

# Certificate Authority Infrastructure Hands-On Lab

## Part 1: ADCS Installation & Configuration

*Information Technology & Security*

### CLASS DESCRIPTION

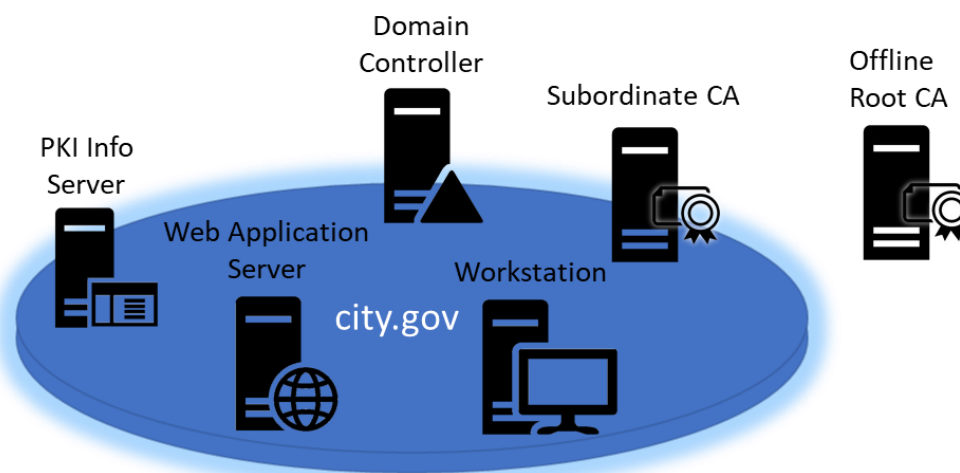
The first of a two-part hands-on-lab series; this lab will take you step-by-step through the installation and configuration of an enterprise Public Key Infrastructure (PKI) using Microsoft Active Directory Certificate Services (ADCS).

### OVERVIEW

We will be deploying the PKI environment described below in *Figure 1* and *Table 1*. The installation procedure will follow these major steps:

- Provision a web server to host PKI information (CDP and AIA).
- Deploy a standalone root CA
- Deploy an enterprise subordinate CA

**NOTE:** All domain and local account passwords are set to **pw**



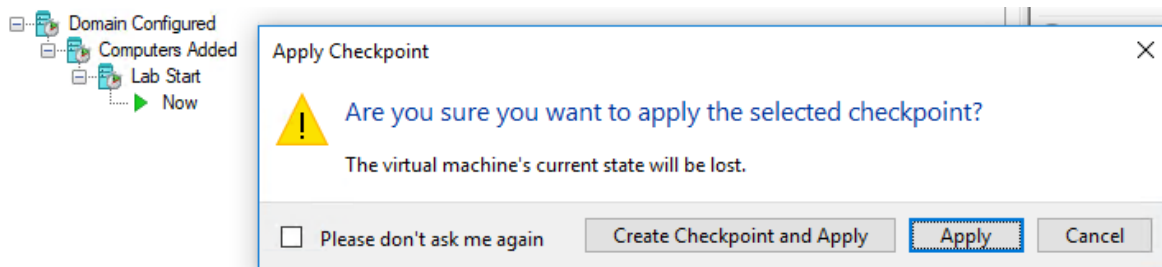
*Figure 1 - Lab Infrastructure*

Machine	Roles	FQDN [IP]
Domain Controller	DC, DNS, DHCP, WINS	dc.city.gov [10.10.10.10]
Root CA	Certificate Authority	rootca.city.gov [10.10.10.5]
Subordinate CA	Certificate Authority, Web Enrollment	subca.city.gov [DHCP]
PKI Info Server	IIS, File Share	pkiinfo.city.gov [DHCP]
Web Application Server	IIS	webapps.city.gov [DHCP]
Workstation	Windows Client OS	workstation.city.gov [DHCP]

*Table 1 - Listing of Lab Machines*

## ADCS INSTALLATION AND CONFIGURATION HANDS-ON-LAB

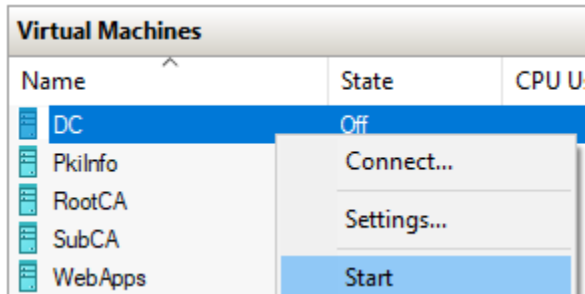
**TIP:** Before starting any VM in this lab for the first time, you should apply the **Lab Start** checkpoint





## Provisioning the PKI Information Distribution Server

1. Start the Domain Controller (**DC**) if it isn't already running, wait for it to



2. Start the PKI Information server (**PkiInfo**)
3. Start a Hyper-V Virtual Machine Connection to **PkiInfo** and login as domain administrator

---

**NOTE:** Domain administrator credentials are *user name:* **CITY\Administartor** *password:* **pw**

---

**TIP:** When logged in as the domain administrator you should see the following information in the top right of the desktop wallpaper:

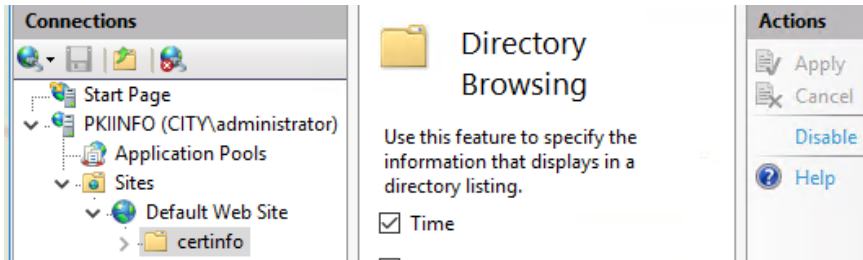
<b>Host Name:</b>	<b>PKIINFO</b>
<b>Machine Domain:</b>	<b>CITY</b>
<b>IP Address:</b>	<b>10.10.10.12</b>

---

If the information shown is different you may have logged in as local administrator, log out and try again.

---

4. Start Internet Information Services Manager (**IIS Manager**) and verify that the **certinfo** directory is exists under the **Default Web Site** and directory browsing is enabled



5. Start Internet Explorer and verify that you can browse to **http://pkiinfo.city.gov/certinfo**



## Deploying the Root Certificate Authority – Installation



1. Start the Root CA server (**RootCA**) and login as local Administrator

---

**NOTE:** A DNS entry for rootca.city.gov [10.10.10.5] has already been manually created for this server since it is **not** a domain member and hence will **not** self-register with the domain DNS.

---

2. Start Server Manager and select **Add roles and features**, under the *Configure this local server* section

### 1 Configure this local server

- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

3. On the **Select installation type** screen, select Role-based or feature-based installation and click next

DESTINATION SERVER  
RootCA

### Select installation type

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

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.

- On the **Select destination server** screen ensure the **RootCA** server is selected and click next

Select destination server

DESTINATION SERVER  
RootCA

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
RootCA	10.10.10.5	Microsoft Windows Server 2016 Datacenter

- On the **Select server roles** screen, select **Activity Directory Certificate Services** then click Add Features in the dialog window. Click Next.

Select server roles

DESTINATION SERVER  
RootCA

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

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

Roles	Description
<input checked="" type="checkbox"/> Active Directory Certificate Services	Active Directory Certificate Services (AD CS) is used to create...
<input type="checkbox"/> Active Directory Federation Services	Active Directory Federation Services (AD FS) is used to create...
<input type="checkbox"/> Active Directory Lightweight Directory Services	Active Directory Lightweight Directory Services (AD LDS) is used to create...
<input type="checkbox"/> Active Directory Rights Management Services	Active Directory Rights Management Services (AD RMS) is used to create...
<input type="checkbox"/> Active Directory Web Services	Active Directory Web Services (AD WS) is used to create...
<input type="checkbox"/> Active Directory Certificate Services (AD CS) Tools	Active Directory Certificate Services (AD CS) Tools
<input type="checkbox"/> Active Directory Federation Services (AD FS) Tools	Active Directory Federation Services (AD FS) Tools
<input type="checkbox"/> Active Directory Lightweight Directory Services (AD LDS) Tools	Active Directory Lightweight Directory Services (AD LDS) Tools
<input type="checkbox"/> Active Directory Rights Management Services (AD RMS) Tools	Active Directory Rights Management Services (AD RMS) Tools
<input type="checkbox"/> Active Directory Web Services (AD WS) Tools	Active Directory Web Services (AD WS) Tools
<input type="checkbox"/> Active Directory Certificate Services (AD CS) Tools (related to issue...)	Active Directory Certificate Services (AD CS) Tools (related to issue...)
<input type="checkbox"/> Active Directory Federation Services (AD FS) Tools (related in a...)	Active Directory Federation Services (AD FS) Tools (related in a...)
<input type="checkbox"/> Active Directory Lightweight Directory Services (AD LDS) Tools	Active Directory Lightweight Directory Services (AD LDS) Tools
<input type="checkbox"/> Active Directory Rights Management Services (AD RMS) Tools	Active Directory Rights Management Services (AD RMS) Tools
<input type="checkbox"/> Active Directory Web Services (AD WS) Tools	Active Directory Web Services (AD WS) Tools
<input type="checkbox"/> Device Management	Device Management
<input type="checkbox"/> DHCP Server	DHCP Server
<input type="checkbox"/> DNS Server	DNS Server
<input type="checkbox"/> Fax Server	Fax Server
<input type="checkbox"/> File and Storage Services	File and Storage Services
<input type="checkbox"/> Host Group	Host Group
<input type="checkbox"/> Hyper-V	Hyper-V
<input type="checkbox"/> MultiPoint Network Server	MultiPoint Network Server
<input type="checkbox"/> Network	Network
<input type="checkbox"/> Network	Network
<input type="checkbox"/> Print and Document Services	Print and Document Services
<input type="checkbox"/> RemoteApp and Desktop Connections	RemoteApp and Desktop Connections
<input type="checkbox"/> RemoteApp and Desktop Connections	RemoteApp and Desktop Connections
<input type="checkbox"/> Volume Shadow Copy Service	Volume Shadow Copy Service
<input type="checkbox"/> Web Services	Web Services

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)

Add Features Cancel

- Skip to the **Roles Services** screen under AD CS and verify that only the **Certificate Authority** role service is selected. Click Next

### Select role services

DESTINATION SERVER  
RootCA

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
AD CS  
**Role Services**

Select the role services to install for Active Directory Certificate Services

Role services	Description
<input checked="" type="checkbox"/> <b>Certification Authority</b>	Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.
<input type="checkbox"/> Certificate Enrollment Policy Web Service	
<input type="checkbox"/> Certificate Enrollment Web Service	
<input type="checkbox"/> Certification Authority Web Enrollment	
<input type="checkbox"/> Network Device Enrollment Service	
<input type="checkbox"/> Online Responder	

- On the **Confirm installation selections** screen, check the box to allow automatic restarts during installation and click Yes in the dialog box and finally click Install

### Confirm installation selections

DESTINATION SERVER  
RootCA

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
AD CS  
Role Services  
**Confirmation**  
Results

