Solucionar problemas de certificados de Expressway

Contenido

Introducción

Este documento describe cómo funcionan los certificados y los problemas y sugerencias más comunes para los certificados en los servidores de Expressway.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servidores de Expressway y Video Communications Server (VCS)
- Capa de sockets seguros (SSL)
- Certificados
- Dispositivos de Telepresence
- Acceso móvil y remoto
- Implementaciones de colaboración

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Expressway x14

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

SSL y los certificados son un estándar y funcionan igual en otros dispositivos y marcas. Este documento se centra en los usos de certificados en Expressways.

Definiciones

Los certificados se utilizan para crear una conexión segura entre dos dispositivos. Se trata de una firma digital que autentica la identidad de un servidor o dispositivo. Algunos protocolos como Protocolo de transferencia de hipertexto seguro (HTTPS) o Protocolo de inicio de sesión (SIP) y Seguridad de la capa de transporte (TLS) requieren el uso de certificados para funcionar.

Distintos términos utilizados cuando se habla de certificados:

- Solicitud de firma de certificado (CSR): plantilla creada con los nombres que identifican un dispositivo para que se firme posteriormente y se convierta en un certificado de cliente o de servidor
- Certificado: CSR que se ha firmado. Se trata de un tipo de identidad que se instala en un dispositivo para su uso en negociaciones SSL. Pueden estar firmadas por sí mismas o por una autoridad de certificación.
- Firma del certificado: Identidad que verifica que el certificado en cuestión es legítimo; se presenta en forma de otro certificado.
- Certificado autofirmado: un certificado de cliente o servidor firmado por sí mismo
- Autoridad de certificación (CA): entidad que firma certificados
    - Certificado intermedio: certificado de CA que no está firmado por sí mismo sino por otro certificado de CA, normalmente firmado por un certificado raíz pero que también puede estar firmado por otro certificado intermedio
    - Certificado raíz: certificado de CA firmado por sí mismo

Principio básico

Cuando un cliente habla con un servidor e inicia una conversación SSL, intercambia certificados, que se utilizan posteriormente para cifrar el tráfico entre los dispositivos. Como parte del intercambio, los dispositivos también determinan si los certificados son de confianza. Se deben cumplir varias condiciones para determinar si un certificado es de confianza, algunas son:

- El nombre de dominio completo (FQDN) utilizado inicialmente para ponerse en contacto con el servidor coincide con un nombre dentro del certificado presentado por el servidor.

    - Por ejemplo, al abrir una página Web en un explorador, cisco.com resuelve la dirección IP de un servidor que proporciona un certificado, que debe incluir cisco.com como nombre para que se pueda confiar en él.

- El certificado de CA que firmó el certificado de servidor presentado por el servidor (o el mismo certificado de servidor cuando se firmó automáticamente) está presente en la lista de certificados de confianza de CA del dispositivo.
    - Los dispositivos tienen una lista de certificados de CA de confianza; los equipos suelen incluir una lista predefinida con entidades emisoras de certificados públicas conocidas.

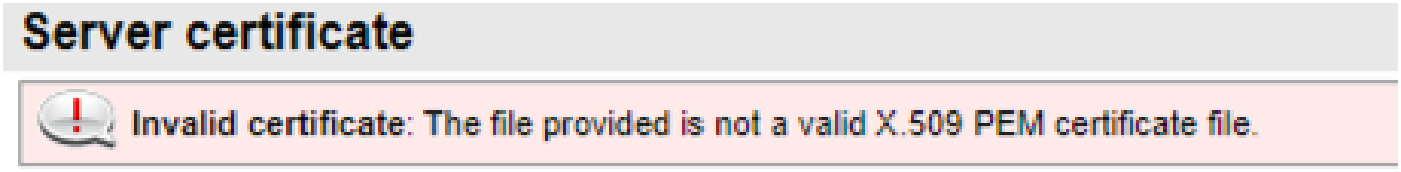
- La fecha y hora actuales se encuentran dentro del período de validez del certificado.
    - Las autoridades de certificados solo firman CSR durante un período de tiempo establecido, que determina la CA.

- El certificado no está revocado.
    - Las autoridades de certificados públicos suelen incluir una dirección URL de lista de revocación de certificados dentro del certificado. Esto es para que la parte que recibe el certificado pueda confirmar que no ha sido revocado por la CA.

Problemas comunes

Error al cargar el certificado de Expressway

Hay un par de condiciones que pueden causar esto. Causan un error descriptivo diferente.



