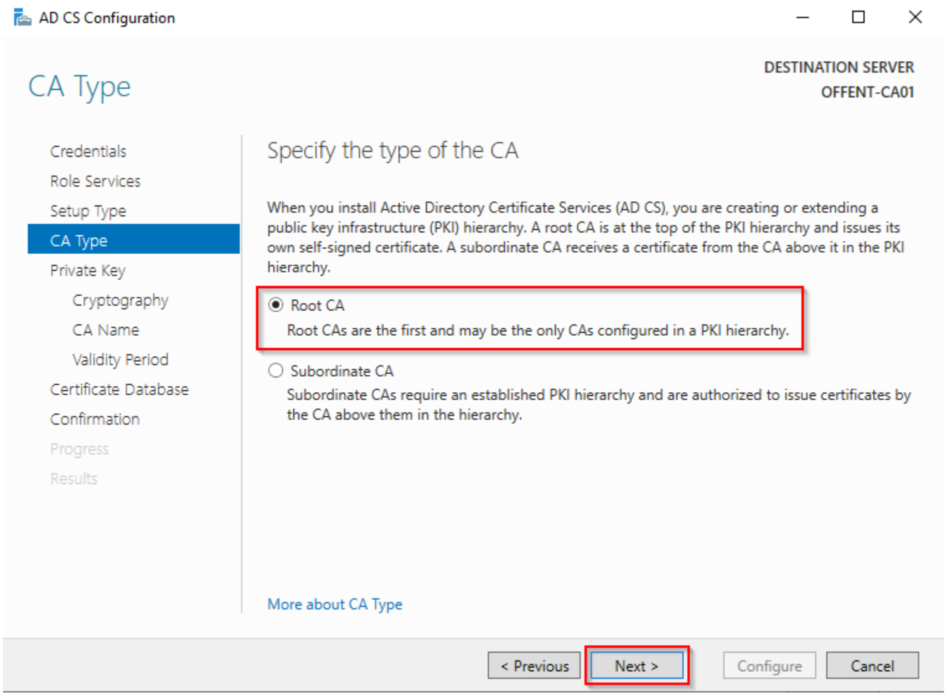
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

○ Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

● Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

More about Setup Type

20. As this server is the root of the PKI hierarchy select “Root CA” and press “Next”



AD CS Configuration

CA Type

DESTINATION SERVER
OFFENT-CA01

Specify the type of the CA

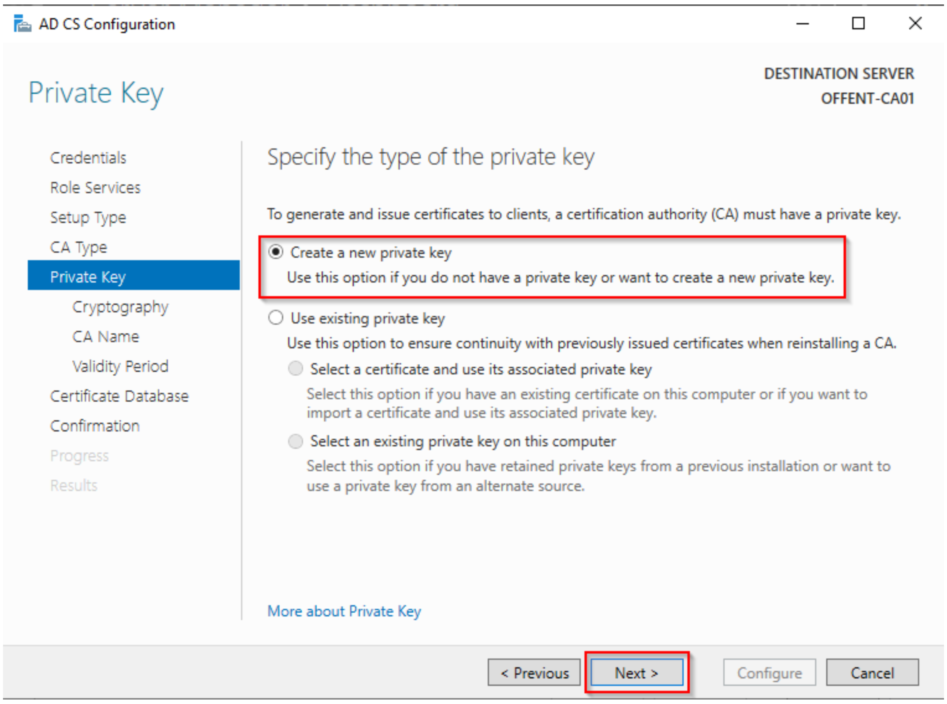
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

● Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

○ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

More about CA Type

21. Select “Create a new private key” and press “Next” to continue.



AD CS Configuration

Private Key

DESTINATION SERVER
OFFENT-CA01

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

● Create a new private key
Use this option if you do not have a private key or want to create a new private key.

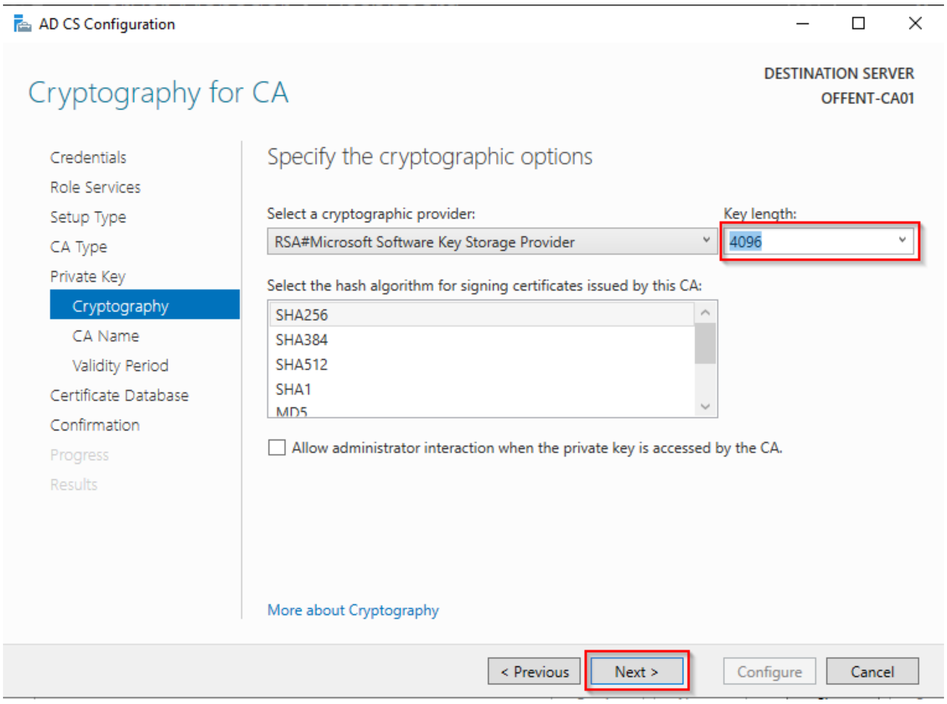
○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

○ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

More about Private Key

22. Because this is the Root CA Certificate I use a longer Key length of 4096. This will increase the security.


AD CS Configuration

Cryptography for CA

DESTINATION SERVER
OFFENT-CA01

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 4096

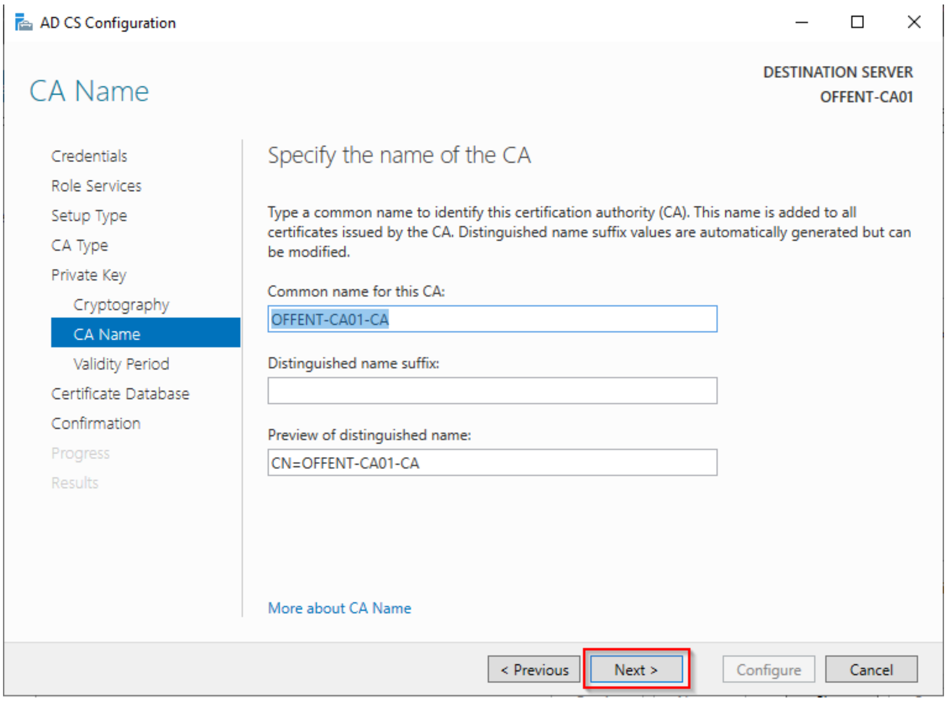
Select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512
- SHA1
- MD5

□ Allow administrator interaction when the private key is accessed by the CA.

