SYBEROFFENSE

Lab - Installing Certificate Services

Overview

In this lab, you will learn to configure certificate services for Server 2012 r2. Certificate Services, a service running on a Windows server operating system, receives requests for new digital certificates over transports such as RPC or HTTP. It checks each request against custom or site-specific policies, sets optional properties for a certificate to be issued, and issues the certificate. Certificate Services allows administrators to add elements to a certificate revocation list (CRL), and to publish signed CRLs on a regular basis.

Lab configuration

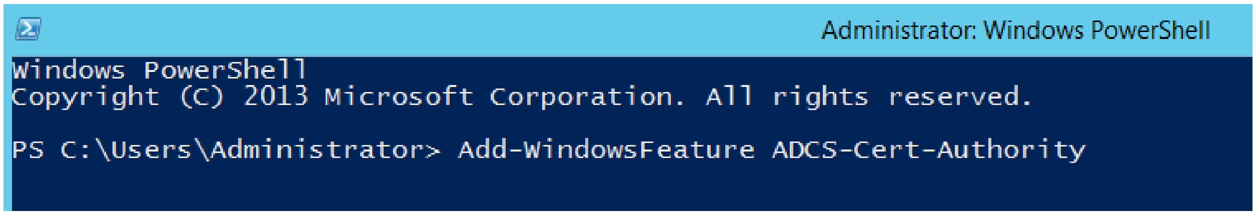
- Clean virtual install of Server 2012
- Server joined to the existing domain.
- IIS installed

Instructions

Installing an Enterprise Certificate of Authority

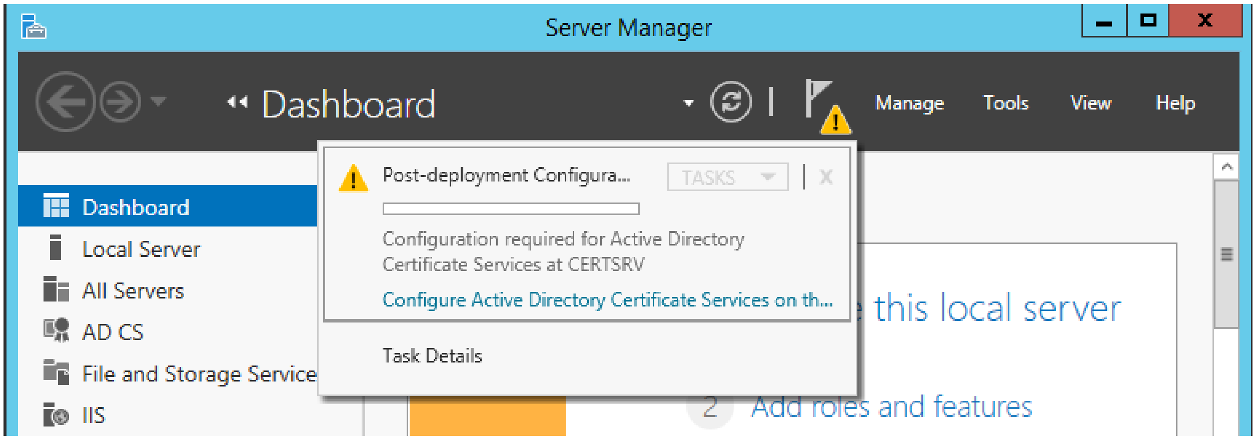
Open PowerShell and type in the following command:

```
Add-WindowsFeature ADCS-Cert-Authority
```



