Administrar certificado de componentes PCCE para SPOG

Contenido

Introducción

Este documento describe cómo intercambiar los certificados SSL autofirmados de la estación de trabajo de administración (AW) en el portal de voz del cliente (CVP), Finesse, Cisco Enterprise Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (IDS) y Virtualized Voice Browser (VB) para Package Contact Center Enterprise (PCCE) Single Pane of Glass (SPOG).

Colaborado por Nagarajan Paramasivam y Robert Rogier, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Empresas de Contact Center empaquetadas/unificadas (PCCE/UCCE)
- Plataforma VOS
- Gestión de certificados

- Almacén de claves de certificado

Componentes Utilizados

La información de este documento se basa en estos componentes:

- Estación de trabajo de administración (CCEADMIN/SPOG)
- CVP
- Finesse
- CUIC, IDS
- VVB
- CEPE de Cisco

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.

Antecedentes

Se recomienda que haya leído y entendido la Guía de administración y configuración de PCCE, específicamente el apéndice de referencia al final que cubre la configuración y configuración del certificado. Guía de configuración y administración de PCCE

Nueva interfaz de usuario - SPOG

Packaged CCE 12.0 tiene una nueva interfaz de usuario que se ajusta a otras aplicaciones del centro de contacto. La interfaz de usuario permite configurar la solución a través de una aplicación. Inicie sesión en el nuevo Unified CCE Administration en https://<IP Address>/cceadmin. <IP Address> es la dirección del Lado A o B Unified CCE AW o del HDS externo opcional.

En esta versión, la interfaz de administración de Unified CCE le permite configurar lo siguiente:

- Campañas
- Devolución de llamada por cortesía
- Grupos de servidores SIP
- Transferencias de archivos: La transferencia de archivos solo es posible a través de AW principal (AW del lado A en la implementación de agentes en 2000 y AW configurado en implementaciones de agentes en 4000 y agentes en 12000).
- Patrones de enrutamiento: El modelo de número marcado en Unified CVP Operations Console se denomina ahora Patrón de enrutamiento en Unified CCE Administration.
- Ubicaciones: En Unified CCE Administration, el código de enrutamiento es ahora el prefijo de ubicación en lugar del ID de sitio.
- Configuración del dispositivo: Unified CCE Administration permite configurar los siguientes dispositivos: Servidor CVP, CVP Reporting Server, VVB, Finesse, Identity Service (configuración de inicio de sesión único).
- Recursos del equipo: Unified CCE Administration permite definir y asociar los siguientes recursos a los equipos de agentes: Diseño de las variables de llamada, Diseño del escritorio, Listas telefónicas, Flujos de trabajo, Motivos (No preparado, Cerrar sesión, Cierre de sesión).
- Correo electrónico y chat

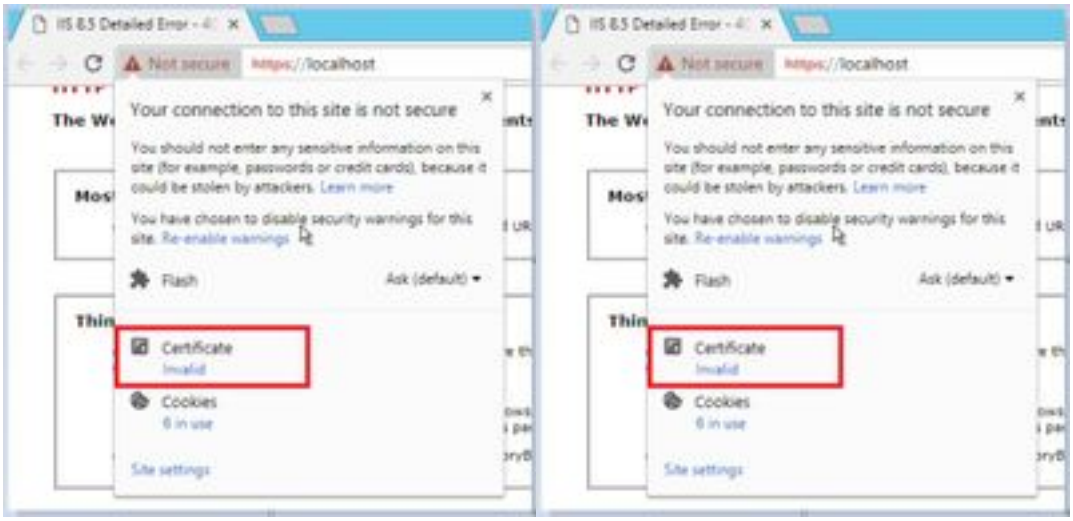
Antes de intentar gestionar el sistema a través de SPOG, es necesario intercambiar los

certificados SSL entre el portal de voz del cliente (CVP), Finesse, Cisco Enterprice Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (IDS) y Virtual Voice Browser (VB) y Admin Workstation (AW) para establecer una comunicación de confianza.

