

# Intercambiar certificados autofirmados en una solución UCCE

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Background](#)

[Procedimiento](#)

[Servidores CCE AW y servidores de aplicaciones principales CCE](#)

[Sección 1: Intercambio de certificados entre Router/Logger, PG y AW Server.](#)

[Sección 2: Intercambio de certificados entre las aplicaciones de la plataforma VOS y el servidor AW.](#)

[Servidor CVP OAMP y servidores de componentes CVP](#)

[Sección 1: Intercambio de certificados entre CVP OAMP Server y CVP Server y Reporting Servers.](#)

[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 los servidores CVVB.](#)

[CVP CallStudio WEBSERVICE Integration](#)

[Información Relacionada](#)

## Introducción

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

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

## Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCCE versión 12.5(1)
- Portal de voz del cliente (CVP) versión 12.5 (1)
- Navegador de voz virtualizado (VVB) de Cisco

## Componentes Utilizados

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

- UCCE 12.5(1)
- CVP 12.5(1)
- Cisco VVB 12.5
- Consola de operaciones de CVP (OAMP)
- CVP Nuevo OAMP (NOAMP)

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Background

En la solución UCCE, la configuración de nuevas funciones que involucra aplicaciones principales como Roggers, Gateways periféricos (PG), estaciones de trabajo administrativas (AW), Finesse, Cisco Unified Intelligent Center (CUIC), etc. se realiza a través de la página de administración de Contact Center Enterprise (CCE). Para aplicaciones de respuesta de voz interactiva (IVR) como CVP, Cisco VVB y gateways, NOAMP controla la configuración de nuevas funciones. Desde CCE 12.5(1) debido al cumplimiento de la gestión de seguridad (SRC), toda la comunicación al administrador CCE y a NOAMP se realiza estrictamente a través del protocolo HTTP seguro.

Para lograr una comunicación segura y fluida entre estas aplicaciones en un entorno de certificados autofirmado, el intercambio de estos certificados entre los servidores se convierte en una obligación. En la siguiente sección se explican en detalle los pasos necesarios para intercambiar certificados autofirmados entre:

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

## Procedimiento

### Servidores CCE AW y servidores de aplicaciones principales CCE

Estos son los componentes a partir de los cuales se exportan los certificados autofirmados y los componentes a los que se deben importar los certificados autofirmados.

**Servidores CCE AW:** Este servidor requiere certificado de:

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

**Nota:** Se necesitan certificados IIS y de marco de diagnóstico.

- 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 \ Servidor de registrador:** Este servidor requiere certificado de:

- Plataforma de Windows: Todos los servidores AW certificado IIS.

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

Sección 1: Intercambio de certificados entre Router\Logger, PG y AW Server.

Sección 2: Intercambio de certificados entre la aplicación de la plataforma VOS y el servidor AW.

### Sección 1: Intercambio de certificados entre Router\Logger, PG y AW Server.

Los pasos necesarios para completar este intercambio con éxito son:

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

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

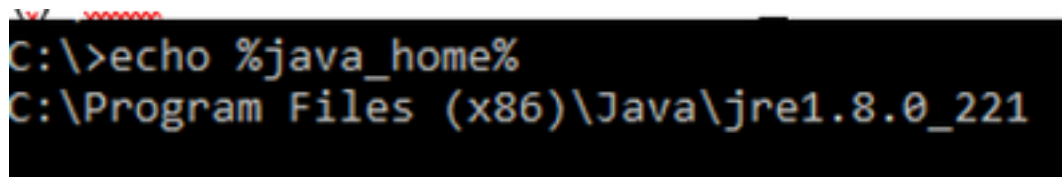
Paso 3. Importe los certificados IIS y DFP del Router\Logger, PG a los servidores AW.

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 la casa de java como administrador.

