Certificados autofirmados de Exchange en una solución UCCE 12.6

Contenido

Introducción **Prerequisites Requirements Componentes Utilizados** Antecedentes Procedimiento Servidores CCE AW y servidores de aplicaciones de núcleo CCE Sección 1: Intercambio de certificados entre router\registrador, PG y servidor AW 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 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 Integración del servicio web de CVP CallStudio Información Relacionada

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 la solución de UCCE de las nuevas funciones que implican las aplicaciones principales, como Roggers, Peripheral Gateways (PG), Admin Workstations (AW)/Administration Data Server (ADS), Finesse, Cisco Unified Intelligence Center (CUIC), etc., se realiza 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}, puerta de enlace periférica (PG){A/B} y todos los AW/ADS.

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

• Plataforma VOS: 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. Exporte certificados IIS desde Router\Logger, PG y todos los servidores AW.

Paso 2. Exporte certificados DFP desde Router\Logger, PG y todos los servidores AW.

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

Paso 4. Importe el certificado IIS a Router\Logger y PG desde servidores AW.

Precaución: antes de comenzar, debe realizar una copia de seguridad del almacén de claves y abrir un símbolo del sistema 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

| | Panel > System and Security > System | | |
|---|--|--|--|
| Control Panel Home | System Properties | < | |
| Device Manager | Computer Name Hardware Advanced Remote | Environment Variables | |
| Remote settings Advanced system settings | You must be logged on as an Administrator to make most of these changes. Performance | User variables for Administrate | or |
| | Haue enects, processor acreating, menny dage, and menny | Variable | Value |
| | Settings | Path | C:\Users\Administrator\AppData\Lo |
| | Liner Desiline | TEMP | C:\Users\Administrator\AppData\Lo |
| | Desktop settings related to your sign-in | TMP | C:\Users\Administrator\AppData\Lo |
| | Startup and Recovery | | |
| | System startup, system rature, and debugging intomation | | |
| | System stanup, system raiure, and deougging mormation | System variables | |
| | System stanup, system nature, and deodyging momaton Settings | System variables Variable | Value |
| | System stanup, system nature, and deodyging momaton Settings | System variables Variable CCE_JAVA_HOME | Value C:\Program Files (x86)\OpenJDK\jre |
| | System stanup, system nature, and deodyging momaton Settings | System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_Protilem | Value C:\Program Files (x86)\OpenJDK\jre EnableV2Profiler |
| | System standp, system haure, and deodyging momadon Settings Environment Variables OK Cancel Apply | System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_Profiler ComSpec | Value C:\Program Files (x86)\OpenJDK\jre C: EnableV2Profiler C:\Windows\system32\cmd.exe |
| | System standp, system naure, and deodyging momation Settings Environment Variables OK Cancel Apply | System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_Protiler ComSpec COR_ENABLE_PROFILING COR_PROFILER | Value C:\Program Files (x86)\OpenJDK\jre C: EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler |
| | System standp, system haure, and deodyging momaton Settings Environment Variables OK Cancel Apply | System variables Variable CCE_JAVA_HOME COMPLUS_ProfAPI_Profiler ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI | Value C:\Program Files (x86)\OpenJDK\jre EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 |
| | System standp, system naure, and deodyging momaton Settings Environment Variables OK Cancel Apply | System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_Profiler ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER | Value C:\Program Files (x86)\OpenJDK\jre C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 AooDvnamics.AgentProfiler |
| | System standp, system naure, and deodyging momadon Settings Environment Variables OK Cancel Apply | System variables Variable CCE_JAVA_HOME COMPLUS_ProfAPI_Profiler ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER | Value C:\Program Files (x86)\OpenJDK\jre C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 AppDvnamics.AgentProfiler |
| | System standp, system naure, and deodyging monitation Environment Variables OK Cancel Apply | System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_Protilen ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER | Value C:\Program Files (x86)\OpenJDK\jre C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 AooDvnamics.AgentProfiler |
| | OK Cancel Apply | System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_Protilen ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER | Value C:\Program Files (x86)\OpenJDK\jre EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 AooDynamics.AgentProfiler |
| | System standp, system naure, and deodyging momadon Environment Variables OK Cancel Apply | System variables Variable CCE_JAVA_HOME COMPLUS_ProfAPI_Profiler ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER | Value C:\Program Files (x86)\OpenJDK\jre C: |
| See also | System standp, system naute, and deodyging momadon Settings Environment Variables OK Cancel Apply | System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_Protilen ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER | Value C:\Program Files (x86)\OpenJDK\jre C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 AppDvnamics.AgentProfiler |

