

# Konfigurieren der Wiederverwendung des Tomcat-Zertifikats für CallManager in CUCM 14

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[1. Tomcat-Zertifikat als Multi-SAN festlegen](#)

[selbstsigniert](#)

[CA-signiert](#)

[2. Tomcat-Zertifikat für CallManager wiederverwenden](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird die Wiederverwendung des Multi-SAN Tomcat-Zertifikats für CallManager auf einem Cisco Unified Communications Manager (CUCM)-Server beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf CUCM 14.0.1.13900-155.







Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

# Hintergrundinformationen

Die beiden Hauptdienste für CUCM sind Tomcat und CallManager. In den früheren Versionen waren für den gesamten Cluster unterschiedliche Zertifikate für die einzelnen Dienste erforderlich. In CUCM-Version 14 wurde eine neue Funktion hinzugefügt, um das Multi-SAN Tomcat-Zertifikat auch für den CallManager-Dienst wiederzuverwenden. Die Verwendung dieser Funktion bietet folgende Vorteile:

- Reduziert die Kosten für das Abrufen von zwei Zertifikaten, die von einer öffentlichen Zertifizierungsstelle (Public Certificate Authority, CA) für einen Cluster von Zertifikaten mit Zertifizierungsstelle (CA) signiert wurden.
- Diese Funktion reduziert die Größe der ITL-Datei und damit den Overhead.

 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, <u>Ipsec</u> 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	

## Konfigurieren



Vorsicht: Stellen Sie vor dem Hochladen eines Tomcat-Zertifikats sicher, dass die einmalige Anmeldung (Single Sign-on, SSO) deaktiviert ist. Falls sie aktiviert ist, muss SSO deaktiviert und erneut aktiviert werden, sobald der Tomcat-Zertifikatregenerierungsprozess abgeschlossen ist.



Low Impact

### 1. Tomcat-Zertifikat als Multi-SAN festlegen

In CUCM 14 kann das Tomcat Multi-SAN-Zertifikat selbstsigniert oder CA-signiert sein. Wenn Ihr Tomcat-Zertifikat bereits Multi-SAN ist, überspringen Sie diesen Abschnitt.

selbstsigniert

Schritt 1: Melden Sie sich bei an, Publisher > Operating System (OS) Administration und navigieren Sie zu Security > Certificate Management > Generate Self-Signed.

Schritt 2. Wählen Sie Certificate Purpose: tomcat > Distribution: Multi-Server SAN. Die SAN-Domänen und die übergeordnete Domäne werden automatisch ausgefüllt.

**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.

Bildschirm "Generate Self-Signed Multi-SAN Tomcat Certificate"

Schritt 3. Klicken Sie Generate, und überprüfen Sie, dass alle Knoten unter der Certificate upload operation successful Nachricht aufgeführt sind. Klicken Sie auf .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.

Erfolgreiche selbstsignierte Erfolgsmeldung für Multi-SAN-Tomcat generieren

Schritt 4: Starten Sie den Tomcat-Dienst neu, öffnen Sie eine CLI-Sitzung mit allen Knoten des Clusters, und führen Sie den `utils service restart Cisco Tomcat` Befehl aus.

**Schritt 5:** Navigieren Sie zu Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services , und starten Sie das Cisco DRF Master Service und Cisco DRF Local Service neu.

**Schritt 6.** Navigieren Sie zu jedem Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services und starten Sie neu Cisco DRF Local Service.

CA-signiert

**Schritt 1:** Melden Sie sich bei an, Publisher > Operating System (OS) Administration und navigieren Sie zu Security > Certificate Management > Generate CSR.

**Schritt 2.** Wählen Sie Certificate Purpose: tomcat > Distribution: Multi-Server SAN. Die SAN-Domänen und die übergeordnete Domäne werden automatisch ausgefüllt.

### 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.

Bildschirm "Generate Multi-SAN CSR for Tomcat Certificate"

Schritt 3. Klicken Sie **Generate**, und überprüfen Sie alle Ihre Knoten sind unter der CSR export operation successful Nachricht aufgeführt. Klicken Sie auf **Close**

### Generate Certificate Signing Request

Generate
 Close

**Status**

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

Schritt 4. Klicken Sie auf **Download CSR > Certificate Purpose: tomcat > Download.**

Bildschirm "Tomcat CSR" herunterladen

Schritt 5: Senden Sie den CSR zur Signatur an Ihre Zertifizierungsstelle.

Schritt 6: Um die Zertifizierungsstellen-Vertrauenskette hochzuladen, navigieren Sie **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust.** Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die Vertrauensketten-Dateien.

Schritt 7: Laden Sie das CA-signierte Zertifikat hoch, navigieren Sie zu **Certificate Management > Upload certificate > Certificate Purpose: tomcat.** Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die CA-signierte Zertifikatsdatei.

