

Vereisten voor certificaten voor mobiele en externe toegang en ATS-geschiedenis begrijpen

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Op Expressway versie 14.0.2](#)

[Gedrag op eerdere versies tot 14.0.8](#)

[Gedrag op versies 14.0.8 en hoger](#)

[Deel](#)

[Gedrag op versies x15.3](#)

[Wat te verwachten wanneer Callmanager één certificaat deelt met meerdere services](#)

[Stappen voor hergebruik certificaat](#)

[Versiegeschiedenis van Apache Traffic Server](#)

Inleiding

Dit document beschrijft de vereisten voor het uploaden van certificaten voor CUCM voor mobiele en externe toegang.

Achtergrondinformatie

De Cisco Expressway maakt gebruik van de Apache Traffic Server (ATS). De verkeersserver is een zeer belangrijk onderdeel in traversal-oplossingen, voornamelijk gebruikt voor deze functies:

- Certificaatverificatie: het voert certificaatverificatie uit van Cisco Unified Communications Manager (CUCM), IM & Presence en Unity-serverknooppunten voor MRA-services.
- Proxying en caching: Het fungeert als een snelle, schaalbare caching proxy server voor HTTP / HTTPS-verkeer.

Op Expressway versie 14.0.2

Verkeersserver (ATS) begint een lichte handhaving van 'certificaatverificatie' te zien wanneer het met CUCM praat tijdens MRA-provisioning.

De vereiste is gedocumenteerd onder [CSCvz45074](#) waarbij de basiscertificaten die de Expressway Core-servercertificaten hebben ondertekend, op CUCM moeten worden geüpload als Tomcat-Trust en Callmanager Trust: <https://cdetsng.cisco.com/summary/#/defect/CSCvz45074>.

- Verkeersserver dwingt certificaatverificatie af.
- Voordat u een upgrade uitvoert naar de X14.0.2-versie, moet u ervoor zorgen dat aan deze

certificaatvereiste wordt voldaan.

Vereiste - De CA-keten (Root + Intermediary) die het Expressway-C-certificaat heeft ondertekend, moet worden toegevoegd aan de lijst met tomcat-trust en CallManager-trust van CUCM, zelfs als de Unified Communications Manager (UCM) zich in een niet-beveiligde modus bevindt.

Reden - De verkeersserverservice in Expressway verzendt het certificaat wanneer een server-UCM daarom vraagt. Deze verzoeken hebben betrekking op diensten die worden uitgevoerd op andere poorten dan 8443 (bijvoorbeeld poorten 6971, 6972, enzovoort). Dit dwingt certificaatverificatie af, zelfs als UCM zich in de niet-beveiligde modus bevindt. Zie de [Implementatiehandleiding voor mobiele en externe toegang via Expressway voor](#) meer informatie.

Gedrag op eerdere versies tot 14.0.8

De verkeersserver op Expressway-C die beveiligde HTTPS-bidirectionele verbindingen tussen Expressway-C en Unified Communication-knooppunten afhandelt, heeft het certificaat dat werd gepresenteerd door het externe einde niet geverifieerd. Onder MRA-configuratie is er een optie om TLS-certificaatverificatie door de configuratie van de TLS-verificatiemodus in 'Aan' te zetten wanneer CUCM-, IM&P- of Unity-servers worden toegevoegd onder Configuratie > Unified Communications > Unified CM-servers/IM- en Presence Service-knooppunten/Unity Connection-servers. De configuratieoptie wordt weergegeven in de volgende schermafbeelding, die aangeeft dat de FQDN of IP in het SAN wordt geverifieerd, evenals de geldigheid van het certificaat en of het is ondertekend door een vertrouwde CA.

Er was ook een bekend probleem waarbij twee certificaten met dezelfde GN-naam niet kunnen worden geladen in de Expressway-vertrouwenswinkel. Deze beperking veroorzaakte twee problemen:

1. Als u ervoor kiest om het certificaat voor gespreksbeheer in de Expressway Trust-winkel te laden, mislukt TLS-verificatie 'Aan' bij het toevoegen van CUCM's.
- 2: Als u ervoor kiest om het Tomcat-certificaat in de Expressway Trust-winkel te laden, mislukken beveiligde sip-registraties op 5061.

Dit gedrag is gedocumenteerd in [CSCwa12894](#).

Deze verificatie van het TLS-certificaat wordt ook alleen uitgevoerd bij de detectie van de CUCM/IM&P/Unity-servers en niet op het moment dat de MRA-client wordt geleverd.

Het nadeel van deze configuratie is dat deze alleen wordt geverifieerd voor het adres van de uitgever dat u toevoegt. Het valideert niet of het certificaat op de abonneeknooppunten correct is ingesteld omdat het de abonneeknoopinformatie (FQDN of IP) ophaalt uit de database van de uitgeversknooppunt.

CISCO Cisco Expressway-C

Status > System > Configuration > Applications > Users > Maintenance >

This system has 0 alarms

You are here: Configuration > Unified Communications > Unified CM servers > Edit

Unified CM servers

Warning: The CSRF Protection status is automatically enabled after the software upgrade. We recommend keeping CSRF protection Enabled. To change it, please log in to the CLI.

