Configurar y solucionar problemas de certificados de Collaboration Edge (MRA)

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Autoridad de certificación pública frente a autoridad de certificación privada (CA)
Cómo funcionan las cadenas de certificados
Resumen del intercambio de señales de SSL
Configurar
Zona transversal y de confianza de Expressway-C y Expressway-E
Generar y firmar CSR
Configuración de Expressway-C y Expressway-E para que confíen entre sí
Protección de las comunicaciones entre Cisco Unified Communications Manager (CUCM) y Expressway-C
Overview
Configuración de la confianza entre CUCM y Expressway-C
Servidores de CUCM con certificados autofirmados
Consideraciones sobre clústeres de Expressway-C y Expressway-E
Certificados de clúster
Listas de autoridades de certificación de confianza
Verificación
Comprobar la información del certificado actual
Leer/Exportar un certificado en Wireshark
Troubleshoot
Pruebe para saber si un certificado es de confianza en Expressway
Terminales de Synergy Light (teléfonos de las series 7800 y 8800)
Recursos de video
Generar una CSR para MRA o Clustered Expressways
Instalar certificado de servidor en Expressway
Cómo configurar la confianza de certificados entre Expressways

Introducción

Este documento describe los certificados relacionados con las implementaciones de acceso remoto móvil (MRA).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Autoridad de certificación (CA) pública o privada

Hay un número de opciones para firmar certificados en los servidores de Expressway-C y E. Puede optar por que la Solicitud de firma de certificado (CSR) esté firmada por una CA pública como GoDaddy, Verisign u otros, o puede firmarla internamente si utiliza su propia Autoridad de certificación (puede estar autofirmada con OpenSSL o una CA empresarial interna como un servidor de Microsoft Windows). Para obtener más información sobre cómo crear y firmar los CSR utilizados por cualquiera de estos métodos, consulte la Guía de creación de certificados de Video Communication Server (VCS).

El único servidor que realmente necesita la firma de una CA pública es Expressway-E. Este es el único servidor donde los clientes ven el certificado cuando inician sesión a través de MRA, por lo tanto, utilice una CA pública para asegurarse de que los usuarios no tengan que aceptar manualmente el certificado. Expressway-E puede funcionar con un certificado firmado por una CA interna, pero a los usuarios primerizos se les solicitará que acepten el certificado no fiable. El registro MRA de teléfonos de las series 7800 y 8800 no funcionaría con certificados internos porque no se puede modificar su lista de certificados de confianza. Para simplificar, se recomienda que los certificados de Expressway-C y Expressway-E estén firmados por la misma CA; sin embargo, esto no es un requisito siempre que haya configurado correctamente las listas de CA de confianza en ambos servidores.

Cómo funcionan las cadenas de certificados

Los certificados se vinculan en una cadena de dos o más que se utiliza para comprobar el origen que firmó el certificado del servidor. Hay tres tipos de certificados en una cadena: el certificado de cliente/servidor, el certificado intermedio (en algunos casos) y el certificado raíz (también denominado CA raíz, ya que es la autoridad de nivel superior que firmó el certificado).

Los certificados contienen dos campos principales que crean la cadena: el asunto y el emisor.

El asunto es el nombre del servidor o la autoridad que representa este certificado. En el caso de Expressway-C o Expressway-E (u otros dispositivos de Unified Communications (UC)), se crea a partir del nombre de dominio completamente calificado (FQDN).

El emisor es la autoridad que validó el certificado específico. Dado que cualquier persona puede firmar un certificado (que incluye el servidor que creó el certificado, para empezar, también conocido como certificados autofirmados), los servidores y clientes tienen una lista de emisores o CA en los que confían como auténticos.

Una cadena de certificados siempre termina con un certificado raíz o de nivel superior autofirmado. A medida que se desplaza por la jerarquía de certificados, cada certificado tiene un emisor diferente en relación con el sujeto. Finalmente, encontrará la CA raíz donde coinciden el asunto y el emisor. Esto indica que es el certificado de nivel superior y, por lo tanto, el que debe ser de confianza para la lista de CA de confianza de un cliente o servidor.

Resumen del intercambio de señales de SSL

En el caso de la zona transversal, Expressway-C siempre actúa como cliente, mientras que Expressway-E

siempre es el servidor. El intercambio simplificado funciona como se muestra a continuación:

Expressway-C Expressway-E

---------Saludo del cliente-------->

<--------Hello--------- de servidor

<----Certificado de servidor-------

<----Solicitud de certificadoâ€”

------Certificado de cliente------>

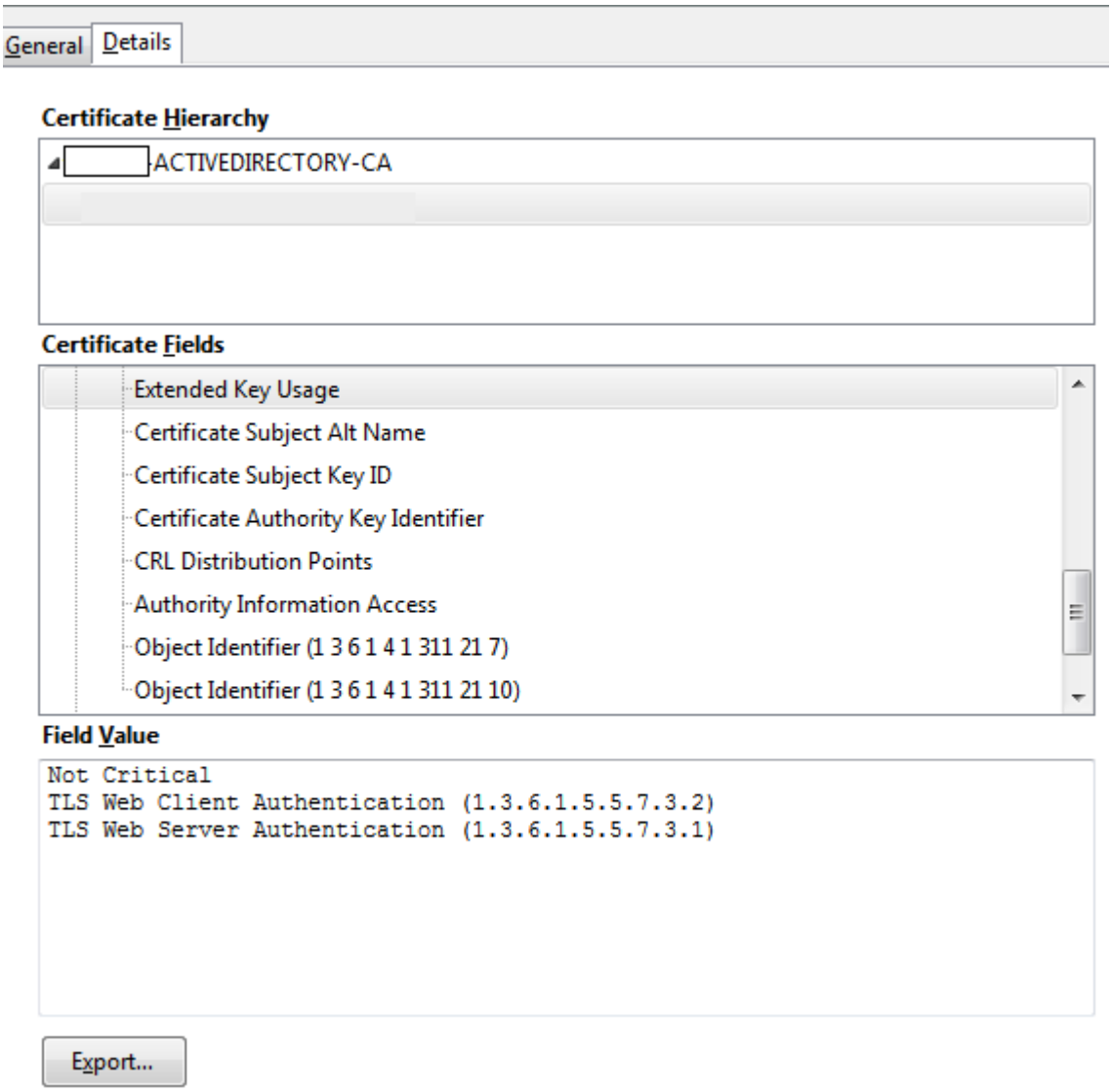
La clave aquí está en el intercambio, ya que Expressway-C siempre inicia la conexión y, por lo tanto, siempre es el cliente. Expressway-E es el primero en enviar su certificado. Si Expressway-C no puede validar este certificado, elimina el protocolo de enlace y no puede enviar su propio certificado a Expressway-E.

Otro aspecto importante que vale notar son los atributos de autenticación de cliente web de seguridad de capa de transporte (TLS) y los atributos de autenticación de servidor web de TLS. Estos atributos se determinan en la CA que firmó el CSR (si se utiliza una CA de Windows, se determina por la plantilla seleccionada) e indican si el certificado es válido en la función del cliente o del servidor (o en ambos). Debido a que para un VCS o Expressway, se puede basar en la situación (siempre es lo mismo para una zona transversal), y el certificado debe tener atributos de autenticación de cliente y de servidor.

