

Beheben gängiger Probleme bei der Zertifikatverlängerung in CUCM

Einleitung

In diesem Dokument werden häufige Probleme nach dem Regenerieren von Zertifikaten in Cisco Unified Communications Manager (CUCM) und deren Behebung beschrieben.

Voraussetzungen

Anforderungen

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

- Erneuerungsprozess für CUCM-Zertifikate
- Benutzeroberfläche des CUCM
- Expressway-Server
- Geräteregistrierung beim CUCM-Prozess
- Certificate Authority Proxy-Funktion
- Sicherheitsleitfaden für Cisco Unified Communications Manager

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:







- CUCM-Version 15

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.

Geschäftliche Auswirkungen

Diese Tabelle zeigt die geschäftlichen Auswirkungen jeder Zertifikatverlängerung in Ihrem Betrieb. Überprüfen Sie die Informationen sorgfältig. Erneuern Sie erforderliche Zertifikate nach Stunden oder in Ruhezeiten, basierend auf dem Risikograd der einzelnen Zertifikate.

 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, Ipsec 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	

Szenario 1: Telefone werden nach der Erneuerung des Call Manager-, TVS- und ITL-Zertifikats nicht registriert



Anmerkung: Dieses Szenario gilt für Bereitstellungen im gemischten Modus mit CUCM und in nicht sicheren Clustern sowie für selbstsignierte Zertifikate und Zertifizierungsstellenzertifikate.

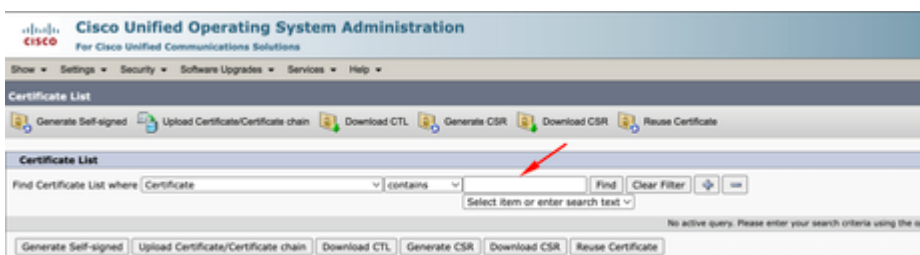
Wenn Call Manager-, TVS- und ITL-Zertifikate abgelaufen sind und gleichzeitig erneuert wurden, führt dies dazu, dass alle unsere Telefone nicht registriert sind, was erhebliche Auswirkungen auf das System hat. Dies ist ein erwartetes Verhalten, da wir die Telefone dazu veranlassen, dem CUCM nicht zu vertrauen.

Verifizierung

1. Stellen Sie sicher, dass die Zertifikate unter Cisco Unified OS Administration > Security > Certificate Management bereits abgelaufen sind.



2. Suchen Sie nach Callmanager, TVS oder ITL unter dem Filter oben auf der Seite und verwenden Sie die enthält oder beginnt mit Optionen:



3. Die Zertifikate müssen in der Spalte "Ablaufdatum" aktuell und eindeutig angezeigt werden (dies gilt auch für TVS- und ITL-Zertifikate).

Certificate	Common Name/Common Name, SerialNumber	Usage	Type	Key Size	Distribution	Issued By	Expiration	Description
CallManager	885.0000.ccm	Identity	CSR Only	2048	self team-cm	---	---	---
CallManager	885.0000.ccm_4885854832309c33a171262088	Identity	Self-signed	2048	self team-cm	self team-cm	8675/0209	Self signed certificate generated by system

4. Nachdem überprüft wurde, ob nach der Erneuerung des Zertifikats alles in Ordnung ist, werden die Telefone als nicht registriert angezeigt.

Device Name(s)	Description	Device Pool	Device Protocol	Status	Phone	Last Registered	Last Active	Unified CM
SEP045104PDC41	SEP045104PDC41	Default	SIP	Unregistered	Never	Feb 22, 2024 12:05:42 AM	Dec 29, 2023 7:32:23 PM	ccm@Soc3

Lösung

Es gibt zwei Optionen, um das Problem zu beheben:

1. Das Telefon auf die Werkseinstellungen zurücksetzen, sodass die aktuellen Sicherheitseinstellungen gelöscht und die neuen Zertifikate abgerufen werden können
2. Aktualisieren Sie die ITL- und CTL-Zertifikate von der CLI auf dem Publisher-Knoten, und verwenden Sie den Befehl `utils itl reset localkey`.

Dieser Schritt betrifft alle Telefone, einschließlich der registrierten Telefone. Stellen Sie sicher, dass Sie diesen Schritt nach Geschäftsschluss durchführen.



High Impact.

Szenario 2: Die einmalige Anmeldung funktioniert nach der Erneuerung des Tomcat-Zertifikats nicht



Anmerkung: Dieses Szenario kann auf Bereitstellungen angewendet werden, die eine clusterweite oder knotenbasierte Vereinbarung für die Konfiguration der einmaligen Anmeldung verwenden.