Unified CM server lookup

Unified CM publisher address: cucmpubnew.lomcat.com

Username: comradmin

Password: *****

TLS verify mode: On

Deployment: lomcat.com

AES GCM support: Off

SIP UPDATE for session refresh: Off

ICE Passthrough support: Off

Save Delete Cancel

Currently found Unified CM nodes				
Name	UCM Version	Zone Protocol	Zone Status	Role
10.106.79.106	15.0.1.12960(234)	TCP	TCP Address resolvable	Subscriber
**10.106.79.102	15.0.1.12960(234)	TCP	TCP Address resolvable	Publisher

Information

If TLS verify mode is enabled, the Unified CM system's FQDN or IP address must be contained within the X.509 certificate presented by that system (in either the Subject Common Name or the Subject Alternative Name attributes of the certificate). The certificate itself must also be valid and signed by a trusted certificate authority.

Default: On

Gedrag op versie 14.0.8 en hoger

Vanaf versie X14.0.8 voert de Expressway-server TLS-certificaatverificatie uit voor elke afzonderlijke HTTPS-aanvraag die via de verkeersserver wordt gedaan. Dit betekent dat het ook dit uitvoert wanneer de TLS Verify Mode is ingesteld op 'Off' tijdens de detectie van de CUCM/IM&P/Unity nodes. Wanneer de verificatie niet slaagt, wordt de TLS-handshake niet voltooid en mislukt het verzoek, wat kan leiden tot verlies van functionaliteit, zoals redundantie, failover-problemen of volledige aanmeldingsfouten. Ook, met TLS Verify Mode ingesteld op 'On', garandeert het niet dat alle verbindingen goed werken zoals in het voorbeeld later wordt behandeld.

De exacte certificaten die de Expressway controleert in de richting van de CUCM/IM&P/Unity-knooppunten zijn zoals weergegeven in het gedeelte van de [MRA-gids](#).

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-0/mra/exwy_b_mra-deployment-guide-x150.pdf

Deel

Certificaatvereisten > Certificaatuitwisselingsvereisten

Vanwege deze veranderingen in de manier waarop de communicatie tussen Expressway-Core en CUCM plaatsvindt, moet ervoor worden gezorgd dat:

1. U raadt aan CA-ondertekende certificaten te gebruiken voor mobiele en externe toegang.
2. Elk Unified CM-cluster moet het Expressway-C-certificaat vertrouwen. Zorg voor elk cluster voor:
 - Als de gemengde modus is ingeschakeld, moet het Expressway-C-certificaat worden geïnstalleerd in de CallManager-trust- en Tomcat-trust-winkel op Unified CM.
 - Als de gemengde modus is uitgeschakeld, moet het CA-hoofdcertificaat dat het Expressway-C-certificaat ondertekent, worden geïnstalleerd in de CallManager-trust- en Tomcat-trust-winkel op Unified CM. Start deze vervolgens opnieuw op: · Tomcat Service · CallManager Service · HA Proxy Service (als u TLS op Tomcat gebruikt).

Op Expressway - Core, zorg ervoor dat deze acties worden genomen:

- Expressway-C moet de certificaten vertrouwen die worden aangeboden door elk Unified CM- en IM- en Presence Service-cluster.

Het vertrouwensarchief van Expressway-C moet het root CA-certificaat bevatten dat de Unified CM- en IM- en Presence Service-certificaten voor alle UC-clusters ondertekent.



Opmerking: zorg ervoor dat u alle root- en intermediate CA-certificaten of volledige CA-keten die wordt gebruikt om het Expressway-C-certificaat te ondertekenen, toevoegt aan de Tomcat-trust- en CallManager-vertrouwenslijst van Cisco Unified Communications Manager (UCM), ook al werkt de UCM in de niet-beveiligde modus.

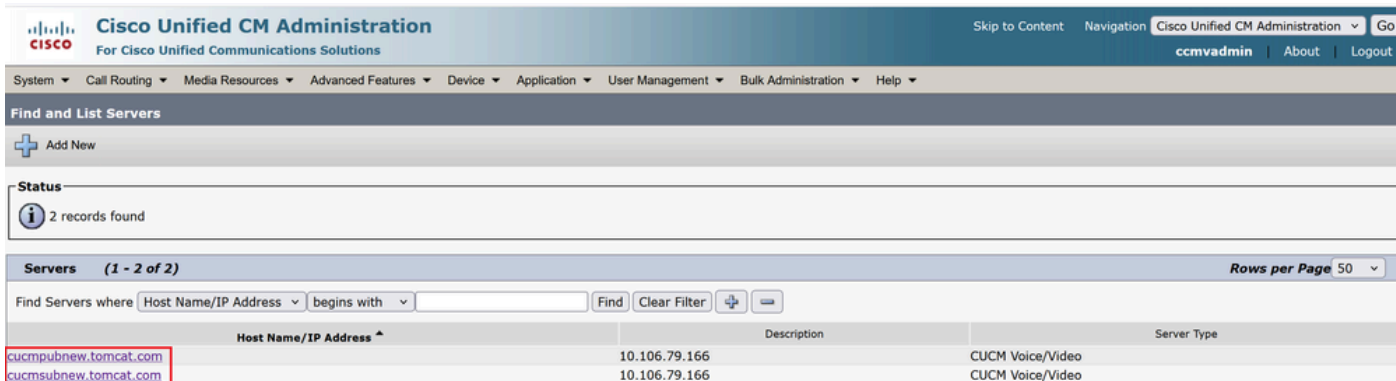
Reden - De verkeersserverservice in Expressway verzendt het certificaat wanneer een server (UCM) daarom vraagt. Deze verzoeken hebben betrekking op diensten die worden uitgevoerd op andere poorten dan 8443 (bijvoorbeeld poorten 6971, 6972, enzovoort). Dit dwingt certificaatverificatie af, zelfs als UCM zich in de niet-beveiligde modus bevindt.

