

Troubleshoot Common Issues with Certificate Renewal in CUCM

Introduction

This document describes common issues after regenerate certificates in Cisco Unified Communications Manager (CUCM) and how to resolve them.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CUCM certificate renewal process
- CUCM GUI interface
- Expressway servers
- Device registration with CUCM process
- Certificate Authority Proxy Function
- Security Guide for Cisco Unified Communications Manager

Components Used

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

- CUCM version 15

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.

Business Impact

This table displays the business impact of each certificate renewal in your operation. Review the information carefully. Renew required certificates after hours or in quiet periods, based on the risk level of each certificate.

● Low Impact
 ● Medium Impact.
 ● High Impact.

Type	Risk	Trust List	Impact	Phone Restart	Service Restart
Tomcat	●	-	Web services, SSO, EM/EMCC Login	None	Tomcat
IPSec	●	-	DRS, Ipsec Tunnels	None	DRF Master/Local
CAPF	●	CTL + ITL	LSC must be updated, secure features	All	CAPF
Callmanager	●	CTL + ITL	Registration, TL issues, Trunks, CTI	All	CM,CTI,TFTP
TVS	●	ITL	Verification of TLs, CFG files, https connection	Some	TVS
ITLRecovery	●	CTL + ITL	Signer or SAST backup for ITL/CTL	All	

Scenario 1: Phones Not Register after Call Manager, TVS and ITL Certificate Renewal



Note: This scenario apply to deployments under CUCM mixed-mode and non-secure clusters, in addition, applies to the self-signed certificates and CA certificates.

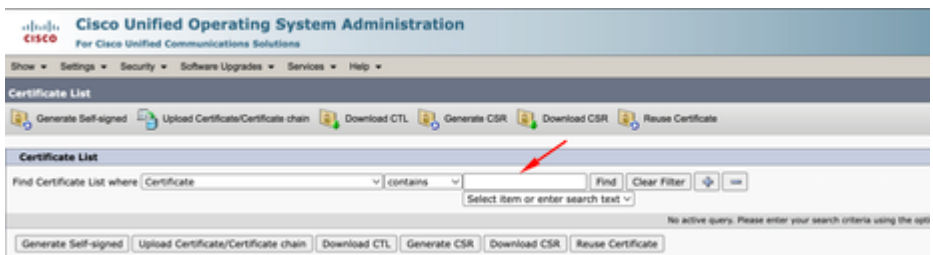
When Call Manager , TVS and ITL certificates expired and they were renewed at the same time, It causes to have all our phones in an unregistered state thta causes a major Impact on the system, this is an expected behaviours as we trigger the phones to not trust in the CUCM.

Verification

1. Ensure the certificates are already expired under **Cisco Unified OS Administration >Security >Certificate Management**



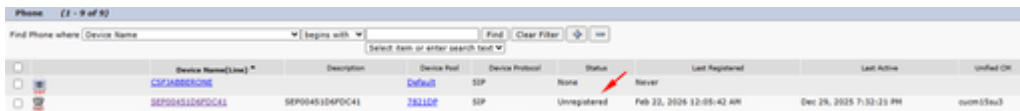
2. Search by Callmanager, TVS or ITL under the filter at the top of the page and use the contains or begins with options:



3. The certificates must see up to date and verify under the **Expiration** column (same for TVS and ITL certificates)



4. Once verified everything is good after the certificate renewal, the phones are shown as **Unregistered** state.



Solution

There is 2 options to fix the issue:

1. Perform a factory reset of the phone that allows the phone erase the currently security settings and allow the phone to grab the new certificates
2. Update the ITL and CTL certificates from CLI on the publisher node and use the command **utils itl reset localkey**.
This step affects all phones including registered phones, make sure to perform this after hours.



