Cómo descargar certificados de teléfonos IP de Cisco

Contenido

Introducción

Este documento describe el procedimiento para recuperar certificados de un teléfono IP de Cisco cuando el servicio Cisco Authority Proxy Function (CAPF) se ejecuta en el editor de Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Certificados SSL en el teléfono
- administración de CUCM
- Gestión de la interfaz de línea de comandos (CLI) en CUCM

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Unified Communications Manager (CUCM) versión 11.5.1.1900-26
- Teléfono IP Cisco 8811 - sip88xx.12-5-1SR1-4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El servicio CAPF debe estar activo en el editor de CUCM y el certificado CAPF en Administración de Cisco Unified OS debe estar actualizado.

Para los teléfonos IP de Cisco, hay dos alternativas de certificados instalados en ellos:

- MIC (certificado instalado por el fabricante)
- MIC y LSC (certificado de importancia local)

Los teléfonos se preinstalan con el certificado MIC y no se pueden eliminar ni regenerar. Además, el MIC no se puede utilizar una vez que la validez ha caducado. Los MIC son certificados de clave de 2048 bits firmados por la Autoridad de Certificación de Cisco.

El LSC posee la clave pública para el teléfono IP de Cisco, que está firmado por la clave privada CAPF de CUCM. No está instalado en el teléfono de forma predeterminada y este certificado es obligatorio para el teléfono para funcionar en modo seguro

Configurar

Paso 1. En CUCM, vaya a **Administración de Cisco Unified CM > Dispositivo > Teléfono**.

Paso 2. Busque y seleccione el teléfono desde el que desea recuperar los certificados.

Paso 3. En la página de configuración del teléfono, vaya a la sección **Información sobre la función de proxy de la autoridad de certificación (CAPF)**.

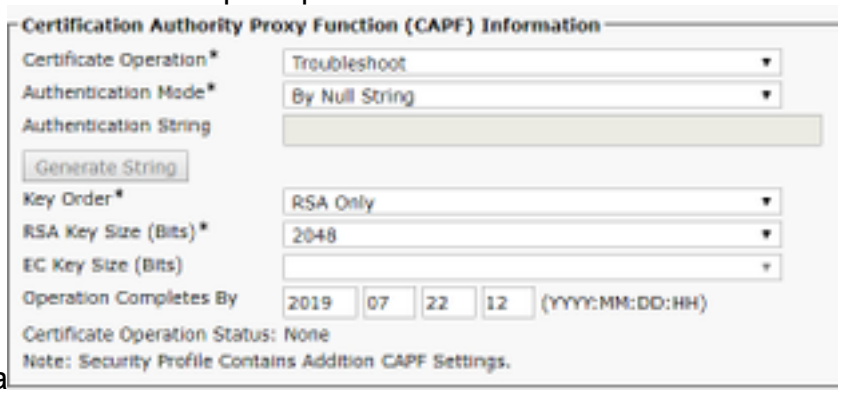
Paso 4. Como se muestra en la imagen, aplique estos parámetros:

Operación del certificado: Troubleshoot

Modo de autenticación: Por cadena nula

Tamaño de clave (bits): 1024

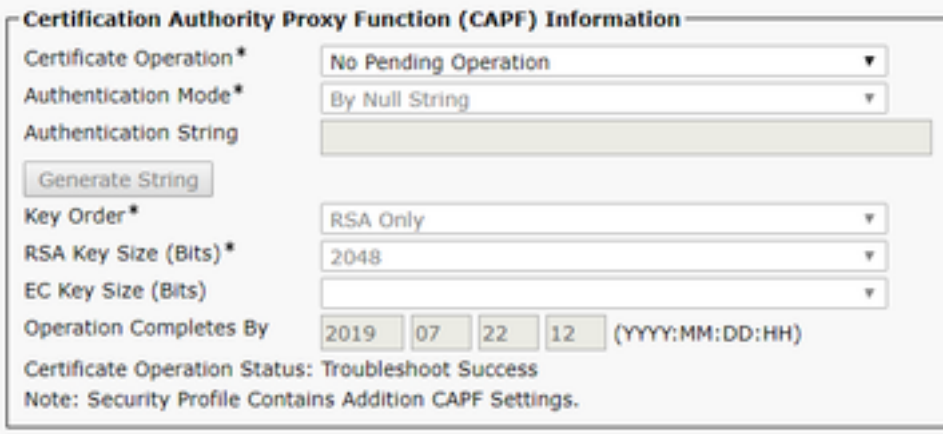
La operación se completa por: Fecha futura



Paso 5. Haga clic en **Guardar** y **Restablecer** el teléfono.

Paso 6. Una vez que el dispositivo se haya registrado nuevamente en el clúster de CUCM, asegúrese en la página de configuración del teléfono de que la operación de resolución de problemas se haya completado como se muestra en la

imagen:



Paso 7. Abra una sesión SSH para el servidor de CUCM Publisher y ejecute el comando para mostrar los certificados asociados al teléfono como se muestra en la imagen:

file list activelog /cm/trace/capf/sdi/SEP<MAC_Address>*

```
admin:file list activelog /cm/trace/capf/sdi/SEP*
SEPF87B204EED99-L1.cer                    SEPF87B204EED99-M1.cer
dir count = 0, file count = 2
admin:
```

Hay dos opciones para que se muestren los archivos:

Solo MIC: SEP<MAC_Address>-M1.cer

MIC y LSC: SEP<MAC_Address>-M1.cer y SEP<MAC_Address>-L1.cer

Paso 8. Para descargar los certificados, ejecute este comando: **file get activelog /cm/trace/capf/sdi/SEP<MAC_Address>***

Se necesita un servidor de protocolo seguro de transferencia de archivos (SFTP) para guardar el archivo como se muestra en la imagen

```
admin:file get activelog /cm/trace/capf/sdi/SEPF87B204EED99-M1.cer
Please wait while the system is gathering files info ...
 Get file: /var/log/active/cm/trace/capf/sdi/SEPF87B204EED99-M1.cer
done.
Sub-directories were not traversed.
Number of files affected: 1
Total size in Bytes: 1159
Total size in Kbytes: 1.1318359
Would you like to proceed [y/n]? y
SFTP server IP: 10.1.99.201
SFTP server port [22]:
User ID: alegarc2
Password: *********
Download directory: /

The authenticity of host '10.1.99.201 (10.1.99.201)' can't be established.
RSA key fingerprint is 33:83:bd:c7:8e:4d:1c:5a:b3:be:b2:e2:38:2b:fc:26.
Are you sure you want to continue connecting (yes/no)? yes
```

Información Relacionada

- Certificados del teléfono IP