

# Neue Zertifikate aus signierten Zertifizierungsstellenzertifikaten erstellen

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Informationen vor der Prüfung](#)

[Zertifikate konfigurieren und neu erstellen](#)

[Tomcat-Zertifikat](#)

[CallManager-Zertifikat](#)

[IPSec-Zertifikat](#)

[CAPF-Zertifikat](#)

[TVS-Zertifikat](#)

[Fehlerbehebung bei häufig hochgeladenen Zertifikatfehlermeldungen](#)

[Das Zertifizierungsstellenzertifikat ist im Vertrauensstellungsspeicher nicht verfügbar.](#)

[Datei /usr/local/platform/.security/tomcat/keys/tomcat.csr existiert nicht](#)

[Öffentlicher CSR-Schlüssel und öffentlicher Zertifikatschlüssel stimmen nicht überein](#)

[CSR-Betreff Alternativer Name \(SAN\) und Zertifikat-SAN stimmen nicht überein](#)

[Vertrauenswürdige Zertifikate mit derselben CN werden nicht ersetzt](#)

## Einleitung

In diesem Dokument wird beschrieben, wie die von einer Zertifizierungsstelle (Certificate Authority, CA) in Cisco Unified Communications Manager (CUCM) signierten Zertifikate neu generiert werden.

## Voraussetzungen

### Anforderungen

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

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

### Verwendete Komponenten

- CUCM-Versionen 10.x, 11.x und 12.x

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 verstehen.

## Informationen vor der Prüfung

**Anmerkung:** Informationen zur Regeneration von selbstsignierten Zertifikaten finden Sie im [Certificate Regeneration Guide](#). Informationen zur Wiederherstellung von CA-signierten Multi-SAN-Zertifikaten finden Sie im [Multi-SAN Certificate Regeneration Guide](#).

Informationen zu den Auswirkungen der einzelnen Zertifikate und ihrer Erneuerung finden Sie im [Self-Signed Regeneration Guide](#).

Jeder CSR-Typ (Certificate Signing Request) weist unterschiedliche Schlüsselverwendungen auf, die für das signierte Zertifikat erforderlich sind. Der [Sicherheitsleitfaden](#) enthält eine Tabelle mit den erforderlichen Schlüsselverwendungen für jeden Zertifikatstyp.

Führen Sie den folgenden Befehl aus, um die Betreffeeinstellungen (Lokalität, Status, Organisationseinheit usw.) zu ändern:

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

Das Tomcat-Zertifikat wird automatisch neu generiert, nachdem Sie das `set web-security` aus. Das neue selbstsignierte Zertifikat wird erst angewendet, wenn der Tomcat-Dienst neu gestartet wird. Weitere Informationen zu diesem Befehl finden Sie in den folgenden Handbüchern:

- [Befehlszeilenreferenz](#)
- [Link zu Cisco Community-Schritten](#)
- [Video](#)

## Zertifikate konfigurieren und neu erstellen

Die Schritte zum Regenerieren von Einzelknoten-Zertifikaten in einem von einer Zertifizierungsstelle signierten CUCM-Cluster werden für jeden Zertifikatstyp aufgelistet. Es ist nicht erforderlich, alle Zertifikate im Cluster neu zu generieren, wenn sie nicht abgelaufen sind.

### Tomcat-Zertifikat

**Achtung:** Überprüfen Sie, ob SSO im Cluster deaktiviert ist (**CM Administration > System > SAML Single Sign-On**). Wenn SSO aktiviert ist, muss es deaktiviert und nach Abschluss der Tomcat-Zertifikatregeneration aktiviert werden.

Auf allen Knoten (CallManager und IM&P) des Clusters:

Schritt 1: Navigieren Sie zu **Cisco Unified OS Administration > Security > Certificate Management > Find** und das Ablaufdatum des Tomcat-Zertifikats überprüfen.

Schritt 2: Klicken Sie auf **Generate CSR > Certificate Purpose: tomcat**. Wählen Sie die gewünschten Einstellungen für das Zertifikat aus, und klicken Sie auf **Generate**. Warten Sie, bis die Erfolgsmeldung angezeigt wird, und klicken Sie auf **Close**.

**Generate Certificate Signing Request**

Generate Close

**Status**

Success: Certificate Signing Request Generated

**Generate Certificate Signing Request**

Certificate Purpose\*\* tomcat

Distribution\* 115pub

Common Name\* 115pub

**Subject Alternate Names (SANs)**

Parent Domain

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.

Schritt 3: CSR herunterladen Klicken Sie auf **Download CSR** , wählen **Certificate Purpose: tomcat**, und klicke auf **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.

Schritt 4: Senden Sie den CSR an die Zertifizierungsstelle.

Schritt 5: Die Zertifizierungsstelle gibt zwei oder mehr Dateien für die signierte Zertifikatskette zurück. Laden Sie die Zertifikate in der folgenden Reihenfolge hoch:

- Stammzertifikat der Zertifizierungsstelle als tomcat-trust. Navigieren Sie zu **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die Stammzertifikatdatei.
- Zwischenzertifikat als tomcat-trust (Optional). **Navigieren Sie zu Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die Datei für das Zwischenzertifikat.

