Certificados autofirmados de Exchange en una solución UCCE 12.6

Contenido

Introducción

Este documento describe cómo intercambiar certificados autofirmados en la solución Unified Contact Center Enterprise (UCCE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCCE versión 12.6(2)
- Customer Voice Portal (CVP) versión 12.6(2)
- Navegador de voz virtualizado (VB) de Cisco

Componentes Utilizados

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

- UCCE 12.6(2)
- CVP 12.6(2)
- Cisco VB 12.6(2)
- Consola de operaciones de CVP (OAMP)
- CVP Nuevo OAMP (NOAMP)

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.

Antecedentes

En la configuración de soluciones de UCCE, las nuevas funciones que incluyen aplicaciones principales como Roggers, Peripheral Gateways (PG), Admin Workstations (AW), Finesse, Cisco Unified Intelligent Center (CUIC), etc. se realizan a través de la página de administración de Contact Center Enterprise (CCE). Para las aplicaciones de respuesta de voz interactiva (IVR) como CVP, Cisco VB y gateways, NOAMP controla la configuración de las nuevas funciones. A partir de CCE 12.5(1), debido al cumplimiento de la gestión de seguridad (SRC), toda la comunicación con CCE Admin y NOAMP se realiza estrictamente a través del protocolo HTTP seguro.

Para lograr una comunicación segura y sin problemas entre estas aplicaciones en un entorno de certificados autofirmado, el intercambio de certificados entre los servidores es imprescindible. La siguiente sección explica en detalle los pasos necesarios para intercambiar certificados autofirmados entre:

- Servidores CCE AW y servidores de aplicaciones de núcleo CCE
- Servidor CVP OAMP y servidores de componentes CVP

Nota: este documento SOLO se aplica a CCE versión 12.6. Consulte la sección de información relacionada para obtener enlaces a otras versiones.

Procedimiento

Servidores CCE AW y servidores de aplicaciones de núcleo CCE

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

Servidores CCE AW: Este servidor requiere un certificado de:

- Plataforma Windows: router y registrador (Rogger){A/B}, gateway periférico (PG){A/B}, todos los servidores AW/ADS y de correo electrónico y chat (ECE).

Nota: se necesitan certificados de marco de diagnóstico e IIS.

- Plataforma VOS: Cisco Unified Call Manager (CUCM), Finesse, CUIC, Live Data (LD), Identity Server (IDS) , Cloud Connect y otros servidores aplicables que forman parte de la base de datos de inventario.

Lo mismo se aplica a otros servidores AW de la solución.

Router \ Logger Server: Este servidor requiere certificado de:

- Plataforma Windows: todos los servidores AW certificados IIS.

Los pasos necesarios para intercambiar eficazmente los certificados autofirmados por CCE se dividen en estas secciones.

Sección 1: Intercambio de certificados entre router\registrador, PG y servidor AW.
Sección 2: Intercambio de certificados entre la aplicación de plataforma VOS y el servidor AW.

Sección 1: Intercambio de certificados entre router\registrador, PG y servidor AW

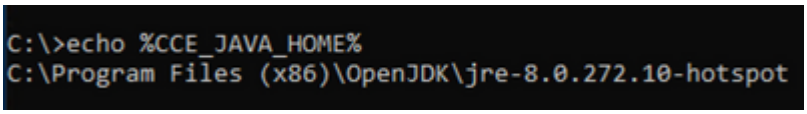
Los pasos necesarios para completar este intercambio correctamente son:

Paso 1. Exportar certificados IIS desde Router\Logger ,PG y todos los servidores AW.
Paso 2. Exportar certificados de Diagnostic Framework Portico (DFP) de los servidores Router\Logger y PG.
Paso 3. Importe certificados IIS y DFP de Router\Logger, PG a servidores AW.
Paso 4. Importe el certificado IIS al Router\Logger desde los servidores AW.