Expressway-C y Expressway-E producen un error cuando se cargan en un nuevo certificado de servidor, si no se aplican ambos.

Si no está seguro de si un certificado tiene estos atributos, puede abrir los detalles del certificado en un navegador o en su sistema operativo, y verificar la sección Uso de clave extendida (vea la imagen). El formato puede variar y depende de cómo mire el certificado.

Ejemplo:



Configurar

Zona transversal y de confianza de Expressway-C y Expressway-E

Generar y firmar CSR

Como se ha descrito anteriormente, los certificados de Expressway-C y Expressway-E deben estar firmados por una CA interna o externa, o por OpenSSL para que se firmen automáticamente.

> **Nota**: no puede utilizar el certificado temporal que se incluye en el servidor de Expressway, ya que no es compatible. Si utiliza certificados comodín en los que tiene un certificado de firma de CA y la línea de asunto no está definida específicamente, no se admite.

El primer paso es generar el CSR y que lo firme el tipo de CA preferida. Este proceso se detalla específicamente en la guía de creación de certificado. Al crear la CSR, es importante tener en cuenta los nombres alternativos de asunto (SAN) necesarios que deben incluirse en los certificados. Esto también se detalla en la guía de certificados y la guía de implementación de acceso remoto móvil. Consulte las versiones más recientes de la guía a medida que se añaden nuevas funciones. Lista de SAN comunes que se deben incluir, en función de las funciones utilizadas:

Expressway-C

- Cualquier dominio (interno o externo) agregado a la lista de dominios.
- Cualquier alias de nodo de chat persistente si se utiliza la federación XMPP.
- Proteja los nombres de perfiles de dispositivos en CUCM si se utilizan perfiles de dispositivos seguros.

Expressway-E

- Cualquier dominio configurado en Expressway-C.
- Cualquier alias de nodo de chat persistente si se utiliza la federación XMPP.
- Cualquier dominio publicitado para federaciones XMPP.

Nota: si el dominio base utilizado para las búsquedas de registros de servicio externos (SRV) no se incluye como SAN en el certificado de Expressway-E (xxx.com o collab-edge.xxx.com), los clientes Jabber siguen requiriendo que el usuario final acepte el certificado en la primera conexión y los terminales TC no se podrán conectar en absoluto.

Configuración de Expressway-C y Expressway-E para que confíen entre sí

Para que la zona transversal de Unified Communications establezca una conexión, Expressway-C y Expressway-E deben confiar en los certificados de los demás. Para este ejemplo, suponga que el certificado de Expressway-E fue firmado por una CA pública que usa esta jerarquía.

Certificado 3

Emisor: CA raíz de GoDaddy

Asunto: CA raíz de GoDaddy

Certificado 2

Emisor: CA raíz de GoDaddy

Asunto: Autoridad intermedia de GoDaddy

Certificado 1

Emisor: Autoridad intermedia de GoDaddy

Asunto: Expressway-E.lab

Expressway-C debe configurarse con el certificado de confianza 1. En la mayoría de los casos, basándose en los certificados de confianza aplicados al servidor, sólo envía su certificado de servidor de nivel más bajo. Esto significa que para que Expressway-C confíe en el certificado 1, debe cargar los certificados 2 y 3 en la lista de CA de confianza de Expressway-C (**Mantenimiento> Seguridad > Lista de CA de confianza**). Si deja fuera el certificado intermedio 2 cuando Expressway-C recibe el certificado de Expressway-E, no puede tener una manera de vincularlo a la CA raíz de GoDaddy de confianza, por lo tanto, se rechazaría.

Certificado 3

Emisor: CA raíz de GoDaddy

Asunto: CA raíz de GoDaddy

Certificado 1

Emisor: Autoridad intermedia de GoDaddy: no es de confianza

Asunto: Expressway-E.lab

Además, si solo carga el certificado intermedio sin la raíz en la lista de CA de confianza de Expressway-C, vería que la autoridad intermedia de GoDaddy es de confianza, pero está firmado por una autoridad superior, en este caso, CA raíz de GoDaddy que no es de confianza, por lo tanto, fallaría.

Certificado 2

Emisor: CA raíz de GoDaddy: no es de confianza

Asunto: Autoridad intermedia de GoDaddy

Certificado 1

Emisor: Autoridad intermedia de GoDaddy

Asunto: Expressway-E.lab

Una vez que se agregaron todas las autoridades intermedias y la raíz a la lista de CA de confianza, se puede comprobar el certificado...

Certificado 3

Emisor: CA raíz de GoDaddy: el certificado autofirmado de nivel superior es de confianza y la cadena está completa.

