Black•Vault HSM
Microsoft CA
Integration Guide

9565 Soquel Drive
Aptos, CA 95003
Phone +1 831.688.1021
1 877.ENGAGE4 (364.2434)
sales@engageblack.com

Version 1.2.0 January 7, 2021

Disclaimer and Warranty

Engage Black is a business unit of Engage Communication.

Engage Communications, Inc. 9565 Soquel Drive Aptos, CA 95003

Phone +1(831) 688-1021

http://www.engageblack.com/

http://www.engageinc.com/

Sales +1 (831) 688-1021 sales@engageblack.com

Global Technical Support +1 (831) 688-1021 **(extension 3)** support@engageblack.com

Table of Contents

1. Introduction

A primary security control in a Public Key Infrastructure (PKI) is how the private keys are stored and managed, especially when it concerns Certification Authorities (CAs). A strong key protection strategy is critical to maintaining and ensuring security. The BlackVault HSM enhances the security of CAs and PKIs. It does this by providing an easy to use, hardware based secure storage system of the private keys, as well as providing a dedicated cryptographic processor to perform the desired cryptographic operations.

Microsoft uses its cryptographic API interfaces to talk to the BlackVault HSM. When Windows is interfacing with a BlackVault HSM, the HSM functions as a Cryptographic Services Provider (CSP). To use the BlackVault HSM as a CSP with a Microsoft CA, the BlackVault HSM libraries must be installed and the BlackVault HSM must be correctly set up and in the operational state.

It is highly recommended that a strong protection strategy is taken when using the BlackVault HSM. This includes ensuring that the BlackVault HSM resides in a secure place, storing the smart cards associated with the operators of the BlackVault correctly, and properly backing up the BlackVault HSM databases (user and smart card).

For a complete installation and use guide for the Microsoft CA, please consult Microsoft documentation. This guide should be used more as an overview on how to integrate the BlackVault HSM with the Microsoft CA.

The benefits of using a BlackVault HSM with Microsoft CA include:

- Secure storage of the private key
- Signing code within a cryptographically secure environment
- FIPS 140-2 level 3 validated hardware

2. Procedure

To proceed the following is needed:

- BlackVault HSM
- BlackVault smart card set
- BlackVault HSM setup CD
- A client computer that has a supported Operating System installed.

Additionally, the BlackVault HSM must be Initialized and Configured properly (see the BlackVault HSM User Guide for more details).

To setup Microsoft CA with the BlackVault HSM:

- **Install the BlackVault HSM Libraries onto the Client Machine by running the application bv-setup.exe (included in the setup folder)**

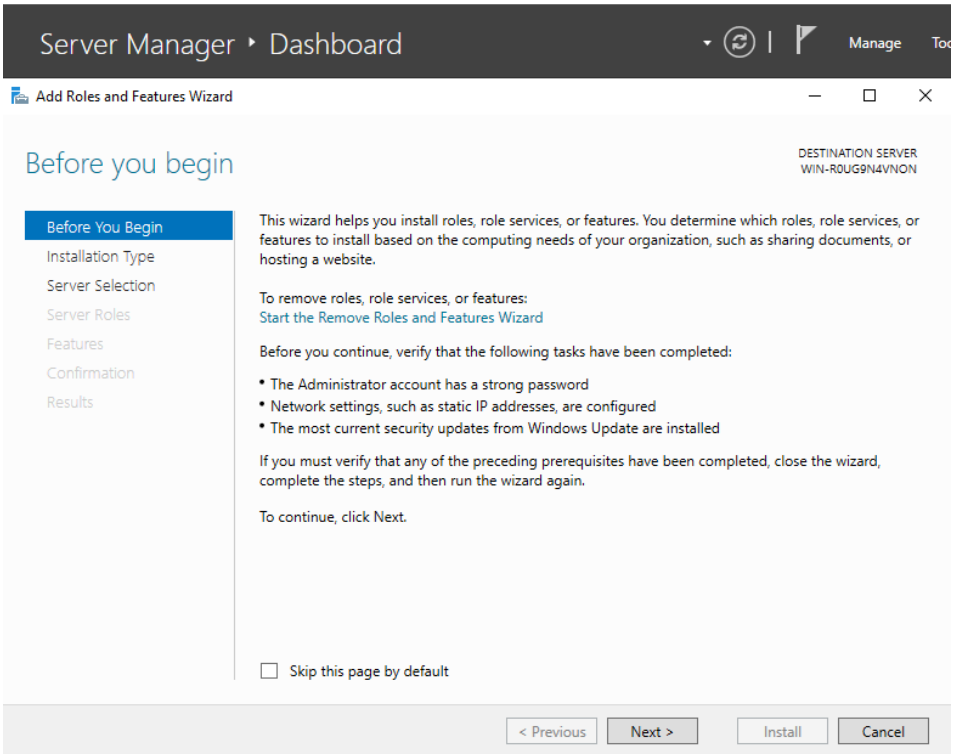
The following assumes you already initialized the BlackVault HSM and are installing this software on a machine that does not already have a Microsoft CA setup.

2.1. Integration with MSCA

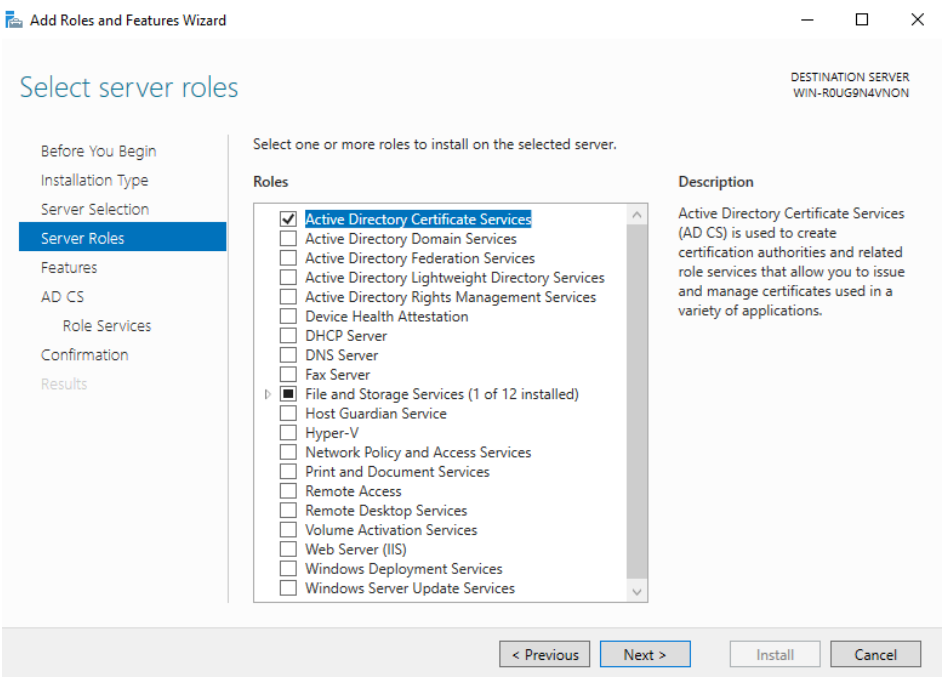
2.1.1. Installing Active Directory Certificate Services

