Activer la fonction de configuration chiffrée sur CUCM

Contenu

Introduction

Ce document décrit l'utilisation de fichiers téléphoniques de configuration chiffrés sur Cisco Unified Communications Manager (CUCM).

Informations générales

L'utilisation de fichiers de configuration chiffrés pour les téléphones est une fonctionnalité de sécurité facultative disponible dans CUCM.

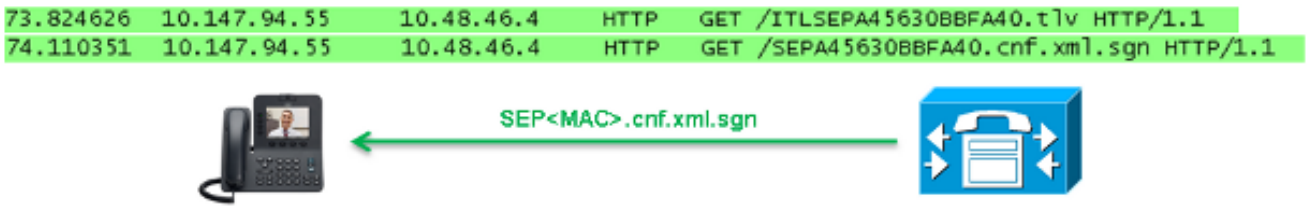
Vous n'êtes pas obligé d'exécuter le cluster CUCM en mode Mixed pour que cette fonctionnalité fonctionne correctement, car les informations de certificat CAPF (Certificate Authority Proxy Function) sont contenues dans le fichier de liste de confiance d'identité (ITL).

> **Note**: Il s'agit de l'emplacement par défaut de toutes les versions de CUCM 8.X et ultérieures. Pour les versions de CUCM antérieures à la version 8.X, vous devez vous assurer que le cluster fonctionne en mode Mixed si vous souhaitez utiliser cette fonctionnalité.

Présentation de la fonction de configuration chiffrée

Cette section décrit le processus qui se produit lorsque des fichiers téléphoniques de configuration chiffrés sont utilisés dans CUCM.

Lorsque vous activez cette fonctionnalité, réinitialisez le téléphone et téléchargez le fichier de configuration, vous recevez une demande pour le fichier avec une extension **.cnf.xml.sgn** :



Cependant, une fois que la fonction de configuration chiffrée est activée sur CUCM, le service TFTP ne génère plus de fichier de configuration complet avec l'extension **.cnf.xml.sgn**. Il génère plutôt le fichier de configuration partielle, comme illustré dans l'exemple suivant.

> **Note**: Lorsque vous utilisez cette méthode pour la première fois, le téléphone compare le hachage MD5 du certificat du téléphone dans le fichier de configuration au hachage MD5 du certificat LSC ou des certificats installés de fabrication (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>
```

```
</device>
```

Si le téléphone identifie un problème, il tente d'initier une session avec le CAPF, à moins que le mode d'authentification CAPF ne corresponde *Par chaînes d'authentification*, auquel cas vous devez entrer manuellement la chaîne. Voici quelques problèmes que le téléphone peut identifier :

- Le hachage ne correspond pas.
- Le téléphone ne contient pas de certificat.
- La valeur MD5 est vide (comme dans l'exemple précédent).

> **Note**: Par défaut, le téléphone initie une session TLS (Transport Layer Security) au service CAPF sur le port 3804.

Le certificat CAPF doit être connu pour le téléphone, il doit donc être inclus dans le fichier ITL ou le fichier CTL (Certificate Trust List) (si le cluster s'exécute en mode Mixed).

```
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
```

Une fois la communication CAPF établie, le téléphone envoie au CAPF des informations sur le LSC ou le MIC utilisé. Le CAPF extrait ensuite la clé publique du téléphone à partir du LSC ou du MIC, génère un hachage MD5 et stocke les valeurs de la clé publique et du hachage de certificat dans la base de données CUCM.

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

Une fois la clé publique stockée dans la base de données, le téléphone réinitialise et demande un nouveau fichier de configuration. Le téléphone tente de télécharger à nouveau le fichier de configuration avec l'extension **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>
```

Le téléphone compare de nouveau **cerHash**, et s'il ne détecte pas le problème, il télécharge le fichier de configuration chiffré avec l'extension **.cnf.xml.enc.sgn**.