De manier waarop het CUCM-adres wordt toegevoegd onder Systeem > Server speelt een zeer belangrijke rol bij het toevoegen van CUCM/IMP aan de Expressway-kern onder Configuratie > Unified Communications > Unified CM-servers/IM- en Presence Service-knooppunten.

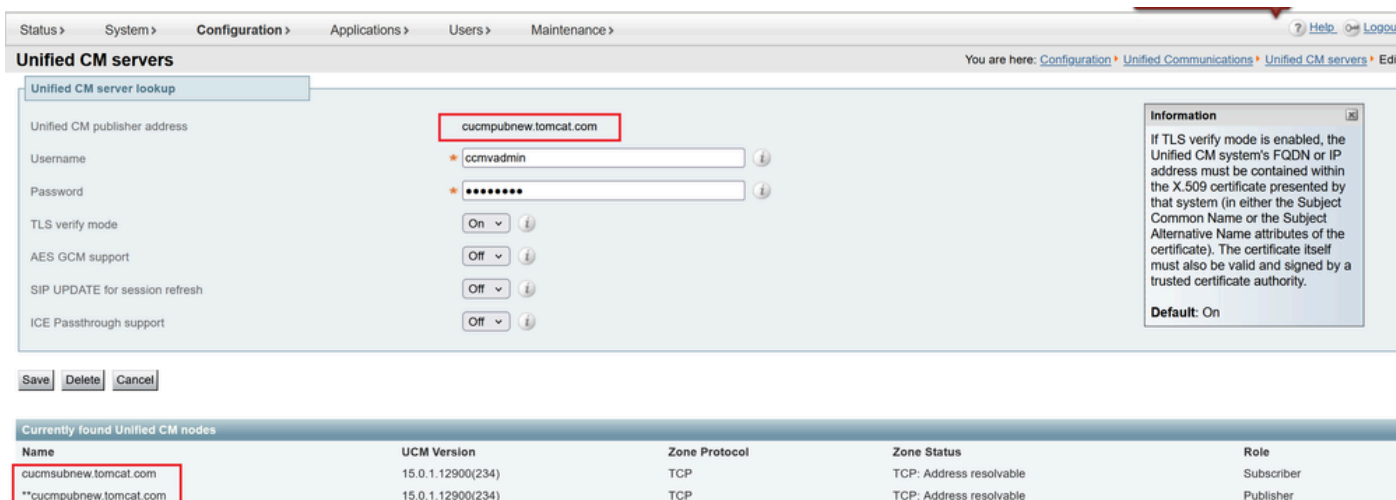
CUCM moet altijd worden toegevoegd met FQDN en niet met hostnaam of IP-adres. Als wordt waargenomen dat CUCM onder Systeem > Server wordt toegevoegd als hostnaam/IP-adres

tijdens de TLS-handshake mislukt de TLS-verificatie 'Aan' en wordt het CUCM-cluster niet toegevoegd aan de Expressway-Core.

In deze afbeelding ziet u CUCM toegevoegd als hostnaam:



Deze afbeelding toont CUCM toegevoegd op Expressway-Core met FQDN met TLS verify Mode = ON:



Er werd ook een wijziging geïntroduceerd in X14.2 die cijfers tijdens een TLS-handdruk (client hello) in verschillende volgorde van voorkeur zal presenteren. Dit was afhankelijk van het upgradepad en veroorzaakte onverwachte TLS-verbindingen na een software-upgrade. Het kan zijn dat vóór de upgrade tijdens TLS-handshake het Cisco Tomcat- of Cisco CallManager-certificaat van CUCM heeft aangevraagd. Maar dat na de upgrade, vroeg het voor de ECDSA-variant (die de veiligere cijfervariant is dan RSA). De Cisco Tomcat-ECDSA- of Cisco CallManager-ECDSA-certificaten kunnen worden ondertekend door een andere CA of gewoon nog steeds zelf ondertekende certificaten (de standaard).

