

# Create New Certificates from Signed CA Certificates

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Pre-check Information](#)

### [Configure and Regenerate Certificates](#)

[Tomcat Certificate](#)

[CallManager Certificate](#)

[IPSec Certificate](#)

[CAPE Certificate](#)

[TVS Certificate](#)

### [Troubleshoot Common Uploaded Certificate Error Messages](#)

[CA Certificate is Not Available in the Trust-Store](#)

[File /usr/local/platform/security/tomcat/keys/tomcat.csr Does Not Exist](#)

[CSR Public Key and Certificate Public Key Do Not Match](#)

[CSR Subject Alternate Name \(SAN\) and Certificate SAN Does Not Match](#)

[Trust Certificates with the Same CN are Not Replaced](#)

---

## Introduction

This document describes how to regenerate the certificates signed by a Certificate Authority (CA) in Cisco Unified Communications Manager (CUCM).

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Real-Time Monitoring Tool (RTMT)
- CUCM Certificates


### Components Used

- CUCM release 10.x , 11.x, and 12.x.

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.

## Pre-check Information

---

 **Note:** For Self-Signed certificate regeneration, refer to the [Certificate Regeneration Guide](#). For CA-Signed Multi-SAN certificate regeneration, refer to the [Multi-SAN Certificate Regeneration Guide](#)

---

To understand the impact of each certificate and its regeneration, refer to the [Self-Signed Regeneration Guide](#).

Each Certificate Signing Request (CSR) type has different key usages and those are required in the Signed Certificate. The [Security Guide](#) includes a table with the required key usages for each type of certificate.

To change the Subject Settings (Locality, State, Organization Unit, and so on) run this command:

- `set web-security orgunit orgname locality state [country] [alternatename]`

The Tomcat certificate is regenerated automatically after you run the `set web-security` command. The new Self-Signed certificate is not applied unless the Tomcat service is restarted. Please refer to these guides for more information about this command:


- [Command Line Reference Guide](#)
- [Link to Cisco Community Steps](#)
- [Video](#)

## Configure and Regenerate Certificates

The steps to regenerate Single-Node certificates in a CUCM cluster signed by a CA are listed for each type of certificate. It is not necessary to regenerate all the certificates in the cluster if they have not expired.

### Tomcat Certificate

---

 **Caution:** Verify SSO is disabled in the cluster (**CM Administration > System > SAML Single Sign-On**). If SSO is enabled, it must be disabled and then enabled once the Tomcat certificate regeneration process is completed.

---

On all the nodes (CallManager and IM&P) of the cluster:

Step 1. Navigate to **Cisco Unified OS Administration > Security > Certificate Management > Find** and verify the expiration date of the Tomcat certificate.

Step 2. Click **Generate CSR > Certificate Purpose: tomcat**. Select the desired settings for the certificate, then click **Generate**. Wait for the success message to appear and click **Close**.

### Generate Certificate Signing Request

Generate Close

**Status**

Success: Certificate Signing Request Generated

**Generate Certificate Signing Request**

Certificate Purpose\*\* tomcat

Distribution# 115pub [REDACTED]

Common Name# 115pub [REDACTED]

**Subject Alternate Names (SANs)**

Parent Domain [REDACTED]

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.

Step 3. Download the CSR. Click Download CSR, select **Certificate Purpose: tomcat**, and click 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

#- indicates required item.


Step 4. Send the CSR to the Certificate Authority.

Step 5. The Certificate Authority returns two or more files for the signed certificate chain. Upload the certificates in this order:

- Root CA certificate as tomcat-trust. Navigate to **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. Set the description of the certificate and browse the Root certificate file.
- Intermediate certificate as tomcat-trust (Optional). Navigate to **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. Set the description of the certificate and browse the intermediate certificate file.