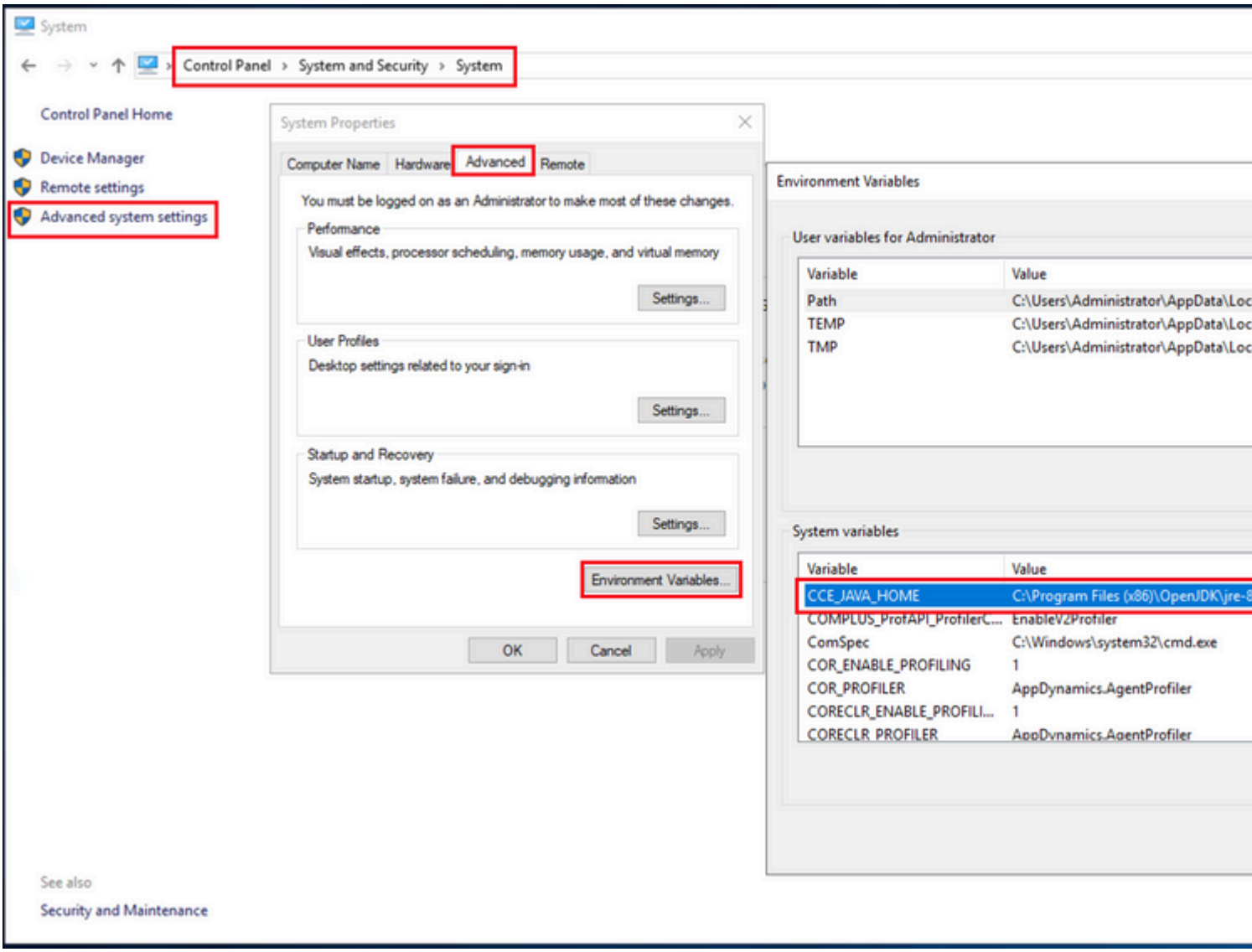
> **Precaución**: Antes de comenzar, debe realizar una copia de seguridad del almacén de claves y ejecutar los comandos desde el directorio raíz de Java como administrador.