Scenario 2: Single sign-on does not work after Tomcat certificate renewal



Note: This scenario can apply to deployments that uses cluster-wide or per-node agreement for single sign-on configuration

Login within CUCM with Single Sign-on (SSO) it displays an error message "Error while processing saml response" or "Error while processing saml response Failed to decrypt the secret key"

Verification

1. Ensure all nodes contains a valid tomcat certificate if self-signed or contains the new multi-san tomcat certificate associated.
2. Use **set samltrace level debug** in all CUCM nodes via CLI in order to activate SSO logs on debug level
3. Recreate the issue by login again to CUCM and use SSO method.
4. Collect Tomcat SSO logs after the incident, and verify you get this message:

```
2026-01-10 06:06:31,274 ERROR [http-nio-81-exec-157]  cpi.sso.saml.sp.security.authentication
com.sun.identity.saml2.common.SAML2Exception: Failed to decrypt the secret key.
    at com.sun.identity.saml2.xmlenc.FMEncProvider.getEncryptionKey(FMEncProvider.
    at com.sun.identity.saml2.xmlenc.FMEncProvider.decrypt(FMEncProvider.java:607)
    at com.sun.identity.saml2.assertion.impl.EncryptedAssertionImpl.decrypt(Encryp
...

```

Solution

Export of CUCM metadata after Tomcat certificate renewal and import to the Identity Provider Server to ensure they have the new tomcat certificate for this communication.

Procedure to renew tomcat with SSO deployment enabled:



Caution: Technical Assistance Center (TAC) recommends the next steps in order to prevent any issue after the renew of Tomcat certificate, recommend to perform this procedure after hours.

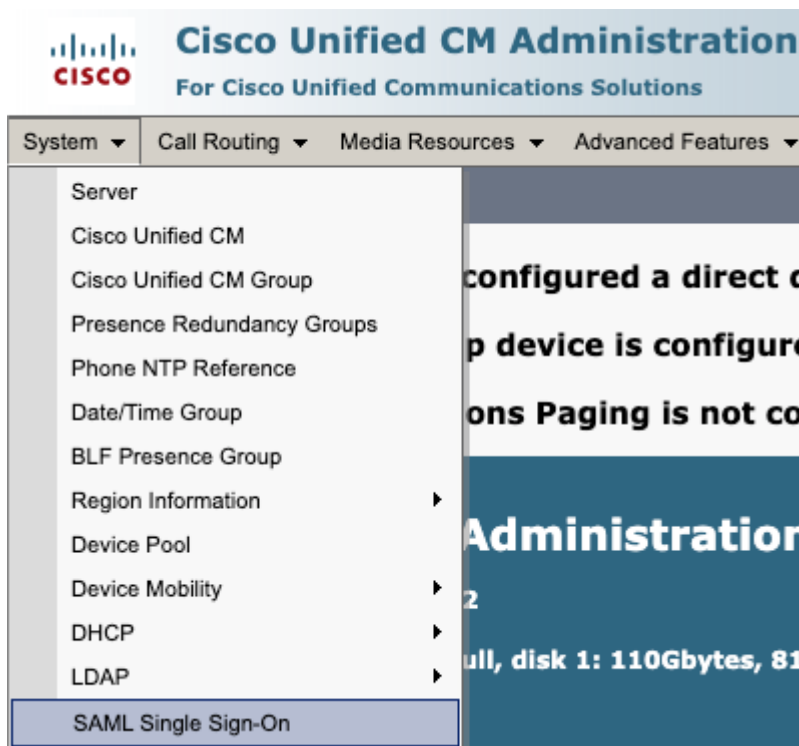


Low Impact

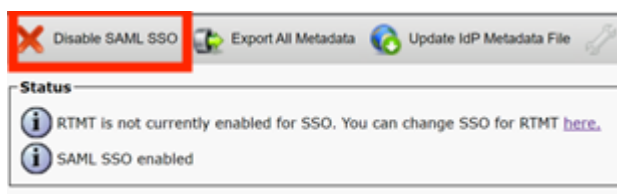
1. Disable SSO in all CUCM nodes



- Access to **CM administration > System > SAML Single Sign-on**



- Select **Disable SAML SSO**



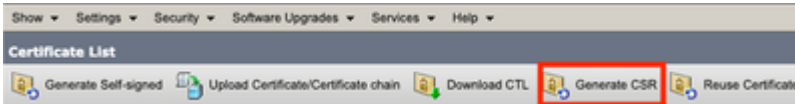
- This process needs to be performed in all the rest of the nodes via GUI if per-node agreement is used.

