

Unified Communications Cluster instellen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Verifiëren](#)

[CallManager SAN-certificaat voor meerdere servers](#)

[Problemen oplossen](#)

[Bekende voorbehouden](#)

Inleiding

In dit document wordt beschreven hoe u een Unified Communications Cluster kunt instellen met de door de Use Certificate Authority (CA) ondertekende SAN-certificaten voor meerdere servers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Communications Manager (CUCM)
- CUCM IM en Presence versie 10.5

Zorg er voordat u deze configuratie probeert voor dat deze services zijn ingesteld en functioneel zijn:

- Cisco-webservice voor platform-beheer
- Cisco Tomcat-service

Als u deze services op een webinterface wilt controleren, navigeert u naar **Cisco Unified Servicability Page Services > Network Service > Selecteer een server**. Om ze op de CLI te controleren, voert u de opdracht **Lijst met hulpprogrammatuur** in.

Als SSO in het CUCM-cluster is ingeschakeld, moet het opnieuw worden uitgeschakeld en ingeschakeld.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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

In CUCM Versie 10.5 en hoger kan dit certificaat van vertrouwensopslag Signing Aanvraag (CSR) Onderwerp Alternatieve Naam (SAN) en alternatieve domeinen omvatten.

1. Tomcat - CUCM en IM&P
2. Cisco CallManager - alleen CUCM
3. Cisco Unified Presence-Extended Messaging and Presence Protocol (CUP-XMPP) - alleen voor IM&P
4. CUP-XMPP server-to-server (S2S) - alleen IM&P



Het is eenvoudiger om een CA-ondertekend certificaat in deze versie te verkrijgen. Er hoeft slechts één CSR te worden ondertekend door CA in plaats van de verplichting om van elk serverknooppunt een CSR te verkrijgen en vervolgens een CA-ondertekend certificaat voor elke CSR te verkrijgen en deze individueel te beheren.

Configureren


Stap 1.

Log in bij de Publisher's Operating System (OS) Administration en navigeer naar **Security > Certificaatbeheer > Generate CSR**.

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*

Distribution*


Common Name*

Subject Alternate Names (SANs)

Parent Domain

Key Length*



Hash Algorithm*

 *- indicates required item.


Stap 2.

Kies een SAN met meerdere servers in distributie.

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*

Distribution*


Common Name*

Subject Alternate Names (SANs)

Parent Domain

Key Length*



Hash Algorithm*

 *- indicates required item.

De SAN-domeinen en het parent-domein worden automatisch ingevuld.

Controleer of alle knooppunten van uw cluster zijn opgenomen voor Tomcat: alle CUCM- en IM&P-knooppunten voor CallManager: alleen CUCM-knooppunten zijn vermeld.

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*

Distribution*

Common Name*

Subject Alternate Names (SANs)

Auto-populated Domains

cs-ccm-pub.com
cs-ccm-sub.com
cs-imp.com

Parent Domain

Other Domains


--

No file selected.

Please import .TXT file only.
For more information please refer to the notes in the Help Section

Key Length*



Hash Algorithm*

 *- indicates required item.

Stap 3.

Klik op Genereren en controleer na het genereren van de CSR of alle in de CSR genoemde knooppunten ook worden weergegeven in de lijst met succesvolle CSR-exportproducten.

Generate Certificate Signing Request

 Generate  Close

Status



Success: Certificate Signing Request Generated



CSR export operation successful on the nodes [cs-ccm-sub.com, cs-ccm-pub.com, cs-imp.com].

Bij certificaatbeheer wordt de SAN-aanvraag gegenereerd:

Certificate List (1 - 15 of 15)						
Find Certificate List where Certificate begins with tomcat Find Clear Filter + -						
Certificate ^	Common Name	Type	Key Type	Distribution	Issued By	
tomcat	115pub-ms-██████████	CSR Only	RSA	Multi-server(SAN)	--	
tomcat	115pub-ms-██████████	CA-signed	RSA	Multi-server(SAN)	██████████	

Stap 4.

Klik op **CSR downloaden** en kies het doel van het certificaat en klik op **CSR downloaden**.

The screenshot shows the Cisco Unified Operating System Administration interface. At the top, there is a navigation menu with options like Show, Settings, Security, Software Upgrades, Services, and Help. Below this, the 'Certificate List' section is visible, with a 'Download CSR' button highlighted in a red box. Below the main interface, a 'Download Certificate Signing Request' dialog box is open. It contains a warning icon and the message: 'Certificate names not listed below do not have a corresponding CSR'. There is a dropdown menu for 'Certificate Purpose*' with 'tomcat' selected. At the bottom of the dialog, there are 'Download CSR' and 'Close' buttons. A note at the bottom left states: '*- indicates required item.'

