

# Navegar por el cliente ECU Sunset con Expressway x15.5

## Introducción

Este documento describe cómo navegar por la puesta de sol de ECU del cliente con Cisco Expressway x15.5.

## Antecedentes

Los certificados digitales son credenciales electrónicas emitidas por entidades emisoras de certificados (CA) de confianza que protegen la comunicación entre servidores y clientes garantizando la autenticación, la integridad de los datos y la confidencialidad. Estos certificados contienen campos de uso extendido de claves (ECU) que definen su propósito:

- La autenticación de servidor ECU (id-kp-serverAuth) se utiliza cuando un servidor presenta su certificado para probar la identidad.
- La autenticación de cliente ECU (id-kp-clientAuth) se utiliza en conexiones de TLS mutuo (mTLS) donde ambas partes se autentican mutuamente.

Tradicionalmente, un único certificado podía contener tanto ECU de autenticación de cliente como de servidor, lo que le permitía cumplir dos propósitos. Esto es especialmente importante para productos como Cisco Expressway que actúan como servidor y cliente en diferentes escenarios de conexión.

## Definición del problema

### Cambio de la política del programa raíz de Chrome

A partir de junio de 2026, la política del programa raíz de Chrome restringe los certificados de la autoridad certificadora (CA) raíz incluidos en el almacén raíz de Chrome, eliminando gradualmente las raíces multifunción para alinear todas las jerarquías de la infraestructura de clave pública (PKI) para servir solo casos de uso de autenticación de servidor TLS.

### Requisitos de política clave

- Las CA raíz públicas deben afirmar el uso de clave ampliada (EKU) SOLO para la autenticación de servidor (id-kp-serverAuth).
- La inclusión de la autenticación de cliente ECU en estos certificados está prohibida.
- No más CA raíz de uso mixto para certificados TLS de servidor público.
- Plazos de aplicación: Junio de 2026

## Plazos de respuesta de CA pública

- Octubre de 2025: Muchas CA públicas (DigiCert, Sectigo, SSL) comenzaron a emitir certificados solo de servidor de forma predeterminada.
- Mayo de 2026: Los servidores de CA pública dejan de emitir certificaciones ECU de autenticación de cliente
- Junio de 2026: La política del programa de raíz de Chrome se vuelve totalmente efectiva



Nota: Esta directiva sólo se aplica a los certificados emitidos por CA públicas. Esta directiva no afecta a la PKI privada ni a los certificados autofirmados.

---

Si está interesado en leer sobre el impacto de la extinción de la ECU del cliente en Expressway, consulte [Preparación de Expressway para la extinción de la ECU de autenticación del cliente en certificados de CA pública.](#)

## Expressway versión x15.5 con solución

### Expressway x15.5

Expressway x15.5 viene con una solución propuesta para un problema que surge debido a la eliminación de ECU del cliente por todas las autoridades de certificados públicos. Se trata de un problema global que afecta a todos los proveedores e implementaciones que deciden utilizar certificados PKI públicos.

x15.4, una versión anterior, tenía un switch de comando CLI que permitía al administrador cargar el certificado Server ECU only (no hay ECU de cliente presente) en Expressway E.

Certificado XCP TLS de xConfiguration CVS EnableServerEkuUpload: Encendido

---



Nota: Este comando está obsoleto en x15.5.

---

## Adición de almacén de certificados X15.5

x15.5 tiene dos almacenes de certificados:

1. Almacén de certificados de servidor
2. Almacén de certificados de cliente

Expressway (NIC única o NIC doble): Ambas interfaces de Expressway pueden utilizar 2 almacenes de certificados según sea necesario.


Ejemplo:


- Cuando Expressway actúa como cliente durante el intercambio de señales TLS, se presenta el certificado de cliente.
- Cuando Expressway actúa como servidor durante el intercambio de señales TLS, se presenta el certificado del servidor.





Nota: Ambos almacenes de certificados (Cliente y Servidor) utilizan la misma biblioteca de CA de confianza. Asegúrese de que la entidad emisora de certificados que firmó los certificados de servidor y de cliente se carga correctamente en el almacén de confianza. Los registros de diagnóstico ahora incluyen el certificado de servidor y el certificado de cliente en formato de archivo 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

## Actualización de X15.4 o versión anterior a X15.5

Cuando se realiza una actualización, el certificado de servidor de x15.4 o una versión anterior, el almacén de certificados de servidor de Expressway se copia en el almacén de certificados de cliente de x15.5. Los almacenes de certificados de cliente y de servidor de x15.5 tienen el mismo certificado.

### Ejemplo con capturas de pantalla

servidor de Expressway en 15.4, certificado de servidor actual Número de serie  
46:df:76:aa:00:00:00:00:29

Certificado:

Versión: 3 (0x2)

Serial Number:

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

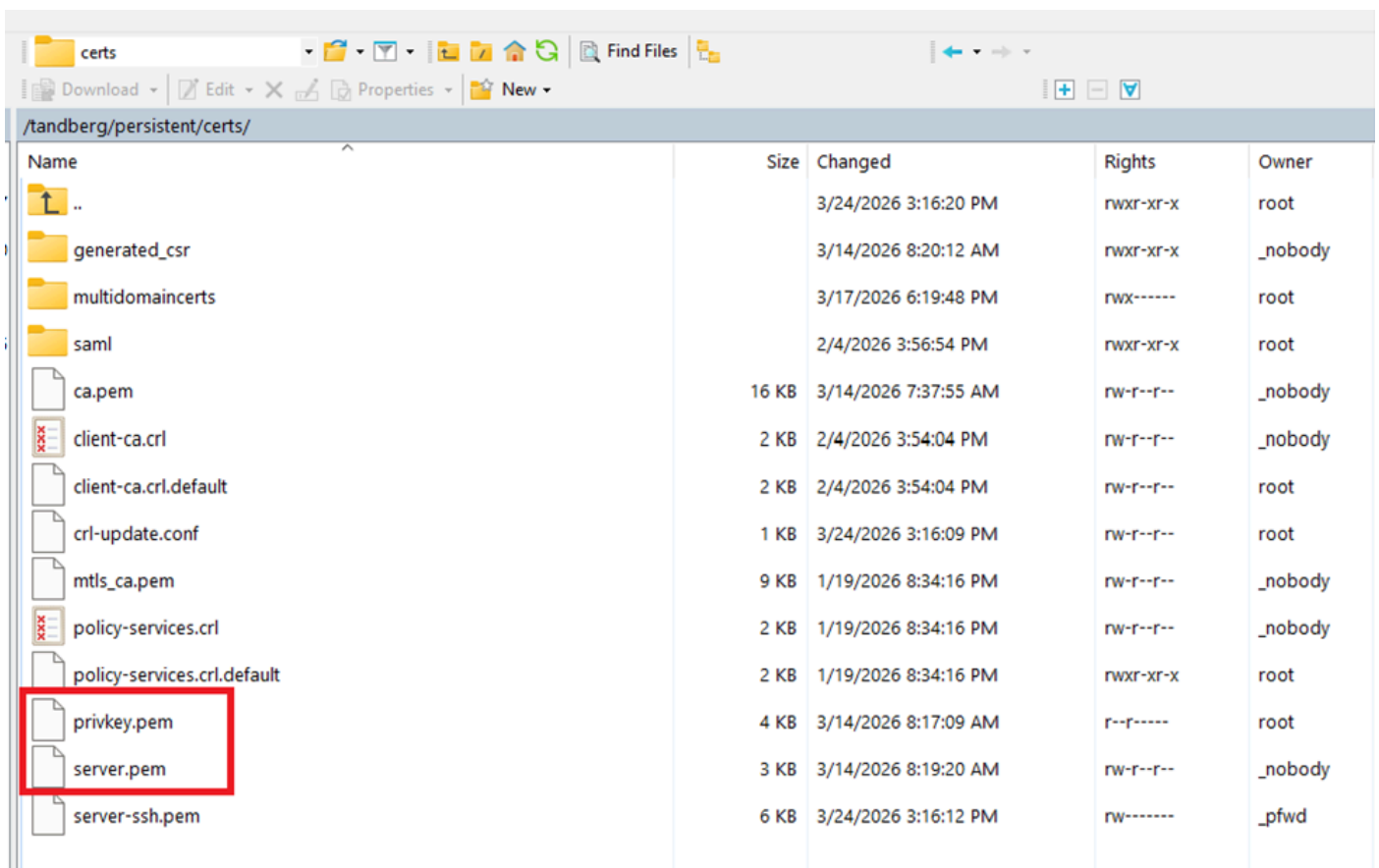
Validez

No antes: 14 de marzo 02:37:40 2026 GMT

No después de: 14 de marzo 02:47:40 2028 GMT

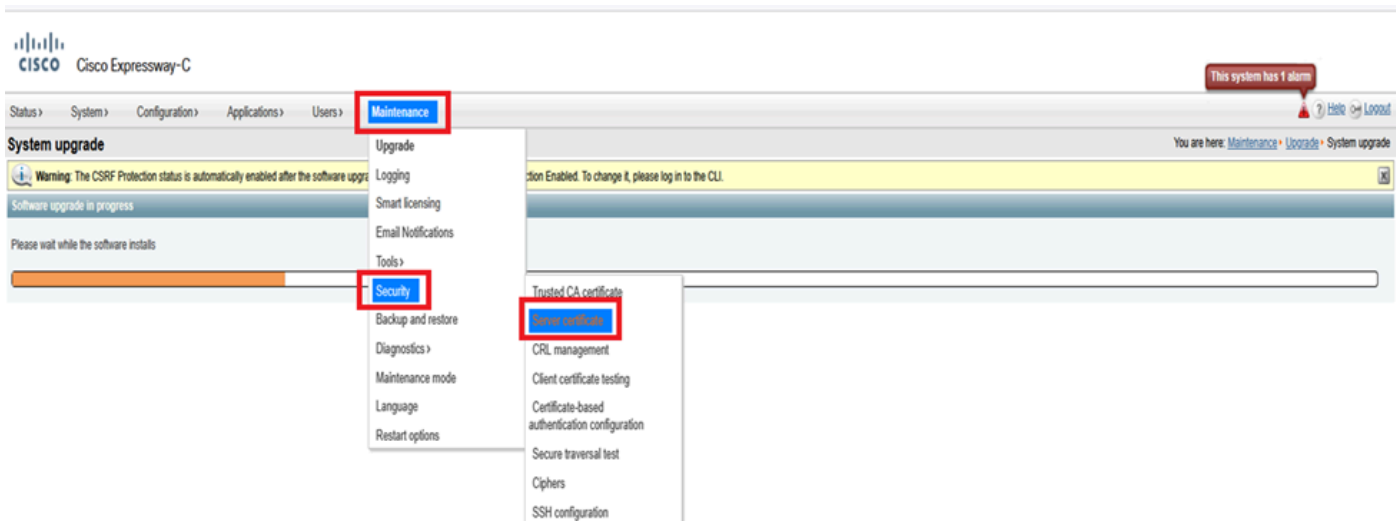
Asunto: C = IN, ST = KA, L = KA, O = Cisco, OU = TAc, CN = cluster.s.com

Directorio persistent/cert del sistema de archivos de Expressway en x15.4:



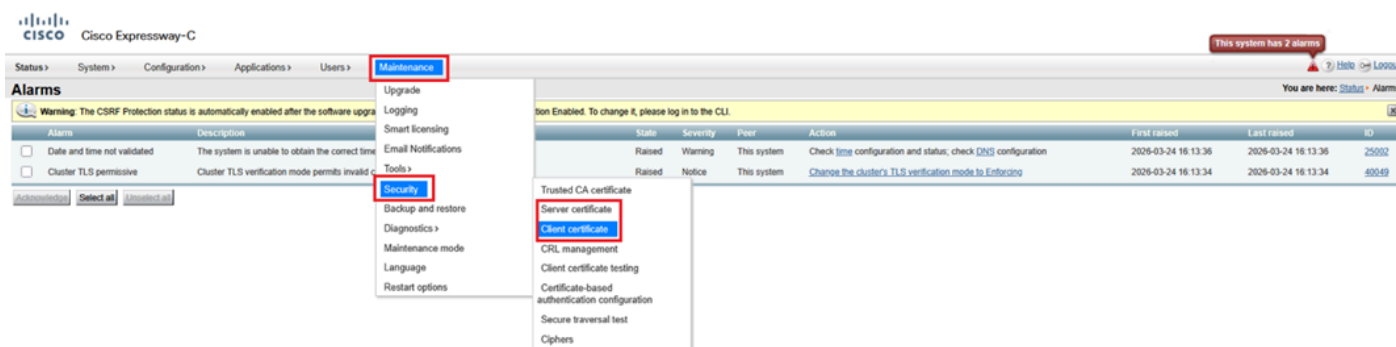
Name	Size	Changed	Rights	Owner
..		3/24/2026 3:16:20 PM	nwxr-xr-x	root
generated_csr		3/14/2026 8:20:12 AM	nwxr-xr-x	_nobody
multidomaincerts		3/17/2026 6:19:48 PM	nwx-----	root
saml		2/4/2026 3:56:54 PM	nwxr-xr-x	root
ca.pem	16 KB	3/14/2026 7:37:55 AM	nw-r--r--	_nobody
client-ca.crl	2 KB	2/4/2026 3:54:04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

