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		
CAPF 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 <u>Certificate Regeneration Guide</u>. For CA-Signed Multi-SAN certificate regeneration, refer to the <u>Multi-SAN Certificate Regeneration Guide</u>

To understand the impact of each certificate and its regeneration, refer to the <u>Self-Signed Regeneration</u> <u>Guide</u>.

Each Certificate Signing Request (CSR) type has different key usages and those are required in the Signed Certificate. The <u>Security Guide</u> 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] [alternatehostname]

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
- <u>Video</u>

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			
Close Close			
Status			
(i) Success: Certificate Signing Res	quest Generated		
<u> </u>			
Generate Certificate Signing Req	uest		
Certificate Purpose**	tomcat 🗸		
Distribution *	115pub		
Common Name*	11Spub		
Subject Alternate Names (SANs)			
Parent Domain			
Key Type**	RSA		
Key Length*	2048 ~		
Hash Algorithm*	SHA256 V		
Generate Close			
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.			

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 v			
Download CSR Close				

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.

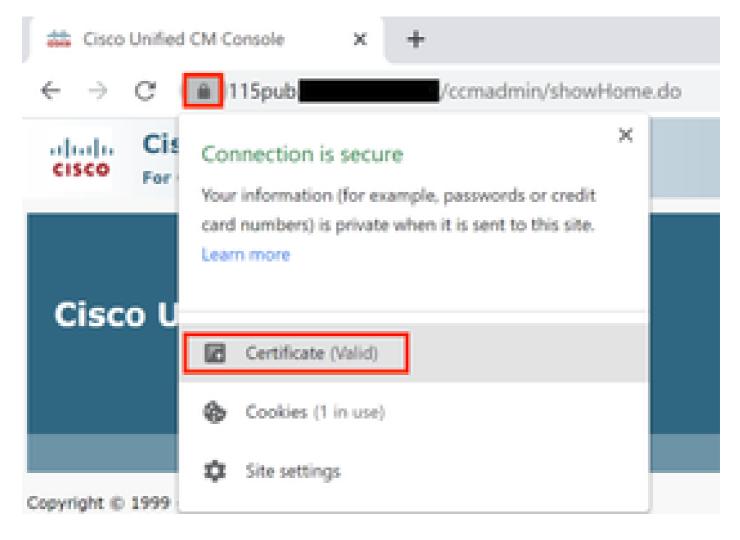
Note: Some CAs do not provide an intermediate certificate. If only the Root certificate was provided, this step can be omitted.

• 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.



Certifica	te Information
	is intended for the following purpose(s): he identity of a remote computer
 Choures to 	ve idencity of a remote computer
Issued to:	115put
Issued to:	115put

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

×

Issuer Statement

OK.

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: <u>Token</u> or <u>Tokenless</u>. 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
- $\bullet \quad Cisco \ Unified \ Serviceability > Tools > Control \ Center \ \ Feature \ Services > Cisco \ Call Manager$
- 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 ia uploaded. If you receive an error message after the certificate is uploaded, please refer to the **Upload Certificate Common Error Messages** /strong> 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 <u>CAPF Certificate as Self-Signed</u>.

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 ia 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 popup 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,

• 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 popup 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.

CSR Public Key and Certificate Public Key Do Not Match

This error appears when the certificate provided by the CA has a different public key than the one sent in the CSR file. Possible reasons are:

- The incorrect certificate (maybe from another node) is uploaded.
- The CA certificate was generated with a different CSR.
- The CSR was regenerated, and it replaced the old CSR that was used to get the signed certificate.

To verify the CSR and certificate public key match, there are multiple tools online such as <u>SSL</u>.

