

Navigieren Client ECU Sunset mit Expressway x15.5

Einleitung

In diesem Dokument wird die Navigation durch den Client-EKU-Sonnenuntergang mit Cisco Expressway x15.5 beschrieben.

Hintergrundinformationen

Digitale Zertifikate sind von vertrauenswürdigen Zertifizierungsstellen (Certificate Authorities, CAs) ausgestellte elektronische Zertifikate, die die Kommunikation zwischen Servern und Clients durch die Gewährleistung von Authentifizierung, Datenintegrität und Vertraulichkeit schützen. Diese Zertifikate enthalten Extended Key Usage (EKU)-Felder, die ihren Zweck definieren:

- Die Serverauthentifizierungs-EKU (id-kp-serverAuth) wird verwendet, wenn ein Server sein Zertifikat zum Identitätsnachweis vorlegt.
- Die Client-Authentifizierungs-EKU (id-kp-clientAuth) wird in gegenseitigen TLS-Verbindungen (mTLS) verwendet, bei denen sich beide Parteien gegenseitig authentifizieren.

Bisher konnte ein einzelnes Zertifikat sowohl Server- als auch Clientauthentifizierungs-EKUs enthalten, sodass es für zwei Zwecke verwendet werden konnte. Dies ist besonders wichtig für Produkte wie Cisco Expressway, die in verschiedenen Verbindungsszenarien sowohl als Server als auch als Client fungieren.

Problemdefinition

Änderung der Chrome-Stammprogrammrichtlinie

Ab Juni 2026 schränkt die Chrome Root Program Policy die im Chrome Root Store enthaltenen Zertifikate der Root Certificate Authority (CA) ein, wobei die Mehrzweck-Roots schrittweise abgeschafft werden, um alle Public-Key Infrastructure (PKI)-Hierarchien so auszurichten, dass sie nur für Anwendungsfälle der TLS-Serverauthentifizierung verwendet werden.

Wichtige Richtlinienanforderungen

- Öffentliche Stammzertifizierungsstellen müssen die Extended Key Usage (EKU) NUR für die Serverauthentifizierung (id-kp-serverAuth) geltend machen.
- Die Aufnahme der Clientauthentifizierungs-EKU in diese Zertifikate ist nicht zulässig.
- Keine gemischten Stammzertifizierungsstellen mehr für TLS-Zertifikate für öffentliche Server.
- Durchsetzungszeitleiste: Juni 2026

Öffentliche Zertifizierungsstelle - Reaktionszeit

- Oktober 2025: Viele öffentliche CAs (DigiCert, Sectigo, SSL) begannen standardmäßig mit der Ausgabe von Zertifikaten nur für Server.
- Mai 2026: Öffentliche Zertifizierungsstellen-Server stellen keine Client Authentication/EKU-Zertifizierungen mehr aus
- Juni 2026: Chrome Root-Programm-Richtlinie wird voll wirksam



Anmerkung: Diese Richtlinie gilt nur für Zertifikate, die von öffentlichen Zertifizierungsstellen ausgestellt wurden. Private PKI und selbstsignierte Zertifikate sind von dieser Richtlinie nicht betroffen.

Wenn Sie mehr über die Auswirkungen der Sonnenuntergang-Einstellung von Client EKU auf Expressways erfahren möchten, lesen Sie [Expressway für Client Auth EKU Sonnenuntergang in öffentlichen Zertifizierungsstellenzertifikaten vorbereiten.](#)

Expressway Release x15.5 mit Lösung

Expressway x15,5

Expressway x15.5 kommt mit einem Vorschlag zur Behebung eines Problems, das durch die Sonnenuntergang der Client-EKU durch alle öffentlichen Zertifizierungsstellen entsteht. Dies ist ein globales Problem, das alle Anbieter/Bereitstellungen betrifft, die öffentliche PKI-Zertifikate verwenden möchten.

x15.4, eine frühere Version, verfügte über einen CLI-Befehlsschalter, der es dem Administrator ermöglichte, ein Server-EKU-Only-Zertifikat (kein Client-EKU vorhanden) auf Expressway E hochzuladen.



Anmerkung: Dieser Befehl ist für x15.5 veraltet.

X15.5-Zertifikatspeichererweiterung

x15.5 verfügt über zwei Zertifikatspeicher:

1. Server-Zertifikatspeicher
2. Client-Zertifikatspeicher


Expressways (Single NIC oder Dual NIC): Beide Expressway-Schnittstellen können je nach Bedarf zwei Zertifikatspeicher nutzen.


Beispiel:


- Wenn die Schnellstraße während des TLS-Handshakes als Client fungiert, wird ein Client-Zertifikat präsentiert.
- Wenn die Schnellstraße während des TLS-Handshakes als Server fungiert, wird ein Serverzertifikat angezeigt.





Anmerkung: Beide Zertifikatspeicher (Client und Server) verwenden dieselbe Bibliothek vertrauenswürdiger Zertifizierungsstellen. Stellen Sie sicher, dass die Zertifizierungsstelle, die Server- und Clientzertifikate signiert hat, ordnungsgemäß in den Trust Store hochgeladen wird. Diagnoseprotokolle enthalten jetzt Serverzertifikate und Clientzertifikate im PEM-Dateiformat.


 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 von X15.4 oder früheren Versionen auf X15.5

Wenn ein Upgrade durchgeführt wird, wird das Serverzertifikat aus x15.4 oder einer früheren Version des Expressway-Serverzertifikatsspeichers in den Clientzertifikatsspeicher auf x15.5 kopiert. Die Client- und Serverzertifikatsspeicher auf x15.5 verfügen über dasselbe Zertifikat.