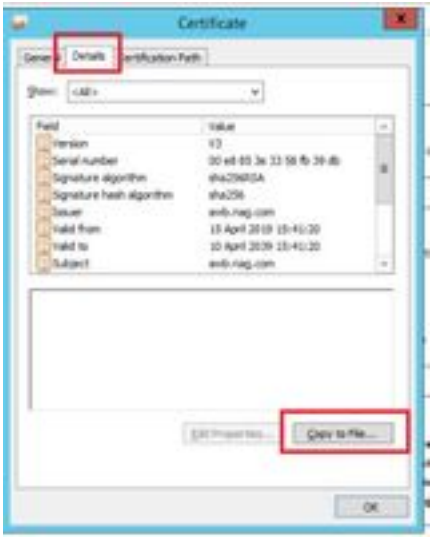
Exportación de certificado SSL

Estación de trabajo de administración (AW)

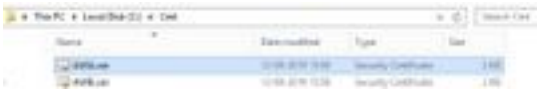
Paso 1. Acceda a la URL https://localhost en el servidor AW y descargue los certificados SSL del servidor.



Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

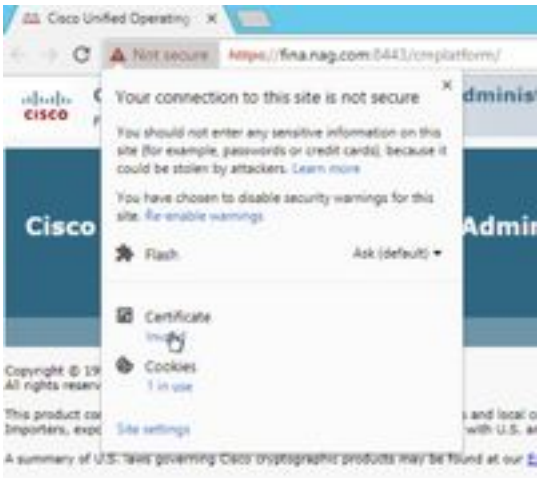


Paso 3.Seleccione Base-64 codificada X.509 (CER) y guarde el certificado en el almacenamiento local.



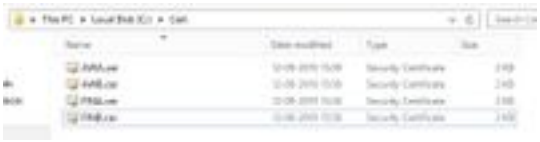
Finesse

Paso 1. Acceda a https://Finesseserver:8443/cmplatform y descargue el certificado tomcat.



Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

Paso 3. Seleccione Base-64 codificado X.509 (CER) y guarde el certificado en el almacenamiento local.



CEPE de Cisco

Paso 1. Acceda a https://ECEWebServer y descargue el certificado SSL del servidor.

Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

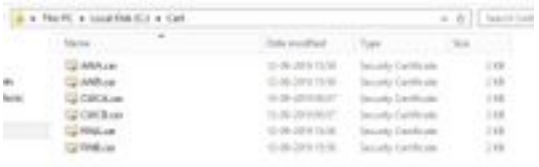
Paso 3. Seleccione Base-64 codificado X.509 (CER) y guarde el certificado en el almacenamiento local.

CUIC

Paso 1. Acceda a https://CUICServer:8443/cmplatform y descargue el certificado tomcat.

Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

Paso 3. Seleccione Base-64 codificado X.509 (CER) y guarde el certificado en el almacenamiento local.

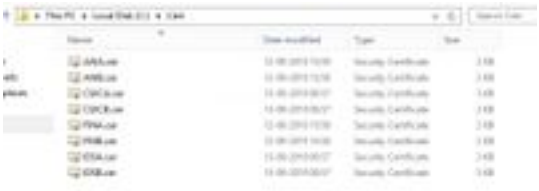


IDS de Cisco

Paso 1. Acceda a https://IDSServer:8553/idsadmin/ y descargue el certificado tomcat.

Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

Paso 3. Seleccione Base-64 codificado X.509 (CER) y guarde el certificado en el almacenamiento local.

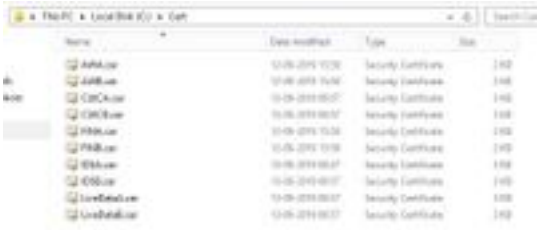


LiveData

Paso 1. Acceda a https://LiveDataServer:8444/cuic/gadget/LiveData/ y descargue el certificado tomcat.

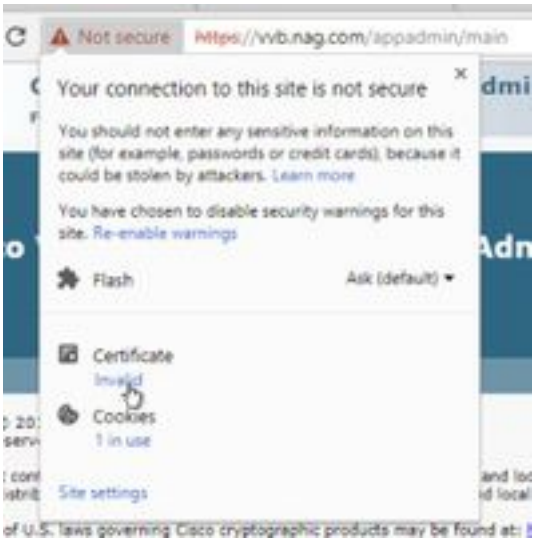
Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

Paso 3. Seleccione Base-64 codificado X.509 (CER) y guarde el certificado en el almacenamiento local.



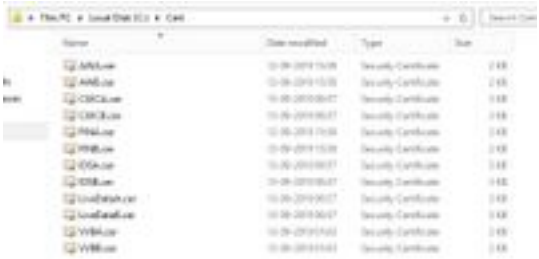
VVB

Paso 1. Acceda a https://VVBServer/appadmin/main y descargue el certificado tomcat.



Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

Paso 3. Seleccione Base-64 codificado X.509 (CER) y guarde el certificado en el almacenamiento local.



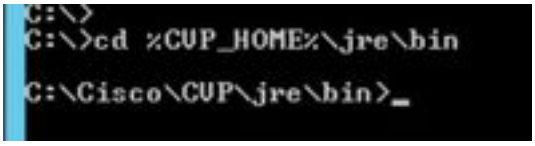
Importación de certificado SSL al almacén de claves

Servidor de llamadas y servidor de informes CVP

Paso 1. Inicie sesión en el servidor CVP y copie los certificados de administrador de AW CCE en el **C:\cisco\cvp\conf\security**.

Paso 2. Navegue hasta **%CVP_HOME%\conf** y abra security.properties para copiar la contraseña del almacén de claves.

Paso 3. Abra el símbolo del sistema como administrador y ejecute el comando **cd %CVP_HOME%\jre\bin**.



Paso 4. Utilice este comando para importar los certificados AW al servidor CVP.

keytool -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias awa.nag.com -archivo C:\Cisco\CVP\conf\security\AWA.cer

Paso 5. En el mensaje de contraseña, pegue la contraseña copiada de security.properties.

Paso 6. Escriba **yes** para confiar en el certificado y asegurarse de que obtiene el resultado **Se agregó el certificado al almacén de claves.**

Paso 7. Se le solicita una advertencia junto con la importación correcta. Esto se debe al formato propietario Keystore, puede ignorarlo.

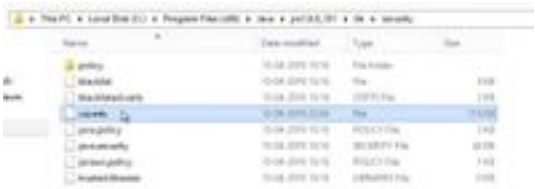
Advertencia:

El almacén de claves JCEKS utiliza un formato propietario. Se recomienda migrar a PKCS12, que es un formato estándar del sector utilizando "keytool -importkeystore -srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore -deststoretype pkcs12".