**Anmerkung:** Einige CAs stellen kein Zwischenzertifikat bereit. Wenn nur das Root-Zertifikat angegeben wurde, kann dieser Schritt ausgelassen werden.

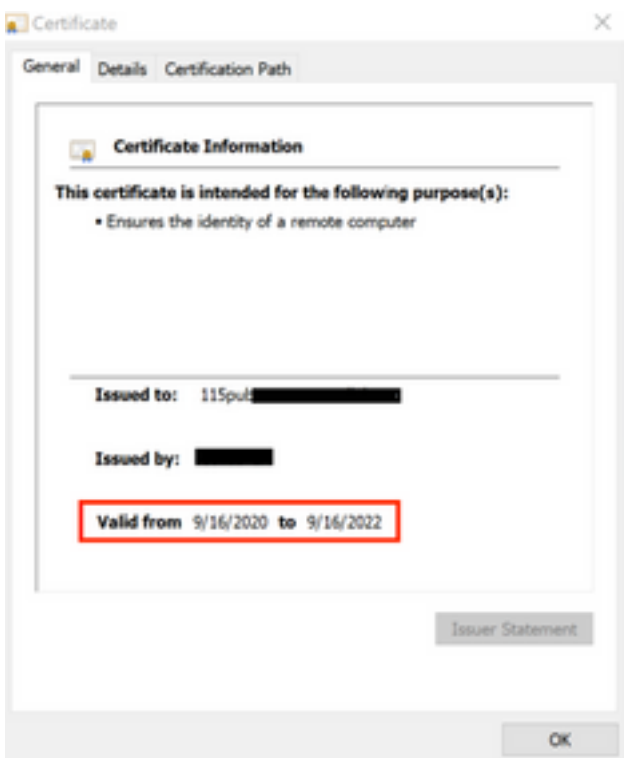
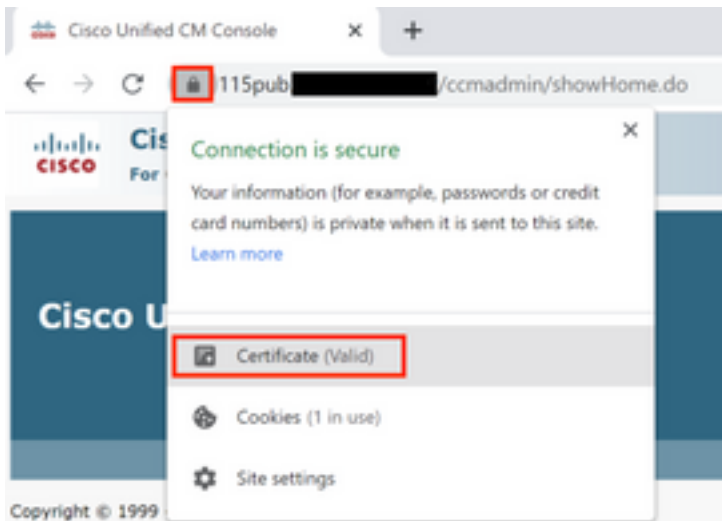
- CA-signiertes Zertifikat als Tomcat. **Navigieren Sie zu Certificate Management > Upload certificate >**

**Certificate Purpose:** tomcat. Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die CA-signierte Zertifikatsdatei für den aktuellen CUCM-Knoten.

**Anmerkung:** An diesem Punkt vergleicht CUCM den CSR mit dem hochgeladenen, von einer Zertifizierungsstelle signierten Zertifikat. Wenn die Informationen übereinstimmen, wird der CSR gelöscht, und das neue von der Zertifizierungsstelle signierte Zertifikat wird hochgeladen. Wenn Sie nach dem Hochladen des Zertifikats eine Fehlermeldung erhalten, lesen Sie den Upload Certificate Common Error Messages Abschnitt.

Schritt 6: Um das neue Zertifikat auf den Server anzuwenden, muss der Cisco Tomcat-Dienst über die CLI neu gestartet werden (zuerst mit Publisher und dann mit den Abonnenten). Verwenden Sie hierzu den Befehl `utils service restart Cisco Tomcat`.

Zur Validierung wird das Tomcat-Zertifikat jetzt von CUCM verwendet. Navigieren Sie zur Webseite des Knotens, und wählen Sie Site Information (Symbol sperren) im Browser auf die Schaltfläche `certificate`, und überprüfen Sie das Datum des neuen Zertifikats.



## CallManager-Zertifikat

**Vorsicht:** Generieren Sie nicht gleichzeitig CallManager- und TVS-Zertifikate. Dies führt zu einer nicht wiederherstellbaren Diskrepanz zwischen der installierten ITL auf den Endpunkten, die das Entfernen der ITL von ALLEN Endpunkten im Cluster erfordert. Beenden Sie den gesamten Prozess für CallManager, und starten Sie den Prozess für das TVS, sobald die Telefone wieder registriert sind.

