

Navigeer door Client ECU Sunset met Expressway x15.5

Inleiding

In dit document wordt beschreven hoe u met Cisco Expressway x15.5 door de ECU-zonsondergang van de client navigeert.

Achtergrondinformatie

Digitale certificaten zijn elektronische referenties die worden uitgegeven door vertrouwde certificeringsinstanties (CA's) die de communicatie tussen servers en clients beveiligen door authenticatie, gegevensintegriteit en vertrouwelijkheid te waarborgen. Deze certificaten bevatten ECU-velden (Extended Key Usage) die hun doel definiëren:

- Serververificatie ECU (id-kp-serverAuth) wordt gebruikt wanneer een server zijn certificaat presenteert om zijn identiteit te bewijzen.
- Client Authentication ECU (id-kp-clientAuth) wordt gebruikt in wederzijdse TLS (mTLS) verbindingen waar beide partijen elkaar authenticeren.

Traditioneel kan een enkel certificaat zowel server- als clientverificatie-ECU's bevatten, waardoor het voor twee doeleinden kan worden gebruikt. Dit is vooral belangrijk voor producten zoals Cisco Expressway die zowel als server als client fungeren in verschillende verbindingsscenario's.

probleemdefinitie

Wijziging van het rootprogramma van Chrome

Met ingang van juni 2026 beperkt het Chrome Root Program Policy Root Certificate Authority (CA) -certificaten die zijn opgenomen in de Chrome Root Store, waardoor multifunctionele roots worden uitgefaseerd om alle public-key infrastructuur (PKI) -hiërarchieën uit te lijnen om alleen TLS-serverauthenticatie te gebruiken.

Belangrijkste beleidsvereisten

- Public Root CA's moeten EKU (Extended Key Usage) ALLEEN voor serververificatie (id-kp-serverAuth) bevestigen.
- Het opnemen van Client Authentication EKU in deze certificaten is verboden.
- Geen root-CA's voor gemengd gebruik meer voor TLS-certificaten voor openbare servers.
- Tijdschema voor handhaving: juni 2026

Openbare CA-responstijdlijn

- Oktober 2025: Veel publieke CA's (DigiCert, Sectigo, SSL) begonnen standaard met het uitgeven van alleen-servercertificaten.
- Mei 2026: Openbare CA-servers geven geen EKU-certificeringen voor clientverificatie meer uit
- Juni 2026: Chrome Root Program Policy wordt volledig effectief



Opmerking: dit beleid is alleen van toepassing op certificaten die zijn uitgegeven door openbare CA's. Particuliere PKI en zelf ondertekende certificaten worden niet beïnvloed door dit beleid.

Als u geïnteresseerd bent in het lezen over de impact van zonsondergang van client EKU op Expressways, raadpleeg dan [Prepare Expressway for Client Auth EKU Sunset in Public CA Certificates](#).

Expressway Release x15.5 met oplossing

Expressway x15.5

Expressway x15.5 wordt geleverd met een voorgestelde oplossing voor een probleem dat zich voordoet als gevolg van het niet instellen van client-EKU door alle openbare certificeringsinstanties. Dit is een wereldwijd probleem en treft alle leveranciers/implementaties die ervoor kiezen om openbare PKI-certificaten te gebruiken.

x15.4, een eerdere release, had een CLI-opdrachtcertificaat waarmee de beheerder alleen het EKU-servercertificaat (geen client-EKU aanwezig) kon uploaden op Expressway E.

xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload: On



Opmerking: deze opdracht is uitgeschakeld op x15.5.

Toevoeging X15.5 Certificate Store

X15.5 heeft twee certificaatstores:

1. Servercertificaatarchief
2. Clientcertificaatarchief


Expressways (één NIC of twee NIC's): beide Expressway-interfaces kunnen naar behoefte gebruikmaken van twee certificaatstores.


Voorbeeld:


- Wanneer de expressway als client fungeert tijdens de TLS-handshake, wordt het clientcertificaat weergegeven.
- Wanneer de expressway tijdens de TLS-handshake als server fungeert, wordt het servercertificaat weergegeven.





Opmerking: beide certificaatstores (client en server) gebruiken dezelfde vertrouwde CA-bibliotheek. Zorg ervoor dat de CA die server- en clientcertificaten heeft ondertekend, correct wordt geüpload in de Trust-opslag. Diagnostische logboeken bevatten nu een servercertificaat en een clientcertificaat in PEM-bestandsindeling.


 ca_vcs8c_2026-03-25_03_20_11.pem


 client_vcs8c_2026-03-25_03_20_11.pem


 eth0_diagnostic_logging_tcpdump00_vcs8c_2026-03-25_03_20_11.pcap

 loggingsnapshot_vcs8c_2026-03-25_03_20_11.txt

 server_vcs8c_2026-03-25_03_20_11.pem

 xconf_dump_vcs8c_2026-03-25_03_20_11.txt

 xconf_dump_vcs8c_2026-03-25_03_20_11.xml

 xstat_dump_vcs8c_2026-03-25_03_20_11.txt

 xstat_dump_vcs8c_2026-03-25_03_20_11.xml

Upgrade van X15.4 of eerdere versie naar X15.5

Wanneer een upgrade wordt uitgevoerd, wordt het servercertificaat van x15.4 of een eerdere versie, de ExpressWay-servercertificaatopslag gekopieerd naar de clientcertificaatopslag op x15.5. Client- en servercertificaatstores op x15.5 hebben hetzelfde certificaat.

Voorbeeld met screenshots

Expressway-server op 15.4, huidig servercertificaat Serienummer 46:df:76:aa:00:00:00:00:29

Certificaat:

Versie: 3 (0x2)

Serienummer:

46:DF:76:AA:00:00:00:00:29

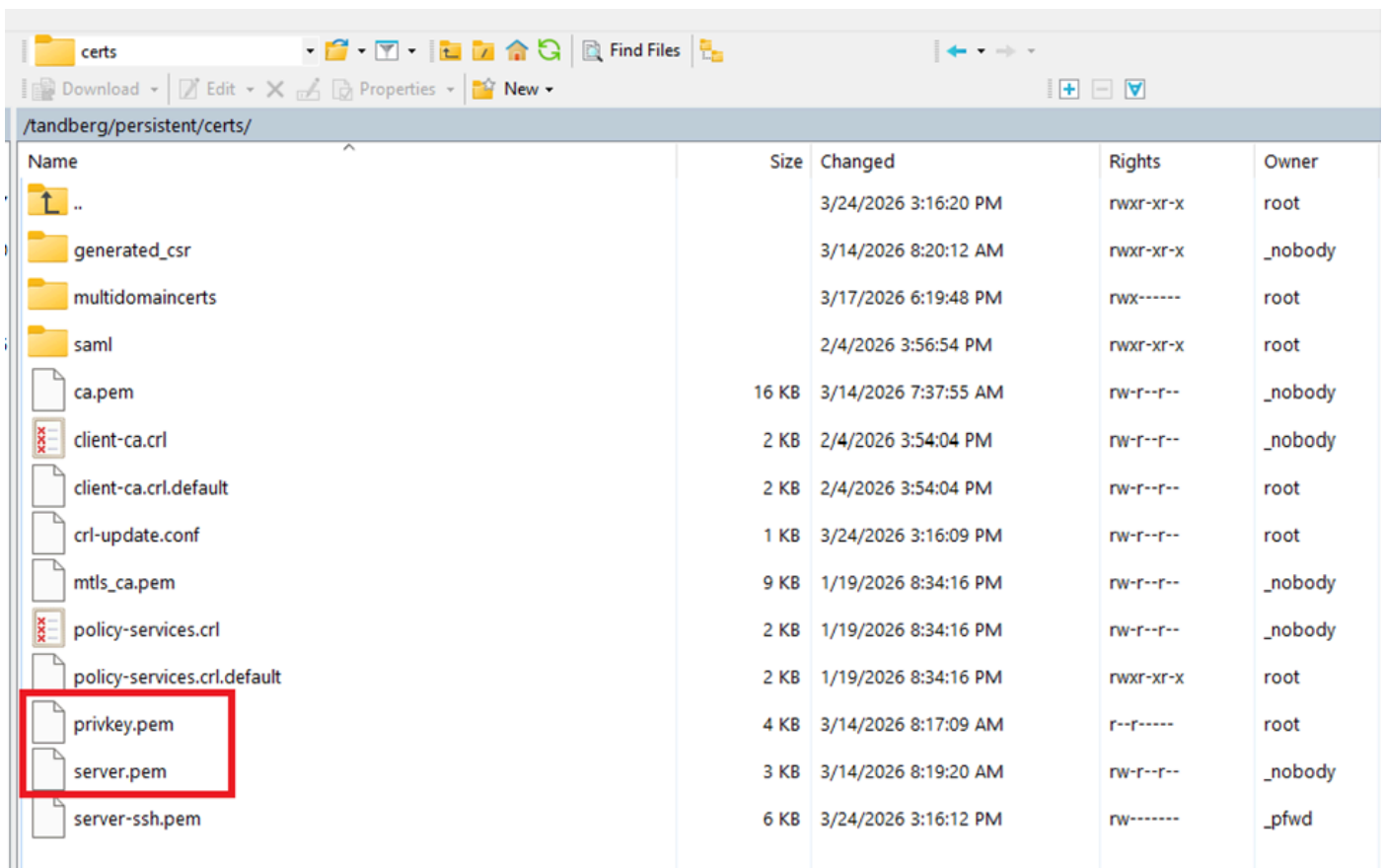
geldigheid

Niet eerder: Mrt 14 02:37:40 2026 GMT

Niet na: Mrt 14 02:47:40 2028 GMT

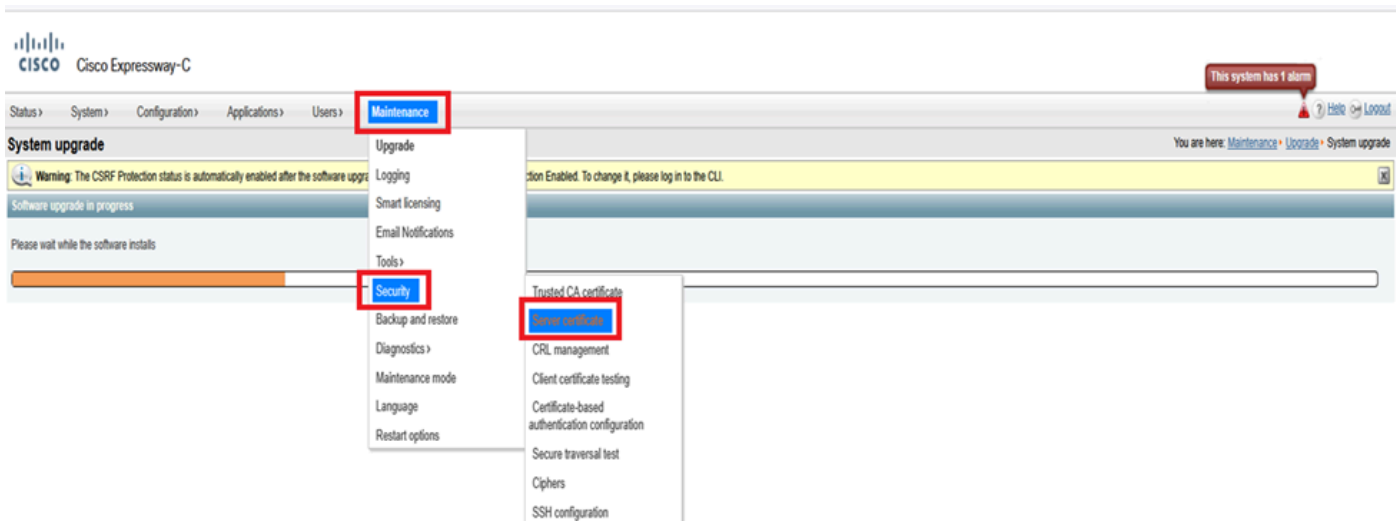
Onderwerp: C = IN, ST = KA, L = KA, O = Cisco, OU = TAc, CN = cluster.s.com

Expressway-bestandssysteempersistente/cert-directory op x15.4:



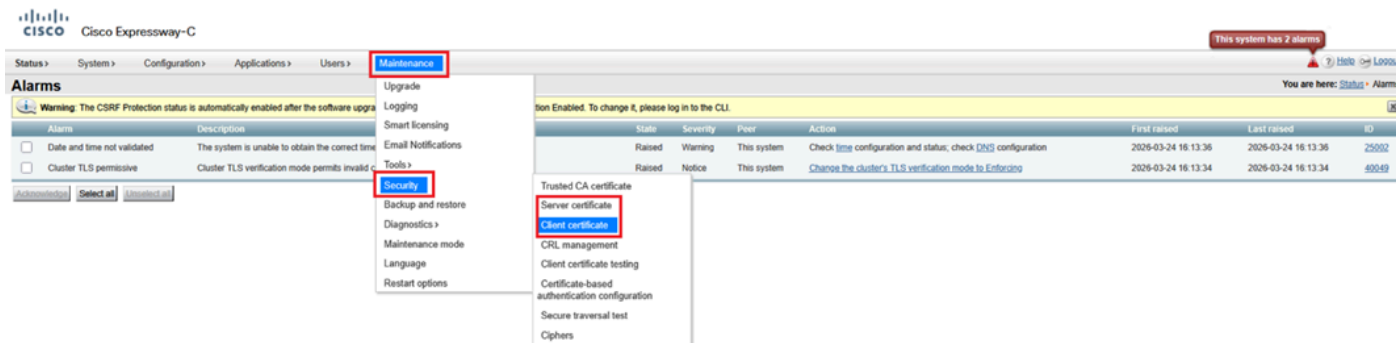
Name	Size	Changed	Rights	Owner
..		3/24/2026 3:16:20 PM	rw-r--r--	root
generated_csr		3/14/2026 8:20:12 AM	rw-r--r--	_nobody
multidomaincerts		3/17/2026 6:19:48 PM	rw-r--r--	root
saml		2/4/2026 3:56:54 PM	rw-r--r--	root
ca.pem	16 KB	3/14/2026 7:37:55 AM	rw-r--r--	_nobody
client-ca.crl	2 KB	2/4/2026 3:54:04 PM	rw-r--r--	_nobody
client-ca.crl.default	2 KB	2/4/2026 3:54:04 PM	rw-r--r--	root
crl-update.conf	1 KB	3/24/2026 3:16:09 PM	rw-r--r--	root
mtls_ca.pem	9 KB	1/19/2026 8:34:16 PM	rw-r--r--	_nobody
policy-services.crl	2 KB	1/19/2026 8:34:16 PM	rw-r--r--	_nobody
policy-services.crl.default	2 KB	1/19/2026 8:34:16 PM	rw-r--r--	root
privkey.pem	4 KB	3/14/2026 8:17:09 AM	r--r--r--	root
server.pem	3 KB	3/14/2026 8:19:20 AM	rw-r--r--	_nobody
server-ssh.pem	6 KB	3/24/2026 3:16:12 PM	rw-r--r--	_pftd

