

Nieuwe certificaten maken van ondertekende CA-certificaten

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Informatie vooraf controleren](#)

[Certificaten configureren en opnieuw genereren](#)

[Tomcat Certificate](#)

[CallManager-certificaat](#)

[IPsec-certificaat](#)

[CAPF-certificaat](#)

[TV-certificaat](#)

[Probleemoplossing voor gebruikelijke geüploade certificaatfoutmeldingen](#)

[CA-certificaat is niet beschikbaar in de Trust-Store](#)

[Bestand /usr/local/platform/.security/tomcat/keys/tomcat.csr bestaat niet](#)

[MVO Openbare sleutel en Certificaat Openbare sleutel komen niet overeen](#)

[MVO alternatieve naam \(SAN\) en certificaat SAN komt niet overeen](#)

[Trustcertificaten met dezelfde GN worden niet vervangen](#)

Inleiding

Dit document beschrijft hoe u de certificaten kunt regenereren die door een certificaatinstantie (CA) zijn ondertekend in Cisco Unified Communications Manager (CUCM).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Realtime Monitoring Tool (RTMT)
- CUCM-certificaten

Gebruikte componenten

- CUCM release 10.x, 11.x en 12.x.

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.

Informatie vooraf controleren

Opmerking: Voor zelfondertekende certificaatregeneratie raadpleegt u de [Handleiding certificaatregeneratie](#). Raadpleeg voor door CA ondertekend multi-SAN-certificaatregeneratie de [multi-SAN-certificaatregeneratiegids](#).

Om de impact van elk certificaat en de regeneratie ervan te begrijpen, raadpleegt u de [zelfondertekende regeneratiegids](#).

Elk type certificaatondertekeningaanvraag (CSR) heeft verschillende belangrijke gebruiksdoeleinden en die zijn vereist in het ondertekende certificaat. De [Security Guide](#) bevat een tabel met de vereiste belangrijkste gebruiksdoeleinden voor elk type certificaat.

U kunt de onderwerpinstellingen (locatie, staat, organisatie-eenheid, enzovoort) als volgt wijzigen:

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

Het Tomcat-certificaat wordt automatisch opnieuw gegenereerd nadat u de `set web-security` uit. Het nieuwe zelfondertekende certificaat wordt niet toegepast tenzij de Tomcat-service opnieuw wordt gestart. Raadpleeg deze handleidingen voor meer informatie over deze opdracht:

- [Naslaghandleiding opdrachtregel](#)
- [Link naar Cisco Community-stappen](#)
- [Video](#)

Certificaten configureren en opnieuw genereren

De stappen voor het regenereren van certificaten met één knooppunt in een CUCM-cluster die door een CA zijn ondertekend, worden vermeld voor elk type certificaat. Het is niet nodig om alle certificaten in de cluster te regenereren als ze niet zijn verlopen.

Tomcat Certificate

Waarschuwing: controleer of SSO in het cluster is uitgeschakeld (**CM Administration > System > SAML Single Sign-On**). Als SSO is ingeschakeld, moet deze worden uitgeschakeld en weer worden ingeschakeld zodra het Tomcat-certificaatregeneratieproces is voltooid.

Op alle knooppunten (CallManager en IM&P) van het cluster:

Stap 1. Navigeer naar **Cisco Unified OS Administration > Security > Certificate Management > Find** en controleert de vervaldatum van het Tomcat-certificaat.

Stap 2. Klik op **Generate CSR > Certificate Purpose: tomcat**. Selecteer de gewenste instellingen voor het certificaat en klik vervolgens op **Generate**. Wacht tot het succesbericht verschijnt en klik op **Close**.

Generate Certificate Signing Request

Generate Close

Status

Success: Certificate Signing Request Generated

Generate Certificate Signing Request

Certificate Purpose** tomcat

Distribution* 115pub

Common Name* 115pub

Subject Alternate Names (SANs)

Parent Domain

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

Generate Close

*- indicates required item.

**When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

Stap 3. Download de CSR. Klik **Download CSR** , selecteer **Certificate Purpose: tomcat**, en klik op **Download**.

Download Certificate Signing Request

Download CSR Close

Status

Warning: Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

Certificate Purpose* tomcat

Download CSR Close

*- indicates required item.

Stap 4. Verzend de MVO naar de certificaatautoriteit.

Stap 5. De certificeringsinstantie retourneert twee of meer bestanden voor de ondertekende certificaatketen. Upload de certificaten in deze volgorde:

- Root CA certificaat als tomcat-trust. Navigeer naar **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. Stel de beschrijving van het certificaat in en blader door het basiscertificaatbestand.
- Tussentijds certificaat als tomcat-trust (optioneel). **Navigeer naar Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. Stel de beschrijving van het certificaat in en blader door het tussenliggende certificaatbestand.