2. Renew Tomcat certificate in CUCM cluster

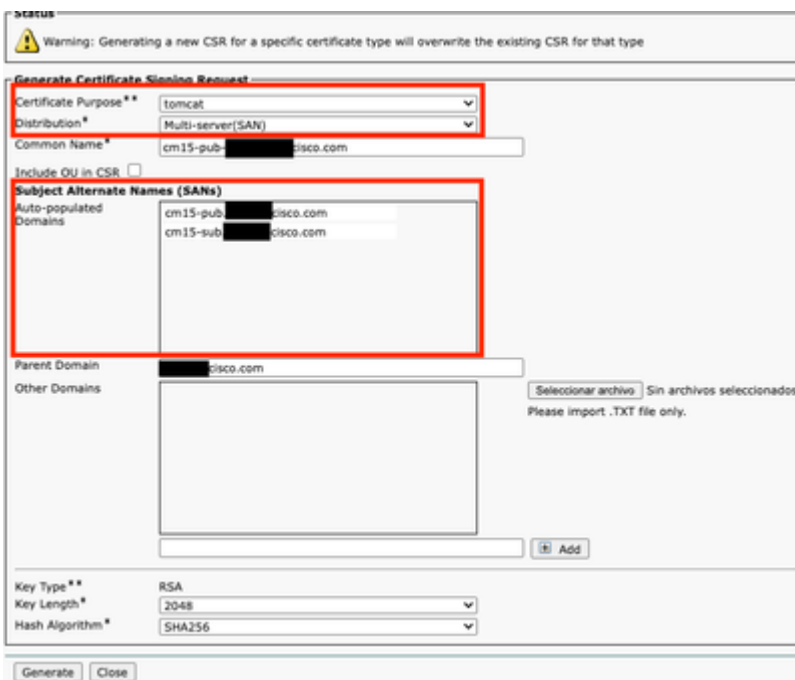


Overall procedure to renew Tomcat multi-san certificate in CUCM cluster:

- Navigate to **OS administration > Security > Certificate management.**
- Select **Generate CSR**



- Select **Tomcat** in Certificate Purpose.
- Select **Multi-SAN** in Distribution.
- Ensure all nodes in the cluster are listed under **Auto-populated Domains**.



- Select **Generate**. Ensure CSR is created in all the nodes in the cluster.
- Download the generated CSR from CUCM publisher and sign it with a Certificate Authority (CA) server.
- Go to **OS administration > Security > Certificate management**. Select **Upload certificate/Certificate chain**.
- Upload CA certificates as Tomcat-trust.
- Repeat step 6 and now upload the Tomcat signed certificate as Tomcat.
- Once completed and verified all nodes have the new tomcat certificate applied, restart Tomcat service through CLI in all the nodes in the cluster with this command **utils service restart Cisco Tomcat**.

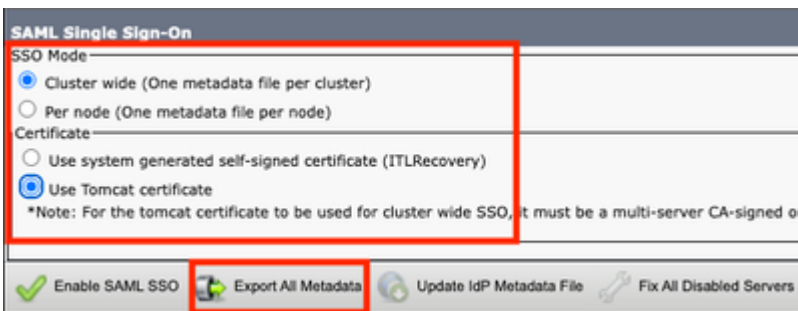
For more information refer to the this documentation:

- [Regenerate Tomcat self-signed certificate](#)
- [Regenerate Tomcat CA-signed certificate.](#)

3. Export Service Provider (SP) metadata



- Go to **CM administration > System > Single Sign-On**
- Configure SSO options (In this case cluster wide on **SSO mode** and **Use tomcat certificate** on certificate is configured as an example) then select **export all metadata**



- Import SP metadata to the Identity Provider (IdP) server. For more information, refer to [Configure SAML SSO on Identity Provider](#)

4. Enable SSO in CUCM cluster



- Go to **CM administration > System > Single Sign-On**
- With same SSO options selected while the export of CUCM metadata, select **Enable SAML SSO** and select **continue**.