More about Cryptography

23. Use the default settings and press “Next” to continue.


AD CS Configuration

CA Name

DESTINATION SERVER
OFFENT-CA01

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

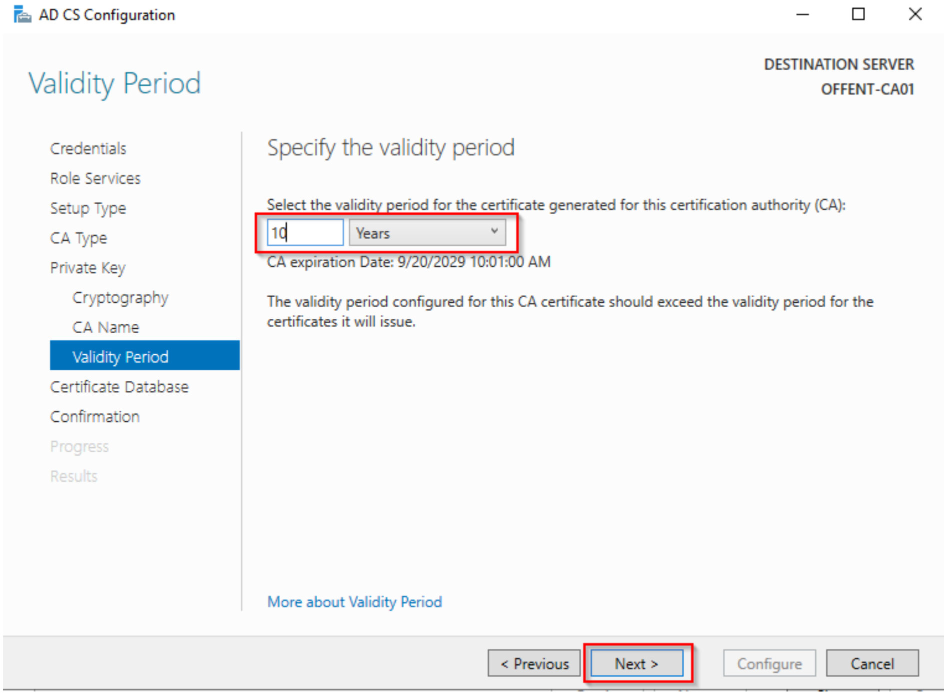
Common name for this CA: OFFENT-CA01-CA

Distinguished name suffix:

Preview of distinguished name: CN=OFFENT-CA01-CA

More about CA Name

24. Because this server will be used in a Test Environment I extend the validity period to 10 years. Press “Next” to continue.



Validity Period

Specify the validity period

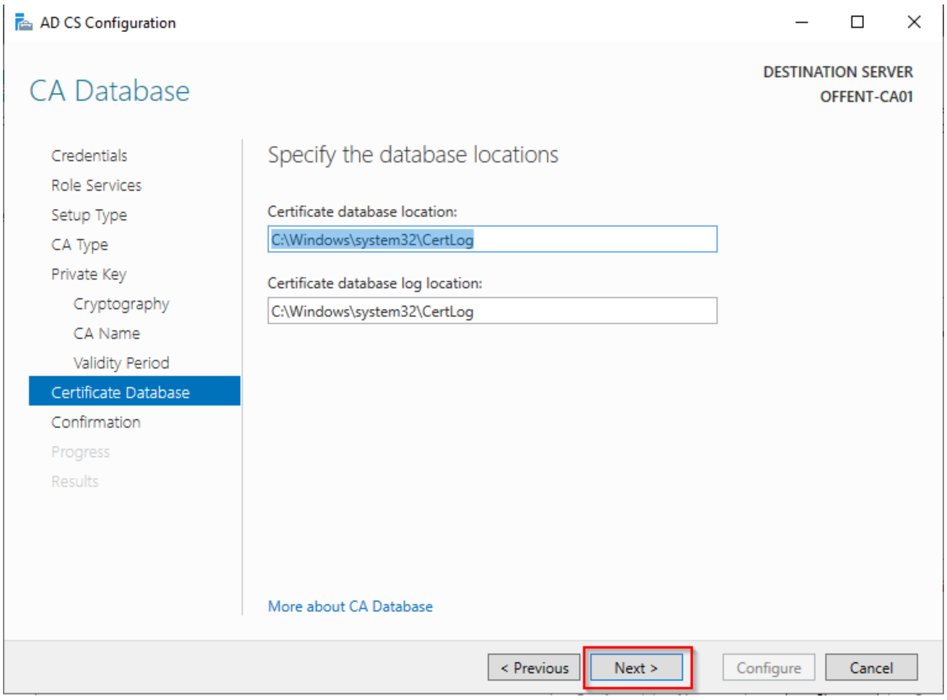
Select the validity period for the certificate generated for this certification authority (CA):

10 Years

CA expiration Date: 9/20/2029 10:01:00 AM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

25. Use the default settings and press “Next” to continue.



CA Database

Specify the database locations

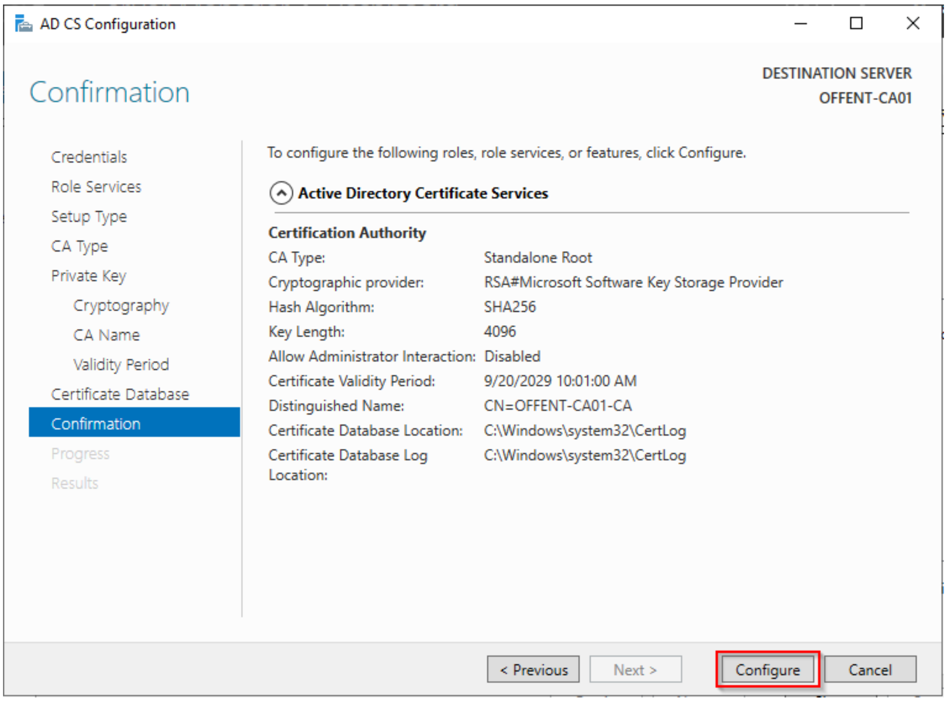
Certificate database location:

C:\Windows\system32\CertLog

Certificate database log location:

C:\Windows\system32\CertLog

26. Press “Configure” to configure the server.



Confirmation

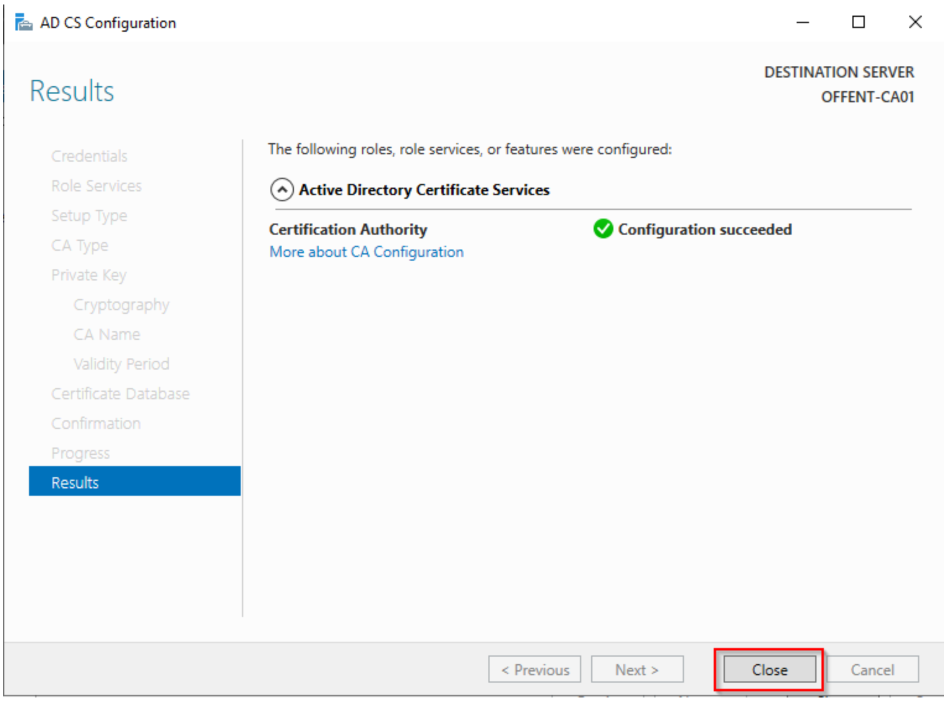
To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority

```
CA Type:                          Standalone Root
Cryptographic provider:           RSA#Microsoft Software Key Storage Provider
Hash Algorithm:                   SHA256
Key Length:                       4096
Allow Administrator Interaction:  Disabled
Certificate Validity Period:      9/20/2029 10:01:00 AM
Distinguished Name:               CN=OFFENT-CA01-CA
Certificate Database Location:    C:\Windows\system32\CertLog
Certificate Database Log          C:\Windows\system32\CertLog
Location:
```

