Implement CA Signed Certificates in a CCE 12.6 Solution

Contents

Introduction
Prerequisites
Requirements
Components Used
Background
Procedure
CCE Windows Based Servers
1. Generate CSR
2. Obtain the CA Signed Certificates
3. Upload the CA Signed Certificates
4. Bind the CA-Signed Certificate to IIS
5. Bind the CA-Signed Certificate to Diagnostic Portico
6. Import the Root and Intermediate Certificate into Java Keystore
CVP Solution
1. Generate Certificates with FQDN
2. Generate the CSR
3. Obtain the CA Signed Certificates
4. Import the CA Signed Certificates
VOS Servers
1. Generate CSR Certificate
2. Obtain the CA Signed Certificates
3. Upload the Application and Root Certificates
Verify
Troubleshoot
RelatedInformation

Introduction

This document describes how to Implement Certificate Authority (CA) Signed certificates in Cisco Contact Center Enterprise (CCE) solution.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Unified Contact Center Enterprise (UCCE) Release 12.6.2
- Package Contact Center Enterprise Release 12.6.2
- Customer Voice Portal (CVP) Release 12.6.2
- Cisco Virtualized Voice Browser (VVB)
- Cisco CVP Operations and Administration Console (OAMP)
- Cisco Unified Intelligence Center (CUIC)

- Cisco Unified Communication Manager (CUCM)

Components Used

The information in this document is based on these software versions:

- PCCE 12.6.2
- CVP 12.6.2
- Cisco VVB 12.6.2
- Finesss 12.6.2
- CUIC 12.6.2
- Windows 2019

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background

Certificates are used to ensure that communication is secure with the authentication between clients and servers. Users can purchase certificates from a CA or they can use self-signed certificates.

Self-signed certificates (as the name implies) are signed by the same entity whose identity they certify, as opposed to be signed by a certificate authority. Self-signed certificates are not considered to be as secure as CA certificates, but they are used by default in many applications.

In the Package Contact Center Enterprise (PCCE) solution version 12.x all components of the solution are controlled by Single Pane of Glass (SPOG), which is hosted in the principal Admin Workstation (AW) server.

Due to Security Management Compliance (SRC) in the PCCE 12.5(1) version, all communication between SPOG and other components in the solution are done via secure HTTP protocol.

This document explains in detail the steps needed to implement CA signed certificates in a CCE Solution for secure HTTP communication. For any other UCCE security considerations, refer to UCCE Security Guidelines.

For any additional CVP secure communication different from secure HTTP, refer to the security guidelines in the CVP Configuration guide: CVP Security Guidelines.

> **Note**: This document applies to CCE version 12.6 ONLY. See related information section for links to other versions.

Procedure

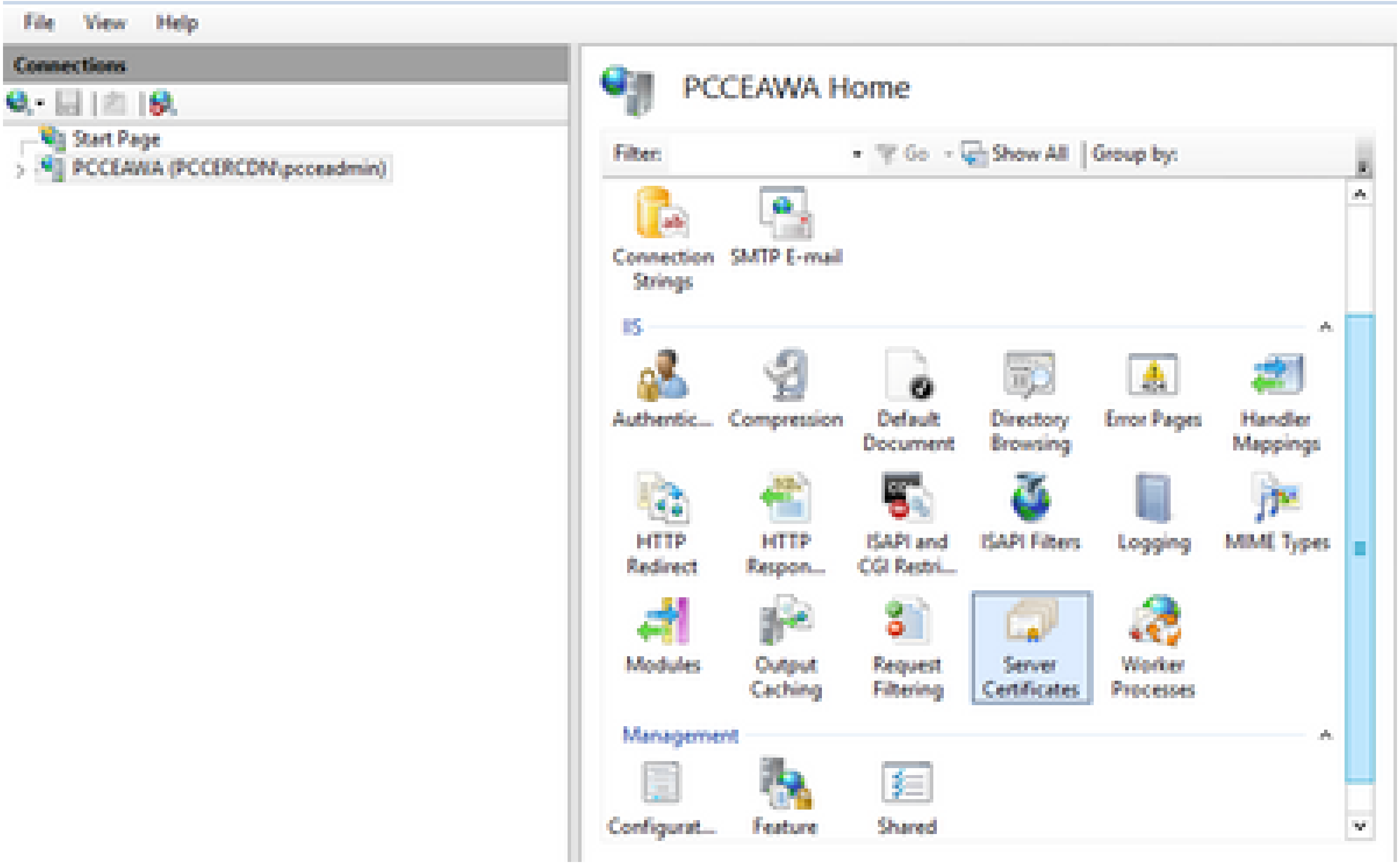
CCE Windows Based Servers

1. Generate CSR

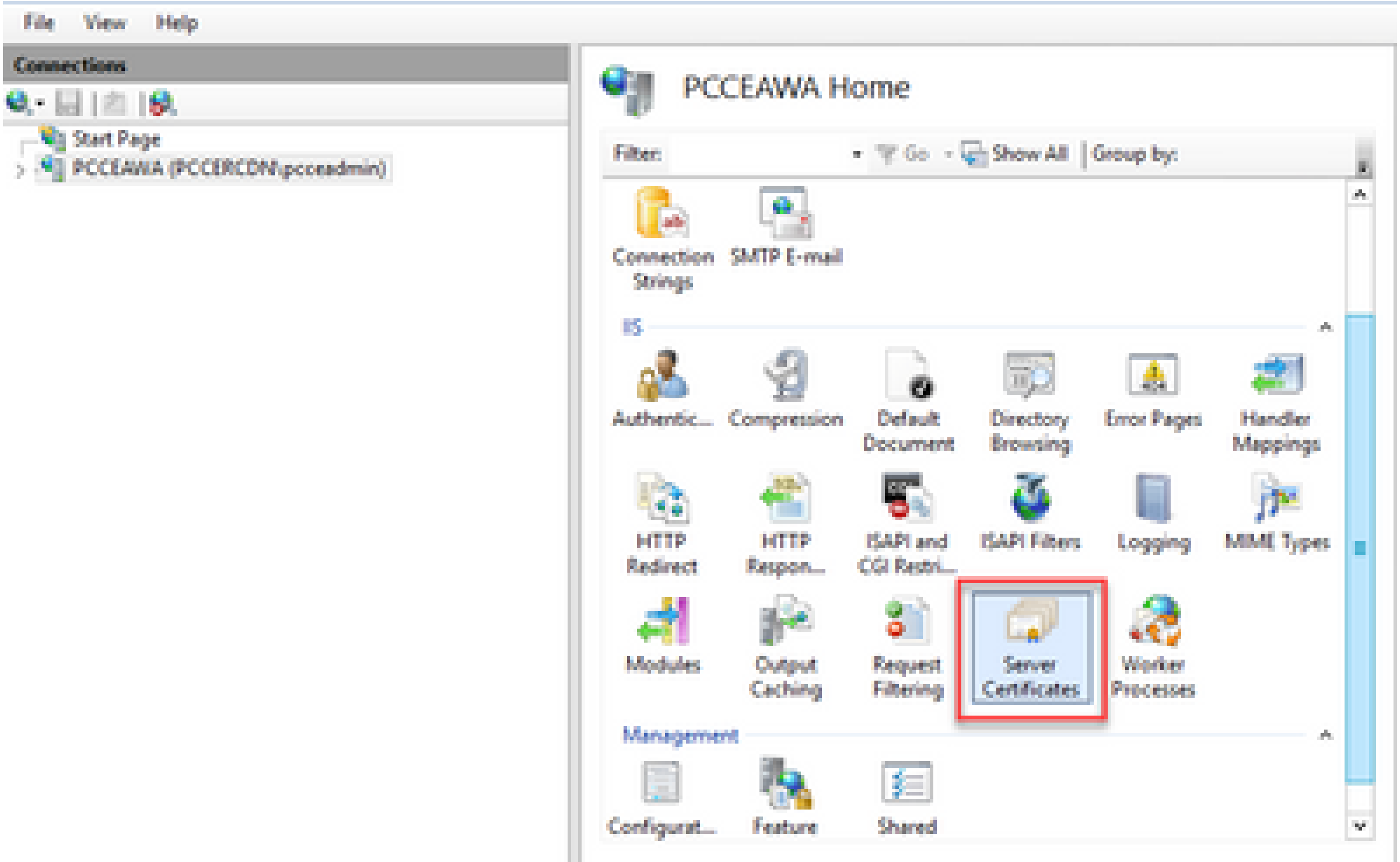
This procedure explains how to generate a Certificate Signing Request (CSR) from Internet Information Services (IIS) Manager.

Step 1. Log in to Windows and choose **Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.

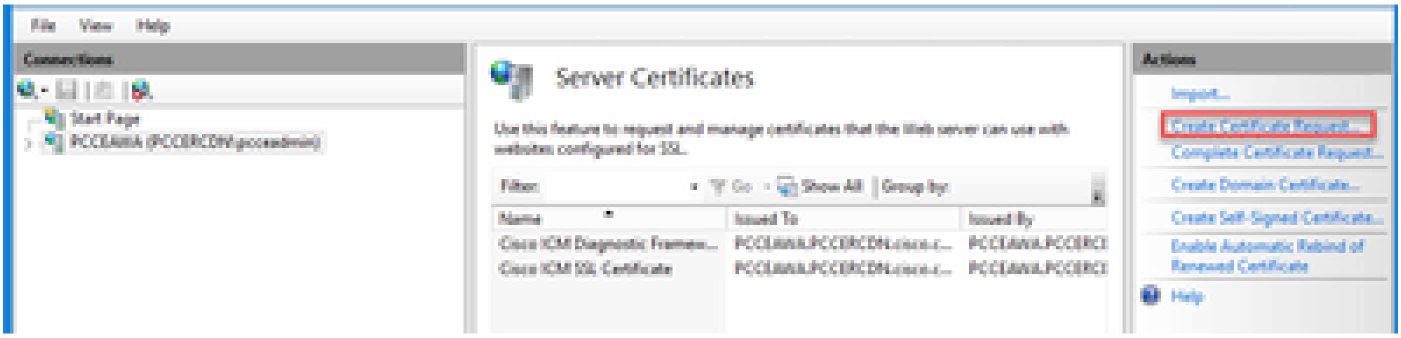
Step 2. In the Connections pane, click the server name. The server Home pane appears.



Step 3. In the IIS area, double-click Server Certificates.



Step 4. In the Actions pane, click **Create Certificate Request**.

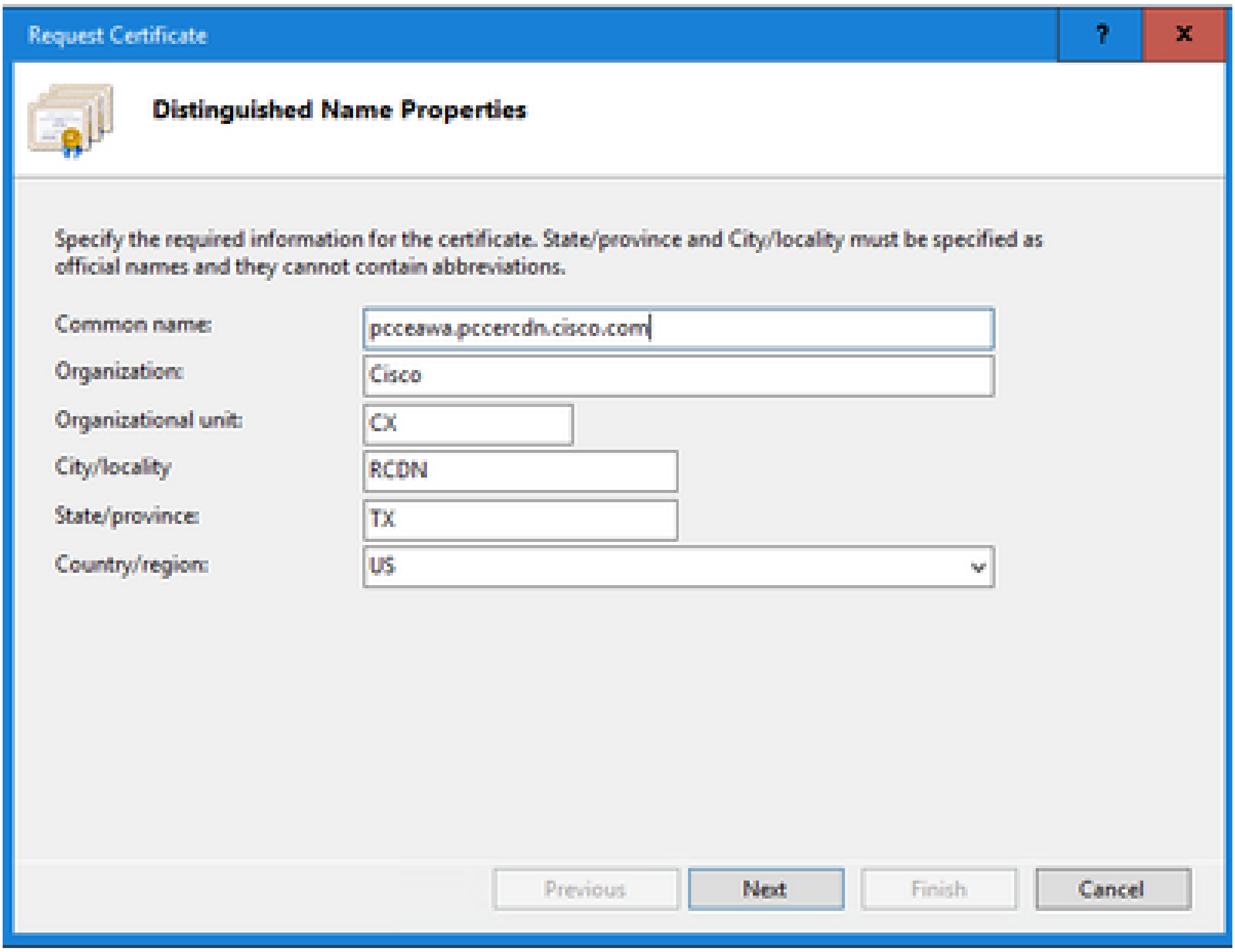

File
View
Help
Connections
Start Page
PCCEAWA (PCCERCDN\pcceadmin)
Server Certificates
Filter:
Go
Show All
Group by:
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

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

Name	Issued To	Issued By
Cisco ICM Diagnostic Framew...	PCCEAWA.PCCERCDN.cisco.c...	PCCEAWA.PCCERCI
Cisco ICM SSL Certificate	PCCEAWA.PCCERCDN.cisco.c...	PCCEAWA.PCCERCI

Step 5. In the Request Certificate dialog box, do this:

Specify the required information in the displayed fields and click **Next**.



