How to Download Certificates from Cisco IP Phones

Contents

Introduction

This document describes the procedure in order to retrieve certificates from a Cisco IP Phone when Cisco Authority Proxy Function (CAPF) service runs in Cisco Unified Communications Manager (CUCM) publisher.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SSL Certificates in phone
- CUCM administration
- Command Line Interface (CLI) management in CUCM

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Unified Communications Manager (CUCM) version 11.5.1.11900-26
- Cisco IP Phone 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

CAPF service must be active in CUCM publisher and CAPF certificate under Cisco Unified OS Adminsitration must be up-to-date.

For Cisco IP Phones, there are two alternatives of certificates installed on them:

- MIC (Manufacturer Installed Certificate)
- MIC and LSC (Locally Significant Certificate)

Phones are pre-installed with the MIC certificate and it cannot be deleted neither regenerated. Also, MIC cannot be used once the validity is expired. MICs are 2048-bit key certificates that are signed by the Cisco Certificate Authority.

The LSC possesses the public key for the Cisco IP phone, which is signed by the CUCM CAPF private key. It is not installed on the phone by default and this certificate is required for the phone in order to operate in secure mode

Configure

Step 1. In CUCM, navigate to **Cisco Unified CM Administration > Device > Phone**.

Step 2. Find and select the phone which certificates you want to retrieve from.

Step 3. In the phone configuration page, navigate to **Certification Authority Proxy Function (CAPF) Information** section.

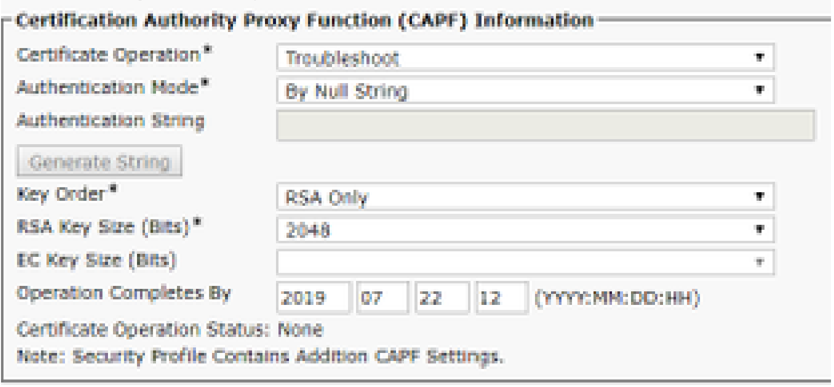
Step 4. As shown in the image, apply these parameters:

Certificate Operation: Troubleshoot

Authentication Mode: By Null String

Key Size (Bits): 1024

Operation Completes By: Date in the future



Certification Authority Proxy Function (CAPF) Information

Certificate Operation*: Troubleshoot

Authentication Mode*: By Null String

Authentication String:

Key Order*: RSA Only

RSA Key Size (Bits)*: 2048

EC Key Size (Bits):

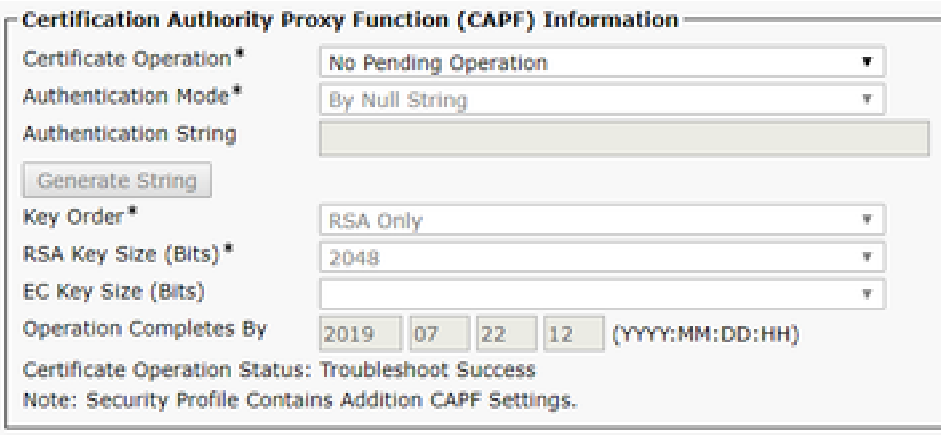
Operation Completes By: 2019 07 22 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

Step 5. Click on **Save** and **Reset** the phone.