27. Press “Close” to continue.



Results

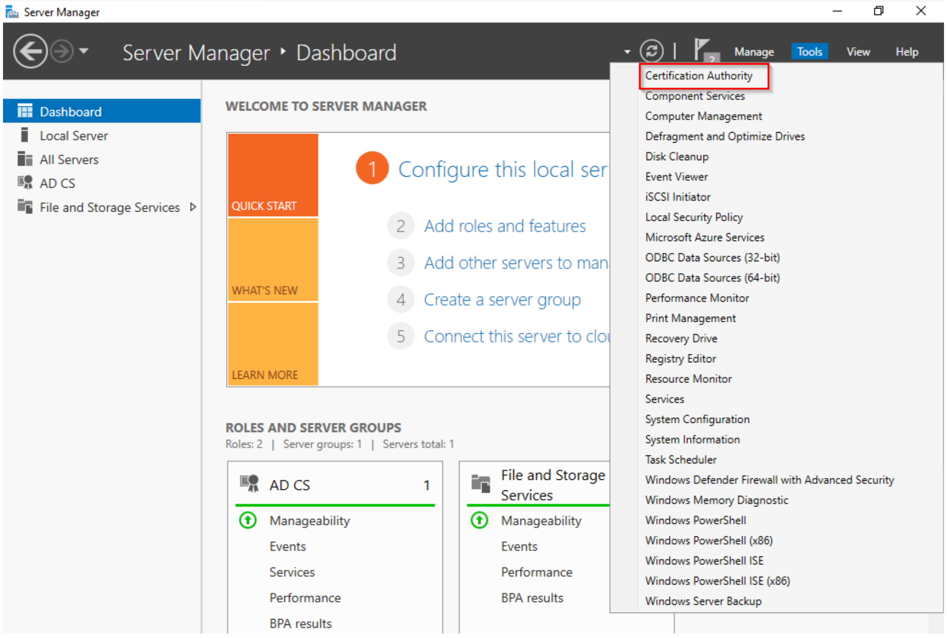
The following roles, role services, or features were configured:

Active Directory Certificate Services

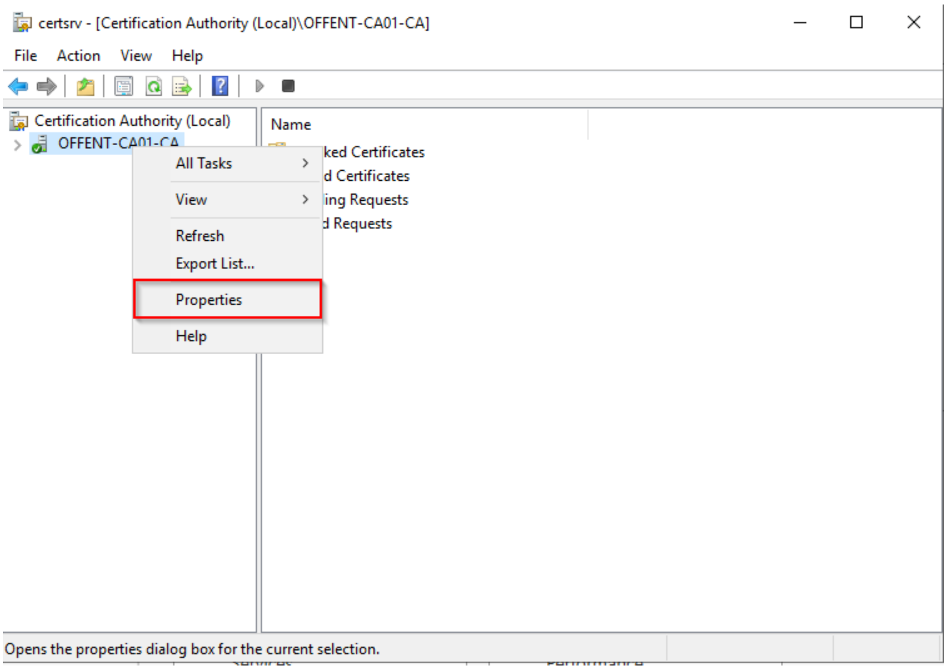
Certification Authority ✓ **Configuration succeeded**

More about CA Configuration

28. Press “Tools” in the Server Manager and select “Certification Authority”

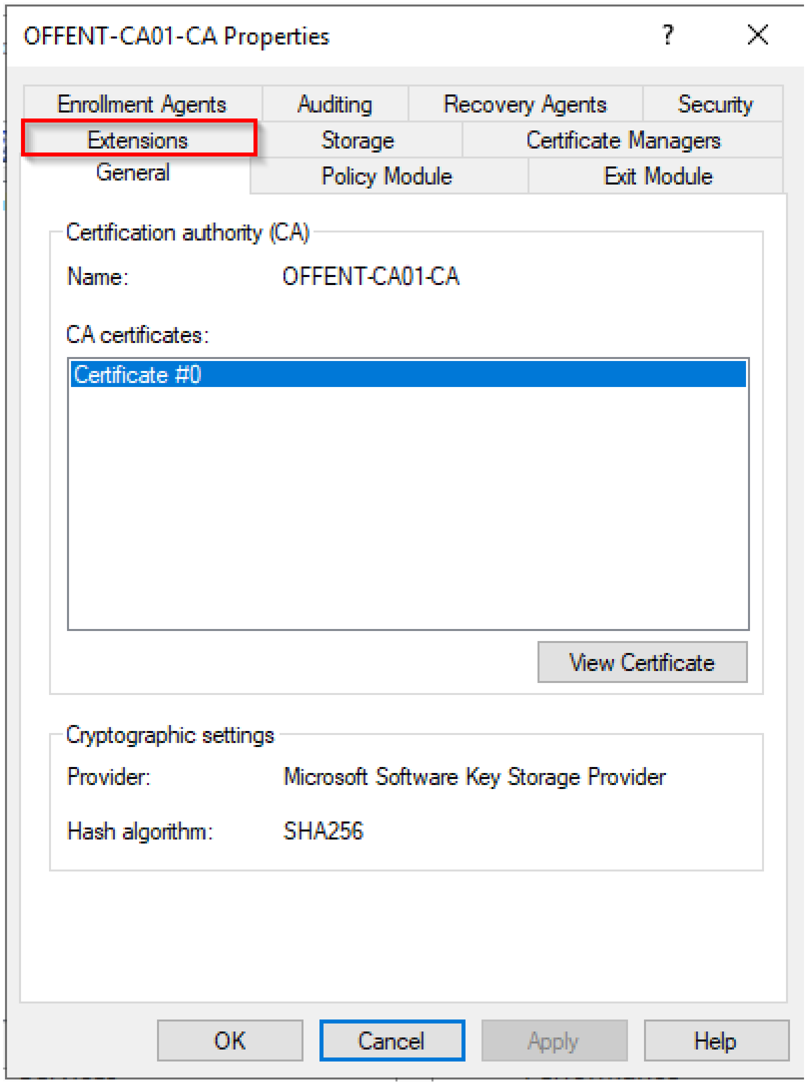


29. Right click the Servername and select “Properties”



Opens the properties dialog box for the current selection.

30. Select the “Extensions” tab



Certification authority (CA)

Name: OFFENT-CA01-CA

CA certificates:

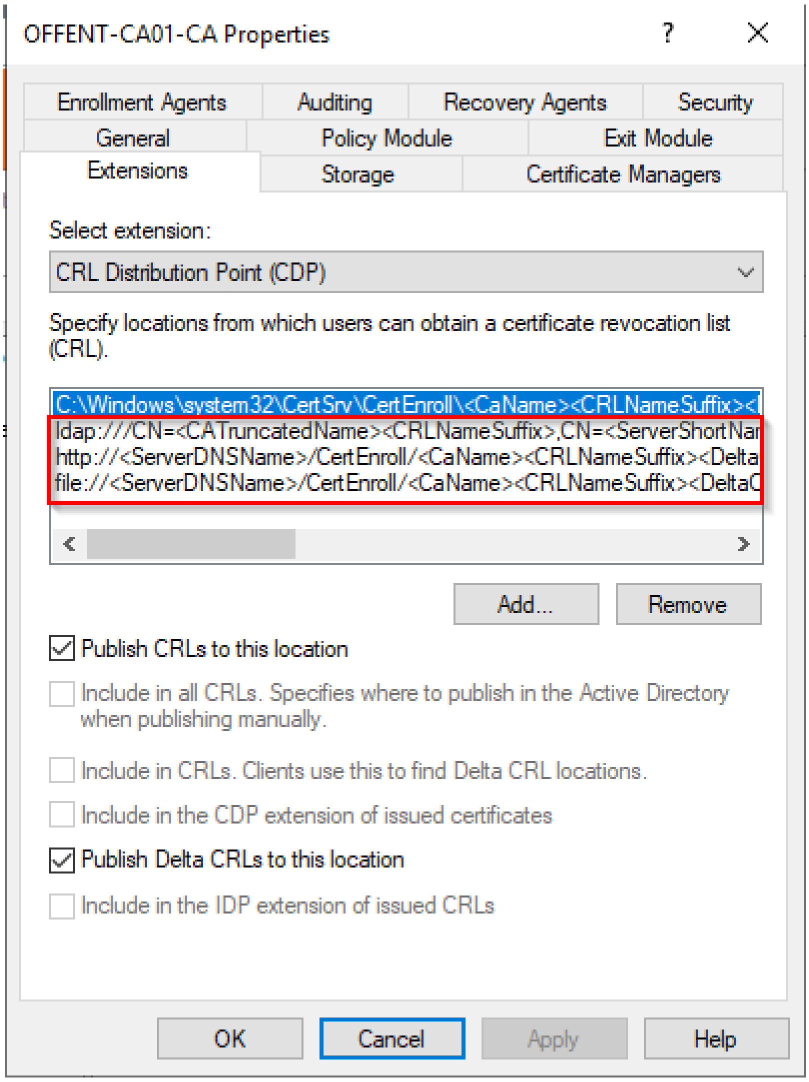
Certificate #0

Cryptographic settings

Provider: Microsoft Software Key Storage Provider

Hash algorithm: SHA256

31. In the “Extensions tab” select the extension “CRL Distribution Point (CDP) and remove all locations except the “C:\*” Location.



Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNar
http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Delta
file://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaC
```

☑ Publish CRLs to this location

□ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

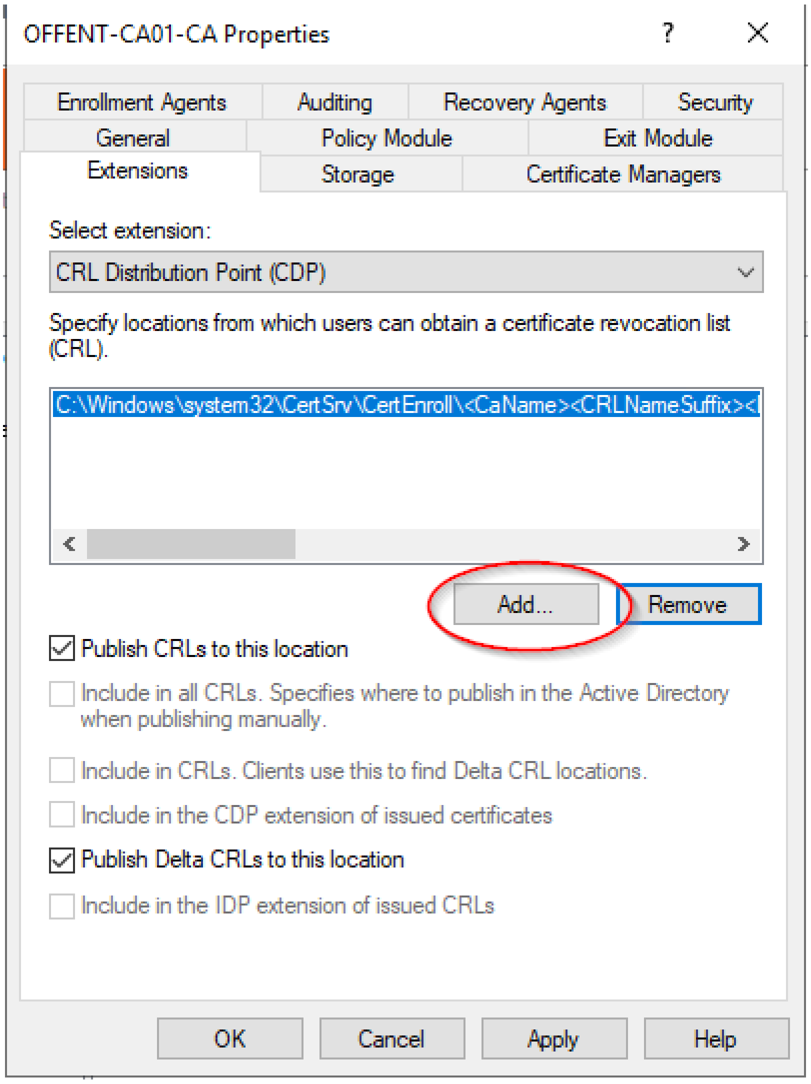
□ Include in CRLs. Clients use this to find Delta CRL locations.

□ Include in the CDP extension of issued certificates

☑ Publish Delta CRLs to this location

□ Include in the IDP extension of issued CRLs

32. Because this server will be offline it cannot be contacted, therefore a location needs to be added to the subordinate server. Press “Add” to add the CDP on the Subordinate Server.



Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><

☑ Publish CRLs to this location

☐ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

☐ Include in CRLs. Clients use this to find Delta CRL locations.

☐ Include in the CDP extension of issued certificates

☑ Publish Delta CRLs to this location

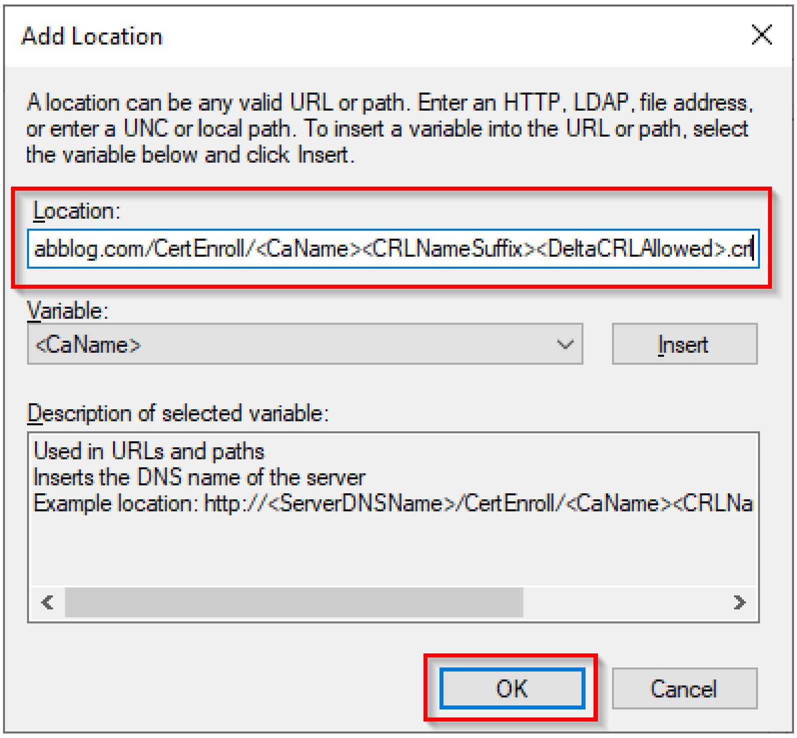
☐ Include in the IDP extension of issued CRLs

33. Enter the following location and press “OK”

`http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`

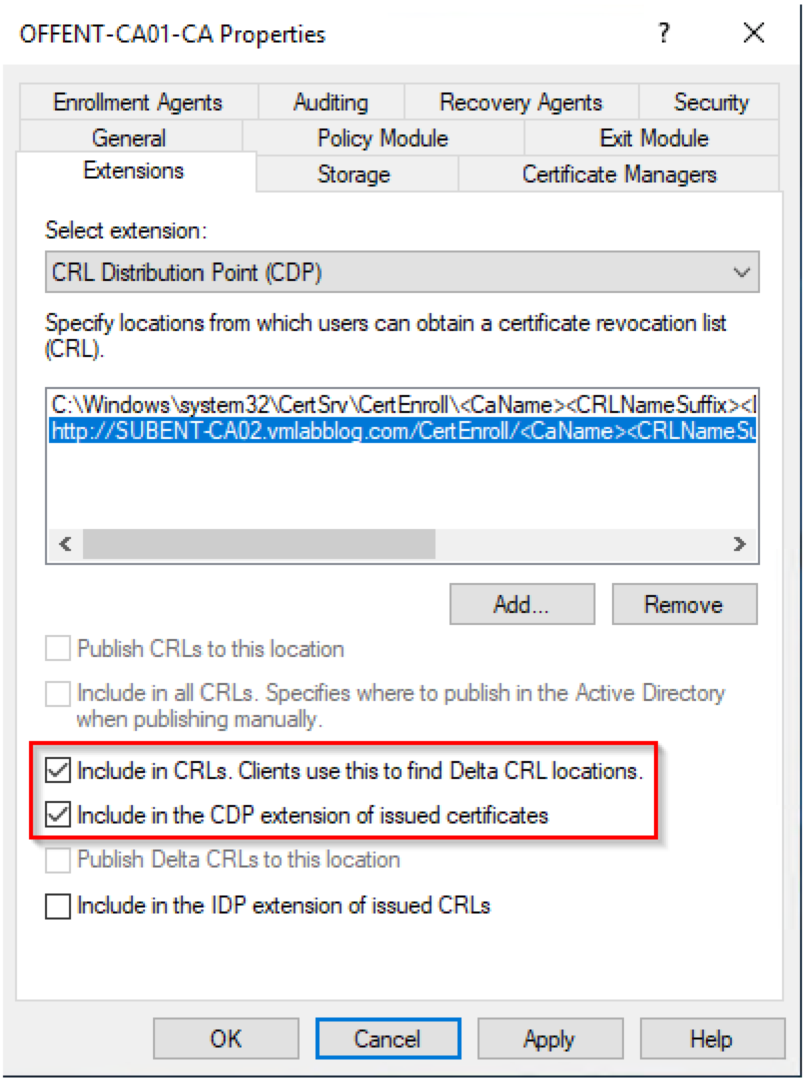
Replace <serverDNSName> with the dnsname of the Subordinateserver in this demo the location will be:

`http://SUBENT-CA02.vmlabblog.com/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`



Add Location
A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.
Location:
abblog.com/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
Variable:
<CaName>
Insert
Description of selected variable:
Used in URLs and paths
Inserts the DNS name of the server
Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNa
OK
Cancel

24. Check the boxes beginning with “Include in CRLs*” and “Include in the CDP*” and press “Apply”


OFFENT-CA01-CA Properties

Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><I
http://SUBENT-CA02.vmlabblog.com/CertEnroll/<CaName><CRLNameSu
```