Menú de Expressway (Mantenimiento > Seguridad > Certificado de servidor) en x15.4 (solo el campo de certificado de servidor está presente):



Después de actualizar correctamente a x15.5

Aquí, verá 2 opciones de certificado bajo Mantenimiento > Seguridad > certificado de cliente y certificados de servidor. Después de actualizar a x15.5, los portales de certificado de servidor y de cliente en la administración web muestran el mismo certificado porque el certificado de servidor de x15.4 se copió en el almacén de certificados de cliente en x15.5.



La actualización posterior al certificado y la clave privada x15.5 existentes se ha copiado en el almacén de certificados del cliente.

Directorio persistent/cert del sistema de archivos de Expressway en 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

## Comprobación de EKU X15.5 durante intercambio de señales TLS

En x15.5, se ha introducido un nuevo comando CLI para verificar el uso extendido de claves (EKU) durante el intercambio de señales TLS. El valor predeterminado es "ON". El conjunto de comandos es válido en Expressway Core y Edge.

El conjunto de comandos activa una comprobación para todas las conexiones SIP TLS ENTRANTES en Expressway. (saludos de cliente entrante/certificado presentado). Cuando está activada, esta opción comprueba si el certificado presentado por el iniciador de TLS contiene EKU del cliente en el certificado. Si se desconecta, se omite la comprobación; sin embargo, la EKU del servidor se verifica si está presente en el certificado.

xconfiguration SIP TLS Certificate Extended KeyModo de Verificación de Uso: ON/OFF:



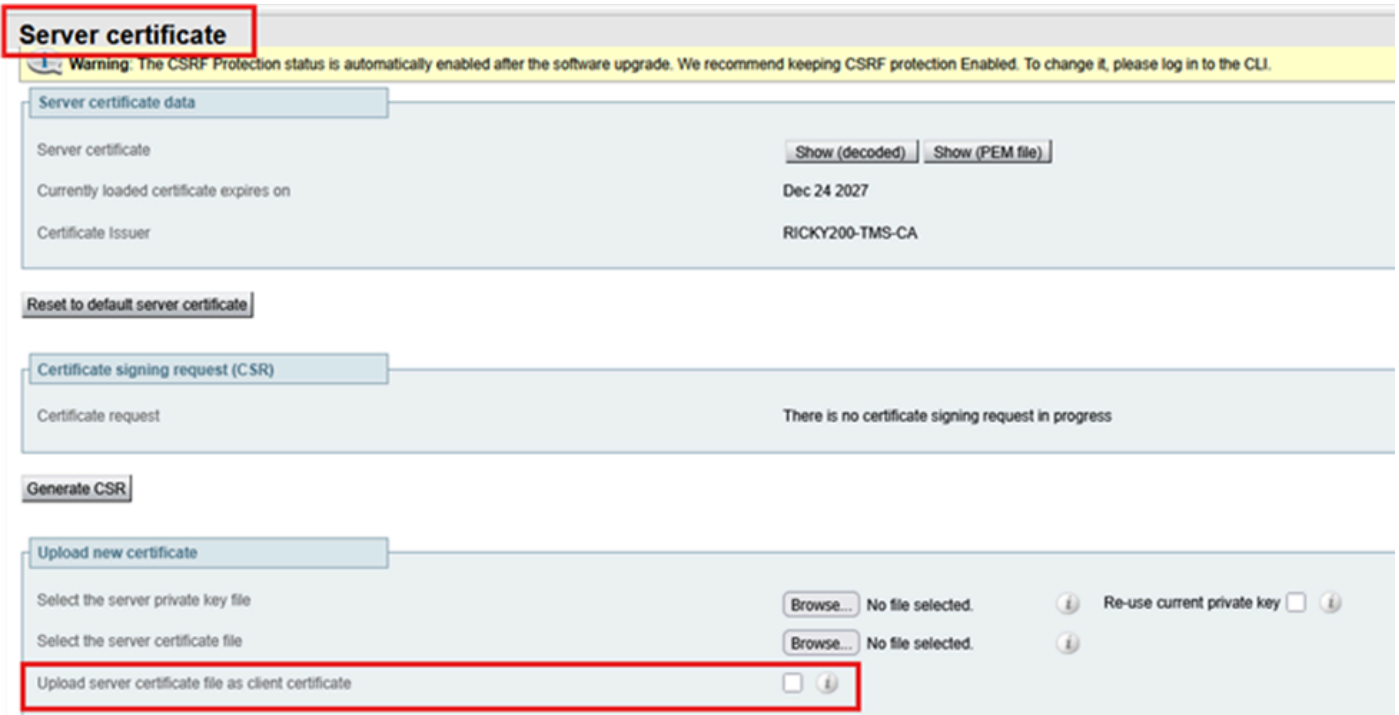
Nota: Si genera un certificado de cliente, firmando un CSR que no contiene ECU de cliente (un ejemplo de certificado firmado por CA pública), no podrá cargar este certificado manualmente en el almacén de certificados de cliente. Por lo tanto, debe asegurarse de que los certificados generados mediante la firma de una CSR siempre contengan la ECU del cliente (se puede utilizar una CA privada para insertar la ECU del cliente).



Consejo: Este error se hace evidente cuando intenta cargar un certificado firmado CSR, que falta en la ECU del cliente, desde el almacén de certificados del cliente.

The screenshot shows the Cisco Expressway-E web interface. The top navigation bar includes links for Status, System, Configuration, Applications, Users, and Maintenance. The main heading is "Client certificate". Below this, a red-bordered 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 the error message, a yellow box contains a warning: "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 titled "Client certificate data" with a search bar.

Sin embargo, si elige cargar un certificado que sólo tiene una ECU de servidor (sin ECU de cliente) a través del almacén de certificados de servidor y selecciona Cargar archivo de certificado de servidor como certificado de cliente, el certificado se copia en el almacén de certificados de cliente. Los administradores que no deseen utilizar un certificado firmado de CA privada en Expressway-Edge pueden elegir copiar el ECU del servidor solo desde el almacén de certificados del servidor al almacén de certificados del cliente.