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

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}.

| General Details Certification Path | | 🗧 🌽 Certificate Export Wizard |
|---|--|---|
| Show: <all> Field Version Serial number Signature algorithm Signature hash algorithm Issuer Valid from Valid to Schoort</all> | Value V3 0091088279797a0660 sha256RSA sha256 UCCE-AW.ccwebex.com Tuesday, February 21, 2023 4 Monday, February 16, 2043 4 | Export File Format Certificates can be exported in a variety of Select the format you want to use: O DER encoded binary X.509 (.CER) Base-64 encoded X.509 (.CER) O Cryptographic Message Syntax Sta |
| E | dit Properties Copy to File OK | Include all certificates in the cer Personal Information Exchange - Pi Include all certificates in the cer Delete the private key if the ex Export all extended properties Enable certificate privacy Microsoft Serialized Certificate Stor |

(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. Exporte certificados DFP desde Router\Logger, PG y todos los servidores AW.

(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. Importe certificados IIS y DFP de Router\Logger, PG y AW a servidores AW.

Comando para importar los certificados autofirmados de IIS en el servidor AW. Ruta de acceso para ejecutar la herramienta Clave: %CCE_JAVA_HOME%\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}_DFF 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 a Router\Logger y PG desde servidores AW.

Comando para importar los certificados autofirmados de AW IIS en los servidores Router\Logger y PG:

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

Reinicie el servicio Apache Tomcat en los servidores Router\Logger y PG.

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
- $CUIC \setminus LD \setminus IDS$
- 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: <u>https://FQDN:8443/cmplatform</u>.

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

| educity Cisco Unified Operating System Admit | nistrat | ion | | administrator About Logo |
|--|---------|-----|--|---|
| Certificate List | | | | |
| 🔒 Generale Self-agenet 🐴 Upical Catholes/Cathole chain 🔒 Generale | CSR | | | |
| turnest-trust Case ECC Rest CA | Sal- | 60 | Com, RCC, And, CA | Coox_BCC_Asot_GA |
| toweshing the state of the second state of the | Saf- | 854 | Nelenic, Academic, and Jasearch, Institutions, RootCA, 202 | Mellenic, Academic, and Jeaserch, Institution |
| turnest-trust 00072 millerlay disket Aust 08 CA | Salf- | 854 | 01578_W15ekey_Globel_Rook_GB_CA | 00178_WDierlay_Global_Root_68_CA |
| torical-trust Amazon Root CA. 4 | Self- | ec. | Amazon_Root_CA_4 | Amazon, Root, CA, 4 |
| torical-built 017 Red CA x3 | Self- | 854 | DST_RevE_CA_X3 | DDT_RHH_CA_X3 |
| toward-base Addition Edward Ch. Red | Self- | 854 | AddTrust_External_CA_Root | AddTrust_External_CA_Root |
| turneat-trust coultana.com | Deff- | 834 | op.how.com | ophora.com |
| towat-but 12bits. Scialing Con. 3 | Self- | 434 | Melec_Gobalkost_Cass_3 | T-frieler_GobeRoot_Case_3 |
| tomoshimut <u>DisiCert Global Root G2</u> | Self | 854 | DigiCert_Global_Root_G2 | DigiCert_Global_Root_G2 |

(iii) Seleccione el **certificado** y haga clic en el archivo **download** .PEM para guardarlo en una carpeta temporal en el servidor AW.

| - Certifica | te Settings | | _ |
|---|--|--|--------|
| File Nam | e | ccp.bora.com.pem | |
| Certificat | te Purpose | tomcat-trust | |
| Certificat | te Type | trust-certs | |
| Certificat | te Group | product-cpi | |
| Descripti | on(friendly name) | Trust Certificate | |
| Certifica | te File Data | | _ |
| Version Serial I Signatu Issuer Validity Subject Key: R | n: V3 Number: SC3SB3A ureAlgorithm: SHA Name: L=BXB, ST / From: Mon Dec 1 To: Sat Dec 14 10 t Name: L=BXB, S SA (1.2.840.11354 alue: | 89A8974719BB85B6A92CF710D 256withRSA (1.2.840.113549.1.1.11) =ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 6 10:55:22 EST 2019 0:55:21 EST 2024 T=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 19.1.1.1) | |
| 3082010 69f9980 88e0e81 f140216 520da30 | 0a0282010100c14 a1246814be9a3c5 l6e64ad444c39f03 a5e5aca1f787b14f 0a39b206d213b32 | 20ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 66s8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722 387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f 9d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a | - |
| 88e0e81 f140216 520da30 Delete | 6e64ad444c39f03 a5e5aca1f787b14f 0a39b206d213b32 | f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb72 387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6 9d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7 File Download .DER File | 2 f |

Nota: Realice los mismos pasos para el suscriptor.