□ Publish CRLs to this location

□ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

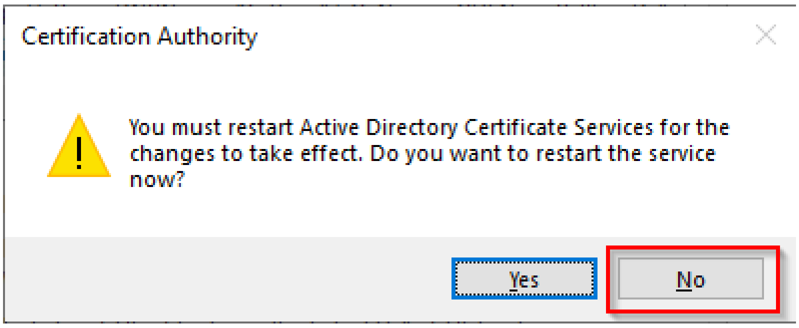
☑ Include in CRLs. Clients use this to find Delta CRL locations.

☑ Include in the CDP extension of issued certificates

□ Publish Delta CRLs to this location

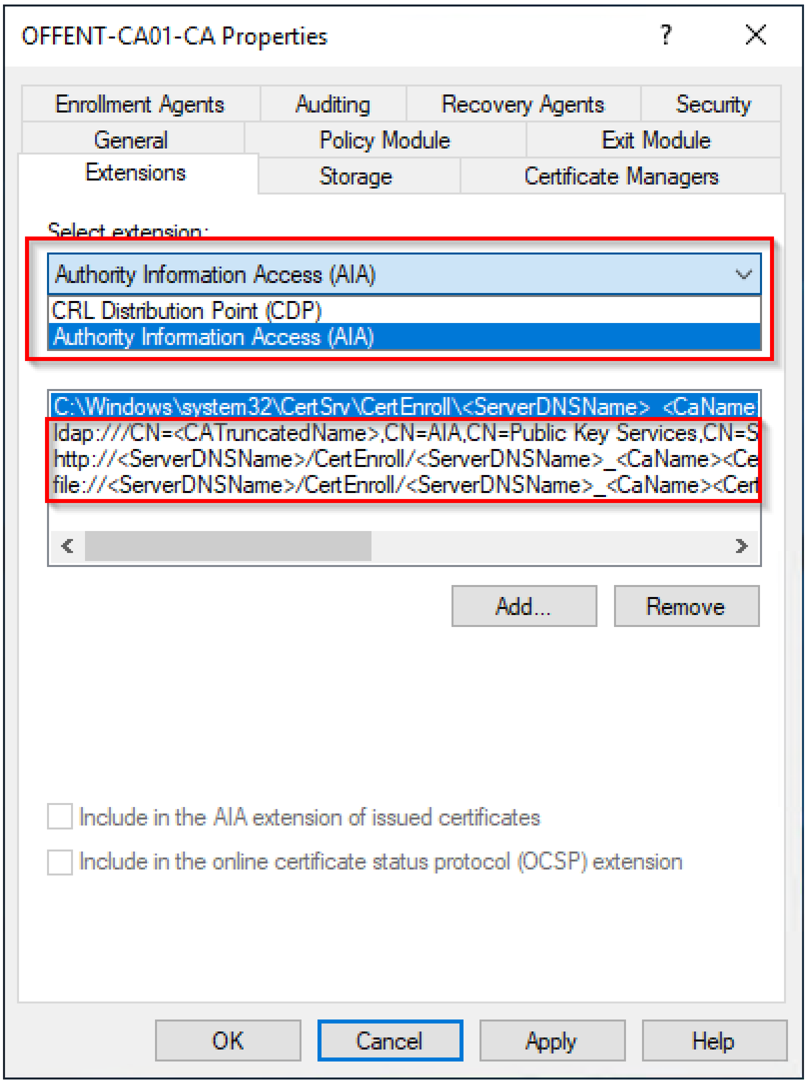
□ Include in the IDP extension of issued CRLs

35. Press “No” when asked to restart the service.


Certification Authority

You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now?

36. Select in “Select extension” the “Authority Information Access (AIA)” and remove all locations except the “C:\*” Location.



OFFENT-CA01-CA Properties

Select extension:

Authority Information Access (AIA)

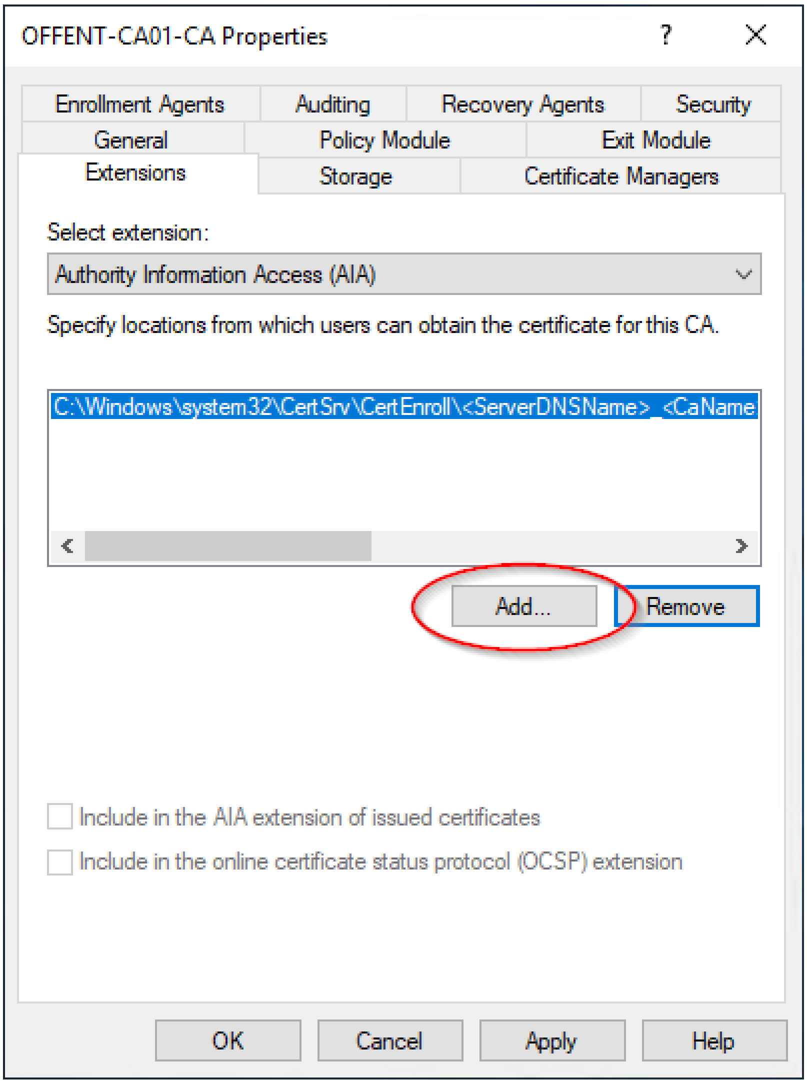
CRL Distribution Point (CDP)
Authority Information Access (AIA)

```
C:\Windows\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaName
ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=S
http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><Ce
file://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><Cert
```

□ Include in the AIA extension of issued certificates

□ Include in the online certificate status protocol (OCSP) extension

37. Press “Add” to add the AIA location on the Subordinate Server.



Select extension: Authority Information Access (AIA)

Specify locations from which users can obtain the certificate for this CA.

