Implementación de certificados firmados por CA en una solución CCE

Contenido

Introducción

Este documento describe cómo implementar certificados firmados por la autoridad certificadora (CA) en la solución Cisco Contact Center Enterprise (CCE).

Colaboración de Anuj Bhatia, Robert Rogier y Ramiro Amaya, ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Unified Contact Center Enterprise (UCCE) versión 12.5(1)
- Paquete Contact Center Enterprise versión 12.5(1)
- Customer Voice Portal (CVP) versión 12.5 (1)
- Navegador de voz virtualizado (VB) de Cisco
- Consola de administración y operaciones de Cisco CVP (OAMP)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Unified Communications Manager (CUCM)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- PCCE 12.5(1)
- CVP 12.5(1)
- Cisco VB 12.5
- Finesss 12,5
- CUIC 12.5
- Windows 2016

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Background

Los certificados se utilizan para garantizar que la comunicación es segura con la autenticación entre clientes y servidores.

Los usuarios pueden comprar certificados de una CA o pueden utilizar certificados autofirmados.

Los certificados autofirmados (como su nombre indica) están firmados por la misma entidad cuya identidad certifican, en lugar de estar firmados por una entidad emisora de certificados. Los certificados autofirmados no se consideran tan seguros como los certificados de CA, pero se utilizan de forma predeterminada en muchas aplicaciones.

En la versión 12.x de la solución Package Contact Center Enterprise (PCCE), todos los componentes de la solución están controlados por un único panel de acceso (SPOG), que se aloja en el servidor principal de la estación de trabajo de administración (AW).

Debido al cumplimiento de la gestión de seguridad (SRC) en la versión PCCE 12.5(1), toda la comunicación entre SPOG y otros componentes de la solución se realiza a través del protocolo HTTP seguro. En UCCE 12.5, la comunicación entre componentes también se realiza a través del protocolo HTTP seguro.

Este documento explica en detalle los pasos necesarios para implementar certificados firmados

por CA en una solución CCE para la comunicación HTTP segura. Para cualquier otra consideración de seguridad de UCCE, consulte las Pautas de seguridad de UCCE. Para cualquier comunicación segura de CVP adicional distinta de HTTP seguro, consulte las directrices de seguridad en la Guía de configuración de CVP: Directrices de seguridad de CVP.

Procedimiento

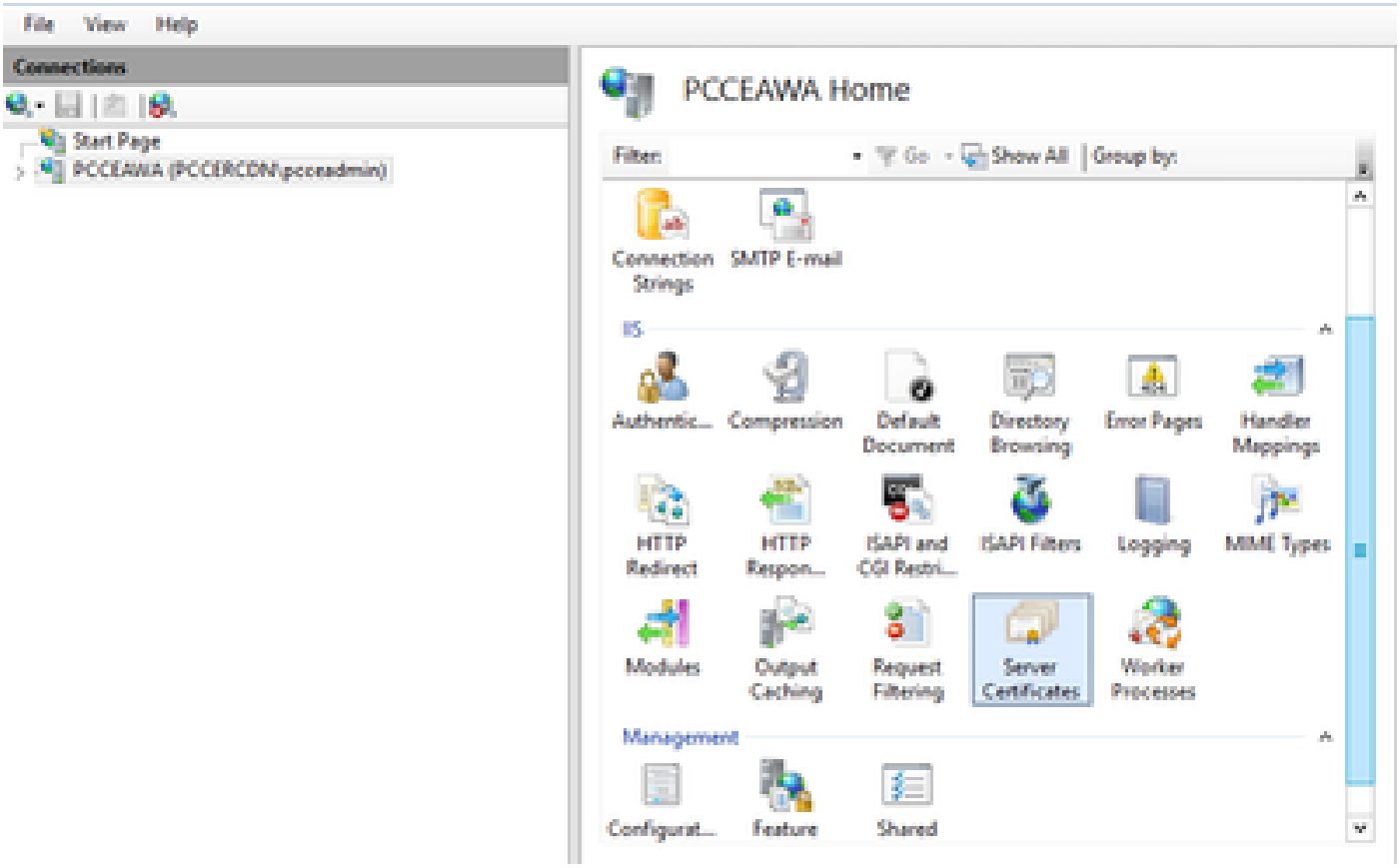
Servidores basados en Windows de CCE

1. Generar CSR

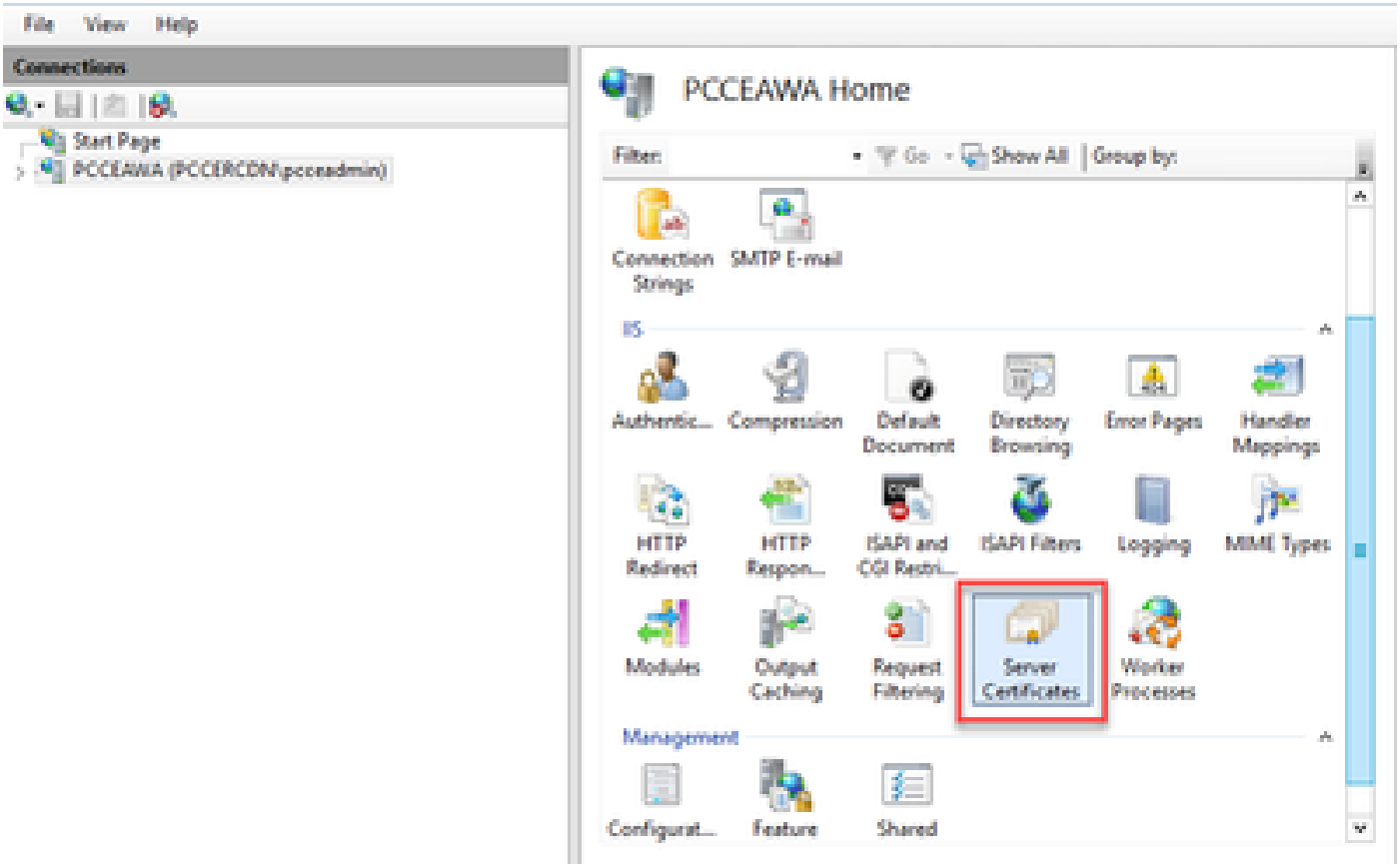
Este procedimiento explica cómo generar una Solicitud de firma de certificado (CSR) desde el Administrador de Internet Information Services (IIS).

Paso 1. Inicie sesión en Windows y seleccione Panel de control > Herramientas administrativas > Administrador de Internet Information Services (IIS).

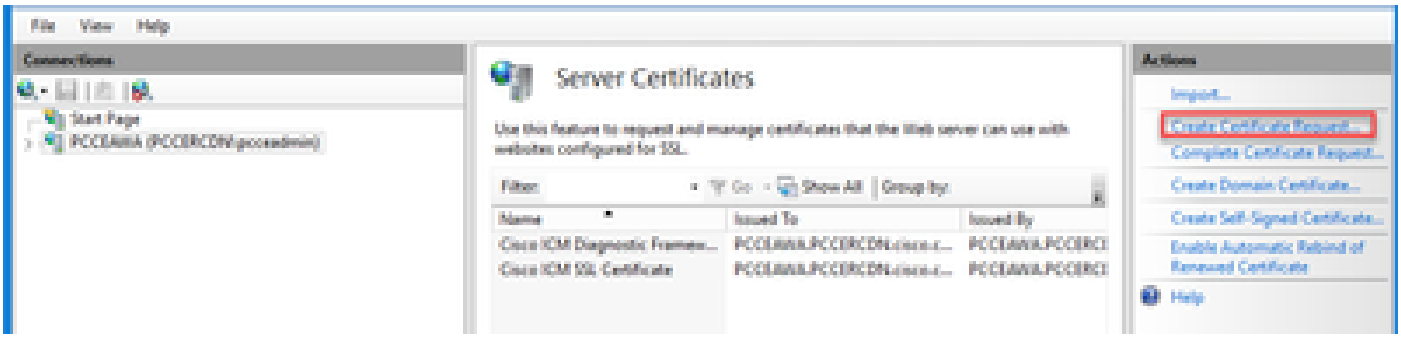
Paso 2. En el panel Conexiones, haga clic en el nombre del servidor. Aparecerá el panel Inicio del servidor.



Paso 3. En el área IIS, haga doble clic en Server Certificates.

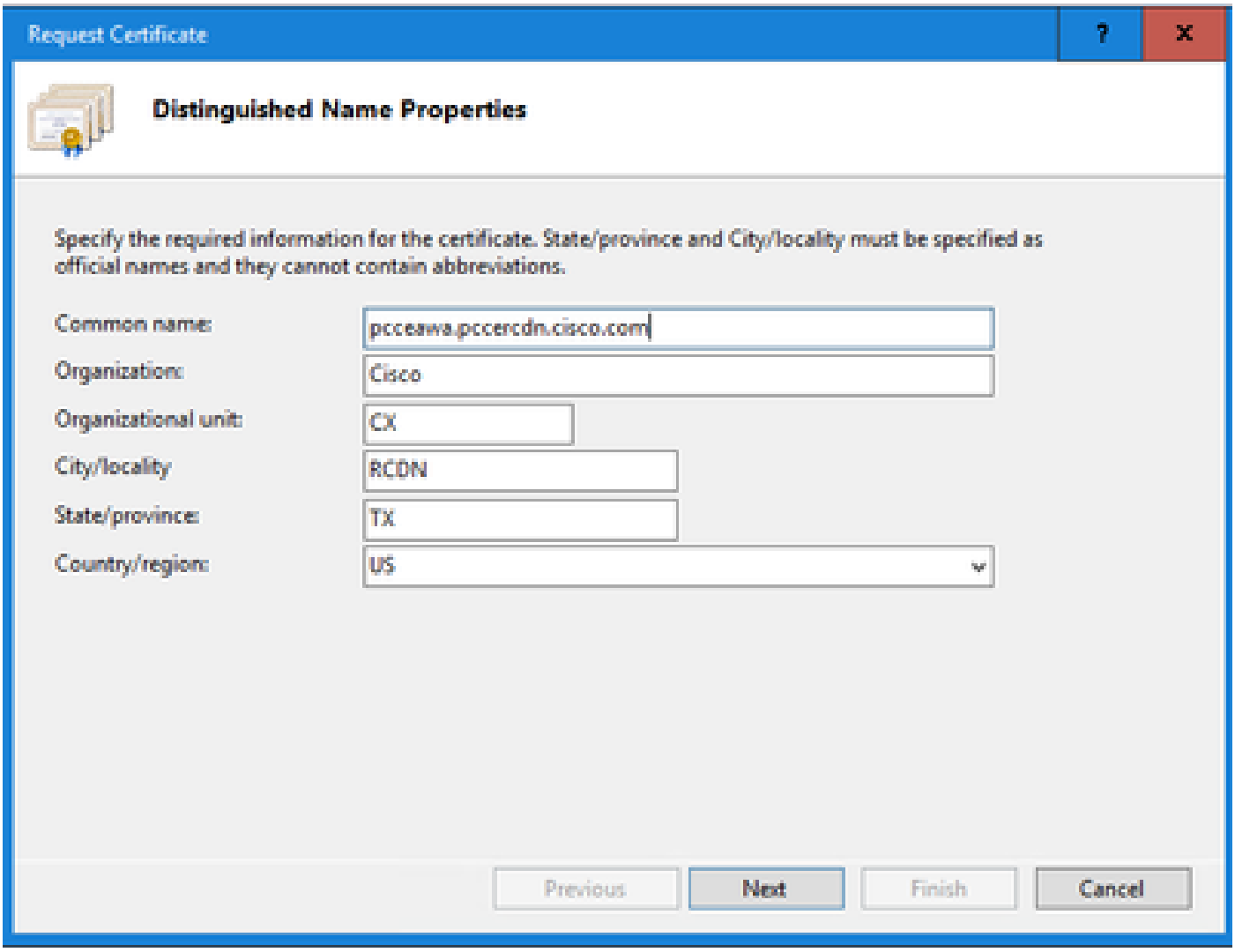


Paso 4. En el panel Acciones, haga clic en Crear solicitud de certificado.



