Problemen oplossen met veelvoorkomende problemen met certificaatvernieuwing in CUCM

Inleiding

In dit document worden veelvoorkomende problemen beschreven nadat u certificaten hebt geregenereerd in Cisco Unified Communications Manager (CUCM) en wordt beschreven hoe u deze kunt oplossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CUCM-certificaatvernieuwingsproces
- CUCM GUI-interface
- Expressway-servers
- Apparaatregistratie met CUCM-proces
- proxy-functie van de certificaatautoriteit
- Beveiligingsgids voor Cisco Unified Communications Manager

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CUCM versie 15

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

gevolgen voor het bedrijfsleven

Deze tabel geeft de zakelijke impact van elke certificaatvernieuwing in uw bedrijf weer. Bekijk de informatie zorgvuldig. Vereiste certificaten verlengen na uren of in rustige periodes, op basis van het risiconiveau van elk certificaat.

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	

Scenario 1: Telefoons niet registreren na Call Manager, TVS en ITL Certificaat Vernieuwing

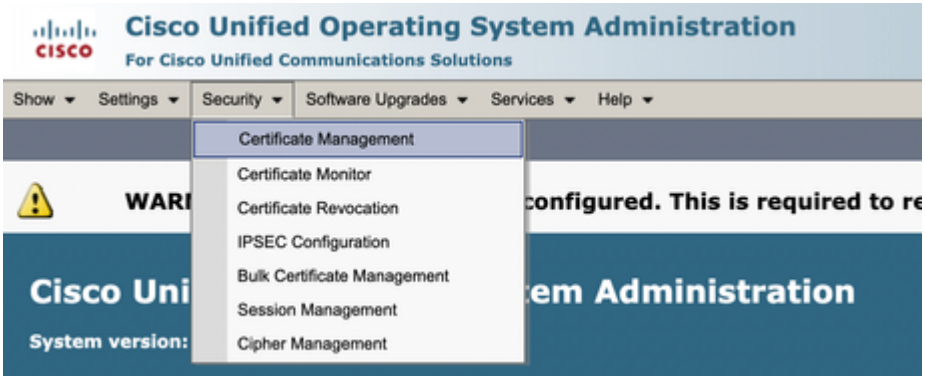
---

Opmerking: dit scenario is van toepassing op implementaties in het kader van CUCM-clusters met gemengde modus en niet-beveiligde clusters en is bovendien van toepassing op de zelf ondertekende certificaten en CA-certificaten.

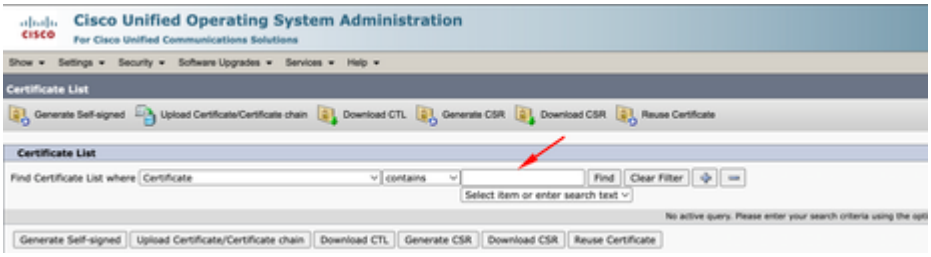
Wanneer Call Manager, TVS en ITL certificaten verlopen en ze werden verlengd op hetzelfde moment, Het zorgt ervoor dat al onze telefoons in een niet-geregistreerde staat die een grote impact op het systeem veroorzaakt, dit is een verwacht gedrag als we leiden de telefoons niet vertrouwen in de CUCM.

Verificatie

1. Controleer of de certificaten al zijn verlopen onder Cisco Unified OS Administration > Security > Certificate Management

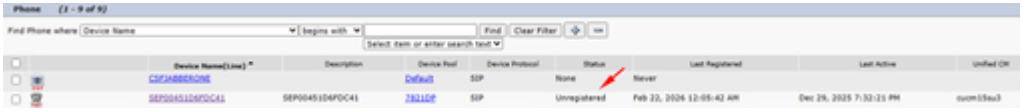


2. Zoek op Callmanager, TVS of ITL onder het filter bovenaan de pagina en gebruik de optie bevat of begint met opties:



3. De certificaten moeten worden bijgewerkt en gecontroleerd in de kolom Vervaldatum (hetzelfde voor TVS- en ITL-certificaten)

4. Zodra alles goed is geverifieerd na de verlenging van het certificaat, worden de telefoons weergegeven als niet-geregistreerde staat.



Oplossing

Er zijn 2 opties om het probleem op te lossen:

1. Voer een fabrieksreset van de telefoon uit waarmee de telefoon de huidige beveiligingsinstellingen kan wissen en de telefoon de nieuwe certificaten kan pakken
2. Werk de ITL- en CTL-certificaten van CLI bij op de node van de uitgever en gebruik de opdracht Hiermee wordt ITL LocalKey gereset.

Deze stap is van invloed op alle telefoons, inclusief geregistreerde telefoons, zorg ervoor dat u dit na uren uitvoert.

Scenario 2: Eenmalige aanmelding werkt niet na vernieuwing Tomcat-certificaat

Opmerking: dit scenario kan van toepassing zijn op implementaties waarbij gebruik wordt gemaakt van clusterbrede of per-node-overeenkomst voor configuratie met eenmalige aanmelding

Login binnen CUCM met Single Sign-on (SSO) het geeft een foutmelding ¨Fout tijdens het verwerken van kleine respons¨ of ¨Fout tijdens het verwerken van kleine respons De geheime sleutel is niet ontsleuteld¨

Verificatie

1. Zorg ervoor dat alle knooppunten een geldig tomcat-certificaat bevatten als ze zelf zijn ondertekend of het nieuwe multi-san tomcat-certificaat bevatten dat is gekoppeld.
2. Gebruik debug op sampltrace-niveau in alle CUCM-nodes via CLI om SSO-logs op debug-niveau te activeren
3. Maak het probleem opnieuw door opnieuw in te loggen bij CUCM en gebruik de SSO-methode.
4. Verzamel de logboeken van Tomcat SSO na het incident en controleer of u dit bericht ontvangt:
   -

```
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
...
```

Oplossing

Export van CUCM-metagegevens na vernieuwing van het Tomcat-certificaat en import naar de Identity Provider Server om ervoor te zorgen dat ze het nieuwe tomcat-certificaat voor deze communicatie hebben.

Procedure voor het vernieuwen van tomcat met SSO-implementatie ingeschakeld:

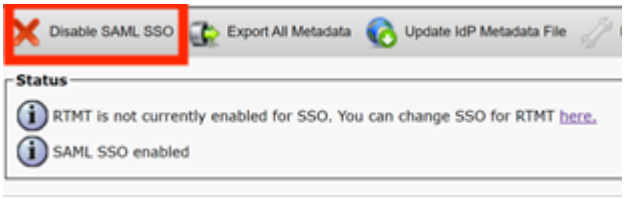
⚠ Waarschuwing: het Technical Assistance Centre (TAC) beveelt de volgende stappen aan om problemen na de verlenging van het Tomcat-certificaat te voorkomen en deze procedure na uren uit te voeren.

