

# 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.

 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	

## 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.

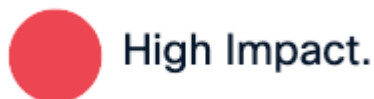
Wanneer Call Manager, TVS en ITL certificaten verlopen en ze werden verlengd op hetzelfde moment, Het zorgt ervoor dat al onze telefoons in een niet-geregistreerde staat die een grote impact op het systeem veroorzaakt, dit is een verwacht gedrag als we leiden de telefoons niet vertrouwen in de CUCM.

### Verificatie

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



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.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
...

```

## 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.

---

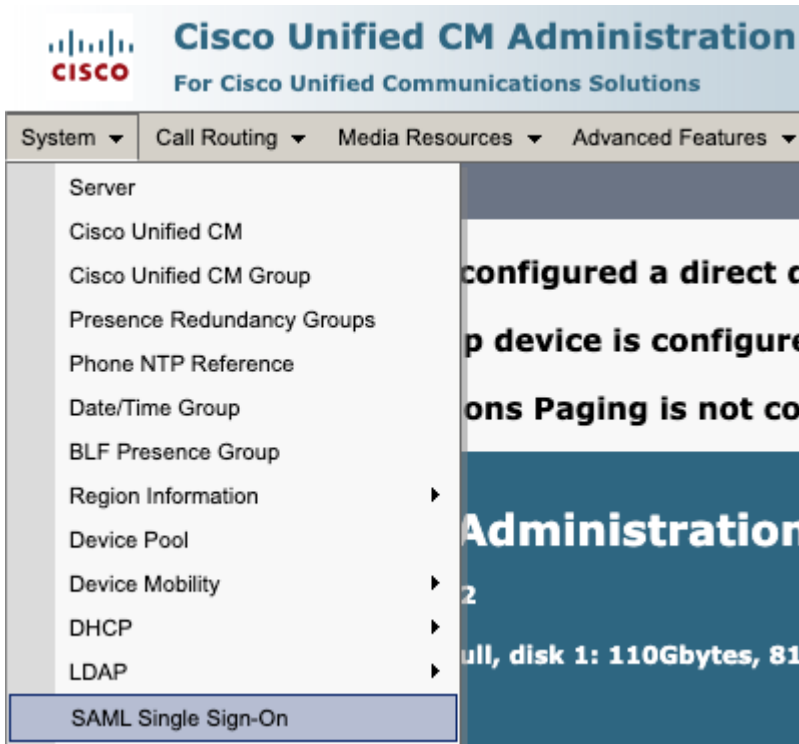


Low Impact

### 1. SSO uitschakelen in alle CUCM-knooppunten



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



- Selecteer SAML SSO uitschakelen



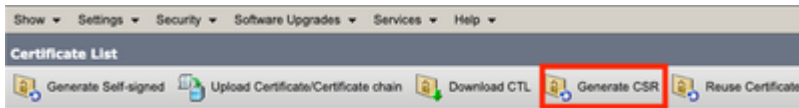
- Dit proces moet worden uitgevoerd in alle andere knooppunten via GUI als per-node overeenkomst wordt gebruikt.

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

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\* cm15-pub-...cisco.com

Include OU in CSR

Subject Alternate Names (SANs)

Auto-populated Domains

|                       |
|-----------------------|
| cm15-pub-...cisco.com |
| cm15-sub-...cisco.com |

Parent Domain cisco.com

Other Domains

Seleccionar archivo Sin archivos seleccionados  
