Solución del paquete CCE: Procedimiento para obtener y para cargar los Certificados de CA de tercera persona

Contenido

Introducción

Este documento describe los pasos implicados para obtener y instalar un certificado del Certification Authority (CA), generado de un proveedor externo para establecer una conexión HTTPS entre la delicadeza y los servidores unificados Cisco del centro de la inteligencia (CUIC).

Para utilizar el HTTPS para la comunicación segura entre la delicadeza y los servidores CUIC, la configuración de los Certificados de la Seguridad es necesaria. Por abandono, estos servidores proporcionan los certificados autofirmados se utilizan que o los clientes pueden procurar y instalar los Certificados de CA. Estos Certificados de CA se pueden obtener de un proveedor externo como Verisign, Thawte, GeoTrust o se pueden producir internamente.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Empresa del Centro de contacto del paquete de Cisco (PCCE)
- CUIC
- Delicadeza de Cisco
- Certificados de CA

Componentes Utilizados

La información usada en el documento se basa en la versión de la solución 11.0 PCCE (1).

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 su red está viva, aseegurese que usted entiende el impacto potencial de cualquier paso.

Procedimiento

Para configurar los Certificados para la comunicación HTTPS en la delicadeza y los servidores CUIC, siga los siguientes pasos:

- Genere y descargue el pedido de firma de certificado (el CSR)
- Obtenga el certificado de la raíz, del intermedio (si procede) y de la aplicación de CA con el uso del CSR
- Cargue los Certificados a los servidores

Genere y descargue el CSR

1. Los pasos descritos aquí son para generar y descargar el CSR. Estos pasos son lo mismo para la delicadeza y los servidores CUIC.

2. Abra la **página de administración del sistema operativo de las Comunicaciones unificadas de Cisco** con el URL y ingrese con la cuenta de administración del operating system (OS) creada a la hora del proceso de instalación. **https://hostname del servidor primario/del cmplatform**

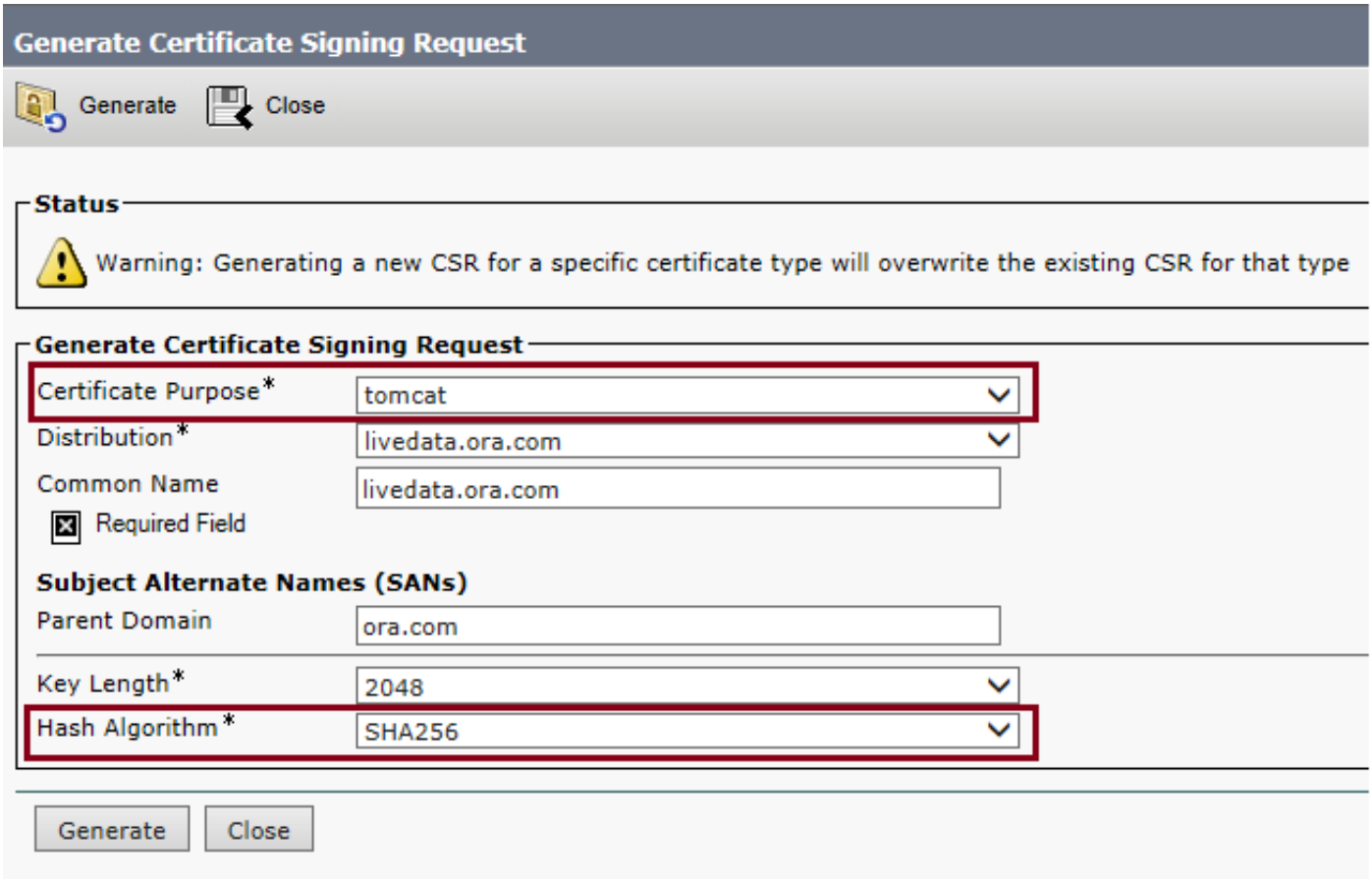
3. Genere el pedido de firma de certificado.

