2018 CONNECT
delivering connected communities

Certificate Authority Infrastructure Hands-On Lab

Part 2: ADCS Administration & Maintenance

Information Technology & Security

CLASS DESCRIPTION

The second in a two-part hands-on-lab series; this lab will introduce the tasks you will need to perform to administer and maintain an ADCS public key infrastructure (PKI).

OVERVIEW

We will practice performing the following administrative tasks on the PKI you deployed in part 1 of this lab:

- Issuing Certificates
- Revoking Certificates
- Backing up a Certificate Authority
- Restoring a Backed-up Certificate Authority

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

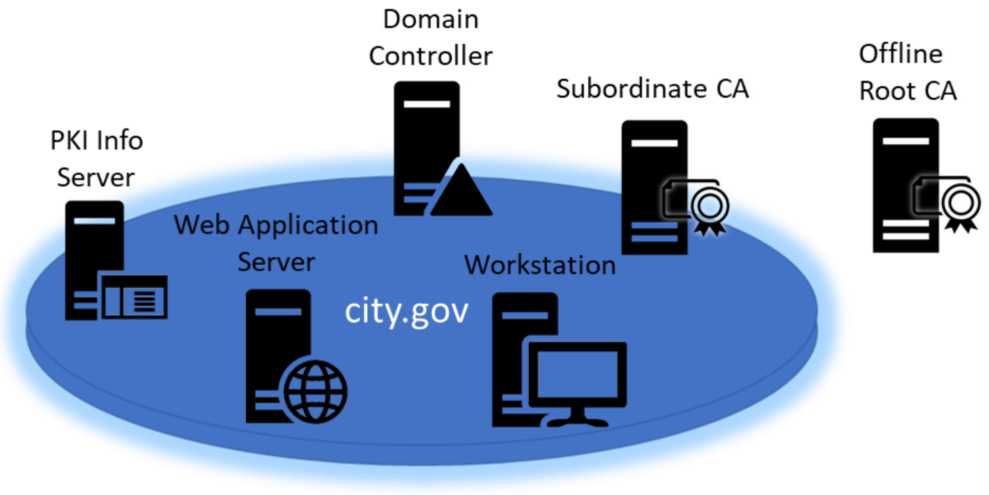


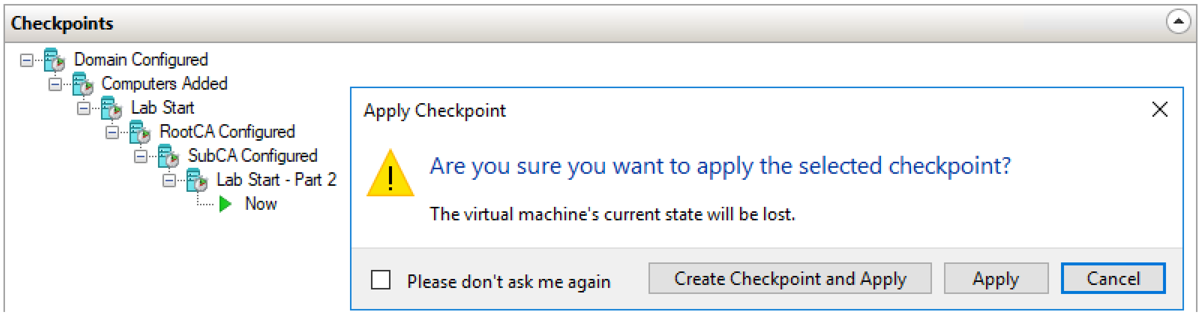
Figure 1 - Lab Infrastructure

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 ADMINISTRATION AND MAINTENANCE HANDS-ON-LAB

TIP: If you did not complete all tasks in part 1 of this lab, you may jump ahead by applying the **Lab Start – Part 2** checkpoints on the **DC**, **RootCA**, **PkiInfo** and **SubCA** virtual machines.



Apply Checkpoint

Are you sure you want to apply the selected checkpoint?

The virtual machine's current state will be lost.

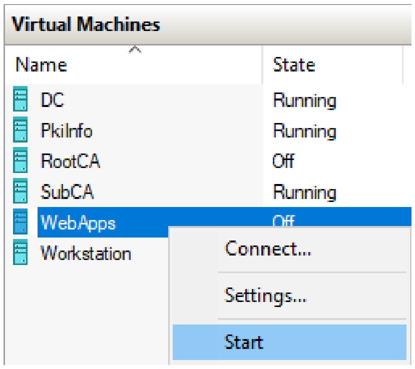
☐ Please don't ask me again

Web Application Server

Certificate Authority Administration – Requesting & Issuing a SSL Certificate

NOTE: We have already experienced manually requesting and issuing a certificate during the provisioning of the subordinate CA. Here we will look at the experience of using client tooling to automatically submit a certificate request which will be automatically issued.

1. Start the Web Application Server (**WebApps**) and login as the domain Administrator



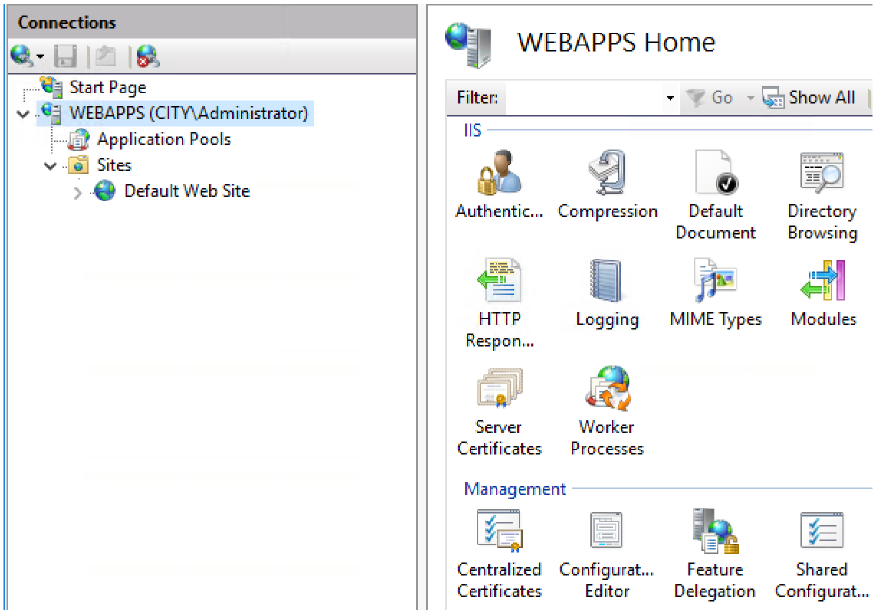
Virtual Machines

Name	State
DC	Running
PkiInfo	Running
RootCA	Off
SubCA	Running
WebApps	Off
Workstation	

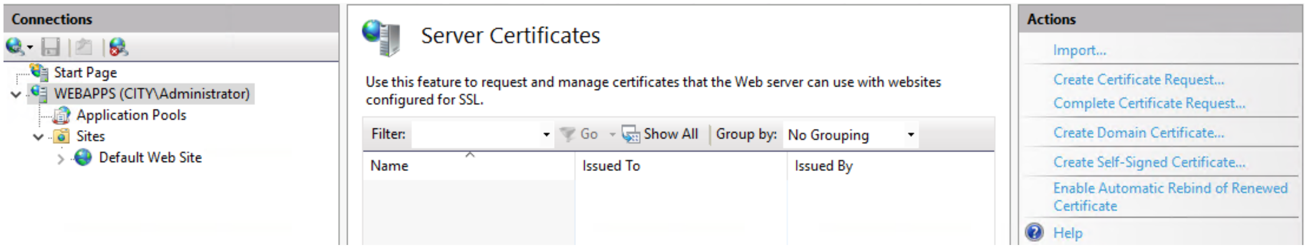
TIP: To login as domain administrator enter the user name as **City\Administrator**

2. Start the Internet Information Services (IIS) Manager

3. In the left navigation pane, select the **WEBAPPS** server



4. In the center **WEBAPPS Home** pane, double-click **Server Certificates**


Connections
Start Page
WEBAPPS (CITY\Administrator)
Application Pools
Sites
Default Web Site
Filter:
Go
Show All
Group by:
No Grouping
Name
Issued To
Issued By
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

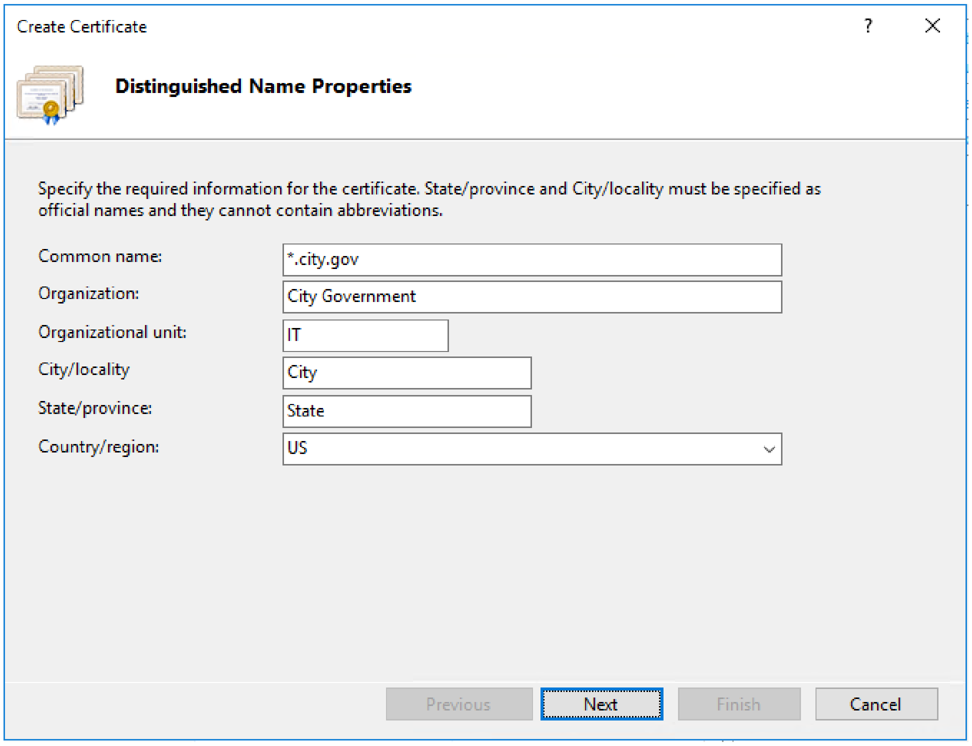
Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

5. In the right **Actions** menu, select **Create Domain Certificate…**

NOTE: It can take a few seconds for the Create Certificate wizard dialog to show

6. Enter the following information on the **Distinguished Name Properties** page then click Next



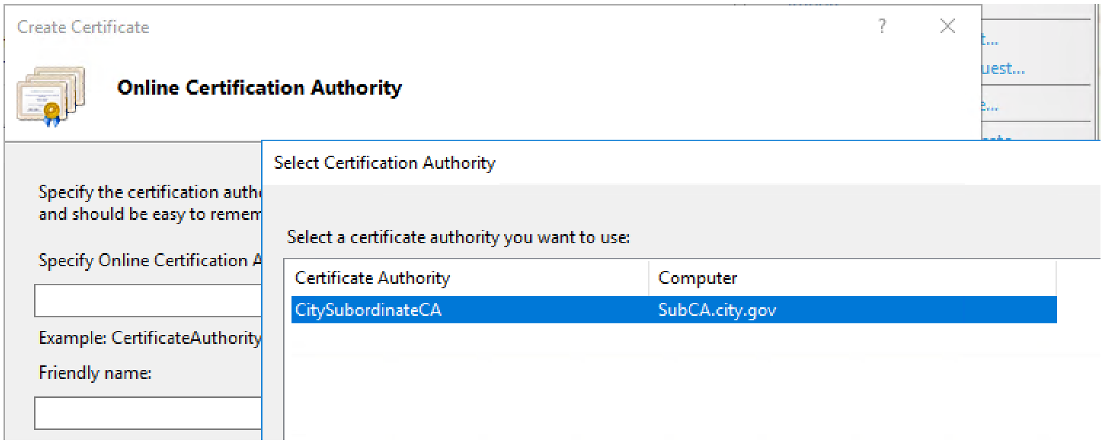
Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	*.city.gov
Organization:	City Government
Organizational unit:	IT
City/locality	City
State/province:	State
Country/region:	US

NOTE: We are requesting a wildcard certificate!