Expressway-menu (Onderhoud > Beveiliging > Servercertificaat) op x15.4 (alleen veld Servercertificaat aanwezig):



Na succesvolle upgrade naar x15.5

Hier ziet u 2 certificaatopties onder Onderhoud > Beveiliging > clientcertificaat en servercertificaten. Na het upgraden naar x15.5 wordt hetzelfde certificaat weergegeven op zowel de server- als de clientcertificaatportals op webbeheer, omdat het servercertificaat van x15.4 is gekopieerd naar de clientcertificaatopslag op x15.5.



Na de upgrade naar x15.5 zijn het bestaande certificaat en de privésleutel gekopieerd naar het clientcertificaatarchief.

Expressway-bestandssysteempersistente/cert-directory op x15.5:

Name	Size	Changed
..		3/24/2026 4:13:44 PM
generated_csr		3/14/2026 8:20:12 AM
multidomaincerts		3/17/2026 6:19:48 PM
saml		3/24/2026 4:12:43 PM
ca.pem	16 KB	3/14/2026 7:37:55 AM
client.pem	3 KB	3/24/2026 4:12:46 PM
client-ca.crl	2 KB	2/4/2026 3:54:04 PM
client-ca.crl.default	2 KB	2/4/2026 3:54:04 PM
clientprivkey.pem	4 KB	3/24/2026 4:12:46 PM
client-ssh.pem	6 KB	3/24/2026 4:13:37 PM
crl-update.conf	1 KB	3/24/2026 4:13:34 PM
mtls_ca.pem	9 KB	1/19/2026 8:34:16 PM
policy-services.crl	2 KB	1/19/2026 8:34:16 PM
policy-services.crl.default	2 KB	1/19/2026 8:34:16 PM
privkey.pem	4 KB	3/14/2026 8:17:09 AM
server.pem	3 KB	3/14/2026 8:19:20 AM
server-ssh.pem	6 KB	3/24/2026 4:13:37 PM

X15.5 EKU-controle tijdens TLS-handshake

Op x15.5 is een nieuwe CLI-opdracht geïntroduceerd om Extended key use (EKU) tijdens TLS-handshake te controleren. De standaardwaarde is "ON". De opdrachtset is geldig op Expressway Core en Edge.

De opdrachtset activeert een controle voor alle INBOUND SIP TLS-verbindingen naar Expressway. (Inkomende client-HELLO's/certificaat gepresenteerd). Wanneer deze optie is ingeschakeld, wordt gecontroleerd of het certificaat dat door de TLS-initiator wordt gepresenteerd, client-EKU in certificaat bevat. ALS DEZE OPTIE IS UITGESCHAKELD, wordt de controle overgeslagen; de server-EKU wordt echter gecontroleerd als deze aanwezig is op het certificaat.

xconfiguration SIP TLS Certificate ExtendedKeyUse Checking Mode: AAN/UIT:



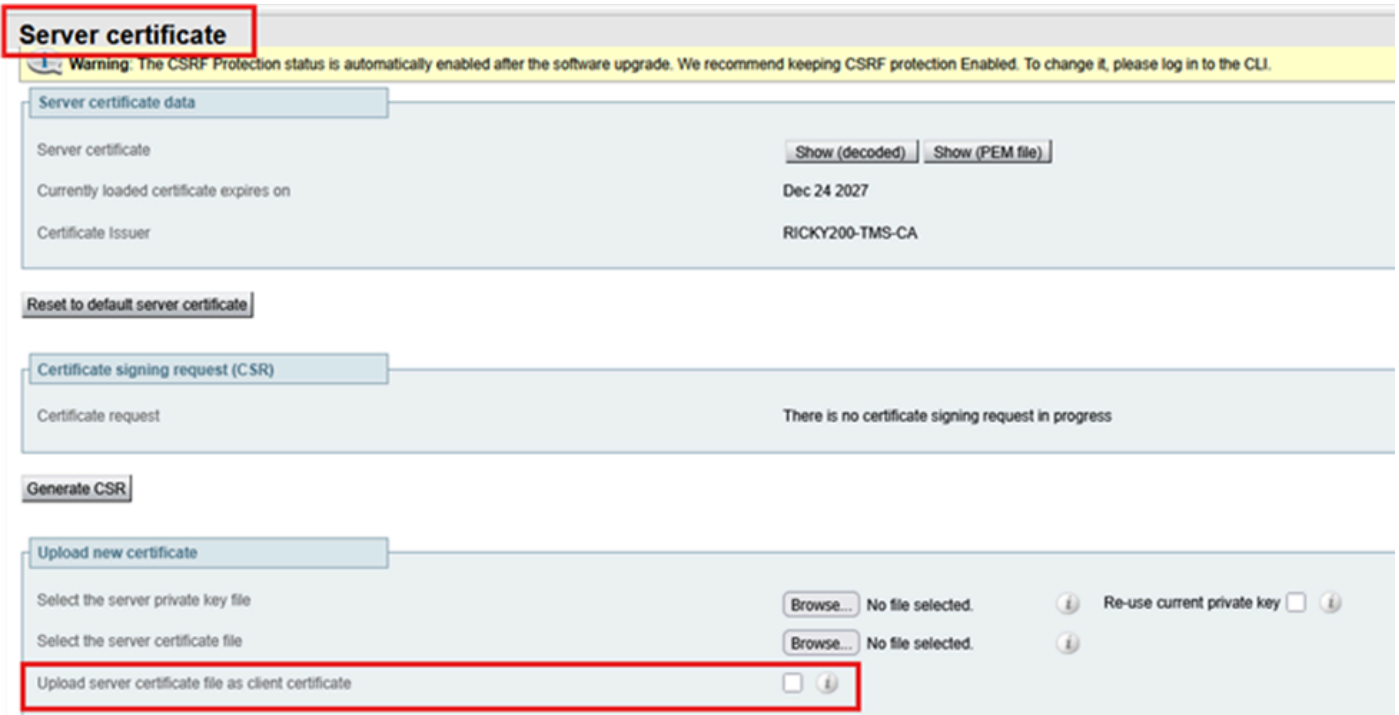
Opmerking: als u een clientcertificaat genereert en een CSR ondertekent die geen client-EKU bevat (een voorbeeld van een openbaar CA-ondertekend certificaat), kunt u dit certificaat niet handmatig uploaden in het clientcertificaatarchief. U moet er dus voor zorgen dat certificaten die worden gegenereerd door het ondertekenen van een CSR altijd de ECU van de klant bevatten (een particuliere CA kan worden gebruikt om de ECU van de klant in te voegen).



Tip: deze fout wordt duidelijk wanneer u probeert een certificaat met een CSR-handtekening te uploaden, dat de ECU van de client mist, in de certificaatopslag van de client.

