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	

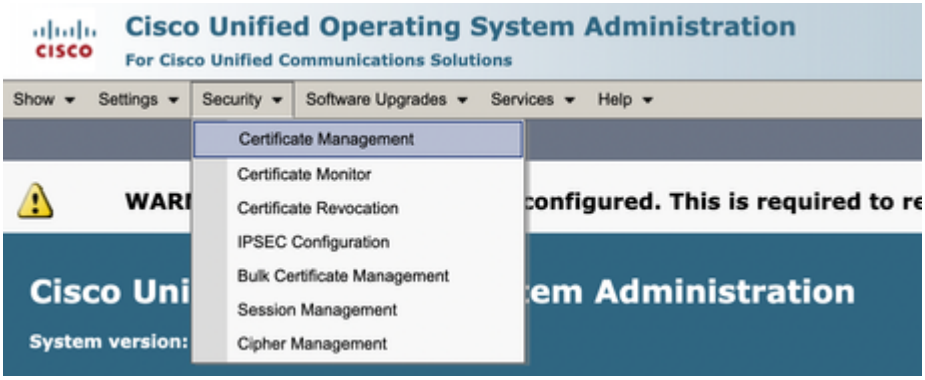
Szenario 1: Telefone werden nach der Erneuerung des Call Manager-, TVS- und ITL-Zertifikats nicht registriert

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

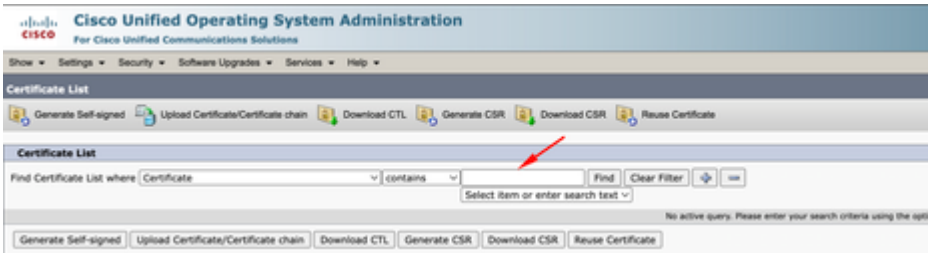
Wenn Call Manager-, TVS- und ITL-Zertifikate abgelaufen sind und gleichzeitig erneuert wurden, führt dies dazu, dass alle unsere Telefone nicht registriert sind, was erhebliche Auswirkungen auf das System hat. Dies ist ein erwartetes Verhalten, da wir die Telefone dazu veranlassen, dem CUCM nicht zu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

Verifizierung

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

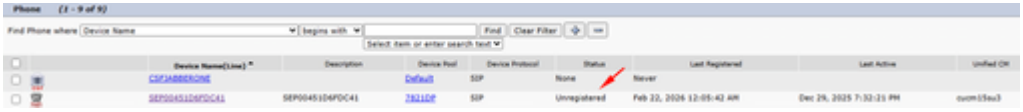


2. Suchen Sie nach Callmanager, TVS oder ITL unter dem Filter oben auf der Seite und verwenden Sie die enthält oder beginnt mit Optionen:



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

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



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.

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.authenticatio
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.

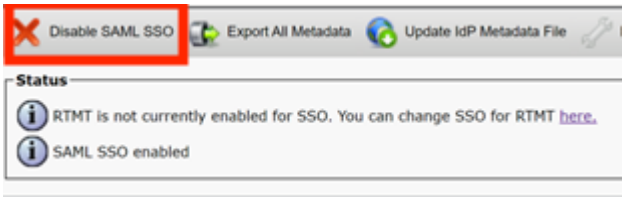
Verfahren zur Verlängerung von Tomcat bei aktivierter SSO-Bereitstellung:

⚠ 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.

1. SSO in allen CUCM-Knoten deaktivieren

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

- SAML SSO deaktivieren auswählen

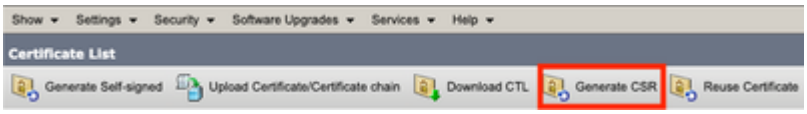


- Dieser Prozess muss in allen anderen Knoten über die GUI ausgeführt werden, wenn eine knotenspezifische Vereinbarung verwendet wird.

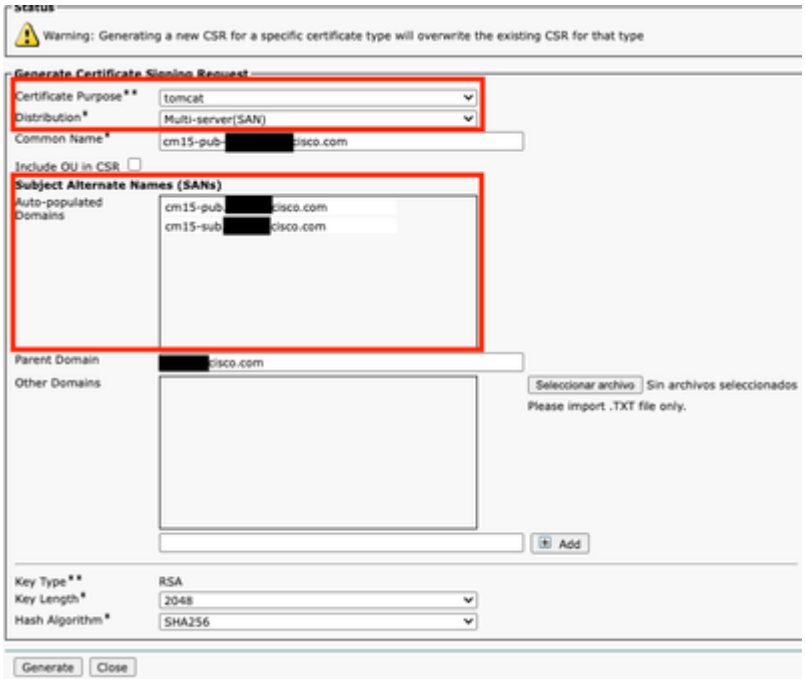
2. Tomcat-Zertifikat im CUCM-Cluster erneuern

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.