C:\Windows\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaName

□ Include in the AIA extension of issued certificates

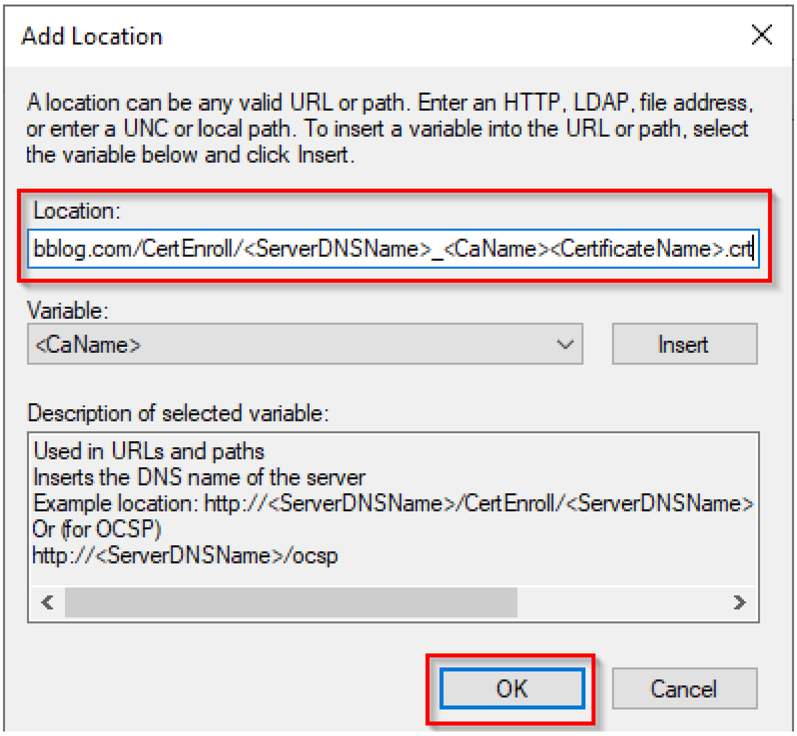
□ Include in the online certificate status protocol (OCSP) extension

38. Enter the following location and press “OK”

```
http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
```

Replace <serverDNSName> with the dnsname of the Subordinateserver in this demo the location will be:

```
http://SUBENT-CA02.vmlabblog.com/CertEnroll/<ServerDNSName>_<CaName>
<CertificateName>.crt
```



Add Location

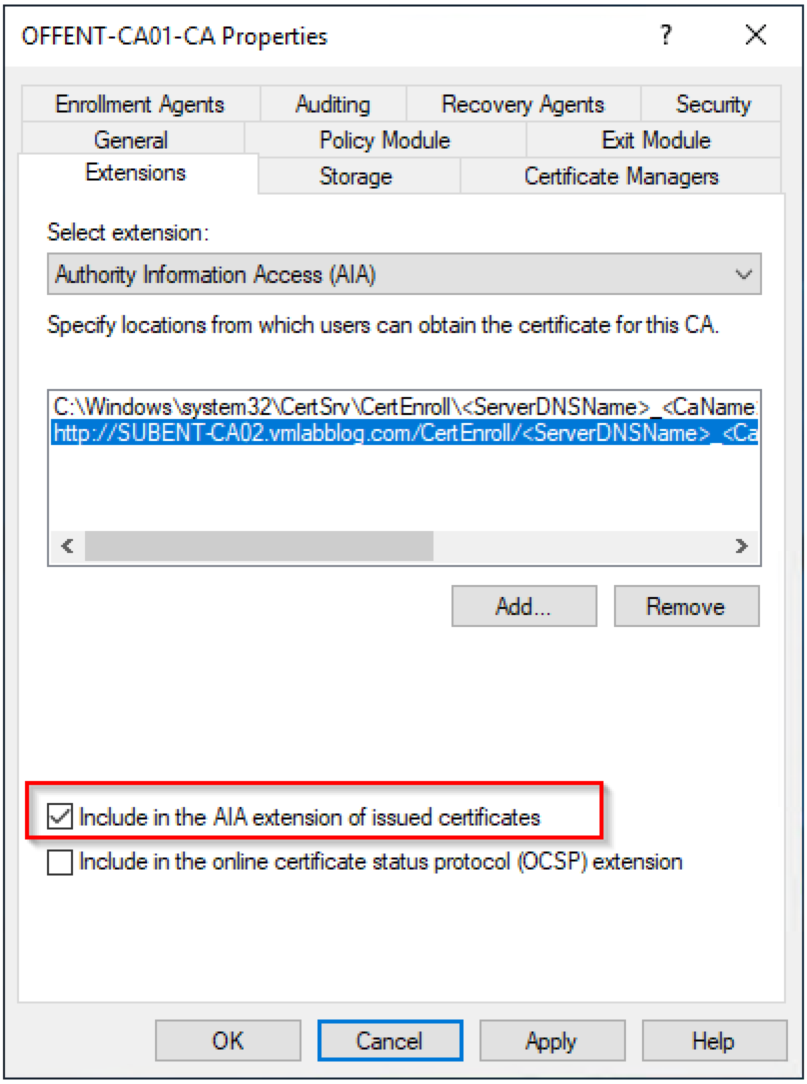
A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:
bblog.com/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt

Variable:
<CaName>

Description of selected variable:
Used in URLs and paths
Inserts the DNS name of the server
Example location: http://<ServerDNSName>/CertEnroll/<ServerDNSName>
Or (for OCSP)
http://<ServerDNSName>/ocsp

39. Check the box “Include in the AIA extension of issued certificates” and press “Apply”



OFFENT-CA01-CA Properties

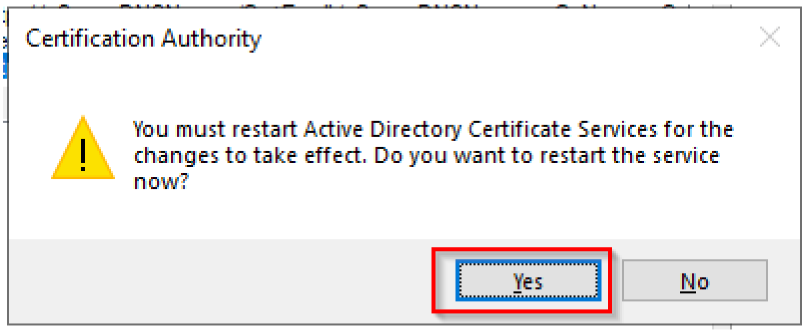
Select extension:
Authority Information Access (AIA)

Specify locations from which users can obtain the certificate for this CA.

C:\Windows\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaName
http://SUBENT-CA02.vmlabblog.com/CertEnroll/<ServerDNSName>_<Ca

☑ Include in the AIA extension of issued certificates
□ Include in the online certificate status protocol (OCSP) extension

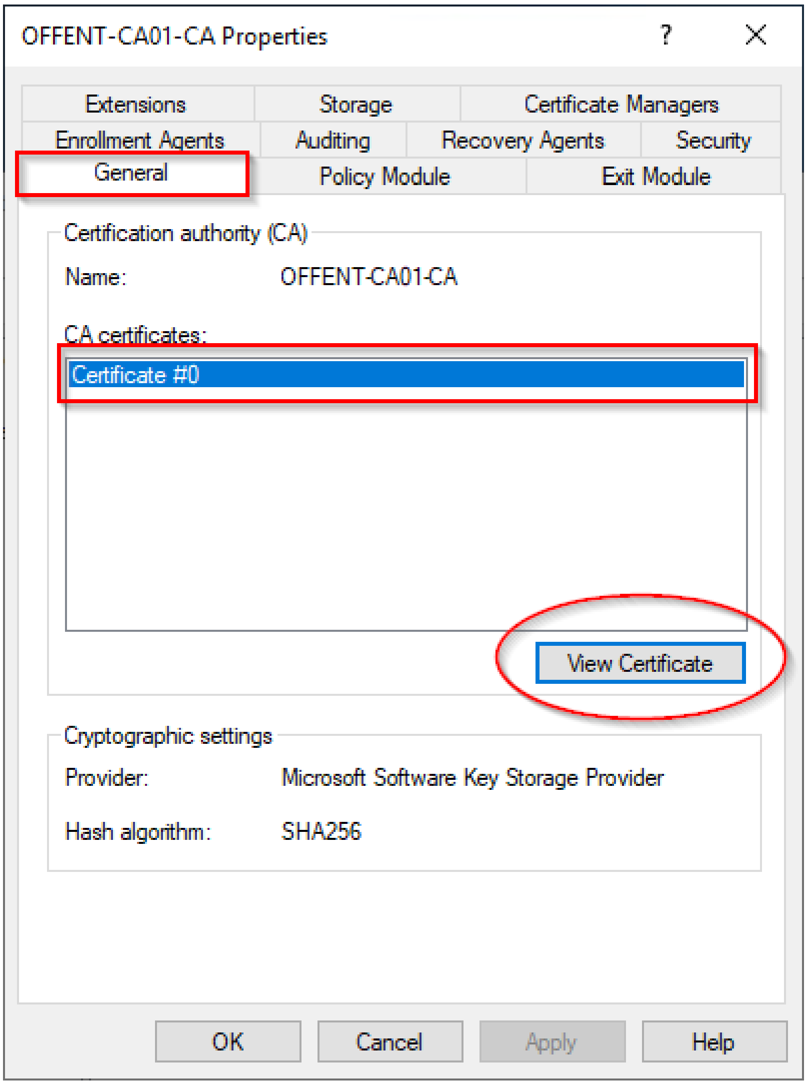
40. Press “Yes” when asked to restart the service.



Certification Authority

You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now?