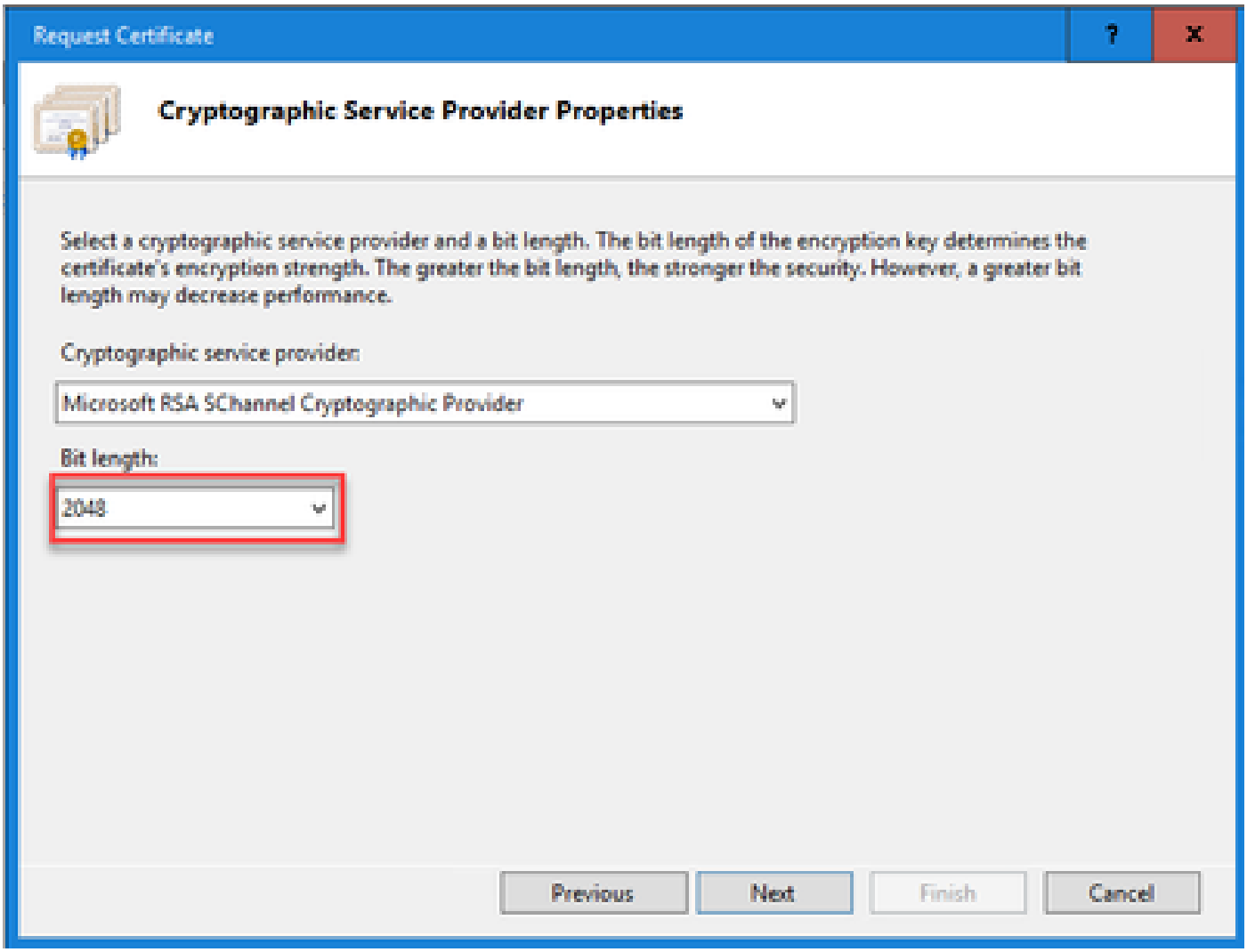
Paso 5. En el cuadro de diálogo Solicitar certificado, haga lo siguiente:

Especifique la información necesaria en los campos mostrados y haga clic en Next.

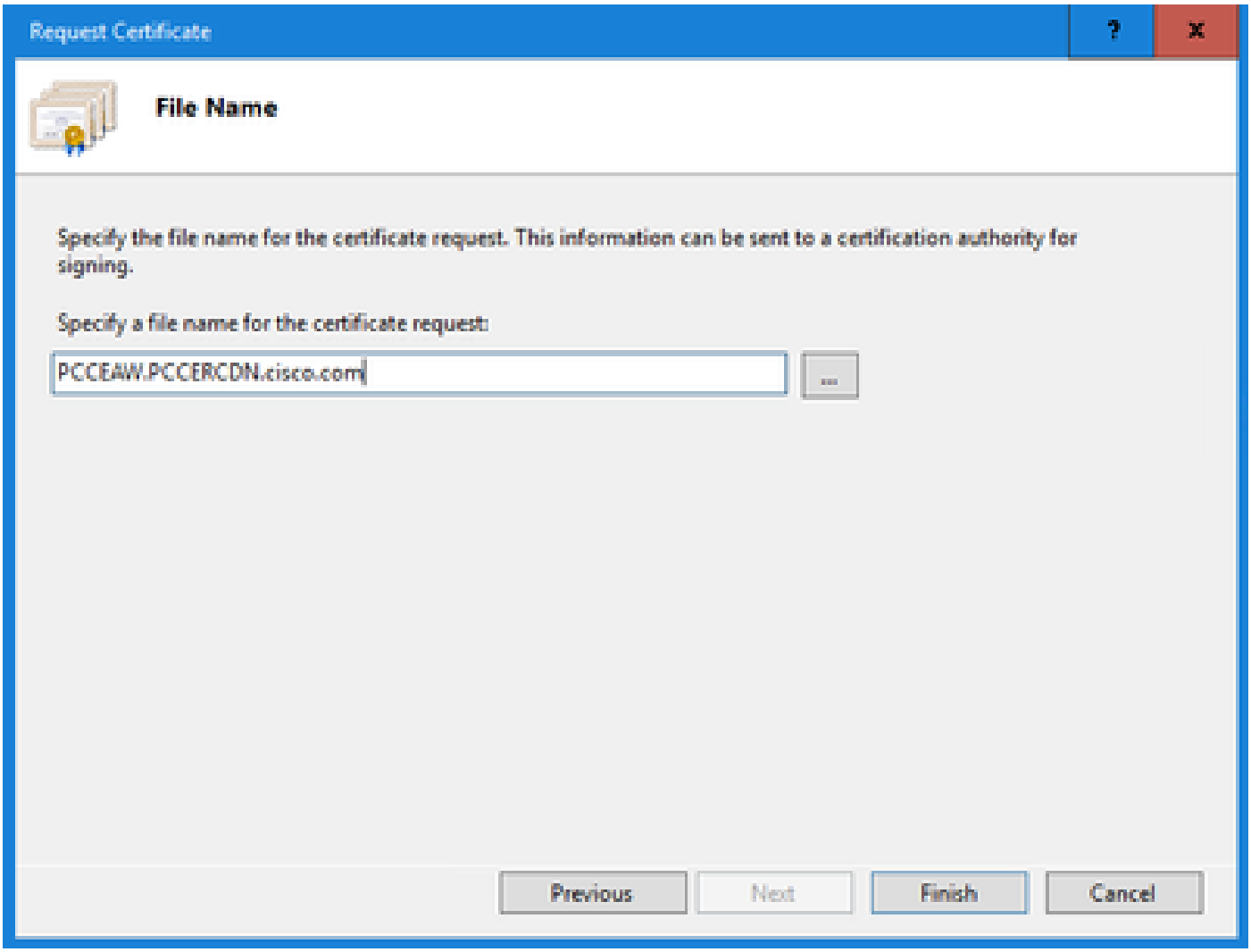


En la lista desplegable Proveedor de servicios criptográficos, deje la configuración predeterminada.

En la lista desplegable Longitud de bits, seleccione 2048.



Paso 6. Especifique un nombre de archivo para la solicitud de certificado y haga clic en Finalizar.



2. Obtenga los certificados firmados por la CA

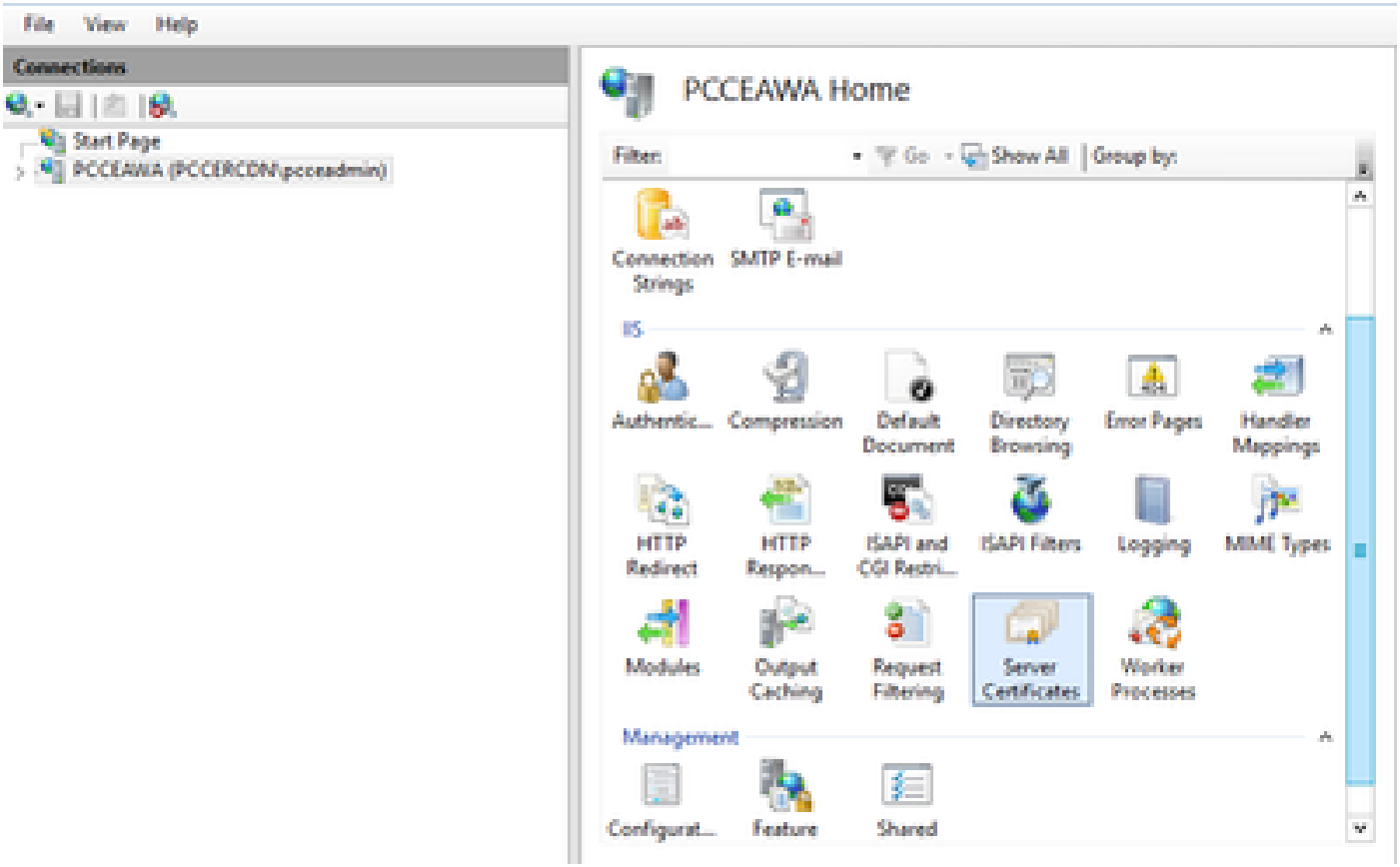
Paso 1. Firmar el certificado en una CA.

Nota: asegúrese de que la plantilla de certificado utilizada por la CA incluya autenticación de cliente y servidor.

