

# Sunset dell'EKU di Navigate Client con Expressway x15.5

## Introduzione

Questo documento descrive come navigare nel tramonto dell'EKU del client con Cisco Expressway x15.5.

## Premesse

I certificati digitali sono credenziali elettroniche rilasciate da Autorità di certificazione (CA) attendibili che proteggono la comunicazione tra server e client garantendo l'autenticazione, l'integrità dei dati e la riservatezza. Questi certificati contengono campi di utilizzo chiavi esteso (EKU, Extended Key Usage) che ne definiscono lo scopo:

- Autenticazione server EKU (id-kp-serverAuth) viene utilizzato quando un server presenta il proprio certificato per provare l'identità.
- L'utilizzo chiavi avanzato di autenticazione client (id-kp-clientAuth) viene utilizzato nelle connessioni Mutual TLS (mTLS) in cui entrambe le parti si autenticano a vicenda.

In genere, un singolo certificato può contenere sia gli EKU di autenticazione server che quelli di autenticazione client, consentendone il doppio utilizzo. Ciò è particolarmente importante per prodotti come Cisco Expressway che agiscono sia come server che come client in diversi scenari di connessione.

## Descrizione del problema

### Modifica criteri programma radice riquadro

A partire da giugno 2026, i criteri del programma radice Chrome limitano i certificati CA (Certification Authority) radice inclusi nell'archivio radice Chrome, eliminando gradualmente le radici multiuso per allineare tutte le gerarchie di infrastrutture a chiave pubblica (PKI) per servire solo i casi di utilizzo dell'autenticazione del server TLS.

### Requisiti principali dei criteri

- Le CA radice pubbliche devono dichiarare l'utilizzo chiavi avanzato (EKU) SOLO per l'autenticazione del server (id-kp-serverAuth).
- Non è consentito includere l'utilizzo chiavi avanzato di autenticazione client nei certificati.
- Non sono più disponibili CA radice per utilizzo misto per i certificati TLS del server pubblico.
- Sequenza temporale applicazione: Giugno 2026

## Sequenza temporale risposta CA pubblica

- Ottobre 2025: Per impostazione predefinita, molte CA pubbliche (DigiCert, Sectigo, SSL) hanno iniziato a rilasciare certificati solo server.
- Maggio 2026: I server CA pubblici non rilasciano più certificazioni EKU di autenticazione client
- Giugno 2026: Chrome Root Program Policy diventa pienamente efficace



Nota: Questo criterio si applica solo ai certificati rilasciati da CA pubbliche. Questo criterio non influisce sulla PKI privata e sui certificati autofirmati.

---

Se si è interessati a conoscere l'impatto di sunsetting di EKU client su Expressways, fare riferimento a [Preparare Expressway for Client Auth EKU Sunset in Public CA Certificates.](#)

## Expressway release x15.5 con soluzione

### Expressway x15.5

Expressway x15.5 viene fornito con una correzione proposta per un problema che si verifica a causa del sunsetting dell'EKU client da parte di tutte le autorità di certificazione pubbliche. Si tratta di un problema globale che interessa tutti i fornitori/distribuzioni che scelgono di utilizzare certificati PKI pubblici.

x15.4, una versione precedente, disponeva di un commutatore di comando CLI che consentiva all'amministratore di caricare un certificato solo EKU server (nessun EKU client presente) su Expressway E.

CVS certificato XCP TLS xConfiguration EnableServerEkuUpload: On

---



Nota: Questo comando è obsoleto in x15.5.

---

## Aggiunta archivio certificati X15.5

x15.5 dispone di due archivi certificati:

1. Archivio certificati server
2. Archivio certificati client

Expressways (NIC singola o doppia): Entrambe le interfacce Expressway sono in grado di utilizzare 2 archivi di certificati in base alle esigenze.


Esempio:


- Quando expressway funge da client durante l'handshake TLS, viene presentato il certificato client.
- Quando expressway funge da server durante l'handshake TLS, viene presentato il certificato server.




Nota: Entrambi gli archivi certificati (client e server) utilizzano la stessa libreria CA attendibile. Verificare che la CA che ha firmato i certificati del server e del client sia caricata correttamente nell'archivio attendibile. I registri di diagnostica includono ora il certificato del server e il certificato del client in formato PEM.


---


 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

Aggiornamento da X15.4 o versione precedente a X15.5

Quando viene eseguito un aggiornamento, il certificato server da x15.4 o versione precedente, l'archivio certificati server Expressway viene copiato nell'archivio certificati client su x15.5. Gli archivi certificati client e server su x15.5 hanno lo stesso certificato.

Esempio con schermate

Expressway server su 15.4, certificato server corrente Numero di serie  
46:df:76:aa:00:00:00:00:29

Certificato:

Version: 3 (0x2)

Numero di serie:

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

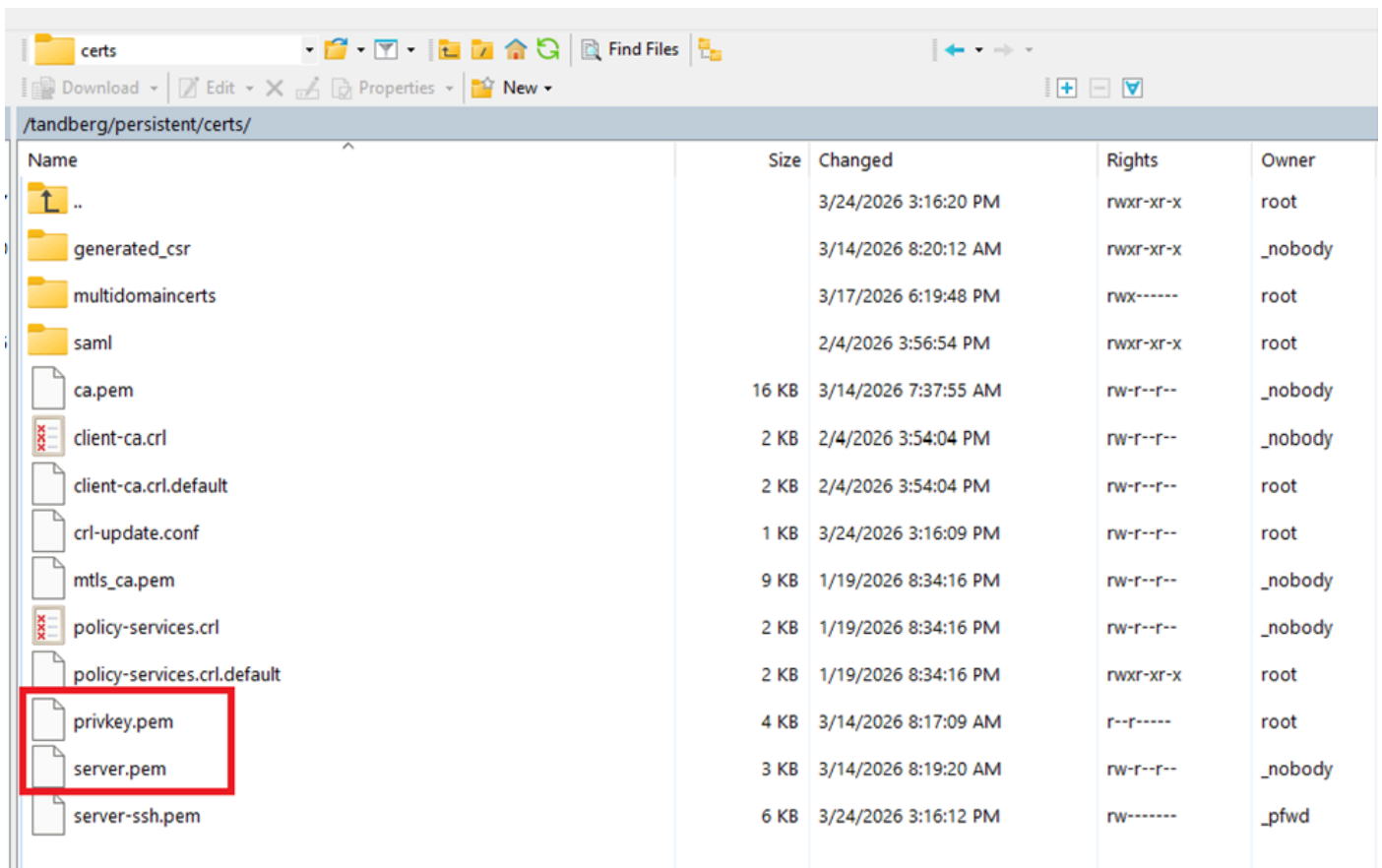
## Validità

Non prima del: 14 mar 02:37:40 2026 GMT

Non dopo : 14 mar 02:47:40 2028 GMT

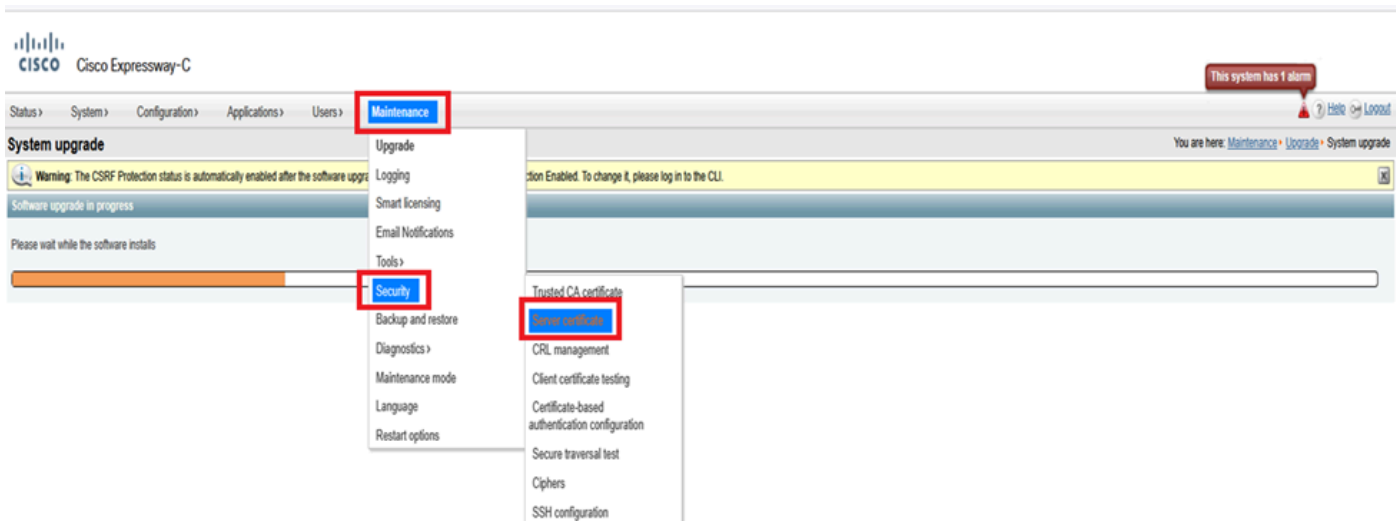
Oggetto: C = IN, ST = KA, L = KA, O = Cisco, OU = TAc, CN = cluster.s.com

Directory permanente/certificati del file system Expressway in x15.4:



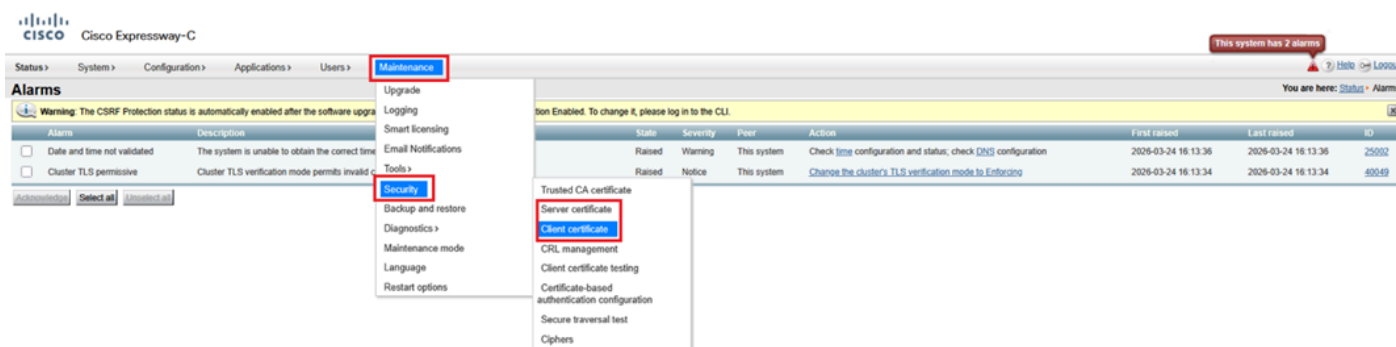
Name	Size	Changed	Rights	Owner
..		3/24/2026 3:16:20 PM	nwxr-xr-x	root
generated_csr		3/14/2026 8:20:12 AM	nwxr-xr-x	_nobody
multidomaincerts		3/17/2026 6:19:48 PM	nwx-----	root
saml		2/4/2026 3:56:54 PM	nwxr-xr-x	root
ca.pem	16 KB	3/14/2026 7:37:55 AM	nw-r--r--	_nobody
client-ca.crl	2 KB	2/4/2026 3:54:04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

Menu Expressway (Manutenzione > Sicurezza > Certificato server) su x15.4 (presente solo il campo del certificato server):



Dopo il corretto aggiornamento a x15.5

Qui è possibile vedere 2 opzioni di certificato in Manutenzione > Sicurezza > certificato client e certificati server. Dopo l'aggiornamento a x15.5, i portali dei certificati server e client sull'amministrazione Web mostrano lo stesso certificato perché il certificato server da x15.4 è stato copiato nell'archivio certificati client su x15.5.



Nell'archivio certificati client è stata copiata la chiave privata e il certificato esistente di post-aggiornamento a x15.5.

Directory permanente/certificati del file system Expressway in x15.5:

/tandberg/persistent/certs/		
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

## Controllo EKU X15.5 durante handshake TLS

In x15.5 è stato introdotto un nuovo comando CLI per controllare l'utilizzo esteso della chiave (EKU) durante l'handshake TLS. Il valore predefinito è "ON". Il set di comandi è valido su Expressway Core e Edge.

Il set di comandi attiva un controllo per tutte le connessioni TLS SIP IN ENTRATA in Expressway. (presentazioni di hellos client in ingresso/certificato). Quando è attivata, questa opzione verifica se il certificato presentato dall'iniziatore TLS contiene EKU client nel certificato. Se l'opzione è disattivata, il controllo viene ignorato; tuttavia, l'EKU del server viene verificato se è presente nel certificato.

Modalità di controllo Exconfiguration SIP TLS Certificate ExtendedKeyUsage: ACCESO/SPENTO:



Nota: Se si genera un certificato client, firmando un CSR che non contiene l'EKU client (un esempio di certificato firmato dalla CA pubblica), non sarà possibile caricare il certificato manualmente nell'archivio certificati client. Pertanto, è necessario assicurarsi che i certificati generati firmando un CSR contengano sempre l'EKU del client (è possibile utilizzare una CA privata per inserire l'EKU del client).



Suggerimento: Questo errore diventa evidente quando si tenta di caricare un certificato firmato da CSR, privo dell'EKU client, dall'archivio certificati client.

The screenshot shows the Cisco Expressway-E web interface. The breadcrumb navigation includes Status > System > Configuration > Applications > Users > Maintenance >. The page title is "Client certificate". A yellow warning banner at the top reads: "Invalid certificate: The file provided does not have a client usage attribute. Services requiring mutual TLS may not work." Below this, another warning banner states: "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." The "Client certificate data" section is currently empty.

Se tuttavia si sceglie di caricare un certificato con solo EKU server (senza EKU client) tramite l'archivio certificati server e si seleziona Carica file di certificato server come certificato client, il certificato viene copiato nell'archivio certificati client. Gli amministratori che non desiderano utilizzare un certificato firmato da una CA privata su Expressway-Edge possono scegliere di copiare l'EKU del server solo dall'archivio certificati del server all'archivio certificati del client.

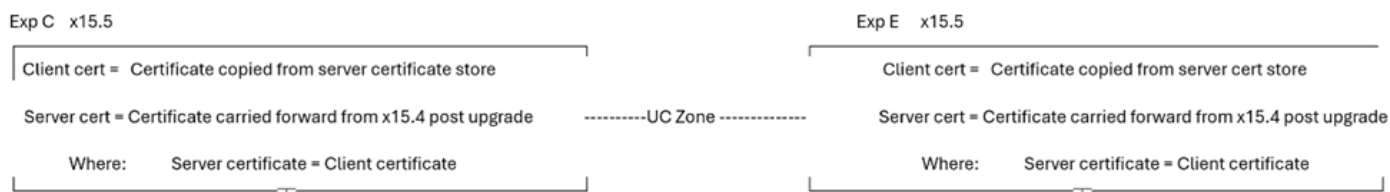
The screenshot shows the "Server certificate" section of the Cisco Expressway-E web interface. A yellow warning banner at the top reads: "Warning: The CSRF Protection status is automatically enabled after the software upgrade. We recommend keeping CSRF protection Enabled. To change it, please log in to the CLI." The "Server certificate data" section displays the following information: "Server certificate" with buttons for "Show (decoded)" and "Show (PEM file)"; "Currently loaded certificate expires on" set to "Dec 24 2027"; and "Certificate issuer" set to "RICKY200-TMS-CA". Below this is a "Reset to default server certificate" button. The "Certificate signing request (CSR)" section shows "Certificate request" with the message "There is no certificate signing request in progress". The "Generate CSR" section is partially visible. The "Upload new certificate" section includes fields for "Select the server private key file" and "Select the server certificate file", both with "Browse..." buttons and "No file selected." status. A checkbox labeled "Upload server certificate file as client certificate" is highlighted with a red box and is currently unchecked.

## Più archivi certificati, più scenari di distribuzione

Poiché ora esistono due archivi certificati in Expressway, esistono più scenari di archivi certificati.

### Condizione 1: Aggiornamento

Quando Expressway viene aggiornato da x15.4 o da una versione precedente a x15.5, questa condizione è vera. I certificati esistenti della versione x15.4 vengono copiati in due (2) archivi certificati. Sul client e sul server x15.5, i certificati sono gli stessi.

