Navegar por el cliente EKU Sunset con Expressway x15.5

Introducción

Este documento describe cómo navegar por la puesta de sol de EKU 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 (EKU) que definen su propósito:

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

Tradicionalmente, un único certificado podía contener tanto EKU 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 EKU 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 EKU 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 EKU del cliente en Expressway, consulte Preparación de Expressway para la extinción de la EKU 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 EKU 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 EKU only (no hay EKU 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

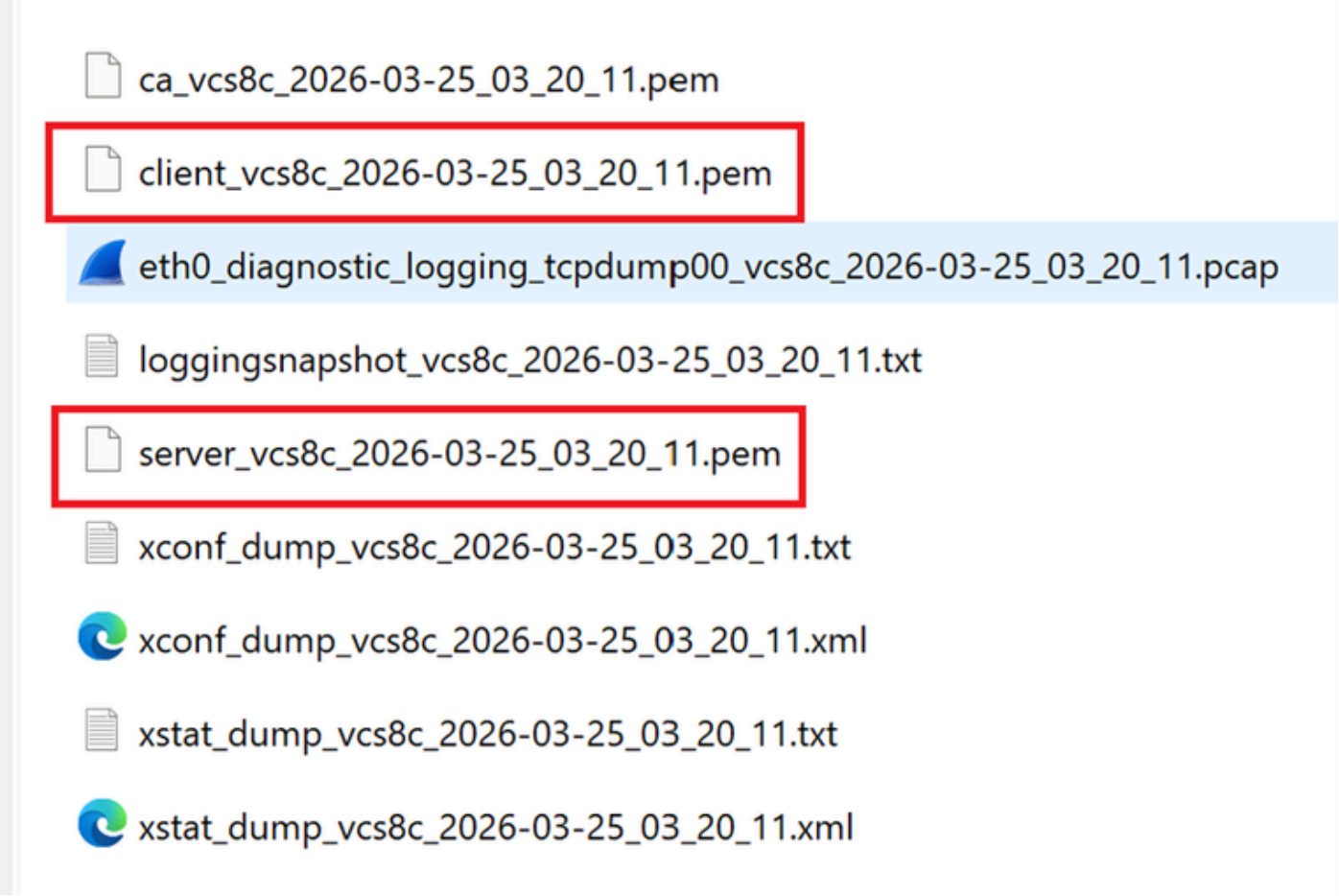
2. Almacén de certificados de cliente

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.



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:00:00:00:00:00:29

Certificado:

Versión: 3 (0x2)

Serial Number:

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

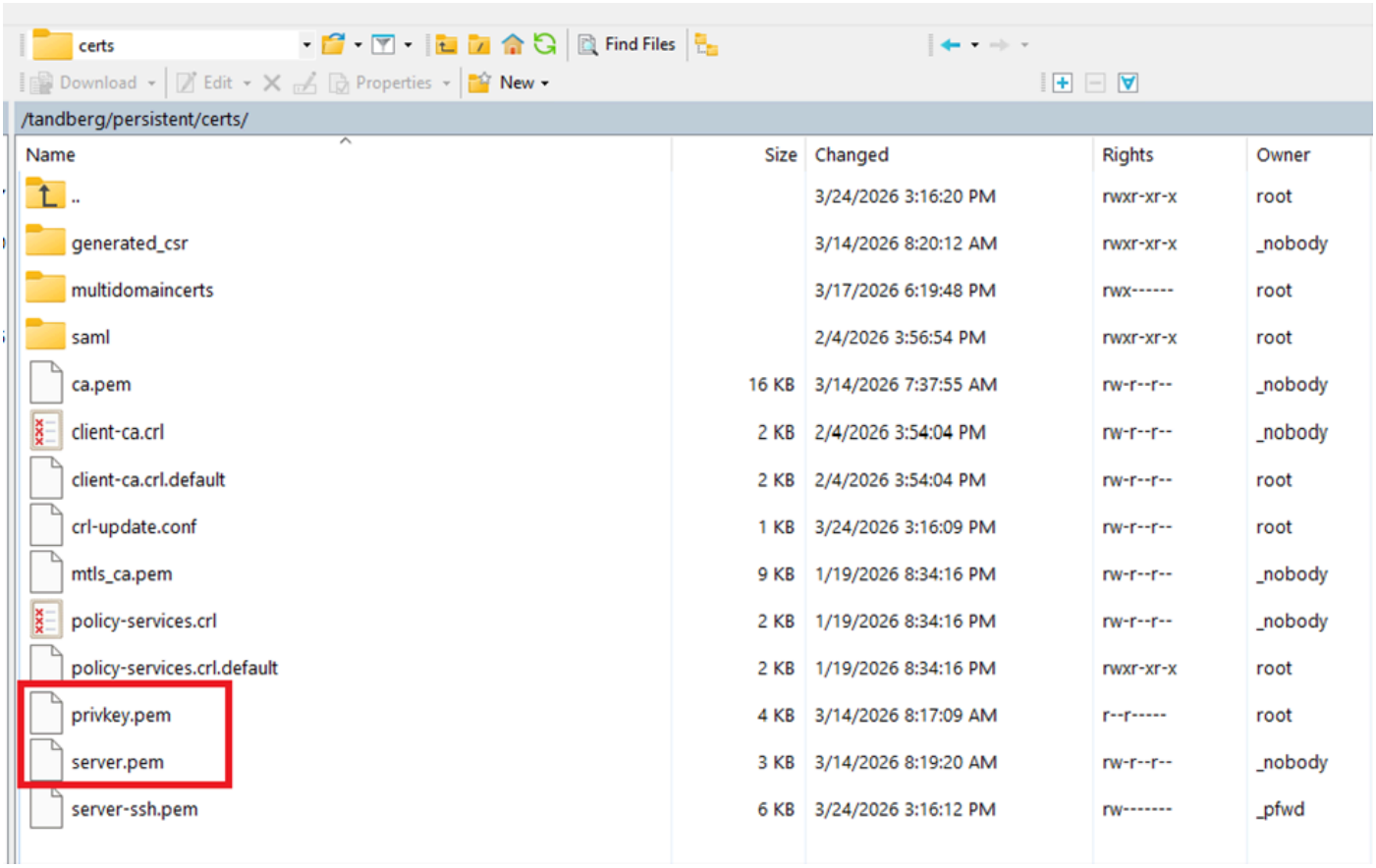
Validez

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

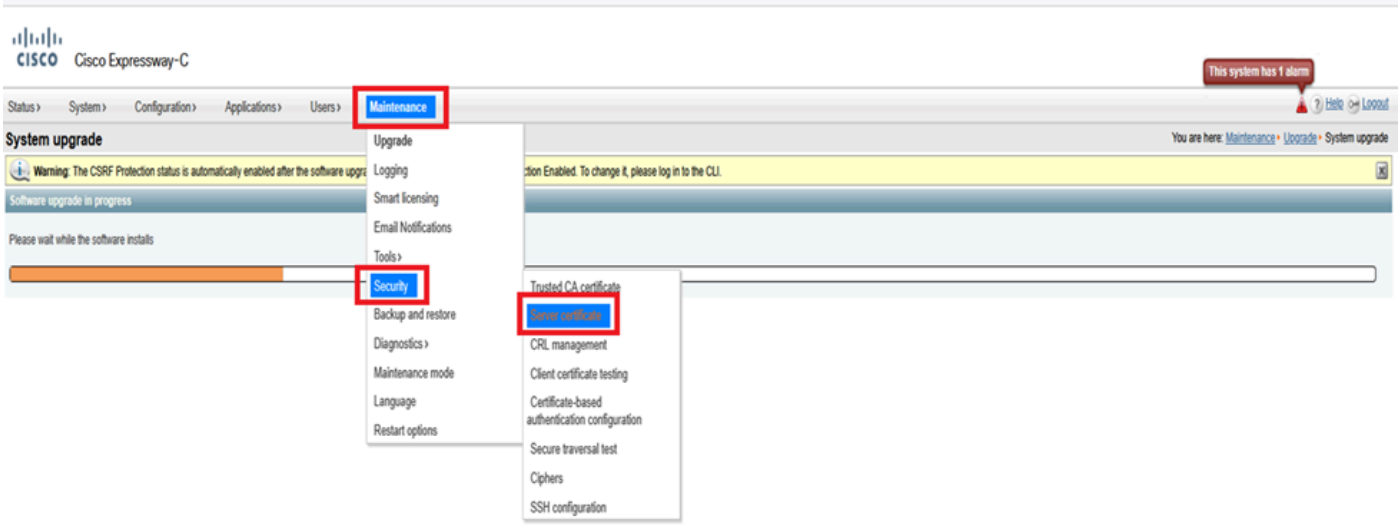
No después de: 14 de marzo 02:47:40 2028 GMT

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:

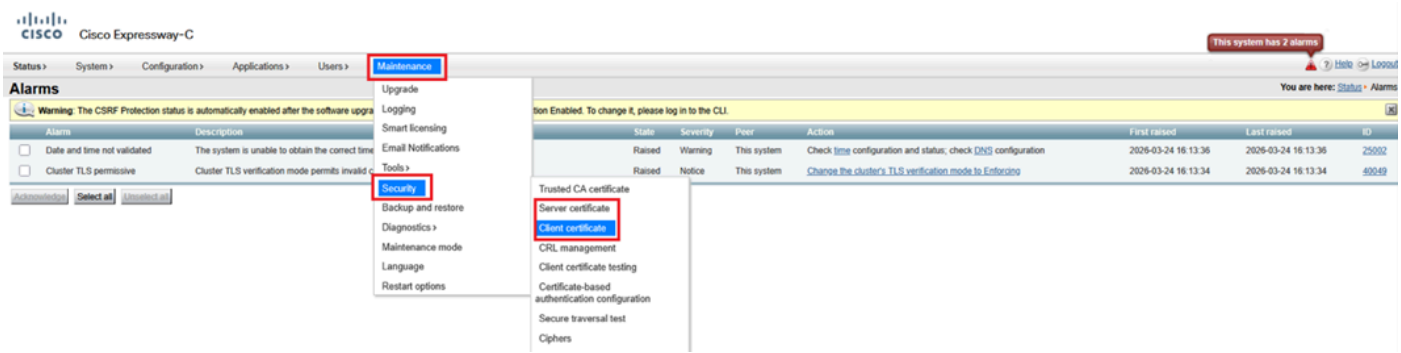


Menú de Expressway (Mantenimiento > Seguridad > Certificado de servidor) en x15.4 (solo el campo de certificado de servidor está presente):



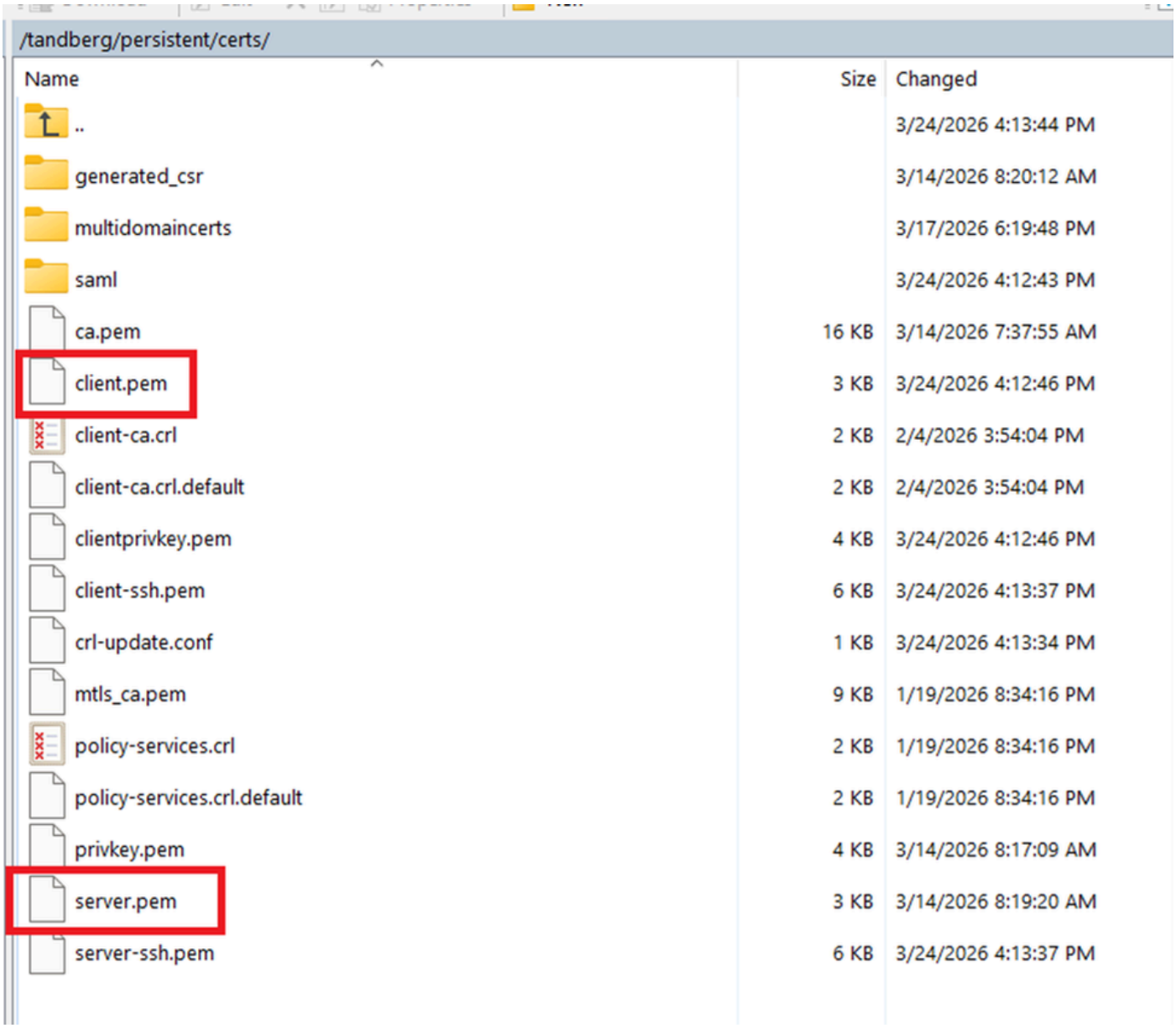
Después de actualizar correctamente a x15.5