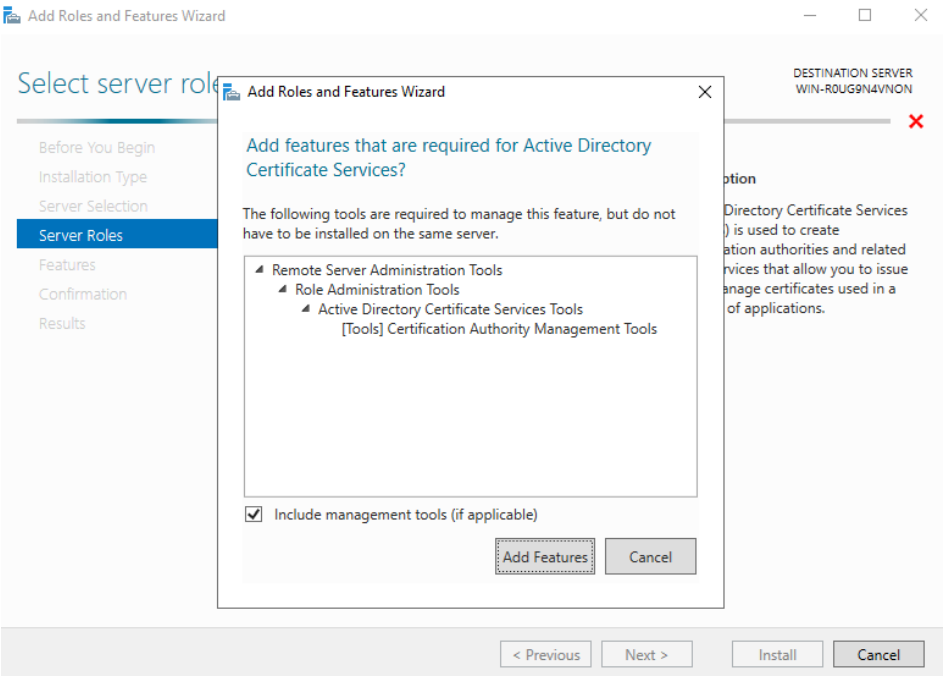
1. Copy the already configured pkcs.dat to C:\Windows\System32\. Alternatively, you can set the BV_PKCS_PATH system environment variable to specify the path to the pkcs.dat file.
2. Log into BlackVault HSM as User

3. Add Microsoft Active Directory Certificate services
    a. Open the **Server Manager** application
    b. Under the **Manage** dropdown menu, select **Add Roles and Features**

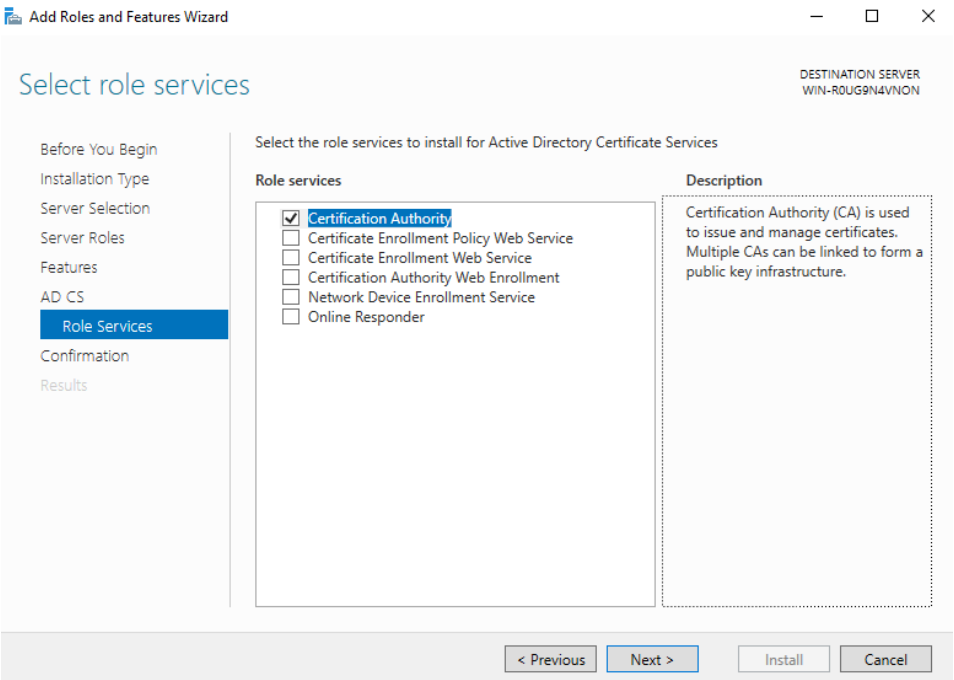


    c. A prompt for installation type will appear. Select **Role-based or feature-based installation** then press Next to continue.
    d. The next screen prompts to select **destination server**. Press Next to continue.
    e. Select all role services that are needed. The only role required for this configuration is **Active Directory Certificate Services.**


Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-R0UG9N4VNON
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
Description
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
< Previous
Next >
Install
Cancel

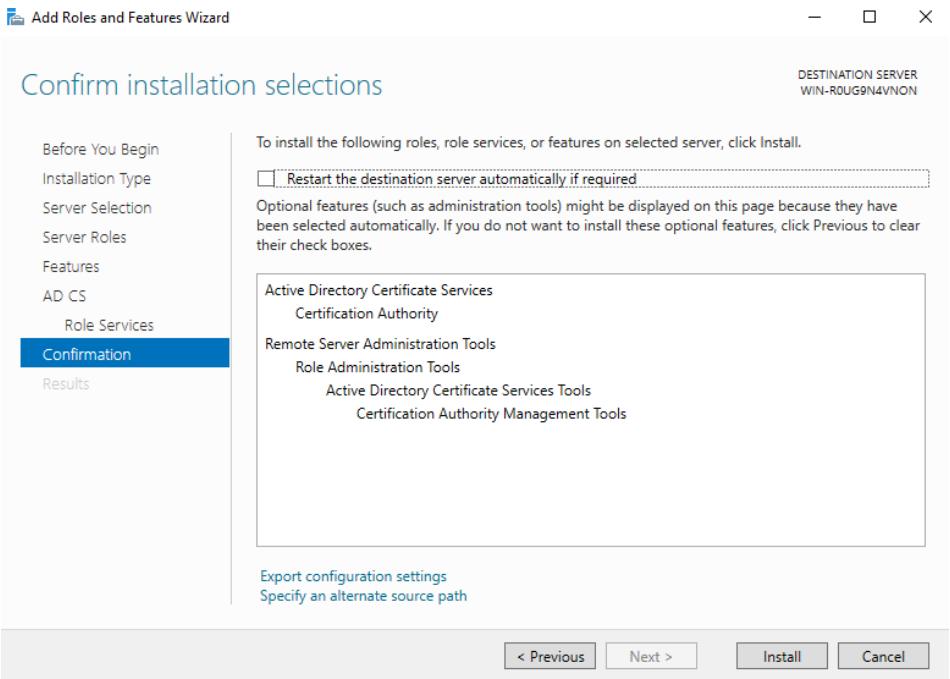

Add Roles and Features Wizard
Add Roles and Features Wizard
Add features that are required for Active Directory Certificate Services?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
Active Directory Certificate Services Tools
[Tools] Certification Authority Management Tools
Include management tools (if applicable)
Add Features
Cancel
DESTINATION SERVER
WIN-R0UG9N4VNON
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
< Previous
Next >
Install
Cancel

f. The next screen is to **Select Features**. Press Next to continue.
g. The next screen is the description of Active Directory Certificate Services. Press Next to continue.
h. On the Select role services page, select the role services required for this installation (at least Certification Authority), and press Next to continue.