Opmerking: Sommige CA's geven geen tussentijds certificaat, als alleen het basiscertificaat werd verstrekt, kan deze stap worden weggelaten.

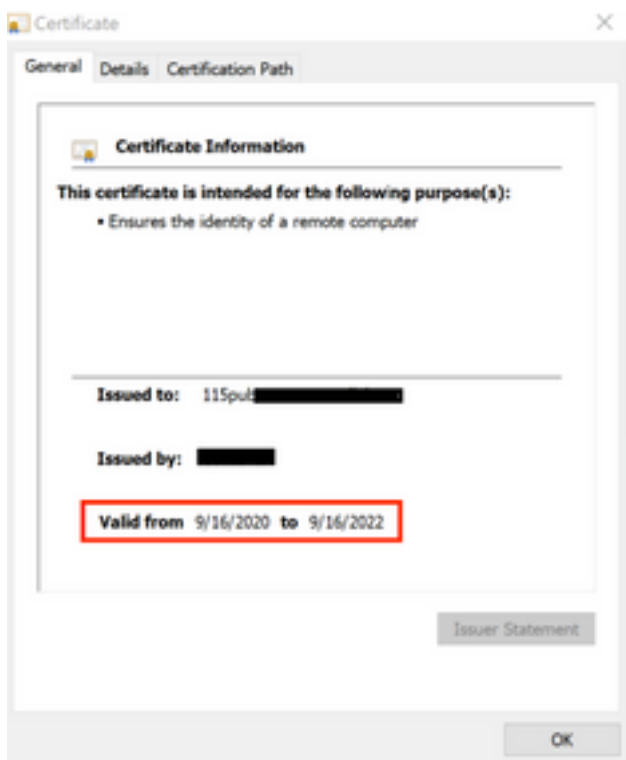
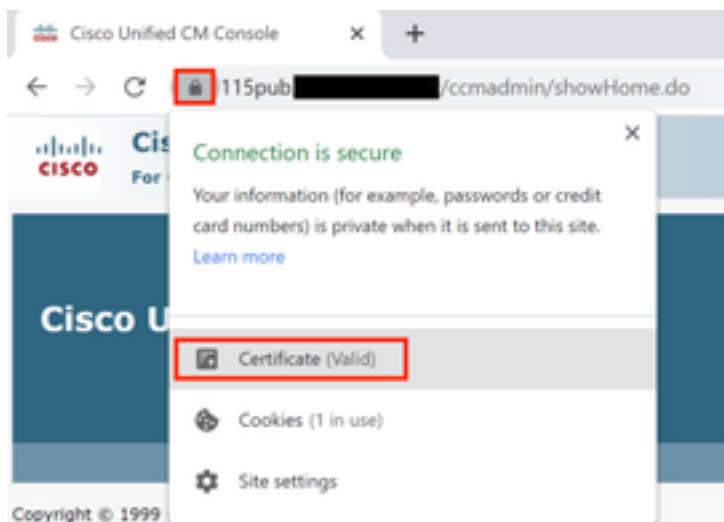
- CA-ondertekend certificaat als tomcat. **Navigeer naar Certificate Management > Upload certificate > Certificate Purpose: tomcat1**. Stel de beschrijving van het certificaat in en blader door het CA-

ondertekende certificaatbestand voor het huidige CUCM-knooppunt.

Opmerking: Op dit punt vergelijkt CUCM de CSR en het geüploade CA-ondertekende certificaat. Als de informatie overeenkomt, verdwijnt de MVO en wordt het nieuwe CA-ondertekende certificaat geüpload. Als u een foutbericht ontvangt nadat het certificaat is geüpload, raadpleegt u de Upload Certificate Common Error Messages doorsnede.

Stap 6. Om het nieuwe certificaat op de server te kunnen toepassen, moet de Cisco Tomcat-service via CLI worden herstart (start met Publisher, en vervolgens moeten abonnees, één voor één) de opdracht gebruiken `utils service restart Cisco Tomcat`.

Om het Tomcat-certificaat te valideren wordt nu gebruikt door CUCM. Navigeer naar de webpagina van het knooppunt en selecteer Site Information (Vergrendelingspictogram) in de browser, klikt u op de `certificate` van het nieuwe certificaat.



CallManager-certificaat

Voorzichtig: Regeneer CallManager- en TVS-certificaten niet tegelijkertijd. Dit veroorzaakt een onherstelbare mismatch met de geïnstalleerde ITL op endpoints die de verwijdering van ITL van ALLE endpoints in het cluster vereist. Voltooi het gehele proces voor CallManager en zodra de telefoons terug zijn geregistreerd, start het proces voor de TVS.

Opmerking: om te bepalen of het cluster in gemengde modus staat, navigeer u naar **Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == niet-beveiligd; 1 == gemengde modus)**.