Estación de trabajo de administración

Paso 1. Inicie sesión en el servidor AW y abra el símbolo del sistema como administrador.

Paso 2. Vaya a C:\Program Files(x86)\Java\jre1.8.0_181\lib\security and ensure the cacerts file exist.



Paso 3. Escriba el comando **cd %JAVA_HOME%** e ingrese.

Paso 4. Utilice este comando para importar los certificados Finesse al servidor AW.

keytool -import -file C:\Users\Administrator.NAG\Downloads\Cert\FINA.cer -alias fina.nag.com-

keystore.\lib\security\cacerts

Paso 5. La primera vez que utilice esta herramienta de claves, utilice el **cambio de** contraseña para cambiar la contraseña de un almacén de certificados.

Paso 6. Introduzca una nueva contraseña para el almacén de claves y vuelva a introducirla para confirmar la contraseña.

Paso 7. Escriba **yes** para confiar en el certificado y asegurarse de que obtiene el resultado **El certificado fue agregado al almacén de claves.**

Nota: Los pasos 1 a 7 deben repetirse con todos los demás nodos Finesse y con todos los nodos CUIC

Paso 8. Si la contraseña del almacén de claves se ha introducido incorrectamente o ha realizado los pasos sin restablecer, se espera que obtenga esta excepción.

¿Confía en este certificado? [no]: sí

El certificado se agregó al almacén de claves

error de la herramienta clave: java.io.FileNotFoundException: .\lib\security\cacerts (El sistema no encuentra la ruta especificada)

Introduzca la contraseña del almacén de claves:
error de la herramienta clave: java.io.IOException: El almacén de claves se ha alterado o la contraseña es incorrecta

Paso 9. Para cambiar la contraseña del almacén de claves, utilice este comando y reinicie el procedimiento de nuevo desde el Paso 4 con la nueva contraseña.

keytool -storepasswd -keystore .\lib\security\cacerts

Paso 10. Después de la importación correcta, utilice este comando para ver el certificado del almacén de claves.

keytool -list -keystore .\lib\security\cacerts -alias fina.nag.com

keytool -list -keystore .\lib\security\cacerts -alias cuic.nag.com

Finesse, CUIC, Cisco IDS y VVB

Paso 1. Inicie sesión en la página de administración del sistema operativo del servidor Finesse y cargue los certificados SSL de AW en la confianza de tomcat.

Paso 2. Vaya a **Administración del sistema operativo > Seguridad > Administración de certificados.**

Paso 3. Haga clic en Cargar certificado\cadena de certificado y seleccione tomcat-trust en el menú desplegable.

Paso 4. Examine el almacén de certificados en el almacenamiento local y haga clic en el botón Cargar.

Paso 5. Repita los pasos para cargar todo el certificado de servidor AW en el clúster de Finesse.

> **Nota:** No es necesario cargar el certificado tomcat-trust en el nodo secundario, esto se replica automáticamente.

Paso 6. Reinicie el servicio tomcat para que los cambios del certificado tengan efecto.

Paso 7. En CUIC, IDS y VVB, siga los pasos del 2 al 4 y cargue el certificado AW.

Intercambio de certificados entre Finesse y CUIC/LiveData

Paso 1. Mantenga los certificados Finesse, CUIC y LiveData en una carpeta independiente.

Paso 2. Inicie sesión en la página Finesse, CUIC y LiveData OS Administration.

Paso 3. Vaya a **Administración del sistema operativo > Seguridad > Administración de certificados.**

Paso 4. Haga clic en Cargar certificado\cadena de certificado y seleccione tomcat-trust en el menú desplegable.

Paso 5. Examine el almacén de certificados en el almacenamiento local y seleccione el certificado de servidores como se muestra a continuación y, a continuación, haga clic en el botón Cargar.

En el servidor Finesse - CUIC y LiveData como confianza de Tomcat

En el servidor CUIC: Finesse y LiveData como confianza de tomcat

En LiveData Server: CUIC y Finesse como confianza de Tomcat

> **Nota:** No es necesario cargar el certificado tomcat-trust en el nodo secundario, esto se replica automáticamente.

Paso 6. Reinicie el servicio tomcat en cada nodo para que los cambios del certificado surtan efecto.