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-WindowsFeature ADCS-Cert-Authority
```

Once the installation has completed successfully, open Server Manager and click on the information warning for Configure Certificate Services on the destination server. This same link is available from the installation page of the wizard.



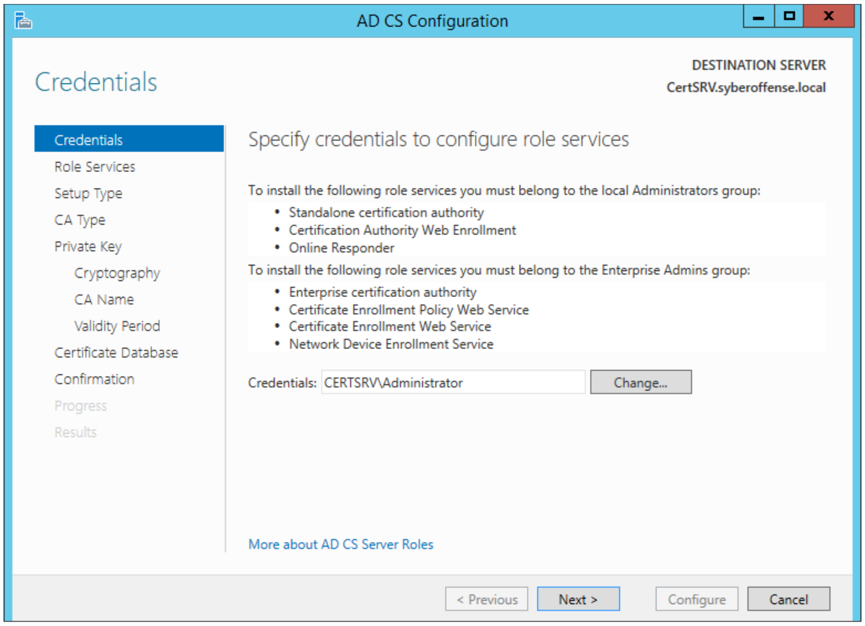
Post-deployment Configura...

Configuration required for Active Directory Certificate Services at CERTSRV

Configure Active Directory Certificate Services on th...

Task Details

On the Credentials page, change your credentials to that of your domain administrator account. Next.



Credentials

DESTINATION SERVER
CertSRV.syberoffense.local

Specify credentials to configure role services

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

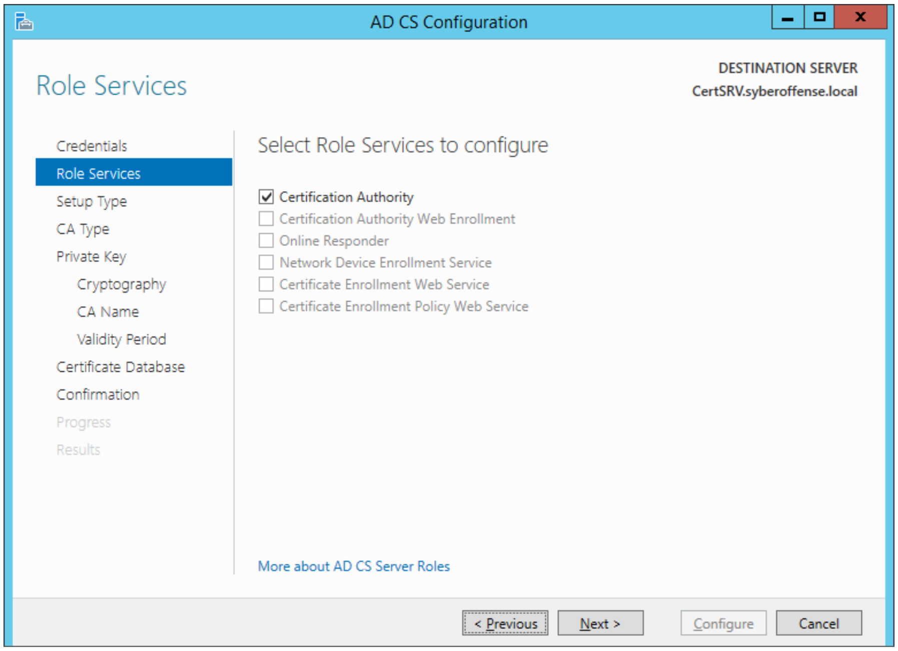
- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

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: CERTSRV\Administrator

On the Select role, services to configure page, click to select Certificate Authority and click Next.



Role Services

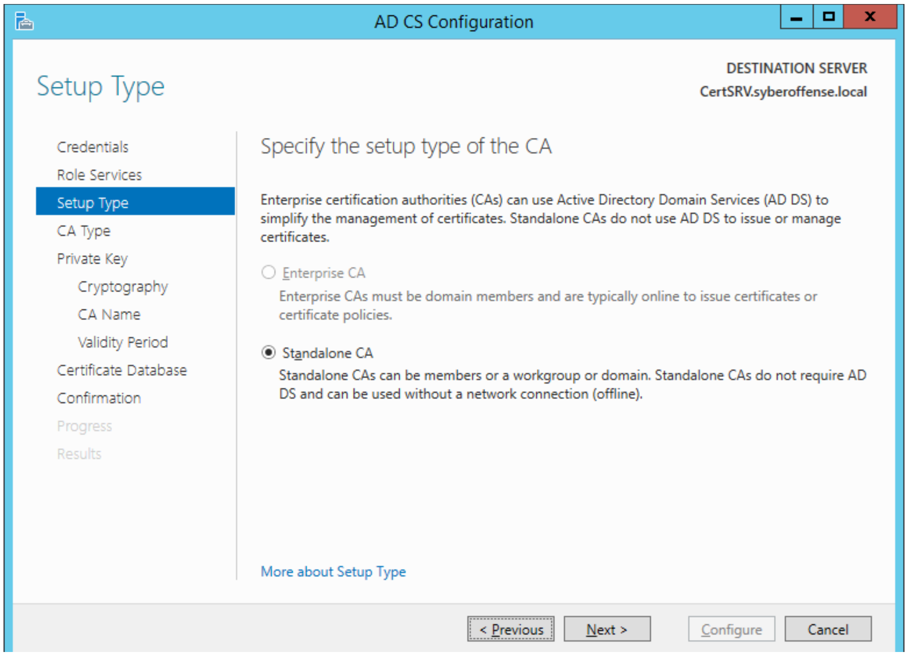
DESTINATION SERVER
CertSRV.syberoffense.local

Select Role Services to configure

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

More about AD CS Server Roles

On the Setup Type page, ensure that Standalone CA is selected and click Next.



Setup Type

DESTINATION SERVER
CertSRV.syberoffense.local

Specify the setup type of the CA

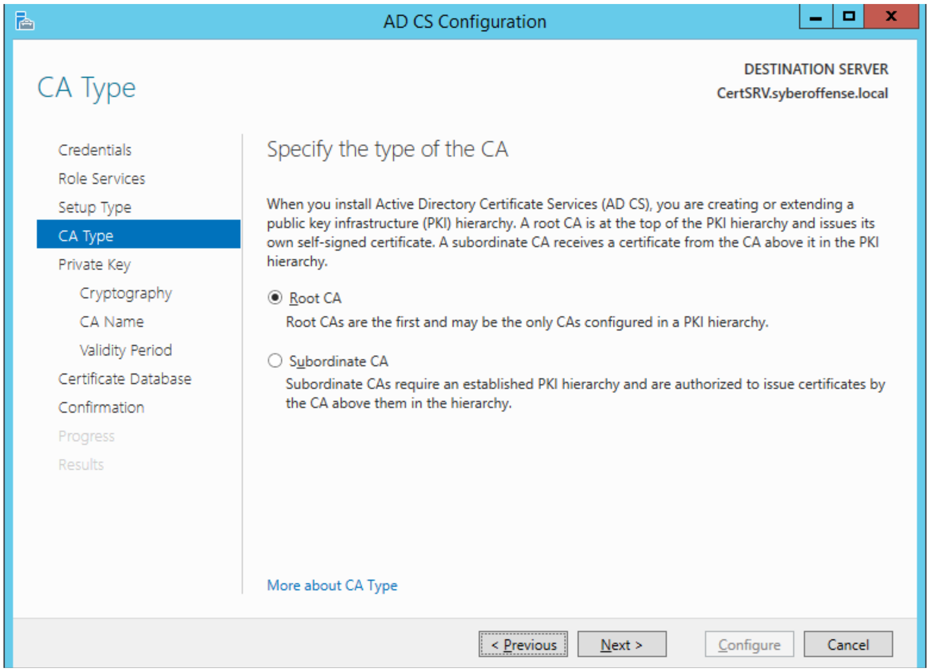
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

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

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

More about Setup Type

On the CA Type page, ensure that Root CA is selected and click Next.



CA Type

DESTINATION SERVER
CertSRV.syberoffense.local

Specify the type of the CA

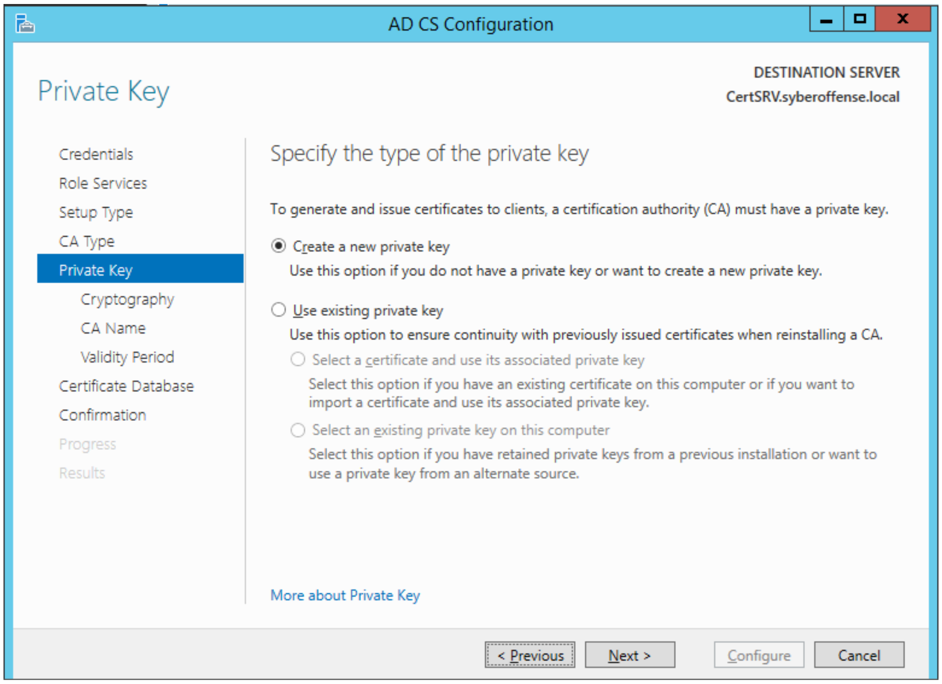
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

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

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

More about CA Type

On the Private Key page, click to select Create a new Private key and click Next.



Private Key

DESTINATION SERVER
CertSRV.syberoffense.local

Specify the type of the private key

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

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

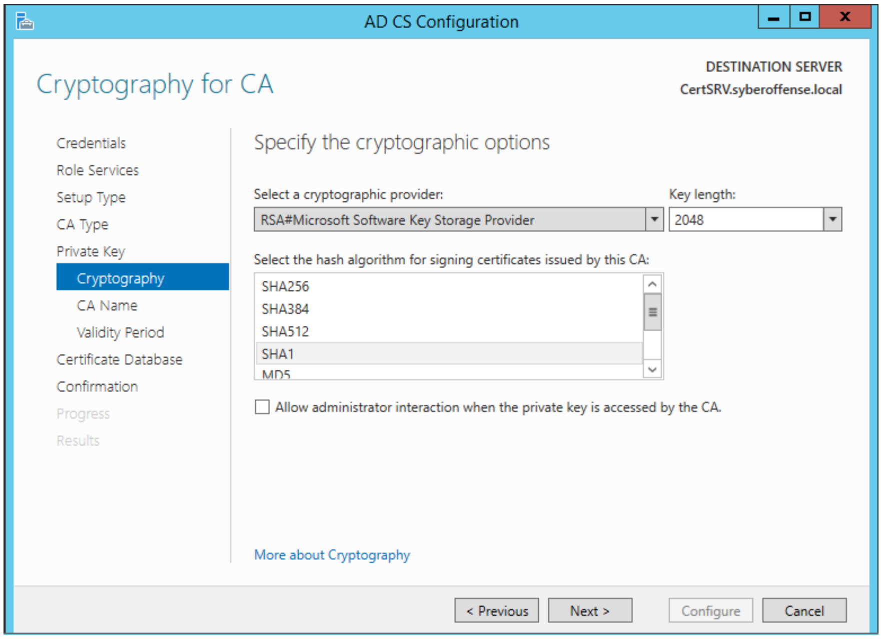
○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

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

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

