Certificados autofirmados de Exchange en una solución PCCE 12.6

Contenido

Introducción

Este documento describe cómo intercambiar certificados autofirmados en la solución Cisco Packaged Contact Center Enterprise (PCCE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- PCCE versión 12.6(2)
- Customer Voice Portal (CVP) versión 12.6(2)
- Virtualized Voice Browser (VB) 12.6(2)
- Estación de trabajo de administración / Servidor de fecha de administración (AW/ADS)

12.6(2)
- Cisco Unified Intelligence Server (CUIC)
- Plataforma de colaboración con clientes (CCP) 12.6(2)
- Chat y correo electrónico empresarial (ECE) 12.6(2)

Componentes Utilizados

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

- PCCE 12.6(2)
- CVP 12.6(2)

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

En la solución PCCE de 12.x, todos los dispositivos se controlan a través de un único panel de acceso (SPOG) alojado en el servidor principal de AW. Debido a la conformidad con la gestión de seguridad (SRC) de la versión PCCE 12.5(1), toda la comunicación entre SPOG y otros servidores de la solución se realiza estrictamente a través del protocolo HTTP seguro.

Los certificados se utilizan para lograr una comunicación segura y sin problemas entre SPOG y los otros dispositivos. En un entorno de certificados autofirmado, el intercambio de certificados entre los servidores es imprescindible.

Procedimiento

Éstos son los componentes desde los que se exportan los certificados autofirmados y los componentes en los que se deben importar los certificados autofirmados.

(i) Todos los servidores AW/ADS: Estos servidores requieren certificado de:

- Plataforma Windows:
    - ICM: Router y registrador (Rogger){A/B}, gateway periférico (PG){A/B}, todos los servidores AW/ADS y ECE.

Nota: se necesitan IIS y Diagnostic Framework Portico (DFP).

    - CVP: servidores CVP, servidor de informes CVP.

Nota: se necesita el certificado de administración de servicios web (WSM) de todos los servidores. Los certificados deben tener un nombre de dominio completamente calificado (FQDN).

- Plataforma VOS: Cloud Connect, Cisco Virtualized Voice Browser (VB), Cisco Unified Communication Manager (CUCM), Finesse, Cisco Unified Intelligence Center (CUIC), Live Data (LD), Identity Server (IDS) y otros servidores aplicables.

(ii) Router \ Logger Servers: Estos servidores requieren certificado de:

- Plataforma Windows: todos los servidores AW/ADS certificados IIS.

(iii) Servidores PG: Estos servidores requieren certificado de:

- Plataforma Windows: todos los servidores AW/ADS certificados IIS.
- Plataforma VOS: CUCM publisher (solo servidores CUCM PG); Cloud Connect y CCP (solo servidor MR PG).

Nota: Esto es necesario para descargar el cliente JTAPI del servidor CUCM.

(iv) Servidores CVP: Estos servidores requieren un certificado de

- Plataforma Windows: todos los servidores ADS certificado IIS
- Plataforma VOS: servidor Cloud Connect, servidores VB.

(v) Servidor de informes de CVP: Este servidor requiere un certificado de:

- Plataforma Windows: todos los servidores ADS certificado IIS

(vi) Servidores VB: Este servidor requiere certificado de:

- Plataforma Windows: todos los servidores ADS certificado IIS, certificado VXML del servidor CVP y certificado Callserver del servidor CVP
- Plataforma VOS: servidor Cloud Connect.

Los pasos necesarios para intercambiar eficazmente los certificados autofirmados en la solución se dividen en tres secciones.

Sección 1: Intercambio de certificados entre servidores CVP y servidores ADS.

Sección 2: Intercambio de certificados entre las aplicaciones de la plataforma VOS y el servidor ADS.

Sección 3: Intercambio de certificados entre Roggers, PG y ADS Server.

Sección 1: Intercambio de certificados entre servidores CVP y ADS

Los pasos necesarios para completar este intercambio correctamente son:

Paso 1. Exportar certificados WSM de servidores CVP.

Paso 2. Importar servidores CVP Certificado WSM a servidores ADS.

Paso 3. Exportar certificado de servidor ADS.

Paso 4. Importar el servidor ADS a servidores CVP y servidor de informes CVP.

Paso 1. Exportar certificados de servidor CVP

Antes de exportar los certificados de los servidores CVP, debe volver a generar los certificados con el FQDN del servidor; de lo contrario, pocas funciones, como Smart Licensing, Virtual Agent Voice (VAV) y la sincronización de CVP con SPOG pueden experimentar problemas.