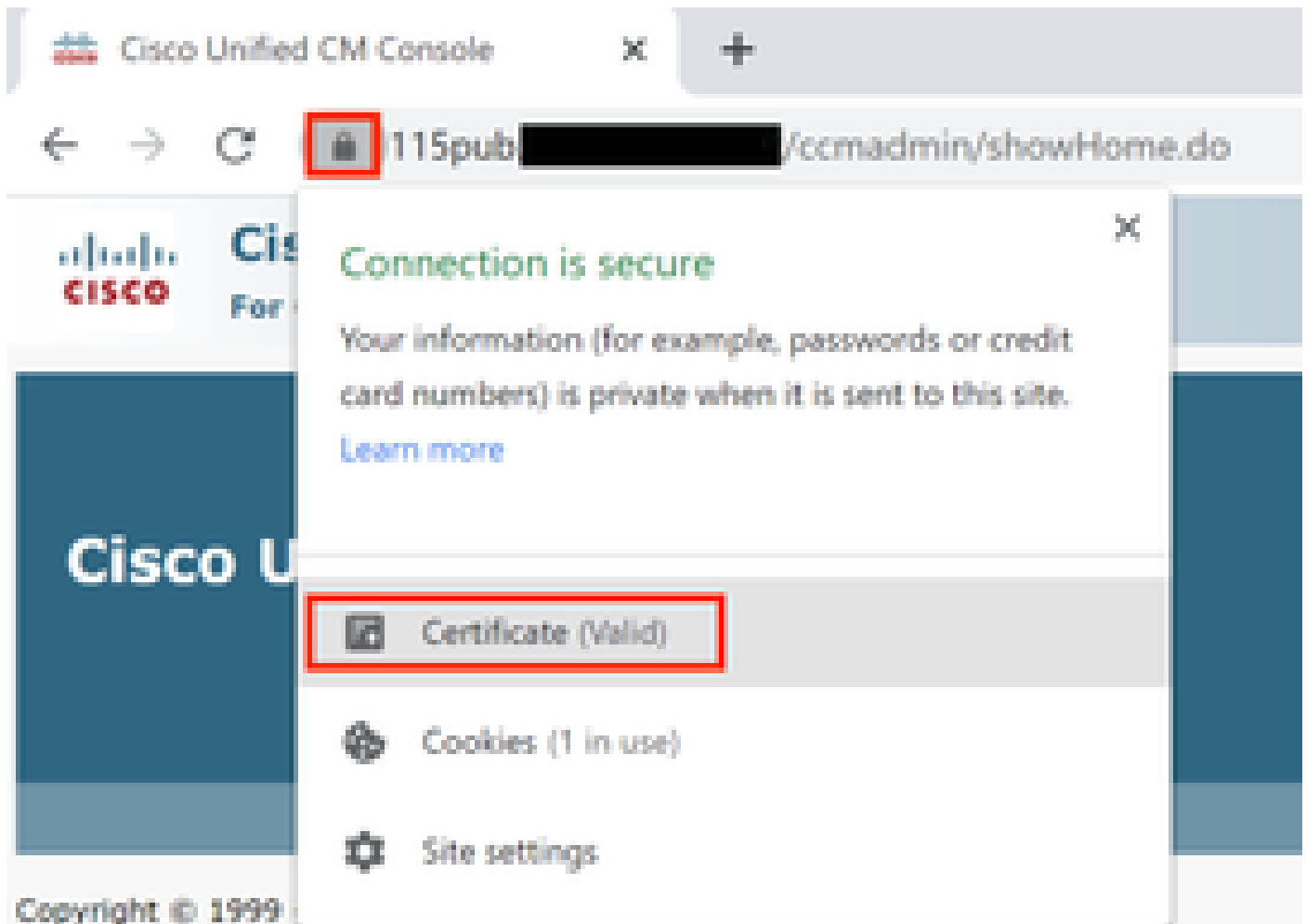
 **Note:** Some CAs do not provide an intermediate certificate. If only the Root certificate was provided, this step can be omitted.

- CA-signed certificate as tomcat. Navigate to Certificate Management > Upload certificate > Certificate Purpose: tomcat. Set the description of the certificate and browse the CA-signed certificate file for the current CUCM node.

 **Note:** At this point, CUCM compares the CSR and the uploaded CA-signed certificate. If the information matches, the CSR disappears, and the new CA-signed certificate is uploaded. If you receive an error message after the certificate is uploaded, refer to the Upload Certificate Common Error Messages section.

Step 6. To get the new certificate applied to the server, the Cisco Tomcat service needs to be restarted via CLI (start with Publisher, and then subscribers, one at a time), use the command `utils service restart Cisco Tomcat`.

To validate the Tomcat certificate is now used by CUCM, navigate to the web page of the node and select Site Information (Lock Icon) in the Browser. Click the certificate option, and verify the **date of the new certificate**.