Note: In the last section of this guide, we supply examples of basic MSCA function via web. If you wish to perform functions via web you must also select **Certification Authority Web Enrollment.**

i. On the Confirmation page press Install.



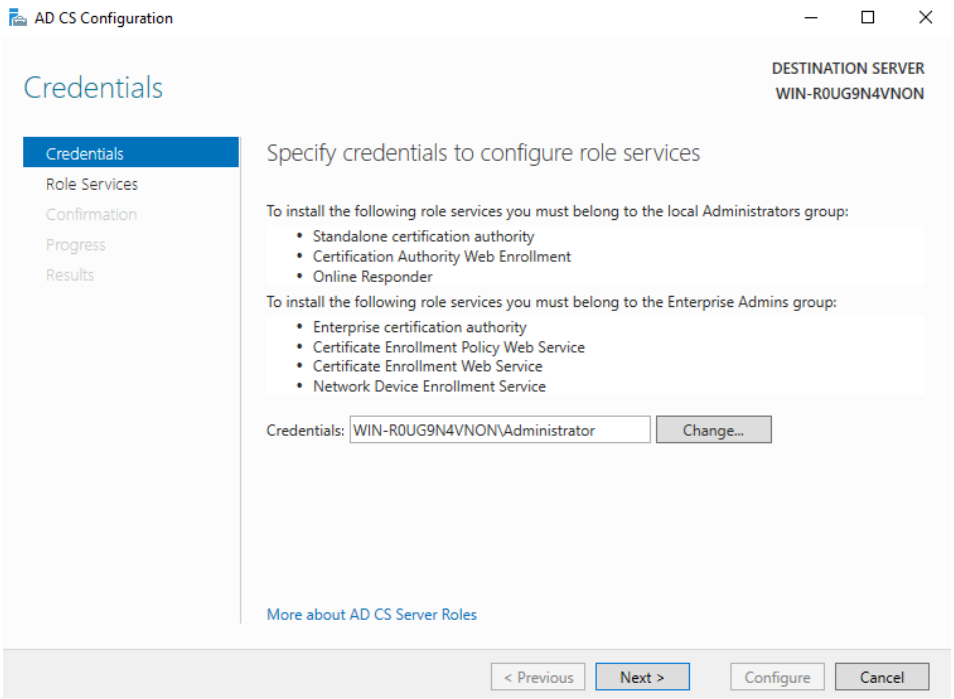
Note: This page will show more information if you chose to install Certification Authority Web Enrollment as well.

j. After the wizard has finished installing, on the Results page, press Close

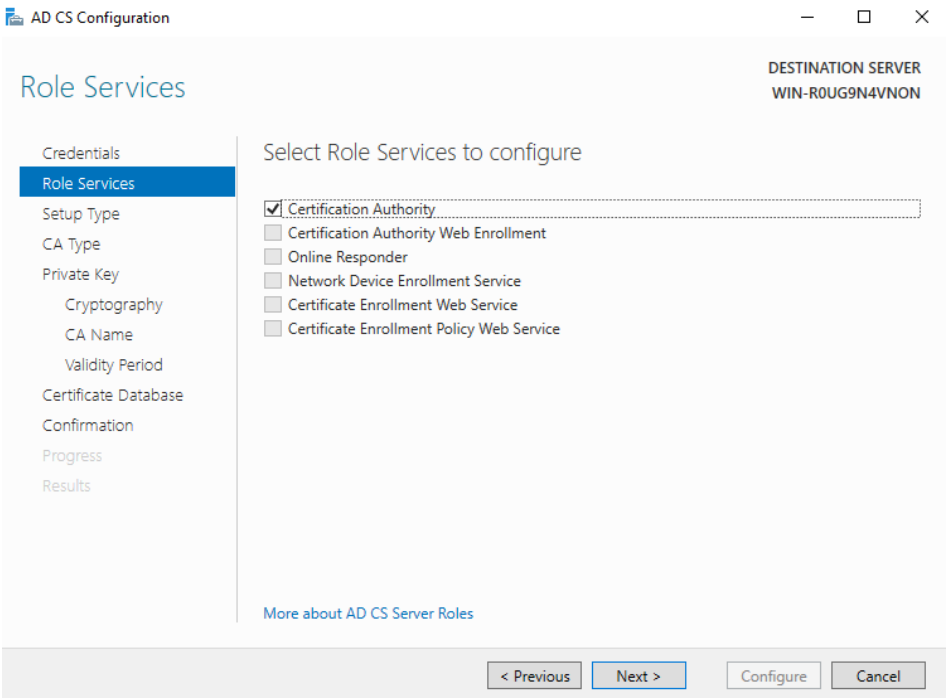
2.1.2. Configuring the Active Directory Certificate Authority

1. Select the notification flag in the right-hand corner of the **Server Manager** application.

2. Select **Configure Active Directory Certificate Services on the destination server.**
3. The **AD CS Configuration** window will now be displayed. Press Next to continue.

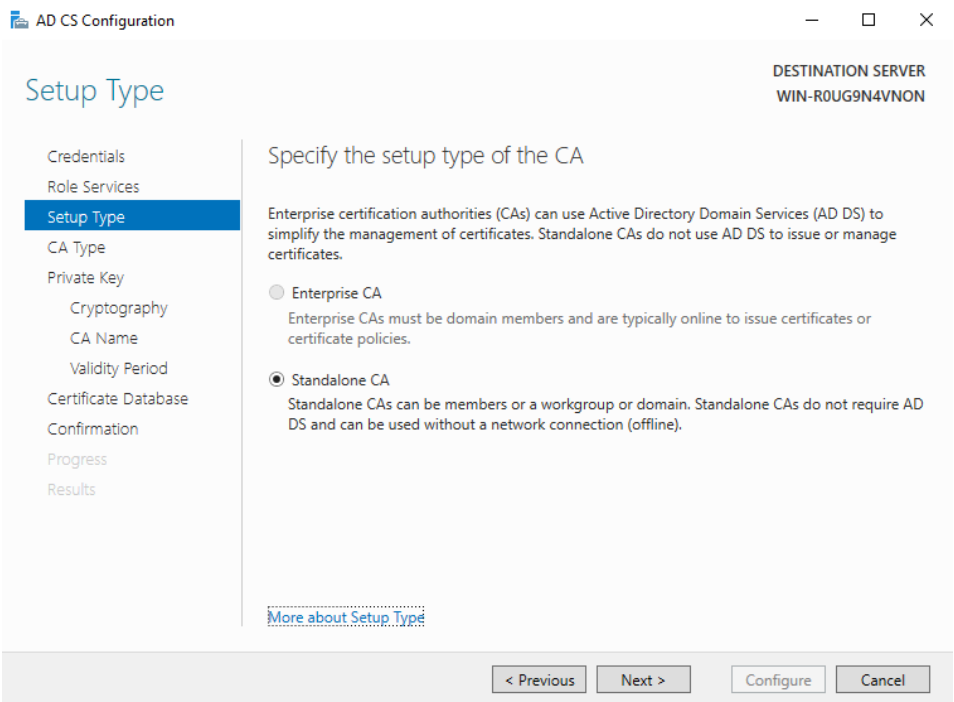


4. On the **Role Services** page, select the roles you wish to configure (choosing at least **Certificate Authority**) and press Next.

