

Intercambio de certificados autofirmados en una solución PCCE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Background](#)

[Procedimiento](#)

[Sección 1: Intercambio de certificados entre CVP y servidores ADS](#)

[Paso 1. Exportar certificados de servidor CVP](#)

[Paso 2. Importar servidores CVP Certificado WSM al servidor ADS](#)

[Paso 3. Exportar certificado de servidor ADS](#)

[Paso 4. Importar servidor ADS a servidores CVP y servidor de informes](#)

[Sección 2: Intercambio de certificados entre aplicaciones de la plataforma VOS y servidor ADS](#)

[Paso 1. Exportar certificados de servidor de aplicaciones de la plataforma VOS.](#)

[Paso 2. Importar aplicación de plataforma VOS al servidor ADS](#)

[Sección 3: Intercambio de certificados entre los servidores Roggers, PG y ADS](#)

[Paso 1. Exportar certificado IIS de servidores Rogger y PG](#)

[Paso 2. Exportar certificado Portico de Marco de Diagnóstico \(DFP\) de servidores Rogger y PG](#)

[Paso 3. Importar certificados al servidor ADS](#)

[Sección 4: CVP CallStudio WEBSERVICE Integration](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo intercambiar certificados autofirmados entre el servidor de administración principal (ADS/AW) y otro servidor de aplicaciones en la solución Cisco Packaged Contact Center Enterprise (PCCE).

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

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- PCCE versión 12.5(1)
- Portal de voz del cliente (CVP) versión 12.5 (1)

Componentes Utilizados

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

- PCCE 12.5(1)
- CVP 12.5(1)

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 PCCE de 12.x, todos los dispositivos se controlan a través de un único panel de vidrio (SPOG) alojado en el servidor principal de AW. Debido a la conformidad con la gestión de la seguridad (SRC) en la versión 12.5(1) de PCCE, todas las comunicaciones entre SPOG y otros servidores de la solución se realizan estrictamente mediante el protocolo HTTP seguro.

Los certificados se utilizan para lograr una comunicación segura y fluida entre SPOG y los otros dispositivos. En un entorno de certificados autofirmados, el intercambio de certificados entre los servidores se convierte en un imperativo. Este intercambio de certificados también es necesario para habilitar las nuevas funciones presentes en la versión 12.5(1), como Smart Licensing, Webex Experience Management (WXM) y Customer Virtual Assistant (CVA).

Procedimiento

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 principal AW: Este servidor requiere certificado de:

- Plataforma de Windows: ICM: Router y registrador(Rogger){A/B}, gateway periférico (PG){A/B}, todos los servidores ADS y de correo electrónico y chat (ECE). Nota: Se necesitan certificados IIS y de marco de diagnóstico.CVP: Servidores CVP, servidor de informes CVP. Nota 1: Se necesita el certificado de administración de servicios web (WSM) de los servidores.Nota 2: Los certificados deben tener un nombre de dominio completo (FQDN).
- Plataforma VOS: Cloud Connect, Cisco Virtual Voice Browser (VB), Cisco Unified Call Manager (CUCM), Finesse, Cisco Unified Intelligent Center (CUIC), Live Data (LD), Identity Server (IDS) y otros servidores aplicables.

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

(ii) Router \ Servidor registrador: Este servidor requiere certificado de:

- Plataforma de Windows: certificado IIS de todos los servidores ADS.

(iii) Servidor PG de CUCM: Este servidor requiere certificado de:

- Plataforma VOS: editor de CUCM. Nota: Esto es necesario para descargar el cliente JTAPI del servidor CUCM.

(iv) Servidor CVP: Este servidor requiere el certificado de

- Plataforma Windows: certificado IIS de todos los servidores ADS
- Plataforma VOS: Servidor Cloud Connect para integración WXM, servidor VVB para

comunicación segura SIP y HTTP.

v) **Servidor de informes CVP:** Este servidor requiere certificado de:

- Plataforma Windows: certificado IIS de todos los servidores ADS

(vi) **Servidor VVB:** Este servidor requiere certificado de:

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

Los pasos necesarios para intercambiar eficazmente los certificados autofirmados de 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 CVP y servidores ADS

Los pasos necesarios para completar este intercambio con éxito son:

Paso 1. Exportar certificados WSM del servidor CVP.

