Solucionar problemas de certificados do Expressway

Contents

Introdução

Este documento descreve como os certificados funcionam e os problemas mais comuns e dicas para certificados em servidores Expressway.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Servidores Expressway e Video Communications Server (VCS)
- SSL (Secure Sockets Layer - Camada de Soquetes Segura)
- Certificados
- Dispositivos de telepresença
- Acesso móvel e remoto
- Implantações de colaboração

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Expressway x14

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

SSL e certificados são um padrão e funcionam da mesma forma em outros dispositivos e marcas. Este documento se concentra nos usos do certificado no Expressways.

Definições

Os certificados são usados para criar uma conexão segura entre dois dispositivos. São uma assinatura digital que autentica uma identidade de servidor ou dispositivo. Alguns protocolos como Hypertext Transfer Protocol Secure (HTTPS) ou Session Initiation Protocol (SIP) Transport Layer Security (TLS) exigem o uso de certificados para funcionar.

Termos diferentes usados quando você fala sobre certificados:

- CSR (Certificate Signing Request, Solicitação de assinatura de certificado): um modelo criado com os nomes que identificam um dispositivo para ser assinado e convertido posteriormente em um certificado de cliente ou servidor
- Certificado: um CSR assinado. São um tipo de identidade e são instalados em um dispositivo para uso em negociações SSL. Eles podem ser assinados por ele mesmo ou por uma autoridade de certificação.
- Assinatura do certificado: a identidade que verifica se o certificado em questão é legítimo; estes são apresentados sob a forma de outro certificado.
- Certificado Autoassinado: um certificado de cliente ou servidor autoassinado
- Autoridade de Certificação (CA): entidade que assina certificados
    - Certificado intermediário: Certificado de CA que não é assinado por si mesmo, mas por outro Certificado de CA, geralmente assinado por um Certificado raiz, mas também pode ser assinado por outro Certificado intermediário
    - Certificado raiz: certificado CA que é assinado por si mesmo

Princípio básico

Quando um cliente conversa com um servidor e inicia uma conversação SSL, ele troca certificados, que são usados posteriormente para criptografar o tráfego entre os dispositivos. Como parte da troca, os dispositivos também determinam se os certificados são confiáveis. Várias condições devem ser atendidas para determinar se um certificado é confiável. Algumas são:

- O Nome de Domínio Totalmente Qualificado (FQDN) usado inicialmente para entrar em contato com o servidor corresponde a um nome dentro do certificado apresentado pelo servidor.

    - Por exemplo, quando você abre uma página da Web em um navegador, cisco.com resolve o IP de um servidor que fornece um certificado, que deve incluir cisco.com como um nome para ser confiável.

- O Certificado de Autoridade de Certificação que assinou o certificado de servidor apresentado pelo servidor (ou o mesmo certificado de servidor quando autoassinado) está presente na lista de Certificados Confiáveis de Autoridade de Certificação do dispositivo.
    - Os dispositivos têm uma lista de certificados CA que são confiáveis, os computadores normalmente incluem uma lista pré-compilada com autoridades de certificação públicas bem conhecidas.

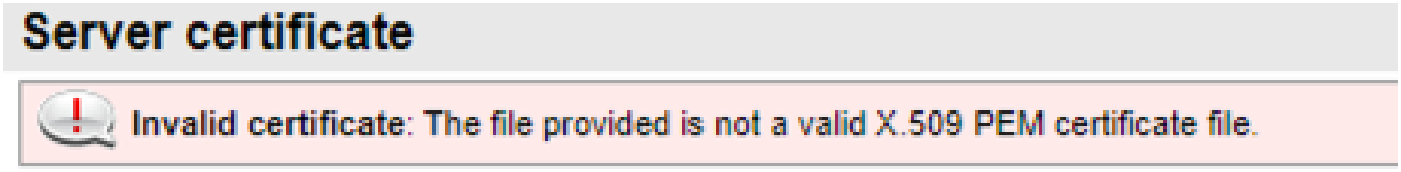
- A data e a hora atuais estão dentro do período de validade do certificado.
    - As Autoridades de Certificação só assinam CSRs por um determinado período, que é determinado pela CA.

- O certificado não foi revogado.
    - As Autoridades de Certificação Públicas normalmente incluem uma URL de Lista de Revogação de Certificado dentro do certificado. Isso ocorre para que a parte que recebe o certificado possa confirmar que ele não foi revogado pela CA.

Problemas comuns

Falha no upload do certificado do Expressway

Há algumas condições que podem causar isso. Eles causam um erro descritivo diferente.