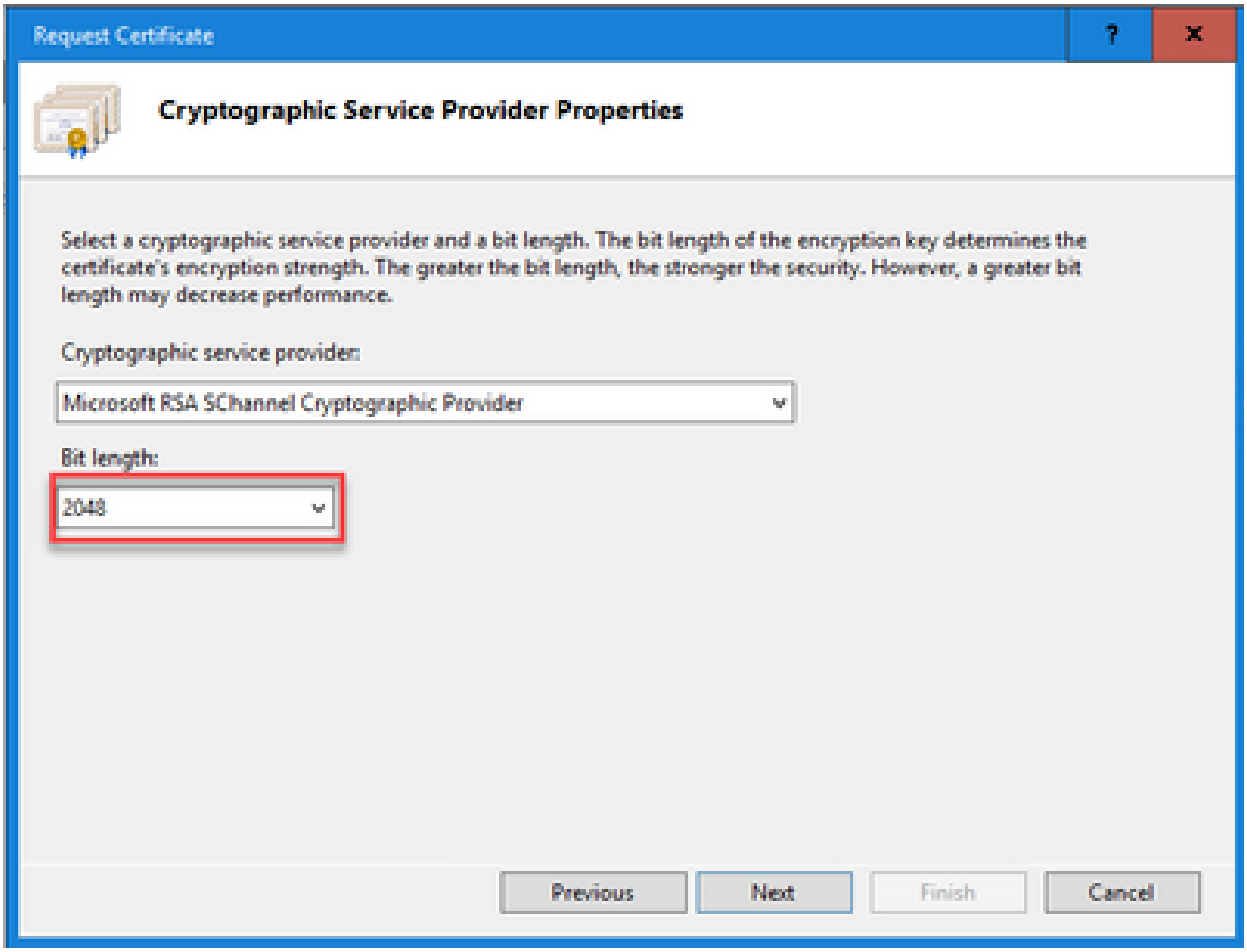
Distinguished Name Properties

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:	pcceawa.pccercdn.cisco.com
Organization:	Cisco
Organizational unit:	CX
City/locality	RCDN
State/province:	TX
Country/region:	US

In the Cryptographic service provider drop-down list, leave the default setting.

From the Bit length drop-down list, select **2048**.



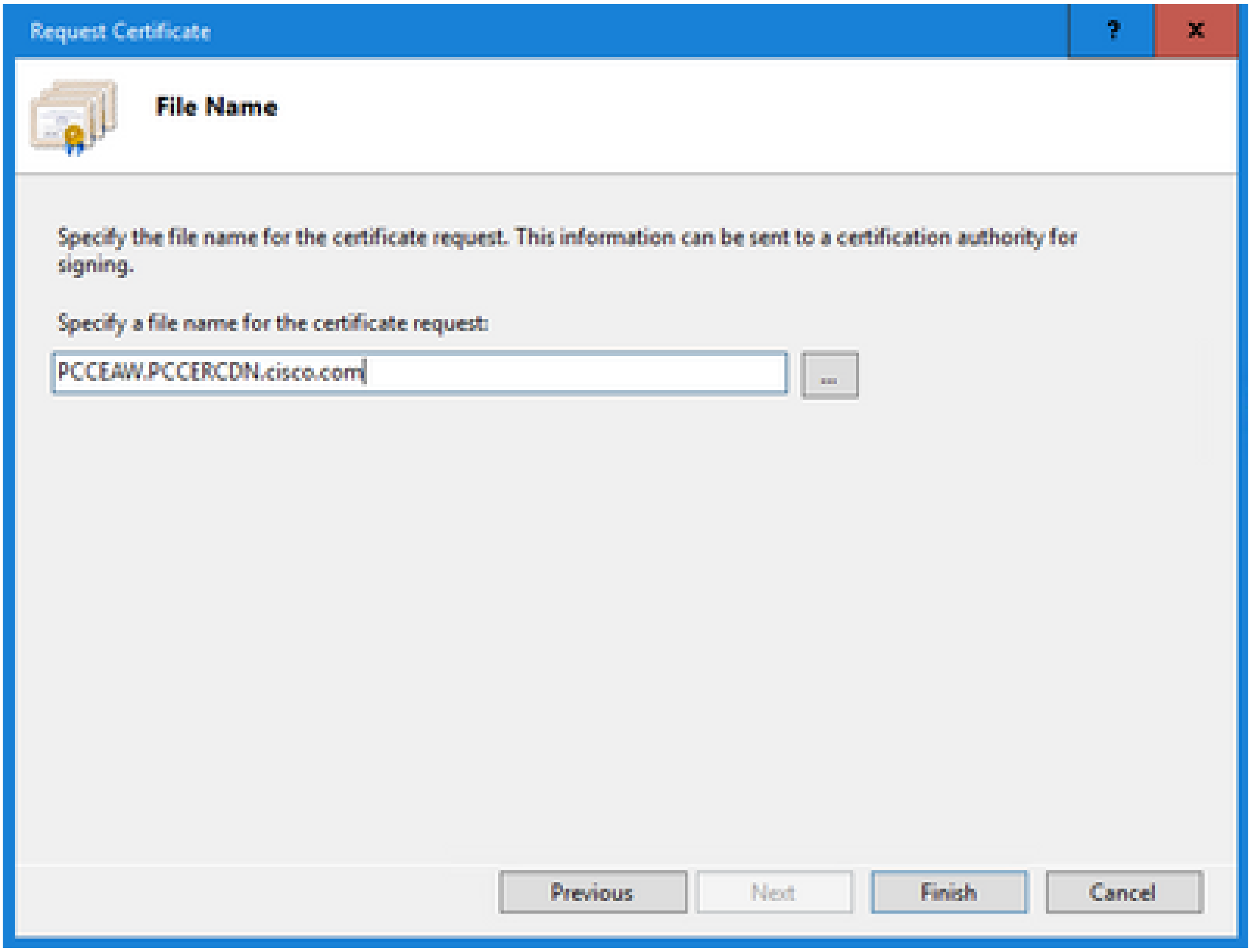
Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

Bit length: 2048

Step 6. Specify a file name for the certificate request and click **Finish**.



Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:

PCCEAW.PCCERCDN.cisco.com

2. Obtain the CA Signed Certificates

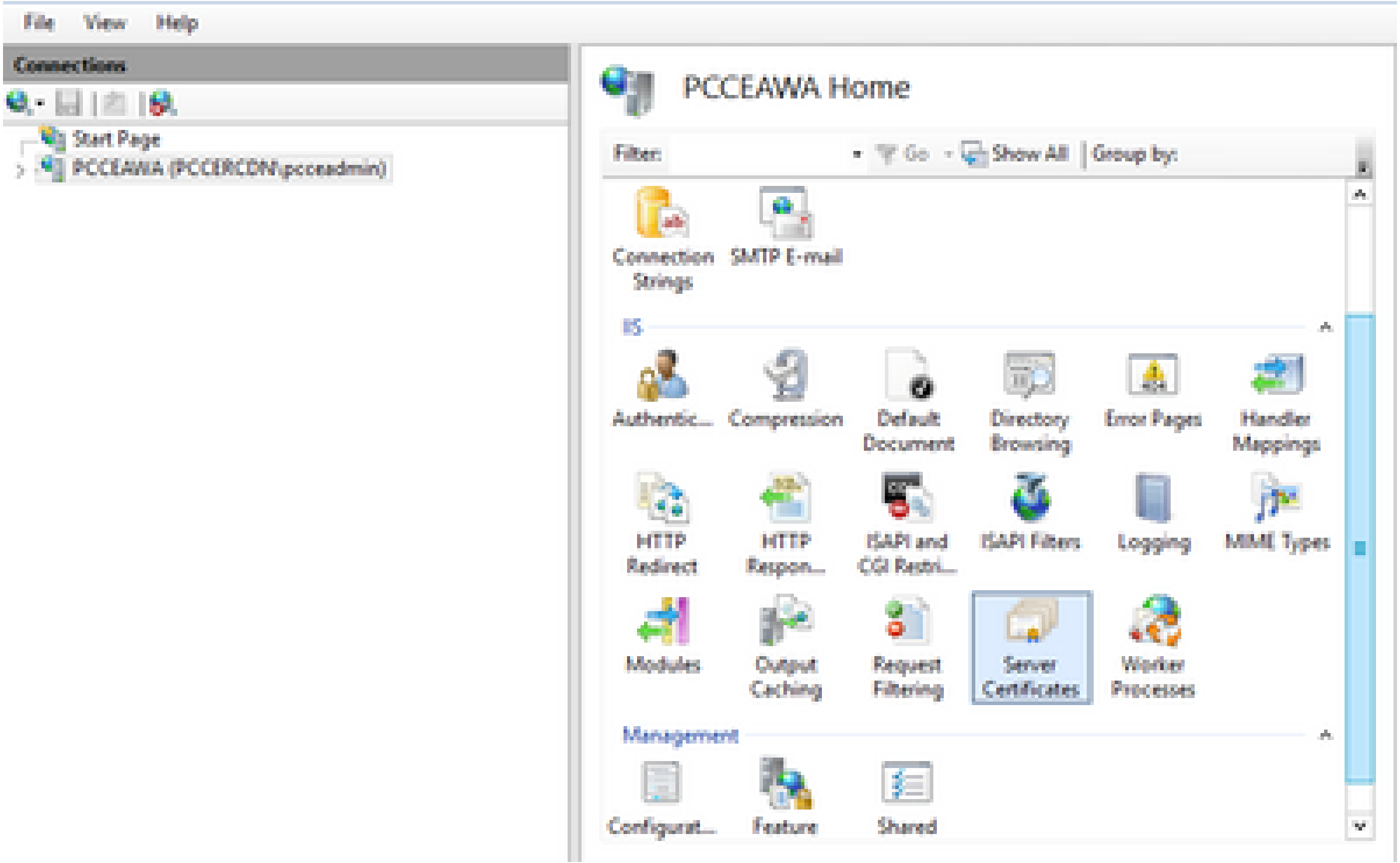
Step 1. Sign the certificate on a CA.

Note: Ensure that the certificate template used by the CA includes client and server authentication.

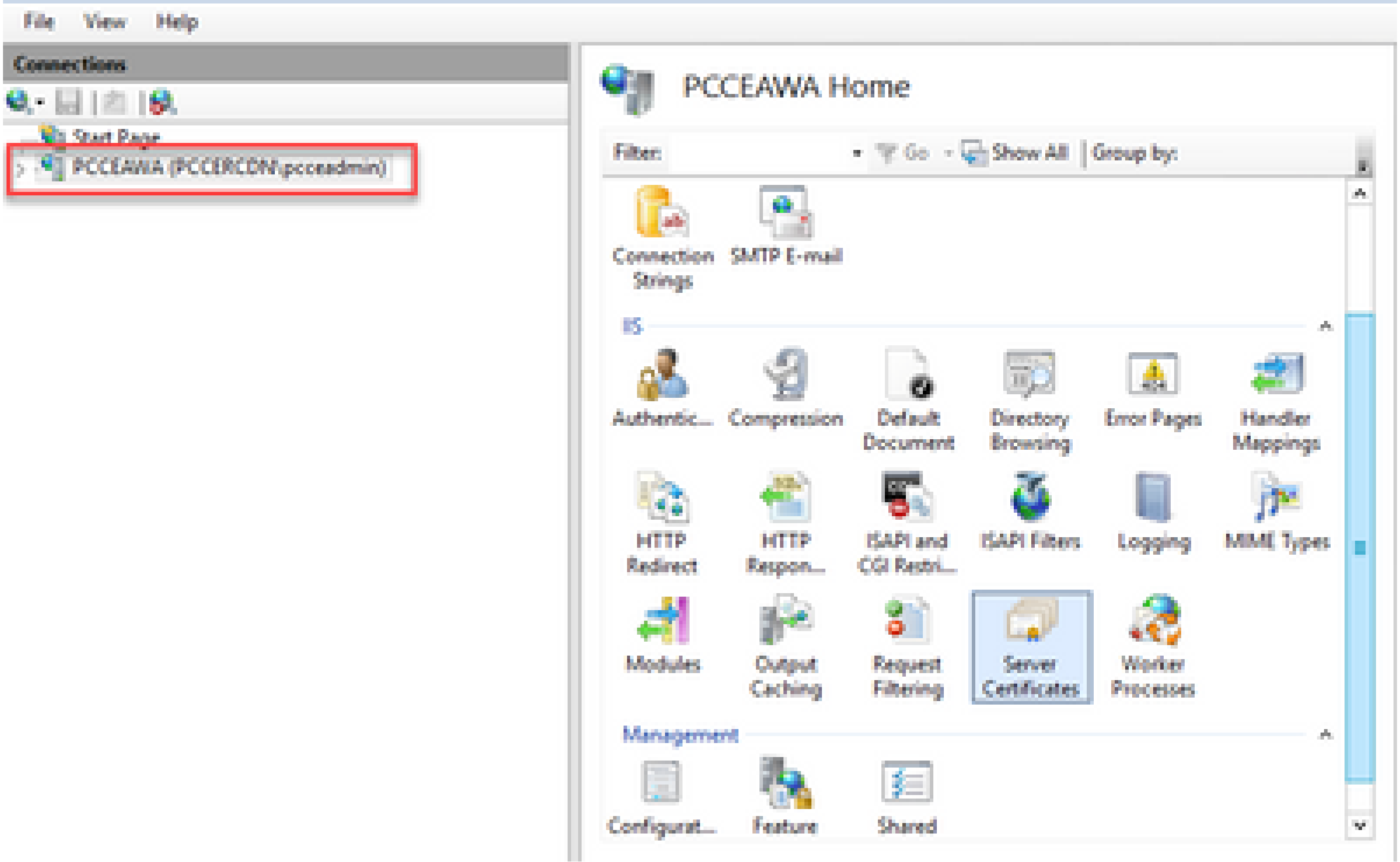
Step 2. Obtain the CA Signed Certificates from your Certificate Authority (Root, Application and Intermediate if any).