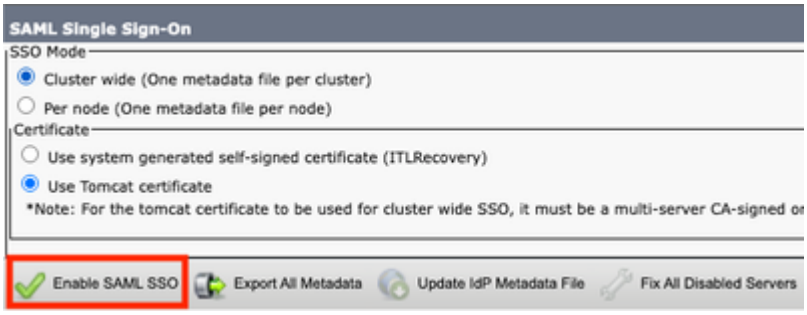
3. Exportieren von Service Provider-Metadaten (SP)

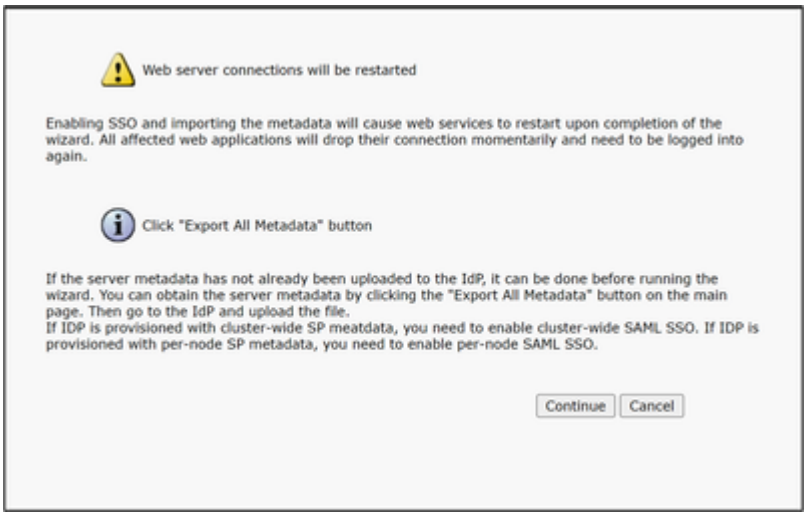
- Gehen Sie zu CM Administration > System > Single Sign-On
- Konfigurieren Sie SSO-Optionen (in diesem Fall ist der SSO-Modus clusterweit und die Verwendung des Tomcat-Zertifikats auf dem Zertifikat als Beispiel konfiguriert), und wählen Sie dann Alle Metadaten exportieren aus.

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

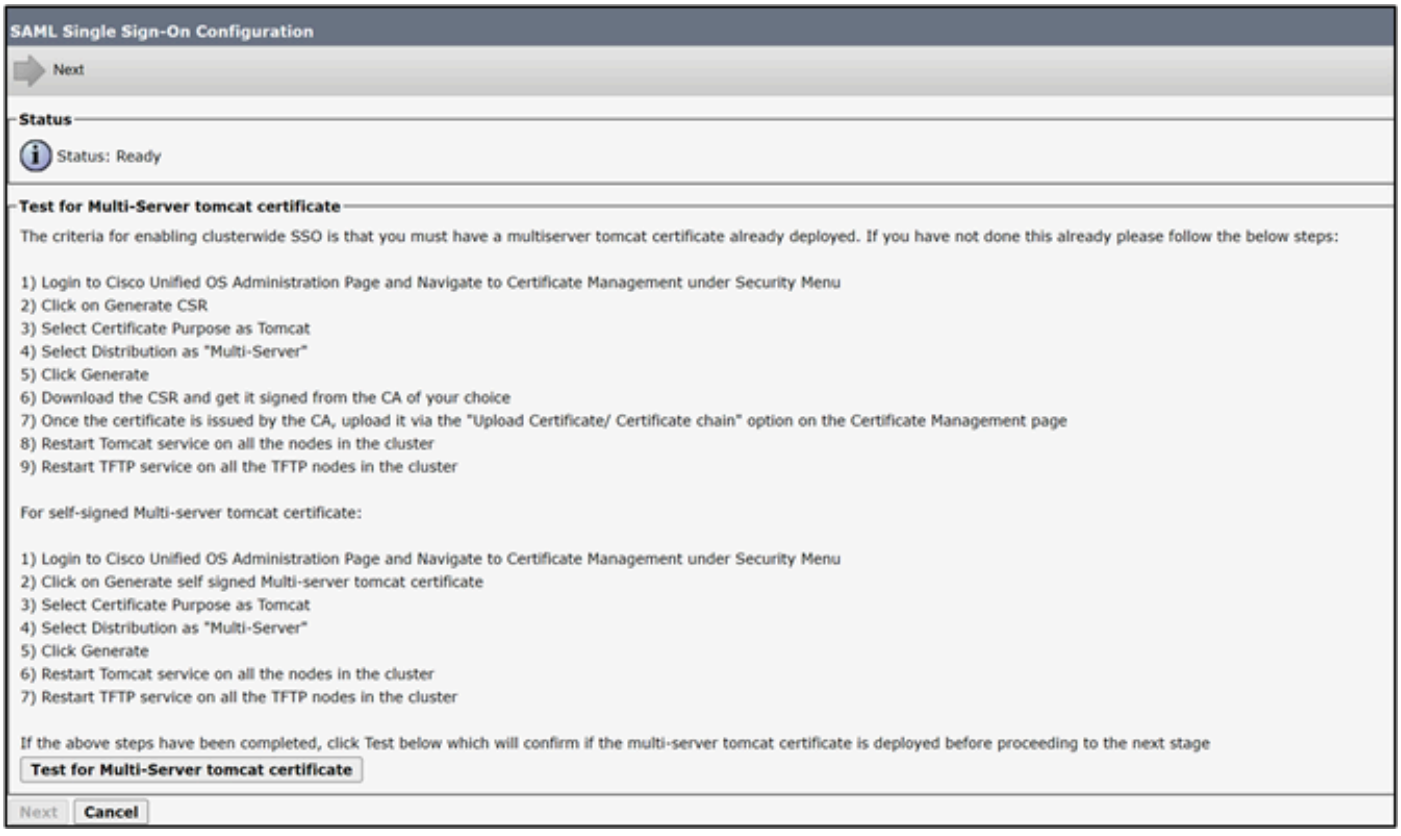
4. SSO im CUCM-Cluster aktivieren

- 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.