(i) 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 %CCE_JAVA_HOME%**



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

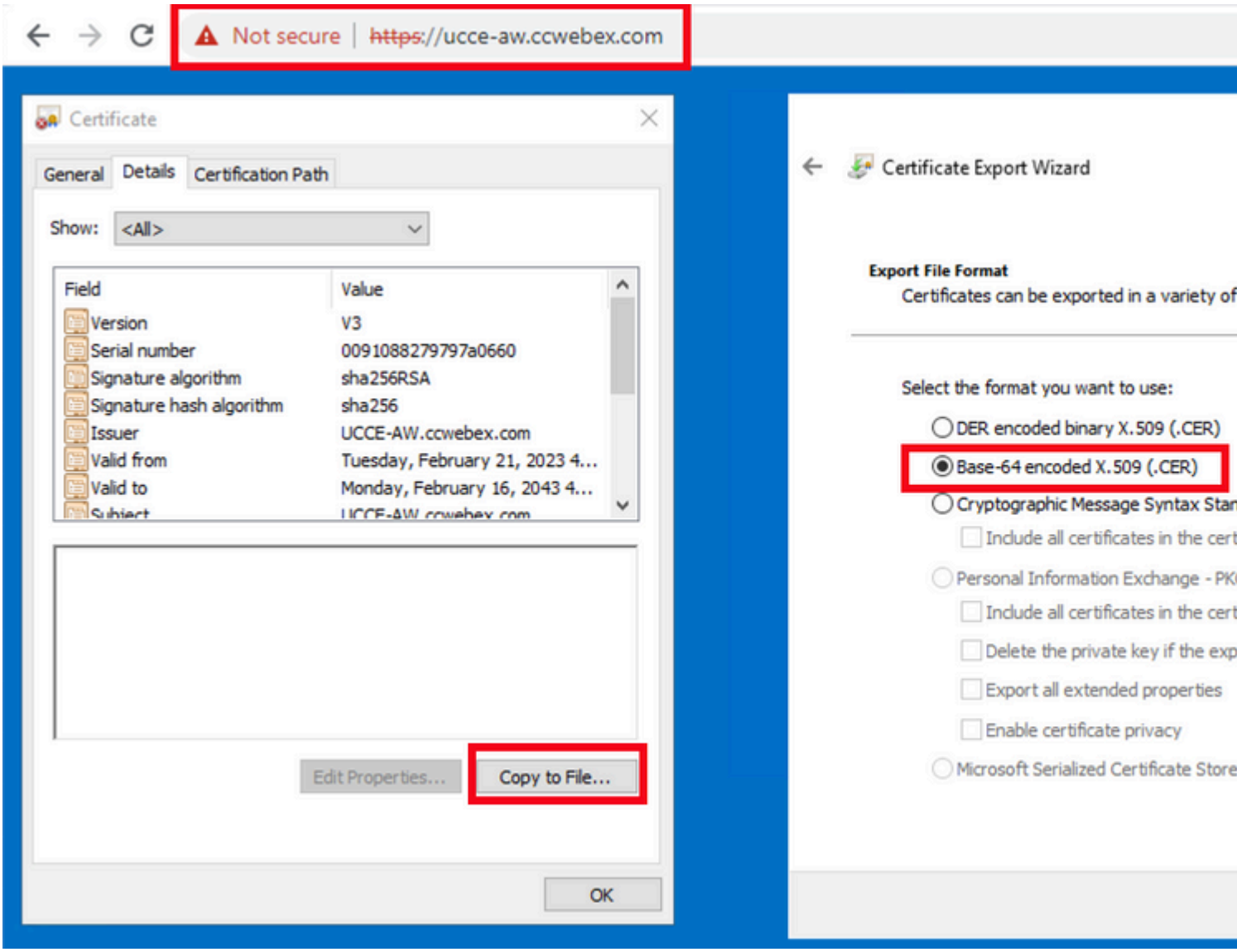


(ii) Haga una copia de seguridad del archivo cacerts desde la carpeta <directorio de instalación de ICM>ssl\ **.** Puede copiarlo en otra ubicación.

(iii) Abra una ventana de comandos como Administrador para ejecutar los comandos.

Paso 1. Exportar certificados IIS desde Router\Logger, PG y todos los servidores AW.

