

Configure Tomcat Certificate Reuse for CallManager in CUCM 14

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[1. Set Tomcat Certificate as Multi-SAN](#)

[Self-Signed](#)

[CA-Signed](#)

[2. Reuse Tomcat Certificate for CallManager](#)

[Verify](#)

[Related Information](#)

Introduction

This document describes how to reuse the Multi-SAN Tomcat certificate for CallManager on a Cisco Unified Communications Manager (CUCM) server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CUCM certificates
- Real-Time Monitoring Tool (RTMT)
- Identity Trust List (ITL)

Components Used

The information in this document is based on CUCM 14.0.1.13900-155.

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.

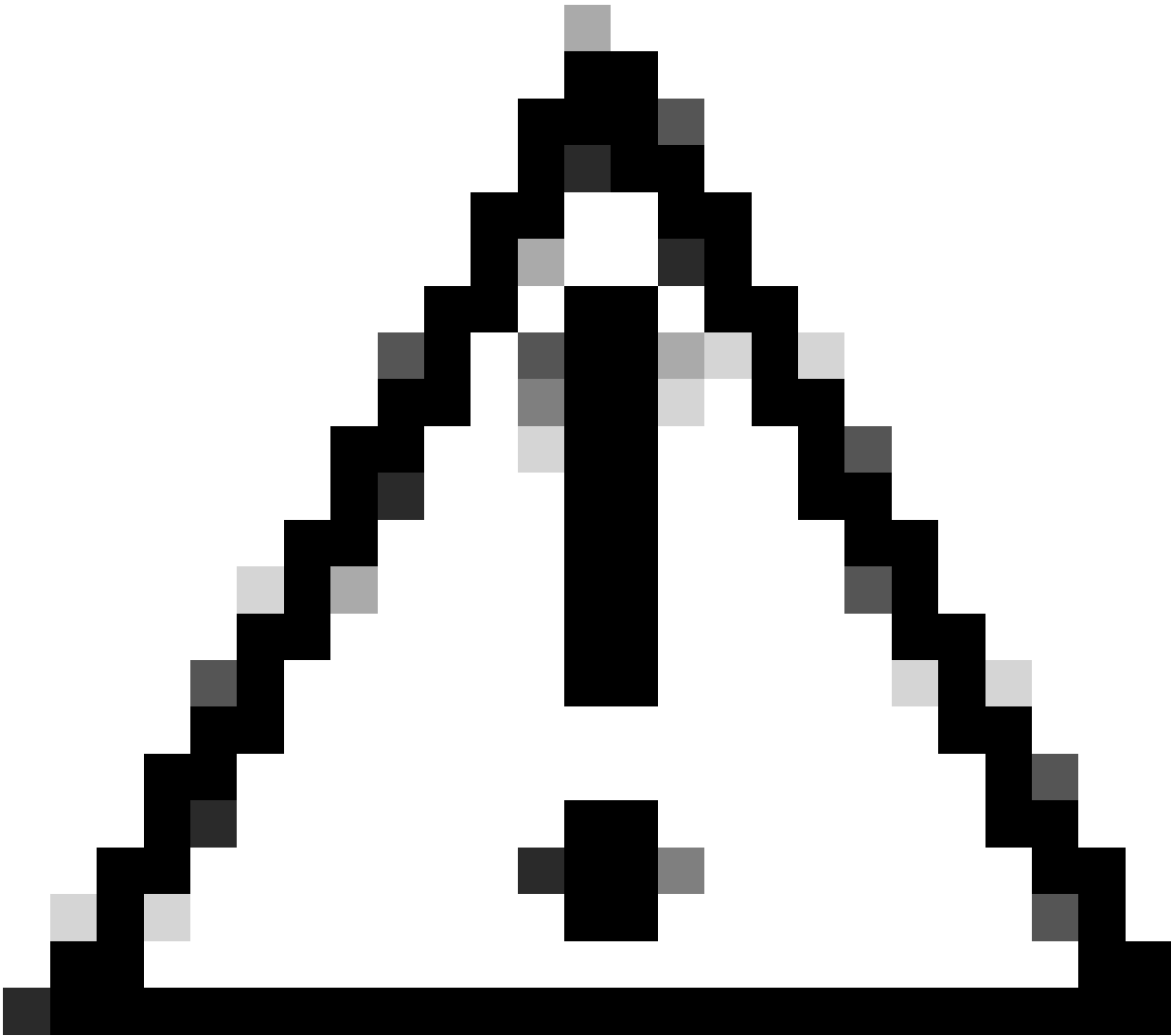
Background Information

The two main services for CUCM are Tomcat and CallManager. In the earlier versions, different certificates for each service were required for the complete cluster. In CUCM version 14, a new feature was added to reuse the Multi-SAN Tomcat certificate for CallManager service as well. The benefits of using this feature

are:

- Reduces the cost of getting two certificates signed by a Public Certificate Authority(CA) for one cluster of CA-signed certificates.
- This feature reduces the size of the ITL file, thereby reducing the overhead.

Configure



Caution: Before you upload a Tomcat certificate, verify Single sign-on (SSO) is disabled. In case it is enabled, SSO must be disabled and re-enabled once the Tomcat certificate regeneration process is finished.

1. Set Tomcat Certificate as Multi-SAN

In CUCM 14, the Tomcat Multi-SAN certificate can be Self-Signed or CA-signed. If your Tomcat certificate is already Multi-SAN, skip this section.

Self-Signed

Step 1. Log in to Publisher > Operating System (OS) Administration and navigate to Security > Certificate Management > Generate Self-Signed.

Step 2. Choose Certificate Purpose: tomcat > Distribution: Multi-Server SAN. It auto-populates the SAN domains and the parent domain.

Generate New Self-signed Certificate

Generate Close

Status

Generating a new certificate will overwrite any existing certificate information. When generating Call Manager, CAPF, or TVS, all devices will be reset automatically.

Generate Self-signed

Certificate Purpose** tomcat

Distribution* Multi-server(SAN)

Common Name* 14pub.

Subject Alternate Names (SANs)

Auto-populated Domains

14pub.

14sub.

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

Validity Period (in years)* 5

Generate Close

i *- indicates required item.

i **When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

Generate Self-Signed Multi-SAN Tomcat Certificate Screen

Step 3. Click Generate, and validate that all your nodes are listed under the Certificate upload operation successful message. Click Close.

Generate New Self-signed Certificate

Generate Close

Status

i Certificate upload operation successful for the nodes 14sub., 14pub.

i Restart Cisco Tomcat Service for the nodes 14sub., 14pub. using the CLI "utils service restart Cisco Tomcat". Restart the Cisco DRF Master and Cisco DRF Local services on the publisher node. Restart ONLY the Cisco DRF Local service on the subscriber node(s).

i If SAML SSO is enabled, please disable and re-enable it. Also re-provision the SP metadata on the IDP.

Generate Self-Signed Multi-SAN Tomcat Successful Message

Step 4. Restart Tomcat service, open a CLI session to all the nodes of the cluster, and run `utils service restart Cisco`

Tomcat command.

Step 5. Navigate to the Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services and restart the Cisco DRF Master Service and Cisco DRF Local Service.

Step 6. Navigate to each Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services and restart Cisco DRF Local Service.

CA-Signed

Step 1. Log in to Publisher > Operating System (OS) Administration and navigate to Security > Certificate Management > Generate CSR.

Step 2. Choose Certificate Purpose: tomcat > Distribution: Multi-Server SAN. It auto-populates the SAN domains and the parent domain.

Generate Certificate Signing Request



Generate



Close

Status



Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose** tomcat

Distribution* Multi-server(SAN)

Common Name* 14pub-ms.

Include OU in CSR

Subject Alternate Names (SANs)

Auto-populated Domains
14pub.
14sub.

Parent Domain

Other Domains

Choose File No file chosen

Please import .TXT file only.

+ Add

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

Generate

Close



*- indicates required item.



**When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

Generate Multi-SAN CSR for Tomcat Certificate Screen

Step 3. Click Generate, and validate all your nodes are listed under the CSR export operation successful message. Click Close.

Generate Certificate Signing Request

Generate Close

Status

- Success: Certificate Signing Request Generated
- CSR export operation successful on the nodes [14sub. , 14pub.].

Generate Multi-SAN CSR Tomcat Successful Message

Step 4. Click Download CSR > Certificate Purpose: tomcat > Download.