Het is mogelijk om de lokale CA of een externe CA zoals VeriSign te gebruiken om de CSR (Bestand gedownload in de vorige stap) te laten ondertekenen.

Dit voorbeeld laat de configuratiestappen zien voor een Microsoft Windows Server-gebaseerde CA. Als u een andere CA of een externe CA gebruikt, gaat u naar Stap 5.

Log in op <https://<windowsserveradres>/certsrv/>

Kies **Certificaat aanvragen > Geavanceerd certificaataanvragen**.

Kopieer de inhoud van het CSR-bestand naar het veld Base-64-encoded certificate request en klik op **Submit**.

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Leg het MVO verzoek zoals hier getoond voor.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded
certificate request
(CMC or
PKCS #10 or
PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBIjCCAGCQAGv9bQWCAZBgPYSATAK3OHqaw
BARDQwckBqVwEA1YVQOZEFEXK9jzE0BkGALTE
Cyl1Ez0t0FV1LnLnCjFuay5jEj0c0K0TFRBqBY
N0B1ZK5M0G0Rd1Z0B5Z0Q0N01H0A1Y1L0W1X
N0T1Y0gR1N0G0C3q0R1N0C0R0A0A01R0N0g0gR
< >
```

Additional Attributes:

Attributes

< >

Submit >

Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

Your Request Id is 32.

Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with this web browser within 10 days to retrieve your certificate

Stap 5.

Opmerking: Voordat u een Tomcat-certificaat uploadt, moet u controleren of SSO uitgeschakeld is. Als deze optie is ingeschakeld, moet SSO worden uitgeschakeld en opnieuw worden ingeschakeld zodra alle regeneratieproces van het Tomcat-certificaat is voltooid.

Met het getekende certificaat, upload de CA-certificaten als tomcat-trust. Eerst het basiscertificaat en dan het tussenliggende certificaat als het bestaat.

The screenshot shows the Cisco Unified Operating System Administration interface. The page title is "Certificate List". Below the title, there are four buttons: "Generate Self-signed", "Upload Certificate/Certificate chain", "Generate CSR", and "Download CSR". The "Upload Certificate/Certificate chain" button is highlighted with a red rectangle.

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* tomcat-trust

Description(friendly name)

Upload File Choose File certchain.p7b

Upload Close

Stap 6.