Asunto: CA raíz de GoDaddy

Certificado 2

Emisor: CA raíz de GoDaddy

Asunto: Autoridad intermedia de GoDaddy

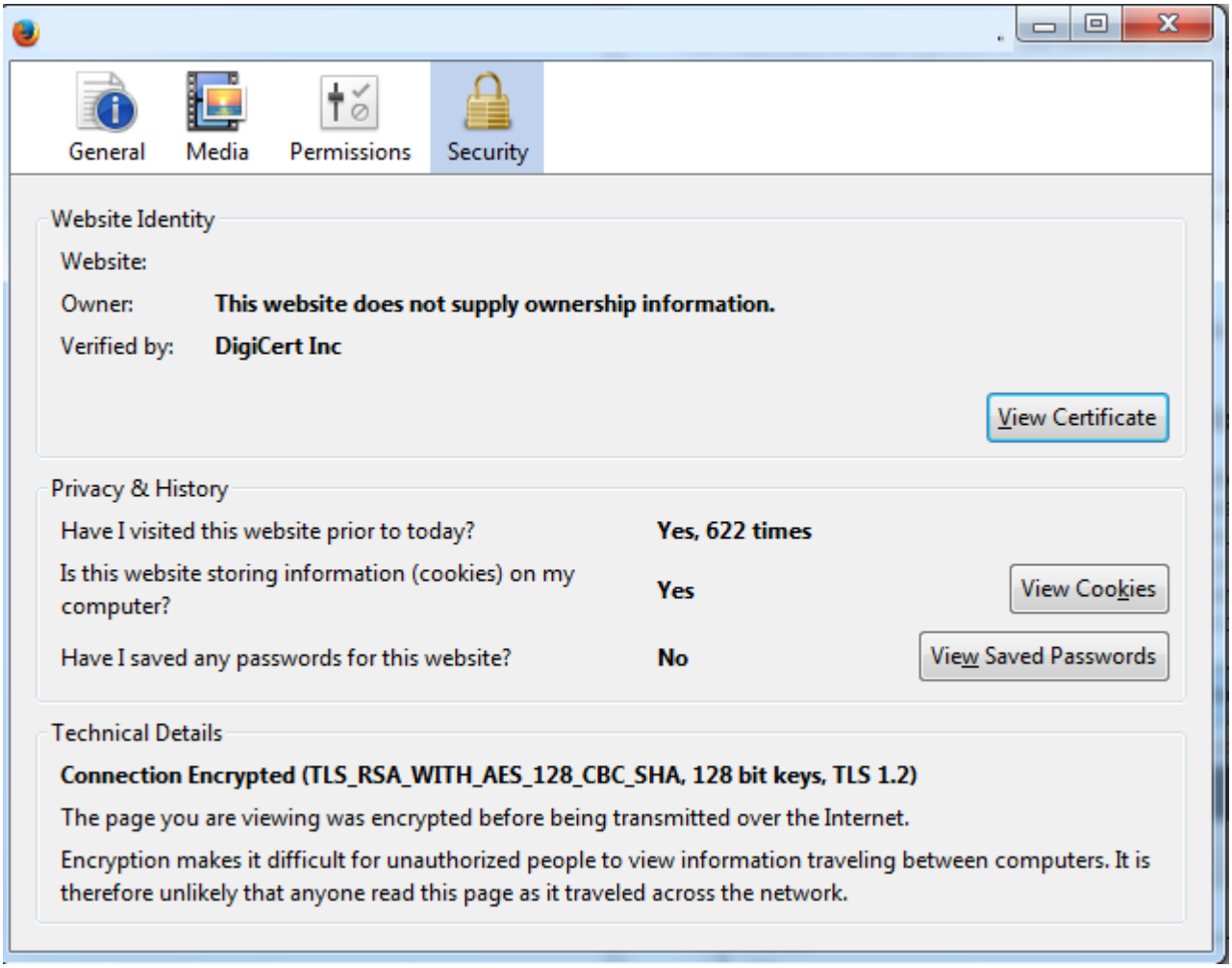
Certificado 1

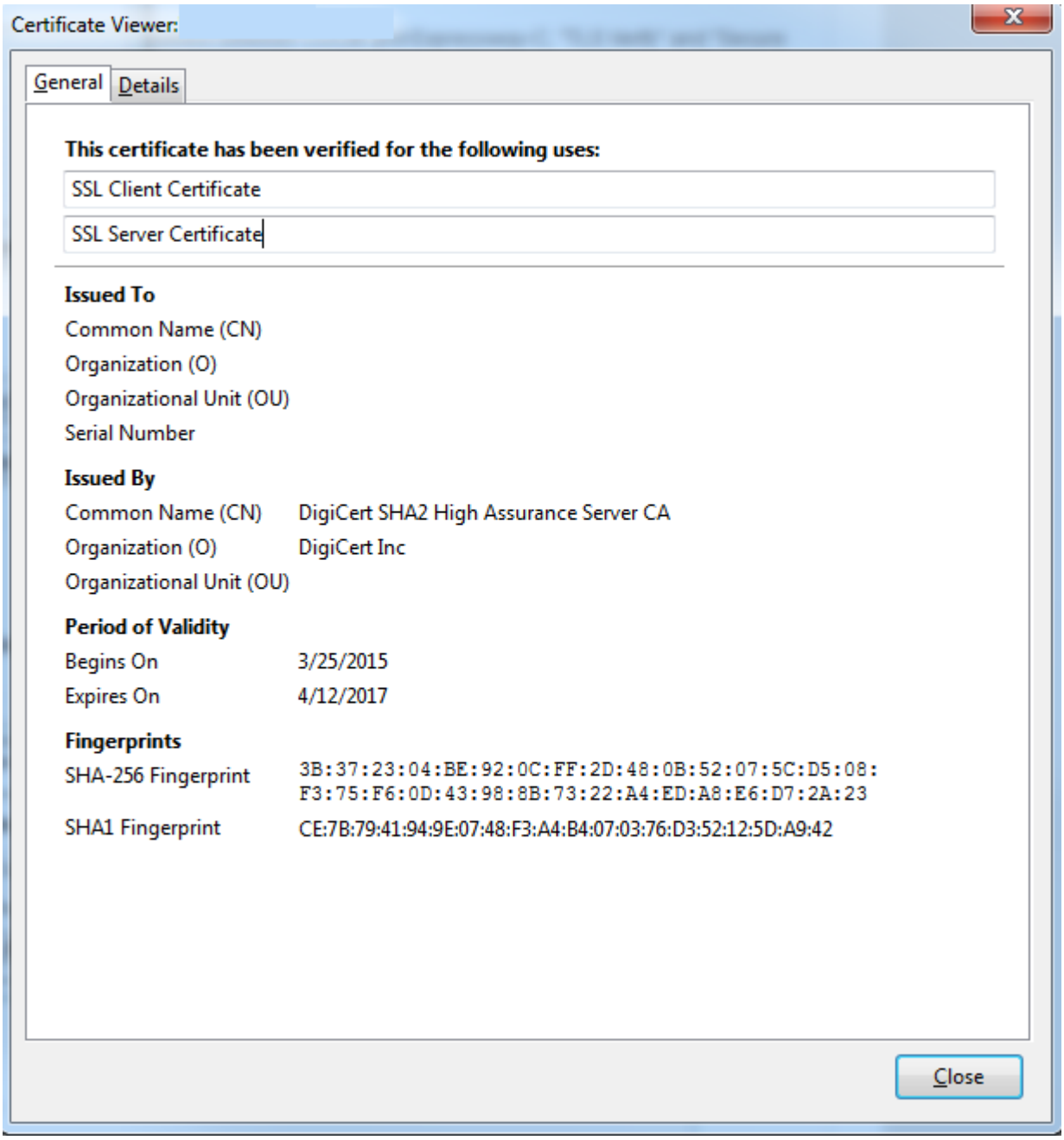
Emisor: Autoridad intermedia de GoDaddy

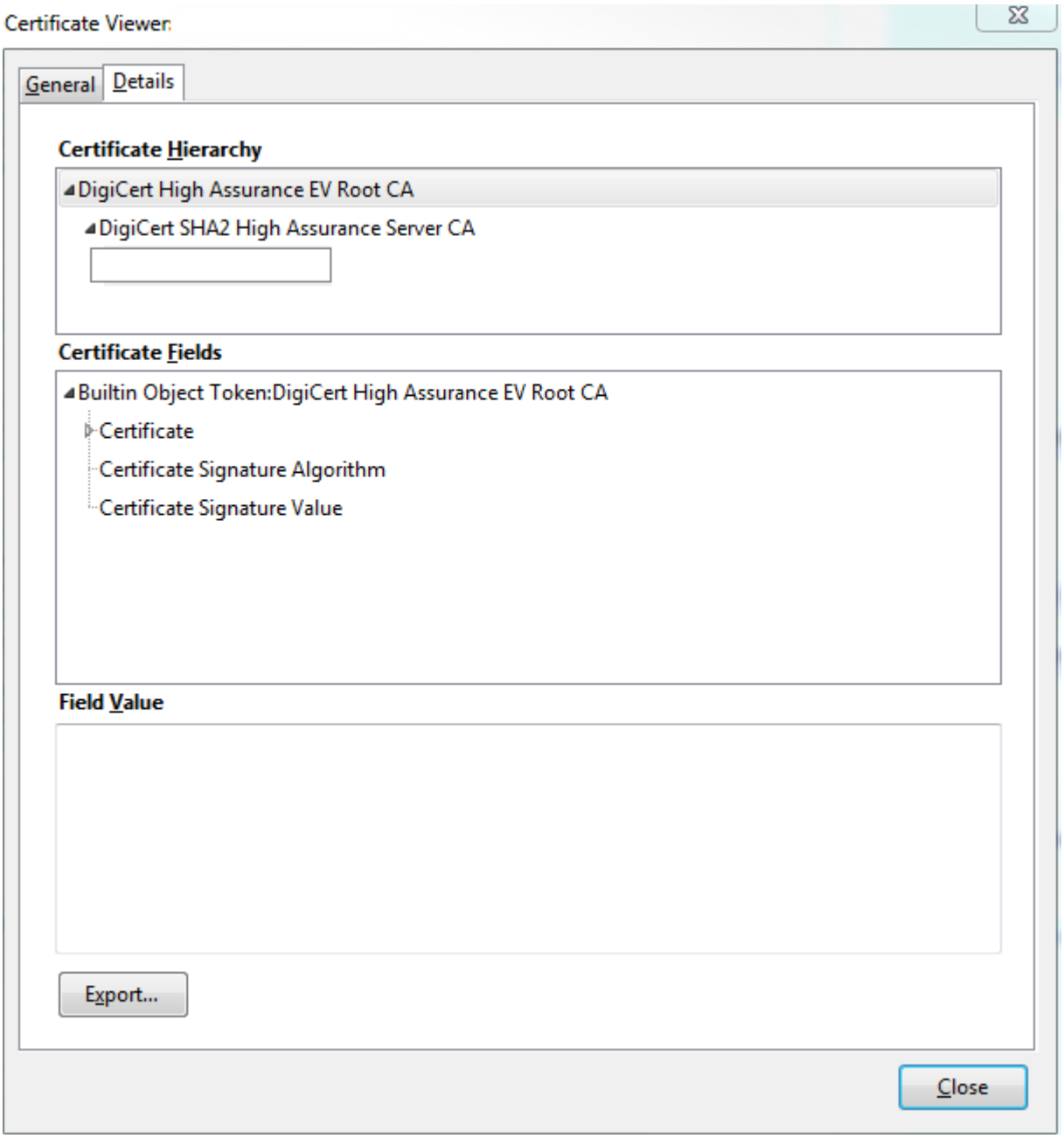
Asunto: Expressway-E.lab

Si no está seguro de cuál es la cadena de certificados, puede comprobar el explorador cuando inicie sesión en la interfaz web de Expressway específica. El proceso varía ligeramente en función de su navegador, pero en Firefox, puede hacer clic en el icono de candado en el extremo izquierdo de la barra de direcciones. A continuación, en el menú emergente, haga clic en **Más información > Ver certificado > Detalles**. Si su navegador puede unir toda la cadena, puede ver la cadena de arriba a abajo. Si el certificado de nivel superior no tiene un asunto y un emisor que coincidan, eso significa que la cadena no está completa. También puede exportar cada certificado de la cadena por sí mismo, si hace clic en **exportar** con el

certificado deseado resaltado. Esto resulta útil si no está 100 % seguro de haber cargado los certificados correctos a la lista de confianza de CA.