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

Für alle CallManager-Knoten des Clusters:

Schritt 1: Navigieren Sie zu **Cisco Unified OS Administration > Security > Certificate Management > Find** und das Ablaufdatum des CallManager-Zertifikats überprüfen.

Schritt 2: Klicken Sie auf **Generate CSR > Certificate Purpose: CallManager**. Wählen Sie die gewünschten Einstellungen für das Zertifikat aus, und klicken Sie auf **Generate**. Warten Sie, bis die Erfolgsmeldung angezeigt wird, und klicken Sie auf **Close**.

Schritt 3: CSR herunterladen Klicken Sie auf **Download CSR**. Select **Certificate Purpose: CallManager** and click **Download**.

Schritt 4: Senden Sie den CSR an das Certificate Authority .

Schritt 5: Die Zertifizierungsstelle gibt zwei oder mehr Dateien für die signierte Zertifikatskette zurück. Laden Sie die Zertifikate in der folgenden Reihenfolge hoch:

- Stammzertifikat der Zertifizierungsstelle als CallManager-trust. Navigieren Sie zu **Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust**. Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die Stammzertifikatdatei.
- Zwischenzertifikat als CallManager-trust (Optional). Navigieren Sie zu **Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust**. Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die Datei für das Zwischenzertifikat.

**Anmerkung:** Einige CAs stellen kein Zwischenzertifikat bereit. Wenn nur das Root-Zertifikat angegeben wurde, kann dieser Schritt ausgelassen werden.

- CA-signiertes Zertifikat als CallManager. Navigieren Sie zu **Certificate Management > Upload certificate > Certificate Purpose: CallManager**. Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die CA-signierte Zertifikatsdatei für den aktuellen CUCM-Knoten.

**Anmerkung:** An diesem Punkt vergleicht CUCM den CSR mit dem hochgeladenen, von einer Zertifizierungsstelle signierten Zertifikat. Wenn die Informationen übereinstimmen, wird der CSR gelöscht, und das neue von der Zertifizierungsstelle signierte Zertifikat wird hochgeladen. Wenn Sie nach dem Hochladen des Zertifikats eine Fehlermeldung erhalten, lesen Sie den Abschnitt **Häufige Fehlermeldungen beim Hochladen von Zertifikaten**.

Schritt 6: Wenn sich der Cluster im gemischten Modus befindet, aktualisieren Sie die CTL, bevor

die Dienste neu starten: [Token](#) oder [Tokenlos](#). Wenn sich der Cluster im ungesicherten Modus befindet, überspringen Sie diesen Schritt, und fahren Sie mit dem Neustart der Dienste fort.

Schritt 7: Um das neue Zertifikat auf den Server anzuwenden, müssen die erforderlichen Dienste neu gestartet werden (nur wenn der Dienst ausgeführt wird und aktiv ist). Navigieren Sie zu:

- 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

Schritt 8. Alle Telefone zurücksetzen:

- Navigieren Sie zu Cisco Unified CM Administration > System > Enterprise Parameters > Reset. Ein Popup-Fenster mit der Anweisung Sie sind im Begriff, alle Geräte im System zurückzusetzen wird angezeigt. Diese Aktion kann nicht rückgängig gemacht werden. Fortfahren? auswählen OK und dann auf Reset .

**Anmerkung:** Überwachung der Geräteregistrierung über RTMT Sobald sich alle Telefone wieder registriert haben, können Sie mit dem nächsten Zertifikatstyp fortfahren.

## IPSec-Zertifikat

**Vorsicht:** Eine Sicherungs- oder Wiederherstellungsaufgabe darf nicht aktiv sein, wenn das IPSec-Zertifikat neu generiert wird.

Für alle Knoten (CallManager und IM&P) des Clusters:

Schritt 1: Navigieren Sie zu Cisco Unified OS Administration > Security > Certificate Management > Find und das Ablaufdatum des IPSec-Zertifikats überprüfen.

Schritt 2: Klicken Sie auf **CSR erstellen > Zertifikatzweck: IPsec**. Wählen Sie die gewünschten Einstellungen für das Zertifikat aus, und klicken Sie dann auf **Generate (Generieren)**. Warten Sie, bis die Erfolgsmeldung angezeigt wird, und klicken Sie dann auf **Schließen**.

Schritt 3: CSR herunterladen Klicken Sie auf **CSR herunterladen**. Wählen Sie Zertifikatzweck ipsec aus, und klicken Sie auf **Herunterladen**.

Schritt 4: Senden Sie den CSR an die Zertifizierungsstelle.

Schritt 5: Die Zertifizierungsstelle gibt zwei oder mehr Dateien für die signierte Zertifikatskette zurück. Laden Sie die Zertifikate in der folgenden Reihenfolge hoch:

- Zertifikat der Stammzertifizierungsstelle als ipsec-trust. Navigieren Sie zu **Zertifikatsverwaltung > Zertifikat hochladen > Zertifikatzweck: ipsec-trust**. Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die Stammzertifikatdatei.
- Zwischenzertifikat als ipsec-trust (optional). Navigieren Sie zu **Zertifikatsverwaltung > Zertifikat hochladen > Zertifikatzweck: auf Katzenvertrauen**. Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die Datei für das Zwischenzertifikat.

