Contenido

Introducción

Para utilizar el HTTPS para la comunicación segura entre la delicadeza, Cisco unificó la inteligencia de centro (CUIC) y los servidores de datos vivos, configuración de los Certificados de la Seguridad son necesarios. Por abandono estos servidores proporcionan los certifcates uno mismo-firmados se utilizan que o los clientes pueden procurar y instalar el certificado 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 instalar un certificado del Certification Authority (CA), generado de un proveedor externo para establecer una conexión HTTPS entre la delicadeza, Cisco unificó el centro de la inteligencia (CUIC), y a los servidores de datos vivos.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Contact Center Enterprise (UCCE)
- Datos del cisco live
- Cisco unificó el centro de la inteligencia (CUIC)
- Delicadeza de Cisco
- CA certificó

Componentes Utilizados

La información usada en el documento se basa en la versión de la solución UCCE 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 el certificado para la comunicación HTTPS en la delicadeza, CUIC y los servidores de datos vivos requieren los pasos siguientes

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

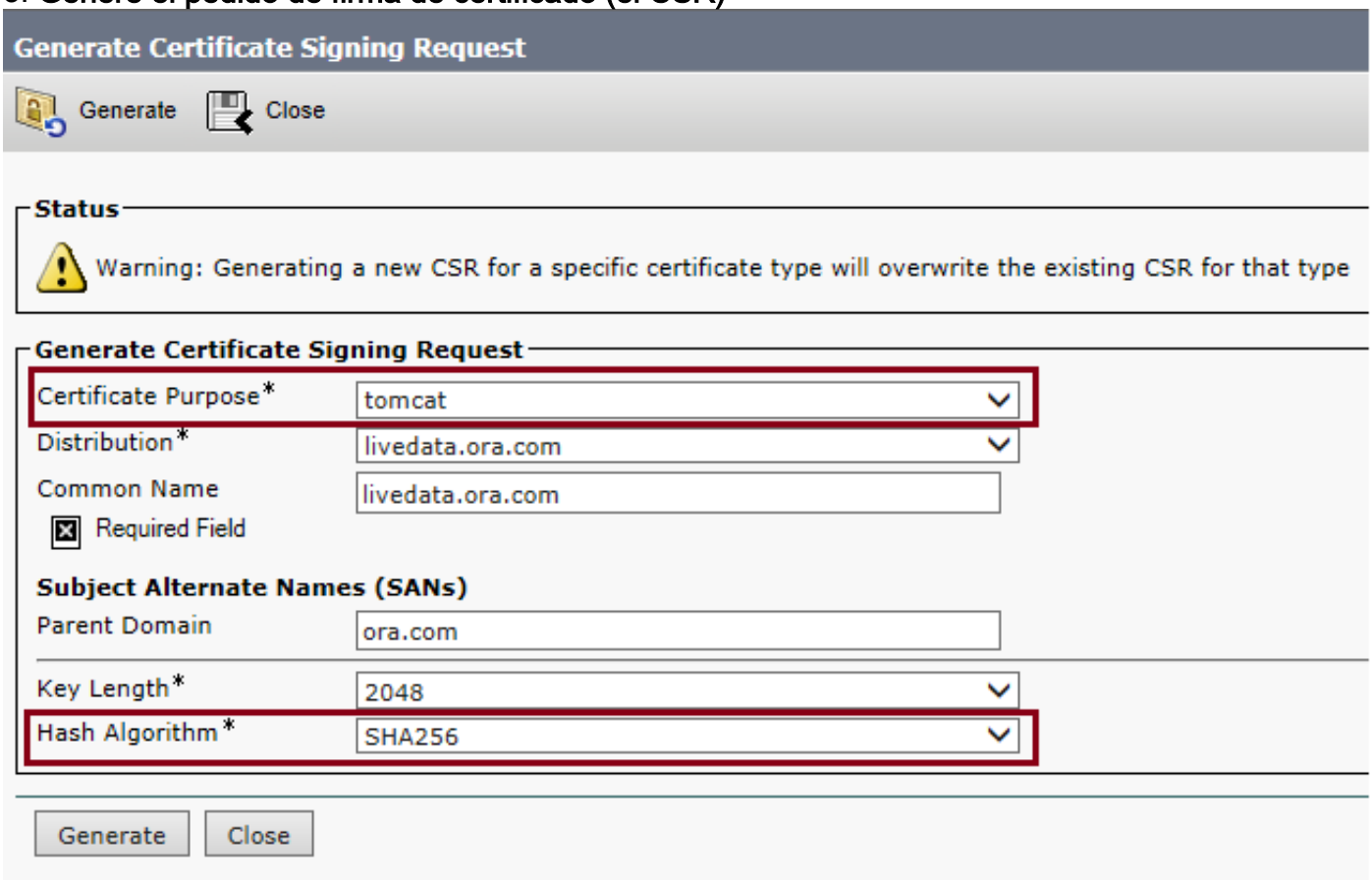
Paso 1: Genere y descargue el pedido de firma de certificado (el CSR)

---

1. Los pasos descritos más abajo para generar y descargar el CSR son lo mismo para la delicadeza, CUIC y los datos vivos separan.