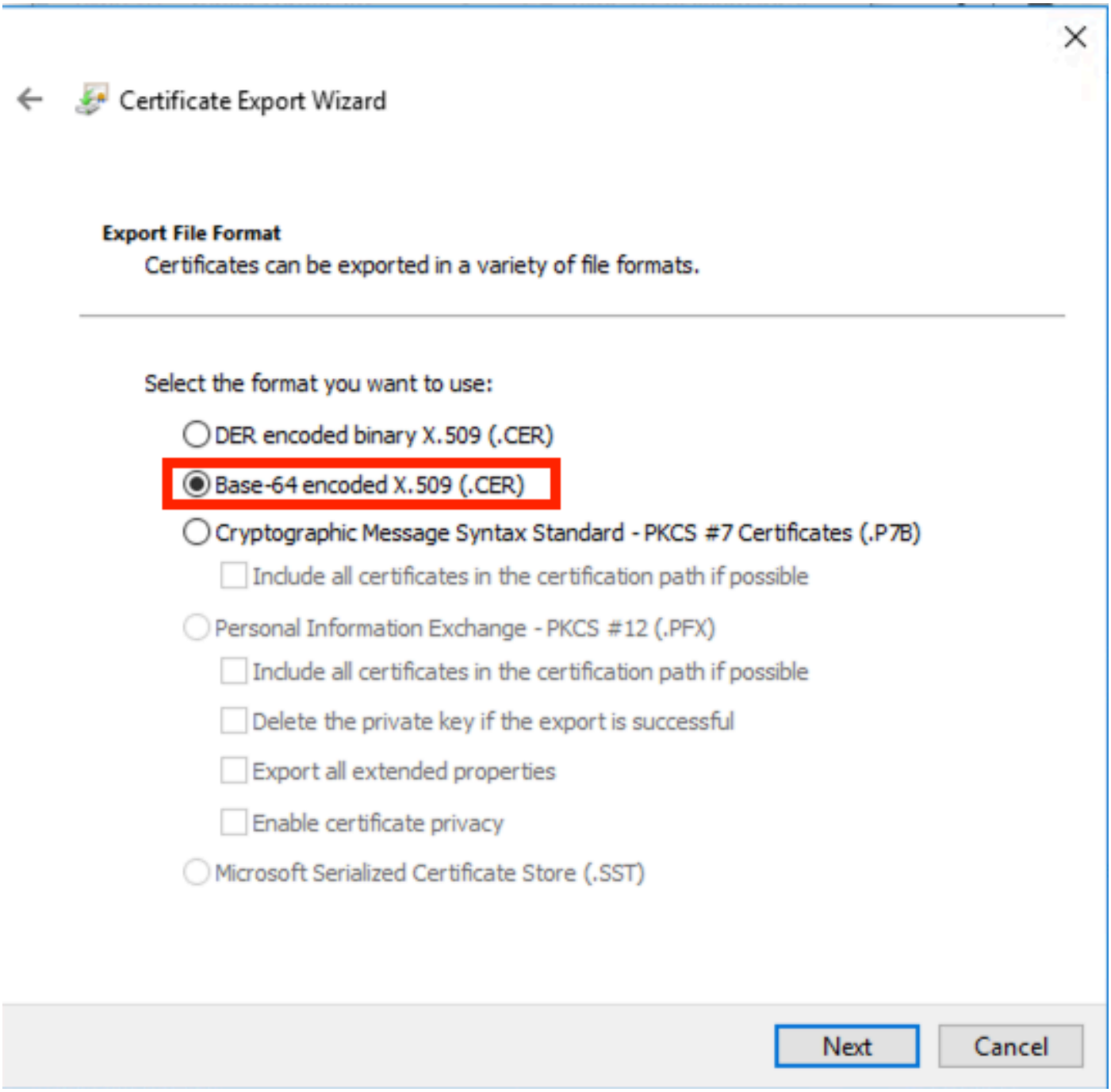
Formato de certificado no válido

Este primer error se produce cuando el certificado no tiene un formato válido. La extensión del archivo no importa.