Deze wijziging van de volgorde van de coderingsvoorkeur is niet altijd relevant voor u, omdat deze afhankelijk is van het upgradepad zoals wordt weergegeven in de [opmerkingen](#) bij de [release van Expressway X14.2.1](#). Kortom, u kunt zien vanuit Onderhoud > Beveiliging > Coderingen voor elk van de cijferlijsten of het ECDHE-RSA-AES256-GCM-SHA384 al dan niet vooraf gaat. Als dit niet het geval is, geeft het de voorkeur aan het nieuwere ECDSA-cijfer boven het RSA-cijfer. Als dat zo is, dan heb je het gedrag zoals eerder bij RSA dat dan de hogere voorkeur heeft.

De volgende schermafbeelding wordt weergegeven in het rode vak ECDSA-codering geadverteerd door Expressway-kern tijdens het TLS-onderhandelingsbericht in Client hello, #IF TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 wordt gekozen door Remote responder (CUCM) in server hello, dan TLS-onderhandeling mislukt als:

ROOT CA-certificaten of feitelijke ECDSA-certificaten van Responder, dat wil zeggen dat CUCM in dit geval niet is geïnstalleerd in de Expressway Trust-winkel.

```
▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
  Content Type: Handshake (22)
  Version: TLS 1.0 (0x0301)
  Length: 512
  ▼ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 508
    > Version: TLS 1.2 (0x0303)
      Random: b82e6720580ae3f044e8bde95d5a0a2f68b240e720e5a75f4471cdfc25784cf8
      Session ID Length: 32
      Session ID: b18bb9a287a1cc5bcc1087470f608423d4ccd6710f276dff95e5faf613e4716d
      Cipher Suites Length: 66
    ▼ Cipher Suites (33 suites)
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
      Cipher Suite: TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)
      Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a9)
      Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a8)
```

U kunt ook Expressway-coderingen wijzigen zodat ECDSA geen voorrang krijgt.

1. Wijzig SIP-codering door GCM-Sha384 open SSL-tekenreeks toe te voegen.

"ECDHE-RSA-AES256-GCM-SHA384:EECDH:EDH:HIGH:.....:!MD5:!PSK:!NULL:!NULL:!aDH"

2. Voeg + toe om het cijfer bij laatste voorkeur te verplaatsen of voeg ! toe om ECDSA permanent uit te schakelen.

Cijfercode: "EECDH: EDH: HIGH: -
AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!NULL:!NULL:!aDH:+ECDSA"

3. Voeg het basiscertificaat en het tussenliggende CA-certificaat toe dat het ECDSA-certificaat op CUCM heeft ondertekend of voeg het Tomcat-ECDSA-certificaat toe op het Expressway-vertrouwensarchief (in sommige gevallen).

Echter, als gevolg van de verandering in de cipher voorrang, na de upgrade, MRA implementaties kunnen breken, dus TAC zal hebben om de eerder genoemde workaround uit te voeren om dingen weer te laten werken.

Met de introductie van TLS 1.3 wordt het nog moeilijker om te controleren welke certificaten er in Wireshark worden uitgewisseld.

Gedrag op versies x15.3

Alleen voor de SIP-interface kunt u ervoor kiezen om RSA- of ECDSA-coderingen te gebruiken.

Met X15.x is TLS 1.3 afgedwongen. Zoals te zien op het veld, wordt RSA-algoritme meestal gekozen boven ECDSA. Klanten die nu upgraden naar x15.2 kunnen kiezen

tussen RSA en ECDSA-algoritme met deze opdrachtset:

```
xConfiguration SIP Advanced TLSSignatureAlgoPrefRsa: aan/uit
```

TlssignatureAlgoPrefRSA werkt alleen als de SIP-interface TLS 1.3 heeft

```
xConfiguration SIP Advanced SipTlsVersions: "TLSv1.3"
```

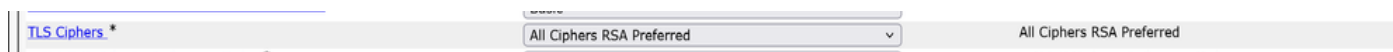


Opmerking: dit komt alleen in aanmerking voor SIP-interface vanaf nu. Traffic Server en Tomcat overwegingen op 8443 blijft ongewijzigd zoals eerder gedocumenteerd.

Codeerpakken die tijdens 'client hello' door Expressway naar CUCM worden verzonden, worden weergegeven zoals wordt weergegeven wanneer RSA wordt gekozen.

- Handtekeningalgoritme: rsa_pss_rsae_sha512 (0x0806)
- Handtekeningalgoritme: rsa_pss_rsae_sha384 (0x0805)
- Handtekeningalgoritme: rsa_pss_rsae_sha256 (0x0804)
- Handtekeningalgoritme: ecdsa_secp521r1_sha512 (0x0603)
- Handtekeningalgoritme: ecdsa_secp384r1_sha384 (0x0503)
- Handtekeningalgoritme: ecdsa_secp256r1_sha256 (0x0403)

De eerdere configuratie werkt in tandem op welke configuratie u hebt gekozen op CUCM naar TLS-cijfers onder Enterprise Parameters > Security Parameters.