Download Certificate Signing Request

Download CSR Close

Status

! Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

Certificate Purpose* tomcat

Download CSR Close

i *- indicates required item.

Download Tomcat CSR Screen

Step 5. Send the CSR to your CA for signing.

Step 6. In order to upload the CA trust chain, navigate Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust. Set the description of the certificate and browse the trust-chain files.

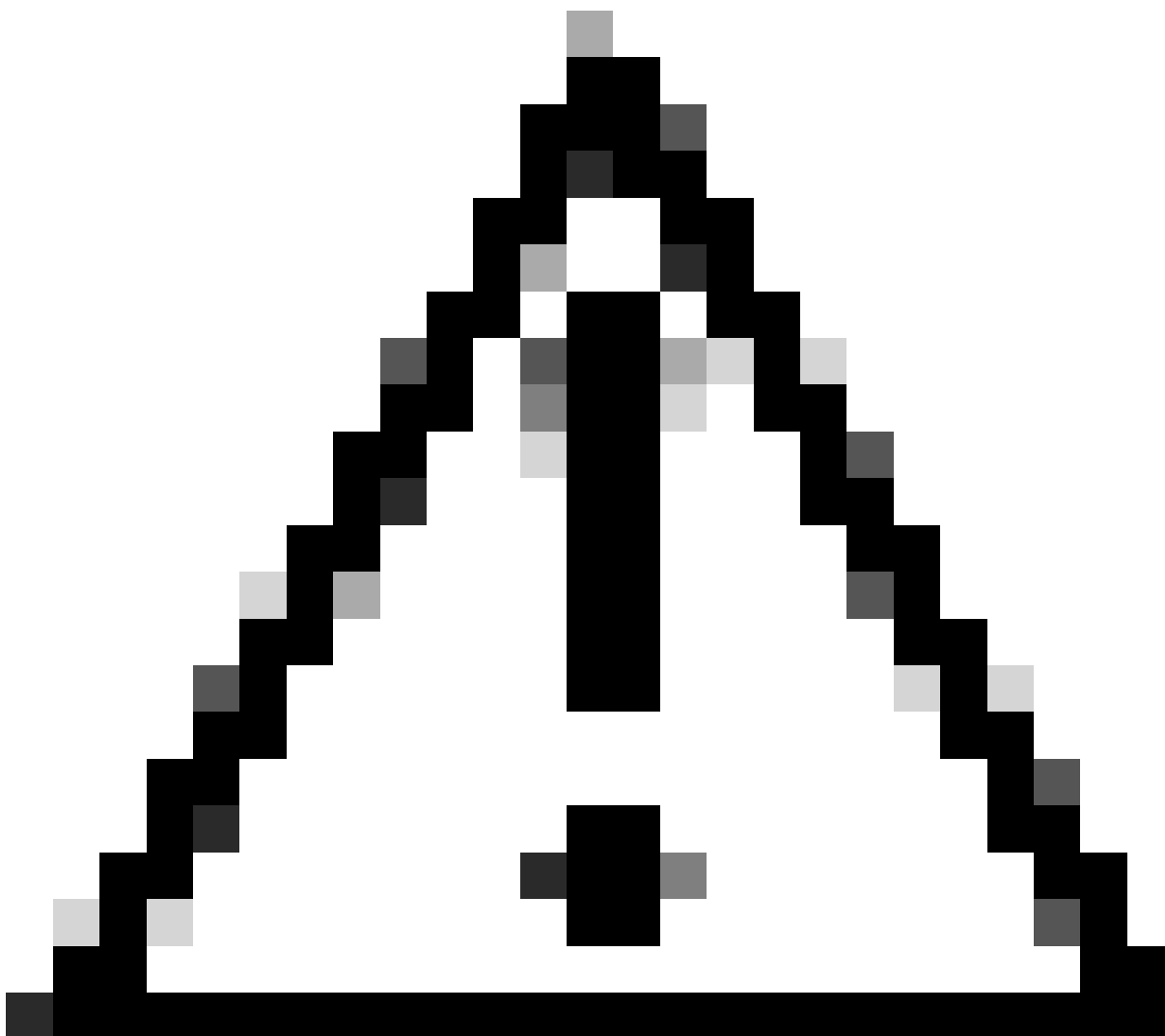
Step 7. Upload the CA-signed certificate, navigate to Certificate Management > Upload certificate > Certificate Purpose: tomcat. Set the description of the certificate and browse the CA-signed certificate file.