Si el certificado no se abre, se puede solicitar uno nuevo a la CA en el formato correcto

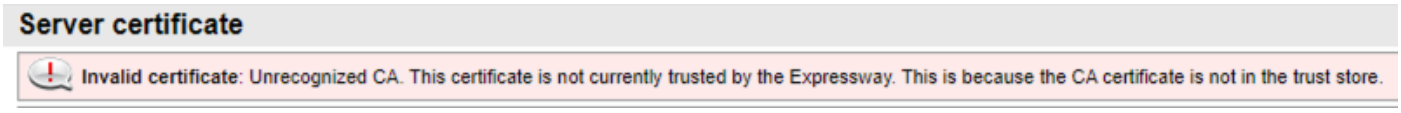
Si el certificado se abre, siga estos pasos:

Paso 1. Abra el certificado y vaya a la pestaña Detalles.
Paso 2. Seleccione Copiar en archivo.
Paso 3. Siga el asistente y asegúrese de que la opción Codificado en base 64 esté seleccionada.



Selección de formato de certificado

Paso 4. Una vez guardado, cargue el nuevo archivo en Expressway.



Cadena de certificados de CA no fiable

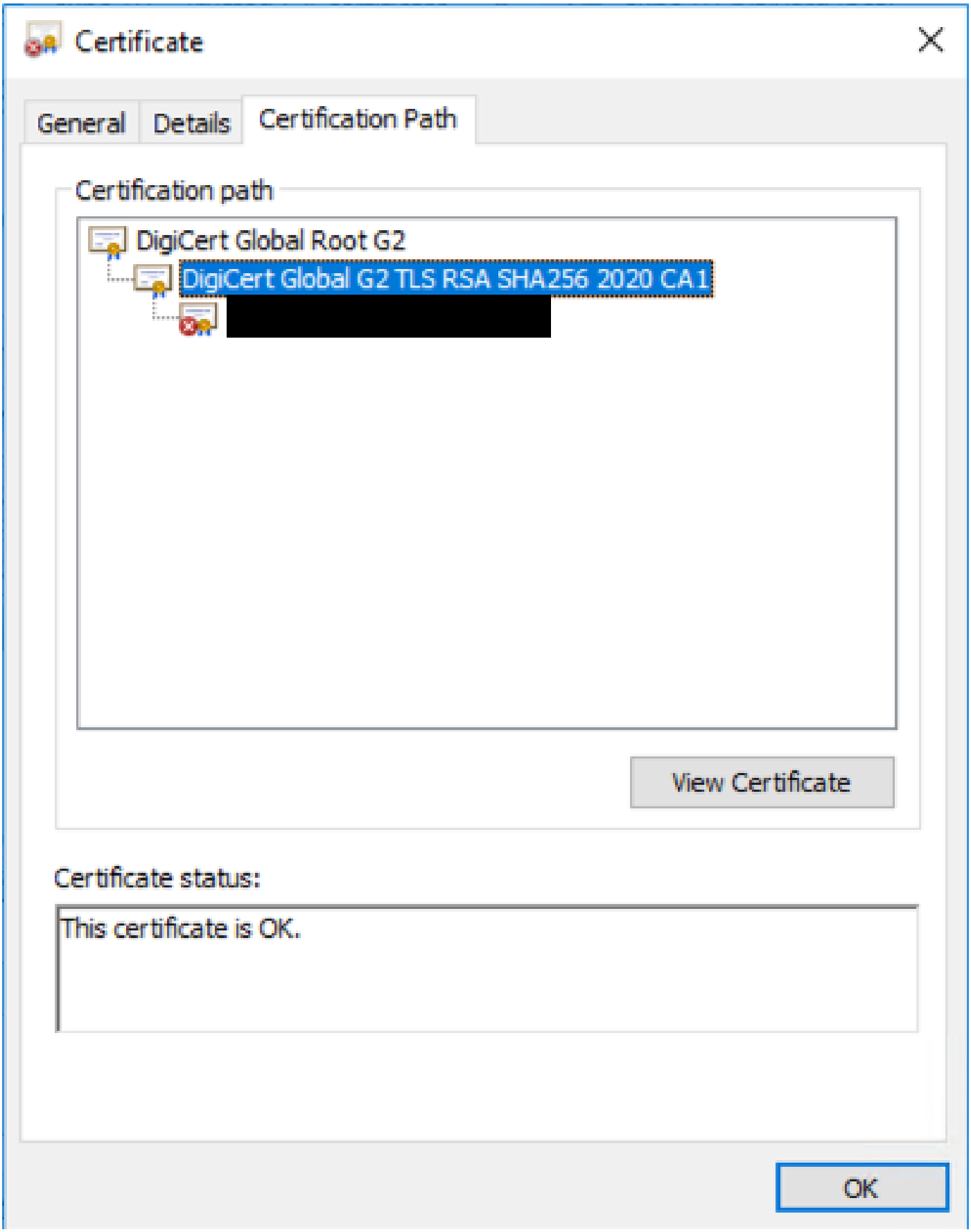
Este error se produce cuando los certificados de CA que firmaron el certificado de servidor no son de confianza. Antes de cargar un certificado de servidor, el servidor debe confiar en todos los certificados de CA de la cadena.