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

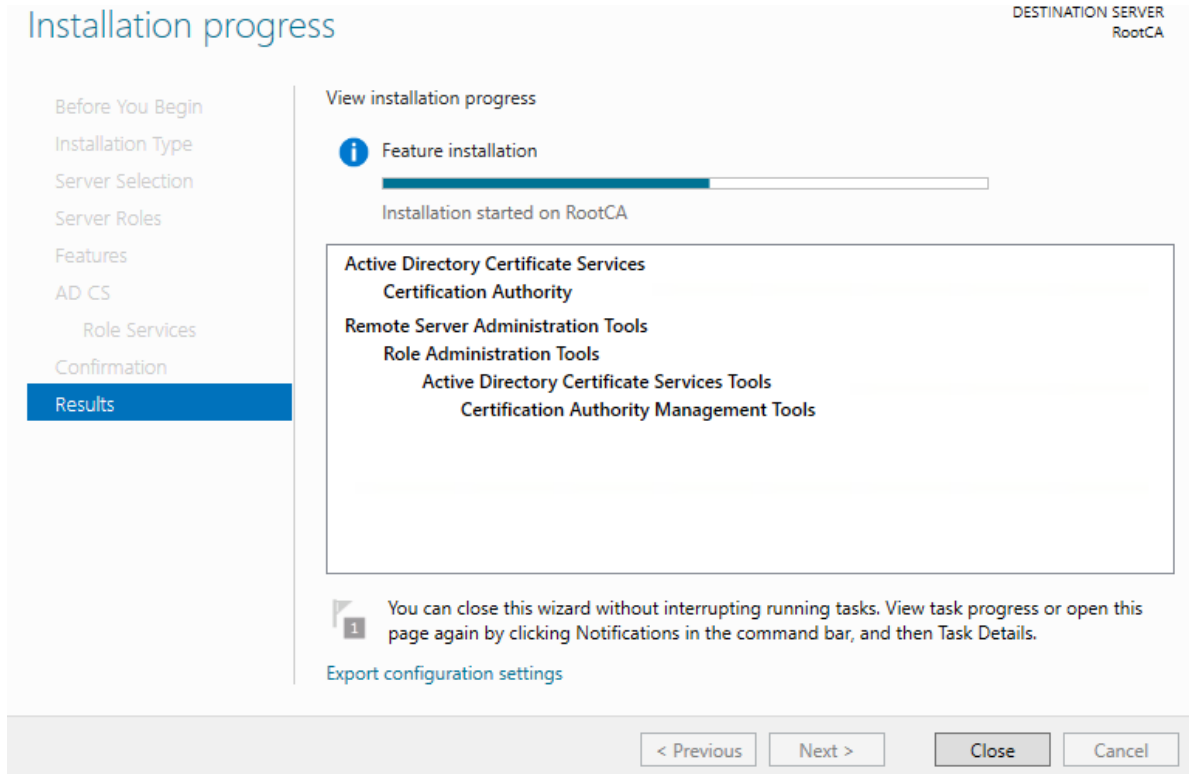
Role

**Add Roles and Features Wizard**

If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?

Export configuration settings  
Specify an alternate source path

8. Wait for the installation to complete then click Close. The Certificate Authority role is now installed.

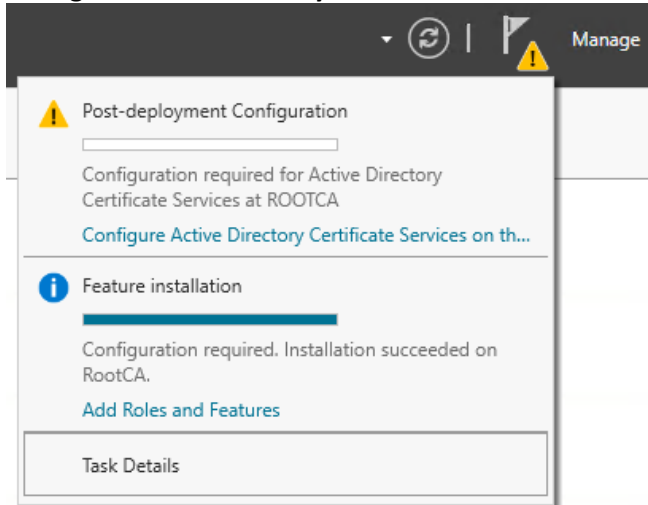


The screenshot shows the 'Installation progress' window for 'DESTINATION SERVER RootCA'. On the left is a navigation pane with the following items: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'AD CS', 'Role Services', 'Confirmation', and 'Results' (which is highlighted in blue). The main area is titled 'View installation progress' and shows a progress bar for 'Feature installation' which is approximately 75% complete. Below the progress bar, it states 'Installation started on RootCA'. A list of installed features is shown in a box: 'Active Directory Certificate Services', 'Certification Authority', 'Remote Server Administration Tools', 'Role Administration Tools', 'Active Directory Certificate Services Tools', and 'Certification Authority Management Tools'. At the bottom of the main area, there is a tip: '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.' Below the tip is a link for 'Export configuration settings'. At the very bottom of the window are four buttons: '< Previous', 'Next >', 'Close', and 'Cancel'.

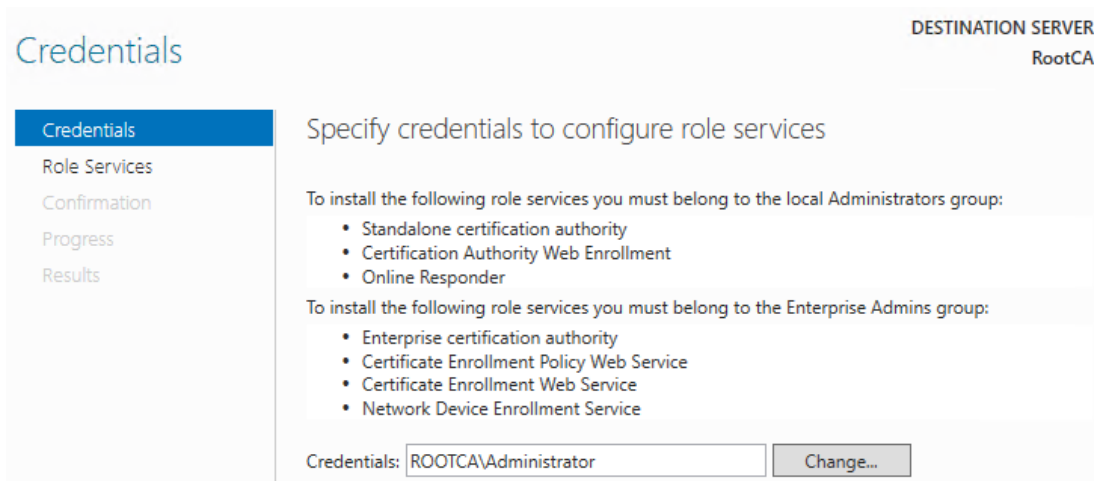
## Deploying the Root Certificate Authority – Configuration



1. In the Server Manager notifications menu, find the **Post-deployment Configuration** notification and click the **Configure Active Directory Certificate Services on the destination server** link



2. On the **Credentials** screen of the AD CS Configuration wizard, accept the default local Administrator credentials and click Next



- On the **Roles Services** screen, select **Certificate Authority** then click Next

DESTINATION SERVER  
RootCA

## Role Services

- Credentials
- Role Services**
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name

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

- On the **Setup Type** screen ensure **Standalone CA** is selected then click Next.

DESTINATION SERVER  
RootCA

## Setup Type

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

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).

- On the **CA Type** screen ensure **Root CA** is selected then click Next

DESTINATION SERVER  
RootCA

## CA Type

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

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.

- On the **Private Key** screen select **Create a new private key** then click Next

DESTINATION SERVER  
RootCA

### Private Key

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key**
- Cryptography
- CA Name
- Validity Period
- Certificate Database

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

- On the **Cryptography for CA** screen ensure **RSA#Microsoft Software Key Storage Provider** and **SHA256** are selected, however, change the Key Length to **4096** and check the **Allow administrator interaction when the private key is accessed by the CA** option then click Next

DESTINATION SERVER  
RootCA

### Cryptography for CA

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

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
- MDS

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

- On the **CA Name** screen, enter a common name for you Root CA, we will use **CityRootCA** for this lab

DESTINATION SERVER  
RootCA

### CA Name

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

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:  
CityRootCA

Distinguished name suffix:  
\_\_\_\_\_

Preview of distinguished name:  
CN=CityRootCA

9. On the **Validity Period** screen enter the period for which the Root CA certificate will be valid, we will use **15** years for this lab

### Validity Period

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography
- CA Name
- Validity Period

DESTINATION SERVER  
RootCA

#### Specify the validity period

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

CA expiration Date: 4/3/2033 4:03:00 PM

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

---

**TIP:** Given cryptography settings of **SHA256** and **4096** key length or stronger, 10 – 20 years is a reasonable range for validity periods.

---

10. On the **CA Database** screen accept the default locations and click Next

### CA Database

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

DESTINATION SERVER  
RootCA

#### Specify the database locations

Certificate database location:

Certificate database log location:

11. On the **Confirmation** screen, verify all choices then click Configure

**Confirmation** DESTINATION SERVER  
RootCA

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

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: Enabled  
Certificate Validity Period: 4/3/2033 4:03:00 PM  
Distinguished Name: CN=CityRootCA  
Certificate Database Location: C:\Windows\system32\CertLog  
Certificate Database Log Location: C:\Windows\system32\CertLog

< Previous    Next >    **Configure**    Cancel

12. The **Certificate Authority** role service is now configured. Click Close.

**Results** DESTINATION SERVER  
RootCA

Credentials  
Role Services  
Setup Type  
CA Type

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

⤴ **Active Directory Certificate Services**

**Certification Authority** ✔ Configuration succeeded  
[More about CA Configuration](#)

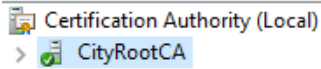
**NOTE:** We now need to configure the locations of the CDP and AIA to point to the PKI Information Server, so that the domain infrastructure has access to information published by the Root CA once it is offline

13. In the **Tools** menu of Server Manager, launch the **Certificate Authority** management console

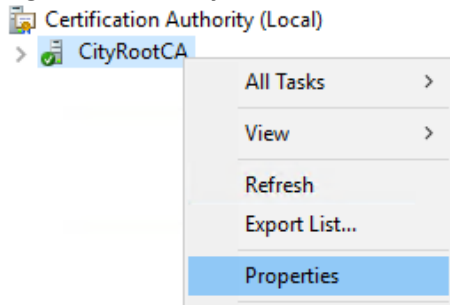
Manage **Tools**

- Certificate Authority**
- Component Services
- Computer Management

14. Verify that the **CityRootCA** certificate authority service is running (green check mark)



15. Right click the **CityRootCA** node and select Properties

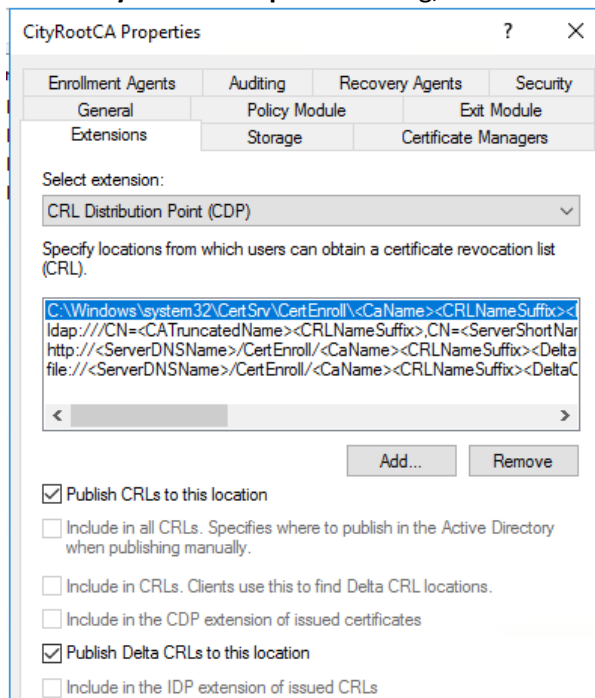



---

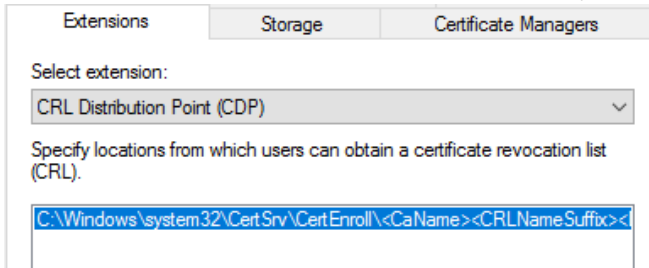
**NOTE:** It takes a few seconds for the Properties dialog box to show

