

CUCM での暗号化設定機能の有効化

内容

[概要](#)

[背景説明](#)

[暗号化された設定機能の概要](#)

[暗号化された設定機能の有効化](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Cisco Unified Communications Manager (CUCM) での暗号化された電話機設定ファイルの使用について説明します。

背景説明

電話機に対する暗号化された設定ファイルの使用は、CUCM で使用できるオプションのセキュリティ機能です。

Certificate Authority Proxy Function (CAPF) の証明書情報が Identity Trust List (ITL) ファイルに含まれるので、この機能を正しく動作させるために CUCM クラスタを混合モードで実行する必要はありません。

注：CUCM バージョン 8.X 以降ではすべて、ここがデフォルトの場所です。バージョン 8.X より前の CUCM では、この機能を使用するにはクラスタが混合モードで動作していることを確認する必要があります。

暗号化された設定機能の概要

このセクションでは、暗号化された電話機設定ファイルを使用する際に発生するプロセスを説明します。

この機能を有効にし、電話機をリセットし、設定ファイルをダウンロードすると、.cnf.xml.sgn 拡張子を持つ次のファイルのリクエストを受信します。

```
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
```



ただし、暗号化された設定機能が CUCM で有効化された後、TFTP サービスは、.cnf.xml.sgn 拡張子を持つ完全な設定ファイルを生成しません。代わりに、次の例に示すように部分的な設定ファイルを生成します。

注：この方法を初めて使用する際、電話機は、設定ファイル中の電話機証明書の MD5 ハッシュを、ローカルで有効な証明書 (LSC) または Manufacturing Installed Certificate (MIC) の MD5 ハッシュと比較します。

```
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>
```

電話機が問題を認識すると、認証局プロキシ機能 (CAPF) によりセッションを開始しようとします。ただし、CAPF 認証モードが *By Authenticaion Strings* に一致する場合は、文字列を手動で入力する必要があります。電話機が認識する可能性のある問題を次に示します。

- ハッシュが一致しない。
- 電話機に証明書が含まれていない。
- MD5 値が空白である (前述の例の状況) 。



注：電話機はデフォルトで、ポート 3804 の認証局プロキシ機能 (CAPF) サービスへの Transport Layer Security (TLS) セッションを開始します。

CAPF 証明書は電話機にとって既知である必要があるため、ITL ファイルか証明書信頼リスト (CTL) ファイル (クラスタが混合モードで実行されている場合) のどちらかに含まれている必要があります。

```
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
```

CAPF の通信が確立された後、電話機は、使用された LSC または MIC に関する情報を CAPF に

送信します。次いで CAPF は、LSC または MIC から電話機の公開キーを取得し、MD5 ハッシュを生成し、公開鍵および証明書ハッシュの値を CUCM データベースに保存します。

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

公開キーがデータベースに格納されると、電話機はリセットされ、新しい設定ファイルをリクエストします。電話機は、.cnf.xml.sgn 拡張子を持つ設定ファイルのダウンロードを再度試みます。



```
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>
電話機はcerHash を再度比較し、問題が検出されない場合、.cnf.xml.enc.sgn 拡張子を持つ暗号化されたファイルをダウンロードします。



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

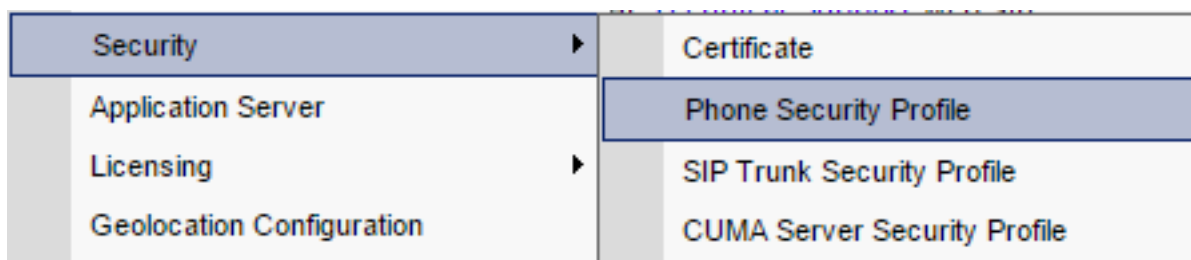
```
.....c..)CN=cucm85;OU=It;O=Cisco;L=KRK;ST=PL;C=PL...Z.....)CN=cucm85;
OU=It;O=Cisco;L=KRK;ST=PL;C=PL.....
.....C.<...Y6.Lh.|(.w+...0.a.&
O.....V...T...Z..R^..f....|.e.@...5.....G...[.....n.....=
.A..H.(...Z...{.!%[... SEPA45630BBFA40.cnf.xml.enc.sgn...R.DD..M.....
Uu.C..@.....
```