**Anmerkung:** Einige CAs stellen kein Zwischenzertifikat bereit. Wenn nur das Root-Zertifikat angegeben wurde, kann dieser Schritt ausgelassen werden.

- CA-signiertes Zertifikat als ipsec. Navigieren Sie zu **Zertifikatsverwaltung > Zertifikat hochladen > Zertifikatzweck: IPsec**. Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die CA-signierte Zertifikatsdatei für den aktuellen CUCM-Knoten.

**Anmerkung:** An diesem Punkt vergleicht CUCM den CSR mit dem hochgeladenen, von einer Zertifizierungsstelle signierten Zertifikat. Wenn die Informationen übereinstimmen, verschwindet der CSR, und das neue CA-signierte Zertifikat wird hochgeladen. Wenn Sie nach dem Hochladen des Zertifikats eine Fehlermeldung erhalten, lesen Sie den **Abschnitt Allgemeine Fehlermeldungen beim Hochladen von Zertifikaten**.

Schritt 6: Um das neue Zertifikat auf den Server anzuwenden, müssen die erforderlichen Dienste neu gestartet werden (nur wenn der Dienst ausgeführt wird und aktiv ist). Navigieren Sie zu:

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

## CAPF-Zertifikat

**Hinweis:** Um festzustellen, ob sich der Cluster im gemischten Modus befindet, wechseln Sie zu **Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non-Secure; 1 == Mixed Mode)**.

**Hinweis:** Der CAPF-Dienst wird nur auf dem Publisher ausgeführt, und nur dieses Zertifikat wird verwendet. Es ist nicht erforderlich, von einer Zertifizierungsstelle signierte Subscriber-Knoten zu erhalten, da sie nicht verwendet werden. Wenn das Zertifikat in den Abonnenten abgelaufen ist und Sie die Warnungen abgelaufener Zertifikate vermeiden möchten, können Sie CAPF-Abonnementzertifikate als selbstsigniert neu generieren. Weitere Informationen finden Sie unter [CAPF-Zertifikat als selbstsigniert](#).

Im Publisher:

Schritt 1: Navigieren Sie zu **Cisco Unified OS Administration > Security > Certificate Management > Find and verify the expiry date of the CAPF certificate**.

Schritt 2: Klicken Sie auf **CSR erstellen > Zertifikatzweck: CAPF**. Wählen Sie die gewünschten Einstellungen für das Zertifikat aus, und klicken Sie dann auf **Generate (Generieren)**. Warten Sie, bis die Erfolgsmeldung angezeigt wird, und klicken Sie auf **Schließen**.

Schritt 3: CSR herunterladen Klicken Sie auf **CSR herunterladen**. Wählen Sie CAPF für Zertifikatzwecke aus, und klicken Sie auf **Herunterladen**.

Schritt 4: Senden Sie den CSR an die Zertifizierungsstelle.

Schritt 5: Die Zertifizierungsstelle gibt zwei oder mehr Dateien für die signierte Zertifikatskette zurück. Laden Sie die Zertifikate in der folgenden Reihenfolge hoch:

- Stammzertifikat der Zertifizierungsstelle als CAPF-trust. Navigieren Sie zu



**Zertifikatsverwaltung > Zertifikat hochladen > Zertifikatzweck: CAPF-Trust** Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die Stammzertifikatsdatei.

- **Zwischenzertifikat als CAPF-trust (Optional).** Navigieren Sie zu **Zertifikatsverwaltung > Zertifikat hochladen > Zertifikatzweck: CAPF-Trust.** Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die Datei für das Zwischenzertifikat.

**Anmerkung:** Einige CAs stellen kein Zwischenzertifikat bereit. Wenn nur das Root-Zertifikat angegeben wurde, kann dieser Schritt ausgelassen werden.

- Von der Zertifizierungsstelle signiertes Zertifikat als CAPF. Navigieren Sie zu **Zertifikatsverwaltung > Zertifikat hochladen > Zertifikatzweck: CAPF.** Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die CA-signierte Zertifikatsdatei für den aktuellen CUCM-Knoten.

**Anmerkung:** An diesem Punkt vergleicht CUCM den CSR mit dem hochgeladenen, von einer Zertifizierungsstelle signierten Zertifikat. Wenn die Informationen übereinstimmen, verschwindet der CSR, und das neue CA-signierte Zertifikat wird hochgeladen. Wenn Sie nach dem Hochladen des Zertifikats eine Fehlermeldung erhalten, lesen Sie den Abschnitt **Häufige Fehlermeldungen beim Hochladen von Zertifikaten.**

Schritt 6: Wenn sich der Cluster im gemischten Modus befindet, aktualisieren Sie die CTL, bevor die Dienste neu starten: [Token](#) oder [Tokenlos](#). Wenn sich der Cluster im ungesicherten Modus befindet, überspringen Sie diesen Schritt, und fahren Sie mit dem Neustart des Diensts fort.