Beispiel mit Screenshots

Expressway-Server auf 15.4, aktuelles Serverzertifikat Seriennummer 46:df:76:aa:00:00:00:00:29

Zertifikat:

Version: 3 (0 x 2)

Seriennummer:

46:df:76:aa:00:00:00:00:29

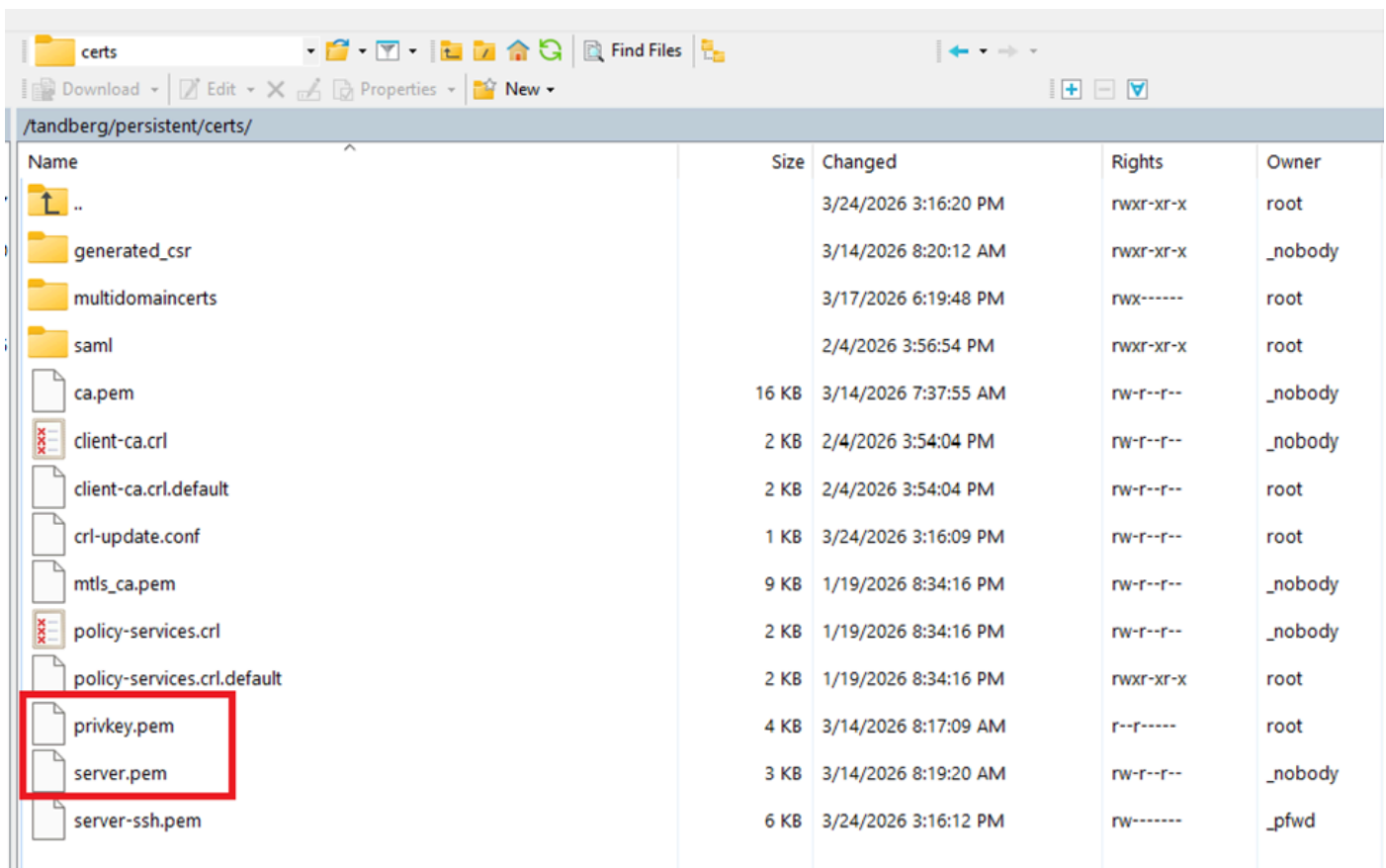
Gültigkeit

Nicht vor: 14. März 2026 02:37:40 Uhr GMT

Nicht nachher: 14.03.2028 02:47:40 Uhr GMT

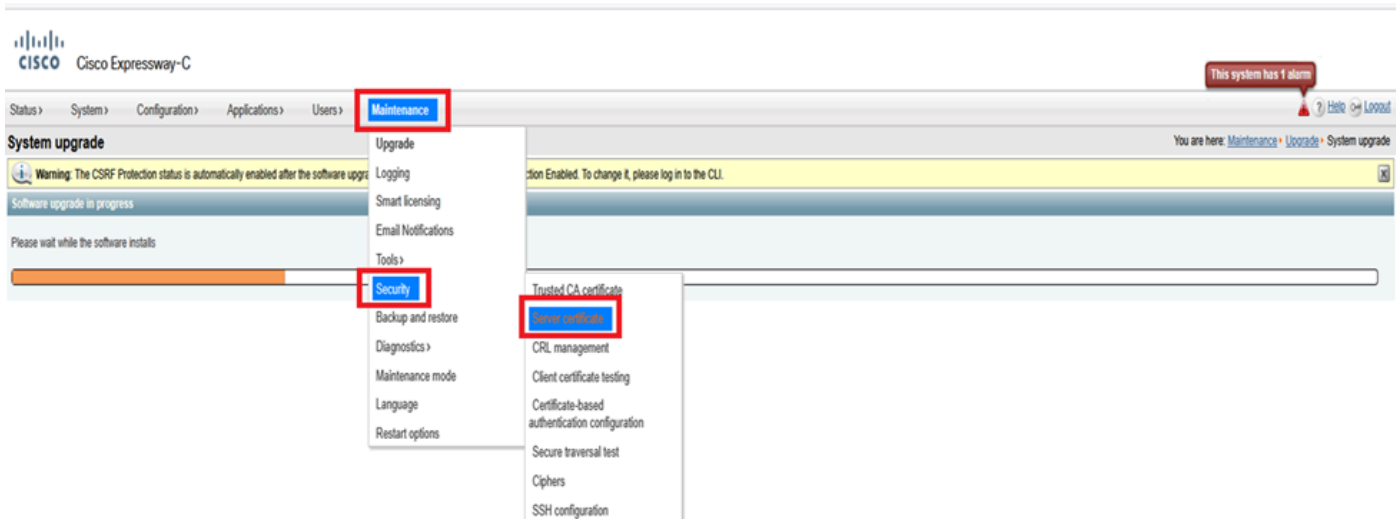
Betreff: C = IN, ST = KA, L = KA, O = Cisco, OU = TAc, CN = cluster.s.com

Expressway-Dateisystem, Verzeichnis "persistent/cert" auf x15.4:



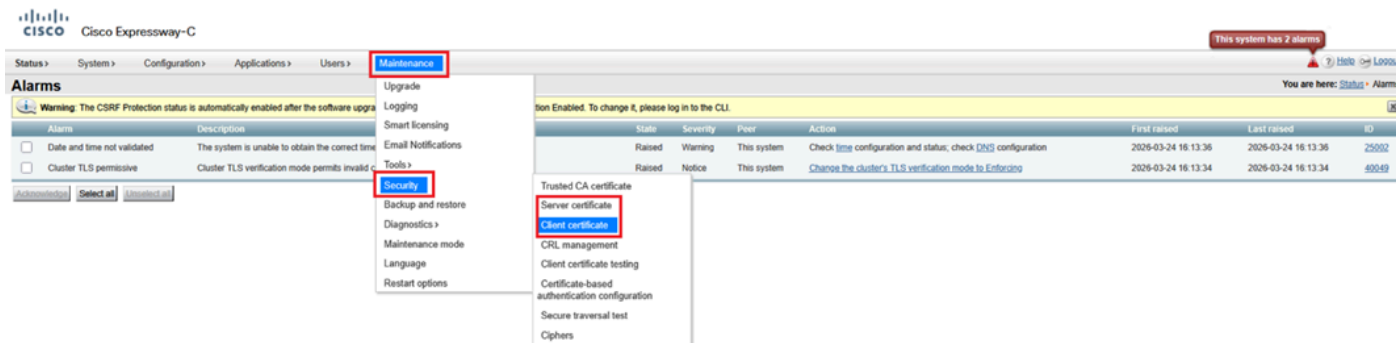
Name	Size	Changed	Rights	Owner
..		3/24/2026 3:16:20 PM	rw-r--r--	root
generated_csr		3/14/2026 8:20:12 AM	rw-r--r--	_nobody
multidomaincerts		3/17/2026 6:19:48 PM	rw-r--r--	root
saml		2/4/2026 3:56:54 PM	rw-r--r--	root
ca.pem	16 KB	3/14/2026 7:37:55 AM	rw-r--r--	_nobody
client-ca.crl	2 KB	2/4/2026 3:54:04 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--	_pfwd

Expressway-Menü (Maintenance > Security > Server certificate) auf x15.4 (nur Server-Zertifikatfeld vorhanden):



Nach erfolgreichem Upgrade auf x15.5

Hier sehen Sie 2 Zertifikatoptionen unter Wartung > Sicherheit > Clientzertifikat und Serverzertifikate. Nach dem Upgrade auf x15.5 zeigt sowohl das Server- als auch das Client-Zertifikatportal auf dem Webadministrator dasselbe Zertifikat an, da das Serverzertifikat von x15.4 in den Client-Zertifikatspeicher auf x15.5 kopiert wurde.



Nach dem Upgrade auf x15.5 wurden ein vorhandenes Zertifikat und ein privater Schlüssel in den Zertifikatspeicher des Clients kopiert.

Expressway-Dateisystem, Verzeichnis "persistent/cert" auf 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-Prüfung während TLS-Handshake

Auf x15.5 wurde ein neuer CLI-Befehl eingeführt, um die Verwendung des erweiterten Schlüssels (Extended Key Usage, EKU) während des TLS-Handshakes zu überprüfen. Der Standardwert ist "ON". Der Befehlssatz ist auf Expressway Core und Edge gültig.

Der Befehlssatz löst eine Überprüfung aller INBOUND SIP TLS-Verbindungen in Expressway aus. (eingehende Client-Hellos/Zertifikat dargestellt). Wenn "ON" aktiviert ist, wird überprüft, ob das vom TLS-Initiator präsentierte Zertifikat die Client-EKU im Zertifikat enthält. WENN DIESE OPTION AUSGESCHALTET IST, WIRD DIE PRÜFUNG UMGEHT. Die Server-EKU wird jedoch überprüft, ob sie im Zertifikat vorhanden ist.

xconfiguration SIP-TLS-Zertifikat, ExtendedKeyUsage-Überprüfungsmodus: EIN/AUS:



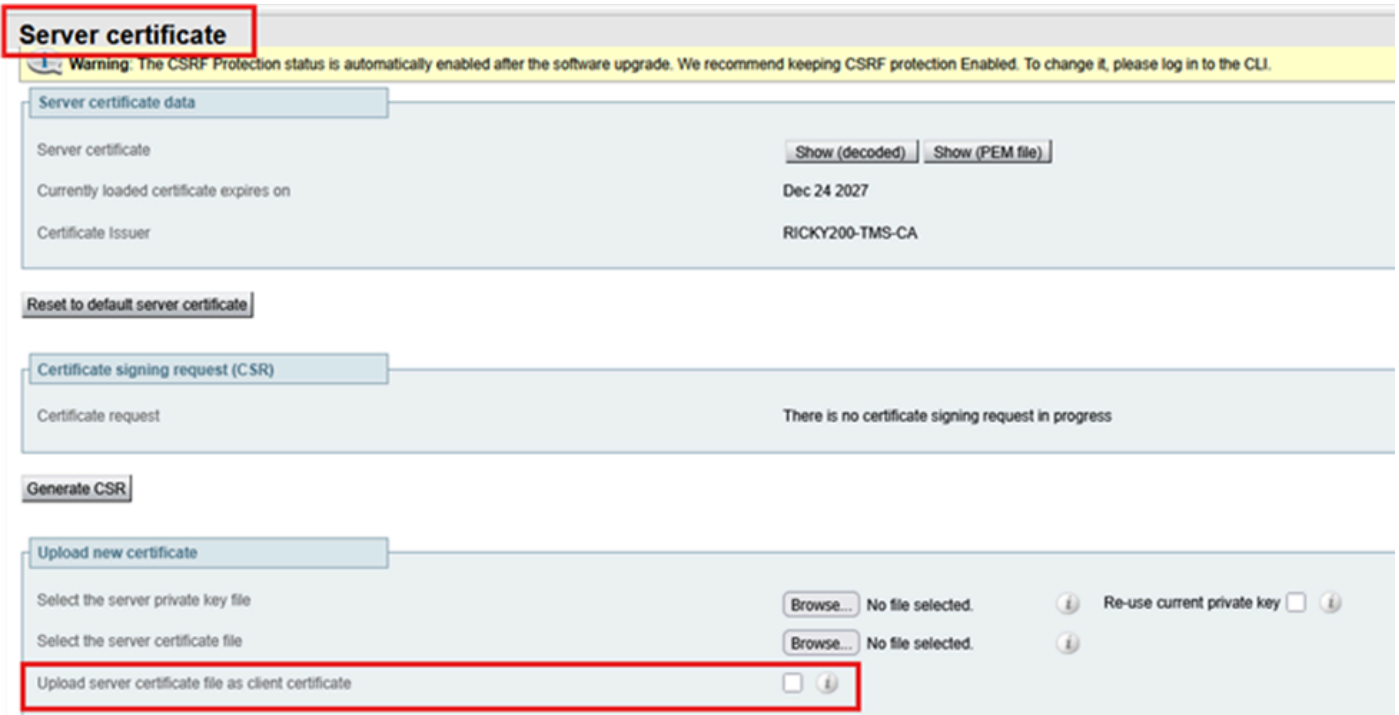
Anmerkung: Wenn Sie ein Clientzertifikat generieren und einen CSR signieren, der keine Client-EKU enthält (ein Beispiel für ein öffentlich signiertes CA-Zertifikat), können Sie dieses Zertifikat nicht manuell in den Clientzertifikatsspeicher hochladen. Daher müssen Sie sicherstellen, dass Zertifikate, die durch das Signieren eines CSR generiert werden, immer die Client-EKU enthalten (eine private Zertifizierungsstelle kann verwendet werden, um die Client-EKU einzufügen).