SAML Single Sign-On

SSO Mode

Cluster wide (One metadata file per cluster)

Per node (One metadata file per node)

Certificate

Use system generated self-signed certificate (ITLRecovery)

Use Tomcat certificate


*Note: For the tomcat certificate to be used for cluster wide SSO, it must be a multi-server CA-signed or

Enable SAML SSO


Export All Metadata

Update IdP Metadata File

Fix All Disabled Servers

 Web server connections will be restarted

Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.


 Click "Export All Metadata" button

If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.


If IDP is provisioned with cluster-wide SP metadata, you need to enable cluster-wide SAML SSO. If IDP is provisioned with per-node SP metadata, you need to enable per-node SAML SSO.

- If cluster-wide, this step is available to check multi-san certificate in all the nodes, select **Test for multi-server tomcat certificate**. once completed, select **Next**.

SAML Single Sign-On Configuration

 Next

Status

 Status: Ready

Test for Multi-Server tomcat certificate

The criteria for enabling clusterwide SSO is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:

- 1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
- 2) Click on Generate CSR
- 3) Select Certificate Purpose as Tomcat
- 4) Select Distribution as "Multi-Server"
- 5) Click Generate
- 6) Download the CSR and get it signed from the CA of your choice
- 7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
- 8) Restart Tomcat service on all the nodes in the cluster
- 9) Restart TFTP service on all the TFTP nodes in the cluster

For self-signed Multi-server tomcat certificate:

- 1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
- 2) Click on Generate self signed Multi-server tomcat certificate
- 3) Select Certificate Purpose as Tomcat
- 4) Select Distribution as "Multi-Server"
- 5) Click Generate
- 6) Restart Tomcat service on all the nodes in the cluster
- 7) Restart TFTP service on all the TFTP nodes in the cluster

If the above steps have been completed, click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage

- Upload IdP metadata, select **Import IdP Metadata** and once complete, select **Next**

SAML Single Sign-On Configuration

Next

Status

- Status: Ready
- Import succeeded for all servers

Import the IdP Metadata Trust File

This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.

1) Select the IdP Metadata Trust File

Choose File No file chosen

2) Import this file to the Collaboration servers

This action must be successful for at least the Publisher before moving on to the next task in this wizard.

Import IdP Metadata Import succeeded for all servers

Next Cancel

- On Test SSO Setup select an user with **Standard CCM Super Users** group assigned, and select **Run SSO Test** until get success.

SAML Single Sign-On Configuration

Back

Status

- The server metadata file must be installed on the IdP before this test is run.

Test SSO Setup

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on any

1) Pick a valid username to use for this test

You must already know the password for the selected username.
This user must have administrator rights and also exist in the IdP.

Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

Valid administrator Usernames

admin@

2) Launch SSO test page

Run SSO Test...