Schritt 7: Um das neue Zertifikat auf den Server anzuwenden, müssen die erforderlichen Dienste neu gestartet werden (nur wenn der Dienst ausgeführt wird und aktiv ist). Navigieren Sie zu:

- **Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service** (Alle Knoten, auf denen der Service ausgeführt wird)
- **Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP** (Alle Knoten, auf denen der Service ausgeführt wird)
- **Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco Certificate Authority Proxy Function** (Publisher)

Schritt 8. Alle Telefone zurücksetzen:

- Navigieren Sie zu **Cisco Unified CM Administration > System > Enterprise Parameters > Reset.** Ein Popup-Fenster mit der Anweisung Sie sind im Begriff, alle Geräte im System zurückzusetzen wird angezeigt. Diese Aktion kann nicht rückgängig gemacht werden. Fortfahren? Wählen Sie **OK aus**, und klicken Sie dann auf **Zurücksetzen**.

**Anmerkung:** Überwachung der Geräteregistrierung über RTMT Sobald sich alle Telefone wieder registriert haben, können Sie mit dem nächsten Zertifikatstyp fortfahren.

## TVS-Zertifikat

**Vorsicht:** Generieren Sie nicht gleichzeitig CallManager- und TVS-Zertifikate. Dies führt zu einer nicht wiederherstellbaren Diskrepanz zwischen der installierten ITL auf den



Endpunkten, die das Entfernen der ITL von ALLEN Endpunkten im Cluster erfordert.  
Beenden Sie den gesamten Prozess für CallManager, und starten Sie den Prozess für das TVS, sobald die Telefone wieder registriert sind.

Für alle TVS-Knoten des Clusters:

Schritt 1: Navigieren Sie zu **Cisco Unified OS Administration > Security > Certificate Management > Find** and verify the expiry date of the TVS certificate.

Schritt 2: Klicken Sie auf **CSR erstellen > Zertifikatzweck: TVS**. Wählen Sie die gewünschten Einstellungen für das Zertifikat aus, und klicken Sie dann auf **Generate (Generieren)**. Warten Sie, bis die Erfolgsmeldung angezeigt wird, und klicken Sie auf **Schließen**.

Schritt 3: CSR herunterladen Klicken Sie auf **CSR herunterladen**. Wählen Sie **Zertifikatzweck-TVS aus**, und klicken Sie auf **Herunterladen**.

Schritt 4: Senden Sie den CSR an die Zertifizierungsstelle.

Schritt 5: Die Zertifizierungsstelle gibt zwei oder mehr Dateien für die signierte Zertifikatskette zurück. Laden Sie die Zertifikate in der folgenden Reihenfolge hoch:

- Zertifikat der Stammzertifizierungsstelle als TVS-trust. Navigieren Sie zu **Zertifikatsverwaltung > Zertifikat hochladen > Zertifikatzweck: TVS-Trust**. Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die Stammzertifikatdatei.
- Zwischenzertifikat als TVS-trust (Optional). Navigieren Sie zu **Zertifikatsverwaltung > Zertifikat hochladen > Zertifikatzweck: TVS-Trust**. Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die Datei für das Zwischenzertifikat.

**Anmerkung:** Einige CAs stellen kein Zwischenzertifikat bereit. Wenn nur das Root-Zertifikat angegeben wurde, kann dieser Schritt ausgelassen werden.

- CA-signiertes Zertifikat als TVS. Navigieren Sie zu **Zertifikatsverwaltung > Zertifikat hochladen > Zertifikatzweck: TVS**. Legen Sie die Beschreibung des Zertifikats fest, und durchsuchen Sie die CA-signierte Zertifikatsdatei für den aktuellen CUCM-Knoten.

**Anmerkung:** An diesem Punkt vergleicht CUCM den CSR mit dem hochgeladenen, von einer Zertifizierungsstelle signierten Zertifikat. Wenn die Informationen übereinstimmen, wird der CSR gelöscht, und das neue von der Zertifizierungsstelle signierte Zertifikat wird hochgeladen. Wenn Sie nach dem Hochladen des Zertifikats eine Fehlermeldung erhalten, lesen Sie den Abschnitt **Häufige Fehlermeldungen beim Hochladen von Zertifikaten**.

Schritt 6: Um das neue Zertifikat auf den Server anzuwenden, müssen die erforderlichen Dienste neu gestartet werden (nur wenn der Dienst ausgeführt wird und aktiv ist). Navigieren Sie zu:

- **Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP** (Alle Knoten, auf denen der Service ausgeführt wird)
- **Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service** (Alle Knoten, auf denen der Service ausgeführt wird)

Schritt 7. Alle Telefone zurücksetzen:

- Navigieren Sie zu **Cisco Unified CM Administration > System > Enterprise Parameters > Reset**. Ein Popup-Fenster mit der Anweisung Sie sind im Begriff, alle Geräte im System zurückzusetzen wird angezeigt. Diese Aktion kann nicht rückgängig gemacht werden. Fortfahren? Wählen Sie **OK aus**, und klicken Sie dann auf **Zurücksetzen**.