---

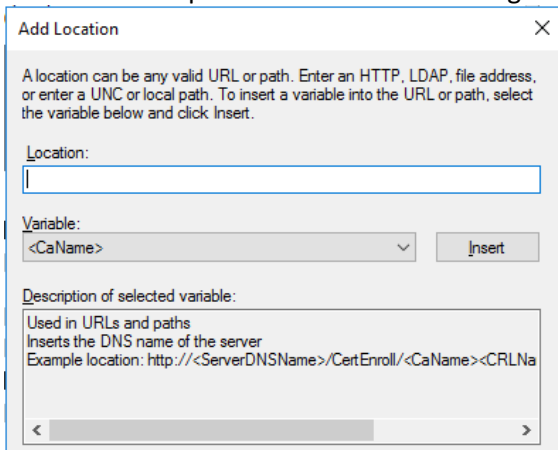
16. In the **CityRootCA Properties** dialog, select the **Extensions** tab



17. Remove all entries for the CRL Distribution Point, except for the file system entry on drive C:

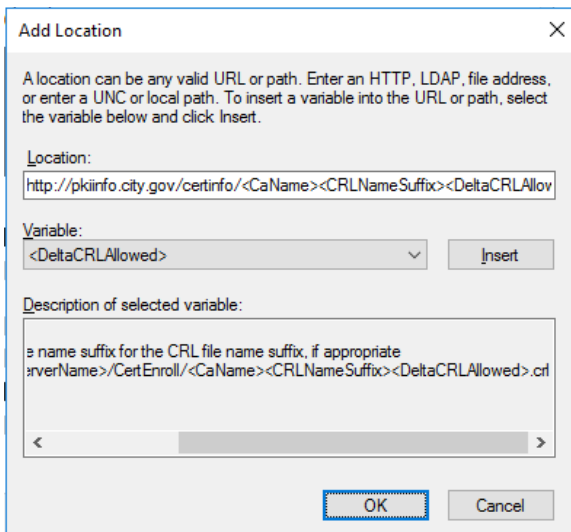


18. Click Add... to open the Add Location dialog



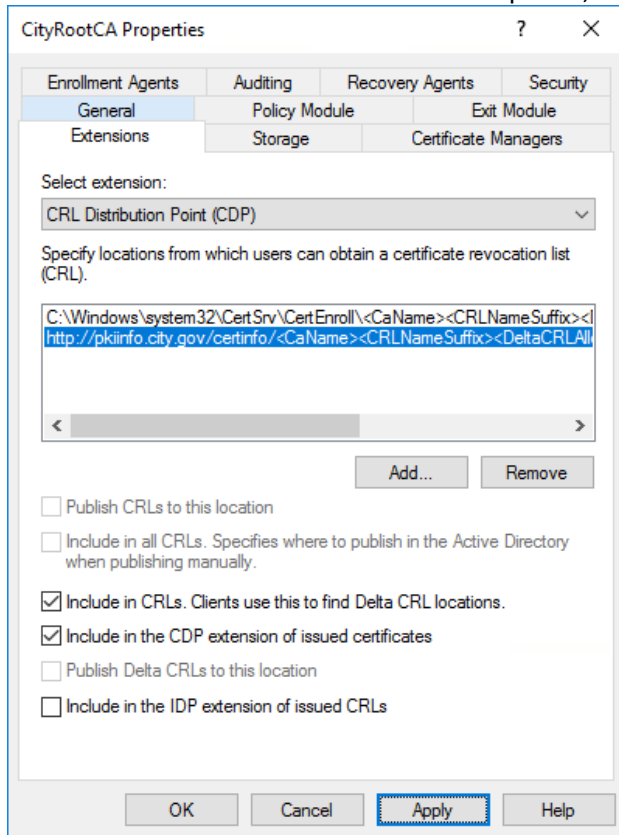
19. Enter for following URL to the PKI Information Server and click OK

<http://pkiinfo.city.gov/certinfo/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl>

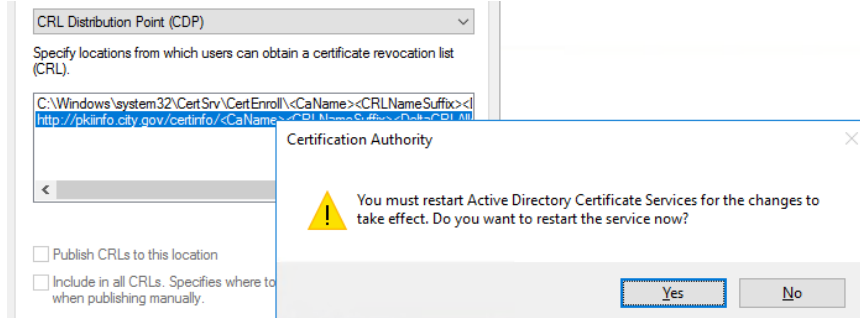


**TIP:** Use the **Variable** dropdown to insert the URL parts to avoid typos

20. For this location check both the **Include in CRLs. Clients use this to find Delta CRL Locations** and the **Include in the CDP extension of issued certificates** options, then click Apply



21. Click Yes in the Certificate Authority dialog box to restart the CA service



22. In the **Select extension** dropdown, choose Authority Information Access (AIA)

Extensions    Storage    Certificate Managers

Select extension:

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

23. Just as we did for the CDP, remove all entries except for the file system entry on drive C:

Extensions    Storage    Certificate Managers

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>

24. Click Add... and enter for following URL to the PKI Information Server then click OK

[http://pkiinfo.city.gov/certinfo/<ServerDNSName>\\_<CaName><CertificateName>.crt](http://pkiinfo.city.gov/certinfo/<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.

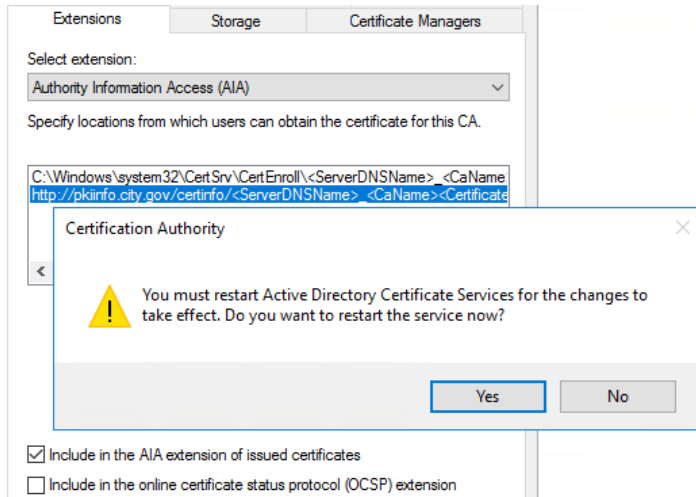
Location:  
http://pkiinfo.city.gov/certinfo/<ServerDNSName>\_<CaName><CertificateName>.crt

Variable:  
<CaName>    Insert

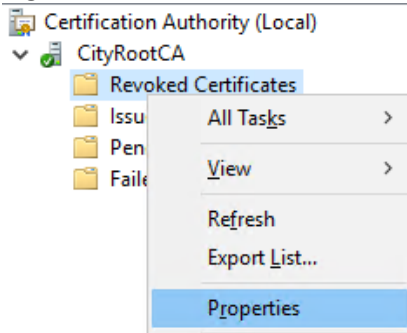
Description of selected variable:  
Used in URLs and paths  
Inserts the DNS name of the server  
Example location: http://<ServerDNSName>/CertEnroll/<ServerDNSName>  
Or (for OCSP)  
http://<ServerDNSName>/ocsp

OK    Cancel

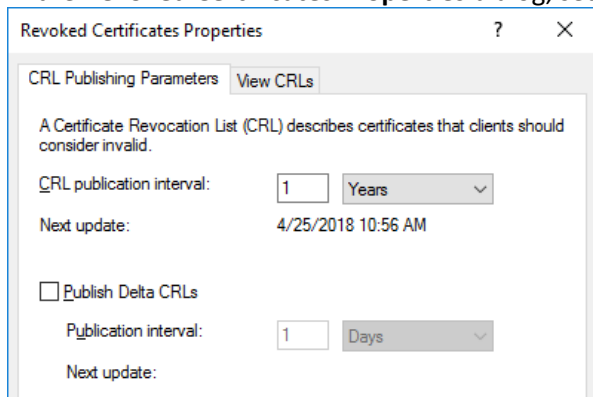
25. For this location check the **Include AIA extension of issued certificates** options, click OK then click Yes to restart the CA service



26. Right-click the **Revoked Certificates** node and select **Properties**



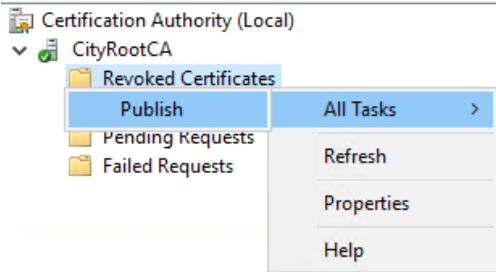
27. In the **Revoked Certificates Properties** dialog, set the **CRL publication interval** to **1 year**, then click OK



**TIP:** Expired CRLs will prevent online CA services from starting. Be careful to choose a publication interval that is sensible for your organization

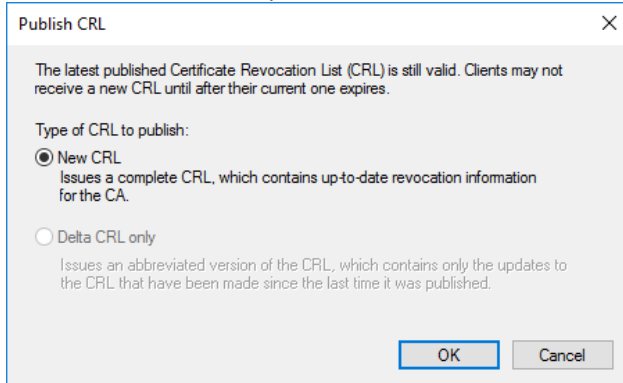
**NOTE:** We now need to publish the certificate revocation list (CRL) along with the AIA certificate that signs the CRL

28. In the **Certificate Authority** management console, right click **Revoked Certificates** folder under **CityRootCA**, go to **All Tasks** and click **Publish**



