CUCM에서 암호화된 컨피그레이션 기능 활성화

목차

소개

이 문서에서는 Cisco CUCM(Unified Communications Manager)에서 암호화된 컨피그레이션 전화 파일의 사용에 대해 설명합니다.

배경 정보

전화기에 암호화된 컨피그레이션 파일을 사용하는 것은 CUCM에서 사용할 수 있는 선택적 보안 기능입니다.

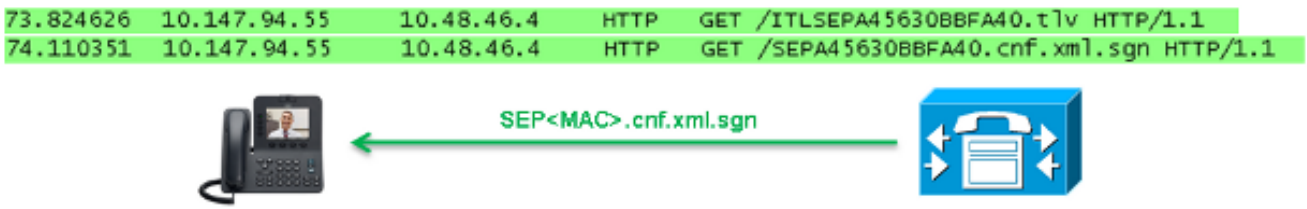
CAPF(Certificate Authority Proxy Function) 인증서 정보가 ITL(Identity Trust List) 파일에 포함되어 있으므로 이 기능이 제대로 작동하려면 혼합 모드에서 CUCM 클러스터를 실행할 필요가 없습니다.

> **참고:**모든 CUCM 버전 8.X 이상에 대한 기본 위치입니다.버전 8.X 이전 CUCM 버전의 경우 이 기능을 사용하려면 클러스터가 혼합 모드에서 실행되어야 합니다.

암호화된 구성 기능 개요

이 섹션에서는 CUCM 내에서 암호화된 컨피그레이션 전화 파일이 사용될 때 발생하는 프로세스에 대해 설명합니다.

이 기능을 활성화하고 전화기를 재설정하고 컨피그레이션 파일을 다운로드할 때 **.cnf.xml.sgn** 확장명으로 파일에 대한 요청을 받습니다.



그러나 CUCM에서 암호화된 컨피그레이션 기능을 활성화한 후에는 TFTP 서비스가 더 이상 **.cnf.xml.sgn** 확장자가 있는 전체 컨피그레이션 파일을 생성하지 않습니다.대신 다음 예와 같이 부분 구성 파일을 생성합니다.

참고:이 방법을 처음 사용하는 경우 전화기는 컨피그레이션 파일의 전화 인증서의 MD5 해시를 LSC(Locally Significant Certificate) 또는 MIC(Manufacturing Installed Certificates)의 MD5 해시와 비교합니다.

```
HTTP/1.1 200 OK
Content-length: 759
Cache-Control: no-store
Content-type: */*
<fullConfig>False</fullConfig>
<loadInformation>SIP75.9-3-1SR2-1S</loadInformation>
<ipAddressMode>0</ipAddressMode>
<capfAuthMode>0</capfAuthMode>
<capfList>
<capf>
<phonePort>3804</phonePort>
<processNodeName>10.48.46.4</processNodeName>
</capf>
</capfList>
```

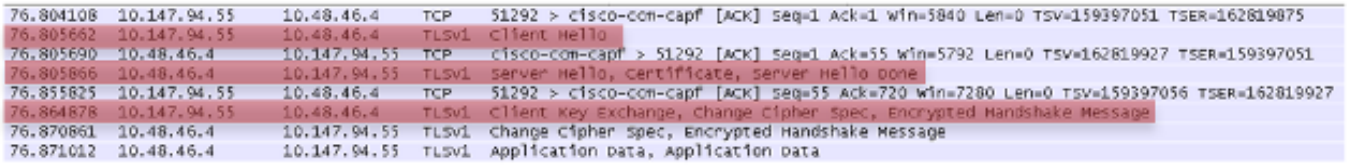
```
</device>
```

전화기에서 문제를 식별한 경우 CAPF 인증 모드가 *인증 문자열별*과 일치하지 않는 한 CAPF를 사용하여 세션을 시작하려고 합니다. 이 경우 문자열을 수동으로 입력해야 합니다.전화기에서 식별할 수 있는 몇 가지 문제는 다음과 같습니다.