3. Upload the CA Signed Certificates

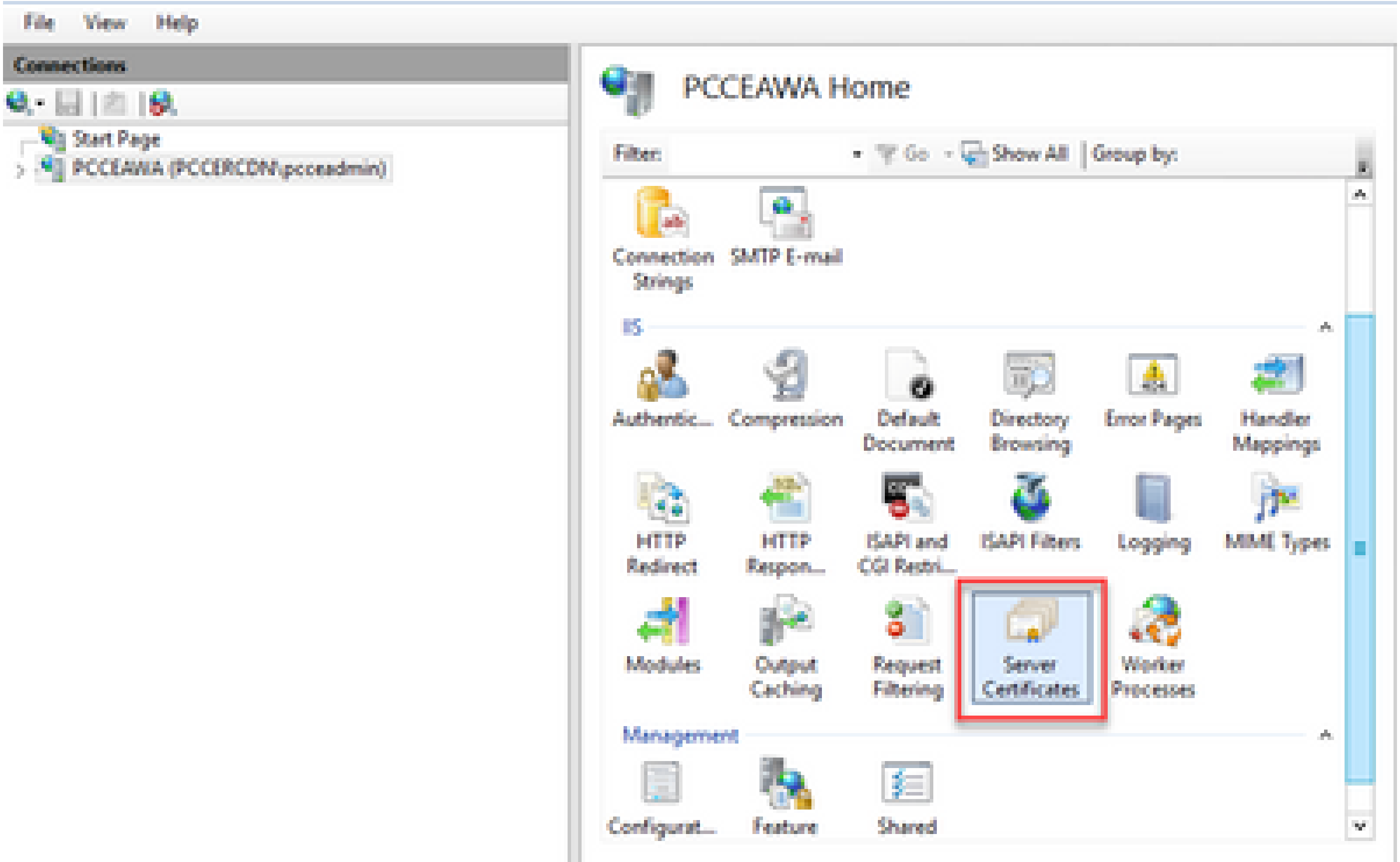
Step 1. Log in to Windows and choose **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.



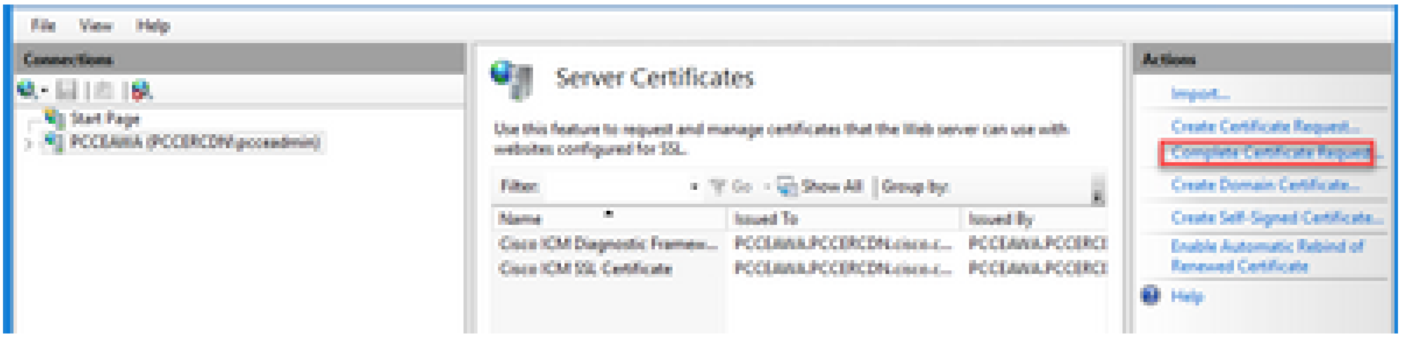
Step 2. In the Connections pane, click the server name.



Step 3. In the IIS area, double-click **Server Certificates**.



Step 4. In the Actions pane, click **Complete Certificate Request**.


File
View
Help
Connections
Start Page
PCCEAWA (PCCERCDN\pcceadmin)
Server Certificates
Filter:
Go
Show All
Group by:
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

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

Name	Issued To	Issued By
Cisco ICM Diagnostic Framew...	PCCEAWA.PCCERCDN.cisco.c...	PCCEAWA.PCCERCI
Cisco ICM SSL Certificate	PCCEAWA.PCCERCDN.cisco.c...	PCCEAWA.PCCERCI

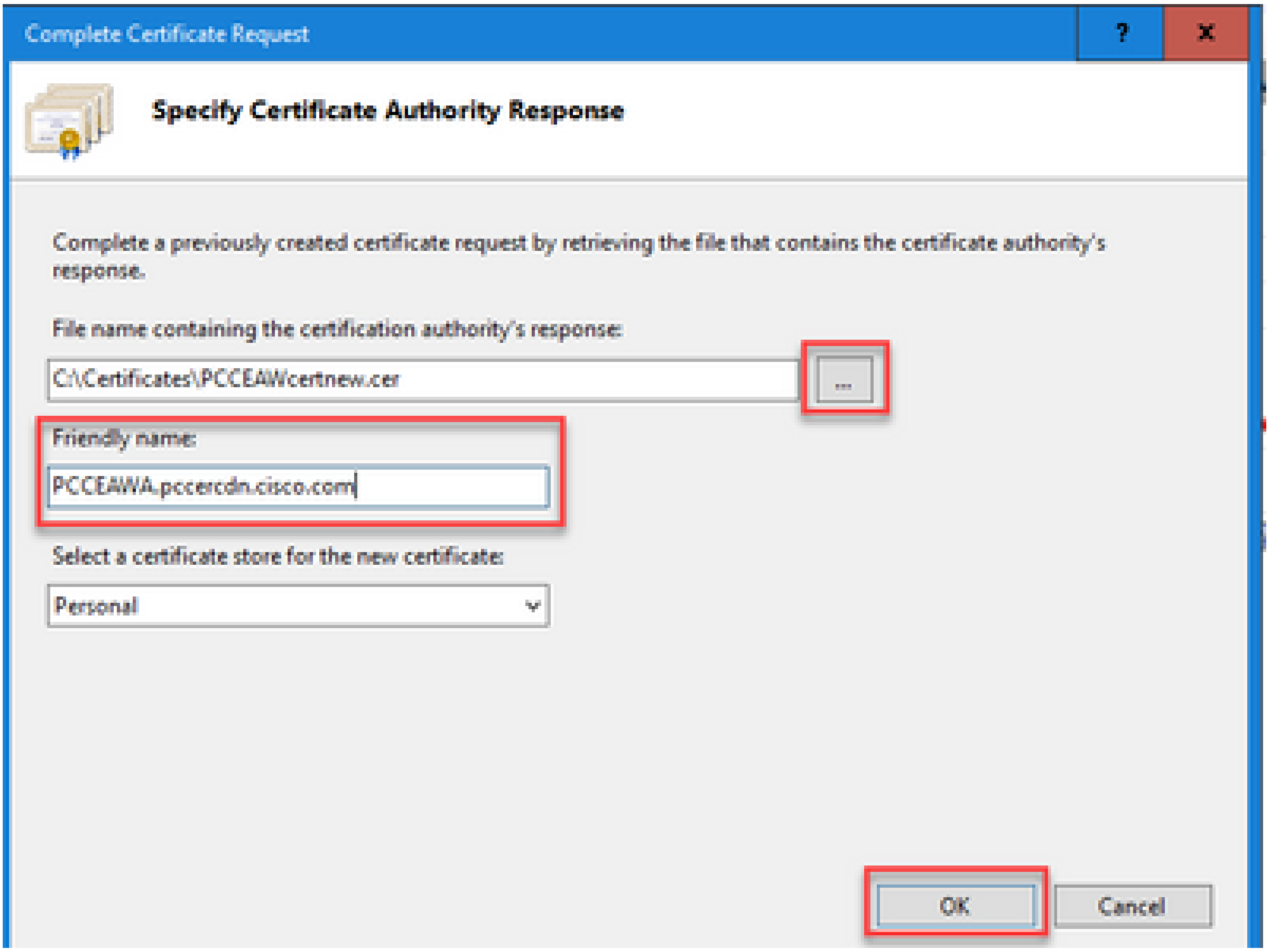
Step 5. In the Complete Certificate Request dialog box, complete these fields:

In the File name which contains the certification authority response field, click the … button.

Browse to the location where signed application certificate is stored and then click Open.

Note: If this is a 2-tier CA implementation and the root certificate is not already in the server certificate store, then the root needs to be uploaded to the Windows store before you import the signed cert. Refer to this document if you need to upload the root CA to the windows store Microsoft - Installing the Trusted Root Certificate.

In the Friendly name field, enter the Fully Qualified Domain Name (FQDN) of the server or any significant name for you. Ensure that the **Select a certificate store for the new certificate** drop-down remains as **Personal**.


Complete Certificate Request
?
x
Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

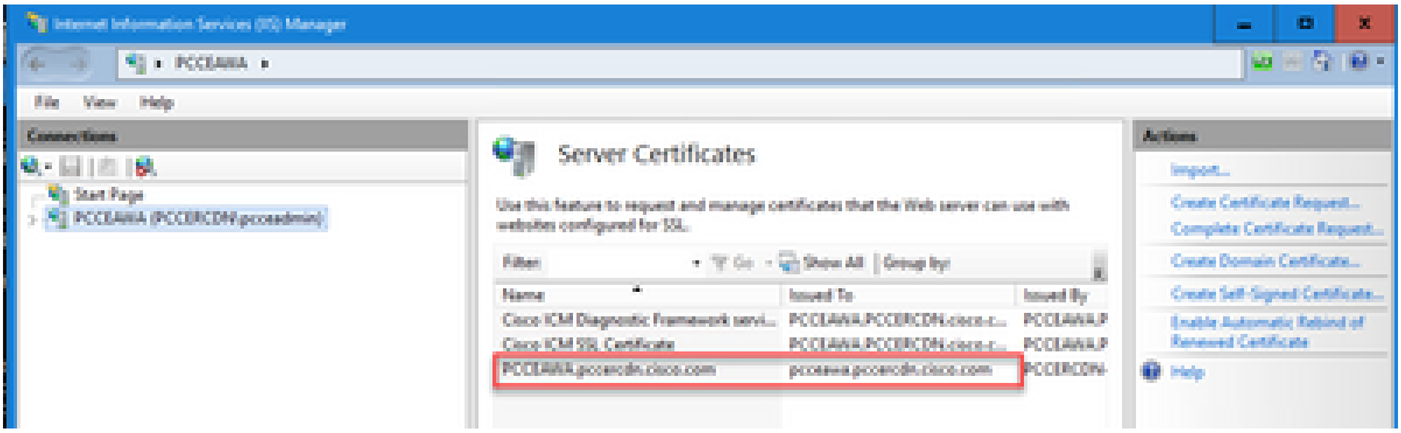
File name containing the certification authority's response:
C:\Certificates\PCCEAWcertnew.cer

Friendly name:
PCCEAWA.pccercdn.cisco.com

Select a certificate store for the new certificate:
Personal

Step 6. Click **OK** to upload the certificate.

If the certificate upload is successful, the certificate appears in the Server Certificates pane.