The screenshot shows the Cisco Expressway-E web interface. The navigation menu includes Status, System, Configuration, Applications, Users, and Maintenance. The page title is 'Client certificate'. A red box highlights an error message: 'Invalid certificate: The file provided does not have a client usage attribute. Services requiring mutual TLS may not work.' Below this is a warning message: '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.' At the bottom, there is a section for 'Client certificate data'.

Als u er echter voor kiest om een certificaat met alleen een server-EKU (geen client-EKU) te uploaden via de servercertificaatopslag en Servercertificaatbestand uploaden als clientcertificaat selecteert, wordt het certificaat gekopieerd naar de clientcertificaatopslag. Beheerders die geen door een particuliere certificeringsinstantie ondertekend certificaat op Expressway-Edge willen gebruiken, kunnen ervoor kiezen de ECU-server alleen te kopiëren van het servercertificaatarchief naar het clientcertificaatarchief.



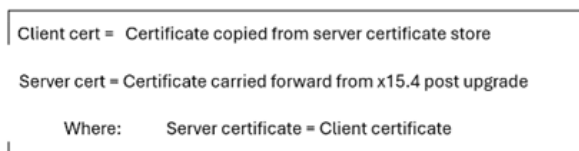
Meerdere certificaatwinkels, meerdere implementatiescenario's

Omdat er nu twee certificaatwinkels op Expressway zijn, zijn er meerdere scenario's van certificaatwinkels.

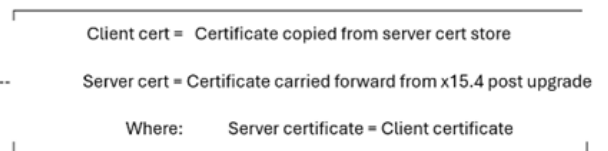
Voorwaarde 1: Upgrade

Wanneer de Expressway wordt bijgewerkt van x15.4 of eerder dan x15.5, is deze voorwaarde waar. Bestaande certificaten uit de x15.4-versie worden gekopieerd naar twee (2) certificaatstores. Op de x15.5-client en -server zijn de te-certificaten hetzelfde.

Exp C x15.5



Exp E x15.5

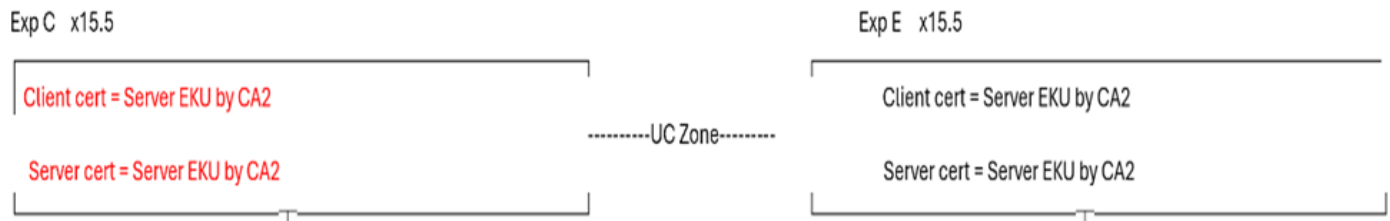


Voorwaarde 2: wanneer de beheerder een nieuw certificaat installeert op x15.5 (bestaande certificaten verlopen)

CA 1 = Interne CA

CA 2 = Openbare CA

In de volgende afbeelding heeft Expressway Core een clientcertificaat met server-EKU dat alleen is ondertekend door CA 2 (Public CA) en een servercertificaat met server-EKU dat alleen is ondertekend door CA 2 (Public CA). Op dezelfde manier heeft Expressway E een clientcertificaat met de server ECU ondertekend door CA2 (openbare CA) en een servercertificaat met server ECU alleen ondertekend door CA 2 (openbare CA).



Als het Expressway-kernservercertificaat geen client-EKU, Unified communications traversal zone, MRA heeft, werkt de WebRTC-proxy niet. Zorg ervoor dat het Expressway Core-servercertificaat een client-EKU heeft. Dit is een veel voorkomend geval waarbij gebruikers ervoor kiezen om alle certificaten van openbare CA te ondertekenen. Aangezien de openbare CA Client ECU niet in certificaten opneemt, wordt de zone Unified communications traversal wel actief.

Als u de UC-zone actief wilt maken, kunt u de ECU-controle op Expressway E uitschakelen. Dit brengt de UC-zone naar voren. SSH-tunnels blijven echter inactief. Vanaf vandaag vereist de SSH-tunnelcommunicatie op 2222 validatie van de klant-EKU.

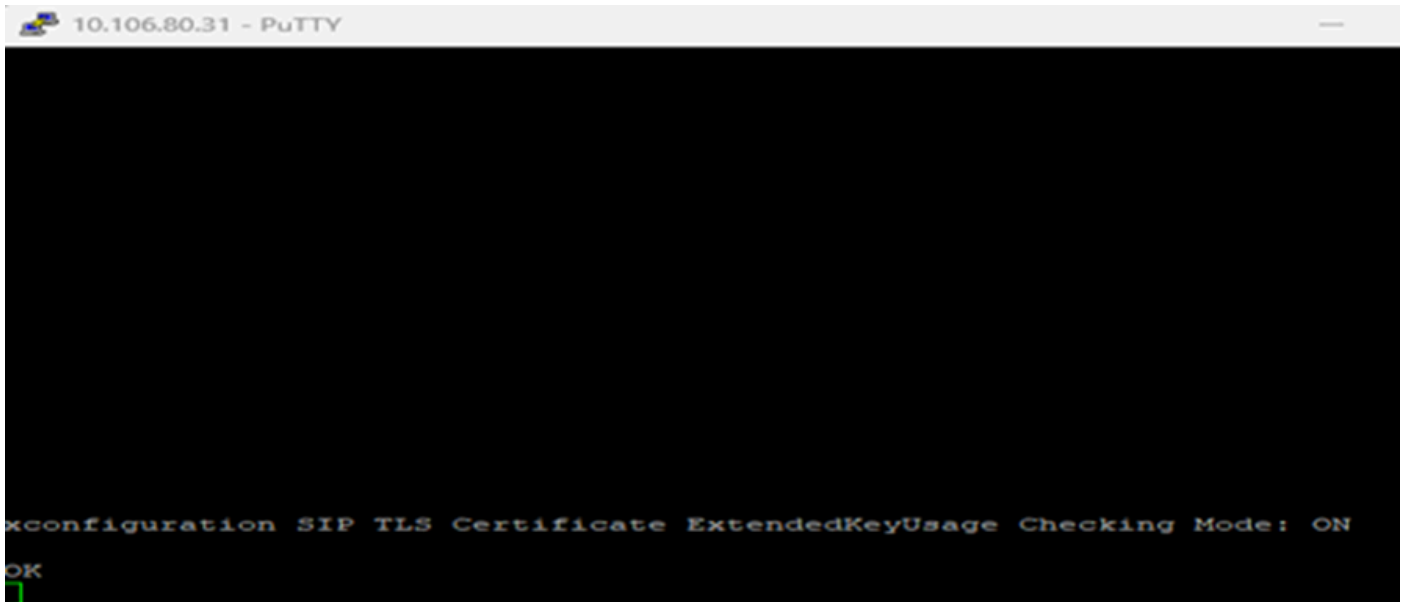
MRA-cliantaanmelding en WebRTC-proxyfuncties werken niet. Je zou je toevlucht kunnen nemen tot een privé-CA.