a. Navegue al **Certificate Management (Administración de certificados) de la Seguridad > generan el CSR**.

b. De la lista desplegable de Purpose* del certificado, seleccione el **tomcat**.

c. Seleccione el algoritmo de troceo como **SHA256**.

d. El tecleo **genera** tal y como se muestra en de la imagen.

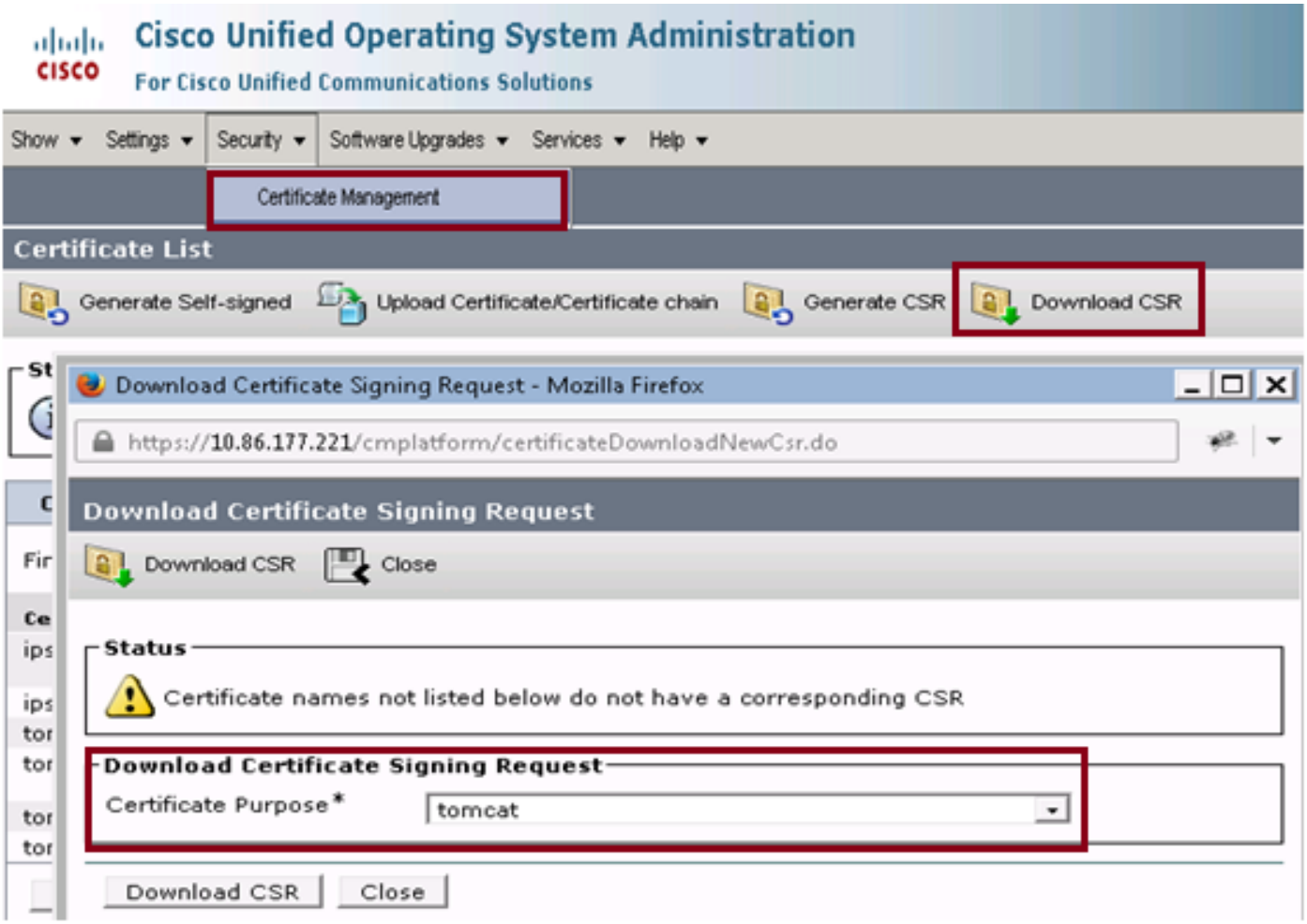


4. Descarga CSR.

a. Navegue al **Certificate Management (Administración de certificados) > a la descarga CSR de la Seguridad**.

b. De la lista desplegable de Purpose* del certificado, seleccione el **tomcat**.

c. Haga clic la **descarga CSR** tal y como se muestra en de la imagen.



Note: Realice estos pasos en el servidor secundario con el URL **https://hostname del servidor secundario/del cmplatform** para obtener los CSR para CA.

Obtenga el certificado de la raíz, del intermedio (si procede) y de la aplicación de CA

1. Proporcione la información primaria y del servidor secundario CSR al otro vendedor CA como Verisign, Thawte, GeoTrust etc.

2. De CA, usted debe recibir este la Cadena de certificados para el primario y los servidores secundarios:

- Servidores de la delicadeza: Certificado de la raíz, del intermedio y de la aplicación
- Servidores CUIC: Certificado de la raíz y de la aplicación

Certificados de la carga a los servidores

Esta sección describe en cómo cargar la Cadena de certificados correctamente en la delicadeza y los servidores CUIC.

Servidores de la delicadeza

1. Certificado primario de la raíz del servidor de la delicadeza de la carga:

a. En la **página de administración del sistema operativo de las Comunicaciones unificadas de Cisco del** servidor primario, navegue al **Certificate Management (Administración de certificados) de la Seguridad > al certificado de la carga**.

b. De la lista desplegable del propósito del certificado, seleccione la Tomcat-**confianza**.

c. En el campo del archivo de la carga, el tecleo **hojea** y hojea el **archivo de certificado raíz**.

d. **Archivo de la carga del** tecleo.

2. Certificado intermedio del servidor primario de la delicadeza de la carga:

a. De la lista desplegable del propósito del certificado, seleccione la Tomcat-**confianza**.

b. En el certificado raíz clasifiado, ingrese el nombre del certificado raíz que está cargado en el paso anterior. Éste es un archivo del **.pem** se genera que cuando la raíz/el certificado público fue instalada.

Para ver este archivo, navegue a la **administración de certificados > al hallazgo**. En la lista del certificado, el nombre del archivo del **.pem** es mencionado contra la Tomcat-confianza.

c. En el campo del archivo de la carga, el tecleo **hojea** y hojea el **archivo de certificado intermedio**.

d. **Archivo de la carga del** tecleo.

> **Note**: Mientras que el almacén de la Tomcat-confianza se replica entre el primario y los servidores secundarios, no es necesario cargar la raíz del servidor de la delicadeza o el certificado primaria del intermedio al servidor secundario de la delicadeza.

3. Certificado primario de la aplicación del servidor de la delicadeza de la carga:

a. De la lista desplegable del propósito del certificado, seleccione el **tomcat**.

b. En el campo del certificado raíz, ingrese el nombre del certificado intermedio que está cargado en el paso anterior. Incluya la extensión del **.pem** (por ejemplo, TEST-SSL-CA.pem).

c. En el campo del archivo de la carga, el tecleo **hojea** y hojea el **archivo de certificado de la aplicación**.

d. **Archivo de la carga del** tecleo.

4. Raíz del servidor de la delicadeza de la carga y certificado secundarios del intermedio:

a. Siga los mismos pasos como se menciona en los pasos 1 y 2 en el servidor secundario para sus Certificados.

> **Note**: Mientras que el almacén de la Tomcat-confianza se replica entre el primario y los servidores secundarios, no es necesario cargar la raíz del servidor de la delicadeza o el certificado secundaria del intermedio al servidor primario de la delicadeza.

5. Certificado secundario de la aplicación del servidor de la delicadeza de la carga:

a. Siga los mismos pasos como se menciona en el paso 3. en el servidor secundario para sus propios Certificados.