Internet Information Services (IIS) Manager
PCCEAWA
File
View
Help
Connections
Start Page
PCCEAWA (PCCERCDN\pccEadmin)
Server Certificates
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Filter:
Go
Show All
Group by:

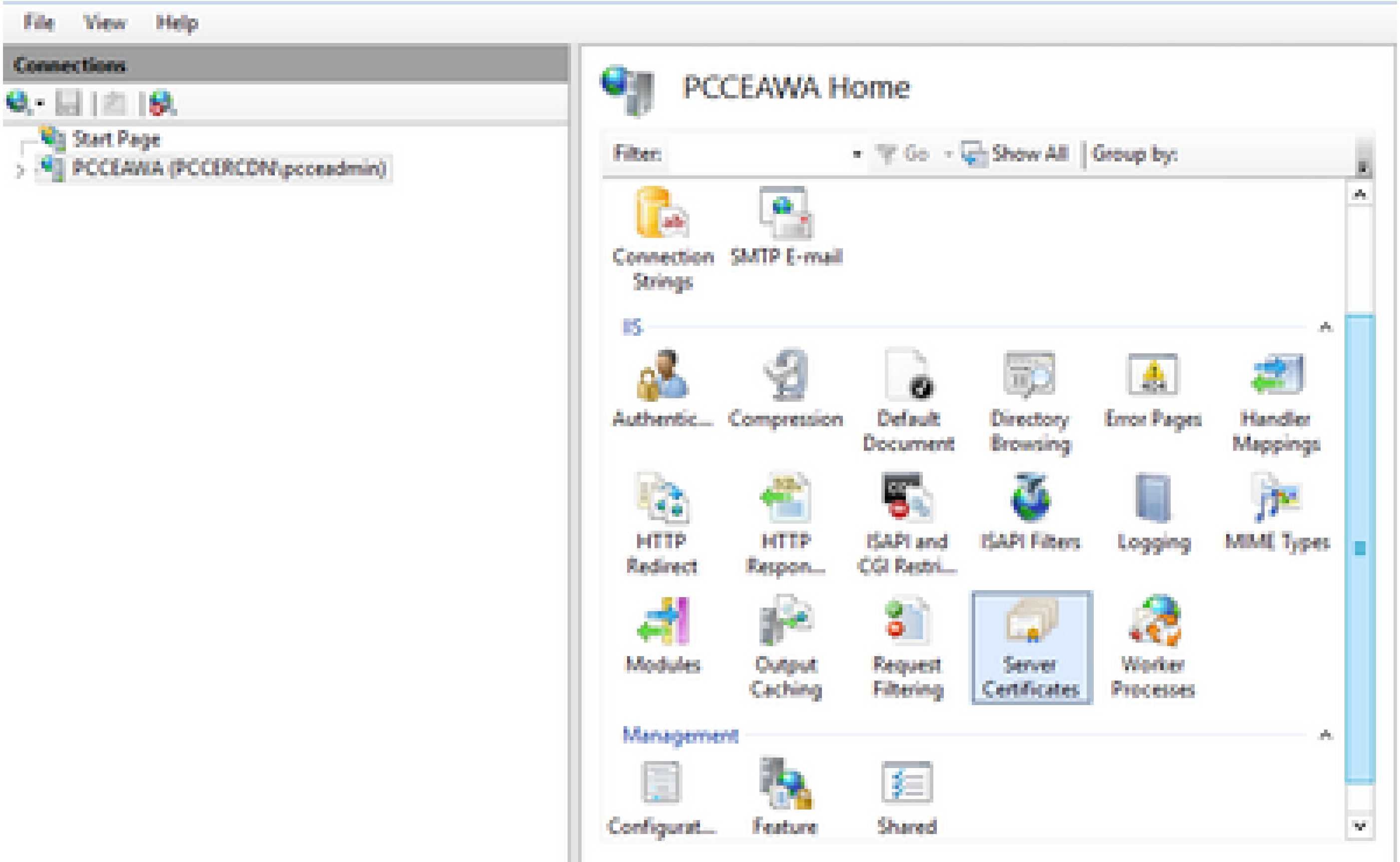
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By
Cisco ICM Diagnostic Framework servi...	PCCEAWA.PCCERCDN.cisco.c...	PCCEAWA.P
Cisco ICM SSL Certificate	PCCEAWA.PCCERCDN.cisco.c...	PCCEAWA.P
PCCEAWA.pccercdn.cisco.com	pcceawa.pccercdn.cisco.com	PCCERCDN-

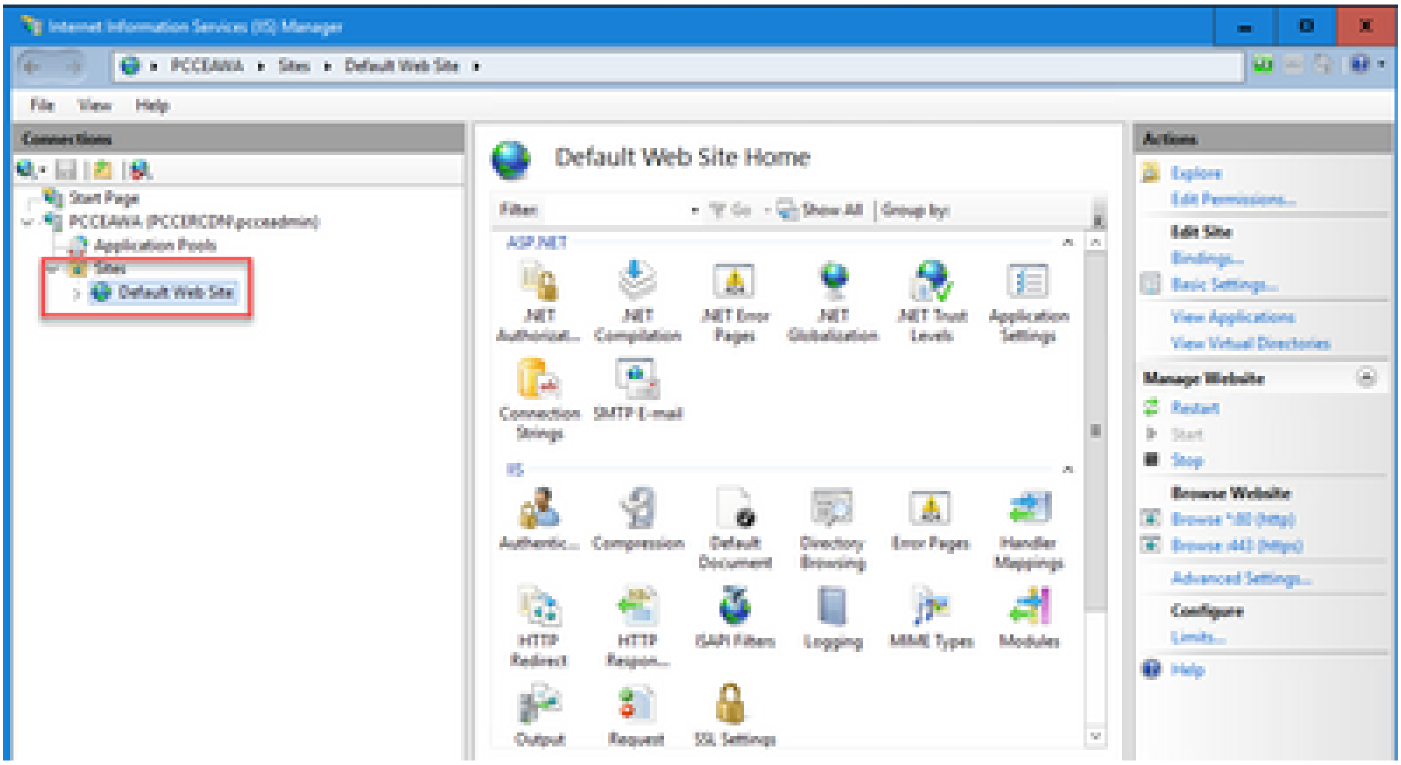
4. Bind the CA-Signed Certificate to IIS

This procedure explains how to bind a CA Signed certificate in the IIS Manager.

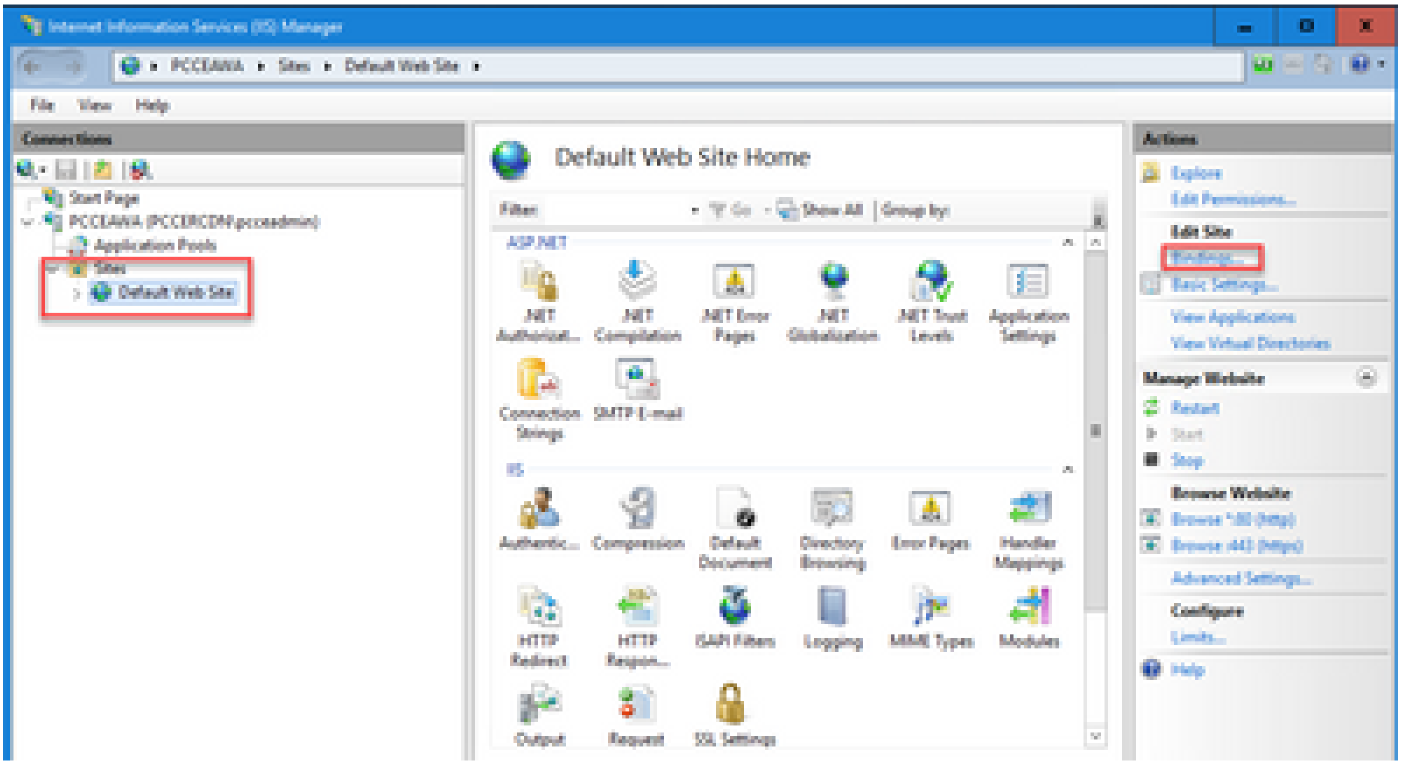
Step 1. Log in to Windows and choose **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.



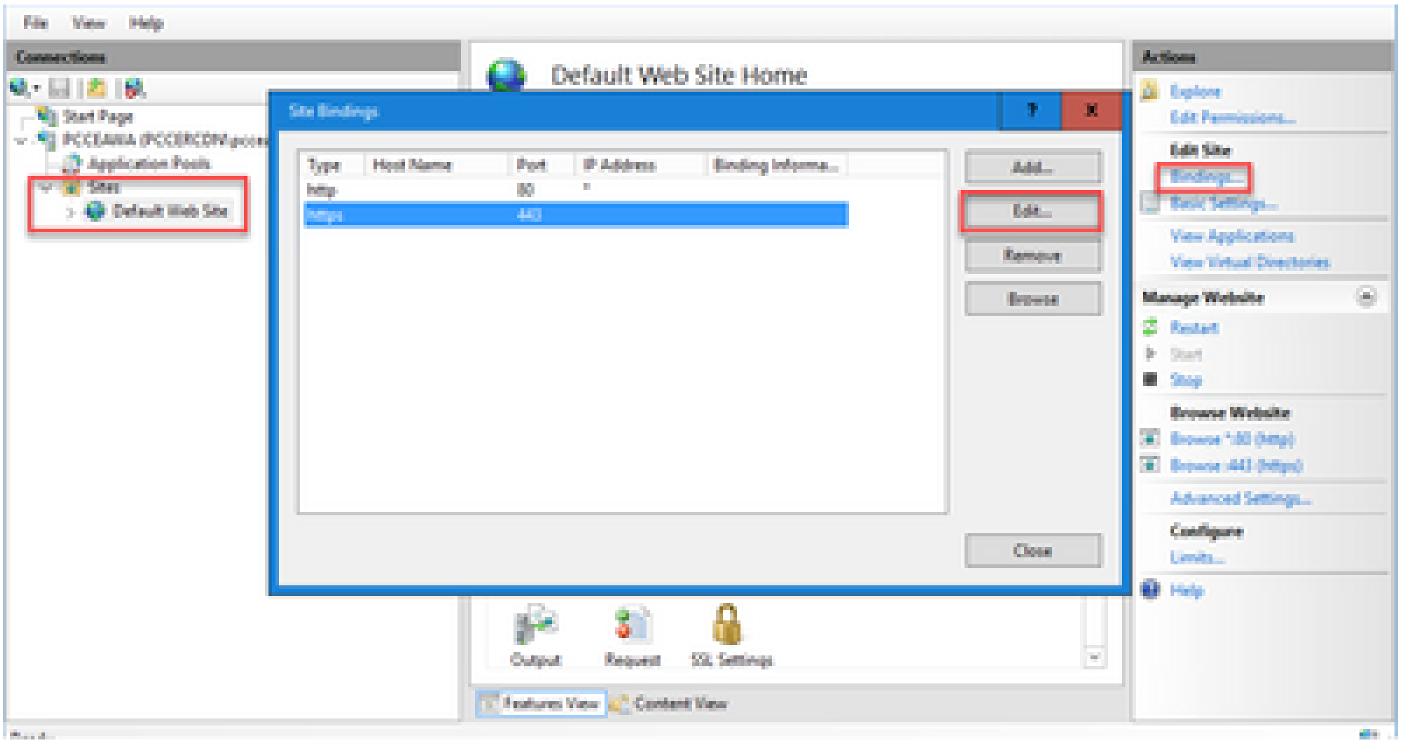
Step 2. In the Connections pane, choose **<server_name> > Sites > Default Web Site**.



Step 3. In the Actions pane, click **Bindings...**.