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:



Comprobación de EKU X15.5 durante intercambio de señales TLS

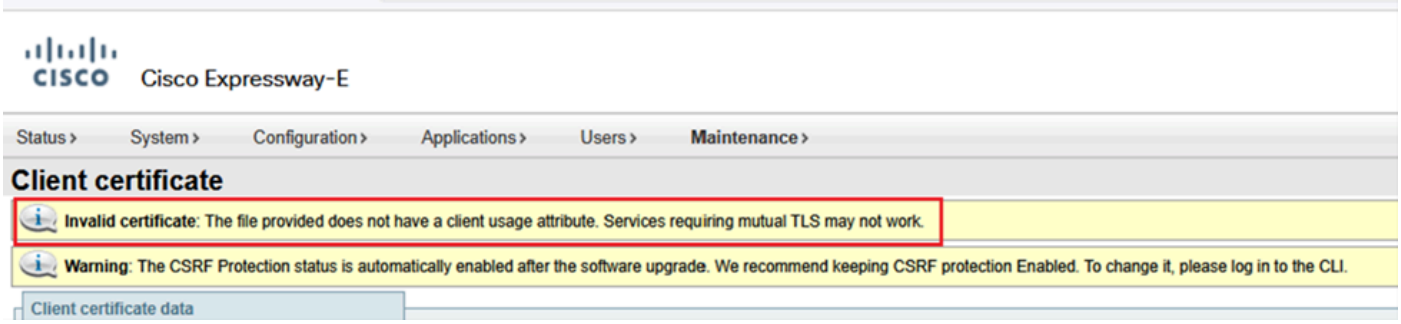
En x15.5, se ha introducido un nuevo comando CLI para verificar el uso extendido de claves (EKU) durante el intercambio de señales TLS. El valor predeterminado es "ON". El conjunto de comandos es válido en Expressway Core y Edge.

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.

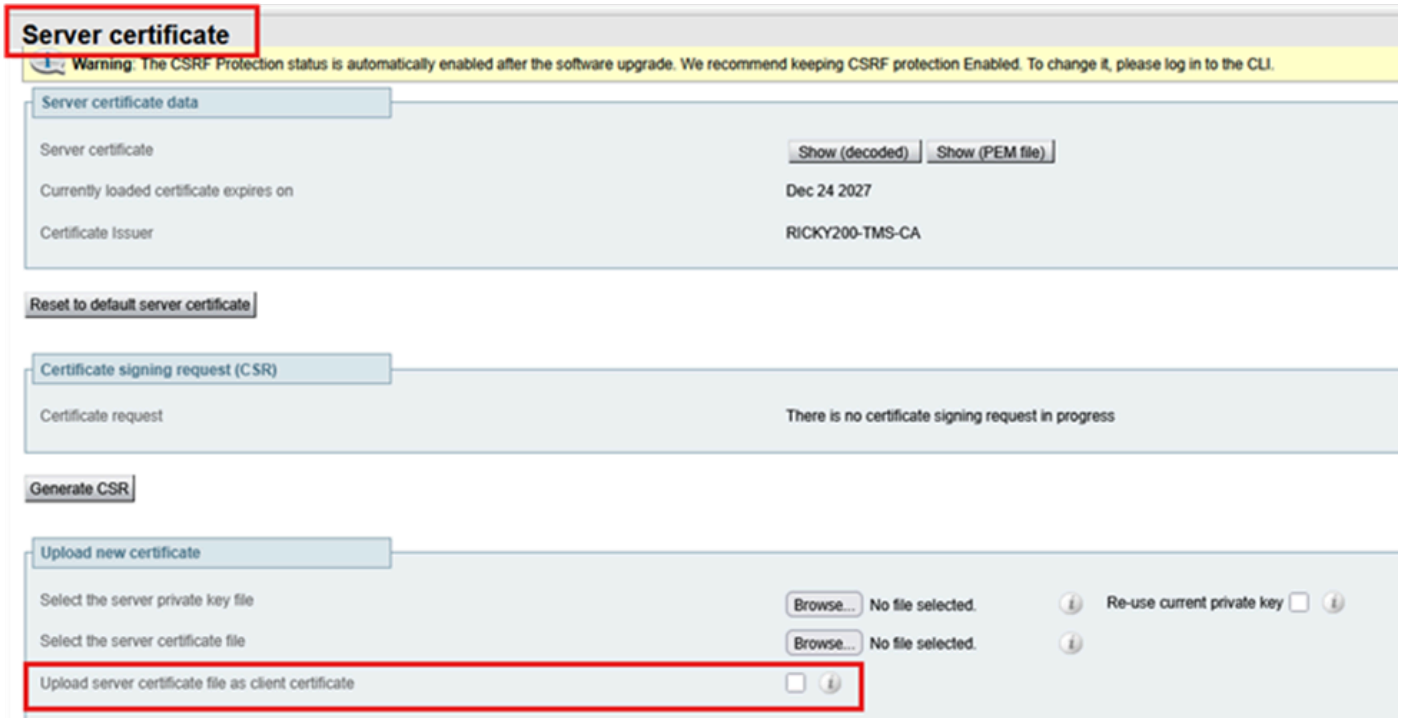
xconfiguration SIP TLS Certificate Extended KeyModo de Verificación de Uso: ON/OFF:

Nota: Si genera un certificado de cliente, firmando un CSR que no contiene EKU 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 EKU del cliente (se puede utilizar una CA privada para insertar la EKU del cliente).

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



Sin embargo, si elige cargar un certificado que sólo tiene una EKU de servidor (sin EKU 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 EKU del servidor solo desde el almacén de certificados del servidor al almacén de certificados del cliente.

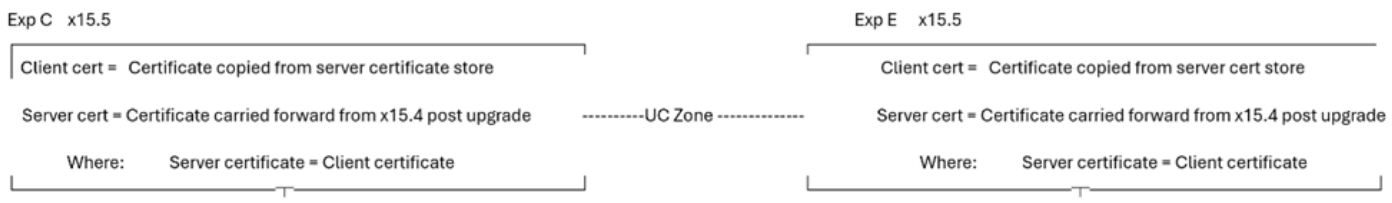


Varios almacenes de certificados, varios escenarios de implementación

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.

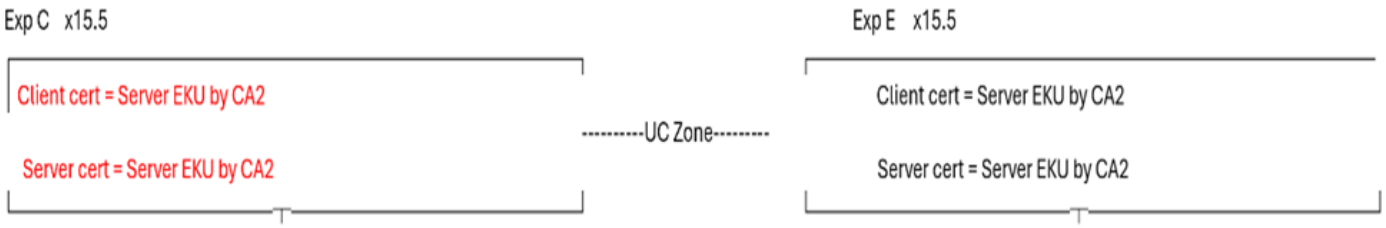


Condición 2: Cuando el administrador instala un nuevo certificado en x15.5 (certificados existentes caducados)

CA 1 = CA interna

CA 2 = CA pública

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



Si el certificado de servidor de núcleo de Expressway no tiene una EKU 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 EKU 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 EKU 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 EKU 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 EKU del cliente.