**Anmerkung:** Überwachung der Geräteregistrierung über RTMT Sobald sich alle Telefone wieder registriert haben, können Sie mit dem nächsten Zertifikatstyp fortfahren.

## Fehlerbehebung bei häufig hochgeladenen Zertifikatfehlermeldungen

In diesem Abschnitt werden einige der häufigsten Fehlermeldungen beim Hochladen eines von einer Zertifizierungsstelle signierten Zertifikats aufgeführt.

### Das Zertifizierungsstellenzertifikat ist im Vertrauensstellungsspeicher nicht verfügbar.

Dieser Fehler bedeutet, dass das Stamm- oder Zwischenzertifikat nicht in den CUCM hochgeladen wurde. Überprüfen Sie, ob diese beiden Zertifikate als vertrauenswürdiger Speicher hochgeladen wurden, bevor das Dienstzertifikat hochgeladen wird.

### Datei `/usr/local/platform/.security/tomcat/keys/tomcat.csr` existiert nicht

Dieser Fehler wird angezeigt, wenn für das Zertifikat kein CSR vorhanden ist (tomcat, callmanager, ipsec, capf, tvs). Überprüfen Sie, ob der CSR zuvor erstellt wurde und ob das Zertifikat auf Grundlage dieses CSR erstellt wurde. Wichtige Punkte:

- Pro Server und Zertifikatstyp kann nur ein CSR vorhanden sein. Das heißt, wenn eine neue CSR erstellt wird, wird die alte ersetzt.
- Platzhalterzertifikate werden von CUCM nicht unterstützt.
- Es ist nicht möglich, ein bereits bestehendes Servicegesetz ohne neuen CSR zu ersetzen.
- Ein weiterer möglicher Fehler für dasselbe Problem ist "Die Datei `/usr/local/platform/upload/certs//tomcat.der` konnte nicht hochgeladen werden." Dies hängt von der CUCM-Version ab.

### Öffentlicher CSR-Schlüssel und öffentlicher Zertifikatschlüssel stimmen nicht überein

Dieser Fehler tritt auf, wenn das von der Zertifizierungsstelle bereitgestellte Zertifikat einen anderen öffentlichen Schlüssel als den in der CSR-Datei gesendeten hat. Mögliche Gründe:

- Das falsche Zertifikat (möglicherweise von einem anderen Knoten) wird hochgeladen.
- Das CA-Zertifikat wurde mit einem anderen CSR generiert.
- Der CSR wurde neu generiert und ersetzte den alten CSR, der zum Erhalt des signierten Zertifikats verwendet wurde.


Zur Überprüfung der Übereinstimmung von CSR und öffentlichem Zertifikatschlüssel stehen mehrere Online-Tools wie [SSL zur Verfügung](#).

## What to Check

- Check if a Certificate and a Private Key match
- Check if a CSR and a Certificate match

### Enter your Certificate:

```
Tj13aw4xMxDt1DRFAsQ049UHvibGj1iws2v5j1fwu2vYdmjzAMsQ049Uzvy
dmjZXMsQ049Q29uZmindXjdGhVbixEQz1jB2xsYWsREM9bxg/Y2VydGimaWVh
dGV5ZXZvY2F0aW9uTGZldD9mYXNpZ29iaWVjZENsYXNzPWV5TERpc3RyaWJ1dGlv
bWV5W50MIG7BggBgEgEFBQcBAQ5BjCBqzCBqAYIKwYBBQUHMAKGZtsZGFwOisv
L0NOPUNvGxhYIUyMENBLENOPUFjQsxDt1QdWjSaWMIjBLZXIMjBTZjZaWNI
cyxDt1T2Q2aWNIcyxDt1Db25maWd1cmF0aW9uLERDPWNvGxhYixEQz1teD9j
QUlncnRpZmlyXkFpZ2hc2U/b2jZWN0Q2xhc3M9Y2VydGimaWVhSGVibkF1dGhv
cmI0eTAhBgkrBgEEAYI3FAIEFB45AFcAZQBIAFMAZQByAHYAZQByMAOGCSqGSib3
DQEBCWUAA4BAQCFqz2Bc28CMxkunQavdYaUioDrfDpMLSA/7hisqW55xvBEQs
9LqyftmddCmkoMPGk42vMie40TpKBYAQvbrApG001mWV5u+f1Io9PvrygWtYL
D+ve7rMp8sirVo1Tmhe/26in3lbn+Ofwe5NuvCx3wNudLRR3904KcaFCcsVLQ6Aw
PtmvAz/9K2GRhzqacd9fVJuoWTKDj2Qsladcgsl5cvFMz3BBf0MjGBNX16jGiiQ
yZZBr6Gm4pa4yKq6sUrcOxHylomecYeRheKuSkuPusOeEfwWSzjQMT7P4Ww
ZBpT2TkrQdODAZHjGujP+yBa75OGGTZWVvg1
-----END CERTIFICATE-----
```

 The certificate and CSR do NOT match!