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 los provcess de la instalación
https://hostname del servidor primario/del cmplatform

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

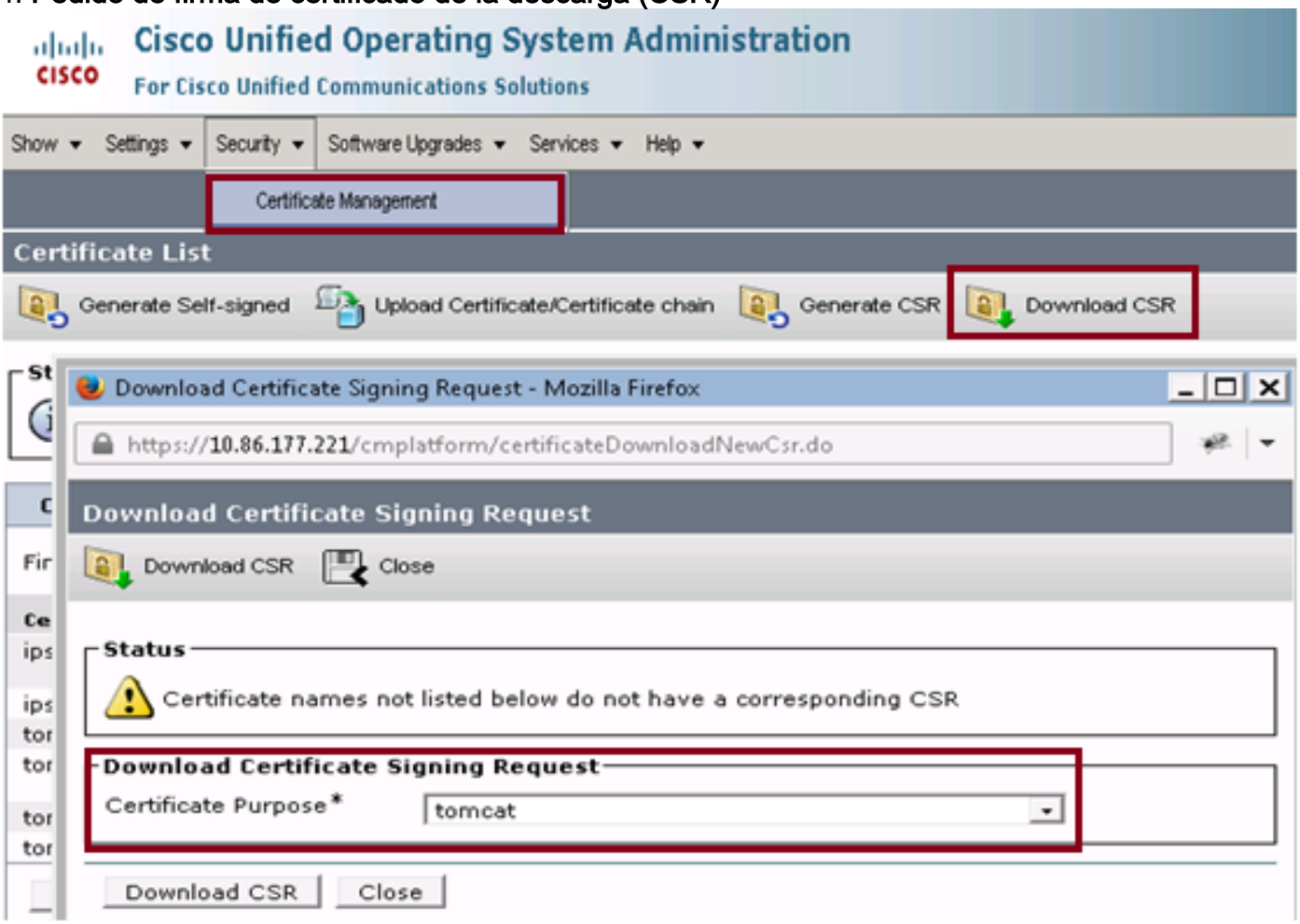


a) El Certificate Management (Administración de certificados) selecto de la Seguridad > genera el CSR.