Normalmente, la CA proporciona los certificados de CA junto con el certificado de servidor

firmado. Si están disponibles, vaya directamente al paso 6.

Si los certificados de la CA no están disponibles, se pueden obtener del certificado del servidor. Siga estos pasos:

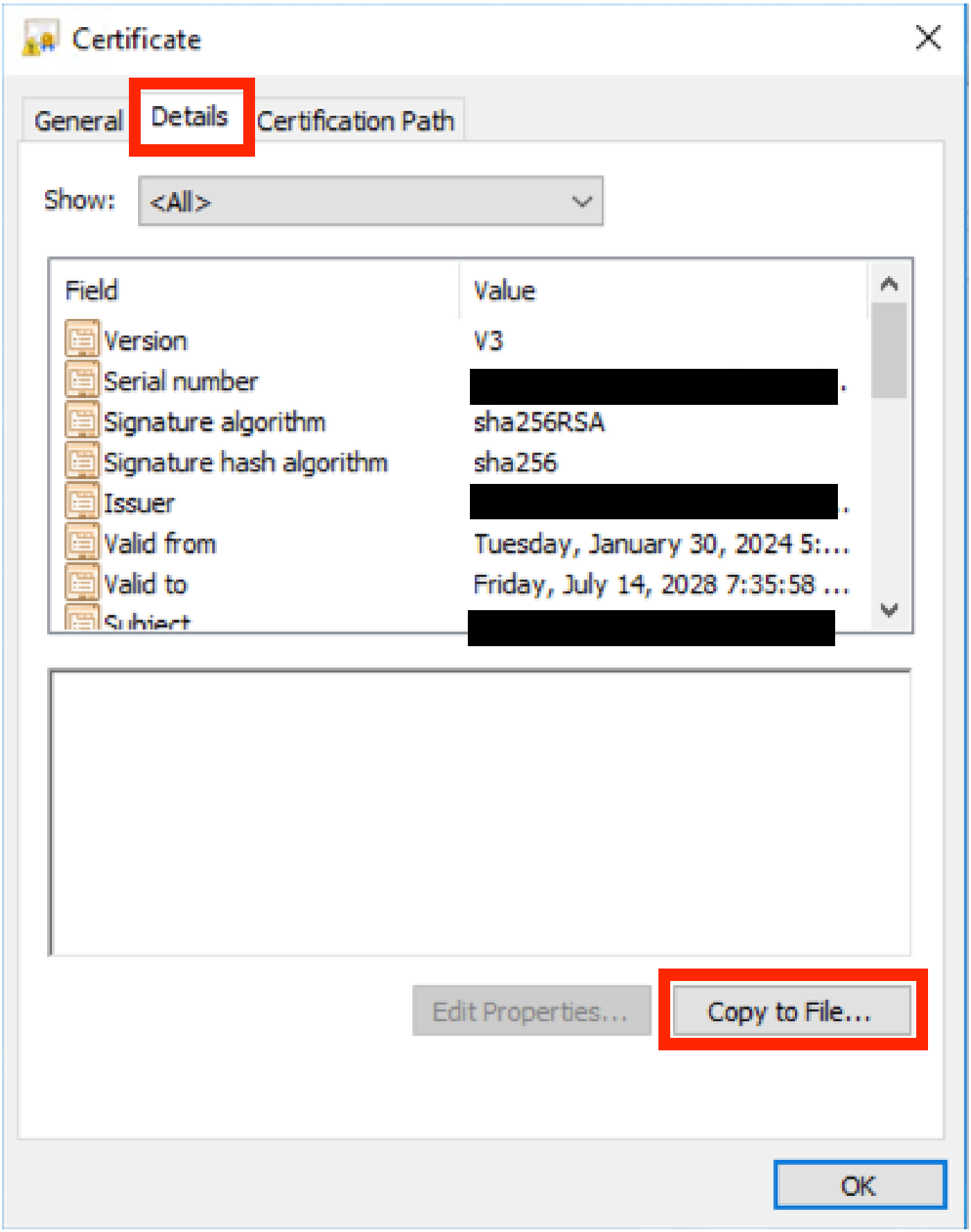
Paso 1. Abra el certificado del servidor.
Paso 2. Vaya a la pestaña Ruta de certificación. El certificado superior se considera el certificado de CA raíz. El inferior es el certificado de servidor y todos los intermedios se consideran certificados CA intermedios.
Paso 3. Elija un certificado de CA y seleccione Ver certificado.