Tipp: Dieser Fehler wird deutlich, wenn Sie versuchen, ein CSR-signiertes Zertifikat, bei dem die Client-EKU fehlt, aus dem Client-Zertifikatsspeicher hochzuladen.

The screenshot shows the Cisco Expressway-E web interface. At the top left is the Cisco logo and the text 'Cisco Expressway-E'. Below this is a navigation menu with items: Status >, System >, Configuration >, Applications >, Users >, and Maintenance >. The main heading is 'Client certificate'. Below the heading, there is a yellow warning box with an information icon and the text: 'Invalid certificate: The file provided does not have a client usage attribute. Services requiring mutual TLS may not work.' Below this is another yellow warning box with an information icon and the text: '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 blue button labeled 'Client certificate data'.

Wenn Sie jedoch ein Zertifikat hochladen, das nur über eine Server-EKU (keine Client-EKU) verfügt, über den Server-Zertifikatsspeicher, und Server-Zertifikatdatei als Client-Zertifikat hochladen auswählen, wird das Zertifikat in den Client-Zertifikatsspeicher kopiert. Administratoren, die auf Expressway-Edge kein privates CA-signiertes Zertifikat verwenden möchten, können die Server-EKU nur aus dem Server-Zertifikatsspeicher in den Client-Zertifikatsspeicher kopieren.



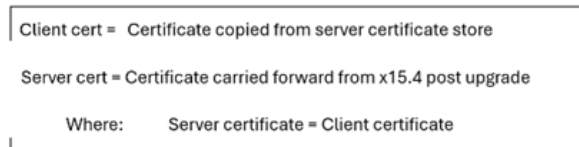
Mehrere Zertifikatspeicher, verschiedene Bereitstellungsszenarien

Da es jetzt zwei Zertifikatspeicher auf Expressway gibt, gibt es mehrere Szenarien für Zertifikatspeicher.

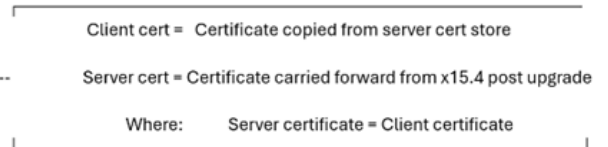
Bedingung 1: Upgrade

Wenn Expressway von x15.4 oder vor x15.5 aktualisiert wird, ist diese Bedingung wahr. Vorhandene Zertifikate aus x15.4-Version werden in zwei (2) Zertifikatspeicher kopiert. Auf dem x15.5-Client und -Server sind die Zertifikate identisch.

Exp C x15.5



Exp E x15.5

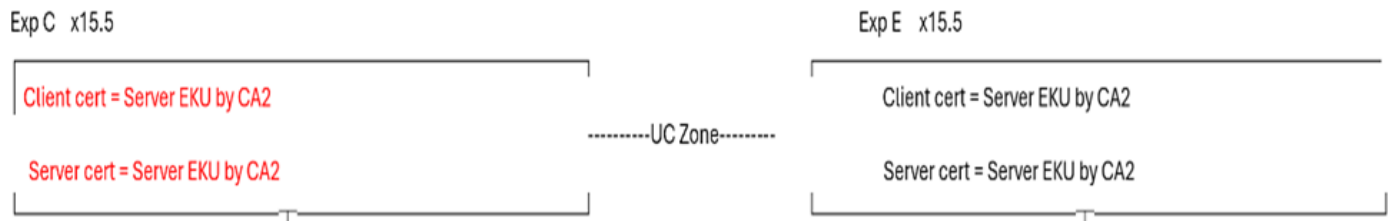


Bedingung 2: Wenn der Administrator ein neues Zertifikat auf x15.5 installiert (vorhandene Zertifikate abgelaufen)

CA 1 = Interne CA

CA 2 = Öffentliche Zertifizierungsstelle

In der Abbildung unten verfügt Expressway Core über ein Client-Zertifikat, bei dem der Server EKU nur von CA 2 (Public CA) signiert ist, und über ein Server-Zertifikat, bei dem der Server EKU nur von CA 2 (Public CA) signiert ist. Ebenso verfügt Expressway E über ein Client-Zertifikat mit dem Server EKU, der von CA2 (öffentliche CA) signiert ist, und ein Server-Zertifikat mit dem Server EKU, das nur von CA 2 (öffentliche CA) signiert ist.



Wenn das Expressway-Core-Serverzertifikat keine Client-EKU, Unified Communications Traversal Zone, MRA, aufweist, funktioniert der WebRTC-Proxy nicht. Stellen Sie sicher, dass das Expressway Core-Serverzertifikat über eine Client-EKU verfügt. Dies ist ein gängiger Anwendungsfall, bei dem Benutzer alle Zertifikate von einer öffentlichen Zertifizierungsstelle signieren. Da die öffentliche CA die Client-EKU nicht in Zertifikaten enthält, wird die Unified Communications-Überbrückungszone aktiviert.