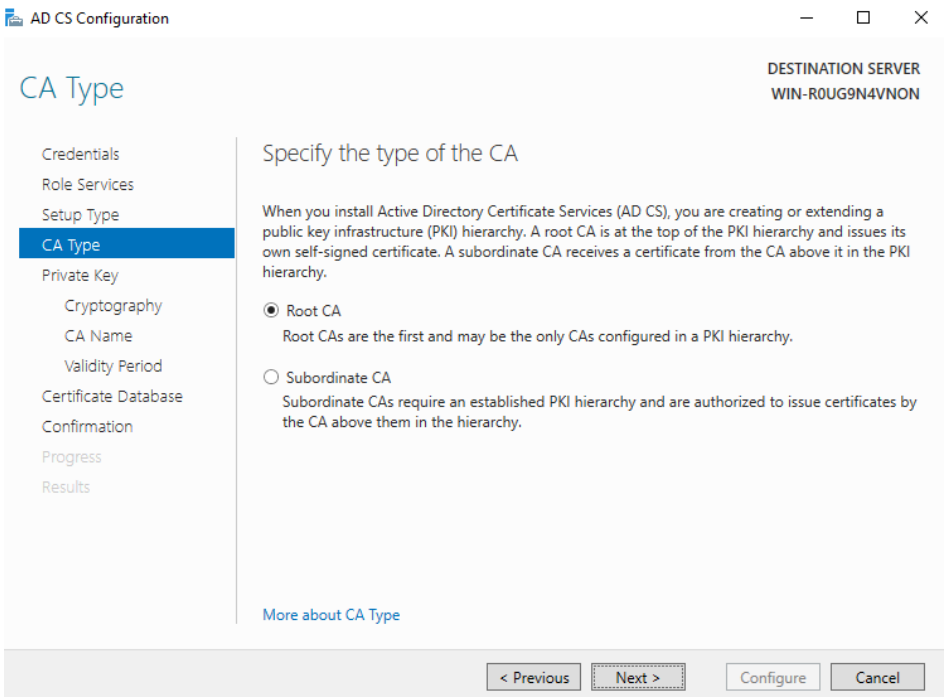


Note: If you decided to install **Certification Authority Web Enrollment,** select that as well**.**

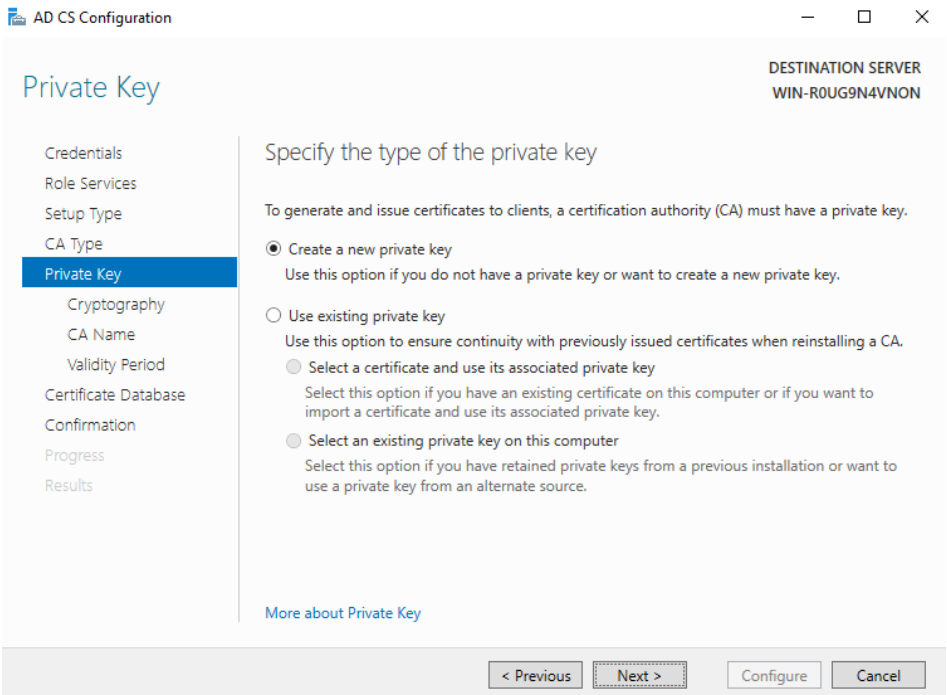
5. On the Setup Type page, select standalone CA and press Next



6. On the CA Type page, choose CA type (root ca for this example) and press Next



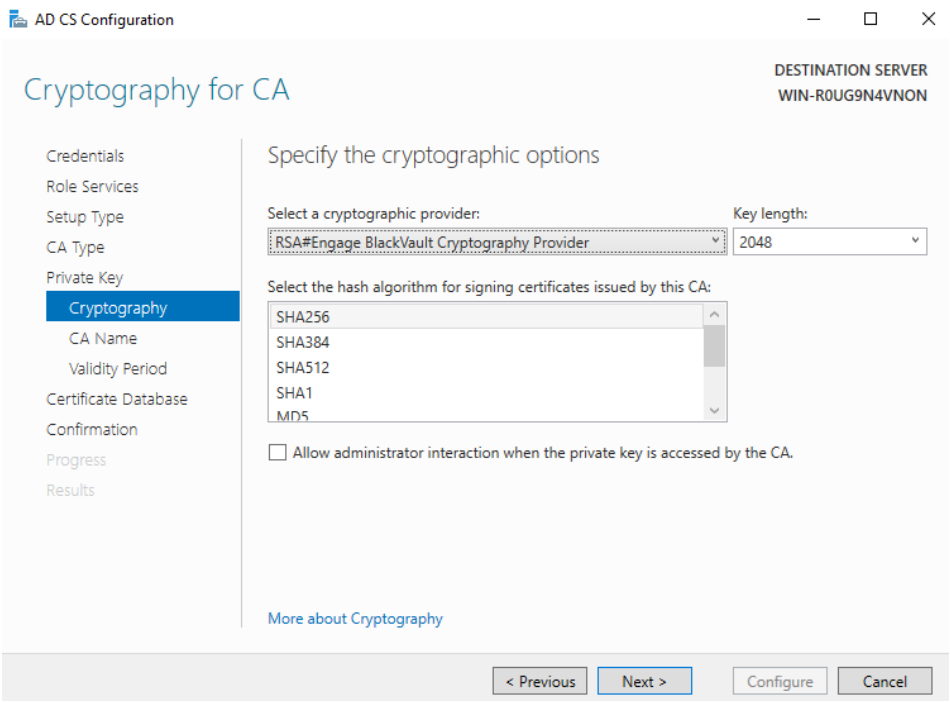
7. On the Private Key page, select “Create a new private key” and press Next