41. Select the “General” and select the Root Certificate and press “View Certificate”.



OFFENT-CA01-CA Properties

Certification authority (CA)

Name: OFFENT-CA01-CA

CA certificates:

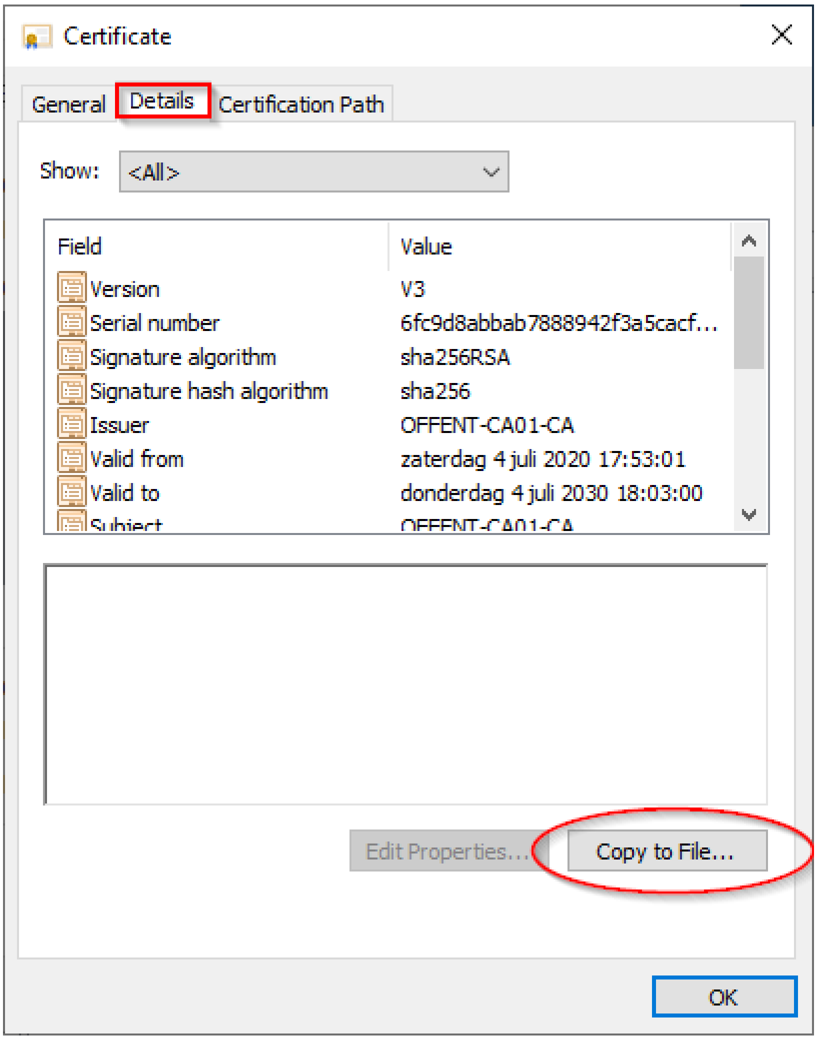
Certificate #0

Cryptographic settings

Provider: Microsoft Software Key Storage Provider

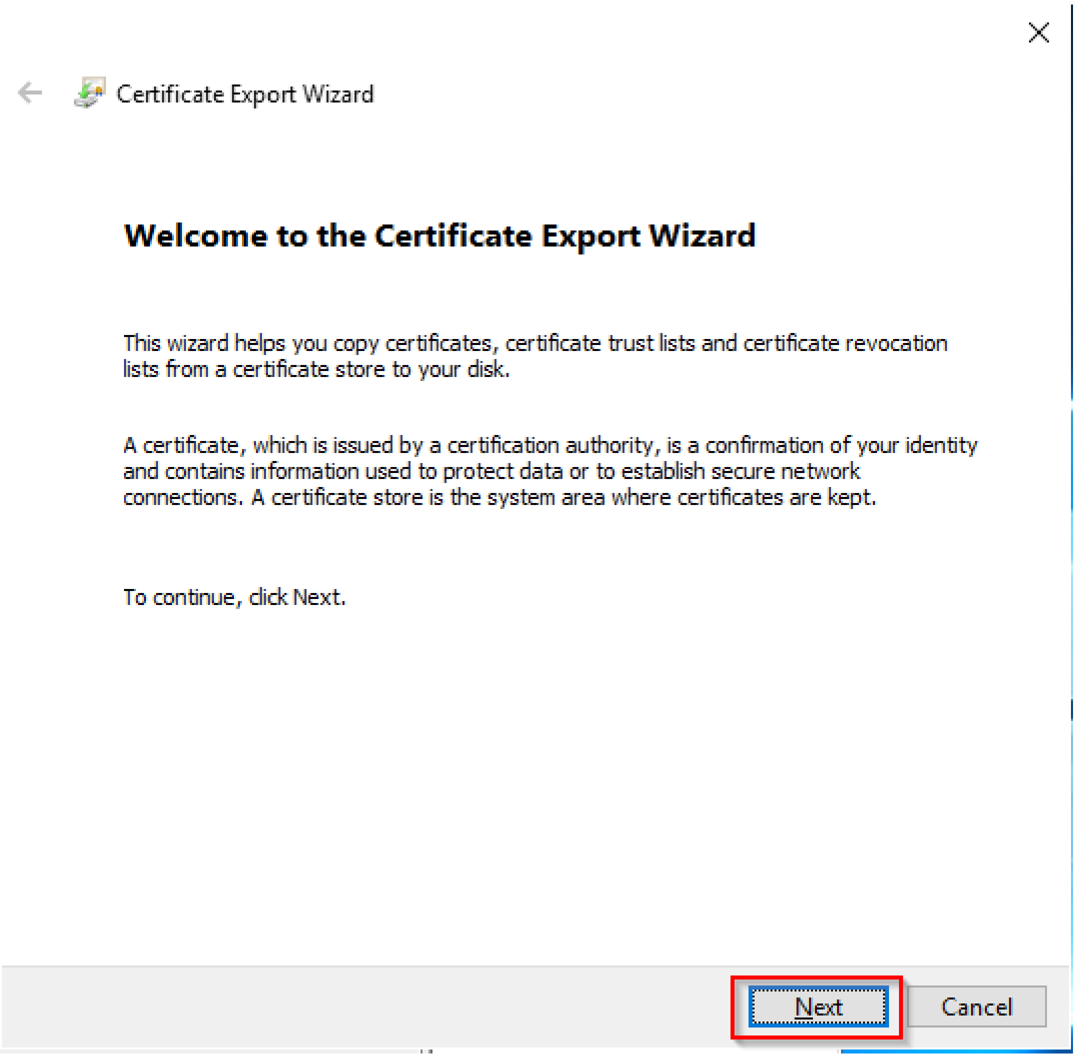
Hash algorithm: SHA256

42. Select the tab “Details” and press “Copy to File…”.



Field	Value
Version	V3
Serial number	6fc9d8abbab7888942f3a5cacf...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	OFFENT-CA01-CA
Valid from	zaterdag 4 juli 2020 17:53:01
Valid to	donderdag 4 juli 2030 18:03:00
Subject	OFFENT-CA01-CA

43. In the Certificate Export Wizard press “Next”.



Certificate Export Wizard

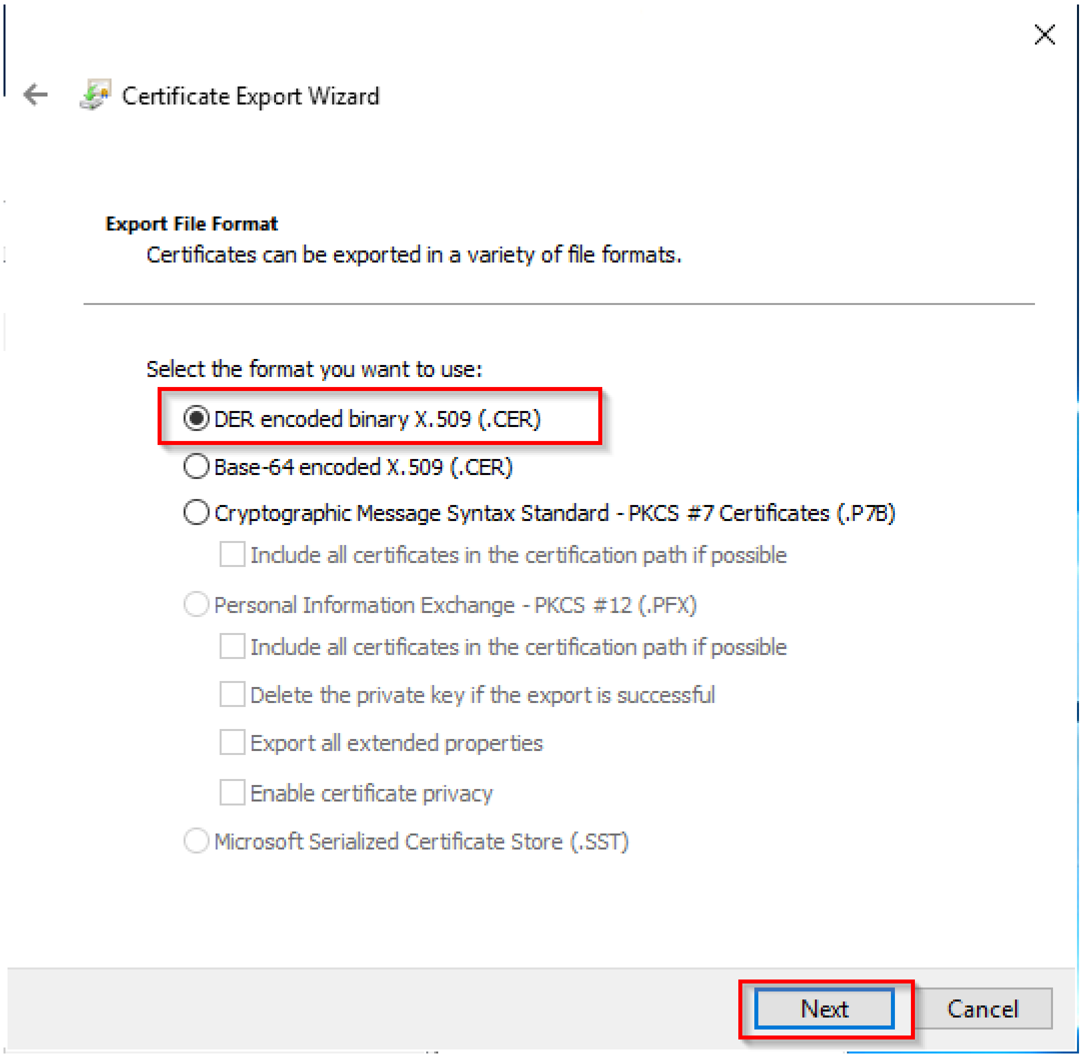
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

