

Herstel CUCM IM/P Service zelfondertekende certificaten

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Gebruik van certificaatarchief](#)

[Cisco Unified Presence \(CUP\)-certificaat](#)

[Cisco Unified Presence - Uitbreidbaar certificaat voor Messaging and Presence Protocol \(CUP-XMPP\)](#)

[Cisco Unified Presence - Uitbreidbaar Messaging and Presence Protocol - Server-to-Server \(CUP-XMPP-S2S\) - certificaat](#)

[IP-beveiligingscertificaat \(IPSec\)](#)

[Tomcat Certificate](#)

[Certificaatregeneratieproces](#)

[CUP-certificaat](#)

[CUP-XMPP certificaat](#)

[CUP-XMPP-S2S-certificaat](#)

[IPsec-certificaat](#)

[Tomcat Certificate](#)

[Verlopen vertrouwenscertificaten verwijderen](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft een aanbevolen stapsgewijze procedure voor het regenereren van certificaten in CUCM IM/P 8.x en hoger.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de IM & Presence (IM/P) servicecertificaten.

Gebruikte componenten

De informatie in dit document is gebaseerd op IM/P release 8.x en hoger.

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.

Achtergrondinformatie

Gebruik van certificaatarchief

Cisco Unified Presence (CUP)-certificaat

Gebruikt voor beveiligde SIP-verbindingen voor SIP Federation, Microsoft Remote Call Control voor Lync/OCS/LCS, beveiligde verbinding tussen Cisco Unified Certificate Manager (CUCM) en IM/P, enzovoort.

Cisco Unified Presence - Uitbreidbaar certificaat voor Messaging and Presence Protocol (CUP-XMPP)

Wordt gebruikt om beveiligde verbindingen voor XMPP-clients te valideren wanneer een XMPP-sessie wordt gemaakt.

Cisco Unified Presence - Uitbreidbaar Messaging and Presence Protocol - Server-to-Server (CUP-XMPP-S2S) - certificaat

Gebruikt om beveiligde verbindingen te valideren voor XMPP interdomineifederaties met een extern gefedereerd XMPP-systeem.

IP-beveiligingscertificaat (IPSec)


Gebruikt voor:


- Valideren van beveiligde verbinding voor noodherstelsysteem (DRS)/noodherstelkader (DRF)
- Valideer beveiligde verbinding voor IPsec-tunnels naar Cisco Unified Communications Manager (CUCM) en IM/P-knooppunten in het cluster

Tomcat Certificate

Gebruikt voor:

- Valideren van verschillende webtoegang, zoals toegang tot servicepagina's van andere knooppunten in het cluster en Jabber Access.
- Valideren van beveiligde verbinding voor SAML Single Sign-On (SSO).
- Valideren van beveiligde verbinding voor Intercluster Peer.

 **Waarschuwing:** als u de SSO-functie op uw Unified Communications-servers gebruikt en de Cisco Tomcat-certificaten worden geregenereerd, moet de SSO opnieuw worden geconfigureerd met de nieuwe certificaten. De link om SSO op CUCM en ADFS 2.0 te configureren is: <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html>.

 **Opmerking:** de link naar CUCM-proces voor certificaatregeneratie/verlenging is: <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/200199-CUCM-Certificate-Regeneration-Renewal-Pr.html>.

Certificaatregeneratieproces

CUP-certificaat

Stap 1. Open een grafische gebruikersinterface (GUI) voor elke server in uw cluster. Start met de IM/P-uitgever, open vervolgens een GUI voor elke IM/P-abonneeserver en navigeer naar Cisco Unified OS Administration > Security > Certificate Management.

Stap 2. Begin met de uitgever GUI, en kies Find om alle certificaten te tonen. Kies het cup.pem certificaat. Eenmaal geopend, kies Regenerate en wacht tot u succes ziet voordat de pop-up wordt gesloten.

Stap 3. Ga verder met volgende abonnees, raadpleeg dezelfde procedure als in stap 2. en vul alle abonnees in uw cluster in.

Stap 4. Nadat het CUP-certificaat op alle knooppunten is geregenereerd, moeten de services opnieuw worden gestart.