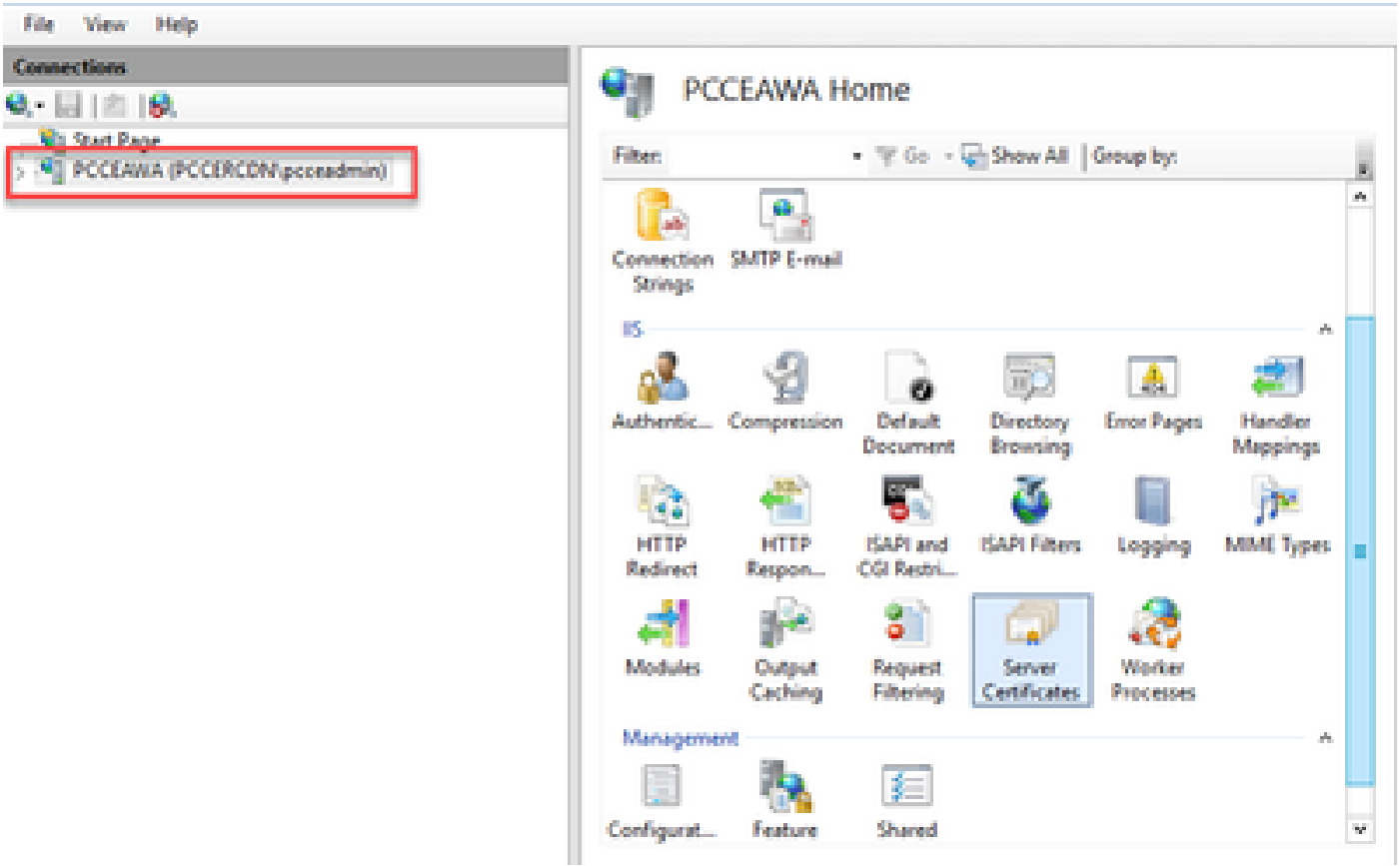
Paso 2. Obtenga los certificados firmados por la CA de su autoridad de certificación (raíz, aplicación e intermedio, si los hubiera).

3. Cargue los certificados firmados por la CA

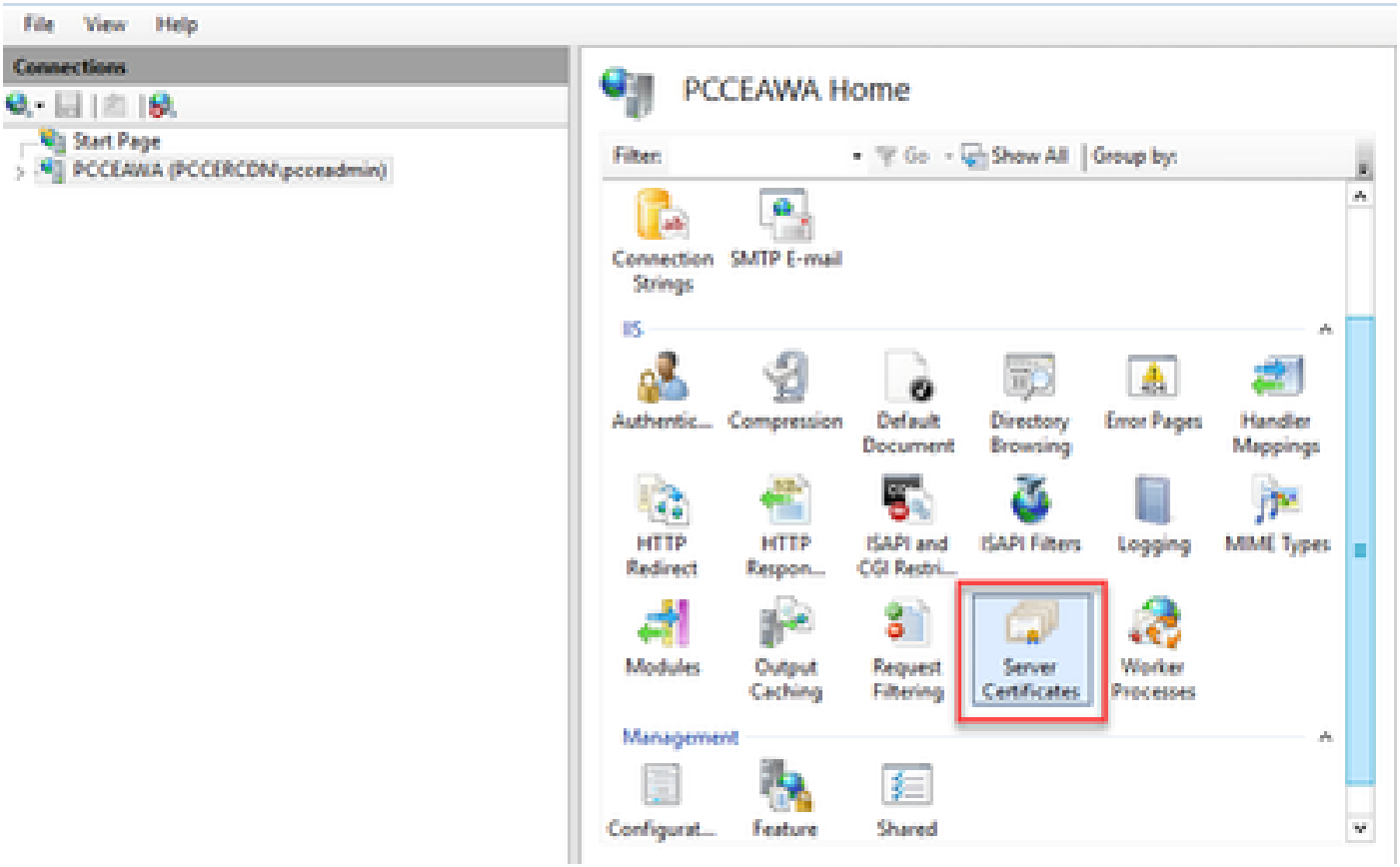
Paso 1. Inicie sesión en Windows y seleccione Panel de control > Herramientas administrativas > Administrador de Internet Information Services (IIS).



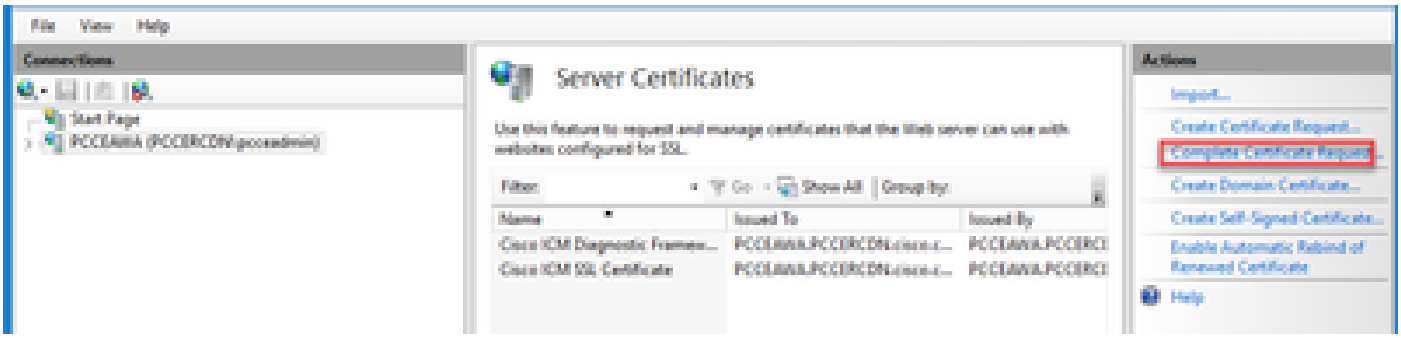
Paso 2. En el panel Conexiones, haga clic en el nombre del servidor.



Paso 3. En el área IIS, haga doble clic en Server Certificates.



Paso 4. En el panel Acciones, haga clic en Completar solicitud de certificado.



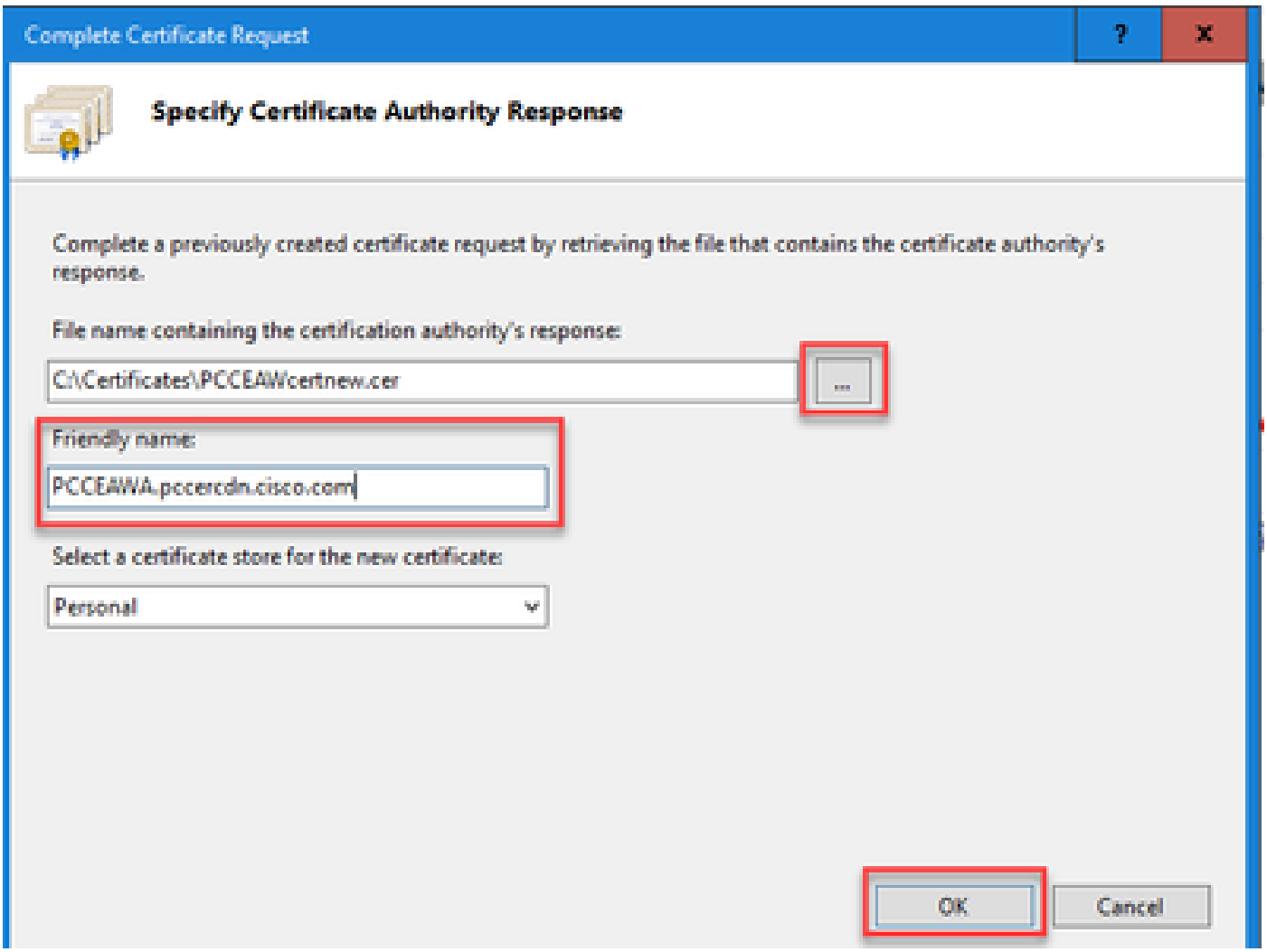
Paso 5. En el cuadro de diálogo Completar solicitud de certificado, complete estos campos:

En el campo Nombre de archivo que contiene la respuesta de la entidad emisora de certificados, haga clic en el botón de puntos suspensivos (...).

Busque la ubicación donde se almacena el certificado de aplicación firmado y, a continuación, haga clic en Abrir.

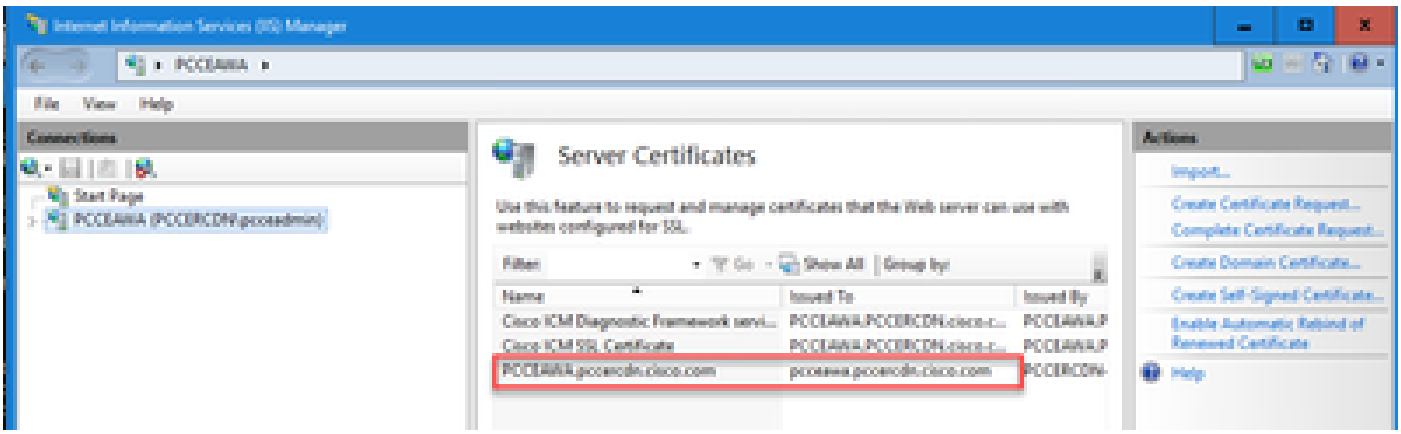
Nota: si se trata de una implementación de CA de nivel 2 y el certificado raíz no está todavía en el almacén de certificados del servidor, la raíz debe cargarse en el almacén de Windows antes de importar el certificado firmado. Consulte este documento si necesita cargar la CA raíz en el almacén de Windows https://learn.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate.