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

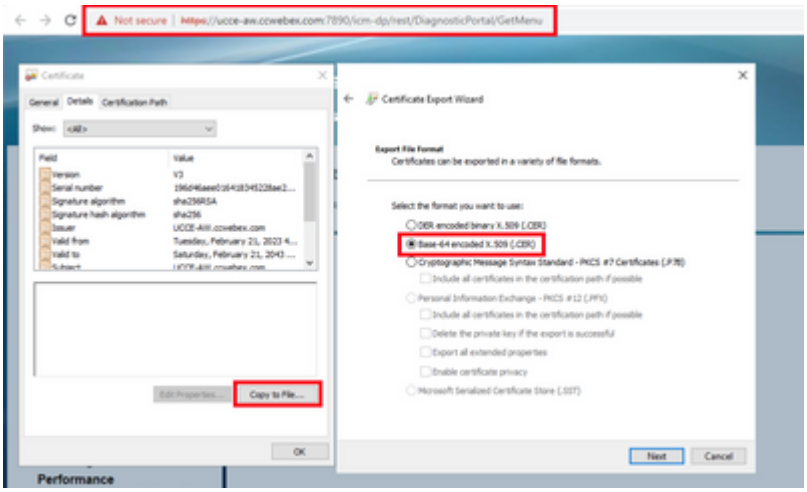


(ii) Guarde el certificado en una carpeta temporal. Por ejemplo, c:\temp\certs y asígnele el nombre ICM{svr}[ab].cer.

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

Paso 2. Exportar certificados de Diagnostic Framework Portico (DFP) desde servidores Router\Logger y PG.

(i) En el servidor AW, abra un navegador y navegue hasta los servidores (Router, Logger o Roggers, PGs) URL DFP: 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

---

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

Paso 3. Importar certificado IIS y DFP de Rogger, PG a servidores AW.

Comando para importar los certificados autofirmados de IIS en el servidor AW. La ruta para ejecutar la herramienta Clave: C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\IIS{svr}[ab].cer -alias {fqdn_of_server}_IIS
Example:%CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\IISAWA.cer -alias AWA_IIS -keystore
```

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

Comando para importar los certificados autofirmados DFP en servidores AW:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\dfp{svr}[ab].cer -alias {fqdn_of_server}_DFP
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\dfpAWA.cer -alias AWA_DFP -keystore
```

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

Reinicie el servicio Apache Tomcat en los servidores AW.

Paso 4. Importe el certificado IIS al Router\Logger desde los servidores AW.

Comando para importar los certificados autofirmados de IIS en servidores Rogger:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\IIS{svr}[ab].cer -alias {fqdn_of_server}_IIS
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\IISAWA.cer -alias AWA_IIS -keystore
```

Nota: Importe todos los certificados de servidor AW IIS exportados a los lados Rogger A y B.

Reinicie el servicio Apache Tomcat en los servidores Rogger.

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

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 AW.

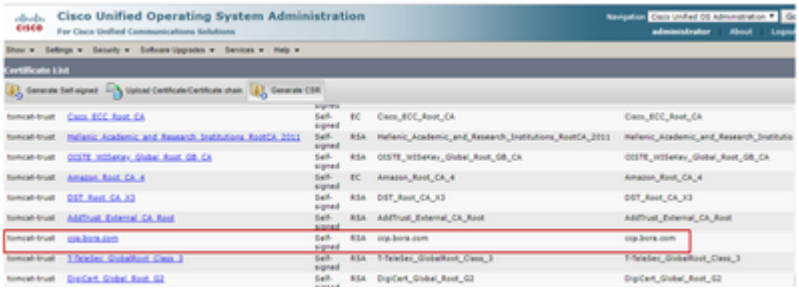
Este proceso es aplicable a aplicaciones VOS como:

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

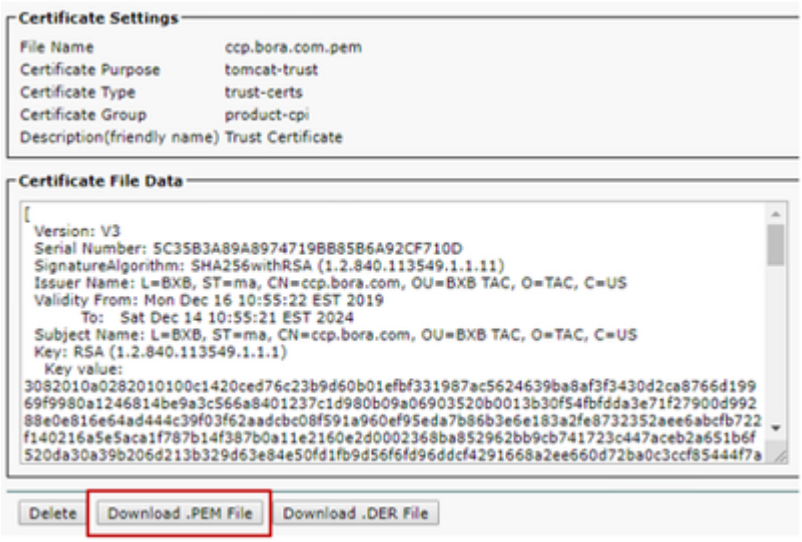
Paso 1. Exportar certificados de servidor de aplicaciones de la plataforma VOS.

(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 el archivo **download** .PEM para guardarlo en una carpeta temporal en el servidor AW.



Nota: Realice los mismos pasos para el suscriptor.

Paso 2. Importar aplicación de plataforma VOS al servidor AW.

Ruta para ejecutar la herramienta Clave: C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin

Comando para importar los certificados autofirmados:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\vosapplicationX.pem -alias {fqdn_of_VOS} -ke
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\CUICPub.pem -alias CUICPub -keysto
```