Opmerking: als de configuratie van de Presence Redundancy Group de optie Hoge beschikbaarheid inschakelen heeft ingeschakeld, Uncheck doet u dit voordat de services opnieuw worden gestart. U hebt toegang tot de configuratie van de Presence Redundancy Group op CUCM Pub Administration > System > Presence Redundancy Group. Een herstart van de diensten veroorzaakt een tijdelijke stroomonderbreking van IM/P en moet buiten de productieuren worden gedaan.

Start de services in deze volgorde opnieuw:

- Log in op Cisco Unified Servicability van de uitgever:

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco SIP-proxy-service.

Restart c. Nadat de service is opgestart, gaat u verder met de abonnees en de Cisco SIP Proxy-service.

d. Begin met de uitgever en ga dan met de abonnees verder. Restart Cisco SIP Proxy-service (ook van Cisco Unified Serviceability > Tools > Control Center - Feature Services).

- Log in op Cisco Unified Servicability van de uitgever:

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco Presence Engine-service

c. Nadat de service is opgestart, gaat u verder met Restart het gebruik van Cisco Presence Engine Service op de abonnees.




Opmerking: indien geconfigureerd voor SIP Federation, Restart Cisco XCP SIP Federation Connection Manager service (zie Cisco Unified Serviceability > Tools > Control Center - Feature Services). Begin met de uitgever en ga dan door met de abonnees.


CUP-XMPP certificaat



Opmerking: aangezien Jabber de CUCM- en IM/P-Tomcat- en de CUP-XMPP-servercertificaten gebruikt om de verbindingen voor Tomcat en de CUP-XMPP-diensten te valideren, zijn deze CUCM- en IM/P-certificaten in de meeste gevallen CA-ondertekend. Stel dat het Jabber-apparaat niet beschikt over de hoofdmap en een tussenliggend certificaat dat deel uitmaakt van het CUP-XMPP-certificaat dat is geïnstalleerd in het vertrouwensarchief van het certificaat. In dat geval geeft de Jabber-client een veiligheidswaarschuwing weer



die verschijnt voor het onbetrouwbare certificaat. Als nog niet geïnstalleerd in het certificaat van het Jabber-apparaatvertrouwensarchief, moeten de wortel en elk tussenliggend certificaat naar het Jabber-apparaat worden geduwd door middel van groepsbeleid, MDM, e-mail enzovoort, dat afhankelijk is van de Jabber-client.



Opmerking: als het CUP-XMPP-certificaat zelf is ondertekend, verschijnt er een beveiligingswaarschuwing voor het onbetrouwbare certificaat als het CUP-XMPP-certificaat niet is geïnstalleerd in het vertrouwensarchief van het Jabber-apparaatcertificaat. Als het nog niet is geïnstalleerd, moet het zelf-ondertekende CUP-XMPP certificaat naar het Jabber apparaat worden geduwd door middel van groepsbeleid, MDM, e-mail, enzovoort, dat afhankelijk is van de Jabber-client.

Stap 1. Open een GUI voor elke server in uw cluster. Begin met de IM/P-uitgever, open vervolgens een GUI voor elke IM/P-abonneeserver en navigeer naar **Cisco Unified OS Administration > Security > Certificate Management**.


Stap 2. Begin met de uitgever GUI, en kies Find om alle certificaten te tonen. Bepaal uit de typekolm voor het cup-xmpp.pem certificaat of het zelfondertekend of CA-ondertekend is. Als het cup-xmpp.pem certificaat een door derden ondertekend (type CA-ondertekend) distributiemeer multi-SAN is, raadpleegt u deze link wanneer u een multi-SAN CUP-XMPP CSR genereert en bij CA een door CA ondertekend CUP-XMPP-certificaat indient; [Unified Communications Cluster Setup met CA-ondertekend multi-server subject Alternate Name Configuration Voorbeeld](#).

Als het cup-xmpp.pem certificaat een door een derde ondertekend (door CA ondertekend type) distributienetwerk met één knooppunt is (distributiennaam is de algemene naam voor het certificaat), raadpleegt u deze link wanneer u een CUP-XMPP CSR met één knooppunt genereert en bij CA een CA-ondertekend CUP-XMPP-certificaat indient; [Jabber Complete How-To Guide voor certificaatvalidatie](#). Als het cup-xmpp.pem certificaat zelf is ondertekend, gaat u verder met Stap 3.