General Details Certification Path

 **Certificate Information**

**This certificate is intended for the following purpose(s):**

- Ensures the identity of a remote computer

**Issued to:** 115pub [REDACTED]


**Issued by:** [REDACTED]

**Valid from 9/16/2020 to 9/16/2022**


Issuer Statement

OK

### CallManager Certificate

 **Caution:** Do not regenerate CallManager and TVS certificates at the same time. This causes an unrecoverable mismatch to the installed ITL on endpoints which requires the removal of the ITL from ALL endpoints in the cluster. Finish the entire process for CallManager, and once the phones are

---

 registered back, start the process for the TVS.

---

 **Note:** 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)**.

---

For all the CallManager nodes of the cluster:

Step 1. Navigate to Cisco Unified OS Administration > Security > Certificate Management > Find and verify the **expiration date** of the CallManager certificate.

Step 2. Click Generate CSR > Certificate Purpose: CallManager. Select the desired settings for the certificate, then click Generate. Wait for the success message to appear and click Close.


Step 3. Download the CSR. Click **Download CSR**. Select **Certificate Purpose: CallManager** and click **Download**.

Step 4. Send the CSR to the Certificate Authority .

Step 5. The Certificate Authority returns two or more files for the signed certificate chain. Upload the certificates in this order:

- Root CA certificate as CallManager-trust. Navigate to Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust. Set the description of the certificate and browse the Root certificate file.
- Intermediate certificate as CallManager-trust (Optional). Navigate to Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust. Set the description of the certificate and browse the intermediate certificate file.


---

 **Note:** Some CAs do not provide an intermediate certificate. If only the Root certificate was provided, this step can be omitted.

---

- CA-signed certificate as CallManager. Navigate to Certificate Management > Upload certificate > Certificate Purpose: CallManager. Set the description of the certificate and browse the CA-signed certificate file for the current CUCM node.

---

 **Note:** At this point, CUCM compares the CSR and the uploaded CA-signed certificate. If the information matches, the CSR disappears, and the new CA-signed certificate is uploaded. If you receive an error message after the certificate is uploaded, refer to the Upload Certificate Common Error Messages section.

---

Step 6. If the cluster is in Mixed Mode, update the CTL before the services restart: [Token](#) or [Tokenless](#). If the cluster is in Non-Secure Mode, skip this step and proceed with the services restart.


Step 7. To get the new certificate applied to the server, the required services must be restarted (only if the service runs and is active). Navigate to:

- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CallManager
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CTIManager

Step 8. Reset all the phones:

- Navigate to Cisco Unified CM Administration > System > Enterprise Parameters > Reset. A pop-up window appears with the statement, You are about to reset all devices in the system. This action cannot be undone. Continue? select OK and then click Reset .


---

 **Note:** Monitor device registration via RTMT. Once all phones register back you can proceed with the next certificate type.

---

## IPSec Certificate

---

 **Caution:** A backup or restore task must not be active when the IPSec certificate is regenerated.

---

For all the nodes (CallManager and IM&P) of the cluster:

Step 1. Navigate to Cisco Unified OS Administration > Security > Certificate Management > Find and verify the **expiration date** of the ipsec certificate.

Step 2. Click **Generate CSR > Certificate Purpose: ipsec**. Select the desired settings for the certificate, then click **Generate**. Wait for the success message to appear and then click **Close**.


Step 3. Download the CSR. Click **Download CSR**. Select Certificate Purpose ipsec and click **Download**.

Step 4. Send the CSR to the Certificate Authority.

Step 5. The Certificate Authority returns two or more files for the signed certificate chain. Upload the certificates in this order:

- Root CA certificate as ipsec-trust. Navigate to **Certificate Management > Upload certificate > Certificate Purpose: ipsec-trust**. Set the description of the certificate and browse the Root certificate file.
- Intermediate certificate as ipsec-trust (Optional). Navigate to **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. Set the description of the certificate and browse the intermediate certificate file.


---

 **Note:** Some CAs do not provide an intermediate certificate. If only the Root certificate was provided, this step can be omitted.

---

- CA-signed certificate as ipsec. Navigate to **Certificate Management > Upload certificate > Certificate Purpose: ipsec**. Set the description of the certificate and browse the CA-signed certificate file for the current CUCM node.