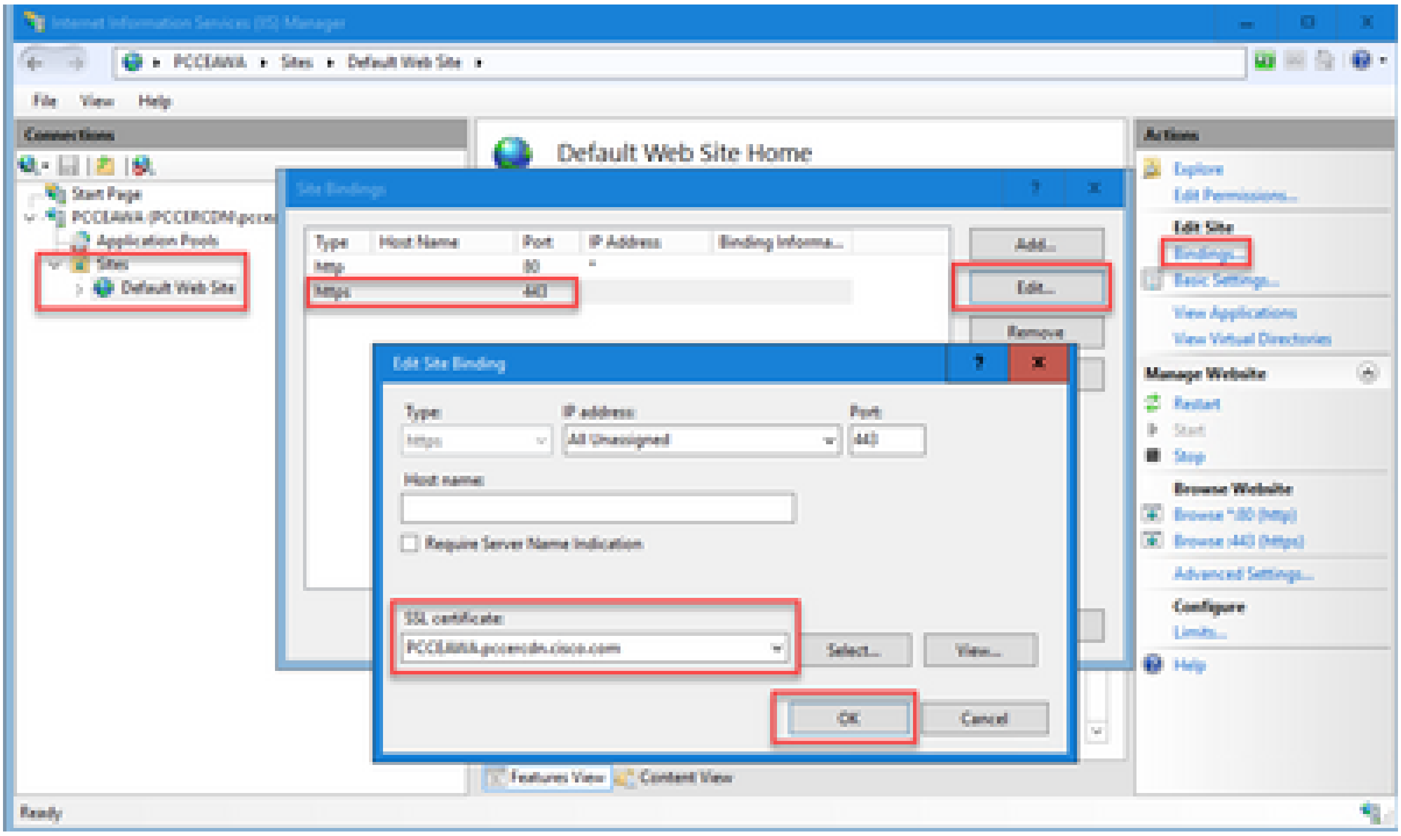


Step 4. Click the type **https** with port **443**, and then click **Edit...**.



Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443		

Step 5. From the SSL certificate drop-down list, select the certificate with the same friendly name as given in previous step.



Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443		

Type: https

IP address: All Unassigned

Port: 443

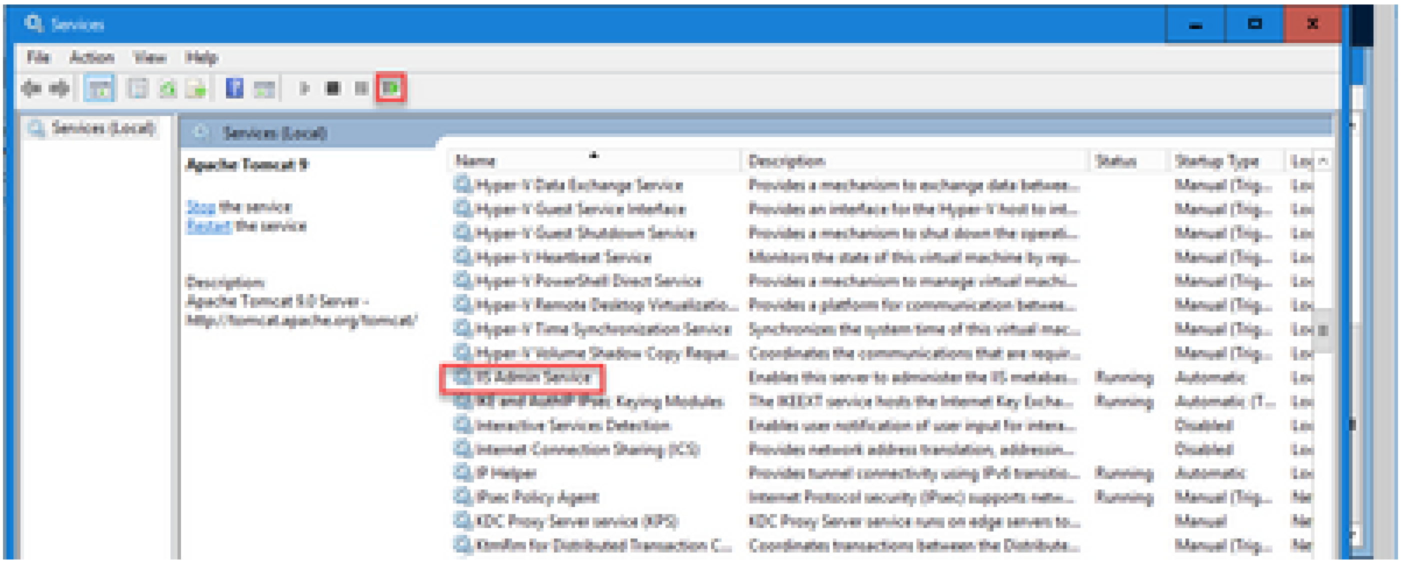
Host name:

□ Require Server Name Indication

SSL certificate: PCCEAWA.pccercdn.cisco.com

Step 6. Click **OK**.

Step 7. Navigate to **Start > Run > services.msc** and restart the IIS Admin Service.



Description:
Apache Tomcat 9.0 Server - http://tomcat.apache.org/tomcat/

Name	Description	Status	Startup Type	Lo
Hyper-V Data Exchange Service	Provides a mechanism to exchange data betwee...		Manual (Trig...	Loc
Hyper-V Guest Service Interface	Provides an interface for the Hyper-V host to int...		Manual (Trig...	Loc
Hyper-V Guest Shutdown Service	Provides a mechanism to shut down the operati...		Manual (Trig...	Loc
Hyper-V Heartbeat Service	Monitors the state of this virtual machine by rep...		Manual (Trig...	Loc
Hyper-V PowerShell Direct Service	Provides a mechanism to manage virtual machi...		Manual (Trig...	Loc
Hyper-V Remote Desktop Virtualizatio...	Provides a platform for communication betwee...		Manual (Trig...	Loc
Hyper-V Time Synchronization Service	Synchronizes the system time of this virtual mac...		Manual (Trig...	Loc
Hyper-V Volume Shadow Copy Reque...	Coordinates the communications that are requir...		Manual (Trig...	Loc
IIS Admin Service	Enables this server to administer the IIS metabas...	Running	Automatic	Loc
IKE and AuthIP IPsec Keying Modules	The IKEEXT service hosts the Internet Key Excha...	Running	Automatic (T...	Loc
Interactive Services Detection	Enables user notification of user input for intera...		Disabled	Loc
Internet Connection Sharing (ICS)	Provides network address translation, addressin...		Disabled	Loc
IP Helper	Provides tunnel connectivity using IPv6 transitio...	Running	Automatic	Loc
IPsec Policy Agent	Internet Protocol security (IPsec) supports netw...	Running	Manual (Trig...	Net
KDC Proxy Server service (KPS)	KDC Proxy Server service runs on edge servers to...		Manual	Net
KtmRm for Distributed Transaction C...	Coordinates transactions between the Distribute...		Manual (Trig...	Net

5. Bind the CA-Signed Certificate to Diagnostic Portico

This procedure explains how to bind a CA Signed Certificate in the Diagnostic Portico.

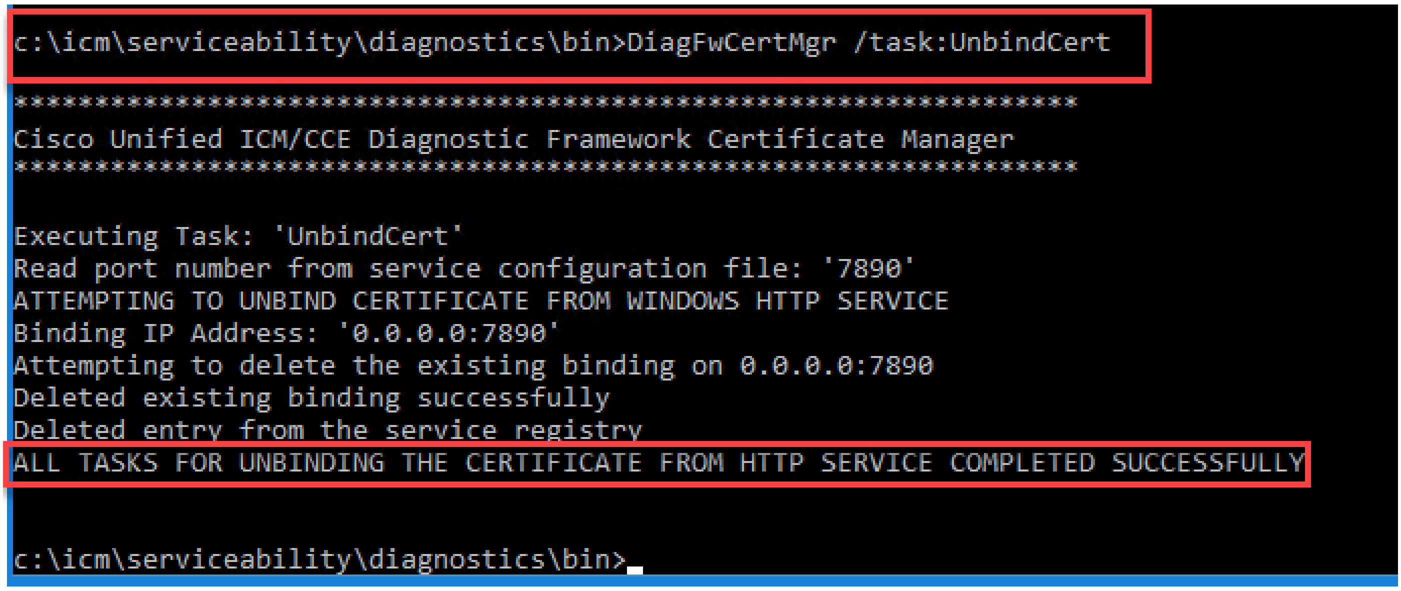
Step 1. Open the command prompt (Run as Administrator).

Step 2. Navigate to the Diagnostic Portico home folder. Run this command:

```
cd c:\icm\serviceability\diagnostics\bin
```

Step 3. Remove the current certificate binding to the Diagnostic Portico. Run this command:

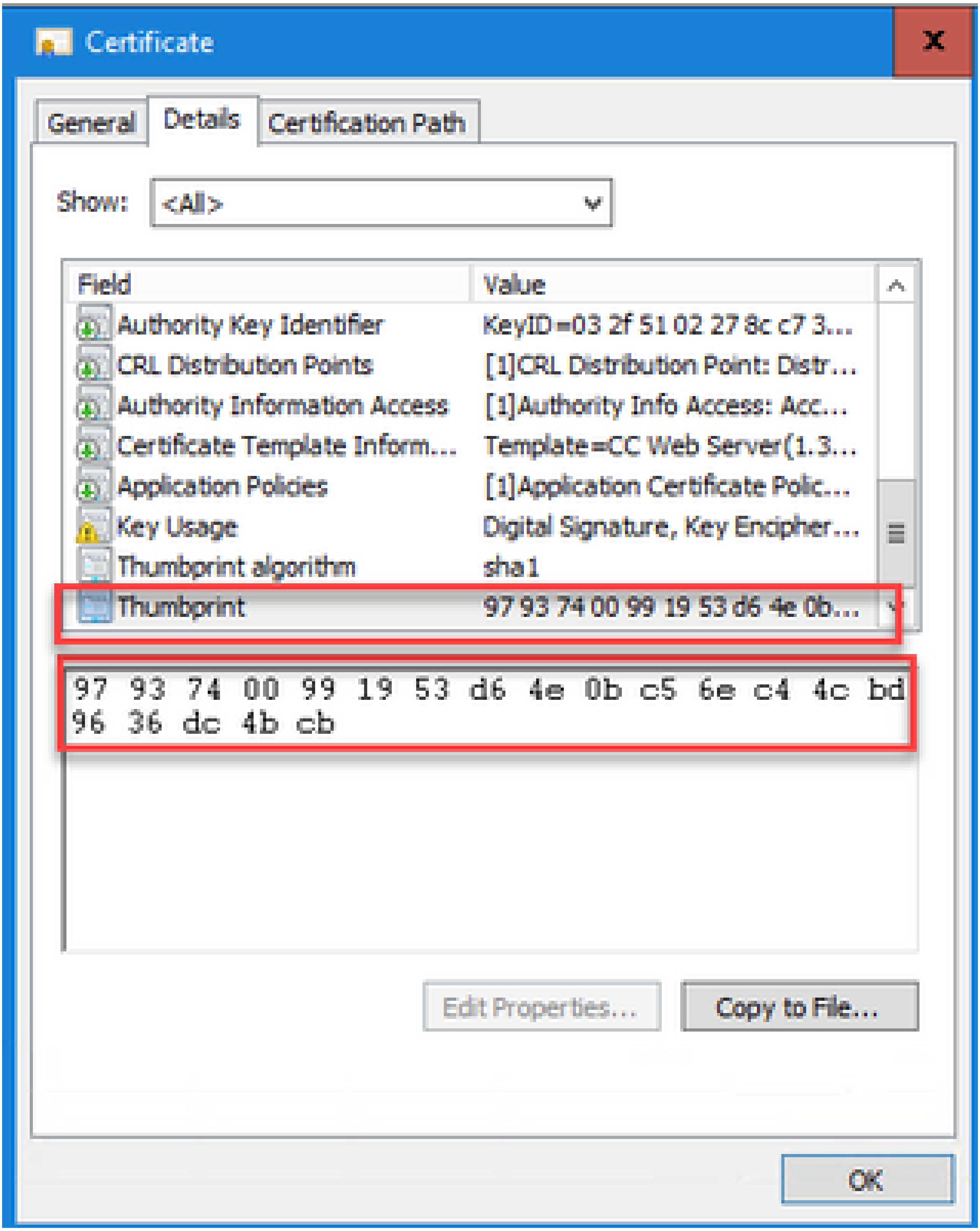
```
DiagFwCertMgr /task:UnbindCert
```



```
c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:UnbindCert

*******************************************************************
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
*******************************************************************

Executing Task: 'UnbindCert'
Read port number from service configuration file: '7890'
ATTEMPTING TO UNBIND CERTIFICATE FROM WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Attempting to delete the existing binding on 0.0.0.0:7890
Deleted existing binding successfully
Deleted entry from the service registry
ALL TASKS FOR UNBINDING THE CERTIFICATE FROM HTTP SERVICE COMPLETED SUCCESSFULLY

c:\icm\serviceability\diagnostics\bin>
```

Step 4. Open the signed certificate and copy the hash content (without spaces) of the Thumbprint field.