Um die UC-Zone zu aktivieren, können Sie die EKU-Prüfung auf dem Expressway E deaktivieren. Dadurch wird der UC-Bereich aktiviert. SSH-Tunnel bleiben jedoch inaktiv. Ab heute ist für die SSH-Tunnelkommunikation auf 2222 eine Validierung der Client-EKU erforderlich.

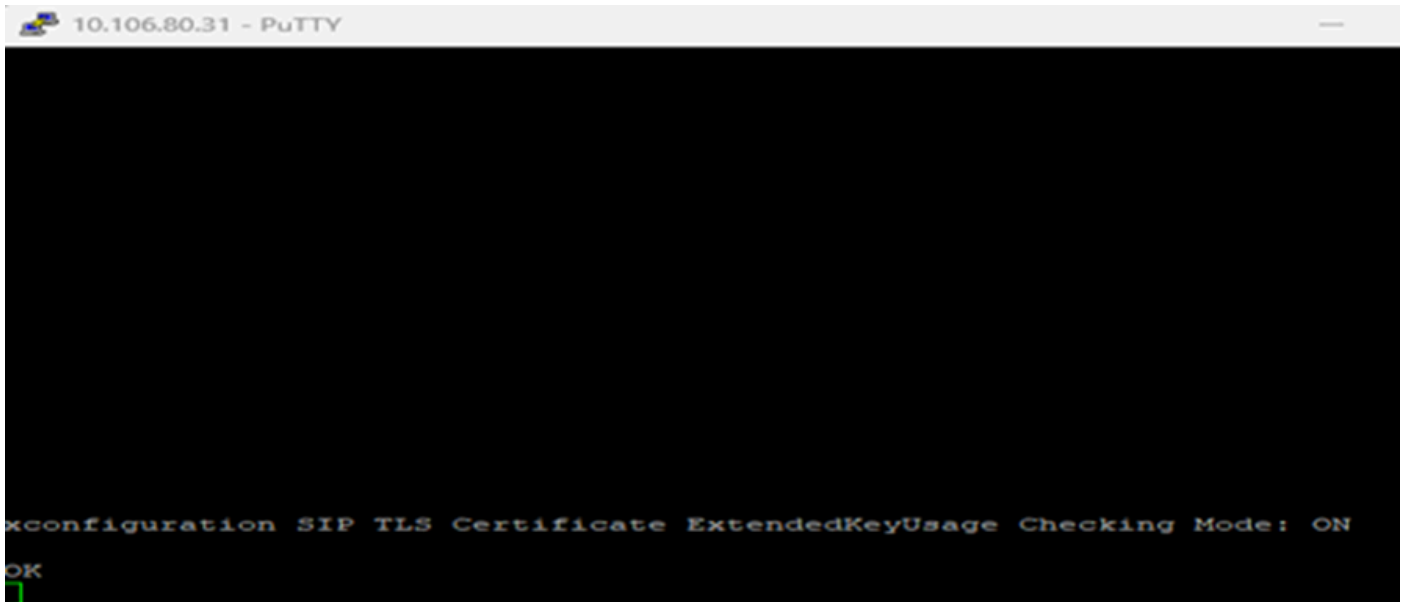
MRA-Client-Anmeldung und WebRTC-Proxy-Funktionen funktionieren nicht. Man könnte auf eine private CA zurückgreifen.

Testfall 1

- Wenn die EKU-Prüfung auf dem Expressway E "ON" ist
- Wenn das Client- und Server-Zertifikat auf dem Expressway-Core nur über Server-EKU verfügt
- UC-Zonenstatus ist FEHLGESCHLAGEN

Auf Expressway-Edge ExtendedKeyUsage Check ON.

xconfiguration SIP-TLS-Zertifikat, ExtendedKeyUsage-Überprüfungsmodus: On (Aktiviert):



Ausfall der Unified Communications-Zone:



Expressway-E-Protokolle zeigen an, wo 10.106.80.16 = Expressway Core, 10.106.80.31 = Expressway Edge:



Testfall 2

- Bei ECU-Prüfung auf Expressway E
- Wenn das Client- und Server-Zertifikat auf dem Expressway Core nur über den Server ECU verfügt
- Der Status der UC-Zone ist AKTIV.

Deaktivieren Sie die ECU-Prüfung auf dem Expressway E.

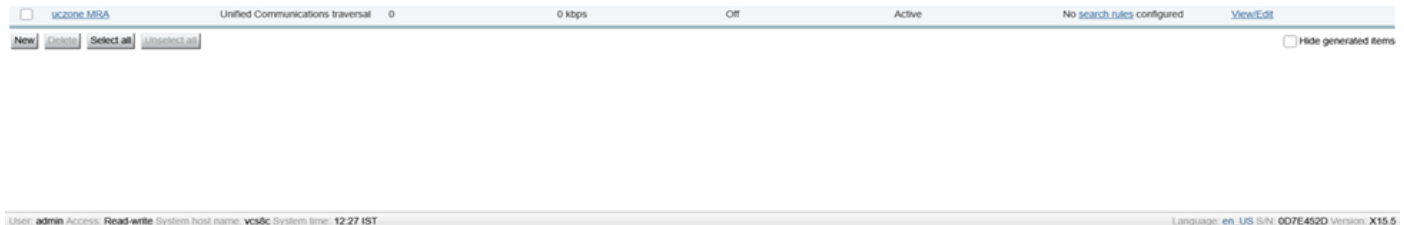
xconfiguration SIP-TLS-Zertifikat, ExtendedKeyUsage-Überprüfungsmodus: Aus

```

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

```

Unified Communication Zone Aktiv:



Allerdings sind die SSH-Tunnel noch immer ausgefallen:

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

Unified Communications SSH tunnels status You are here: [Status](#) > [Unified Communications status](#) > Unified Communication

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-Ereignisprotokolle:

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 smartslavsmartst 22222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:28:56.519+05:30	ssh: Detail="ssh: connect to host smartslavsmartst 22222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:28:24.476+05:30	ssh: Detail="ssh: connect to host smartslavsmartst 22222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:27:52.445+05:30	ssh: Detail="ssh: connect to host smartslavslast smt 2222:port 2222: Connection timed out" Level="ERROR"