#### ✔ Certificate Hash:

684ad486131856ce0015d4b3e615e1ed  
3b3bef6b8f590a493921661a4c4f62e9

#### ✔ CSR Hash:

635f45c1ebcd876526a3133d1ee73d9a8  
4544876fdbbc8dc3a4d8fed377dcc635

### Enter your CSR:

```
q+hjgokSx+ogqVavFSNRdqTh0Grls1ga0pj5sGxOOLCqAtQH EARNEcGyanZtrK
gSjTQHfBjStD2vDyD3wg5iyhwNlqkMUl3IRD5qcSD/nyfLGLs8hB9y5HqtaDA3
1WUj5Q4RXk2188ESCILtB3bAoZegZo5Vw4/h5fP8r09e/CTWsxZtBfLgytvcDGk
OGrdW2xLueUv2u29jvYtmLD70CNXCM9XypLj6suyMuf0Bfh+s0F1Mr7gal3b
hXkS4ZjoFIMkYBWSFDwexH7XfD+HqaPeM4Y50N4YqhxAgMBAAQgbzBtBgkqhkiG
9w0BCQ4xYDBEMBOGA1UdjqQWMBQGCCSGAQUBwMBBgggBgEgEFBQcDAJALBGNWHQBE
BAMCBLAWMAYDVR0RBCKw4iOY3VjB55jB2xsYWVubXCFTEhXNB1Y15jdWNIcmNv
bGxhYi5teDANBgkqhkiG9w0BAQsFAAOCQAQEAhBgli76T59rWxOFjsg7hsj36vf
ubcW7HGFrNyx6/pl9UydunR0KDXQtZzWWc9IOA3/fpcjrz+8LdHtR1FnnwBwCV
Yca9s0nWZsmU1+clbTH1H5g8FFoHADg+FR3+1AE7GNfGK0CA0RipRihZPGzQ6dO
6ZTR5Q45LbcWxe4EZ05xjEQW7Zrkjfwby1GQKYg3CuXCETy3UunMCZnWjmNkKg0
n7B1nNdx7Ybgfz1IeY+ZozPHWgbu2HwChuh1bOAMUpkwiFebQZn9H+R7drjBAZR
IeXEYWL739M7BTveNmHoOnR6SkwvHYbb7iqDjnHxS9R0S0S2vUthkj7Hw==
-----END CERTIFICATE REQUEST-----
```

Ein weiterer möglicher Fehler für dasselbe Problem ist "Die Datei /usr/local/platform/upload/certs//tomcat.der konnte nicht hochgeladen werden." Dies hängt von der CUCM-Version ab.

## CSR-Betreff Alternativer Name (SAN) und Zertifikat-SAN stimmen nicht überein

Die SANs zwischen dem CSR und dem Zertifikat müssen identisch sein. Dadurch wird die Zertifizierung für nicht zulässige Domänen verhindert. Führen Sie die folgenden Schritte aus, um die SAN-Diskrepanz zu überprüfen:

1. Decodieren Sie die CSR und das Zertifikat (Basis 64). Es stehen verschiedene Decoder online zur Verfügung, z.B. der [Decoder](#).
2. Vergleichen Sie die SAN-Einträge, und stellen Sie sicher, dass alle übereinstimmen. Die Reihenfolge ist nicht wichtig, aber alle Einträge im CSR müssen im Zertifikat gleich sein.

Beispielsweise wurden dem CA-signierten Zertifikat zwei zusätzliche SAN-Einträge hinzugefügt: der Common Name des Zertifikats und eine zusätzliche IP-Adresse.

CSR Summary	
Subject: 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
Properties: 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:CB:79:FE:88:4A:86:96:77:0A:C5:8B: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	
Subject	
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
Properties	
Property	Value
Issuer	CN = Collab-CA,DC = collab,DC = mx
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:BD:0F
Fingerprint (MD5)	D8:22:33:92:59:F7:70:2A:D5:28:90:2D: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. Nachdem Sie festgestellt haben, dass das SAN nicht übereinstimmt, gibt es zwei Optionen, um dies zu beheben:

1. Bitten Sie Ihren CA-Administrator, ein Zertifikat mit genau den SAN-Einträgen auszustellen, die im CSR gesendet werden.
2. Erstellen Sie in CUCM einen CSR, der den Anforderungen der CA entspricht.

**So ändern Sie den vom CUCM erstellten CSR:**


1. Wenn die CA die Domäne entfernt, kann ein CSR im CUCM ohne die Domäne erstellt werden. Entfernen Sie während der CSR-Erstellung die Domäne, die standardmäßig eingetragen ist.
2. Wenn ein [Multi-SAN-Zertifikat](#) erstellt wird, gibt es einige Zertifizierungsstellen, die das Zeichen "-ms" im allgemeinen Namen nicht akzeptieren. Das Zeichen "-ms" kann nach der Erstellung aus dem CSR entfernt werden.