---

 **Note:** At this point, CUCM compares the CSR and the uploaded CA-signed certificate. If the information matches, the CSR disappears, and the new CA-signed certificate is uploaded. If you receive an error message after the certificate is uploaded, please refer to the **Upload Certificate Common Error Messages** section.

---

Step 6. To get the new certificate applied to the server, the required services must be restarted (only if the service runs and is active). Navigate to:

- **Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco DRF Master(Publisher)**


- **Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco DRF Local** (Publisher and Subscribers)

## CAPF Certificate

---

 **Note:** 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)**.

---

 **Note:** CAPF service only runs in the Publisher, and that is the only certificate used. It is not necessary to get Subscriber nodes signed by a CA because they are not used. If the certificate is expired in the Subscribers and you would like to avoid the alerts of expired certificates, you can regenerate subscriber CAPF certificates as Self-Signed. For more information, see [CAPF Certificate as Self-Signed](#).

---

In the Publisher:

Step 1. Navigate to **Cisco Unified OS Administration > Security > Certificate Management > Find** and verify the **expiration date** of the CAPF certificate.

Step 2. Click **Generate CSR > Certificate Purpose: CAPF**. Select the desired settings for the certificate, then click **Generate**. Wait for the success message to appear and click **Close**.


Step 3. Download the CSR. Click **Download CSR**. Select Certificate Purpose CAPF and click **Download**.

Step 4. Send the CSR to the Certificate Authority.

Step 5. The Certificate Authority returns two or more files for the signed certificate chain. Upload the certificates in this order:

- Root CA certificate as CAPF-trust. Navigate to **Certificate Management > Upload certificate > Certificate Purpose: CAPF-trust**. Set the description of the certificate and browse the Root certificate file.
- Intermediate certificate as CAPF-trust (Optional). Navigate to **Certificate Management > Upload certificate > Certificate Purpose: CAPF-trust**. Set the description of the certificate and browse the intermediate certificate file.


---

 **Note:** Some CAs do not provide an intermediate certificate. If only the Root certificate was provided, this step can be omitted.

---

- CA-signed certificate as CAPF. Navigate to **Certificate Management > Upload certificate > Certificate Purpose: CAPF**. Set the description of the certificate and browse the CA-signed certificate file for the current CUCM node.

---

 **Note:** At this point, CUCM compares the CSR and the uploaded CA-signed certificate. If the information matches, the CSR disappears, and the new CA-signed certificate is uploaded. If you receive an error message after the certificate is uploaded, please refer to the **Upload Certificate Common Error Messages** section.

---

Step 6. If the cluster is in Mixed Mode, update the CTL before the services restart: [Token](#) or [Tokenless](#). If



the cluster is in Non-Secure Mode, skip this step and proceed with the service restart.


Step 7. To get the new certificate applied to the server the required services must be restarted (only if the service runs and is active). Navigate to:

- **Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service** (All nodes where the service runs.)
- **Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP** (All nodes where the service runs.)
- **Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco Certificate Authority Proxy Function** (Publisher)

Step 8. Reset all the phones:

- Navigate to **Cisco Unified CM Administration > System > Enterprise Parameters > Reset**. A pop-up window appears with the statement, You are about to reset all devices in the system. This action cannot be undone. Continue? select **OK** and then click **Reset**.


---

 **Note:** Monitor device registration via RTMT. Once all phones register back you can proceed with the next certificate type.

---

## TVS Certificate

---

 **Caution:** Do not regenerate CallManager and TVS certificates at the same time. This causes an unrecoverable mismatch to the installed ITL on endpoints which requires the removal of the ITL from ALL endpoints in the cluster. Finish the entire process for CallManager and once the phones are registered back, start the process for the TVS.

---

For all the TVS nodes of the cluster:

Step 1. Navigate to **Cisco Unified OS Administration > Security > Certificate Management > Find** and verify the expiration date of the TVS certificate.

Step 2. Click **Generate CSR > Certificate Purpose: TVS**. Select the desired settings for the certificate, then click **Generate**. Wait for the success message to appear and click **Close**.


Step 3. Download the CSR. Click **Download CSR**. Select **Certificate Purpose TVS** and click **Download**.

Step 4. Send the CSR to the Certificate Authority.

