

Enable the Encrypted Configuration Feature on the CUCM

Contents

[Introduction](#)

[Background Information](#)

[Encrypted Configuration Feature Overview](#)

[Enable Encrypted Configuration Feature](#)

[Troubleshoot](#)

Introduction

This document describes the use of encrypted configuration phone files on the Cisco Unified Communications Manager (CUCM).

Background Information

The use of encrypted configuration files for phones is an optional security feature that is available in the CUCM.

You are not required to run the CUCM cluster in Mixed mode in order for this feature to function properly, as the Certificate Authority Proxy Function (CAPF) certificate information is contained within the Identity Trust List (ITL) file.

Note: This is the default location for all of the CUCM Versions 8.X and later. For CUCM versions prior to Version 8.X, you must ensure that the cluster runs in Mixed mode if you desire to use this feature.

Encrypted Configuration Feature Overview

This section describes the process that occurs when encrypted configuration phone files are used within the CUCM.

When you enable this feature, reset the phone, and download the configuration file, you receive a request for the file with a **.cnf.xml.sgn** extension:

```
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
```



However, after the encrypted configuration feature is enabled on the CUCM, the TFTP service no

longer generates a full configuration file with the **.cnf.xml.sgn** extension. Instead, it generates the partial configuration file, as shown in the next example.

Note: When you use this method for the first time, the phone compares the MD5 hash of the phone certificate in the configuration file to the MD5 hash of the Locally Significant Certificate (LSC) or the Manufacturing Installed Certificates (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>
<certHash></certHash>
<encrConfig>true</encrConfig>
</device>
```

If the phone identifies a problem, it attempts to initiate a session with the CAPF, unless the CAPF authentication mode matches *By Authentication Strings*, in which case you must manually enter the string. Here are some problems that the phone might identify:

- The hash does not match.
- The phone does not contain a certificate.
- The MD5 value is blank (as in the previous example).



Note: The phone initiates a Transport Layer Security (TLS) session to the CAPF service on port 3804 by default.

The CAPF certificate must be known for the phone, so it must be included in either the ITL file or Certificate Trust List (CTL) file (if the cluster runs in Mixed mode).

```
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
76.805666 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
```

After the CAPF communication is established, the phone sends information to the CAPF about the LSC or MIC that is used. The CAPF then extracts the phone public key from the LSC or MIC, generates a MD5 hash, and stores the values for the public key and certificate hash in the CUCM database.

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

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

After the public key is stored in the database, the phone resets and requests a new configuration file. The phone attempts to download the configuration file with the **cnf.xml.sgn** extension once again.