Please import .TXT file only.

Add

Key Type\*\* RSA

Key Length\* 2048

Hash Algorithm\* SHA256

Generate Close

- 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.

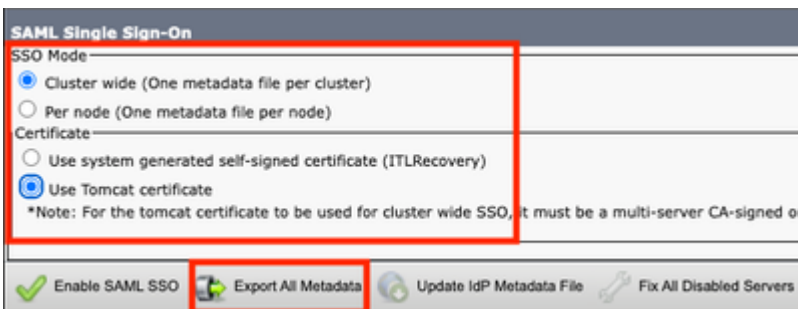
Voor meer informatie verwijzen wij u naar deze documentatie:

- [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

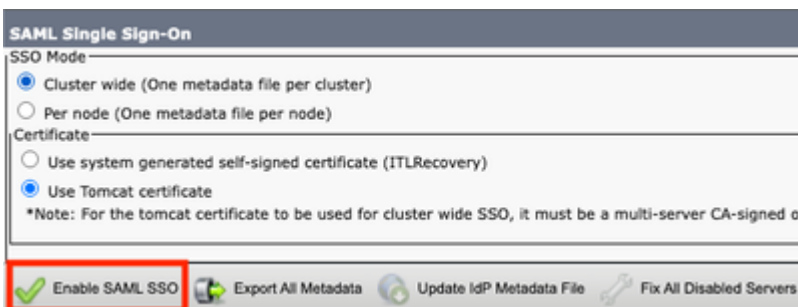



- SP-metagegevens importeren naar de Identity Provider (IdP)-server. Raadpleeg [SAML SSO configureren op Identity Provider voor](#) meer informatie

### 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.



 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.


- 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.

**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


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

**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.


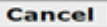
1) Select the IdP Metadata Trust File

 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 succeeded for all servers


 

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

**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.

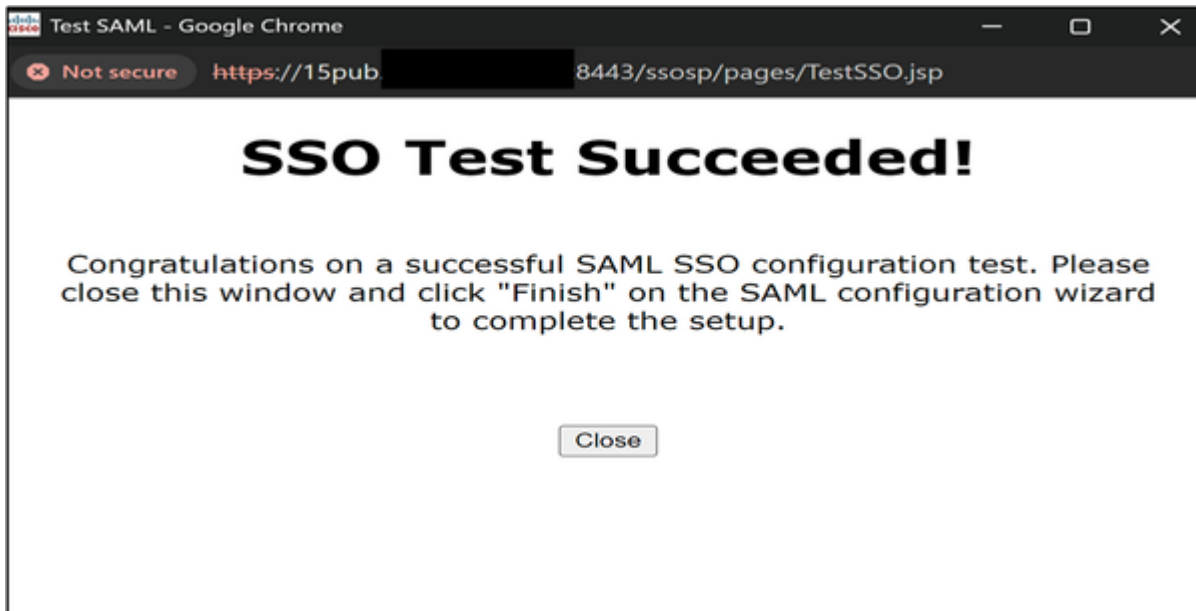
Valid administrator Usernames

admin@ [redacted]

2) Launch SSO test page



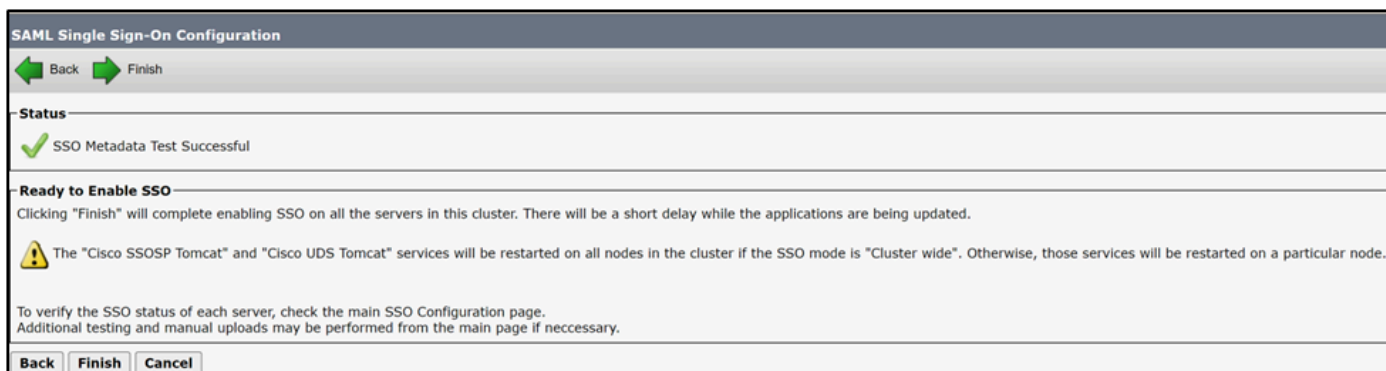
 



4. Start de vereiste services opnieuw op nadat de SSO is ingeschakeld.



- 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" 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
```