Certificate Viewer:
General
Details
This certificate has been verified for the following uses:
SSL Client Certificate
SSL Server Certificate
Issued To
Common Name (CN)
Organization (O)
Organizational Unit (OU)
Serial Number
Issued By
Common Name (CN) DigiCert SHA2 High Assurance Server CA
Organization (O) DigiCert Inc
Organizational Unit (OU)
Period of Validity
Begins On 3/25/2015
Expires On 4/12/2017
Fingerprints
SHA-256 Fingerprint 3B:37:23:04:BE:92:0C:FF:2D:48:0B:52:07:5C:D5:08:
F3:75:F6:0D:43:98:8B:73:22:A4:ED:A8:E6:D7:2A:23
SHA1 Fingerprint CE:7B:79:41:94:9E:07:48:F3:A4:B4:07:03:76:D3:52:12:5D:A9:42
Close



Ahora que Expressway-C confía en el certificado de Expressway-E, asegúrese de que funcione en la dirección opuesta. Si el certificado de Expressway-C está firmado por la misma CA que firmó Expressway-E, el proceso es sencillo. Cargue los mismos certificados en la lista de CA de confianza en Expressway-E que ya realizó en la C. Si la CA está firmada por una CA diferente, debe utilizar el mismo proceso que se muestra en la imagen, pero en su lugar utilice la cadena que firmó el certificado de Expressway-C.

Protección de las comunicaciones entre Cisco Unified Communications Manager (CUCM) y Expressway-C

Overview

A diferencia de la zona transversal entre Expressway-C y Expressway-E, NO se requiere señalización segura entre Expressway-C y CUCM. A menos que las políticas de seguridad internas no lo permitan, debe configurar siempre MRA para que funcione con perfiles de dispositivos no seguros en CUCM en primer lugar para confirmar que el resto de la implementación es correcta antes de continuar con este paso.

Existen dos funciones de seguridad principales que se pueden habilitar entre CUCM y Expressway-C:

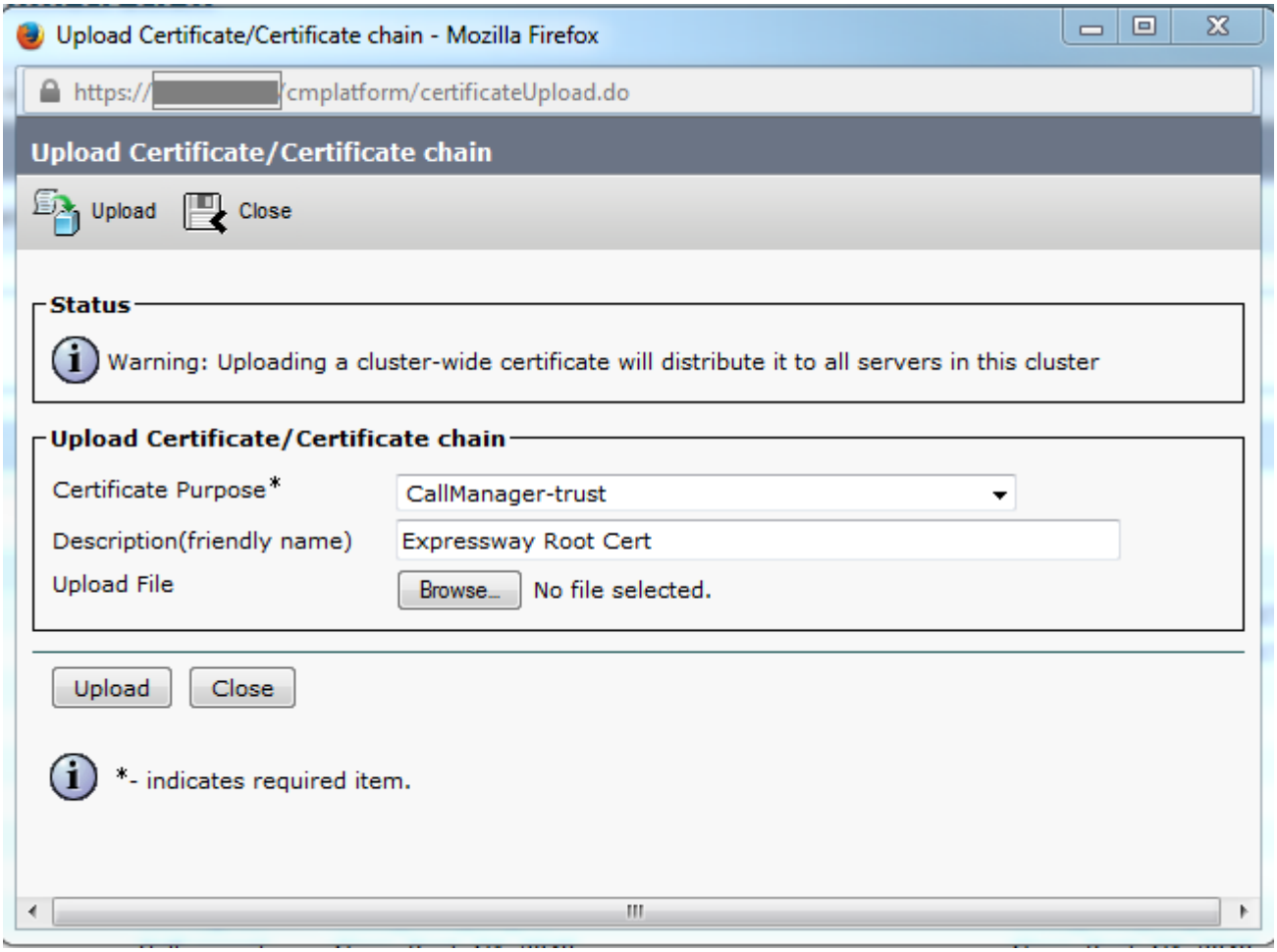
verificación de TLS y registros de dispositivos seguros. Hay una diferencia importante entre estos dos porque usan dos certificados diferentes en el lado de CUCM en el intercambio de señales de SSL.

Comprobación de TLS: certificado Tomcat

Registros seguros en SIP: certificado de CallManager

Configuración de la confianza entre CUCM y Expressway-C

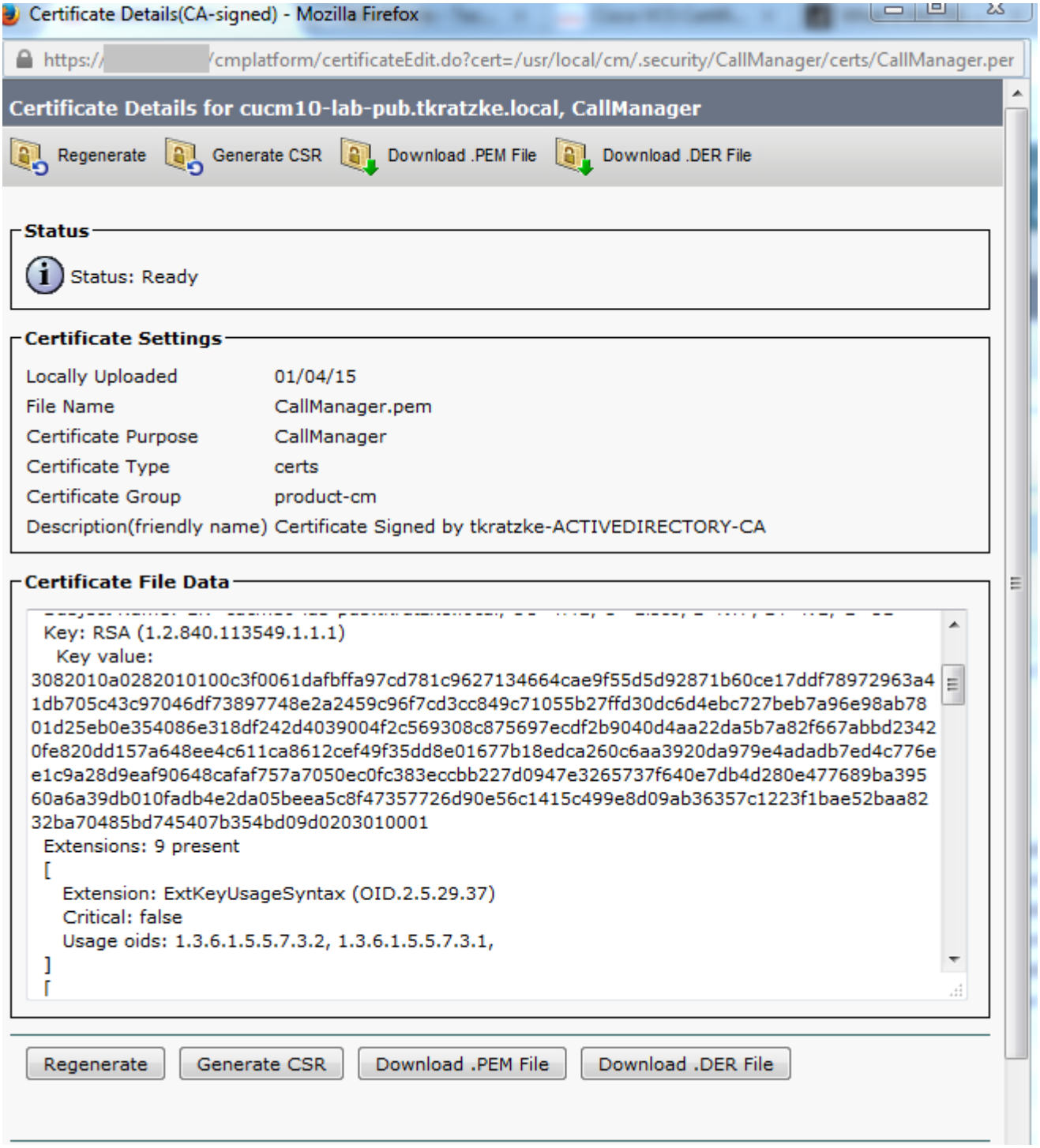
El concepto, en este caso, es exactamente el mismo que entre Expressway-C y Expressway-E. CUCM en primer lugar debe confiar en el certificado del servidor de Expressway-C. Esto significa que en CUCM, los certificados intermedios y raíz de Expressway-C deben cargarse como un certificado de confianza de Tomcat para la función de verificación de TLS y un certificado de confianza de CallManager para los registros de dispositivos seguros. Para lograrlo, navegue hasta **Cisco Unified OS Administration** en la parte superior derecha de la GUI web de CUCM y, a continuación, **Security**> **Certificate Management**. Aquí puede hacer clic en **Cargar certificado/cadena de certificado y seleccionar el formato correcto de confianza o hacer clic en Buscar para ver la lista de certificados cargados actualmente.**