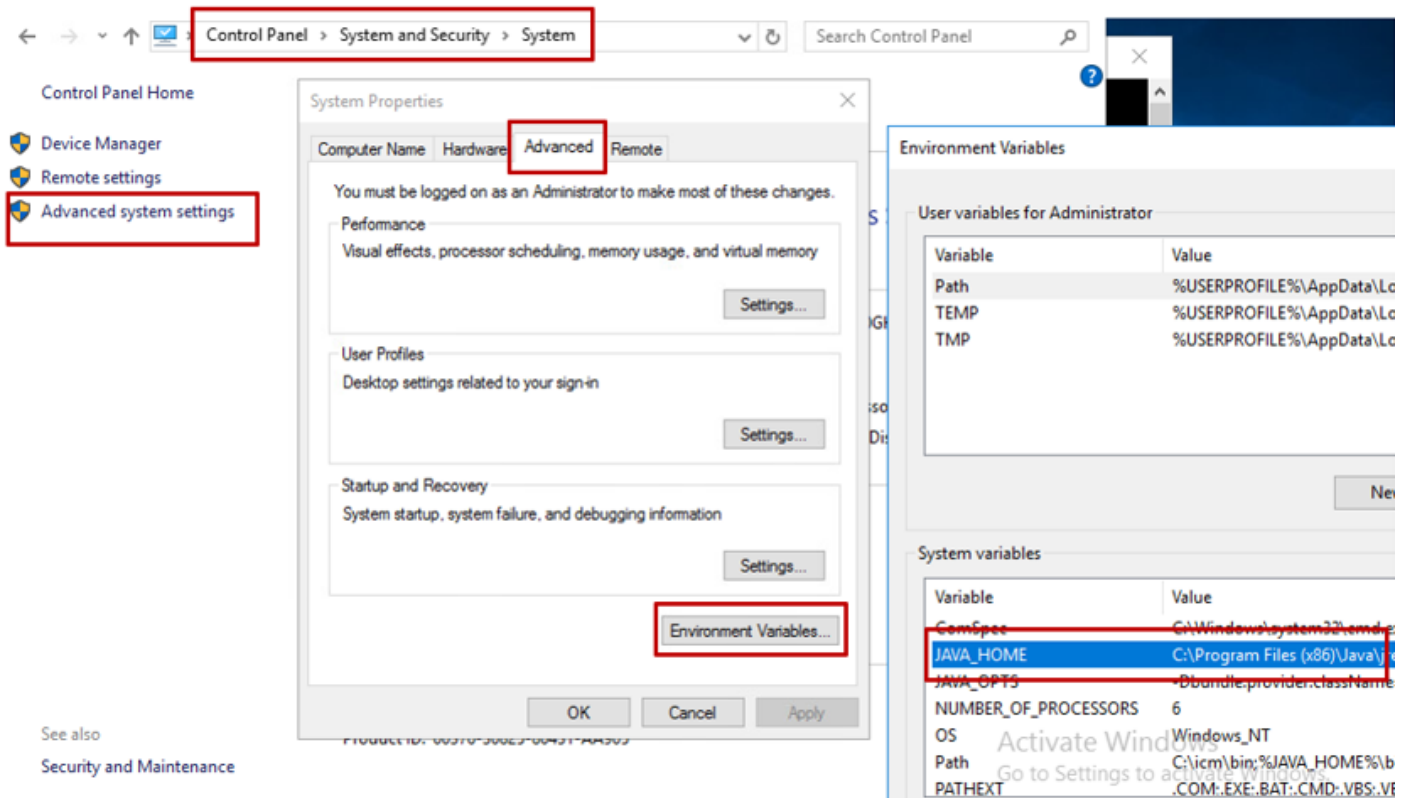
(i) Conocer la ruta de acceso a casa de java para asegurarse de dónde se aloja la herramienta de claves de java. Hay un par de maneras de encontrar el camino de casa java.

Opción 1: Comando CLI: `echo %JAVA_HOME%`



```
C:\>echo %java_home%
C:\Program Files (x86)\Java\jre1.8.0_221
```

Opción 2: Manualmente mediante 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 (obligatorio OpenJDK ES), utilice CCE\_JAVA\_HOME en lugar de JAVA\_HOME, ya que la ruta del almacén de datos ha cambiado con OpenJDK. Más información sobre la migración de OpenJDK en CCE y CVP en estos documentos: [Instalar y migrar a OpenJDK en CCE 2.5\(1\)](#) e [instalar y migrar a OpenJDK en CVP 12.5\(1\)](#).