Upload nu het door CUCM ondertekende certificaat als Tomcat en controleer of alle knooppunten van uw cluster zijn vermeld in de "succesvolle handeling voor het uploaden van certificaten" zoals getoond in de afbeelding:

Upload Certificate/Certificate chain

Upload Close

Status

i Certificate upload operation successful for the nodes cs-ccm-pub.com,cs-ccm-sub.com,cs-imp.com.

i Restart Cisco Tomcat Service for the nodes cs-ccm-pub.com,cs-ccm-sub.com,cs-imp.com using the CLI "utils service restart Cisco Tomcat".

Upload Certificate/Certificate chain

Certificate Purpose* tomcat

Description(friendly name) Self-signed certificate

Upload File Browse... No file selected.

Upload Close

i *- indicates required item.

SAN met meerdere servers wordt in certificaatbeheer vermeld zoals in het afbeelding:

ipsecc-trust	cs-csm-pub.100000.com	Self-signed	cs-csm-pub.100000.com	cs-csm-pub.100000.com	04/18/2019	Trust Certificate
ITLRecovery	ITLRECOVERY.cs-csm-pub.vasank.com	Self-signed	ITLRECOVERY.cs-csm-pub.100000.com	ITLRECOVERY.cs-csm-pub.100000.com	04/18/2019	Self-signed certificate generated by system
tomcat	cs-csm-pub.100000.com.ms	CA-signed	Multi-server(SAN)	100000-DC1-CA	12/19/2015	Certificate Signed by 100000-DC1-CA
tomcat-trust	cs-csm-pub.100000.com.ms	CA-signed	Multi-server(SAN)	100000-DC1-CA	12/19/2015	Trust Certificate
tomcat-trust	cs-csm-pub.100000.com	Self-signed	cs-csm-pub.100000.com	cs-csm-pub.100000.com	04/21/2019	Trust Certificate
tomcat-trust	VeriSign Class 3 Secure Server CA - G3	CA-signed	VeriSign Class 3 Secure Server CA - G3	VeriSign Class 3 Public Primary Certification Authority - G5	02/08/2020	Trust Certificate
tomcat-trust	dc1-csm-pub.100000.com	Self-signed	dc1-csm-pub.100000.com	dc1-csm-pub.100000.com	04/17/2019	Trust Certificate
tomcat-trust	dc1-csm-pub.100000.com	Self-signed	dc1-csm-pub.100000.com	dc1-csm-pub.100000.com	04/18/2019	Trust Certificate
tomcat-trust	100000-DC1-CA	Self-signed	100000-DC1-CA	100000-DC1-CA	04/29/2064	Root CA
TVS	cs-csm-pub.vasank.com	Self-signed	cs-csm-pub.100000.com	cs-csm-pub.100000.com	04/18/2019	Self-signed certificate generated by system

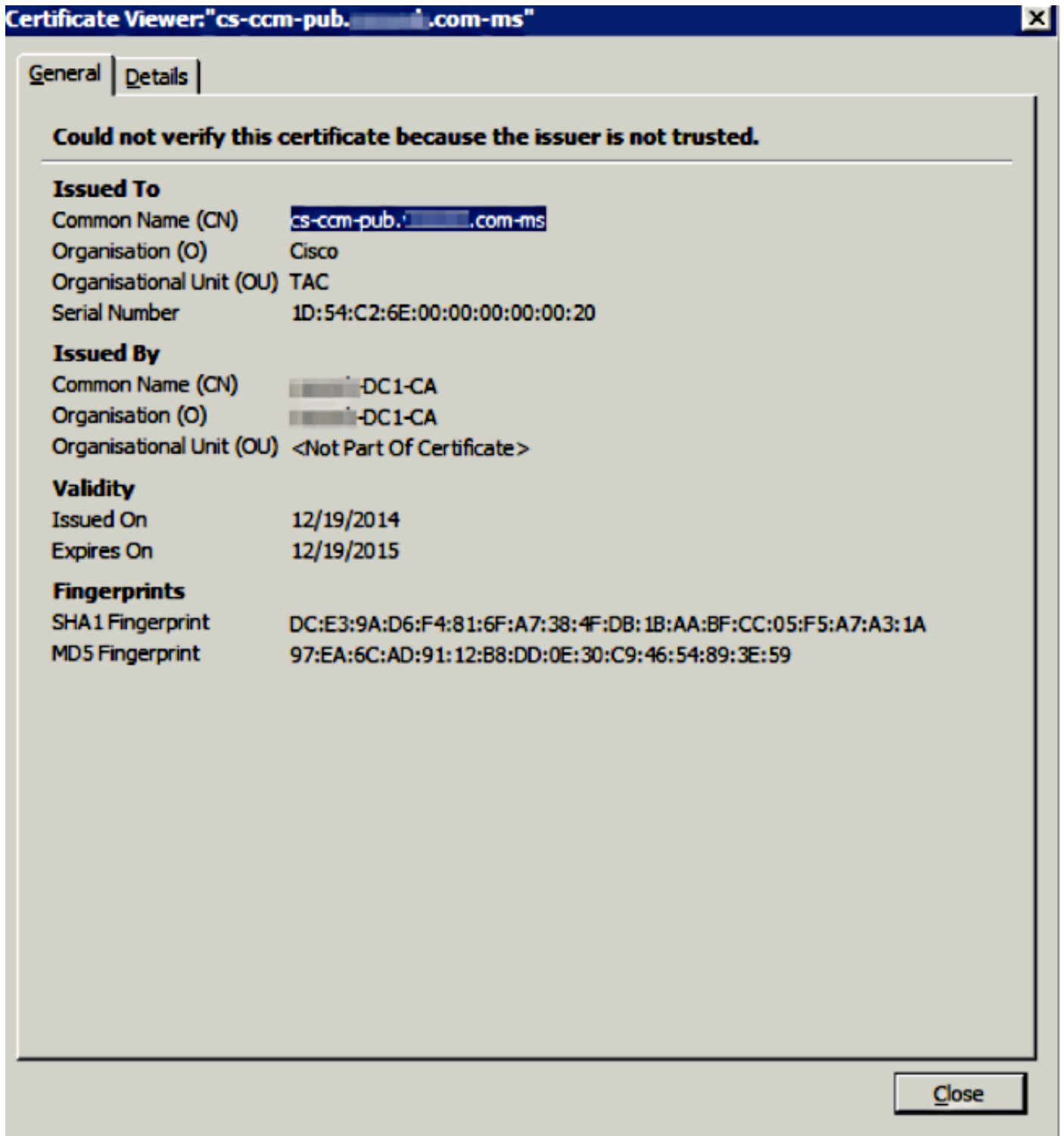
Stap 7.

Start de Tomcat-service opnieuw op alle knooppunten in de SAN-lijst (eerst uitgever en vervolgens abonnees) via CLI met de opdracht: **start Cisco Tomcat opnieuw op vanaf serviceniveau van Utils.**