Debe asegurarse de que Expressway-C confía en la CA que firmó los certificados de CUCM. Esto se puede lograr si los agrega a la lista de CA de confianza. En casi todos los casos, si firmó los certificados de CUCM con una CA, los certificados de Tomcat y CallManager deben estar firmados por la misma CA. Si son diferentes, debe confiar en ambos si utiliza la verificación de TLS y los registros seguros.

Para los registros SIP seguros, también debe asegurarse de que el nombre de perfil de dispositivo seguro en CUCM que se aplica al dispositivo aparezca como una SAN en el certificado de Expressway-C. Si esto no contiene los mensajes de registro seguro, fallaría con un 403 de CUCM, que indica una falla de TLS.

Nota: cuando se produce el protocolo de enlace SSL entre CUCM y Expressway-C para un registro SIP seguro, se producen dos protocolos de enlace. En primer lugar, Expressway-C actúa como cliente e inicia la conexión con CUCM. Una vez que se haya completado correctamente, CUCM inicia otro intercambio de señales como cliente para responder. Esto significa que, al igual que Expressway-C, en el certificado de CallManager en CUCM se deben aplicar los atributos de autenticación de cliente web de TLS y de servidor web de TLS. La diferencia es que CUCM permite que estos certificados se carguen sin ambos, y los registros seguros internos funcionarían bien si CUCM solo tiene el atributo de autenticación del servidor. Puede confirmar esto en CUCM si busca el certificado de CallManager en la lista y lo selecciona. Allí, puede ver los oids de uso en la sección Extension (Extensión). Puede ver 1.3.6.1.5.5.7.3.2 para la autenticación del cliente y 1.3.6.1.5.5.7.3.1 para la autenticación del servidor. También puede descargar el certificado en esta ventana.



Nota: los certificados de confianza aplicados al editor de un clúster deben replicarse en los suscriptores. Es bueno confirmar iniciando sesión en ellos por separado en una nueva configuración.

Nota: para que Expressway-C valide correctamente el certificado de CUCM, los servidores de CUCM DEBEN agregarse en Expressway-C con el FQDN, no la dirección IP. La única forma de que la dirección IP funcione es si la IP de cada nodo de CUCM se agrega como una SAN en el certificado, lo que casi nunca se hace.

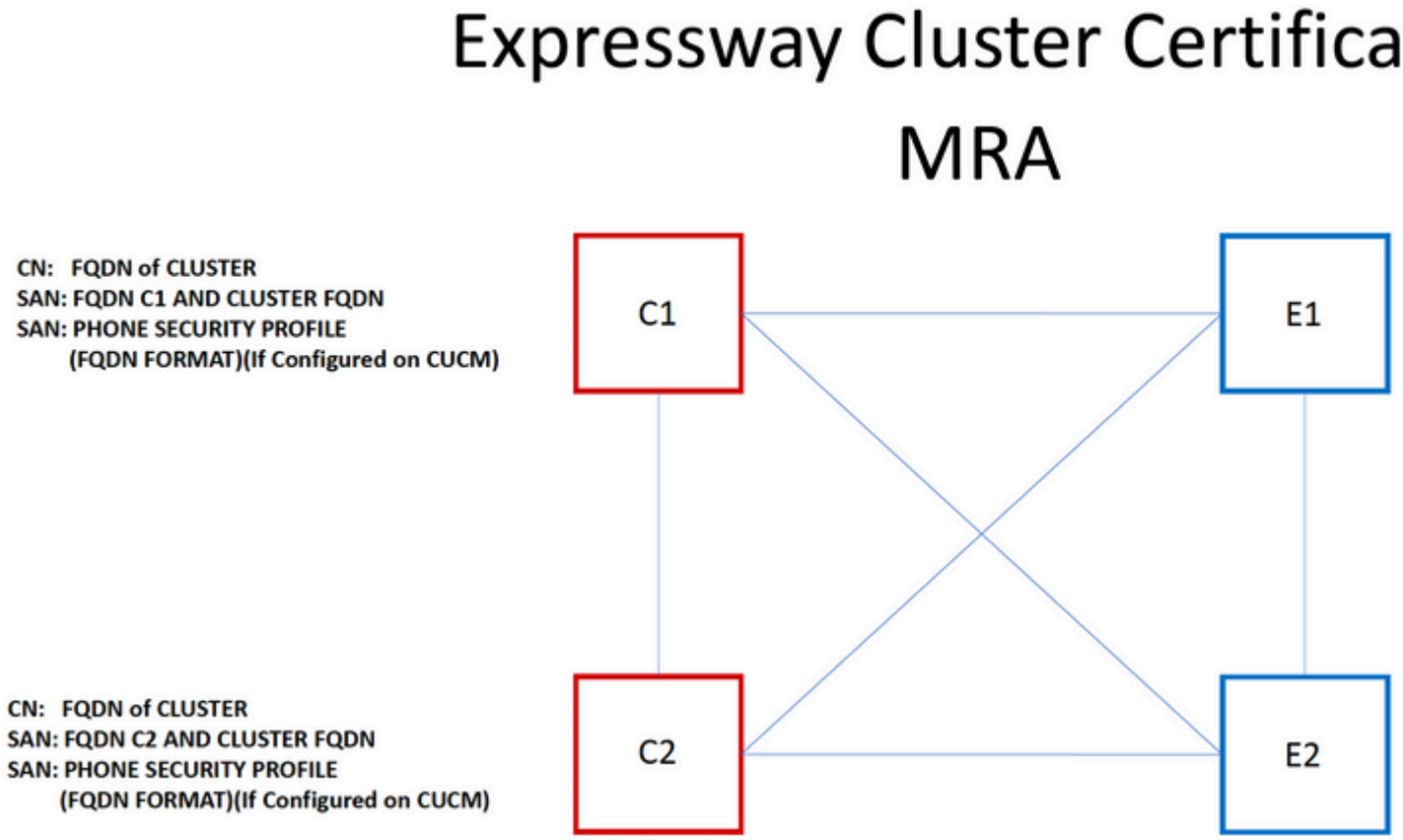
Servidores de CUCM con certificados autofirmados

De forma predeterminada, un servidor de CUCM incluye certificados autofirmados. Si están en su lugar, no es posible utilizar la verificación de TLS y los registros de dispositivos seguros al mismo tiempo. Cualquiera de las funciones se puede utilizar por sí sola, pero como los certificados son autofirmados, significa que tanto los certificados Tomcat autofirmados como los certificados CallManager autofirmados deben cargarse en la lista de CA de confianza en Expressway-C. Cuando Expressway-C busca en su lista de confianza para validar un certificado, se detiene una vez que encuentra uno con un asunto que coincide. Debido a esto, cualquiera que sea el valor más alto en la lista de confianza, tomcat o CallManager, esa función funcionaría. La inferior fallaría como si no estuviera presente. La solución a esto es firmar los certificados de CUCM con una CA (pública o privada) y confiar solo en esa CA.