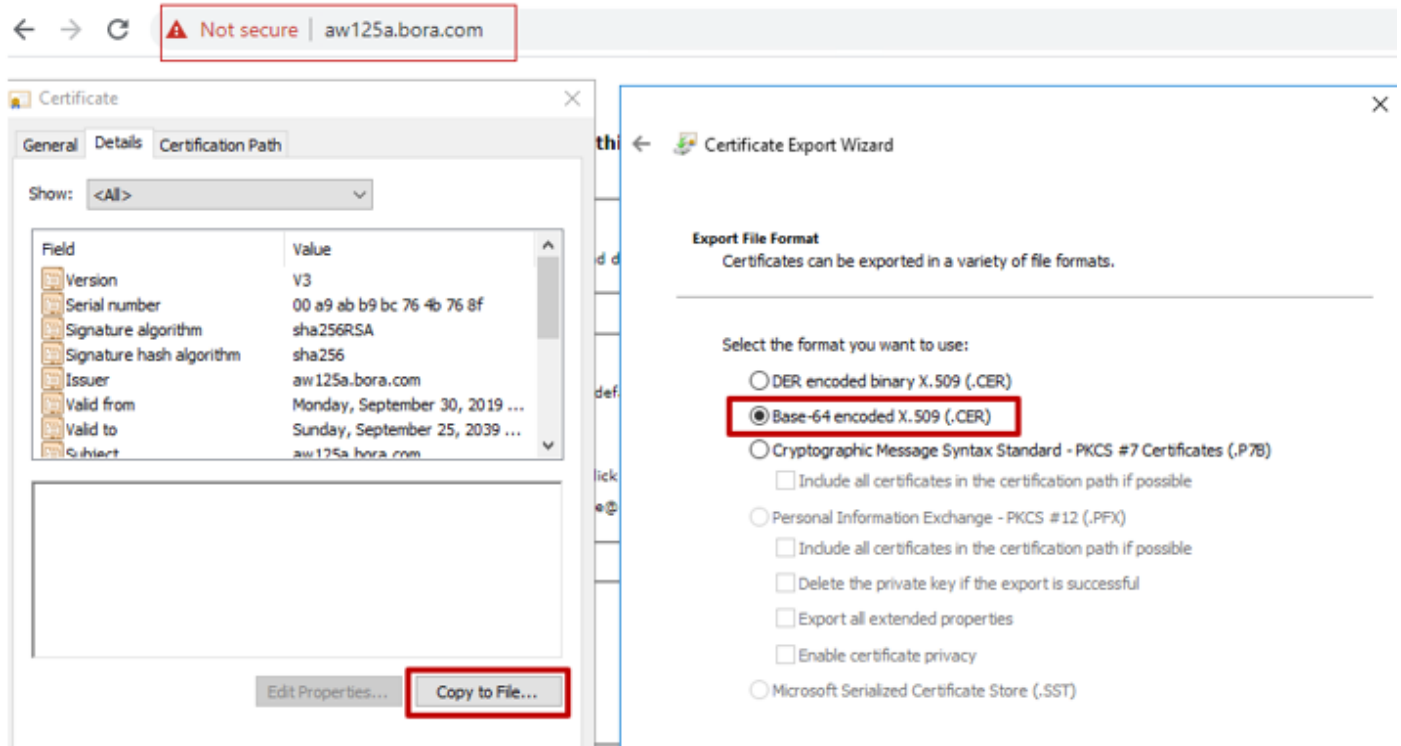
(ii) Realice una copia de seguridad del archivo **cacerts** desde la carpeta C:\Program Files (x86)\Java\jre1.8.0\_221\lib\security. Puede copiarlo en otra ubicación.