Step 5. The Certificate Authority returns two or more files for the signed certificate chain. Upload the certificates in this order:


- Root CA certificate as TVS-trust. Navigate to **Certificate Management > Upload certificate > Certificate Purpose: TVS-trust**. Set the description of the certificate and browse the Root certificate file.
- Intermediate certificate as TVS-trust (Optional). Navigate to **Certificate Management > Upload certificate > Certificate Purpose: TVS-trust**. Set the description of the certificate and browse the intermediate certificate file.

---

 **Note:** Some CAs do not provide an intermediate certificate. If only the Root certificate was provided,

---


---

 this step can be omitted.

---

- CA-signed certificate as TVS. Navigate to **Certificate Management > Upload certificate > Certificate Purpose: TVS**. Set the description of the certificate and browse the CA-signed certificate file for the current CUCM node.

---

 **Note:** At this point, CUCM compares the CSR and the uploaded CA-signed certificate. If the information matches, the CSR disappears, and the new CA-signed certificate is uploaded. If you receive an error message after the certificate is uploaded, refer to the Upload Certificate Common Error Messages section.

---


Step 6. To get the new certificate applied to the server, the required services must be restarted (only if the service runs and is active). Navigate to:

- **Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP** (All nodes where the service runs.)
- **Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service** (All nodes where the service runs.)

Step 7. Reset all the phones:

- Navigate to **Cisco Unified CM Administration > System > Enterprise Parameters > Reset**. A pop-up window appears with the statement, You are about to reset all devices in the system. This action cannot be undone. Continue? select **OK** and then click **Reset**.

---

 **Note:** Monitor device registration via RTMT. Once all phones register back, you can proceed with the next certificate type.

---

## Troubleshoot Common Uploaded Certificate Error Messages

In this section are listed some of the most common Error Messages when a CA-signed certificate is uploaded.

### CA Certificate is Not Available in the Trust-Store

This error means the root or intermediate certificate was not uploaded to the CUCM. Verify those two certificates were uploaded as trust-store before the service certificate is uploaded.

### File /usr/local/platform/.security/tomcat/keys/tomcat.csr Does Not Exist

This error appears when a CSR does not exist for the certificate (tomcat, callmanager, ipsec, capf, tvs). Verify the CSR was created before and the certificate was created based on that CSR. Important points to keep in mind:

- Only 1 CSR per server and certificate type can exist. That means that if a new CSR is created, the old one is replaced.
- Wildcard certificates are not supported by CUCM.
- It is not possible to replace a service certificate that is currently in place without a new CSR.
- Another possible error for the same issue is “The file /usr/local/platform/upload/certs//tomcat.der could not be uploaded.” This depends on the CUCM version.



Another possible error for the same issue is “The file /usr/local/platform/upload/certs//tomcat.der could not be uploaded.” This depends on the CUCM version.

## CSR Subject Alternate Name (SAN) and Certificate SAN Does Not Match

The SANs between the CSR and the Certificate must be the same. This prevents certification for Domains that are not allowed. To verify the SAN mismatch, these are the next steps:

1. Decode the CSR and the certificate (base 64). There are different decoders available online, such as the [Decoder](#).
2. Compare the SAN entries and verify all of them match. The order is not important, but all the entries in the CSR must be the same in the Certificate.

For example, the CA-signed certificate has two extra SAN entries added, the Common Name of the certificate and an extra IP address.

CSR Summary	
<b>Subject</b> domain.com	
RDN	Value
Common Name (CN)	pub-ms.domain.com
Organizational Unit (OU)	Collaboration
Organization (O)	Cisco
Locality (L)	CUCM
State (ST)	CDMX
Country (C)	MX
<b>Properties</b> domain.com	
Property	Value
Subject	CN = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX
Key Size	2048 bits
Fingerprint (SHA-1)	C3:87:05:C8:79:F8:88:4A:86:96:77:0A:C5:88:63:27:55:3C:A4:84
Fingerprint (MD5)	CE:5C:9D:59:3F:8E:E3:26:C5:21:9D:A2:F1:CA:68:86
SANS	domain.com, sub.domain.com, pub.domain.com, imp.domain.com