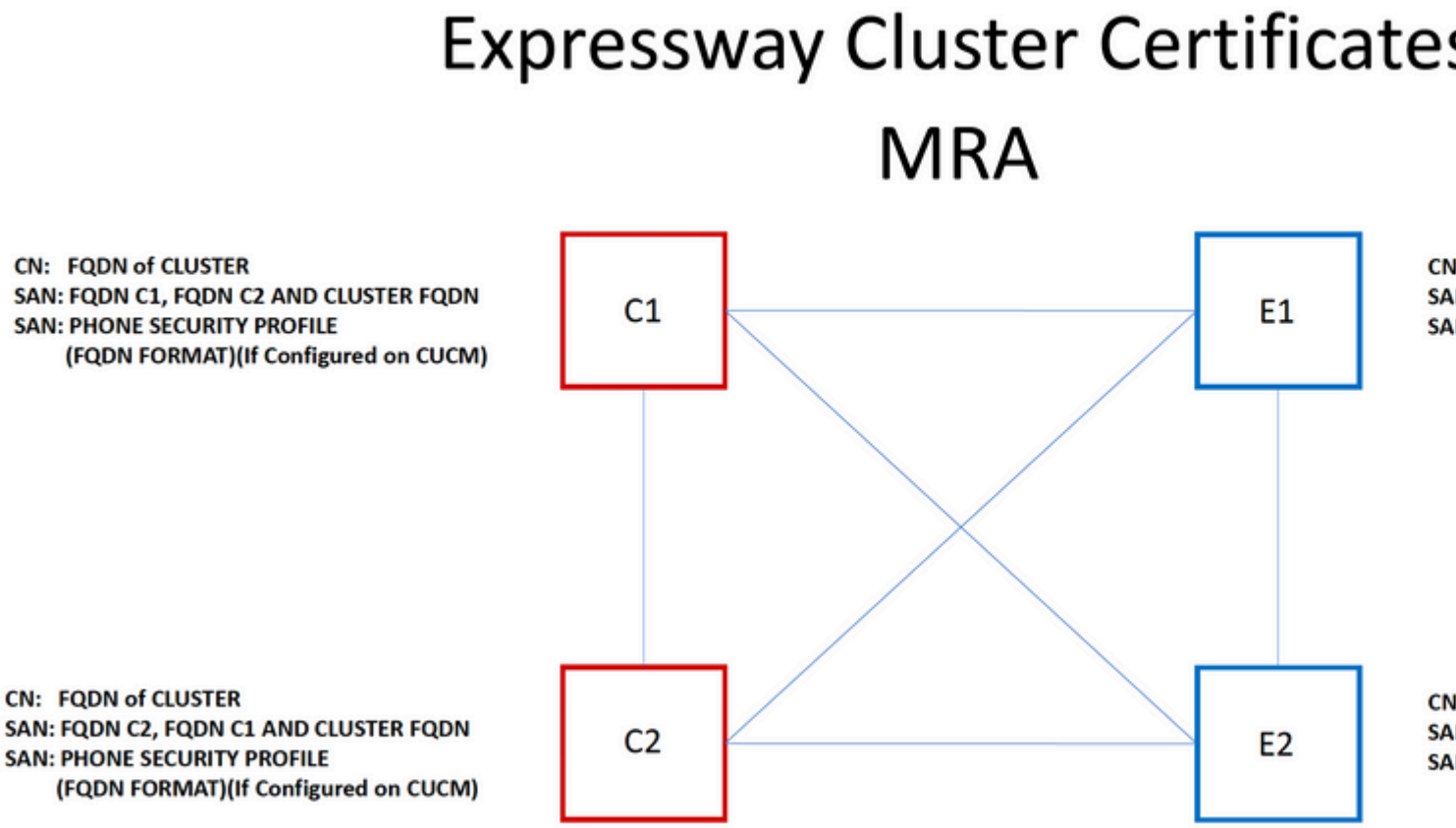
Consideraciones sobre clústeres de Expressway-C y Expressway-E

Certificados de clúster

Se recomienda encarecidamente que, si dispone de un clúster de servidores Expressway-C o Expressway-E para obtener redundancia, genere una CSR independiente para cada servidor y que la haga firmar por una CA. En el escenario anterior, el nombre común (CN) de cada certificado de pares sería el mismo nombre de dominio completamente calificado (FQDN) del clúster y las SAN serían el FQDN del clúster y el FQDN de los pares respectivos, como se muestra en la imagen:



Es posible utilizar el FQDN del clúster como CN y cada FQDN del mismo nivel y el FQDN del clúster en la SAN para utilizar el mismo certificado para todos los nodos del clúster y, por lo tanto, evitar el coste de varios certificados firmados por una CA pública.



> **Nota**: Los nombres de los perfiles de seguridad del teléfono del certificado Cs solo son necesarios si utiliza perfiles de seguridad del teléfono seguro en UCM. El dominio externo o collab-edge.example.com (donde example.com es su dominio) es un requisito solo para el registro de teléfonos IP y terminales TC a través de MRA. Esta opción es opcional para el registro de Jabber a través de MRA. Si no está presente, Jabber le pedirá que acepte el certificado cuando inicie sesión sobre MRA.

Si es absolutamente necesario, esto se puede hacer con el siguiente proceso o puede utilizar OpenSSL para generar la clave privada y CSR manualmente:

Paso 1. Genere un CSR en el principal del clúster y configúrelo para que incluya el alias del clúster como CN. Agregue todos los pares del clúster como nombres alternativos, junto con todas las demás SAN necesarias.

Paso 2. Firme este CSR y cárguelo en el par principal.

Paso 3. Inicie sesión en la clave primaria como root y descargue la clave privada ubicada en /Tandberg/persistent/certs.

Paso 4. Cargue el certificado firmado y la clave privada coincidente entre los pares del clúster.

> **Nota**: no se recomienda por los siguientes motivos:
> 1. Es un riesgo de seguridad porque todos los pares utilizan la misma clave privada. Si uno de ellos se ve comprometido de alguna manera, un atacante puede descifrar el tráfico de cualquiera de los servidores.

---

2. Si necesita hacer un cambio en el certificado, se debe seguir todo este proceso de nuevo en vez de hacer una simple generación y firma de CSR.

Listas de autoridades de certificación de confianza

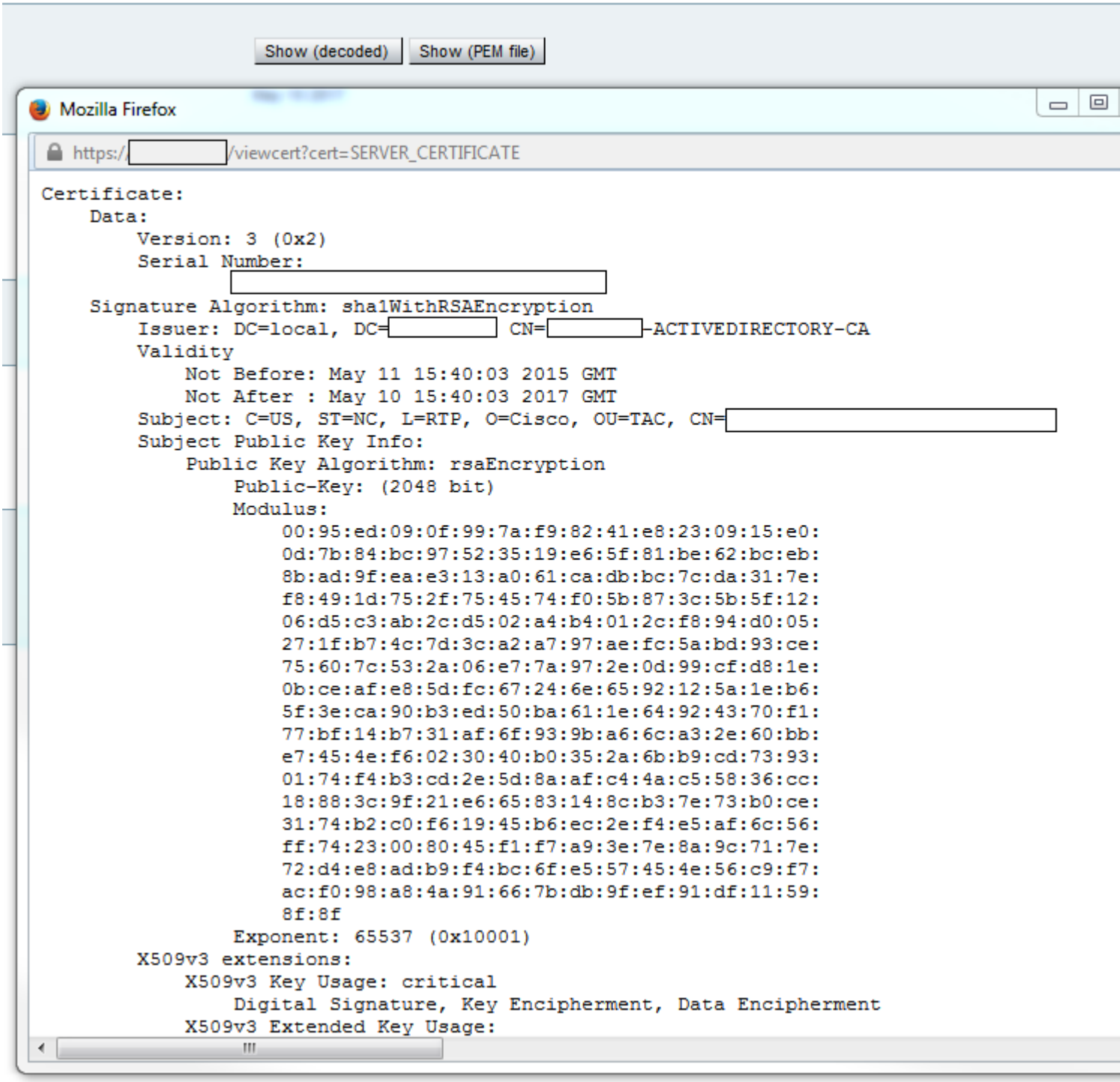
A diferencia de los suscriptores de CUCM en un clúster, la lista de autoridades de certificación de confianza NO se replica de un par a otro en un clúster de VCS o Expressway. Esto significa que si tiene un clúster, debe cargar manualmente certificados de confianza en la lista de CA de cada par.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Comprobar la información del certificado actual

