

# De functie Encrypt Configuration op CUCM inschakelen

## Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Overzicht van versleutelde configuratie](#)

[Functie versleutelde configuratie inschakelen](#)

[Problemen oplossen](#)

## Inleiding

Dit document beschrijft het gebruik van gecodeerde configuratietelefoonbestanden in Cisco Unified Communications Manager (CUCM).

## Achtergrondinformatie

Het gebruik van gecodeerde configuratiebestanden voor telefoons is een optionele beveiligingsfunctie die beschikbaar is in CUCM.

U hoeft het CUCM-cluster niet in gemengde modus te uitvoeren om deze functie goed te laten functioneren, aangezien de certificaatinformatie (CAPF)-certificaat in het ITL-bestand (Identity Trust List) bevat.

**Opmerking:** Dit is de standaardlocatie voor alle CUCM versies 8.X en hoger. Voor CUCM-versies voorafgaand aan versie 8.X moet u ervoor zorgen dat het cluster in gemengde modus draait als u deze optie wilt gebruiken.

## Overzicht van versleutelde configuratie

In deze sectie wordt het proces beschreven dat plaatsvindt wanneer versleutelde configuratiebestanden in de CUCM worden gebruikt.

Wanneer u deze optie activeert, de telefoon opnieuw instelt en het configuratiebestand downloaden, ontvangt u een verzoek voor het bestand met een extensie van **.cnf.xml.sgn**:

```
73.824626 10.147.94.55 10.48.46.4 HTTP GET /ITLSEPA45630BBFA40.tlv HTTP/1.1
74.110351 10.147.94.55 10.48.46.4 HTTP GET /SEPA45630BBFA40.cnf.xml.sgn HTTP/1.1
```



Nadat de versleutelde configuratiefunctie op het CUCM is ingeschakeld, genereert de TFTP-

service echter niet langer een volledig configuratiebestand met de extensie **.cnf.xml.sgn**. In plaats daarvan genereert het het gedeeltelijke configuratiebestand, zoals in het volgende voorbeeld wordt getoond.

**Opmerking:** Wanneer u deze methode voor het eerst gebruikt, wordt in de telefoon de MD5-hash van het telefooncertificaat in het configuratiebestand vergeleken met de MD5-hash van het plaatselijk significante certificaat (LSC) of de Manufacturing Geïnstalleerde certificaten (MIC).

```
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>
```

Als de telefoon een probleem identificeert, probeert het een sessie met CAPF te openen, tenzij de CAPF authenticatiemodus aansluit *door Verificatiestings*, in welk geval u de string handmatig moet invoeren. Hier zijn een paar problemen die de telefoon zou kunnen identificeren:

- De hash komt niet overeen.
- De telefoon bevat geen certificaat.
- De MD5 waarde is leeg (zoals in het vorige voorbeeld).



**Opmerking:** De telefoon start een TLS-sessie (Transport Layer Security) naar de CAPF-service op poort 3804 standaard.

Het CAPF-certificaat moet bekend zijn voor de telefoon, dus moet het in het ITL-bestand of het CTL-bestand (certificaatlijst) worden opgenomen (als het cluster in gemengde modus loopt).

76.804108	10.147.94.55	10.48.46.4	TCP	51292 > cisco-con-capf [ACK] seq=1 ack=1 win=5840 Len=0 Tsv=159397051 Tser=162819875
76.805662	10.147.94.55	10.48.46.4	TLSv1	Client Hello
76.805690	10.48.46.4	10.147.94.55	TCP	cisco-con-capf > 51292 [ACK] seq=1 ack=55 win=5792 Len=0 Tsv=162819927 Tser=159397051
76.805866	10.48.46.4	10.147.94.55	TLSv1	server Hello, certificate, server Hello done
76.855825	10.147.94.55	10.48.46.4	TCP	51292 > cisco-con-capf [ACK] seq=55 ack=720 win=7280 Len=0 Tsv=159397056 Tser=162819927
76.864678	10.147.94.55	10.48.46.4	TLSv1	Client Key Exchange, change cipher spec, Encrypted Handshake Message
76.870861	10.48.46.4	10.147.94.55	TLSv1	change cipher spec, Encrypted Handshake Message
76.871012	10.48.46.4	10.147.94.55	TLSv1	Application data, Application data

Nadat de CAPF-communicatie tot stand is gebracht, stuurt de telefoon informatie naar CAPF over de LSC of MIC die wordt gebruikt. CAPF haalt dan de openbare sleutel van de LSC of MIC uit, genereert een MD5 hash en slaat de waarden voor de openbare sleutel en de certificaathash in de CUCM database op.