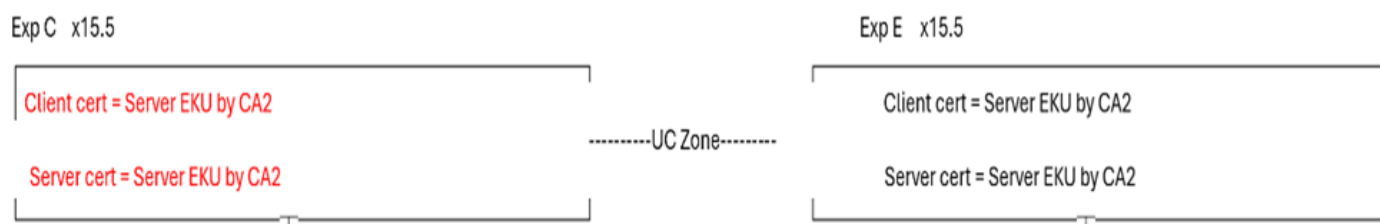


Condizione 2: Quando l'amministratore installa il nuovo certificato su x15.5 (certificati esistenti scaduti)

CA 1 = CA interna

CA 2 = CA pubblica

Nella Figura riportata di seguito, Expressway Core dispone di un certificato client con ECU server firmato solo da CA 2 (CA pubblica) e di un certificato server con ECU server firmato solo da CA 2 (CA pubblica). Analogamente, Expressway E ha un certificato client con l'ECU del server firmato da CA2 (CA pubblica) e un certificato del server con l'ECU del server firmato solo da CA 2 (CA pubblica).



Se il certificato del server principale Expressway non dispone di un ECU client, di una zona di attraversamento delle comunicazioni unificate o di un MRA, il proxy WebRTC non funzionerà. Verificare che il certificato del server Expressway Core disponga di un ECU client. Si tratta di un caso di utilizzo comune in cui gli utenti scelgono di firmare tutti i certificati da una CA pubblica. Poiché la CA pubblica non include l'utilizzo chiavi avanzato client nei certificati, la zona di attraversamento comunicazioni unificate diventa attiva.

Per rendere attiva la zona UC, è possibile disattivare rapidamente il controllo dell'utilizzo chiavi avanzato (EKU) in Expressway E. Questo richiama la zona UC. Tuttavia, i tunnel SSH rimangono inattivi. A partire da oggi, la comunicazione del tunnel SSH sullo switch 2222 richiede la convalida dell'EKU del client.

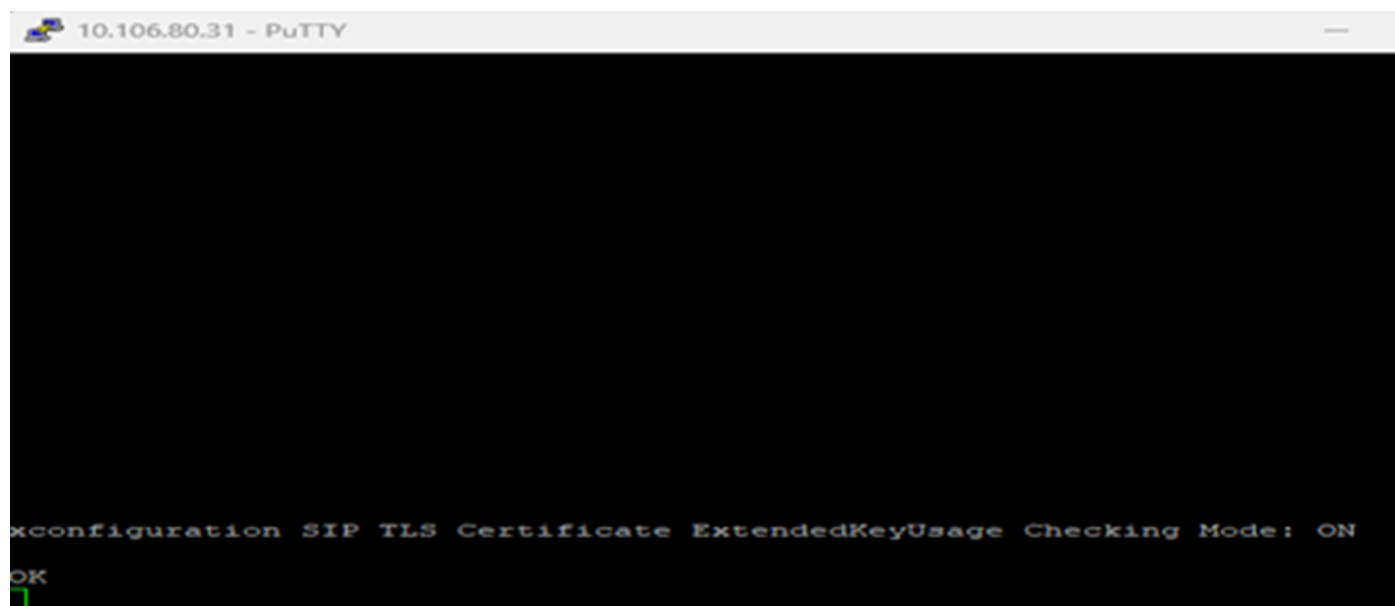
Le funzioni di accesso client MRA e proxy WebRTC non funzionano. Potrebbe essere necessario ricorrere a una CA privata.

#### Test case 1

- Quando il controllo dell'utilizzo chiavi avanzato è attivato su Expressway E
- Quando il certificato client e server nella memoria di base di Expressway include solo l'utilizzo chiavi avanzato del server
- Lo stato della zona UC è FAILED

Controllo On Expressway-Edge ExtendedKeyUsage attivato.