More about Private Key

On the Cryptography for CA page, leave the key length to 20148 and click Next.



AD CS Configuration

Cryptography for CA

DESTINATION SERVER
CertSRV.syberoffense.local

Specify the cryptographic options

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

Key length: 2048

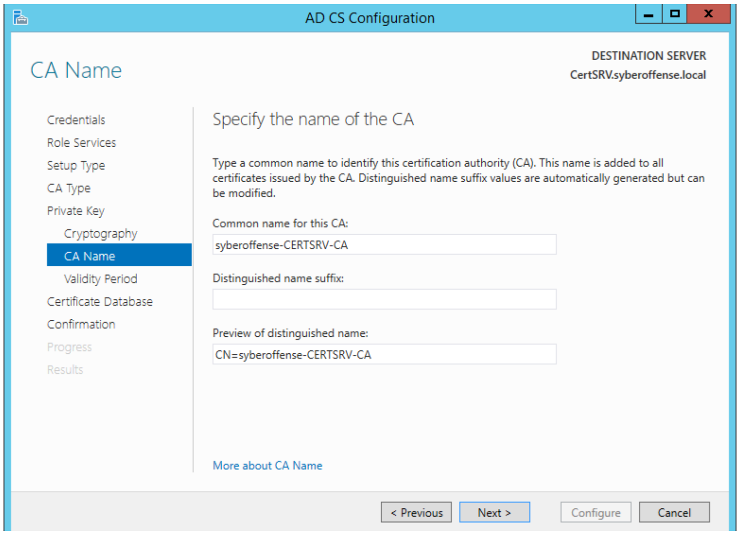
Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

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

More about Cryptography

On the CA Name page, accept the default name and click Next.



AD CS Configuration

CA Name

DESTINATION SERVER
CertSRV.syberoffense.local

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.

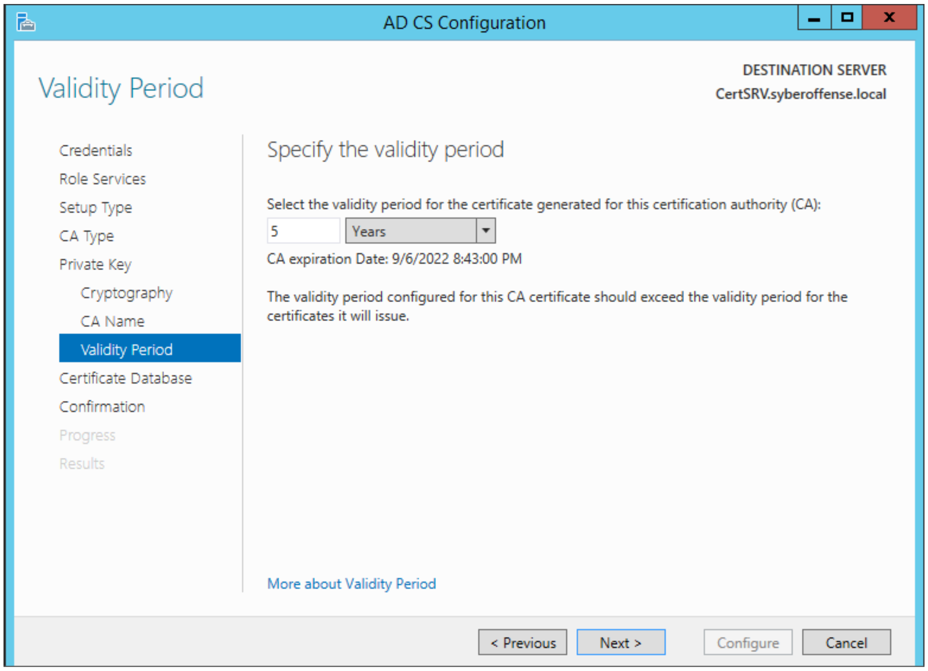
Common name for this CA: syberoffense-CERTSRV-CA

Distinguished name suffix:

Preview of distinguished name: CN=syberoffense-CERTSRV-CA

More about CA Name

On the Validity Period page, accept the defaults and click Next.



Validity Period

DESTINATION SERVER
CertSRV.syberoffense.local

Specify the validity period

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

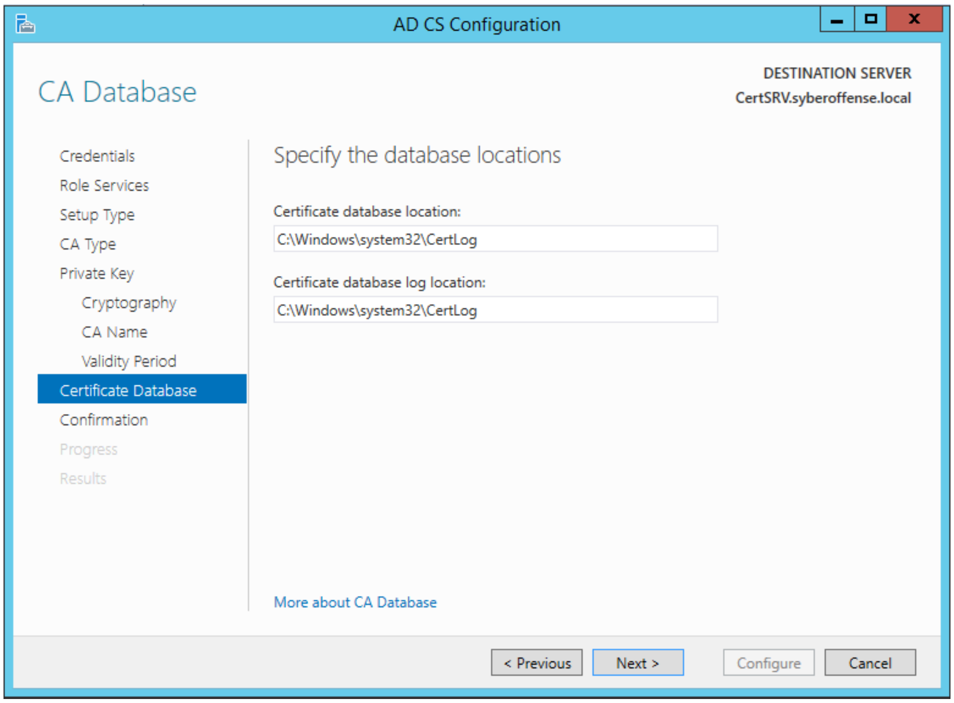
5 Years

CA expiration Date: 9/6/2022 8:43:00 PM

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

More about Validity Period

The CA Database page displays the default location where the database will be located.



CA Database

DESTINATION SERVER
CertSRV.syberoffense.local

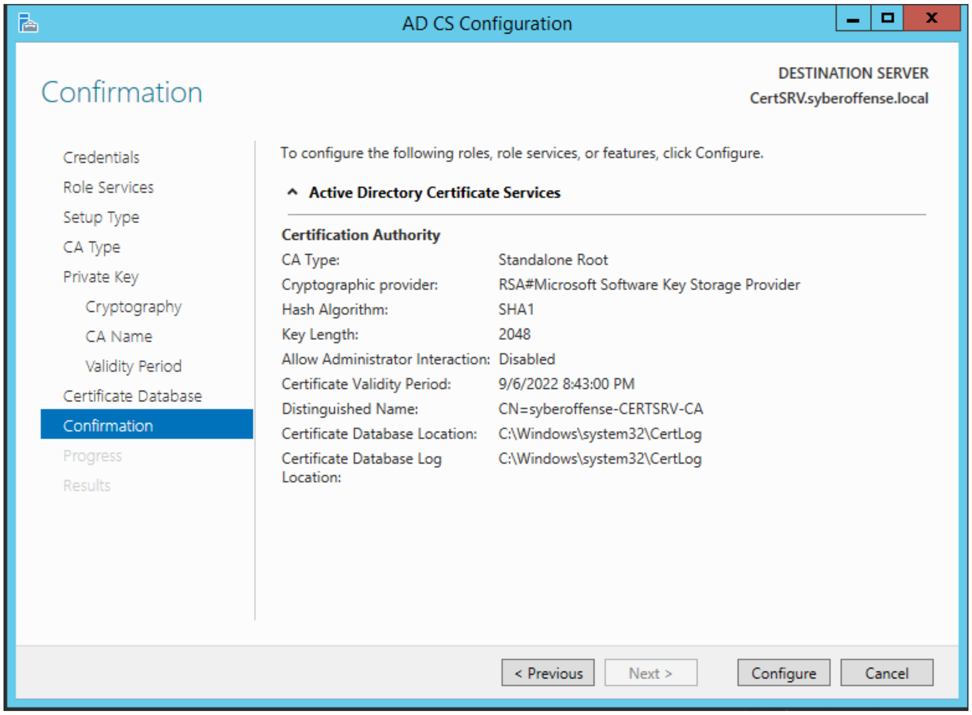
Specify the database locations

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

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

More about CA Database

Click Next. On the Confirmation page, click Configure.



DESTINATION SERVER
CertSRV.syberoffense.local

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:	SHA1
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	9/6/2022 8:43:00 PM
Distinguished Name:	CN=syberoffense-CERTSRV-CA
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Once the configuration is complete, click Close twice.

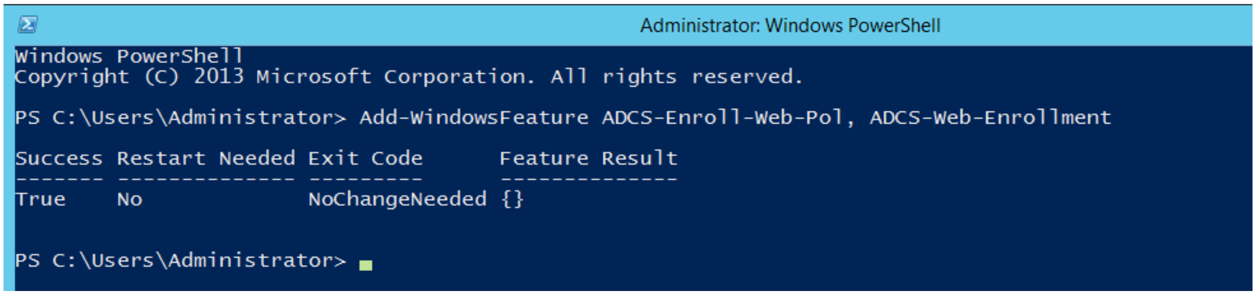
We now need to install some additional features and to do this we will be using PowerShell.

We will Install these two features:

- Certification Authority Web Enrollment
- Certificate Web Enrollment

We can Install both features using one command

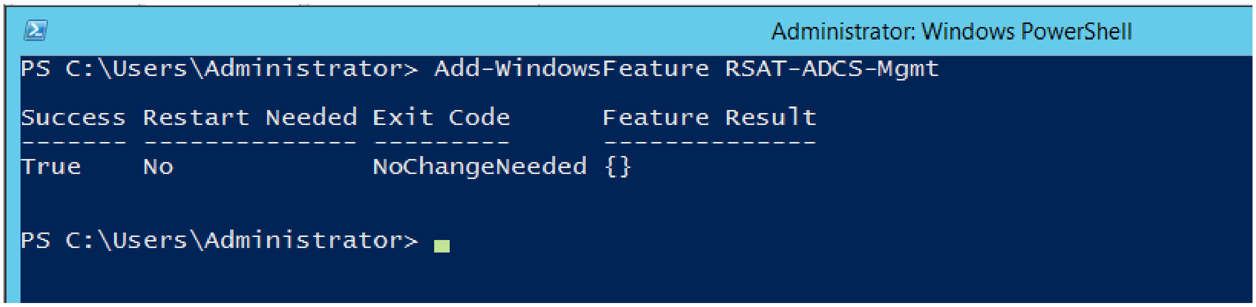
```
Add-WindowsFeature ADCS-Enroll-Web-Pol, ADCS-Web-Enrollment
```



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-WindowsFeature ADCS-Enroll-Web-Pol, ADCS-Web-Enrollment

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


PS C:\Users\Administrator>
```