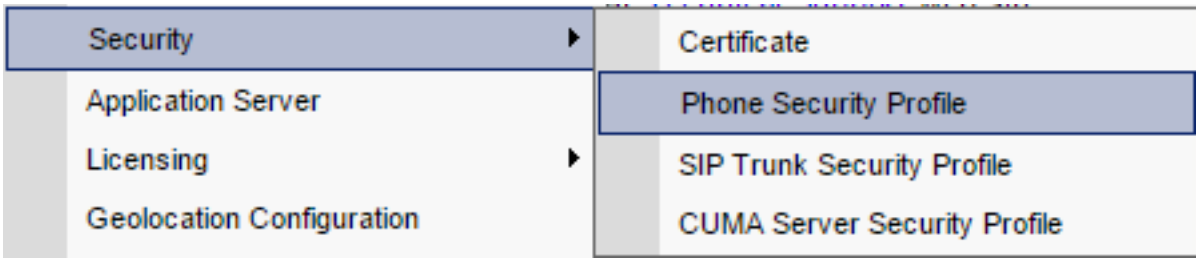

```
130.708816 10.147.94.55     10.48.46.4     HTTP   GET /SEPA45630BBFA40.cnf.xml.enc.sgn HTTP/1.1
```

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

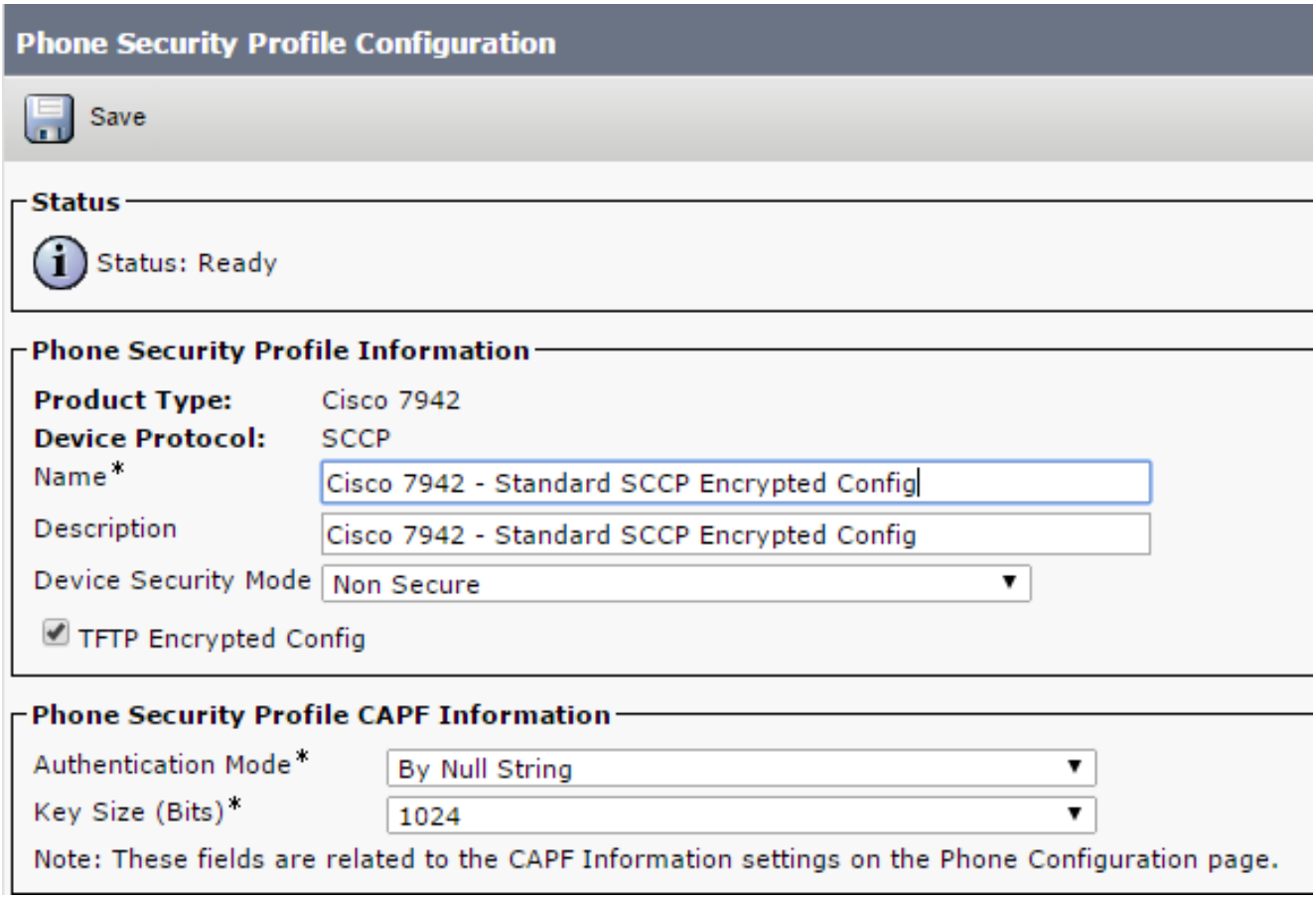
Activer la fonction de configuration chiffrée