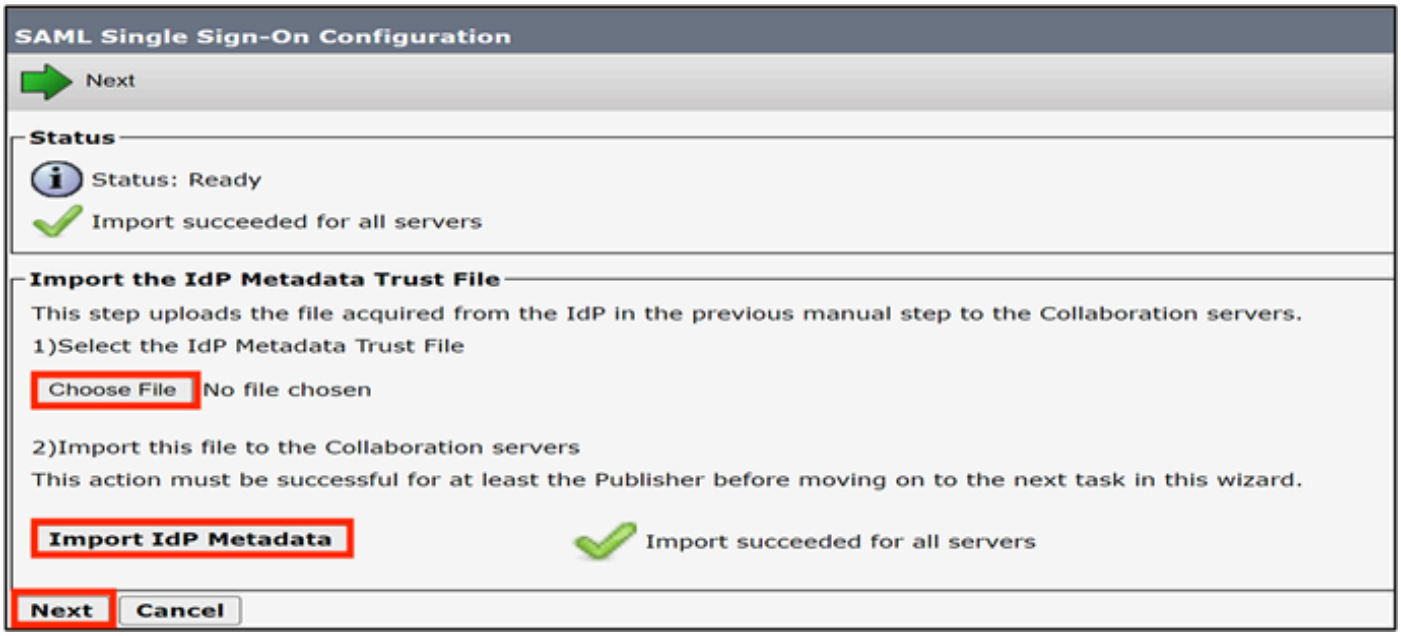




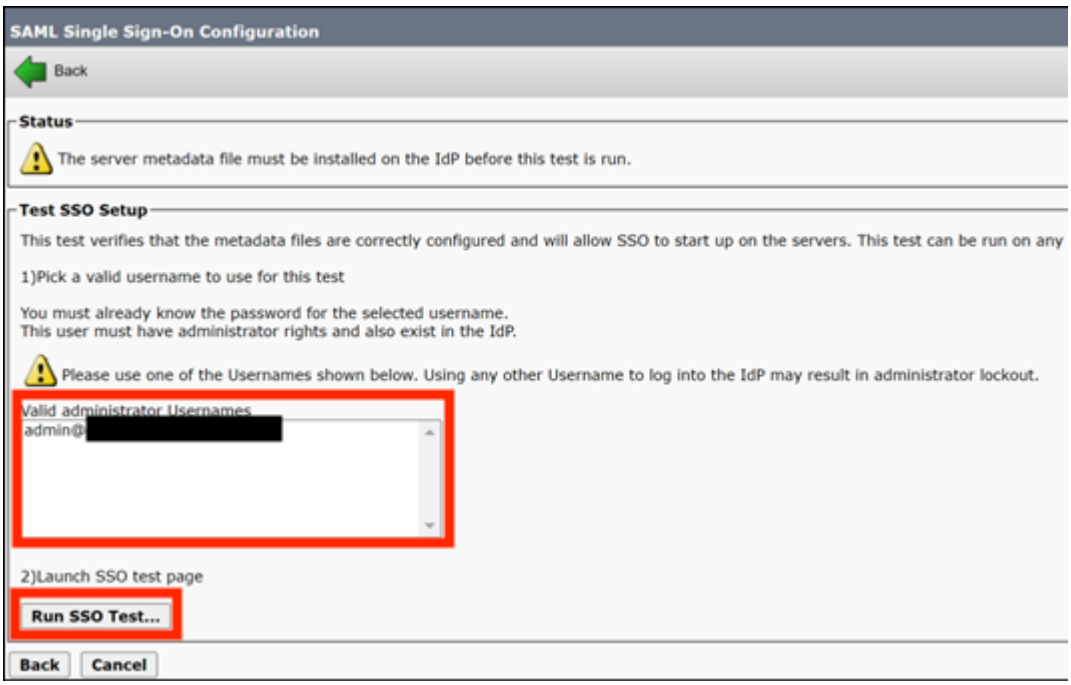
- Wenn Sie den gesamten Cluster verwenden, können Sie in diesem Schritt das Multi-SAN-Zertifikat auf allen Knoten überprüfen. Wählen Sie Test for multi-server tomcat certificate (Test für Multi-Server-Tomcat-Zertifikat). Wählen Sie nach Abschluss Weiter aus.