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

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

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

## CCE via Chrome Browser



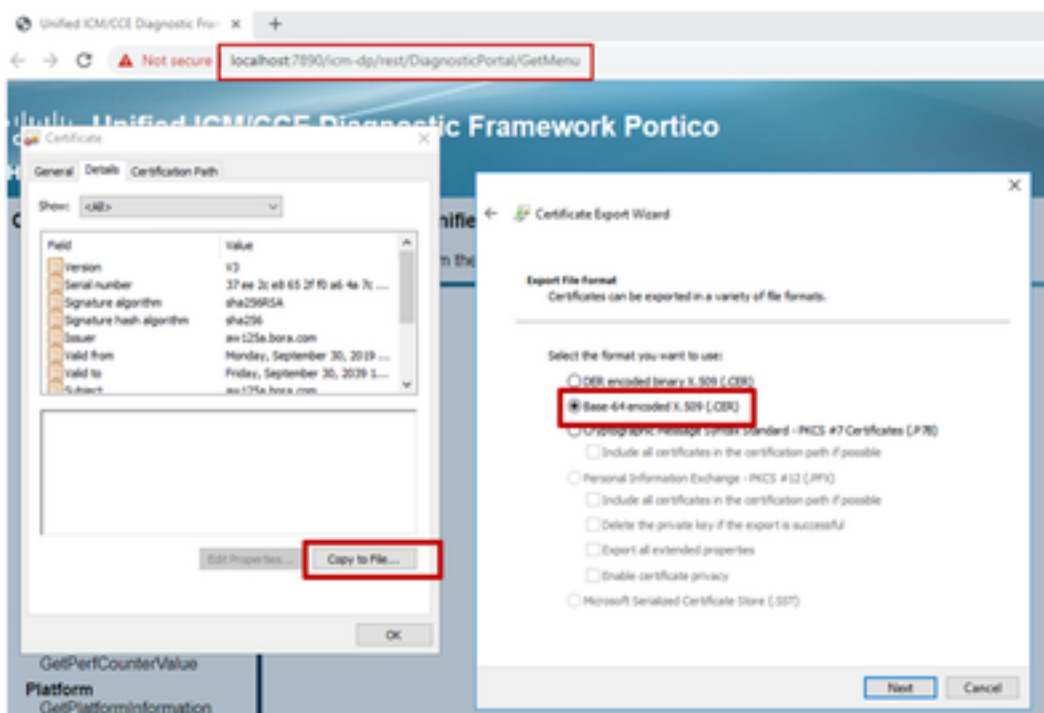
(ii) Guarde el certificado en una carpeta temporal, por ejemplo `c:\temp\certs` y asigne el nombre de cert como `ICM{svr}[ab].cer`.

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

### Paso 2. Exportar certificados Portico de marco de diagnóstico (DFP) desde servidores Router\Logger y PG.

(i) En el servidor AW, abra un navegador y navegue hasta los servidores (Router, Logger o Roggers, PG) URL de DFP: <https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion>.

## Portico via Chrome Browser



(ii) Guarde el certificado en la carpeta, ejemplo c:\temp\certs y asigne el nombre de cert como dfp{svr}{ab}.cer

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

### Paso 3. Importe el certificado IIS y DFP de Rogger, PG a los servidores AW.

Comando para importar los certificados autofirmados de IIS en el servidor AW. Ruta para ejecutar la herramienta Clave: C:\Program Archivos (x86)\Java\jre1.8.0\_221\bin:

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -storepass changeit -alias {fqdn_of_server}_IIS -file c:\temp\certs\ ICM{svr}{ab}.cer  
Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -storepass changeit -alias myrgra.domain.com_IIS -file c:\temp\certs\ICMrgra.cer
```

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

Comando para importar los certificados autofirmados de DFP a los servidores AW:

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -storepass changeit -alias {fqdn_of_server}_DFP -file c:\temp\certs\ dfp{svr}{ab}.cer  
Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -storepass changeit -alias myrgra.domain.com_DFP -file c:\temp\certs\dfprgra.cer
```