Voor alle CallManager-knooppunten van het cluster:

Stap 1. Navigeer naar **Cisco Unified OS Administration > Security > Certificate Management > Find** en de verlooptdatum van het CallManager-certificaat verifiëren.

Stap 2. Klik op **Generate CSR > Certificate Purpose: CallManager**. Selecteer de gewenste instellingen voor het certificaat en klik vervolgens op **Generate**. Wacht tot het succesbericht verschijnt en klik op **Close**.

Stap 3. Download de CSR. Klik **Download CSR**. Select **Certificate Purpose: CallManager** and click **Download**.

Stap 4. Verzend de MVO naar de **Certificate Authority** .

Stap 5. De certificeringsinstantie retourneert twee of meer bestanden voor de ondertekende certificaatketen. Upload de certificaten in deze volgorde:

- CA-certificaat als CallManager-trust. Navigeer naar **Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust**. Stel de beschrijving van het certificaat in en blader door het basiscertificaatbestand.
- Tussentijds certificaat als CallManager-trust (optioneel). Navigeer naar **Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust**. Stel de beschrijving van het certificaat in en blader door het tussenliggende certificaatbestand.

Opmerking: Sommige CA's geven geen tussentijds certificaat, als alleen het basiscertificaat werd verstrekt, kan deze stap worden weggelaten.

- Door CA ondertekend certificaat als CallManager. Navigeer naar **Certificate Management > Upload certificate > Certificate Purpose: CallManager**. Stel de beschrijving van het certificaat in en blader door het CA-ondertekende certificaatbestand voor het huidige CUCM-knooppunt.

Opmerking: Op dit punt vergelijkt CUCM de CSR en het geüploade CA-ondertekende certificaat. Als de informatie overeenkomt, verdwijnt de MVO en wordt het nieuwe CA-ondertekende certificaat geüpload. Als u een foutbericht ontvangt nadat het certificaat is geüpload, raadpleegt u de sectie **Gemeenschappelijke foutmeldingen in uploadcertificaat**.

Stap 6. Als het cluster zich in de gemengde modus bevindt, update de CTL voordat de services opnieuw worden gestart: [Token](#) of [Tokenloos](#). Als het cluster zich in de niet-beveiligde modus bevindt, slaat u deze stap over en gaat u verder met het opnieuw opstarten van de services.

Stap 7. Om het nieuwe certificaat op de server toegepast te krijgen, moeten de vereiste services opnieuw opgestart worden (alleen als de service draait en actief is). Navigeren naar:

- **Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service**

- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CallManager
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CTIManager

Stap 8. Zet alle telefoons terug:

- Navigeer naar Cisco Unified CM Administration > System > Enterprise Parameters > Reset. Er verschijnt een pop-upvenster met de verklaring U staat op het punt alle apparaten in het systeem te resetten. Deze actie kan niet ongedaan worden gemaakt. Doorgaan? selecteren OK en klik vervolgens op Reset .

Opmerking: Monitorapparaatregistratie via RTMT. Zodra alle telefoons registreren terug kunt u met het volgende certificaatype te werk gaan.

IPsec-certificaat

Voorzichtig: Een back-up- of terugzettaak mag niet actief zijn wanneer het IPsec-certificaat wordt geregenereerd.

Voor alle knooppunten (CallManager en IM&P) van het cluster:

Stap 1. Navigeer naar Cisco Unified OS Administration > Security > Certificate Management > Find en de vervaldatum van het ipsec-certificaat te verifiëren.

Stap 2. Klik op **Generate CSR > Certificate Purpose: ipsec**. Selecteer de gewenste instellingen voor het certificaat en klik vervolgens op **Generate**. Wacht totdat het succesbericht verschijnt en klik vervolgens op **Sluiten**.

Stap 3. Download de CSR. Klik op **CSR downloaden**. Selecteer ipsec voor certificaatdoeleinden en klik op **Downloaden**.

Stap 4. Verzend de MVO naar de certificaatautoriteit.

Stap 5. De certificeringsinstantie retourneert twee of meer bestanden voor de ondertekende certificaatketen. Upload de certificaten in deze volgorde:

- Root CA-certificaat als ipsec-trust. Navigeren naar **certificaatbeheer > Uploadcertificaat > Doel certificaat: ipsec-trust**. Stel de beschrijving van het certificaat in en blader door het basiscertificaatbestand.
- Tussentijds certificaat als ipsec-trust (optioneel). Navigeren naar **certificaatbeheer > Uploadcertificaat > Doel certificaat: Tomcat-trust**. Stel de beschrijving van het certificaat in en blader door het tussenliggende certificaatbestand.

Opmerking: Sommige CA's geven geen tussentijds certificaat, als alleen het basiscertificaat werd verstrekt, kan deze stap worden weggelaten.