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

```
md5hash name
```

```
=====
6e566143c1c14566c9da943d949a79c8 SEPA45630BBFA40
```

Nadat de openbare sleutel in het gegevensbestand wordt opgeslagen, stelt de telefoon terug en verzoekt om een nieuw configuratiebestand. De telefoon probeert het configuratiebestand opnieuw te downloaden in combinatie met de extensie **cnf.xml.sgn**.



```
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>
```

De telefoon vergelijkt de cerHash opnieuw en als het probleem niet wordt gedetecteerd, downloads het gecodeerde configuratiebestand met de bestandsextensie **cnf.xml.enc.sgn**.



```
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.
[...]
```

## Functie versleutelde configuratie inschakelen


Om de gecodeerde telefoonbestanden van de configuratie in te schakelen moet u een nieuw (of huidige) telefoonbeveiligingsprofiel maken en aan de telefoon toewijzen. Voltooi deze stappen om de versleutelde configuratie optie op het CUCM in te schakelen:

1. Meld u aan bij de CUCM-beheerpagina en navigeer naar **system > Beveiliging > Telefonische beveiligingsprofiel**:

Security	Certificate
Application Server	Phone Security Profile
Licensing	SIP Trunk Security Profile
Geolocation Configuration	CUMA Server Security Profile


2. Kopieert een actueel profiel of maakt een nieuw telefoonbeveiligingsprofiel en controleer het vakje **TFTP Encrypted Config**:

### Phone Security Profile Configuration

 Save

---

**Status**

 Status: Ready

---

**Phone Security Profile Information**

**Product Type:** Cisco 7942  
**Device Protocol:** SCCP  
**Name\***   
**Description**   
**Device Security Mode**   
 TFTP Encrypted Config

---

**Phone Security Profile CAPF Information**

**Authentication Mode\***   
**Key Size (Bits)\***   
 Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

3. Geef het profiel aan de telefoon toe:

**Protocol Specific Information**

**Packet Capture Mode\***   
**Packet Capture Duration**   
**BLF Presence Group\***   
**Device Security Profile\***   
**SUBSCRIBE Calling Search Space**   
 Unattended Port  
 Require DTMF Reception  
 RFC2833 Disabled

**Device Security Profile\*** dropdown menu options:  
 -- Not Selected --  
 Cisco 7942 - Standard SCCP Encrypted Config  
 Cisco 7942 - Standard SCCP Non-Secure Profile  
 Universal Device Template - Model-independent Security Profile

## Problemen oplossen

Voltooi deze stappen om systeemproblemen met betrekking tot de versleutelde configuratie te verhelpen:

1. Zorg ervoor dat de CAPF-dienst actief is en correct op het Uitgevers-knooppunt in de CUCM-cluster draait.
2. Download het gedeeltelijke configuratiebestand en controleer of het poort- en IP-adres van de CAPF-service bereikbaar is vanaf de telefoon.

3. Controleer de TCP-communicatie op poort 3804 naar de Uitgeverij.
4. Start de eerder genoemde opdracht Structured Query Language (SQL) om te controleren of de CAPF-service informatie heeft over de LSC of MIC die door de telefoon wordt gebruikt.
5. Als het probleem zich blijft voordoen, moet u mogelijk aanvullende informatie bij het systeem verzamelen. Start de telefoon opnieuw en verzamel deze informatie:

Tloggen voor telefoonconsole  
Cisco TFTP-weblogs  
Cisco CAPF-logs  
Packet neemt u op van CUCM en de telefoon

Raadpleeg deze bronnen voor aanvullende informatie over hoe u pakketvastlegging vanuit het CUCM en de telefoon kunt uitvoeren:

- [CUCM-sporen verzamelen op CUCM 8.6.2 voor een TAC-SR](#)
- [Packet Capture voor Unified Communications Manager-applicatie](#)
- [Het verzamelen van een pakketvastlegging van een Cisco IP-telefoon](#)

Bij de logbestanden en pakketvastlegging moet u ervoor zorgen dat het proces dat in de vorige secties wordt beschreven, correct werkt. Controleer met name of:

- De telefoon downloads het gedeeltelijke configuratiebestand met de juiste CAPF-informatie.
- De telefoon sluit via TLS aan op de CAPF dienst, en dat de informatie over LSC of MIC in de database wordt bijgewerkt.
- De telefoon downloads het volledige gecodeerde configuratiebestand.