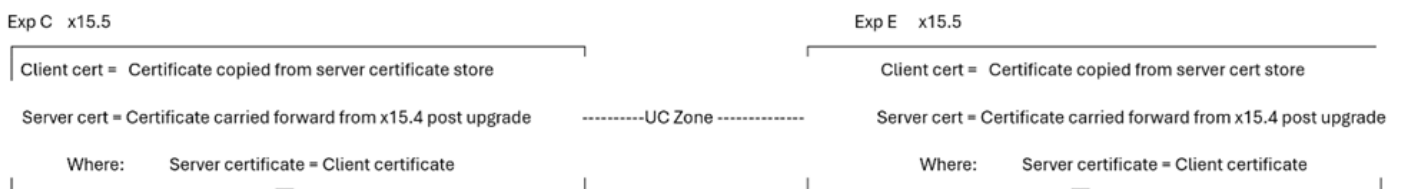


## Varios almacenes de certificados, varios escenarios de implementación

Dado que ahora hay dos almacenes de certificados en Expressway, hay varios escenarios de almacenes de certificados.

### Condición 1: Actualizar

Cuando Expressway se actualiza desde x15.4 o anterior a x15.5, esta condición es verdadera. Los certificados existentes de la versión x15.4 se copian en dos (2) almacenes de certificados. En el cliente y el servidor x15.5, los certificados son los mismos.

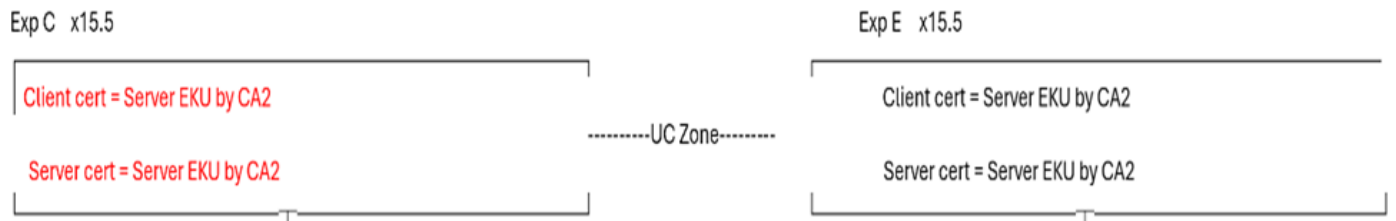


Condición 2: Cuando el administrador instala un nuevo certificado en x15.5 (certificados existentes caducados)

CA 1 = CA interna

CA 2 = CA pública

En la figura siguiente, Expressway Core tiene un certificado de cliente con ECU de servidor solo firmado por CA 2 (CA pública) y un certificado de servidor con ECU de servidor solo firmado por CA 2 (CA pública). Del mismo modo, Expressway E tiene un certificado de cliente con el servidor ECU firmado por CA2 (CA pública) y un certificado de servidor con el servidor ECU firmado solamente por CA 2 (CA pública).



Si el certificado de servidor de núcleo de Expressway no tiene una ECU de cliente, zona transversal de Unified Communications, MRA, el proxy de WebRTC no funciona. Asegúrese de que el certificado de servidor de Expressway Core tenga una ECU de cliente. Este es un caso práctico común en el que los usuarios eligen firmar todos los certificados de CA pública. Dado que la CA pública no incluye la ECU del cliente en los certificados, la zona transversal de Unified Communications se activa.

Para activar la zona de UC, una solución rápida es desactivar la comprobación ECU en Expressway E. Esto nos lleva a la zona de UC. Sin embargo, los túneles SSH permanecen inactivos. A partir de hoy, la comunicación del túnel SSH en 2222 requiere la validación de la ECU del cliente.

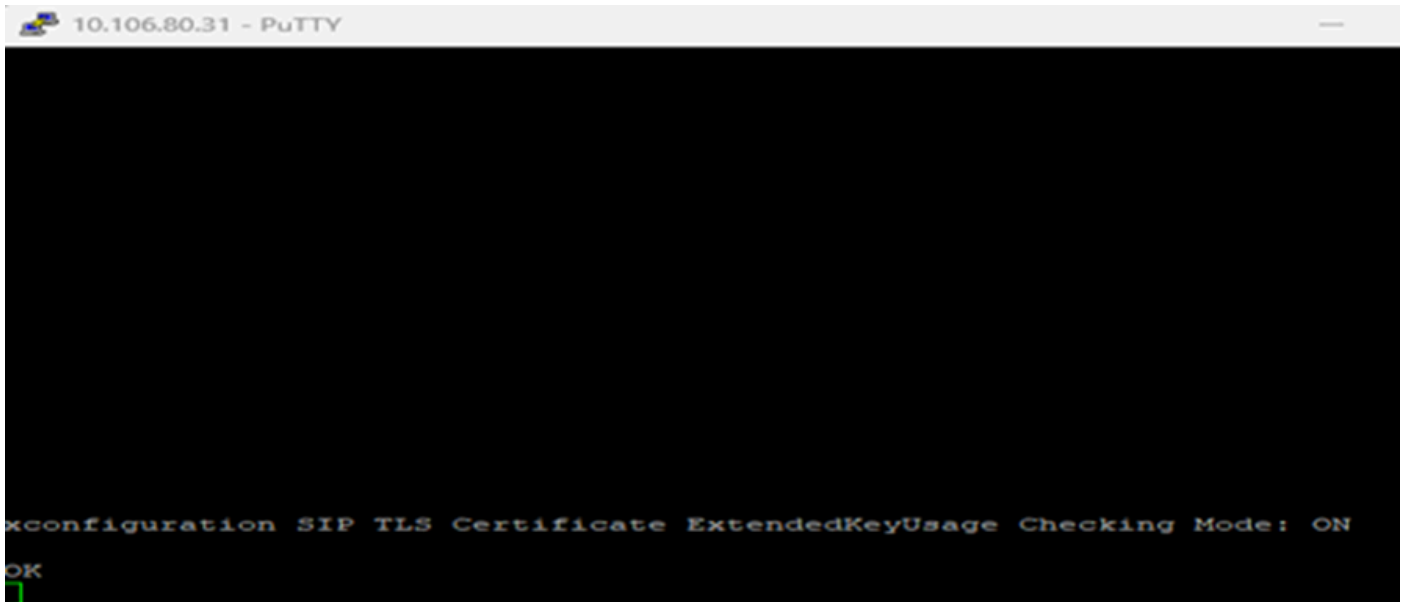
Las funciones de inicio de sesión del cliente MRA y proxy WebRTC no funcionan. Podría tener que recurrir a una CA privada.