En el campo Friendly name (Nombre descriptivo), introduzca el nombre de dominio completo (FQDN) del servidor o cualquier nombre significativo. Asegúrese de que la lista desplegable Select a certificate store for the new certificate se mantenga como Personal.



Paso 6. Haga clic en Aceptar para cargar el certificado.

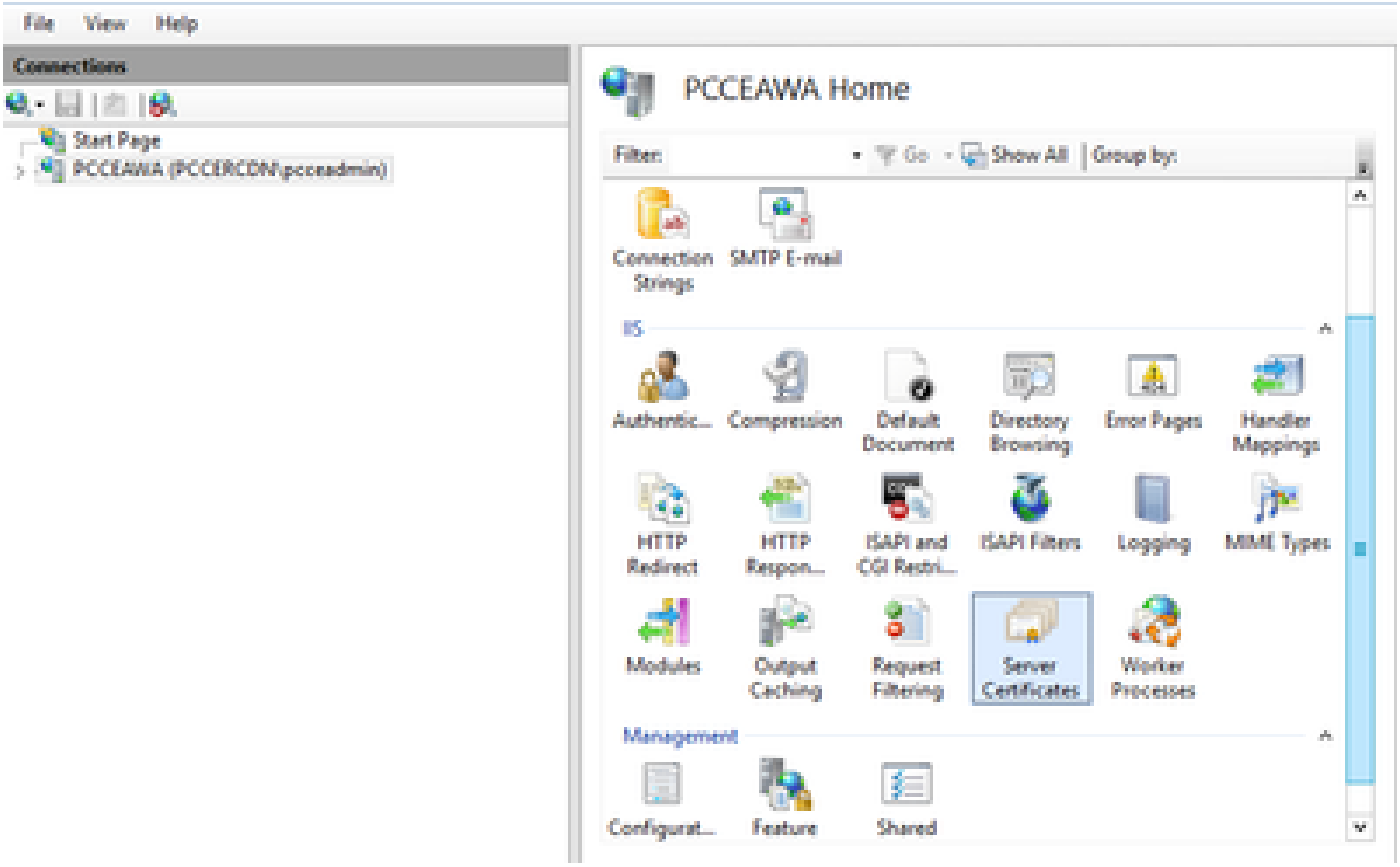
Si la carga del certificado se realiza correctamente, el certificado aparece en el panel Certificados de servidor.



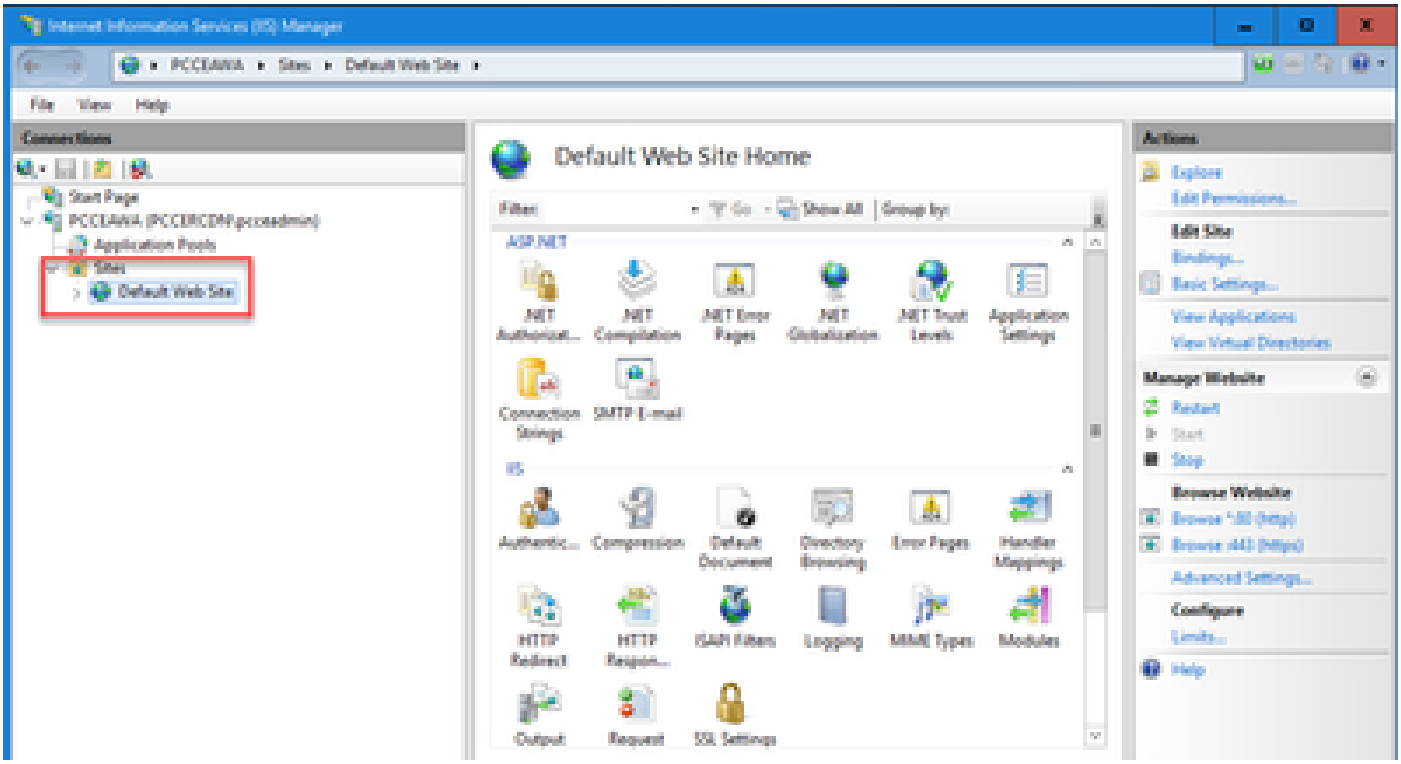
4. Enlazar el certificado firmado por la CA a IIS

Este procedimiento explica cómo enlazar un certificado firmado por una CA en el Administrador de IIS.

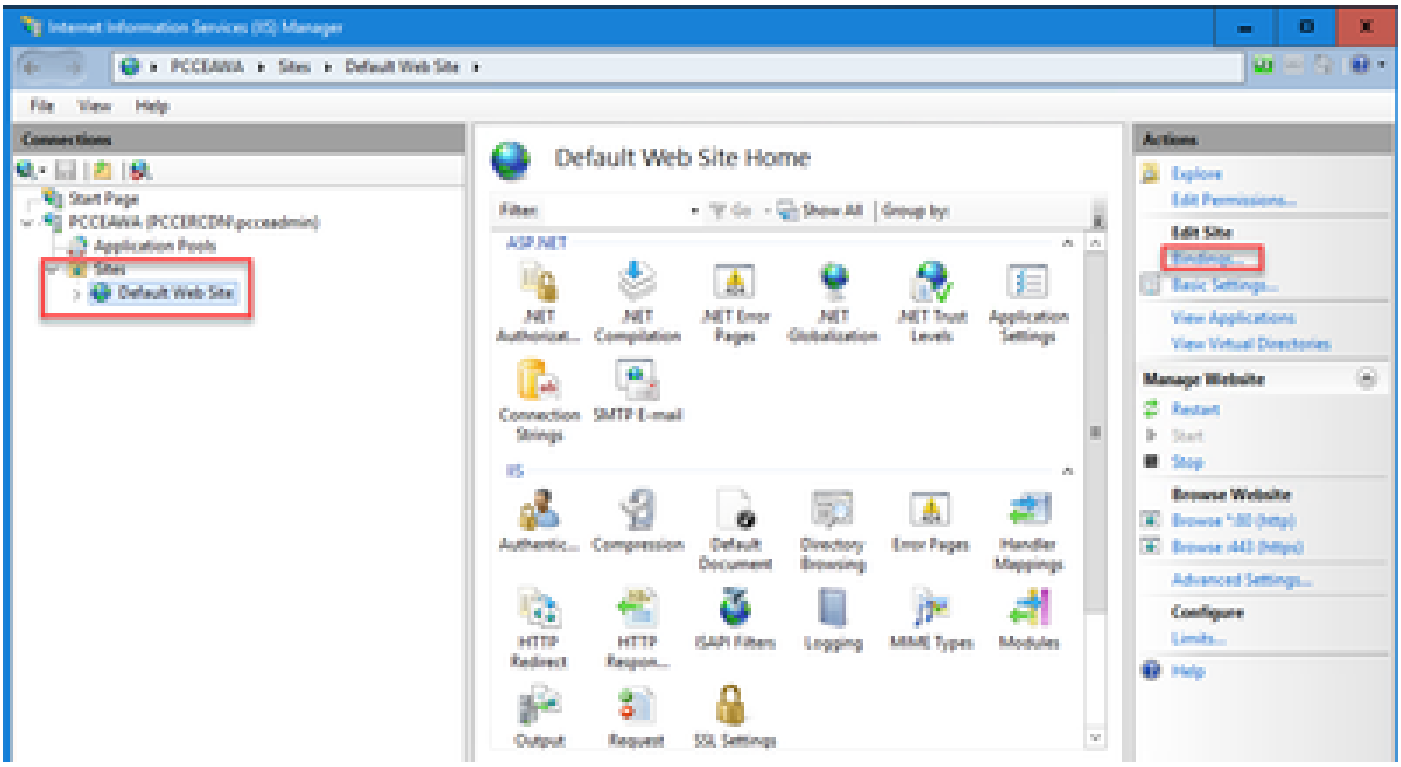
Paso 1. Inicie sesión en Windows y seleccione Panel de control > Herramientas administrativas > Administrador de Internet Information Services (IIS).



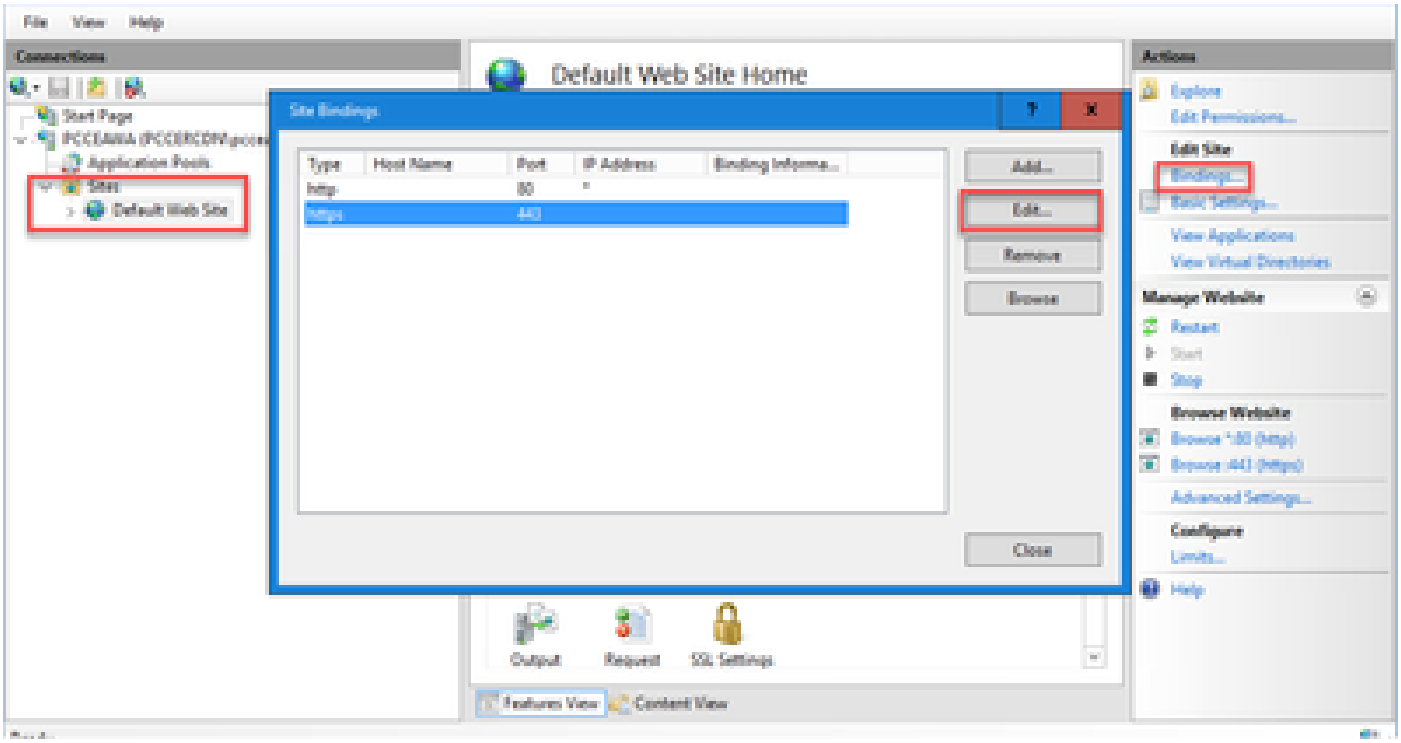
Paso 2. En el panel Conexiones, elija <nombre_servidor> > Sitios > Sitio Web predeterminado.