What to Check

O Check if a Certificate and a Private Key match

Check if a CSR and a Certificate match

Enter your Certificate:

TJ13aW4xMixDTJ1DRFAsQ049UHVIbGIJTIwS2V5JTIWU2VydmIJ2XMsQ049U2Vy dmIJ2XMsQ049Q29u2mindXJhdGNbixEQ21Jb2xSYWISREM9bXg/Y2VydGImaWNh dGVS2X2VY2F0aW9uTGI2dD9HYXNIP29IamVjdENSYXN2PWNSTERpc3RyaWJ1dGiv bI8vaW50MIG78ggrBgEFBQcBAQ58rjCBqzCBqAYIKWYBBQUHMAXGg2xs2GFwOI8v L0NOPUNvbGxhYIUyMENBLENOPUFJQSxDTJ1QdWJsaWMIMJBL2XkIMJBT2XJ2aWNI cyxDTJ1T2XJ2aWNIcyxDTJ1Db25maWd1cmF0aW9uLERDPWNvbGxhYrxEQ21bcD9J QUNIcnRp2mIJYXRIP2Jhc2U/b2Jq2WN0Q2xhc3M9Y2VydGimaWNhdGNbkF1dGhv cmI0eTAhBgkrBgEEAY13FAIEFB4SAFcA2QBIAFMA2QByAHYA2QByMA0GC5qG5ib3 DQEBCwUAA4BAQCfq2Bc28cMxkurQavdYaUIoDrfDpMLSA/7YhisqW55x/bEQs 9LyqftmIddCmkoMPtGK4t2vMie4oTpKBYAQvbrApGO01mWV5u+f1lo9PvYrygWEyL D+ve7rMp8sirVo1Tmhe/26in3bm+Ofwe5NuvCx3wN/dLRR39O4KcaPCxsVLQ6Aw PtmAz/KX2GRhzqacd9fVLJU0WTKDJ2QsIadcgs5cvFMz3BBf0MJGBNX16JGIQ yZ2br6Gm4pa4yIQISUrCXxHYsIomeCYeRheKuSkuPusOoEIVIWszJ0QMT7P4/Ww 2BpT2TkrQdODA2HJGuJP+yBa7SOGGT2WVVg1 ----END CERTIFICATE----

Enter your CSR:

q+h(jgokSx+ogqVavFSNRdqTh0Girls1ga0pjSsGxOOLCqAtQhEARnEcGyanZtrK gSjTQhf8jStD2vDYyD3wg5lyhwNiqkMUI3tRD5qcSD/TrflLGLs8hB9ySHqtaDA3 1IwLj5Q4RXt2188ESciLt83bAo2egZo5Vw4/h5tP8r09e/cTWsXZt8fLGytvcDGk OGrdW2xLuaUV2u29JWTmLD70iCN/XCMI9XYpLjb6utyMLif00Ph+s0PiMr7gal5b hXk54ZjoFIMkXY8WSPDwexH7XtD+HQaPeM4T50N4TrqhxAgMBAAGgbz8t8gkqhkiG 9w08CQ4xYD8eM80GA1UdjQQWM8QGCCsGAQUF8wM88ggr8gfE8QcDAJAL8gNVHQ8E BAMCBLAwMAYDVR0R8Ckwj4iOY3Vjb55jb2xsYWiubXiCFTExNX81Yt5jdWNtLmNv bGxhri5teDAN8gkqhkiG9w08AQsFAAOCAQEAA8ggi7f5T59rWXOFJsg7hsj36vf ubcW7HGPrNYx6/pI9UydunRXKDxQTI2ZWWc9IOA3/Fpcfr2+8LdHtR1Fnmw8WCV YcA9soNiWZsmU1+clbTH1H5g8FFoHAdg+FR3+1AE7GNfGk0CA0RipPihZPGzQ6dO 62TRSfQ4SLbcWxe4EZO5xjEQW7ZrkjfWby1GQKYg3cuXCEtrJ3UunMCZriWjmNxKg0 n781nNdx7YbgF21ikY+2ozPHWgbu2HwCHuH1bOAMUpkwIPebQ2n9H+R7drsj8AZR ieXEYWL739M7BTveNmHoOnR65kwVHYbb7iq0jnhXcSy9R05052vUhkj7Hw== ----END CERTIFICATE REQUEST-----

The certificate and CSR do NOT match!