6. Servidores del reinicio:

a. Acceda el CLI en los servidores primarios y secundarios de la delicadeza y ejecute el **reinicio de sistema del utils del** comando para recomenzar los servidores.

Servidores CUIC

1. Certificado de la raíz del servidor primario de la carga CUIC (público):

a. En la **página de administración del sistema operativo de las Comunicaciones unificadas de Cisco del** servidor primario, navegue al **Certificate Management (Administración de certificados) de la Seguridad > al certificado de la carga**.

b. De la lista desplegable del propósito del certificado, seleccione la Tomcat-**confianza**.

c. En el campo del archivo de la carga, el tecleo **hojea** y hojea el **archivo de certificado raíz**.

d. **Archivo de la carga del** tecleo.

> **Note**: Mientras que el almacén de la Tomcat-confianza se replica entre el primario y los servidores secundarios, no es necesario cargar el certificado primario de la raíz del servidor CUIC a los servidores secundarios CUIC.

2. Certificado (primario) de la aplicación de servidor primario de la carga CUIC:

a. De la lista desplegable del propósito del certificado, seleccione el **tomcat**.

b. En el campo del certificado raíz, ingrese el nombre del certificado raíz que está cargado en el paso anterior.

Éste es un archivo del **.pem** se genera que cuando la raíz/el certificado público fue instalada. Para ver este archivo, navegue a la **administración de certificados > al hallazgo**.

En el **.pem de la** lista del certificado el nombre del archivo es mencionado contra la Tomcat-confianza. Incluya esa extensión del .pem (por ejemplo, TEST-SSL-CA.pem).

c. En el campo del archivo de la carga, el tecleo **hojea** y hojea el **archivo de certificado (primario) de la aplicación**.

d. **Archivo de la carga del** tecleo.

3. Certificado de la raíz del servidor secundario de la carga CUIC (público):

a. En el servidor secundario CUIC, siga los mismos pasos como se menciona en el paso 1. para su certificado raíz.

> **Note**: Mientras que el almacén de la Tomcat-confianza se replica entre el primario y los servidores secundarios, no es necesario cargar el certificado secundario de la raíz del

servidor CUIC al servidor primario CUIC.

4. Certificado (primario) de la aplicación de servidor secundario de la carga CUIC:

a. Siga el mismo proceso como se afirma en el paso 2. en el servidor secundario para su propio certificado.

5. Servidores del reinicio:

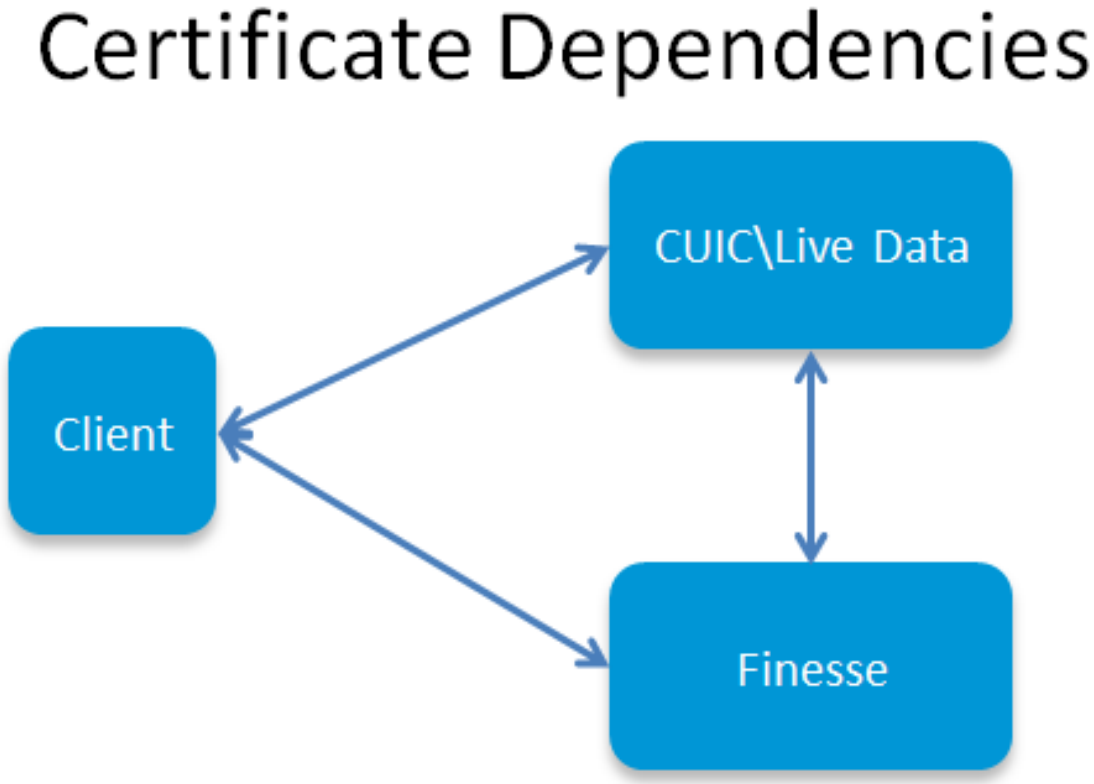
a. Acceda el CLI en los servidores primarios y secundarios CUIC y ejecute el **reinicio de sistema del utils del** comando para recomenzar los servidores.