Hay varias maneras de comprobar la información de un certificado existente. La primera opción es a través del navegador web. Utilice el método descrito en la sección anterior, que también se puede utilizar para exportar un certificado específico de la cadena. Si necesita verificar las SAN u otros atributos agregados al certificado de servidor de Expressway, puede hacerlo directamente a través de la interfaz gráfica de usuario (GUI) web, navegue hasta **Mantenimiento > Certificados de seguridad > Certificado de servidor**, luego haga clic en **Mostrar decodificado**.

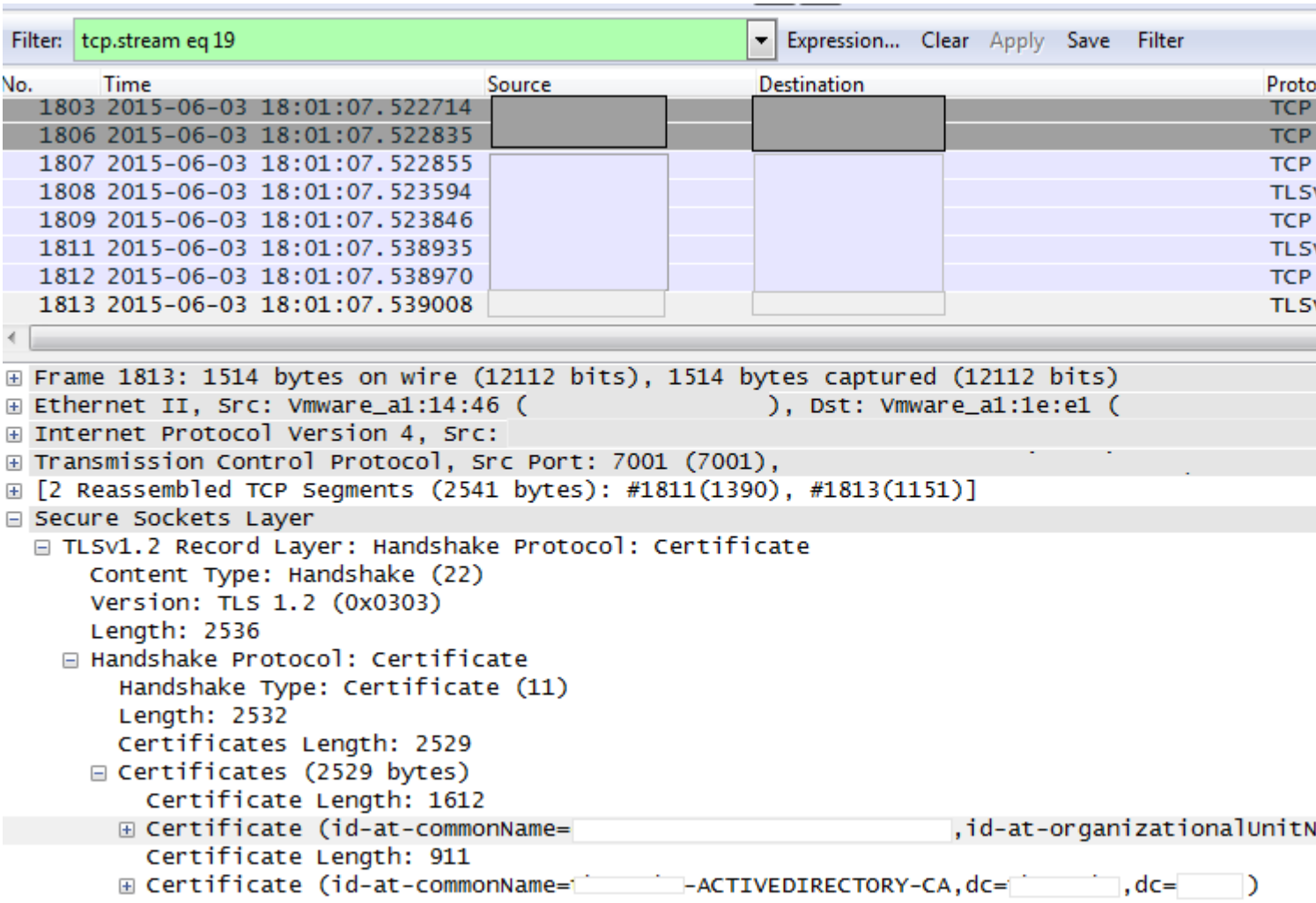


Aquí puede ver todos los detalles específicos del certificado sin necesidad de descargarlo. También puede hacer lo mismo para una CSR activa si aún no se ha cargado el certificado firmado asociado.

Leer/Exportar un certificado en Wireshark

Si tiene una captura Wireshark del intercambio de señales SSL que incluye el intercambio de certificados, Wireshark puede descodificar el certificado por usted y puede exportar cualquier certificado de la cadena (si se intercambia la cadena completa) desde dentro. Puede filtrar la captura de paquetes para el puerto específico del intercambio de certificados (generalmente 7001 en el caso de la zona transversal). A continuación, si no ve los paquetes hello del cliente y el servidor junto con el protocolo de enlace SSL, haga clic con el botón derecho en uno de los paquetes del flujo TCP y seleccione **decode as**. Aquí, seleccione

SSL y haga clic en **apply**. Ahora, si ha capturado el tráfico correcto, debe ver el intercambio de certificados. Busque el paquete del servidor correcto que contiene el certificado en la carga útil. Expanda la sección SSL en el panel inferior hasta que vea la lista de certificados como se muestra en la imagen:



Aquí puede expandir cualquiera de los certificados para ver todos los detalles. Si desea exportar el certificado, haga clic con el botón derecho en el certificado deseado de la cadena (si hay varios) y seleccione **Exportar bytes de paquete seleccionados**. Introduzca un nombre para el certificado y haga clic en **guardar**. Ahora, debe poder abrir el certificado en el Visor de certificados de Windows (si le ha asignado una extensión .cer) o cargarlo en cualquier otra herramienta para su análisis.

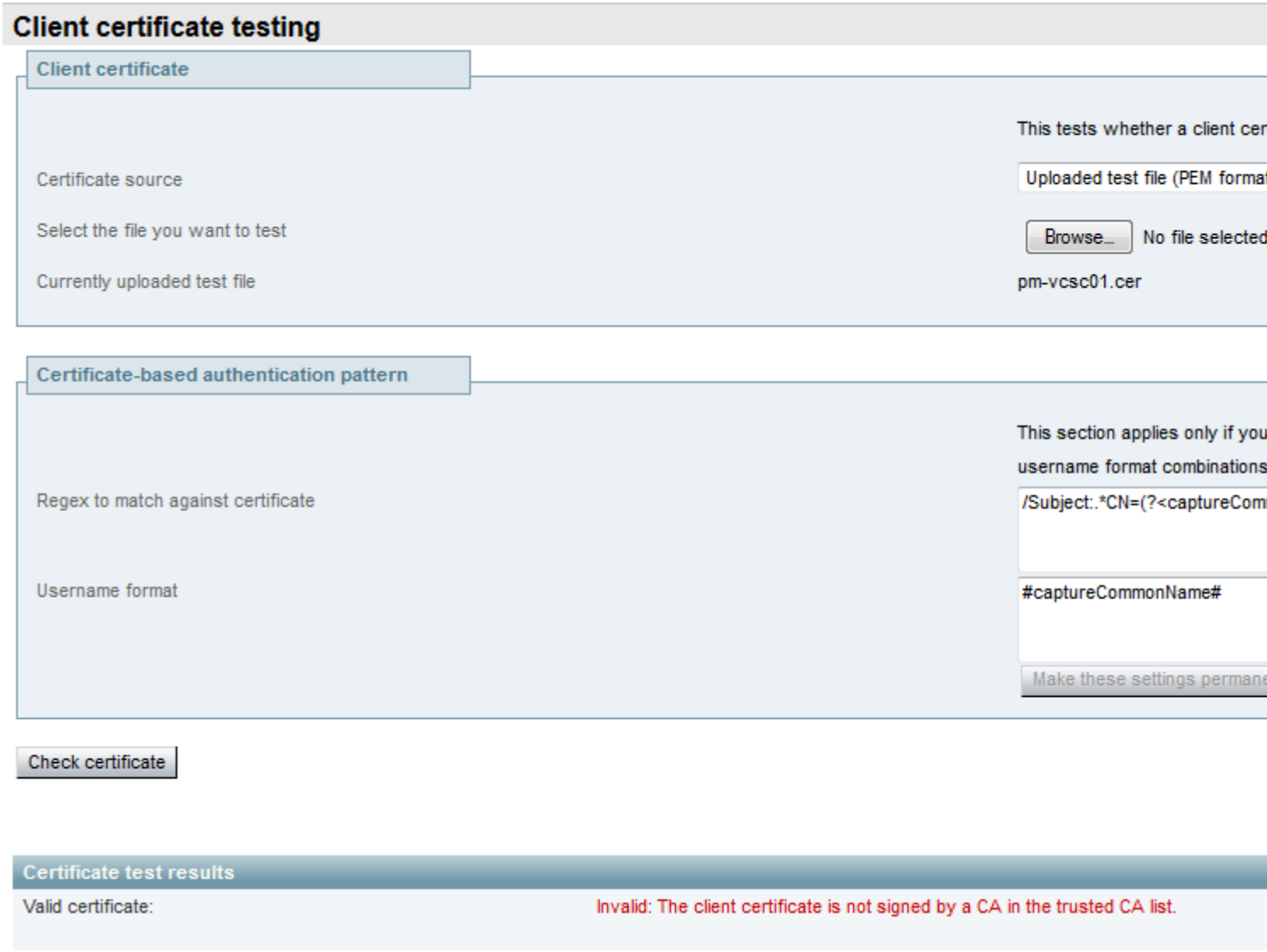
Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