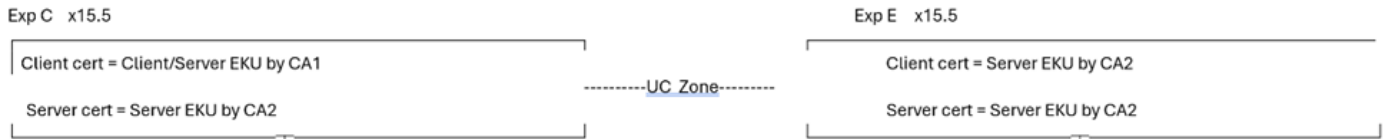
Bedingung 2.1: Erfolgsfall

CA 1 = Interne CA

CA 2 = Öffentliche Zertifizierungsstelle

- Wenn das Expressway Core Client-Zertifikat von CA 1 (interne CA) signiert wird und beide enthält, Client/Server EKU.
- Das Expressway Core Server-Zertifikat wird von der öffentlichen CA 2 signiert und enthält nur Server-EKU.

- Das Expressway Edge Server-Zertifikat wird von der öffentlichen CA 2 signiert und enthält nur Server-EKU.
- Das Expressway Edge-Clientzertifikat wird von der öffentlichen CA 2 signiert und enthält nur Server-EKU.



Diese Bedingung ist ein Erfolgsfall. Unabhängig davon, ob der EKU-Prüfmodus ON/OFF ist, werden sowohl die Unified Communication Zone als auch der SSH-Tunnel aktiviert. MRA-Clients arbeiten.

Dabei spielt es keine Rolle, ob der Expressway Edge EKU-Check AUS oder EIN ist. Das Expressway Core Client-Zertifikat enthält die 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-Tunnel auf Expressway Core Aktiv:

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-Tunnel am Expressway Edge aktiv:

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

Unified Communications MRA-Zonenstatus Aktiv:

uczone.MRA Unified Communications traversal 0 0 kbps Off Active No search rules configured View/Edit

New Update Select all Unselect all Hide generated items

User: admin Access: Read-write System host name: vcs8c System time: 12:58 IST Language: en_US S/N: 007E452D Version: X15.5

- Das Expressway-Core-Clientzertifikat weist Server-EKU und Client-EKU auf.
- Das Expressway Core Server-Zertifikat enthält nur Server-EKU.

The image shows two side-by-side windows displaying certificate details. The left window is titled 'Certificate' and shows the details for a client certificate. The 'Enhanced Key Usage' field is expanded, showing two entries: 'Server Authentication (1.3.6.1.5.5.7.3.1)' and 'Client Authentication (1.3.6.1.5.5.7.3.2)'. Both entries are highlighted with a red box. Below the table, the text 'Expressway core client certificate' is visible. The right window is also titled 'Certificate' and shows the details for a server certificate. The 'Enhanced Key Usage' field is expanded, showing one entry: 'Server Authentication (1.3.6.1.5.5.7.3.1)', which is highlighted with a red box. Below the table, the text 'Expressway core Server certificate' is visible.

MRA-Client meldet sich an und registriert:

The screenshot shows the Cisco Jabber interface. At the top, the window title is "Cisco Jabber" with standard Windows window controls. Below the title bar, there is a user profile section with a placeholder icon and the text "hanu@". A search bar with the text "Search or call" and a grid icon is also visible. The main content area is divided into a left sidebar with icons for calls and calendar, and a main pane titled "Connection Status".

The "Connection Status" window displays the following information:

- Cisco Jabber**
Version 12.6.1 (284405)
- Softphone** (indicated by a green checkmark):
 - 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** (indicated by a green checkmark):
 - Status: Last connection successful.
 - Protocol: MAPI
 - Address: Outlook (Unknown)
- Directory** (indicated by a green checkmark):
 - Status: Last connection successful.

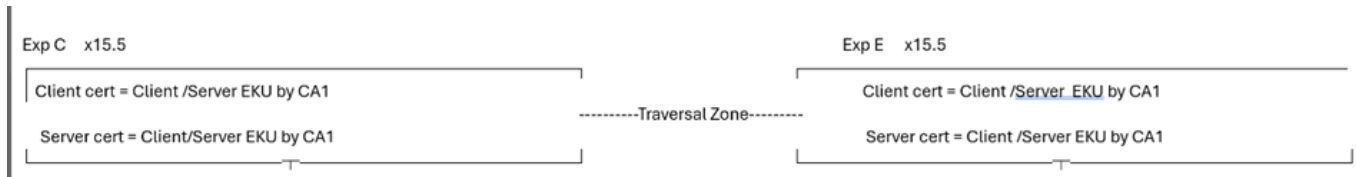


Anmerkung: Vergleichen und notieren Sie die EKUs, die in Zertifikaten für MRA- und WebRTC-Proxy vorhanden sind, damit sie funktionieren. Es handelt sich um einen Vergleich zwischen funktionierender und nicht funktionierender Bereitstellung.

Bedingung 3: Signiert alle Zertifikate mit privater Zertifizierungsstelle

CA 1 = Interne CA

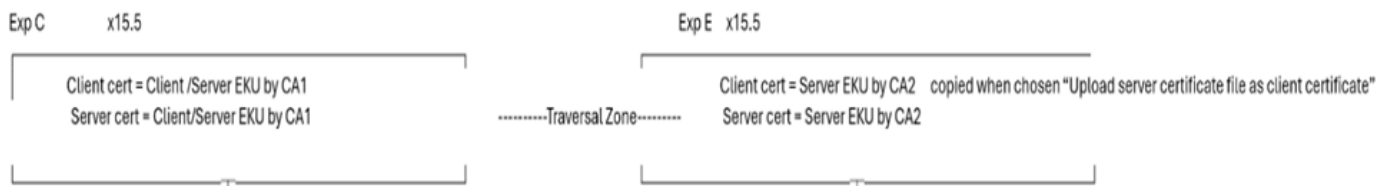
CA 2 = Öffentliche Zertifizierungsstelle



In Bedingung 3 werden alle Zertifikate von der internen CA (CA1) signiert.

