

Cisco IP Phone에서 인증서를 다운로드하는 방법

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[관련 정보](#)

소개

이 문서에서는 CUCM(Cisco Unified Communications Manager) 게시자에서 Cisco CAPF(Authority Proxy Function) 서비스가 실행될 때 Cisco IP Phone에서 인증서를 검색하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 전화기의 SSL 인증서
- CUCM 관리
- CUCM의 CLI(Command Line Interface) 관리

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

CAPF 서비스는 CUCM 게시자에서 활성화되어야 하며 Cisco Unified OS Administration(Cisco Unified OS 관리)의 CAPF 인증서가 최신 버전이어야 합니다.

Cisco IP Phone에는 두 가지 대체 인증서가 설치되어 있습니다.

- MIC(제조업체가 설치한 인증서)
- MIC 및 LSC(Locally Significant Certificate)

전화기는 MIC 인증서와 함께 미리 설치되어 있으며 삭제하거나 재생성할 수 없습니다. 또한 MIC는 유효기간이 만료된 후에는 사용할 수 없습니다. MIC는 Cisco Certificate Authority에서 서명한 2048비트 키 인증서입니다.

LSC는 CUCM CAPF 개인 키로 서명된 Cisco IP Phone의 공개 키를 보유합니다. 기본적으로 전화기에 설치되어 있지 않으며 보안 모드로 작동하기 위해 전화기에 이 인증서가 필요합니다

구성

1단계. CUCM에서 Cisco Unified CM Administration(Cisco Unified CM 관리) > Device(디바이스) > Phone(전화기)으로 이동합니다.

2단계. 인증서를 검색할 전화기를 찾아 선택합니다.

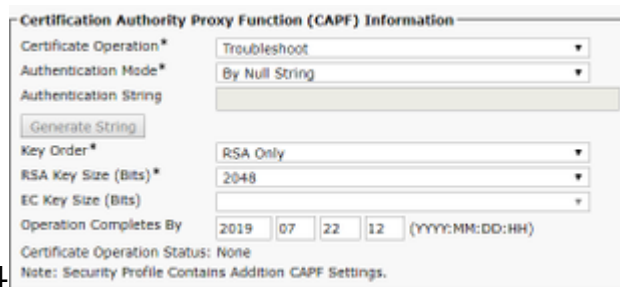
3단계. 전화기 컨피그레이션 페이지에서 CAPF(Certification Authority Proxy Function) 정보 섹션으로 이동합니다.

4단계. 그림과 같이 다음 매개변수를 적용합니다.

인증서 작업: 문제 해결

인증 모드: Null 문자열

키 크기(비트): 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.	

작업 완료자: 미래의 날짜

5단계. Save and Reset the phone을 클릭합니다.

6단계. 해당 장치가 CUCM 클러스터에 다시 등록되면 전화기 컨피그레이션 페이지에서 이미지에 표시된 대로 문제 해결 작업이 완료되었는지 확인합니다.

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.	

7단계. CUCM 게시자 서버에 대한 SSH 세션을 열고 이 명령을 실행하여 이미지에 표시된 대로 전화기와 연결된 인증서를 나열합니다.

파일 목록 `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:
```

나열할 파일에는 두 가지 옵션이 있습니다.

MIC만: `SEP<MAC_Address>-M1.cer`

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

8단계. 인증서를 다운로드하려면 다음 명령을 실행합니다. 파일 `get activelog /cm/trace/capf/sdi/SEP<MAC_Address>*`

이미지에 표시된 대로 파일을 저장하려면 SFTP(Secure File Transfer Protocol) 서버가 필요합니다

```
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
```

관련 정보

- [IP Phone 인증서](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.