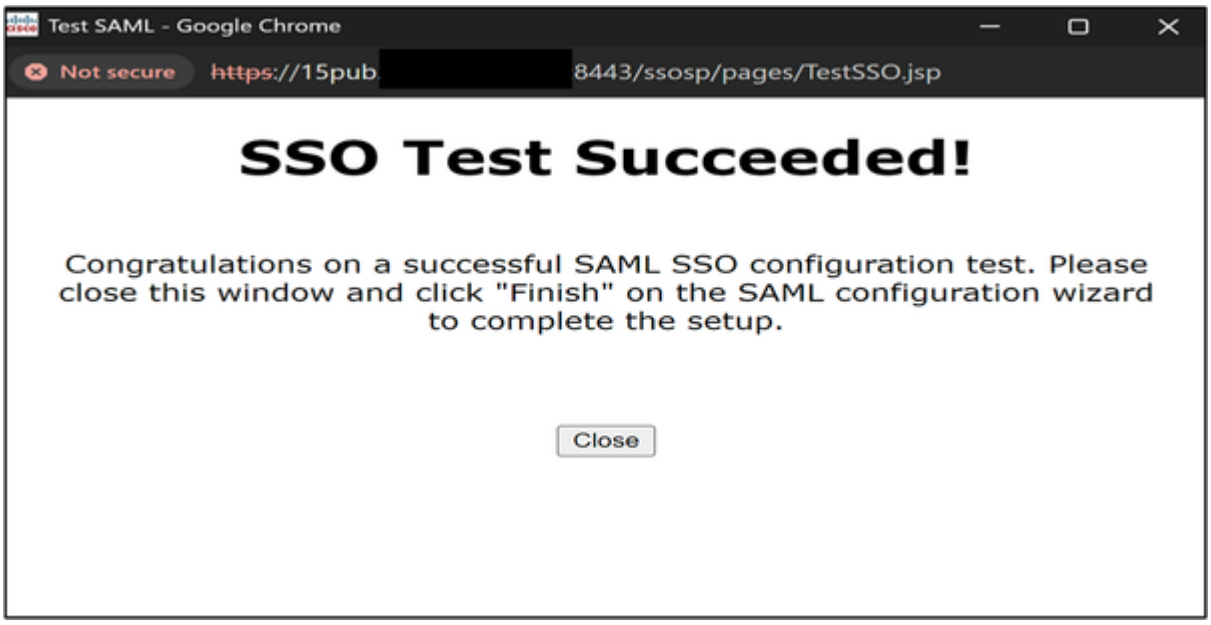


- IdP-Metadaten hochladen, IdP-Metadaten importieren auswählen und nach Abschluss die Option Weiter auswählen



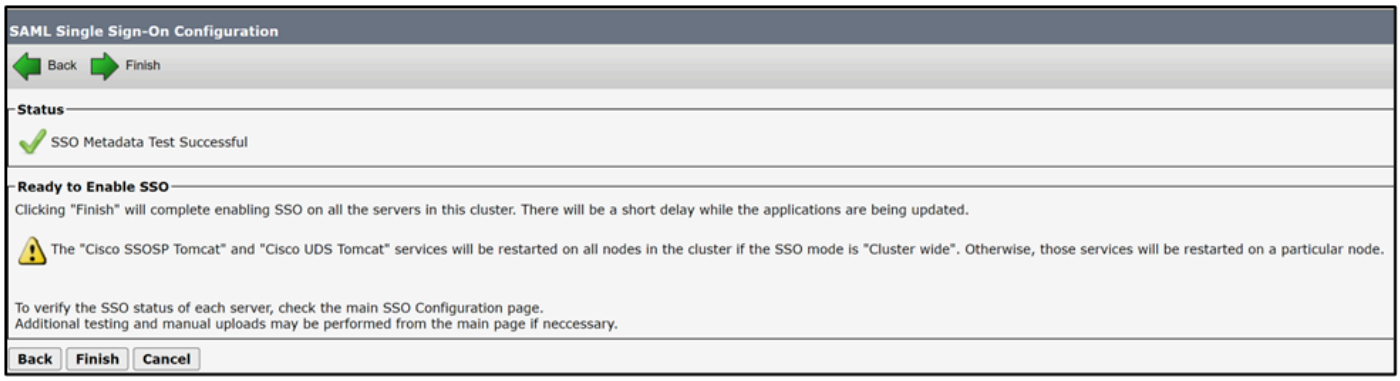
- Wählen Sie beim Test-SSO-Setup einen Benutzer aus, dem die Standard-CCM-Gruppe "Super Users" zugewiesen ist, und wählen Sie Run SSO Test (SSO-Test ausführen), bis Sie erfolgreich sind.





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" Module
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

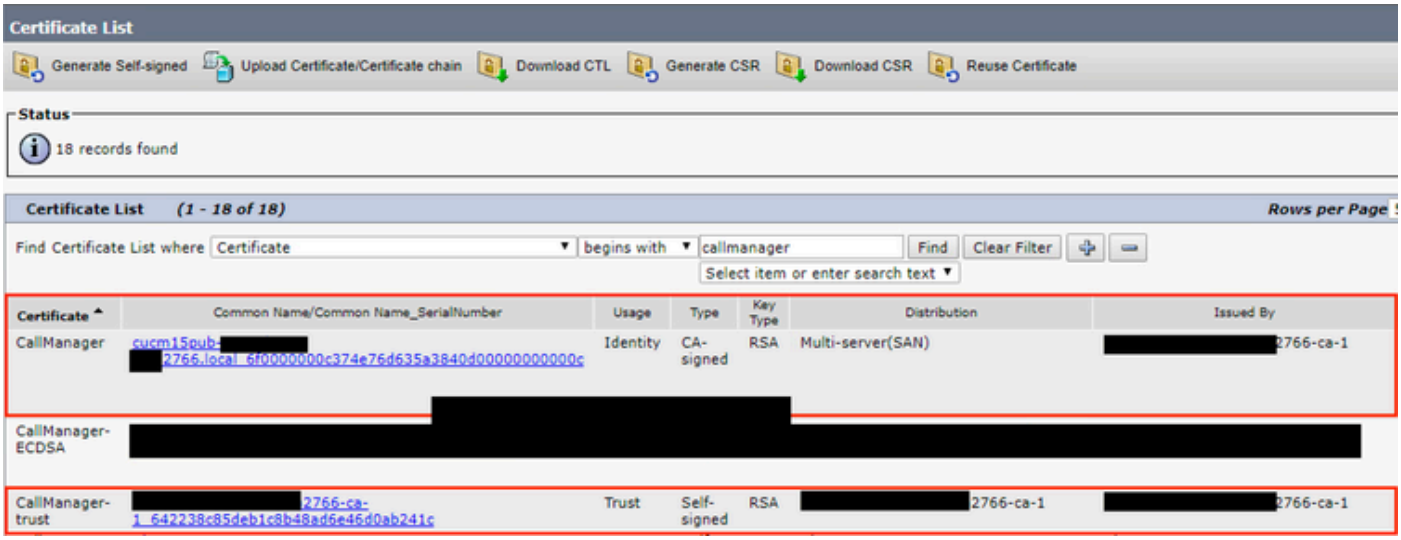
Exportieren und importieren Sie Zertifikate zwischen CUCM und Expressway-C, um die Vertrauensstellung sicherzustellen.