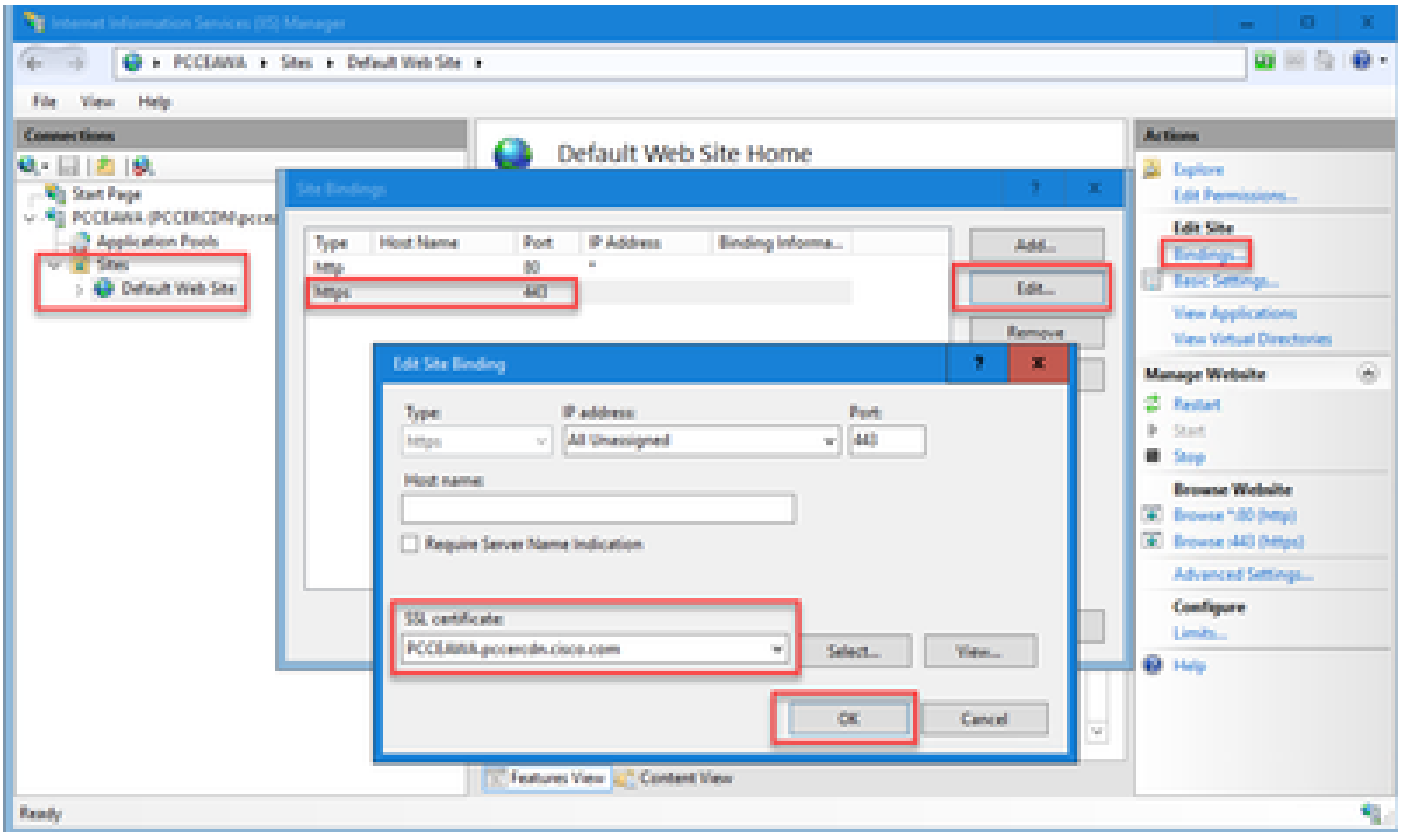
Paso 3. En el panel Acciones, haga clic en Enlaces...



Paso 4. Haga clic en el tipo https con el puerto 443, y luego haga clic en Edit....

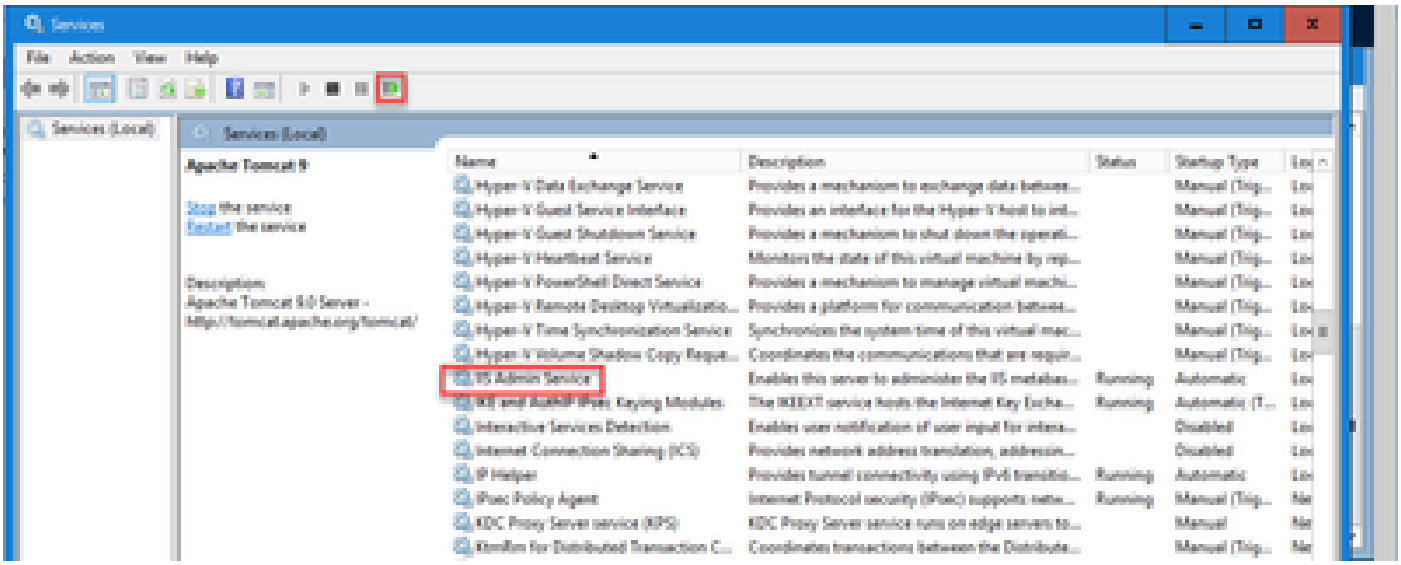


Paso 5. En la lista desplegable Certificado SSL, seleccione el certificado con el mismo nombre descriptivo que en el paso anterior.



Paso 6. Click OK.

Paso 7. Vaya a Inicio > Ejecutar > services.msc y reinicie el Servicio de administración de IIS.



Si IIS se reinicia correctamente, las advertencias de error de certificado no aparecen cuando se inicia la aplicación.

5. Enlace el certificado firmado por la CA al pórtico de diagnóstico

Este procedimiento explica cómo enlazar un certificado firmado por CA en el pórtico de diagnóstico.

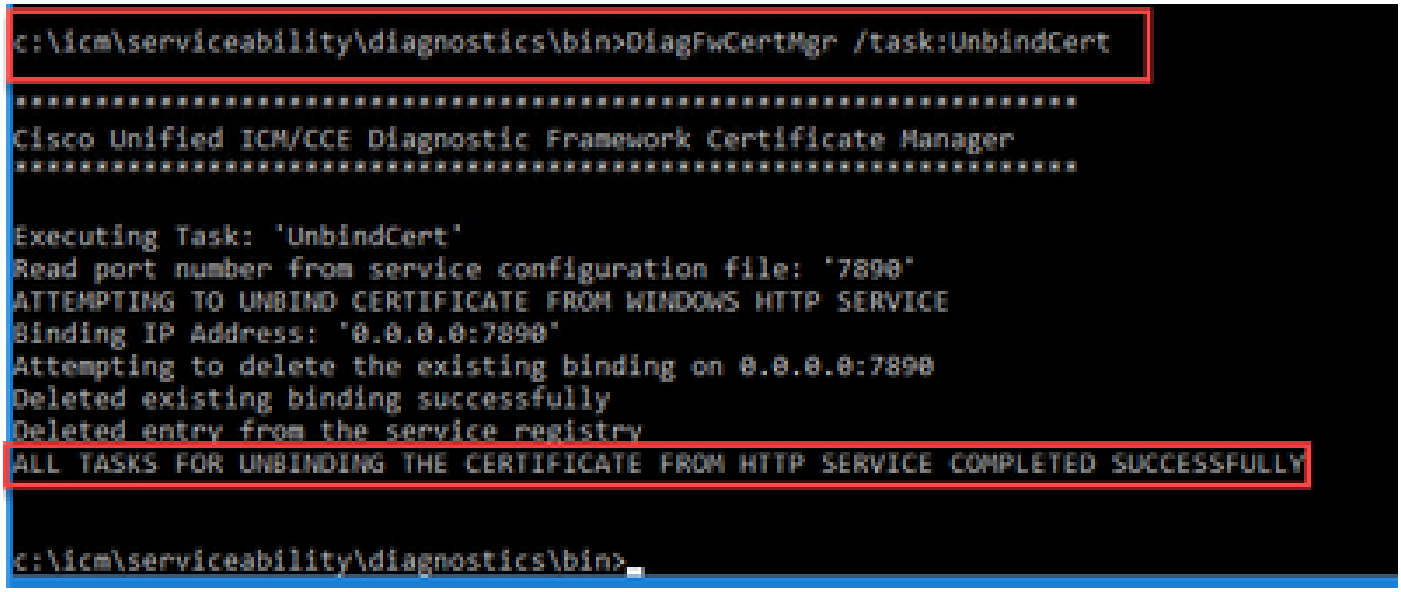
Paso 1. Abra el símbolo del sistema (Ejecutar como administrador).

Paso 2. Vaya a la carpeta principal de Diagnostic Portico (Pórtico de diagnóstico). Ejecute este comando:

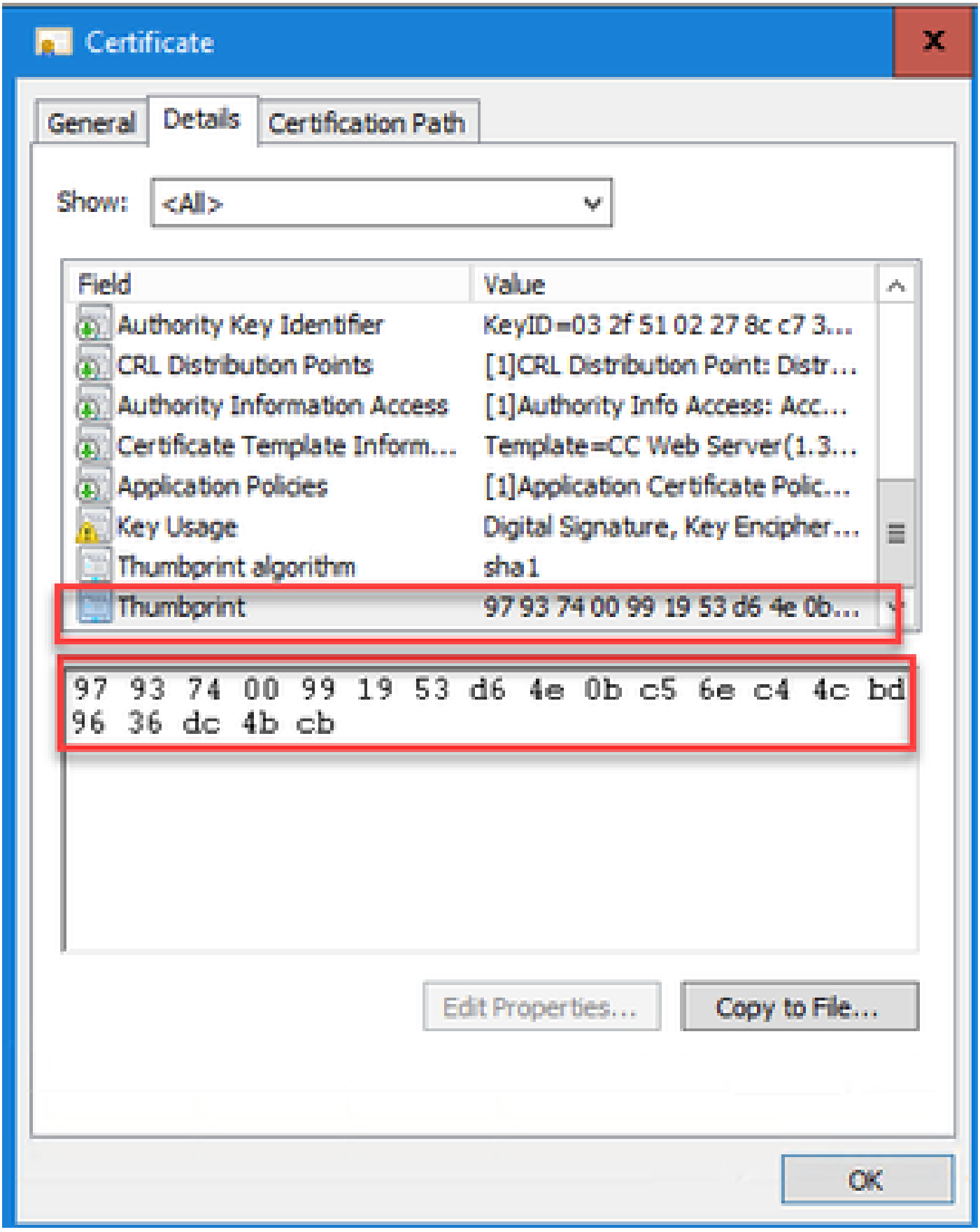
```
cd c:\icm\serviceability\diagnostics\bin
```

