

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Procedimiento](#)

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

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

[Paso 3: Certificados de la carga a los servidores](#)

[Servidores de la delicadeza:](#)

[Servidores CUIC:](#)

a) [Certificado raíz de los servidores de la carga CUIC en el servidor primario de la delicadeza](#)

b) [Raíz de la delicadeza de la carga \ certificado intermedio en el servidor primario CUIC](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

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 certficates 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).

Prerrequisitos

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, asegúrese 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)

Generate Certificate Signing Request

Generate Close

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose* tomcat

Distribution* livedata.ora.com

Common Name livedata.ora.com

Required Field

Subject Alternate Names (SANs)

Parent Domain ora.com

Key Length* 2048

Hash Algorithm* SHA256

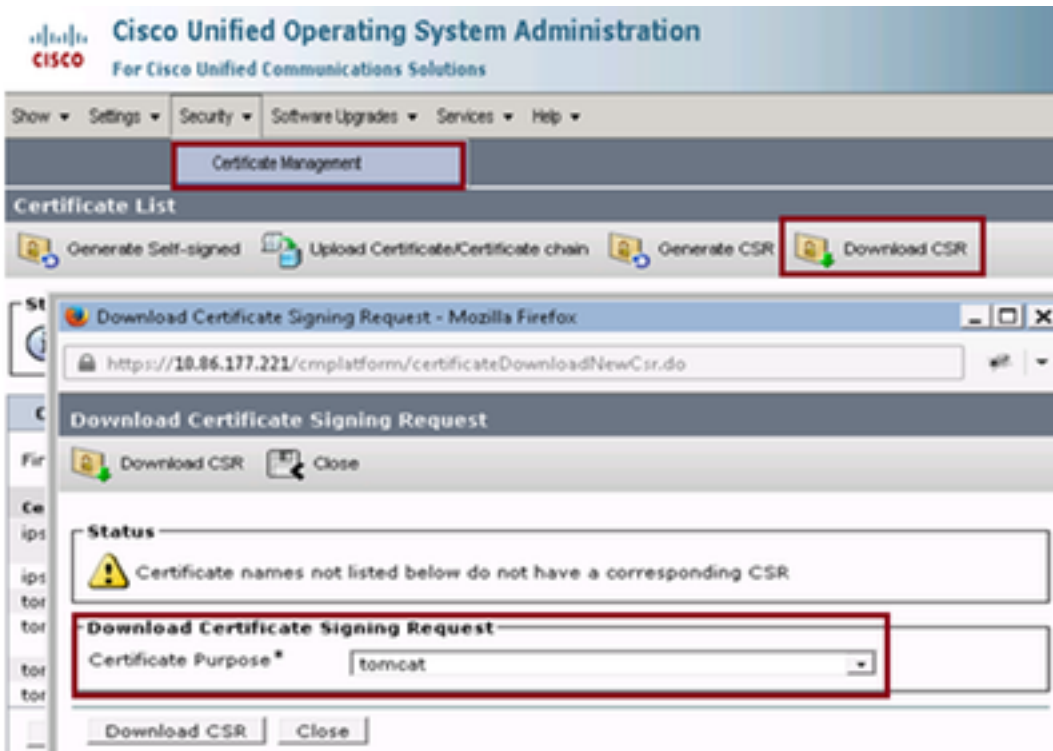
Generate Close

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 teclado 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 secondary usando el URL "https://hostname del servidor/del cmplatform secondary" 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 secondary del pedido de firma de certificado de los servidores (CSR) a la autoridad de Certificate del otro vendedor (CA) como Verisign, Thawte, GeoTrust etc.
 2. De la autoridad de Certificate (CA) uno debe recibir la Cadena de certificados siguiente para los servidores primarios y secondary.
 - **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 hojear y hojear 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 clasificado, 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 hojear y hojear 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 secondary 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 hojear y hojear 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 secondary del intermedio.

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

Nota:

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

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

a)

6. Recomience los servidores

Acceda el CLI en los servidores primarios y secondary 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 hojear y hojear 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 secondary 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 hojear y hojear al archivo de certificado (primario) de la aplicación.

d) Archivo de la carga del tecleo

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

a) En el servidor cuic secondary 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 secondary no es necesario cargar el certificado secondary de la raíz del servidor de CUIC al servidor primario CUIC.

certificado (primario) secondary cuic de la aplicación del servidor 4.Upload.

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

6. Recomience los servidores

Acceda el CLI en los servidores primarios y secondary 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).

Dependencias del certificado:

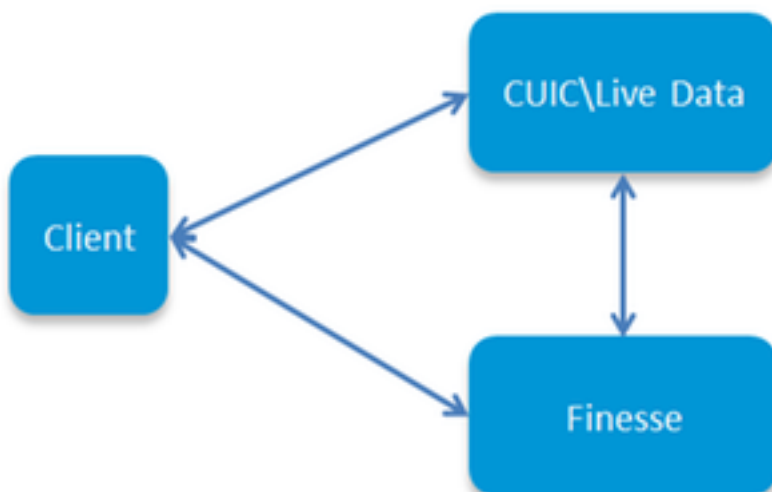
=====

Como

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

- 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

Certificate Dependencies



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

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 hojear y hojear al archivo de certificado raíz.
- d) Archivo de la carga del tecleo.

certificado raíz 3.Upload Secondary 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 hojear y hojear 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 secondary no es necesario cargar los certificados raíz CUIC al servidor secundario de la delicadeza.

4. Acceda el CLI en los servidores primarios y secondary 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 hojear y hojear al archivo de certificado raíz.
- d) Archivo de la carga del tecleo.

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

- i
- ii) En el certificado raíz clasificado, ingrese el nombre del certificado raíz que usted cargó en el paso anterior.

iii) En el campo del archivo de la carga, el tecleo hojear y hojear al archivo de certificado intermedio.

iv) Archivo de la carga del tecleo.

4. Realice los mismos pasos (2 y 3) para la raíz secondary de la delicadeza \ los Certificados intermedios en el servidor de datos vivo primario.

Nota:

Mientras que el almacén de la Tomcat-confianza se replica entre los servidores primarios y secondary no es necesario cargar el certificado de /intermediate de la raíz de la delicadeza a los servidores secundarios CUIIC.

5. Acceda el CLI en los servidores primarios y secondary CUIIC y ingrese el comando "reinicio de sistema del utils" de recomenzar los servidores.