Step 6. Once that device is registered back in CUCM cluster, ensure in phone configuration page that troubleshoot operation has completed as shown in the image:



Certification Authority Proxy Function (CAPF) Information

Certificate Operation* No Pending Operation

Authentication Mode* By Null String

Authentication String

Key Order* RSA Only

RSA Key Size (Bits)* 2048

EC Key Size (Bits)

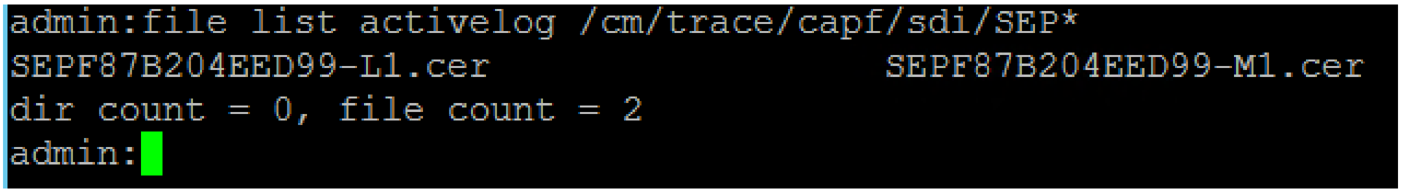
Operation Completes By 2019 07 22 12 (YYYY:MM:DD:HH)

Certificate Operation Status: Troubleshoot Success

Note: Security Profile Contains Addition CAPF Settings.

Step 7. Open an SSH session for the CUCM Publisher server and run the command to list the certificates associated to the phone as shown in the image:

file list activelog /cm/trace/capf/sdi/SEP<MAC_Address>*



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

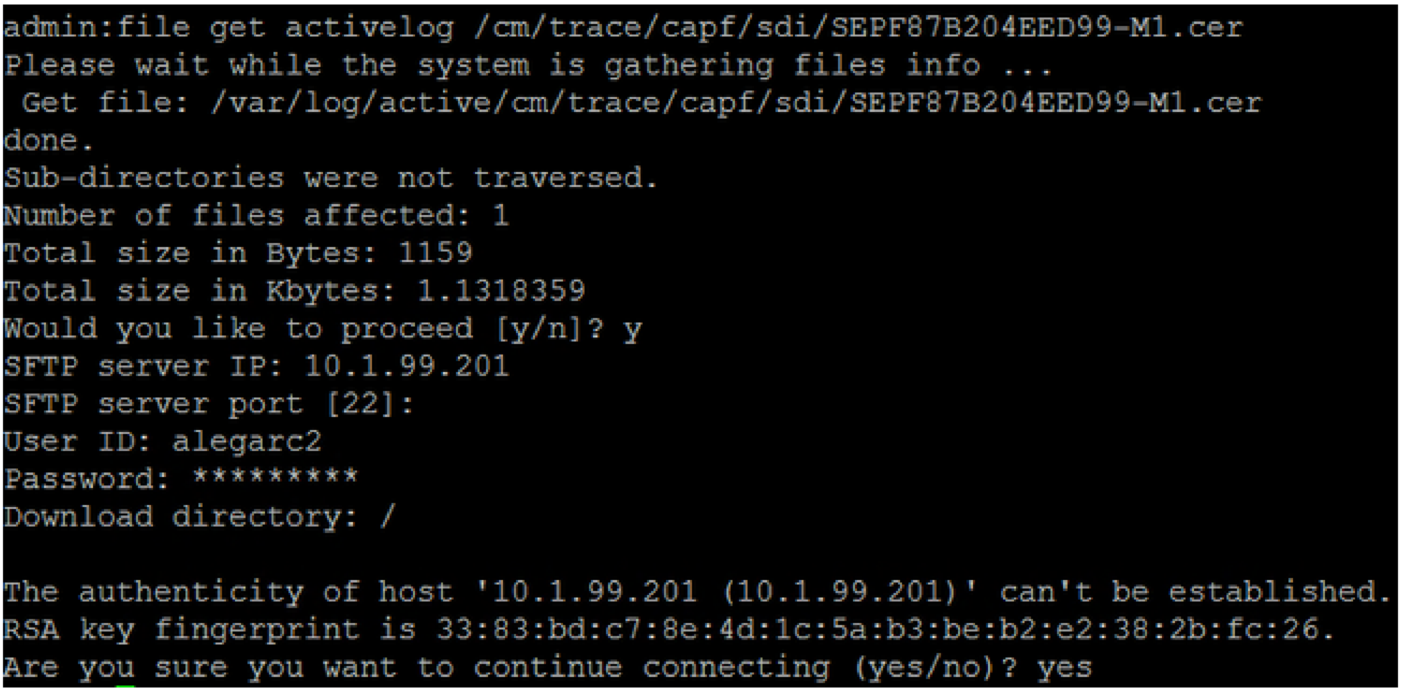
There are two options for the files to be listed:

Only MIC: SEP<MAC_Address>-M1.cer

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

Step 8. In order to download the certificates, run this command: **file get activelog /cm/trace/capf/sdi/SEP<MAC_Address>***

An Secure File Transfer Protocol (SFTP) server is required to save the file as shown in the 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
```

Related Information

- **IP Phone certificates**