Bei der Anmeldung beim CUCM mit Single Sign-on (SSO) wird eine Fehlermeldung angezeigt "Fehler beim Verarbeiten der kleinen Antwort " oder " Fehler beim Verarbeiten der kleinen Antwort Fehler beim Entschlüsseln des geheimen Schlüssels "

Verifizierung

1. Stellen Sie sicher, dass alle Knoten ein gültiges Tomcat-Zertifikat enthalten, wenn sie selbst signiert sind, oder dass das neue zugeordnete Multi-San-Tomcat-Zertifikat enthalten ist.
2. Verwenden Sie die Option `set sam trace level debug` in all CUCM-Knoten via CLI, um SSO-Protokolle auf Debugebene zu aktivieren.
3. Erstellen Sie das Problem erneut, indem Sie sich erneut bei CUCM anmelden und die SSO-Methode verwenden.
4. Erfassen Sie nach dem Vorfall Tomcat SSO-Protokolle, und stellen Sie sicher, dass Sie die folgende Meldung erhalten:

- ```
2026-01-10 06:06:31,274 ERROR [http-nio-81-exec-157] cpi.sso.saml.sp.security.authentication.com.sun.identity.saml2.common.SAML2Exception: Failed to decrypt the secret key.
 at com.sun.identity.saml2.xmlenc.FMEncProvider.getEncryptionKey(FMEncProvider.
 at com.sun.identity.saml2.xmlenc.FMEncProvider.decrypt(FMEncProvider.java:607)
 at com.sun.identity.saml2.assertion.impl.EncryptedAssertionImpl.decrypt(Encryp
```

...

## Lösung

Export von CUCM-Metadaten nach Erneuerung des Tomcat-Zertifikats und Import in den Identitätsanbieter-Server, um sicherzustellen, dass das neue Tomcat-Zertifikat für diese Kommunikation vorhanden ist.

Verfahren zur Verlängerung von Tomcat bei aktivierter SSO-Bereitstellung:

---



Vorsicht: Das Technical Assistance Center (TAC) empfiehlt die nächsten Schritte, um Probleme nach der Erneuerung des Tomcat-Zertifikats zu vermeiden. Wir empfehlen, dieses Verfahren nach Feierabend durchzuführen.

---

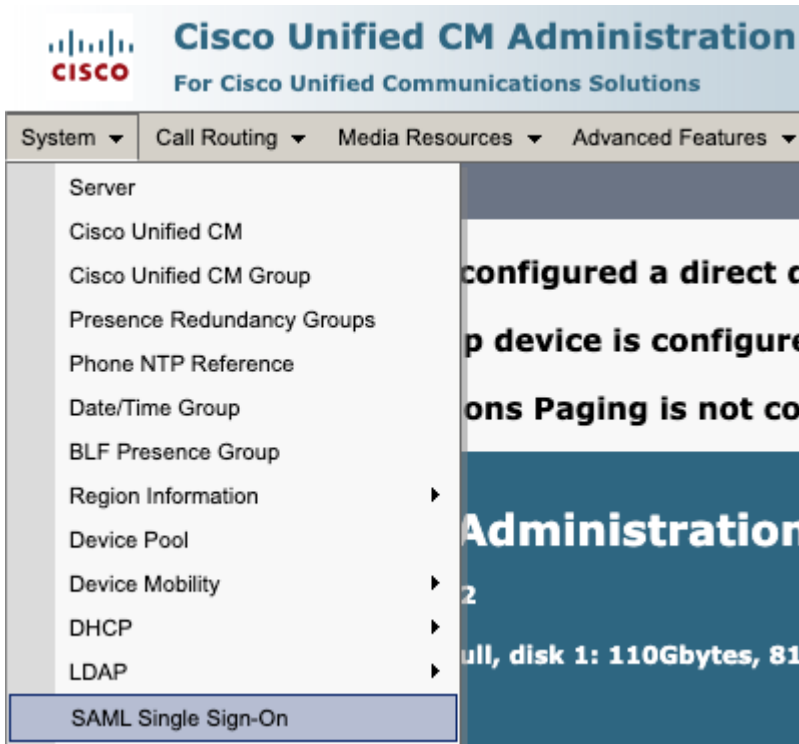


Low Impact

### 1. SSO in allen CUCM-Knoten deaktivieren



- Zugriff auf die CM-Administration > System > SAML Single Sign-on



- SAML SSO deaktivieren auswählen



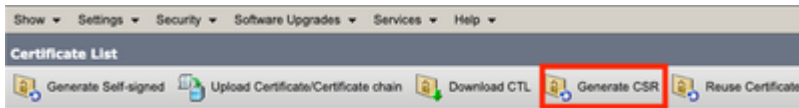
- Dieser Prozess muss in allen anderen Knoten über die GUI ausgeführt werden, wenn eine knotenspezifische Vereinbarung verwendet wird.