⚠ Precaución: antes de empezar, debe hacer lo siguiente:
1. Abra una ventana de comandos como administrador.
2. Para 12.6.2, para identificar la contraseña del almacén de claves, vaya a la carpeta %CVP_HOME%\bin y ejecute el archivo DecryptKeystoreUtil.bat.
3. Para 12.6.1, para identificar la contraseña del almacén de claves, ejecute el comando more %CVP_HOME%\conf\security.properties.
4. Necesita esta contraseña cuando ejecute los comandos keytool.
5. En el directorio %CVP_HOME%\conf\security\, ejecute el comando copy .keystore backup.keystore.

✎ Nota: Puede simplificar los comandos utilizados en este documento mediante el uso del parámetro keytool -storepass. Proporcione la contraseña de la herramienta clave identificada para todos los servidores CVP. Para los servidores ADS, la contraseña predeterminada es: changeit

---

Para regenerar el certificado en los servidores CVP, ejecute estos pasos:

(i) Enumere los certificados en el servidor

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

✎ Nota: Los servidores CVP tienen los siguientes certificados autofirmados: wsm_certificate, vxml_certificate y callserver_certificate. Si utiliza el parámetro -v de la herramienta clave, podrá ver información más detallada de cada certificado. Además, puede agregar el símbolo "**>**" al final del comando keytool.exe list para enviar el resultado a un archivo de texto, por ejemplo: **>** test.txt

---

ii) Suprimir los antiguos certificados autofirmados

Servidores CVP: Comandos para eliminar los certificados autofirmados:

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

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

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

Servidores de informes de CVP: Comandos para eliminar los certificados autofirmados:

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

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

Nota: Los servidores de informes de CVP tienen los siguientes certificados autofirmados: wsm_certificate, callserver_certificate.

(iii) Generar los nuevos certificados autofirmados con el FQDN del servidor

Servidores CVP

Comando para generar el certificado autofirmado para WSM:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

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.

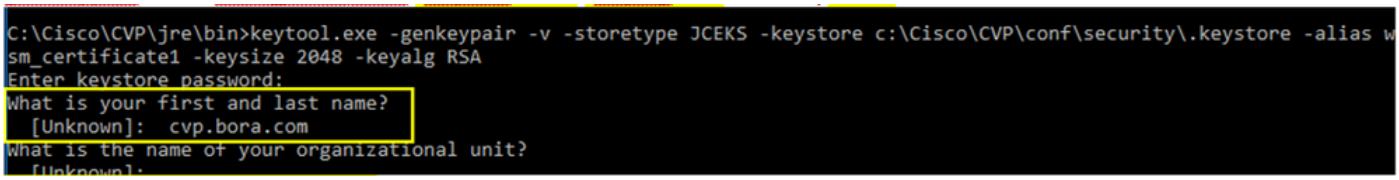
Estas son algunas entradas de validez estándar:

Un año	365
Dos años	730
Tres años	1095

Cuatro años	1460
Cinco años	1895
Diez años	3650

⚠ Precaución: a partir de certificados 12.5 deben ser SHA 256, Key Size 2048, y encryption Algorithm 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 apellido?



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.

Realice los mismos pasos para vxml_certificate y callserver_certificate:

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

```
genkeypair -alias vxml_certificate -keysize 2048 -keyalg RSA -validity XXXX

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias callserver_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Reinicie el servidor de llamadas CVP.

Servidores de informes de CVP

Comando para generar los certificados autofirmados para WSM:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

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.

Realice los mismos pasos para callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias callserver_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Reinicie los servidores de informes.

(iv) Exportar wsm_Certificate desde CVP y servidores de informes

a) Exporte el certificado WSM de cada servidor CVP a una ubicación temporal y cambie el nombre del certificado con el nombre que desee. Puede cambiarle el nombre por wsmcsX.crt. Sustituya "X" por el nombre de host del servidor. Por ejemplo, wsmcsa.crt, wsmcsb.crt , wsmrepa.crt , wsmrepb.crt.

Comando para exportar los certificados autofirmados:

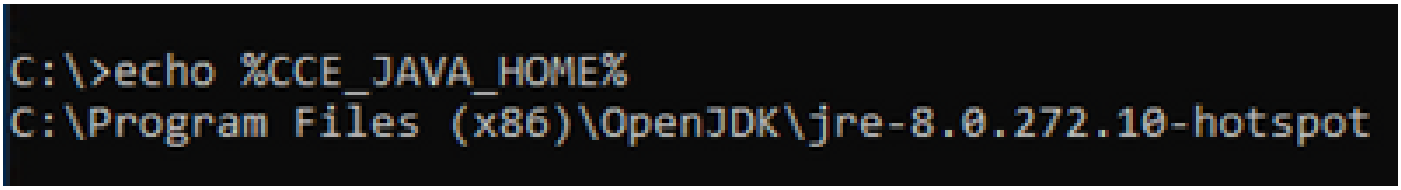
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
export -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

b) Copie el certificado de la ruta de acceso %CVP_HOME%\conf\security\wsm.crt, cámbiele el nombre a wsmcsX.crt y muévalo a una carpeta temporal en el servidor ADS.

Paso 2. Importar certificado WSM de servidores CVP a servidor ADS

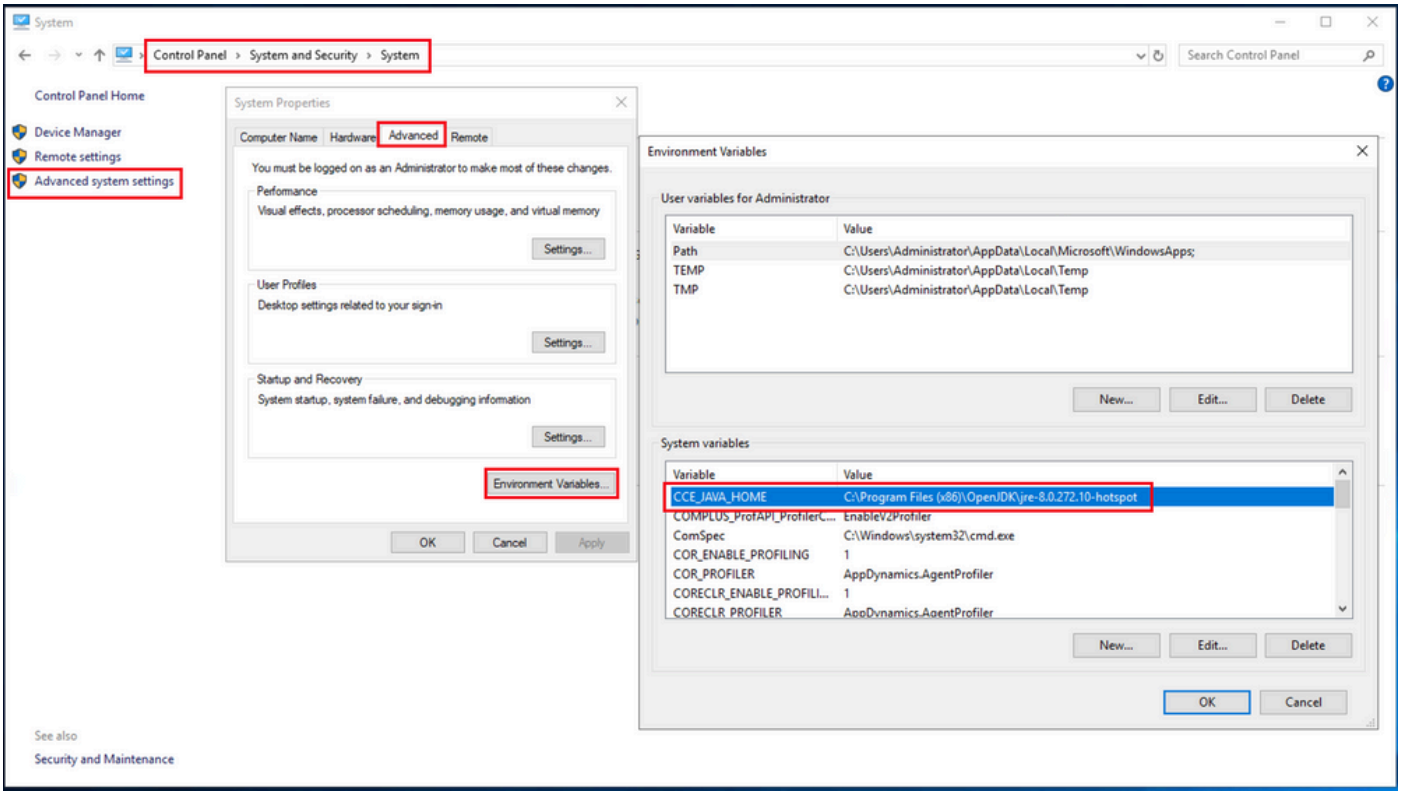
Para importar el certificado en el servidor de ADS debe utilizar la herramienta de claves que forma parte del conjunto de herramientas de Java. Hay un par de maneras que usted puede encontrar la ruta de inicio de Java donde se aloja esta herramienta.

(i) Comando CLI > echo %CCE_JAVA_HOME%



java home path

(ii) Manualmente a través de la configuración avanzada del sistema, como se muestra en la imagen.



Variables de entorno

En PCCE 12.6, la ruta predeterminada de OpenJDK es C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin

Comandos para importar los certificados autofirmados:

```
cd %CCE_JAVA_HOME%\bin
keytool.exe -import -file C:\Temp\certs\wsmcsX.crt -alias {fqdn_of_CVP} -keystore {ICM install directory}\ssl\cacerts
```

Nota: Repita los comandos para cada CVP de la implementación y realice la misma tarea en otros servidores ADS

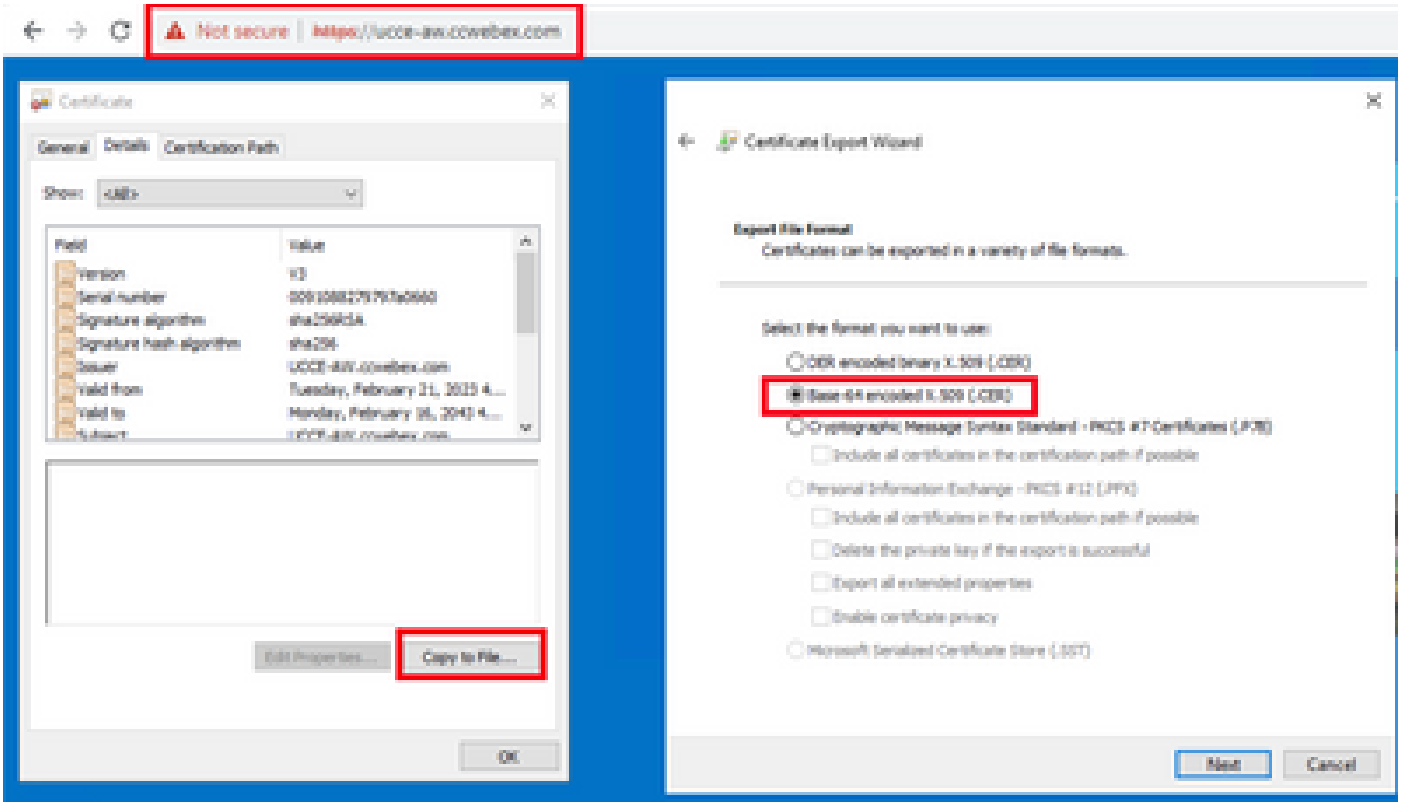
(iii) Reinicie el servicio Apache Tomcat en los servidores ADS.

Paso 3. Exportar certificado de servidor ADS

Estos son los pasos para exportar el certificado de ADS:

(i) En el servidor ADS desde un navegador, navegue hasta la url del servidor: https://<servername>.

(ii) Guarde el certificado en una carpeta temporal, por ejemplo: c:\temp\certs y denomine el certificado como ADS<svr>[ab].cer.



Exportar certificados de ADS

Nota: Seleccione la opción Codificado Base-64 X.509 (.CER).

Paso 4. Importar certificado de servidor ADS a servidores CVP y servidor de informes

(i) Copie el certificado en los servidores de CVP y en el servidor de informes de CVP en el directorio %CVP_HOME%\conf\security.

(ii) Importar el certificado a servidores CVP y servidor de informes CVP.

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -trustcacerts -alias {fqdn_of_ads} -file %CVP_HOME%\conf\security\ADS{svr}[ab].cer
```

Realice los mismos pasos para otros certificados de servidores ADS.

(iii) Reinicie los servidores CVP y el servidor de informes

Sección 2: Intercambio de certificados entre las aplicaciones de la plataforma VOS y el servidor ADS

Los pasos necesarios para completar este intercambio correctamente son:

Paso 1. Exportar certificados de servidor de aplicaciones de la plataforma VOS.