Paso 2. Importar certificado WSM del servidor CVP al servidor ADS.

Paso 3. Exportar certificado de servidor ADS.

Paso 4. Importe el Servidor ADS a los Servidores CVP y al Servidor de informes CVP.

Paso 1. Exportar certificados de servidor CVP

Antes de exportar los certificados desde los servidores CVP, debe regenerar los certificados con el FQDN del servidor; de lo contrario, pocas funciones como Smart Licensing, CVA y la sincronización CVP con SPOG pueden experimentar problemas.

Precaución: Antes de comenzar, debe hacer lo siguiente:

- Obtenga la contraseña del almacén de claves. Ejecute este comando:
más %CVP_HOME%\conf\security.properties
- Copie la carpeta %CVP_HOME%\conf\security a otra carpeta.
- Abra una ventana de comandos como Administrador para ejecutar los comandos.

Nota: Puede optimizar los comandos utilizados en este documento mediante el uso del parámetro keytool -storepass. Para todos los servidores CVP, se pega la contraseña obtenida del archivo security.properties especificado. Para los servidores ADS, escriba la contraseña: **cambio**

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

i) Enumerar 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 estos certificados autofirmados: wsm_certificate , vxml_certificate , callserver_certificate . Si utiliza el parámetro -v de la herramienta de claves, 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: 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 CVP: comando 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 estos 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
```

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

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

Complete estas otras preguntas:

¿Cuál es el nombre de su unidad organizativa?

[Desconocido]: <especifique 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/provincia>

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

[Desconocido]: <especifique el 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 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 siga los mismos pasos que 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.

Nota: De forma predeterminada, los certificados autofirmados se generan durante dos años. Utilice -invalid XXXX para establecer la fecha de vencimiento cuando se regeneran los certificados; de lo contrario, los certificados son válidos durante 90 días. Para la mayoría de estos certificados, 3-5 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 12.5 los certificados 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.

(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 por el nombre deseado. Puede cambiarle el nombre a wsmcsX.crt. Reemplace "X" por un número o letra únicos. es wsmcsa.crt, wsmcsb.crt.

Comando para exportar los certificados autofirmados:

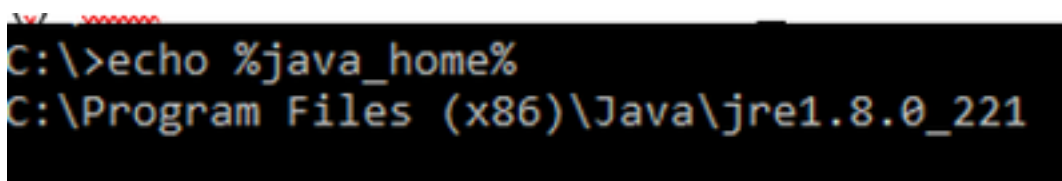
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -export -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

b) Copie el certificado de la ruta **C:\Cisco\CVP\conf\security\wsm.crt**, cámbielo a **wsmcsX.crt** y muévelo a una carpeta temporal en el servidor ADS.

Paso 2. Importar servidores CVP Certificado WSM al servidor ADS

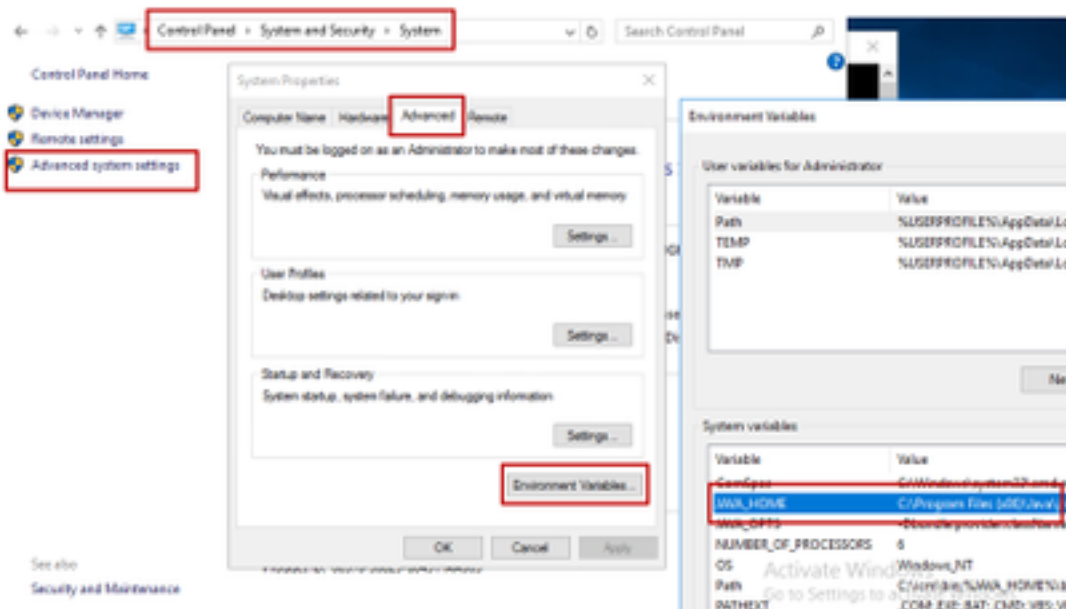
Para importar el certificado en el servidor ADS, debe utilizar la herramienta de claves que forma parte del conjunto de herramientas de Java. Hay un par de formas en las que puede encontrar la ruta de inicio de java donde se aloja esta herramienta.

(i) Comando CLI > **echo %JAVA_HOME%**



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

ii) Manualmente mediante la **configuración del sistema avanzado**, como se muestra en la imagen.



En PCCE 12.5, la ruta predeterminada es **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_cvp} -file c:\temp\certs\wsmcsX.crt
```