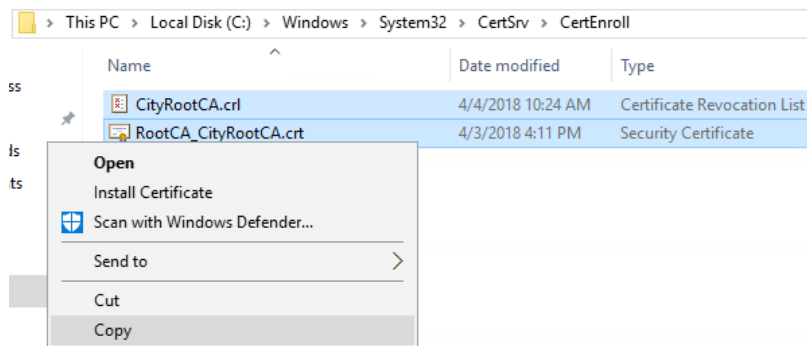
**NOTE:** It can take a few seconds for the Publish CRL dialog box to show

29. Ensure the **New CRL** option is selected and click **OK**



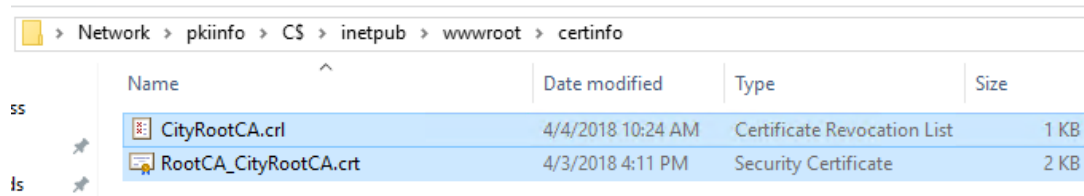
30. In Windows Explorer browse to the following path and copy the *crl* and *crt* files. These are the certificate revocation list and AIA cert

**C:\Windows\System32\CertSrv\CertEnroll**



31. Browse to the administrative share for drive C: on the PKI Information Server (**PkiInfo**) and copy the *crl* and *crt* files to the **certinfo** folder of the web server

\\pkiinfo\C\$\inetpub\wwwroot\certinfo



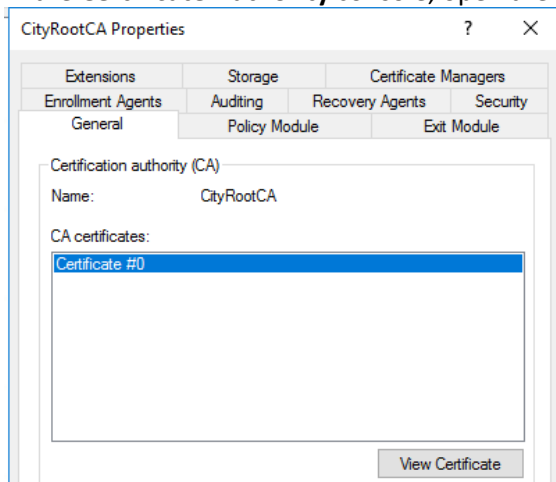
32. Use Internet Explorer to verify that the *crl* and *crt* files are available via the PKI Information Server URL

http://pkiinfo.city.gov/certinfo

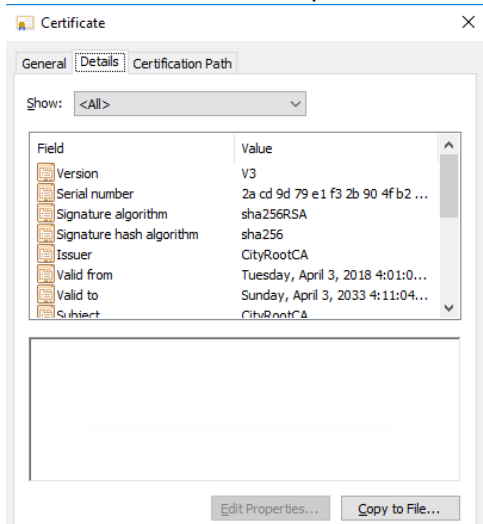


**NOTE:** Next we will make the Root CA certificate available via the PKI Information Server

33. In the **Certificate Authority** console, open the **properties** of the CityRootCA and go to the **General** tab

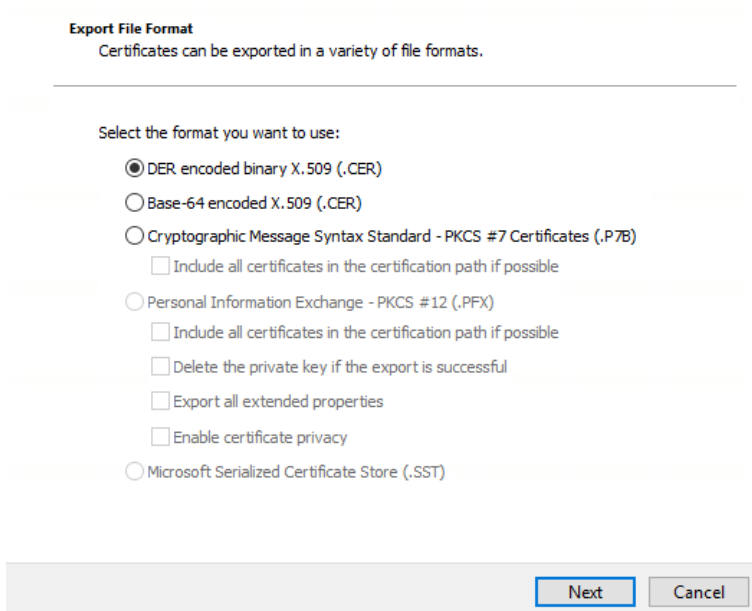


34. Click View Certificate to open the Certificate dialog and go to the **Details** tab



35. Click **Copy to File...** then click Next in the **Certificate Export Wizard** dialog. Ensure the **DER encoded binary X.509 (.CER)** option is selected then click Next

← Certificate Export Wizard



36. Enter the following file path for the Root CA certificate export, then click Next

C:\Windows\System32\CertSrv\CertEnroll\CityRootCA.cer

← Certificate Export Wizard

**File to Export**  
Specify the name of the file you want to export

---

File name:

37. Verify the information in the summary screen shows then click Finish

← Certificate Export Wizard

**Completing the Certificate Export Wizard**

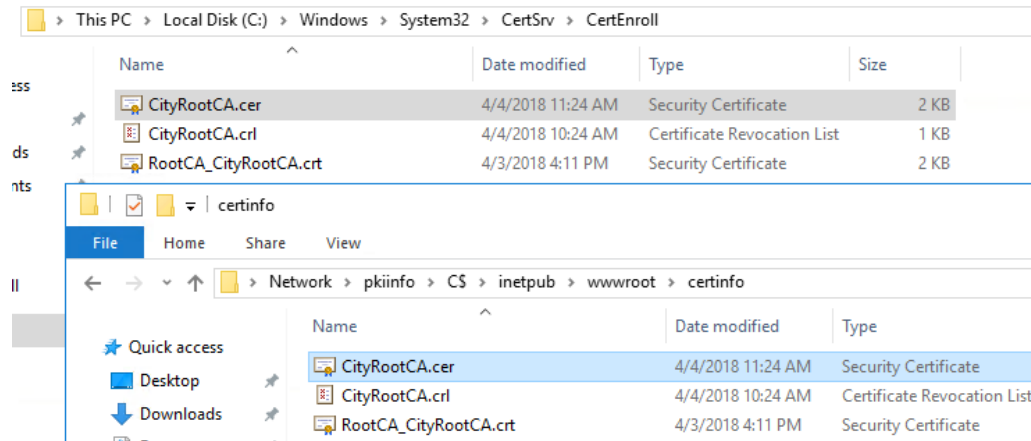
You have successfully completed the Certificate Export wizard.

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)

<

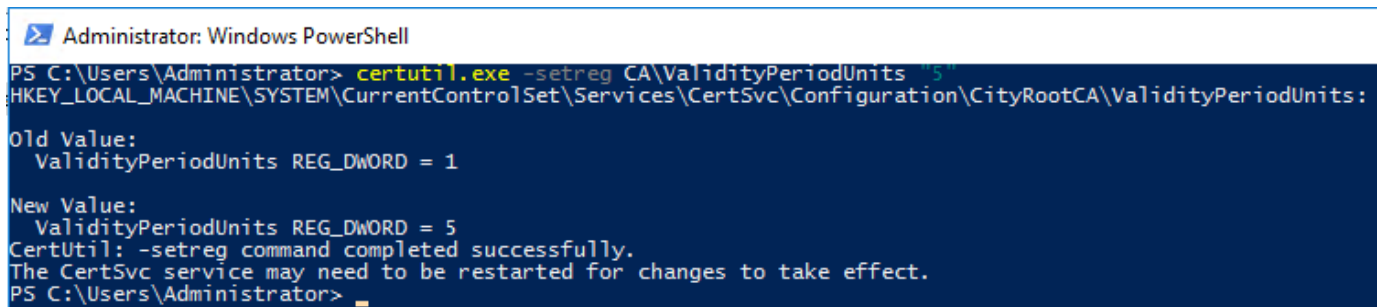
38. Copy the CityRootCA.cer file to the PKI Information Server



**NOTE:** Lastly, we update the validity period of certificates created by the Root CA to 5 years

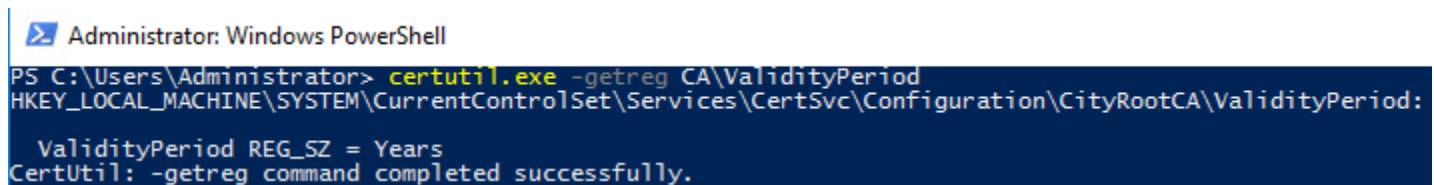
39. In **PowerShell** run the following command

`certutil.exe -setreg CA\ValidityPeriodUnits "5"`

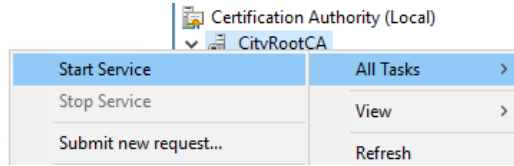
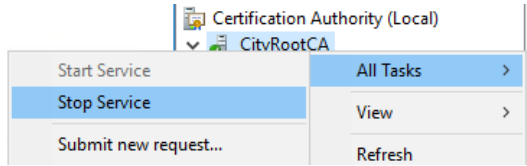


**TIP:** Whenever modifying validity period units, always verify that the validity period is set correctly, to years in this case