Paso 2. Importar certificados de aplicación de la plataforma VOS al servidor ADS.

Paso 3. Importar certificados de aplicación de plataforma de CUCM a servidores CUCM PG.

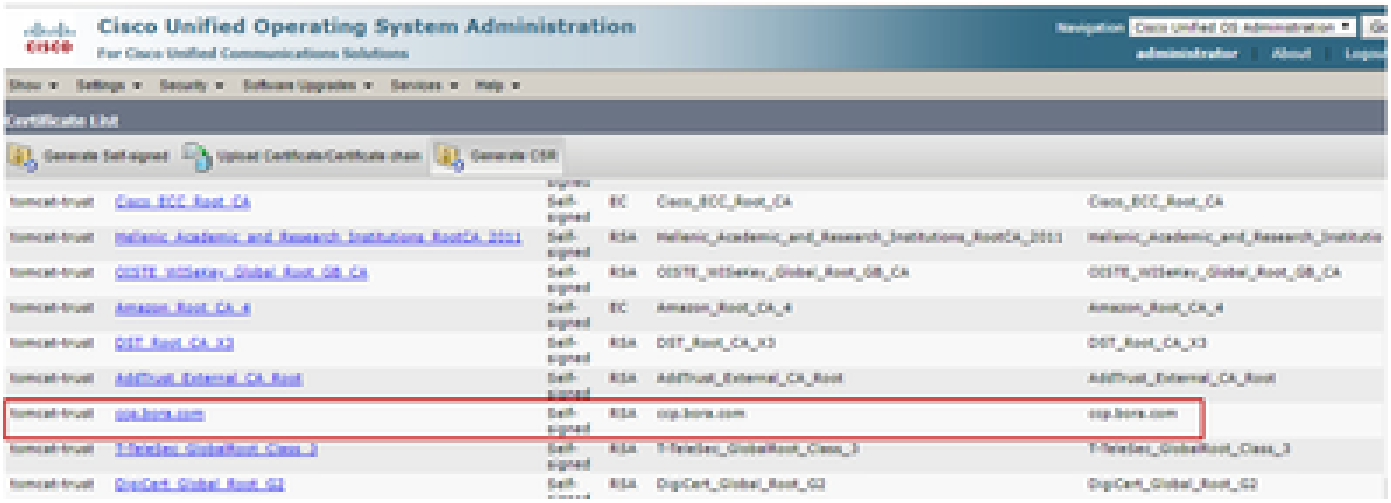
Este proceso se aplica a todas las aplicaciones VOS, como:

- CUCM
- VVB
- Finesse
- CUIC \ LD \ IDS
- Conexión a la nube

Paso 1. Exportar certificados de servidor de aplicaciones de la plataforma VOS.

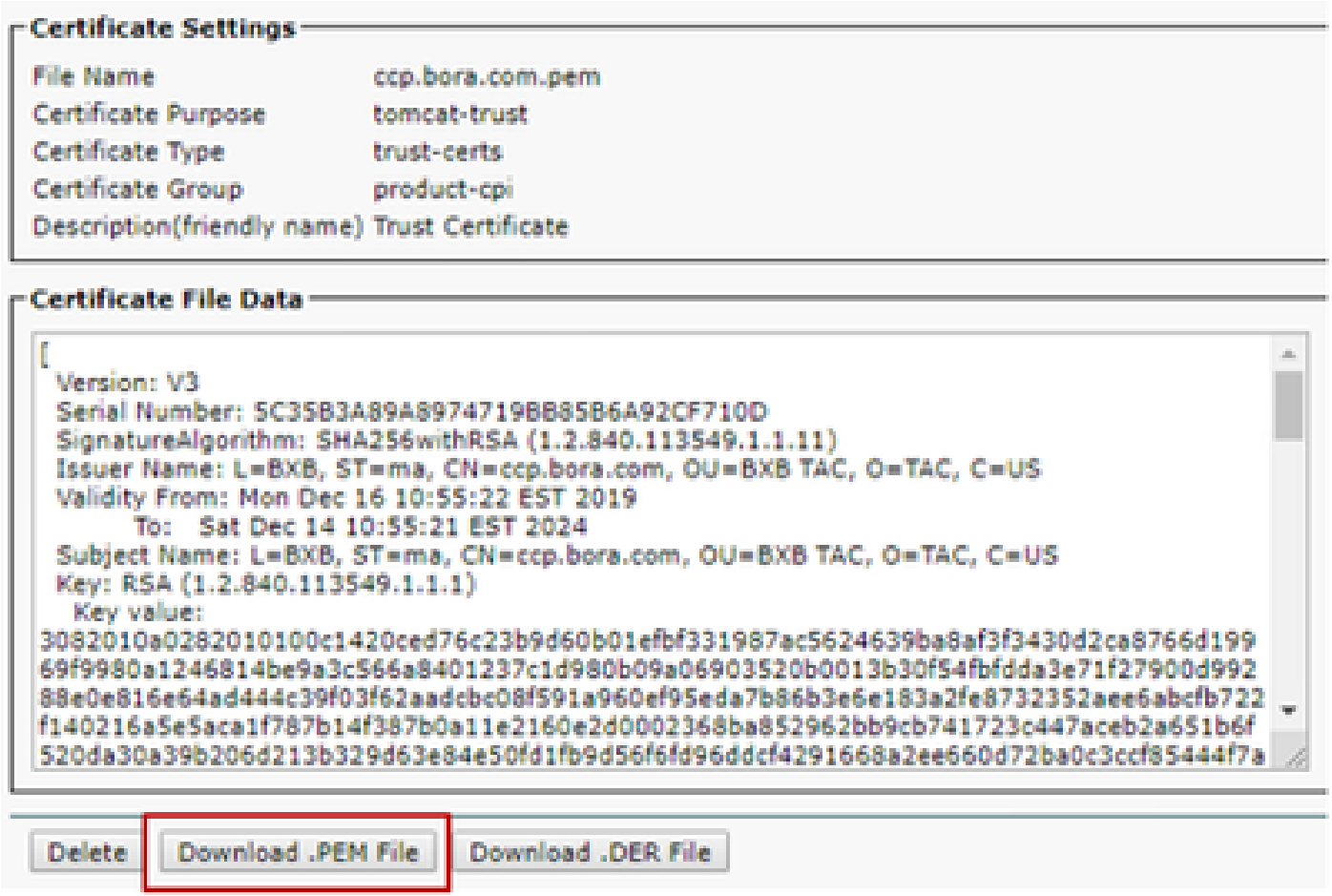
(i) Vaya a la página de administración del sistema operativo Cisco Unified Communications: https://FQDN:8443/cmplatform.