- 해시가 일치하지 않습니다.
- 전화기에 인증서가 없습니다.
- MD5 값은 비어 있습니다(이전 예와 같이).

참고:기본적으로 전화기는 포트 3804에서 CAPF 서비스에 대한 TLS(Transport Layer Security) 세션을 시작합니다.

전화기에 대해 CAPF 인증서를 알고 있어야 하므로 ITL 파일 또는 CTL(Certificate Trust List) 파일에 포함되어야 합니다(클러스터가 혼합 모드에서 실행되는 경우).



CAPF 통신이 설정되면 전화기에서 사용되는 LSC 또는 MIC에 대한 정보를 CAPF에 보냅니다. 그런 다음 CAPF는 LSC 또는 MIC에서 전화 공개 키를 추출하고 MD5 해시를 생성하며 공개 키 및 인증서 해시의 값을 CUCM 데이터베이스에 저장합니다.

```
admin:run sql select md5hash,name from device where name='SEPA45630BBFA40'
md5hash name
================================ ===============
6e566143c1c14566c9da943d949a79c8 SEPA45630BBFA40
```

공개 키가 데이터베이스에 저장되면 전화기가 재설정되고 새 구성 파일을 요청합니다.전화기에서 다시 한 번 cnf.**xml.sgn** 확장자로 컨피그레이션 파일**을 다운로드하려고** 시도합니다.


```
128.078706 10.147.94.55     10.48.46.4     HTTP   GET /SEPA45630BBFA40.cnf.xml.sgn HTTP/1.1
```

```
HTTP/1.1 200 OK
Content-length: 759
Cache-Control: no-store
Content-type: */*
<fullConfig>False</fullConfig>
<loadInformation>SIP75.9-3-1SR2-1S</loadInformation>
<ipAddressMode>0</ipAddressMode>
<capfAuthMode>0</capfAuthMode>
<capfList>
<capf>
<phonePort>3804</phonePort>
<processNodeName>10.48.46.4</processNodeName>
</capf>
</capfList>
```

```
</device>
```

전화기에서 cerHash를 다시 비교하며, 문제가 발견되지 않으면 암호화된 구성 파일을 **.cnf.xml.enc.sgn** 확장자**와** 다운로드합니다.


```
130.708816 10.147.94.55     10.48.46.4     HTTP   GET /SEPA45630BBFA40.cnf.xml.enc.sgn HTTP/1.1
```

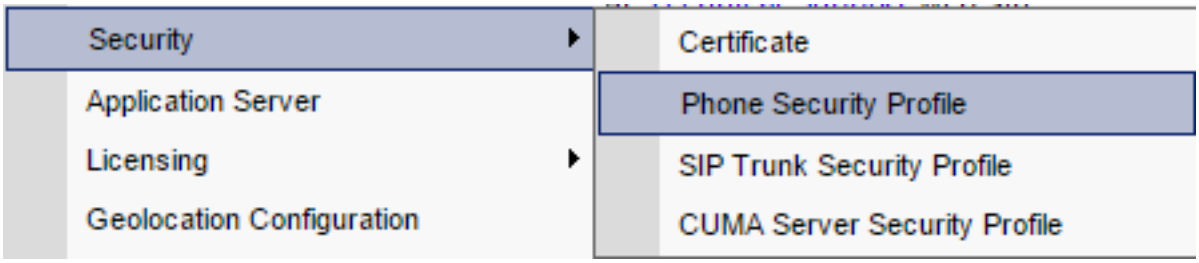
```
............c..)CN=cucm85;OU=It;O=Cisco;L=KRK;ST=PL;C=PL....Z.........)CN=cucm85;
OU=It;O=Cisco;L=KRK;ST=PL;C=PL...........
.........C.<...Y6.Lh.|(..w+..,.0.a.&.
O.........V....T...Z..R^..f....|.=.e.@...5...........G...[.........n.........=
.A..H.(....Z...{.!%[.. SEPA45630BBFA40.cnf.xml.enc.sgn....R.DD..M...........
Uu.C..@...........
..................m.b.......6y ..x.^b..-8.^..^'.4.<Wb.n.....5...we.0@..g..
V7.,..r.9
```

```
Qs>..).w....pt/...}A.']
.r.t%G..d_.;u.rEI.pr.F
.....M..r...o.N
.=..g.^P....Pz....J..E.S...d|Z).....J..&..I....7.r..g8.{f..o.....:.~..U...5G+V.
[...]
```