7. On the **Online Certification Authority** page, click **Select…** and choose the **CitySubordinateCA**



Create Certificate

Online Certification Authority

Specify the certification auth
and should be easy to remem

Specify Online Certification A

Example: CertificateAuthority

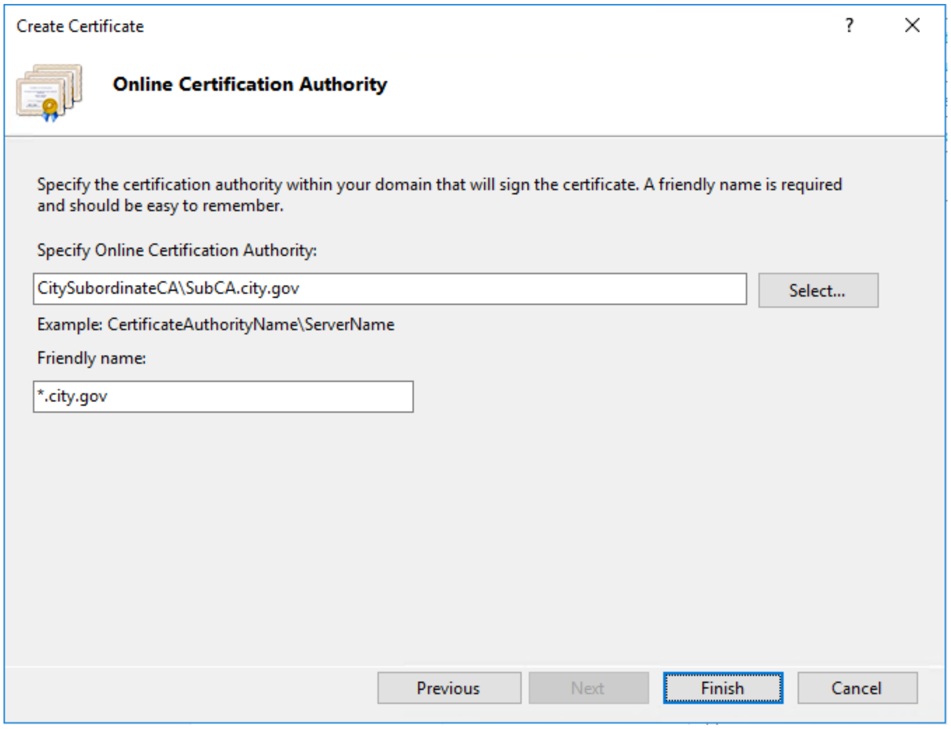
Friendly name:

Select Certification Authority

Select a certificate authority you want to use:

Certificate Authority	Computer
CitySubordinateCA	SubCA.city.gov

8. On the **Online Certification Authority** page, enter ***.city.gov** as the friendly name for the requested certificate



Create Certificate

Online Certification Authority

Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember.

Specify Online Certification Authority:

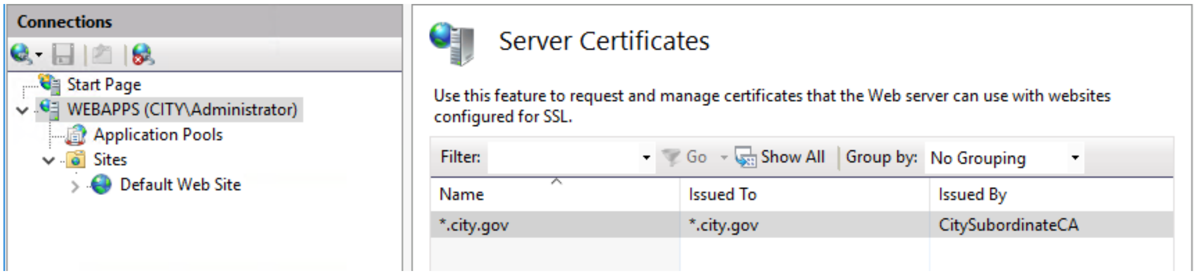
CitySubordinateCA\SubCA.city.gov

Example: CertificateAuthorityName\ServerName

Friendly name:

*.city.gov

9. Click Finish and wait for the certificate to be issued



Server Certificates

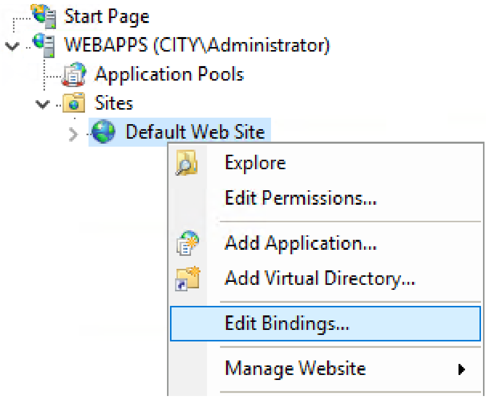
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Group by: No Grouping

Name	Issued To	Issued By
*.city.gov	*.city.gov	CitySubordinateCA

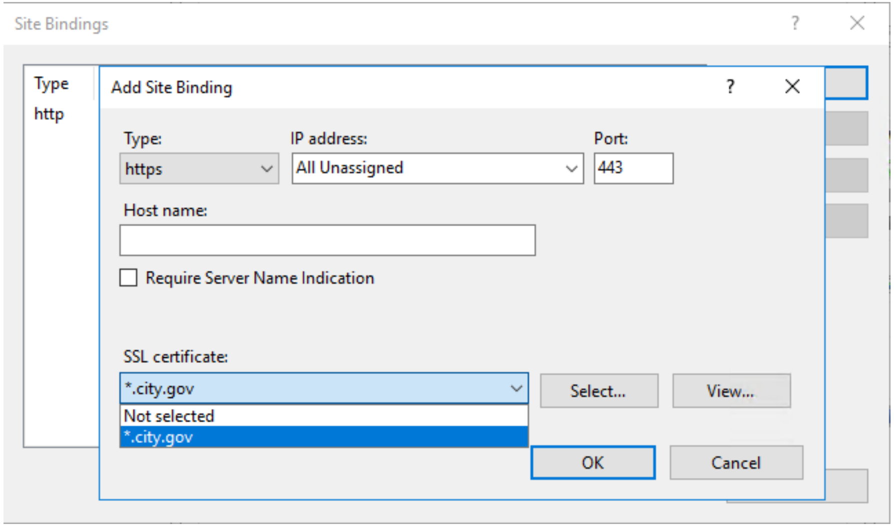
TIP: If the certificate request fails the first time, simply click Finish again to resubmit the request.

10. In the left navigation pane, right-click the **Default Web Site** and select **Edit Bindings…**



11. In the **Site Bindings** dialog, click Add…

12. In the **Add Site Binding** dialog select **https** from the Type dropdown and ***.city.gov** from the SSL certificate dropdown then click OK and click Close



Type: https

IP address: All Unassigned

Port: 443

Host name:

□ Require Server Name Indication

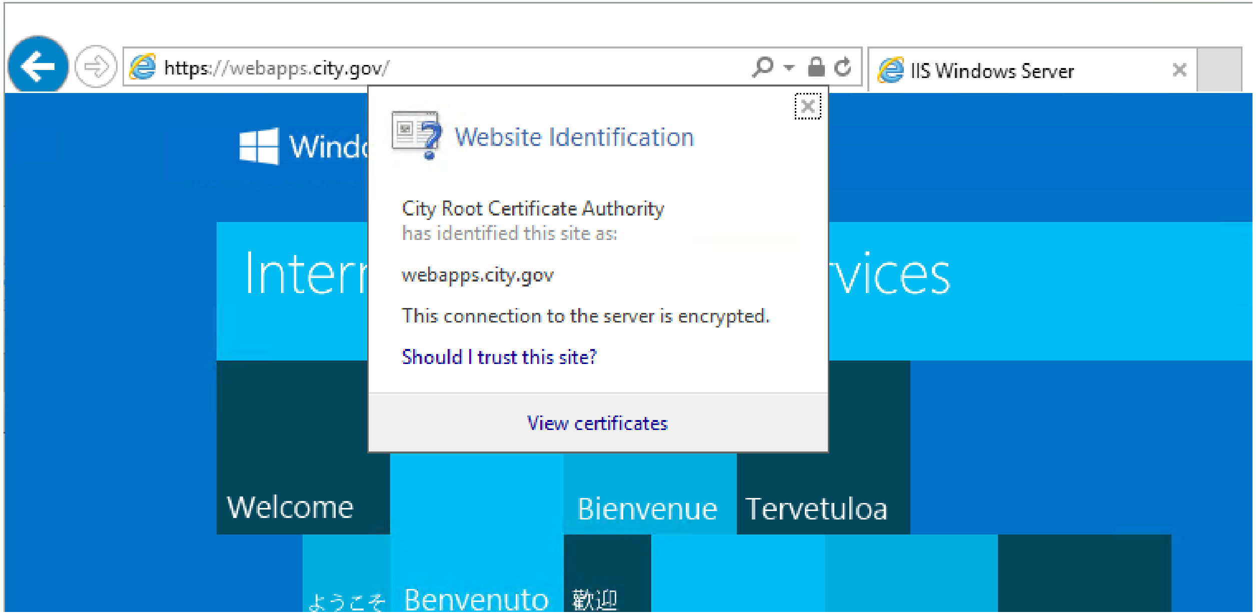
SSL certificate: *.city.gov

Workstation

Certificate Authority Administration – Client Testing of Valid Certificate

1. Start the windows 10 client virtual machine (**Workstation**) and login as the domain Administrator

2. Open **Internet Explorer** and browse to **https://webapps.city.gov** and verity that the site loads securely



City Root Certificate Authority
has identified this site as:

webapps.city.gov

This connection to the server is encrypted.