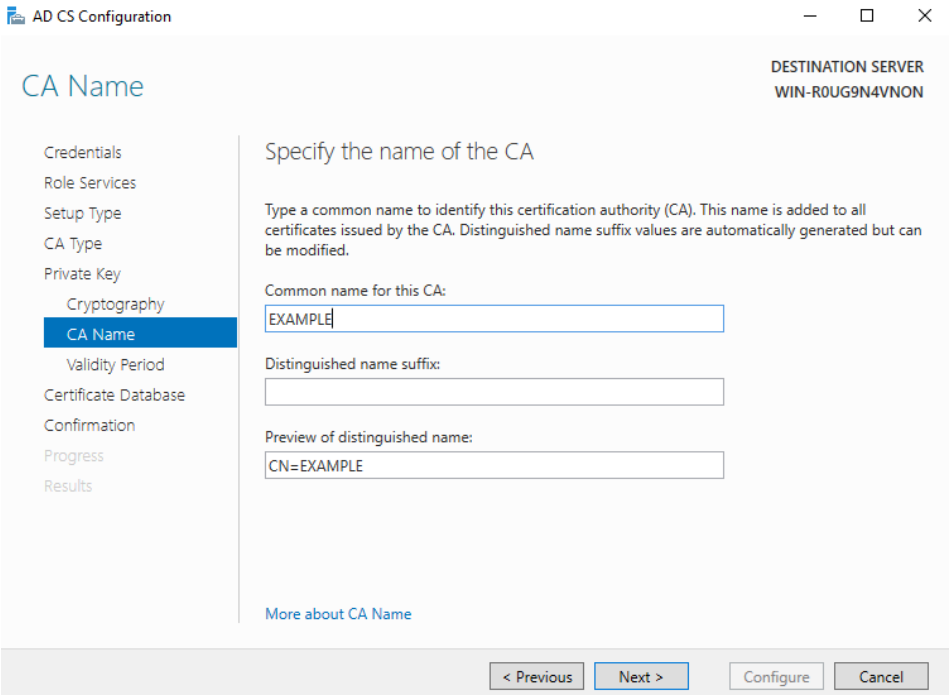
8. Next is the **Cryptography for CA** page
    i. In the **Select a cryptographic provider** drop down menu, select one of the Engage Black-Vault Cryptography Providers, this includes:
        - ECDSA_P256#Engage BlackVault Cryptography Provider
        - ECDSA_P384#Engage BlackVault Cryptography Provider
        - RSA#Engage BlackVault Cryptography Provider
        - RSA_SIGN#Engage BlackVault Cryptography Provider

Note: In this example we are using RSA#Engage BlackVault Cryptography Provider

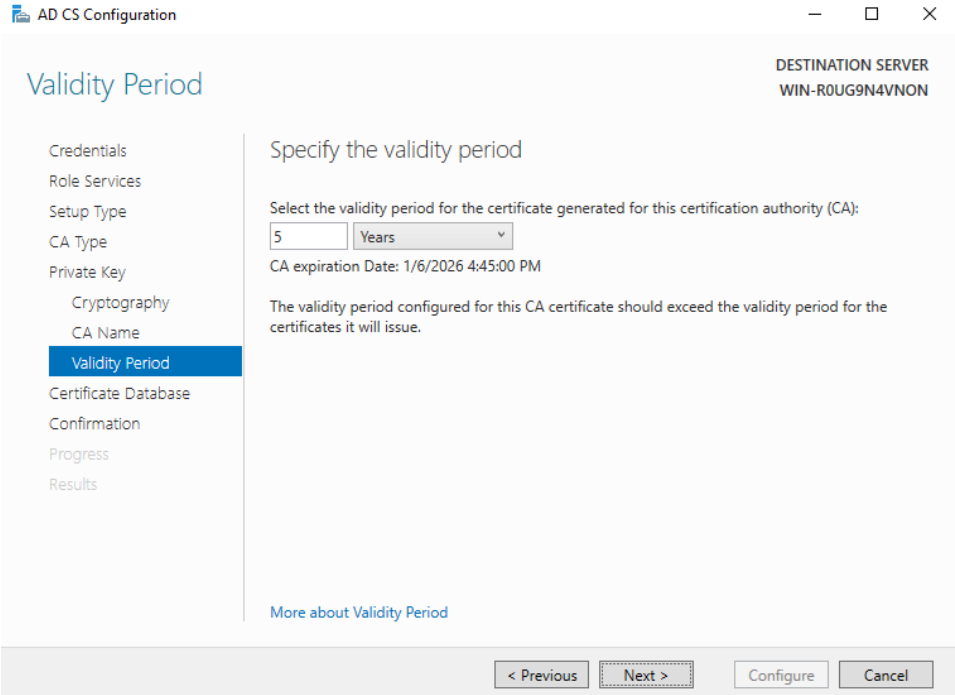
    ii. Specify the key length and hash algorithm of your choice



