Abilitare la funzionalità di configurazione crittografata in CUCM

Sommario

Introduzione

Questo documento descrive l'utilizzo di file telefonici di configurazione crittografati su Cisco Unified Communications Manager (CUCM).

Premesse

L'uso di file di configurazione crittografati per i telefoni è una funzione di sicurezza opzionale disponibile in CUCM.

Per il corretto funzionamento di questa funzionalità non è necessario eseguire il cluster CUCM in modalità mista, in quanto le informazioni sul certificato CAPF (Certificate Authority Proxy Function) sono contenute nel file dell'elenco di certificati di identità attendibili (ITL, Identity Trust List).

> **Nota:** Questa è la posizione predefinita per tutte le versioni di CUCM 8.X e successive. Per le versioni di CUCM precedenti alla versione 8.X, è necessario verificare che il cluster venga eseguito in modalità mista se si desidera utilizzare questa funzionalità.

Panoramica della funzionalità di configurazione crittografata

In questa sezione viene descritto il processo che si verifica quando vengono utilizzati file telefonici di configurazione crittografati all'interno di CUCM.

Quando abiliti questa funzione, ripristina il telefono e scarica il file di configurazione, ricevi una richiesta per il file con estensione **.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
```

Tuttavia, dopo aver abilitato la funzionalità di configurazione crittografata sul CUCM, il servizio

TFTP non genera più un file di configurazione completo con estensione **.cnf.xml.sgn**. Viene invece generato il file di configurazione parziale, come illustrato nell'esempio seguente.

> **Nota:** Quando si utilizza questo metodo per la prima volta, il telefono confronta l'hash MD5 del certificato telefonico nel file di configurazione con l'hash MD5 del certificato LSC (Locally Significant Certificate) o del 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>
```

Se il telefono identifica un problema, tenta di avviare una sessione con CAPF, a meno che la modalità di autenticazione CAPF non corrisponda a *By Authentication Strings*, nel qual caso è necessario immettere manualmente la stringa. Ecco alcuni problemi che il telefono potrebbe identificare:

- Hash non corrispondente.
- Il telefono non contiene un certificato.
- Il valore MD5 è vuoto (come nell'esempio precedente).

> **Nota:** Per impostazione predefinita, il telefono avvia una sessione TLS (Transport Layer Security) con il servizio CAPF sulla porta 3804.

Il certificato CAPF deve essere noto per il telefono, quindi deve essere incluso nel file ITL o nel file CTL (Certificate Trust List) se il cluster viene eseguito in modalità mista.

```
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
```

Una volta stabilita la comunicazione CAPF, il telefono invia informazioni al CAPF relative all'LSC o MIC utilizzato. Il file CAPF estrae quindi la chiave pubblica del telefono da LSC o MIC, genera un hash MD5 e memorizza i valori per la chiave pubblica e l'hash del certificato nel database CUCM.

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

Dopo aver memorizzato la chiave pubblica nel database, il telefono si reimposta e richiede un nuovo file di configurazione. Il telefono tenta di scaricare di nuovo il file di configurazione con l'estensione **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>
```

Il telefono confronta di nuovo **cerHash** e, se non rileva il problema, scarica il file di configurazione crittografato con l'estensione **.cnf.xml.enc.sgn**.

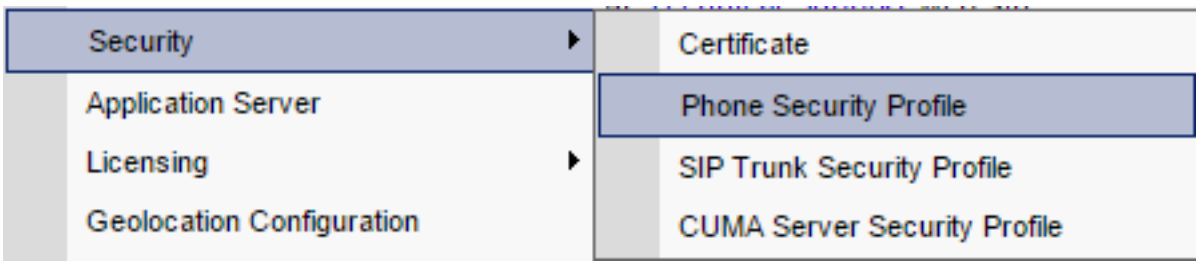