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

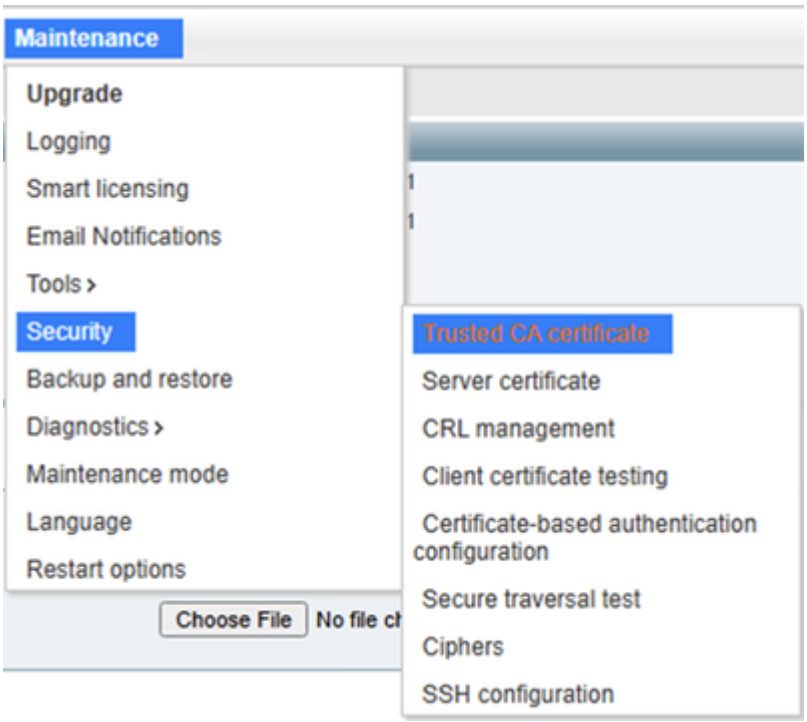
---

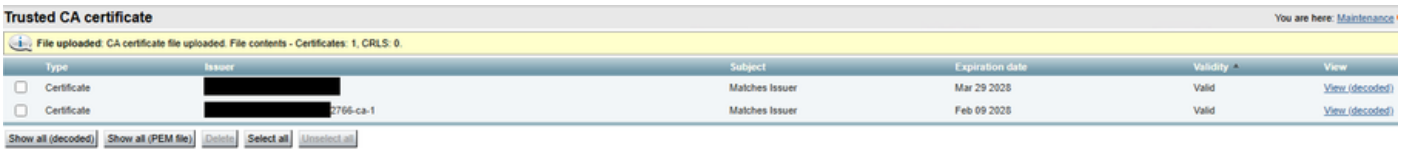
1. Verfahren zum Abschließen der Vertrauensstellung zwischen CUCM und Expressway mit von CA signierten Zertifikaten

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.



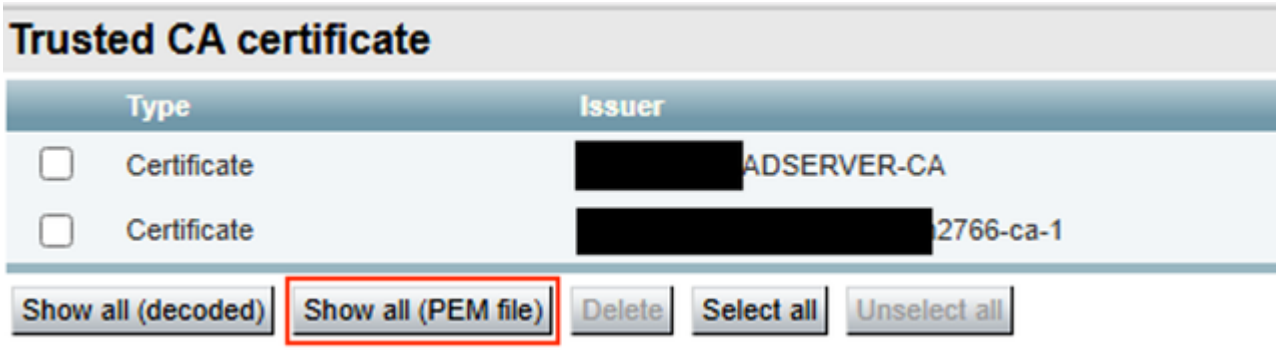
Navigieren Sie anschließend zu Expressway-C > Maintenance > Security > Trusted CA certificate, und laden Sie das CA-Zertifikat des Call Manager- und Tomcat-Zertifikats hoch.