Testcase 1

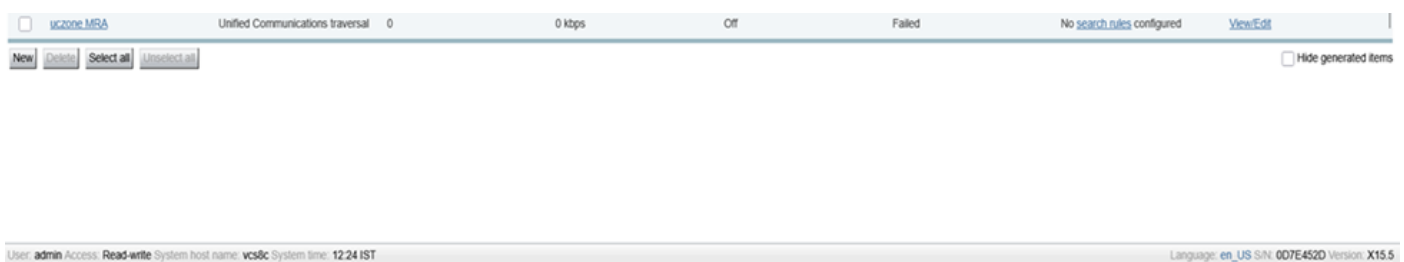
- Wanneer ECU-controle "ON" is op Expressway E
- Wanneer client- en servercertificaat op Expressway core Server alleen ECU heeft
- UC-zonestatus is MISLUKT

On Expressway-Edge ExtendedKeyUsage controleren ON.

xconfiguration SIP TLS Certificate ExtendedKeyUse Checking Mode: Aan:



Mislukte Unified Communication Zone:



Expressway E-logs tonen waar 10.106.80.16 = Expressway Core, 10.106.80.31 = Expressway Edge:



Testcase 2

- Wanneer ECU-controle is UITGESCHAKELD op Expressway E
- Wanneer client- en servercertificaat op Expressway Core-server alleen ECU heeft
- UC-zonestatus is ACTIEF

Schakel de ECU-controle uit op Expressway E.

xconfiguration SIP TLS Certificate ExtendedKeyUse Checking Mode: Uit

```

10.106.80.31 - PuTTY
xconfiguration SIP TLS Certificate ExtendedKeyUsage Checking Mode: Off
OK

```

Unified communication zone Actief:

The screenshot shows a network management interface with a status bar at the top. The status bar includes: 'uczone.MRA', 'Unified Communications traversal', '0', '0 kbps', 'Off', 'Active', 'No search rules configured', and 'View/Edit'. Below the status bar are buttons for 'New', 'Delete', 'Select all', and 'Unselect all'. At the bottom, there is a footer with user information: 'User: admin Access: Read-write System host name: vcsbc System time: 12:27 IST' and language/version info: 'Language: en_US S/N: 007E452D Version: X15.5'.

De ssh-tunnels mislukten echter nog steeds:

Unified Communications SSH tunnels status

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.

Target	Domain	Status	Tunnel Created	Reason	Peer
smartslave.vikdutta.com	555.federation.com	Failed	29/03/2026 07:09:26	Permission denied	10.106.80.16
smartslave.vikdutta.com	tomcat.com	Failed	29/03/2026 07:09:26	Permission denied	10.106.80.16

Expressway-gebeurtenislogboeken:

Results

2026-03-29T12:33:12.384+05:30	ssh: Detail="ssh: connect to host smartslavsmarts 22222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:31:56.811+05:30	ssh: Detail="ssh: connect to host smartslavsmarts 22222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:28:56.519+05:30	ssh: Detail="ssh: connect to host smartslavsmarts 22222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:28:24.476+05:30	ssh: Detail="ssh: connect to host smartslavsmarts 22222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:27:52.445+05:30	ssh: Detail="ssh: connect to host smartslavsmarts 22222:port 2222: Connection timed out" Level="ERROR"

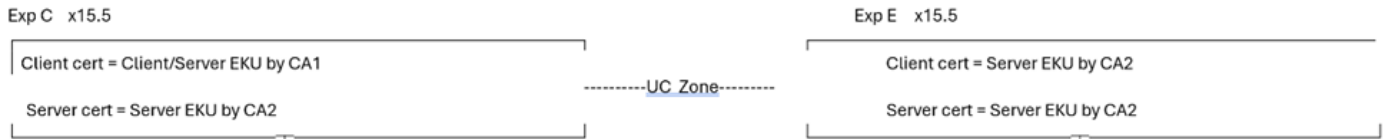
Voorwaarde 2.1: Succesgeval

CA 1 = Interne CA

CA 2 = Openbare CA

- Waar het Expressway-kernclientcertificaat is ondertekend door CA 1 (interne CA) en waarin Client/Server-EKU is opgenomen, worden beide ondertekend.
- Het Expressway-kernservercertificaat is ondertekend door CA 2 public CA en bevat alleen Server EKU.

- Het Expressway Edge-servercertificaat is ondertekend door CA 2 public CA en bevat alleen Server EKU.
- Het Expressway Edge-clientcertificaat is ondertekend door CA 2 public CA en bevat alleen server-EKU.



Deze voorwaarde is een succesgeval. Ongeacht of de EKU-controlemodus AAN/UIT is, worden de zone voor Unified Communication en de SSH-tunnel beide actief. MRA-klienten werken.

Het maakt niet uit of de Expressway Edge EKU-controle UIT of AAN is. Het Expressway-kernclientcertificaat bevat client-EKU:

```
10.106.80.31 - PuTTY
xconfiguration SIP TLS Certificate ExtendedKeyUsage Checking Mode: Off
OK
```

```
10.106.80.31 - PuTTY
xConfiguration SIP TLS Certificate ExtendedKeyUsage Checking Mode: "On"
OK
```

SSH-tunnels op Expressway-kern Actief:

CISCO Cisco Expressway-C

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

Unified Communications SSH tunnels status

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.

Target	Domain	Status	Tunnel Created
smartslave.vikdutta.com	tomcat.com	Active	29/03/2026 07:21:27
smartslave.vikdutta.com	555.federation.com	Active	29/03/2026 07:19:26

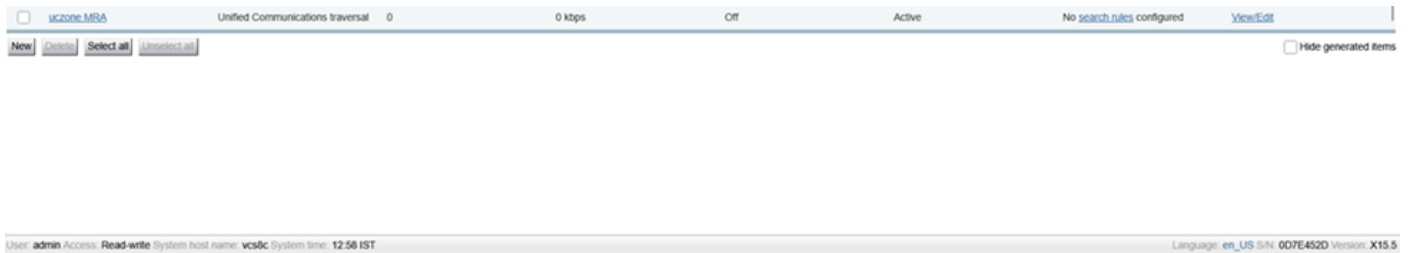
SSH-tunnels op Expressway Edge Active:

Unified Communications SSH tunnels status

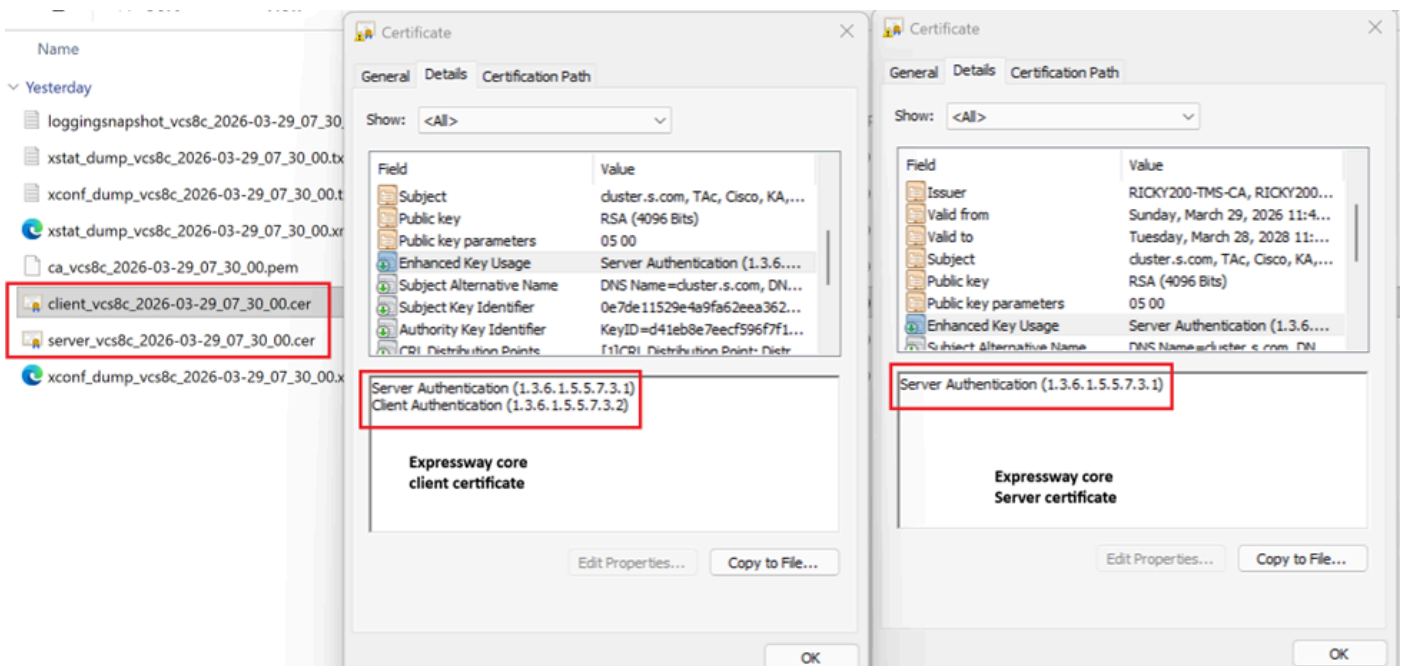
Warning: The CSRF Protection status is automatically enabled after the software upgrade. We recommend keeping CSRF protection Enabled. To change it, please log in to the CLI.

Target	Domain	Status	Tunnel Created
vcs8c	tomcat.com	Active	29/03/2026 07:21:27
vcs8c	555.federation.com	Active	29/03/2026 07:19:26

MRA-zonestatus voor Unified Communication Actief:



- Expressway-Core-clientcertificaat heeft Server ECU en Client ECU.
- Expressway Core Server-certificaat heeft alleen server-ECU.



MRA Client logt in en registreert:

The screenshot shows the Cisco Jabber interface. The main window is titled "Cisco Jabber" and shows the user "hanu@". A search bar is visible. A "Connection Status" window is open, displaying the following information:

Cisco Jabber
Version 12.6.1 (284405)

✓ Softphone	Status: Connected
	Protocol: SIP
	Address: 10.106.79.162 (CCMCIP - Expressway) (IPv4)
	Device: CSFHanu
	Line: 7777
Deskphone	Status: Not connected
	Protocol: CTI
	Address: (CTI) (Unknown)
✓ Outlook address book	Status: Last connection successful.
	Protocol: MAPI
	Address: Outlook (Unknown)
✓ Directory	Status: Last connection successful.

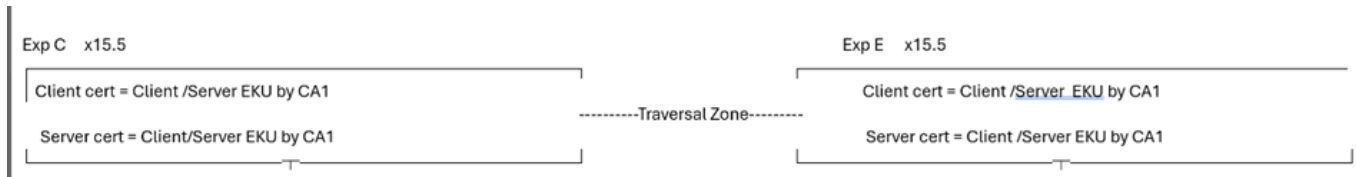


Opmerking: vergelijk en noteer EKU's die aanwezig zijn in certificaten voor MRA en WebRTC-proxy om te werken. Het is een vergelijking tussen werkende en niet-werkende implementatie.

Voorwaarde 3: Ondertekent alle certificaten met privé-CA

CA 1 = Interne CA

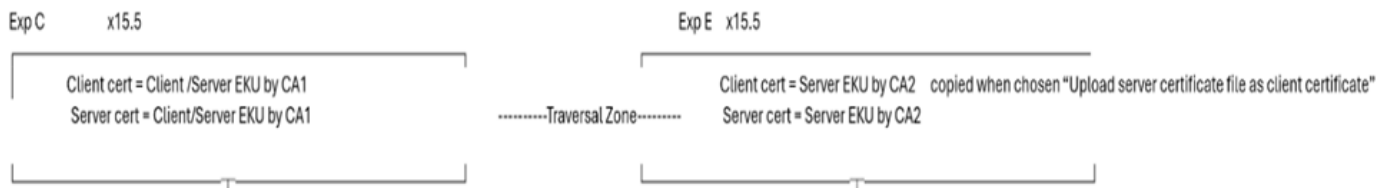
CA 2 = Openbare CA



In voorwaarde 3 worden alle certificaten ondertekend door interne CA (CA1).

- Wanneer Expressway-E een TLS-verbinding verzendt, moet CA 1 root/intermediate worden uitgewisseld met een far-end entiteit. Als far-end geen mogelijkheid heeft of niet toestaat dat een privé CA-certificaat wordt geüpload, is de TLS-verbinding mislukt.
- MRA-clients krijgen certificaten om pop-ups te accepteren als het privécertificaat zich niet in de OS-vertrouwenswinkel bevindt.