Modalità di controllo Exconfiguration SIP TLS Certificate ExtendedKeyUsage: On:

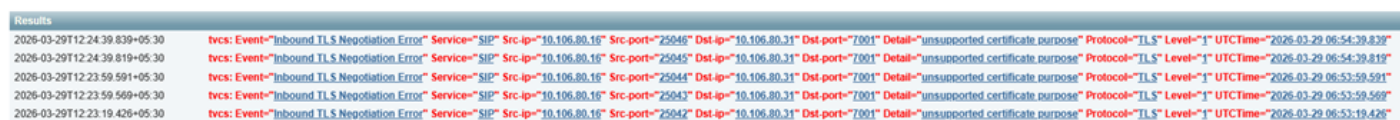


```
10.106.80.31 - PuTTY
xconfiguration SIP TLS Certificate ExtendedKeyUsage Checking Mode: ON
OK
```

Errore dell'area di comunicazione unificata:



I registri Expressway E mostrano dove 10.106.80.16 = Expressway Core, 10.106.80.31 = Expressway Edge:

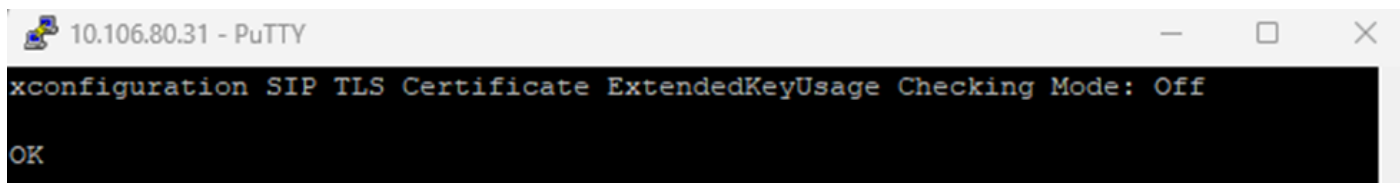


## Test case 2

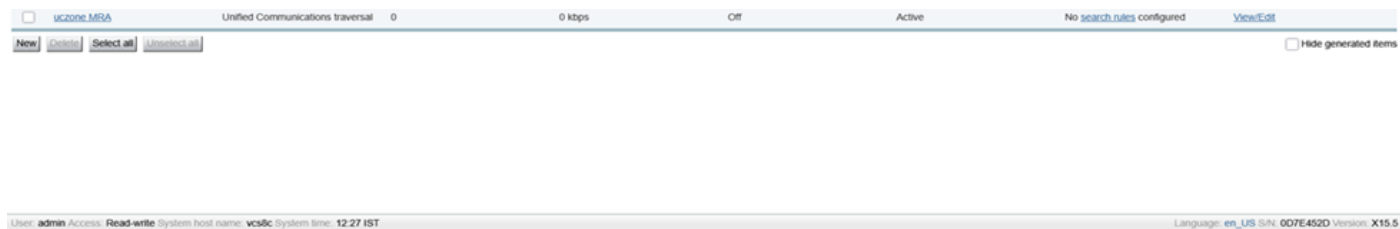
- Quando il controllo ECU è disattivato su Expressway E
- Quando il certificato client e server in Expressway Core dispone solo di ECU server
- Stato zona UC attivo

Disattiva controllo ECU su Expressway E.

Modalità di controllo Exconfiguration SIP TLS Certificate ExtendedKeyUsage: Spento



Zona di comunicazione unificata attiva:



Tuttavia, i tunnel ssh non sono riusciti:

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

Registri eventi Expressway:

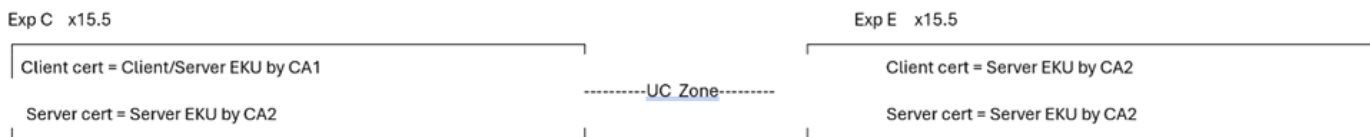
Results	
2026-03-29T12:33:12.384+05:30	ssh: Detail="ssh: connect to host smartslav:ports 2222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:31:56.811+05:30	ssh: Detail="ssh: connect to host smartslav:smartst 2222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:28:56.519+05:30	ssh: Detail="ssh: connect to host smartslav:smartst 2222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:28:24.476+05:30	ssh: Detail="ssh: connect to host smartslav:martst 2222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:27:52.445+05:30	ssh: Detail="ssh: connect to host smartslav:last smrt 2222:port 2222: Connection timed out" Level="ERROR"

Condizione 2.1: Caso di successo

CA 1 = CA interna

CA 2 = CA pubblica

- Dove il certificato client principale Expressway è firmato dalla CA 1 (CA interna) e include l'utilizzo chiavi avanzato client/server.
- Il certificato del server principale Expressway è firmato dalla CA pubblica CA 2 e include solo l'utilizzo chiavi avanzato del server.
- Il certificato di Expressway Edge Server è firmato dalla CA pubblica CA 2 e include solo l'utilizzo chiavi avanzato (EKU) del server.
- Il certificato client Expressway Edge è firmato dalla CA pubblica CA 2 e include solo l'utilizzo chiavi avanzato (EKU) del server.



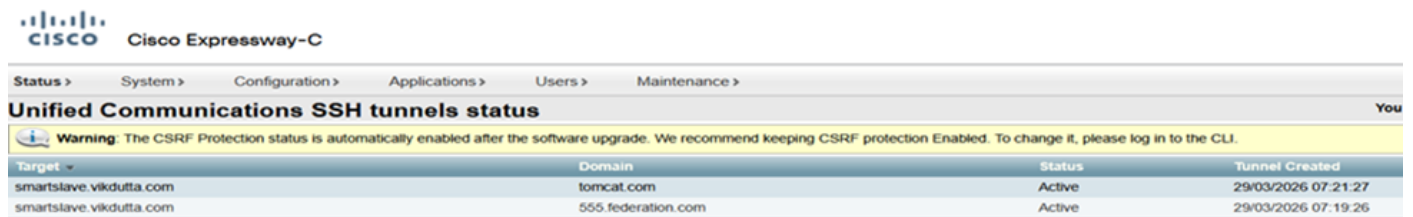
Questa condizione è un caso di successo. A prescindere dal fatto che la modalità di controllo ECU sia attiva/disattiva, la zona di comunicazione unificata e il tunnel SSH diventano entrambi attivi. I client MRA funzionano.