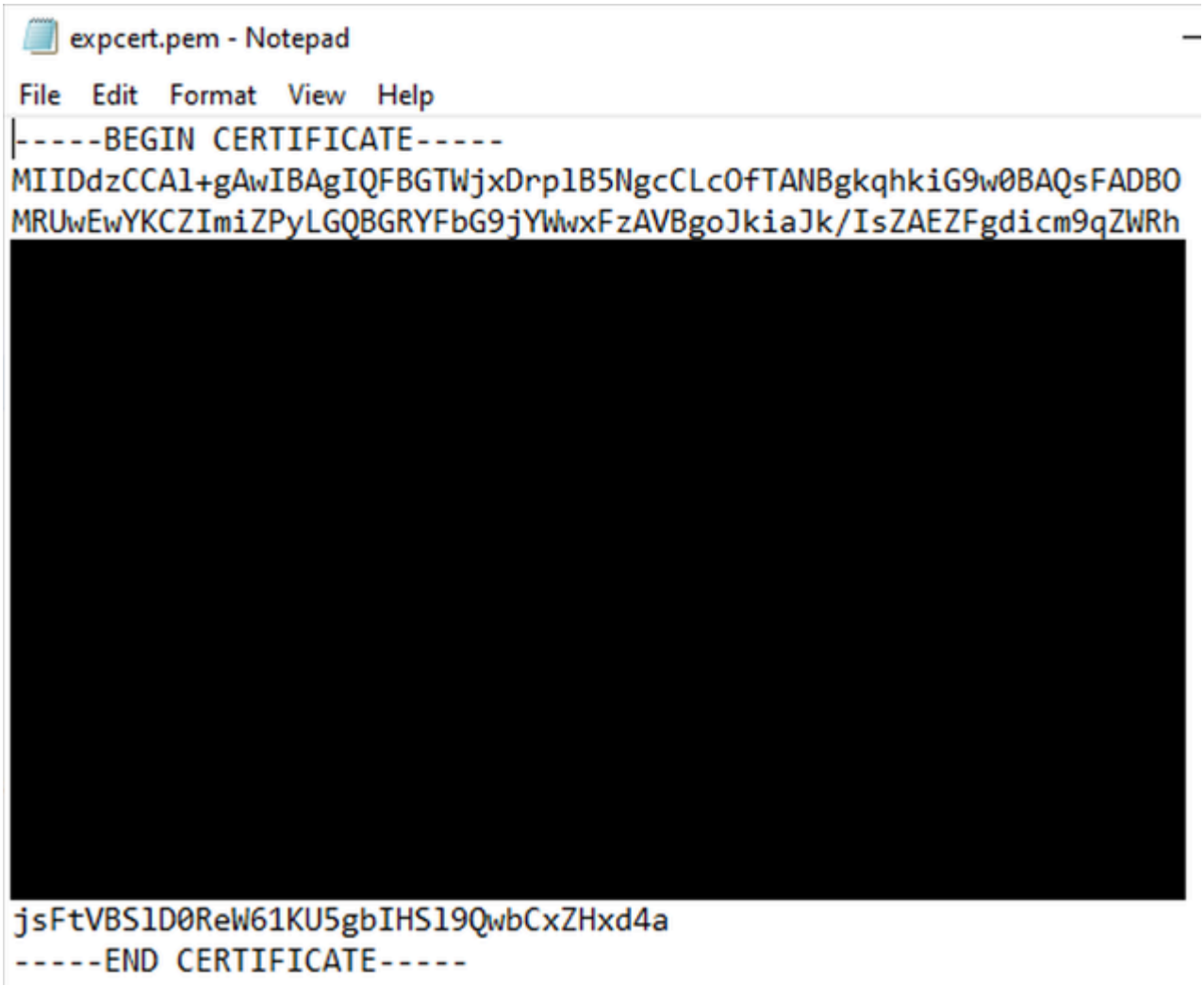


Anmerkung: In Szenarien, in denen der Call Manager und das Tomcat-Zertifikat selbstsigniert sind, laden Sie das eigentliche Call Manager- und Tomcat-Zertifikat herunter und laden es auf Expressway hoch.

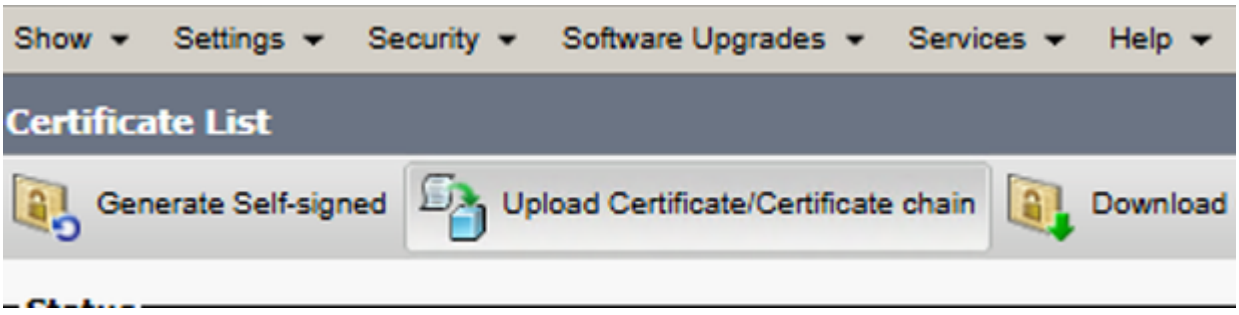
Navigieren Sie zu Expressway-C > Maintenance > Security > Trusted CA certificate > Show all (PEM-Datei).

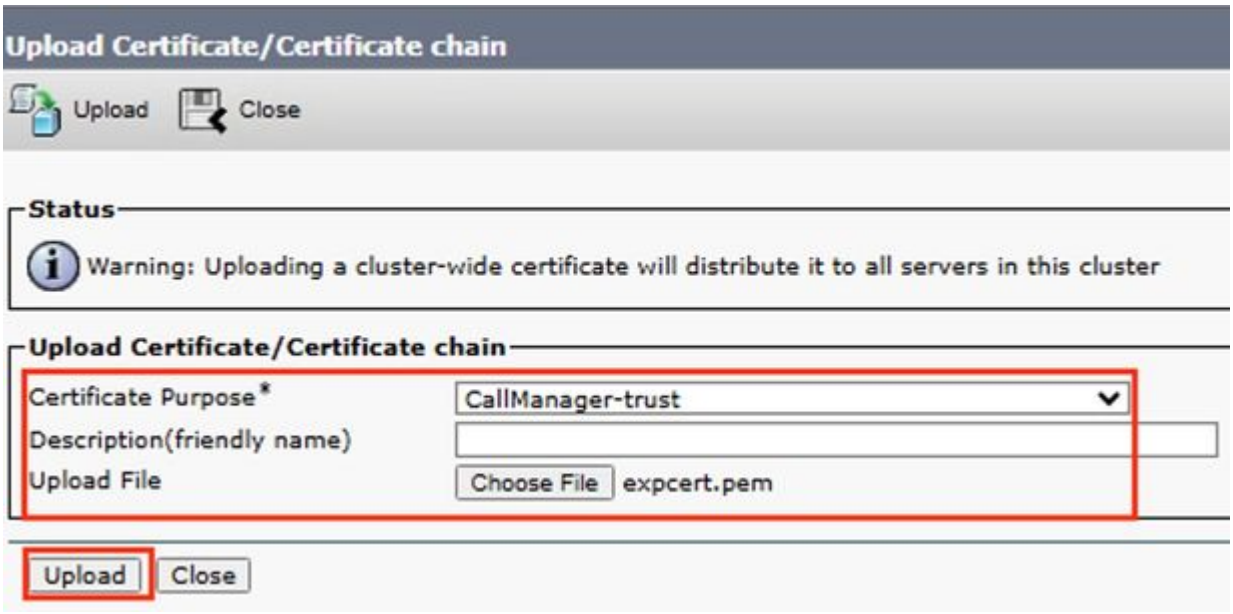


Kopieren Sie den PEM-Wert des Zertifizierungsstellenzertifikats, das Expressway-C signiert, und speichern Sie ihn in einer Textdatei.



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.