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

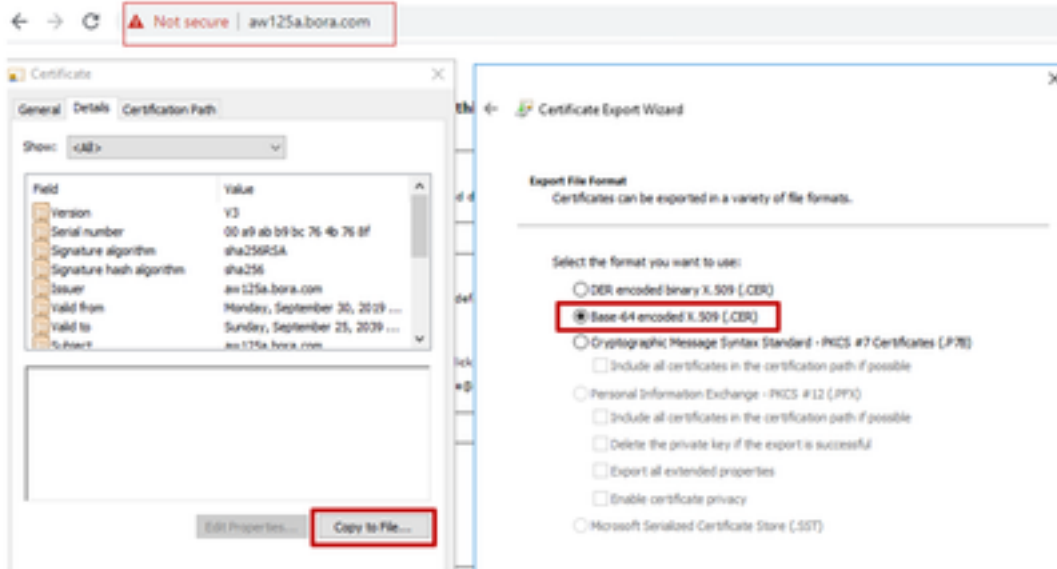
d) Reinicie el servicio Apache Tomcat en los servidores ADS.

Paso 3. Exportar certificado de servidor ADS

Para el servidor de informes CVP, debe exportar el certificado ADS e importarlo al servidor de informes. Éstos son los pasos:

- (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 nombre el certificado como **ADS{svr}[ab].cer**

CCE via Chrome Browser



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

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

(i) Copie el certificado a los servidores CVP y al servidor de informes CVP en el directorio **C:\Cisco\CVP\conf\security**.