Step 8. Restart the Tomcat service, open a CLI session to all the nodes of the cluster, and run the `utils service restart Cisco Tomcat` command.

Step 9. Navigate to the Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services and restart the Cisco DRF Master Service and Cisco DRF Local Service.

Step 10. Navigate to each Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services and restart Cisco DRF Local Service.

2. Reuse Tomcat Certificate for CallManager



Caution: For CUCM 14, a new enterprise parameter Phone Interaction on Certificate Update is introduced. Use this field to reset phones either manually or automatically as applicable when one of the TVS, CAPF, or TFTP (CallManager/ITLRecovery) certificates are updated. This parameter is by default set to reset the phones automatically. After regeneration, deletion, and updation of certificates, ensure appropriate services are restarted.

Step 1. Navigate to your CUCM publisher, and then to Cisco Unified OS Administration > Security > Certificate Management.

Step 2. Click Reuse Certificate.

Step 3. From the choose Tomcat type drop-down list, choose tomcat.

Step 4. From the Replace Certificate for the following purpose pane, check the CallManager check box.

Use Tomcat Certificate For Other Services



Finish



Close

Status



Tomcat-ECDSA Certificate is Not Multi-Server Certificate



Tomcat Certificate is Multi-Server Certificate

Source

Choose Tomcat Type*

tomcat

Replace Certificate for the following purpose



CallManager



CallManager-ECDSA

Finish

Close

Reuse Tomcat Certificate for Other Services Screen



Note: If you choose Tomcat as the certificate type, CallManager is enabled as the replacement. If you choose tomcat-ECDSA as the certificate type, CallManager-ECDSA is enabled as the replacement.

Step 5. Click **Finish** in order to replace the CallManager certificate with the Tomcat Multi-SAN certificate.