`certutil.exe -getreg CA\ValidityPeriod`



40. Stop, then Start the Certificate Authority service to pick up these registry changes




---

**TIP:** You can also run the following commands to stop and start the CA service:

`stop-service certsvc` then `start-service certsvc`

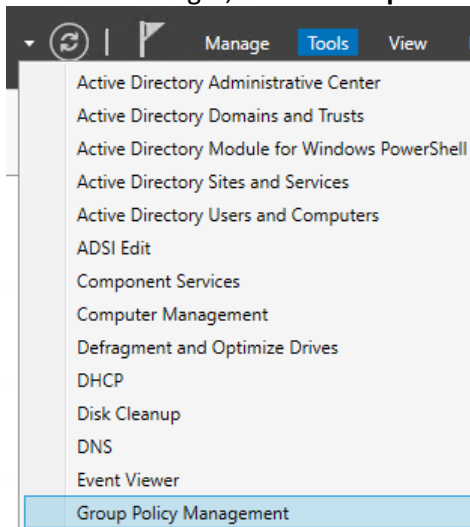
---



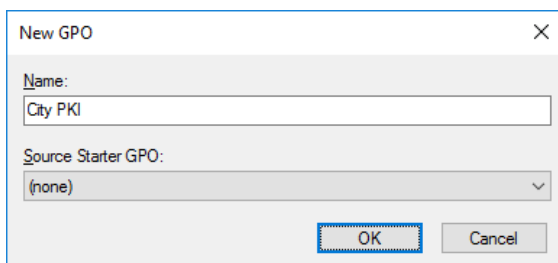
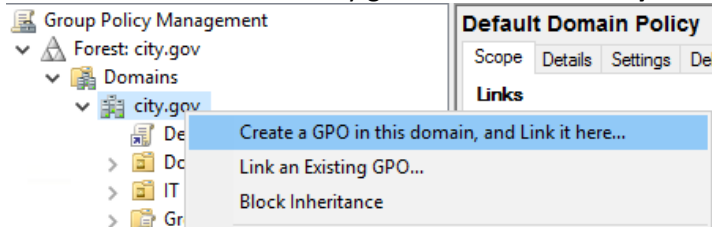
## Deploying the Root Certificate Authority – Trusted Root Certificate Group Policy

**NOTE:** Now we need to configure a domain group policy so that all machines in the domain will trust the RootCA

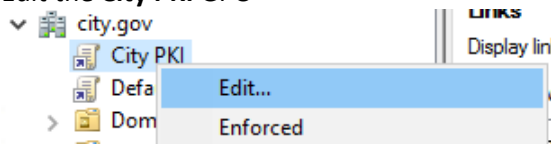
1. Open a Virtual Machine Connection to the Domain Controller (DC) and login
2. In Server Manager, launch **Group Policy Manager** from the **Tools** menu



3. Create a new GPO for the city.gov domain named **City PKI**

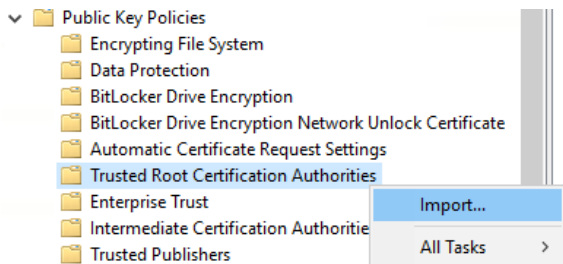


4. Edit the **City PKI** GPO



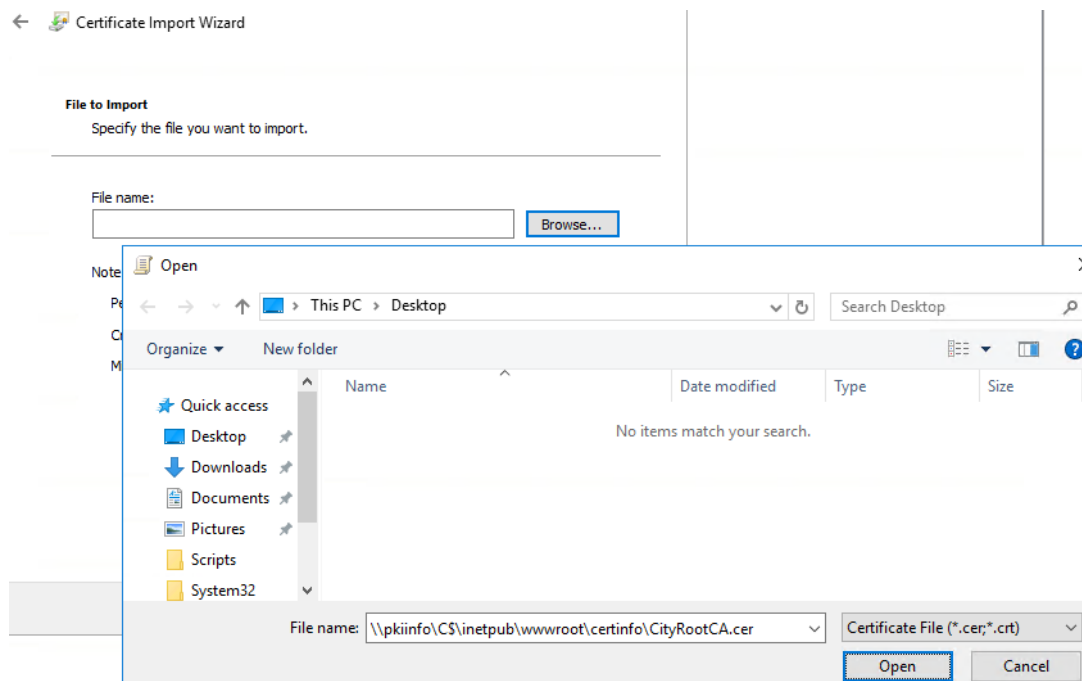
5. In the **Group Policy Management Editor** navigate to the following policy path then right click and select **Import** from the **Trusted Root Certification Authorities** node

**Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities**




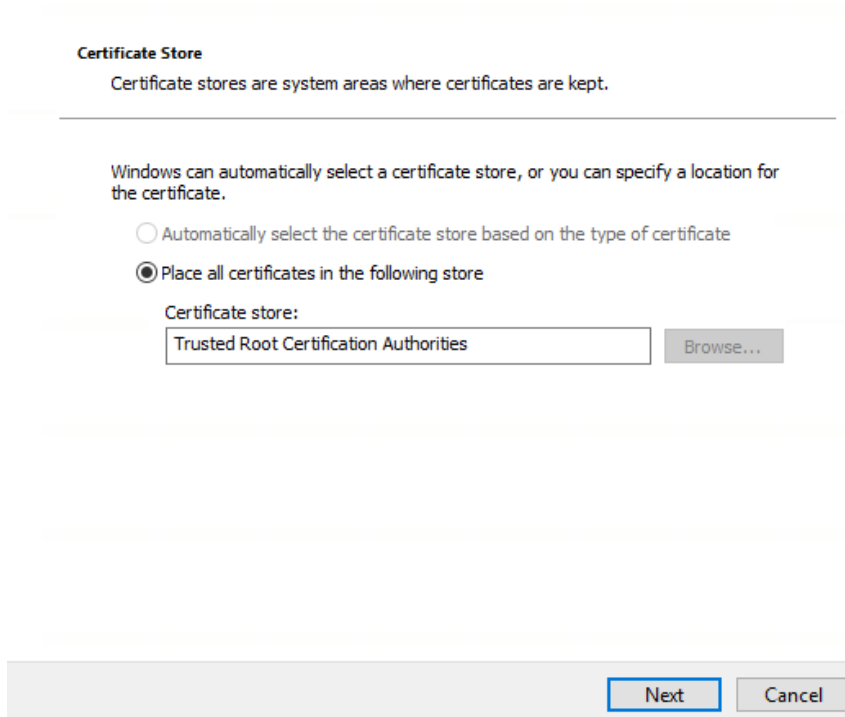
6. In the Certificate Import Wizard dialog click Next and then Browser... and enter the following path to the Root CA certificate, then click Open then click Next

**\\pkiinfo\CS\inetpub\wwwroot\certinfo\CityRootCA.cer**



7. On the **Certificate Store** page of the Certificate Import Wizard, ensure the certificate store is set to **Trusted Root Certification Authorities**, then click Next then click Finish

←  Certificate Import Wizard



**Certificate Store**  
Certificate stores are system areas where certificates are kept.

---

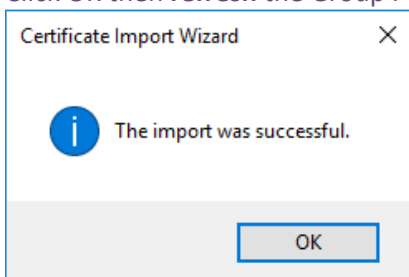
Windows can automatically select a certificate store, or you can specify a location for the certificate.

Automatically select the certificate store based on the type of certificate

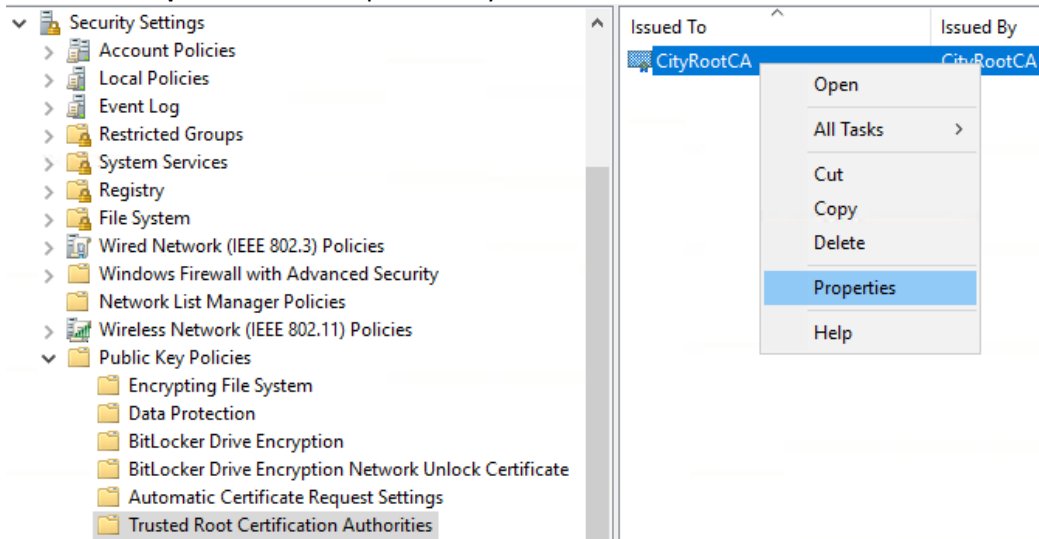
Place all certificates in the following store

Certificate store:

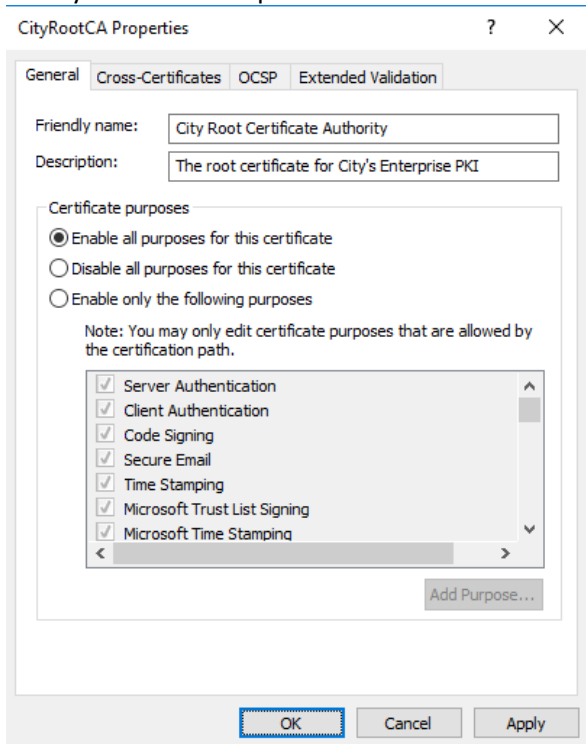
**NOTE:** It will take a few seconds to import the Root CA certificate. Once imported you will see the following dialog. Click OK then **refresh** the Group Policy Manager Editor



8. Go to the **Properties** of the imported CityRootCA certificate



9. Here you can make updates to the Root CA certificate, we will update Friendly Name and Description



**NOTE:** We now have a fully configured Root Certificate Authority!

You may need to run **gpupdate /force** on domain members to immediately pull these GPO updates.