Het is ook belangrijk op te merken dat tijdens een gebroken TLS-handshake over TLS 1.3 tussen Expressway-C en CUCM, de fouten die zijn afgedrukt in diagnostische logs of PCAP niet erg nuttig zijn. Het is de moeite waard om deze debugs in te schakelen tijdens het werken met TAC, zodat componentafdrukken fouten wissen om problemen op te lossen.

```
xConfiguration Logger Developer.trafficServer.http Niveau: "DEBUG"  
xConfiguration Logger Developer.trafficServer.http_trans Niveau: "DEBUG"  
xConfiguration Logger Developer.trafficServer.ioCore Niveau: "DEBUG"  
xConfiguration Logger Developer.trafficServer.ssl Niveau: "DEBUG"
```

Wat te verwachten wanneer Callmanager één certificaat deelt met meerdere services

Dingen veranderen enigszins met hergebruik van certificaten op CUCM.

Vanaf CUCM 14.0 kunt u certificaten van Tomcat, Tomcat en Tomcat ECDSA hergebruiken als

Call manager en Call manager ECDSA.

Tomcat certificaat kan worden hergebruikt als Callmanager certificaat.

Het Tomcat-ECDSA certificaat kan hergebruikt worden als Callmanager-ECDSA certificaat.

Dit maakt het leven gemakkelijk.

1. Meerdere diensten op CUCM gebruiken nu één certificaat, waardoor de kosten van het certificaat dalen.

2. Minder beheer van certificaten.

3. Als u Tomcat/Callmanager of Tomcat-ECDSA/Callmanager-ECDSA-certificaat (om welke reden dan ook) moet uploaden naar de ExpressWay-Core-vertrouwenswinkel, is dit slechts één certificaat dat u moet uploaden. Het zal geen probleem zijn om dezelfde GN-naamkwesitie te hebben (eerder in dit document besproken).



Opmerking: hergebruik van certificaten vindt alleen plaats als Tomcat en Tomcat-ECDSA multisite-certificaten zijn.

Certificaten voor Post Reuse, Callmanager en Callmanager ECDSA-servers zijn niet zichtbaar in het CUCM-vertrouwensarchief. U kunt hergebruik van certificaten valideren vanuit CLI door opdrachten uit te voeren:

bepaalde CallManager weergeven

Toon Certown Tomcat


Stappen voor hergebruik certificaat

Tomcat CSR pub aanmaken toevoegen.

Certificate Details for cucmpubnew-ms.stark.com, tomcat

 Regenerate  Generate CSR  Download .PEM File  Download .DER File

Status

 Status: Ready

Certificate Settings

Locally Uploaded	06/09/25
File Name	tomcat.pem
Certificate Purpose	tomcat
Certificate Type	certs
Certificate Group	product-cpi
Description(friendly name)	Certificate Signed by WIN-9G89V8O9OR2