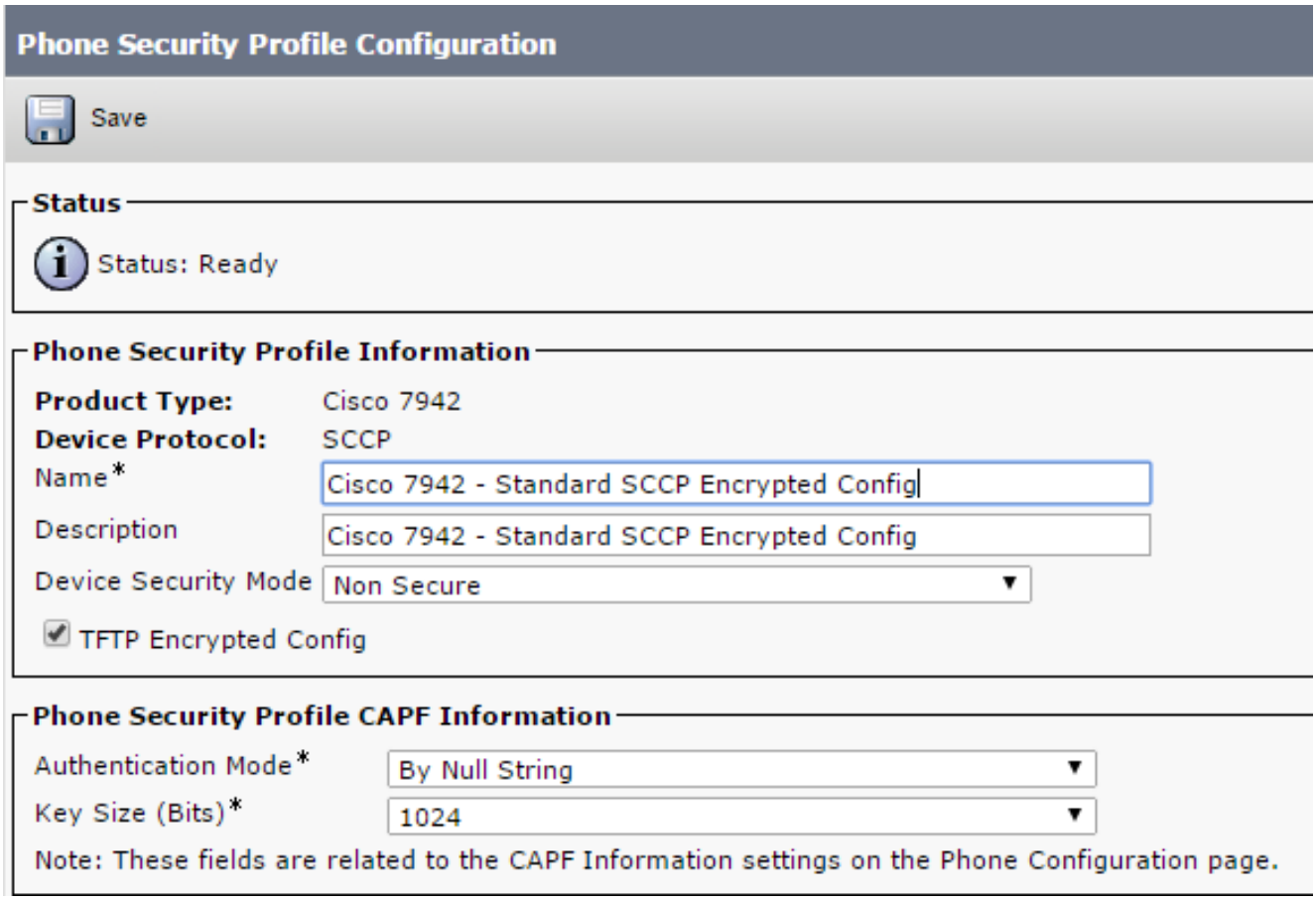
암호화된 구성 기능 사용

암호화된 컨피그레이션 전화 파일을 활성화하려면 새(또는 현재) Phone Security Profile(전화기 보안 프로파일 수정)을 생성하여 전화기에 할당해야 합니다.CUCM에서 암호화된 컨피그레이션 기능을 활성화하려면 다음 단계를 완료합니다.