- Door CA ondertekend certificaat als ipsec. Navigeren naar **certificaatbeheer > Uploadcertificaat > Doel certificaat: ipsec**. Stel de beschrijving van het certificaat in en blader door het CA-ondertekende certificaatbestand voor het huidige CUCM-knooppunt.

Opmerking: Op dit punt vergelijkt CUCM de CSR en het geüploade CA-ondertekende

certificaat. Als de informatie overeenkomt, verdwijnt de MVO en wordt het nieuwe CA-ondertekende certificaat geüpload. Als u een foutbericht ontvangt nadat het certificaat is geüpload, raadpleegt u de **sectie Gemeenschappelijke foutmeldingen uploaden van het uploadcertificaat**.

Stap 6. Om het nieuwe certificaat op de server toegepast te krijgen, moeten de vereiste services opnieuw opgestart worden (alleen als de service draait en actief is). Navigeren naar:

- **Cisco Unified Service > Tools > Control Center - netwerkservices > Cisco DRF Master**(Uitgever)
- **Cisco Unified Servicability > Tools > Control Center - netwerkservices > Cisco DRF lokaal** (uitgever en abonnees)

CAPF-certificaat

Opmerking: om te bepalen of het cluster in gemengde modus staat, moet u navigeren naar **Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode** (0 == niet-beveiligd; 1 == gemengde modus).

Opmerking: CAPF service draait alleen in de uitgever, en dat is het enige certificaat dat wordt gebruikt. Het is niet nodig om Subscriber-knooppunten ondertekend te krijgen door een CA, omdat ze niet worden gebruikt. Als het certificaat in de abonnees is verlopen en u de waarschuwingen van verlopen certificaten wilt voorkomen, kunt u de CAPF-certificaten van de abonnee opnieuw genereren als zelfondertekend. Zie [CAPF-certificaat als zelfondertekend voor](#) meer informatie.

In de uitgeverij:

Stap 1. Navigeer naar **Cisco Unified OS-beheer > Beveiliging > certificaatbeheer > Zoek** en controleer de verloopdatum van het CAPF-certificaat.

Stap 2. Klik op **Generate CSR > Certificate Purpose: CAPF**. Selecteer de gewenste instellingen voor het certificaat en klik vervolgens op **Generate**. Wacht tot het succesbericht verschijnt en klik op **Sluiten**.

Stap 3. Download de CSR. Klik op **CSR downloaden**. Selecteer Certificaat Doel CAPF en klik op **Downloaden**.

Stap 4. Verzend de MVO naar de certificaatautoriteit.

Stap 5. De certificeringsinstantie retourneert twee of meer bestanden voor de ondertekende certificaatketen. Upload de certificaten in deze volgorde:

- CA-basiscertificaat als CAPF-trust. Navigeren naar **certificaatbeheer > Uploadcertificaat > Doel certificaat: CAPF-trust**. Stel de beschrijving van het certificaat in en blader door het basiscertificaatbestand.
- Tussentijds certificaat als CAPF-trust (optioneel). Navigeren naar **certificaatbeheer > Uploadcertificaat > Doel certificaat: CAPF-trust**. Stel de beschrijving van het certificaat in en blader door het tussenliggende certificaatbestand.

Opmerking: Sommige CA's geven geen tussentijds certificaat, als alleen het basiscertificaat werd verstrekt, kan deze stap worden weggelaten.

- Door CA ondertekend certificaat als CAPF. Navigeren naar **certificaatbeheer > Uploadcertificaat > Doel certificaat: CAPF**. Stel de beschrijving van het certificaat in en blader door het CA-ondertekende certificaatbestand voor het huidige CUCM-knooppunt.

Opmerking: Op dit punt vergelijkt CUCM de CSR en het geüploade CA-ondertekende certificaat. Als de informatie overeenkomt, verdwijnt de MVO en wordt het nieuwe CA-ondertekende certificaat geüpload. Als u een foutbericht ontvangt nadat het certificaat is geüpload, raadpleegt u de sectie **Gemeenschappelijke foutmeldingen** in **uploadcertificaat**.

Stap 6. Als het cluster zich in de gemengde modus bevindt, update de CTL voordat de services opnieuw worden gestart: [Token](#) of [Tokenloos](#). Als het cluster zich in de niet-beveiligde modus bevindt, slaat u deze stap over en gaat u verder met het opnieuw opstarten van de service.