(ii) Importar el certificado a los servidores CVP y al 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\ICM{svr}[ab].cer
```

Realice los mismos pasos para otros servidores ADS.

iii) Reiniciar los servidores CVP y el servidor de informes

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

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 ADS.

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

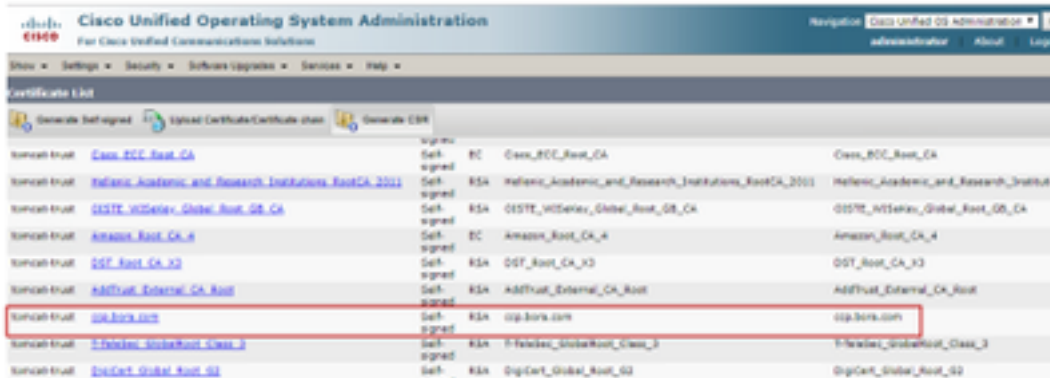
- CUCM
- VVB
- Finesse
- CUIC \ LD \ IDS
- Conexión a la nube

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

(i) Acceda a la página Administración del Sistema Operativo de Cisco Unified Communications:

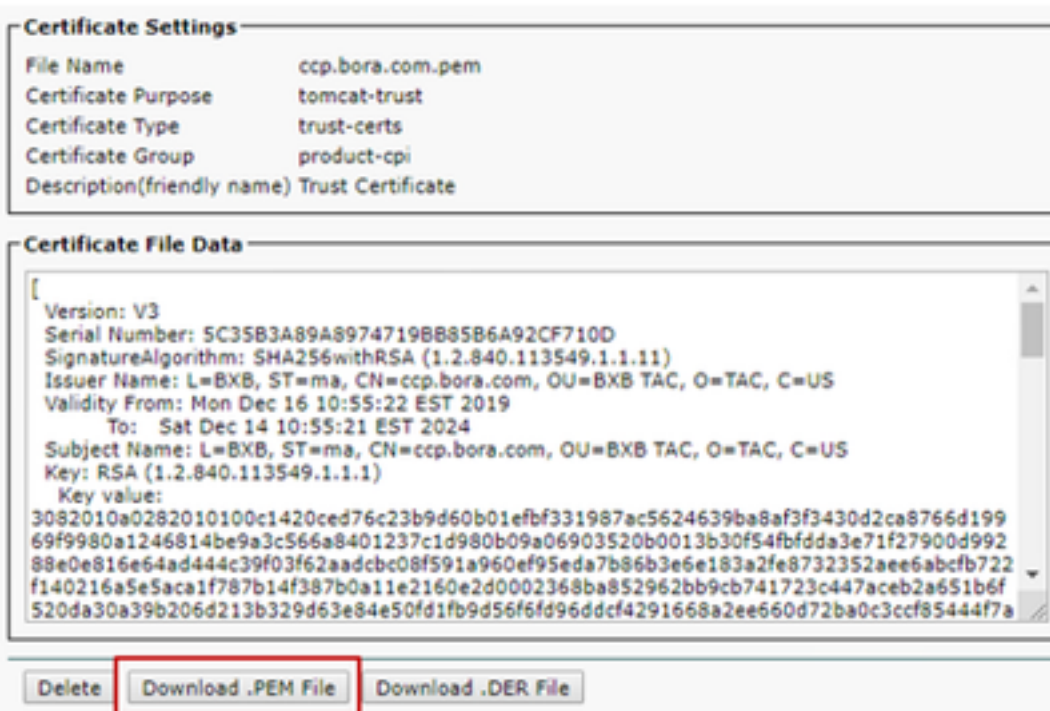
<https://FQDN:8443/cmplatform>

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



tomcat-trust	Case_ECC_Root_CA	Self-signed	EC	Case_ECC_Root_CA	Case_ECC_Root_CA
tomcat-trust	Hellenic_Academic_and_Research_Institutions_RootCA_2011	Self-signed	RSA	Hellenic_Academic_and_Research_Institutions_RootCA_2011	Hellenic_Academic_and_Research_Institutions
tomcat-trust	OSTE_WISetec_Global_Root_GB_CA	Self-signed	RSA	OSTE_WISetec_Global_Root_GB_CA	OSTE_WISetec_Global_Root_GB_CA
tomcat-trust	Amazon_Root_CA_4	Self-signed	EC	Amazon_Root_CA_4	Amazon_Root_CA_4
tomcat-trust	DST_Root_CA_X3	Self-signed	RSA	DST_Root_CA_X3	DST_Root_CA_X3
tomcat-trust	AddTrust_Eternal_CA_Root	Self-signed	RSA	AddTrust_Eternal_CA_Root	AddTrust_Eternal_CA_Root
tomcat-trust	ccp.bora.com	Self-signed	RSA	ccp.bora.com	ccp.bora.com
tomcat-trust	T-TeleSec_GlobalRoot_Class_3	Self-signed	RSA	T-TeleSec_GlobalRoot_Class_3	T-TeleSec_GlobalRoot_Class_3
tomcat-trust	OpCert_Global_Root_G2	Self-signed	RSA	OpCert_Global_Root_G2	OpCert_Global_Root_G2

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



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