## Deploying the Enterprise Subordinate Certificate Authority – Installation

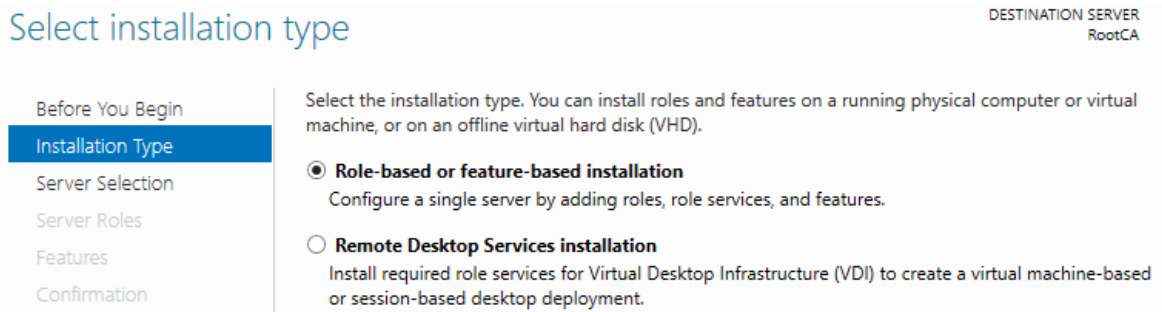


1. In **Hyper-V Manager**, start the Subordinate CA (**SubCA**) virtual machine
2. Open a Virtual Machine Connection to the Subordinate CA (**SubCA**) and login as domain Administrator
3. Start Server Manager and select **Add roles and features**, under the *Configure this local server* section

### 1 Configure this local server

- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

4. On the **Select installation type** screen, select Role-based or feature-based installation and click next



Select installation type

DESTINATION SERVER  
RootCA

Before You Begin  
**Installation Type**  
Server Selection  
Server Roles  
Features  
Confirmation

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.



- Skip to the **Roles Services** screen under **AD CS** and select **Certificate Authority Web Enrollment** then click Add Features to Add the IIS dependency.

Select role services

DESTINATION SERVER  
SubCA.city.gov

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
AD CS  
**Role Services**  
Confirmation  
Results

Select the role services to install for Active Directory Certificate Services

Role services

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

**Add Roles and Features Wizard**

Add features that are required for Certification Authority Web Enrollment?

You cannot install Certification Authority Web Enrollment unless the following role services or features are also installed.

- Web Server (IIS)
  - Management Tools
    - IIS 6 Management Compatibility
    - IIS 6 Metabase Compatibility
    - [Tools] IIS Management Console
  - Web Server
    - Application Development
      - ASP
      - ISAPI Extensions
    - Common HTTP Features
      - Default Document
      - Directory Browsing

Include management tools (if applicable)

Add Features Cancel

- Ensure both the Certificate Authority and Certificate Authority Web Enrollment role services are selected, then click Next

Select role services

DESTINATION SERVER  
SubCA.city.gov

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
AD CS  
**Role Services**  
Web Server Role (IIS)  
Role Services

Select the role services to install for Active Directory Certificate Services

Role services	Description
<input checked="" type="checkbox"/> Certification Authority	Certification Authority Web Enrollment provides a simple Web Enrollment interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.
<input type="checkbox"/> Certificate Enrollment Policy Web Service	
<input type="checkbox"/> Certificate Enrollment Web Service	
<input checked="" type="checkbox"/> Certificate Authority Web Enrollment	
<input type="checkbox"/> Network Device Enrollment Service	
<input type="checkbox"/> Online Responder	

- Skip to the Configuration page and check **Restart the destination server automatically if required**, before clicking Install

DESTINATION SERVER  
SubCA.city.gov

### Confirm installation selections

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
AD CS  
Role Services  
Web Server Role (IIS)  
Role Services  
**Confirmation**  
Results

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
  - Certification Authority Web Enrollment
- Remote Server Administration Tools
  - Role Administration Tools
  - Active Directory Certificate Services Tools
  - Certification Authority Management Tools
- Web Server (IIS)
  - Management Tools
  - IIS 6 Management Compatibility
  - IIS 6 Metabase Compatibility

Export configuration settings  
Specify an alternate source path

< Previous   Next >   Install   Cancel

- Wait for the installation process to complete then click Close

DESTINATION SERVER  
SubCA.city.gov

### Installation progress

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
AD CS  
Role Services  
Web Server Role (IIS)  
Role Services  
Confirmation  
**Results**

View installation progress

**i** Feature installation  
Installation started on SubCA.city.gov

- Active Directory Certificate Services
  - Certification Authority
  - Certification Authority Web Enrollment
- Remote Server Administration Tools
  - Role Administration Tools
  - Active Directory Certificate Services Tools
  - Certification Authority Management Tools
- Web Server (IIS)
  - Management Tools
  - IIS 6 Management Compatibility
  - IIS 6 Metabase Compatibility

**i** 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.

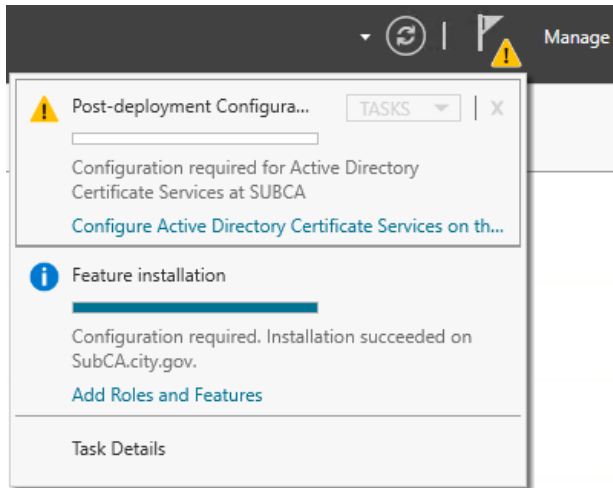
Export configuration settings

< Previous   Next >   Close   Cancel

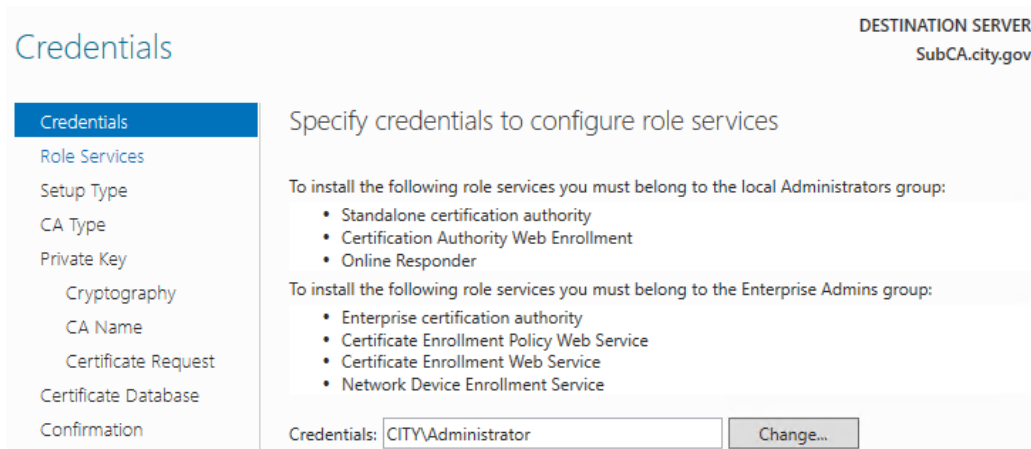
## Deploying the Enterprise Subordinate Certificate Authority – Configuration



1. In the **Server Manager** notifications menu, find the **Post-deployment Configuration** notification and click the **Configure Active Directory Certificate Services on the destination server** link



2. On the **Credentials** screen of the AD CS Configuration wizard, accept the default domain Administrator credentials and click Next



- On the **Roles Services** screen, select **Certificate Authority** and **Certificate Authority Web Enrollment** for configuration, then click Next

## Role Services

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography
- CA Name

DESTINATION SERVER  
SubCA.city.gov

### 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

- On the **Setup Type** screen ensure **Enterprise CA** is selected then click Next.

## Setup Type

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

DESTINATION SERVER  
SubCA.city.gov

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

- On the **CA Type** screen ensure **Subordinate CA** is selected then click Next

## CA Type

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography
- CA Name
- Certificate Request
- Certificate Database
- Confirmation

DESTINATION SERVER  
SubCA.city.gov

### 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.

- On the **Private Key** screen select **Create a new private key** then click Next

DESTINATION SERVER  
SubCA.city.gov

### Private Key

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key**
- Cryptography
- CA Name
- Certificate Request
- Certificate Database

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

- On the **Cryptography for CA** screen ensure **RSA#Microsoft Software Key Storage Provider** and **SHA256** are selected, however, change the Key Length to **4096** and **uncheck the Allow administrator interaction when the private key is accessed by the CA** option then click Next

DESTINATION SERVER  
SubCA.city.gov

### Cryptography for CA

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography**
- CA Name
- Certificate Request
- Certificate Database
- Confirmation
- Progress

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
- MDS

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

- On the **CA Name** screen, enter a common name for you Root CA; we will use **CitySubordinateCA** for this lab

DESTINATION SERVER  
SubCA.city.gov

### CA Name

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

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: CitySubordinateCA

Distinguished name suffix: DC=city,DC=gov

Preview of distinguished name: CN=CitySubordinateCA,DC=city,DC=gov

9. On the **Certificate Request** screen, save the request as a file

### Certificate Request

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

DESTINATION SERVER  
SubCA.city.gov

#### Request a certificate from parent CA

You require a certificate from a parent certification authority (CA) to allow this subordinate CA to issue certificates. You can request a certificate from an online CA or you can store your request to a file to submit to the parent CA.

Send a certificate request to a parent CA:

Select:

CA name

Computer name

Parent CA:  Select...

Save a certificate request to file on the target machine:

File name:

i You must manually get a certificate back from the parent CA to make this CA operational.