Low Impact

1. SSO uitschakelen in alle CUCM-knooppunten

- Toegang tot CM-beheer > Systeem > SAML Eenmalige aanmelding

- Selecteer SAML SSO uitschakelen

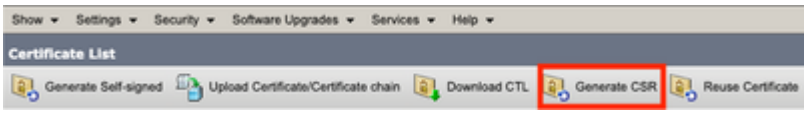


- Dit proces moet worden uitgevoerd in alle andere knooppunten via GUI als per-node overeenkomst wordt gebruikt.

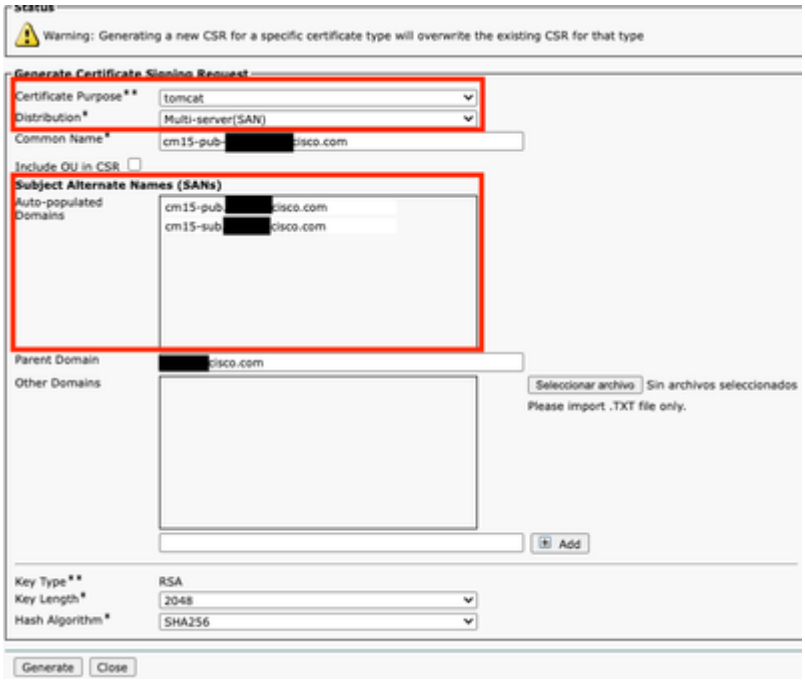
2. Tomcat-certificaat vernieuwen in CUCM-cluster

Algemene procedure voor het vernieuwen van het Tomcat multi-san certificaat in het CUCM-cluster:

- Navigeer naar Beheer van besturingssysteem > Beveiliging > Certificaatbeheer.
- Selecteer CSR genereren



- Selecteer Tomcat in Certificate Porpuse.
- Selecteer Multi-SAN in Distributie.
- Zorg ervoor dat alle knooppunten in het cluster worden vermeld onder Automatisch gevulde domeinen.



- Selecteer Genereren. Zorg ervoor dat CSR wordt gemaakt in alle knooppunten in het cluster.
- Download de gegenereerde CSR van CUCM-uitgever en onderteken deze met een CA-server (Certificate Authority).
- Ga naar Beheer besturingssysteem > Beveiliging > Certificaatbeheer. Selecteer Certificaat/certificaatketen uploaden.
- CA-certificaten uploaden als Tomcat-trust.
- Herhaal stap 6 en upload nu het door Tomcat ondertekende certificaat als Tomcat.
- Nadat alle nodes het nieuwe tomcat-certificaat hebben toegepast en zijn geverifieerd, start u de Tomcat-service opnieuw op via CLI in alle nodes in het cluster met deze opdracht om de service Cisco Tomcat opnieuw op te starten.

Voor meer informatie verwijzen wij u naar deze documentatie:

- Zelfondertekend certificaat van Tomcat regenereren
- Tomcat CA-ondertekend certificaat regenereren.

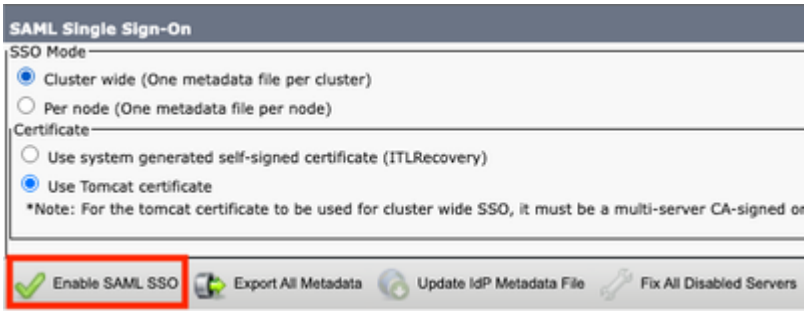
3. Metagegevens van de Export Service Provider (SP)

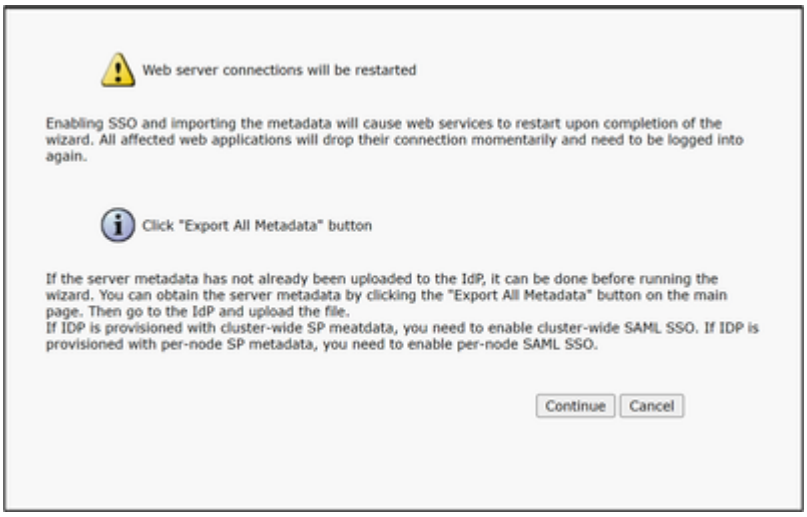
- Ga naar Beheer CM > Systeem > Eenmalige aanmelding
- Configureer SSO-opties (In dit geval is cluster wide in de SSO-modus en Use tomcat certificate on certificate als voorbeeld geconfigureerd) en selecteer export van alle metagegevens

- SP-metagegevens importeren naar de Identity Provider (IdP)-server. Raadpleeg SAML SSO configureren op Identity Provider voor meer informatie

