

如何從Cisco IP電話下載證書

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[相關資訊](#)

簡介

本檔案將說明在Cisco Unified Communications Manager(CUCM)發佈器中執行Cisco Authority Proxy Function(CAPF)服務時從Cisco IP電話檢索憑證的程式。

必要條件

需求

思科建議您瞭解以下主題：

- 電話中的SSL證書
- CUCM管理
- CUCM中的命令列介面(CLI)管理

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科整合通訊管理員(CUCM)版本11.5.1.11900-26
- Cisco IP電話8811 - sip88xx.12-5-1SR1-4

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

CAPF服務在CUCM發佈器中必須處於活動狀態，Cisco Unified OS Administration下的CAPF證書必須是最新的。

對於Cisco IP電話，其上安裝兩種備用證書：

- MIC（製造商安裝的證書）
- MIC和LSC（本地有效證書）

電話預裝有MIC證書，無法刪除，也無法重新生成。此外，一旦有效性過期，將無法使用MIC。MIC是由思科證書頒發機構簽名的2048位金鑰證書。

LSC擁有思科IP電話的公鑰，該公鑰由CUCM CAPF私鑰簽名。預設情況下，它未安裝在電話上，電話需要此證書才能在安全模式下運行

設定

步驟1.在CUCM中，導航至Cisco Unified CM Administration > Device > Phone。

步驟2.查詢並選擇要從中檢索證書的電話。

步驟3.在電話配置頁面中，導航到證書頒發機構代理功能(CAPF)資訊部分。

步驟4.如圖所示，應用以下引數：

證書操作：疑難排解

身份驗證模式：按Null字串

金鑰大小 (位)：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)

Operation Completes By 2019 07 22 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

操作完成者：未來的日期

步驟5.按一下Save和Reset電話。

步驟6.裝置註冊回CUCM集群後，在電話配置頁中確保故障排除操作已完成，如下圖所示

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.

步驟7.開啟CUCM Publisher伺服器的SSH會話，然後運行命令以列出與電話關聯的證書，如下圖所示：

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:█
```

要列出的檔案有兩個選項：

僅MIC:SEP<MAC_Address>-M1.cer

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

步驟8.若要下載憑證，請運行此命令：`file get activelog /cm/trace/capf/sdi/SEP<MAC_Address>*`

若要儲存檔案，需要安全檔案傳輸通訊協定(SFTP)伺服器，如下圖所示

```
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
```

相關資訊

- [IP電話證書](#)