

Solución unificada CCE: Procedimiento para obtener y para cargar los Certificados de CA de tercera persona (versión 11.x)

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

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

[Paso 2. Obtenga la raíz, intermedio \(si el applicableStep 5. y certificado de la aplicación del Certificate Authority.](#)

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

[Servidores de la delicadeza](#)

[Servidores CUIC \(si se asume que ningún Certificados del intermedio presente en la Cadena de certificados\)](#)

[Servidores de datos vivos](#)

[Dependencias vivas del certificado de servidores de datos](#)

[Verificación](#)

[Troubleshooting](#)

Introducción

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 los servidores vivos de los datos (LD).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Contact Center Enterprise (UCCE)
- Datos del cisco live (LD)
- 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, asegúrese que usted entiende el impacto potencial de cualquier paso.

Antecedentes

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

Configurar

Configurando el certificado para la comunicación HTTPS en la delicadeza, CUIIC y los servidores de datos vivos requieren estos pasos:

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

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

1. Los pasos descritos aquí para generar y descargar el CSR son lo mismo para la delicadeza, CUIIC y los datos vivos separan.
2. Abra la **página de administración del sistema operativo de las Comunicaciones unificadas de Cisco** usando el URL expuesto y ingrese con la cuenta de administración OS creada durante el proceso de instalación
<https://FQDN:8443/cmplatform>
3. Genere el pedido de firma de certificado (CSR) tal y como se muestra en de la imagen:

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

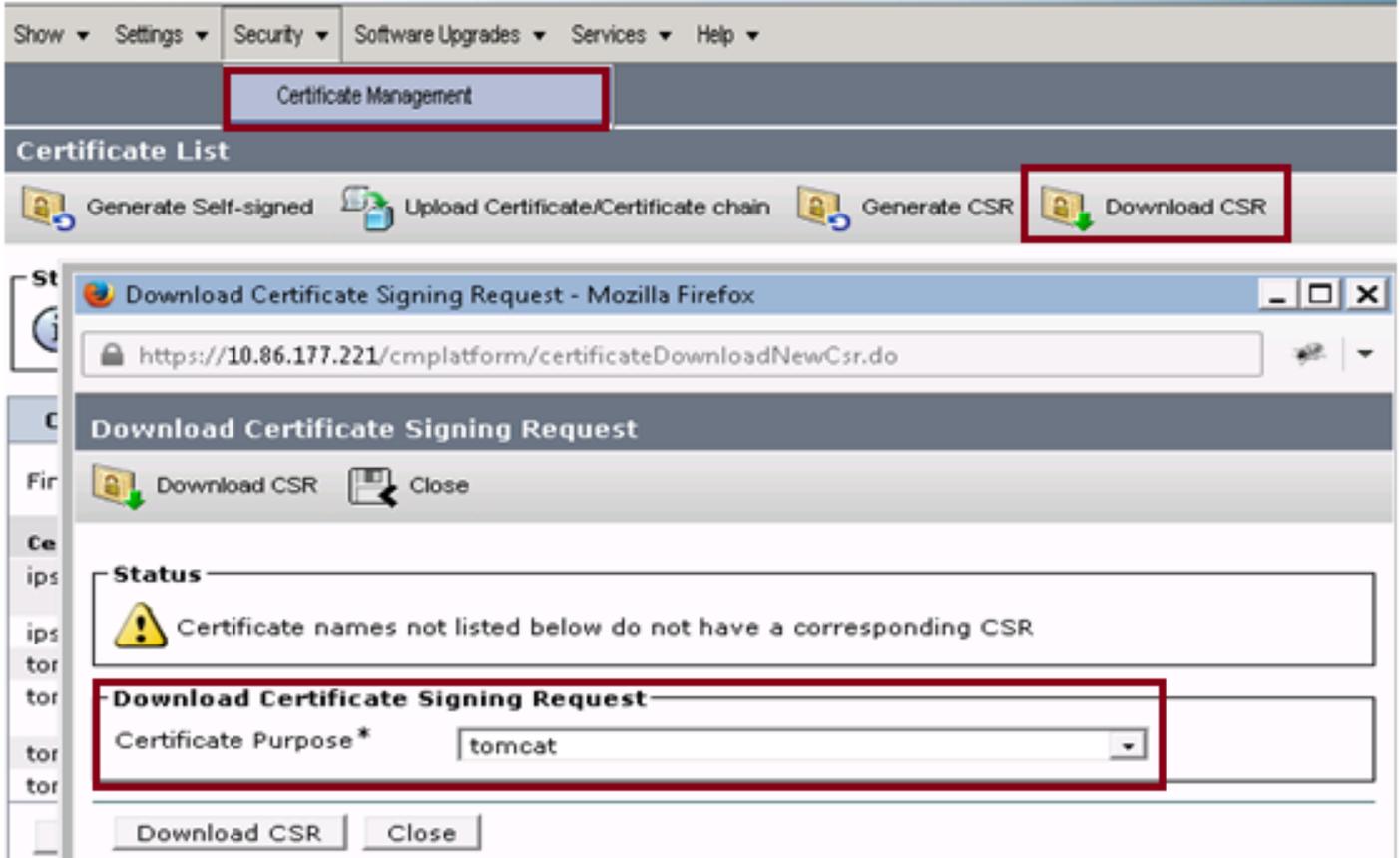
Generate Close

Paso 1. Navegue al **Certificate Management (Administración de certificados) de la Seguridad** > **generan el CSR**. Paso 2. De la lista desplegable del nombre del propósito del certificado, seleccione el tomcat. Paso 3. Seleccione el algoritmo de troceo y la longitud de clave depeping sobre las necesidades comerciales.

- Longitud de clave: 2048 \ algoritmo de troceo: Se recomienda SHA256

Paso 4. El tecleo **genera el CSR**. **Note:** Si el negocio requiere el padre sujeto de los nombres alternos (sin) que el campo del dominio que se llenará del Domain Name entonces satisface sea consciente de los direccionamientos del problema en el documento ["sin el problema con un certificado firmado del otro vendedor en la delicadeza"](#).

4. Descargue el pedido de firma de certificado (CSR) tal y como se muestra en de la imagen:



Paso 1. Navegue al **Certificate Management (Administración de certificados)** > a la descarga CSR de la Seguridad.

Paso 2. De la lista desplegable del nombre del certificado, seleccione el tomcat.

Paso 3. Descarga CSR del teclado.

Nota:

Note: Realice los pasos antedichos en el servidor secundario que usa el URL <https://FQDN:8443/cmplatform> para obtener los CSR para el Certificate Authority

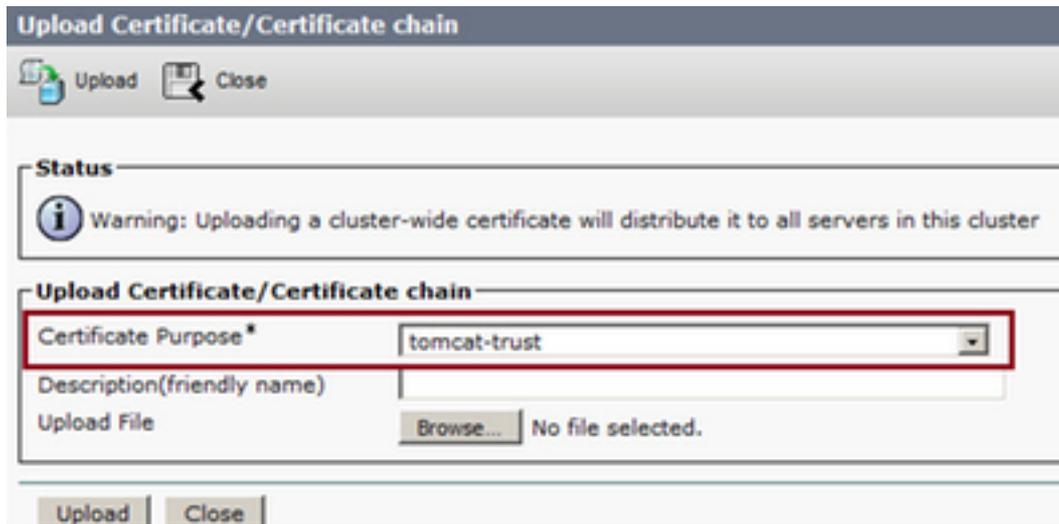
Paso 2. Obtenga la raíz, intermedio (si el aplicableStep 5. y certificado de la aplicación del Certificate Authority.

1. Proporcione el primario y a los servidores secundarios información del pedido de firma de certificado (CSR) a la autoridad de Certificate del otro vendedor como Verisign, Thawte, GeoTrust etc.
2. De la autoridad del certificate una debe recibir la Cadena de certificados siguiente para los servidores primarios y secondary.
 - Servidores de la delicadeza: Certificado arraigue, del intermedio (opcional) y de la aplicación
 - Servidores CUIC: Certificado arraigue, del intermedio (opcional) y de la aplicación
 - Servicios vivos de los datos: Certificado arraigue, del intermedio (opcional) 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. Cargue el certificado raíz en el servidor primario de la delicadeza con la ayuda de estos pasos:

Paso 1. 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.

Paso 2. De la lista desplegable del nombre del certificado, seleccione la Tomcat-confianza.
Paso 3. En el campo del archivo de la carga, el tecleo hojear y hojear al archivo de certificado raíz.