We now need to install the management console for certificate services. For this, we can use the following command:

```
Add-WindowsFeature RSAT-ADCS-Mgmt
```

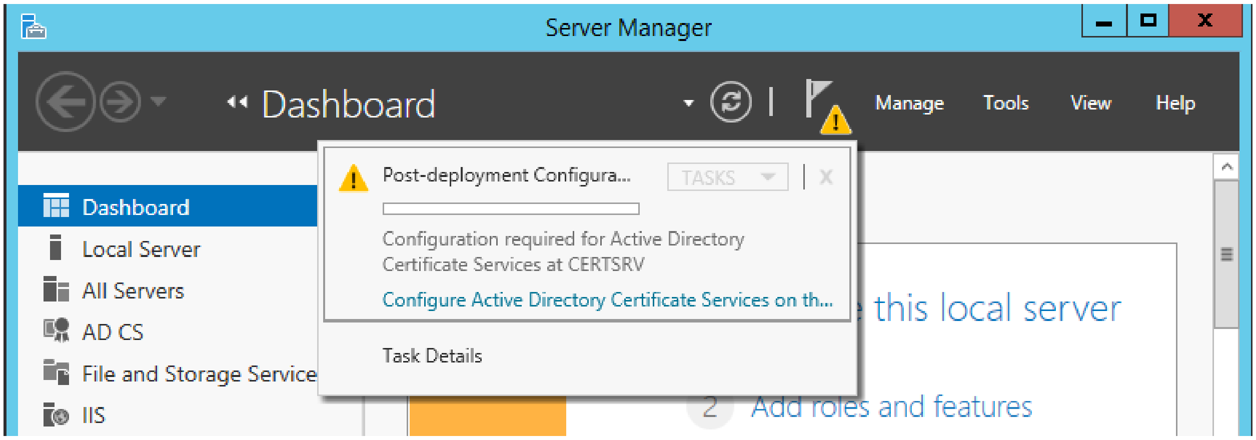


```
PS C:\Users\Administrator> Add-WindowsFeature RSAT-ADCS-Mgmt

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


PS C:\Users\Administrator>
```

Open Certificate of Authority **from Tools in Server Manager.**

We can now return to Server Manager and once again, we need to configure the new features we installed.

As before, if Server Manager does not have a notification waiting for us, we can either use the refresh option or close and restart Server Manager for the notification to appear.

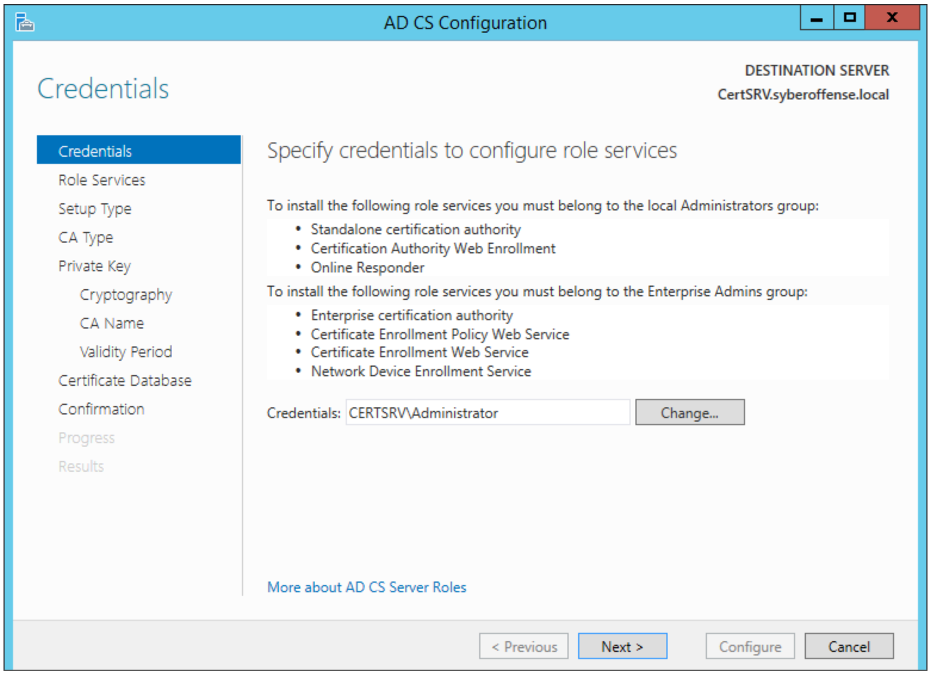


Post-deployment Configura...