NOTE: You might need to force a group policy update to ensure the workstation trusts the root certificate

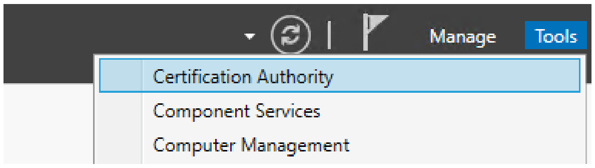
```
gpupdate /force
```

Subordinate CA

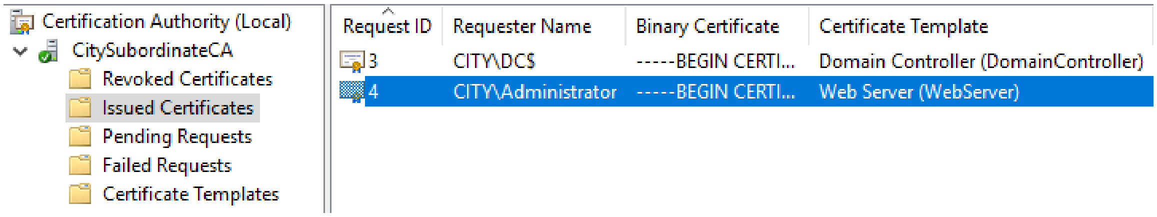
Certificate Authority Administration – Certficate Revocation

1. Open a Virtual Machine Connection to the subordinate CA (**SubCA**) and login as domain Administrator

2. Launch the **Certificate Authority** management console from the **Tools** menu in **Server Manager**

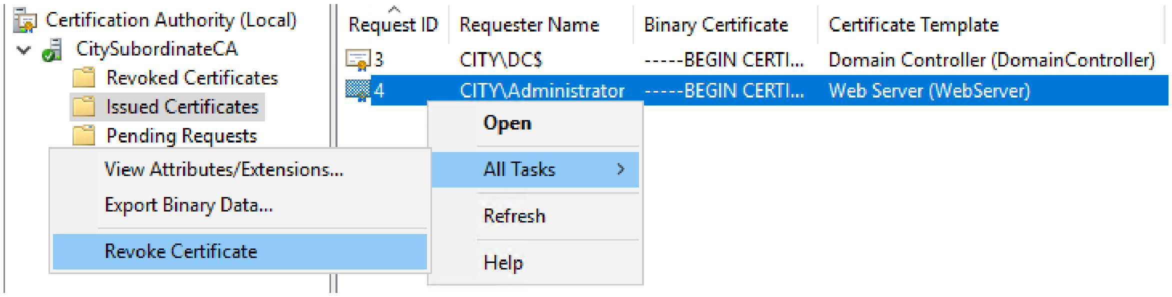


3. In the **Certificate Authority** management console, find the issued SSL certificate in the **Issued Certificates** node



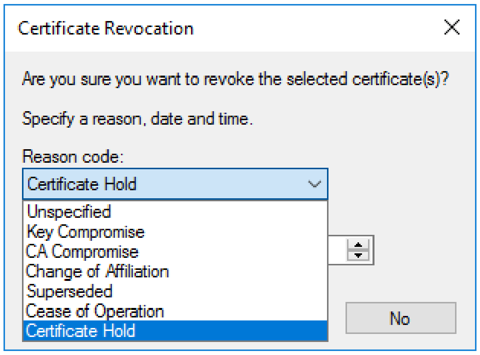
Request ID	Requester Name	Binary Certificate	Certificate Template
3	CITY\DC$	-----BEGIN CERTI...	Domain Controller (DomainController)
4	CITY\Administrator	-----BEGIN CERTI...	Web Server (WebServer)

4. Right-click the certificate and choose **Revoke Certificate** from the **All Tasks** menu



Request ID	Requester Name	Binary Certificate	Certificate Template
3	CITY\DC$	-----BEGIN CERTI...	Domain Controller (DomainController)
4	CITY\Administrator	-----BEGIN CERTI...	Web Server (WebServer)

5. In the **Certificate Revocation** dialog select **Certificate Hold** as the **Reason code** then click Yes


Certificate Revocation

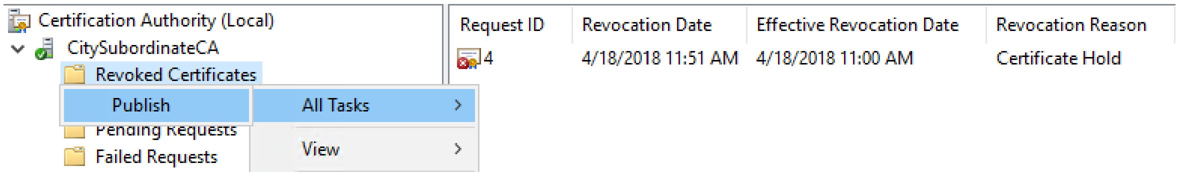
Are you sure you want to revoke the selected certificate(s)?

Specify a reason, date and time.

Reason code: Certificate Hold

NOTE: Certificate Hold is the **only** reversible revocation reason. All other revocations are permanent!

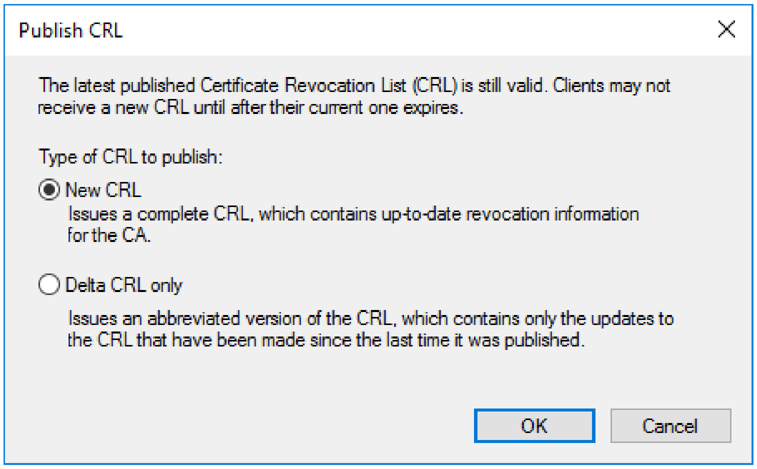
6. Right-click the **Revoked Certificates** node and select **Publish** from the **All Tasks** menu



Request ID	Revocation Date	Effective Revocation Date	Revocation Reason
4	4/18/2018 11:51 AM	4/18/2018 11:00 AM	Certificate Hold

NOTE: It can take about 15 seconds for the Publish CRL dialog to show

7. In the **Publish CRL** dialog, select **New CRL** and click OK



The latest published Certificate Revocation List (CRL) is still valid. Clients may not receive a new CRL until after their current one expires.

Type of CRL to publish:

● New CRL
Issues a complete CRL, which contains up-to-date revocation information for the CA.

○ Delta CRL only
Issues an abbreviated version of the CRL, which contains only the updates to the CRL that have been made since the last time it was published.

NOTE: It can take a few seconds before CRL publication finishes and the console is once again responsive

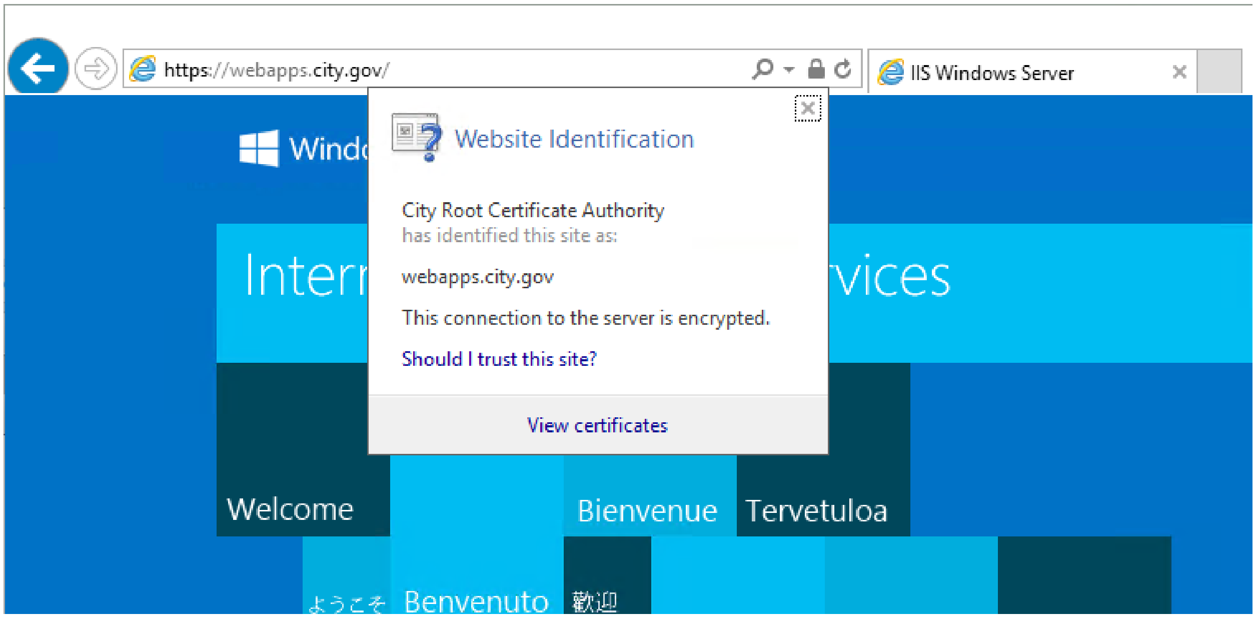
Workstation

Certificate Authority Administration – Client Testing of Revoked Certificate

1. Open a Virtual Machine Connection to the workstation VM (**Workstation**) and login as domain Administrator

2. Open **Internet Explorer** and browse to **https://webapps.city.gov**

   Notice whether the browser treats the revoked certificate as valid; in all likelihood the certificate will be treated as valid since the CRL was updated only moments ago and Windows has not yet retrieved the updates



Website Identification

City Root Certificate Authority
has identified this site as:

webapps.city.gov

This connection to the server is encrypted.