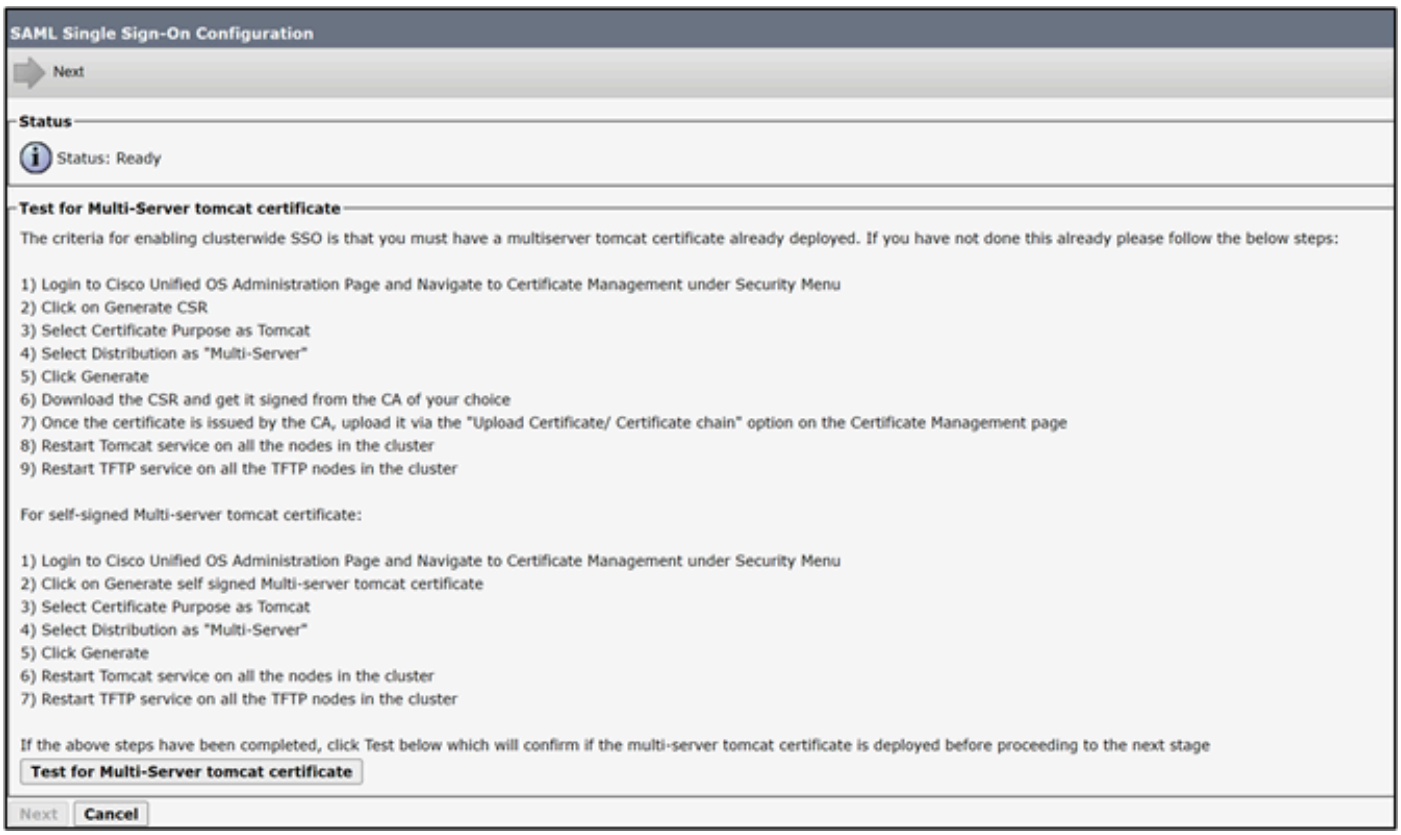
4. SSO inschakelen in CUCM-cluster

- Ga naar Beheer CM > Systeem > Eenmalige aanmelding
- Als dezelfde SSO-opties zijn geselecteerd terwijl u CUCM-metagegevens exporteert, selecteert u SAML SSO inschakelen en selecteert u Doorgaan.