Configuration required for Active Directory Certificate Services at CERTSRV

Configure Active Directory Certificate Services on th...

Task Details



Credentials

DESTINATION SERVER
CertSRV.syberoffense.local

Specify credentials to configure role services

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

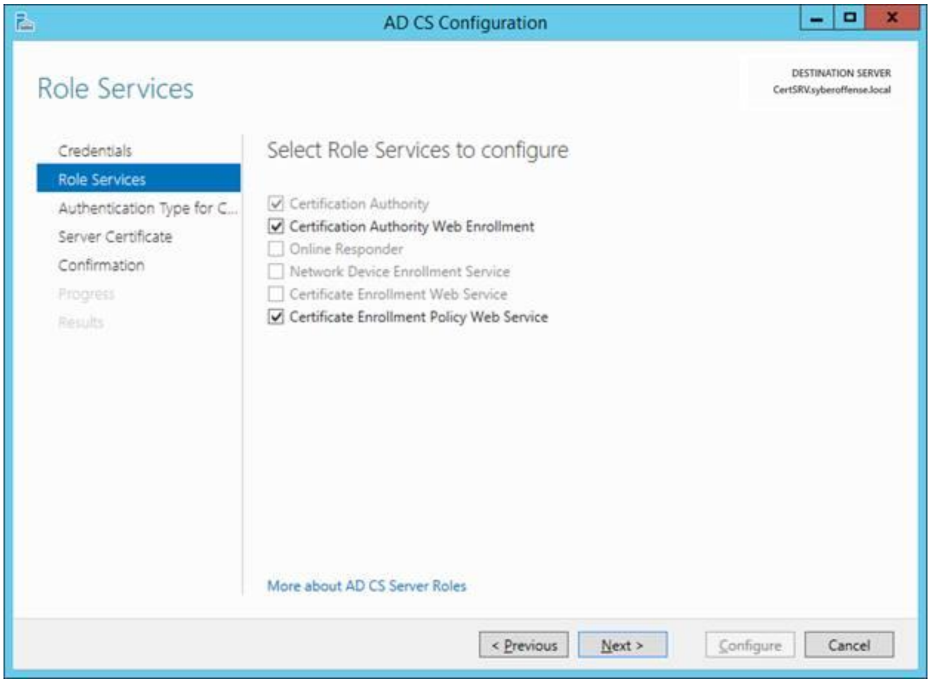
- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

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: CERTSRV\Administrator

Check the boxes for Certification Authority Web Enrollment and Certificate Enrollment Policy Web Service.



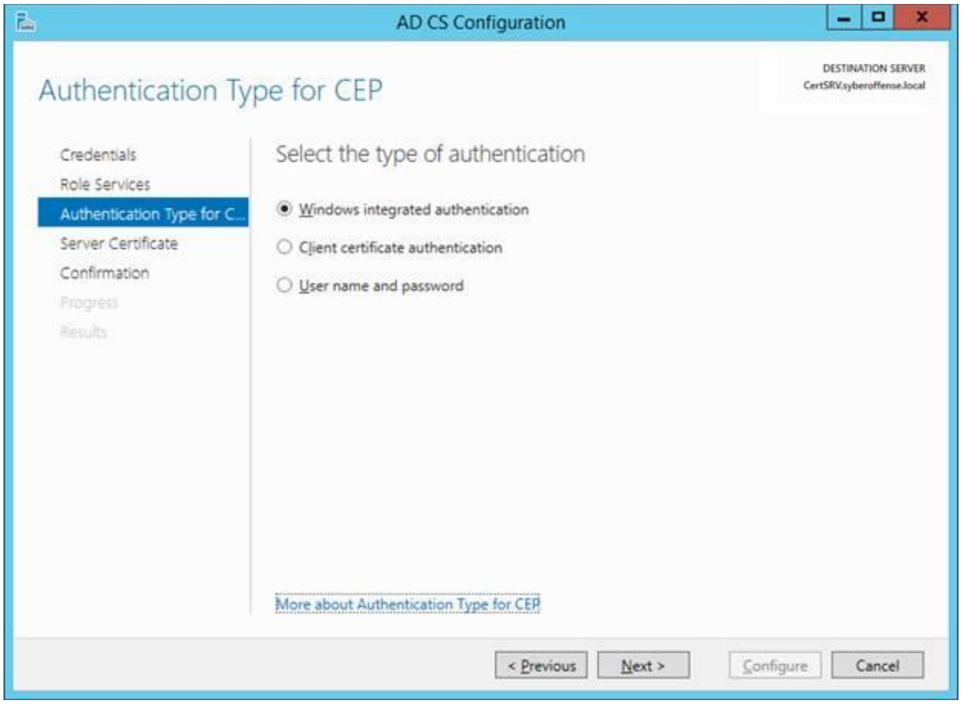
Role Services

DESTINATION SERVER
CertSRV.syberoffense.local

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

Select, Windows Integrated Authentication.



Authentication Type for CEP

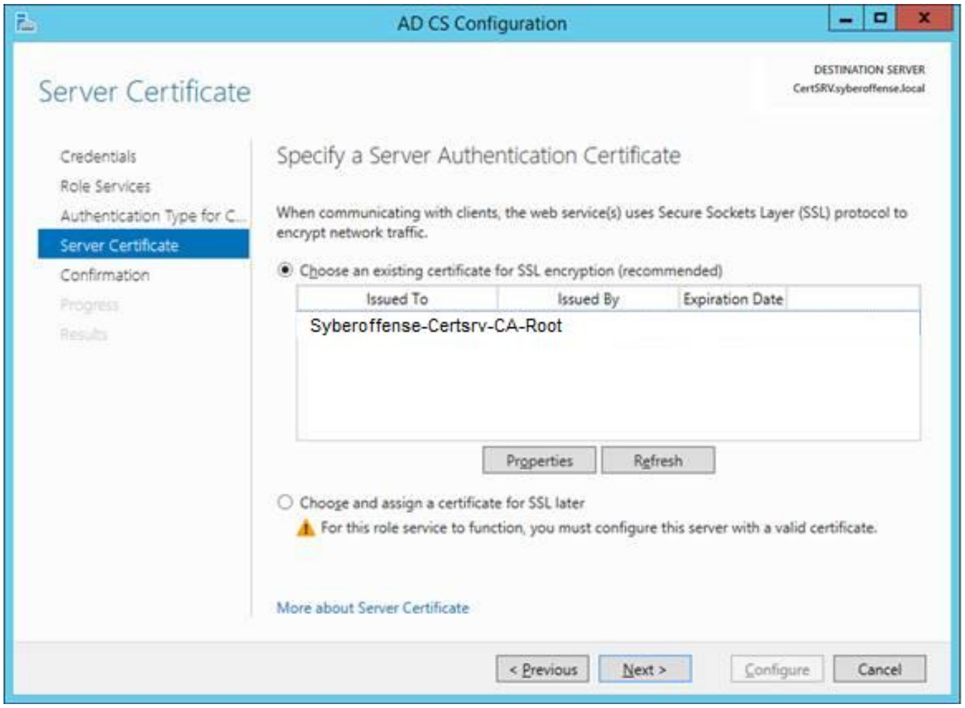
Select the type of authentication

● Windows integrated authentication

○ Client certificate authentication

○ User name and password

Select the Server Authentication Certificate with your domain name.