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

Function) auf dem CUCM-Publisher keine Authentifizierung mit ASA durch.

Verifizierung

1. Telefonstatusmeldungen zeigen "802.1x Authentication: Fehlgeschlagen

2. Überprüfen Sie die Telefonprotokolle des betroffenen Servers, und suchen Sie nach "SSL_ERROR_WANT_READ".

```
4592 NOT Feb 17 11:01:25.041733 (349-349) PAE: -Secure Connection Handshake in progress - status SSL_ER
4593 NOT Feb 17 11:01:25.041826 (349-349) PAE: -EV_REQUEST_REC, ST_AUTHENTICATING->ST_AUTHENTICATING
++ EAP-Failure
4594 NOT Feb 17 11:01:25.041898 (349-349) PAE: -send EAP-Resp/TLS - id 9
4595 NOT Feb 17 11:01:25.042032 (349-349) PAE: -authWhile timer set: 30 sec
4596 NOT Feb 17 11:01:27.061822 (349-349) PAE: -[0001-0] 08-cc-a7-1c-bb-ae vid=0xfff=4095 static=0 pri=
4597 NOT Feb 17 11:01:27.061950 (349-349) PAE: -port=0
4598 NOT Feb 17 11:01:27.062009 (349-349) PAE: -cprCdpGetPort address:  8:CC:A7:1C:BB:AE  Phyport=0 app
4599 NOT Feb 17 11:01:27.062068 (349-349) PAE: - >>>>>>>>>>>>> port obtained = 0 for mac macAddress 08:
4600 NOT Feb 17 11:01:27.062134 (349-349) PAE: -rcvd EAP-Failure
4601 NOT Feb 17 11:01:27.062189 (349-349) PAE: -EV_FAILURE, ST_AUTHENTICATING->ST_HELD
4602 WRN Feb 17 11:01:27.062462 (349-349) PAE: -802.1X auth FAILED
4603 NOT Feb 17 11:01:27.062550 (349-349) PAE: -paeInfoToInetd: PAE info sent to NETSD
4604 NOT Feb 17 11:01:27.062717 (1786-1880) JAVA-Calling handleNetSDEvent
4605 WRN Feb 17 11:01:27.062953 (1786-1880) JAVA-Thread-11|cip.sec.Security:? - Security: Received a pr
4606 DEB Feb 17 11:01:27.063039 (1786-1880) JAVA-openQue(): que->/tmp/pae_msg_que, key->0x101019ab
4607 DEB Feb 17 11:01:27.063069 (1786-1880) JAVA-openQue(): que->/tmp/pae_rsp_que, key->0x10101c4c
4608 DEB Feb 17 11:01:27.063091 (1786-1880) JAVA-getpaeinfo: send pae info message paeCmd.mtype=1880, p
4609 DEB Feb 17 11:01:27.063121 (1786-1880) JAVA-getpaeinfo: recv pae info resp ret=-1, errno=No messag
4610 NOT Feb 17 11:01:27.063306 (349-349) PAE: -paeInfoToInetd: Netsd event NETSD_EV_PAE sent to NETSD
4611 NOT Feb 17 11:01:27.063370 (349-349) PAE: - PAE RE-AUTH, not sending SEC_DOWN Netsd event for CDP
4612 NOT Feb 17 11:01:27.063423 (349-349) PAE: -paeSetLastSupStatus: LastSupStatus 0
4613 NOT Feb 17 11:01:27.063475 (349-349) PAE: -heldWhile timer set: 60 sec
4614 NOT Feb 17 11:01:27.064074 (349-349) PAE: -paeNetsdRcvMsg(349): PAE event: status: FAIL : Resource
```

Lösung

Laden Sie das CAPF-Zertifikat vom CUCM-Publisher herunter, laden Sie es auf den

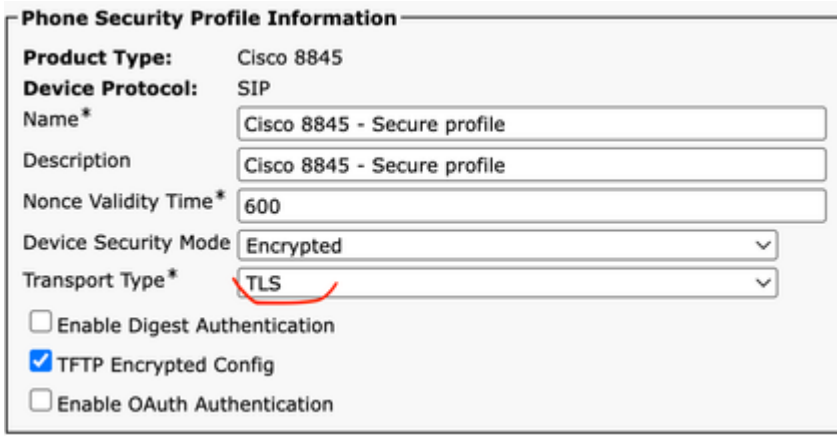
Authentifizierungsserver hoch, umgehen Sie 802.1x, um die Registrierung zu ermöglichen und das LSC-Zertifikat auf den betroffenen Telefonen zu installieren.

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.



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

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

Medium Impact.

