

在CUCM上啟用加密配置功能

目錄

[簡介](#)

[背景資訊](#)

[加密配置功能概述](#)

[啟用加密配置功能](#)

[疑難排解](#)

簡介

本檔案介紹思科整合通訊管理員(CUCM)上使用加密組態電話檔案的情況。

背景資訊

電話使用加密配置檔案是CUCM中提供的可選安全功能。

您不需要在混合模式下運行CUCM群集才能使此功能正常運行，因為證書頒發機構代理功能(CAPF)證書資訊包含在身份信任清單(ITL)檔案中。

附註：這是所有CUCM 8.X及更高版本的預設位置。對於8.X版之前的CUCM版本，如果您希望使用此功能，必須確保群集在混合模式下運行。

加密配置功能概述

本節介紹在CUCM中使用加密的配置電話檔案時發生的過程。

啟用此功能、重設電話以及下載組態檔時，您會收到一個使用.cnf.xml.sgn 副檔名的檔案要求：

```
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
```



但是，在CUCM上啟用加密配置功能後，TFTP服務不再生成副檔名為.cnf.xml.sgn的完整配置檔案。而是生成部分配置檔案，如下一個示例所示。

附註：當您首次使用此方法時，電話會將配置檔案中的電話證書的MD5雜湊與本地有效證書(LSC)或製造安裝證書(MIC)的MD5雜湊進行比較。

```

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>
```

如果電話發現問題，它將嘗試使用CAPF啟動會話，除非CAPF身份驗證模式匹配*By Authentication Strings* (在這種情況下必須手動輸入字串)。以下是電話可能會識別的一些問題：

- 雜湊不匹配。
- 電話不包含證書。
- MD5值為空 (如上一個示例所示)。



附註：預設情況下，電話會啟動到埠3804上CAPF服務的傳輸層安全(TLS)會話。

電話必須知道CAPF證書，因此必須將其包括在ITL檔案或證書信任清單(CTL)檔案中 (如果集群在混合模式下運行)。

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=7200 Len=0 TSV=159397056 TSER=162819927
76.864878	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

在CAPF通訊建立後，電話向CAPF傳送有關使用的LSC或MIC的資訊。然後，CAPF從LSC或MIC提取電話公鑰，生成MD5雜湊，並將公鑰和證書雜湊的值儲存在CUCM資料庫中。

```

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

```

```
6e566143c1c14566c9da943d949a79c8 SEPA45630BBFA40
```

將公鑰儲存在資料庫中後，電話將重置並請求新的配置檔案。電話會再次嘗試下載副檔名為 **cnf.xml.sgn** 的配置檔案。



```
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>
```

電話再次比較cerHash，如果它沒有檢測到問題，將下載副檔名為.cnf.xml.enc.sgn的加密配置檔案。



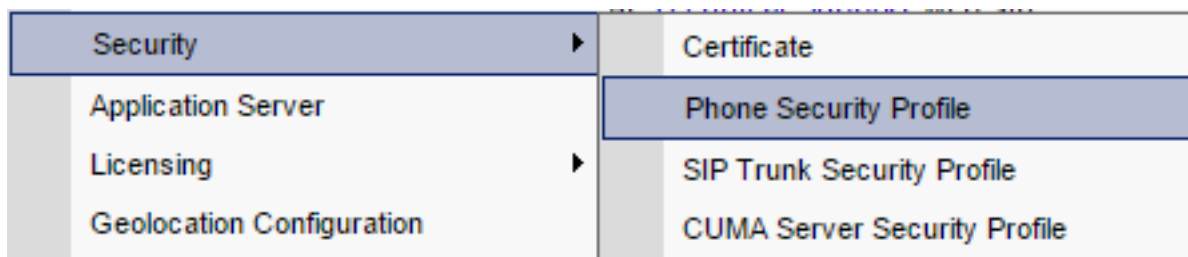
```
130.708816 10.147.94.55 10.48.46.4 HTTP GET /SEPA45630BBFA40.cnf.xml.enc.sgn HTTP/1.1
```

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

啟用加密配置功能

要啟用加密的配置電話檔案，您必須建立新的（或編輯當前的）電話安全配置檔案，並將其分配給電話。完成以下步驟，以便在CUCM上啟用加密配置功能：

1. 登入到CUCM Administration頁面，然後導航到System > Security > Phone Security Profile:



2. 複製當前或建立新的電話安全配置檔案，並選中TFTP Encrypted Config覈取方塊：

The screenshot shows the 'Phone Security Profile Configuration' page. At the top, there is a 'Save' button. Below it is a 'Status' section with an information icon and the text 'Status: Ready'. The main section is 'Phone Security Profile Information', which includes: 'Product Type: Cisco 7942', 'Device Protocol: SCCP', 'Name*: Cisco 7942 - Standard SCCP Encrypted Config', 'Description: Cisco 7942 - Standard SCCP Encrypted Config', 'Device Security Mode: Non Secure' (selected in a dropdown), and a checked checkbox for 'TFTP Encrypted Config'. Below this is the 'Phone Security Profile CAPF Information' section, which includes: 'Authentication Mode*: By Null String' (selected in a dropdown), 'Key Size (Bits)*: 1024' (selected in a dropdown), and a note: 'Note: These fields are related to the CAPF Information settings on the Phone Configuration page.'

3. 將配置檔案分配給電話：

The screenshot shows the 'Protocol Specific Information' section of the configuration page. It includes: 'Packet Capture Mode*: None' (selected in a dropdown), 'Packet Capture Duration: 0', 'BLF Presence Group*: Standard Presence group' (selected in a dropdown), 'Device Security Profile*: -- Not Selected --' (selected in a dropdown), and 'SUBSCRIBE Calling Search Space: -- Not Selected --'. Below these are three checkboxes: 'Unattended Port', 'Require DTMF Reception', and 'RFC2833 Disabled'. A dropdown menu is open, showing the following options: 'Cisco 7942 - Standard SCCP Encrypted Config' (highlighted in blue), 'Cisco 7942 - Standard SCCP Non-Secure Profile', and 'Universal Device Template - Model-independent Security Profile'.

疑難排解

完成以下步驟，對加密組態功能的系統問題進行疑難排解：

1. 確保CAPF服務處於活動狀態，並在CUCM群集中的發佈器節點上正常運行。
2. 下載部分配置檔案，並驗證電話是否可以訪問CAPF服務的埠和IP地址。
3. 驗證埠3804上到發佈伺服器節點的TCP通訊。
4. 運行前面提到的結構化查詢語言(SQL)命令，以驗證CAPF服務是否包含電話使用的LSC或MIC的相關資訊。
5. 如果問題仍然存在，則可能需要從系統中收集其他資訊。重新啟動電話並收集以下資訊：

電話控制檯日誌Cisco TFTP日誌Cisco CAPF日誌從CUCM和電話捕獲資料包有關如何從CUCM和電話運行資料包捕獲的其他資訊，請參閱以下資源：

- [從CUCM 8.6.2收集TAC SR的CUCM跟蹤](#)
- [Unified Communications Manager裝置型號上的資料包捕獲](#)
- [從Cisco IP電話收集資料包捕獲](#)

在日誌和資料包捕獲中，必須確保前面幾節中描述的過程正常運行。具體來說，請驗證：

- 電話將下載包含正確CAPF資訊的部分配置檔案。
- 電話通過TLS連線到CAPF服務，並且有關LSC或MIC的資訊在資料庫中更新。
- 電話下載完全加密的配置檔案。