

Herunterladen von Zertifikaten von Cisco IP-Telefonen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird das Verfahren zum Abrufen von Zertifikaten von einem Cisco IP-Telefon beschrieben, wenn der CAPF-Dienst (Cisco Authority Proxy Function) im CUCM-Publisher (Cisco Unified Communications Manager) ausgeführt wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SSL-Zertifikate im Telefon
- CUCM-Verwaltung
- CLI-Management (Command Line Interface) in CUCM

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Unified Communications Manager (CUCM) Version 11.5.1.11900-26
- Cisco IP-Telefon 8811 - sip88xx.12-5-1SR1-4

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Der CAPF-Service muss im CUCM-Publisher aktiv sein, und das CAPF-Zertifikat unter Cisco Unified OS-Administration muss aktuell sein.

Für Cisco IP-Telefone gibt es zwei Alternativen für Zertifikate, die auf diesen installiert sind:

- MIC (Manufacturer Installed Certificate)
- MIC und LSC (Locally Significant Certificate)

Telefone sind mit dem MIC-Zertifikat vorinstalliert und können weder gelöscht noch neu generiert werden. Außerdem kann das MIC nach Ablauf der Gültigkeit nicht mehr verwendet werden. MICs sind 2048-Bit-Schlüsselzertifikate, die von der Cisco Certificate Authority signiert werden.

Das LSC verfügt über den öffentlichen Schlüssel für das Cisco IP-Telefon, der vom privaten CUCM-CAPF-Schlüssel signiert wird. Es ist nicht standardmäßig auf dem Telefon installiert, und dieses Zertifikat ist für das Telefon erforderlich, um im sicheren Modus zu arbeiten.

Konfigurieren

Schritt 1: Navigieren Sie in CUCM zu Cisco Unified CM Administration > Device > Phone (Cisco Unified CM-Verwaltung > Gerät > Telefon).

Schritt 2: Suchen Sie das Telefon, von dem Sie Zertifikate abrufen möchten, und wählen Sie es aus.

Schritt 3: Navigieren Sie auf der Seite für die Telefonkonfiguration zum Abschnitt Certification Authority Proxy Function (CAPF) Information (CAPF-Informationen).

Schritt 4: Wenden Sie die folgenden Parameter an (siehe Abbildung):

Zertifikatvorgang: Fehlerbehebung

Authentifizierungsmodus: Nach Nullzeichenfolge

Schlüsselgröße (Bit): 1024

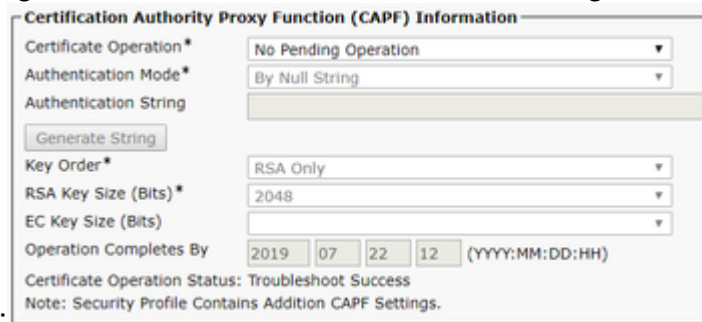
Vorgang abgeschlossen von: Termin für die Zukunft

The screenshot shows the 'Certification Authority Proxy Function (CAPF) Information' configuration page. The settings are as follows:

Certificate Operation*	Troubleshoot
Authentication Mode*	By Null String
Authentication String	
Generate String	Generate String
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	
Operation Completes By	2019 07 22 12 (YYYY:MM:DD:HH)
Certificate Operation Status:	None
Note: Security Profile Contains Addition CAPF Settings.	

Schritt 5. Klicken Sie auf Speichern und Zurücksetzen des Telefons.

Schritt 6: Nachdem das Gerät wieder im CUCM-Cluster registriert wurde, stellen Sie auf der Seite für die Telefonkonfiguration sicher, dass die Fehlerbehebung wie in der Abbildung dargestellt



abgeschlossen ist:

Schritt 7: Öffnen Sie eine SSH-Sitzung für den CUCM Publisher-Server, und führen Sie den Befehl aus, um die dem Telefon zugeordneten Zertifikate aufzulisten, wie im Bild gezeigt:

Dateiliste `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:
```

Es gibt zwei Optionen für die aufzulistenden Dateien:

Nur MIC: `SEP<MAC_Address>-M1.cer`

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

Schritt 8: Führen Sie den folgenden Befehl aus, um die Zertifikate herunterzuladen: Datei `get activelog /cm/trace/capf/sdi/SEP<MAC_Address>*`

Ein SFTP-Server (Secure File Transfer Protocol) ist erforderlich, um die Datei wie im Bild dargestellt zu speichern

```
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
```

Zugehörige Informationen

- [IP-Telefonzertifikate](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.