(ii) Navegue hasta Seguridad > Administración de certificados y busque los certificados del servidor primario de la aplicación en la carpeta tomcat-trust.



(iii) Seleccione el certificado y haga clic en Descargar archivo .PEM para guardarlo en una

carpeta temporal en el servidor ADS.



Nota: Realice los mismos pasos para el suscriptor.

Paso 2. Importar certificado de aplicación de la plataforma VOS al servidor ADS

Ruta para ejecutar la herramienta Clave: %CCE_JAVA_HOME%\bin

Comandos para importar los certificados autofirmados:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\vosapplicationX.cer -alias
{fqdn_of_VOS>} -keystore {ICM install directory}\ssl\cacerts
```

Reinicie el servicio Apache Tomcat en los servidores ADS.

Nota: Realice la misma tarea en otros servidores ADS

Paso 3. Importar certificado de aplicación de plataforma de CUCM al servidor CUCM PG

Ruta para ejecutar la herramienta Clave: %CCE_JAVA_HOME%\bin

Comandos para importar los certificados autofirmados:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\cucmapplicationX.cer -alias
{fqdn_of_cucm>} -keystore {ICM install directory}\ssl\cacerts
```

Reinicie el servicio Apache Tomcat en los servidores PG.

Nota: Realice la misma tarea en otros servidores CUCM PG

Sección 3: Intercambio de certificados entre Roggers , PG y servidores ADS

Los pasos necesarios para completar este intercambio correctamente son:

Paso 1. Exportar certificado IIS desde servidores Rogger y PG

Paso 2. Exportar certificado DFP de servidores Rogger y PG

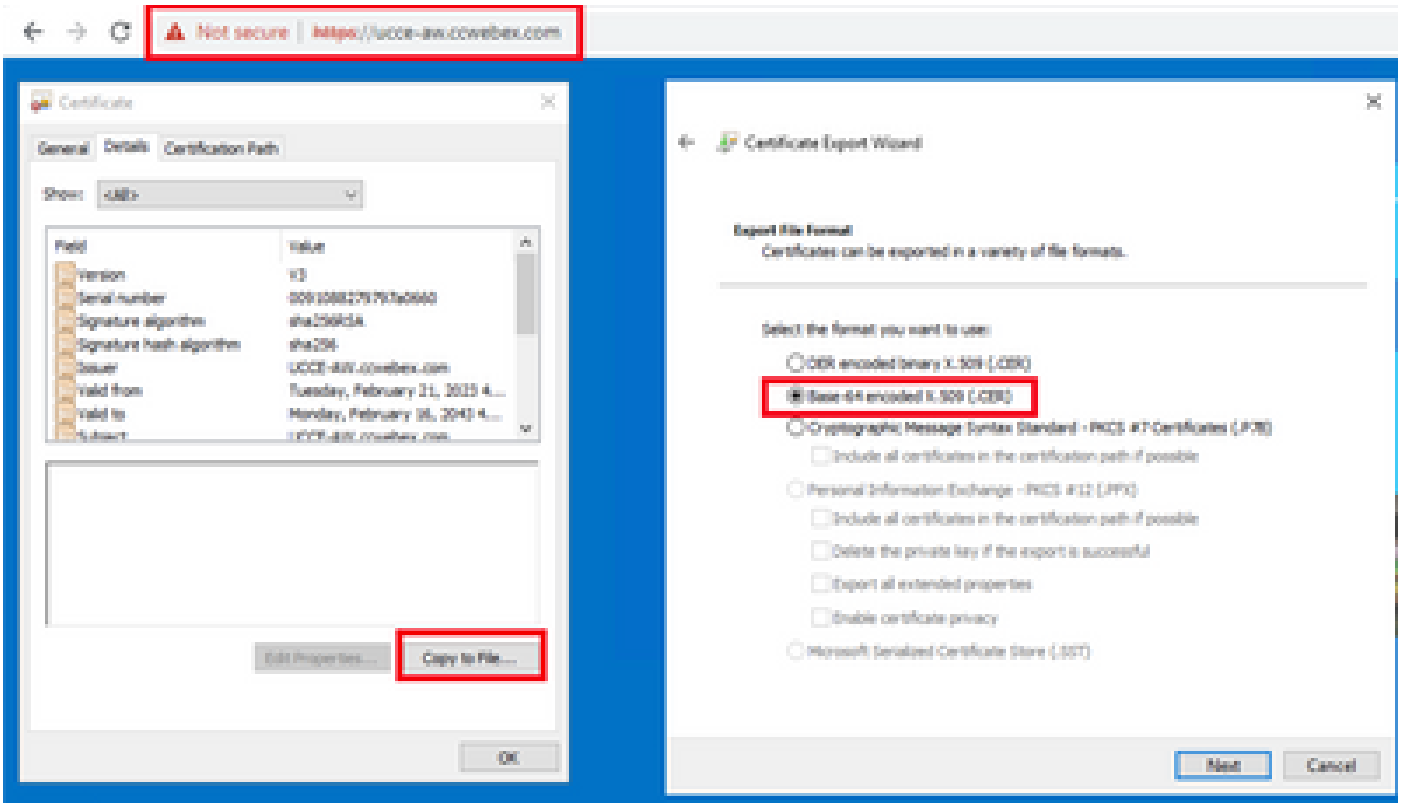
Paso 3. Importar certificados en servidores ADS

Paso 4. Importar certificado de ADS en servidores Rogger y PG

Paso 1. Exportar certificado IIS desde servidores Rogger y PG

(i) En el servidor ADS desde un navegador, navegue hasta la url de los servidores (Roggers , PG): https://{servername}

(ii) Guarde el certificado en una carpeta temporal, por ejemplo c:\temp\certs y denomínelo como ICM<svr>[ab].cer