Paso 4. Archivo de la carga del tecleo.

2. Cargue el certificado intermedio en el servidor primario de Fineese con la ayuda de estos pasos:

Paso 1. Los pasos en cargar el certifiacte intermedio son lo mismo que el certificado raíz tal y como se muestra en del paso 1.

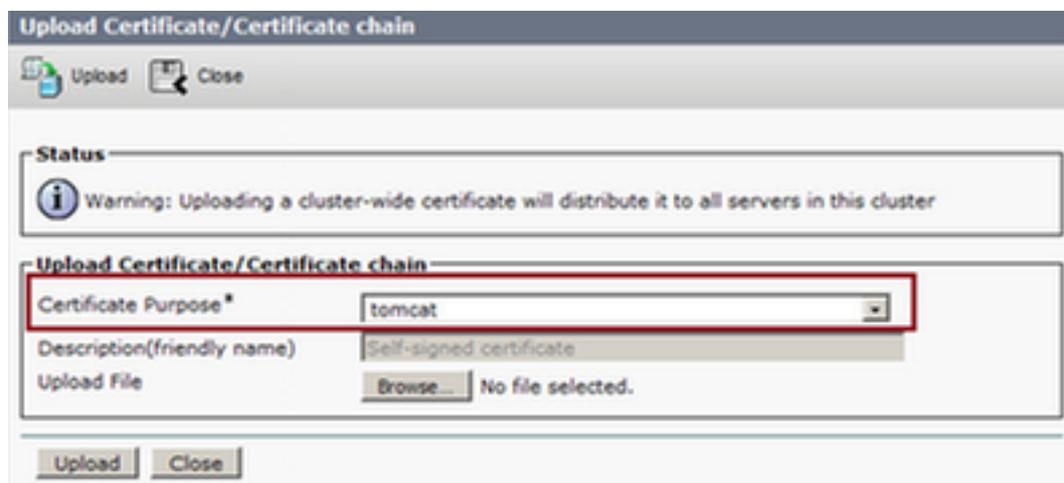
Paso 2. En la página de administración del sistema operativo de las Comunicaciones unificadas de Cisco del servidor primario, navegue al **Certificate Management (Administración de certificados) de la Seguridad > al certificado de la carga.**

Paso 3. De la lista desplegable del nombre del certificado, seleccione la Tomcat-confianza.

Paso 4. En el campo del archivo de la carga, el tecleo hojear y hojear al archivo de certificado intermedio.

Paso 5. 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 o el certificado del intermedio al servidor secundario de la delicadeza.

3. Cargue el certificado primario de la aplicación del servidor de la delicadeza tal y como se muestra en de la imagen:



Paso 1. De la lista desplegable del nombre del certificado, seleccione el tomcat.**Paso 2.** En el campo del archivo de la carga, el tecleo **hojea** y **hojea** al archivo de certificado de la aplicación.

Paso 3. Carga del tecleo para cargar el archivo.

4. Cargue el certificado secundario de la aplicación del servidor de Fineese.

En este paso siga el mismo proceso como se menciona en el paso 3 en el servidor secundario para su propio certificado de la aplicación.

5. Ahora usted puede recomenzar los servidores.

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

Servidores CUIIC (si se asume que ningún Certificados del intermedio presente en la Cadena de certificados)

1. Cargue el certificado raíz en el servidor primario CUIIC.

Paso 1. 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/a la Cadena de certificados de la carga.**

Paso 2. De la lista desplegable del nombre del certificado, seleccione la Tomcat-confianza.

Paso 3. En el campo del archivo de la carga, el tecleo **hojea** y **hojea** al archivo de certificado raíz.

Paso 4. 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 raíz al servidor secundario CUIIC.

2. Certificado primario de la aplicación del servidor de la carga CUIIC.

Paso 1. De la lista desplegable del nombre del certificado, seleccione el tomcat.

Paso 2. En el campo del archivo de la carga, el tecleo **hojea** y **hojea** al archivo de certificado de la aplicación.

Paso 3. Archivo de la carga del tecleo.

3. Certificado secundario de la aplicación del servidor de la carga CUIIC.
Siga el mismo proceso como se afirma en el paso (2) en el servidor secundario para su propio certificado de la aplicación
4. Recomience los servidores
Acceda el CLI en los servidores primarios y secundarios CUIIC y ingrese el comando **“reinicio de sistema del utils”** de recomenzar los servidores.
Note: Si la autoridad de CA proporciona la Cadena de certificados que incluye los Certificados intermedios entonces los pasos mencionados en los servidores de la delicadeza que la sección es aplicable a los servicios CUIIC también.