```
[
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:
3082010a0282010100c1420ced76c23b9d60b01efbf331967ac5624639ba8af3f3430d2ca8766d199
69f9980a1246814be9a3c566a8401237c1d980b09a06903520b0013b30f54bfd3e71f27900d992
88e0e816e64ad444c39f03f62aadcb08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722
f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f
520da30a39b206d213b329d63e84e50fd1fb9d56f6d96ddcf4291668a2ee660d72ba0c3ccf85444f7a
]
```

Buttons: Delete, Download .PEM File, Download .DER File

Nota: Realice los mismos pasos para el suscriptor.

Paso 2. Importar aplicación de plataforma VOS al servidor ADS

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.cer
```

Reinicie el servicio Apache Tomcat en los servidores ADS.

Nota: Realice la misma tarea en otros servidores ADS

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

Los pasos necesarios para completar este intercambio con éxito son:

Paso 1: Exportar certificado IIS de servidores Rogger y PG

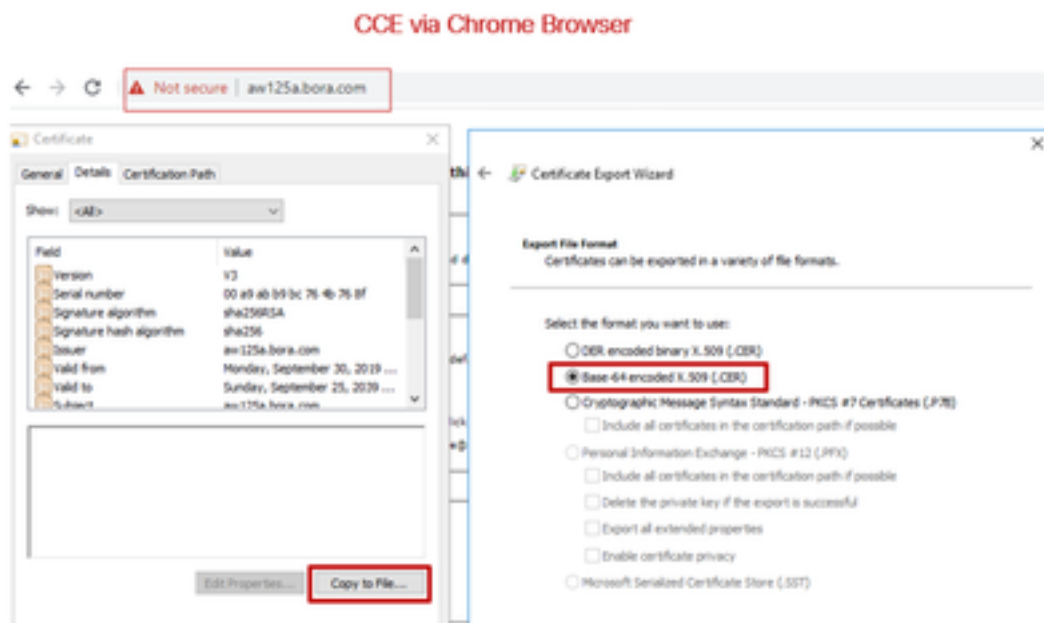
Paso 2: Exportar certificado Portico de Marco de Diagnóstico (DFP) de servidores Rogger y PG