Stap 7. Om het nieuwe certificaat op de server toegepast te krijgen, moeten de vereiste services opnieuw opgestart worden (alleen als de service draait en actief is). Navigeren naar:

- **Cisco Unified Service > Tools > Control Center - Netwerkservices > Cisco Trust Verification Service** (Alle knooppunten waar de service wordt uitgevoerd)
- **Cisco Unified Servicability > Tools > Control Center - functieservices > Cisco TFTP** (Alle knooppunten waar de service wordt uitgevoerd)
- **Cisco Unified Servicability > Tools > Control Center - functieservices > Cisco Certificate Authority Proxy-functie** (uitgever)

Stap 8. Zet alle telefoons terug:

- Ga naar **Cisco Unified CM Management > System > Enterprise Parameters > Reset**. Er verschijnt een pop-upvenster met de verklaring U staat op het punt alle apparaten in het systeem te resetten. Deze actie kan niet ongedaan worden gemaakt. Doorgaan? Selecteer **OK** en klik vervolgens op **Reset**.

Opmerking: Monitorapparaatregistratie via RTMT. Zodra alle telefoons registreren terug kunt u met het volgende certificaatype te werk gaan.

TV-certificaat

Voorzichtig: Regeneer CallManager- en TVS-certificaten niet tegelijkertijd. Dit veroorzaakt een onherstelbare mismatch met de geïnstalleerde ITL op endpoints die de verwijdering van ITL van ALLE endpoints in het cluster vereist. Voltooi het gehele proces voor CallManager en zodra de telefoons terug zijn geregistreerd, start het proces voor de TVS.

Voor alle TVS-knooppunten van het cluster:

Stap 1. Navigeer naar **Cisco Unified OS-beheer > Beveiliging > certificaatbeheer > Zoek** en controleer de verlooptdatum van het TV-certificaat.

Stap 2. Klik op **Generate CSR > Certificate Purpose: TV**. Selecteer de gewenste instellingen voor het certificaat en klik vervolgens op **Generate**. Wacht tot het succesbericht verschijnt en klik op **Sluiten**.

Stap 3. Download de CSR. Klik op **CSR downloaden**. Selecteer **TVS voor certificaatdoeleinden** en klik op **Downloaden**.

Stap 4. Verzend de MVO naar de certificaatautoriteit.

Stap 5. De certificeringsinstantie retourneert twee of meer bestanden voor de ondertekende certificaatketen. Upload de certificaten in deze volgorde:

- CA-basiscertificaat als TVS-trust. Navigeren naar **certificaatbeheer > Uploadcertificaat > Doel certificaat: TVS-trust**. Stel de beschrijving van het certificaat in en blader door het basiscertificaatbestand.
- Tussentijds certificaat als TVS-trust (optioneel). Navigeren naar **certificaatbeheer > Uploadcertificaat > Doel certificaat: TVS-trust**. Stel de beschrijving van het certificaat in en blader door het tussenliggende certificaatbestand.

Opmerking: Sommige CA's geven geen tussentijds certificaat, als alleen het basiscertificaat werd verstrekt, kan deze stap worden weggelaten.

- Door CA ondertekend certificaat als TVS. Navigeren naar **certificaatbeheer > Uploadcertificaat > Doel certificaat: TV**. Stel de beschrijving van het certificaat in en blader door het CA-ondertekende certificaatbestand voor het huidige CUCM-knooppunt.

Opmerking: Op dit punt vergelijkt CUCM de CSR en het geüploade CA-ondertekende certificaat. Als de informatie overeenkomt, verdwijnt de MVO en wordt het nieuwe CA-ondertekende certificaat geüpload. Als u een foutbericht ontvangt nadat het certificaat is geüpload, raadpleegt u de sectie **Gemeenschappelijke foutmeldingen** in **uploadcertificaat**.

Stap 6. Om het nieuwe certificaat op de server toegepast te krijgen, moeten de vereiste services opnieuw opgestart worden (alleen als de service draait en actief is). Navigeren naar:

- **Cisco Unified Servicability > Tools > Control Center - functieservices > Cisco TFTP** (Alle knooppunten waar de service wordt uitgevoerd)
- **Cisco Unified Service > Tools > Control Center - Netwerkservices > Cisco Trust Verification Service** (Alle knooppunten waar de service wordt uitgevoerd)

Stap 7. Reset alle telefoons:

- Ga naar **Cisco Unified CM Management > System > Enterprise Parameters > Reset**. Er verschijnt een pop-upvenster met de verklaring U staat op het punt alle apparaten in het systeem te resetten. Deze actie kan niet ongedaan worden gemaakt. Doorgaan? Selecteer **OK** en klik vervolgens op **Reset**.

Opmerking: Monitorapparaatregistratie via RTMT. Zodra alle telefoons registreren terug kunt u met het volgende certificaatype te werk gaan.

Probleemoplossing voor gebruikelijke geüploade certificaatfoutmeldingen

In deze sectie worden enkele van de meest voorkomende foutmeldingen weergegeven wanneer een CA-ondertekend certificaat is geüpload.

CA-certificaat is niet beschikbaar in de Trust-Store

Deze fout betekent dat het wortel- of tussencertificaat niet naar de CUCM is geüpload. Controleer of deze twee certificaten zijn geüpload als vertrouwensarchief voordat het servicecertificaat wordt geüpload.