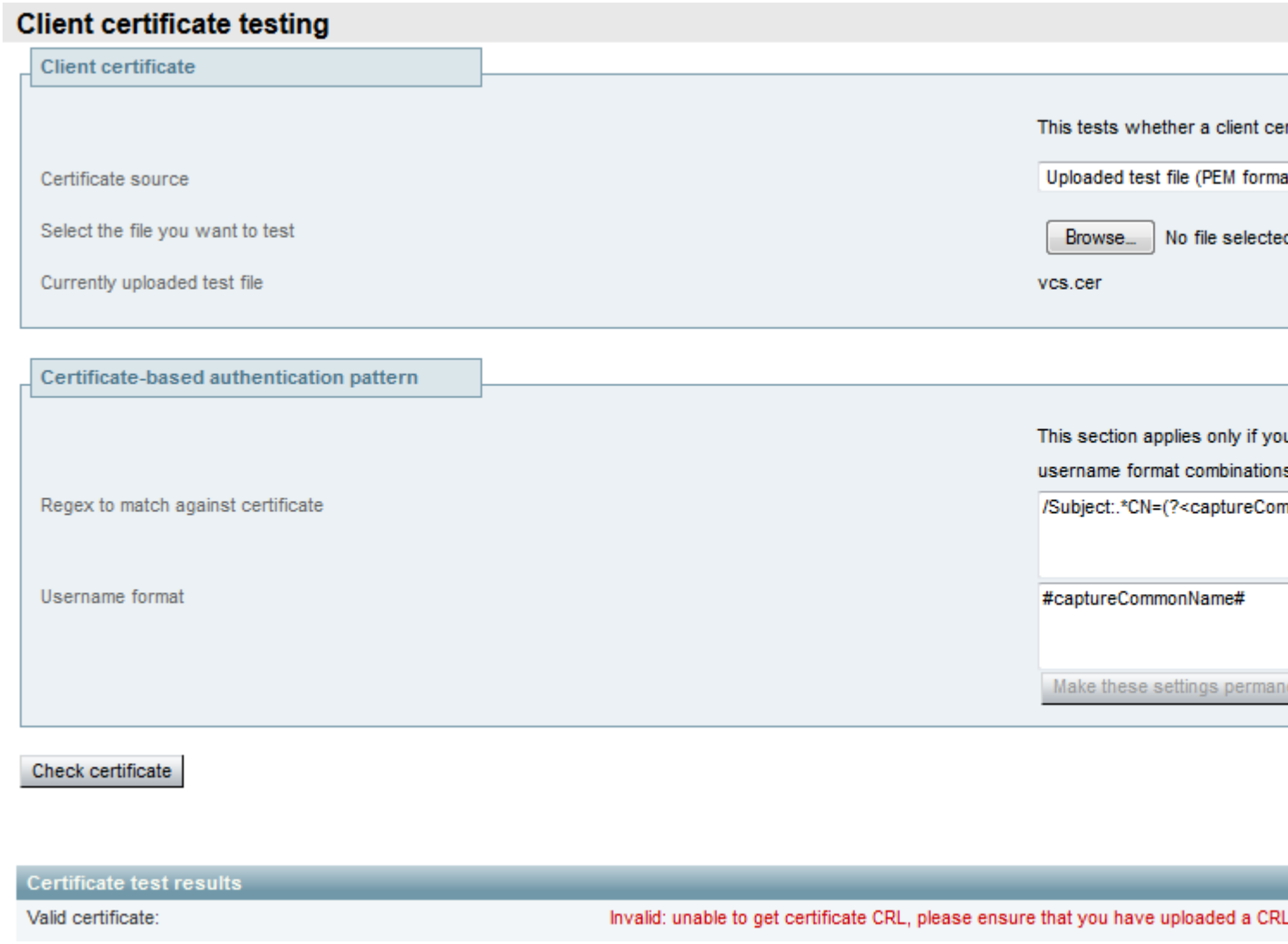
Pruebe para saber si un certificado es de confianza en Expressway

Aunque el mejor método es comprobar manualmente la cadena de certificados y asegurarse de que todos los miembros estén incluidos en la lista de CA de confianza de Expressway, puede comprobar rápidamente que Expressway confía en un certificado de cliente específico con la ayuda de la **prueba de certificados de cliente** en **Mantenimiento** > Certificados de seguridad en la GUI web. Mantenga la misma configuración predeterminada. Seleccione **Cargar archivo de prueba** (formato pem) en el menú desplegable y seleccione el certificado de cliente que desea verificar. Si el certificado no es de confianza, obtendrá un error, como se muestra en la imagen, que explica la razón por la que se rechazó. El error que ve es la información

descodificada del certificado cargado como referencia.



Si obtiene un error que indica que Expressway no puede obtener la CRL del certificado, pero Expressway no usa la comprobación de CRL, esto significa que el certificado sería de confianza y ha pasado todas las demás comprobaciones.



Terminales de Synergy Light (teléfonos de las series 7800 y 8800)

Estos nuevos dispositivos incluyen una lista de certificados de confianza rellenada previamente, que incluye un gran número de CA públicas conocidas. Esta lista de confianza no se puede modificar, lo que significa que el certificado de Expressway-E DEBE estar firmado por una de estas CA públicas coincidentes para funcionar con estos dispositivos. Si está firmado por una CA interna o una CA pública diferente, la conexión fallaría. No hay ninguna opción para que el usuario pueda aceptar manualmente el certificado como con los clientes de Jabber.

Nota: en algunas implementaciones se ha observado que el uso de un dispositivo como Citrix NetScaler con una CA de la lista incluida en los teléfonos de las series 7800/8800 puede registrarse a través de MRA incluso si Expressway-E usa una CA interna. La CA raíz de NetScalers debe cargarse en Expressway-E y la CA raíz interna debe cargarse en Netscaler para que funcione la autenticación SSL. Se ha demostrado que esto funciona y que es el mejor apoyo posible.

Nota: si la lista de CA de confianza parece tener todos los certificados correctos en, pero aún así se rechaza, asegúrese de que no haya otro certificado superior en la lista con el mismo asunto que pueda entrar en conflicto con el correcto. Cuando todo lo demás falla, siempre puede exportar la cadena directamente desde el navegador o Wireshark y cargar todos los certificados en la lista de CA de

---

servidores opuestos. Esto garantizaría que sea el certificado de confianza.

Nota: Cuando resuelve un problema de zona transversal, a veces el problema puede parecer estar relacionado con un certificado, pero en realidad es algo del lado del software. Asegúrese de usar el nombre de usuario y la contraseña correctos de la cuenta que se utiliza para la zona transversal.

Nota: VCS o Expressway no admite más de 999 caracteres en el campo SAN de un certificado. Cualquier SAN que supere este límite (que requiere muchos nombres alternativos) se ignorará como si no estuviera allí.

Recursos de video

Esta sección proporciona información en el video que puede guiarle a través de todos los procesos de configuración de certificados.

Generar una CSR para MRA o Clustered Expressways

Instalar certificado de servidor en Expressway

Cómo configurar la confianza de certificados entre Expressways

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).