Paso 3: Importar certificados a servidores ADS

Paso 1. Exportar certificado IIS de servidores Rogger y PG

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

(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).

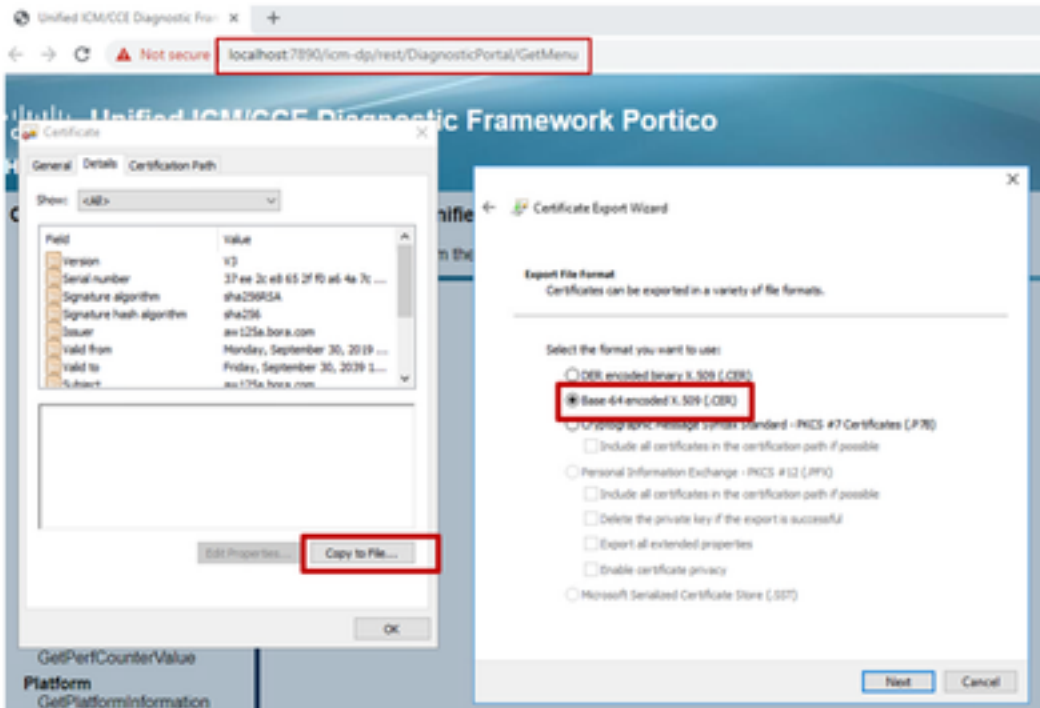
Paso 2. Exportar certificado Portico de Marco de Diagnóstico (DFP) de servidores Rogger y PG

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

(ii) Guarde el certificado en la carpeta, ejemplo `c:\temp\certs` y asigne el nombre de cert como

dfp{svr}{ab}.cer

Portico via Chrome Browser



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

Paso 3. Importar certificados al servidor ADS

Comando para importar los certificados autofirmados de IIS en el servidor ADS. 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 ADS.

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

```
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 ADS.

Reinicie el servicio Apache Tomcat en los servidores ADS.

Sección 4: 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](#)
- 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](#)