Non importa se il controllo EKU di Expressway Edge è disattivato o attivato. Il certificato client principale di Expressway contiene l'EKU del client:

```
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
```

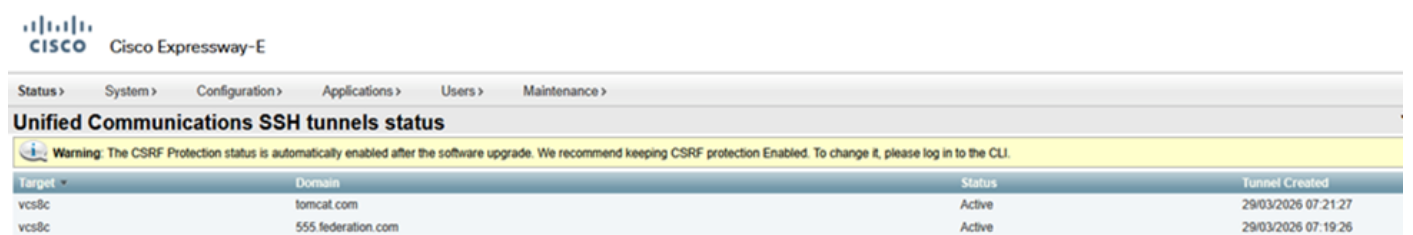
Tunnel SSH su Expressway core attivo:



The screenshot shows the Cisco Expressway-C web interface. The top navigation bar includes Status, System, Configuration, Applications, Users, and Maintenance. The main heading is "Unified Communications SSH tunnels status". A warning message states: "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." Below the warning is a table with the following data:

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

Tunnel SSH su Expressway Edge attivi:



The screenshot shows the Cisco Expressway-E web interface. The top navigation bar includes Status, System, Configuration, Applications, Users, and Maintenance. The main heading is "Unified Communications SSH tunnels status". A warning message states: "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." Below the warning is a table with the following data:

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

Stato zona Autorità registrazione integrità di Unified Communications attivo:

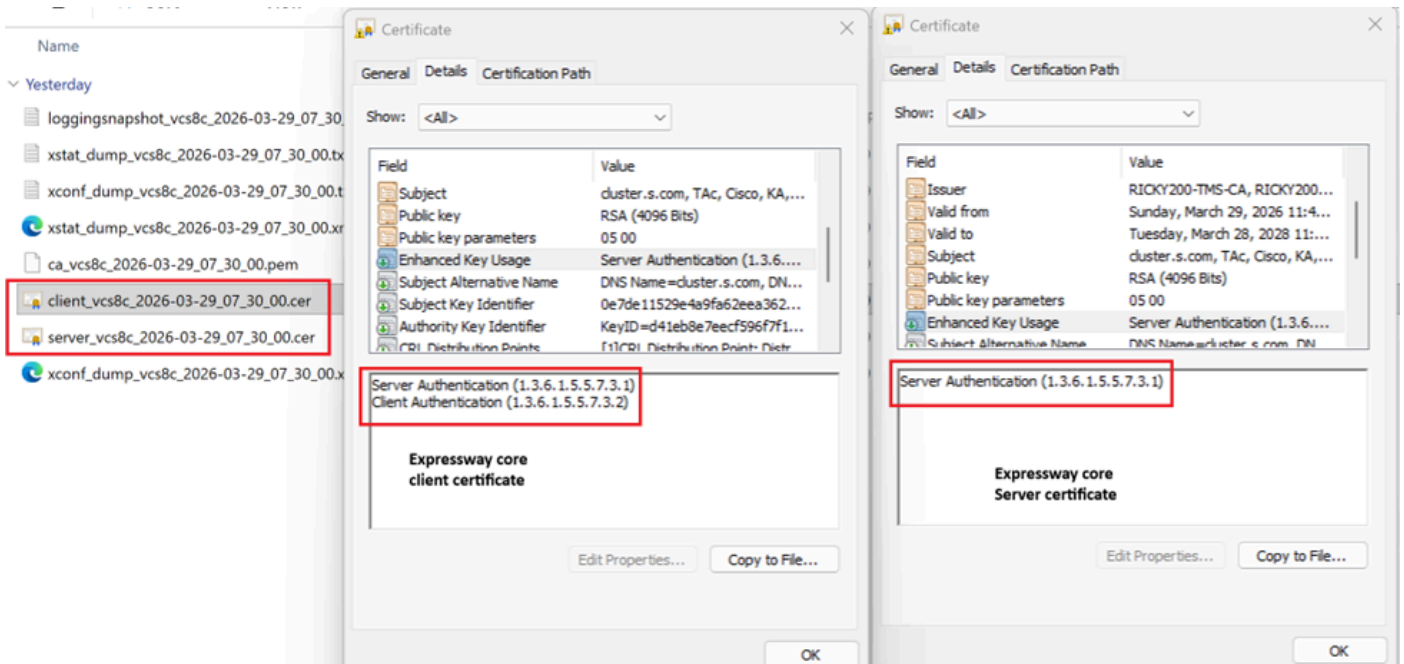


The screenshot shows the "uczone.MRA" configuration page for Unified Communications traversal. The status is "Active". The page includes a table with the following data:

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

At the bottom of the page, there is a footer with the following information: "User: admin Access: Read-write System host name: vcs8c System time: 12:58 IST Language: en\_US S/N: 007E452D Version: X15.5"

- Il certificato client Expressway-Core dispone di ECU server e ECU client.
- Il certificato del server principale Expressway include solo l'utilizzo chiavi avanzato del server.



Il client MRA effettua l'accesso e viene registrato:

The screenshot shows the Cisco Jabber interface with a 'Connection Status' window open. The window title is 'Cisco Jabber' and the version is 'Version 12.6.1 (284405)'. The status is as follows:

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

The IP address '10.106.79.162 (CCMCIP - Expressway) (IPv4)' and the device name 'CSFHanu' are highlighted with a red box in the original image.