9. On the CA name page, enter in the Common name, and the Distinguished name in the appropriate fields then press Next.

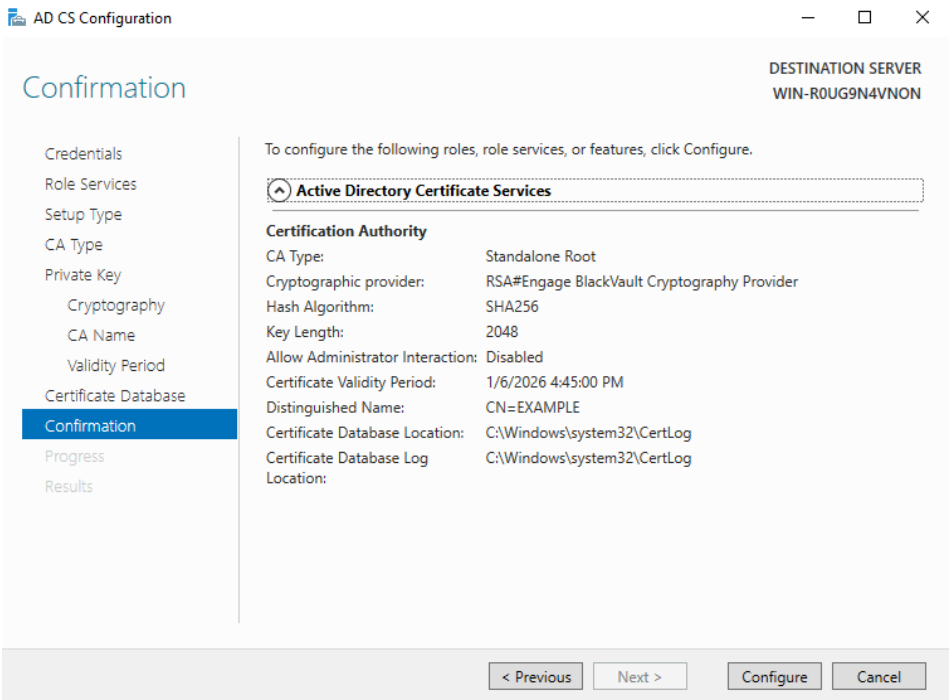


10. On the Validity Perion page, select the how long you want the CA to remain valid, then press Next.

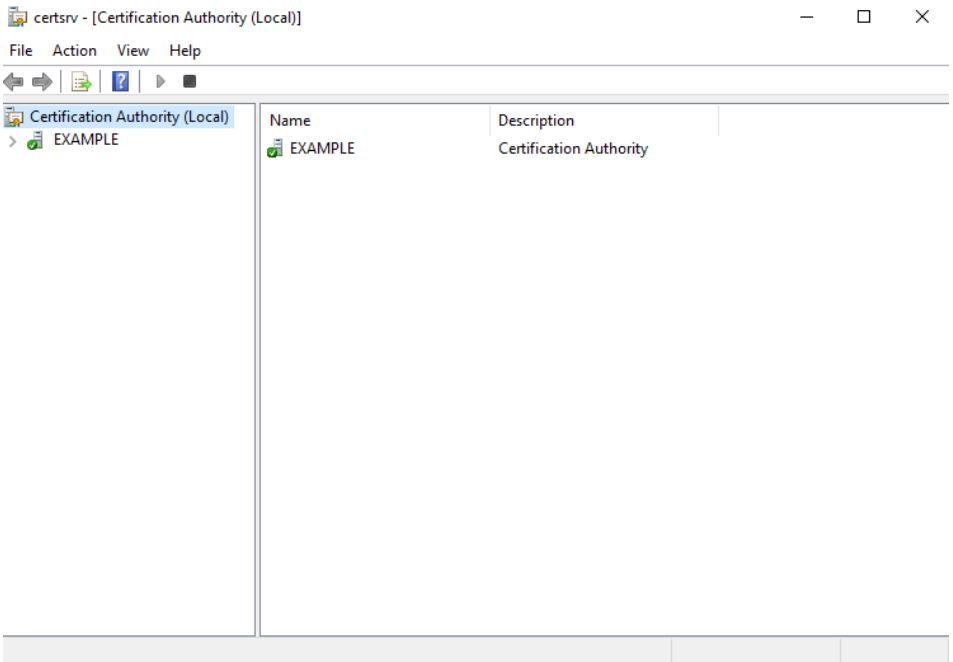


11. On the CA Database name, if you want the database and log locations in a different place than default, choose so now, then press Next.

12. On the confirmation screen, review the configuration, then press Configure



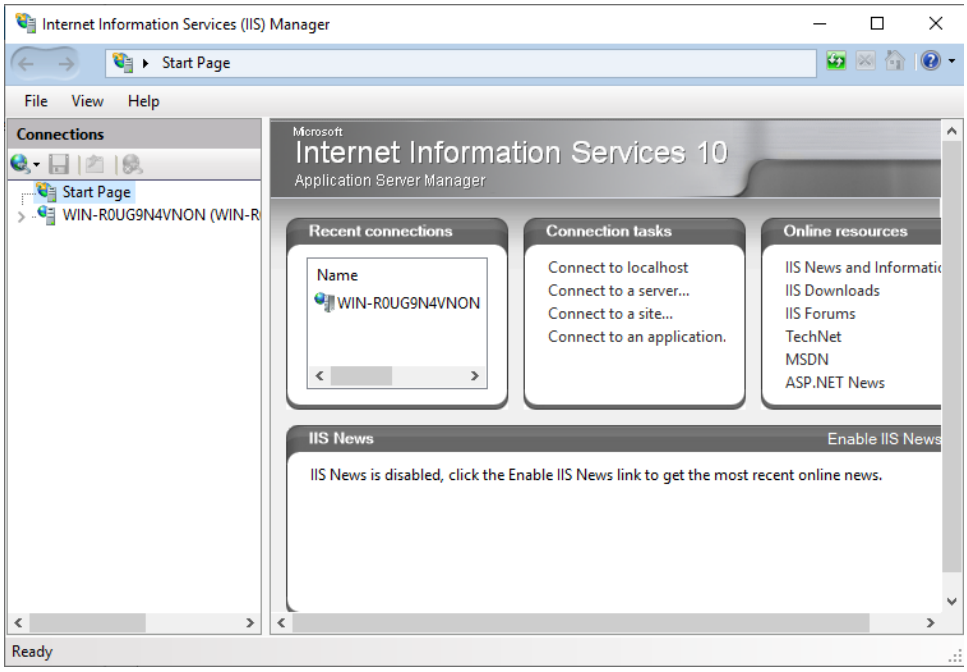
13. The configuration will now begin, once the results screen shows up, press Close to complete the process.
14. To verify the CA configuration, in the **Server Manager tools** dropdown menu, select **Certification Authority.**



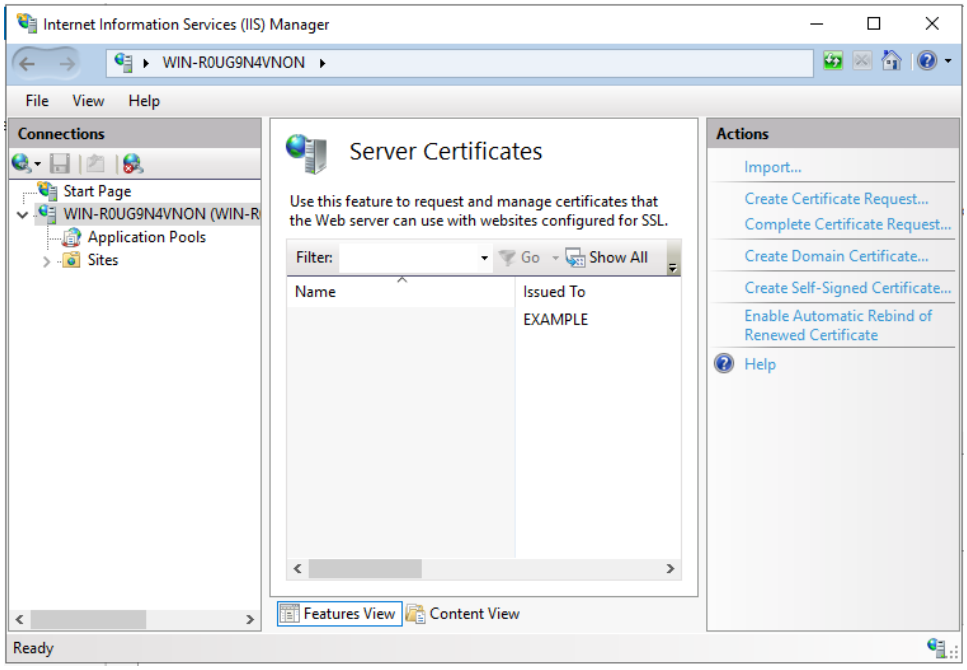
2.2. Setting Up Internet Information Services (IIS) For Certification Authority Web Enrollment (optional)

This section will describe how to set up Internet Information Services for Certification Authority Web Enrollment, you will need a proper SSL certificate for this.