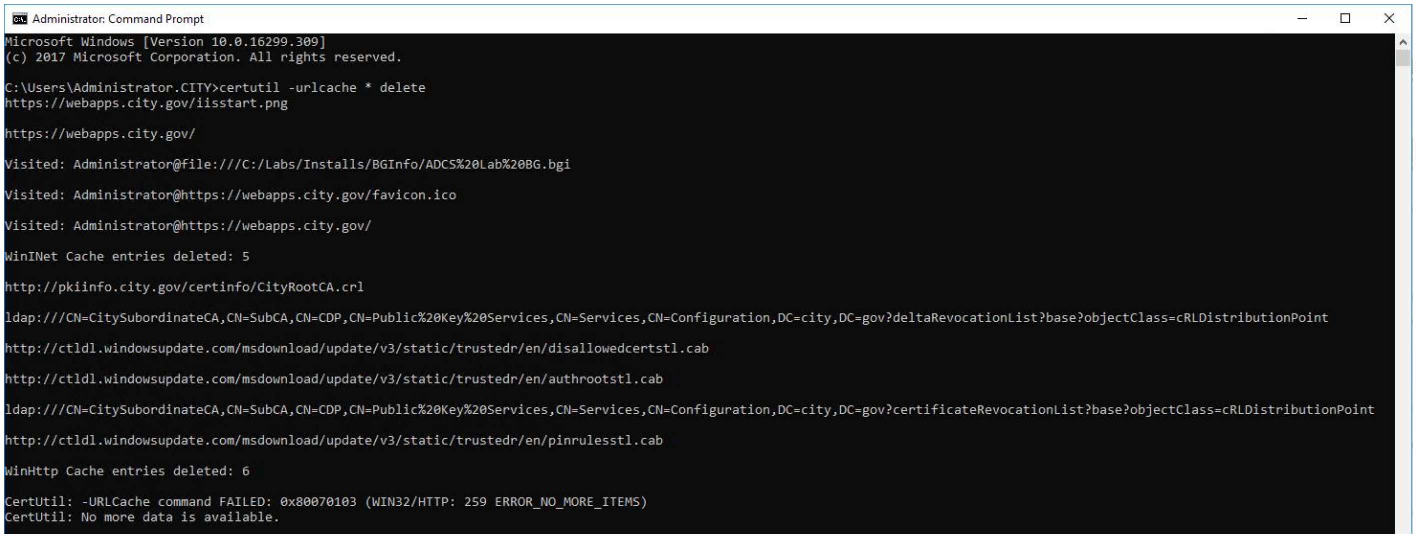
Should I trust this site?

NOTE: Windows and other software/infrastructure will cache CRLs and only periodically check for updates!

We will force windows to flush the CRL cache, which should cause IE to read the updated CRL

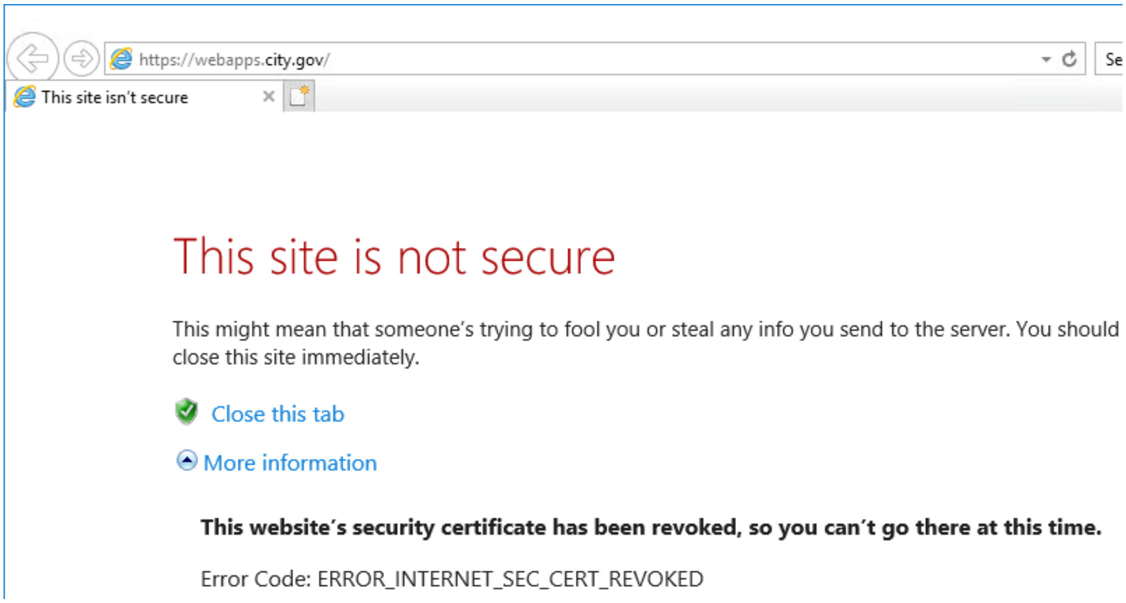
3. Start an administrative command prompt and run the following **certutil** command

   certutil -urlcache * delete



```
Microsoft Windows [Version 10.0.16299.309]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.CITY>certutil -urlcache * delete
https://webapps.city.gov/iisstart.png

https://webapps.city.gov/

Visited: Administrator@file:///C:/Labs/Installs/BGInfo/ADCS%20Lab%20BG.bgi

Visited: Administrator@https://webapps.city.gov/favicon.ico

Visited: Administrator@https://webapps.city.gov/

WinINet Cache entries deleted: 5

http://pkiinfo.city.gov/certinfo/CityRootCA.crl

ldap:///CN=CitySubordinateCA,CN=SubCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=city,DC=gov?deltaRevocationList?base?objectClass=cRLDistributionPoint

http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab

http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab

ldap:///CN=CitySubordinateCA,CN=SubCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=city,DC=gov?certificateRevocationList?base?objectClass=cRLDistributionPoint

http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab

WinHttp Cache entries deleted: 6

CertUtil: -URLCache command FAILED: 0x80070103 (WIN32/HTTP: 259 ERROR_NO_MORE_ITEMS)
CertUtil: No more data is available.
```

4. In **Internet Explorer** refresh the URL **https://webapps.city.gov** and verify that the certificate is rejected



This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Close this tab

More information

This website's security certificate has been revoked, so you can't go there at this time.

Error Code: ERROR_INTERNET_SEC_CERT_REVOKED

NOTE: There is no option to continue to the site, as in the case of an untrusted certificate chain

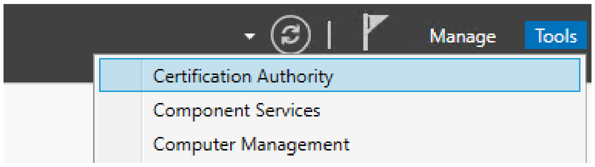
Subordinate CA

Certificate Authority Administration – Certificate UnRevocation

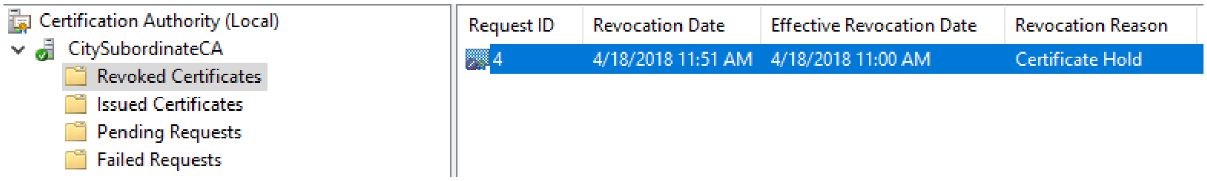
NOTE: Only certificates revoked with a Certificate Hold reason code can be reinstated and removed from the CRL

1. Open a Virtual Machine Connection to the subordinate CA (**SubCA**) and login as domain Administrator

2. Launch the **Certificate Authority** management console from the **Tools** menu in **Server Manager**

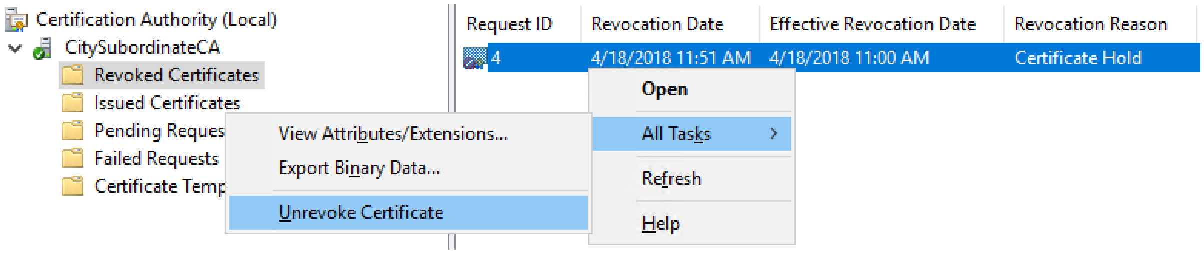


3. In the **Certificate Authority** console find the revoked SSL certificate in the **Revoked Certificates** node



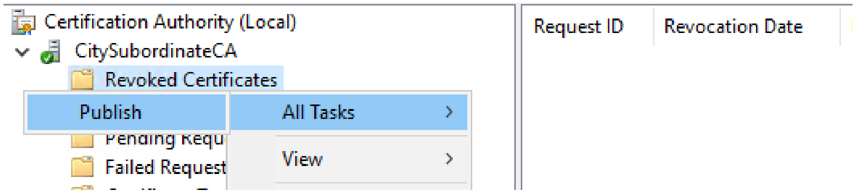
Request ID	Revocation Date	Effective Revocation Date	Revocation Reason
4	4/18/2018 11:51 AM	4/18/2018 11:00 AM	Certificate Hold

4. Right-click the certificate and choose **Revoke Certificate** from the **All Tasks** menu



Request ID	Revocation Date	Effective Revocation Date	Revocation Reason
4	4/18/2018 11:51 AM	4/18/2018 11:00 AM	Certificate Hold

5. Right-click the **Revoked Certificates** node and choose **Publish** from the **All Tasks** menu

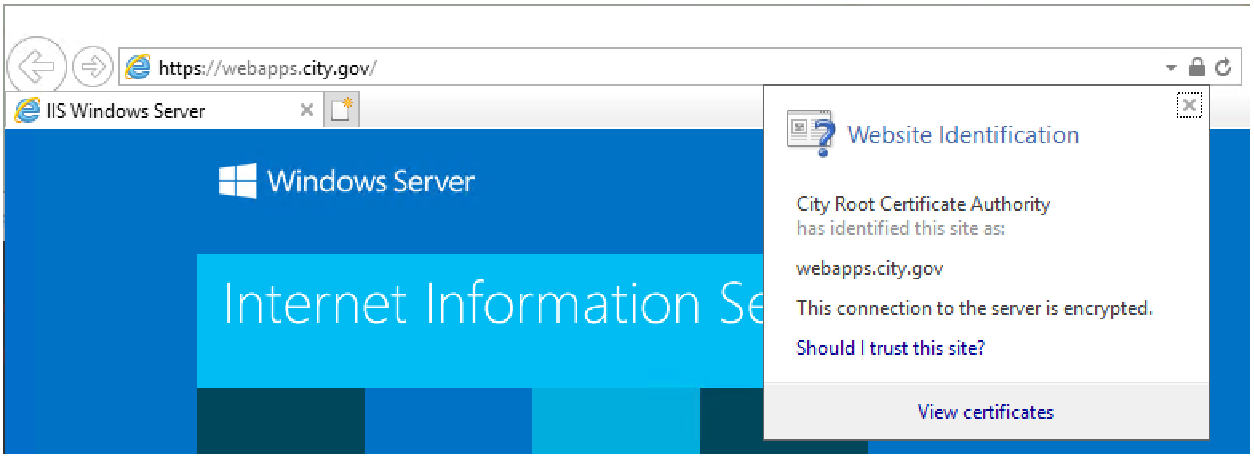


Workstation

Certificate Authority Administration – Client Testing of UnRevoked Certificate

1. Open a Virtual Machine Connection to the workstation VM (**Workstation**) and login as domain Administrator

2. Open **Internet Explorer** and browse to **https://webapps.city.gov** and verify the certificate is again accepted



Website Identification

City Root Certificate Authority
has identified this site as:

webapps.city.gov

This connection to the server is encrypted.

