Ejemplo de configuración CA-firmado de tercera persona de la generación y de la importación CUCM LSC

Contenido

Introducción

Función de proxy del Certificate Authority (CAPF) localmente - local-se firman los Certificados significativos (LSC). Sin embargo, usted puede ser que requiera los teléfonos utilizar el Certificate Authority (CA) de tercera persona - los LSC firmados. Este documento describe un procedimiento que le ayude a alcanzar esto.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de Cisco unificó al administrador de la comunicación (CUCM).

Componentes Utilizados

La información en este documento se basa en la versión 10.5(2) CUCM; sin embargo, esta característica trabaja de la versión 10.0 y posterior.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Aquí están los pasos implicados en este procedimiento, que se detalla en su propia sección:

1. Cargue el certificado de la CA-raíz
2. Fije CA offline para el problema del certificado al punto final
3. Genere un pedido de firma de certificado (CSR) para los teléfonos
4. Consiga el CSR generado del administrador de las Comunicaciones unificadas de Cisco (CUCM) al servidor FTP
5. Consiga el certificado del teléfono de CA
6. Convierta .cer al formato .der
7. Comprima los Certificados (.der) al formato .tgz
8. Transferencia el archivo .tgz al servidor del shell seguro FTP (SFTP)
9. Importe el archivo .tgz al servidor CUCM
10. Firme el CSR con el Certificate Authority de Microsoft Windows 2003
11. Consiga el certificado raíz de CA

Cargue el certificado de la CA-raíz

1. El registro en Cisco unificó la red GUI de la administración del operating system (OS).
2. Navegue a la **Administración del Security Certificate**.
3. Haga clic el **certificado/la Cadena de certificados de la carga**.
4. Elija la CallManager-**confianza** bajo el propósito del certificado.
5. Hojee al certificado raíz de CA y haga clic la **carga**.

Fije CA offline para el problema del certificado al punto final

1. Registro en la red GUI de la administración CUCM.
2. Navegue al **sistema > al parámetro de servicio**.
3. Elija el servidor CUCM y seleccione la **función de proxy del Certificate Authority de Cisco**

para el servicio.

4. Seleccione **CA offline** para el problema del certificado al punto final.

Genere un pedido de firma de certificado (CSR) para los teléfonos

1. Registro en la red GUI de la administración CUCM.
2. Navegue a los **teléfonos del dispositivo**.
3. Elija el teléfono cuyo LSC se debe firmar por CA externo.
4. Cambie el perfil de seguridad del dispositivo asegurado (si no el presente, agrega un sistema en el perfil de seguridad del teléfono de la Seguridad).
5. En la página de la Configuración del teléfono, bajo sección del CAPF, elija **instalan/actualización** para la operación de la certificación. Complete este paso para todos los teléfonos cuyo LSC se deba firmar por CA externo. Usted debe ver la **operación pendiente** para el estado de la operación del certificado.

   Perfil de seguridad del teléfono (modelo 7962).

   Ingrese el **comando count csr del capf del utils** en la sesión del Secure Shell (SSH) para confirmar si un CSR está generado. (Esta captura de pantalla muestra que un CSR fue generado para tres teléfonos.)

   Note: Sigue habiendo el estado de la operación del certificado bajo sección del CAPF del teléfono en el estado **pendiente de la operación**.

Consiga el CSR generado del CUCM al servidor FTP (o TFTP)

1. SSH en el servidor CUCM.
2. Ejecute el **comando dump csr del capf del utils**. Esta captura de pantalla muestra el volcado que es transferido al FTP.
3. Abra el archivo de volcado con WinRAR y extraiga el CSR a su máquina local.

Consiga el certificado del teléfono

1. Envíe los CSR del teléfono a CA.

2. CA provee de usted un certificado firmado.

   Note: Usted puede utilizar un servidor de Microsoft Windows 2003 como CA. El procedimiento para firmar el CSR con un Microsft Windows 2003 CA se explica más adelante en este documento.

Convertido .cer al formato .der

Si los Certificados recibidos están en el formato de .cer, después retitúlelos a .der.

Comprima los Certificados (.der) al formato .tgz

Usted puede utilizar la raíz del servidor CUCM (Linux) para comprimir el formato del certificado. Usted puede también hacer esto en un sistema Linux normal.

1. Transferencia 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.

```
tar -zcvf <file_name>.tgz    *.der
```

Transferencia el archivo .tgz al servidor SFTP

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

Importe el archivo .tgz al servidor CUCM

1. SSH en el servidor CUCM.

2. Ejecute el **comando import CERT del capf del utils**.

   Una vez que los Certificados se importan con éxito, después usted puede ver la cuenta CSR hacer cero.

Firme el CSR con el Certificate Authority de Microsoft Windows 2003

Ésta es información opcional para Microsoft Windows 2003 - CA.

1. Abra las autoridades de certificación.

2. Haga clic con el botón derecho del ratón CA y navegue a **todas las tareas > someten la nueva petición…**

3. Seleccione el CSR y haga clic **abierto**. Haga esto para todos los CSR.

   Toda la visualización abierta CSR en la carpeta pendiente de las peticiones.

4. Haga clic con el botón derecho del ratón cada uno y navegue a **todas las tareas > problema** para publicar los Certificados. Haga esto para todas las peticiones pendientes.

5. Para descargar el certificado, elija el **certificado publicado**.

6. Haga clic con el botón derecho del ratón el certificado y haga clic **abierto**.

7. Usted puede ver a los detalles del certificado. Para descargar el certificado, seleccione la lengueta de los detalles y elija la **copia para clasifiar…**

8. En el Asisitente de la exportación del certificado, elija el **DER X.509 binario codificado (.CER)**.

9. Nombre el archivo algo apropiado. Este ejemplo utiliza el formato <MAC>.cer.

10. Consiga los Certificados para otros teléfonos bajo sección publicada del certificado con este procedimiento.

Consiga el certificado raíz de CA

1. Abra las **autoridades de certificación**.

2. Complete los pasos mostrados en esta captura de pantalla para descargar raíz CA.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

1. Vaya a la página de la Configuración del teléfono.

2. Bajo sección del CAPF, el estado de la operación del certificado debe visualizar como **éxito de la actualización**.

> **Note**: Refiérase generan e importan los LSC CA-firmados otro vendedor para más información.

Troubleshooting

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