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.
```

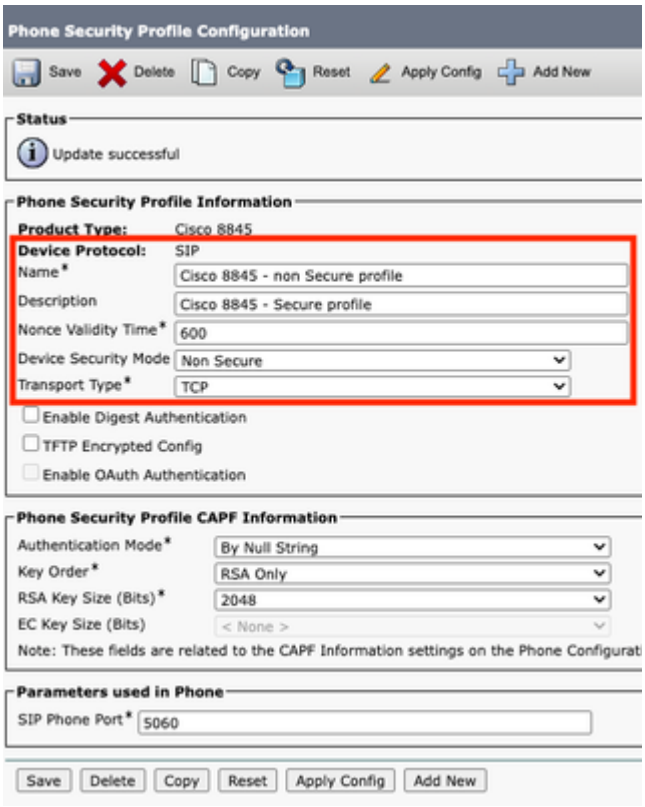
Aktualisieren Sie die CTL-Datei nach der CAPF-Regeneration. Melden Sie sich bei der CLI des Verlegers an, und geben Sie den Befehl utils ctl update CTLFile ein.

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.

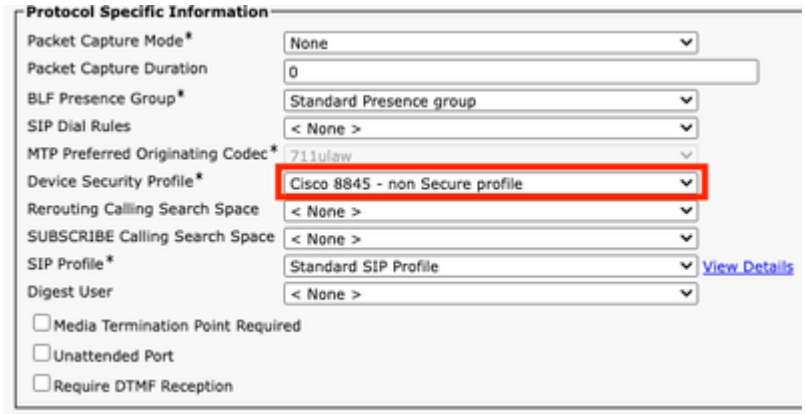
- Navigieren Sie zu CM Administration > System > Security > Phone Security Profile.

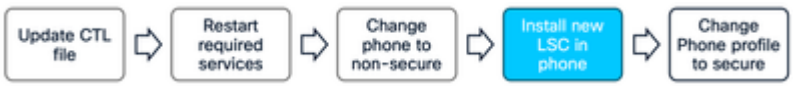
- Aktuelles Telefon-Sicherheitsprofil kopieren, das den erforderlichen Telefonen zugewiesen ist

- 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.



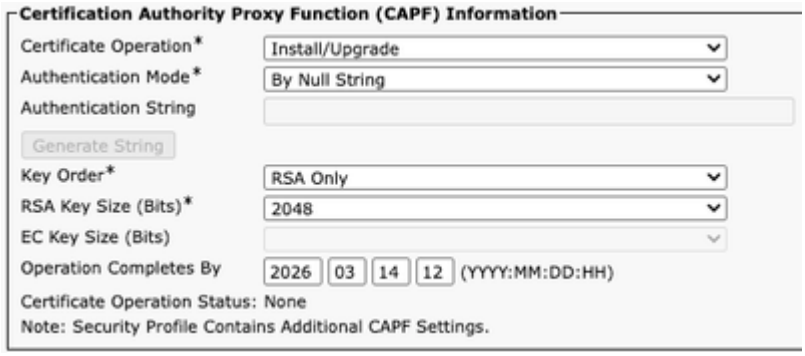
- Wenden Sie das erstellte Gerätesicherheitsprofil auf die erforderliche Telefonkonfiguration an, und wählen Sie Save and Apply Config (Speichern und Konfiguration anwenden).





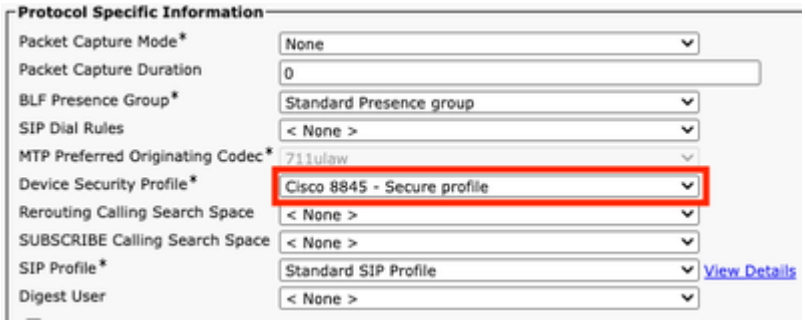
Verwenden Sie den CAPF-Informationsabschnitt in der Gerätekonfiguration der betroffenen Telefone, um das LSC-Zertifikat auf den erforderlichen Telefonen zu installieren.

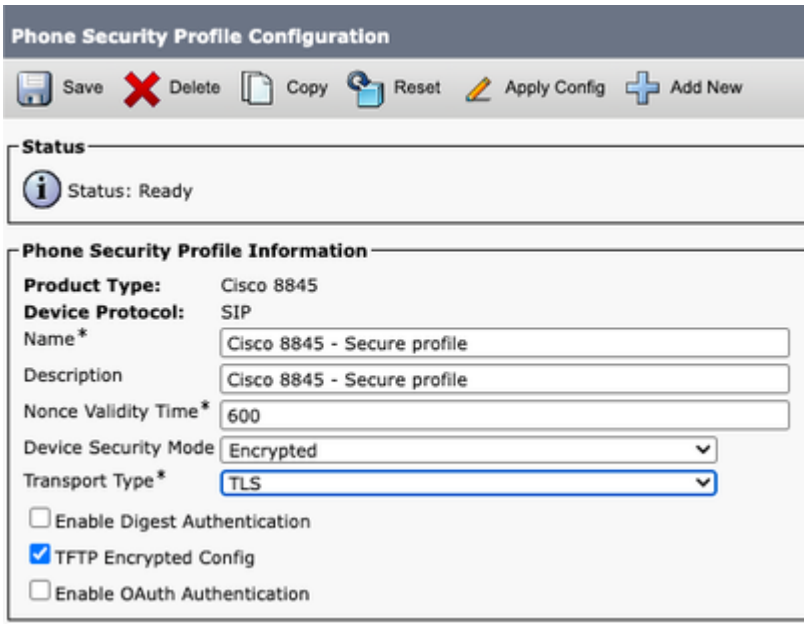
- Wählen Sie unter CAPF information die Option Install/Upgrade in Certificate Operation (Installation/Upgrade im Zertifikatsbetrieb) aus.



- Wählen Sie Speichern und Konfig. anwenden aus.
- Warten Sie, bis der Status des Zertifikatvorgangs 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.





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

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.