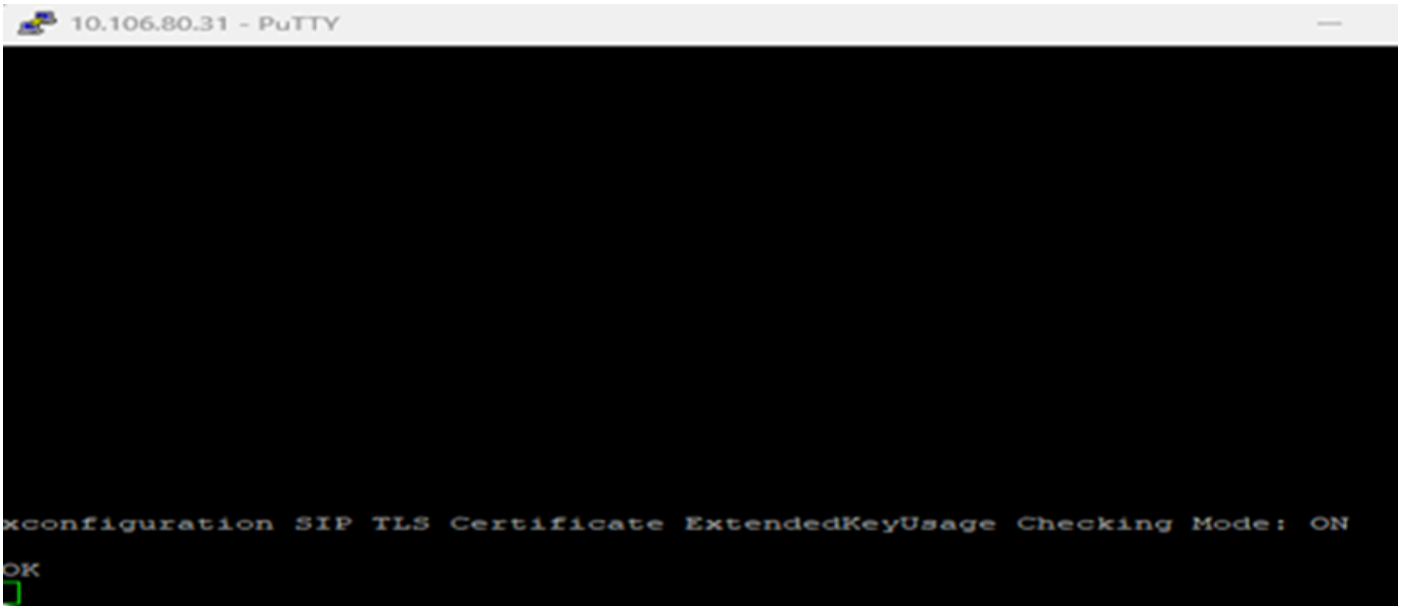
Las funciones de inicio de sesión del cliente MRA y proxy WebRTC no funcionan. Podría tener que recurrir a una CA privada.

Caso de prueba 1

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

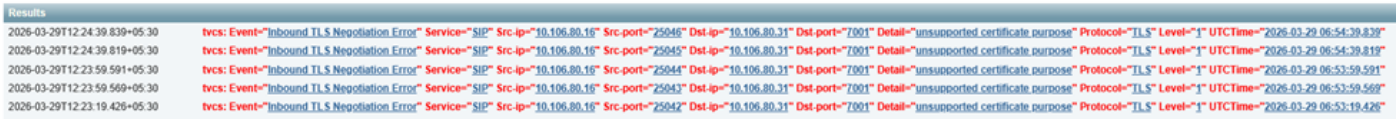
En Expressway-Edge ExtendedKeyUsage Active.

xconfiguration SIP TLS Certificate Extended KeyModo 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:

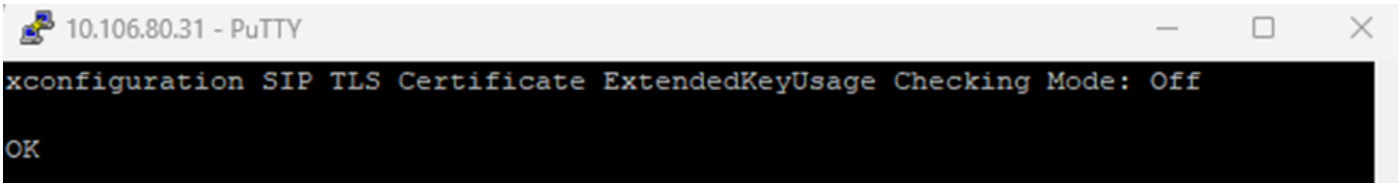


Caso de prueba 2

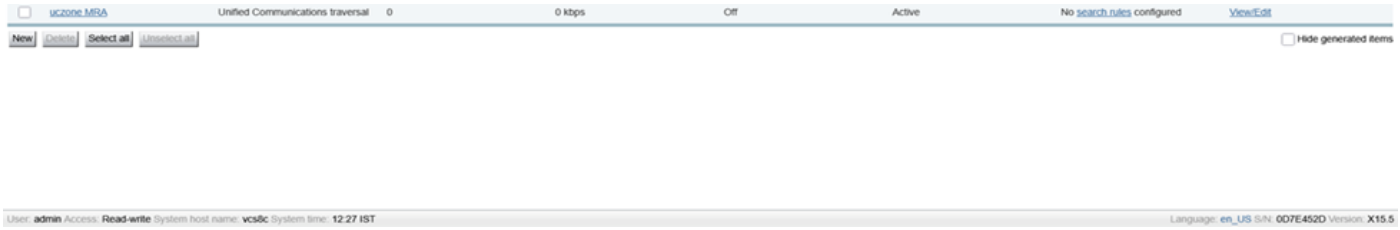
- Cuando la comprobación EKU está desactivada en Expressway E
- Cuando el certificado de cliente y servidor en Expressway Core tiene solo EKU de servidor
- El estado de la zona de UC es ACTIVO

Desactive la comprobación EKU en Expressway E.

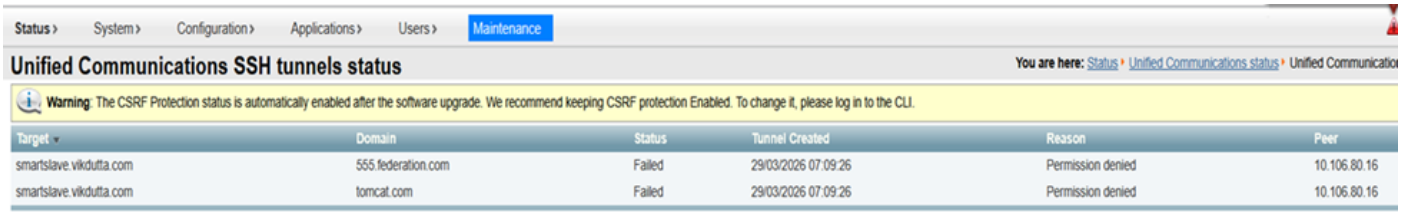
xconfiguration SIP TLS Certificate Extended KeyModo de Verificación de Uso: Desactivado



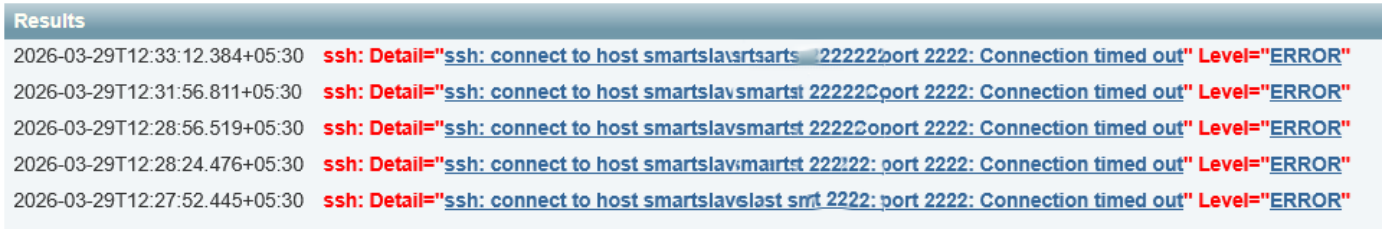
Zona de comunicación unificada activa:



Sin embargo, los túneles ssh aún fallaron:



Registros de eventos de Expressway:



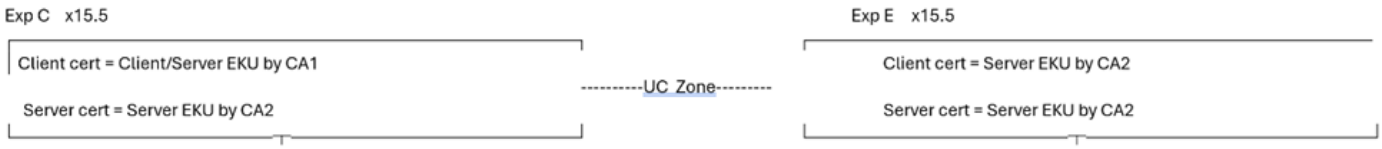
Condición 2.1: Caso de éxito

CA 1 = CA interna

CA 2 = CA pública

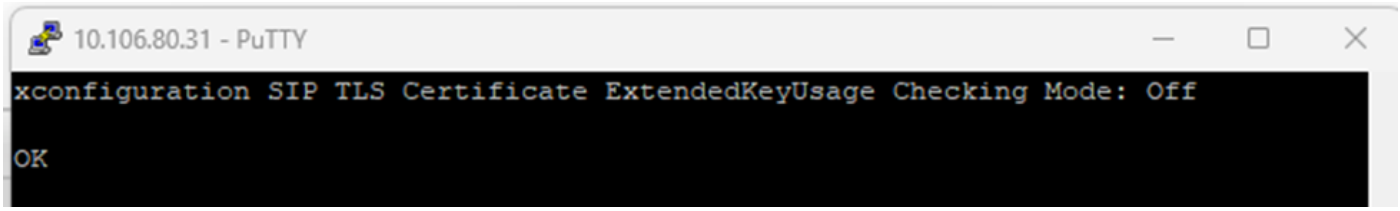
- Donde el certificado de cliente de núcleo de Expressway está firmado por CA 1 (CA interna) e incluye EKU cliente/servidor.
- El certificado de servidor de núcleo de Expressway está firmado por CA 2 pública e incluye solo EKU de servidor.

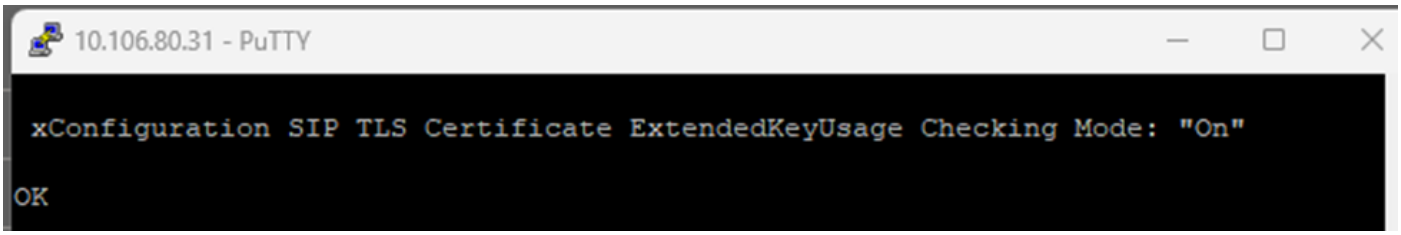
- El certificado de servidor perimetral de Expressway está firmado por CA 2 pública e incluye solo EKU de servidor.
- El certificado de cliente de Expressway Edge está firmado por una CA 2 pública e incluye solo EKU de servidor.



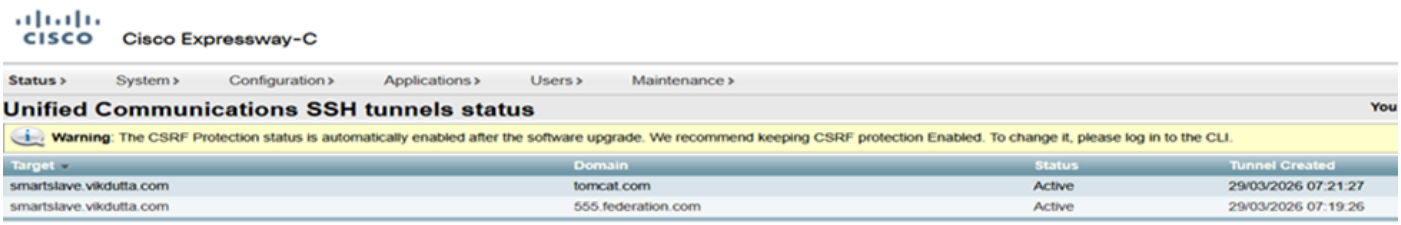
Esta condición es un caso de éxito. Independientemente de si el modo de verificación EKU está activado/desactivado, la zona de Unified Communication y el túnel SSH se activan. Los clientes de MRA trabajan.

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:

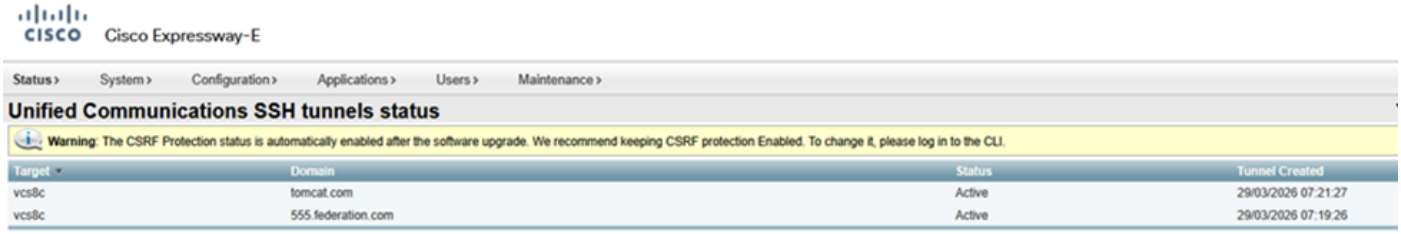




Túneles SSH en núcleo de Expressway activo:

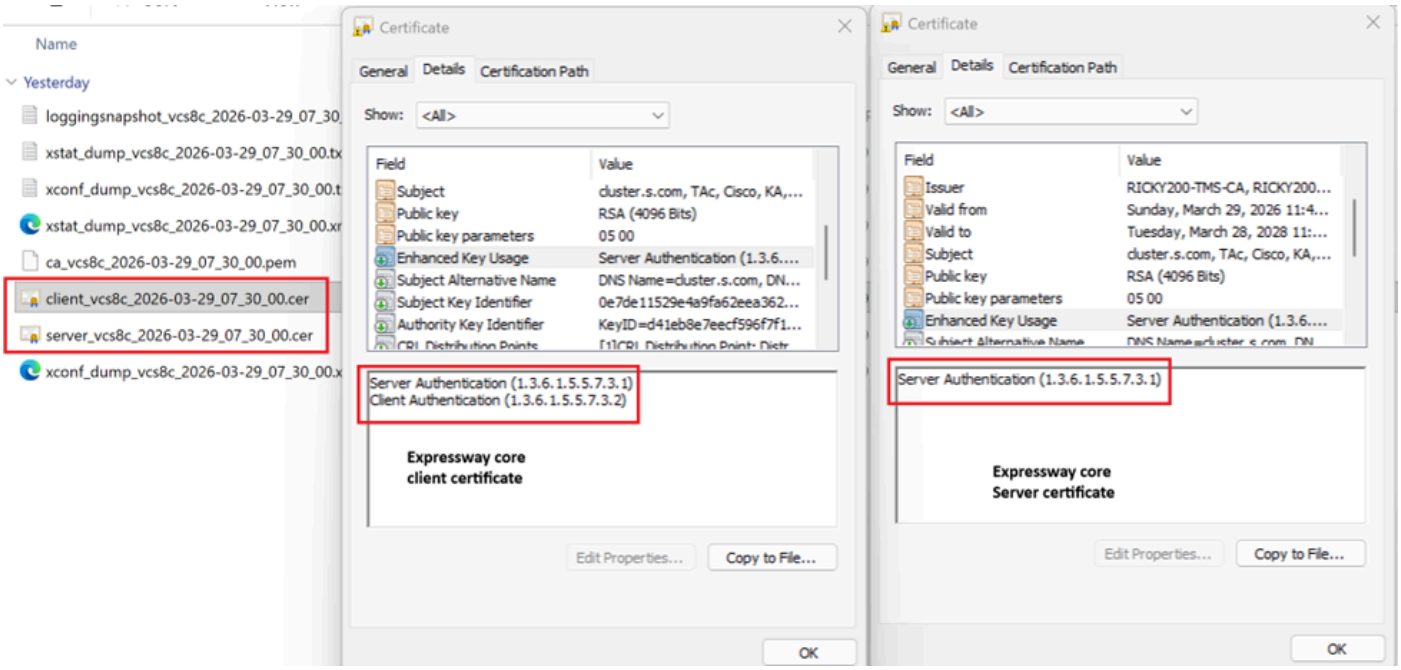


Túneles SSH en Expressway Edge Active:

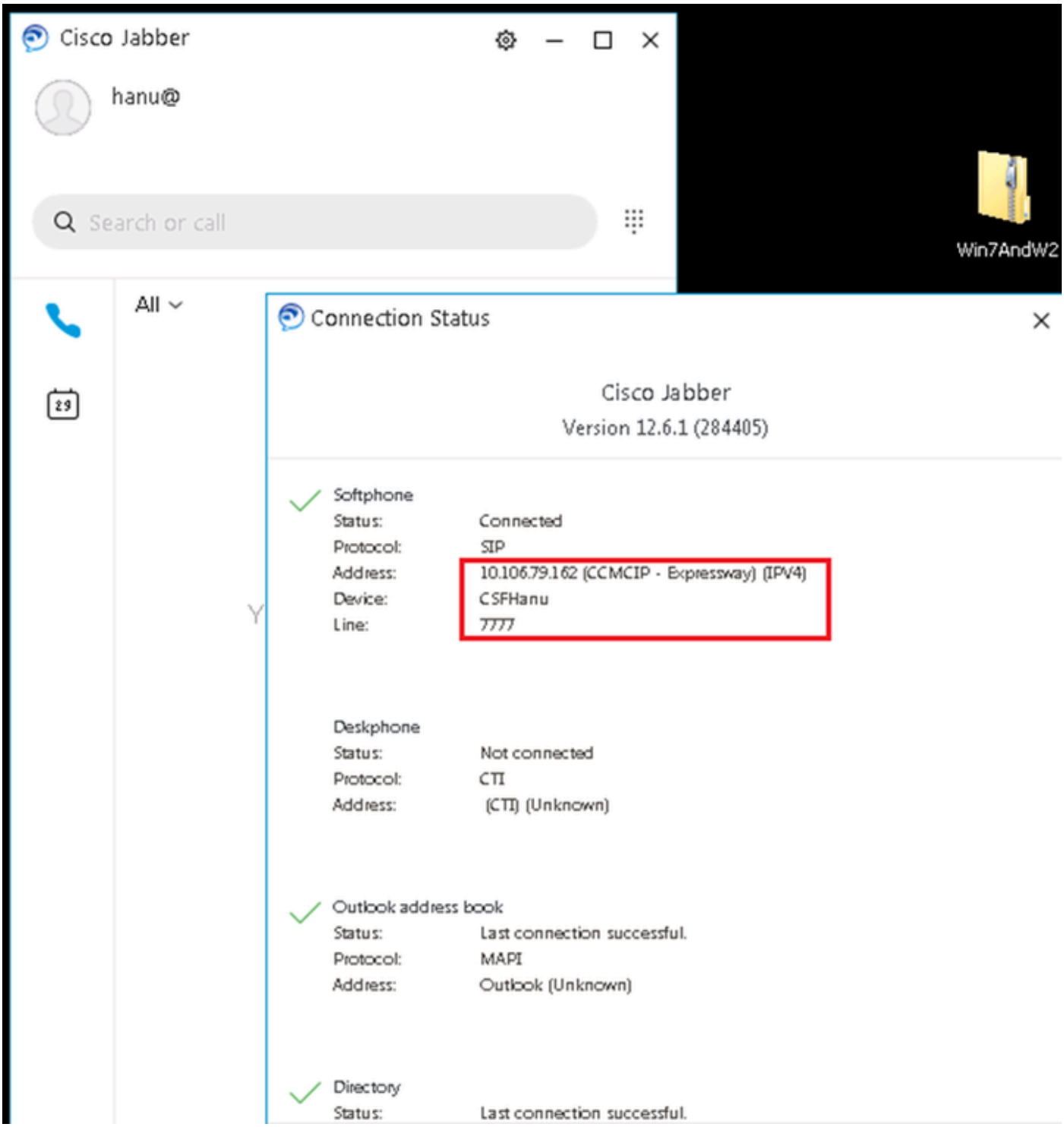


Estado de la zona MRA de Unified Communication Activo:

- 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:

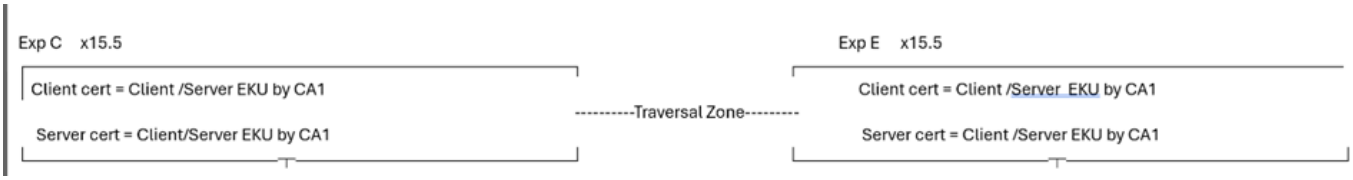


Nota: Compare y tome nota de las EKU presentes en los certificados para que MRA y el proxy WebRTC funcionen. Se trata de una comparación de la implementación en funcionamiento y la no en funcionamiento.

Condición 3: Firma todos los certificados con una CA privada

CA 1 = CA interna

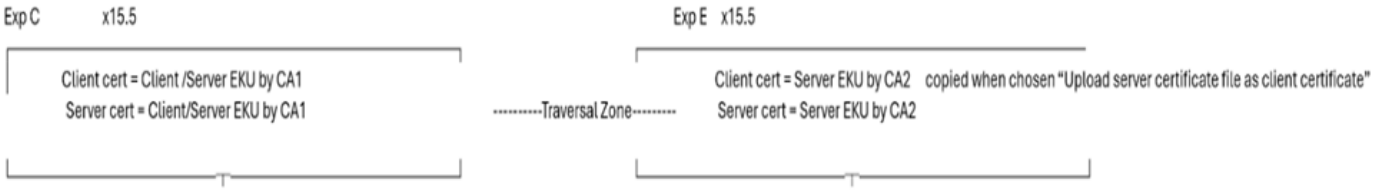
CA 2 = CA pública



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 EKU de servidor



En la condición 4, los certificados de servidor y cliente de núcleo de Expressway son (CA1) CA interna firmada y tienen presente EKU de servidor y cliente. El certificado de servidor de Expressway E es una CA pública firmada y solo tiene EKU 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 EKU del cliente (ya que el certificado de cliente no tiene EKU 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 (2f0000004c869c77c8981becde00000000004c).