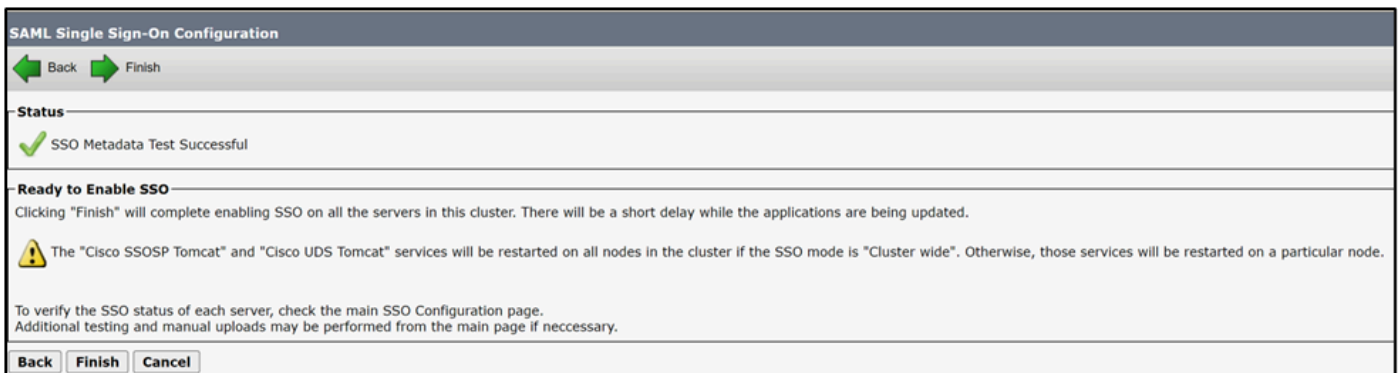
Back Cancel



4. Restart required services after SSO enabled.



- Enablement of SSO restart the tomcat service.



However, TAC recommend to restart Tomcat (**utils service restart Cisco Tomcat**) and UDS Tomcat (**utils service restart CiscoUDSTomcat**) service manually in all the nodes after SSO enablement process.

Scenario 3: Mobility and Remote Access registration issues after certificate renewal

Webex app unable to register with CUCM via Mobility and Remote Access (MRA) after Call manager, Tomcat and Expressway C certificates renew on mixed-mode deployments.

Verification

1. CUCM Call manager and Tomcat certificate are CA signed certificates.
2. CUCM and Expressway deployment runs on mixed-mode (TLS).
3. inspect Expressway-C logs shows "SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca".
<#root>

```
2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]: UTCTime="2026-01-29 19:01:16,974" Module
HTTPMSG:
|GET /CSFmarcoalh.cnf.xml HTTP/1.1
Host: expc.cisco.com:6972
Accept: */*
Cookie:<CONCEALED>
User-Agent: WebEx/0.0.0.0
TrackingID: fxxxxxxx-86f6-4030-8259-0b768c07723e
Client-ip: xxx.xxx.xxx.xxx
X-Forwarded-For: xxx.xxx.xxx.xxx, 127.0.0.1
Via: https/1.1 vcs[0fxxxxxx-c853-xxxx-aa16-0a290bf56fc8] (ATS), http/1.1 vcs[5xxxxxxx-7feb-4xxx-9
|
2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]:[ET_NET 1]ERROR:SSL connection failed for
SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca
```

Solution

Export and import certificates between CUCM and Expressway-C to ensure trust relation.



Caution: TAC recommend to perform this after hours as this procedure requires services restart. Business Impact is



Medium Impact.

1. Procedure to complete trust relation between CUCM and Expressway with CA signed certificates



Navigate to **OS administration > Security > Certificate management** and download the root CA certificate and intermediate (if any) that signs Call Manager and Tomcat certificate.

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR Download CSR Reuse Certificate

Status
18 records found

Certificate List (1 - 18 of 18) Rows per Page

Find Certificate List where Certificate begins with callmanager Find Clear Filter

Certificate	Common Name/Common Name_SerialNumber	Usage	Type	Key Type	Distribution	Issued By
CallManager	cucm15sub- 2766.local_6f9000000c374e76d635a3840d0000000000c	Identity	CA- signed	RSA	Multi-server(SAN)	2766-ca-1
CallManager- ECDSA						
CallManager- trust	2766-ca- 1_642238c85deb1c8b48ad6e46d0ab241c	Trust	Self- signed	RSA	2766-ca-1	2766-ca-1

Then navigate to **Expressway-C > Maintenance > Security > Trusted CA certificate** and upload the CA certificate of Call Manager and Tomcat certificate.

Maintenance

- Upgrade
- Logging
- Smart licensing
- Email Notifications
- Tools >
- Security**
 - Trusted CA certificate
 - Server certificate
 - CRL management
 - Client certificate testing
 - Certificate-based authentication configuration
 - Secure traversal test
 - Ciphers
 - SSH configuration
- Backup and restore
- Diagnostics >
- Maintenance mode
- Language
- Restart options

Choose File No file chosen

Upload

Select the file containing trusted CA certificates Choose File No file chosen

Trusted CA certificate You are here: [Maintenance](#)

File uploaded: CA certificate file uploaded. File contents - Certificates: 1, CRLS: 0.

