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

## Contenido



## Introducción

Para utilizar el HTTPS para la comunicación segura entre la delicadeza y Cisco unificó los servidores de centro de la inteligencia (CUIC), los Certificados de la Seguridad que la configuración es necesaria. Por abandono estos servidores proporcionan los certifcates uno mismo-firmados se utilizan que o los clientes pueden procurar y instalar los Certificados del Certificate Authority (CA). Estos certs de CA se pueden obtener de un proveedor externo como Verisign, Thawte, GeoTrust o se pueden producir internaly.

Este documento apunta explicar detalladamente los pasos implicados para obtener y para 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).

## Prerequisites

### Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Empresa del Centro de contacto del paquete de Cisco (PCCE)
- Cisco unificó el centro de la inteligencia (CUIC)
- Delicadeza de Cisco

- Certificados de CA

### Componentes Utilizados

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

Configurando los Certificados para la comunicación HTTPS en la delicadeza y el centro unificado Cisco de la inteligencia (CUIC) los servidores requieren los pasos siguientes

- Genere y descargue el pedido de firma de certificado (CSR).
- Obtenga el certificado de la raíz, del intermedio (si procede) y de la aplicación del Certificate Authority usando el CSR.
- Cargue los Certificados a los servidores.

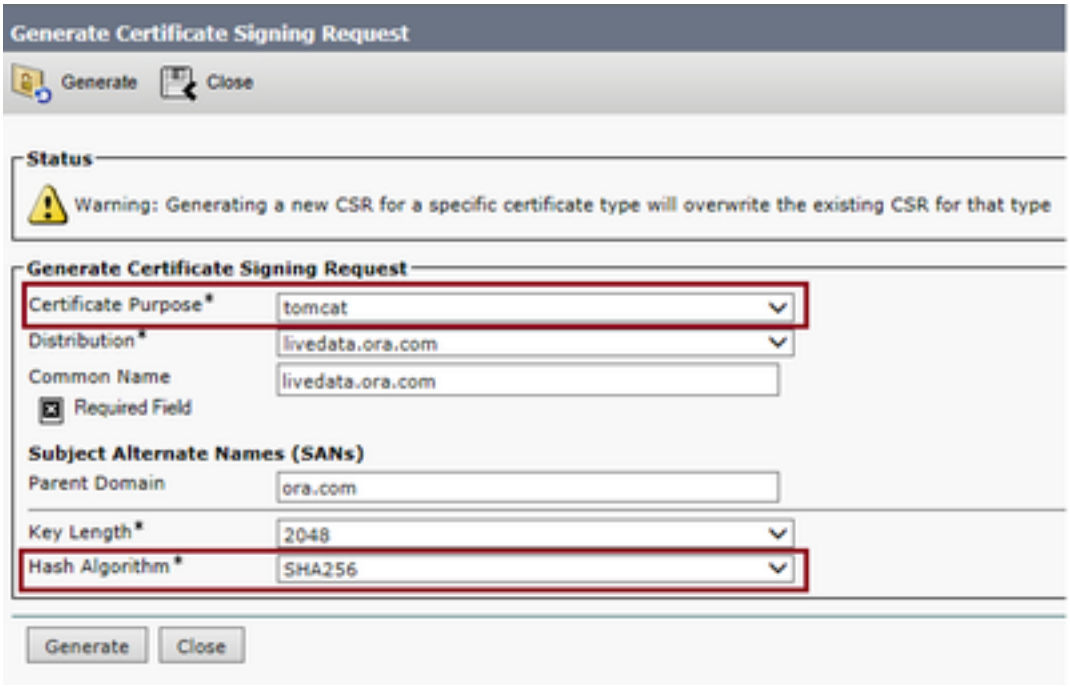
### Paso 1: Genere y descargue el pedido de firma de certificado (el CSR)

---

1. Los pasos descritos más abajo para generar y descargar el CSR 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 usando el URL expuesto abajo y ingrese con la cuenta de administración OS creada durante el proceso de instalación
https://hostname del servidor primario/del cmplatform