**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 los servidores Rogger:

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -storepass changeit -alias {fqdn_of_server}_IIS -file c:\temp\certs\ ICM{svr}[ab].cer  
Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -storepass changeit -alias myrgra.domain.com_IIS -file c:\temp\certs\ICMrgra.cer
```

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

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 con éxito son:

- Paso 1. Exportar certificados de servidor de aplicaciones de la plataforma VOS.
- Paso 2. Importar certificados de aplicación de plataforma VOS al servidor AW.

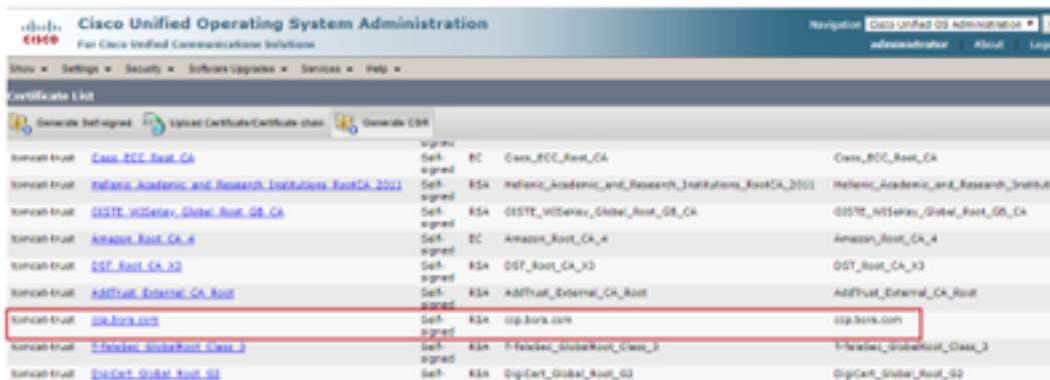
Este proceso se aplica a todas las aplicaciones VOS, como:

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

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

(i) Acceda a la página Administración del Sistema Operativo de 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 el archivo .PEM para guardarlo en una carpeta temporal en el servidor AW.

Certificate Settings	
File Name	ccp.bora.com.pem
Certificate Purpose	tomcat-trust
Certificate Type	trust-certs
Certificate Group	product-cpi
Description(friendly name)	Trust Certificate

Certificate File Data	
<pre>[ Version: V3 Serial Number: 5C35B3A89A8974719BB8586A92CF710D SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11) Issuer Name: L=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US Validity From: Mon Dec 16 10:55:22 EST 2019 To: Sat Dec 14 10:55:21 EST 2024 Subject Name: L=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US Key: RSA (1.2.840.113549.1.1.1) Key value: 3082010a0282010100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 69f9980a1246814be9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 88e0e816e64ad44c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722 f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f 520da30a39b206d213b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a</pre>	

**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 Archivos (x86)\Java\jre1.8.0\_221\bin**

Orden para importar los certificados autofirmados:

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -storepass changeit -alias {fqdn_of_vos} -file c:\temp\certs\vosapplicationX.pem
```

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

Estos son los componentes a partir de los cuales se exportan los certificados autofirmados y los componentes a los que se deben importar los certificados autofirmados.

i) **Servidor CVP OAMP:** Este servidor requiere el certificado de

- Plataforma de Windows: Certificado de Web Services Manager (WSM) de CVP Server y servidores de informes.
- Plataforma VOS: Integración de Cisco VVB para Customer Virtual Agent (CVA), servidor Cloud Connect para la integración de Webex Experience Management (WXM).

ii) **Servidores CVP:** Este servidor requiere el certificado de



- Plataforma de Windows: Certificado WSM del servidor OAMP.
- Plataforma VOS: Servidor Cloud Connect para integración WXM, servidor Cisco VVB para comunicación segura SIP y HTTP.

iii) **Servidores de informes del CVP:** Este servidor requiere el certificado de

- Plataforma de Windows: Certificado WSM del servidor OAMP.

(iv) **Servidores Cisco VVB:** Este servidor requiere certificado de

- Plataforma de Windows: VXML de servidor CVP (HTTP seguro), servidor de llamadas CVP (SIP seguro)

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

Sección 1: Intercambio de certificados entre CVP OAMP Server y CVP Server y Reporting Servers.

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 los servidores VVB.

**Sección 1: Intercambio de certificados entre CVP OAMP Server y CVP Server y Reporting Servers.**

Los pasos necesarios para completar este intercambio con éxito son:

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

Paso 2. Importar certificados WSM desde el servidor CVP y el servidor de informes al servidor OAMP.

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

**Precaución:** Antes de comenzar, debe hacer lo siguiente:

1. Obtenga la contraseña del almacén de claves. Ejecute el comando: más  
%CVP\_HOME%\conf\security.properties
2. Copie la carpeta %CVP\_HOME%\conf\security a otra carpeta.
3. Abra una ventana de comandos como Administrador para ejecutar los comandos.

**Paso 1. Exportar 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 por el nombre deseado. Puede cambiarle el nombre a wsmX.crt.

Reemplace X por un número o letra únicos. 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 -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

(ii) Copie el certificado de la trayectoria **C:\Cisco\CVP\conf\security\wsm.crt** de cada servidor y renómbrela como **wsmX.crt** según el tipo de servidor.