#### Caso de prueba 1

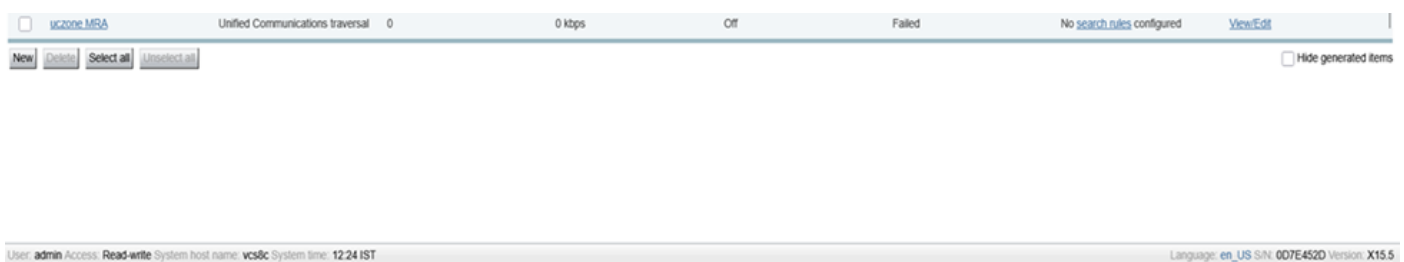
- Cuando la verificación ECU está "ON" en Expressway E
- Cuando el certificado de cliente y servidor en el núcleo de Expressway tiene solamente ECU de servidor
- El estado de la zona UC es FALLIDO

En Expressway-Edge ExtendedKeyUsage Active.

xconfiguration SIP TLS Certificate Extended Key Modo de Verificación de Uso: Encendido



Falla de zona de comunicaciones unificadas:



Los registros de Expressway E muestran dónde 10.106.80.16 = núcleo de Expressway, 10.106.80.31 = extremo de Expressway:



## Caso de prueba 2

- Cuando la comprobación ECU está desactivada en Expressway E
- Cuando el certificado de cliente y servidor en Expressway Core tiene solo ECU de servidor
- El estado de la zona de UC es ACTIVO

Desactive la comprobación ECU en Expressway E.

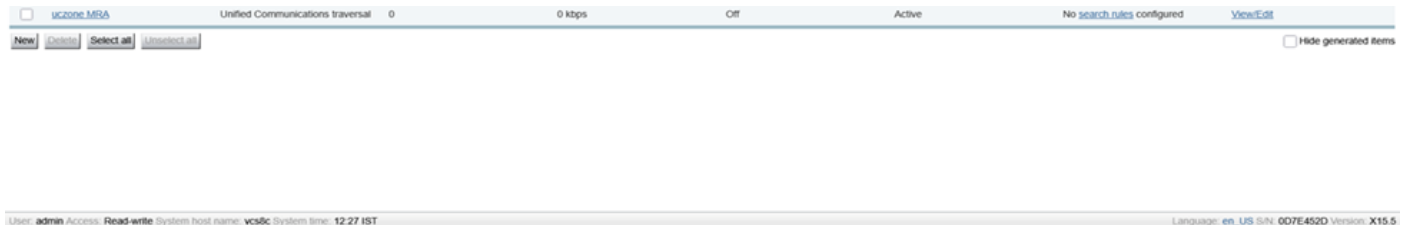
xconfiguration SIP TLS Certificate Extended KeyModo de Verificación de Uso: Desactivado

```

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

```

Zona de comunicación unificada activa:



Sin embargo, los túneles ssh aún fallaron:

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

Registros de eventos de Expressway:

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"

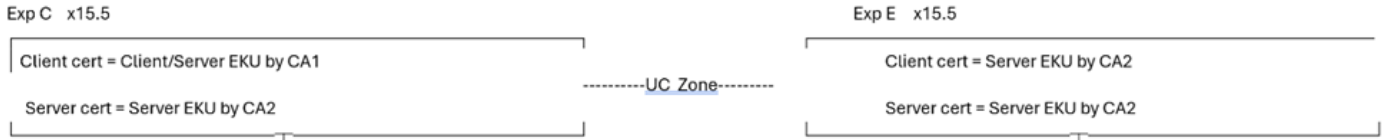
Condición 2.1: Caso de éxito

CA 1 = CA interna

CA 2 = CA pública

- Donde el certificado de cliente de núcleo de Expressway está firmado por CA 1 (CA interna) e incluye EKU cliente/servidor.
- El certificado de servidor de núcleo de Expressway está firmado por CA 2 pública e incluye solo EKU de servidor.

- El certificado de servidor perimetral de Expressway está firmado por CA 2 pública e incluye solo EKU de servidor.
- El certificado de cliente de Expressway Edge está firmado por una CA 2 pública e incluye solo EKU de servidor.



Esta condición es un caso de éxito. Independientemente de si el modo de verificación EKU está activado/desactivado, la zona de Unified Communication y el túnel SSH se activan. Los clientes de MRA trabajan.

No importa si la verificación EKU de Expressway Edge está en OFF o en ON. El certificado de cliente de núcleo de Expressway contiene EKU de cliente:

```
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
```

Túneles SSH en núcleo de Expressway activo:

The screenshot shows the Cisco Expressway-C web interface. The page title 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 of active tunnels.

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

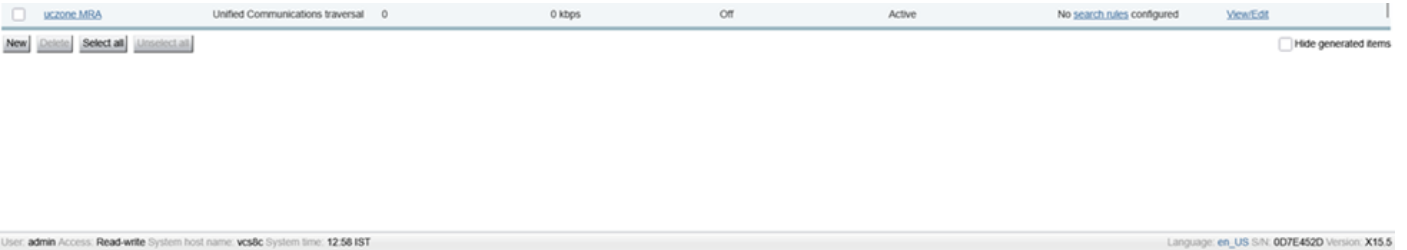
Túneles SSH en Expressway Edge Active:

### Unified Communications SSH tunnels status

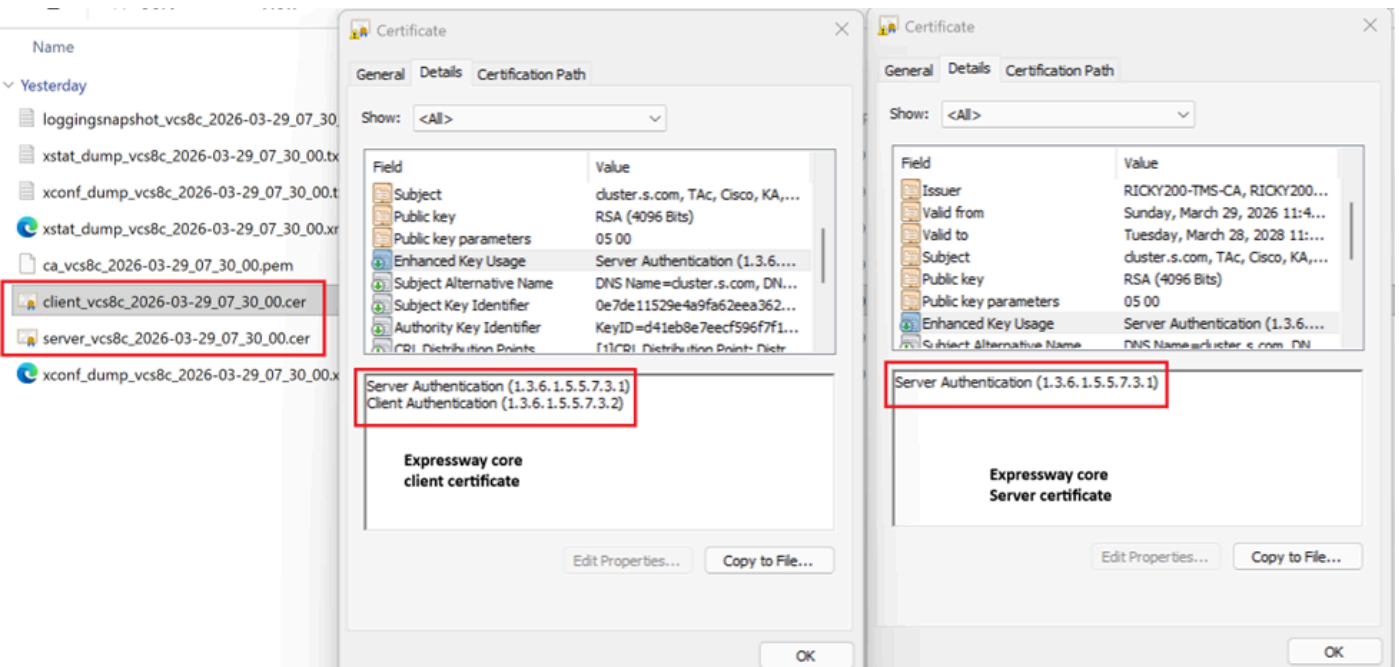
**Warning:** The CSRF Protection status is automatically enabled after the software upgrade. We recommend keeping CSRF protection Enabled. To change it, please log in to the CLI.

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

Estado de la zona MRA de Unified Communication Activo:



- El certificado de cliente de Expressway-Core tiene EKU de servidor y EKU de cliente.
- El certificado de servidor principal de Expressway solo tiene EKU de servidor.



El cliente MRA inicia sesión y se registra:

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 for "hanu@" and a search bar labeled "Search or call". A sidebar on the left contains icons for a phone, a calendar showing "29", and a dropdown menu labeled "All". The main content area is titled "Connection Status" and 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.

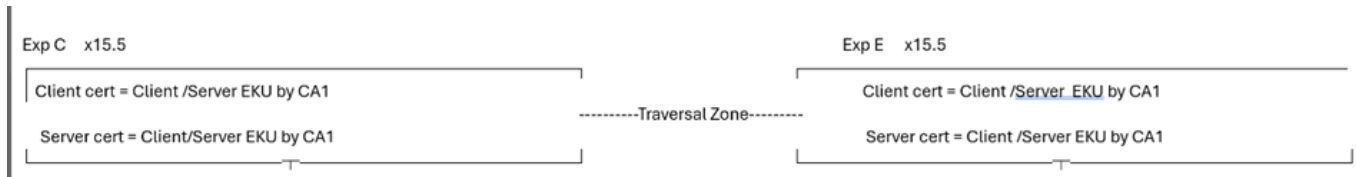


Nota: Compare y tome nota de las EKU presentes en los certificados para que MRA y el proxy WebRTC funcionen. Se trata de una comparación de la implementación en funcionamiento y la no en funcionamiento.

Condición 3: Firma todos los certificados con una CA privada

CA 1 = CA interna

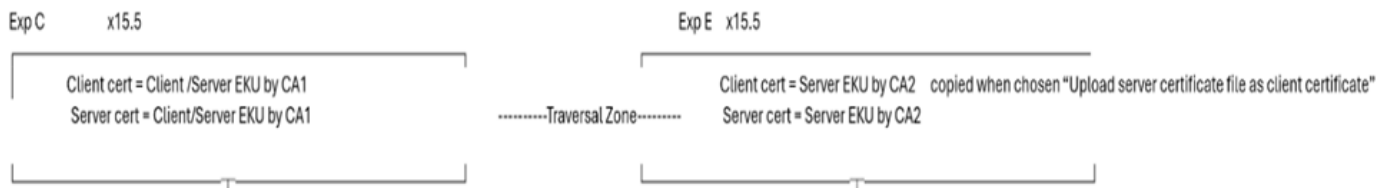
## CA 2 = CA pública



En la condición 3, todos los certificados están firmados por la CA interna (CA1) .

- Cuando Expressway-E envía una conexión TLS, la raíz/intermedia de CA 1 debe intercambiarse con la entidad de extremo lejano. Si el extremo lejano no tiene capacidad o no permite cargar el certificado de CA privada, la conexión TLS no se realiza correctamente.
- Los clientes MRA obtienen certificados para aceptar ventanas emergentes si el certificado privado no está en el almacén de confianza del SO.