Use Tomcat Certificate For Other Services

Finish Close

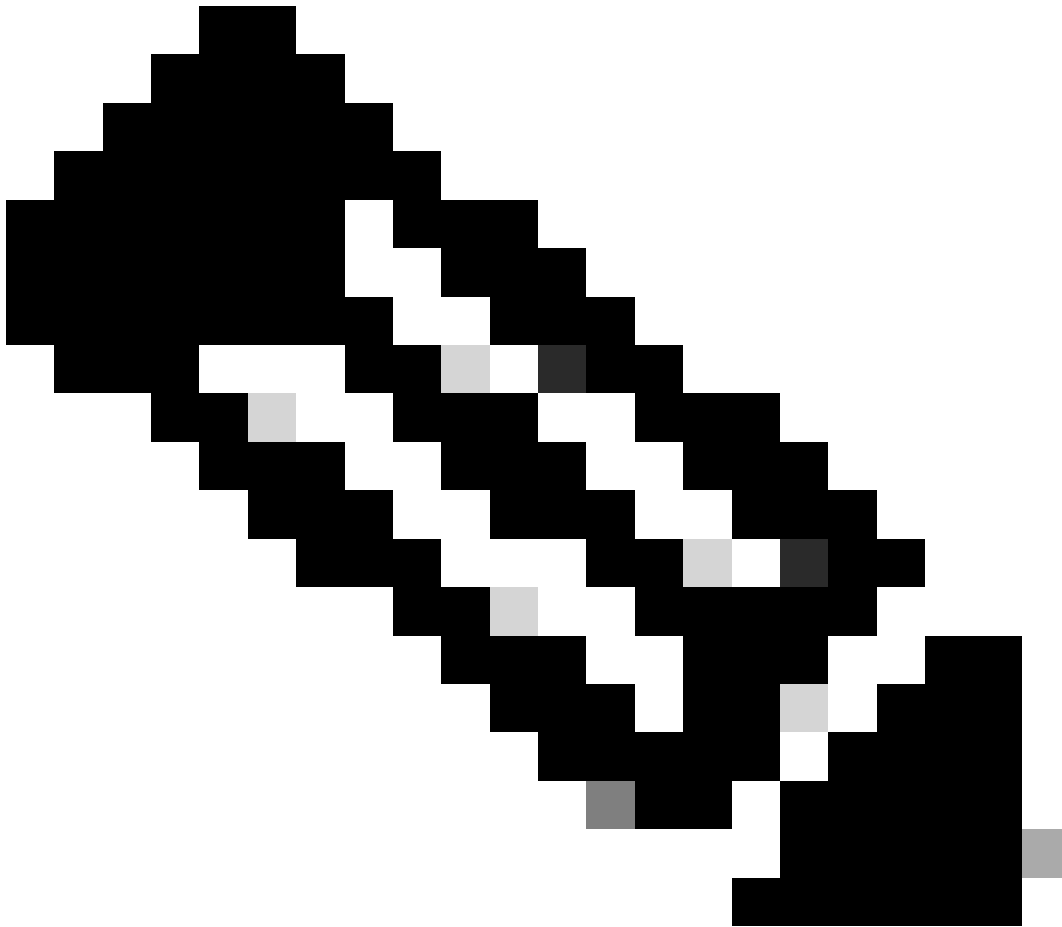
Status

- Certificate Successful Provisioned for the nodes 14sub. [redacted], 14pub. [redacted], .
- Restart Cisco HAProxy Service for the generated certificates to become active.
- If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.

Reuse Tomcat Certificate Successful Message

Step 6. Restart the Cisco HAProxy service, open a CLI session to all the nodes of the cluster, and run the `utils`

service restart Cisco HAProxy command.



Note: In order to determine if the cluster is in Mixed Mode, navigate to Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non-Secure; 1 == Mixed Mode).

Step 7. If your cluster is in Mixed Mode, open a CLI session to the Publisher node, and run `utils ctl update CTLFile` command, and reset all the phones of the cluster for the CTL file updates to take effect.

Verify

Step 1. Navigate to your CUCM publisher and then to Cisco Unified OS Administration > Security > Certificate Management.

Step 2. Filter by Find Certificate List where: Usage > begins with: identity and click Find.

Step 3. CallManager and Tomcat certificates must end with the same Common Name_Serial Number value.

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration **Go**
admin | About | Logout

Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Certificate List

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

Status
8 records found

Certificate List (1 - 8 of 8) Rows per Page 50 ▾

Find Certificate List where Usage ▾ begins with ▾ Identity Find Clear Filter

Select item or enter search text ▾

Certificate ^	Common Name/Common Name_SerialNumber	Usage	Type	Key Type	Distribution	Issued By	Expiration	Description
CallManager	14pub. 45cdf84f42748393feacd6f39c0af1fd	Identity	Self-signed	RSA	Multi-server(SAN)	14pub.cucm.collab.mx	09/25/2028	Reusing tomcat certificate for CallManager
CallManager-ECDSA	14pub-EC. 56a32bfc30d2996d5c5851a8b7e5731f	Identity	Self-signed	EC	14pub.cucm.collab.mx	14pub-EC.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
CAPF	14pub. CAPF-02a10666	Identity	Self-signed	RSA	14pub.cucm.collab.mx	CAPF-02a10666	12/20/2027	Self-signed certificate generated by system
ipsec	14pub. 6f44af5c5cdf753d5ff1538c3879b44	Identity	Self-signed	RSA	14pub.cucm.collab.mx	14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
ITLRecovery	ITLRECOVERY 14pub. 727029eea3d929d99ca9bee38720c89e	Identity	Self-signed	RSA	14pub.cucm.collab.mx	ITLRECOVERY_14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
tomcat	14pub. 45cdf84f42748393feacd6f39c0af1fd	Identity	Self-signed	RSA	Multi-server(SAN)	14pub.cucm.collab.mx	09/25/2028	Multi-server self-signed certificate for tomcat
tomcat-ECDSA	14pub-EC. 6ea1f2edf8f6183cdf629a4a0d447f	Identity	Self-signed	EC	14pub.cucm.collab.mx	14pub-EC.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
TVS	14pub. 7d8022fd6eb2885c3406b77cb4126046	Identity	Self-signed	RSA	14pub.cucm.collab.mx	14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system

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

Verify Tomcat Certificate Reuse for CallManager

Related Information

- [Security Guide for Cisco Unified Communications Manager 14](#)
- [Cisco Technical Support & Downloads](#)