Certificate Summary	
<b>Subject</b>	
RDN	Value
Common Name (CN)	pub-ms.domain.com
Organizational Unit (OU)	Collaboration
Organization (O)	Cisco
Locality (L)	CUCM
State (ST)	CDMX
Country (C)	MX
<b>Properties</b>	
Property	Value
Issuer	CN = Collab CA,DC = collab,DC = ms
Subject	CN = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX
Valid From	17 Sep 2020, 1:24 a.m.
Valid To	17 Sep 2022, 1:24 a.m.
Serial Number	69:00:00:00:2D:5A:92:EB:EA:9A:85:65:C4:00:00:00:00:2D(2341578246081205845683969935281333940237893677)
CA Cert	No
Key Size	2048 bits
Fingerprint (SHA-1)	4E:15:F7:F3:9C:37:A9:8D:52:1A:6C:6D:4D:7D:AF:FE:08:EB:8D:0F
Fingerprint (MD5)	08:22:33:92:50:F7:70:2A:05:28:90:2D:57:C0:F7:EC
SANS	pub-ms.domain.com, domain.com, sub.domain.com, pub.domain.com, imp.domain.com, 10.xx.xx.xx

3. Once you have identified the SAN does not match, there are two options to fix this:
  1. Request your CA administrator to issue a certificate with the exact same SAN entries that are sent in the CSR.
  2. Create a CSR in CUCM that matches the requirements of the CA.

### To modify the CSR created by CUCM:

1. If the CA removes the domain, a CSR in CUCM can be created without the domain. While the CSR creation, remove the domain that is populated by default.
2. If a [Multi-SAN certificate](#) is created, there are some CA that do not accept the -ms in the Common Name. The -ms can be removed from the CSR when it is created.

**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 <sup>Ⓜ</sup> tomcat

Distribution <sup>Ⓜ</sup> Multi-server(SAN)

Common Name <sup>Ⓜ</sup> 115pub-ms

**Subject Alternate Names (SANs)**

Auto-populated Domains

115imp.  
115pub.  
115sub.

Parent Domain

Other Domains

Key Type <sup>Ⓜ</sup> RSA

Key Length <sup>Ⓜ</sup> 2048

Hash Algorithm <sup>Ⓜ</sup> SHA256

Generate Close

3. To add an Alternative Name apart from the ones autocompleted by CUCM:

1. If Multi-SAN certificate is used, more FQDN can be added. (IP addresses are not accepted.)

**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 <sup>Ⓜ</sup>	<input type="text" value="tomcat"/>
Distribution <sup>Ⓜ</sup>	<input type="text" value="Multi-server(SAN)"/>
Common Name <sup>Ⓜ</sup>	<input type="text" value="115pub-ms-██████████"/>
<b>Subject Alternate Names (SANs)</b>	
Auto-populated Domains	<input type="text" value="115imp.██████████"/> <input type="text" value="115pub.██████████"/> <input type="text" value="115sub.██████████"/>
Parent Domain	<input type="text"/>
Other Domains	<input style="border: 1px solid red;" type="text" value="extrahostname.domain.com"/> <span style="float: right; border: 1px solid red; padding: 2px;">+</span> Add
	<input style="border: 1px solid red;" type="text"/> <span style="float: right; border: 1px solid red; padding: 2px;">+</span> Add
Key Type <sup>Ⓜ</sup>	<input type="text" value="RSA"/>
Key Length <sup>Ⓜ</sup>	<input type="text" value="2048"/>
Hash Algorithm <sup>Ⓜ</sup>	<input type="text" value="SHA256"/>

Generate
Close

b. If the certificate is Single Node, use the `set web-security` command. This command applies even for Multi-SAN certificates. (Any kind of domain can be added, also IP addresses are permitted.)

For more information, see the [Command Line Reference Guide](#).

## Trust Certificates with the Same CN are Not Replaced

CUCM was designed to store only one certificate with the same Common Name and same certificate type. This means that if a certificate that is tomcat-trust already exists in the database and it needs to be replaced with a recent one with the same CN, CUCM removes the old certificate and replaces it with the new one.

There are some cases when CUCM does not replace the old certificate:

1. The certificate uploaded is expired: CUCM does not allow you to upload an expired certificate.
2. The old certificate has a more recent FROM date than the new certificate. CUCM keeps the most

recent certificate, and the older FROM date is cataloged as older. For this scenario, it is necessary to delete the unwanted certificate and then upload the new one.