Paso 3. Quite el enlace de certificado actual al pórtico de diagnóstico. Ejecute este comando:

```
DiagFwCertMgr /task:UnbindCert
```

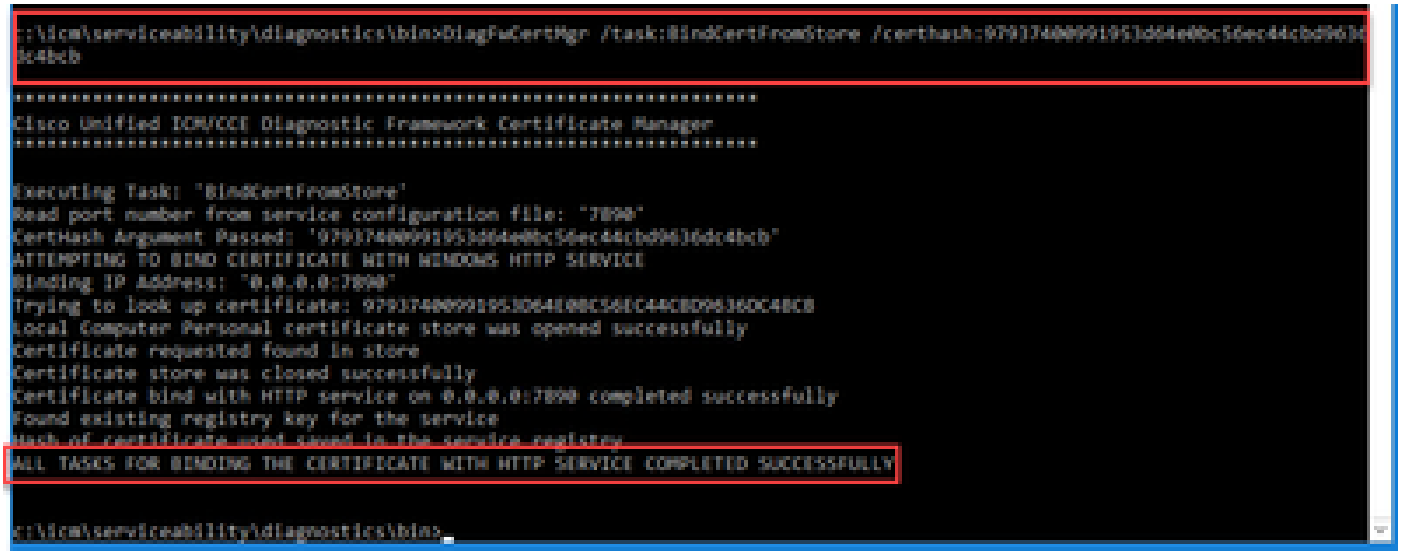


Paso 4. Abra el certificado firmado y copie el contenido hash (sin espacios) del campo Huella digital.



Paso 5. Ejecute este comando y pegue el contenido hash.

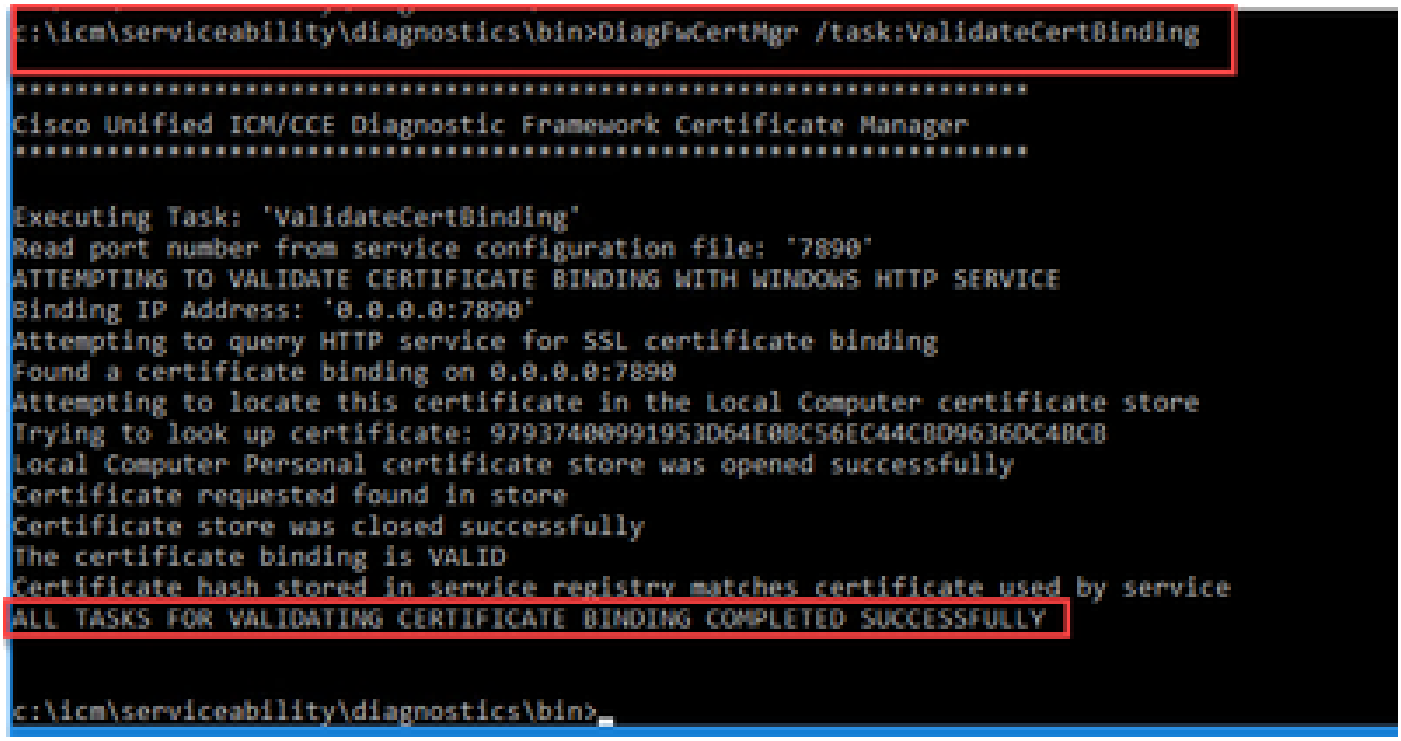
```
DiagFwCertMgr /task:BindCertFromStore /certhash:<hash_value>
```



Si el enlace del certificado es correcto, muestra el mensaje El enlace del certificado es VÁLIDO.

Paso 6. Valide si el enlace de certificado se realizó correctamente. Ejecute este comando:

```
DiagFwCertMgr /task:ValidateCertBinding
```



Nota: DiagFwCertMgr utiliza el puerto 7890 de forma predeterminada.

Si el enlace del certificado es correcto, muestra el mensaje El enlace del certificado es VÁLIDO.

Paso 7. Reinicie el servicio Marco de diagnóstico. Ejecute estos comandos:

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

Si Diagnostic Framework se reinicia correctamente, no aparecerán advertencias de error de certificado cuando se inicie la aplicación.

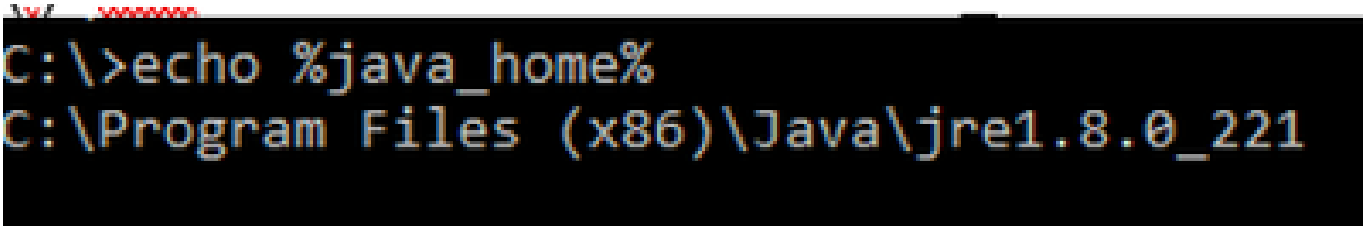
6. Importe el certificado raíz e intermedio en el almacén de claves Java

---

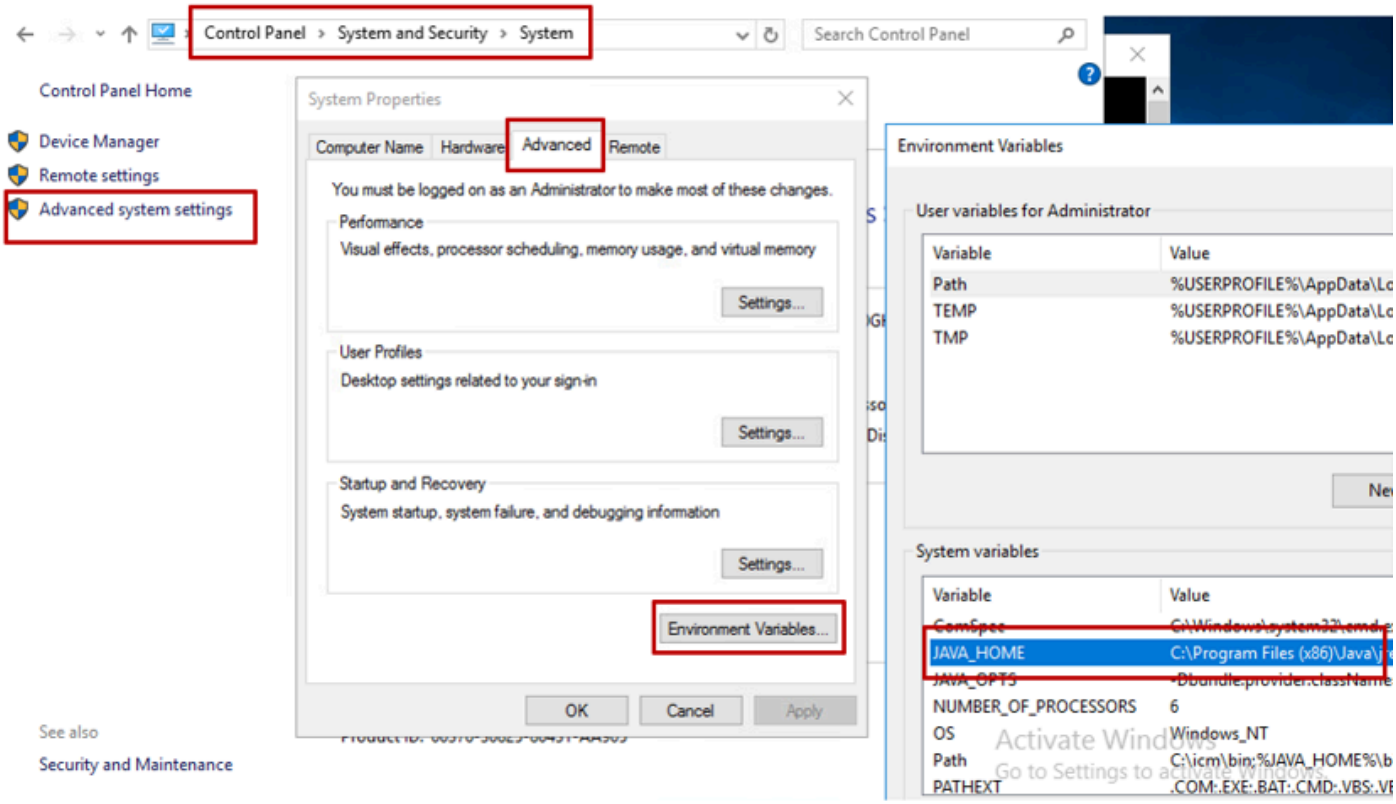
⚠ Precaución: Antes de comenzar, debe realizar una copia de seguridad del almacén de claves y ejecutar los comandos desde el directorio raíz de Java como administrador.

Paso 1. Conozca la ruta de inicio de java para asegurarse de dónde está alojada la herramienta clave de java. Hay un par de maneras de encontrar la ruta de inicio de Java.

Opción 1: comando CLI: echo %JAVA_HOME%



Opción 2: Manualmente a través de la configuración avanzada del sistema, como se muestra en la imagen



Nota: En UCCE 12.5, la ruta predeterminada es C:\Program Files (x86)\Java\jre1.8.0_221\bin. Sin embargo, si ha utilizado el instalador 12.5(1a) o tiene instalado 12.5 ES55 (OpenJDK ES obligatorio), utilice CCE_JAVA_HOME en lugar de JAVA_HOME, ya que la ruta del almacén de datos ha cambiado con OpenJDK.

Paso 2. Realice una copia de seguridad del archivo cacerts desde la carpeta C:\Program Files (x86)\Java\jre1.8.0_221\lib\security. Puede copiarlo en otra ubicación.

Paso 3. Abra una ventana de comandos como Administrador para ejecutar el comando:

```
keytool.exe -keystore ./cacerts -import -file <path where the Root, or Intermediate certificate are sto
```

Nota: los certificados específicos necesarios dependen de la CA que utilice para firmar los certificados. En una CA de dos niveles, típica de las CA públicas y más segura que las CA internas, debe importar tanto los certificados raíz como los intermedios. En una CA independiente sin intermediarios, que generalmente se ve en un laboratorio o en una CA interna más simple, solo necesita importar el certificado raíz.

Solución CVP

1. Generar certificados con FQDN

Este procedimiento explica cómo generar certificados con FQDN para los servicios Web Service

Manager (WSM), Voice XML (VXML), Call Server y Operations Management (OAMP).

Nota: Al instalar CVP, el nombre del certificado sólo incluye el nombre del servidor y no el FQDN; por lo tanto, debe volver a generar los certificados.

Precaución: antes de empezar, debe hacer lo siguiente:
1. Obtenga la contraseña del almacén de claves. Ejecute el comando: more %CVP_HOME%\conf\security.properties. Necesita esta contraseña cuando ejecute los comandos keytool.
2. Copie la carpeta %CVP_HOME%\conf\security en otra carpeta.
3. Abra una ventana de comandos como Administrador para ejecutar los comandos.

Servidores CVP

Paso 1. Para eliminar los certificados de servidores CVP, ejecute estos comandos:

```
%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
```

Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Para generar el certificado WSM, ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Nota: de forma predeterminada, los certificados se generan para dos años. Utilice -valid XXXX para establecer la fecha de caducidad cuando se vuelven a generar los certificados; de lo contrario, los certificados son válidos durante 90 días y deben estar firmados por una CA antes de esta fecha. Para la mayoría de estos certificados, entre 3 y 5 años deben ser un tiempo de validación razonable.