Should I trust this site?

View certificates

NOTE: You might once again need to clear the CRL cache before IE again recognizes the certificate as valid

```
certutil -urlcache * delete
```

Subordinate CA

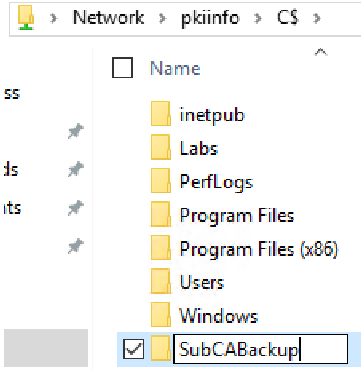
Certificate Authority Maintenance – Backing up a Certificate Authority

1. Open a Virtual Machine Connection to the subordinate CA (**SubCA**) and login as domain Administrator

2. Open **Windows Explorer** and browse to the administrative share for the C Drive on the PKI Info (**PkiInfo**) server

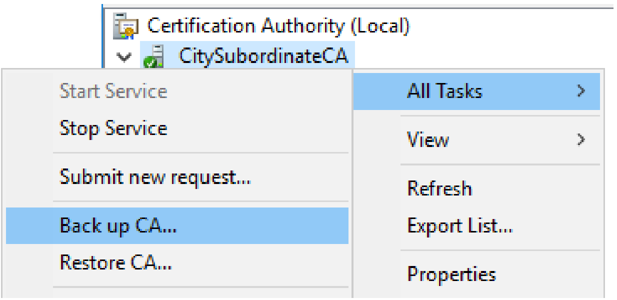
   \\pkiinfo\C$

3. Create a directory named **SubCABackup** which we will use as the backup storage location for this lab



4. Launch the **Certificate Authority** management console from the **Tools** menu in **Server Manager**

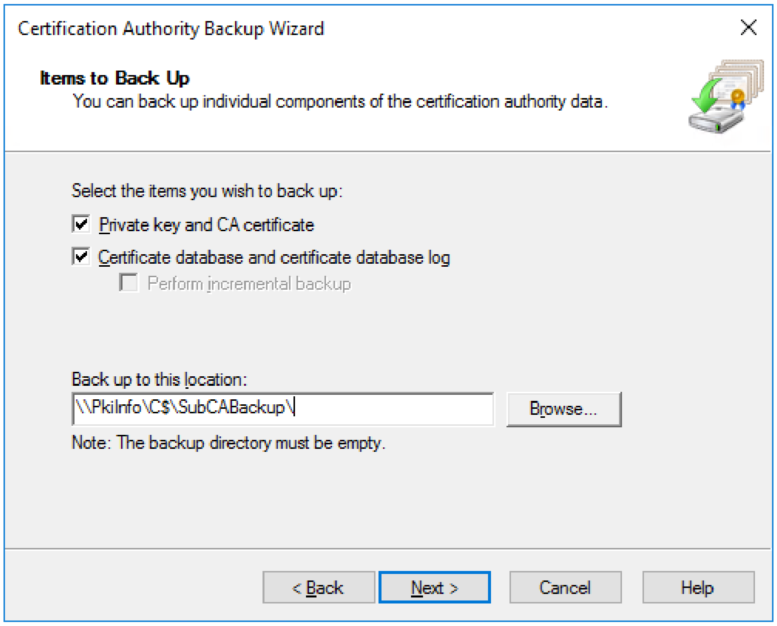
5. Right-click the **CitySubordinateCA** node and select **Back up CA…** from the **All Tasks** menu



6. On the **Certificate Authority Backup Wizard** dialog welcome screen click Next

7. On the **Items to Back Up** screen select the **Private key and CA certificate** and **Certificate database and certificate database log** options then enter the below path as the backup location and click Next

   \\pkiinfo\C$\SubCABackup



Certification Authority Backup Wizard

Items to Back Up

You can back up individual components of the certification authority data.

Select the items you wish to back up:

☑ Private key and CA certificate

☑ Certificate database and certificate database log

□ Perform incremental backup

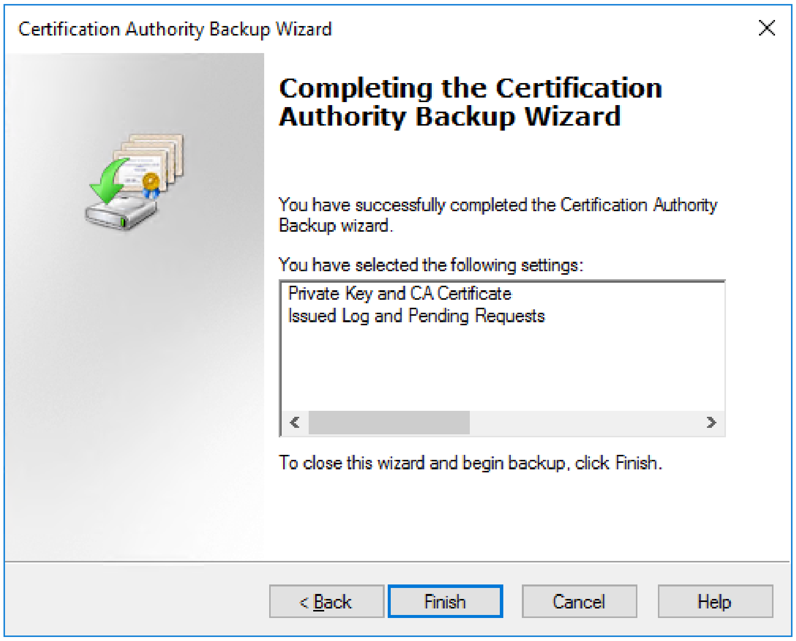
Back up to this location:

\\PkiInfo\C$\SubCABackup\

Note: The backup directory must be empty.

8. On the **Select a Password** screen we will use **pw** as the backup password for this lab

9. On the completion screen verify the items that will be backed up then click Finish



Certification Authority Backup Wizard

Completing the Certification Authority Backup Wizard

You have successfully completed the Certification Authority Backup wizard.

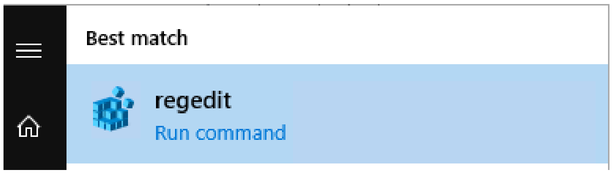
You have selected the following settings:

Private Key and CA Certificate
Issued Log and Pending Requests

To close this wizard and begin backup, click Finish.

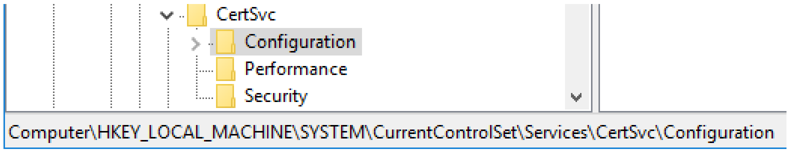
NOTE: We also need to backup the certificate services configuration in the windows registry

10. Run the Windows **Registry Editor**



11. Navigate to the following registry key

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration

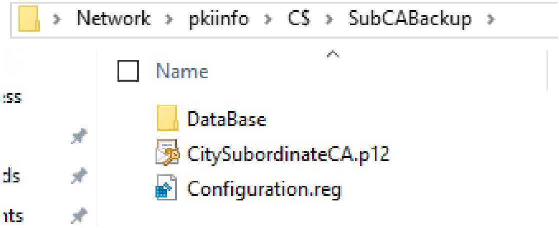


Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration

12. Export the CertSvc **Configuration** key to the backup location created in step #3

\\pkiinfo\C$\SubCABackup\Configuration.reg

13. Your backup directory should have three items; the CA database, the CA key and the CA registry configuration



› Network › pkiinfo › C$ › SubCABackup ›

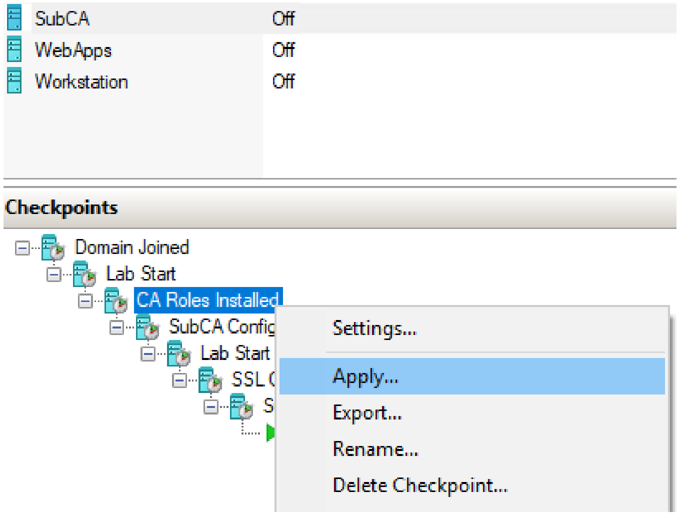
DataBase
CitySubordinateCA.p12
Configuration.reg

Subordinate CA

Certificate Authority Maintenance – Restoring a Backed Up Certificate Authority

1. Open Hyper-V Manager and **shutdown** the Subordinate CA (**SubCA**) virtual machine

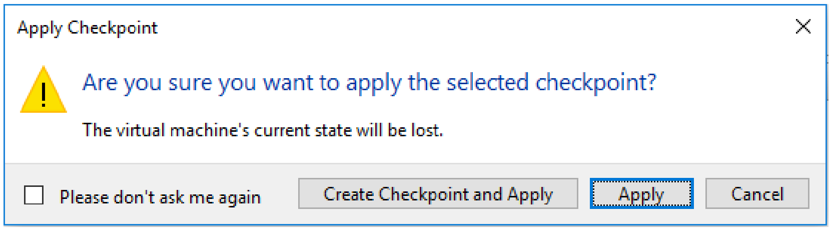
2. **Apply** the **CA Roles Installed** checkpoint on the Subordinate CA (**SubCA**) virtual machine



SubCA	Off
WebApps	Off
Workstation	Off

Checkpoints

```
Domain Joined
  Lab Start
    CA Roles Installed
      SubCA Config
        Lab Start
          SSL (
            S
```



Apply Checkpoint

Are you sure you want to apply the selected checkpoint?