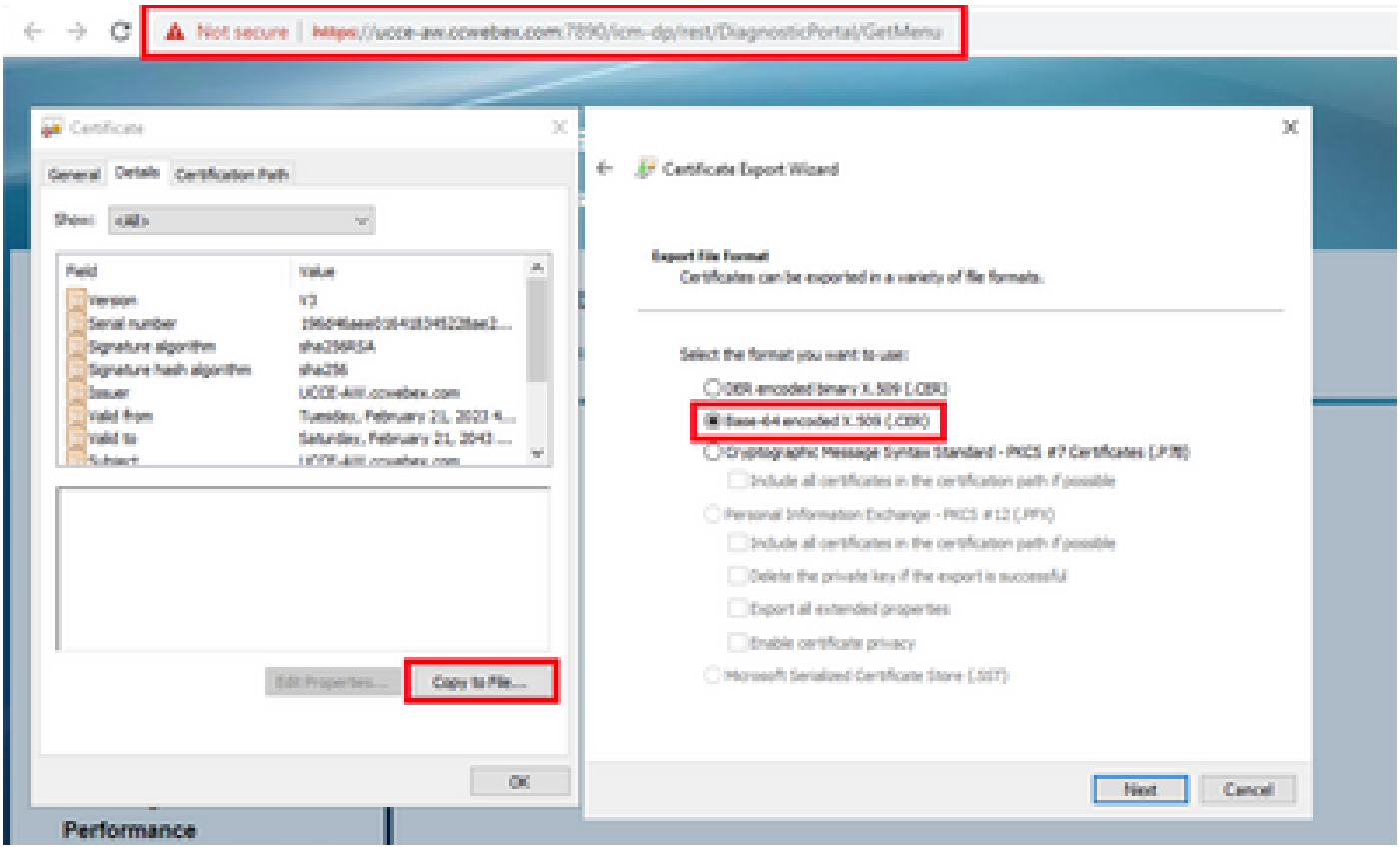
Exportar certificado IIS

Nota: Seleccione la opción Codificado Base-64 X.509 (.CER).

Paso 2. Exportar certificado DFP de servidores Rogger y PG

(i) En el servidor ADS desde un navegador, navegue hasta la URL de DFP de los servidores (Roggers, PGs): https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion

(ii) Guarde el certificado en el ejemplo de carpeta c:\temp\certs y denomine al certificado dfp{svr}[ab].cer



Exportar certificado DFP

Nota: Seleccione la opción Codificado Base-64 X.509 (.CER).

Paso 3. Importar certificados en el servidor de ADS

Comando para importar los certificados autofirmados de IIS en el servidor ADS. Ruta de acceso para ejecutar la herramienta Clave: %CCE_JAVA_HOME%\bin

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\temp\certs\ICM<svr>[ab].cer -alias
{fqdn_of_server}_IIS -keystore {ICM install directory}\ssl\cacerts
```

Nota: Importe todos los certificados de servidor exportados a todos los servidores ADS.

Comando para importar los certificados autofirmados de diagnóstico en el servidor ADS

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\dfp<svr>[ab].cer -alias
{fqdn_of_server}_DFP -keystore {ICM install directory}\ssl\cacerts
```

Nota: Importe todos los certificados de servidor exportados a todos los servidores ADS.

Reinicie el servicio Apache Tomcat en los servidores ADS.

Paso 4. Importar certificado de ADS en servidores Rogger y PG

Comando para importar los certificados autofirmados de IIS en los servidores Rogger y PG. Ruta de acceso para ejecutar la herramienta Clave: %CCE_JAVA_HOME%\bin.

```
%CCE_JAVA_HOME%\bin\keytool -keystore ..\lib\security\cacerts  -import -storepass changeit -
alias {fqdn_of_server}_IIS -file c:\temp\certs\ICM{svr}[ab].cer
```

Nota: Importe todos los certificados IIS del servidor ADS exportados a todos los servidores Rogger y PG.

Reinicie el servicio Apache Tomcat en los servidores Rogger y PG.

Sección 4: Integración del servicio web de CVP CallStudio

Para obtener información detallada sobre cómo establecer una comunicación segura para los elementos Web Services Element y Rest_Client

consulte la Guía del usuario de Cisco Unified CVP VXML Server y Cisco Unified Call Studio Release 12.6(2) - Integración de servicios web [Cisco Unified Customer Voice Portal] - Cisco

Información Relacionada

- Guía de configuración de CVP - Seguridad
- Guía de seguridad de UCCE
- Guía de administración de PCCE
- Certificados autofirmados de Exchange PCCE - PCCE 12.5
- Certificados autofirmados de Exchange UCCE: UCCE 12.5
- Certificados autofirmados de Exchange UCCE: UCCE 12.6
- Implemente certificados firmados por CA: CCE 12.6
- Intercambie certificados con la herramienta Contact Center Uploader
- 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).