Bestand /usr/local/platform/.security/tomcat/keys/tomcat.csr bestaat niet

Deze fout verschijnt wanneer een MVO niet bestaat voor het certificaat (tomcat, callmanager, ipsec, capf, tvs). Controleer of de MVO eerder is opgesteld en of het certificaat op basis van die MVO is opgesteld. Belangrijke punten in gedachten houden:

- Er kan slechts 1 MVO per server en certificaattype bestaan. Dat betekent dat als er een nieuwe MVO wordt gecreëerd, de oude vervangen wordt.
- Wildcard-certificaten worden niet ondersteund door CUCM.
- Het is niet mogelijk een servicecertificaat te vervangen dat momenteel van kracht is zonder een nieuwe MVO.
- Een andere mogelijke fout voor hetzelfde probleem is "Het bestand /usr/local/platform/upload/certs//tomcat.der kan niet worden geüpload." Dit hangt af van de CUCM-versie.

MVO Openbare sleutel en Certificaat Openbare sleutel komen niet overeen

Deze fout verschijnt wanneer het door CA verstrekte certificaat een andere openbare sleutel heeft dan die in het CSR-bestand wordt verzonden. Mogelijke redenen zijn:

- Het onjuiste certificaat (misschien van een ander knooppunt) is geüpload.
- Het CA-certificaat is gegenereerd met een andere MVO.
- De MVO werd geregenereerd en verving de oude MVO die werd gebruikt om het ondertekende certificaat te verkrijgen.


Om de MVO en certificaat openbare sleutel match te verifiëren, zijn er meerdere tools online zoals [SSL](#).

What to Check

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

Enter your Certificate:

```
Tj13aw4xMxDtj1DRFAsQ049UHVibGj1IwS2v5j1fwu2vYdmjzAMsQ049Uzvy
dmjZ0MsQ049Q29uZmindXjhdGhVbixEQz1jB2xsYWsREMs9bxg/Y2VydGimaWVh
dGV5ZXZvY2F0aW9uTGZldD9iYXNpZ9iaewjdENsYXNzPWw5TERpc3RyaWJ1dGlv
bilBvaW50MIG7BggBgEFBQcBAQ5BjCBqzCBqAYIKwYBBQUHMAKGZtsZGFwOi9v
L0NOPUNvbGxhYyUyMENBLENOPUFjQSkDj1QdWJsawMIMjBLZXIMjBTZjQzawVh
cyxDj1T2QzZWVhcyxDj1Db25maWd1cmF0aW9uLERDPWNvbGxhYXEQz1teD9j
QUlncnRpZmlyYXNpZ2h2L2UuL2JqZWN0Q2xhc3M9Y2VydGimaWVhSGVibkF1dGhv
cmliQTAhBgkrBgEEAYI3FAIEFB4SAFCAZQBIAFMAZQByAHYAZQByMAOGCSqGSib3
DQEBCWUAA4BAQCfG2Bc28CMxkunQavdYaUioDrfdPMLSA/7hisqW55x/bEQs
9LqyftmidCmkoMFPgK4t2vMie4oTpKBYAQvbrApG001mWV5u+f1Io9PvrygWtYl
D+ve7rMp8sirVo1Tmhe/25in3lbn+Ofwe5NuvCx3wNudLRR3904KcaFCcsVLQ6aw
PtmvAz/9K2GRhzaqcd9fVJuoWTKDj2Qsladcgsl5cvFMz3BBf0MjGBNX16jGiiQ
yZ2br6Gm4pa4yik6sUrcOxHyslomecYeRheKuSkuPusOeEwW5zj0QMT7P4Ww
ZBpT2TkrQdODAZHjGuJP+yBa75OGGTZWVvg1
-----END CERTIFICATE-----
```

 The certificate and CSR do NOT match!

✔ Certificate Hash:

684ad486131856ce0015d4b3e615e1ed
3b3bef6b8f590a493921661a4c4f62e9

✔ CSR Hash:

635f45c1ebcd876526a3133d1ee73d9a8
4544876fdbbc8dc3a4d8fed377dcc635

Enter your CSR:

```
q+hjgokSx+ogqVavFSNRdqTh0Grls1ga0pJ5sGxOOLCqAtQhEARNecGyanZtrK
gSjTQHfBjStD2vDyD3wg5iyhwnlqkMUl3IRD5qcSD/nyfLGLS8hB9y5HqtaDA3
1hwJ5Q4Rk2188ESCILtB3bAozEgZ05Vw4h5fP809e/CTWsxZtBfLgYtvcDGk
OGrdW2xLueUv2u29jvYmLD70CNxCM9XypLj6uuyMuf0BFh+s0F1Mr7gal3b
hXkS4ZjoFIMIXYBWSFDwexH7XFD+HqaPeM4Y50N4YqhxAgMBAAQgbzBtBqkqkIG
9w0BCQ4xyDBeMBOGA1UdjqQWMBQGCCSGAQUBwMBBggrBgEFBQcDAJALBgVHQBEB
BAMCBLAWMAYDVR0RBCKw4iOY3VjB55jB2xsYWVubXCFTEhXNB1Y15jdWVhLmNv
bGxhY5teDANBgkqhkiG9w0BAQsFAAOCQAQEAhBgli76T59rWxOFjsG7hsj36vf
ubcW7HGPrNyx6/pl9UydunR0KDXQtZzWWc9IOA3/fpcjrz+8LdHtr1FnnwBwCV
Yca9s0NwZsmU1+clbTH1H5g8FFoHAdg+FR3+1AE7GNfGK0CA0RipRihZPGzQ6dO
6ZTR5Q45LbcWxe4EZ05xjEQW7Zrkjfwby1GQKYg3CuXCETy3UunMCZnwjMnXkG0
n781nNdx7Ybgfz1IeY+ZozPHWgbu2HwChuH1bOAMUpkwiFebQZn9H+R7drjBAZR
IeXEYWL739M7BTveNmHoOnR6SkwvHYbb7iqDjnHxS9R0S052vUhkj7Hw==
-----END CERTIFICATE REQUEST-----
```

Een andere mogelijke fout voor hetzelfde probleem is "Het bestand /usr/local/platform/upload/certs//tomcat.der kan niet worden geüpload." Dit hangt af van de CUCM-versie.

MVO alternatieve naam (SAN) en certificaat SAN komt niet overeen

De SAN's tussen de CSR en het certificaat moeten hetzelfde zijn. Dit voorkomt certificering voor domeinen die niet zijn toegestaan. Voer de volgende stappen uit om de SAN-fout te verifiëren:

1. Decodeer de MVO en het certificaat (basis 64). Er zijn verschillende decoders online beschikbaar, zoals de [decoder](#).
2. Vergelijk de SAN-vermeldingen en controleer of ze allemaal overeenkomen. De volgorde is niet belangrijk, maar alle vermeldingen in de MVO moeten dezelfde zijn in het certificaat.

Het CA-ondertekende certificaat heeft bijvoorbeeld twee extra SAN-vermeldingen toegevoegd, de gemeenschappelijke naam van het certificaat en een extra IP-adres.

CSR Summary	
Subject: domain.com	
RDN	Value
Common Name (CN)	pub-ms.domain.com
Organizational Unit (OU)	Collaboration
Organization (O)	Cisco
Locality (L)	CUCM
State (ST)	CDMX
Country (C)	MX
Properties: domain.com	
Property	Value
Subject	CN = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX
Key Size	2048 bits
Fingerprint (SHA-1)	C3:87:05:CB:79:FE:88:4A:86:96:77:0A:C5:8B:63:27:55:3C:A4:84
Fingerprint (MD5)	CE:5C:9D:59:3F:8E:E3:26:C5:21:9D:A2:F1:CA:68:86
SANS	domain.com, sub.domain.com, pub.domain.com, imp.domain.com

Certificate Summary	
Subject	
RDN	Value
Common Name (CN)	pub-ms.domain.com
Organizational Unit (OU)	Collaboration
Organization (O)	Cisco
Locality (L)	CUCM
State (ST)	CDMX
Country (C)	MX
Properties	
Property	Value
Issuer	CN = Collab-CA,DC = collab,DC = mx
Subject	CN = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX
Valid From	17 Sep 2020, 1:24 a.m.
Valid To	17 Sep 2022, 1:24 a.m.
Serial Number	69:00:00:00:2D:5A:92:EB:EA:9A:85:65:C4:00:00:00:00:00:2D(2341578246081205845683969995281333940237893677)
CA Cert	No
Key Size	2048 bits
Fingerprint (SHA-1)	4E:15:F7:F3:9C:37:A9:8D:52:1A:6C:6D:4D:7D:AF:FE:08:EB:BD:0F
Fingerprint (MD5)	D8:22:33:92:5D:F7:7D:2A:D5:28:9D:2D:57:C0:F7:EC
SANS	pub-ms.domain.com, domain.com, sub.domain.com, pub.domain.com, imp.domain.com, 10.xx.xx.xx

3. Zodra u hebt vastgesteld dat het SAN niet overeenkomt, kunt u dit op twee manieren oplossen:

1. Vraag uw CA-beheerder om een certificaat uit te geven met exact dezelfde SAN-vermeldingen die in de CSR worden verzonden.
2. Maak een CSR in CUCM die voldoet aan de eisen van de CA.