Servidores de datos vivos

1. Los pasos implicados en los servidores Vivo-DATA para cargar los Certificados son idénticos a la delicadeza o a los servidores CUIIC dependiendo de la Cadena de certificados.
2. Certificado raíz de la carga en el servidor primario Vivo-DATA.

Paso 1. 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.**

Paso 2. De la lista desplegable del nombre del certificado, seleccione la Tomcat-confianza.
Paso 3. En el campo del archivo de la carga, el tecleo **hojea** y hojea al archivo de certificado raíz.

Paso 4. Carga del tecleo.

3. Certificado intermedio de la carga en el servidor primario Vivo-DATA.

Paso 1. Los pasos en cargar el certificado intermedio son lo mismo que el certificado raíz tal y como se muestra en del paso 1.

Paso 2. 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.**

Paso 3. De la lista desplegable del nombre del certificado, seleccione la Tomcat-confianza.
Paso 4. En el campo del archivo de la carga, el tecleo **hojea** y hojea al archivo de certificado intermedio.

Paso 5. 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 o el certificado del intermedio al servidor secundario Vivo-DATA.

4. Certificado primario de la aplicación del servidor Vivo-DATA de la carga.

Paso 1. De la lista desplegable del nombre del certificado, seleccione el tomcat.

Paso 2. En el campo del archivo de la carga, el tecleo **hojea** y hojea al archivo de certificado de la aplicación.

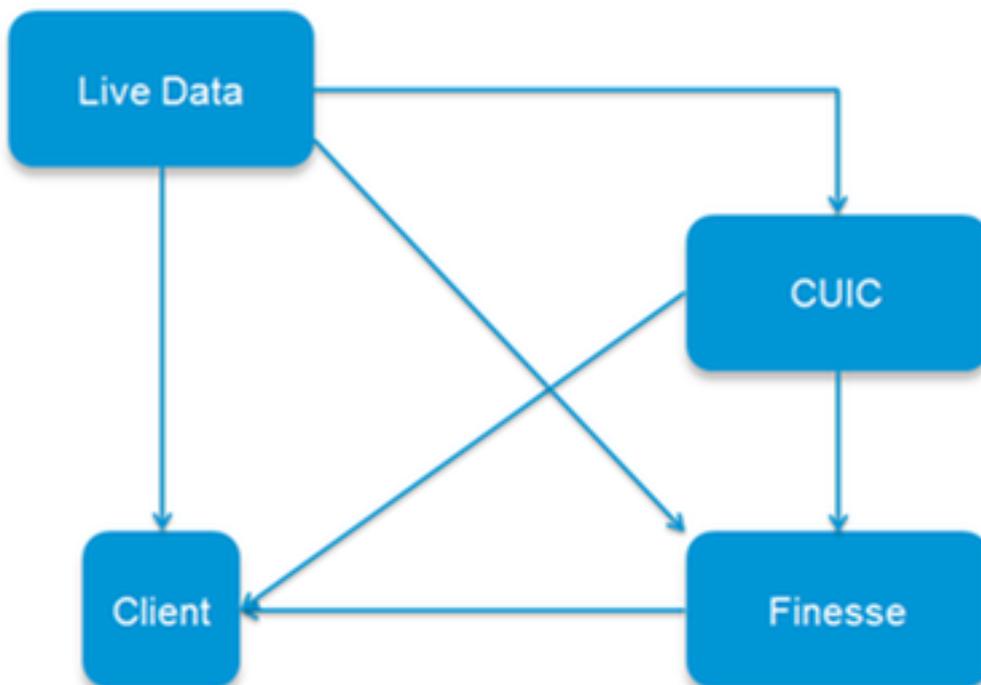
Paso 3. Carga del tecleo.

5. Certificado secundario de la aplicación del servidor Vivo-DATA de la carga.
Siga los mismos pasos como se mencionó anteriormente en (4) en el servidor secondary para su propio certificado de la aplicación.
6. Recomience los servidores
Acceda el CLI en los servidores primarios y secundarios de la delicadeza y ingrese el comando **“reinicio de sistema del utils”** de recomenzar los servidores.

Viven las dependencias del certificado de servidores de datos

Como servidores de datos vivos obran recíprocamente con CUIC y los servidores de la delicadeza, es dependencias del certificado entre estos servidores tal y como se muestra en de la imagen:

Certificate Dependencies



Con respecto al encadenamiento del certificado de CA del otro vendedor los Certificados de la raíz y del intermedio son lo mismo para todos los servidores en la organización. Como consecuencia para que el servidor de datos Live trabaje correctamente, usted tiene que asegurarse de que la delicadeza y los servidores CUIC tienen los Certificados de la raíz y del intermedio cargados correctamente en allí los envases de la Tomcat-confianza.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.