## 2. Tomcat-Zertifikat im CUCM-Cluster erneuern

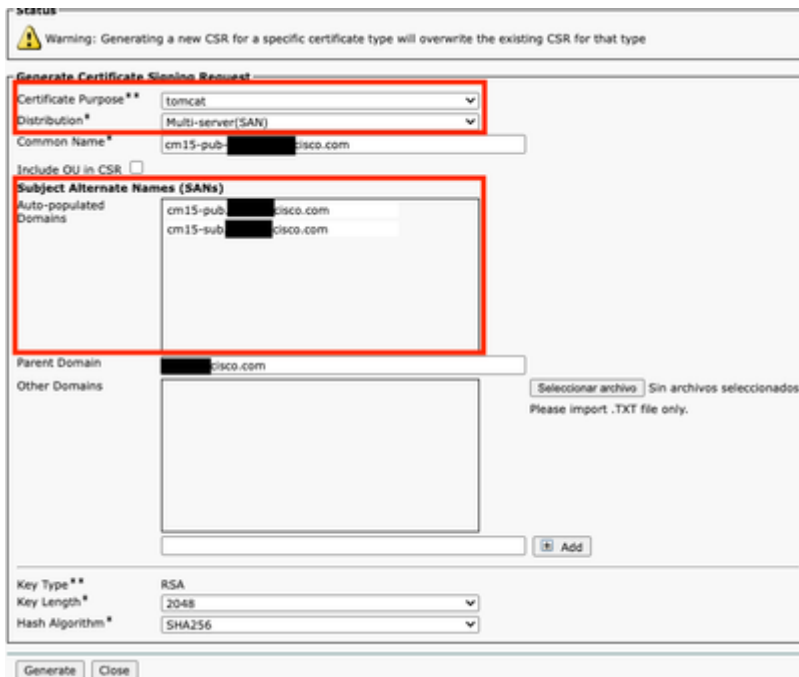


Allgemeines Verfahren zur Verlängerung des Tomcat-Multi-San-Zertifikats im CUCM-Cluster:

- Navigieren Sie zu OS administration > Security > Certificate management.
- Wählen Sie CSR generieren.



- Wählen Sie Tomcat in Certificate Property aus.
- Wählen Sie Multi-SAN in Distribution aus.
- Stellen Sie sicher, dass alle Knoten im Cluster unter Automatisch ausgefüllte Domänen aufgeführt sind.



- Wählen Sie Generate (Erstellen). Stellen Sie sicher, dass CSR auf allen Knoten im Cluster erstellt wird.
- Laden Sie den generierten CSR vom CUCM-Publisher herunter, und signieren Sie ihn mit einem CA-Server (Certificate Authority).
- Gehen Sie zu OS administration > Security > Certificate management. Wählen Sie Zertifikat hochladen/Zertifikatskette aus.
- Laden Sie CA-Zertifikate als Tomcat-trust hoch.
- Wiederholen Sie Schritt 6, und laden Sie das Tomcat-Zertifikat jetzt als Tomcat hoch.
- Nachdem Sie den Vorgang abgeschlossen und überprüft haben, dass auf alle Knoten das neue Tomcat-Zertifikat angewendet wurde, starten Sie den Tomcat-Dienst über die CLI in allen Knoten im Cluster mit diesem Befehl `utils service restart Cisco Tomcat neu`.

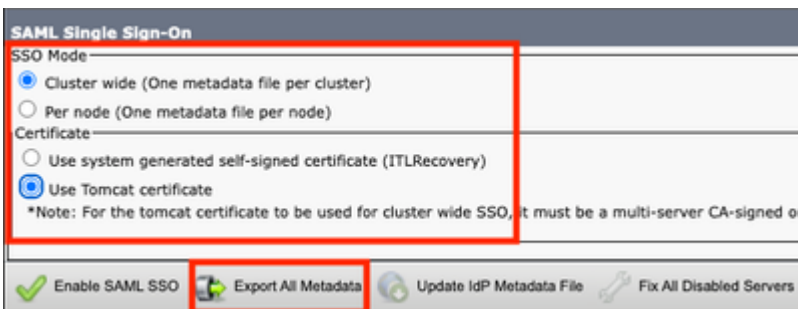
Weitere Informationen finden Sie in dieser Dokumentation:

- [Tomcat selbstsigniertes Zertifikat neu generieren](#)
- [Tomcat CA-signiertes Zertifikat neu generieren.](#)

### 3. Exportieren von Service Provider-Metadaten (SP)



- Gehen Sie zu CM Administration > System > Single Sign-On
- Konfigurieren Sie SSO-Optionen (in diesem Fall ist der SSO-Modus clusterweit und die Verwendung des Tomcat-Zertifikats auf dem Zertifikat als Beispiel konfiguriert), und wählen Sie dann Alle Metadaten exportieren aus.