U kunt de door de CUCM gemaakte MVO als volgt wijzigen:

1. Als CA het domein verwijdert, kan een CSR in CUCM worden gemaakt zonder het domein. Terwijl de creatie van MVO, verwijder het domein dat door gebrek wordt bevolkt.
2. Als een [multi-SAN-certificaat](#) wordt aangemaakt, zijn er bepaalde certificeringsinstanties die de "-ms" niet accepteren in de algemene naam. De "-ms" kan worden verwijderd uit de MVO wanneer deze wordt gecreëerd.

Generate Certificate Signing Request

Generate Close

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose** tomcat

Distribution* Multi-server(SAN)

Common Name* 115pub-ms [REDACTED]

Subject Alternate Names (SANs)

Auto-populated Domains

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

Parent Domain

Other Domains

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

Generate Close

3. Een andere naam toevoegen dan die welke automatisch door CUCM zijn ingevuld:

1. Als het Multi-SAN-certificaat wordt gebruikt, kan meer FQDN worden toegevoegd. (IP-adressen worden niet geaccepteerd.)

Generate Certificate Signing Request

Generate Close

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose** tomcat

Distribution* Multi-server(SAN)

Common Name* 115pub-ms [REDACTED]

Subject Alternate Names (SANs)

Auto-populated Domains

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

Parent Domain [REDACTED]

Other Domains

extrahostname.domain.com [REDACTED]

Choose File For more inform

Add

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

Generate Close

b. Als het certificaat één knooppunt is, gebruikt u de set web-security uit. Deze opdracht is zelfs van toepassing op multi-SAN-certificaten. (Elke vorm van domein kan worden toegevoegd, ook IP-adressen zijn toegestaan.)

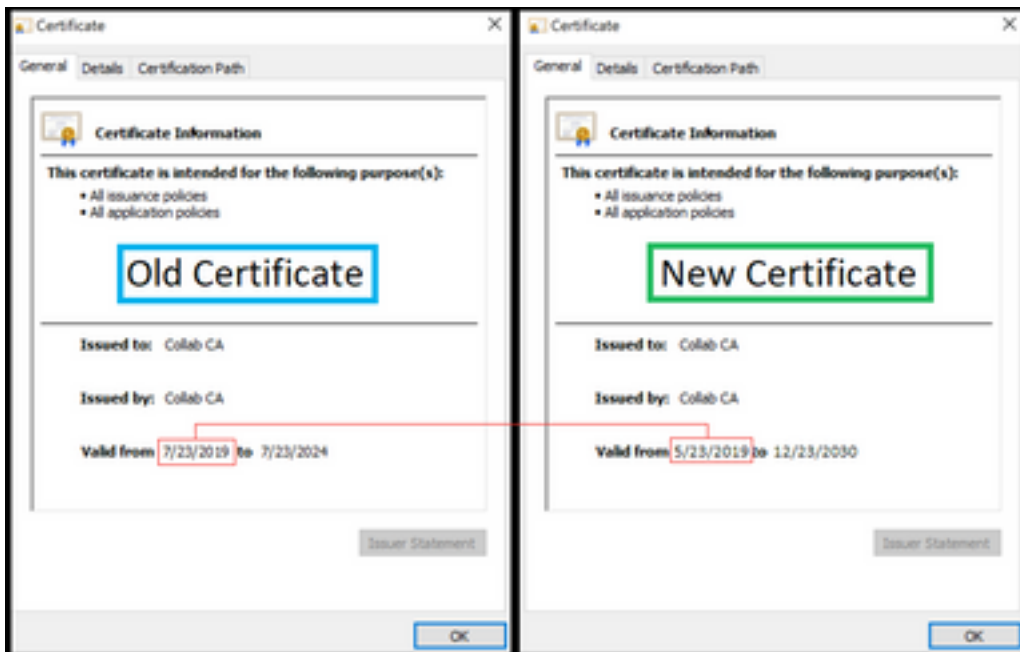
Zie de [Opdrachtlijnhandleiding voor](#) meer informatie.

Trustcertificaten met dezelfde GN worden niet vervangen

CUCM is ontworpen om slechts één certificaat met dezelfde algemene naam en hetzelfde certificaattype op te slaan. Dit betekent dat als een certificaat dat tomcat-trust is, reeds in de databank bestaat en moet worden vervangen door een nieuw certificaat met dezelfde GN, CUCM het oude certificaat verwijdert en vervangt door het nieuwe.

Er zijn enkele gevallen waarin CUCM het oude certificaat niet vervangt:

1. Het geüploade certificaat is verlopen: CUCM staat u niet toe om een verlopen certificaat te uploaden.
2. Het oude certificaat heeft een recentere "VANAF"-datum dan het nieuwe certificaat. CUCM houdt het meest recente certificaat en om een oudere "VAN" datum te hebben catalogiseert het als ouder. Voor dit scenario, is het noodzakelijk om het ongewenste certificaat te wissen en dan het nieuwe te uploaden.



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.