Server Certificate

Specify a Server Authentication Certificate

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

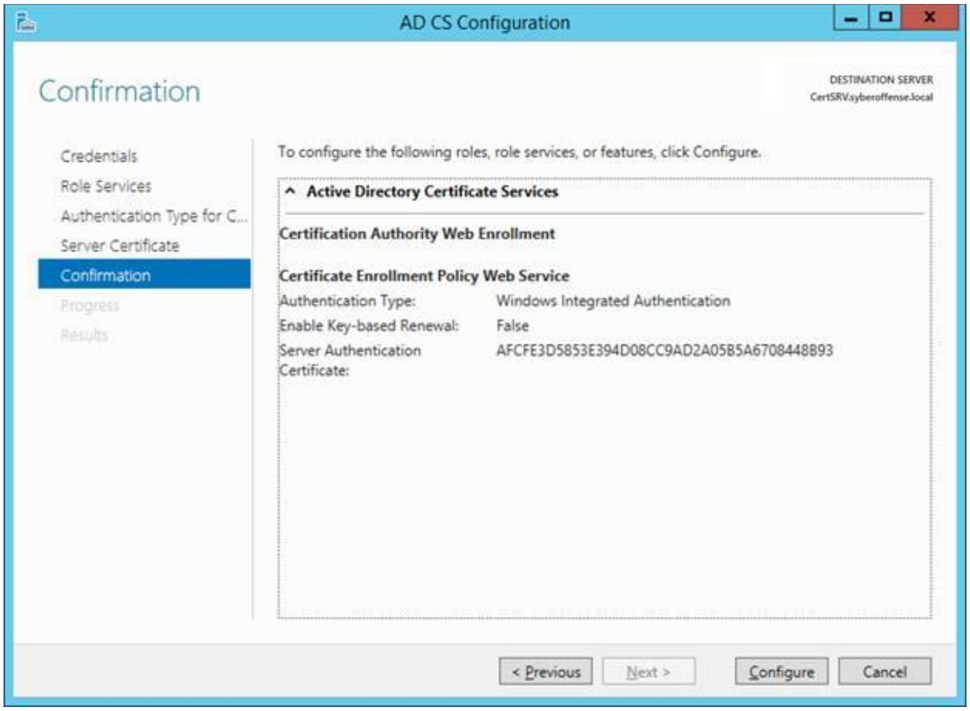
● Choose an existing certificate for SSL encryption (recommended)

Issued To	Issued By	Expiration Date
Syberoffense-Certsrv-CA-Root		

○ Choose and assign a certificate for SSL later

⚠ For this role service to function, you must configure this server with a valid certificate.

Check over the confirmation page and then click Configure.



Confirmation

DESTINATION SERVER
CertSRV.syberoffense.local

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

Active Directory Certificate Services

Certification Authority Web Enrollment

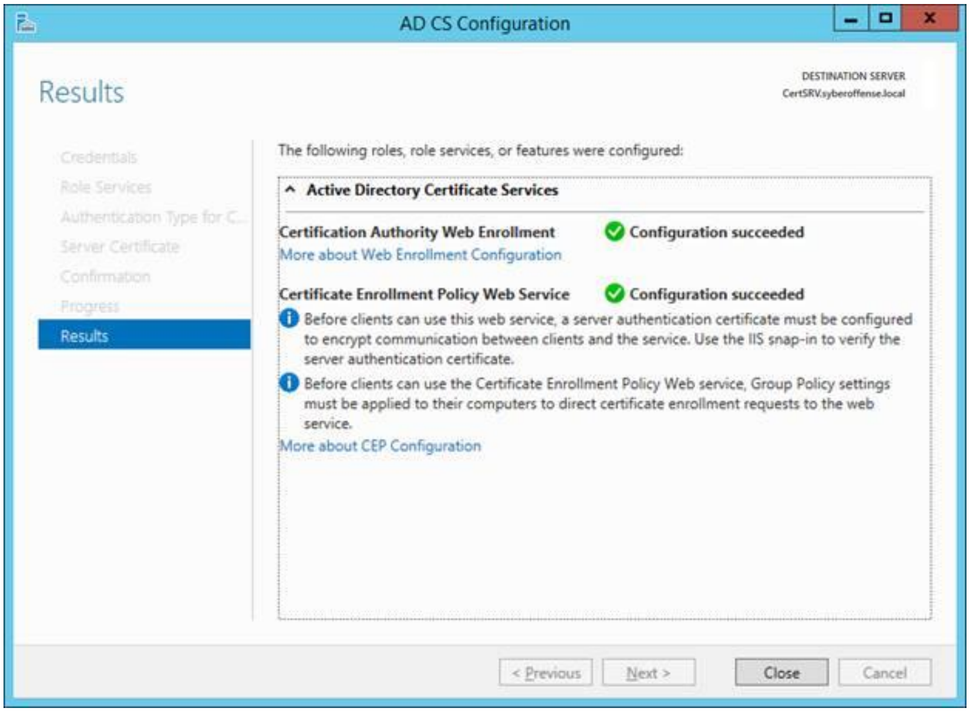
Certificate Enrollment Policy Web Service

Authentication Type: Windows Integrated Authentication

Enable Key-based Renewal: False

Server Authentication Certificate: AFCFE3D5853E394D08CC9AD2A05B5A6708448B93

Once the installation of the additional features has completed, close the



Results

DESTINATION SERVER
CertSRV.syberoffense.local

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

Active Directory Certificate Services

Certification Authority Web Enrollment ✓ **Configuration succeeded**

More about Web Enrollment Configuration

Certificate Enrollment Policy Web Service ✓ **Configuration succeeded**

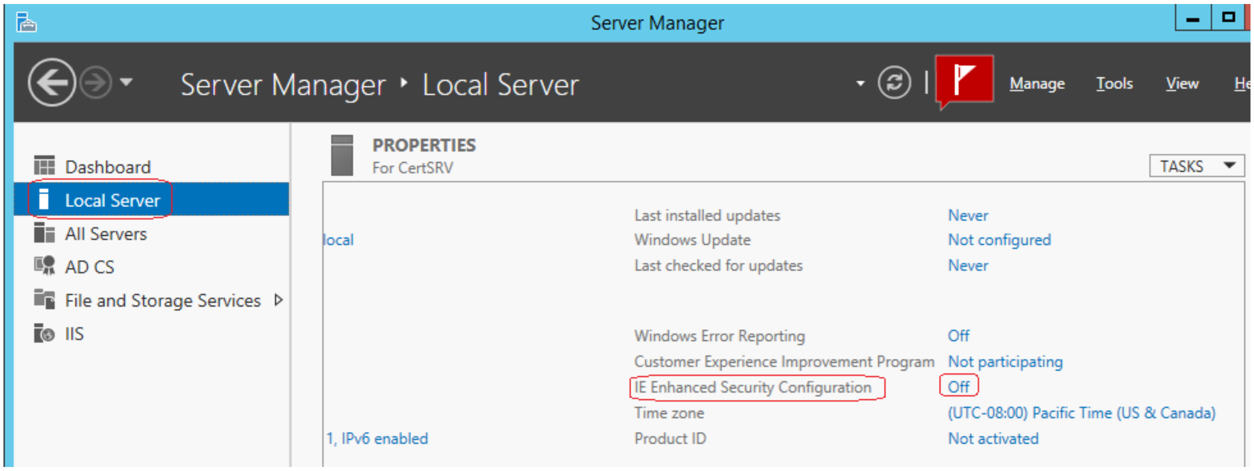
Before clients can use this web service, a server authentication certificate must be configured to encrypt communication between clients and the service. Use the IIS snap-in to verify the server authentication certificate.

Before clients can use the Certificate Enrollment Policy Web service, Group Policy settings must be applied to their computers to direct certificate enrollment requests to the web service.

More about CEP Configuration

We are now ready to test our installation of Certificate Services. To do this, we will attempt to open the Cert Services Web page using IE.

We begin by ensuring the IE Enhanced Security Configuration is turned off.