Ruta de certificación

Paso 4. Navegue hasta la pestaña Details y siga los pasos anteriores para guardar el certificado

en un archivo separado.
Paso 5. Repita estos pasos para todos los certificados de CA presentes.



Ficha Detalles del certificado

Una vez que todos los certificados de CA estén disponibles, cárguelos en la lista de certificados de CA de confianza de Expressway:

Paso 6. Vaya a Mantenimiento > Seguridad > Certificado de CA de confianza en el servidor de Expressway.
Paso 7. Seleccione Elegir archivo y cárguelo.
Paso 8. Repita los pasos 7 para cada certificado de CA.
Paso 9. Una vez cargados todos los certificados de CA en la lista de confianza, cargue el certificado de servidor en el servidor.

Zona transversal desactivada con error Error de negociación TLS

Este error se produce cuando el intercambio SSL entre Expressway-C y Expressway-E no se completa correctamente. Algunos ejemplos que pueden causar esto:

- El nombre de host no coincide con ningún nombre del certificado presentado.
  - Asegúrese de que la dirección de par configurada en la zona transversal de Expressway-C coincida con al menos uno de los nombres del certificado de servidor de Expressway-E
- El nombre de verificación de TLS no coincide con ningún nombre del certificado presentado.
  - Asegúrese de que el nombre de verificación de TLS configurado en la zona transversal de Expressway-E coincida con uno de los nombres del certificado de servidor de Expressway-C. Si es una configuración de clúster, se recomienda que el FQDN de clúster de Expressway-C se configure como TLS. Verifique que el nombre ya que este nombre debe estar presente en todos los nodos del clúster.
- Los servidores no confían en los certificados de CA
  - Del mismo modo que cada servidor debe confiar en sus propios certificados de CA antes de cargar el certificado de servidor en él, otros servidores también deben confiar en esos certificados de CA para confiar en el certificado de servidor. Para ello, asegúrese de que todos los certificados de CA de la ruta de certificación de ambos servidores de Expressway estén presentes en la lista de CA de confianza de todos los servidores involucrados. Los certificados de CA se pueden extraer con los pasos proporcionados anteriormente en este documento.

Zona transversal activa pero SSH se desconecta después de una renovación de certificado

Falla del Túnel SSH

Este error suele ocurrir después de la renovación de un certificado cuando uno o más de los certificados de CA intermedios no son de confianza, la confianza del certificado de CA raíz habilita

la conexión de zona transversal, pero los túneles de SSH son una conexión más detallada y pueden fallar cuando la cadena completa no es de confianza, las autoridades de certificados cambian a menudo el certificado de CA intermedia para que la renovación de un certificado pueda desencadenar este problema. Asegúrese de que todos los certificados de CA intermedios se carguen en todas las listas de confianza de Expressway.

El inicio de sesión de Mobile and Remote Access falla después de una actualización o renovación de certificado

Hay muchas maneras en las que un inicio de sesión puede fallar debido a los certificados, pero en las versiones posteriores del software Expressway se implementaron algunos cambios de software que, por razones de seguridad, fuerzan la verificación del certificado donde no se hizo antes.

Esto se explica mejor aquí: El [servidor de tráfico aplica la verificación de certificados]

Como se indica en la solución alternativa, asegúrese de que los certificados de CA de Expressway-C se cargan en Cisco Unified Communications Manager como tomcat-trust y callmanager-trust y reinicie los servicios requeridos.

Alarma de certificado en Jabber al iniciar sesión en Mobile and Remote Access

Advertencia sobre certificados no fiables de Jabber

Este comportamiento se produce cuando el dominio utilizado en la aplicación no coincide con un

nombre alternativo de sujeto en el certificado de servidor de Expressway-E.
Asegúrese de que el ejemplo .com o el collab-edge.ejemplo .com alternativo sea uno de los nombres alternativos de asunto presentes en el certificado.

Información Relacionada

Soporte técnico y descargas de Cisco

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).