Pour activer les fichiers téléphoniques de configuration chiffrés, vous devez créer un profil de sécurité téléphonique (ou modifier un profil de sécurité téléphonique actuel) et l'affecter au téléphone. Complétez ces étapes afin d'activer la fonctionnalité de configuration chiffrée sur CUCM :

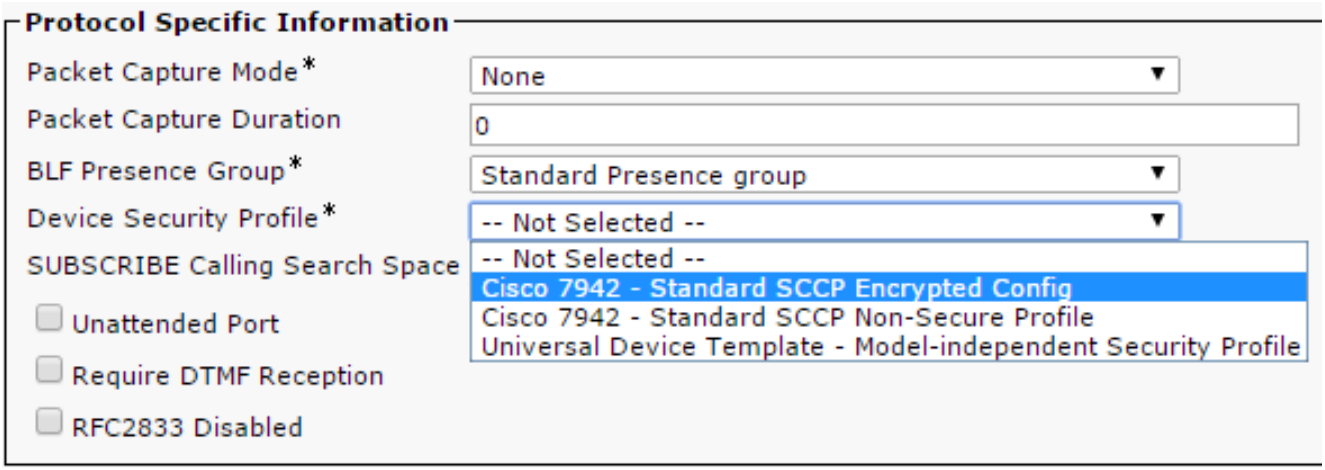
1. Connectez-vous à la page Administration de CUCM et accédez à **System > Security > Phone Security Profile** :



2. Copiez un profil de sécurité téléphonique actuel ou créez-en un nouveau et cochez la case **Config cryptée TFTP** :



3. Attribuez le profil au téléphone :



Dépannage

Complétez ces étapes afin de résoudre les problèmes système liés à la fonctionnalité de configuration chiffrée :

1. Assurez-vous que le service CAPF est actif et s'exécute correctement sur le noeud Publisher dans le cluster CUCM.

2. Téléchargez le fichier de configuration partielle et vérifiez que le port et l'adresse IP du service CAPF sont accessibles depuis le téléphone.

3. Vérifiez la communication TCP sur le port 3804 vers le noeud Publisher.

4. Exécutez la commande SQL (Structured Query Language) mentionnée précédemment afin de vérifier si le service CAPF dispose d'informations sur le LSC ou le MIC utilisé par le téléphone.

5. Si le problème persiste, vous devrez peut-être recueillir des informations supplémentaires auprès du système. Redémarrez le téléphone et collectez ces informations :

   Journaux de la console téléphoniqueJournaux TFTP CiscoJournaux CAPF CiscoCaptures de paquets à partir du CUCM et du téléphone

Référez-vous à ces ressources pour plus d'informations sur l'exécution des captures de paquets à partir de CUCM et du téléphone :

- Collecte des traces CUCM de CUCM 8.6.2 pour un TAC SR
- Capture des parquets sur le modèle appliance Unified Communications Manager
- Collecte d'une capture de paquets à partir d'un téléphone IP Cisco

Dans les journaux et les captures de paquets, vous devez vous assurer que le processus décrit dans les sections précédentes fonctionne correctement. Plus précisément, vérifiez que :

- Le téléphone télécharge le fichier de configuration partielle avec les informations CAPF correctes.
- Le téléphone se connecte via TLS au service CAPF et les informations relatives au LSC ou au MIC sont mises à jour dans la base de données.
- Le téléphone télécharge le fichier de configuration crypté complet.