Aktivieren Sie die Verschlüsselungskonfiguration auf dem CUCM.

Inhalt

Einführung

In diesem Dokument wird die Verwendung verschlüsselter Konfigurationstelefondateien auf dem Cisco Unified Communications Manager (CUCM) beschrieben.

Hintergrundinformationen

Die Verwendung verschlüsselter Konfigurationsdateien für Telefone ist eine optionale Sicherheitsfunktion, die im CUCM verfügbar ist.

Sie müssen den CUCM-Cluster nicht im gemischten Modus ausführen, damit dieses Feature ordnungsgemäß funktioniert, da die CAPF-Zertifikatsinformationen (Certificate Authority Proxy Function) in der ITL-Datei (Identity Trust List) enthalten sind.

> **Hinweis**: Dies ist der Standardspeicherort für alle CUCM-Versionen 8.x und höher. Bei CUCM-Versionen vor Version 8.x müssen Sie sicherstellen, dass der Cluster im gemischten Modus ausgeführt wird, wenn Sie diese Funktion verwenden möchten.

Übersicht über die Funktionen der verschlüsselten Konfiguration

In diesem Abschnitt wird der Prozess beschrieben, der durchgeführt wird, wenn innerhalb des CUCM verschlüsselte Konfigurationstelefon-Dateien verwendet werden.

Wenn Sie diese Funktion aktivieren, das Telefon zurücksetzen und die Konfigurationsdatei herunterladen, erhalten Sie eine Anfrage für die Datei mit der Erweiterung **.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
```

Nachdem die verschlüsselte Konfigurationsfunktion auf dem CUCM aktiviert wurde, generiert der TFTP-Dienst keine vollständige Konfigurationsdatei mehr mit der Erweiterung **.cnf.xml.sgn**. Stattdessen wird die Teilkonfigurationsdatei generiert, wie im nächsten Beispiel gezeigt.

> **Hinweis**: Wenn Sie diese Methode zum ersten Mal verwenden, vergleicht das Telefon den MD5-Hash des Telefonzertifikats in der Konfigurationsdatei mit dem MD5-Hash des LSC (Locally Significant Certificate) oder der MIC (Manufacturing Installed Certificates).

```
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>
```

Wenn das Telefon ein Problem identifiziert, versucht es, eine Sitzung mit dem CAPF zu initiieren, es sei denn, der CAPF-Authentifizierungsmodus stimmt mit *den Authentifizierungszeichenfolgen überein*. In diesem Fall müssen Sie die Zeichenfolge manuell eingeben. Folgende Probleme kann das Telefon identifizieren:

- Der Hash stimmt nicht überein.
- Das Telefon enthält kein Zertifikat.
- Der MD5-Wert ist leer (wie im vorherigen Beispiel).

> **Hinweis**: Das Telefon initiiert standardmäßig eine Transport Layer Security (TLS)-Sitzung mit dem CAPF-Service an Port 3804.

Das CAPF-Zertifikat muss für das Telefon bekannt sein. Daher muss es entweder in die Datei ITL oder CTL (Certificate Trust List) aufgenommen werden (wenn der Cluster im gemischten Modus ausgeführt wird).

```
76.804108  10.147.94.55   10.48.46.4     TCP    51292 > cisco-com-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-com-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-com-capf [ACK] Seq=55 Ack=720 Win=7280 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
```

Nachdem die CAPF-Kommunikation eingerichtet wurde, sendet das Telefon Informationen zum verwendeten LSC oder MIC an die CAPF. Die CAPF extrahiert dann den öffentlichen Telefonschlüssel aus der LSC oder MIC, generiert einen MD5-Hash und speichert die Werte für den öffentlichen Schlüssel und den Zertifikatshash in der CUCM-Datenbank.

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

Nachdem der öffentliche Schlüssel in der Datenbank gespeichert wurde, wird das Telefon zurückgesetzt und eine neue Konfigurationsdatei angefordert. Das Telefon versucht erneut, die Konfigurationsdatei mit der Erweiterung **cnf.xml.sgn** herunterzuladen.


```
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>
```

Das Telefon vergleicht das **cerHash** erneut, und wenn es das Problem nicht erkennt, lädt es die verschlüsselte Konfigurationsdatei mit der Erweiterung **.cnf.xml.enc.sgn herunter**.

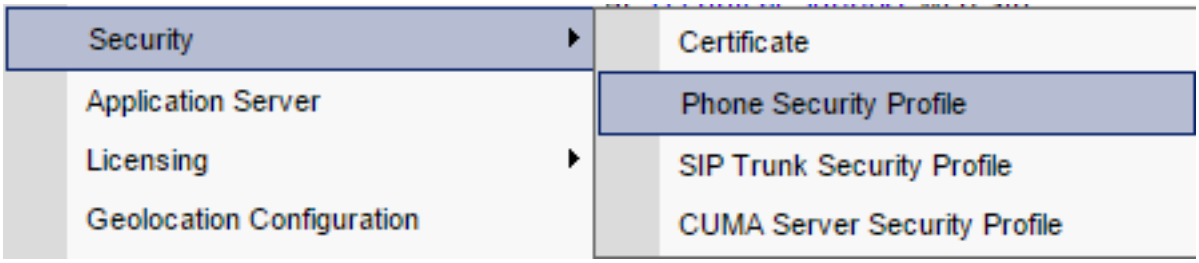