Type	Issuer	Subject	Expiration date	Validity	View
<input type="checkbox"/> Certificate	[REDACTED]	Matches Issuer	Mar 29 2028	Valid	View (decoded)
<input type="checkbox"/> Certificate	[REDACTED]:2766-ca-1	Matches Issuer	Feb 09 2028	Valid	View (decoded)

[Show all \(decoded\)](#)
[Show all \(PEM file\)](#)
[Delete](#)
[Select all](#)
[Unselect all](#)



Note: In scenarios with Call Manager and Tomcat certificate as self-signed, download the actual Call Manager and Tomcat certificate and upload it to Expressway.



Navigate to **Expressway-C > Maintenance > Security > Trusted CA certificate > Show all (PEM file)**

Trusted CA certificate

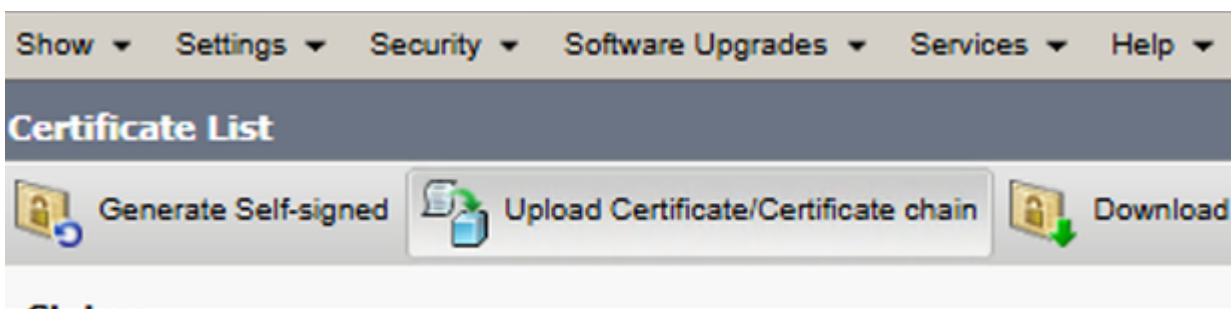
Type	Issuer
<input type="checkbox"/> Certificate	[REDACTED] ADSERVER-CA
<input type="checkbox"/> Certificate	[REDACTED]:2766-ca-1

[Show all \(decoded\)](#)
[Show all \(PEM file\)](#)
[Delete](#)
[Select all](#)
[Unselect all](#)

Copy the PEM value of the CA certificate that signs Expressway-C and save it in a txt file.

```
expcert.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIDdzCCA1+gAwIBAgIQFBGTWjxDrp1B5NgcCLc0FTANBgkqhkiG9w0BAQsFADBO
MRUwEwYKCZImiZPyLGBGRYFbG9jYWwxZjZAVBgoJkiaJk/IsZAEZFgdicm9qZWRh
[REDACTED]
jsFtVBS1D0ReW61KU5gbIHS19QwbCxZHxd4a
-----END CERTIFICATE-----
```

Navigate to **OS administration > Security > Certificate management** and select **Upload Certificate/Certificate Chain** and upload the expressway-C CA cert as Tomcat-trust and Call Manager-trust



Upload Certificate/Certificate chain

Upload Close

Status

i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* CallManager-trust

Description(friendly name)

Upload File Choose File expcert.pem

Upload Close



Restart required services in CUCM cluster:

- Navigate to **Cisco Unified Serviceability > Tools > Control Center - Feature Services** and restart **Cisco CallManager** service in all the nodes that runs it.
- Navigate to **Cisco Unified Serviceability > Tools > Control Center - Feature Services** and restart **Cisco TFTP** service in all the nodes that runs it.
- Restart **Tomcat** service in all the nodes in the cluster via CLI with the command **utils service restart Cisco Tomcat**.
- Restart **Cisco HAproxy** service in all the nodes in the cluster via CLI with the command **utils service restart Cisco HAProxy**.