Stap 3. Kies Find om alle certificaten te tonen en kies vervolgens het cup-xmpp.pem certificaat. Eenmaal geopend, kies Regenerate en wacht tot u succes ziet voordat de pop-up wordt gesloten.

Stap 4. Ga verder met volgende abonnees; raadpleeg dezelfde procedure in stap 2 en vul deze in voor alle abonnees in uw cluster.

Stap 5. Nadat het CUP-XMPP-certificaat op alle knooppunten is geregenereerd, moet de Cisco XCP-routerservice op de IM/P-knooppunten worden herstart.



Opmerking: als de configuratie van de Presence Redundancy Group High Availability inschakelen heeft ingeschakeld, Uncheck doet u dit voordat de service opnieuw wordt gestart. De configuratie van de Presence Redundancy Group is toegankelijk via CUCM Pub Administration > System > Presence Redundancy Group. Een herstart van de dienst veroorzaakt een tijdelijke stroomonderbreking van IM/P en moet buiten de productieuren worden gedaan.

· Log in op Cisco Unified Servicability van de uitgever:

- a. Cisco Unified Serviceability > Tools > Control Center - Network Services.
- b. Restart de Cisco XCP routerservice.
- c. Zodra het opnieuw opstarten van de service is voltooid, gaat u verder met Restart Cisco XCP routerservice op de abonnees.

CUP-XMPP-S2S-certificaat


Stap 1. Open een GUI voor elke server in uw cluster. Begin met de IM/P-uitgever, open vervolgens een GUI voor elke IM/P-abonneeserver en

navigeer naar Cisco Unified OS Administration > Security > Certificate Management.

Stap 2. Begin met de uitgever GUI, kies Find om alle certificaten te tonen, en kies het cup-xmpp-s2s.pem certificaat. Eenmaal geopend, kies Regenerate en wacht tot u succes ziet voordat de pop-up wordt gesloten.

Stap 3. Ga verder met volgende abonnees en raadpleeg dezelfde procedure in stap 2 en vul deze in voor alle abonnees in uw cluster.

Stap 4. Nadat het CUP-XMPP-S2S-certificaat op alle knooppunten is geregenereerd, moeten de services in de vermelde volgorde opnieuw worden gestart.

 **Opmerking:** als de configuratie van de Presence Redundancy Group High Availability inschakelen heeft ingeschakeld, Uncheck doet u dit voordat deze services opnieuw worden gestart. De configuratie van de Presence Redundancy Group kan worden geopend op CUCM Pub Administration > System > Presence Redundancy Group. Een herstart van de diensten veroorzaakt een tijdelijke stroomonderbreking van IM/P en moet buiten de productieuren worden gedaan.


· Log in op Cisco Unified Serviceability van de uitgever:


- a. Cisco Unified Serviceability > Tools > Control Center - Network Services.
- b. Restart de Cisco XCP routerservice.
- c. Nadat het opnieuw opstarten van de service is voltooid, gaat u verder met Restart de ondersteuning van Cisco XCP Router op de abonnees.

· Log in op Cisco Unified Serviceability van de uitgever:

- a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.
- b. Restart de Cisco XCP XMPP Federation Connection Manager-service.
- c. Nadat de herstart van de service is voltooid, gaat u verder met Restart de Cisco XCP XMPP Federation Connection Manager-service op de abonnees.

IPsec-certificaat

 **Opmerking:** het ipsec.pem certificaat in de CUCM-uitgever moet geldig zijn en aanwezig zijn in alle abonnees (CUCM- en IM/P-knooppunten) in het IPSec-vertrouwensarchief. Het ipsec.pem certificaat van de abonnee is niet aanwezig in de uitgever als IPSec vertrouwensopslag in een standaardplaatsing. Om de geldigheid te verifiëren, vergelijk de serienummers in het ipsec.pem certificaat van de CUCM-PUB met het IPSec-vertrouwen in de abonnees. Ze moeten overeenkomen.