```
130.708816 10.147.94.55     10.48.46.4     HTTP   GET /SEPA45630BBFA40.cnf.xml.enc.sgn HTTP/1.1
```

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

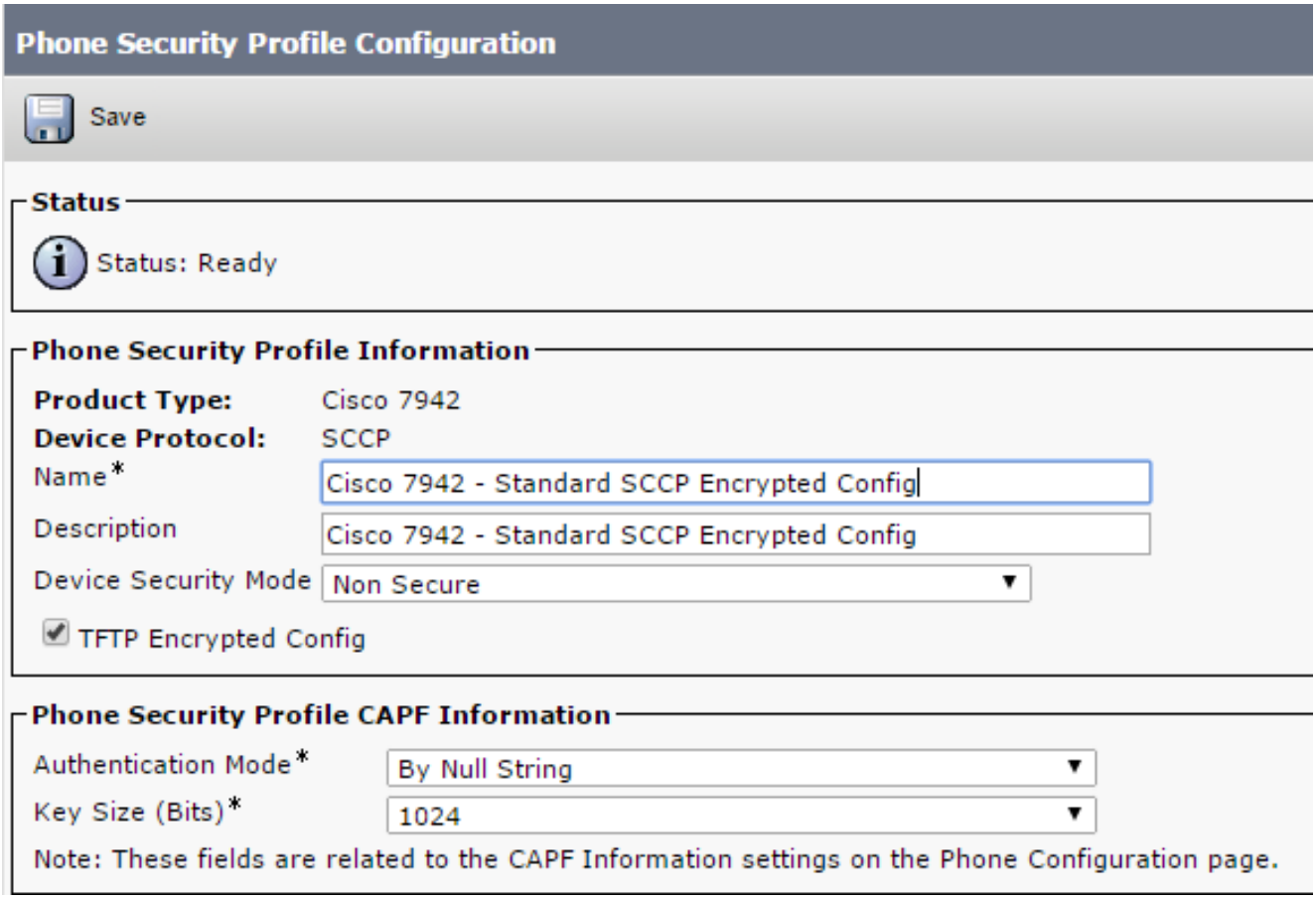
Verschlüsselte Konfigurationsfunktion aktivieren

Um die verschlüsselten Konfigurationstelefondateien zu aktivieren, müssen Sie ein neues (oder ein aktuelles) Telefon-Sicherheitsprofil erstellen und es dem Telefon zuweisen. Gehen Sie wie folgt vor, um die verschlüsselte Konfigurationsfunktion des CUCM zu aktivieren:

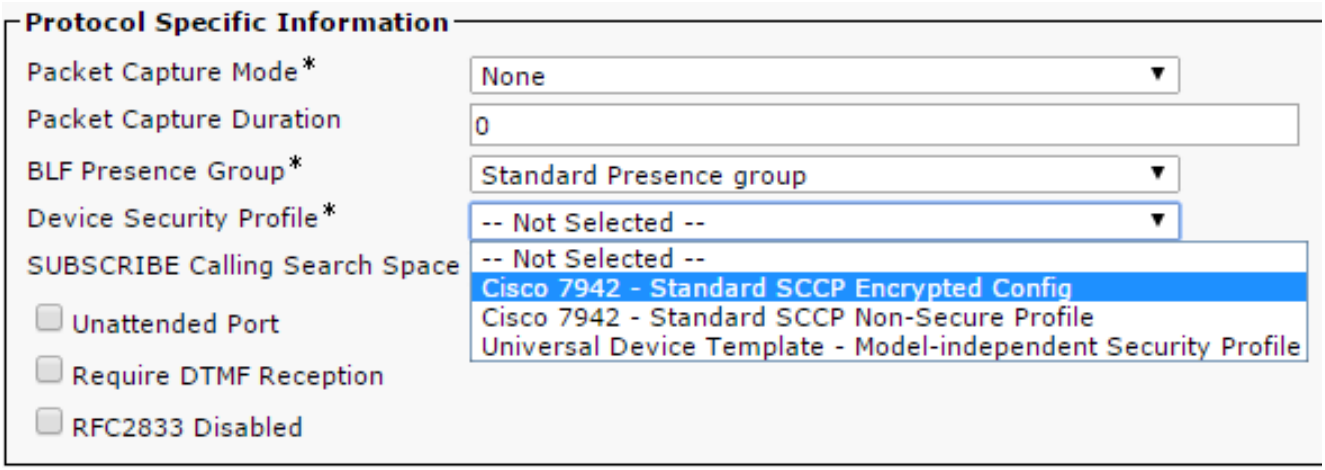
1. Melden Sie sich bei der CUCM-Verwaltungsseite an, und navigieren Sie zu **System > Security > Phone Security Profile**:



2. Kopieren Sie einen aktuellen oder erstellen Sie ein neues Telefonsicherheitsprofil, und aktivieren Sie das Kontrollkästchen **TFTP Encrypted Config** (Verschlüsselte Konfiguration für TFTP):



3. Zuweisen des Profils zum Telefon:



Fehlerbehebung

Gehen Sie wie folgt vor, um Systemprobleme im Zusammenhang mit der verschlüsselten Konfigurationsfunktion zu beheben:

1. Stellen Sie sicher, dass der CAPF-Dienst aktiv ist und ordnungsgemäß auf dem Publisher-Knoten im CUCM-Cluster ausgeführt wird.

2. Laden Sie die Teilkonfigurationsdatei herunter, und überprüfen Sie, ob der Port und die IP-Adresse des CAPF-Services vom Telefon aus erreichbar sind.