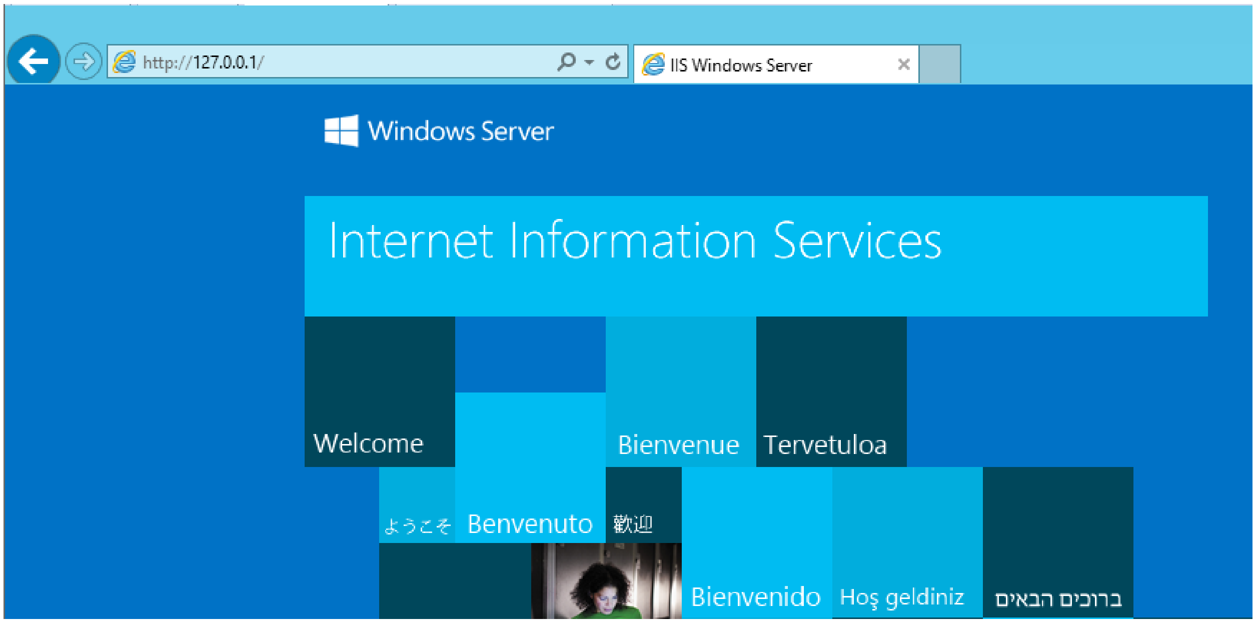
local

1, IPv6 enabled

Last installed updates Never
Windows Update Not configured
Last checked for updates Never

Windows Error Reporting Off
Customer Experience Improvement Program Not participating
IE Enhanced Security Configuration Off
Time zone (UTC-08:00) Pacific Time (US & Canada)
Product ID Not activated

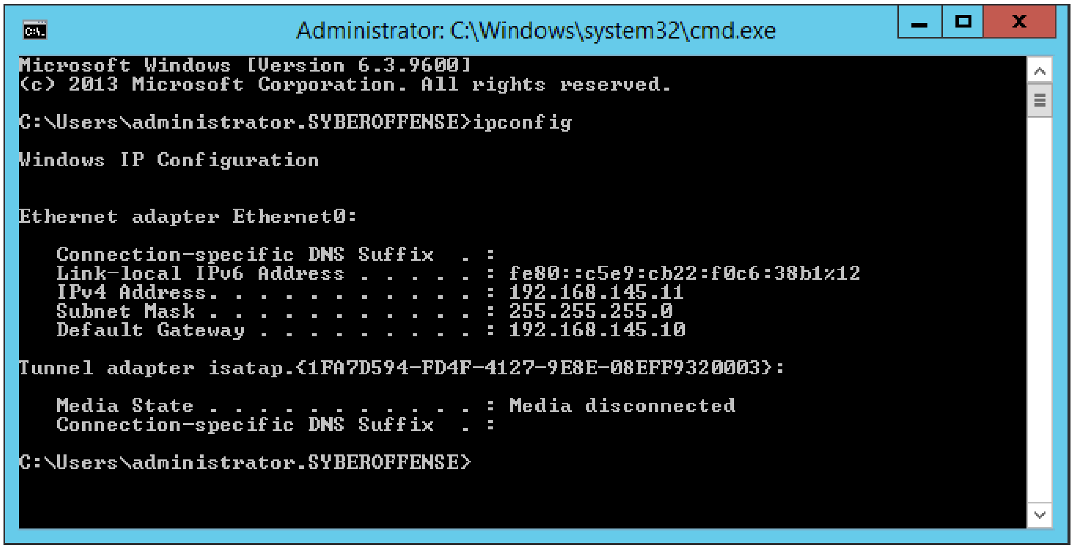
We next open IE, and in the address bar, we type http://127.0.0.1 to confirm that IIS is installed and working. This should open the default web page for your IIS server.



Once IIS has been confirmed as working, we are ready to launch the Cert Server Web page.

The Cert Server web page is using https. The easiest way to connect to the Cert Server web page is using the servers IP address.

If you do not know your cert Servers IP address, bring up a command prompt and type in the IPCONFIG command.

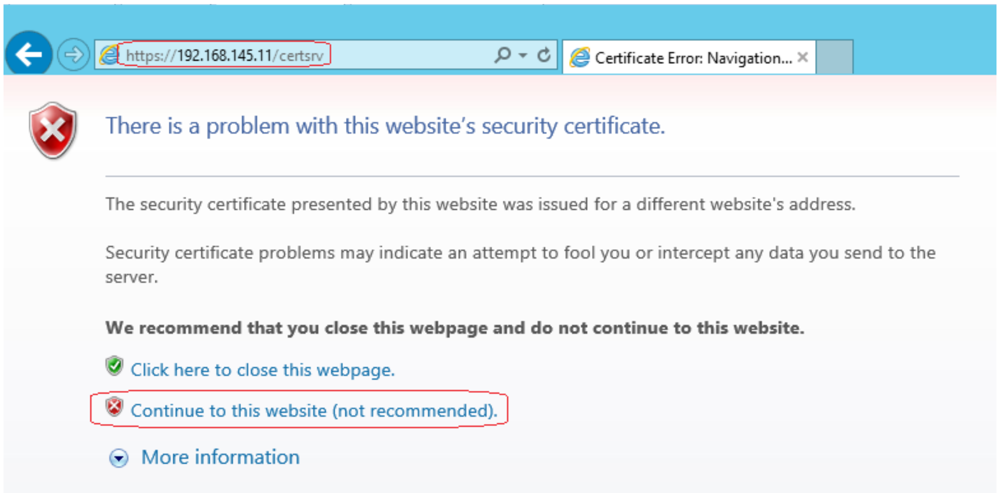


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\administrator.SYBEROFFENSE>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c5e9:cb22:f0c6:38b1%12
   IPv4 Address. . . . . . . . . . . : 192.168.145.11
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.145.10