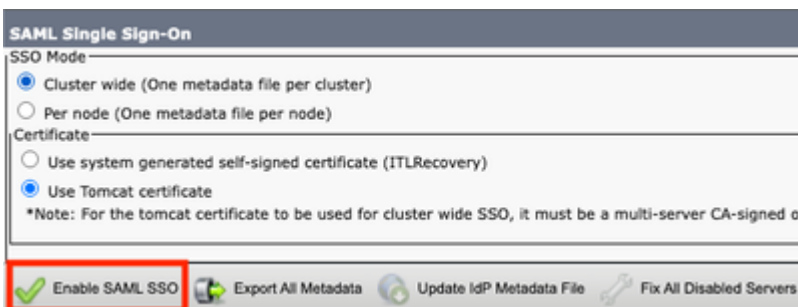



- SP-Metadaten in den Identity Provider (IdP)-Server importieren. Weitere Informationen finden Sie unter [Konfigurieren von SAML SSO auf dem Identitätsanbieter](#).

### 4. SSO im CUCM-Cluster aktivieren




- Gehen Sie zu CM Administration > System > Single Sign-On
- Wenn beim Exportieren von CUCM-Metadaten dieselben SSO-Optionen ausgewählt wurden, wählen Sie SAML SSO aktivieren und anschließend Weiter aus.



 Web server connections will be restarted


Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.

 Click "Export All Metadata" button

If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.  
If IDP is provisioned with cluster-wide SP metadata, you need to enable cluster-wide SAML SSO. If IDP is provisioned with per-node SP metadata, you need to enable per-node SAML SSO.


- Wenn Sie den gesamten Cluster verwenden, können Sie in diesem Schritt das Multi-SAN-Zertifikat auf allen Knoten überprüfen. Wählen Sie Test for multi-server tomcat certificate (Test für Multi-Server-Tomcat-Zertifikat). Wählen Sie nach Abschluss Weiter aus.

**SAML Single Sign-On Configuration**

 Next

---

**Status**

 Status: Ready

---

**Test for Multi-Server tomcat certificate**

The criteria for enabling clusterwide SSO is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:

- 1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
- 2) Click on Generate CSR
- 3) Select Certificate Purpose as Tomcat
- 4) Select Distribution as "Multi-Server"
- 5) Click Generate
- 6) Download the CSR and get it signed from the CA of your choice
- 7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
- 8) Restart Tomcat service on all the nodes in the cluster
- 9) Restart TFTP service on all the TFTP nodes in the cluster

For self-signed Multi-server tomcat certificate:

- 1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
- 2) Click on Generate self signed Multi-server tomcat certificate
- 3) Select Certificate Purpose as Tomcat
- 4) Select Distribution as "Multi-Server"
- 5) Click Generate
- 6) Restart Tomcat service on all the nodes in the cluster
- 7) Restart TFTP service on all the TFTP nodes in the cluster

If the above steps have been completed, click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage

- IdP-Metadaten hochladen, IdP-Metadaten importieren auswählen und nach Abschluss die Option Weiter auswählen

**SAML Single Sign-On Configuration**

Next

**Status**

Status: Ready

Import succeeded for all servers

**Import the IdP Metadata Trust File**

This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.

1) Select the IdP Metadata Trust File

Choose File No file chosen

2) Import this file to the Collaboration servers

This action must be successful for at least the Publisher before moving on to the next task in this wizard.

Import IdP Metadata

Import succeeded for all servers

Next Cancel

- Wählen Sie beim Test-SSO-Setup einen Benutzer aus, dem die Standard-CCM-Gruppe "Super Users" zugewiesen ist, und wählen Sie Run SSO Test (SSO-Test ausführen), bis Sie erfolgreich sind.

**SAML Single Sign-On Configuration**

Back

**Status**

The server metadata file must be installed on the IdP before this test is run.

**Test SSO Setup**

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on any

1) Pick a valid username to use for this test

You must already know the password for the selected username.  
This user must have administrator rights and also exist in the IdP.

Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

Valid administrator Usernames

admin@

2) Launch SSO test page

Run SSO Test...