Reinicie el servicio Apache Tomcat en los servidores AW.

Nota: Realice la misma tarea en otros servidores AW.

Servidor CVP OAMP y servidores de componentes CVP

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) Servidor CVP OAMP: este servidor requiere un certificado de

- Plataforma Windows: certificado del Administrador de servicios web (WSM) de los servidores de CVP Server y Reporting Server.
- Plataforma VOS: servidor Cisco VB y Cloud Connect.

(ii) Servidores CVP: Este servidor requiere un certificado de

- Plataforma Windows: certificado WSM del servidor OAMP.
- Plataforma VOS: servidor Cloud Connect y servidor Cisco VB para una comunicación SIP y HTTP segura.

(iii) Servidores de informes de CVP: este servidor requiere un certificado de

- Plataforma Windows: certificado WSM del servidor OAMP.

(iv) servidores Cisco VB: este servidor requiere un certificado de

- Plataforma Windows: VXML del servidor CVP (HTTP seguro), callserver del servidor CVP (SIP seguro)
- Plataforma VOS: servidor Cloud Connect

Los pasos necesarios para intercambiar eficazmente los certificados autofirmados en el entorno de CVP se explican en estas tres secciones.

Sección 1: Intercambio de certificados entre el servidor CVP OAMP y el servidor CVP y los servidores de informes
Sección 2: Intercambio de certificados entre el servidor OAMP de CVP y las aplicaciones de la plataforma VOS

Sección 3: Intercambio de certificados entre el servidor CVP y las aplicaciones de la plataforma VOS

Sección 1: Intercambio de certificados entre el servidor CVP OAMP y el servidor CVP y los servidores de informes

Los pasos necesarios para completar este intercambio correctamente son:

Paso 1. Exporte el certificado WSM desde el servidor CVP, el servidor de informes y el servidor OAMP.
Paso 2. Importe certificados WSM del servidor CVP y del servidor de informes en el servidor OAMP.
Paso 3. Importe el certificado WSM del servidor CVP OAMP en los servidores CVP Server y Reporting.

> **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. Desde el directorio %CVP_HOME%\conf\security\, ejecute el comando, copy .keystore backup.keystore.

Paso 1. Exporte el certificado WSM desde el servidor CVP, el servidor de informes y el servidor OAMP.

(i) 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 wsmX.crt. Sustituya X por el nombre de host del servidor. Por ejemplo, wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt, wsmoamp.crt.

Comando para exportar los certificados autofirmados:

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

(ii) Copie el certificado de la ruta de acceso %CVP_HOME%\conf\security\wsm.crt de cada servidor y cámbiele el nombre a wsmX.crt según el tipo de servidor.