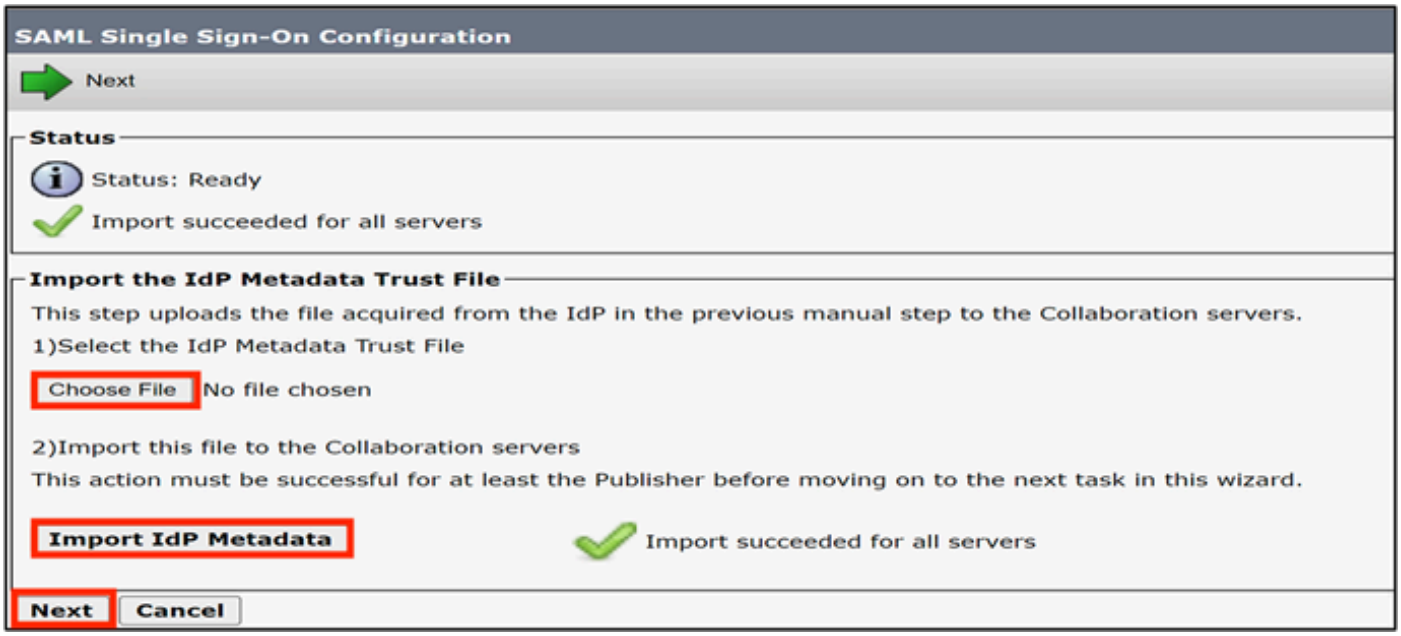




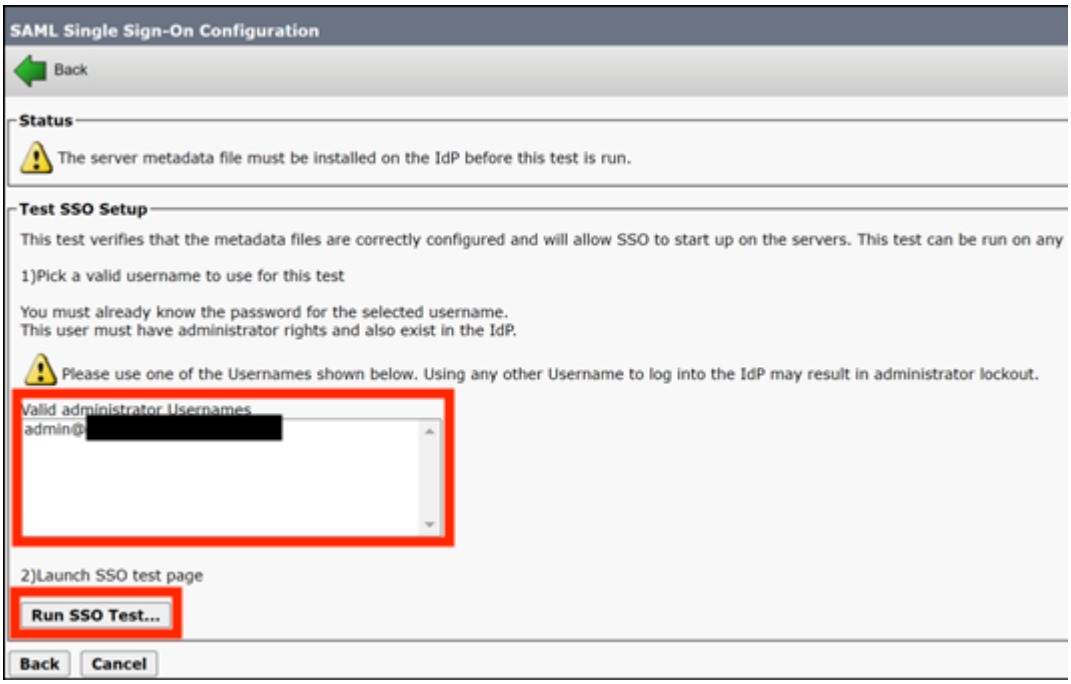
- Als deze stap clusterbreed is, kunt u het multi-san certificaat in alle nodes controleren. Selecteer Test for multi-server tomcat certificate. Selecteer Volgende zodra u klaar bent.

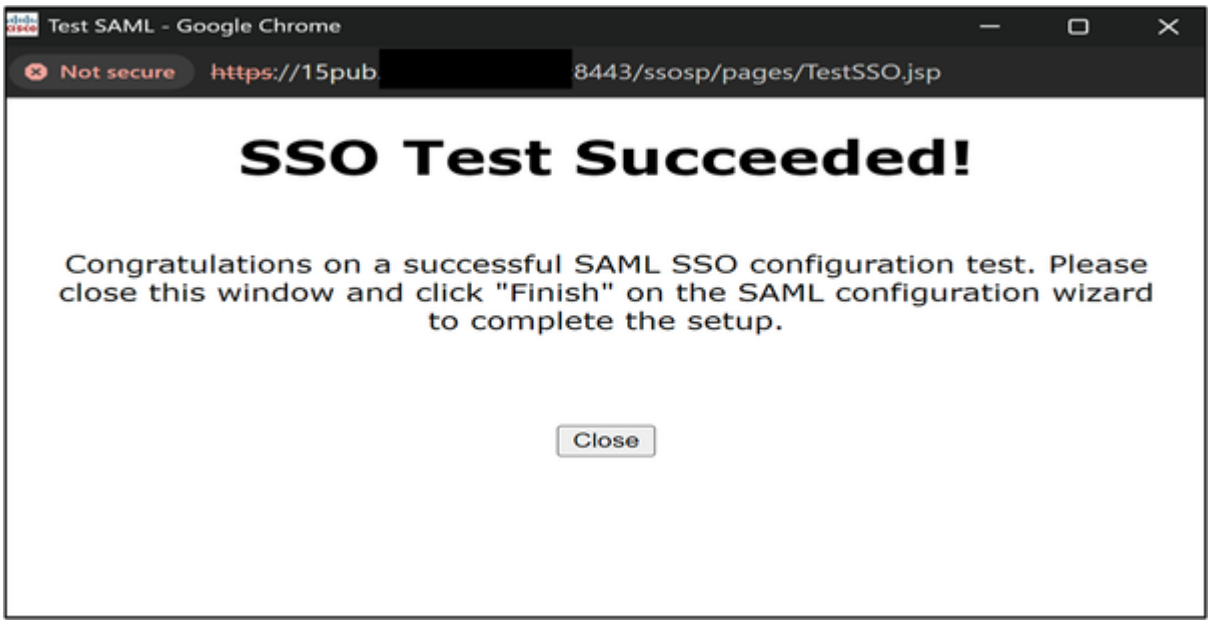


- Upload IdP-metagegevens, selecteer IdP-metagegevens importeren en selecteer Volgende zodra u klaar bent



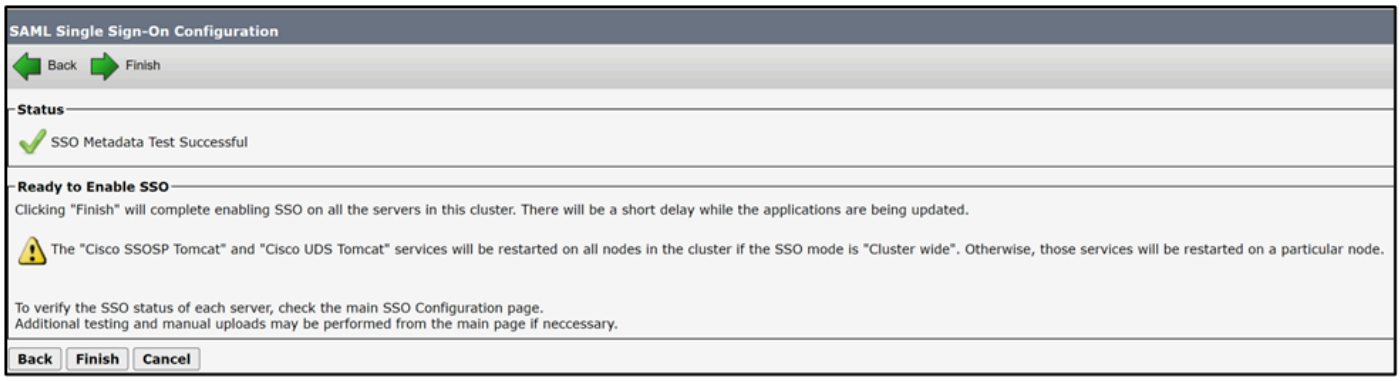
- Selecteer bij SSO-installatie testen een gebruiker met de toegewezen groep Standaard CCM Super Users en selecteer SSO-test uitvoeren tot het succesvol is.





4. Start de vereiste services opnieuw op nadat de SSO is ingeschakeld.

- Inschakelen van SSO herstart de tomcat-service.



TAC raadt echter aan om de Tomcat-service (utils-service herstart Cisco Tomcat) en de UDS Tomcat-service (utils-service herstart CiscoUDSTomcat) handmatig in alle knooppunten te herstarten na het inschakelingsproces voor de SSO.

Scenario 3: Mobiliteit en registratie op afstand na verlenging van het certificaat

Webex-app kan zich niet registreren bij CUCM via Mobility and Remote Access (MRA) nadat Call manager, Tomcat en Expressway C-certificaten zijn verlengd bij gemengde modus-implementaties.