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

Ruta para ejecutar la herramienta Clave: %CCE_JAVA_HOME%\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 -keystop

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) del servidor CVP y los servidores de informes.
- 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.

(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: 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 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 los 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 servidores CVP y servidores de informes.

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**.

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 -a

(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 -a

(iii) Reinicie el servidor.

Paso 3. Importe el certificado WSM del servidor CVP OAMP en servidores CVP y servidores de informes.

(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. Exporte el 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. Exporte el certificado de aplicación desde la plataforma VOS.

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

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

| Certificate L | | | | | | | |
|---------------|--|-----------------|-----|---|---|--|--|
| 🚯 Caranda | lef egyest 🖓 tiphas Centrale Centrale Centrale Cent | | | | | | |
| ternal-trust | theater Primary, Real, CA - 60 | Safe. | 854 | Paulo, Primary, Rod, 54, -, 63 | theate_himery_Root_CA60 | | |
| tomost-trust | Salation | Saf- | 80 | GistalSign | GubeSign | | |
| ternal-trust | EE Certification Centre Root CA | Sal- | 854 | EE_Certification_Certine_Root_CA | BE_Certification_Centre_Root_CA | | |
| tomost-trust | Sistadies Aut. Ch | Salt- signed | 854 | GiobalSign_Root_CA | GobelSign_Root_CA | | |
| tomost-trust | THEA And Catification Authority | Saf- | RSA | TWCA_Root_Certification_Authority | TitCA_Root_Certification_Authority | | |
| tempet-trust | Barrana Casa 3 Root Ch | Sall- | 854 | Byypens, Cens, J., Root, CA | Ropes, Ces, J., Rot, G | | |
| formal trust | Barfaill Services Aust. Certificate Authority - 62 | Saf- | RSA | Darfeld_Services_Root_Certificate_Authority52 | Starfield_Services_Root_Certificate_Authority62 | | |
| tempet-trust | VerSier, Case 3. Addit Avinary, Cethfodier, Authority, J | Self- | 854 | terdige, Case, 3, Aubic, Primary, Cartification, Authority, | VerlSigh, Dass, 3, Public, Primary, Certification, Authority, | | |
| tomost-trust | while how on | Self- signed | 854 | INTER Formation | rub125.bors.com | | |
| tomost-trust | Stana Didal Calification Autority | Dail- | 854 | Rang_Dobal_DetRoton_Authority | Xiang_Guba_Cartification_Authority | | |

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

| Status | |
|---|---|
| i Status: Ready | |
| Certificate Settings- | |
| File Name | vvb125.bora.com.pem |
| Certificate Purpose | tomcat-trust |
| Certificate Type | trust-certs |
| Certificate Group | product-cpi |
| Description(friendly nat | me) Trust Certificate |
| [| A |
| Version: V3 | |
| Serial Number: 68FE | 55F56F863110B44D835B825D84D3 |
| Issuer Name: L=rtp. | ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US |
| Validity From: Thu De | ec 05 06:51:10 PST 2019 |
| To: Tue Dec 0 | 3 06:51:09 PST 2024 |
| Subject Name: L=rtp Key: RSA (1.2.840.11 | , ST=nc, CN=VVD125.bora.com, OU=Iab, O=bora, C=US 13549.1.1.1) |
| Key value: | |
| 3082010a0282010100 | f16d44864befb1687cc517f06c3af77d9d66db719f9dbee922051be3bc7578bb |
| 9fe42726c826e361132 7096e81d65bdcd0cad | 0/018/000178000075a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c |
| a911b95cf7dbc9c9e27 | b9d1d761b52fdb2aa7df0b2db7f8d2449cf529fcf7561cf1b042345358f25009e |
| c77de1da40e15f1c0ae | 40bc03dd815ceab5fc46a00daccd81013bd693614684c27e05de2004553004 |
| | |
| Delete Download | PEM File Download .DER File |
| | |

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: <u>Guía de configuración de</u> <u>CVP - Seguridad</u>.

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 <u>Guía del usuario de Cisco Unified CVP VXML Server y Cisco Unified Call Studio Release</u> 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
- <u>Certificados autofirmados de Exchange PCCE PCCE 12.5</u>
- <u>Certificados autofirmados de Exchange UCCE: UCCE 12.5</u>
- <u>Certificados autofirmados de Exchange PCCE PCCE 12.6</u>

- 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).