3. Überprüfen Sie die TCP-Kommunikation an Port 3804 zum Publisher-Knoten.

4. Führen Sie den zuvor erwähnten SQL-Befehl (Structured Query Language) aus, um zu überprüfen, ob der CAPF-Dienst über Informationen zum vom Telefon verwendeten LSC oder MIC verfügt.

5. Wenn das Problem weiterhin besteht, müssen Sie möglicherweise zusätzliche Informationen vom System sammeln. Starten Sie das Telefon neu, und erfassen Sie folgende Informationen:

   TelefonkonsolenprotokolleCisco TFTP-ProtokolleCisco CAPF-ProtokollePaketerfassungen vom CUCM und vom Telefon aus

Weitere Informationen zum Ausführen von Paketerfassungen vom CUCM und vom Telefon finden Sie in diesen Ressourcen:

- Erfassen von CUCM-Traces vom CUCM 8.6.2 für einen TAC-SR
- Paketerfassung auf dem Appliance-Modell Unified Communications Manager
- Erfassen von Paketen über ein Cisco IP-Telefon

In den Protokollen und Paketerfassungen müssen Sie sicherstellen, dass der in den vorherigen Abschnitten beschriebene Prozess ordnungsgemäß funktioniert. Stellen Sie insbesondere sicher, dass:

- Das Telefon lädt die Teilkonfigurationsdatei mit den richtigen CAPF-Informationen herunter.
- Das Telefon verbindet sich über TLS mit dem CAPF-Service, und die Informationen über das LSC oder MIC werden in der Datenbank aktualisiert.
- Das Telefon lädt die vollständige verschlüsselte Konfigurationsdatei herunter.