Come scaricare certificati da telefoni IP Cisco

Sommario

Introduzione

Questo documento descrive la procedura per recuperare i certificati da un telefono IP Cisco quando il servizio CAPF (Cisco Authority Proxy Function) è in esecuzione nell'editore Cisco Unified Communications Manager (CUCM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Certificati SSL nel telefono
- amministrazione CUCM
- Gestione Command Line Interface (CLI) in CUCM

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Unified Communications Manager (CUCM) versione 11.5.1.1900-26
- Cisco IP Phone 8811 - sip88xx.12-5-1SR1-4

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il servizio CAPF deve essere attivo nell'editore CUCM e il certificato CAPF in Cisco Unified OS Administration deve essere aggiornato.

Per i Cisco IP Phone, esistono due alternative di certificati installati:

- MIC (Certificato del produttore installato)
- MIC e LSC (Certificato significativo a livello locale)

I telefoni sono preinstallati con il certificato MIC e non possono essere eliminati né rigenerati. Inoltre, non è possibile utilizzare MIC una volta scaduta la validità. I MIC sono certificati chiave a 2048 bit firmati da Cisco Certificate Authority.

La chiave LSC possiede la chiave pubblica per il telefono IP Cisco, che è firmata dalla chiave privata CUCM CAPF. Non è installato sul telefono per impostazione predefinita e questo certificato è necessario per il telefono per poter funzionare in modalità protetta

Configurazione

Passaggio 1. In CUCM, selezionare **Cisco Unified CM Administration > Device > Phone** (Amministrazione Cisco Unified CM > Dispositivo > Telefono).

Passaggio 2. Individuare e selezionare il telefono da cui recuperare i certificati.

Passaggio 3. Nella pagina di configurazione del telefono, passare alla sezione **Informazioni sulla funzione proxy dell'autorità di certificazione (CAPF)**.

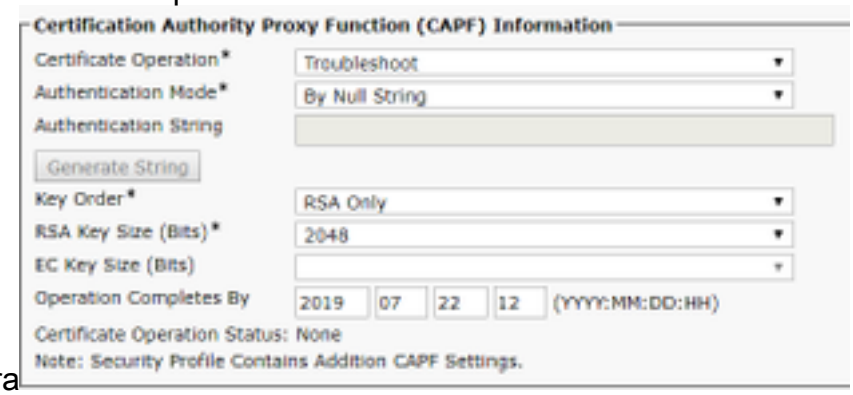
Passaggio 4. Come mostrato nell'immagine, applicare i seguenti parametri:

Operazione certificato: Risoluzione dei problemi

Modalità di autenticazione: Per stringa null

Dimensioni Chiave (Bit): 1024

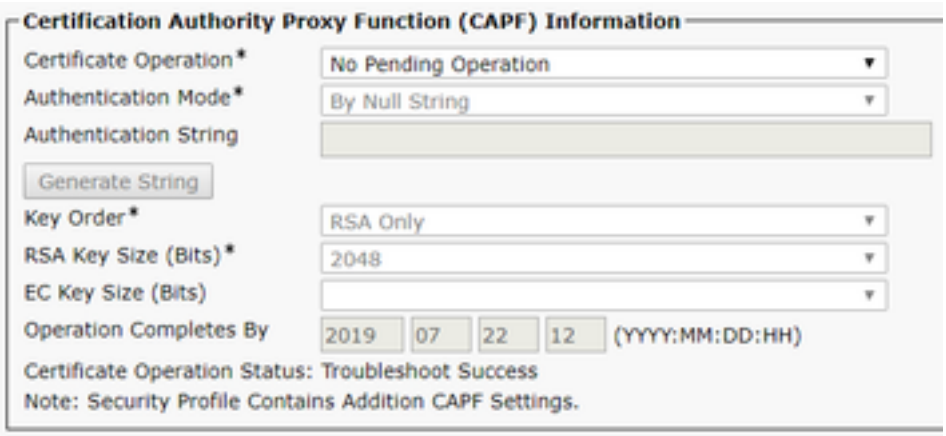
Operazione completata entro: Data futura



Passaggio 5. Fare clic su **Save** and **Reset** the phone (Salva e ripristina il telefono).

Passaggio 6. Dopo aver registrato nuovamente il dispositivo nel cluster CUCM, verificare nella pagina di configurazione del telefono che l'operazione di risoluzione dei problemi sia stata completata come mostrato

nell'immagine:



Passaggio 7. Aprire una sessione SSH per il server CUCM Publisher ed eseguire il comando per visualizzare un elenco dei certificati associati al telefono, come mostrato nell'immagine:

elenco file activelog /cm/trace/capf/sdi/SEP<Indirizzo_MAC>*

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

Per i file da elencare sono disponibili due opzioni:

Solo MIC: SET<Indirizzo_MAC>-M1.cer

MIC e LSC:SEP<Indirizzo_MAC>-M1.cer e SEP<Indirizzo_MAC>-L1.cer

Passaggio 8. Per scaricare i certificati, eseguire questo comando: **file get activelog /cm/trace/capf/sdi/SEP<Indirizzo_MAC>***

Ènecessario un server SFTP (Secure File Transfer Protocol) per salvare il file come mostrato nell'immagine

```
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
```

Informazioni correlate

- Certificati per telefoni IP