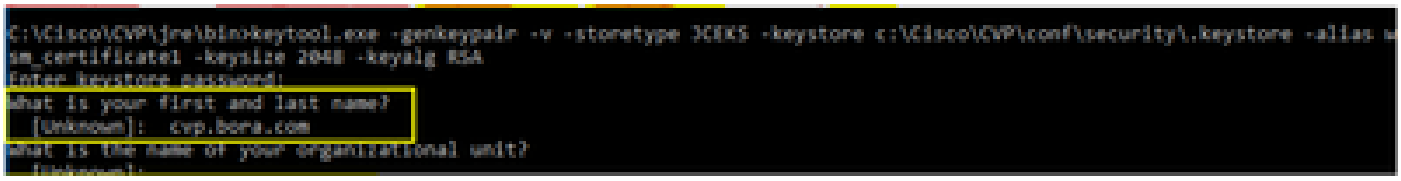
Estas son algunas entradas de validez estándar:

Un año	365

Dos años	730
Tres años	1095
Cuatro años	1460
Cinco años	1895
Diez años	3650

⚠ Precaución: en certificados de 12.5 debe ser SHA 256, tamaño de clave 2048, y algoritmo de cifrado RSA, utilice estos parámetros para establecer estos valores: -keyalg RSA y -keysize 2048. Es importante que los comandos del almacén de claves CVP incluyan el parámetro -storetype JCEKS. Si esto no se hace, el certificado, la clave o peor aún el almacén de claves puede dañarse.

Especifique el FQDN del servidor, en la pregunta ¿cuál es su nombre y apellidos?



Complete estas otras preguntas:

¿Cuál es el nombre de la unidad organizativa?

[Desconocido]: <especificar OU>

¿Cuál es el nombre de su organización?

[Desconocido]: <especifique el nombre de la organización>

¿Cuál es el nombre de su ciudad o localidad?

[Desconocido]: <especifique el nombre de la ciudad/localidad>

¿Cuál es el nombre de su estado o provincia?

[Desconocido]: <especifique el nombre del estado o provincia>

¿Cuál es el código de país de dos letras para esta unidad?

[Desconocido]: <especificar código de país de dos letras>

Especifique yes para las dos entradas siguientes.

Paso 3. Realice los mismos pasos para vxml_certificate y 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
```

servidor de informes de CVP

Paso 1. Para eliminar los certificados de WSM y del servidor de informes, ejecute estos comandos:

```
%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
```

Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Para generar el certificado WSM, ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Especifique el FQDN del servidor para la consulta ¿cuál es su nombre y apellido? y continúe con los mismos pasos que realizó con los servidores CVP.

Paso 3. Realice los mismos pasos para callserver_certificate:

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

CVP OAMP (implementación de UCCE)

Dado que en la versión 12.x de la solución PCCE todos los componentes de la solución están controlados por SPOG y OAMP no está instalado, estos pasos solo son necesarios para una solución de implementación de UCCE.

Paso 1. Para eliminar los certificados de servidor WSM y OAMP, ejecute estos comandos:

```
%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
```

Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Para generar el certificado WSM, ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Especifique el FQDN del servidor para la consulta ¿cuál es su nombre y apellido? y continúe con los mismos pasos que realizó con los servidores CVP.

Paso 3. Realice los mismos pasos para oamp_certificate:

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

2. Generar el CSR

Nota: El explorador compatible con RFC5280 requiere que se incluya el nombre alternativo del sujeto (SAN) con cada certificado. Esto se puede lograr utilizando el parámetro -ext con SAN al generar el CSR.

Nombre alternativo del asunto

El parámetro -ext permite que un usuario utilice extensiones específicas. En el ejemplo que se muestra se agrega un nombre alternativo de sujeto (SAN) con el nombre de dominio completo (FQDN) del servidor, así como el host local. Los campos SAN adicionales se pueden agregar como valores separados por comas.

Los tipos de SAN válidos son:

```
ip:192.168.0.1
```

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

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

Servidores CVP

Paso 1. Genere la solicitud de certificado para el alias. Ejecute este comando y guárdelo en un archivo (por ejemplo, wsm_certificate):

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Realice los mismos pasos para vxml_certificate y 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 -
```

Introduzca la contraseña del almacén de claves cuando se le solicite.

servidor de informes de CVP

Paso 1. Genere la solicitud de certificado para el alias. Ejecute este comando y guárdelo en un archivo (por ejemplo, oampreport_certificate):

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Realice los mismos pasos para callserver_certificate:

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

CVP OAMP (implementación de UCCE)

Paso 1. Genere la solicitud de certificado para el alias. Ejecute este comando y guárdelo en un archivo (por ejemplo, oamp_certificate):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
Ensure to replace "mycvp.mydomain.com" with your OAMP FQDN.
Enter the keystore password when prompted.
```

Paso 2. Realice los mismos pasos para wsm_certificate:

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

3. Obtenga los certificados firmados por la CA

Paso 1. Firme los certificados en una CA (servidor WSM, Callserver y VXML para el servidor CVP; WSM y OAMP para el servidor CVP OAMP, y WSM y Callserver para el servidor Reporting).

Paso 2. Descargue los certificados de aplicación y el certificado raíz de la autoridad de la CA.

Paso 3. Copie el certificado raíz y los certificados firmados por la CA en la carpeta %CVP_HOME%\conf\security\ de cada servidor.

4. Importe los certificados firmados por la CA

Aplique estos pasos a todos los servidores de la solución CVP. Sólo los certificados de los componentes de ese servidor necesitan importar el certificado firmado por la CA.

Paso 1. Importe el certificado raíz. Ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite. En el mensaje Confiar en este certificado, escriba Sí.

Si hay un certificado intermedio, ejecute este comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias intermediate_ca -file
```

Introduzca la contraseña del almacén de claves cuando se le solicite. En el mensaje Confiar en este certificado, escriba Sí.

Paso 2. Importe el WSM firmado por la CA para ese certificado de servidor (CVP, informes y OAMP). Ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite. En el mensaje Confiar en este certificado, escriba Sí.

Paso 3. En los servidores CVP y los servidores de informes importan el certificado CA de Callserver con firma. Ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite. En el mensaje Confiar en este certificado, escriba Sí.

Paso 4. En los servidores CVP, importe el certificado firmado de CA del servidor VXML. Ejecute este comando:

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

Paso 5. En el servidor OAMP de CVP (sólo para UCCE) importe el certificado firmado de CA del servidor OAMP. Ejecute este comando:

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

Paso 6. Reinicie los servidores.

Nota: En la implementación de UCCE, asegúrese de agregar los servidores (Reporting, CVP Server, etc.) en CVP OAMP con el FQDN proporcionado al generar el CSR.

Servidores VOS

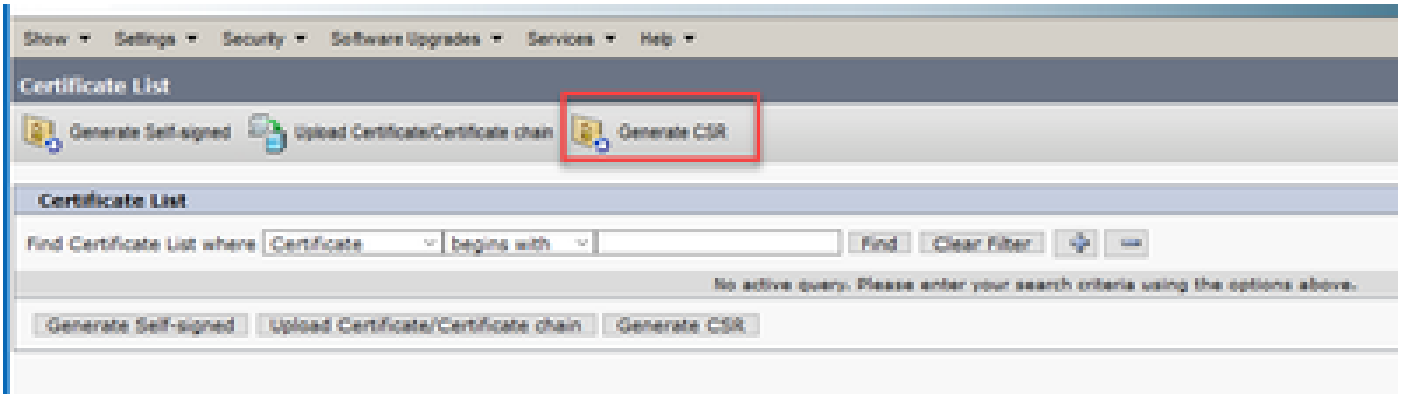
1. Generar certificado CSR

Este procedimiento explica cómo generar el certificado CSR de Tomcat a partir de plataformas basadas en Cisco Voice Operating System (VOS). Este proceso se aplica a todas las aplicaciones basadas en VOS, como:

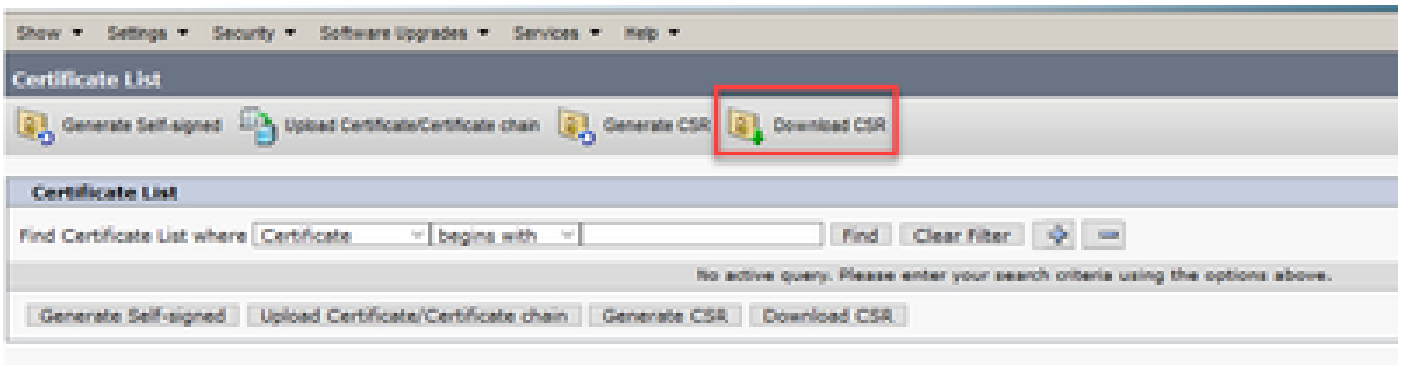
- CUCM
- Finesse
- CUIC \ Datos en directo (LD) \Identity Server(IDS)
- Conexión a la nube
- VB de Cisco

Paso 1. Vaya a la página de administración del sistema operativo Cisco Unified Communications: https://FQDN:<8443 o 443>/cmplatform.

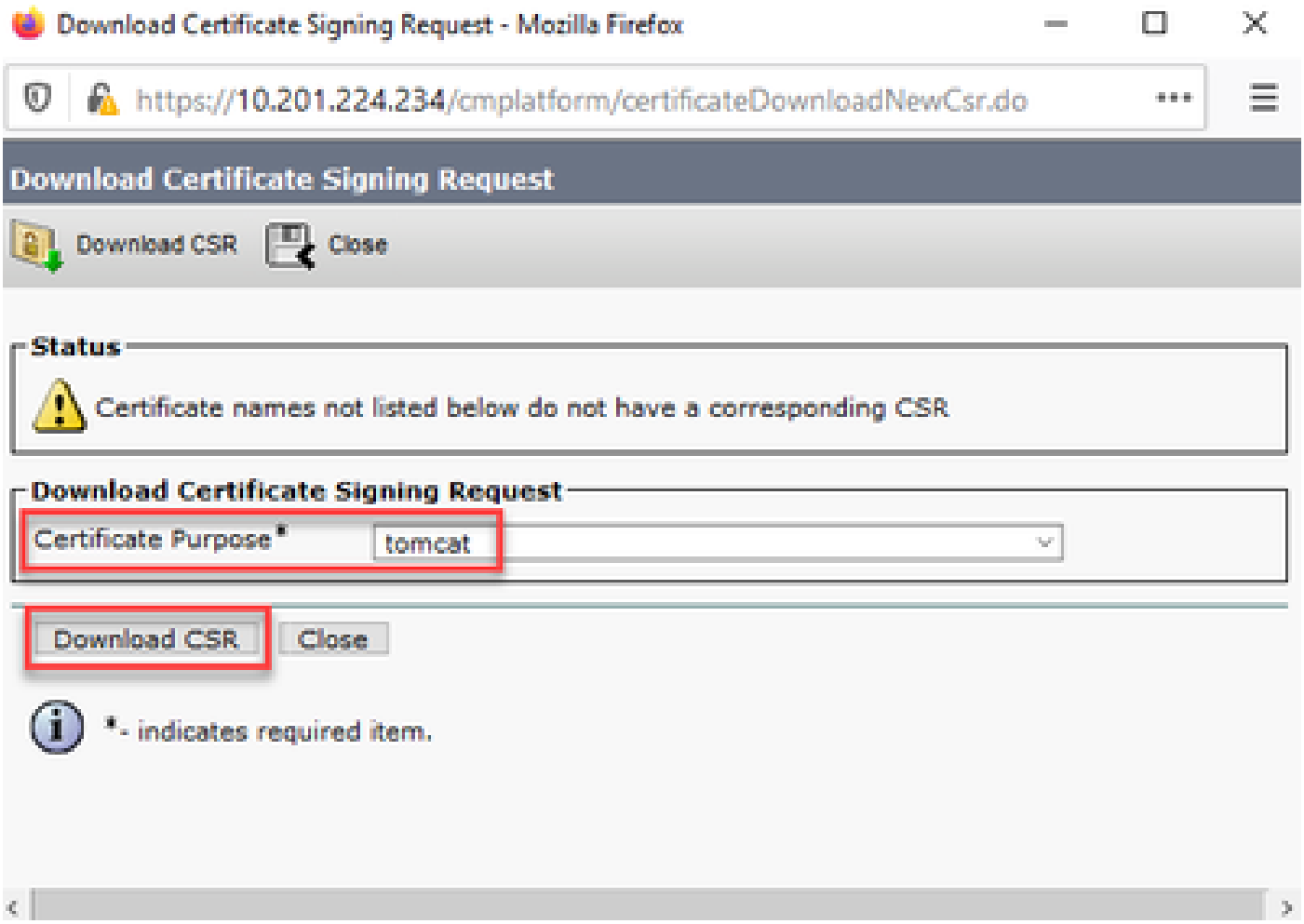
Paso 2. Navegue hasta Seguridad > Administración de certificados y seleccione Generar CSR.