Verificatie

1. CUCM Call manager en Tomcat certificaat zijn CA ondertekende certificaten.
2. De implementatie van CUCM en Expressway wordt uitgevoerd in de gemengde modus (TLS).
3. Inspecteer de logbestanden van Expressway-C en zie "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[5xxxxxx-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
```

Oplossing

Export- en invoercertificaten tussen CUCM en Expressway-C om de vertrouwensrelatie te waarborgen.

⚠ Let op: TAC beveelt aan om dit na uren uit te voeren, omdat deze procedure vereist dat de services opnieuw worden gestart. Business Impact is

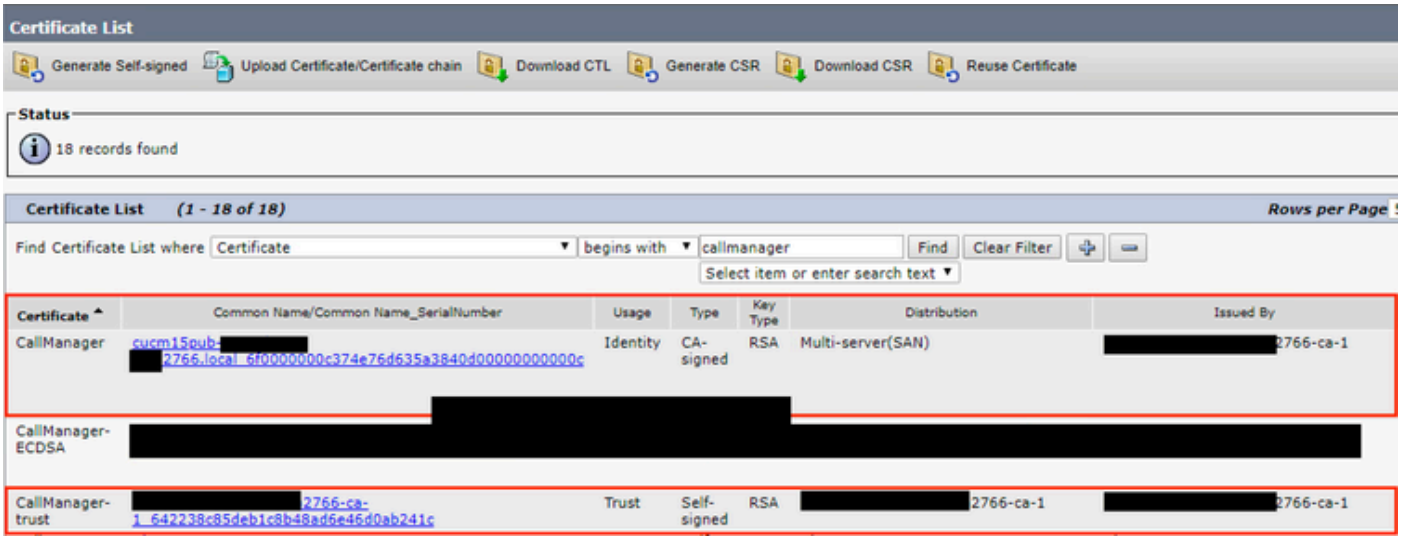
---

Medium Impact.

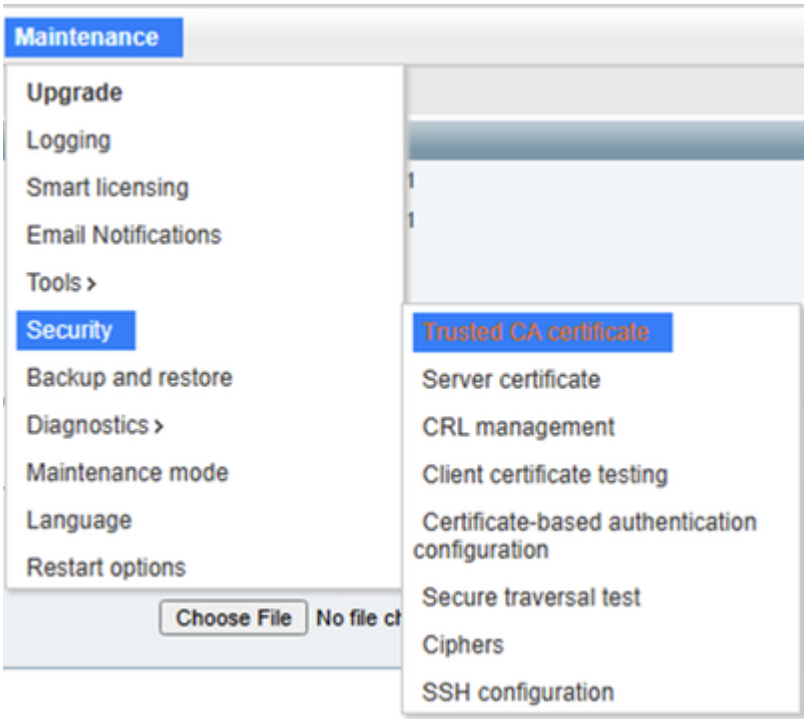
1. Procedure om de vertrouwensrelatie tussen CUCM en Expressway met CA ondertekende

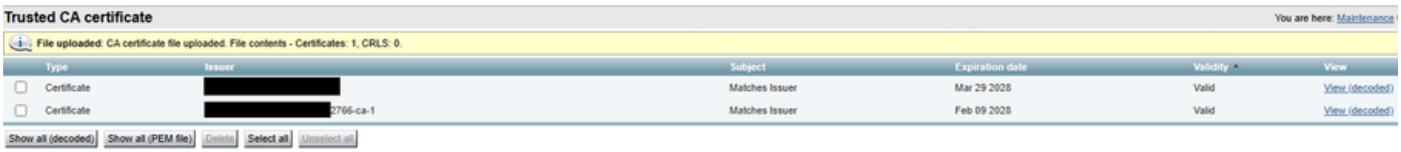
certificaten te voltooien

Navigeer naar Besturingssysteembeheer > Beveiliging > Certificaatbeheer en download het CA-hoofdcertificaat en de tussenpersoon (indien aanwezig) die Call Manager en Tomcat-certificaat ondertekent.



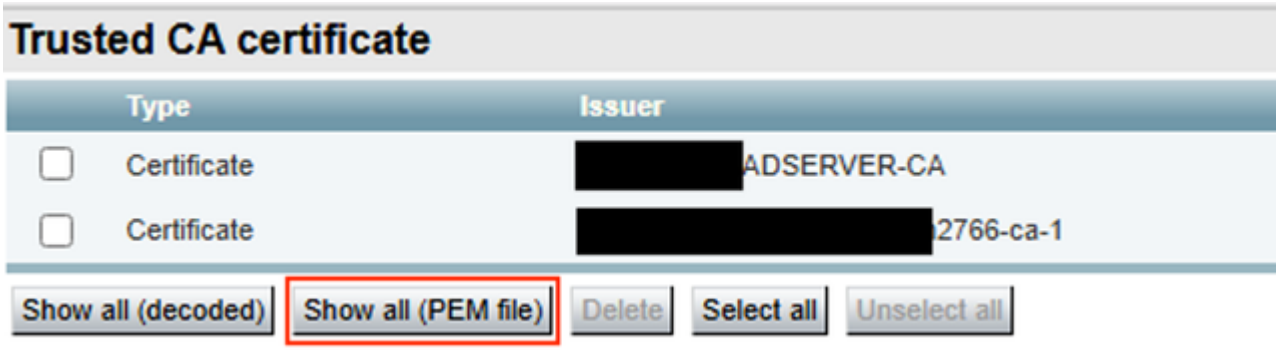
Navigeer vervolgens naar Expressway-C > Onderhoud > Beveiliging > Vertrouwd CA-certificaat en upload het CA-certificaat van Call Manager en Tomcat-certificaat.



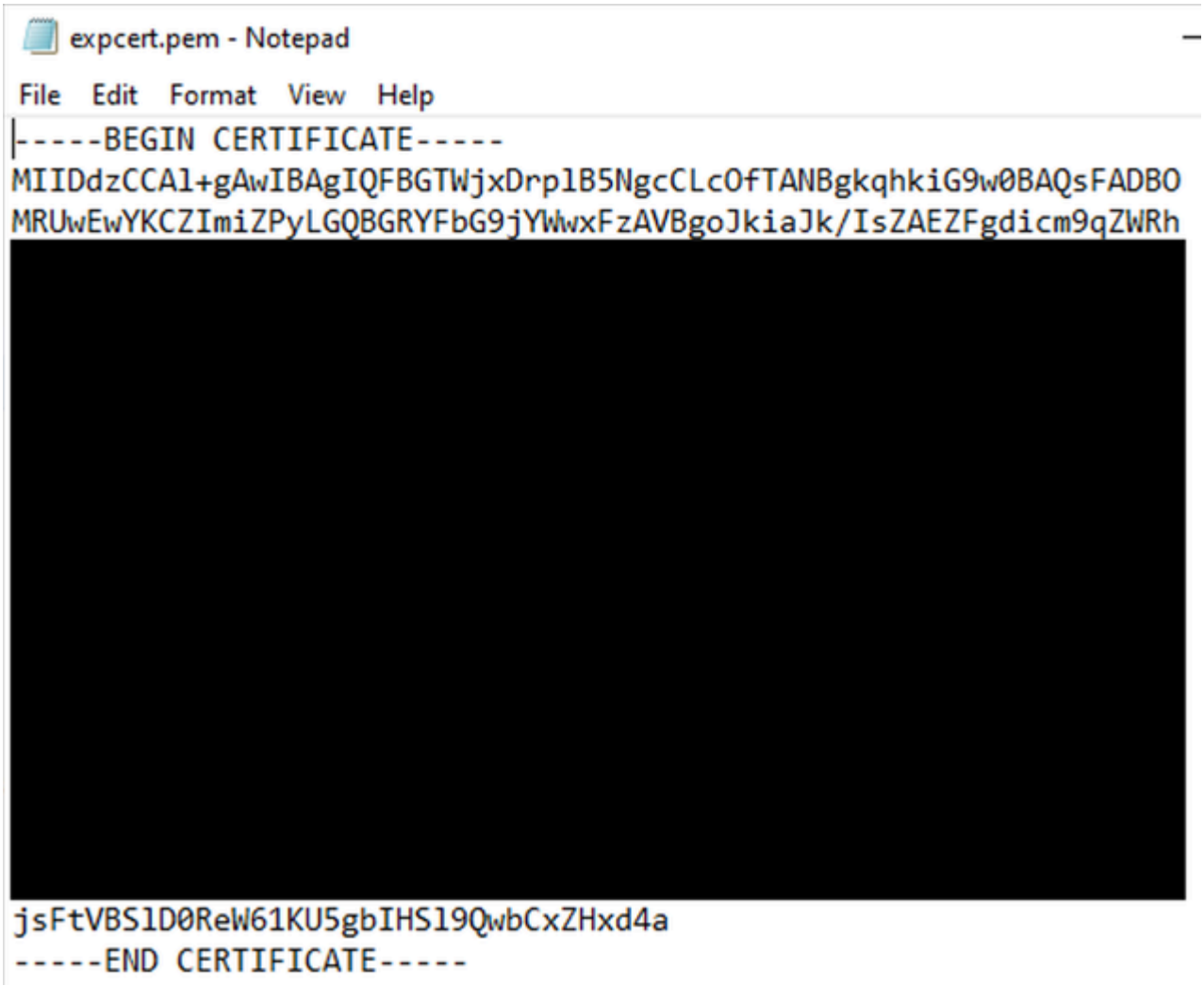


Opmerking: in scenario's met Call Manager en Tomcat-certificaat als zelfondertekend, downloadt u het eigenlijke Call Manager- en Tomcat-certificaat en uploadt u het naar Expressway.

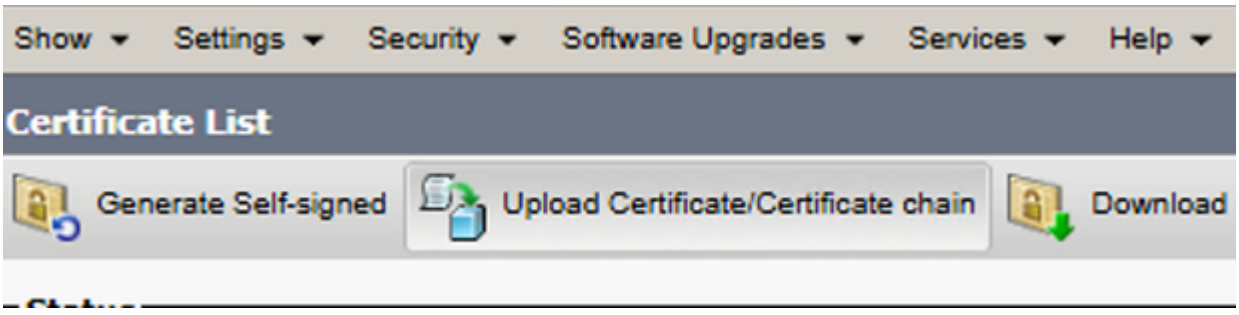
Navigeer naar Expressway-C > Onderhoud > Beveiliging > Vertrouwd CA-certificaat > Alles weergeven (PEM-bestand)