Condición 4: Expressway Edge tiene certificados públicos solo con ECU de servidor



En la condición 4, los certificados de servidor y cliente de núcleo de Expressway son (CA1) CA interna firmada y tienen presente ECU de servidor y cliente. El certificado de servidor de Expressway E es una CA pública firmada y solo tiene ECU de servidor. El certificado de servidor se copia en el almacén de certificados de cliente eligiendo Cargar archivo de certificado de servidor como certificado de cliente.

En la condición 4, cuando la conexión TLS se realiza al extremo lejano, si Expressway -E envía un saludo de cliente TLS, el extremo lejano tiene que deshabilitar la comprobación ECU del cliente (ya que el certificado de cliente no tiene ECU de autenticación de cliente); de lo contrario, la conexión TLS no se realiza correctamente.

Puede haber muchas más condiciones o situaciones sobre el terreno basadas en la implementación de los usuarios y los casos de uso, y no se pueden cubrir todas debido a mi limitada corriente de pensamiento. Sin embargo, los puntos a recordar son:

- # Si Expressway se convierte en cliente durante el intercambio de señales de TLS, el certificado de cliente se presenta a los pares.

- #IF Expressway se convierte en servidor durante el intercambio de señales TLS; el certificado del servidor se presenta al par.

Este razonamiento se ha establecido con estos casos de prueba.

## Escenario 1

Para este escenario, Expressway presenta el certificado de cliente durante el intercambio de señales MTLS con Webex.

Videollamada a una reunión de Webex:

Flujo de llamadas de ejemplo Jabber -à CUCM -à Exp Core —à Exp Edge —à Webex

10.106.80.31= Extremo de Expressway

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 tiene un certificado de cliente con este número de serie (2f0000004c869c77c8981becde0000000004c).

Expressway Edge envía un saludo del cliente a Webex durante la negociación TLS y luego envía un certificado de cliente.

Número de serie 2f0000004c869c77c8981becde0000000004c:

1. Expressway Edge envía saludo de cliente (pkt= 13699) a Webex durante la negociación mTLS.
2. Webex envía un saludo de servidor a Expressway Edge (pkt=13701).
3. Webex envía su certificado a Expressway Edge (pkt=13711).
4. Webex solicita el certificado de Expressway Edge "CertificateRequest" (pkt=13715).

## 5. Expressway Edge envía su certificado a Webex (pkt=13718).

(captura de pantalla)

Network traffic capture showing TLS handshake between 10.106.00.31 and 163.129.37.32. Packet 13718 is highlighted, showing the client certificate being sent. Below the capture is a detailed view of the certificate's fields, including version, serial number, signature algorithm, issuer, and validity dates.

```
13698 2026-03-24 17:25:20.911700 10.106.00.31 163.129.37.32 TCP 66 25003 → 5061 [ACK] Seq=1 Ack=1 Min=64512 Len=0 TSval=840949379 TSecr=3608271268
13699 2026-03-24 17:25:20.912773 10.106.00.31 163.129.37.32 TLSv1.2 583 Client Hello
13700 2026-03-24 17:25:20.956852 163.129.37.32 10.106.00.31 TCP 66 5061 → 25003 [ACK] Seq=1 Ack=518 Min=28544 Len=0 TSval=3608271312 TSecr=840949380
13701 2026-03-24 17:25:20.956925 163.129.37.32 10.106.00.31 TLSv1.2 156 Server Hello
13702 2026-03-24 17:25:20.956963 10.106.00.31 163.129.37.32 TCP 66 25003 → 5061 [ACK] Seq=518 Ack=91 Min=64512 Len=0 TSval=840949424 TSecr=3608271313
13703 2026-03-24 17:25:20.957044 163.129.37.32 10.106.00.31 TCP 1308 5061 → 25003 [ACK] Seq=91 Ack=518 Min=28544 Len=1242 TSval=3608271313 TSecr=840949380 [TCP PDU reassembled in 13711]
13704 2026-03-24 17:25:20.957049 10.106.00.31 163.129.37.32 TCP 66 25003 → 5061 [ACK] Seq=518 Ack=1333 Min=67584 Len=0 TSval=840949425 TSecr=3608271313
13705 2026-03-24 17:25:20.957163 163.129.37.32 10.106.00.31 TCP 1308 5061 → 25003 [ACK] Seq=1333 Ack=518 Min=28544 Len=1242 TSval=3608271313 TSecr=840949380 [TCP PDU reassembled in 13711]
13706 2026-03-24 17:25:20.957170 10.106.00.31 163.129.37.32 TCP 66 25003 → 5061 [ACK] Seq=518 Ack=2575 Min=70656 Len=0 TSval=840949425 TSecr=3608271313
13707 2026-03-24 17:25:20.957175 163.129.37.32 10.106.00.31 TCP 1308 5061 → 25003 [ACK] Seq=2575 Ack=518 Min=28544 Len=1242 TSval=3608271313 TSecr=840949380 [TCP PDU reassembled in 13711]
13708 2026-03-24 17:25:20.957179 10.106.00.31 163.129.37.32 TCP 66 25003 → 5061 [ACK] Seq=518 Ack=3817 Min=72704 Len=0 TSval=840949425 TSecr=3608271313
13709 2026-03-24 17:25:20.957184 163.129.37.32 10.106.00.31 TCP 1308 5061 → 25003 [ACK] Seq=3817 Ack=518 Min=28544 Len=1242 TSval=3608271313 TSecr=840949380 [TCP PDU reassembled in 13711]
13710 2026-03-24 17:25:20.957188 10.106.00.31 163.129.37.32 TCP 66 25003 → 5061 [ACK] Seq=518 Ack=5059 Min=71680 Len=0 TSval=840949425 TSecr=3608271313
13711 2026-03-24 17:25:20.957193 163.129.37.32 10.106.00.31 TLSv1.2 378 Certificate
13712 2026-03-24 17:25:20.957215 10.106.00.31 163.129.37.32 TCP 66 25003 → 5061 [ACK] Seq=518 Ack=5371 Min=72704 Len=0 TSval=840949425 TSecr=3608271313
13713 2026-03-24 17:25:20.958101 163.129.37.32 10.106.00.31 TLSv1.2 404 Server Key Exchange
13714 2026-03-24 17:25:20.958110 10.106.00.31 163.129.37.32 TCP 66 25003 → 5061 [ACK] Seq=518 Ack=5709 Min=73728 Len=0 TSval=840949426 TSecr=3608271314
13715 2026-03-24 17:25:20.958341 163.129.37.32 10.106.00.31 TLSv1.2 124 Certificate Request, Server Hello Done
13716 2026-03-24 17:25:20.958350 10.106.00.31 163.129.37.32 TCP 66 25003 → 5061 [ACK] Seq=518 Ack=5767 Min=73728 Len=0 TSval=840949426 TSecr=3608271315
13717 2026-03-24 17:25:20.967687 10.106.00.31 163.129.37.32 TCP 2558 25003 → 5061 [PSH, ACK] Seq=518 Ack=5767 Min=73728 Len=2484 TSval=840949433 TSecr=3608271315 [TCP PDU reassembled in 13718]
13718 2026-03-24 17:25:20.967897 10.106.00.31 163.129.37.32 TLSv1.2 1178 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
13719 2026-03-24 17:25:21.008804 163.129.37.32 10.106.00.31 TCP 66 5061 → 25003 [ACK] Seq=5767 Ack=3082 Min=26112 Len=0 TSval=3608271365 TSecr=840949435
13721 2026-03-24 17:25:21.030881 163.129.37.32 10.106.00.31 TLSv1.2 72 Change Cipher Spec
```