44. Select “DER encoded binary X.509 (.CER)” and press “Next”.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

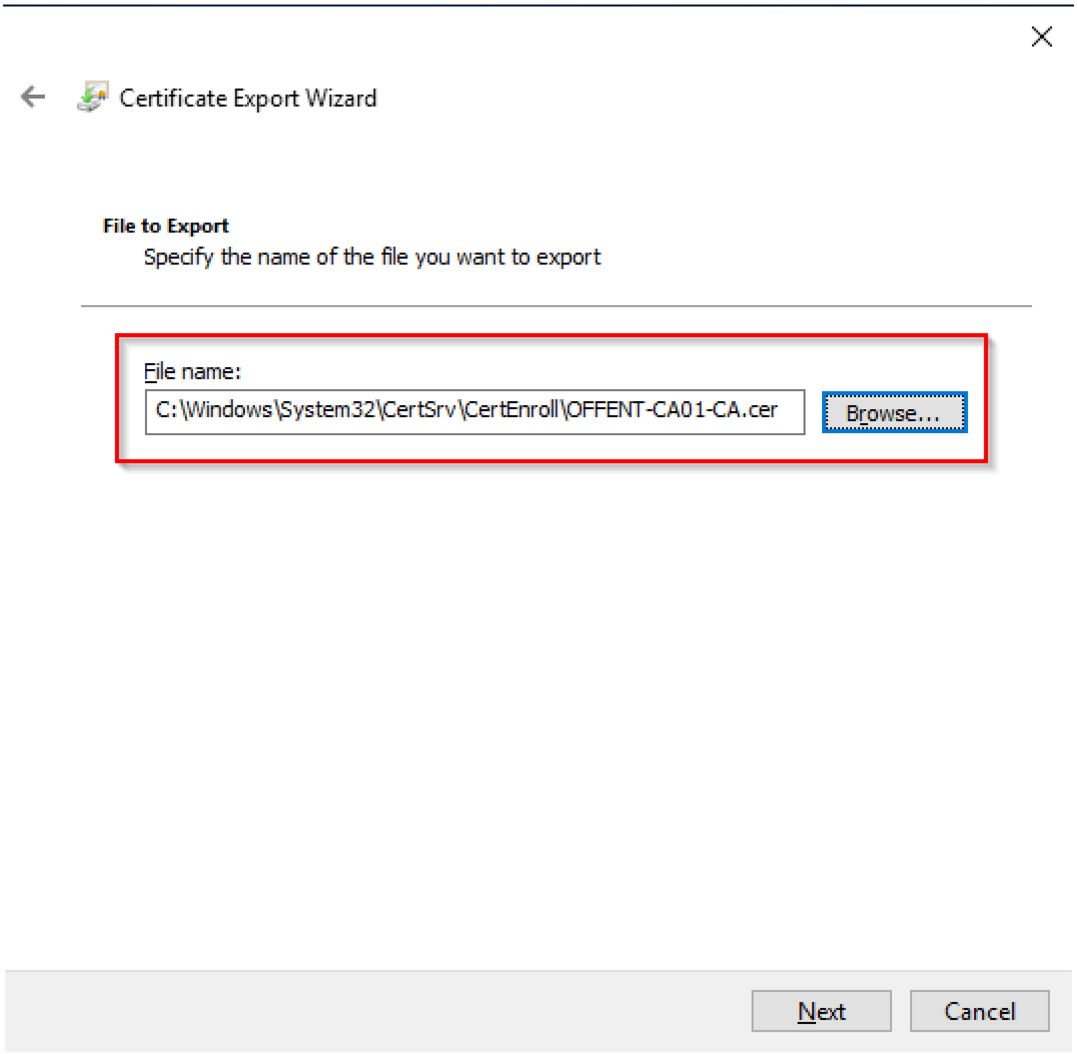
□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

45. In File name enter “C:\Windows\System32\CertSrv\CertEnroll\<CA-NAME>-CA.cer” and press “Next”.



Certificate Export Wizard

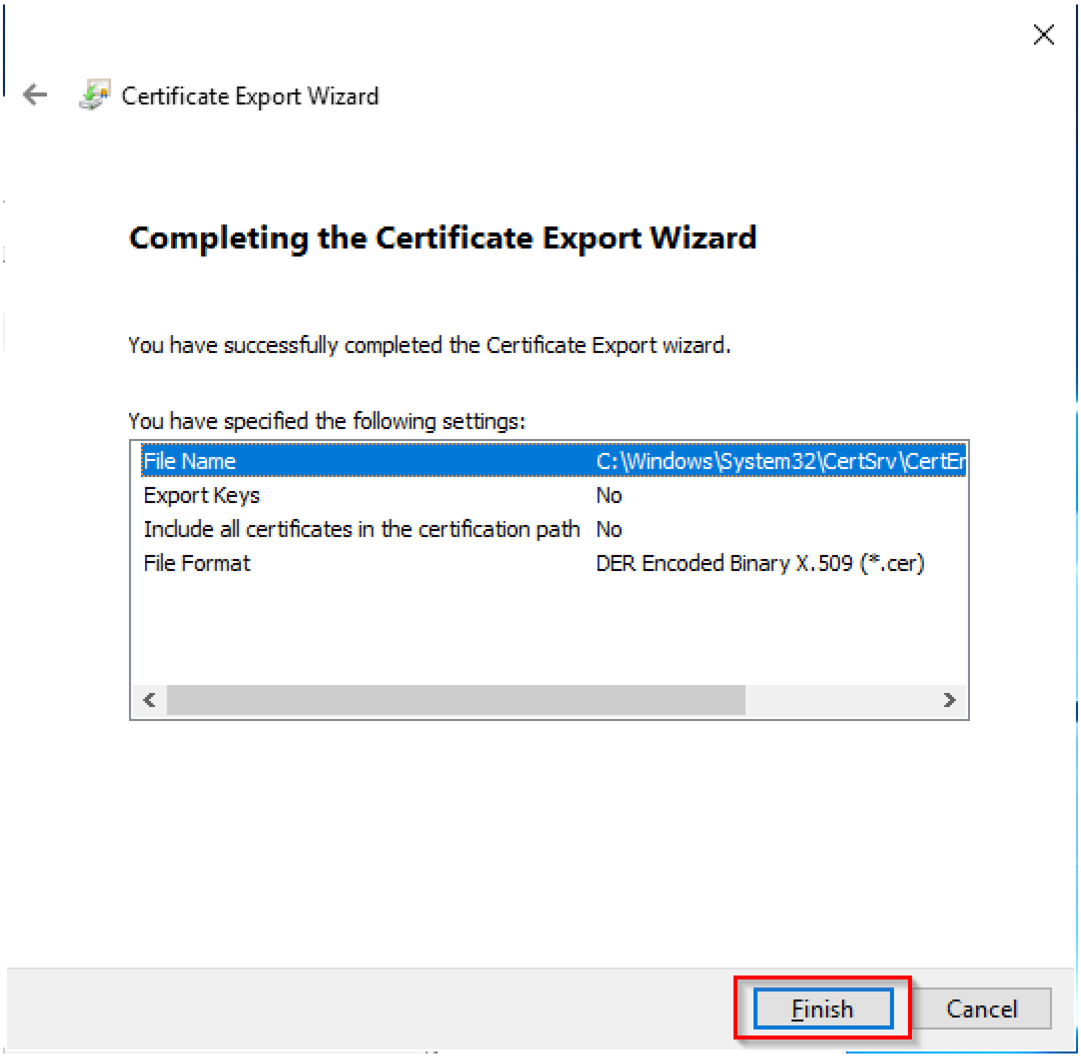
File to Export

Specify the name of the file you want to export

File name:

C:\Windows\System32\CertSrv\CertEnroll\OFFENT-CA01-CA.cer

46. Press “Finish” to export the RootCA Certificate.



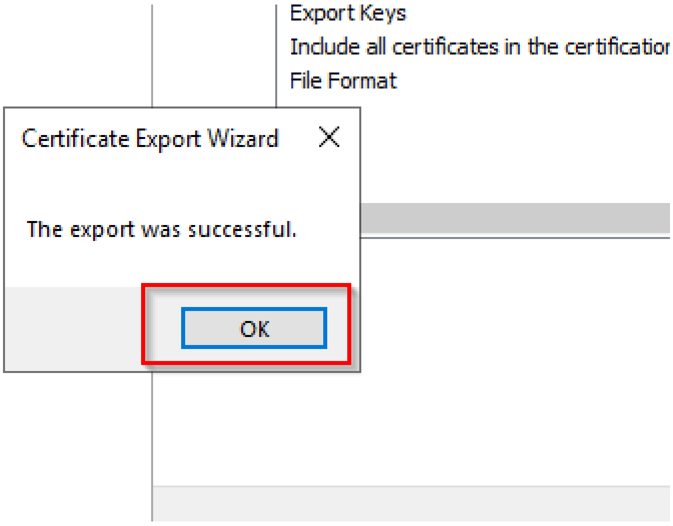
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Windows\System32\CertSrv\CertEr
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Encoded Binary X.509 (*.cer)

47. A popup will appear when the export was successful, press “OK” to continue.



Certificate Export Wizard

The export was successful.

The setup of the Offline RootCA is now completed.

Next: Subordinate CA Server