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.

Nota:

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
- **Servicios vivos de los datos:** 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, CUIC y vivir los servidores de datos.

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 fineese primario del intermedio del servidor 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. No incluya la extensión (por ejemplo, PRUEBE raíz CA 2048).
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.

Nota:
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 Secondory de la carga y certificado del intermedio.**

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

Nota:
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 fineese secondory de la aplicación del servidor de la carga.

a)

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.

Nota:
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. 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 (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.

Nota:
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.

Nota:

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

Servidores de datos vivos:

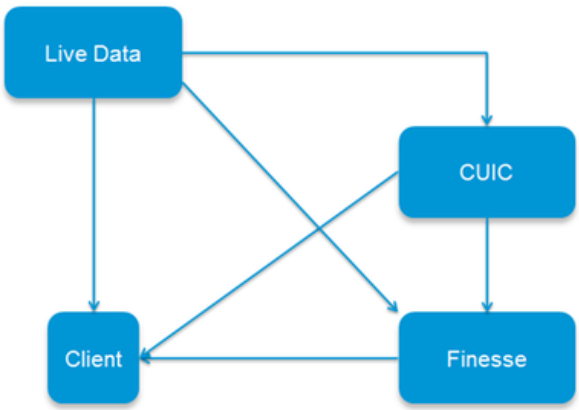
==========

1. Para cargar la raíz de los datos y el certficate vivos de la aplicación siga los mismos pasos según lo delineado arriba para los servidores CUIC.

2. Como servidores de datos vivos obre recíprocamente con CUIC y los servidores uno de la delicadeza tiene que cargar los certificados raíz de estos servidores también en el siguiente orden de mantener las dependencias del certificado.

- **Cargue la** raíz de la delicadeza \ el intermedio y los certificados raíz CUIC en el servidor de datos vivo
- Cargue el certificado raíz de los servidores Vivo-DATA en el servidor primario de la delicadeza
- Cargue el certificado raíz de los servidores CUIC en el servidor primario de la delicadeza
- Cargue los certificados raíz Vivo-DATA en el servidor primario CUIC
- Cargue la raíz de la delicadeza \ el certificado intermedio en el servidor primario CUIC

Certificate Dependencies



a) Cargue la raíz de la delicadeza \ el intermedio y los certificados raíz CUIC en el servidor de datos vivo

---

1. Cargue el certificado raíz primario de la delicadeza

i) En el servidor de datos vivo primario en la página de administración del sistema operativo de las Comunicaciones unificadas de Cisco, selecta

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

ii) De la lista desplegable del nombre del certificado, seleccione la Tomcat-confianza.
III) En el campo del archivo de la carga, el tecleo hojea y hojea al archivo de certificado raíz primario de la delicadeza.
iv) Archivo de la carga del tecleo.

2. 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. No incluya la extensión (por ejemplo, PRUEBE raíz CA 2048).
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.

3. Certificado raíz primario de la carga CUIC
i) En el servidor de datos vivo primario en la página de administración del sistema operativo de las Comunicaciones unificadas de Cisco, selecta

Certificate Management (Administración de certificados) de la Seguridad > certificado de la carga
ii) De la lista desplegable del nombre del certificado, seleccione la Tomcat-confianza.
iii) En el campo del archivo de la carga, el tecleo hojea y hojea al archivo de certificado raíz primario CUIC.
iv) Archivo de la carga del tecleo.

4. Realice los mismos pasos (1 y 2) para la raíz de la delicadeza \ el intermedio y los certificados raíz secondory CUIC en el servidor de datos vivo primario.

Nota:

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

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

b)

---

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 vivo primario de los datos 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.

certificado raíz vivo de los datos 3.Upload Secondory.

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.

Nota:
Mientras que el almacén de la Tomcat-confianza se replica entre los servidores primarios y secondory no es necesario cargar el certificado raíz vivo de los datos al servidor secundario de la delicadeza.

c)

---

la página de administración 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.

Nota:
Mientras que el almacén de la Tomcat-confianza se replica entre los servidores primarios y secondory no es necesario cargar el certificado raíz vivo de los datos 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.

d) Cargue los certificados raíz Vivo-DATA en el servidor primario CUIC

---

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

certificado raíz vivo primario de los datos 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.

certificado raíz vivo de los datos 3.Upload Secondory.

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.

Nota:
Mientras que el almacén de la Tomcat-confianza se replica entre los servidores primarios y secondory no es necesario cargar el certificado raíz vivo de los datos a los servidores secundarios CUIC.

e) 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 primario CUIC.

Nota:

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.