10. On the **CA Database** screen accept the default locations and click Next

### CA Database

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Certificate Request
  - Certificate Database
  - Confirmation

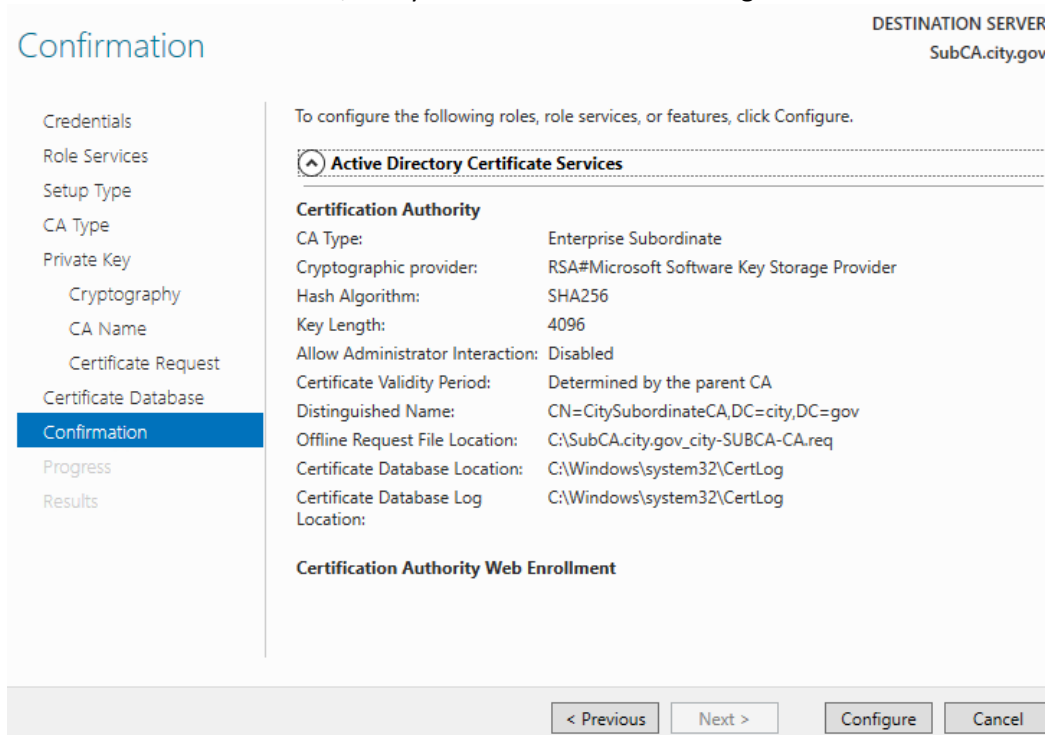
DESTINATION SERVER  
SubCA.city.gov

#### Specify the database locations

Certificate database location:

Certificate database log location:

11. On the **Confirmation** screen, verify all choices then click Configure



**Confirmation** DESTINATION SERVER  
SubCA.city.gov

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
Cryptography  
CA Name  
Certificate Request  
Certificate Database  
**Confirmation**  
Progress  
Results

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

**Active Directory Certificate Services**

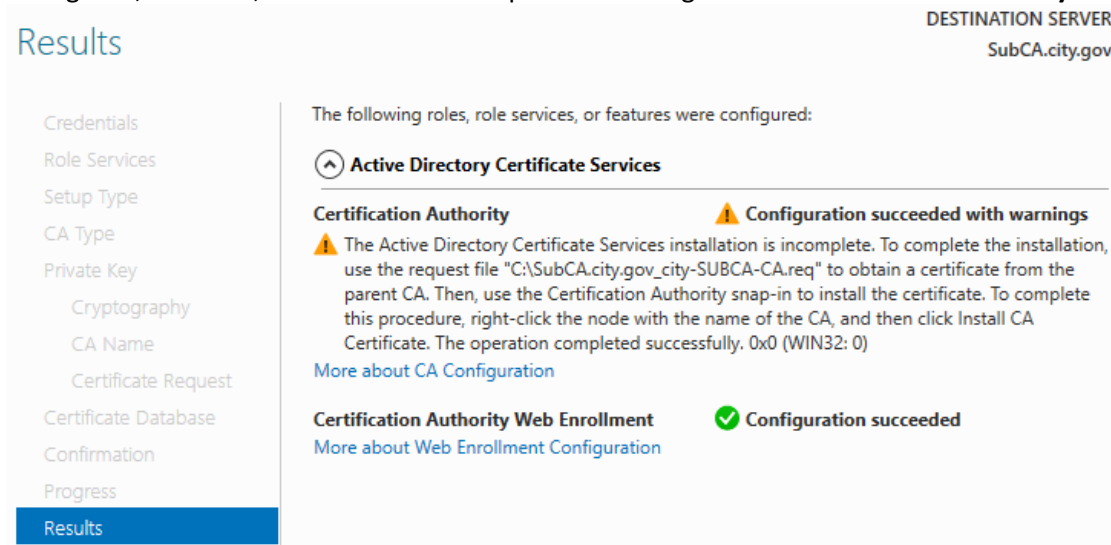
**Certification Authority**

CA Type:	Enterprise Subordinate
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	4096
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	Determined by the parent CA
Distinguished Name:	CN=CitySubordinateCA,DC=city,DC=gov
Offline Request File Location:	C:\SubCA.city.gov_city-SUBCA-CA.req
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

**Certification Authority Web Enrollment**

< Previous    Next >    Configure    Cancel

12. Review to configuration results. The **Certificate Authority Web Enrollment** role service should be completely configured, however, we still need to complete the configuration of **Certificate Authority** role service



**Results** DESTINATION SERVER  
SubCA.city.gov

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
Cryptography  
CA Name  
Certificate Request  
Certificate Database  
Confirmation  
Progress  
**Results**

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

**Active Directory Certificate Services**

**Certification Authority** ⚠ **Configuration succeeded with warnings**

⚠ The Active Directory Certificate Services installation is incomplete. To complete the installation, use the request file "C:\SubCA.city.gov\_city-SUBCA-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)

[More about CA Configuration](#)

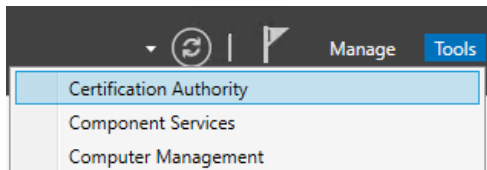
**Certification Authority Web Enrollment** ✔ **Configuration succeeded**

[More about Web Enrollment Configuration](#)

**NOTE:** We now need to have the Root CA issue a certificate for the Subordinate CA. We will do this next by submitting the certificate request file that was just created to the Root CA for issuance.

## Deploying the Enterprise Subordinate Certificate Authority – Certificate Issuance

1. Open a Virtual Machine Connection to the Root CA (**RootCA**) and login
2. In Server Manager, launch the **Certificate Authority** management console from the **Tools** menu

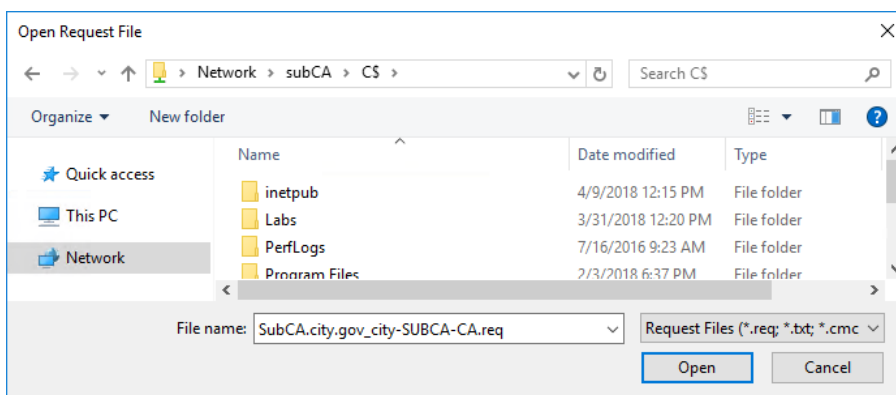


3. Right click the **CityRootCA** node and under the **All Tasks** menu select **Submit new request...**



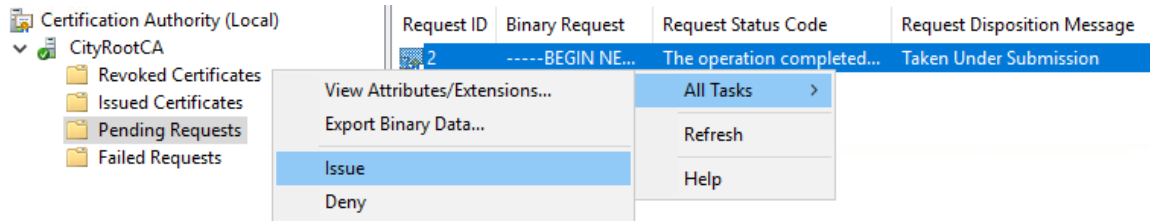
4. In the **Open Request File** dialog box, browse the certificate request created on the Subordinate CA

\\subCA\C\$\SubCA.city.gov\_city-SUBCA-CA.req

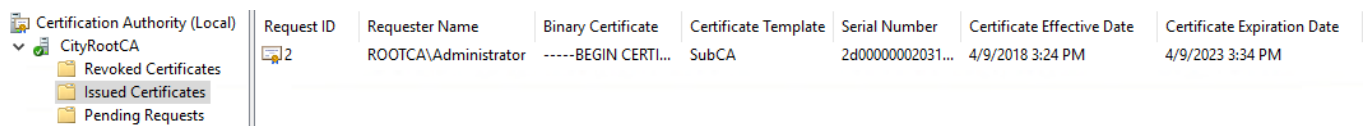


**NOTE:** It can take up to 15 seconds for the request to be imported even though the console remains usable. Refresh the console until you see the certificate request in the Pending Requests node.

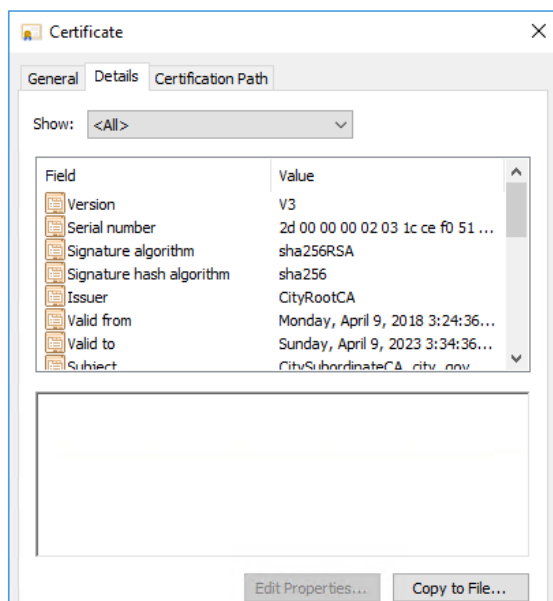
- In the **Pending Requests** node, right click on the imported certificate request and select **All Tasks > Issue**




- In the **Issued Certificates** node, verify that the Subordinate CA certificate has been issued



- Double-click to open the issued certificate and go to the Details tab of the Certificate dialog



- Click **Copy to File...** then click Next in the **Certificate Export Wizard** dialog. Ensure the **Cryptographic Message Syntax Standard** option is selected then click 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)


---

**TIP** Enabling the Include all certificates in the certificate path if possible options will include the root certificate in the export file as well.