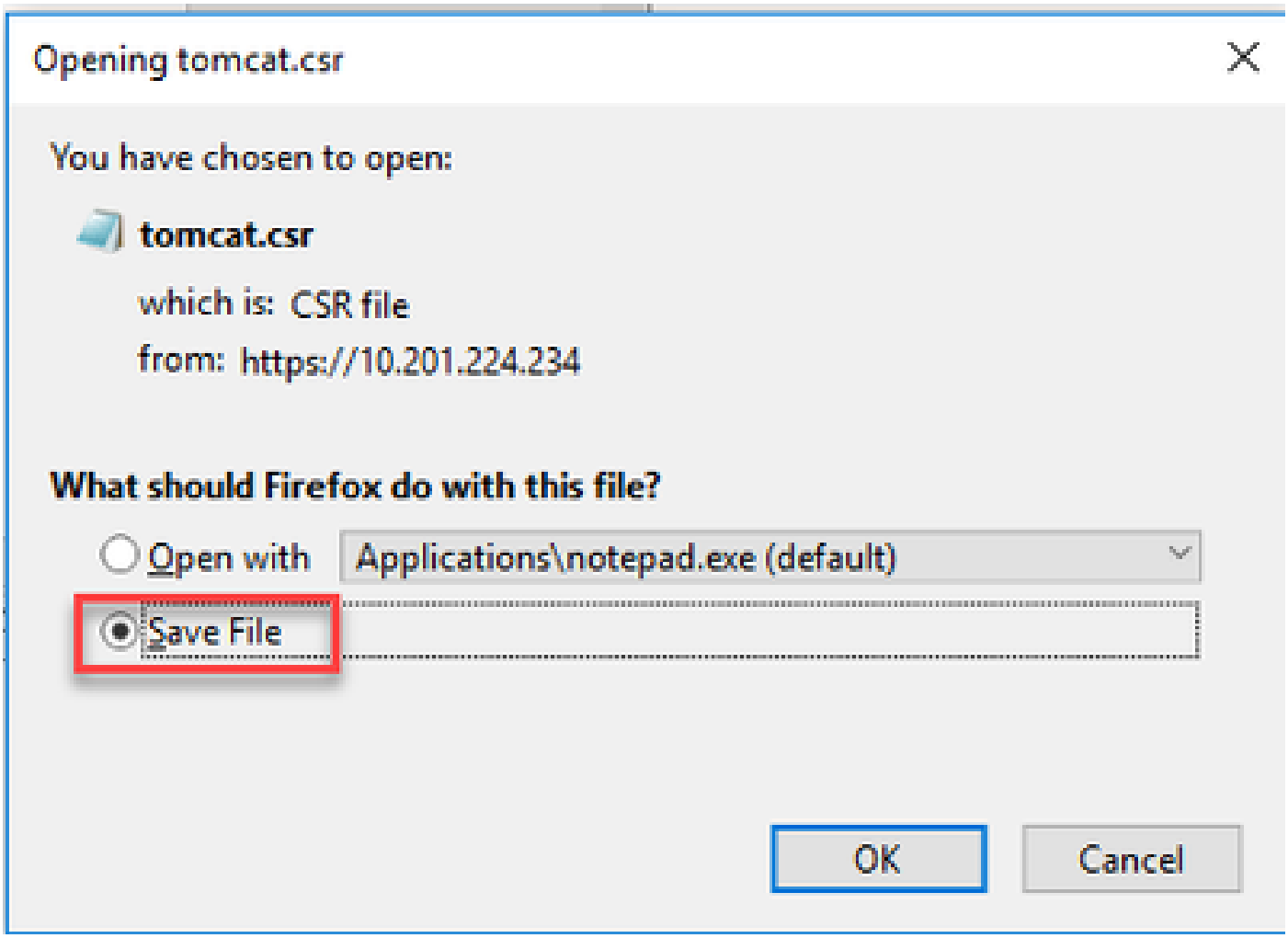
Paso 3. Una vez generado el certificado CSR, cierre la ventana y seleccione Descargar CSR.



Paso 4. Asegúrese de que el propósito del certificado es tomcat y haga clic en Descargar CSR.



Paso 5. Haga clic en Guardar archivo. El archivo se guarda en la carpeta Download (Descargar).



2. Obtenga los certificados firmados por la CA

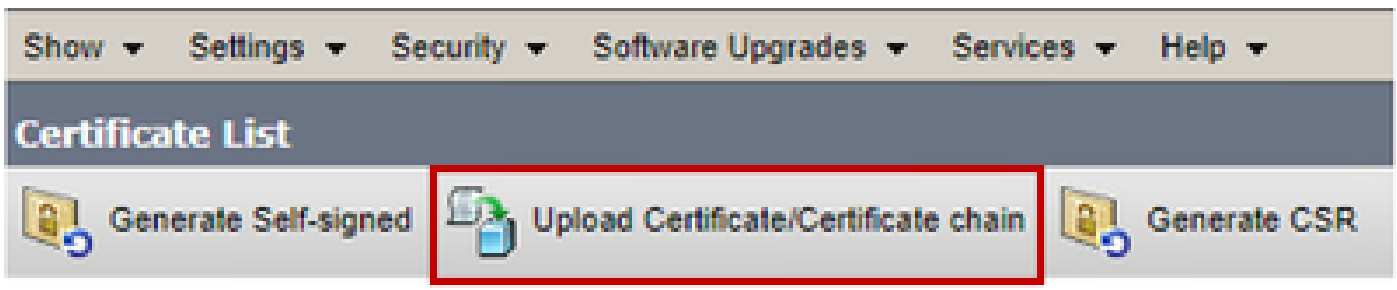
Paso 1. Firmar el certificado de Tomcat exportado en una CA.

Paso 2. Descargue la aplicación y la raíz certificada de la autoridad de la CA.

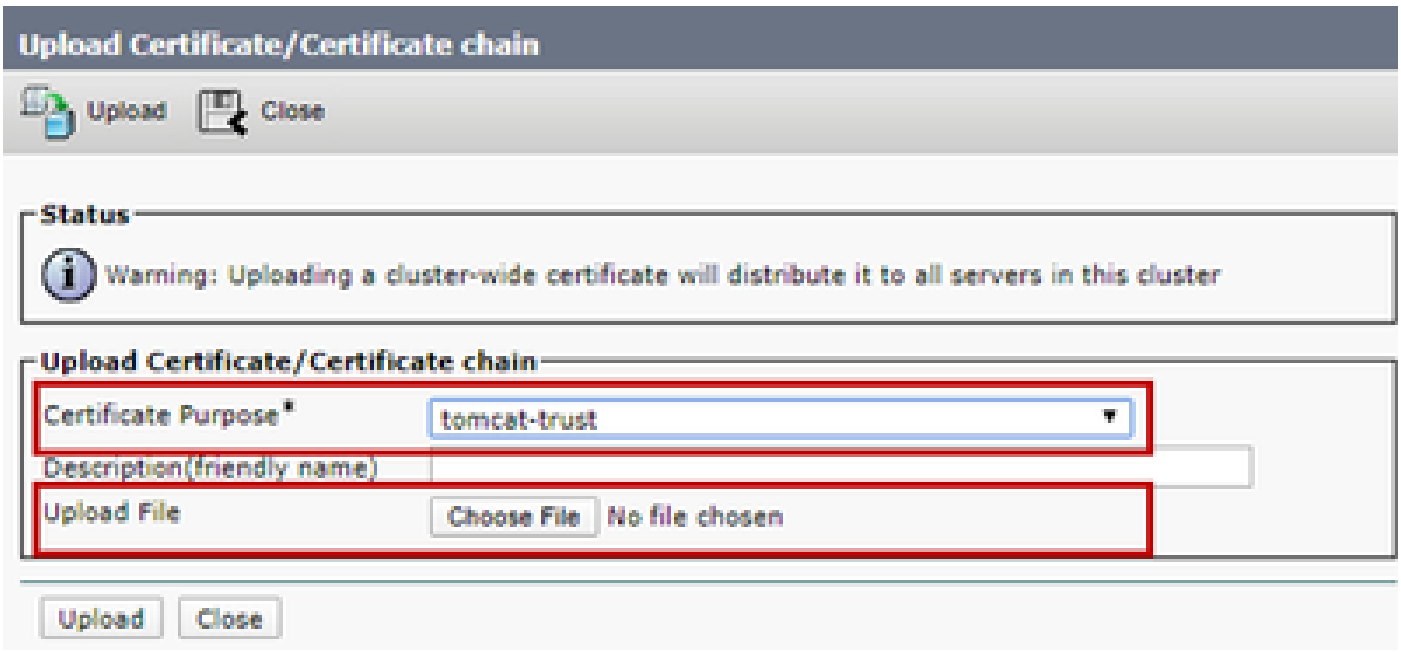
3. Cargue la aplicación y los certificados raíz

Paso 1. Vaya a la página de administración del sistema operativo Cisco Unified Communications: https://FQDN:<8443 o 443>/cmplatform.

Paso 2. Navegue hasta Seguridad > Administración de certificados y seleccione Cargar certificado/cadena de certificados.

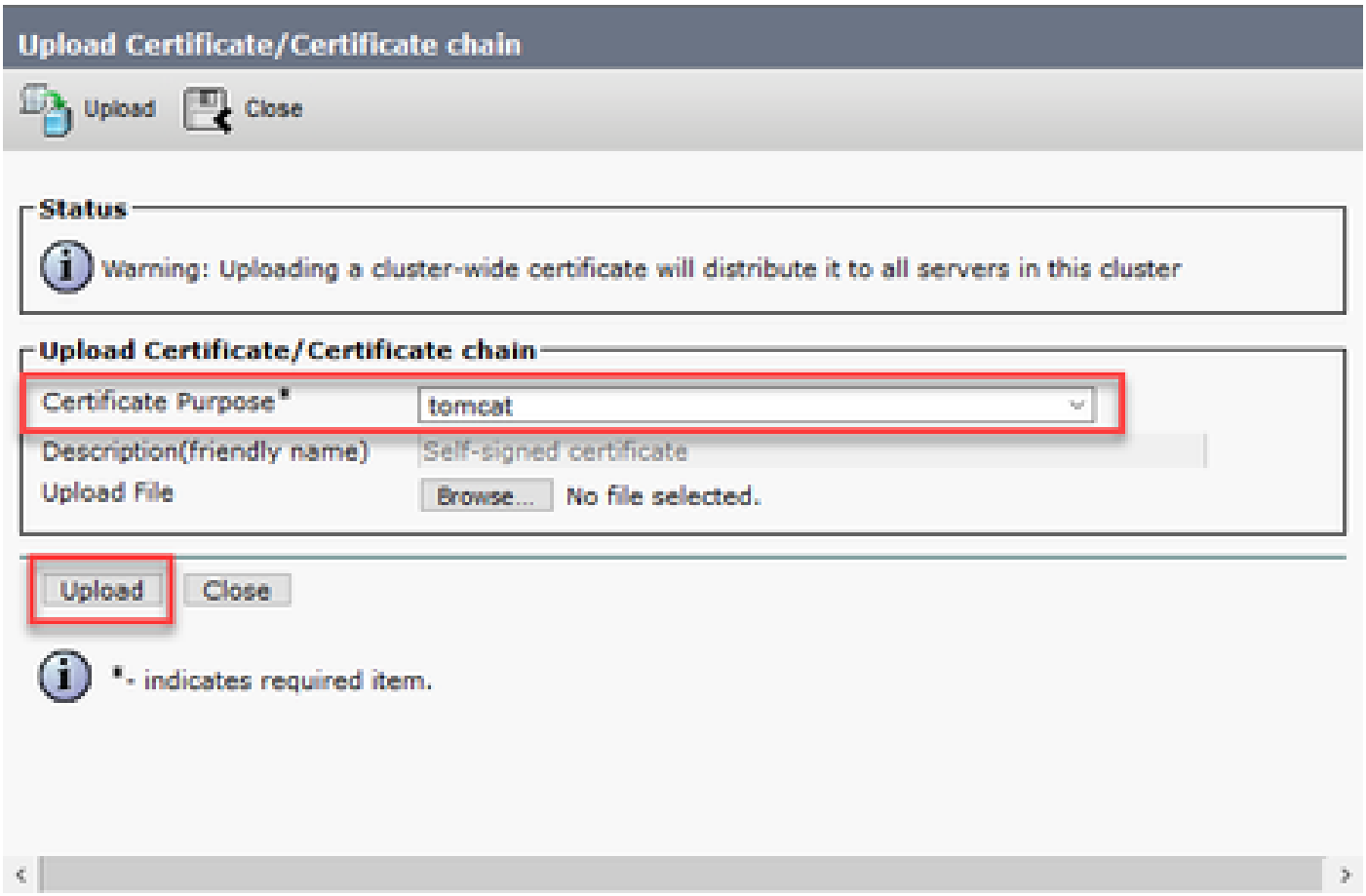


Paso 3. En la ventana Cargar certificado/cadena de certificados, seleccione tomcat-trust en el campo de propósito del certificado y cargue el certificado raíz.



Paso 4. Cargue un certificado intermedio (si lo hubiera) como tomcat-trust.

Paso 5. En la ventana Cargar certificado/cadena de certificado, seleccione ahora tomcat en el campo Propósito del certificado y cargue la aplicación Certificado firmado por CA.



Paso 6. Reinicie el servidor

Verificación

Después de reiniciar el servidor, ejecute estos pasos para verificar la implementación firmada por la CA:

Paso 1. Abra un explorador Web y borre la caché.

Paso 2. Cierre y vuelva a abrir el explorador.

Ahora debe ver el modificador de certificados para iniciar el certificado firmado por la CA y la indicación en la ventana del explorador de que el certificado está autofirmado y, por lo tanto, no es de confianza, debe desaparecer.

Troubleshoot

No hay pasos para solucionar problemas de implementación de certificados firmados por CA en esta guía.

Información Relacionada

- Guía de configuración de CVP: Guía de configuración de CVP - Seguridad

- Guía de configuración de UCCE: Guía de configuración de UCCE: Seguridad
- Guía de administración de PCCE: Guía de administración de PCE - Seguridad
- Certificados autofirmados de UCCE: certificados autofirmados de UCCE de Exchange
- Certificados autofirmados de PCCE: certificados autofirmados de PCCE de Exchange
- Instalar y migrar a OpenJDK en CCE 12.5(1): migración de CCE OpenJDK
- Instalación y migración a OpenJDK en CVP 12.5(1): migración a OpenJDK de CVP

Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).