3. Genere el pedido de firma de certificado (el CSR)

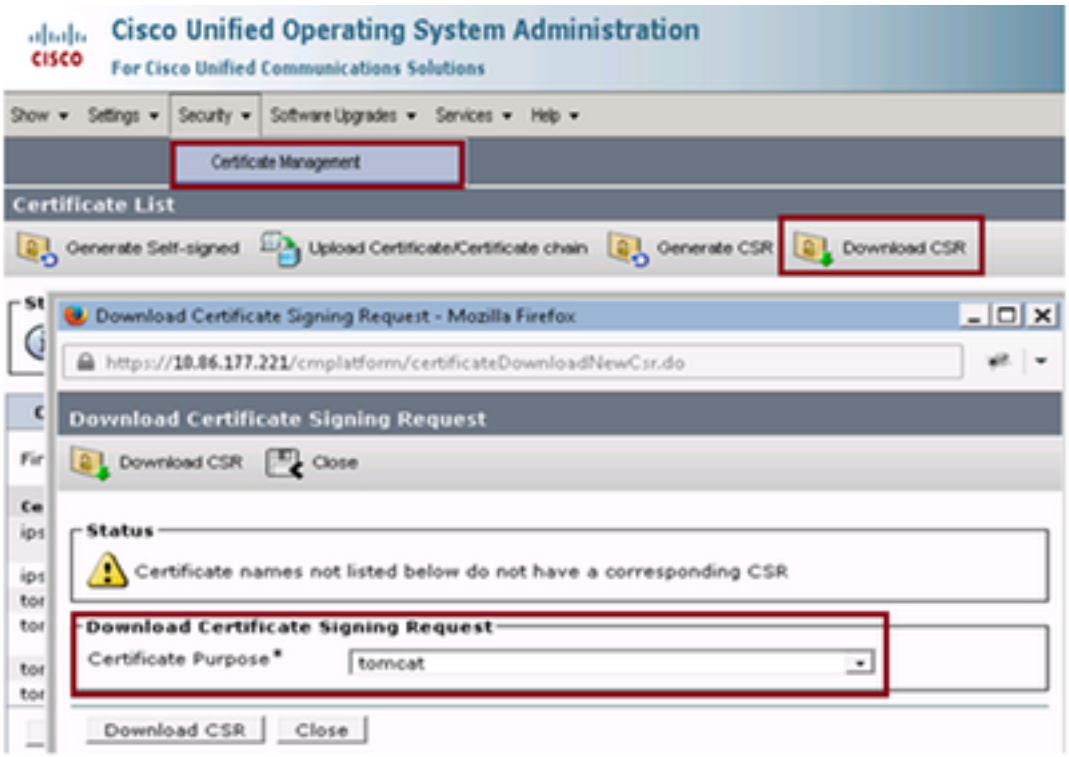



a) El Certificate Management (Administración de certificados) selecto de la Seguridad > genera el CSR.

b) De la lista desplegable del nombre del propósito del certificado, seleccione el tomcat.

c) Seleccione el algoritmo de troceo como SHA256
d) El tecleo genera el CSR.

4. Pedido de firma de certificado de la descarga (CSR)




a) Certificate Management (Administración de certificados) de la Seguridad > descarga selectos CSR.
b) De la lista desplegable del nombre del certificado, seleccione el tomcat.
c) Haga clic la descarga CSR.

*Note:*

*Realice los pasos antedichos en el servidor secondory usando el URL "https://hostname del servidor/del cmplatform secondory" para obtener los CSR para el Certificate Authority.*

## Paso 2: Obtenga el certificado de la raíz, del intermedio (si procede) y de la aplicación del Certificate Authority

---

1. Proporcione la información primaria y secondory del pedido de firma de certificado de los servidores (CSR) a la autoridad de Certifcate del otro vendedor (CA) como Verisign, Thawte, GeoTrust etc.