---

- Enter the following file path for the Root CA certificate export, then click Next

\\subCA\C\$\SubCA.p7b


←  Certificate Export Wizard

**File to Export**  
Specify the name of the file you want to export

---

File name:

10. Verify the information in the summary screen shows then click Finish

←  Certificate Export Wizard

### Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	\\subCA\C\$\SubCA.p7b
Export Keys	No
Include all certificates in the certification path	No
File Format	Cryptographic Message Syntax Stand

## Deploying the Enterprise Subordinate Certificate Authority – Certificate Installation



1. Open a Virtual Machine Connection to the Subordinate CA (**SubCA**) and login as the domain Administrator
2. In a command prompt, force a group policy update to ensure the **City PKI** GPO has been applied

**gpupdate /force**

```
Administrator: Command Prompt
C:\Users\Administrator.CITY>gpupdate /force
Updating policy...

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

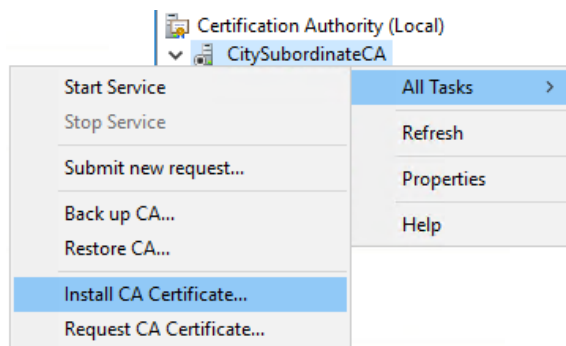
3. In Server Manager, launch the Certificate Authority management console from the Tools menu

---

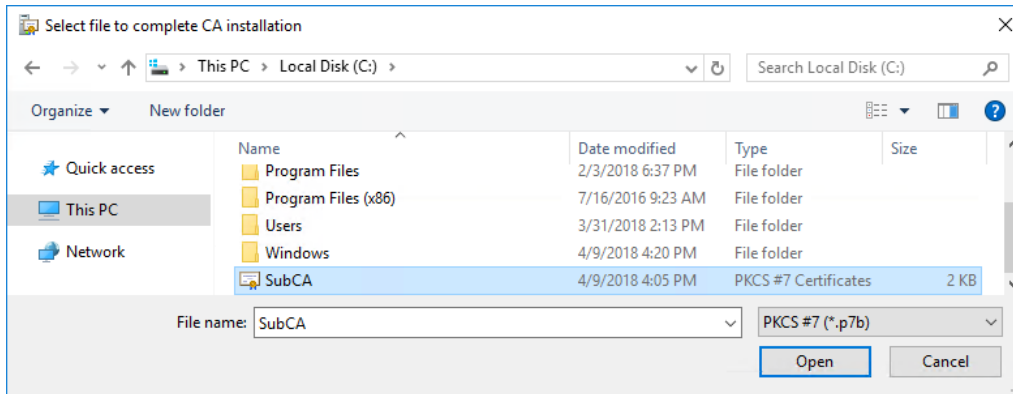
**NOTE:** The Certificate Authority service for the Subordinate CA is currently stopped

---

4. Right click the **CitySubordinateCA** node and select **All Tasks > Install CA Certificate...**



- In the **Select file to complete CA installation** dialog, browse the certificate file (.p7b) that was issued and exported from the Root CA

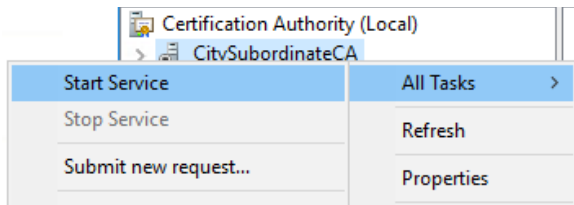



---

**NOTE:** The certificate will take a few seconds to install, during which time the mmc console will be unresponsive

---

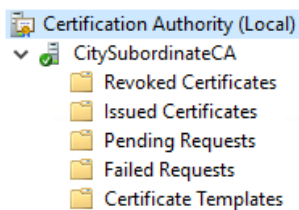
- Right-click the **CitySubordinateCA** node and select **All Tasks > Start Service**




---

**NOTE:** The CA service will take a few seconds to start up.

---

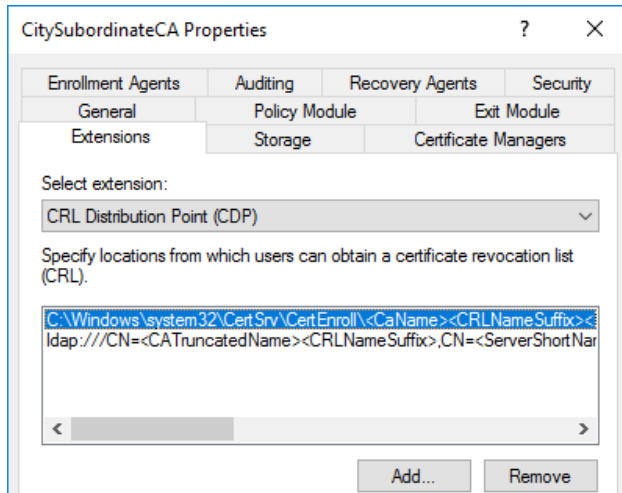



---

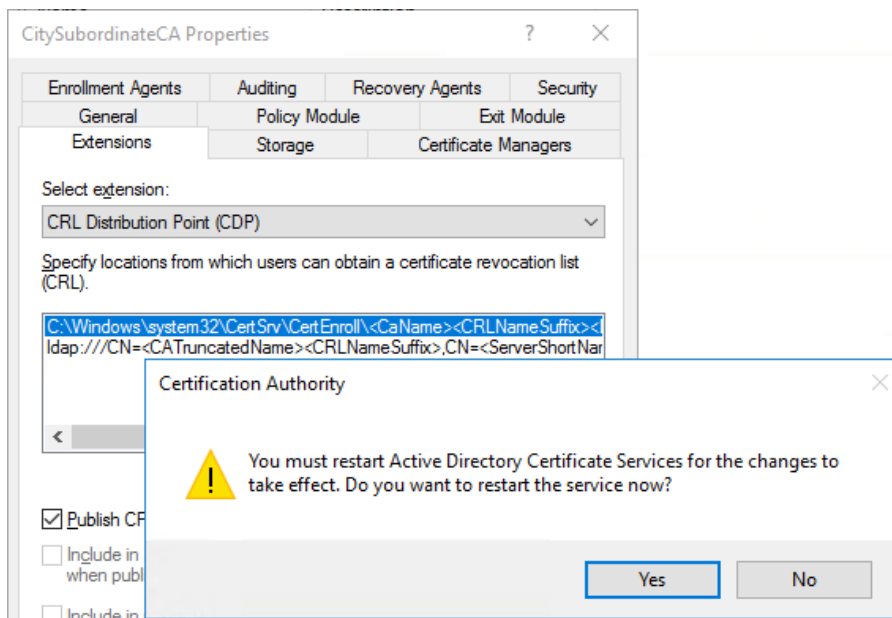
**NOTE:** Lastly, we need to update the CDP and AIA extensions to point to the PKI Information Server

---

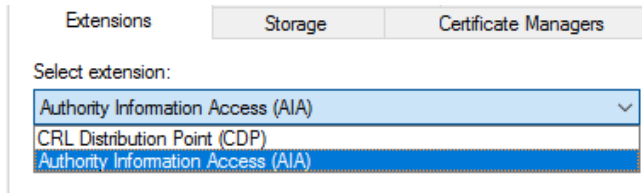
- In the **CitySubordinateCA Properties** dialog, select the **Extensions** tab and remove the **http** and **file** entries for the CRL Distribution Point then click Apply



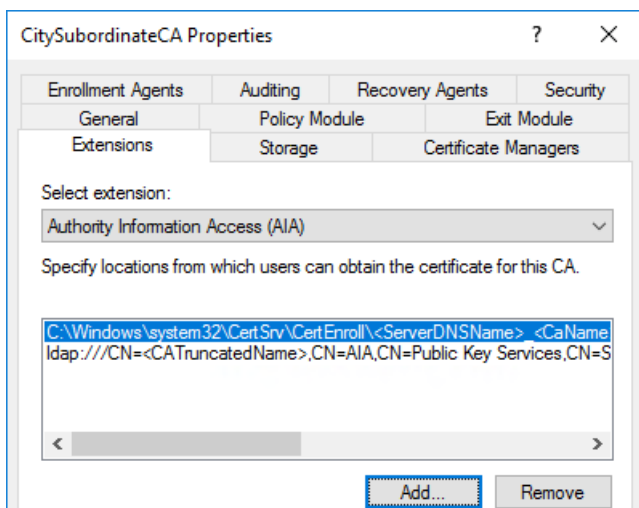
- Click Yes in the Certificate Authority dialog box to restart the CA service



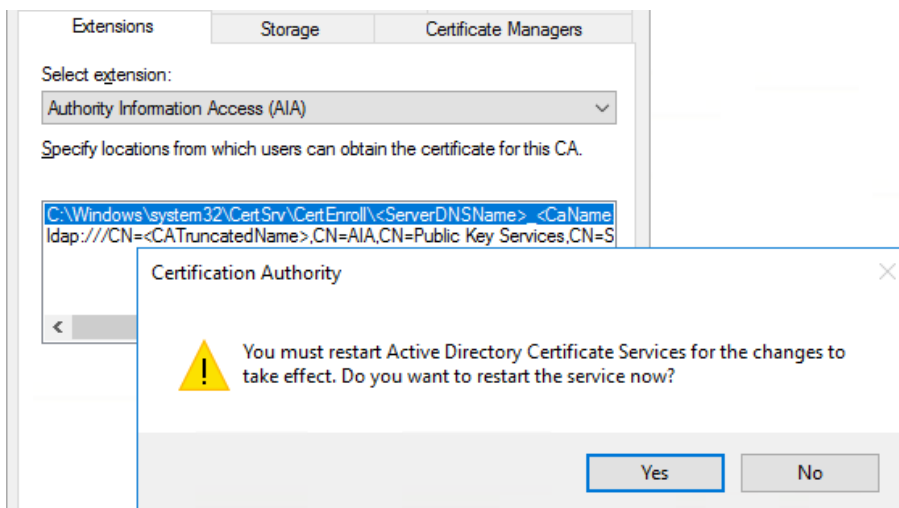
9. In the **Select extension** dropdown, choose Authority Information Access (AIA)



10. Just as we did for the CDP, remove the **http** and **file** entries for the AIA then click Apply

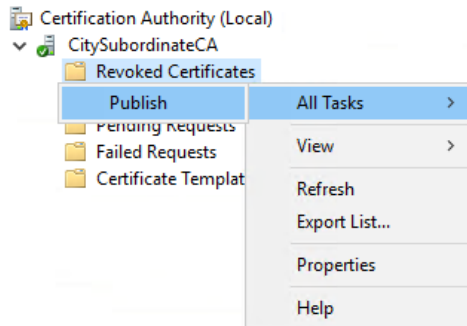


11. Click Yes to restart the CA service



**NOTE:** We now need to publish the certificate revocation list (CRL) along with the AIA certificate that signs the CRL

12. In the **Certificate Authority** management console, right click **Revoked Certificates** folder under CitySubordinateCA, go to All Tasks and click **Publish**

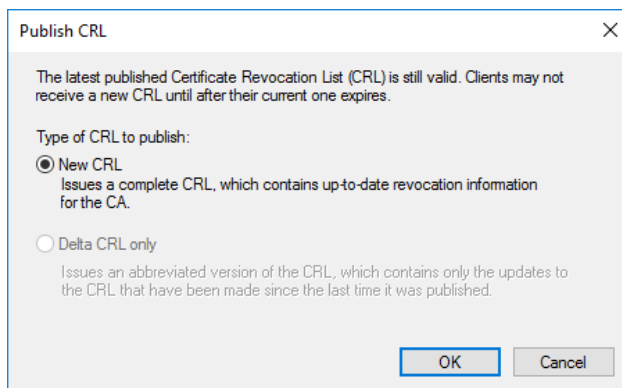



---

**NOTE:** It can take a few seconds for the Publish CRL dialog box to show

---

13. Ensure the **New CRL** option is selected and click OK




---

**NOTE: Congratulations!** You have successfully deployed a Two-Tier Enterprise PKI. You may now shut down the Root CA and keep it offline.

---