Note: Ensure to remove any hidden characters from the beginning or end of the hash content. An editor like Notepad++ can help you to identify these hidden characters.

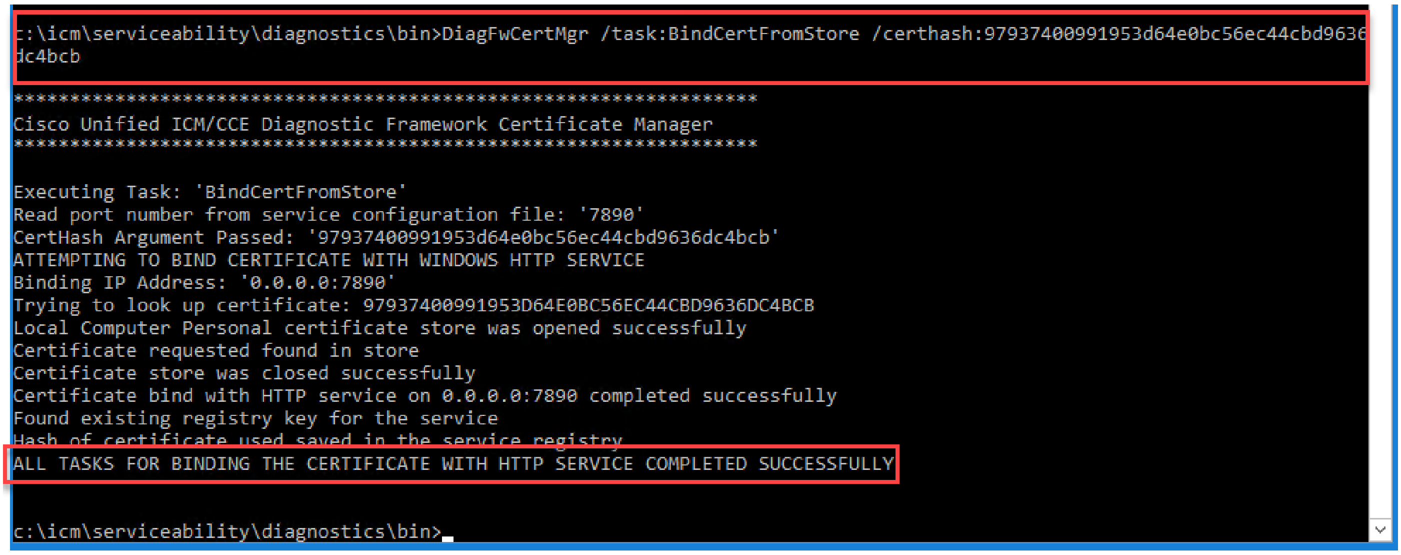


Field	Value
Authority Key Identifier	KeyID=03 2f 51 02 27 8c c7 3...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Certificate Template Inform...	Template=CC Web Server(1.3...
Application Policies	[1]Application Certificate Polic...
Key Usage	Digital Signature, Key Encipher...
Thumbprint algorithm	sha1
Thumbprint	97 93 74 00 99 19 53 d6 4e 0b...

```
97 93 74 00 99 19 53 d6 4e 0b c5 6e c4 4c bd
96 36 dc 4b cb
```

Step 5. Run this command and paste the hash content.

```
DiagFwCertMgr /task:BindCertFromStore /certhash:<hash_value>
```

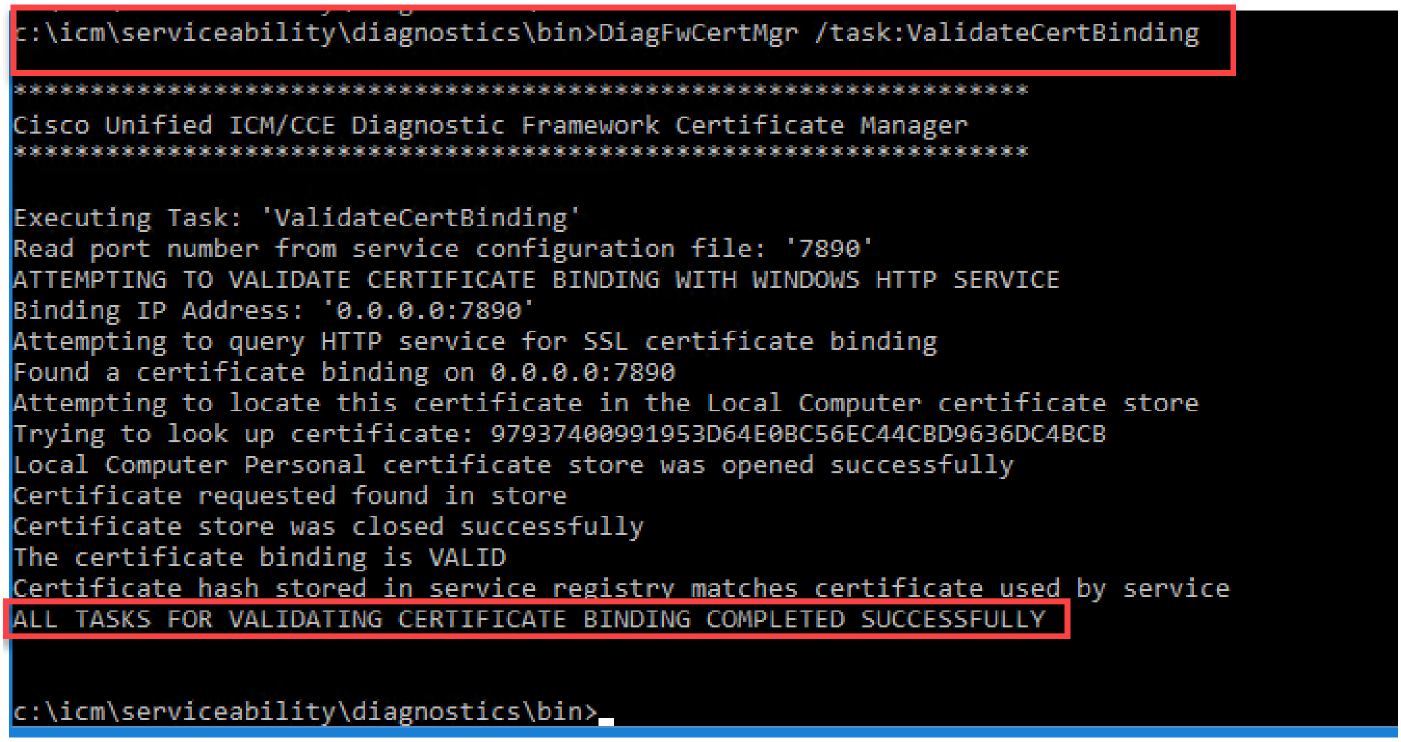


```
c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:BindCertFromStore /certhash:97937400991953d64e0bc56ec44cbd9636
dc4bcb

******************************************************************
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
******************************************************************

Executing Task: 'BindCertFromStore'
Read port number from service configuration file: '7890'
CertHash Argument Passed: '97937400991953d64e0bc56ec44cbd9636dc4bcb'
ATTEMPTING TO BIND CERTIFICATE WITH WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Trying to look up certificate: 97937400991953D64E0BC56EC44CBD9636DC4BCB
Local Computer Personal certificate store was opened successfully
Certificate requested found in store
Certificate store was closed successfully
Certificate bind with HTTP service on 0.0.0.0:7890 completed successfully
Found existing registry key for the service
Hash of certificate used saved in the service registry
ALL TASKS FOR BINDING THE CERTIFICATE WITH HTTP SERVICE COMPLETED SUCCESSFULLY


c:\icm\serviceability\diagnostics\bin>_
```

If certificate binding is successful, it displays **The certificate binding is VALID** message.

Step 6. Validate if the certificate binding was successful. Run this command:

```
DiagFwCertMgr /task:ValidateCertBinding
```



```
c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:ValidateCertBinding

******************************************************************
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
******************************************************************

Executing Task: 'ValidateCertBinding'
Read port number from service configuration file: '7890'
ATTEMPTING TO VALIDATE CERTIFICATE BINDING WITH WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Attempting to query HTTP service for SSL certificate binding
Found a certificate binding on 0.0.0.0:7890
Attempting to locate this certificate in the Local Computer certificate store
Trying to look up certificate: 97937400991953D64E0BC56EC44CBD9636DC4BCB
Local Computer Personal certificate store was opened successfully
Certificate requested found in store
Certificate store was closed successfully
The certificate binding is VALID
Certificate hash stored in service registry matches certificate used by service
ALL TASKS FOR VALIDATING CERTIFICATE BINDING COMPLETED SUCCESSFULLY


c:\icm\serviceability\diagnostics\bin>_
```

Note: DiagFwCertMgr uses port 7890 by default..

If certificate binding is successful, it displays **The certificate binding is VALID** message.

Step 7. Restart the Diagnostic Framework service. Run these commands:

```
net stop DiagFwSvc
net start DiagFwSvc
```

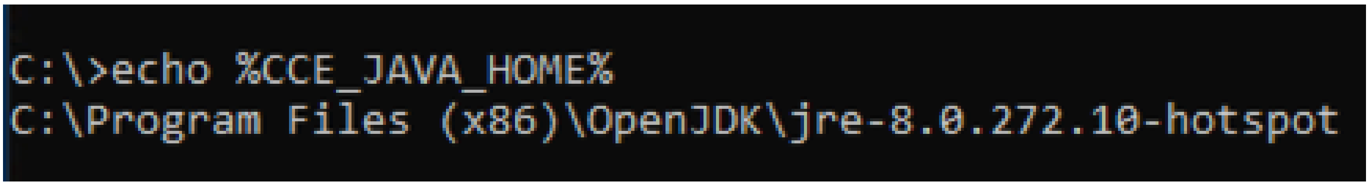
If Diagnostic Framework restarts successfully, certificate error warnings do not appear when the application is launched.

6. Import the Root and Intermediate Certificate into Java Keystore

> **Caution**: Before you begin, you must backup the keystore and run the commands from the java home as an Administrator.

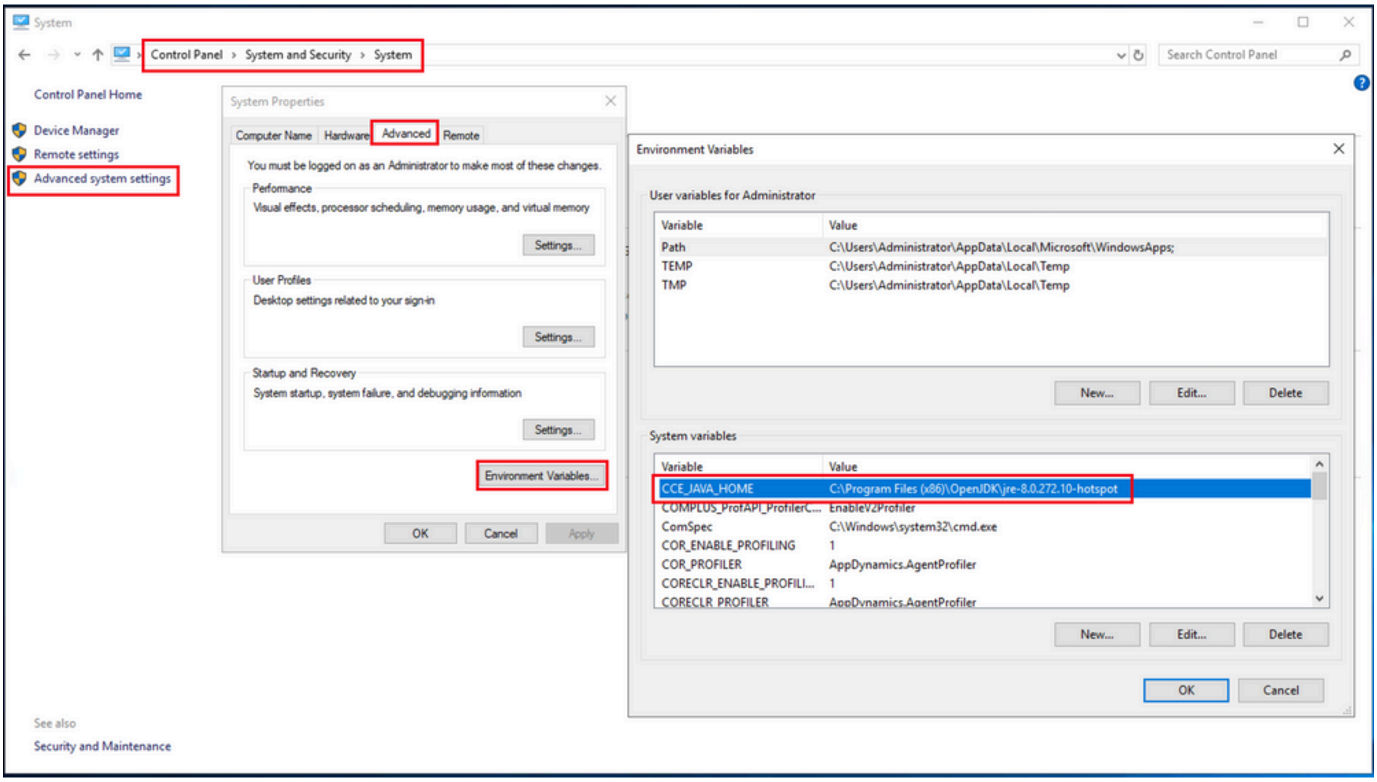
Step 1. Know the java home path to ensure where the java keytool is hosted. There are couple of ways you can find the java home path.

Option 1: CLI command: **echo %CCE_JAVA_HOME%**



```
C:\>echo %CCE_JAVA_HOME%
C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot
```

Option 2: Manually via Advanced system setting, as shown in the image



You must be logged on as an Administrator to make most of these changes.

Visual effects, processor scheduling, memory usage, and virtual memory

Desktop settings related to your sign-in

System startup, system failure, and debugging information

User variables for Administrator

Variable	Value
Path	C:\Users\Administrator\AppData\Local\Microsoft\WindowsApps;
TEMP	C:\Users\Administrator\AppData\Local\Temp
TMP	C:\Users\Administrator\AppData\Local\Temp

System variables

Variable	Value
CCE_JAVA_HOME	C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot
COMPLUS_ProfAPI_ProfilerC...	EnableV2Profiler
ComSpec	C:\Windows\system32\cmd.exe
COR_ENABLE_PROFILING	1
COR_PROFILER	AppDynamics.AgentProfiler
CORECLR_ENABLE_PROFILI...	1
CORECLR_PROFILER	AppDynamics.AgentProfiler

Step 2. Backup the **cacerts** file from both ICM and OpenJDK paths **<ICM install directory>\ssl\** and **%CCE_JAVA_HOME%\lib\security\cacerts.** You can copy these to another location.

Step 3. Open a command window as Administrator and run these commands:

```
cd %CCE_JAVA_HOME%\bin
keytool.exe –keystore <ICM install directory>\ssl\cacerts -trustcacerts -import -file <path where the R
keytool.exe –keystore %CCE_JAVA_HOME%\lib\security\cacerts -trustcacerts -import -file <path where the
```

> **Note**: The specific certificates required depend on the CA that you use to sign your certificates. In a two tier CA, which is typical of public CAs and more secure than internal CAs, then you need to import both the root and intermediate certificates. In a standalone CA with no intermediates, which is generally seen in a lab or more simple internal CA, then you only need to import the root certificate. The root and intermediate certificates must be imported to both ICM and OpenJDK keystores as System CLI still uses the OpenJDK keystore.