Schritt 8: Starten Sie den Tomcat-Dienst neu, öffnen Sie eine CLI-Sitzung mit allen Knoten des Clusters, und führen Sie den **utils service restart Cisco Tomcat** Befehl aus.

Schritt 9: Navigieren Sie zu **Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services** , und starten Sie das **Cisco DRF Master Service** und **Cisco DRF Local Service** neu.

Schritt 10: Navigieren Sie zu jedem **Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services** , und starten Sie neu **Cisco DRF Local Service.**

## 2. Tomcat-Zertifikat für CallManager wiederverwenden



Vorsicht: Für CUCM 14 wird ein neuer Enterprise-Parameter `Phone Interaction on Certificate Update` eingeführt. Verwenden Sie dieses Feld, um Telefone manuell oder automatisch zurückzusetzen, wenn eines der TVS-, CAPF- oder TFTP-Zertifikate (CallManager/ITLRecovery) aktualisiert wird. Dieser Parameter ist standardmäßig auf `reset the phones automatically` eingestellt. Stellen Sie nach der Regeneration, Löschung und Aktualisierung der Zertifikate sicher, dass die entsprechenden Dienste neu gestartet werden.

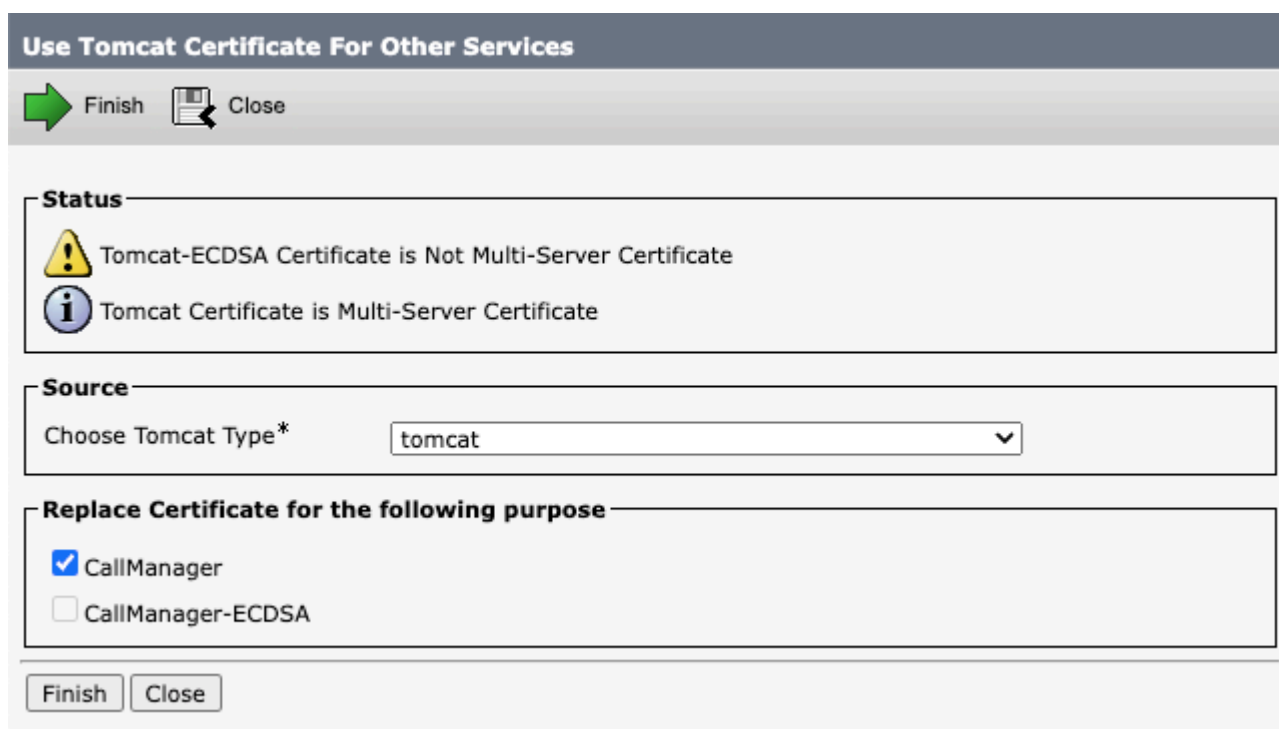
Für eine normale CallManager-Zertifikatregeneration ist ein Neustart der Dienste erforderlich. Aktivieren Sie [Zertifikat neu generieren in Unified Communications Manager](#).

Schritt 1: Navigieren Sie zu Ihrem CUCM-Publisher, und wechseln Sie dann zu `Cisco Unified OS Administration > Security > Certificate Management`.

Schritt 2. Klicken Sie auf `Reuse Certificate`.