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

Número de serie 2f0000004c869c77c8981becde00000000004c:

1. Expressway Edge envía saludo de cliente (pkt= 13699) a ‘Webex durante la negociación mTLS.

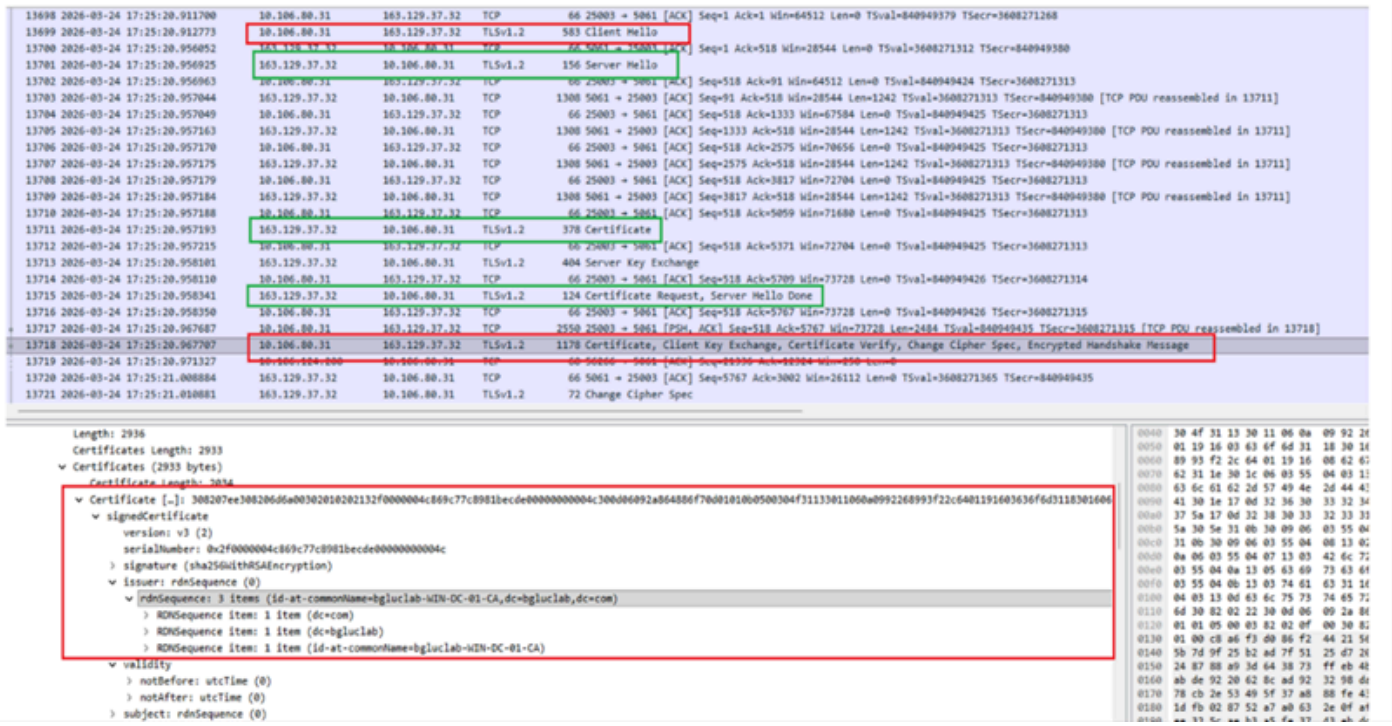
2. Webex envía un saludo de servidor a Expressway Edge (pkt=13701).

3. Webex envía su certificado a Expressway Edge (pkt=13711).

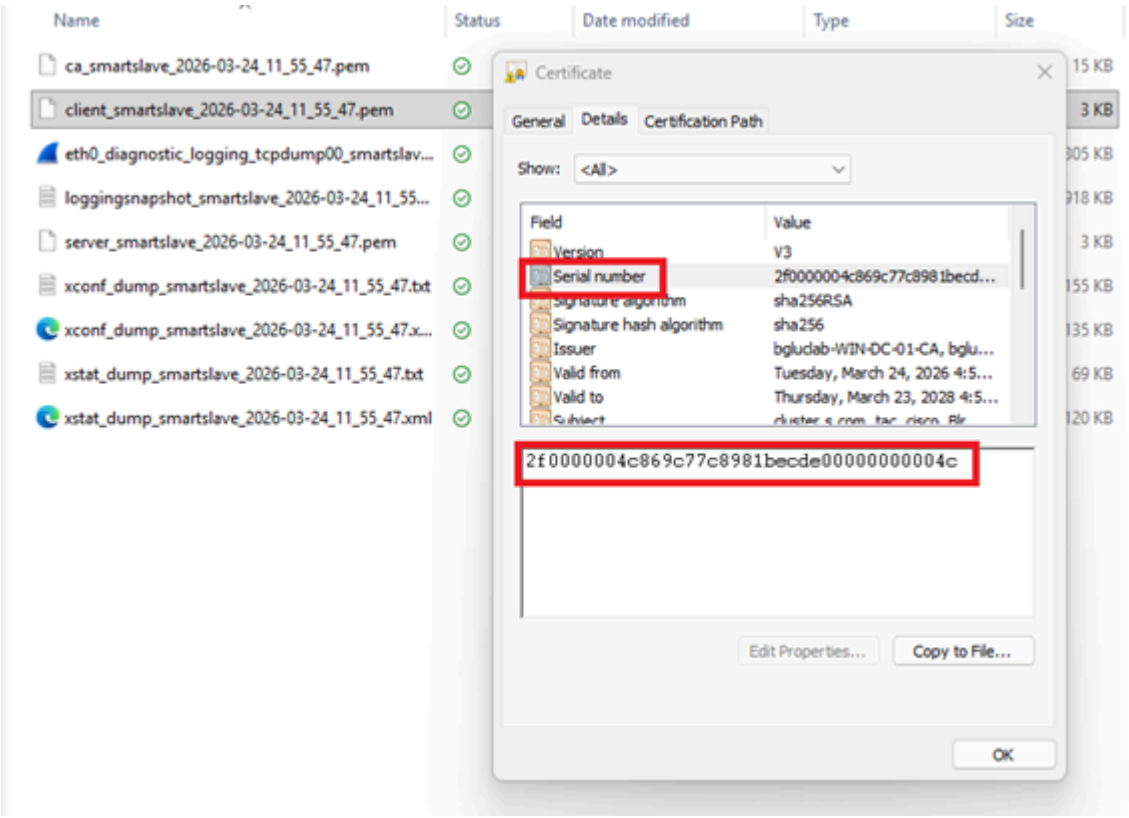
4. Webex solicita el certificado de Expressway Edge "CertificateRequest" (pkt=13715).

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

(captura de pantalla)



Certificado de cliente de Expressway Edge:



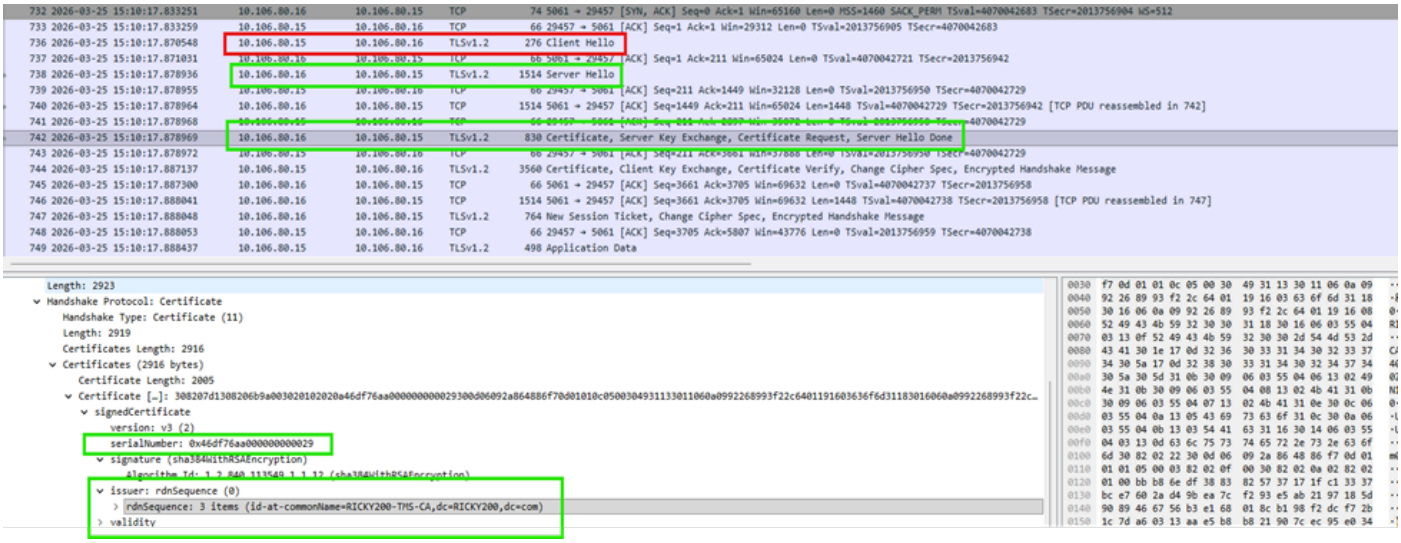
Escenario 2

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

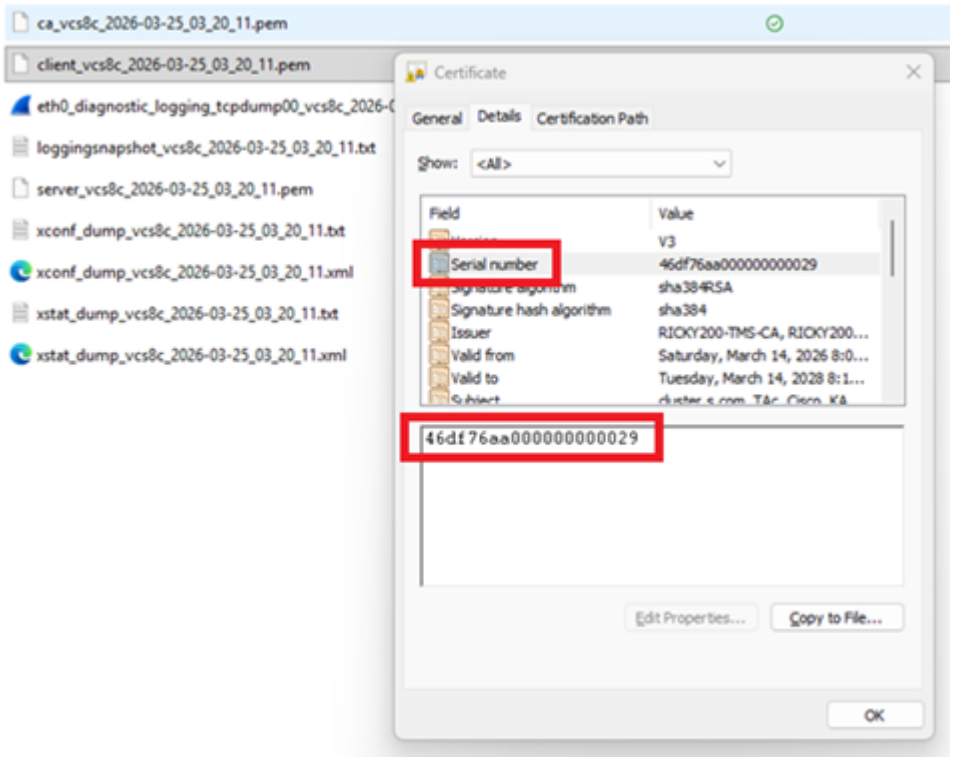
Cuando Expressway presenta el certificado de servidor, Expressway tiene una zona de vecino segura en 5061 con el nombre de verificación ON.

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)
```



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

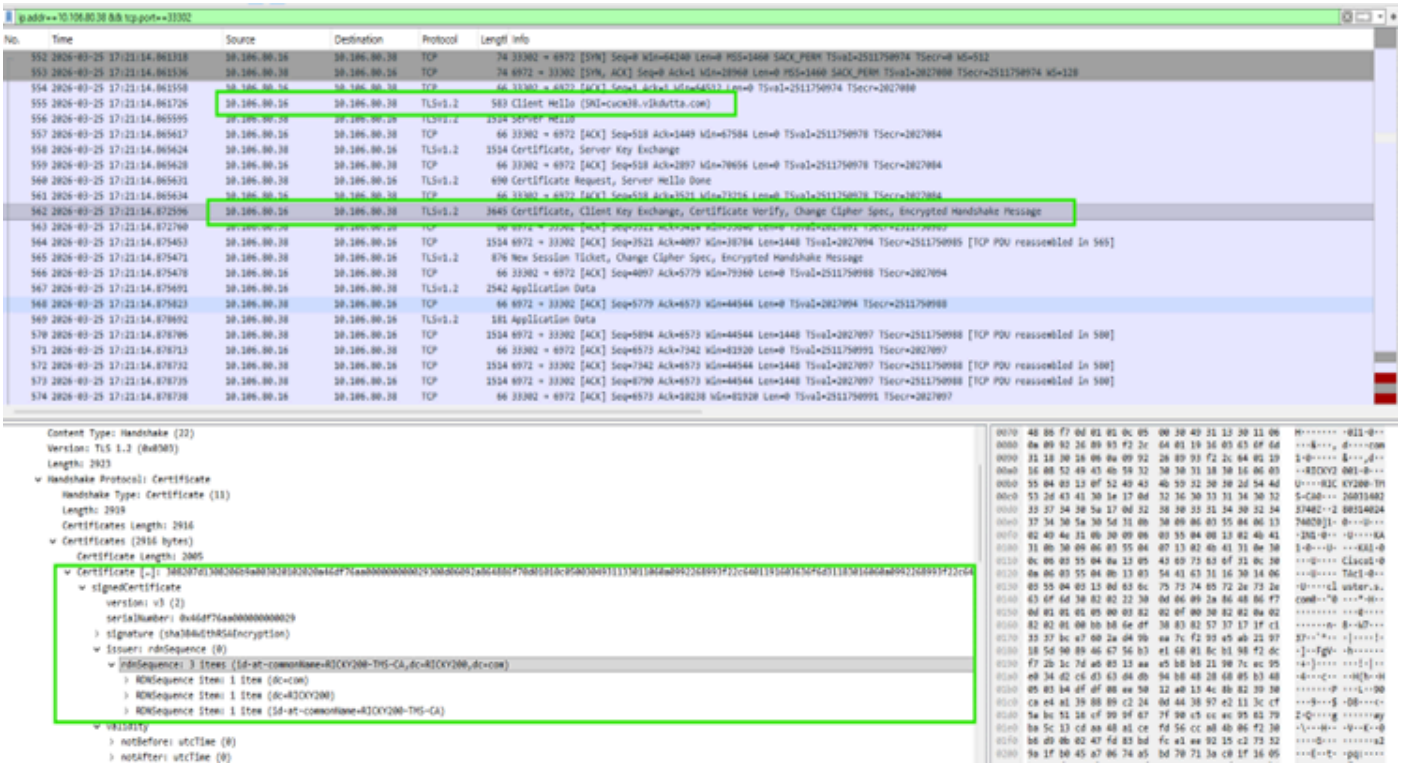


Caso de prueba 3: el cliente MRA se aprovisiona para el inicio de sesión y el flujo de trabajo incluye la verificación del certificado del servidor de tráfico entre Expressway Core y CUCM.

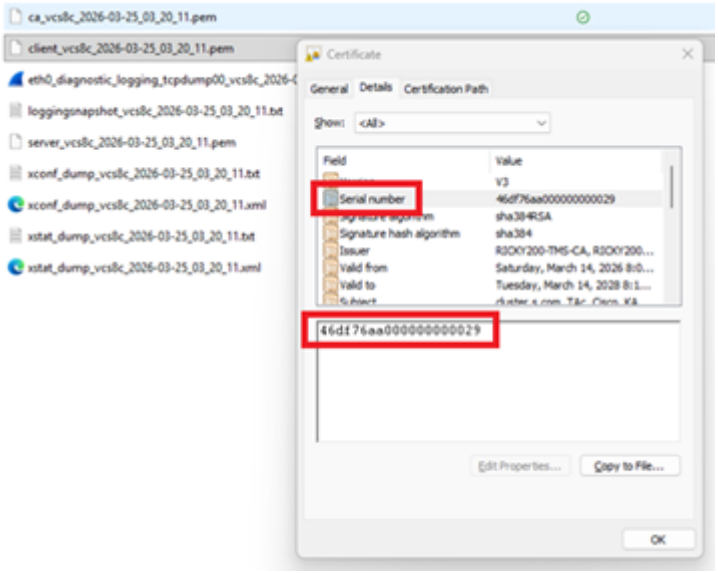
10.106.80.16 = Núcleo de Expressway x15.5

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.



Certificado de cliente de núcleo de Expressway:



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).