Certificate File Data

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      48:00:00:00:04:61:fc:d3:8c:8f:a1:12:92:00:00:00:00:00:04
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC = com, DC = stark, CN = WIN-9G89V8O9OR2
    Validity
      Not Before: Sep  6 05:07:47 2025 GMT
      Not After : Sep  6 05:17:47 2027 GMT
    Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-ms.stark.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
```

Regenerate

Generate CSR

Download .PEM File

Download .DER File

CA-certificaat uploaden dat het Tomcat-certificaat op CUCM ondertekent als Tomcat-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* tomcat-trust

Description(friendly name)

Upload File Browse... shashaCA.cer

Upload Close

i *- indicates required item.

Zodra Tomcat certificaat is ondertekend, upload op uitgever. Start relevante services opnieuw op zoals wordt gevraagd.

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

Description(friendly name)

Upload File Browse... pubcucmtomcat15.cer

Upload Close

i *- indicates required item.

Zodra Tomcat certificaat is ondertekend, upload op uitgever. Start relevante services opnieuw op zoals wordt gevraagd.

Succesvol: certificaat geüpload. Voer een Disaster Recovery-back-up uit zodat de laatste back-up het geüploade certificaat bevat.

Start de Cisco Tomcat-webservice opnieuw op met de CLI-service 'Cisco Tomcat opnieuw starten' op alle clusternodes (UCM/IMP). Start de webservices Cisco UDS Tomcat en Cisco AXL

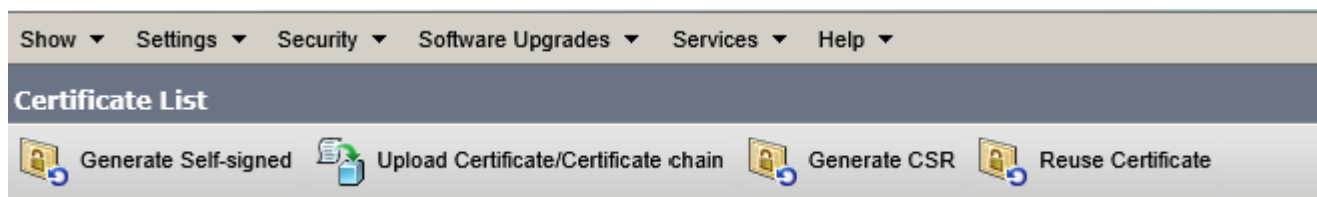
Tomcat opnieuw op met behulp van de CLI-service 'Start Cisco UDS Tomcat opnieuw op en start de service Cisco AXL Tomcat opnieuw op' op alle UCM-clusternodes. Start ook de Cisco DRF Master- en Cisco DRF Local-services opnieuw op in de node van de uitgever. Start alleen de lokale Cisco DRF-service op de abonneeknooppunten opnieuw op.

Tomcat certificaat is nu ondertekend door CA.

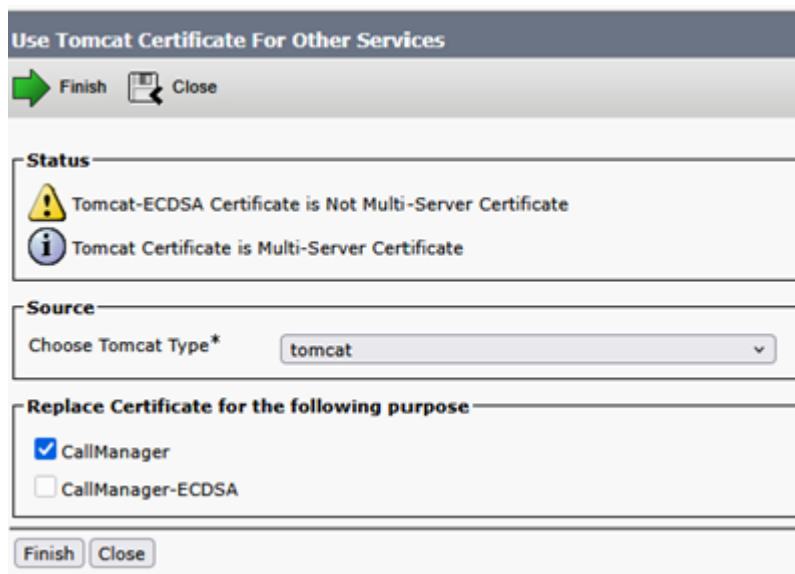
tomcat	cucmoubnw-ms.stark.com/51dc40f400000000000b	signed IdentityCA- signed	RSA	Multi-server(SAN)	RICKY200-TMS-CA	10/23/2027Certificate Signed by RICKY200-TMS-CA
--------	---	---------------------------------	-----	-------------------	-----------------	---

Om Tomcat certificaat nu opnieuw te gebruiken als Callmanager certificaat.

Klik op Certificaat opnieuw gebruiken.



Kies Tomcat in de keuzelijst en controleer het Callmanager-certificaat.



Klik op Finish (Voltooien).

Use Tomcat Certificate For Other Services

Finish Close

Status

- Certificate Successful Provisioned for the nodes cucmpubnew.stark.com,cucmsubnew.stark.com,.
- Restart Cisco HAProxy Service for the generated certificates to become active.
- If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.

Source

Choose Tomcat Type* tomcat

Replace Certificate for the following purpose

CallManager
 CallManager-ECDSA

Finish Close

Het Tomcat-certificaat wordt nu hergebruikt als Callmanager-certificaat. Dit kan worden gevalideerd vanuit CLI.

Callmanager-certificaat Serienummer (SN): 56:ff:6c:71:00:00:00:00:0d

```

admin:show cert own CallManager
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      56:ff:6c:71:00:00:00:00:0d
    Signature Algorithm: sha384WithRSAEncryption
    Issuer: DC = com, DC = RICKY200, CN = RICKY200-TMS-CA
    Validity
      Not Before: Oct 24 08:44:34 2025 GMT
      Not After : Oct 24 08:54:34 2027 GMT
    Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-ms.
tomcat.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:
      00:b4:a6:fa:8f:9a:c3:32:02:74:fa:e9:92:30:de:
      6e:3b:70:cd:d7:4e:64:e4:71:04:fe:17:80:0d:5b:
      44:d1:7f:00:63:69:4a:5c:1a:1b:75:0c:1a:d6:ce:
      10:3f:01:e2:d0:f1:75:33:57:b7:0a:71:e1:60:d1:
      89:3c:e8:a4:8c:3e:30:69:4d:4e:98:da:b8:5d:dd:
      23:8c:4d:69:90:69:9d:43:74:84:20:a8:9f:45:dc:
      5a:aa:7b:c8:d1:d0:6f:05:13:d8:99:58:0e:49:7b:
Press <enter> for 1 line, <space> for one page, or <q> to quit

```

Tomcat-certificaat SN: 56:ff:6c:71:00:00:00:00:0d