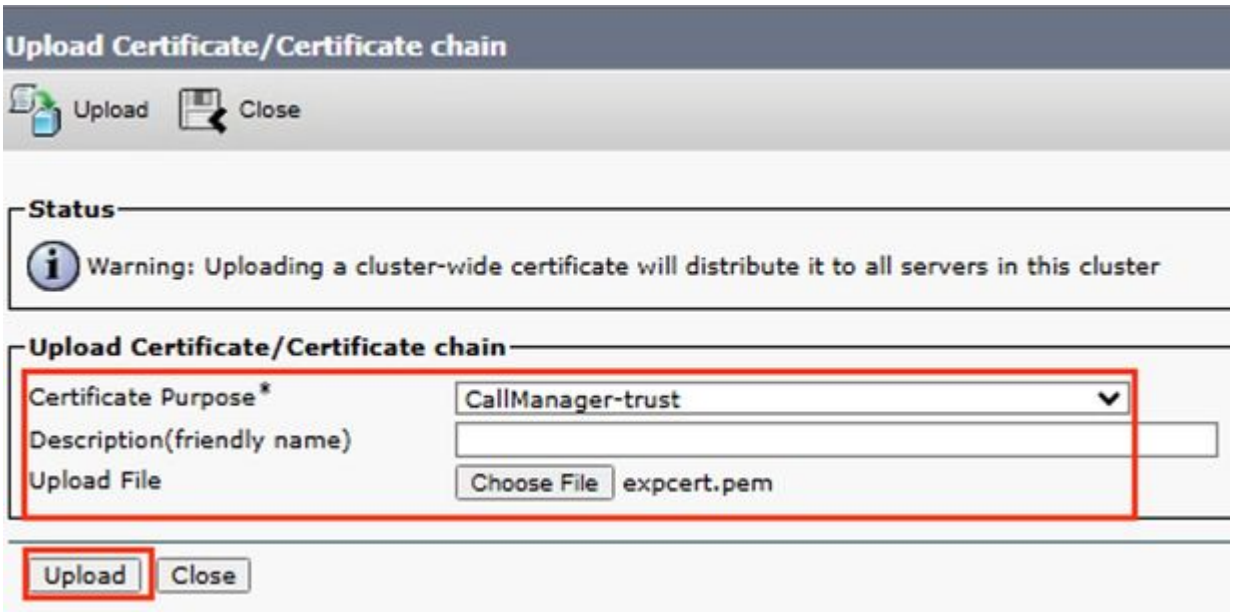


Kopieer de PEM-waarde van het CA-certificaat dat Expressway-C ondertekent en sla deze op in een txt-bestand.



Navigeer naar Besturingssysteembeheer > Beveiliging > Certificaatbeheer en selecteer Certificaat/Certificaatketen uploaden en upload de expressway-CA-cert als Tomcat-trust en Call Manager-trust





Vereiste services opnieuw starten in CUCM-cluster:

- Navigeer naar Cisco Unified Serviceability > Tools > Control Center - Feature Services en start de Cisco CallManager-service opnieuw op in alle knooppunten waarop deze wordt uitgevoerd.
- Navigeer naar Cisco Unified Serviceability > Tools > Control Center - Feature Services en start de Cisco TFTP-service opnieuw op in alle knooppunten waarop deze wordt uitgevoerd.
- Start de Tomcat-service opnieuw op in alle knooppunten in het cluster via CLI met de opdracht Hulpmiddelen-service Cisco Tomcat opnieuw opstarten.
- Start de Cisco HAproxy-service opnieuw op in alle knooppunten in het cluster via CLI met de opdracht Hulpprogramma's service Cisco HAProxy opnieuw opstarten.

Scenario 4: Vernieuwing van certificaat autoriteit proxy functie oorzaak

Scenario 4.1: 802.1x-verificatie mislukt

Telefoon niet authenticeren met ASA na regenereren Certificate Authority Proxy Function (CAPF)

certificaat op CUCM uitgever.

Verificatie

1. Statusberichten voor telefoon tonen "802.1x-verificatie: mislukt"

2. Controleer de telefoonlogboeken van de betreffende server en zoek "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
```