Scenario 4: Renew of Certificate Authority Proxy Function certificate cause

Scenario 4.1: 802.1x authentication failed

Phone do not authenticate with ASA after regenerate Certificate Authority Proxy Function(CAPF) certificate on CUCM publisher.

Verification

Verification

1. Affected Phones contains security profile with TLS mode enabled.

Phone Security Profile Information

Product Type: Cisco 8845
Device Protocol: SIP

Name*
Description
Nonce Validity Time*
Device Security Mode
Transport Type*

Enable Digest Authentication
 TFTP Encrypted Config
 Enable OAuth Authentication

2. Affected phones have LSC certificated installed.
3. Ensure CAPF certificate is up to date.

Certificate List (1 - 15 of 15)

Find Certificate List where begins with

Select item or enter search text

Certificate *	Common Name/Common Name_SerialNumber	Usage	Type	Key Type	Distribution	Issued By	Expiration
CAPF	CAPF-0bc17206	Identity	Self-signed	RSA	cm15- .cisco.com	CAPF-0bc17206	10/01/2028

4. Login to CUCM publisher and use the command **show ctl** that shows old CAPF certificate serial number.
5. Then change the phone security profile to non secure.

Solution

Regenerate CTL file on CUCM and restart required services to ensure phones gets the new CTL file with CAPF file.



Caution: TAC recommend to perform this after hours as this procedure requires services restart. Business Impact is



Medium Impact.

Procedure to ensure renew of CAPF successfully.



```

admin:utils ctl update CTLfile
This operation will update the CTLfile. Do you want to continue? (y/n): y

Updating CTL file
CTL file Updated
Please reset all Encrypted and Authenticated phones for the CTL file updates to take effect.

```

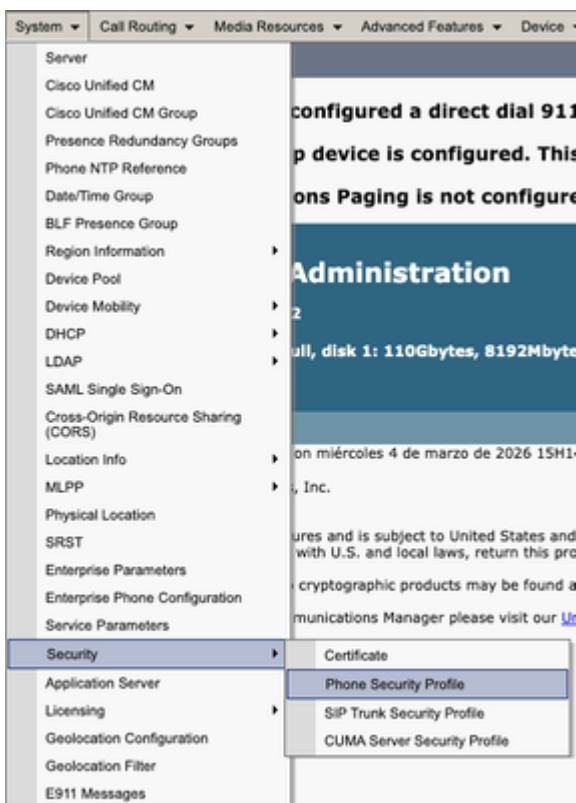
Update CTL file after CAPF regeneration. Log into the CLI of the Publisher and enter the command **utils ctl update CTLFile**.



1. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Feature Services** in CUCM publisher and restart **CAPF** service.
2. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Network Services** and restart **Cisco Trust Verification Service** in all the nodes that runs it.
3. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Feature Services** and restart **Cisco TFTP Service** in all the nodes that runs it