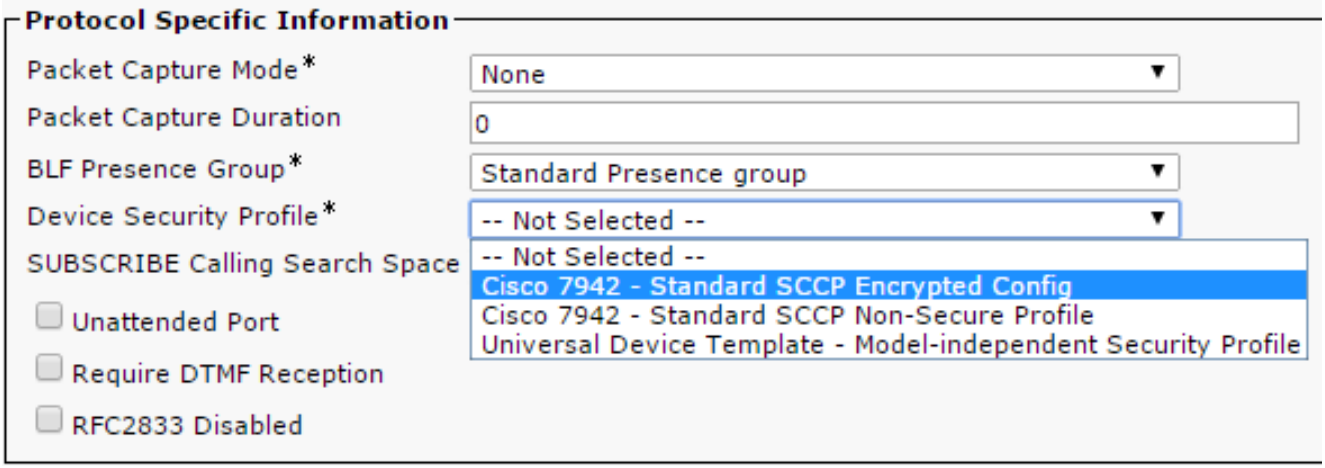
1. CUCM Administration(CUCM 관리) 페이지에 로그인하여 System(시스템) **> Security(보안) > Phone Security Profile(Phone Security 프로파일)로 이동합니다**.



2. 현재 Phone Security Profile을 복사하거나 새 Phone Security Profile을 생성하고 TFTP Encrypted **Config** 확인란을 선택합니다.



3. 전화기에 프로파일을 할당합니다.



문제 해결

암호화된 컨피그레이션 기능과 관련하여 시스템 문제를 해결하려면 다음 단계를 완료하십시오.

1. CAPF 서비스가 활성 상태이고 CUCM 클러스터의 게시자 노드에서 제대로 실행되는지 확인합니다.

2. 부분 구성 파일을 다운로드하고 전화기에서 CAPF 서비스의 포트 및 IP 주소에 연결할 수 있는지 확인합니다.

3. 포트 3804에서 게시자 노드에 대한 TCP 통신을 확인합니다.

4. 앞서 설명한 SQL(Structured Query Language) 명령을 실행하여 CAPF 서비스에 전화기에서 사용되는 LSC 또는 MIC에 대한 정보가 있는지 확인합니다.

5. 문제가 계속되면 시스템에서 추가 정보를 수집해야 할 수 있습니다.전화기를 다시 시작하고 다음 정보를 수집합니다.

   전화 콘솔 로그Cisco TFTP 로그Cisco CAPF 로그CUCM 및 전화기에서 패킷 캡처

CUCM 및 전화기에서 패킷 캡처를 실행하는 방법에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- TAC SR에 대한 CUCM 8.6.2에서 CUCM 추적 수집
- Unified Communications Manager 어플라이언스 모델의 패킷 캡처
- Cisco IP Phone에서 패킷 캡처 수집

로그 및 패킷 캡처에서 이전 섹션에서 설명한 프로세스가 제대로 작동하는지 확인해야 합니다.구체적으로 다음을 확인합니다.

- 전화기는 올바른 CAPF 정보가 포함된 부분 구성 파일을 다운로드합니다.
- TLS를 통해 CAPF 서비스에 연결되며 LSC 또는 MIC에 대한 정보가 데이터베이스에서 업데이트됩니다.
- 전화기가 전체 암호화된 구성 파일을 다운로드합니다.