Oplossing

Download het CAPF-certificaat van CUCM-uitgever en upload naar de verificatieserver en omzeilt

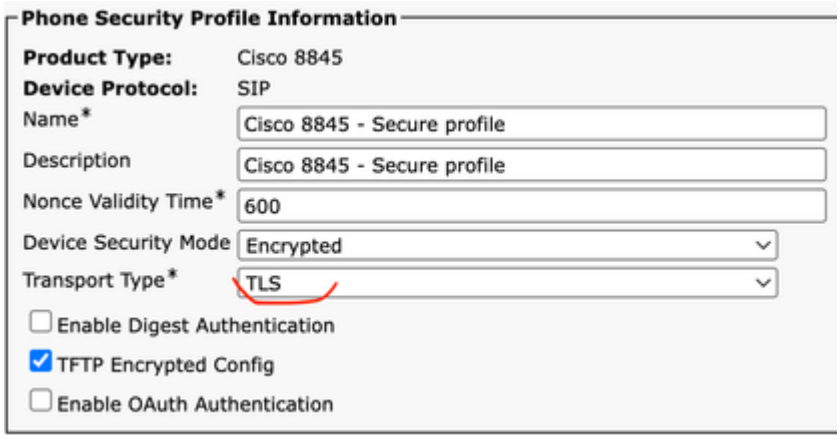
802.1x om registratie toe te staan en het LSC-certificaat op getroffen telefoons te installeren.

Scenario 4.2: Telefoons die zich niet registreren bij CUCM en een beveiligingsprofiel gebruiken in de TLS-modus.

Telefoons tonen "Telefoon registreert zich" na het opnieuw genereren van het CAPF-certificaat op CUCM-uitgever.

Verificatie

1. Affected Phones bevat een beveiligingsprofiel met TLS-modus ingeschakeld.



2. Betrokken telefoons hebben LSC-gecertificeerd geïnstalleerd.
3. Zorg ervoor dat het CAPF-certificaat up-to-date is.

4. Meld u aan bij CUCM publisher en gebruik de opdracht show ctl die het oude CAPF certificaat serienummer toont.
5. Wijzig vervolgens het beveiligingsprofiel van de telefoon in Niet beveiligd.

Oplossing

Regenereer CTL-bestand op CUCM en herstart vereiste services om ervoor te zorgen dat telefoons het nieuwe CTL-bestand met CAPF-bestand krijgen.

⚠ Let op: TAC beveelt aan om dit na uren uit te voeren, omdat deze procedure vereist dat de services opnieuw worden gestart. Business Impact is

---

Medium Impact.

Procedure om een succesvolle verlenging van het CAPF te waarborgen.


```
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.
```

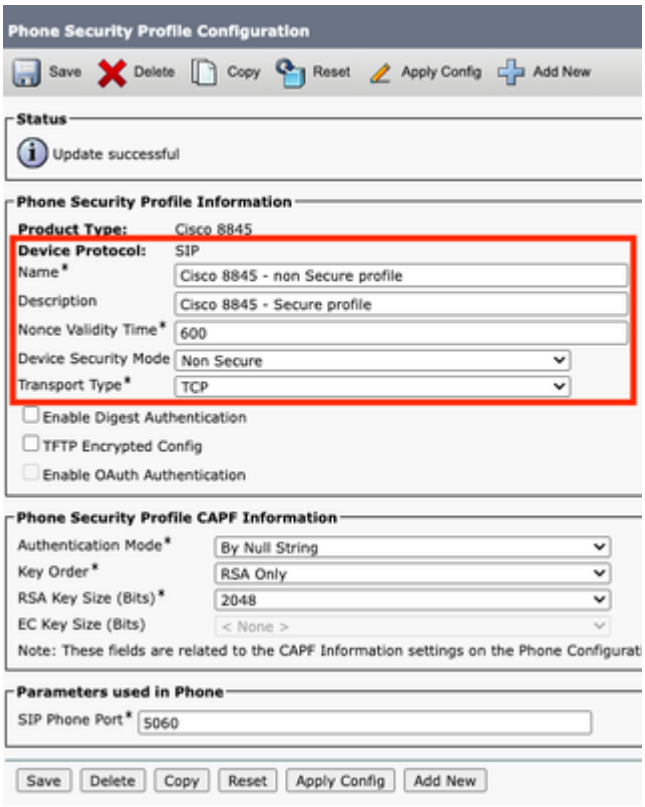
CTL-bestand bijwerken na CAPF-regeneratie. Meld u aan bij de CLI van de uitgever en voer de opdracht ctl update CTLFile in.