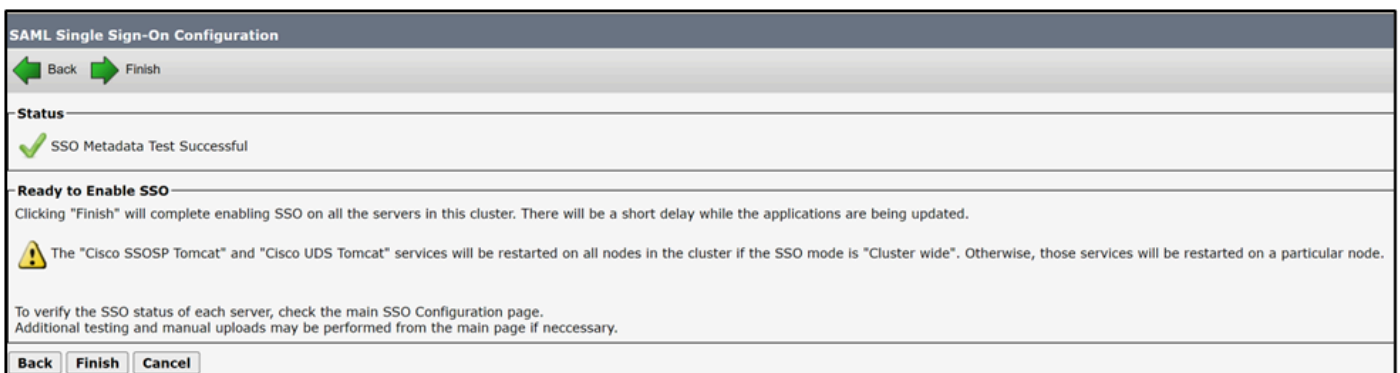
Back Cancel



4. Starten Sie erforderliche Dienste nach Aktivierung von SSO neu.



- Aktivierung von SSO zum Neustarten des Tomcat-Dienstes.



TAC empfiehlt jedoch, den Tomcat-Dienst (`utils service restart Cisco Tomcat`) und den UDS Tomcat-Dienst (`utils service restart CiscoUDSTomcat`) nach dem SSO-Aktivierungsprozess manuell in allen Knoten neu zu starten.

---

## Szenario 3: Registrierungsprobleme bei Mobility und Remote Access nach Erneuerung des Zertifikats

Die WebEx App kann sich nicht über Mobility and Remote Access (MRA) beim CUCM registrieren, nachdem die Anrufmanager-, Tomcat- und Expressway C-Zertifikate bei Bereitstellungen im gemischten Modus erneuert wurden.

## Verifizierung

1. Der CUCM-Anrufmanager und das Tomcat-Zertifikat sind CA-signierte Zertifikate.
2. Die CUCM- und Expressway-Bereitstellung wird im gemischten Modus (TLS) ausgeführt.
3. inspect Expressway-C logs shows "SSL routines:ssl3\_read\_bytes:tlsv1 alert unknown ca".

<#root>

```
2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]: UTCTime="2026-01-29 19:01:16,974" Modu
HTTPMSG:
```

```
|GET /CSFmarcoalh.cnf.xml HTTP/1.1
```

```
Host: expc.cisco.com:6972
```

```
Accept: */*
```

```
Cookie:<CONCEALED>
```

```
User-Agent: WebEx/0.0.0.0
```

```
TrackingID: fxxxxxxx-86f6-4030-8259-0b768c07723e
```

```
Client-ip: xxx.xxx.xxx.xxx
```

```
X-Forwarded-For: xxx.xxx.xxx.xxx, 127.0.0.1
```

```
Via: https/1.1 vcs[0fxxxxxx-c853-xxxx-aa16-0a290bf56fc8] (ATS), http/1.1 vcs[5xxxxxxx-7feb-4xxx-9
```

|

```
2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]:[ET_NET 1]ERROR:SSL connection failed for
```

```
SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca
```

## Lösung

Exportieren und importieren Sie Zertifikate zwischen CUCM und Expressway-C, um die Vertrauensstellung sicherzustellen.



Vorsicht: TAC empfiehlt, diesen Vorgang außerhalb der Geschäftszeiten durchzuführen, da bei diesem Verfahren ein Neustart der Services erforderlich ist. Geschäftliche Auswirkungen sind



**Medium Impact.**

1. Verfahren zum Abschließen der Vertrauensstellung zwischen CUCM und Expressway mit von CA signierten Zertifikaten



Navigieren Sie zu OS administration > Security > Certificate management, und laden Sie das Root-CA-Zertifikat und ggf. Intermediate herunter, die Call Manager und Tomcat-Zertifikat signieren.

**Certificate List**

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

Status  
18 records found

**Certificate List (1 - 18 of 18)** Rows per Page

Find Certificate List where Certificate begins with callmanager Find Clear Filter

| Certificate           | Common Name/Common Name_SerialNumber                            | Usage    | Type            | Key Type | Distribution      | Issued By |
|-----------------------|-----------------------------------------------------------------|----------|-----------------|----------|-------------------|-----------|
| CallManager           | cuem15sub-<br>2766.local:6f0000000c374e76d635a3840d00000000000c | Identity | CA-<br>signed   | RSA      | Multi-server(SAN) | 2766-ca-1 |
| CallManager-<br>ECDSA |                                                                 |          |                 |          |                   |           |
| CallManager-<br>trust | 2766-ca-<br>1_642238c85deb1c8b48ad6e45d0ab241c                  | Trust    | Self-<br>signed | RSA      | 2766-ca-1         | 2766-ca-1 |

Navigieren Sie anschließend zu Expressway-C > Maintenance > Security > Trusted CA certificate, und laden Sie das CA-Zertifikat des Call Manager- und Tomcat-Zertifikats hoch.