```
.....m.b.....6y ..x.^b...-8.^...^'.4.<Wb.n.....5...we.0@.g..
V7...r.9
Qs>..).w....pt/...}A.']}
.r.t%G..d_/i.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.
[...]
```

暗号化された設定機能の有効化


暗号化された電話機の設定ファイルを有効化するには、新しい電話機のセキュリティプロファイルを作成（または現在のプロファイルを編集）し、電話機に割り当てる必要があります。CUCMでの暗号化された設定機能を有効化するには、次の手順を実行します。

1. [CUCM Administration] ページにログインし、[System] > [Security] > [Phone Security Profile] に移動します。




2. 現在の電話機セキュリティプロファイルをコピーするか、新しいプロファイルを作成し、[TFTP Encrypted Config] チェックボックスをオンにします。

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. 電話機にプロファイルを割り当てます。

Protocol Specific Information	
Packet Capture Mode*	None ▼
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group ▼
Device Security Profile*	-- Not Selected -- ▼
SUBSCRIBE Calling Search Space	-- Not Selected -- Cisco 7942 - Standard SCCP Encrypted Config Cisco 7942 - Standard SCCP Non-Secure Profile Universal Device Template - Model-independent Security Profile
<input type="checkbox"/> Unattended Port	
<input type="checkbox"/> Require DTMF Reception	
<input type="checkbox"/> RFC2833 Disabled	

トラブルシューティング

暗号化された設定機能に関連するシステムの問題をトラブルシューティングするには、次の手順を実行します。

1. CAPF サービスがアクティブで、CUCM クラスターのパブリッシャ ノード上で正しく動作することを確認します。
2. 部分的な設定ファイルをダウンロードし、CAPF サービスのポートと IP アドレスが電話機から到達可能であることを確認します。
3. パブリッシャ ノードへのポート 3804 の TCP 通信を確認します。
4. 以前に言及した Structured Query Language (SQL) コマンドを実行し、CAPF サービスに電話機が使用する LSC または MIC に関する情報があるかどうかを確認します。
5. 問題が続く場合、システムから追加の情報を収集する必要がある場合があります。電話機を再起動し、次の情報を収集します。

電話機のコンソール ログ Cisco TFTP ログ Cisco CAPF ログ CUCM および電話機からのパケット キャプチャ

CUCM および電話機からのパケット キャプチャの実行方法の詳細については、次のリソースを参照してください。

- [TAC SR のために CUCM 8.6.2 から CUCM トレースを収集する](#)
- [Unified Communications Manager アプライアンス モデルのパケット キャプチャ](#)
- [Cisco IP Phone からパケット キャプチャを収集する方法](#)

ログとパケット キャプチャでは、前のセクションで説明したプロセスが正しく動作することを確認します。具体的には、次を確認します。

- 電話機が正しい CAPF 情報を持つ部分的な設定ファイルをダウンロードすること。
- 電話機が CAPF サービスに TLS 接続すること、および LSC または MIC に関する情報がデータベース内で更新されること
- 電話機が完全な暗号化された設定ファイルをダウンロードすること。