Voorwaarde 4: Expressway Edge heeft alleen openbare certificaten met server-EKU



In conditie 4 zijn de Expressway-core client- en servercertificaten (CA1) intern CA-ondertekend en zijn zowel client- als server-EKU aanwezig. Het Expressway E-servercertificaat is openbaar, CA-ondertekend en heeft alleen server-EKU. Servercertificaat wordt gekopieerd naar clientcertificaatarchief en kiest Servercertificaatbestand uploaden als clientcertificaat.

In Voorwaarde 4, wanneer de TLS-verbinding wordt gemaakt naar far-end, als Expressway -E een TLS-client hallo stuurt, moet far-end de client-EKU-controle uitschakelen (omdat het clientcertificaat geen client-authentische ECU heeft), anders is de TLS-verbinding mislukt.

Er kunnen veel meer voorwaarden of scenario's in het veld zijn op basis van gebruikersimplementatie en gebruiksscenario's en alle kunnen niet worden gedekt vanwege mijn beperkte gedachtestroom. Punten om te onthouden zijn echter:

- # ALS Expressway een client wordt tijdens TLS-handshake, wordt het clientcertificaat aan peers gepresenteerd.
- #IF Expressway wordt Server tijdens TLS-handshake; het servercertificaat wordt aan peer gepresenteerd.

Deze redenering is vastgesteld met deze testgevallen.

Scenario 1

Voor dit scenario presenteert Expressway het clientcertificaat tijdens de MTLS-handshake met Webex.

Een videogesprek naar de Webex-bijeenkomst:

Voorbeeld gespreksstroom Jabber -à CUCM -à Exp Core - à Exp Edge - à Webex

10.106.80.31= Rand snelweg

163 129 37 33 = Webex

```
2026-03-24T11:54:26.106+00:00 smartslave tvcs: UTCTime="2026-03-24 11:54:26,106"  
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="10.106.80.31" Local-port="25002"  
DST-ip="163.129.37.33" DST-port="5061"
```

Expressway Edge heeft een clientcertificaat met dit serienummer (2f0000004c869c77c8981becde0000000004c).

Expressway Edge stuurt client hallo naar 'Webex' tijdens TLS-onderhandeling en verzendt vervolgens clientcertificaat.

Serienummer 2f0000004c869c77c8981becde0000000004c:

1. Expressway Edge stuurt client hello (pkt= 13699) naar 'Webex tijdens mTLS-onderhandeling.
2. Webex stuurt een server hallo naar Expressway Edge (pkt=13701).
3. Webex stuurt het certificaat naar Expressway Edge (pkt=13711).
4. Webex vraagt het Expressway edge-certificaat "CertificateRequest" aan (pkt=13715).
5. Expressway Edge stuurt het certificaat naar Webex (pkt=13718).

(screenshot)

```

13698 2026-03-24 17:25:20.911700 10.106.80.31 163.129.37.32 TCP 66 25003 + 5061 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=840949379 TSecr=3608271268
13699 2026-03-24 17:25:20.912773 10.106.80.31 163.129.37.32 TLSv1.2 583 Client Hello
13700 2026-03-24 17:25:20.956852 163.129.37.32 10.106.80.31 TCP 66 5061 + 25003 [ACK] Seq=1 Ack=518 Win=28544 Len=0 TSval=3608271312 TSecr=840949380
13701 2026-03-24 17:25:20.956925 163.129.37.32 10.106.80.31 TLSv1.2 156 Server Hello
13702 2026-03-24 17:25:20.956963 10.106.80.31 163.129.37.32 TCP 66 25003 + 5061 [ACK] Seq=518 Ack=91 Win=64512 Len=0 TSval=840949424 TSecr=3608271313
13703 2026-03-24 17:25:20.957044 163.129.37.32 10.106.80.31 TCP 1300 5061 + 25003 [ACK] Seq=91 Ack=518 Win=28544 Len=1242 TSval=3608271313 TSecr=840949380 [TCP PDU reassembled in 13711]
13704 2026-03-24 17:25:20.957049 10.106.80.31 163.129.37.32 TCP 66 25003 + 5061 [ACK] Seq=518 Ack=1333 Win=67584 Len=0 TSval=840949425 TSecr=3608271313
13705 2026-03-24 17:25:20.957163 163.129.37.32 10.106.80.31 TCP 1300 5061 + 25003 [ACK] Seq=1333 Ack=518 Win=28544 Len=1242 TSval=3608271313 TSecr=840949380 [TCP PDU reassembled in 13711]
13706 2026-03-24 17:25:20.957170 10.106.80.31 163.129.37.32 TCP 66 25003 + 5061 [ACK] Seq=518 Ack=2575 Win=70656 Len=0 TSval=840949425 TSecr=3608271313
13707 2026-03-24 17:25:20.957175 163.129.37.32 10.106.80.31 TCP 1300 5061 + 25003 [ACK] Seq=2575 Ack=518 Win=28544 Len=1242 TSval=3608271313 TSecr=840949380 [TCP PDU reassembled in 13711]
13708 2026-03-24 17:25:20.957179 10.106.80.31 163.129.37.32 TCP 66 25003 + 5061 [ACK] Seq=518 Ack=3817 Win=72704 Len=0 TSval=840949425 TSecr=3608271313
13709 2026-03-24 17:25:20.957184 163.129.37.32 10.106.80.31 TCP 1300 5061 + 25003 [ACK] Seq=3817 Ack=518 Win=28544 Len=1242 TSval=3608271313 TSecr=840949380 [TCP PDU reassembled in 13711]
13710 2026-03-24 17:25:20.957188 10.106.80.31 163.129.37.32 TCP 66 25003 + 5061 [ACK] Seq=518 Ack=5059 Win=71680 Len=0 TSval=840949425 TSecr=3608271313
13711 2026-03-24 17:25:20.957193 163.129.37.32 10.106.80.31 TLSv1.2 378 Certificate
13712 2026-03-24 17:25:20.957215 10.106.80.31 163.129.37.32 TCP 66 25003 + 5061 [ACK] Seq=518 Ack=5371 Win=72704 Len=0 TSval=840949425 TSecr=3608271313
13713 2026-03-24 17:25:20.958101 163.129.37.32 10.106.80.31 TLSv1.2 404 Server Key Exchange
13714 2026-03-24 17:25:20.958110 10.106.80.31 163.129.37.32 TCP 66 25003 + 5061 [ACK] Seq=518 Ack=5709 Win=73728 Len=0 TSval=840949426 TSecr=3608271314
13715 2026-03-24 17:25:20.958341 163.129.37.32 10.106.80.31 TLSv1.2 124 Certificate Request, Server Hello Done
13716 2026-03-24 17:25:20.958350 10.106.80.31 163.129.37.32 TCP 66 25003 + 5061 [ACK] Seq=518 Ack=5767 Win=73728 Len=0 TSval=840949426 TSecr=3608271315
13717 2026-03-24 17:25:20.967687 10.106.80.31 163.129.37.32 TCP 2550 25003 + 5061 [PSH, ACK] Seq=518 Ack=5767 Win=73728 Len=2484 TSval=840949435 TSecr=3608271315 [TCP PDU reassembled in 13718]
13718 2026-03-24 17:25:20.967707 10.106.80.31 163.129.37.32 TLSv1.2 1170 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
13719 2026-03-24 17:25:20.971327 10.106.80.31 10.106.80.31 TCP 66 5061 + 25003 [ACK] Seq=5767 Ack=3002 Win=26112 Len=0 TSval=3608271365 TSecr=840949435
13720 2026-03-24 17:25:21.008884 163.129.37.32 10.106.80.31 TCP 66 5061 + 25003 [ACK] Seq=5767 Ack=3002 Win=26112 Len=0 TSval=3608271365 TSecr=840949435
13721 2026-03-24 17:25:21.010881 163.129.37.32 10.106.80.31 TLSv1.2 72 Change Cipher Spec