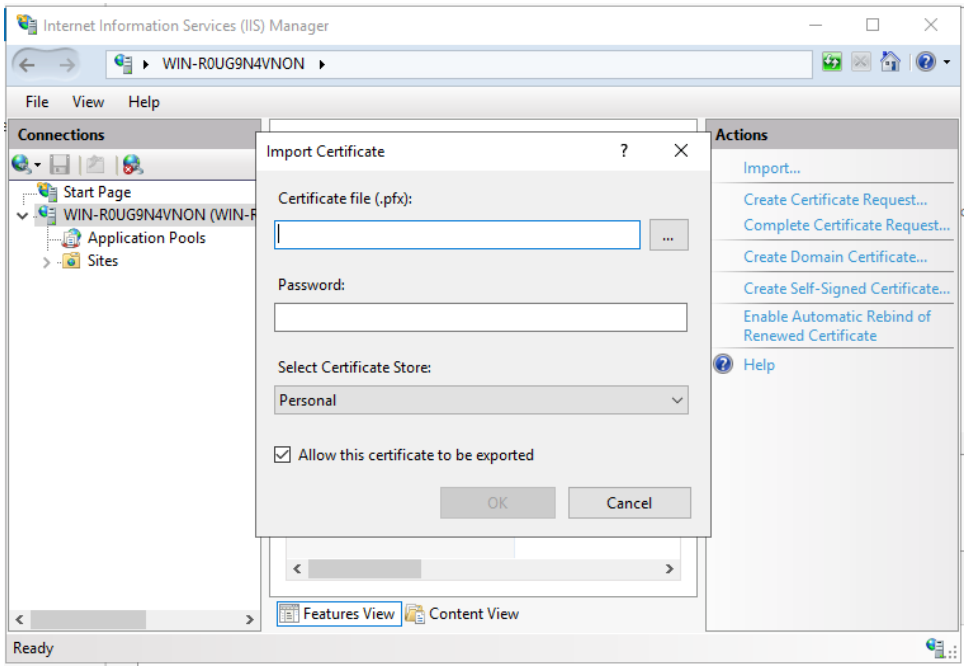
1. From the **Server Manager Tools** dropdown menu, select **Internet Information Services**.



2. In the **Connections** list (on the left), select your server
   a) Locate the **Server Certificates** feature. Right click on the icon and select **Open Feature**

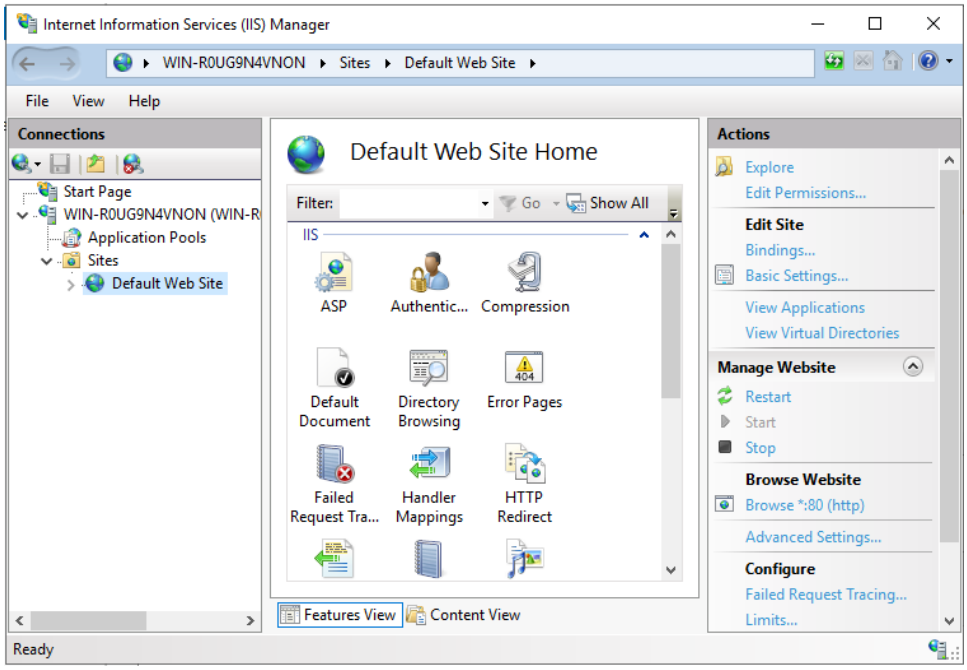


b) Under the **Actions** table on the right, select I**mport...**



c) Import your SSL certificate

3. Double click on your server name in the **Connections** list on the left
4. Double click on **Sites** in the dropdown menu
5. Click on **Default Web Site**