> **Note**: Para evitar la advertencia de la excepción del certificado, usted debe acceder los servidores con el uso del nombre de dominio completo (FQDN).

Dependencias del certificado

Pues los agentes y los supervisores de la delicadeza utilizan los gadgets CUIC para señalar los propósitos, usted tiene que cargar los certificados raíz de estos servidores también, en la orden mencionada aquí para mantener las dependencias del certificado para la comunicación HTTPS entre estos servidores y tal y como se muestra en de la imagen.

- Certificado raíz de los servidores de la carga CUIC en el servidor primario de la delicadeza
- Cargue la raíz de la delicadeza \ el certificado intermedio en el servidor primario CUIC



Cargue el certificado raíz de los servidores CUIC en el servidor primario de la delicadeza

1. En el servidor primario de la delicadeza, la **página de administración** abierta del **sistema**

operativo de las Comunicaciones unificadas de Cisco con el URL y ingresa con la cuenta de administración OS creada a la hora del proceso de instalación:

https://hostname del servidor/del cmplatform primarios de la delicadeza

2. Certificado raíz primario de la carga CUIC.

a. Navegue al Certificate Management (Administración de certificados) de la Seguridad > al certificado de la carga.

b. De la lista desplegable del propósito del certificado, seleccione la Tomcat-confianza.

c. En el campo del archivo de la carga, el tecleo hojea y hojea el archivo de certificado raíz.

d. Archivo de la carga del tecleo.

3. Certificado raíz secundario de la carga CUIC.

a. Navegue al Certificate Management (Administración de certificados) de la Seguridad > al certificado de la carga.

b. De la lista desplegable del propósito del certificado, seleccione la Tomcat-confianza.

c. En el campo del archivo de la carga, el tecleo hojea y hojea el archivo de certificado raíz.

d. Archivo de la carga del tecleo.

> Note: Mientras que el almacén de la Tomcat-confianza se replica entre el primario y los servidores secundarios, no es necesario cargar los certificados raíz CUIC al servidor secundario de la delicadeza.

4. Acceda el CLI en los servidores primarios y secundarios de la delicadeza y ejecute el reinicio de sistema del utils del comando para recomenzar los servidores.

Cargue la raíz de la delicadeza/el certificado intermedio en el servidor primario CUIC

1. En el servidor primario CUIC, la página de administración abierta del sistema operativo de las Comunicaciones unificadas de Cisco con el URL y ingresa con la cuenta de administración OS creada a la hora del proceso de instalación:

https://hostname del servidor primario/del cmplatform CUIC

2. Certificado raíz primario de la delicadeza de la carga:

a. Navegue al Certificate Management (Administración de certificados) de la Seguridad > al certificado de la carga.

b. De la lista desplegable del propósito del certificado, seleccione la Tomcat-confianza.

c. En el campo del archivo de la carga, el tecleo hojea y hojea el archivo de certificado raíz.

d. **Archivo de la carga del** tecleo.

certificado intermedio de la delicadeza primaria 3.Upload:

a. De la lista desplegable del propósito del certificado, seleccione la Tomcat-**confianza**.

b. En el certificado raíz clasifiado, ingrese el nombre del certificado raíz que está cargado en el paso anterior.

c. En el campo del archivo de la carga, el tecleo **hojea** y hojea el **archivo de certificado intermedio**.

d. **Archivo de la carga del** tecleo.

4. Realice el mismo paso 2 y el paso 3. para la raíz secundaria de la delicadeza \ los Certificados intermedios en el servidor de datos vivo primario.

> **Note**: Mientras que el almacén de la Tomcat-confianza se replica entre el primario y los servidores secundarios, no es necesario cargar el certificado de /Intermediate de la raíz de la delicadeza a los servidores secundarios CUIC.

5. Acceda el CLI en los servidores primarios y secundarios CUIC y ejecute el **reinicio de sistema del utils del** comando para recomenzar los servidores.