 **Opmerking:** De DRS maakt gebruik van een op SSL gebaseerde communicatie tussen de Source Agent en de Local Agent voor verificatie en codering van gegevens tussen de CUCM-clusterknooppunten (CUCM- en IM/P-knooppunten). DRS maakt gebruik van de IPSec-certificaten voor de Public/Private Key-codering. Houd er rekening mee dat als u het IPSEC-bestand (hostname.pem) uit de pagina Certificaatbeheer verwijdert, DRS niet werkt zoals verwacht. Als u het IPSEC-vertrouwensbestand handmatig verwijdert, moet u ervoor zorgen dat u het IPSEC-certificaat uploadt naar de IPSEC-vertrouwensopslag. Raadpleeg voor meer informatie de Help-pagina voor certificaatbeheer in de CUCM-beveiligingshandleidingen.

Stap 1. Open een GUI voor elke server in uw cluster. Begin met de IM/P-uitgever, open vervolgens een GUI voor elke IM/P-abonneeserver en navigeer naar Cisco Unified OS Administration > Security > Certificate Management.

Stap 2. Begin met de uitgever GUI, en kies Find om alle certificaten te tonen. Choose het ipsec.pem certificaat. Eenmaal geopend, kies Regenerate en wacht tot u succes ziet voordat de pop-up wordt gesloten.


Stap 3. Ga verder met volgende abonnees en raadpleeg dezelfde procedure in stap 2 en vul deze in voor alle abonnees in uw cluster.


Stap 4. Nadat alle knooppunten het IPSEC-certificaat hebben geregenereerd, Restart dan deze diensten. Navigeer naar de Cisco Unified Servicability van de uitgever; Cisco Unified Serviceability > Tools > Control Center - Network Services.

a. Kies Restart voor de primaire service van Cisco DRF.

b. Nadat de service is herstart, kiest u Restart een lokale Cisco DRF-service op de uitgever en gaat u op elke abonnee verder met Restart de lokale service van Cisco DRF.

Tomcat Certificate

 **Opmerking:** omdat Jabber de CUCM Tomcat- en IM/P Tomcat- en CUP-XMPP-servercertificaten gebruikt om de verbindingen voor Tomcat- en CUP-XMPP-diensten te valideren, zijn deze CUCM- en IM/P-certificaten in de meeste gevallen CA-ondertekend. Veronderstel het apparaat Jabber niet de wortel en om het even welk tussentijds certificaat heeft dat deel van het certificaat Tomcat in zijn certificaatvertrouwensopslag wordt geïnstalleerd is. In dat geval geeft de Jabber-client een pop-up met een veiligheidswaarschuwing weer voor het onbetrouwbare certificaat. Als nog niet geïnstalleerd in het certificaatvertrouwensarchief van het Jabber-apparaat, moeten de wortel en elk tussenliggend certificaat naar het Jabber-apparaat worden geduwd via groepsbeleid, MDM, e-mail enzovoort, dat afhankelijk is van de Jabber-client.

 **Opmerking:** Als het Tomcat-certificaat zelf is ondertekend, geeft de Jabber-client een veiligheidswaarschuwing voor het onbetrouwbare certificaat weer, als het Tomcat-certificaat niet is geïnstalleerd in het certificaatvertrouwensarchief van het Jabber-apparaat. Als het Jabber-apparaat nog niet is geïnstalleerd in het certificaatvertrouwensarchief, moet het zelfondertekende CUP-XMPP-certificaat naar het Jabber-apparaat worden gedrukt via groepsbeleid, MDM, e-mail enzovoort, dat afhankelijk is van de Jabber-client.

Stap 1. Open een GUI voor elke server in uw cluster. Begin met de IM/P-uitgever, open vervolgens een GUI voor elke IM/P-abonneeserver en navigeer naar Cisco Unified OS Administration > Security > Certificate Management.

Stap 2. Begin met de uitgever GUI, en kies Find om alle certificaten te tonen.

· Bepaal vanuit de kolom Type voor hettomcat.pem certificaat of het zelfondertekend of CA-ondertekend is.

· Als het tomcat.pem certificaat een door derden ondertekend (type CA-ondertekend) distributiemeer multi-SAN is, bekijk dan deze link over hoe u een multi-SAN Tomcat CSR kunt genereren en stuur naar CA voor een CA-ondertekend Tomcat-certificaat, [Unified Communications Cluster Setup met CA-ondertekend multi-server Onderwerp Alternate Name Configuratie Voorbeeld](#)

Opmerking: de multi-SAN Tomcat CSR wordt gegenereerd op de CUCM-uitgever en wordt gedistribueerd naar alle CUCM- en IM/P-knooppunten in het cluster.