CVP Solution

1. Generate Certificates with FQDN

This procedure explains how to generate certificates with FQDN for Web Service Manager (WSM), Voice XML (VXML), Call Server and Operations Management (OAMP) services.

> **Note**: When you install CVP the certificate name only includes the name of the server and not the FQDN therefore, you need to regenerate the certificates.

> **Caution**: Before you begin, you must do this:
> 1. Open a command window as administrator.
> 2. For 12.6.2, to identify the keystore password, go to the %CVP_HOME%\bin folder and run the DecryptKeystoreUtil.bat file.
> 3. For 12.6.1, to identify the keystore password, run the command, **more %CVP_HOME%\conf\security.properties.**
> 4. You need this password when running the keytool commands.
> 5. From the %CVP_HOME%\conf\security\ directory, run the command, **copy .keystore backup.keystore**.

CVP Servers

Step 1. To delete the CVP servers certificates run these commands:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
```

Enter the keystore password when prompted.

Step 2. To generate the WSM certificate run this command:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Enter the keystore password when prompted.

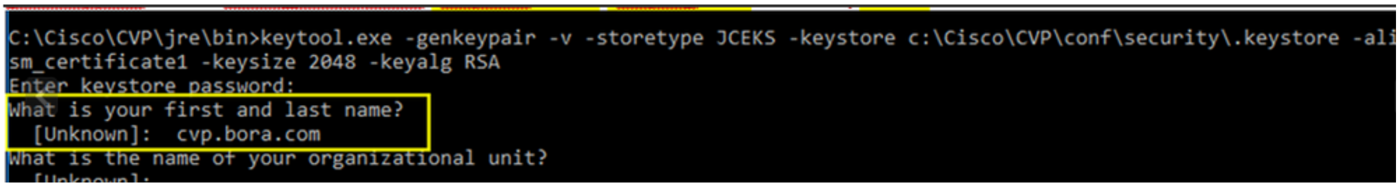
Note: By default, the certificates are generated for two years. Use -validity XXXX to set the expiry date when certificates are regenerated, otherwise certificates are valid for 90 days and need to be signed by a CA before this time. For most of these certificates, 3-5 years must be a reasonable validation time.

Here are some standard validity inputs:

One Year	365
Two Years	730
Three Years	1095
Four Year	1460
Five Years	1895
Ten Years	3650

Caution: From 12.5 certificates must be **SHA 256**, Key Size **2048**, and encryption Algorithm **RSA**, use these parameters to set these values: -keyalg RSA and -keysize 2048. It is important that the CVP keystore commands include the -storetype JCEKS parameter. If this is not done, the certificate, the key, or worse the keystore can become corrupted.

Specify the FQDN of the server, on the question **what is your fist and last name?**



```
C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -v -storetype JCEKS -keystore c:\Cisco\CVP\conf\security\.keystore -ali
sm_certificate1 -keysize 2048 -keyalg RSA
Enter keystore password:
What is your first and last name?
  [Unknown]:  cvp.bora.com
What is the name of your organizational unit?
  [Unknown]:
```

Complete these other questions:

What is the name of your organizational unit?

[Unknown]: <specify OU>

What is the name of your organization?

[Unknown]: <specify the name of the org>

What is the name of your City or Locality?

[Unknown]: <specify the name of the city/locality>

What is the name of your State or Province?

[Unknown]: <specify the name of the state/province>

What is the two-letter country code for this unit?

[Unknown]: <specify two-letter Country code>

Specify **yes** for the next two inputs.

Step 3. Perform the same steps for vxml_certificate and callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

CVP Reporting Server

Step 1. To delete the WSM and Reporting Server certificates run these commands:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -al
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -al
```

Enter the keystore password when prompted.

Step 2. To generate the WSM certificate run this command:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Enter the keystore password when prompted.

Specify the FQDN of the server for the query **what is your fist and last name?** and continue with the same steps as done with CVP servers.

Step 3. Perform the same steps for callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Enter the keystore password when prompted.

CVP OAMP (UCCE deployment)

Since In the PCCE solution version 12.x all components of the solution are controlled by the SPOG and OAMP is not installed, these steps are only required for a UCCE deployment solution.

Step 1. To delete the WSM and OAMP Server certificates run these commands:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
```

Enter the keystore password when prompted.

Step 2. To generate the WSM certificate run this command:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Enter the keystore password when prompted.

Specify the FQDN of the server for the query **what is your fist and last name?** and continue with the same steps as done with CVP servers.

Step 3. Perform the same steps for oamp_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Enter the keystore password when prompted.

2. Generate the CSR

> **Note**: RFC5280 compliant browser requires Subject Alternative Name (SAN) to be included with each certificate. This can be accomplished using the -ext parameter with SAN when generating the CSR.

Subject Alternative Name

The -ext parameter allows a user to specific extensions. The example shown adds a subject alternative name (SAN) with the fully qualified domain name (FQDN) of the server as well as localhost. Additional SAN fields can be added as comma separated values.

Valid SAN Types are:

```
ip:192.168.0.1
dns:myserver.mydomain.com
email:name@mydomain.com
```

For example:

```
 -ext san=dns:mycvp.mydomain.com,dns:localhost
```

CVP Servers

Step 1. Generate the certificate request for the alias. Run this command and save it to a file (for example, wsm_certificate):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Enter the keystore password when prompted.

Step 2. Perform the same steps for vxml_certificate and callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Enter the keystore password when prompted.

CVP Reporting server

Step 1. Generate the certificate request for the alias. Run this command and save it to a file (for example, wsmreport_certificate):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Enter the keystore password when prompted.

Step 2. Perform the same steps for the callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Enter the keystore password when prompted.

CVP OAMP (UCCE deployment only)

Step 1. Generate the certificate request for the alias. Run this command and save it to a file (for example, wsmoamp_certificate):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -a
```

Enter the keystore password when prompted.

Step 2. Perform the same steps for oamp_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -a
```

Enter the keystore password when prompted.

3. Obtain the CA Signed Certificates

Step 1. Sign the certificates on a CA (WSM, Callserver and VXML server for the CVP server; WSM and OAMP for the CVP OAMP server, and WSM and Callserver for the CVP Reporting server).

Step 2. Download the application certificates and the root certificate from the CA authority.

Step 3. Copy the root certificate and the CA signed certificates in to the folder **%CVP_HOME%\conf\security**\ of each server.

4. Import the CA Signed Certificates

Apply these steps to all servers of the CVP solution. Only the certificates for components on that server need to have the CA signed certificate imported.

Step 1. Import the root certificate. Run this command:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t
```

Enter the keystore password when prompted. At Trust this certificate prompt, type **Yes**.

If there is an intermediate certificate, run this command:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t
```

Enter the keystore password when prompted. At Trust this certificate prompt, type **Yes**.

Step 2. Import the CA Signed WSM for that server certificate (CVP, Reporting and OAMP). Run this command:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t
```

Enter the keystore password when prompted. At Trust this certificate prompt, type **Yes**.

Step 3. In the CVP Servers and the Reporting servers import the Callserver CA Signed certificate. Run this command:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t
```

Enter the keystore password when prompted. At Trust this certificate prompt, type **Yes**.

Step 4. In the CVP Servers import the VXML server CA Signed certificate. Run this command:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t
```

Enter the keystore password when prompted. At Trust this certificate prompt, type **Yes**.