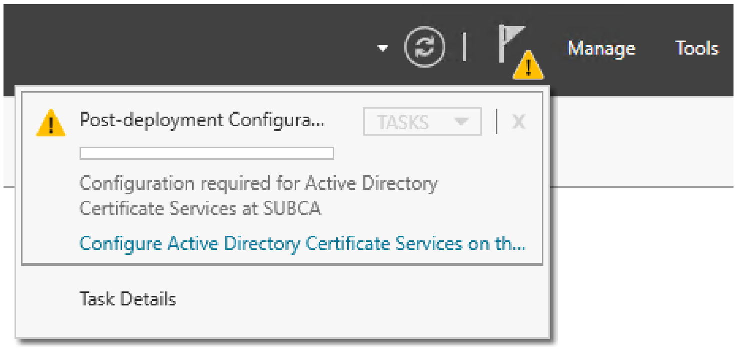
The virtual machine's current state will be lost.

NOTE: The Subordinate CA (**SubCA**) is now in a clean state with the CA Roles installed but **not** configured

When restoring a CA in production ensure that:
> the computer name is the same as the original CA
> the IP address is the same as the original CA (use static or DHCP reserved IP addresses for your CA servers)

3. Start the Subordinate CA (**SubCA**) and login as domain Administrator

4. Start **Server Manager** open the notifications in the top right menu bar



Post-deployment Configura...

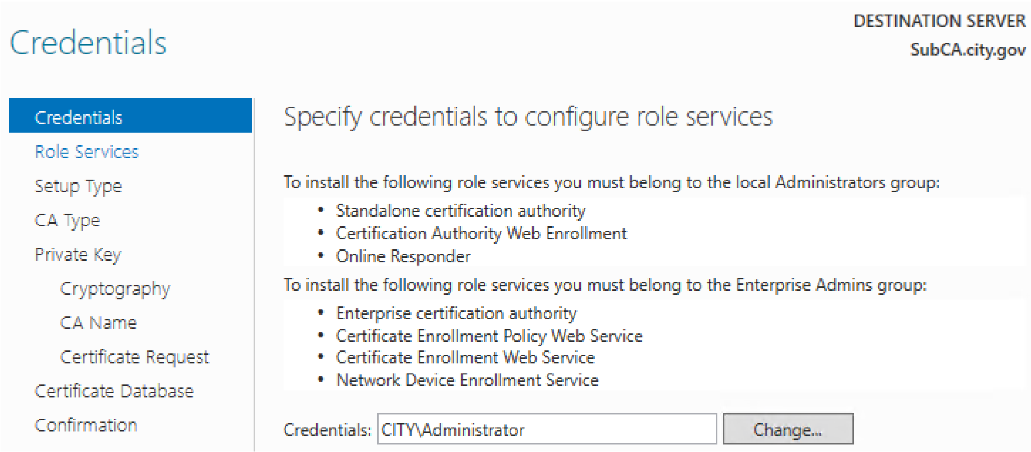
Configuration required for Active Directory Certificate Services at SUBCA

Configure Active Directory Certificate Services on th...

Task Details

5. In the **Post-deployment Configuration** notification, click the **Configure Active Directory Certificate Services on the destination server** link

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



Credentials

DESTINATION SERVER
SubCA.city.gov

Specify credentials to configure role services

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

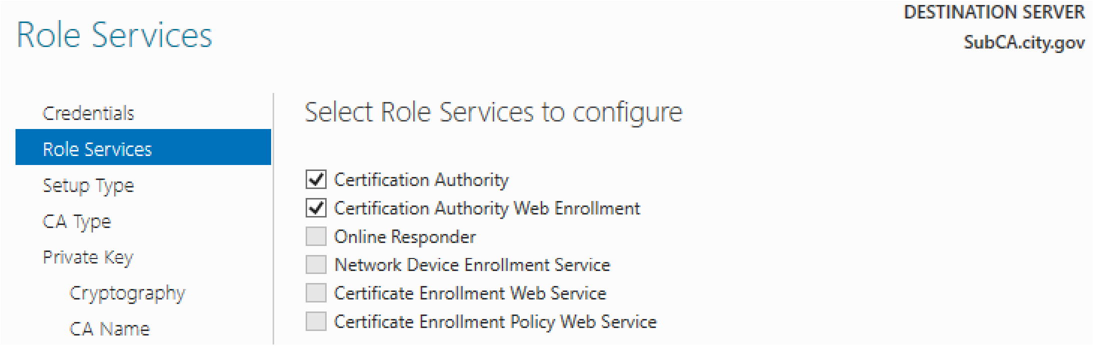
- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

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: CITY\Administrator

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



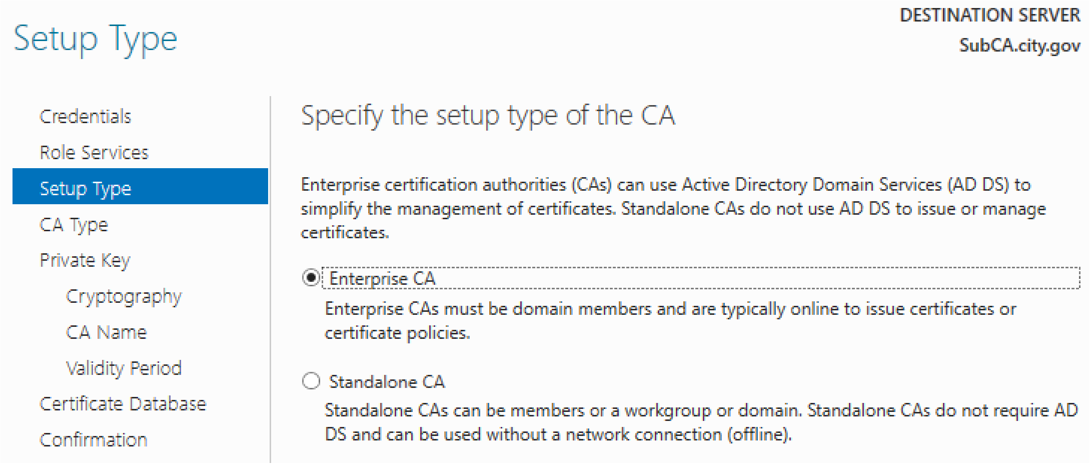
Role Services

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

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



Setup Type

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.

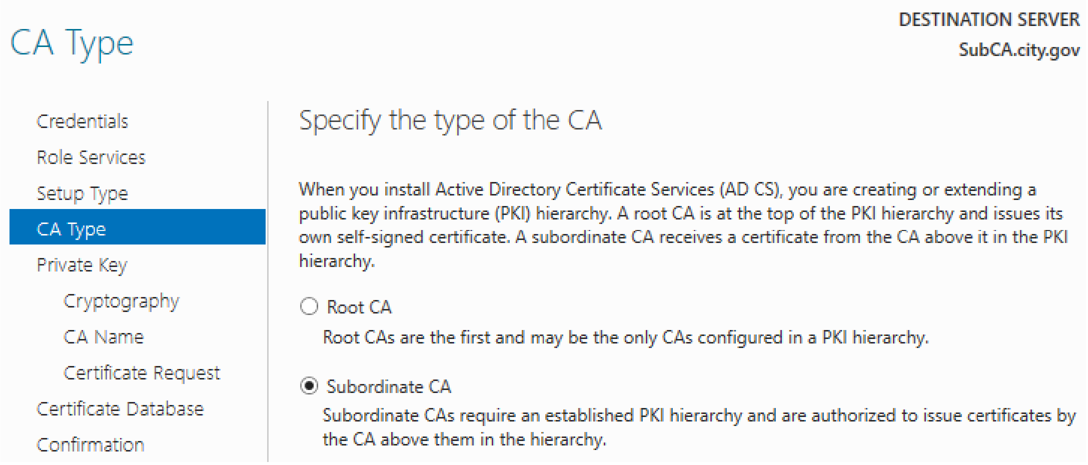
● Enterprise CA

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

○ Standalone CA

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

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



CA Type

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.

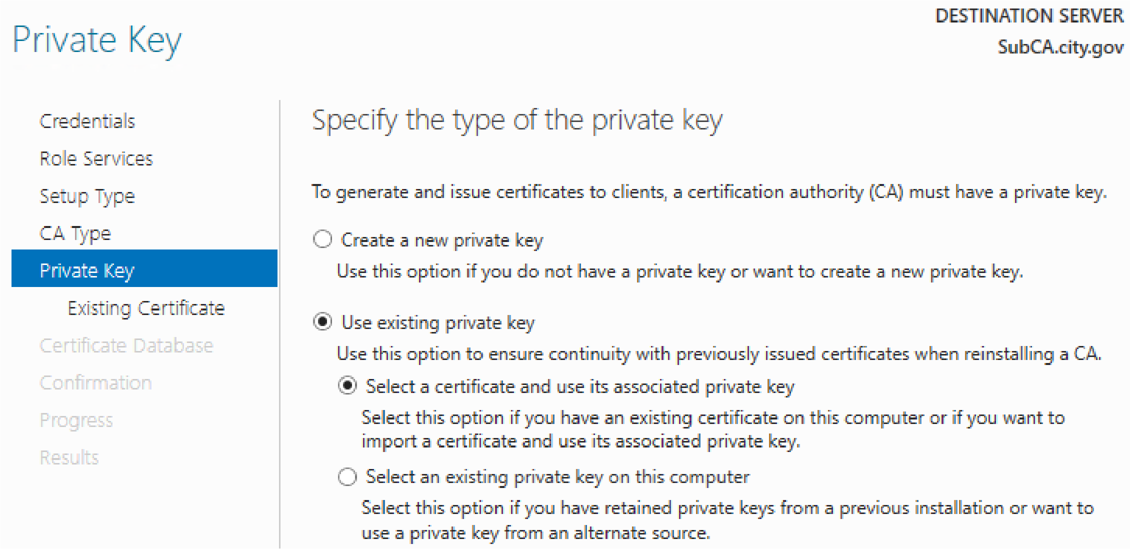
○ Root CA

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.

10. On the **Private Key** screen select **Use existing private key** and **Select a certificate and use its associated private key** then click Next



Private Key

DESTINATION SERVER
SubCA.city.gov

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.