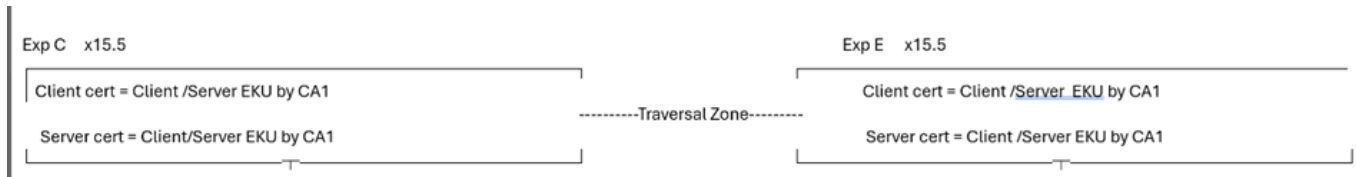


Nota: Confrontare e prendere nota degli ECU presenti nei certificati per il funzionamento dei proxy MRA e WebRTC. È un confronto tra l'installazione funzionante e quella non funzionante.

Condizione 3: Firma tutti i certificati con CA privata

CA 1 = CA interna

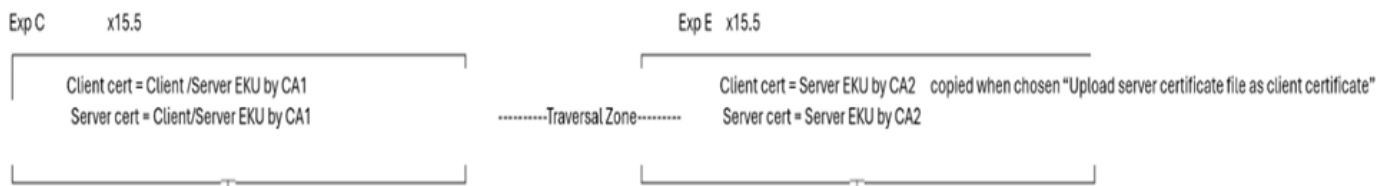
## CA 2 = CA pubblica



Nella condizione 3, tutti i certificati sono firmati dalla CA interna (CA1).

- Quando Expressway-E invia una connessione TLS, è necessario scambiare la radice/intermedia CA 1 con un'entità remota. Se l'estremità remota non dispone di funzionalità o non consente il caricamento di un certificato CA privato, la connessione TLS non riesce.
- I client di Autorità registrazione integrità ottengono i certificati per l'accettazione di popup se il certificato privato non si trova nell'archivio del trust del sistema operativo.

Condizione 4: Expressway Edge dispone solo di certificati pubblici con ECU server



Nella Condizione 4, i certificati client e server di base di Expressway sono firmati dalla CA interna (CA1) e contengono sia l'utilizzo chiavi avanzato client che server. Il certificato del server Expressway E è firmato dalla CA pubblica e dispone solo dell'ECU del server. Il certificato server viene copiato nell'archivio certificati client scegliendo Carica file di certificato server come certificato client.

Nella condizione 4, quando viene stabilita una connessione TLS a un'estremità remota, se Expressway -E invia un messaggio di saluto a un client TLS, l'estremità remota deve disabilitare il controllo ECU del client (poiché il certificato client non dispone dell'ECU di autenticazione client). In caso contrario, la connessione TLS non riesce.

Possono esistere molte più condizioni o scenari sul campo in base ai casi di utilizzo e di distribuzione degli utenti e non tutti possono essere coperti a causa del mio limitato flusso di pensiero. Tuttavia, i punti da ricordare sono:

- # SE Expressway diventa un client durante l'handshake TLS, il certificato client viene

presentato ai peer.

- #IF Expressway diventa Server durante l'handshake TLS; il certificato del server viene presentato al peer.

Questo ragionamento è stato stabilito con questi test case.

## Scenario 1

Per questo scenario, Expressway presenta il certificato client durante l'handshake MTLS con Webex.

Una videochiamata a Webex meeting:

Flusso di chiamata di esempio Jabber -à CUCM -à Exp Core —à Exp Edge —à Webex

10.106.80.31= Expressway Edge

163.129.37.33 = Webex

```
2026-03-24T11:54:26.106+00:00 smartslave tv: 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 dispone di un certificato client con questo numero di serie (2f0000004c869c77c8981becde0000000004c).

Expressway Edge invia il saluto del client a "Webex durante la negoziazione TLS", quindi invia il certificato del client.

Numero di serie 2f0000004c869c77c8981becde0000000004c:

1. Expressway Edge invia un messaggio di saluto (pkt= 13699) a "Webex durante la negoziazione mTLS".
2. Webex invia un messaggio di benvenuto al server a Expressway Edge (pkt=13701).
3. Webex invia il proprio certificato a Expressway Edge (pkt=13711).

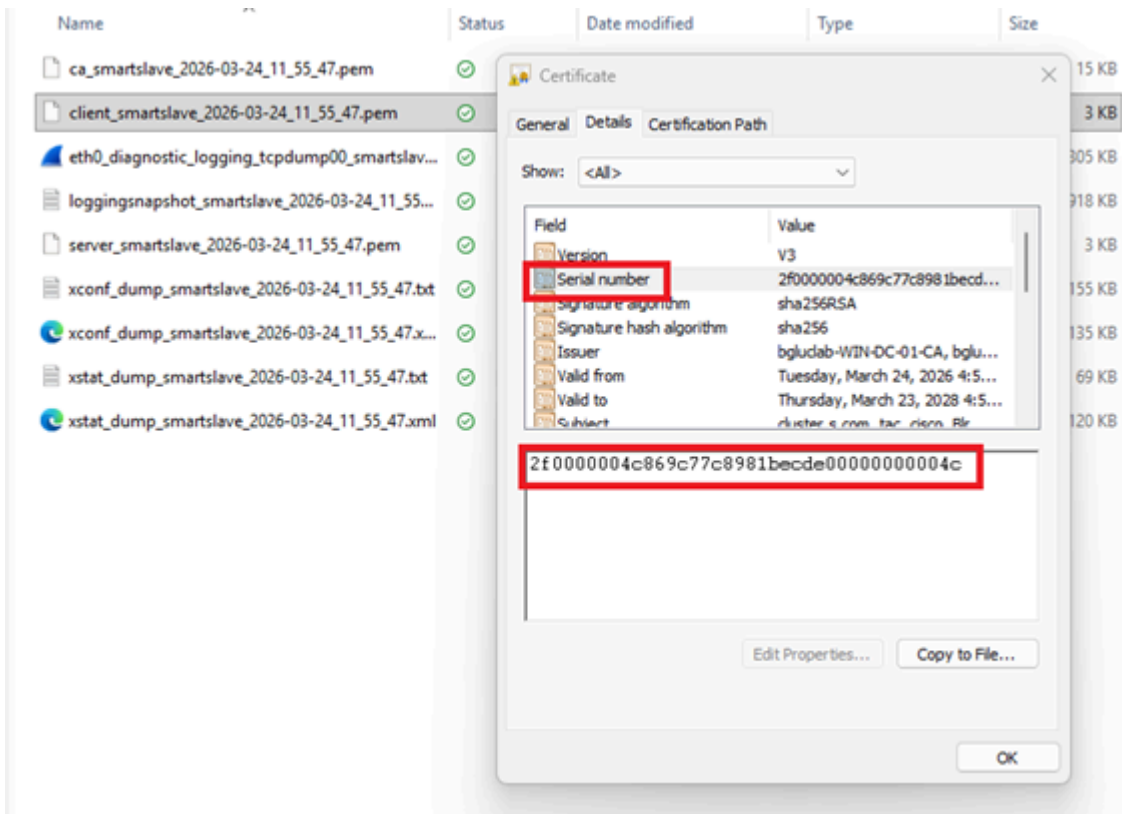
4. Webex richiede il certificato periferico Expressway "CertificateRequest" (pkt=13715).

5. Expressway Edge invia il proprio certificato a Webex (pkt=13718).

(screenshot)