Step 5. In the CVP OAMP server (for UCCE only) import the OAMP server CA Signed certificate. Run this command:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t
```

Enter the keystore password when prompted. At Trust this certificate prompt, type **Yes**.

Step 6. Reboot the servers.

> **Note**: In UCCE deployment, ensure to add the servers (CVP Reporting, CVP Server, and so on) in CVP OAMP with the FQDN that you provided when you genarated the CSR.

VOS Servers

1. Generate CSR Certificate

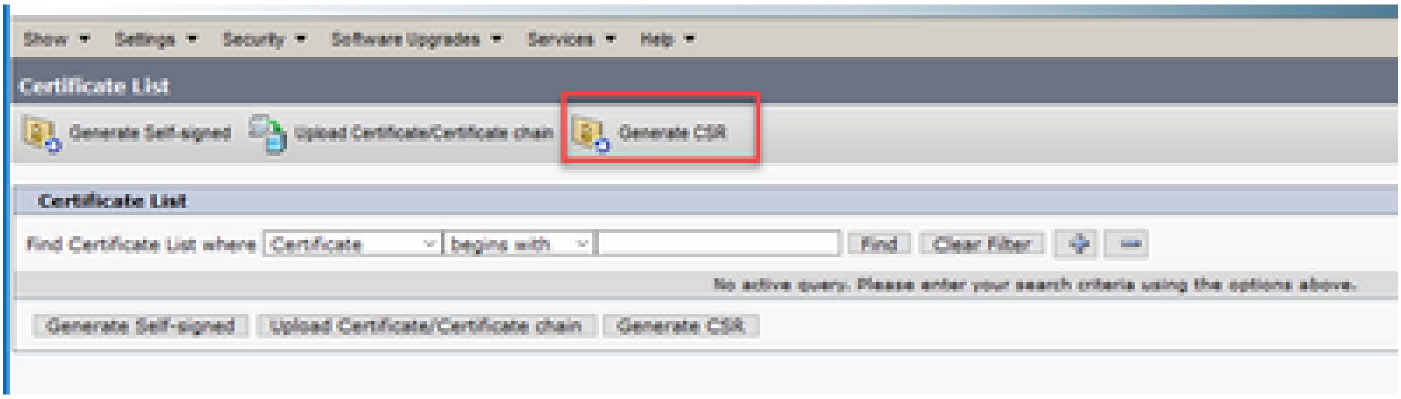
This procedure explains how to generate Tomcat CSR certificate from a Cisco Voice Operating System (VOS) based platforms.

This process is applicable for VOS based applications such as:

- Finesse
- CUIC \ Live Data (LD) \Identity Server(IDS)
- Cloud Connect
- Cisco VVB

Step 1. Navigate to Cisco Unified Communications Operating System Administration page:https://FQDN :<8443 or 443>/cmplatform.

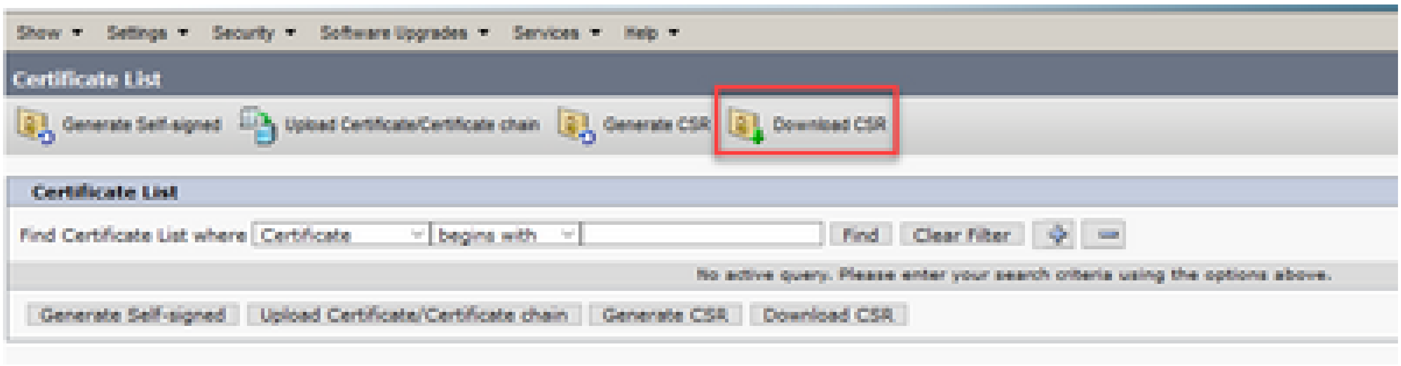
Step 2. Navigate to **Security** > **Certificate Management** and select **Generate CSR**.



Find Certificate List where Certificate begins with

No active query. Please enter your search criteria using the options above.

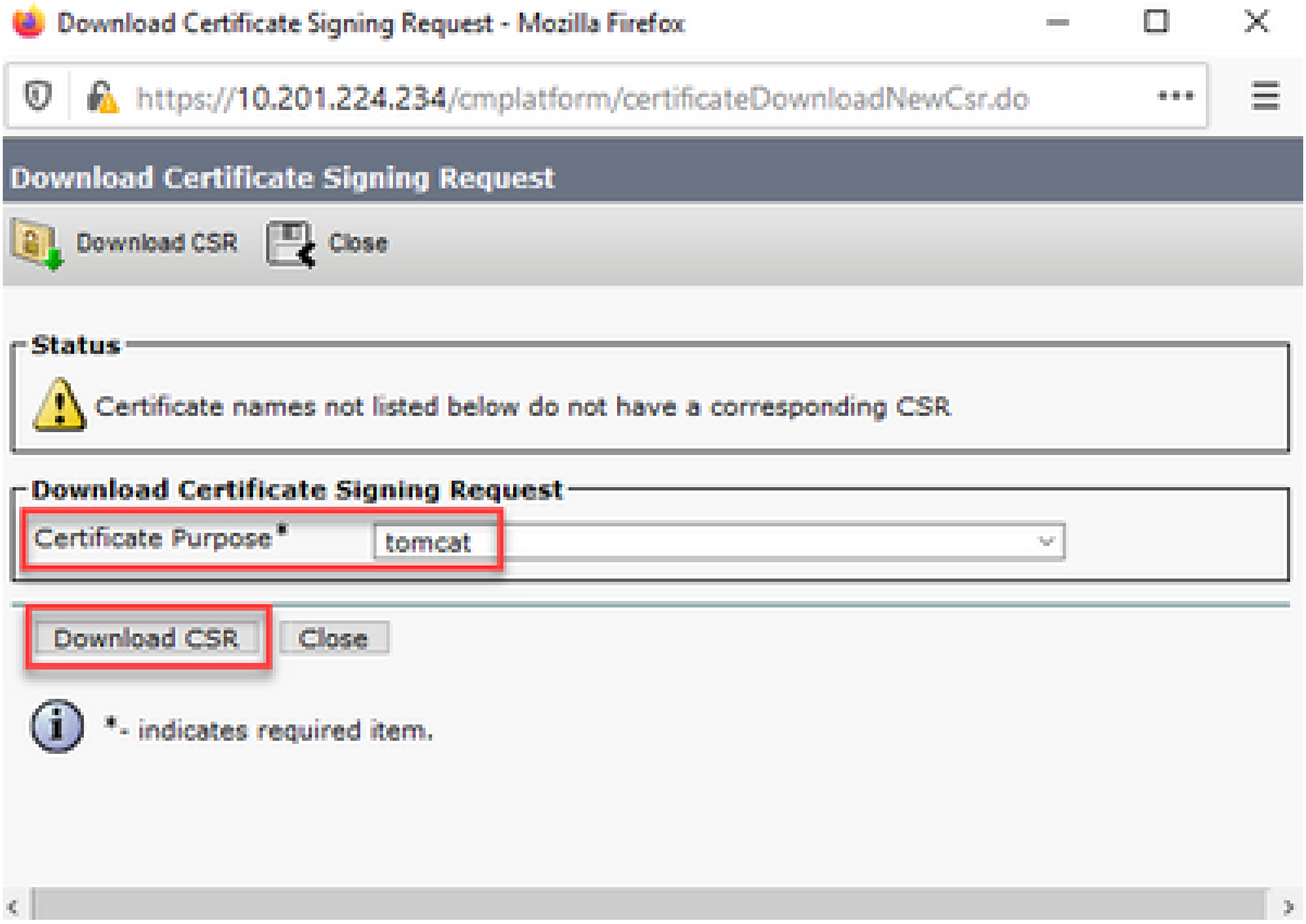
Step 3. After the CSR certificate is generated, close the window and select **Download CSR**.



Find Certificate List where Certificate begins with

No active query. Please enter your search criteria using the options above.

Step 4. Ensure that the Certificate purpose is tomcat and click **Download CSR**.



Download Certificate Signing Request - Mozilla Firefox

https://10.201.224.234/cmplatform/certificateDownloadNewCsr.do

Download Certificate Signing Request

Download CSR   Close

Status

⚠ Certificate names not listed below do not have a corresponding CSR

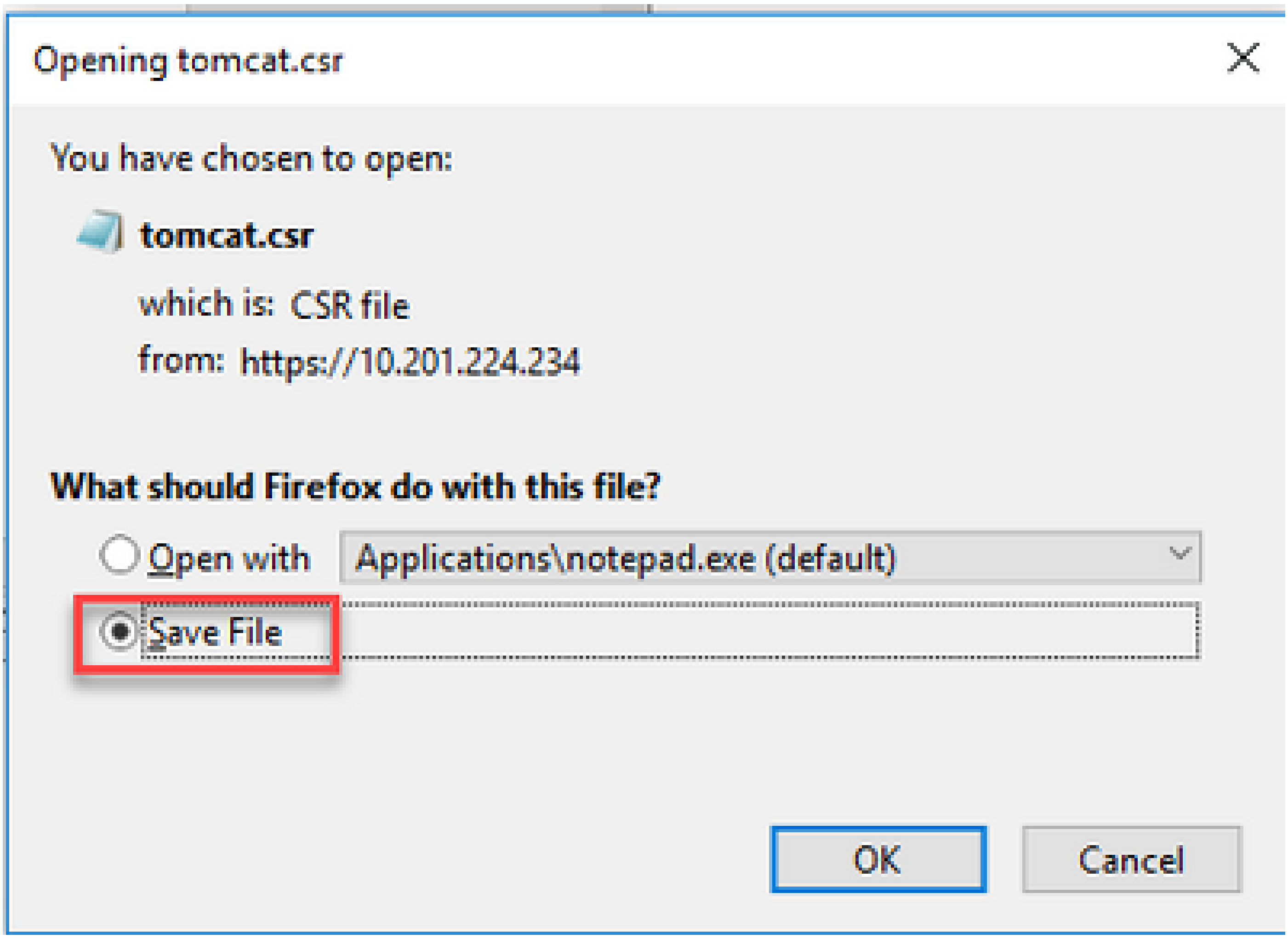
Download Certificate Signing Request

Certificate Purpose* tomcat

Download CSR   Close

ⓘ *- indicates required item.

Step 5. Click **Save File**. The file is saved on the Download folder.



Opening tomcat.csr

You have chosen to open:

tomcat.csr

which is: CSR file

from: https://10.201.224.234

What should Firefox do with this file?

○ Open with Applications\notepad.exe (default)

● Save File

2. Obtain the CA Signed Certificates

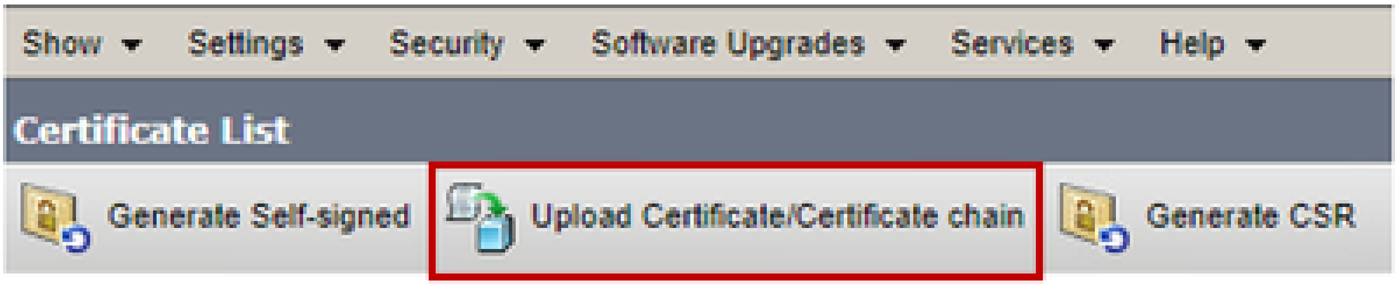
Step 1. Sign the tomcat certificate exported on a CA.

Step 2. Download the application and the root certificated from the CA authority.

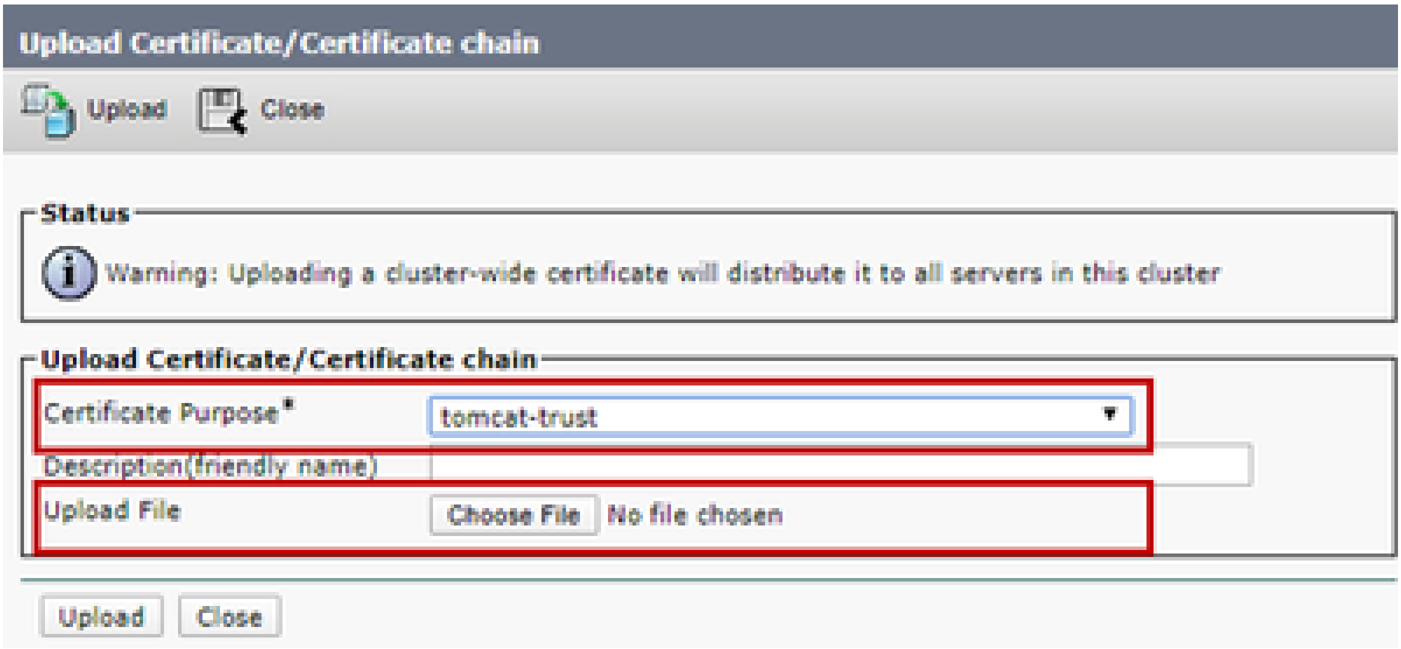
3. Upload the Application and Root Certificates

Step 1. Navigate to Cisco Unified Communications Operating System Administration page: **https://FQDN:<8443 or 443>/cmplatform.**

Step 2. Navigate to **Security** > **Certificate Management** and select **Upload Certificate/Certificate chain**.



Step 3. On the Upload certificate/Certificate chain window select tomcat-trust in certificate purpose field and upload the Root certificate.



Upload Certificate/Certificate chain

Status

Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

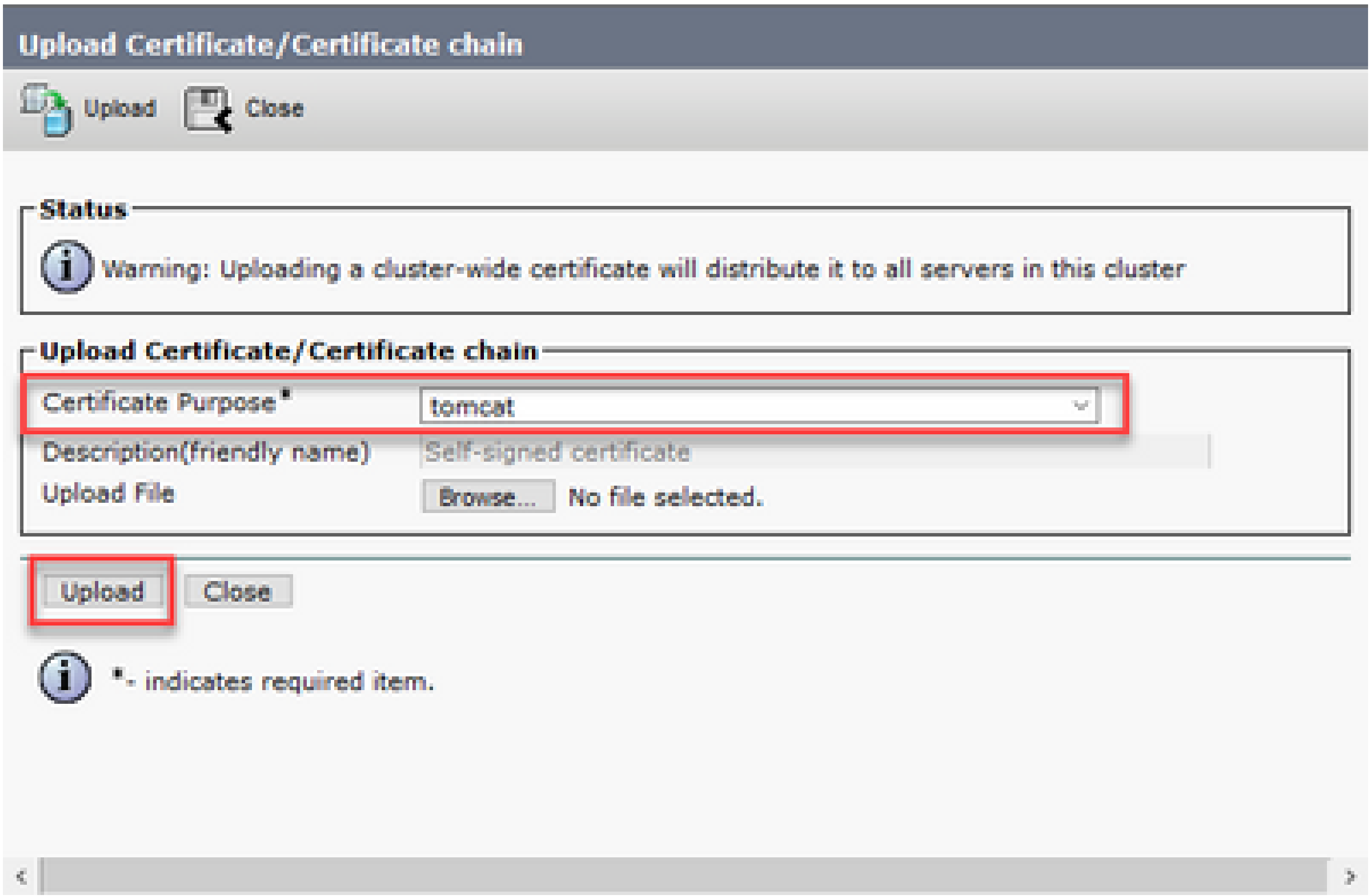
Certificate Purpose* tomcat-trust

Description(friendly name)

Upload File Choose File No file chosen

Step 4. Upload an intermediate certificate (if any) as a tomcat-trust.

Step 5. On the Upload certificate/Certificate chain window select now tomcat in the Certificate Purpose field and upload the application CA signed certificate.



Upload Certificate/Certificate chain

Status

Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* tomcat

Description(friendly name) Self-signed certificate

Upload File Browse... No file selected.

*- indicates required item.

Step 6. Reboot the server.

Verify

After you reboot the server, execute these steps to verify the CA signed implementation:

Step 1. Open a Web Browser and clear the cache.

Step 2. Close and Open the browser again.

Now you must see the certificate switch to begin the CA signed certificate and the indication in the browser window that the certificate is self-signed and therefore not trusted, must go away.

Troubleshoot

There are no steps to troubleshoot the implementation of the CA Signed certificates in this guide.

Related Information

- **CVP Configuration Guide - Security**
- **UCCE Security Guide**
- **PCCE Admin Guide**
- **Exchange PCCE Self-Signed Certificates - PCCE 12.5**
- **Exchange UCCE Self-Signed Certificates - UCCE 12.5**
- **Exchange PCCE Self-Signed Certificates - PCCE 12.6**
- **Exchange UCCE Self-Signed Certificates - UCCE 12.6**
- **Certificate Exchange Utility**
- **Technical Support & Documentation - Cisco Systems**