**Maintenance**

- Upgrade
- Logging
- Smart licensing
- Email Notifications
- Tools >
- Security**
  - Trusted CA certificate
  - Server certificate
  - CRL management
  - Client certificate testing
  - Certificate-based authentication configuration
  - Secure traversal test
  - Ciphers
  - SSH configuration
- Backup and restore
- Diagnostics >
- Maintenance mode
- Language
- Restart options

Choose File No file chosen

Upload

Select the file containing trusted CA certificates Choose File No file chosen

Trusted CA certificate You are here: Maintenance

File uploaded: CA certificate file uploaded. File contents - Certificates: 1, CRLS: 0.

| Type                                 | Issuer               | Subject        | Expiration date | Validity | View                           |
|--------------------------------------|----------------------|----------------|-----------------|----------|--------------------------------|
| <input type="checkbox"/> Certificate | [REDACTED]           | Matches Issuer | Mar 29 2025     | Valid    | <a href="#">View (decoded)</a> |
| <input type="checkbox"/> Certificate | [REDACTED]:2766-ca-1 | Matches Issuer | Feb 09 2025     | Valid    | <a href="#">View (decoded)</a> |

Show all (decoded) Show all (PEM file) Delete Select all Unselect all



Anmerkung: In Szenarien, in denen der Call Manager und das Tomcat-Zertifikat selbstsigniert sind, laden Sie das eigentliche Call Manager- und Tomcat-Zertifikat herunter und laden es auf Expressway hoch.



Navigieren Sie zu Expressway-C > Maintenance > Security > Trusted CA certificate > Show all (PEM-Datei).

**Trusted CA certificate**

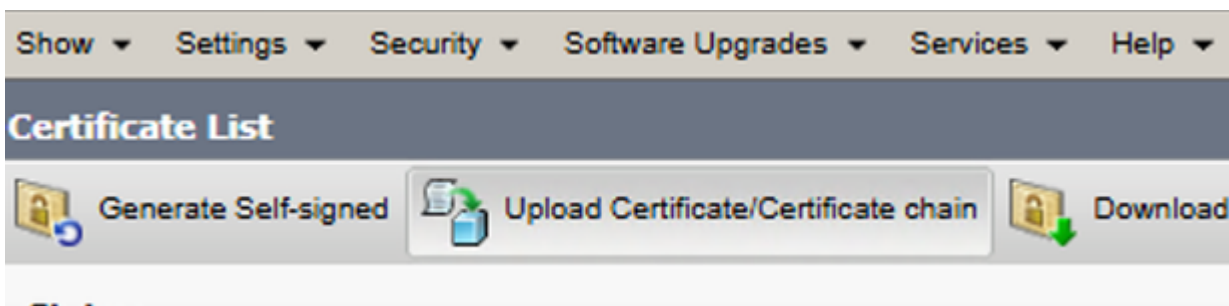
| Type                                 | Issuer                |
|--------------------------------------|-----------------------|
| <input type="checkbox"/> Certificate | [REDACTED]ADSERVER-CA |
| <input type="checkbox"/> Certificate | [REDACTED]:2766-ca-1  |

Show all (decoded) **Show all (PEM file)** Delete Select all Unselect all

Kopieren Sie den PEM-Wert des Zertifizierungsstellenzertifikats, das Expressway-C signiert, und speichern Sie ihn in einer Textdatei.

```
expcert.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIDdzCCA1+gAwIBAgIQFBGTWjxDrp1B5NgcCLc0FTANBgkqhkiG9w0BAQsFADBO
MRUwEwYKCZImiZPyLQBGRYFbG9jYWwxFzAVBgoJkiaJk/IsZAEZFgdicm9qZWRh
[REDACTED]
jsFtVBS1D0ReW61KU5gbIHS19QwbCxZHxd4a
-----END CERTIFICATE-----
```

Navigieren Sie zu OS administration > Security > Certificate management, und wählen Sie Upload Certificate/Certificate Chain aus, und laden Sie das Schnellstraße-C CA-Zertifikat als Tomcat-trust und Call Manager-trust hoch.



**Upload Certificate/Certificate chain**

Upload Close

**Status**

**i** Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

**Upload Certificate/Certificate chain**

Certificate Purpose\* CallManager-trust

Description(friendly name)

Upload File Choose File expcert.pem

Upload Close



Erforderliche Dienste im CUCM-Cluster neu starten:

- Navigieren Sie zu Cisco Unified Serviceability > Tools > Control Center - Feature Services, und starten Sie den Cisco CallManager-Service auf allen Knoten neu, auf denen er ausgeführt wird.
- Navigieren Sie zu Cisco Unified Serviceability > Tools > Control Center - Feature Services, und starten Sie den Cisco TFTP-Service auf allen Knoten neu, auf denen er ausgeführt wird.
- Starten Sie den Tomcat-Dienst in allen Knoten im Cluster über die CLI mit dem Befehl `utils service restart Cisco Tomcat` neu.
- Starten Sie den Cisco HAProxy-Dienst in allen Knoten im Cluster über die CLI mit dem Befehl `utils service restart Cisco HAProxy` neu.