## **Paso 2. Importar certificados WSM desde el servidor CVP y el servidor de informes al servidor OAMP.**

(i) Copie cada certificado WSM de servidor CVP y servidor de informes (**wsmX.crt**) en el directorio **C:\Cisco\CVP\conf\security** en el servidor OAMP.

(ii) Importar estos certificados con el comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -alias {fqdn_of_cvp}_wsm -file c:\cisco\cvp\conf\security\wsmcsX.crt
```

(iii) Reinicie el servidor.

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

(i) Copie el certificado WSM del servidor OAMP (**wsmoampX.crt**) en el directorio **C:\Cisco\CVP\conf\security** en todos los servidores CVP Servers y Reporting.

(ii) Importar los certificados con el comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -alias {fqdn_of_cvp}_wsm -file c:\cisco\cvp\conf\security\wsmoampX.crt
```

(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 con éxito son:

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

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

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

(i) Acceda a la página Administración del Sistema Operativo de 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**.

tomcat trust	Self-signed	RSA	Maxim_Primary_Root_CA_..._02	Maxim_Primary_Root_CA_..._02
tomcat trust	Self-signed	EC	GlobeSign	GlobeSign
tomcat trust	Self-signed	RSA	EE_Certificator_Centre_Root_CA	EE_Certificator_Centre_Root_CA
tomcat trust	Self-signed	RSA	GlobeSign_Root_CA	GlobeSign_Root_CA
tomcat trust	Self-signed	RSA	YrCA_Root_Certification_Authority	YrCA_Root_Certification_Authority
tomcat trust	Self-signed	RSA	Business_Class_3_Root_CA	Business_Class_3_Root_CA
tomcat trust	Self-signed	RSA	Starfield_Services_Root_Certificat_Authority_..._02	Starfield_Services_Root_Certificat_Authority_..._02
tomcat trust	Self-signed	RSA	VeriSign_Class_3_Public_Primary_Certification_Authority_...	VeriSign_Class_3_Public_Primary_Certification_Authority_...
tomcat trust	Self-signed	RSA	vvb125.bora.com	vvb125.bora.com
tomcat trust	Self-signed	RSA	XKARA_Global_Certification_Authority	XKARA_Global_Certification_Authority

(iii) Seleccione el certificado y haga clic en descargar el archivo .PEM para guardarlo en una carpeta temporal en el servidor OAMP.

**Status**

Status: Ready

---

**Certificate Settings**

File Name: vvb125.bora.com.pem  
 Certificate Purpose: tomcat-trust  
 Certificate Type: trust-certs  
 Certificate Group: product-cpi  
 Description(friendly name): Trust Certificate

---

**Certificate File Data**

```
[
Version: V3
Serial Number: 68FE55F56F863110B44D8358825D84D3
Signature Algorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=rtp, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
Validity From: Thu Dec 05 06:51:10 PST 2019
To: Tue Dec 03 06:51:09 PST 2024
Subject Name: L=rtp, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100f16d44864befb1687cc517f06c3af77d9d66db719f9dbee922051be3bc7578bb
9fe42726c826e36113207d187db01780d0d7b1b38462c7df77fa97f17e87e0408077b556ffc2c00065
7096e81d65bdcd0cadbcdd1df1d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c
a911b95cf7dbc9c9e27b9d1d761b52fdb2aa7df0b2db7f8d2449cf529fcf7561cf1b042345358f25009e
c77de1da40e15f1c0ae40bc03dd815ceab5fc46a00dacc81013bd693614684c27e05de2004553004
```