Schritt 3: Wählen Sie aus der `choose Tomcat type` Dropdown-Liste die Option `tomcat`.

Schritt 4. Aktivieren Sie im `Replace Certificate for the following purpose` Fenster das Kontrollkästchen `CallManager`.

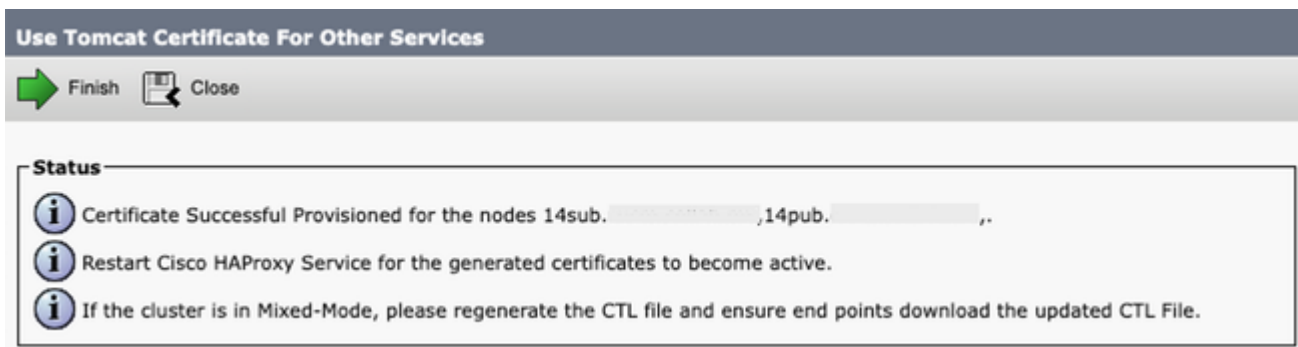


Tomcat-Zertifikat für andere Dienste wiederverwenden, Bildschirm



Anmerkung: Wenn Sie Tomcat als Zertifikatstyp auswählen, ist CallManager als Ersatz aktiviert. Wenn Sie tomcat-ECDSA als Zertifikatstyp auswählen, wird CallManager-ECDSA als Ersatz aktiviert.

Schritt 5: Klicken Sie auf **Finish**, um das CallManager-Zertifikat durch das Tomcat Multi-SAN-Zertifikat zu ersetzen.



Erfolgreiche Nachricht des Tomcat-Zertifikats wiederverwenden

Schritt 6: Starten Sie den Cisco HAProxy-Dienst neu, öffnen Sie eine CLI-Sitzung mit allen Knoten des Clusters, und führen Sie den `utils service restart Cisco HAProxy` Befehl aus.



Anmerkung: Um festzustellen, ob sich der Cluster im gemischten Modus befindet, navigieren Sie zu **Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode** (0 == Nicht sicher; 1 == Mixed Mode).

Schritt 7: Wenn sich Ihr Cluster im gemischten Modus befindet, öffnen Sie eine CLI-Sitzung zum Publisher-Knoten, führen Sie einen `utils ctl update CTLFile` Befehl aus, und setzen Sie alle Telefone des Clusters zurück, damit die CTL-Dateiaktualisierungen wirksam werden.

## Überprüfung

Schritt 1: Navigieren Sie zu Ihrem CUCM-Publisher, und wechseln Sie dann zu **Cisco Unified OS Administration > Security > Certificate Management**.

Schritt 2. Filtern Sie nach **Find Certificate List where: Usage > begins with: identity** und klicken Sie auf **Find**.

Schritt 3: CallManager- und Tomcat-Zertifikate müssen mit demselben **Common Name\_Serial Number** Wert enden.

Cisco

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	CAPF-02a10666	Identity	Self-signed	RSA	14pub.cucm.collab.mx	CAPF-02a10666	12/20/2027	Self-signed certificate generated by system
ipsec	14pub. 6f44af5c5cd753d5ff1538c3879b44	Identity	Self-signed	RSA	14pub.cucm.collab.mx	14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
ITLRecovery	ITLRECOVERY 14pub. 727029eea3d929d99c99bee38720c89e	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. 6ea1f2fedf8f6183cdf629a4a0f0447f	Identity	Self-signed	EC	14pub.cucm.collab.mx	14pub-EC.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
TVS	14pub. 7d8022fd6eb2885c3406b7cb4126046	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

Überprüfen der Wiederverwendung des Tomcat-Zertifikats für CallManager



Anmerkung: Ab SU4 wird bei aktivierter Zertifikatwiederverwendung das Call Manager-Zertifikat nicht mehr in der GUI angezeigt, während beide Zertifikate in SU2 und SU3 sichtbar sind.

## Zugehörige Informationen

- [Sicherheitsleitfaden für Cisco Unified Communications Manager 14](#)
- [Technischer Support und Downloads von Cisco](#)

### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.