· Als het tomcat.pem certificaat een door een derde ondertekende (door CA ondertekende) distributiernaam is (distributiernaam is gelijk aan de algemene naam voor het certificaat), bekijk dan deze link om een single-node CUP-XMPP CSR te genereren, en dien het in bij CA voor CA-ondertekend CUP-XMPP certificaat, [Jabber Complete How-To Guide voor certificaatvalidatie](#)

· Als het tomcat.pem certificaat zelf is ondertekend, gaat u verder met Stap 3

Stap 3. Kies Find om alle certificaten weer te geven:

· Kies het tomcat.pem certificaat.

· Eenmaal geopend, kies Regenerate en wacht tot u de succes pop-up ziet voordat de pop-up wordt gesloten.

Stap 4. Ga verder met elke volgende abonnee, raadpleeg de procedure in stap 2 en vul alle abonnees in uw cluster in.

Stap 5. Nadat alle knooppunten het Tomcat-certificaat hebben geregenereerd, Restart de Tomcat-service op alle knooppunten. Begin met de uitgever, gevolgd door de abonnees.

· Om de Tomcat-service te kunnen Restart gebruiken, moet u een CLI-sessie voor elke knooppunt openen en de opdracht uitvoeren totdat de service Cisco Tomcat opnieuw start, zoals in de afbeelding:

```
admin:
admin:utils service restart Cisco Tomcat
Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

Verlopen vertrouwenscertificaten verwijderen



Opmerking: vertrouwenscertificaten (die eindigen in -trust) kunnen indien nodig worden verwijderd. Vertrouwelijke certificaten die kunnen worden verwijderd zijn certificaten die niet langer nodig zijn, zijn verlopen of verouderd zijn. Verwijder de vijf identiteitsbewijzen niet: de cup.pem , cup-xmpp.pem , cup-xmpp-s2s.pem , ipsec.pem en tomcat.pem certificaten. De service herstart, zoals getoond, is ontworpen om alle in-memory informatie van deze legacy certificaten binnen die services te wissen.

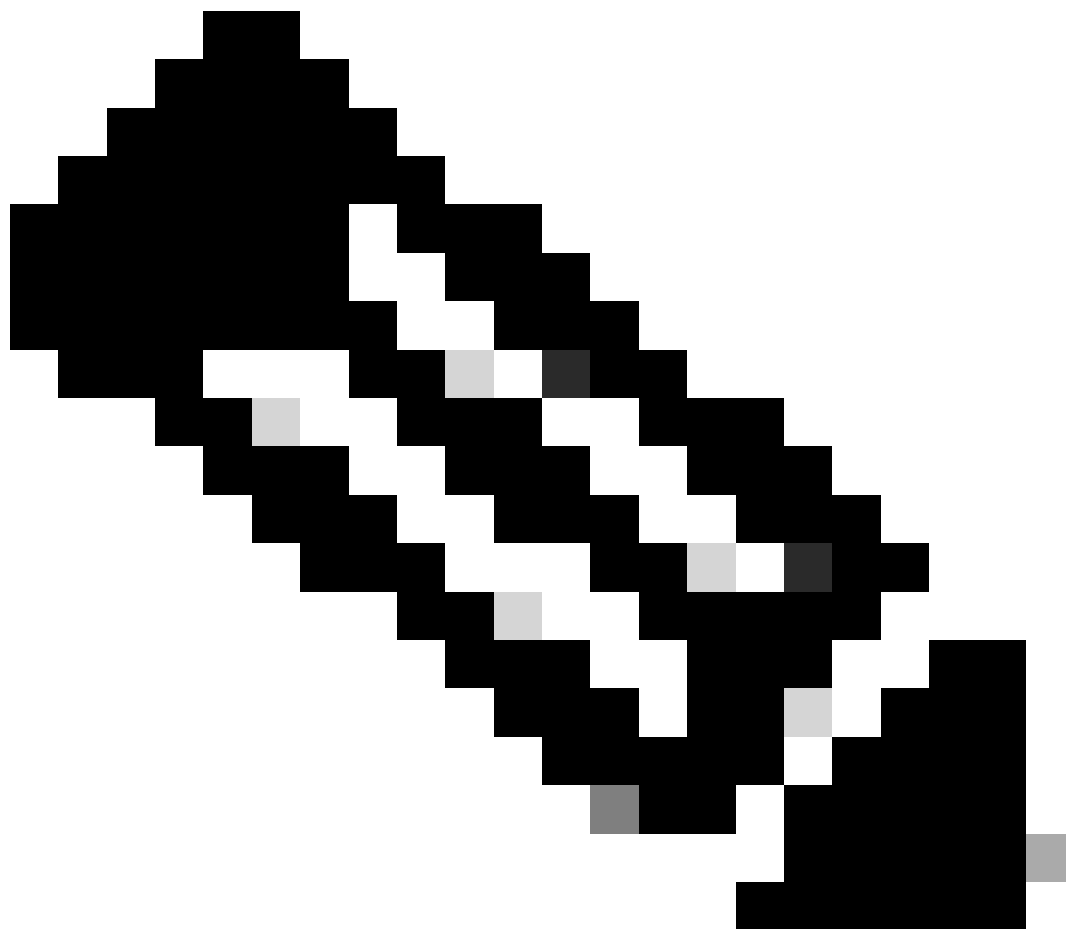


Opmerking: als de configuratie van de Presence Redundancy Group Hoge beschikbaarheid inschakelen heeft ingeschakeld, Uncheck dit voordat een service Stopped/Started of Restartedis ingeschakeld. De configuratie van de Presence Redundancy Group is toegankelijk via CUCM Pub Administration > System > Presence Redundancy Group. Een herstart van sommige van de diensten, zoals getoond, veroorzaakt een tijdelijke stroomonderbreking van IM/P en moet buiten de productieuren worden gedaan.