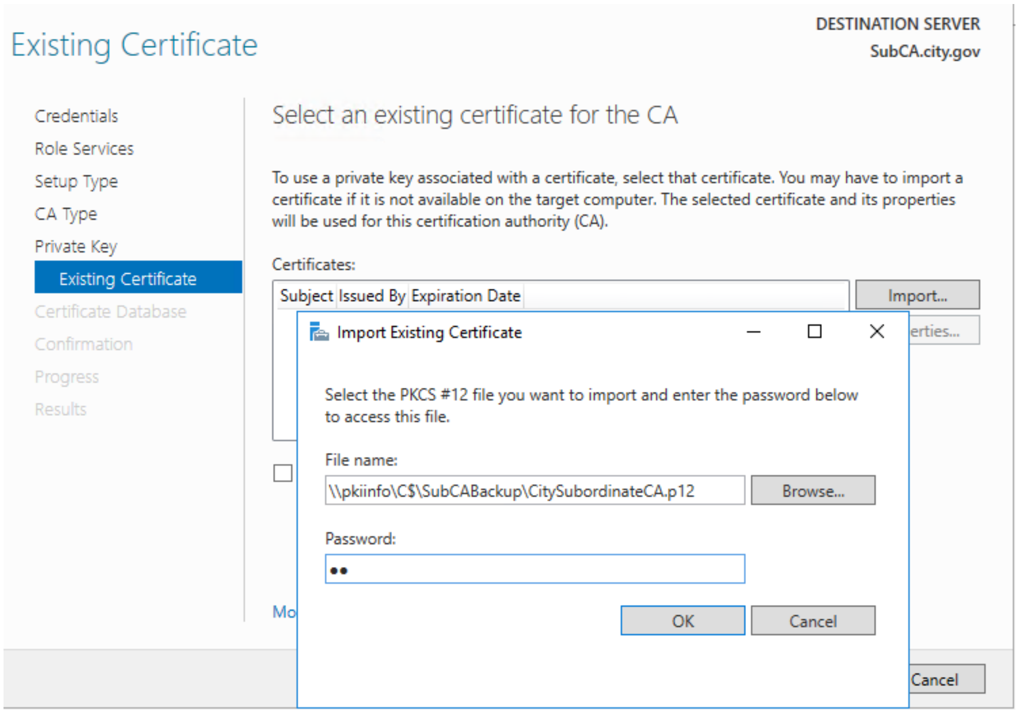
○ Select an existing private key on this computer

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

11. On the **Existing Certificate** screen click **Import…** then **Browse…** to select the backed-up CA certificate

\\pkiinfo\C$\SubCABackup\CitySubordinateCA.p12

Enter **pw** in the **Password** field then click OK



Existing Certificate

DESTINATION SERVER
SubCA.city.gov

Select an existing certificate for the CA

To use a private key associated with a certificate, select that certificate. You may have to import a certificate if it is not available on the target computer. The selected certificate and its properties will be used for this certification authority (CA).

Certificates:

Subject	Issued By	Expiration Date

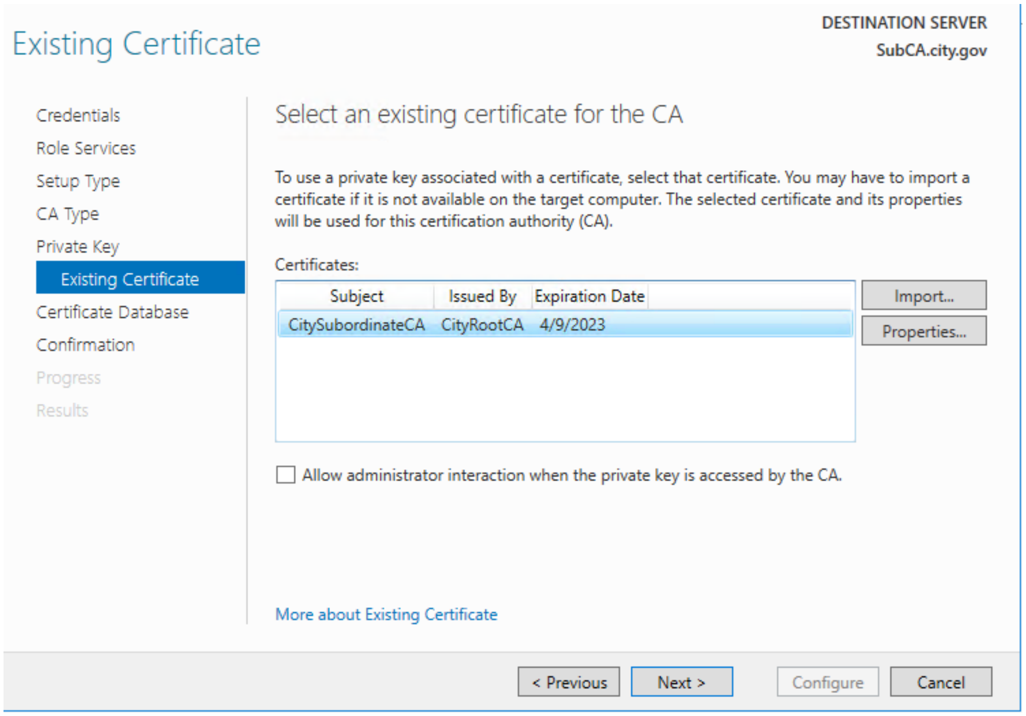
Import Existing Certificate

Select the PKCS #12 file you want to import and enter the password below to access this file.

File name: \\pkiinfo\C$\SubCABackup\CitySubordinateCA.p12

Password: ••

12. Wait for the certificate to import then select it from the **Certificates** list, then click Next



Existing Certificate

DESTINATION SERVER
SubCA.city.gov

Select an existing certificate for the CA

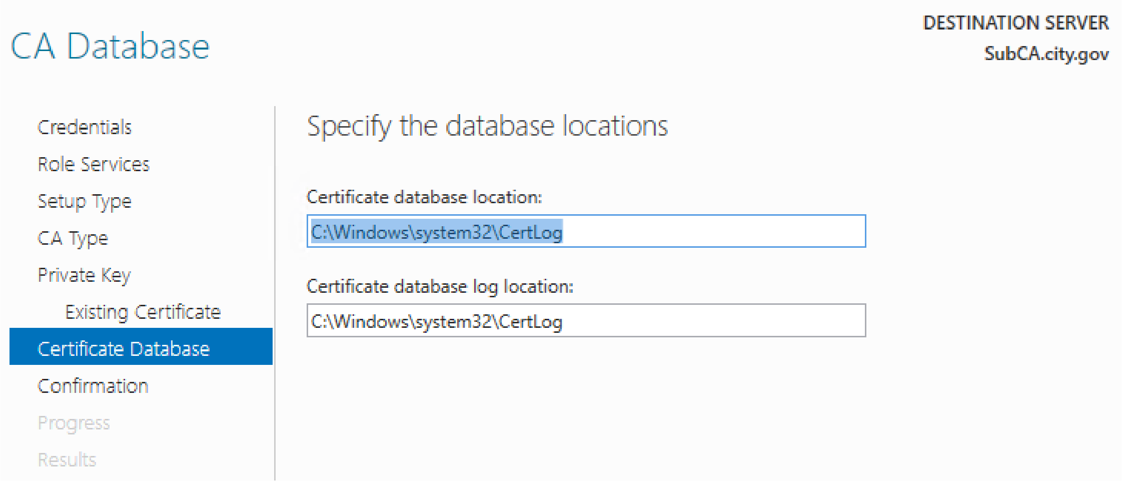
To use a private key associated with a certificate, select that certificate. You may have to import a certificate if it is not available on the target computer. The selected certificate and its properties will be used for this certification authority (CA).

Certificates:

Subject	Issued By	Expiration Date
CitySubordinateCA	CityRootCA	4/9/2023

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

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



CA Database

DESTINATION SERVER
SubCA.city.gov

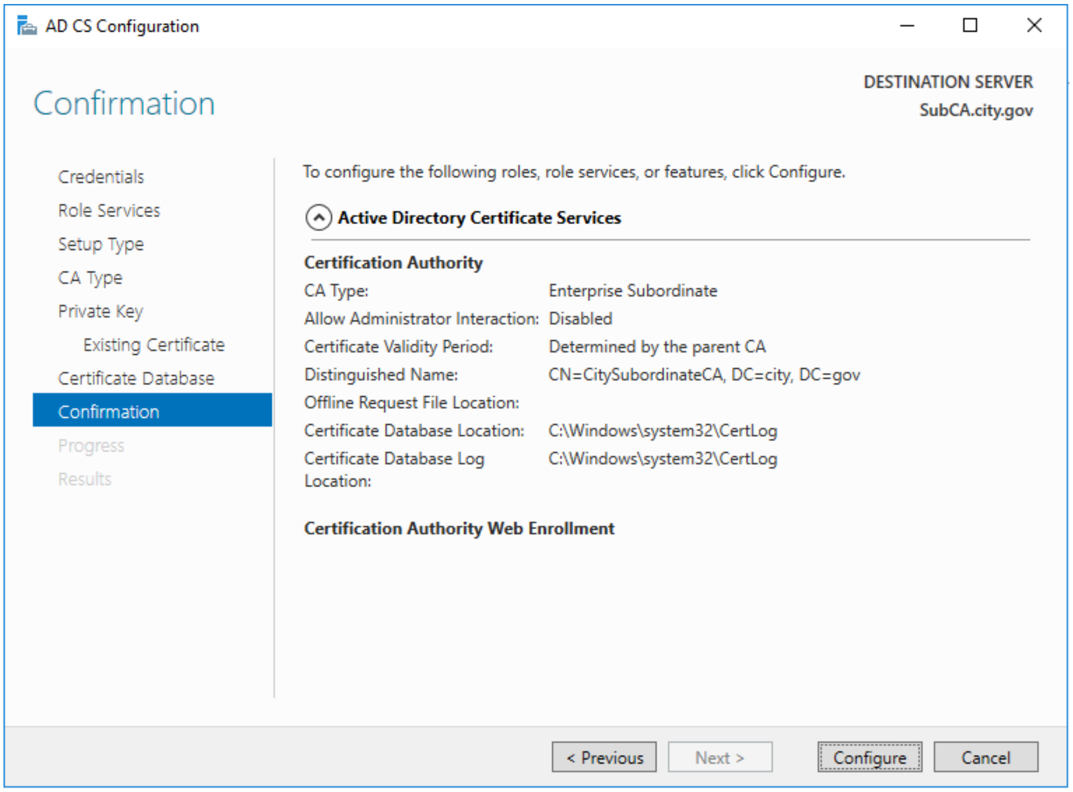
Specify the database locations

Certificate database location: C:\Windows\system32\CertLog

Certificate database log location: C:\Windows\system32\CertLog

NOTE: These values should consistent with the values on original CA at the time of backup. You can verify the original values from the exported registry configuration