```
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:
```

Verifiëren

Log in op <http://<fqdnofcsm>:8443/ccmadmin> om er zeker van te zijn dat het nieuwe certificaat wordt gebruikt.



CallManager SAN-certificaat voor meerdere servers

Een soortgelijke procedure kan worden gevolgd voor het CallManager-certificaat. In dit geval zijn de automatisch gevulde domeinen alleen CallManager-knooppunten. Als de Cisco CallManager-service niet wordt uitgevoerd, kunt u ervoor kiezen om deze in de SAN-lijst te houden of te verwijderen.

Waarschuwing: dit proces heeft gevolgen voor de registratie van gesprekken en de verwerking van gesprekken. Zorg ervoor dat u een onderhoudsvenster inplant voor elk werk met CUCM/TVS/ITL/CAPF-certificaten.

Zorg er vóór het door CA ondertekende SAN-certificaat voor CUCM voor dat:

- De IP-telefoon kan vertrouwen op de Trust Verification Service (TVS). Dit kan worden geverifieerd met toegang tot alle HTTPS-diensten via de telefoon. Bijvoorbeeld, als Corporate Directory toegang werkt, dan betekent het dat de telefoon vertrouwt op TVS-service.
- Controleer of het cluster zich in de niet-beveiligde of de gemengde modus bevindt.

Kies deze optie om te bepalen of het een cluster met gemengde modus is **Cisco Unified CM Management > System > Enterprise Parameters > Cluster Security Mode (0 == niet-beveiligd; 1 == Gemengde modus)**.

Waarschuwing: als u zich in een gemengde cluster bevindt voordat de services opnieuw worden gestart, moet de CTL worden bijgewerkt: [Token](#) of [Tokenless](#).

Nadat u het certificaat hebt geïnstalleerd dat door CA is afgegeven, moet de volgende lijst met services opnieuw worden gestart in de knooppunten die zijn ingeschakeld:

- Cisco Unified Servicability > Tools > Control Center - functieservices > Cisco TFTP
- Cisco Unified Service > Tools > Control Center - functieservices > Cisco CallManager
- Cisco Unified Service > Tools > Control Center - functieservices > Cisco CTIM Manager
- Cisco Unified Service > Tools > Control Center - netwerkservices > Cisco Trust Verification Service

Problemen oplossen

Deze logbestanden kunnen het Cisco Technical Assistance Center helpen om problemen met betrekking tot het genereren en uploaden van een CA-ondertekend certificaat van een SAN met meerdere servers te identificeren.

- Cisco Unified IOS-platform API
- Cisco Tomcat
- IP-platform CertMgr-logbestanden
- [Procedure voor verlenging van het certificaat](#)

Bekende voorbehouden

- Cisco bug ID [CSCur97909](#) - Multiserver cert uploaden verwijdert niet zelf ondertekende certs in DB
- Cisco bug-id [CSCus47235](#) - CUCM 10.5.2 kan niet worden gedupliceerd in SAN voor CSR
- Cisco bug ID [CSCup2852](#) - telefoon elke 7 minuten opnieuw ingesteld vanwege bepaalde update wanneer u multi-server cert gebruikt

Als er een bestaand certificaat voor meerdere servers is, wordt regeneratie in deze scenario's aanbevolen:

- Hostnaam of domein wijzigen. Wanneer een hostname of domeinwijziging wordt uitgevoerd, worden de certificaten automatisch opnieuw gegenereerd als zelfondertekend. Als u de afbeelding wilt wijzigen in een CA-handtekening, moet u de voorgaande stappen volgen.
- Als er een nieuw knooppunt aan het cluster is toegevoegd, moet er een nieuwe MVO worden

gegenereerd om het nieuwe knooppunt op te nemen.

- Wanneer een abonnee is hersteld en er geen back-up is gebruikt, kan de knooppunt nieuwe zelfondertekende certificaten hebben. Er kan een nieuwe MVO voor het volledige cluster vereist zijn om de abonnee op te nemen. (Er is een uitbreidingsaanvraag Cisco bug-id [CSCuv75957](#) deze functie toevoegen.)

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.