```
130.708816 10.147.94.55     10.48.46.4     HTTP   GET /SEPA45630BBFA40.cnf.xml.enc.sgn HTTP/1.1
```

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

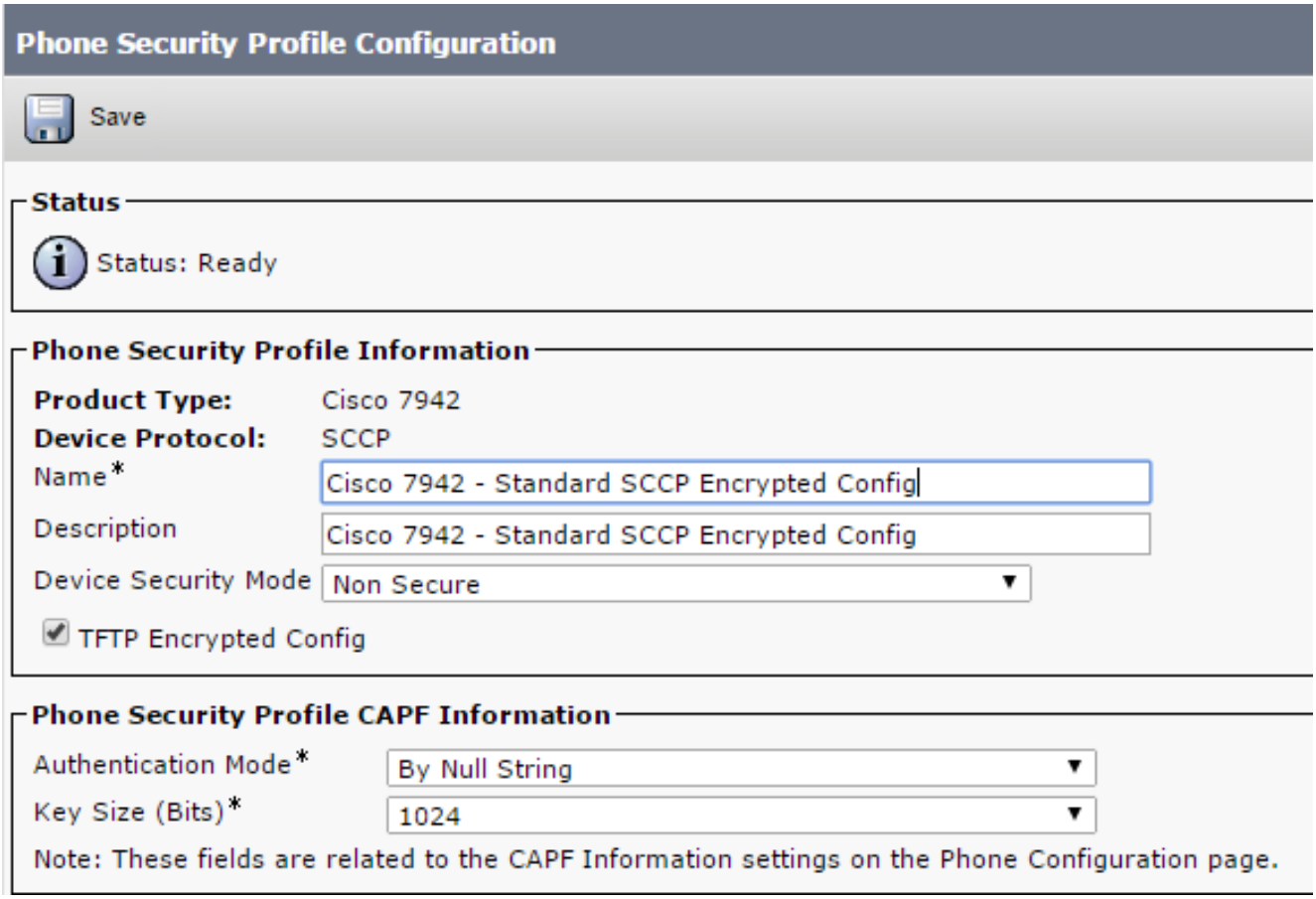
Abilita funzionalità di configurazione crittografata

Per abilitare i file telefonici della configurazione crittografata, è necessario creare un nuovo profilo di sicurezza del telefono (o modificare un profilo corrente) e assegnarlo al telefono. Completare questa procedura per abilitare la funzione di configurazione crittografata sul CUCM:

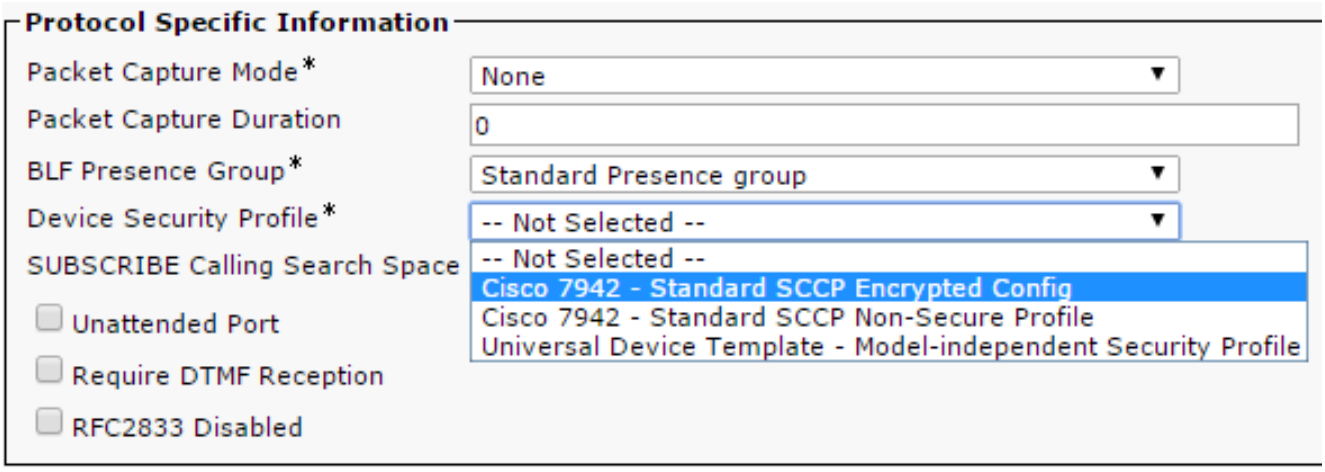
1. Accedere alla pagina Amministrazione CUCM e selezionare **Sistema > Sicurezza > Profilo sicurezza telefono**:



2. Copiare un profilo di sicurezza telefonico corrente o crearne uno nuovo e selezionare la casella di controllo **TFTP Encrypted Config**:



3. Assegna il profilo al telefono:



Risoluzione dei problemi

Completare questi passaggi per risolvere i problemi del sistema relativi alla funzionalità di configurazione crittografata:

1. Verificare che il servizio CAPF sia attivo e funzioni correttamente nel nodo Publisher nel cluster CUCM.

2. Scaricare il file di configurazione parziale e verificare che la porta e l'indirizzo IP del servizio CAPF siano raggiungibili dal telefono.