2. De la autoridad de Certifcate (CA) uno debe recibir la Cadena de certificados siguiente para los servidores primarios y secondory.

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

## Paso 3: Certificados de la carga a los servidores

---

Esta sección describe en cómo cargar la Cadena de certificados correctamente en la delicadeza y los servidores unificados Cisco del centro de la inteligencia (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, selecta

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

b) De la lista desplegable del nombre del certificado, seleccione la Tomcat-confianza.
c) En el campo del archivo de la carga, el tecleo hojea y hojea al archivo de certificado raíz.
d) Archivo de la carga del tecleo.

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

a) De la lista desplegable del nombre del certificado, seleccione la Tomcat-confianza.
b) En el certificado raíz clasifiado, ingrese el nombre del certificado raíz que usted cargó 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 > a ClickFind. En el nombre del archivo del .pem de la lista del certificado sea mencionado contra la Tomcat-confianza.

c) En el campo del archivo de la carga, el tecleo hojea y hojea al archivo de certificado intermedio.
d) Archivo de la carga del tecleo.

*Note:*
*Mientras que el almacén de la Tomcat-confianza se replica entre los servidores primarios y secondory 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 nombre del certificado, seleccione el tomcat.

b) En el campo del certificado raíz, ingrese el nombre del certificado intermedio que usted cargó 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 al 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 secondory del intermedio.

a) Siga los mismos pasos como se mencionó anteriormente en (1) y (2) en el servidor secondory para sus Certificados

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

5. Certificado secondory de la aplicación del servidor de la delicadeza de la carga.

a) Siga los mismos pasos como se mencionó anteriormente en (3) en el servidor secondory para sus propios Certificados.

6. Recomience los servidores

Acceda el CLI en los servidores primarios y secondory de la delicadeza y ingrese el comando “reinicio de sistema del utils” de recomenzar los servidores.

Servidores CUIC:

==========

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

a) En la página de administración del sistema operativo de las Comunicaciones unificadas de Cisco del servidor primario, selecta

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

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

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

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

2. Certificado (primario) cuic de la aplicación de servidor primario de la carga
a) De la lista desplegable del nombre del certificado, seleccione el tomcat.
b) En el campo del certificado raíz, ingrese el nombre del certificado raíz que usted cargó 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 > a ClickFind. En el nombre del archivo del .pem de la lista del certificado sea 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 al archivo de certificado (primario) de la aplicación.
d) Archivo de la carga del tecleo

*3.* Certificado secondory cuic de la raíz del servidor de la carga (público)

a) En el servidor cuic secondory 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 los servidores primarios y secondory no es necesario cargar el certificado secondory de la raíz del servidor de CUIc al servidor primario CUIC.*

certificado (primario) secondory cuic de la aplicación del servidor 4.Upload.
a) Siga el mismo proceso como se afirma en el paso (2) en el servidor secondory para su propio certificado.

6. Recomience los servidores

Acceda el CLI en los servidores primarios y secondory CUIC y ingrese el comando “reinicio de sistema del utils” de recomenzar los servidores.

*Note:*

*Para evitar la excepción del certificado que le advierte debe acceder los servidores usando el nombre del nombre de dominio completo (FQDN).*

Dependencias del certificado:

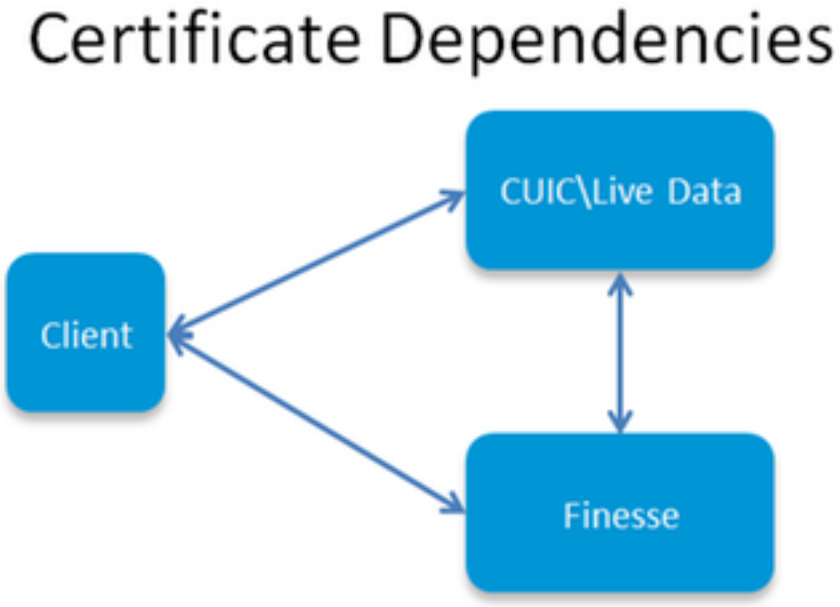
==========

Como

Los agentes y los supervisores de la delicadeza utilizan los gadgets CUIC para señalar los

propósitos uno tienen que cargar los certificados raíz de estos servidores también en el siguiente orden de mantener las dependencias del certificado para la comunicación HTTPS entre estos servidores.

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




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

---

la página de administración abierta del sistema operativo de las Comunicaciones unificadas de Cisco del servidor primario de la delicadeza 1.On usando el URL expuesto abajo y ingresa con la cuenta de administración OS creada durante los provcess de la instalación

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

certificado raíz primario 2.Upload CUIC.
a) Certificate Management (Administración de certificados) de la Seguridad > certificado selectos de la carga.
b) De la lista desplegable del nombre del certificado, seleccione la Tomcat-confianza.
c) En el campo del archivo de la carga, el tecleo hojea y hojea al archivo de certificado raíz.
d) Archivo de la carga del tecleo.

certificado raíz 3.Upload Secondory CUIC.

a) Certificate Management (Administración de certificados) de la Seguridad > certificado selectos de la carga.
b) De la lista desplegable del nombre del certificado, seleccione la Tomcat-confianza.
c) En el campo del archivo de la carga, el tecleo hojea y hojea al archivo de certificado raíz.
d) Archivo de la carga del tecleo.

*Note:*

*Mientras que el almacén de la Tomcat-confianza se replica entre los servidores primarios y secondory no es necesario cargar los certificados raíz CUIC al servidor secundario de la delicadeza.*

4. Acceda el CLI en los servidores primarios y secondory de la delicadeza y ingrese el comando "reinicio de sistema del utils" de recomenzar los servidores.

**b)** **Cargue la raíz de la delicadeza \ el certificado intermedio en el servidor primario CUIC**

**----------**

la página de administración abierta del sistema operativo de las Comunicaciones unificadas de Cisco CUIC del servidor primario 1.On usando el URL expuesto abajo y ingresa con la cuenta de administración OS creada durante los provcess de la instalación
https://hostname del servidor primario/del cmplatform CUIC

**certificado raíz primario de la delicadeza 2.Upload.**
a) Certificate Management (Administración de certificados) de la Seguridad > certificado selectos de la carga.
b) De la lista desplegable del nombre del certificado, seleccione la Tomcat-confianza.
c) En el campo del archivo de la carga, el tecleo hojea y hojea al archivo de certificado raíz.
d) Archivo de la carga del tecleo.

**3. Certificado primario del intermedio de la delicadeza de la carga**

i) De la lista desplegable del nombre del certificado, seleccione la Tomcat-confianza.
ii) En el certificado raíz clasifiado, ingrese el nombre del certificado raíz que usted cargó en el paso anterior.
iii) En el campo del archivo de la carga, el tecleo hojea y hojea al archivo de certificado intermedio.
iv) Archivo de la carga del tecleo.

4. Realice los mismos pasos (2 y 3) para la raíz secondory 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 los servidores primarios y secondory 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 secondory CUIC y ingrese el comando "reinicio de sistema del utils" de recomenzar los servidores.