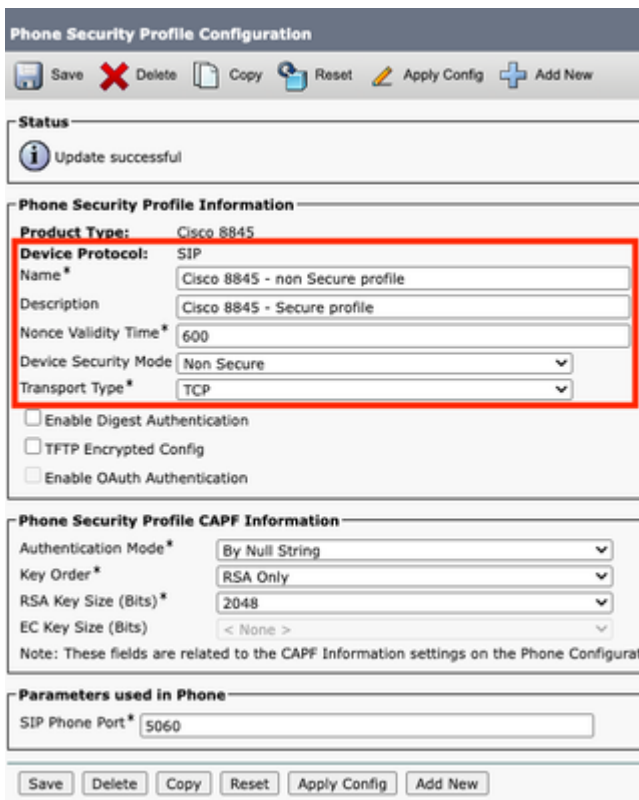
- Navigate to **CM administration > System > Security > Phone Security Profile**.



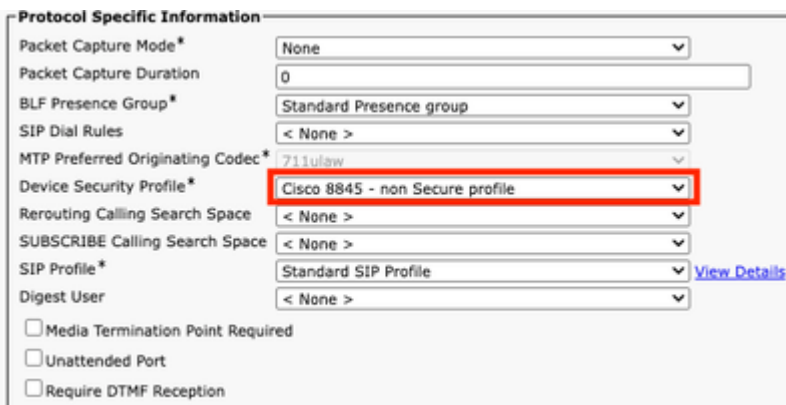
- Copy the current phone security profile assigned to the required phones.



- Change Name and Device Security Mode to **Non Secure** and select **Save and Apply Config** to apply this change to all the required phones.



- Apply the created **Device Security Profile** to required phones configuration, select **Save and Apply Config**.





Use CAPF information section in device configuration of affected phones to install LSC certificate in the required phones.

- In CAPF information, select **Install/Upgrade** in Certificate Operation.

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*

Authentication Mode*

Authentication String

Key Order*

RSA Key Size (Bits)*

EC Key Size (Bits)

Operation Completes By (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Additional CAPF Settings.

- Select **Save and Apply Config**.
- Wait until Certificate Operation Status shows **Operation completed**.



In **Protocol Specific Information** section on **Phone Configuration**, select the Security profile with TLS enabled that was created.

Protocol Specific Information

Packet Capture Mode*

Packet Capture Duration

BLF Presence Group*

SIP Dial Rules

MTP Preferred Originating Codec*

Device Security Profile*

Rerouting Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

Digest User

Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status

Status: Ready

Phone Security Profile Information

Product Type: Cisco 8845
Device Protocol: SIP

Name*
Description
Nonce Validity Time*
Device Security Mode
Transport Type*

Enable Digest Authentication
 TFTP Encrypted Config
 Enable OAuth Authentication

Related Information

- <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/214231-certificate-regeneration-process-for-cis.html>
- <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/217138-regeneration-of-cucm-ca-signed-certifica.html>
- <https://www.cisco.com/c/en/us/support/docs/content-networking/certificates/213295-how-to-install-an-lsc-on-a-cisco-ip-phon.html>
- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-2/mra/exwy_b_mra-deployment-guide-x152.html