

Ejemplo de Configuración de Importación y Generación de LSC Firmados por CA de Terceros de CUCM

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Cargue el certificado raíz de la CA](#)

[Establecer CA sin conexión para emisión de certificado en extremo](#)

[Generar una solicitud de firma de certificado \(CSR\) para los teléfonos](#)

[Obtenga la CSR generada desde CUCM al servidor FTP \(o TFTP\)](#)

[Obtener el certificado del teléfono](#)

[Convertir formato .cer a .der](#)

[Comprimir los certificados \(.der\) en formato .tgz](#)

[Transferir el archivo .tgz al servidor SFTP](#)

[Importar el archivo .tgz al servidor de CUCM](#)

[Firmar el CSR con Microsoft Windows 2003 Certificate Authority](#)

[Obtener el certificado raíz de la CA](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Los certificados de función proxy de autoridad certificadora (CAPF) de importancia local (LSC) están firmados localmente. Sin embargo, es posible que necesite que los teléfonos utilicen LSC firmados por una autoridad de certificación (CA) de terceros. En este documento se describe un procedimiento que le ayudará a lograr este objetivo.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos de Cisco Unified Communication Manager (CUCM).

Componentes Utilizados

La información de este documento se basa en la versión 10.5(2) de CUCM; sin embargo, esta

función funciona a partir de la versión 10.0 y posteriores.

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). If your network is live, make sure that you understand the potential impact of any command.

Configurar

A continuación se indican los pasos de este procedimiento, que se detallan en su propia sección:

1. [Cargue el certificado raíz de la CA](#)
2. [Establecer CA sin conexión para emisión de certificado en extremo](#)
3. [Generar una solicitud de firma de certificado \(CSR\) para los teléfonos](#)
4. [Obtenga la CSR generada de Cisco Unified Communications Manager \(CUCM\) al servidor FTP](#)
5. [Obtener el certificado de teléfono de CA](#)
6. [Convertir formato .cer a .der](#)
7. [Comprimir los certificados \(.der\) en formato .tgz](#)
8. [Transferir el archivo .tgz al servidor FTP de Secure Shell \(SFTP\)](#)
9. [Importar el archivo .tgz al servidor de CUCM](#)
10. [Firmar el CSR con Microsoft Windows 2003 Certificate Authority](#)
11. [Obtener el certificado raíz de la CA](#)

Cargue el certificado raíz de la CA

1. Inicie sesión en la GUI web de administración del sistema operativo (SO) de Cisco Unified.
2. Vaya a Administración de certificados de seguridad.
3. Haga clic en Cargar certificado/cadena de certificado.
4. Elija CallManager-trust bajo Certificate Purpose.
5. Busque el certificado raíz de la CA y haga clic en Cargar.

Establecer CA sin conexión para emisión de certificado en extremo

1. Inicie sesión en la GUI web de administración de CUCM.
2. Vaya a System > Service Parameter.
3. Elija el servidor de CUCM y seleccione Cisco Certificate Authority Proxy Function para el servicio.

4. Seleccione Offline CA para emisión de certificado a terminal.

Generar una solicitud de firma de certificado (CSR) para los teléfonos

1. Inicie sesión en la GUI web de administración de CUCM.
2. Vaya a Teléfonos del dispositivo.
3. Elija el teléfono cuyo LSC debe estar firmado por la CA externa.
4. Cambie el perfil de seguridad del dispositivo por uno seguro (si no está presente, agregue un sistema en el perfil de seguridad del teléfono de seguridad).
5. En la página de configuración del teléfono, en la sección CAPF, elija Install/Upgrade para la operación de certificación. Complete este paso para todos los teléfonos cuyo LSC debe estar firmado por la CA externa. Debería ver Operación pendiente para el estado de operación del certificado.

Perfil de seguridad del teléfono (modelo 7962).

Ingrese el comando `utils capf csr count` en la sesión de Secure Shell (SSH) para confirmar si se genera un CSR. (Esta captura de pantalla muestra que se generó una CSR para tres teléfonos.)



Nota: El estado de operación del certificado en la sección CAPF del teléfono permanece en el estado Operación pendiente.

Obtenga la CSR generada desde CUCM al servidor FTP (o TFTP)

1. SSH en el servidor de CUCM.
2. Ejecute el comando `utils capf csr dump`. Esta captura de pantalla muestra el volcado que se está transfiriendo al FTP.

3. Abra el archivo de volcado con WinRAR y extraiga el CSR en su máquina local.

Obtener el certificado del teléfono

1. Envíe los CSR del teléfono a la CA.
2. La CA le proporciona un certificado firmado.



Nota: puede utilizar un servidor de Microsoft Windows 2003 como CA. El procedimiento para firmar el CSR con una entidad emisora de certificados de Microsoft Windows 2003 se explica más adelante en este documento.

Convertir formato .cer a .der

Si los certificados recibidos están en formato .cer, cámbielos a .der.

Comprimir los certificados (.der) en formato .tgz

Puede utilizar la raíz del servidor de CUCM (Linux) para comprimir el formato del certificado. También puede hacerlo en un sistema Linux normal.

1. Transfiera todos los certificados firmados al sistema Linux con el servidor SFTP.
2. Ingrese este comando para comprimir todos los certificados .der en un archivo .tgz.

```
<#root>
```

```
tar -zcvf
```

```
.tgz *.der
```

Transferir el archivo .tgz al servidor SFTP

Complete los pasos que se muestran en la captura de pantalla para transferir el archivo .tgz al servidor SFTP.

Importar el archivo .tgz al servidor de CUCM

1. SSH en el servidor de CUCM.
2. Ejecute el comando `utils capf cert import`.

Una vez que los certificados se importan correctamente, puede ver que el recuento CSR se convierte en cero.

Firmar el CSR con Microsoft Windows 2003 Certificate Authority

Esta información es opcional para Microsoft Windows 2003 - CA.

1. Autoridad de certificación abierta.
2. Haga clic con el botón secundario en la CA y navegue hasta Todas las tareas > Enviar nueva solicitud...
3. Seleccione el CSR y haga clic en Abrir. Haga esto para todos los CSR.

Todos los CSR abiertos se muestran en la carpeta Solicitudes pendientes.

4. Haga clic con el botón derecho en cada uno y navegue hasta Todas las tareas > Emitir para emitir certificados. Realice esta acción para todas las solicitudes pendientes.

5. Para descargar el certificado, elija Certificado emitido.
6. Haga clic con el botón secundario en el certificado y haga clic en Abrir.
7. Puede ver los detalles del certificado. Para descargar el certificado, seleccione la ficha Detalles y elija Copiar en archivo...
8. En el Asistente para exportación de certificados, elija DER binario codificado X.509 (.CER).
9. Asigne al archivo un nombre adecuado. Este ejemplo utiliza el formato <MAC>.cer.
10. Obtenga los certificados para otros teléfonos en la sección Certificado emitido con este procedimiento.

Obtener el certificado raíz de la CA

1. Autoridad de certificación abierta.
2. Complete los pasos que se muestran en esta captura de pantalla para descargar el root-CA.

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

1. Vaya a la página de configuración del teléfono.
2. En la sección CAPF, el estado de operación del certificado debe aparecer como Upgrade Success.

 Nota: Consulte [Generación e importación de LSC firmados por CA de terceros](#) para obtener más información.

Troubleshoot

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).