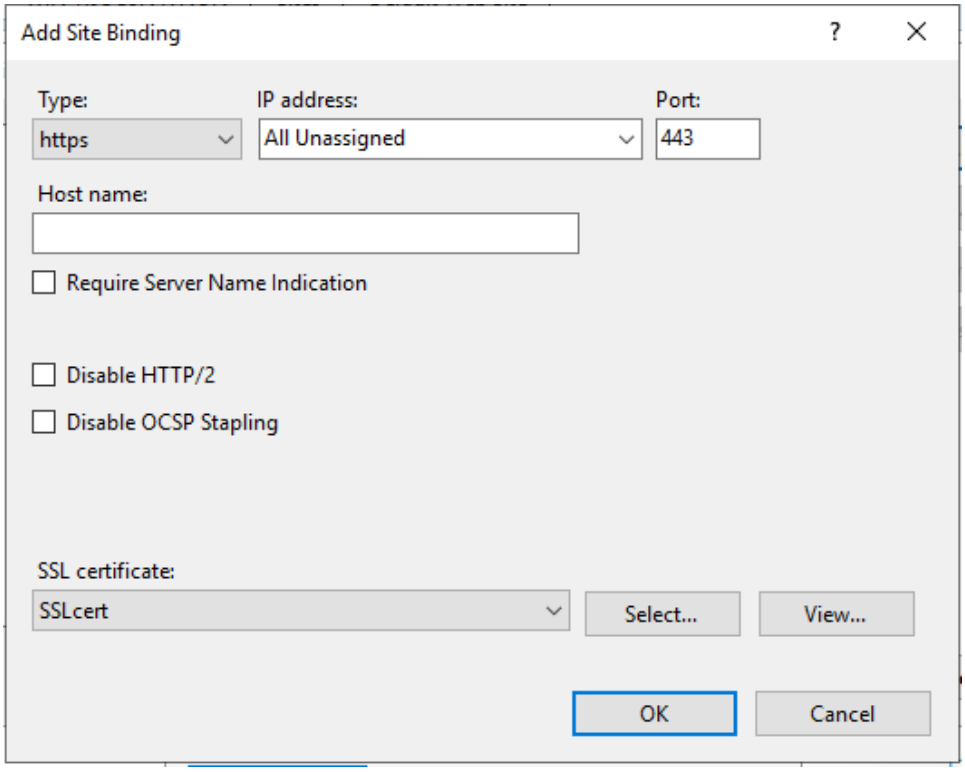


a) Select **Bindings** in the **Actions** panel on the right

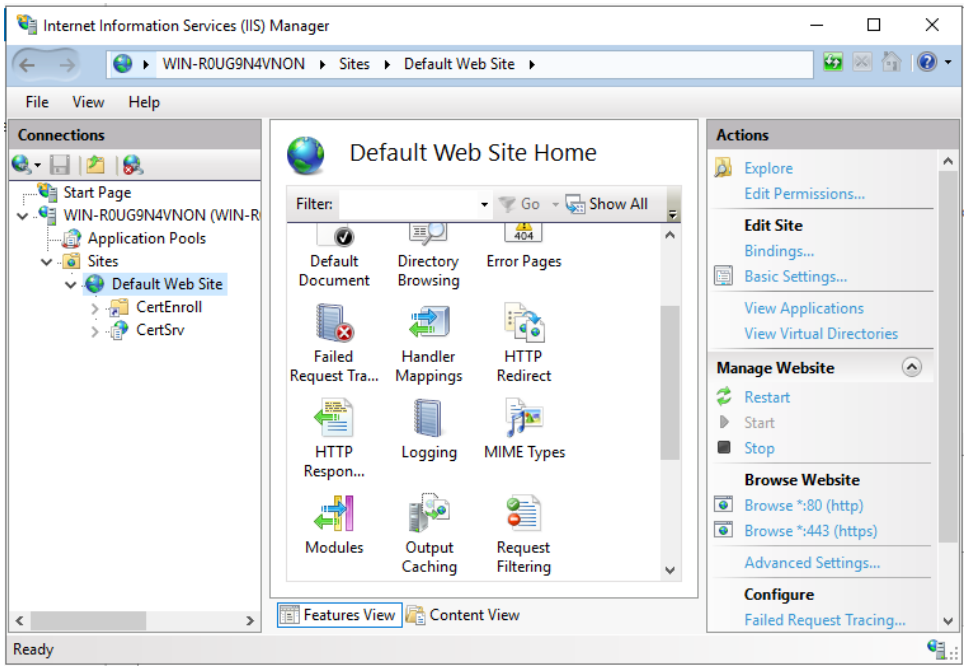
b) Click **Add...**

c) Change the type to https

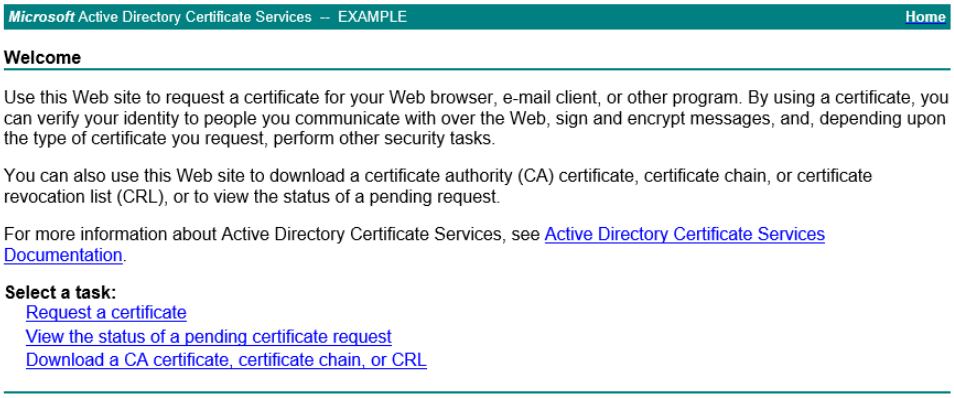
d) Select your SSL certificate



6. Double click on the **Default Web Site** item in the **Connections** list
7. Click on **CertSrv** and then click on **Browse *:443 (https)** in the **Actions** panel



8. You should now have access to the **Microsoft Active Directory Services web interface**



2.3. Using MSCA

These are brief snippets of some of the basic functions the MSCA can do, for full details, please consult the Microsoft documentation.

2.3.1. Import CSR

2.3.1.1. Via web

1. Open a Web browser.
2. You can open **https://*servername*/certsrv**, where *servername* is the name of the server hosting the CA Web enrollment pages or open the browser as we did in step 7 of the previous section.
3. Click **Request a Certificate** then select **advanced certificate request**
4. On Request a Certificate, select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.

Note: The first option, create and submit a request to this CA cannot be chosen due to the BlackVault HSM only accepting one transaction at a time.

5. On the **Submit a Certificate Request or Renewal Request** page, paste your CSR, select your template, and add any additional attributes.
6. Click **Submit**.
7. Do one of the following:
    a. If the **Certificate Pending** web page appears, see Check on a Pending Certificate Request for the procedure to check on a pending certificate.
    b. If the Certificate Issued Web page appears, click Install this certificate.

2.3.1.2. Via certsrv

1. In the **Server Manager** application, in the **Tools** dropdown menu, select **Certification Authority.**
2. Select the CA from the pool you wish to request a certificate from.
3. In the **Action** menu, point to **All Tasks**, and then click **Submit New Request**.
4. This will open a menu; browse to the certificate you want to import and click **Open.**

2.3.2. Issue certificate

2.3.2.1. Via certsrv

1. In the **Server Manager** application, in the **Tools** dropdown menu, select **Certification Authority.**
2. In the console tree, click **Pending Requests.**
3. In the details pane, left click the certificate you want to issue.
4. On the **Action** menu, point to **All Tasks**, and click **Issue**

2.3.3. Export cert

2.3.3.1. Via web

1. Open a Web browser.
2. You can open **https://*servername*/certsrv**, where *servername* is the name of the server hosting the CA Web enrollment pages or open the browser as we did in step 7 of the previous section.
3. Click **Download a CA certificate, certificate chain, or CRL**.
4. Click the encoding method that you want to use for the CRL, **DER** or **Base 64**.
5. Do one of the following:
    - Click **Download CA certificate**.
    - Click **Download CA certificate chain**.
    - Click **Download latest base CRL**.
    - Click **Download latest delta CRL**.
6. When the **File Download** dialog box appears, click **Save**. Select a folder on your computer to store the .crl file, and then click **Save**.
7. Open Windows Explorer and locate the .crl file you just saved.
8. Right-click the .cer or .crl file and click **Install Certificate** or **Install CRL**, and then click **Next**.
9. When the Certificate Import Wizard opens, click **Automatically select the certificate store based on the type of certificate**.

2.3.3.2. Via certsrv

1. In the Start Menu, under administrative tools click on **Certification Authority**
2. In the console tree under the logical store that contains the certificate to export, click **Certificates**.
3. In the details pane, click the certificate that you want to export.
4. On the **Action** menu, point to **All Tasks**, and then click **Export**.
5. In the Certificate Export Wizard, click **No, do not export the private key**. (This option will appear only if the private key is marked as exportable and you have access to the private key.)
6. Provide the following information in the Certificate Export Wizard:
    - Click the file format that you want to use to store the exported certificate: a DER-encoded file, a Base64-encoded file, or a PKCS #7 file.
    - If you are exporting the certificate to a PKCS #7 file, you also have the option to include all certificates in the certification path.
7. If required, in **Password**, type a password to encrypt the private key you are exporting. In **Confirm password**, type the same password again, and then click **Next**.
8. In **File name**, type a file name and path for the PKCS #7 file that will store the exported certificate and private key. Click **Next**, and then click **Finish**.

2.3.4. Revoke cert

2.3.4.1. Via certsrv

1. In the **Server Manager** application, in the **Tools** dropdown menu, select **Certification Authority.**
2. In the console tree, click **Issued Certificates**.
3. In the details pane, left click the certificate you want to revoke.
4. On the **Action** menu, point to **All Tasks**, and click **Revoke Certificate**.
5. Select the reason for revoking the certificate, adjust the time of the revocation, if necessary, and then click **Yes**.

The following reason codes are available:

- Unspecified
- Key Compromise
- CA Compromise
- Change of Affiliation
- Superseded
- Cease of Operation
- Certificate Hold