```

admin:show cert own tomcat
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      56:ff:6c:71:00:00:00:00:0d
    Signature Algorithm: sha384WithRSAEncryption
    Issuer: DC = com, DC = RICKY200, CN = RICKY200-TMS-CA
    Validity
      Not Before: Oct 24 08:44:34 2025 GMT
      Not After : Oct 24 08:54:34 2027 GMT
    Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-ms.tomcat.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:b4:a6:fa:8f:9a:c3:32:02:74:fa:e9:92:30:de:
        6e:3b:70:cd:d7:4e:64:e4:71:04:fe:17:80:0d:5b:
        44:d1:7f:00:63:69:4a:5c:1a:1b:75:0c:1a:d6:ce:
        10:3f:01:e2:d0:f1:75:33:57:b7:0a:71:e1:60:d1:
        89:3c:e8:a4:8c:3e:30:69:4d:4e:98:da:b8:5d:dd:
        23:8c:4d:69:90:69:9d:43:74:84:20:a8:9f:45:dc:
        5a:aa:7b:c8:d1:d0:6f:05:13:d8:99:58:0e:49:7b:
Press <enter> for 1 line, <space> for one page, or <q> to quit

```

Voer dezelfde stappen uit op Abonnee.

Het ECDSA-certificaat nu ondertekenen zodat het opnieuw kan worden gebruikt als Callmanager-ECDSA.

Het huidige Tomcat-ECDSA certificaat is zelf ondertekend.

tomcat	10.106.79.162_5aceb67f000000000000f	IdentityCA-signed	RSA Multi-server(SAN)	RICKY200-TMS-CA	10/25/2027Certificate Signed by RICKY200-TMS-CA
tomcat-ECDSA	cucmpubnew-tl.tomcat.com_4b404cf20zfb4/cabf8aedb/8c/1bd4b	identity-self-signed	EC	cucmpubnew.tomcat.com cucmpubnew-tl.tomcat.com	10/23/2025self-signed certificate generated by system

Ondertekenen multisan CSR voor Tomcat-ECDSA-certificaat.

- 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-ECDSA

Distribution* Multi-server(SAN)

Common Name* 10.106.79.162

Include OU in CSR

Subject Alternate Names (SANs)

Auto-populated Domains
cucmpubnew.tomcat.com
cucmsubnew.tomcat.com

Parent Domain tomcat.com

Other Domains
ec.vikdutta.com
vcs8c.s.com

Browse... No file selected.
Please import .TXT file only.



Key Type** EC

Key Length* 256

Hash Algorithm* SHA256

Onderteken het certificaat met behulp van CSR en upload.

Upload Certificate/Certificate chain

 Upload  Close

Status



Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*

tomcat-ECDSA

Description(friendly name)

Upload File

Browse...



cucmpubecdsa162.cer

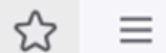
Upload

Close



Upload Certificate/Certificate chain — Mozilla Firefox



  10.106.79.162/cmplatform/certificateUpload.do



Upload Certificate/Certificate chain

 Upload  Close

Status



Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*

Loading, please wait.

Description(friendly name)

Upload File

Browse...

cucmpubecdsa162.cer

Upload

Close



*- indicates required item.

10.106.79.162

Uploaden gelukt. Herstart relevante services zoals gevraagd.

Upload Certificate/Certificate chain

Upload Close

Status

- Certificate upload operation successful for the nodes cucmpubnew.tomcat.com,cucmsubnew.tomcat.com.
- Restart the Cisco Tomcat web service using the CLI "utils service restart Cisco Tomcat" on all cluster nodes (UCM/IMP). Restart Cisco UDS Tomcat and Cisco AXL Tomcat web services using the CLI "utils service restart Cisco UDS Tomcat and utils service restart Cisco AXL Tomcat" on all the UCM cluster nodes. Also, restart the Cisco DRF Master and Cisco DRF Local services on the publisher node. Restart ONLY the Cisco DRF Local service on the subscriber node(s).
- If SAML SSO is enabled, please re-provision the SP metadata on the IDP.

Upload Certificate/Certificate chain

Certificate Purpose* tomcat-ECDSA

Description(friendly name)

Upload File Browse... No file selected.

Upload Close

Tomcat en Tomcat-ECDSA ondertekend door CA.

tomcat	10.106.79.162_Saceb57f000000000000f	signed	IdentityCA- signed	RSA	Multi-server(SAN)	RICKY200-TMS-CA	10/25/2027Certificate Signed by RICKY200-TMS-CA
tomcat-ECDSA	swmsubnew-CC- ms.tomcat.com_2f0000003880becca8a18e8f2300000000038	signed	IdentityCA- signed	EC	Multi-server(SAN)	bgluclab-WIN-DC-01-CA	10/25/2026Certificate Signed by bgluclab-WIN-DC-01-CA

Hergebruik Tomcat-ECDSA nu als Callmanager-ECDSA-certificaat.

Use Tomcat Certificate For Other Services

Finish Close

Status

- Tomcat Certificate is Multi-Server Certificate
- Tomcat-ECDSA Certificate is Multi-Server Certificate

Source

Choose Tomcat Type* tomcat-ECDSA

Replace Certificate for the following purpose



CallManager

CallManager-ECDSA






Finish Close

Uploaden gelukt. Start relevante services opnieuw op zoals wordt gevraagd.

Use Tomcat Certificate For Other Services

 Finish
  Close

Status

-  Certificate Successful Provisioned for the nodes cucmsubnew.tomcat.com,cucmpubnew.tomcat.com,,
-  Restart Cisco HAProxy Service for the generated certificates to become active.
-  If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.
-  Restart Cisco TFTP service.
-  Restart Cisco CallManager Service and other relevant services on certificate provisioned nodes.

Source

Choose Tomcat Type* tomcat-ECDSA

Replace Certificate for the following purpose

CallManager
 CallManager-ECDSA

Certificaten van CLI controleren.

Callmanager-ECDSA-certificaat SN: 2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38