1. Navigeer naar Cisco Unified Serviceability > Tools > Control Center - Feature Services in CUCM publisher en start de CAPF-service opnieuw op.
2. Navigeer naar Cisco Unified Serviceability > Tools > Control Center - Network Services en start Cisco Trust Verification Service opnieuw op in alle knooppunten waarop de service wordt uitgevoerd.
3. Navigeer naar Cisco Unified Serviceability > Tools > Control Center - Feature Services en start Cisco TFTP Service opnieuw op in alle knooppunten waarop deze service wordt uitgevoerd

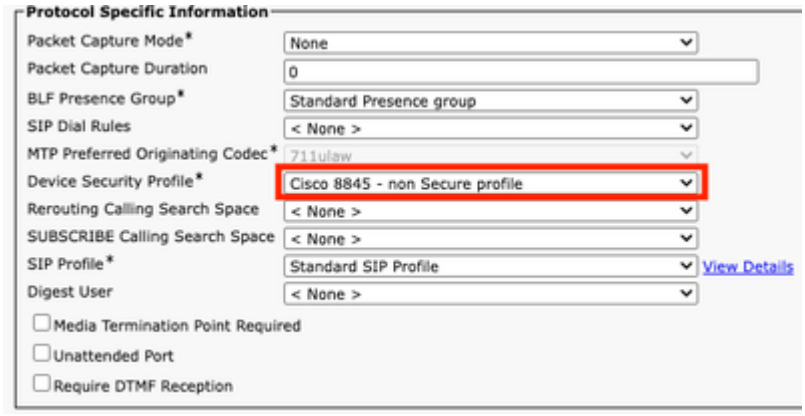
- Navigeer naar Beheer CM > Systeem > Beveiliging > Beveiligingsprofiel telefoon.

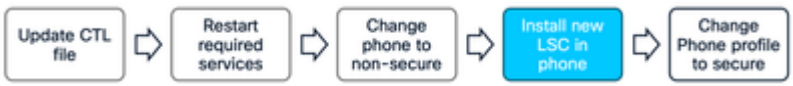
- Kopieer het huidige beveiligingsprofiel van de telefoon dat is toegewezen aan de vereiste telefoons.

- Wijzig de naam en de apparaatbeveiligingsmodus in Niet beveiligd en selecteer Opslaan en Config toepassen om deze wijziging toe te passen op alle vereiste telefoons.



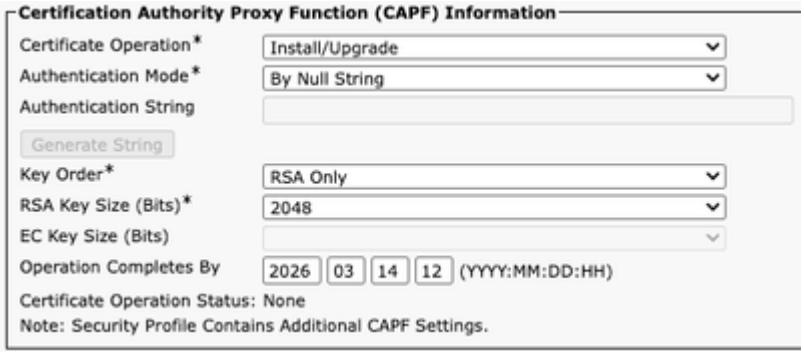
- Pas het gemaakte apparaatbeveiligingsprofiel toe op de vereiste telefoonconfiguratie en selecteer Opslaan en Config toepassen.





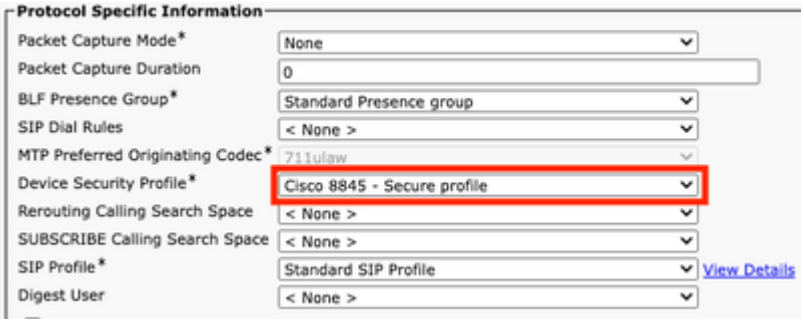
Gebruik de sectie CAPF-informatie in de apparaatconfiguratie van getroffen telefoons om het LSC-certificaat in de vereiste telefoons te installeren.

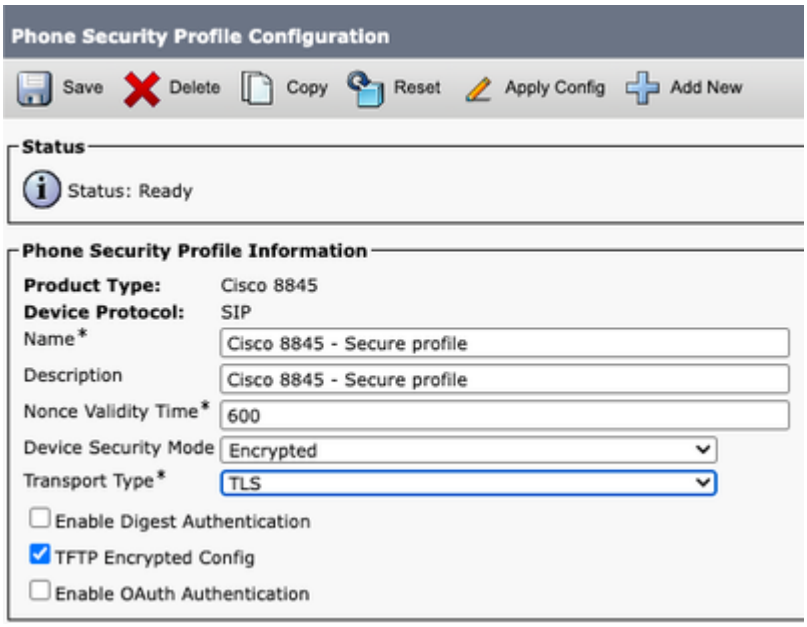
- Selecteer in CAPF-informatie de optie Installeren/upgraden in certificaatbewerking.



- Selecteer Opslaan en Config toepassen.
- Wacht totdat de status van de certificaatbewerking aangeeft dat de bewerking is voltooid.

In het gedeelte Protocolspecifieke informatie over telefoonconfiguratie selecteert u het beveiligingsprofiel met TLS ingeschakeld dat is gemaakt.





Gerelateerde informatie

- 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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.