Stap 1. Navigeer naar Cisco Unified Serviceability > Tools > Control Center - Network Services:

· Kies in het vervolgkeuzemenu uw IM/P-uitgever, kies Stop uit Cisco Certificate Expiry Monitor, gevolgd door Stop in Cisco Intercluster Sync Agent.

· Herhaal Stop deze services voor elke IM/P-knooppunt in uw cluster.



Opmerking: Als het Tomcat-trust certificaat moet worden verwijderd, navigeer dan naar Cisco Unified Serviceability > Tools > Control Center - Network Services de CUCM-uitgever.

-
- Kies in de vervolgkeuzelijst de CUCM-uitgever.
 - Kies Stop uit de Cisco-monitor voor het verlopen van het certificaat, gevolgd door Stop een melding van de wijziging van het Cisco-certificaat.
 - Herhaal dit voor elke CUCM-knooppunt in uw cluster.

Stap 2. Navigeer naar Cisco Unified OS Administration > Security > Certificate Management > Find.

- Vind de verlopen vertrouwenscertificaten (voor versies 10.x en hoger, kunt u filteren op Vervaldatum. Van versies eerder dan 10.0 moet u de specifieke certificaten handmatig of via de RTMT-waarschuwingen (indien ontvangen) identificeren.
- Hetzelfde vertrouwenscertificaat kan in meerdere knooppunten verschijnen, het moet afzonderlijk van elke knooppunt worden verwijderd.

· Kies het vertrouwenscertificaat dat moet worden verwijderd (op basis van de versie, krijgt u een pop-up of u wordt naar het certificaat op dezelfde pagina navigeren).

· Kies Delete (u krijgt een pop-up die begint met "u staat op het punt dit certificaat permanent te verwijderen...").

•Klik op de knop OK.

Stap 3. Herhaal het proces voor elk vertrouwenscertificaat dat moet worden verwijderd.

Stap 4. Na voltooiing moeten diensten die rechtstreeks verband houden met de verwijderde certificaten, opnieuw worden gestart.

· CUP-trust: Cisco SIP proxy, Cisco Presence Engine en indien geconfigureerd voor SIP Federation, Cisco XCP SIP Federation Connection Manager (zie sectie CUP-certificaat)

· CUP-XMPP-trust: Cisco XCP router (zie sectie CUP-XMPP certificaat)

· CUP-XMPP-S2S-trust: Cisco XCP router en Cisco XCP XMPP Federation Connection Manager

· IPsec-trust: lokale DRF-bron/DRF (zie sectie IPsec-certificaat)

· Tomcat-trust: herstart Tomcat Service via de opdrachtregel (zie Tomcat certificaat sectie)

Stap 5. Herstartservices gestopt in stap 1.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

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.