Length: 2936  
Certificates Length: 2933  
Certificates (2933 bytes)  
Certificate length: 2934

```
Certificate [-]: 308207ec308206d6a030201020132f0000004c869c77c8981becde0000000004c  
  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)
```

Certificado de cliente de Expressway Edge:

File explorer showing a list of files, with 'client\_smartslave\_2026-03-24\_11\_55\_47.pem' selected. A 'Certificate' dialog box is open, displaying the details of the selected certificate, including version, serial number, signature algorithm, issuer, and validity dates.

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, bgluclab, B...

2f000004c869c77c8981becde000000004c

## Escenario 2

Expressway se convierte en una entidad de servidor durante el intercambio de señales mTLS y presenta su certificado de servidor:

Cuando Expressway presenta el certificado de servidor, Expressway tiene una zona de vecino segura en 5061 con el nombre de verificación ON.

Zona de vecino seguro entre el nodo x15.5 de Expressway y el nodo x8.11.4 de Expressway:

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)

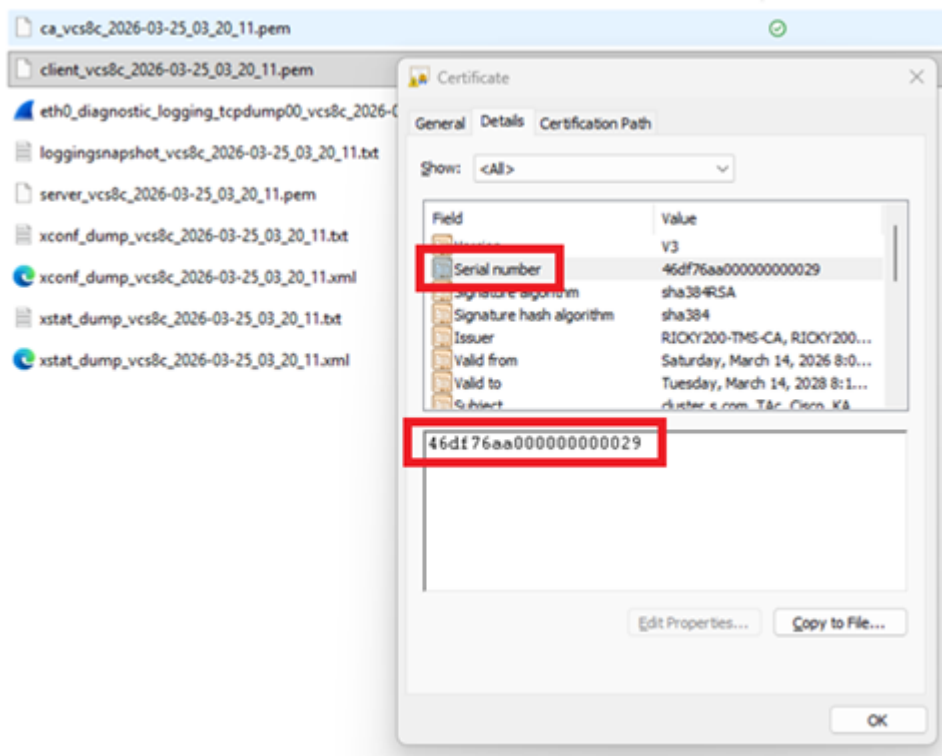
The screenshot displays a network traffic capture of a TLS handshake. The top section shows a list of packets with their details, including source and destination IP addresses, ports, protocols, and application layer data. Key packets include:

- 736: Client Hello from 10.106.80.15 to 10.106.80.16.
- 738: Server Hello from 10.106.80.16 to 10.106.80.15.
- 742: Certificate, Server Key Exchange, Certificate Request, and Server Hello Done from 10.106.80.16 to 10.106.80.15.
- 744: New Session Ticket, Change Cipher Spec, and Encrypted Handshake Message from 10.106.80.15 to 10.106.80.16.

The bottom section provides a detailed view of the Certificate (pkt=742). The certificate structure is as follows:

- Handshake Protocol: Certificate
- Handshake Type: Certificate (11)
- Length: 2919
- Certificates Length: 2916
- Certificates (2916 bytes)
- ▼ Certificate Length: 2005
  - ▼ Certificate [..]: 308207d1308206b9a003020102020a46df76aa00000000029300406092a864886f76d01010c050030491133011060a0992268993f2c6401191603636f6d31183016060a0992268993f2c...
  - ▼ signedCertificate
    - version: v3 (2)
    - serialNumber: 0x46df76aa00000000029
    - ▼ signature (sha256WithRSAEncryption)
    - Algorithm: Id. 1.2.840.113549.1.1.12 (sha256WithRSAEncryption)
    - ▼ Issuer: rdnSequence (0)
      - rdnSequence: 3 items (id-at-commonName=RICKY200-THS-CA,dc=RICKY200,dc=com)
    - ▼ validity

Esta captura de pantalla muestra el certificado del servidor como coincidencias de número de serie:



Caso de prueba 3: el cliente MRA se aprovisiona para el inicio de sesión y el flujo de trabajo incluye la verificación del certificado del servidor de tráfico entre Expressway Core y CUCM.

10.106.80.16 = Núcleo de Expressway x15.5

10 106 80 38 = CUCM

- La exp C 16 envía un saludo de cliente en 6972 TFTP.
- La exp C 16 envía un certificado de cliente durante el intercambio de señales de TLS.



## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).