Paso 2. Importe certificados WSM del servidor CVP y del servidor de informes en el servidor OAMP.

(i) Copie cada certificado WSM del servidor CVP y del servidor de informes (wsmX.crt) en el directorio %CVP_HOME%\conf\security del servidor OAMP.

(ii) Importar estos certificados con el comando:

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

(iii) Reinicie el servidor.

Paso 3. Importe el certificado WSM del servidor CVP OAMP en los servidores CVP Server y Reporting.

(i) Copie el certificado WSM del servidor OAMP (wsmoampX.crt) en el directorio

%CVP_HOME%\conf\security en todos los servidores CVP y servidores de informes.

(ii) Importar los certificados con el comando:

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

(iii) Reinicie los servidores.

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

Los pasos necesarios para completar este intercambio correctamente son:

Paso 1. Exportar certificado de aplicación desde la plataforma VOS.

Paso 2. Importe el certificado de la aplicación VOS en el servidor OAMP.

Este proceso es aplicable a aplicaciones VOS como:

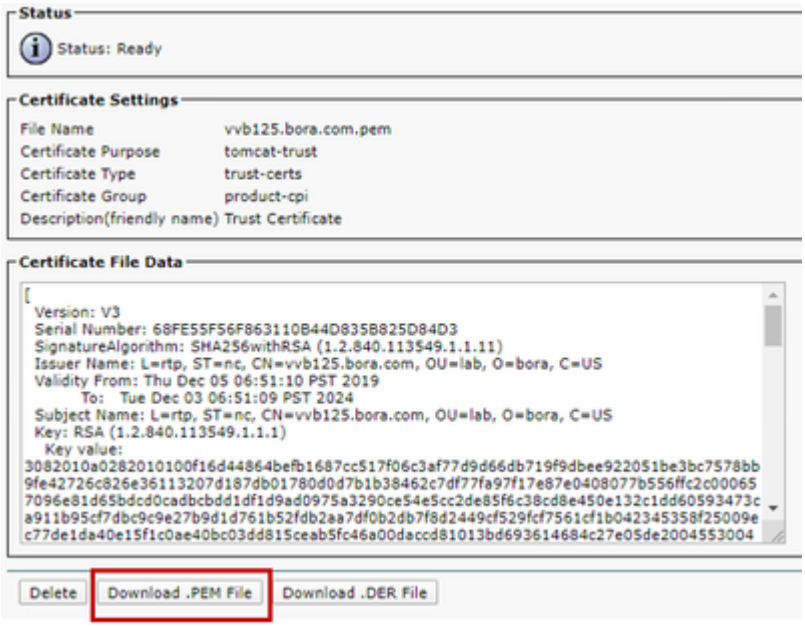
- CUCM
- VVB
- Conexión a la nube

Paso 1. Exportar certificado de aplicación desde 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 el archivo **download** .PEM para guardarlo en una carpeta temporal en el servidor OAMP.



Paso 2. Importe el certificado de la aplicación VOS en el servidor OAMP.

(i) Copie el certificado de VOS en el directorio %CVP_HOME%\conf\security del servidor OAMP.

(ii) Importar los certificados con el comando:

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

(ii) Reinicie el servidor.

Sección 3: Intercambio de certificados entre el servidor CVP y las aplicaciones de la plataforma VOS

Este es un paso opcional para proteger la comunicación SIP entre CVP y otros componentes del Contact Center. Para obtener más información, consulte la Guía de configuración de CVP: Guía de configuración de CVP - Seguridad.

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: Guía de configuración de CVP - Seguridad
- Guía de configuración de UCCE: Guía de seguridad de UCCE
- Guía de administración de PCCE: Guía de administración de PCCE
- Certificados de firma automática de PCCE 12.6: Certificados de firma automática de PCCE de Exchange
- Certificados autofirmados de PCCE 12.5: Certificado autofirmado de PCCE 12.5

- Certificado autofirmado UCCE 12.5: Certificados autofirmados UCCE 12.5
- Certificados firmados de CCE CA 12.5: certificados firmados de CCE CA 12.5
- **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).