## Szenario 4: Erneuerung der Zertifikatsursache der Zertifizierungsstellenproxy-Funktion

### Szenario 4.1: 802.1x-Authentifizierung fehlgeschlagen

Telefone führen nach dem Regenerieren des CAPF-Zertifikats (Certificate Authority Proxy



Authentifizierungsserver hoch, umgehen Sie 802.1x, um die Registrierung zu ermöglichen und das LSC-Zertifikat auf den betroffenen Telefonen zu installieren.

Szenario 4.2: Telefone, die sich nicht beim CUCM registrieren und im TLS-Modus ein Sicherheitsprofil verwenden.

Auf den Telefonen wird angezeigt, dass sich das Telefon registriert, nachdem das CAPF-Zertifikat auf dem CUCM-Publisher neu generiert wurde.

## Verifizierung

1. Die betroffenen Telefone enthalten ein Sicherheitsprofil mit aktiviertem TLS-Modus.

**Phone Security Profile Information**

**Product Type:** Cisco 8845  
**Device Protocol:** SIP

Name\*   
Description   
Nonce Validity Time\*   
Device Security Mode   
Transport Type\*  (highlighted with a red circle)  
 Enable Digest Authentication  
 TFTP Encrypted Config  
 Enable OAuth Authentication

2. Bei den betroffenen Telefonen ist das LSC-Zertifikat installiert.
3. Stellen Sie sicher, dass das CAPF-Zertifikat aktuell ist.

**Certificate List (1 - 15 of 15)**

Find Certificate List where  begins with

Select item or enter search text

| Certificate * | Common Name/Common Name_SerialNumber | Usage    | Type        | Key Type | Distribution        | Issued By     | Expiration |
|---------------|--------------------------------------|----------|-------------|----------|---------------------|---------------|------------|
| CAPF          | <a href="#">CAPF-0bc17206</a>        | Identity | Self-signed | RSA      | cm15-<br>.cisco.com | CAPF-0bc17206 | 10/01/2028 |

4. Melden Sie sich beim CUCM-Publisher an, und verwenden Sie den Befehl show ctl, der die alte Seriennummer des CAPF-Zertifikats anzeigt.
5. Ändern Sie dann das Telefon-Sicherheitsprofil in "Nicht sicher".

## Lösung

Regenerieren Sie die CTL-Datei auf dem CUCM, und starten Sie die erforderlichen Dienste neu, um sicherzustellen, dass die Telefone die neue CTL-Datei mit der CAPF-Datei erhalten.



Vorsicht: TAC empfiehlt, diesen Vorgang außerhalb der Geschäftszeiten durchzuführen,

da bei diesem Verfahren ein Neustart der Services erforderlich ist. Geschäftliche Auswirkungen sind



Verfahren zur erfolgreichen Verlängerung der CAPF



```
admin:utils ctl update CTLfile
This operation will update the CTLFile. Do you want to continue? (y/n): y

Updating CTL file
CTL file Updated
Please reset all Encrypted and Authenticated phones for the CTL file updates to take effect.
```

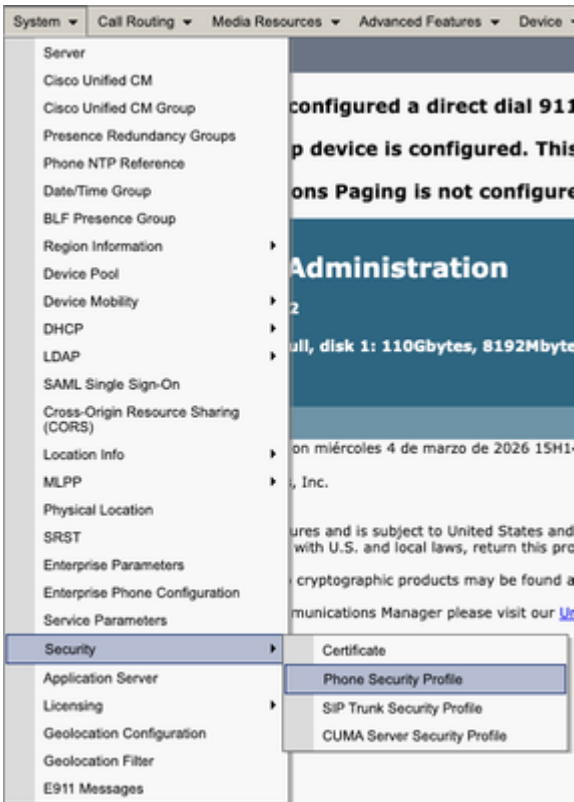
Aktualisieren Sie die CTL-Datei nach der CAPF-Regeneration. Melden Sie sich bei der CLI des Verlegers an, und geben Sie den Befehl `utils ctl update CTLFile` ein.