**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\* 115pub-ms [REDACTED]

**Subject Alternate Names (SANs)**

Auto-populated Domains

115imp [REDACTED]  
115pub [REDACTED]  
115sub [REDACTED]

Parent Domain

Other Domains

---

Key Type\*\* RSA

Key Length\* 2048

Hash Algorithm\* SHA256

Generate Close

3. So fügen Sie einen alternativen Namen neben den vom CUCM automatisch vervollständigten Namen hinzu:

1. Wenn ein Multi-SAN-Zertifikat verwendet wird, können weitere FQDN hinzugefügt werden. (IP-Adressen werden nicht akzeptiert.)

**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\* 115pub-ms- [REDACTED]

**Subject Alternate Names (SANs)**

Auto-populated Domains

115imp [REDACTED]  
115pub [REDACTED]  
115sub [REDACTED]

Parent Domain [REDACTED]

Other Domains

extrahostname.domain.com [REDACTED]

Choose File For more inform

Add

Key Type\*\* RSA

Key Length\* 2048

Hash Algorithm\* SHA256

Generate Close

b. Wenn das Zertifikat Single Node ist, verwenden Sie den `set web-security` aus. Dieser Befehl gilt auch für Multi-SAN-Zertifikate. (Jede Art von Domäne kann hinzugefügt werden, auch IP-Adressen sind zulässig.)

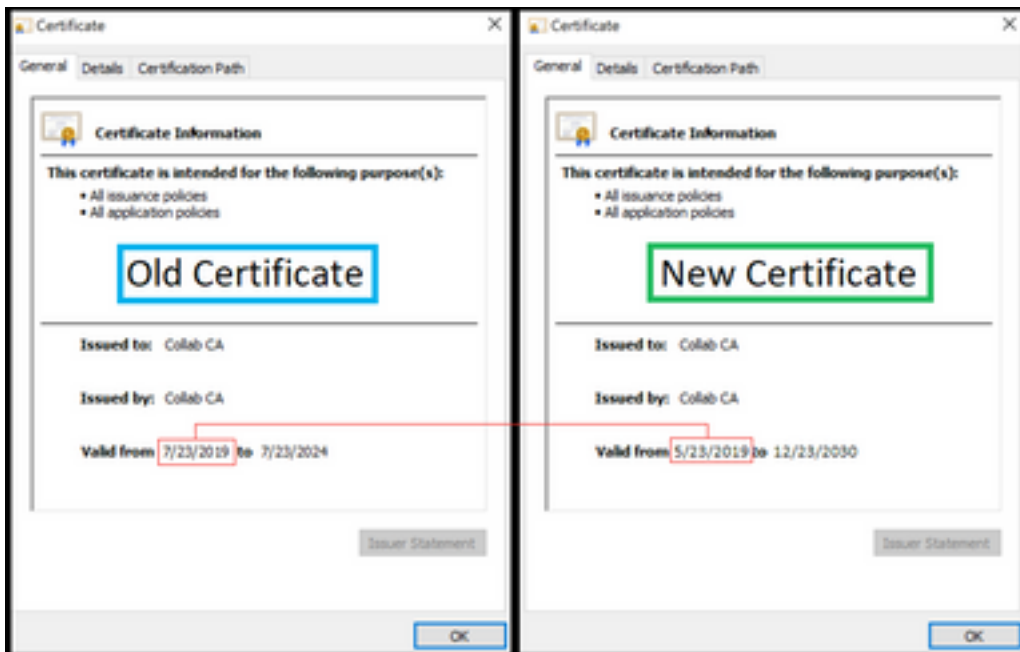
Weitere Informationen finden Sie im [Referenzhandbuch zur Befehlszeile](#).

## Vertrauenswürdige Zertifikate mit derselben CN werden nicht ersetzt

CUCM wurde entwickelt, um nur ein Zertifikat mit demselben gemeinsamen Namen und demselben Zertifikatstyp zu speichern. Das bedeutet, dass CUCM das alte Zertifikat entfernt und durch das neue ersetzt, wenn ein Zertifikat, das als "tomcat-trust" festgelegt ist, bereits in der Datenbank vorhanden ist und durch ein neues Zertifikat mit derselben CN ersetzt werden muss.

In einigen Fällen ersetzt CUCM das alte Zertifikat nicht:

1. Das hochgeladene Zertifikat ist abgelaufen: CUCM lässt das Hochladen eines abgelaufenen Zertifikats nicht zu.
2. Das alte Zertifikat hat ein aktuelleres "Von"-Datum als das neue Zertifikat. CUCM behält das aktuellste Zertifikat bei und katalogisiert es, wenn ein älteres "VON"-Datum vorliegt, als älter. In diesem Szenario müssen Sie das unerwünschte Zertifikat löschen und dann das neue hochladen.





## 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.