```

Length: 2936
Certificates Length: 2933
Certificates (2933 bytes)
Certificate Length: 2834

```

Certificate [..]: 308207ee308206d6a0030201020132f0000004c869c77c8981becde0000000004c300006092a864806f700101000500304f31133011006a0992268993f22c6401191603636fd3118301006
  signedCertificate
    version: v3 (2)
    serialNumber: 0x2f000004c869c77c8981becde0000000004c
    signature (sha256withRSAEncryption)
    issuer: rdnsSequence (0)
    rdnsSequence: 3 items (id-at-commonName=bgluclab-WIN-DC-01-CA,dc=bgluclab,dc=com)
      rdnsSequence item: 1 item (dc=com)
      rdnsSequence item: 1 item (dc=bgluclab)
      rdnsSequence item: 1 item (id-at-commonName=bgluclab-WIN-DC-01-CA)
    validity
      notBefore: utcTime (0)
      notAfter: utcTime (0)
    subject: rdnsSequence (0)

```

Clientcertificaat van Expressway Edge:

The screenshot shows a file explorer with a list of files, including several certificates. A 'Certificate' dialog box is open, displaying the following details:

Field	Value
Version	V3
Serial number	2f000004c869c77c8981becd...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	bgluclab-WIN-DC-01-CA, bglu...
Valid from	Tuesday, March 24, 2026 4:5...
Valid to	Thursday, March 23, 2028 4:5...
Subject	cluster.s.com, bar, rison, fl...

The serial number field is highlighted with a red box, and its full value, 2f000004c869c77c8981becde0000000004c, is shown in a separate red box below the dialog.

Scenario 2

Expressway wordt een serverentiteit tijdens de mTLS-handshake en presenteert het

servercertificaat:

Waar Expressway een servercertificaat presenteert, heeft Expressway een beveiligde buurzone boven 5061 met de verificatiennaam ON.

Beveiligde buurzone tussen Expressway node x15.5 en Expressway node x8.11.4:

10.106.80.15 (x8.11.4) sends a client hello to 10.106.80.16 (x15.5) (pkt=736)

10.106.80.16 sends a server hello to 10.106.80.15 (pkt=738)

10.106.80.16 (x15.5) presents its server cert during TLS handshake (pkt=742) and requests client's cert

10.106.80.15 (x8.11.4) sends client certificate (pkt=744)

The image displays a network traffic capture (likely Wireshark) showing a TLS handshake between two hosts: 10.106.80.15 (client) and 10.106.80.16 (server). The capture includes several packets:

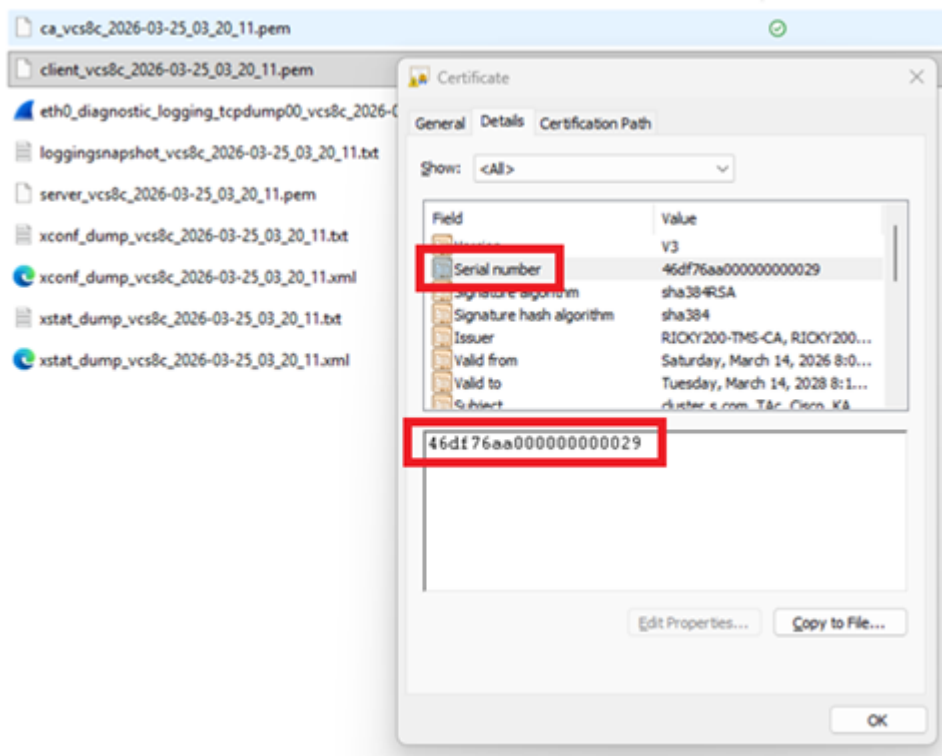
- 736: Client Hello from 10.106.80.15 to 10.106.80.16 (pkt=736).
- 738: Server Hello from 10.106.80.16 to 10.106.80.15 (pkt=738).
- 742: Certificate, Server Key Exchange, Certificate Request, Server Hello Done from 10.106.80.16 to 10.106.80.15 (pkt=742).
- 744: Certificate from 10.106.80.15 to 10.106.80.16 (pkt=744).

The details pane for the Certificate (744) shows the following structure:

- Length: 2923
- Handshake Protocol: Certificate
- Handshake Type: Certificate (11)
- Length: 2919
- Certificates Length: 2916
- Certificates (2916 bytes)
- Certificate Length: 2005
- Certificate [-]: 308207d1308206b9a00302010202046d776aa0000000029300d0692a864886f70d01010c05000304931133011060a0992268993f22c6401191603636fd31183016060a0992268993f22c...
- signedCertificate
 - version: v3 (2)
 - serialNumber: 0x46d776aa0000000029
 - signature (sha384withRSAEncryption)
 - Algorithm: Sha384withRSAEncryption
 - Issuer: rdnSequence (0)
 - rdnSequence: 3 items (id-at-commonName=RICKY200-THS-CA,dc=RICKY200,dc=com)
 - validity

The hex dump on the right shows the raw data of the certificate, starting with 0030 f7 0d 01 01 0c 05 00 30 49 31 13 30 11 06 0a 09 ...

Deze schermafbeelding toont het servercertificaat als overeenkomende serienummers:



Testcase 3: MRA-client is voorzien voor aanmelding en de workflow omvat verificatie van het verkeersservercertificaat tussen Expressway Core en CUCM.

10.106.80.16 = Expressway Core x15.5

10 106 80 38 = CUCM

- Exp C 16 stuurt een klant hallo op 6972 TFTP.
- Exp C 16 verzendt een clientcertificaat tijdens de TLS-handshake.

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.