Comment télécharger des certificats à partir de téléphones IP Cisco

Contenu

Introduction

Ce document décrit la procédure permettant de récupérer des certificats à partir d'un téléphone IP Cisco lorsque le service CAPF (Autorité Proxy Function) de Cisco s'exécute dans l'éditeur de Cisco Unified Communications Manager (CUCM).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Certificats SSL dans le téléphone
- Administration CUCM
- Gestion de l'interface de ligne de commande (CLI) dans CUCM

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Unified Communications Manager (CUCM) version 11.5.1.11900-26
- Téléphone IP Cisco 8811 - sip88xx.12-5-1SR1-4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Le service CAPF doit être actif dans l'éditeur CUCM et le certificat CAPF sous Cisco Unified OS Administration doit être à jour.

Pour les téléphones IP Cisco, il existe deux alternatives aux certificats installés sur ces téléphones :

- MIC (Certificat installé par le fabricant)
- MIC et LSC (certificat d'importance locale)

Les téléphones sont préinstallés avec le certificat MIC et ne peuvent pas être supprimés ni régénérés. En outre, MIC ne peut pas être utilisé une fois la validité expirée. Les MIC sont des certificats de clé de 2 048 bits signés par l'autorité de certification Cisco.

Le LSC possède la clé publique du téléphone IP Cisco, qui est signée par la clé privée CAPF CUCM. Il n'est pas installé sur le téléphone par défaut et ce certificat est requis pour le téléphone afin de fonctionner en mode sécurisé

Configuration

Étape 1. Dans CUCM, accédez à **Cisco Unified CM Administration > Device > Phone**.

Étape 2. Recherchez et sélectionnez le téléphone à partir duquel vous souhaitez récupérer les certificats.

Étape 3. Dans la page de configuration du téléphone, accédez à la section **Informations CAPF (Certification Authority Proxy Function)**.

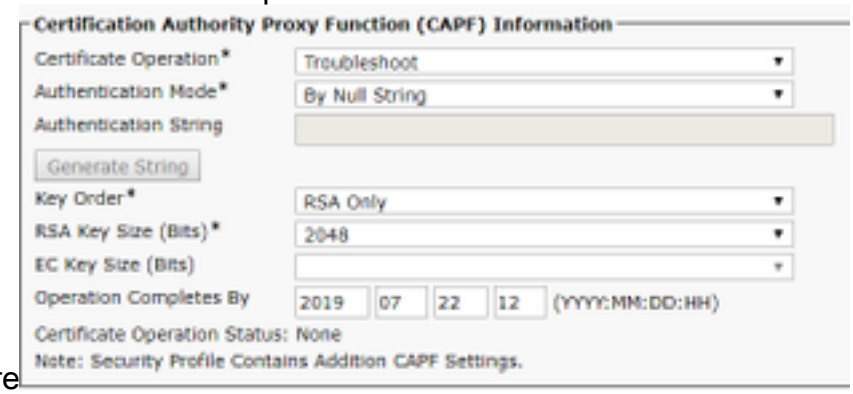
Étape 4. Comme l'illustre l'image, appliquez les paramètres suivants :

Opération de certificat : Dépannage

Mode d'authentification: Par chaîne Null

Taille de clé (bits) : 1024

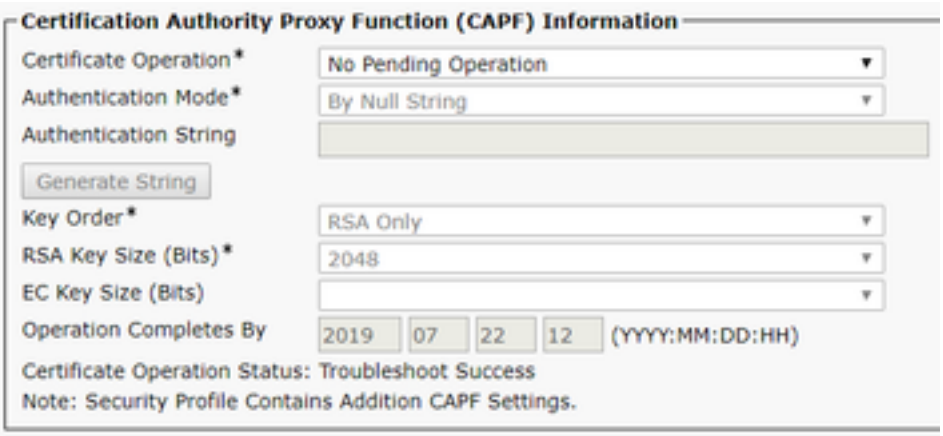
L'opération se termine par : Date future



Étape 5. Cliquez sur **Enregistrer** et **réinitialiser** le téléphone.

Étape 6. Une fois que ce périphérique est de nouveau enregistré dans le cluster CUCM, assurez-vous dans la page de configuration du téléphone que l'opération de dépannage est terminée

comme indiqué sur l'image :



Étape 7. Ouvrez une session SSH pour le serveur de publication CUCM et exécutez la commande pour répertorier les certificats associés au téléphone, comme indiqué dans l'image :

liste de fichiers activelog /cm/trace/capf/sdi/SEP<adresse_MAC>*

```
admin:file list activelog /cm/trace/capf/sdi/SEP*
SEPF87B204EED99-L1.cer                    SEPF87B204EED99-M1.cer
dir count = 0, file count = 2
admin:
```

Il existe deux options pour les fichiers à afficher :

Uniquement MIC : SEP<Adresse_MAC>-M1.cer

MIC et LSC : SEP<MAC_Address>-M1.cer et SEP<MAC_Address>-L1.cer

Étape 8. Pour télécharger les certificats, exécutez cette commande : **fichier get activelog /cm/trace/capf/sdi/SEP<adresse_MAC>***

Un serveur SFTP (Secure File Transfer Protocol) est requis pour enregistrer le fichier comme indiqué dans l'image

```
admin:file get activelog /cm/trace/capf/sdi/SEPF87B204EED99-M1.cer
Please wait while the system is gathering files info ...
 Get file: /var/log/active/cm/trace/capf/sdi/SEPF87B204EED99-M1.cer
done.
Sub-directories were not traversed.
Number of files affected: 1
Total size in Bytes: 1159
Total size in Kbytes: 1.1318359
Would you like to proceed [y/n]? y
SFTP server IP: 10.1.99.201
SFTP server port [22]:
User ID: alegarc2
Password: *********
Download directory: /

The authenticity of host '10.1.99.201 (10.1.99.201)' can't be established.
RSA key fingerprint is 33:83:bd:c7:8e:4d:1c:5a:b3:be:b2:e2:38:2b:fc:26.
Are you sure you want to continue connecting (yes/no)? yes
```

Informations connexes

- Certificats de téléphone IP