## 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.

| Certificate       | Common Name/Common Name_SerialNumber                            | Usage    | Type        | Key Type | Distribution      | Issued By |
|-------------------|-----------------------------------------------------------------|----------|-------------|----------|-------------------|-----------|
| CallManager       | cucm15sub-<br>2766.local_6f0000000c374e76d635a3840d00000000000c | Identity | CA-signed   | RSA      | Multi-server(SAN) | 2766-ca-1 |
| CallManager-ECDSA |                                                                 |          |             |          |                   |           |
| CallManager-trust | 2766-ca-<br>1_642238c85deb1c8b48ad6e46d0ab241c                  | Trust    | Self-signed | RSA      | 2766-ca-1         | 2766-ca-1 |

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

- 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

Upload

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

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]:766-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](#)



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)

**Trusted CA certificate**

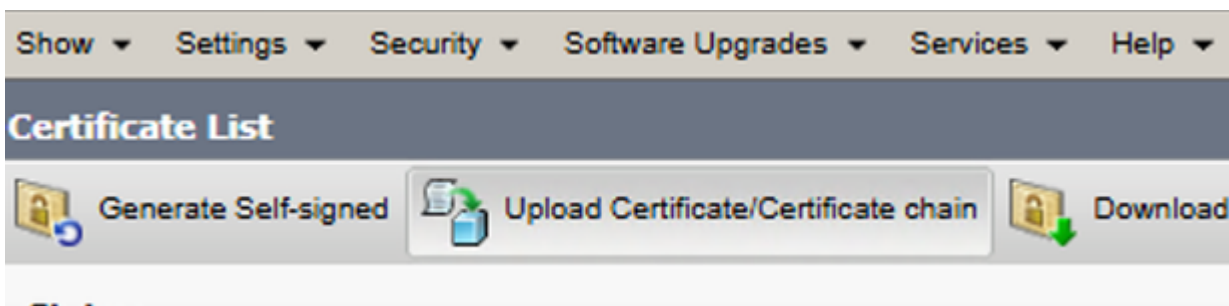
| Type                                 | Issuer                |
|--------------------------------------|-----------------------|
| <input type="checkbox"/> Certificate | [REDACTED]ADSERVER-CA |
| <input type="checkbox"/> Certificate | [REDACTED]:766-ca-1   |

[Show all \(decoded\)](#) [Show all \(PEM file\)](#) [Delete](#) [Select all](#) [Unselect all](#)

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

```
expcert.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIDdzCCA1+gAwIBAgIQFBGTWjxDrp1B5NgcCLc0FTANBgkqhkiG9w0BAQsFADBO
MRUwEwYKCZImiZPyLGOBGRYFbG9jYWwxFzAVBgoJkiaJk/IsZAEZFgdicm9qZWRh
jsFtVBS1D0ReW61KU5gbIHS19QwbCxZHxd4a
-----END CERTIFICATE-----
```

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



**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



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)



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.

**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

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

| 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. 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.

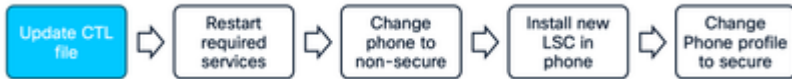
## Oplossing

Regeneer 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

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.
```

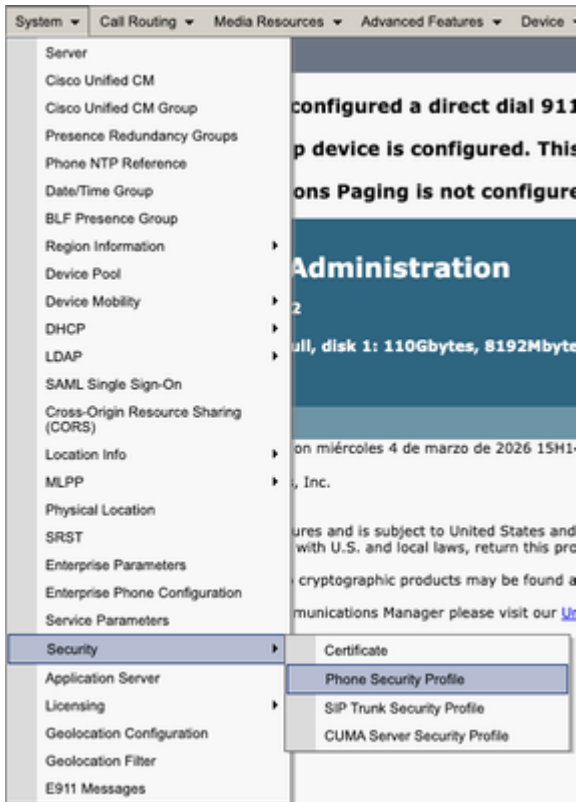
CTL-bestand bijwerken na CAPF-regeneratie. Meld u aan bij de CLI van de uitgever en voer de opdracht `ctl update CTLFile` in.



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 > System > 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.

**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 Configurati

**Parameters used in Phone**

SIP Phone Port\*: 5060

Save Delete Copy Reset Apply Config Add New

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

**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



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.

**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.

- 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.

**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

## 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](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.