```
Length: 2936
Certificates Length: 2933
Certificates (2933 bytes)
Certificate Length: 2934
Certificate [-]: 308207ee308206d6a0030201020132f0000004c869c77c8981becde0000000004c300006092a864806f7000101000500304f31133011060a0992268993f22c6401191603636f6d3118301606
  signedCertificate
    version: v3 (2)
    serialNumber: 0x2f0000004c869c77c8981becde0000000004c
    signature (sha256withRSAEncryption)
    issuer: rdnsSequence (0)
    rdnsSequence: 3 items (id-at-commonName=bgluclab-MIN-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-MIN-DC-01-CA)
    validity
      notBefore: utcTime (0)
      notAfter: utcTime (0)
    subject: rdnsSequence (0)
```

Certificato client da Expressway Edge:



## Scenario 2

Expressway diventa un'entità server durante l'handshake mTLS e presenta il relativo certificato server:

Dove Expressway presenta il certificato del server, Expressway dispone di una zona protetta Adiacente superiore a 5061 con il nome verificato ON.

Zona di sicurezza adiacente tra il nodo Expressway x15.5 e il nodo Expressway 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	88 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=32128 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	88 29457 → 5061 [ACK] Seq=211 Ack=3681 Min=37888 Len=0 TSval=2013756950 TSecr=4070042729
744	2026-03-25 15:10:17.887137	10.106.80.15	10.106.80.16	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 [-]: 308207d1308206b9a003020102020a46d76aa00000000029300006092a864886f78d01010c0500304931133011060a0992268993f22c64011916036f6d31183016060a0992268993f22c...
      signedCertificate
        version: v3 (2)
        serialNumber: 0x46df76aa000000000029
        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
  
```

In questa schermata viene mostrato il certificato del server come il numero di serie corrisponde:

The screenshot shows a file explorer window with a list of files including '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.txt', 'loggingnsnapshot\_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', and 'xstat\_dump\_vcs8c\_2026-03-25\_03\_20\_11.txt'. A 'Certificate' dialog box is open, showing the 'General' tab. The 'Serial number' field is highlighted in red and contains the value '46df76aa000000000029'. Other fields include 'Signature algorithm: sha384RSA', 'Signature hash algorithm: sha384', 'Issuer: RICKY200-TMS-CA, RICKY200...', 'Valid from: Saturday, March 14, 2026 8:0...', and 'Valid to: Tuesday, March 14, 2028 8:1...'. The 'Validity' section shows 'Cluster s.com TMS-CA, Cisco, CA'.

Test case 3: è stato eseguito il provisioning del client MRA per l'accesso e il flusso di lavoro include la verifica del certificato del server di traffico tra Expressway Core e CUCM.

10.106.80.16 = Expressway Core x15.5

10.106.80.38 = CUCM

- L'Exp C 16 invia un saluto al cliente sul 6972 TFTP.

- L'Exp C 16 invia un certificato client durante l'handshake TLS.

The image shows a Wireshark capture of a TLS handshake. The main pane displays a list of packets, with packet 542 (Certificate) highlighted. The 'Certificate' field in the 'Handshake Protocol' pane is expanded, showing the following details:

- Content Type: Handshake (22)
- Version: TLS 1.3 (0x0303)
- Length: 2923
- Handshake Protocol: Certificate
- Handshake Type: Certificate (11)
- Length: 2918
- Certificates length: 2916
- Certificates (2916 bytes)
- Certificate (length: 2885)
  - version: v3 (3)
  - serialNumber: 46d176aa0000000029
  - signature (sha384withRSAEncryption)
  - Issuer: rdSequence (0)
    - rdSequence: 3 items (id-at-commonName-R3COY206-TMS-CA, dc-R3COY206, dc-com)
      - rdSequence Item: 1 item (dc-com)
      - rdSequence Item: 1 item (dc-R3COY206)
      - rdSequence Item: 1 item (id-at-commonName-R3COY206-TMS-CA)
  - Validity
    - notBefore: utcTime (0)
    - notAfter: utcTime (0)

Certificato client di base Expressway:

The image shows a certificate viewer window with the following details:

- Field: Serial number
- Value: 46d176aa0000000029
- Signature algorithm: sha384RSA
- Signature hash algorithm: sha384
- Issuer: R3COY206-TMS-CA, R3COY206...
- valid from: Saturday, March 14, 2026 8:00:00
- valid to: Tuesday, March 14, 2028 8:00:00
- Subject: client.x.com, T&C, Client\_KA

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).