```

admin:show cert own CallManager-ecdsa
Invalid Certificate Name. Certificate Not Found.

admin:show cert own CallManager-Ecdsa
Invalid Certificate Name. Certificate Not Found.

admin:show cert own tomcat-ECDSA
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC = com, DC = bgluclab, CN = bgluclab-WIN-DC-01-CA
    Validity
      Not Before: Oct 25 06:46:37 2025 GMT
      Not After : Oct 25 06:46:37 2026 GMT
  
```

Tomcat-ECDSA-certificaat SN: 2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38.

```

admin:show cert own tomcat-ECDSA
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC = com, DC = bgluclab, CN = bgluclab-WIN-DC-01-CA
    Validity
      Not Before: Oct 25 06:46:37 2025 GMT
      Not After : Oct 25 06:46:37 2026 GMT
    Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-EC-ms.tomcat.com
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (256 bit)
  
```

Aangezien u nu één certificaat gebruikt voor twee services, dat wil zeggen Tomcat-certificaat voor Tomcat- en Callmanager-services en Tomcat-ECDSA voor Tomcat-ECDSA- en Callmanager-ECDSA-services, is het minder omslachtig geworden om certificaten te uploaden op de vertrouwenswinkel van Expressway (indien nodig te uploaden).

Het hebben van TLS om 'On' te verifiëren terwijl UCM wordt toegevoegd aan de expressway-core voor MRA, is eenvoudiger dan ooit tevoren. Alleen al door het toevoegen van één Tomcat-certificaat of CA-servercertificaat wordt de taak uitgevoerd (omdat het certificaat nu wordt gedeeld tussen Callmanager en Tomcat-service).

Unified CM servers You are here: Configuration > Unified Communications

Success: Connection success: The server cucmpubnew.tomcat.com was successfully discovered and queried. Connections established with known cluster nodes. Unchanged: 10.106.79.162, 10.106.79.166

Warning: The CSRF Protection status is automatically enabled after the software upgrade. We recommend keeping CSRF protection Enabled. To change it, please log in to the CLI.

Publisher address	Username	TLS verify mode	Nodes discovered by this lookup	Deployment	AI's GCM support	SIP UPDATE for session refresh	ICE Passthrough support	Actions
<input type="checkbox"/> cucmice.com	appuser	On	cucmice.com	ice.com	Off	Off	Off	View/Edit
<input type="checkbox"/> cucm11su252.s.com	cucmadmin	Off	cucm11su252.s.com	s.com	Off	Off	Off	View/Edit
<input type="checkbox"/> cucm33.vikdutta.com	appuser	Off	cucm33.vikdutta.com	vikdutta.com	Off	Off	Off	View/Edit
<input type="checkbox"/> cucmpubnew.tomcat.com	ccmadmin	On	10.106.79.166, 10.106.79.162	tomcat.com	Off	Off	Off	View/Edit

[Add](#) [Remove](#) [Select all](#) [Unselected](#) [Refresh servers](#) Click Refresh servers to refresh the details of the nodes associated with this page.

Currently found Unified CM nodes	Name	UCM Version	Zone Protocol	Zone Status
cucm.eight10.com	**cucm.eight10.com	11.5.1.10900(97)	TCP	TCP: Address resolvable
cucm11su252.s.com	**cucm11su252.s.com	11.5.1.12900(21)	TCP	TCP: Address resolvable
cucm33.vikdutta.com	**cucm33.vikdutta.com	12.5.1.11900(146)	TLS / TCP	TLS: Address resolvable, TCP: Address resolvable
cucmice.com	**cucmice.com	11.5.1.14900(11)	TLS / TCP	TLS: Address resolvable, TCP: Address resolvable
cucmpubnew.tomcat.com	**10.106.79.162	15.0.1.12900(234)	TCP	TCP: Address resolvable
cucmpubnew.tomcat.com	10.106.79.166	15.0.1.12900(234)	TCP	TCP: Address resolvable

Als een upgrade naar x14.2 of hoger een storing voor mobiele externe toegang heeft veroorzaakt, kunt u [dit](#) uitgebreide document ook doorverwijzen naar Problemen oplossen.

Versiegeschiedenis van Apache Traffic Server

Om de versie op uw server te controleren, logt u in op root en voert u `~ # /apache2/bin/httpd -v` uit.

Expressway x8.11.4

Serverversie: Apache/2.4.34 (Unix)

Server gebouwd: Nov 12 2018 19:04:23

Expressway x12.6

Serverversie: Apache/2.4.43 (Unix)

Server gebouwd: 26 mei 2020 18:27:21

Expressway x14.0.8

Serverversie: Apache/2.4.53 (Unix)
Server gebouwd: 4 mei 2022 08:52:57

Expressway x15.3

Serverversie: Apache/2.4.62 (Unix)
Server gebouwd: 16 jul 2025 12:10:19

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.