🕜 Certificate Hash:

684ad486131856ce0015d4b3e615e1ed 3b3bef6b8f590a493921661a4c4f62e9

🕜 CSR Hash:

635f45c1ebcd876526a3133d1ee73d9a8 4544876fdbc8dc3a4d8fed377dcc635 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 <u>Decoder</u>.

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.

R Summary		Certificate Sum	nary	
ubject	domain.com	Subject		
RDN	Value	RDN		Value
Common Name (CN)	gub-ms.domain.com	Common Name (26	pub-ms.domain.com
Organizational Unit (OU)	Collaboration	Organizational U	iit (0U)	Collaboration
Organization (O)	Cisco	Organization (0)		Csco
ecality (L)	CUCM	Locality (L)		CUCM
State (ST)	CDMX	State (ST)		CDMX
Country (C)	MX	Country (C)		MX
roperties	domain.com	Properties		
Property	Value	Property	Va	hue
ubject	CN = pub-ms.domsin.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX	Issuer	0	x = Collab CA,DC = collab,DC = mx
iey Size	2048 bits	Subject	0	4 = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX
ingerprint (SHA-1)	C3 87.05 C8 79 F8 88 44 86 56 77.0A C5 88 63 27 55 3C 44 84	Valid From	17	Sep 2020, 1:24 a.m.
ingerprint (MDS)	CE:5C:90:59:1F:8E:82:26:C5:23:90:A2:F1:CA:58.86	Valid To	17	Sep 2022, 1:24 a.m.
WS .	domain.com, sub.domain.com, pub.domain.com, imp.domain.com	Serial Number	65	00.00.00.2D 5A 92 E8 EA 9A 85 65 C4 00.00.00.00.2D (2341578246081205845683969935281333940237893677)
,		CA Cert	N	
		Key Size	20	48 bits
		Fingerprint (SHA-	1) 46	15 F7 F3 9C 37 A9 8D 52 1A 6C 6D 4D 70 AF FE 08 88 8D 0F
		Fingerprint (MDS	D	22 33 92 50 F7 70 2A D5 28 00 2D 57 C0 F7 8C
		SANS	pu	b-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 <u>Multi-SAN certificate</u> 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	
Close	
Status	
Warning: Generating a new CSR for a specific cer	tificate type will overwrite the existing CSR for that type
Generate Certificate Signing Request	
Certificate Purpose**	tomcat.
Distribution*	Multi-server(SAN)
Common Name*	11Spub-ms.
Subject Alternate Names (SANs)	
Auto-populated Domains Parent Domain Other Domains	115inp. 115pub. 115iub.
Key Type**	RSA
Key Length*	2048
Hash Algorithm*	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.)

enerate Certificate Signing	Request		
Generate 🖳 Close			
Status			
🚹 Warning: Generating a new	CSR for a specific certificate type will over	erwrite the existing CSR for that	type
Generate Certificate Signing	Request		
Certificate Purpose**	tomcat	~	
Distribution *	Multi-server(SAN)	~	
Common Name*	11Spub-ms.		
Subject Alternate Names (SA	the second se		
Auto-populated Domains	11Simp.		
	115pub		
	115sub.		
Parent Domain			
Other Domains	extraHostname.domain.com	B	Choose File
			For more info
			E Add
			100 MOU
Key Type**	RSA		
Key Length*	2048	~	
Hash Algorithm*	SHA256	~	
	and the second sec		

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 <u>Command Line Reference Guide</u>.

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.

Certificate >	Certificate X
General Details Certification Path	General Details Certification Path
Certificate Information This certificate is intended for the following purpose(s): All issuance policies All application policies	Certificate Information This certificate is intended for the following purpose(s): All issuance policies All application policies
Old Certificate	New Certificate
Issued by: Colab CA	Issued by: Collab CA
Valid from 7/23/2019 to 7/23/2024	Valid from 5/23/2019 to 12/23/2030
Issuer Statement	Issuer Statement
OX	x