- Wenn Expressway-E eine TLS-Verbindung sendet, muss CA1 Root/Intermediate mit einer Gegenstelle ausgetauscht werden. Wenn die Gegenstelle keine Funktion hat oder das Hochladen eines privaten Zertifizierungsstellenzertifikats nicht zulässt, ist die TLS-Verbindung fehlgeschlagen.
- MRA-Clients erhalten Zertifikate für die Annahme von Popup-Fenstern, wenn sich das private Zertifikat nicht im OS Trust Store befindet.

Bedingung 4: Expressway Edge verfügt über öffentliche Zertifikate nur mit Server-EKU



In Bedingung 4 sind die Expressway-Core-Client- und -Serverzertifikate (CA1) von einer internen Zertifizierungsstelle signiert und verfügen über eine Client- und Server-EKU. Das Expressway E-Serverzertifikat ist eine öffentliche CA, die signiert ist, und hat nur eine Server-EKU. Das Serverzertifikat wird in den Clientzertifikatspeicher kopiert. Wählen Sie Serverzertifikatdatei als Clientzertifikat hochladen aus.

Wenn in Bedingung 4 eine TLS-Verbindung mit dem Gegenstück hergestellt wird und Expressway -E einen TLS-Client hello sendet, muss das Gegenstück die Client-EKU-Prüfung deaktivieren (da das Clientzertifikat keine Client-Authentifizierungs-EKU aufweist), andernfalls ist die TLS-Verbindung nicht erfolgreich.

Je nach Anwendungsfall und Bereitstellung durch die Benutzer kann es in der Praxis zu einer Vielzahl von Bedingungen oder Szenarien kommen, die aufgrund meines begrenzten Gedankenguts nicht abgedeckt werden können. Folgende Punkte sollten Sie sich jedoch merken:

- # WENN Expressway während des TLS-Handshakes zum Client wird, wird das Client-

Zertifikat den Peers präsentiert.

- #IF Expressway wird während des TLS-Handshakes zum Server. Das Serverzertifikat wird dem Peer angezeigt.

Diese Argumentation wurde bei diesen Testfällen erarbeitet.

Szenario 1

In diesem Szenario präsentiert Expressway das Client-Zertifikat während des MTL-Handshakes mit WebEx.

Videoanruf zu WebEx Meeting:

Beispiel für einen Anruffluss: Jabber -à CUCM -à Exp Core -à Exp Edge -à WebEx

10.106.80.31= Expressway-Edge

163.129.37.33 = WebEx

```
24.03.2026 11:54:26.106+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 verfügt über ein Client-Zertifikat mit dieser Seriennummer (2f0000004c869c77c8981becde0000000004c).

Expressway Edge sendet Client-Hello an "Webex" während der TLS-Aushandlung und sendet dann Client-Zertifikat.

Seriennummer 2f0000004c869c77c8981becde0000000004c:

1. Expressway Edge sendet Client Hello (pkt= 13699) während der mTLS-Aushandlung an "Webex".
2. WebEx sendet einen Server-Hello an Expressway Edge (pkt=13701).
3. Webex sendet sein Zertifikat an Expressway Edge (pkt=13711).

4. WebEx fordert Expressway-Edge-Zertifikat "CertificateRequest" an (pkt=13715).

5. Expressway Edge sendet sein Zertifikat an Webex (pkt=13718).

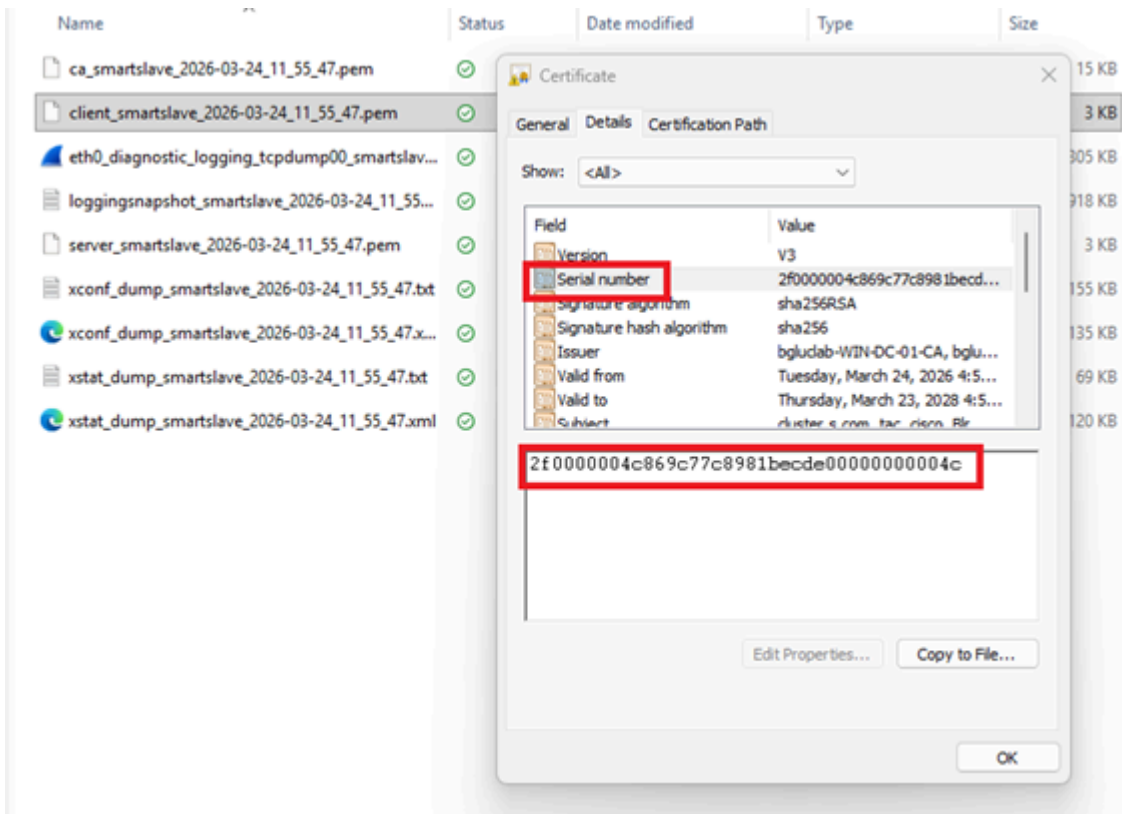
(Screenshot)

The screenshot shows a network traffic analysis tool interface. The top part displays a list of packets with columns for time, source IP, destination IP, protocol, length, and application. The bottom part shows a detailed view of a certificate, with the certificate structure and its fields highlighted by a red box.

