

Hoe Certificaten te downloaden van Cisco IP Phones

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt de procedure beschreven voor het ophalen van certificaten van een Cisco IP Phone wanneer de Cisco Authority Proxy Function (CAPF)-service wordt uitgevoerd in de Cisco Unified Communications Manager (CUCM)-uitgever.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SSL-certificaten in de telefoon
- Toediening van CUCM
- Command Line Interface (CLI)-beheer in CUCM

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De CAPF-service moet actief zijn in de CUCM-uitgever en het CAPF-certificaat onder Cisco Unified OS Administration moet up-to-date zijn.

Voor Cisco IP-telefoons zijn er twee alternatieven voor certificaten die erop zijn geïnstalleerd:

- MIC (door de fabrikant geïnstalleerd certificaat)
- MIC en LSC (lokaal significant certificaat)

Telefoons zijn vooraf geïnstalleerd met het MIC-certificaat en kunnen niet worden verwijderd of opnieuw worden gegenereerd. Ook kan MIC niet worden gebruikt zodra de geldigheid is verlopen. MIC's zijn 2048-bits sleutelcertificaten die zijn ondertekend door de Cisco Certificate Authority.

De LSC beschikt over de publieke sleutel voor de Cisco IP-telefoon, die is ondertekend door de CUCM CAPF-privésleutel. Het is niet standaard op de telefoon geïnstalleerd en dit certificaat is vereist voor de telefoon om in de veilige modus te werken

Configureren

Stap 1. Navigeer in CUCM naar Cisco Unified CM Administration > Apparaat > Telefoon.

Stap 2. Zoek en selecteer de telefoon van welke certificaten u wilt ophalen.

Stap 3. Navigeer op de configuratiepagina van de telefoon naar de sectie Gegevens van de proxyfunctie van de certificeringsinstantie (CAPF).

Stap 4. Zoals weergegeven in de afbeelding, past u deze parameters toe:

Certificaatbewerking: problemen oplossen

verificatiemodus: op null-tekenreeks

Sleutelgrootte (bits): 1024

Certification Authority Proxy Function (CAPF) Information

Certificate Operation *	Troubleshoot
Authentication Mode *	By Null String
Authentication String	
Generate String	
Key Order *	RSA Only
RSA Key Size (Bits) *	2048
EC Key Size (Bits)	1024
Operation Completes By	2019 07 22 12 (YYYY:MM:DD:HH)
Certificate Operation Status:	None
Note: Security Profile Contains Addition CAPF Settings.	

Bewerking voltooid op: Datum in de toekomst

Stap 5. Klik op Opslaan en Reset de telefoon.

Stap 6. Zodra dat apparaat is geregistreerd in het CUCM-cluster, moet u op de pagina voor de configuratie van de telefoon controleren of de probleemoplossingsbewerking is voltooid, zoals in de afbeelding wordt weergegeven:

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	No Pending Operation
Authentication Mode*	By Null String
Authentication 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: Troubleshoot Success	
Note: Security Profile Contains Addition CAPF Settings.	

Stap 7. Open een SSH-sessie voor de CUCM Publisher-server en voer de opdracht uit om de certificaten te vermelden die aan de telefoon zijn gekoppeld, zoals weergegeven in de afbeelding:

bestandslijst actief log /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:
```

Er zijn twee opties voor de bestanden die moeten worden vermeld:

Alleen MIC: SEP<MAC_Address>-M1.cer

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

Stap 8. Voer de volgende opdracht uit om de certificaten te downloaden: bestand activelog /cm/trace/capf/sdi/SEP<MAC_Address>*

Een Secure File Transfer Protocol (SFTP)-server is vereist om het bestand op te slaan, zoals in de afbeelding wordt weergegeven

```
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
```

Gerelateerde informatie

- [IP-telefooncertificaten](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.