```
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>
<certHash>6e566143c1c14566c9da943d949a79c8</certHash>
<encrConfig>true</encrConfig>
</device>
```

The phone compares the **cerHash** again, and if it does not detect the problem, it downloads the encrypted configuration file with the **.cnf.xml.enc.sgn** extension.



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

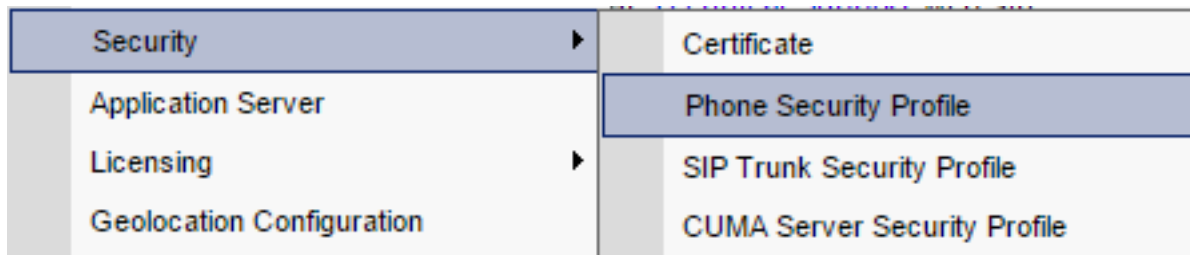
```
.....c..)CN=cucm85;OU=It;O=Cisco;L=KRK;ST=PL;C=PL.....Z.....)CN=cucm85;
OU=It;O=Cisco;L=KRK;ST=PL;C=PL.....
.....C.<...Y6.Lh.|(..w+...0.a.&
O.....V...T...Z..R^.f....|.=.e.@...5.....G...[.....n.....=
.A..H.(...Z...{.!%[...SEPA45630BBFA40.cnf.xml.enc.sgn....R.DD..M.....
Uu.C..@.....
.....m.b.....6y ..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.
```

[...]

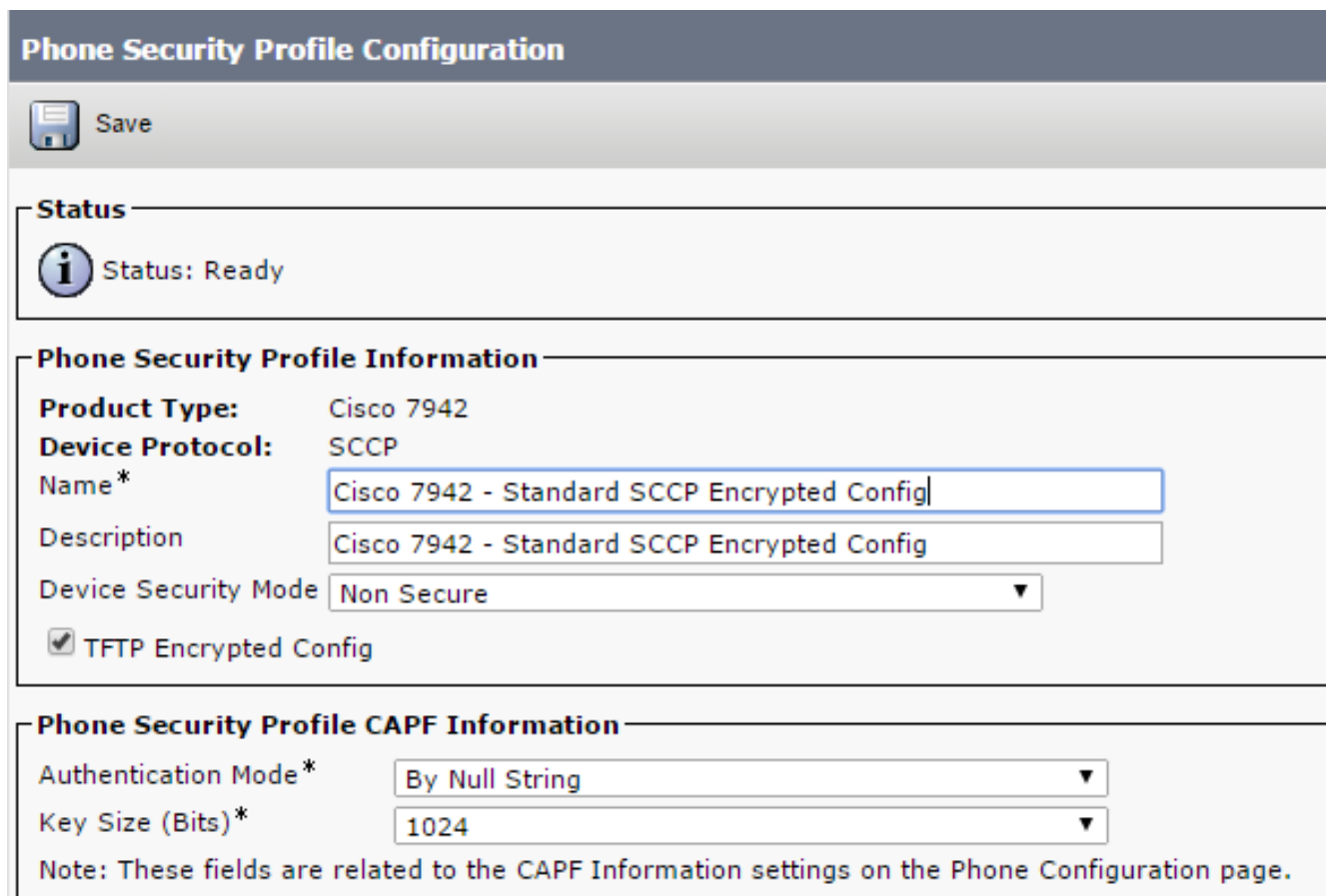
Enable Encrypted Configuration Feature

In order to enable the encrypted configuration phone files, you must create a new (or edit a current) Phone Security Profile and assign it to the phone. Complete these steps in order to enable the encrypted configuration feature on the CUCM:

1. Log into the CUCM Administration page and navigate to **System > Security > Phone Security Profile**:



2. Copy a current, or create a new, Phone Security Profile and check the **TFTP Encrypted Config** check box:

A screenshot of the 'Phone Security Profile Configuration' page. The page has a dark header with the title 'Phone Security Profile Configuration'. Below the header is a 'Save' button with a floppy disk icon. The main content area is divided into sections: 'Status' (with an information icon and 'Status: Ready'), 'Phone Security Profile Information' (with fields for 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, and a checked checkbox for TFTP Encrypted Config), and 'Phone Security Profile CAPF Information' (with fields for Authentication Mode*: By Null String and Key Size (Bits)*: 1024). A note at the bottom states: 'Note: These fields are related to the CAPF Information settings on the Phone Configuration page.'

3. Assign the profile to the phone:

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	

Troubleshoot

Complete these steps in order to troubleshoot system issues in regards to the encrypted configuration feature:

1. Ensure that the CAPF service is active and runs properly on the Publisher node in the CUCM cluster.
2. Download the partial configuration file and verify that the port and IP address of the CAPF service are reachable from the phone.
3. Verify the TCP communication on port 3804 to the Publisher node.
4. Run the previously mentioned Structured Query Language (SQL) command in order to verify whether the CAPF service has information about the LSC or MIC that is used by the phone.
5. If the issue still persists, you might be required to collect additional information from the system. Restart the phone and collect this information:

Phone Console logs
Cisco TFTP logs
Cisco CAPF logs
Packet captures from the CUCM and the phone

Refer to these resources for additional information about how to run packet captures from the CUCM and the phone:

- [Collecting CUCM Traces from CUCM 8.6.2 for a TAC SR](#)
- [Packet Capture on Unified Communications Manager Appliance Model](#)
- [Collecting a packet capture from a Cisco IP Phone](#)

In the logs and packet captures, you must ensure that the process described in the previous sections functions properly. Specifically, verify that:

- The phone downloads the partial configuration file with the correct CAPF information.
- The phone connects via TLS to the CAPF service, and that the information about the LSC or MIC is updated in the database.
- The phone downloads the full encrypted configuration file.