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



Confirmation

DESTINATION SERVER
SubCA.city.gov

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

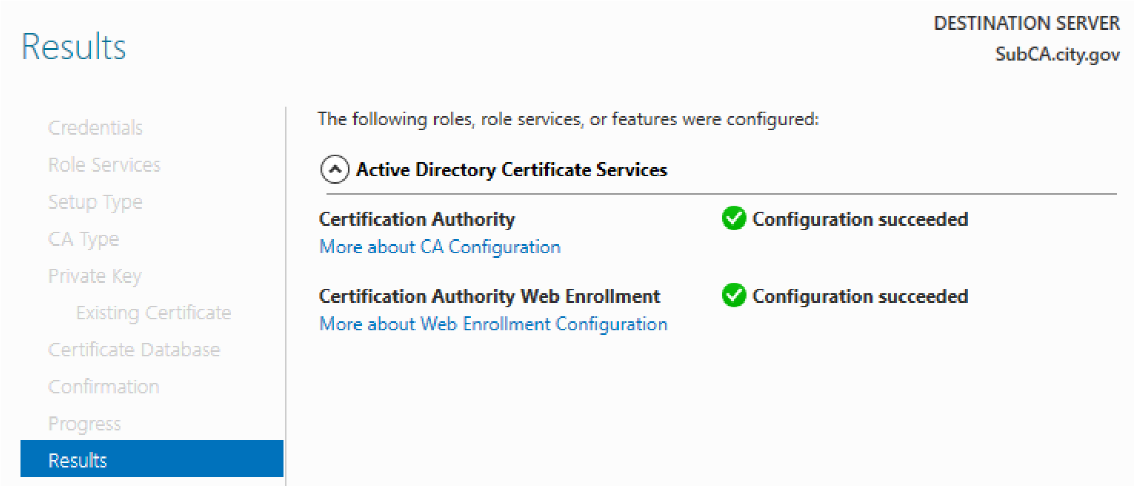
Active Directory Certificate Services

Certification Authority

CA Type: Enterprise Subordinate
Allow Administrator Interaction: Disabled
Certificate Validity Period: Determined by the parent CA
Distinguished Name: CN=CitySubordinateCA, DC=city, DC=gov
Offline Request File Location:
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog

Certification Authority Web Enrollment

15. In the Results screen, verify that all CA roles were successfully configured then click Close



Results

DESTINATION SERVER
SubCA.city.gov

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

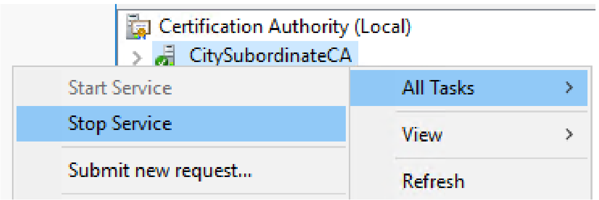
Active Directory Certificate Services

Certification Authority ✓ **Configuration succeeded**
More about CA Configuration

Certification Authority Web Enrollment ✓ **Configuration succeeded**
More about Web Enrollment Configuration

16. Launch the **Certificate Authority** management console from the **Tools** menu in **Server Manager**

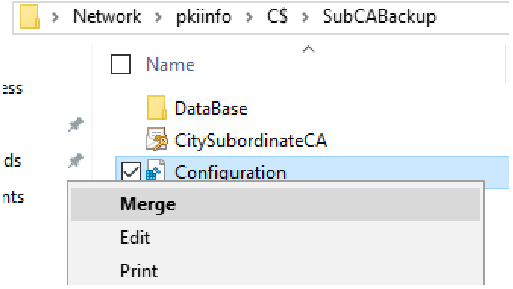
17. Right-click the **CitySubordinateCA** node and select **Stop Service** from the **All Tasks** menu



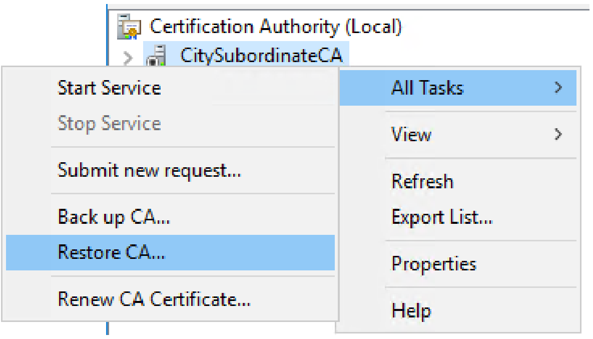
18. Open Windows Explorer and browse to the backup location

\\pkiinfo\C$\SubCABackup

19. Right-click the **Configuration.reg** file and select **Merge**; accept any warnings and click Yes apply registry changes



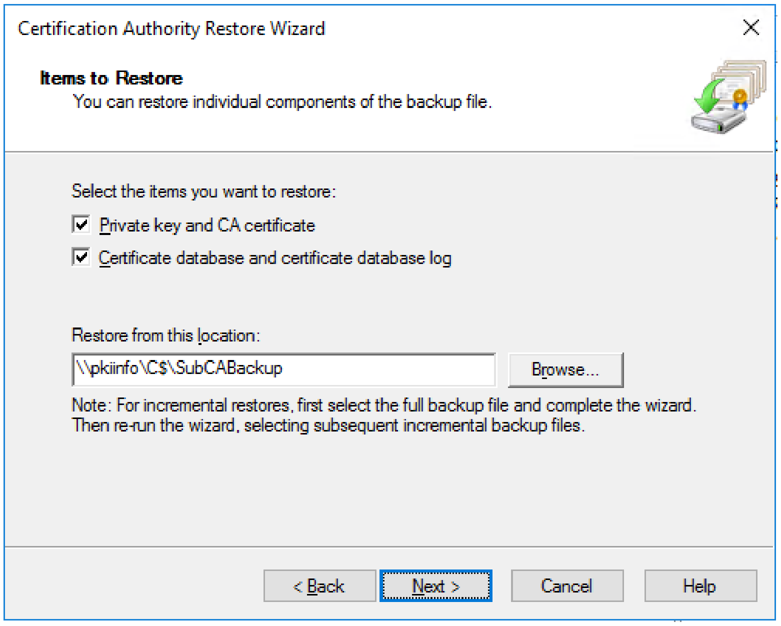
20. In the **Certificate Authority** management console, right-click the **CitySubordinateCA** node and select **Restore CA…** from the **All Tasks** menu



21. Click Next on the Certificate Authority Restore Wizard welcome screen

22. On the **Items to Restore** screen, select the **Private key and CA certificate** and **Certificate database and certificate database log** options, then enter the backup location and click Next

\\pkiinfo\C$\SubCABackup



Certification Authority Restore Wizard

Items to Restore
You can restore individual components of the backup file.

Select the items you want to restore:

☑ Private key and CA certificate

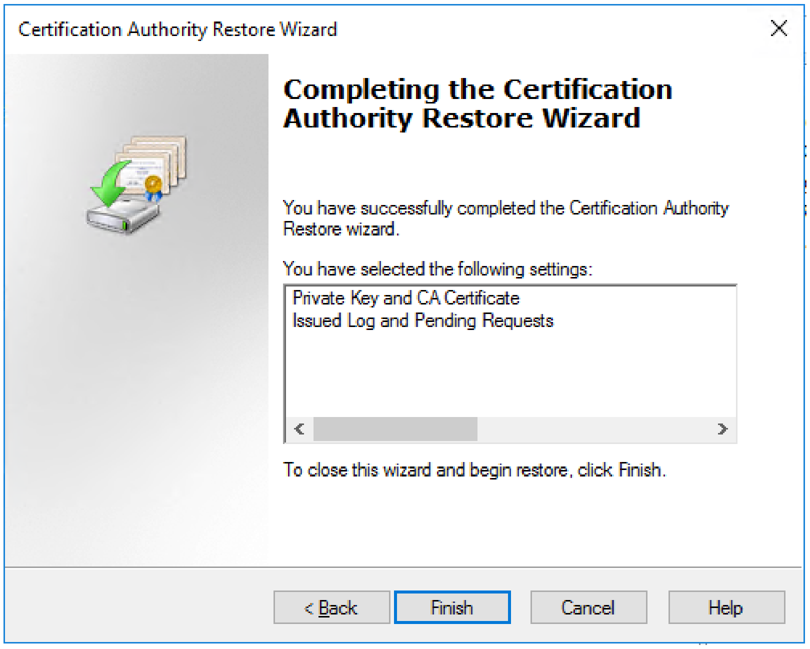
☑ Certificate database and certificate database log

Restore from this location:
\\pkiinfo\C$\SubCABackup

Note: For incremental restores, first select the full backup file and complete the wizard. Then re-run the wizard, selecting subsequent incremental backup files.

23. On the **Provide Password** screen enter **pw** in the **Password** field and click Next

24. Review the items that will be restored then click Finish



Certification Authority Restore Wizard

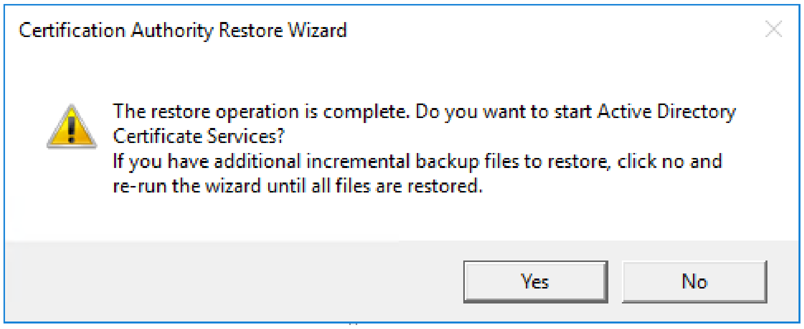
Completing the Certification Authority Restore Wizard

You have successfully completed the Certification Authority Restore wizard.

You have selected the following settings:
Private Key and CA Certificate
Issued Log and Pending Requests

To close this wizard and begin restore, click Finish.

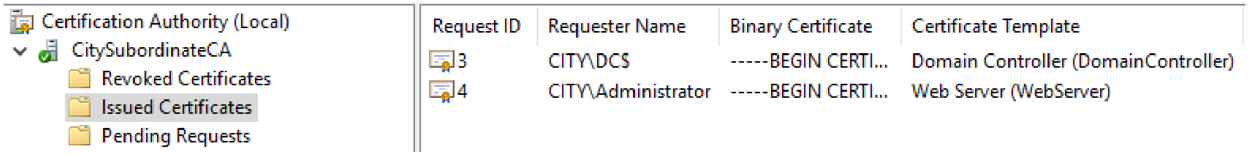
25. Wait for the restoration to complete then click Yes in the **Certification Authority Restore Wizard** dialog



Certification Authority Restore Wizard

The restore operation is complete. Do you want to start Active Directory Certificate Services?
If you have additional incremental backup files to restore, click no and re-run the wizard until all files are restored.

NOTE: You have successfully restored a CA from backup. You can verify that all previously issued/revoked certificates are properly shown in the Certificate Authority console



Certification Authority (Local)
CitySubordinateCA
Revoked Certificates
Issued Certificates
Pending Requests

Request ID	Requester Name	Binary Certificate	Certificate Template
3	CITY\DC$	-----BEGIN CERTI...	Domain Controller (DomainController)
4	CITY\Administrator	-----BEGIN CERTI...	Web Server (WebServer)