Tunnel adapter isatap.{1FA7D594-FD4F-4127-9E8E-08EFF9320003}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\administrator.SYBEROFFENSE>
```

Back at the address bar in IE, we type in the following replacing your Cert Server IP address with the one shown in the example.

https://192.168.145.11/certsrv

This brings up a warning about the website's security certificate. Accept the risk by selecting the option to Continue to this website (not recommended)


https://192.168.145.11/certsrv
Certificate Error: Navigation...

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

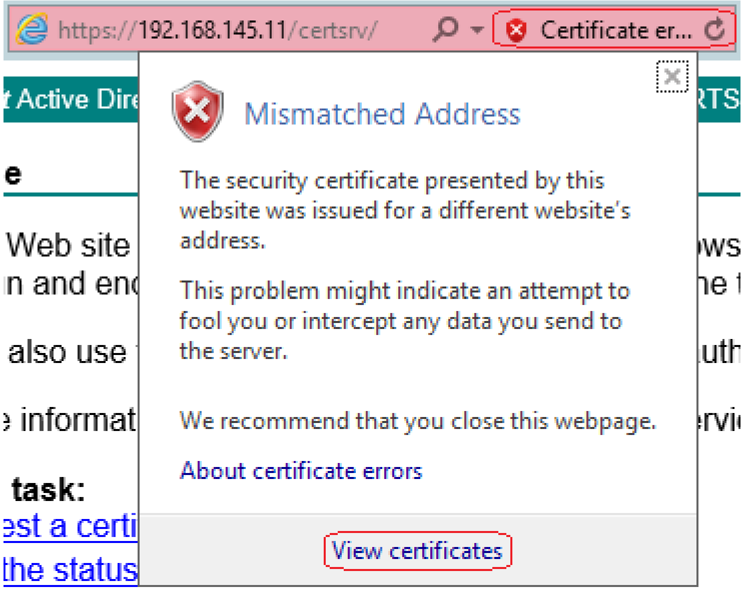
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Once the Cert Server page loads, you can go to the address bar and click on the red x to view and install the problem certificate.



Mismatched Address

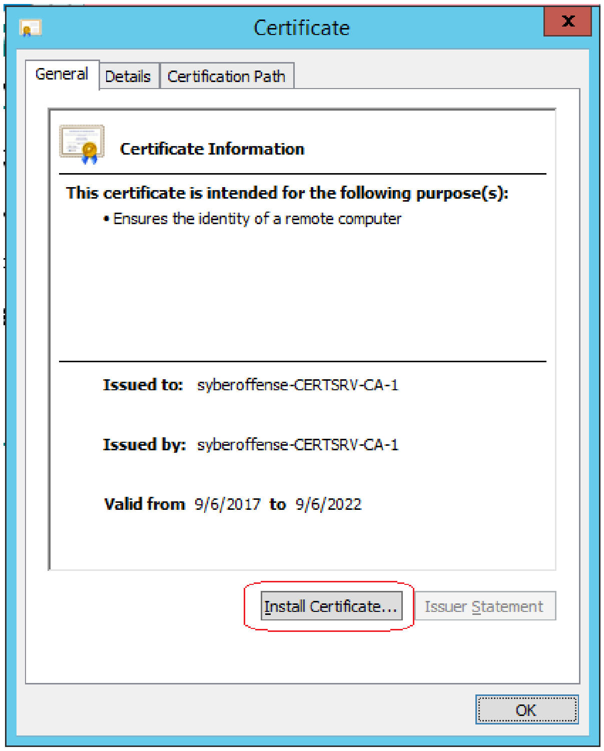
The security certificate presented by this website was issued for a different website's address.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

Click on Install Certificate.



Certificate Information

This certificate is intended for the following purpose(s):

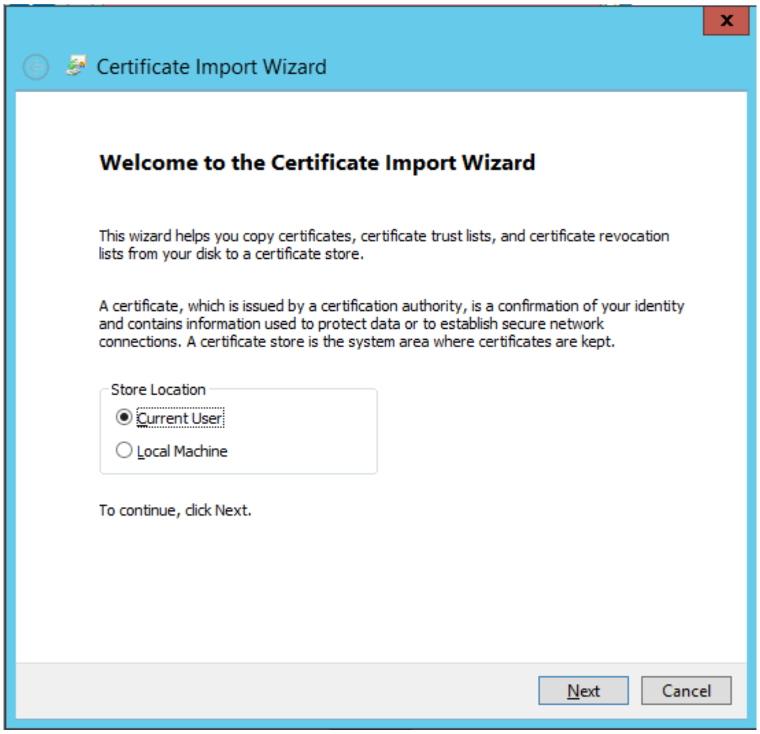
- Ensures the identity of a remote computer

Issued to: syberoffense-CERTSRV-CA-1

Issued by: syberoffense-CERTSRV-CA-1

Valid from 9/6/2017 to 9/6/2022

Accept the default store location, and click next.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

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

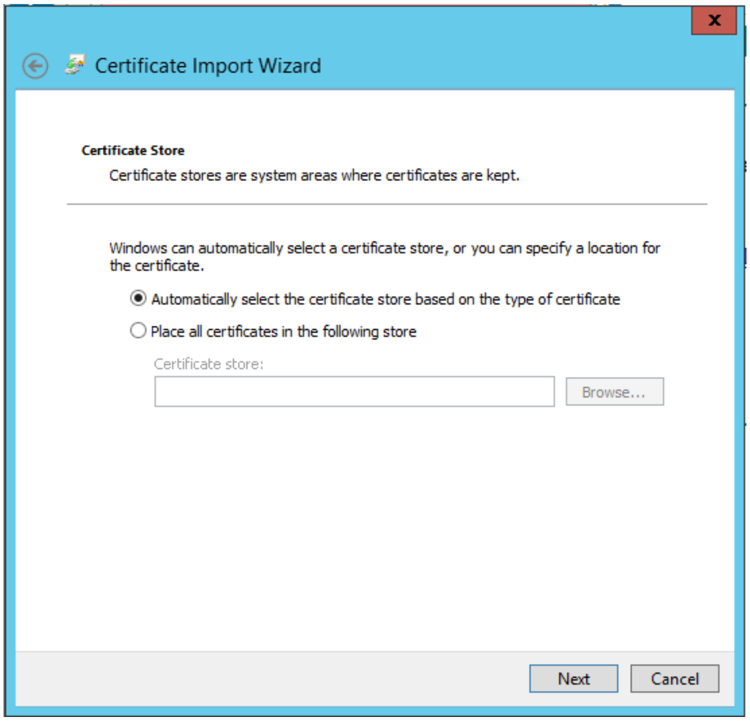
Store Location

● Current User

○ Local Machine

To continue, click Next.

Accept the default for the certificate store.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

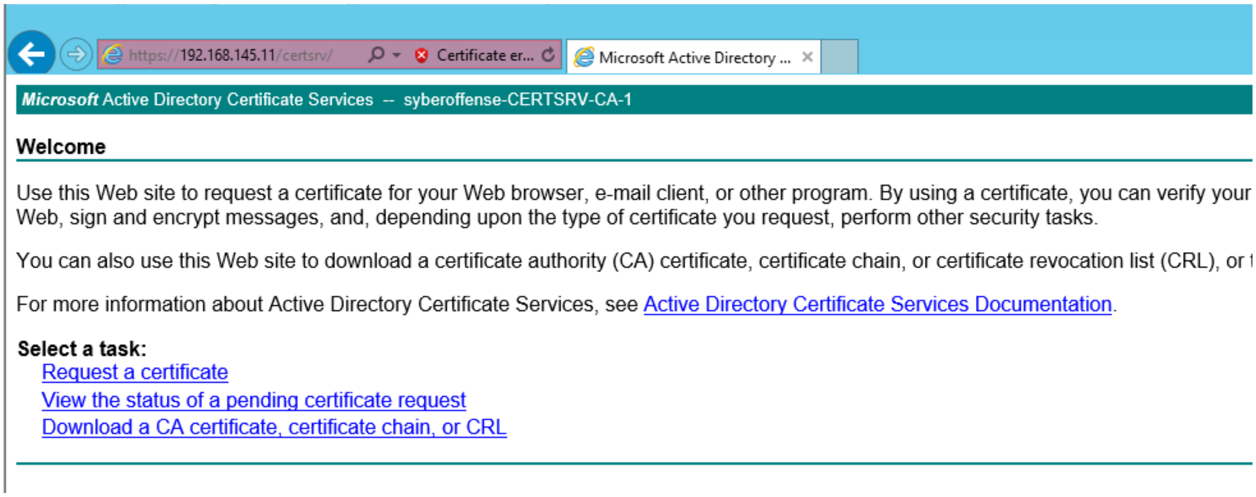
Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

Click Finish to complete the wizard.


https://192.168.145.11/certsrv/
Certificate er...
Microsoft Active Directory ...

Microsoft Active Directory Certificate Services -- syberoffense-CERTSRV-CA-1

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or t

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Summary

In this lab, to learned how to install Certificate Services using PowerShell and the Server Manager. Certificate Services can be used to issues a variety of situation to include Citrix and authentication to Active Directory.

End of the Lab!