Delete Download .PEM File Download .DER File

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

- (i) Copie el certificado VVBC en el directorio C:\Cisco\CVP\conf\security en el servidor OAMP.
- (ii) Importar los certificados con el comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -alias {fqdn_of_vos} -file c:\cisco\cvp\conf\security\vvb.pem
```

- (ii) Reinicie el servidor.

## Sección 3: Intercambio de certificados entre el servidor CVP y los servidores CVVB.

Este es un paso opcional para proteger la comunicación SIP y HTTP entre los servidores CVVB y CVP. Los pasos necesarios para completar este intercambio con éxito son:

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

Paso 2. Importe el certificado de aplicación del vos en los servidores CVP.

Paso 3: Exportar el servidor de llamadas y el certificado vxml de los servidores CVP.

Paso 4: Importe el servidor de llamadas y el certificado vxml en los servidores CVVB.

### Paso 1. Exportar certificado de aplicación desde la plataforma del sistema operativo.

(i) Siga las mismas escaleras que se indican en el paso 1 de la sección 2 para los servidores CVVB.

### Paso 2. Importe el certificado de aplicación de VOS en el servidor CVP.

(i) Siga los mismos pasos que se indican en el paso 2 de la Sección 2 en todos los servidores CVP.

### Paso 3: Exportar servidor de llamadas y certificado vxml de servidores CVP

(i) Exporte el servidor de llamadas y el certificado vxml de cada servidor CVP a una ubicación temporal y cambie el nombre del certificado con el nombre deseado. Puede cambiarle el nombre de callserverX.crt \ vxmlX.crt Reemplazar X por un número o una letra únicos.

Comando para exportar los certificados autofirmados:

```
Callserver certificate : %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore  
%CVP_HOME%\conf\security\.keystore -export -alias callserver_certificate -file  
%CVP_HOME%\conf\security\callserverX.crt
```

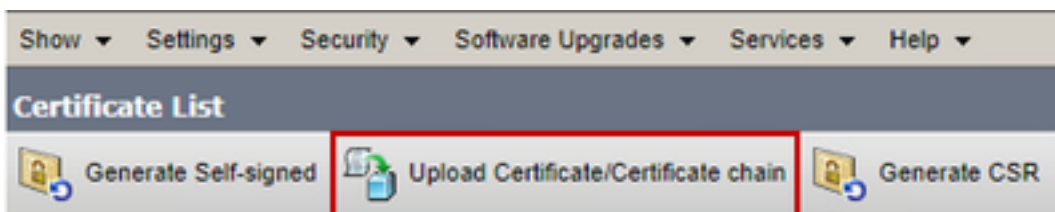
```
Vxml certificate : %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore  
%CVP_HOME%\conf\security\.keystore -export -alias vxml_certificate -file  
%CVP_HOME%\conf\security\vxmlX.crt
```

(ii) Copie el certificado de la ruta C:\Cisco\CVP\conf\security\wsm.crt de cada servidor y cámbielo como callserverX.crt \ vxmlX.crt en función del tipo de certificado.

### Paso 4: Importe el servidor de llamadas y el certificado vxml en los servidores CVVB.

(i) Acceda a la página Administración del Sistema Operativo de Cisco Unified Communications:  
<https://FQDN:8443/cmplatform>.

(ii) Navegue hasta Seguridad > Administración de certificados y seleccione opción cargar certificado/cadena de certificados.



(iii) En la cadena de carga de certificados, seleccione tomcat-trust en el campo de propósito del certificado y cargue los certificados exportados como se realiza en el paso 3.

**Upload Certificate/Certificate chain**

Upload Close

**Status**

**i** 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

Upload Close

(iv) Reinicie el servidor.

## CVP CallStudio WEBSERVICE Integration

Para obtener información detallada sobre cómo establecer una comunicación segura para elemento Web Services Element y Rest\_Client

consulte la [guía del usuario de Cisco Unified CVP VXML Server y Cisco Unified Call Studio Release 12.5\(1\) - Web Service Integration \[Cisco Unified Customer Voice Portal\] - Cisco](#)

## Información Relacionada

- Guía de configuración de CVP: [Guía de configuración de CVP - Seguridad](#)
- Guía de configuración de UCCE: [Guía de configuración de UCCE - Seguridad](#)
- Guía de administración de PCCE: [Guía de administración de PCE - Seguridad](#)
- Certificados con firma automática UCCE: [Intercambio de certificados con firma automática UCCE](#)
- Certificados con firma automática PCCE: [intercambio de certificados con firma automática PCCE](#)
- Instalación y migración a OpenJDK en CCE 12.5(1): [Migración de CCE OpenJDK](#)
- Instalación y migración a OpenJDK en CVP 12.5(1): [Migración de OpenJDK de CVP](#)

[Soporte Técnico y Documentación - Cisco Systems](#)