3. Verificare la comunicazione TCP sulla porta 3804 al nodo Publisher.

4. Eseguire il comando SQL (Structured Query Language) menzionato in precedenza per verificare se il servizio CAPF dispone di informazioni su LSC o MIC utilizzate dal telefono.

5. Se il problema persiste, potrebbe essere necessario raccogliere ulteriori informazioni dal sistema. Riavvia il telefono e raccogli queste informazioni:

   Registri console telefonicaLog Cisco TFTPRegistri CAPF CiscoAcquisizione dei pacchetti dal CUCM e dal telefono

Fare riferimento a queste risorse per ulteriori informazioni su come eseguire le acquisizioni dei pacchetti dal CUCM e dal telefono:

- Raccolta delle tracce CUCM da CUCM 8.6.2 per un TAC SR
- Acquisizione di pacchetti sul modello di appliance Unified Communications Manager
- Raccolta di un pacchetto acquisito da un Cisco IP Phone

Nei log e nelle acquisizioni dei pacchetti, dovete assicurarvi che il processo descritto nelle sezioni precedenti funzioni correttamente. In particolare, verificare che:

- Il telefono scarica il file di configurazione parziale con le informazioni CAPF corrette.
- Il telefono si connette tramite TLS al servizio CAPF e che le informazioni su LSC o MIC vengano aggiornate nel database.
- Il telefono scarica il file di configurazione completamente crittografato.