```
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=3608271288
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 17:25:20.956092 163.129.37.32 10.106.80.31 TCP 66 25003 → 5061 [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 1308 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 1308 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 1308 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 1308 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 17:25:20.967607 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 17:25:20.967797 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: 2934
Certificate [..]: 308207ee3082066de00302010201237f0000004c869c77c8981becde0000000004c300006092a8648067000101000500304f31133011060a0992268993f22c6401191603636f6d3118301606
  signedCertificate
    version: v3 (2)
    serialNumber: 0x2f0000004c869c77c8981becde0000000004c
    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)
```

Client-Zertifikat von Expressway Edge:



Szenario 2

Expressway wird während des mTLS-Handshakes zur Server-Einheit und präsentiert sein Server-Zertifikat:

Wenn Expressway ein Serverzertifikat präsentiert, verfügt Expressway über eine sichere Nachbarzone über 5061 mit dem Verifizierungsnamen ON.

Sicherer Nachbarbereich zwischen Expressway-Knoten x15.5 und Expressway-Knoten 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)

732	2026-03-25 15:10:17.833251	10.106.80.16	10.106.80.15	TCP	74 5061 → 29457 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=4070042683 TSecr=2013756904 WS=512
733	2026-03-25 15:10:17.833259	10.106.80.15	10.106.80.16	TCP	66 29457 → 5061 [ACK] Seq=1 Ack=1 Min=29312 Len=0 TSval=2013756905 TSecr=4070042683
736	2026-03-25 15:10:17.870548	10.106.80.15	10.106.80.16	TLSv1.2	276 Client Hello
737	2026-03-25 15:10:17.871031	10.106.80.16	10.106.80.15	TCP	66 5061 → 29457 [ACK] Seq=1 Ack=211 Min=65024 Len=0 TSval=4070042721 TSecr=2013756942
738	2026-03-25 15:10:17.878936	10.106.80.16	10.106.80.15	TLSv1.2	1514 Server Hello
739	2026-03-25 15:10:17.878955	10.106.80.15	10.106.80.16	TCP	66 29457 → 5061 [ACK] Seq=211 Ack=1449 Min=32128 Len=0 TSval=2013756950 TSecr=4070042729
740	2026-03-25 15:10:17.878964	10.106.80.16	10.106.80.15	TCP	1514 5061 → 29457 [ACK] Seq=1449 Ack=211 Min=65024 Len=1448 TSval=4070042729 TSecr=2013756942 [TCP PDU reassembled in 742]
741	2026-03-25 15:10:17.878968	10.106.80.15	10.106.80.16	TCP	66 29457 → 5061 [ACK] Seq=211 Ack=2097 Min=35672 Len=0 TSval=2013756950 TSecr=4070042729
742	2026-03-25 15:10:17.878969	10.106.80.16	10.106.80.15	TLSv1.2	830 Certificate, Server Key Exchange, Certificate Request, Server Hello Done
743	2026-03-25 15:10:17.878972	10.106.80.15	10.106.80.16	TCP	66 29457 → 5061 [ACK] Seq=211 Ack=3601 Min=37888 Len=0 TSval=2013756950 TSecr=4070042729
744	2026-03-25 15:10:17.887137	10.106.80.16	10.106.80.15	TLSv1.2	3560 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
745	2026-03-25 15:10:17.887300	10.106.80.16	10.106.80.15	TCP	66 5061 → 29457 [ACK] Seq=3661 Ack=3705 Win=69632 Len=0 TSval=4070042737 TSecr=2013756958
746	2026-03-25 15:10:17.888041	10.106.80.16	10.106.80.15	TCP	1514 5061 → 29457 [ACK] Seq=3661 Ack=3705 Win=69632 Len=1448 TSval=4070042738 TSecr=2013756958 [TCP PDU reassembled in 747]
747	2026-03-25 15:10:17.888048	10.106.80.16	10.106.80.15	TLSv1.2	764 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
748	2026-03-25 15:10:17.888053	10.106.80.15	10.106.80.16	TCP	66 29457 → 5061 [ACK] Seq=3705 Ack=5807 Win=43776 Len=0 TSval=2013756959 TSecr=4070042738
749	2026-03-25 15:10:17.888437	10.106.80.15	10.106.80.16	TLSv1.2	498 Application Data


```

Length: 2923
  ▾ Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 2919
    Certificates Length: 2916
    ▾ Certificates (2916 bytes)
      Certificate Length: 2005
      ▾ Certificate [-]: 308207d1308206b9a00302010202046df76aa00000000029300006092a864886f7b0d01010c0500304931133011060a0992268993f22c64011916036f6d31183016060a0992268993f22c...
        ▾ signedCertificate
          version: v3 (2)
          serialNumber: 46df76aa000000000029
          ▾ signature (sha384withRSAEncryption)
            Algorithm Id: 1 3 840 113548 1 1 12 (sha384withRSAEncryption)
          ▾ issuer: rdnSequence (0)
            ▸ rdnSequence: 3 items (id-at-commonName=RICKY200-TMS-CA,dc=RICKY200,dc=com)
          ▸ validity
  
```

Dieser Screenshot zeigt das Serverzertifikat als Übereinstimmung mit der Seriennummer:

The screenshot shows a file explorer window with several files listed, including 'ca_vcs8c_2026-03-25_03_20_11.pem' and 'client_vcs8c_2026-03-25_03_20_11.pem'. A 'Certificate' dialog box is open, displaying the details of a certificate. The 'Serial number' field is highlighted with a red box, showing the value '46df76aa000000000029'. Below the dialog box, the same serial number is displayed in a separate box, also highlighted with a red box.

Testfall 3: Der MRA-Client wird für die Anmeldung bereitgestellt, und der Workflow umfasst die Überprüfung der Datenverkehrsserverzertifikate zwischen Expressway Core und CUCM.

10.106.80.16 = Expressway Core x15.5

10.106.80.38 = CUCM

- Exp. C 16 sendet einen Client-Hello auf 6972 TFTP.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.