1. Navigieren Sie zu Cisco Unified Serviceability > Tools > Control Center - Feature Services im CUCM Publisher, und starten Sie den CAPF-Service neu.
2. Navigieren Sie zu Cisco Unified Serviceability > Tools > Control Center - Network Services, und starten Sie Cisco Trust Verification Service auf allen Knoten neu, auf denen er ausgeführt wird.
3. Navigieren Sie zu Cisco Unified Serviceability > Tools > Control Center - Feature Services, und starten Sie Cisco TFTP Service auf allen Knoten neu, auf denen es ausgeführt wird.



- Navigieren Sie zu CM Administration > System > Security > Phone Security Profile.



- Aktuelles Telefon-Sicherheitsprofil kopieren, das den erforderlichen Telefonen zugewiesen ist



- Ändern Sie Name und Gerätesicherheitsmodus in Nicht sicher, und wählen Sie Save and Apply Config (Speichern und Konfiguration anwenden), um diese Änderung auf alle erforderlichen Telefone anzuwenden.

**Phone Security Profile Configuration**

Save Delete Copy Reset Apply Config Add New

**Status**  
Update successful

**Phone Security Profile Information**

Product Type: Cisco 8845

**Device Protocol:** SIP

Name\*: Cisco 8845 - non Secure profile

Description: Cisco 8845 - Secure profile

Nonce Validity Time\*: 600

Device Security Mode: Non Secure

Transport Type\*: TCP

Enable Digest Authentication  
 TFTP Encrypted Config  
 Enable OAuth Authentication

**Phone Security Profile CAPF Information**

Authentication Mode\*: By Null String

Key Order\*: RSA Only

RSA Key Size (Bits)\*: 2048

EC Key Size (Bits): < None >

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

**Parameters used in Phone**

SIP Phone Port\*: 5060

Save Delete Copy Reset Apply Config Add New

- Wenden Sie das erstellte Gerätesicherheitsprofil auf die erforderliche Telefonkonfiguration an, und wählen Sie Save and Apply Config (Speichern und Konfiguration anwenden).

**Protocol Specific Information**

Packet Capture Mode\*: None

Packet Capture Duration: 0

BLF Presence Group\*: Standard Presence group

SIP Dial Rules: < None >

MTP Preferred Originating Codec\*: 711ulaw

Device Security Profile\*: Cisco 8845 - non Secure profile

Rerouting Calling Search Space: < None >

SUBSCRIBE Calling Search Space: < None >

SIP Profile\*: Standard SIP Profile [View Details](#)

Digest User: < None >

Media Termination Point Required  
 Unattended Port  
 Require DTMF Reception



Verwenden Sie den CAPF-Informationsabschnitt in der Gerätekonfiguration der betroffenen Telefone, um das LSC-Zertifikat auf den erforderlichen Telefonen zu installieren.

- Wählen Sie unter CAPF information die Option Install/Upgrade in Certificate Operation (Installation/Upgrade im Zertifikatsbetrieb) aus.

**Certification Authority Proxy Function (CAPF) Information**

Certificate Operation\*

Authentication Mode\*

Authentication String

Key Order\*

RSA Key Size (Bits)\*

EC Key Size (Bits)

Operation Completes By     (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Additional CAPF Settings.

- Wählen Sie Speichern und Konfig. anwenden aus.
- Warten Sie, bis der Status des Zertifikatsvorgangs anzeigt, dass der Vorgang abgeschlossen ist.



Wählen Sie im Abschnitt "Protocol Specific Information" (protokollspezifische Informationen) in der Telefonkonfiguration das erstellte Sicherheitsprofil mit aktivierter TLS aus.

**Protocol Specific Information**

Packet Capture Mode\*

Packet Capture Duration

BLF Presence Group\*

SIP Dial Rules

MTP Preferred Originating Codec\*

Device Security Profile\*

Rerouting Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile\*  [View Details](#)

Digest User

**Phone Security Profile Configuration**

Save Delete Copy Reset Apply Config Add New

**Status**

Status: Ready

**Phone Security Profile Information**

**Product Type:** Cisco 8845  
**Device Protocol:** SIP

Name\* Cisco 8845 - Secure profile  
Description Cisco 8845 - Secure profile  
Nonce Validity Time\* 600  
Device Security Mode Encrypted  
Transport Type\* TLS

Enable Digest Authentication  
 TFTP Encrypted Config  
 Enable OAuth Authentication

## Zugehörige Informationen

- <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/214231-certificate-regeneration-process-for-cis.html>
- <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/217138-regeneration-of-cucm-ca-signed-certifica.html>
- <https://www.cisco.com/c/en/us/support/docs/content-networking/certificates/213295-how-to-install-an-lsc-on-a-cisco-ip-phon.html>
- [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X15-2/mra/exwy\\_b\\_mra-deployment-guide-x152.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-2/mra/exwy_b_mra-deployment-guide-x152.html)

## 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.