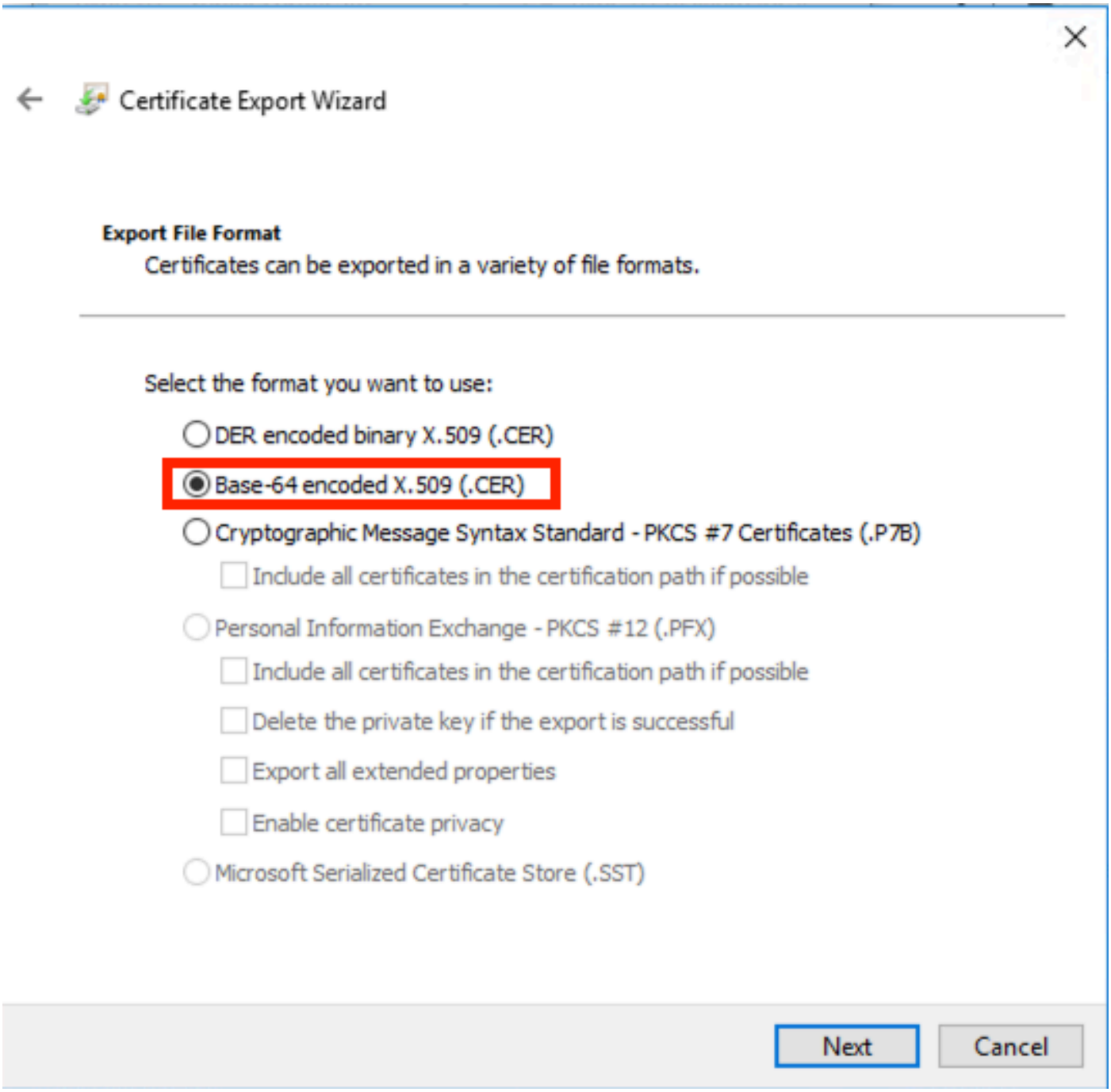
Formato do certificado inválido

Este primeiro erro ocorre quando o certificado não está em um formato válido. A extensão do arquivo não importa.

Se o certificado não for aberto, um novo certificado poderá ser solicitado à CA no formato correto

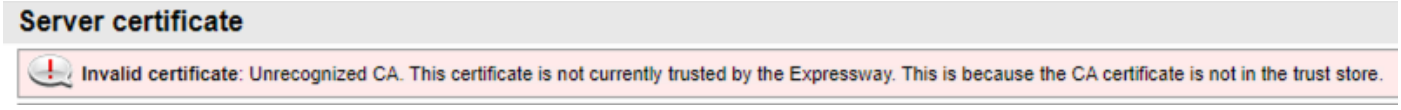
Se o certificado for aberto, siga estas etapas:

Etapa 1. Abra o certificado e navegue até a guia Detalhes.
Etapa 2. Selecione Copiar para arquivo.
Etapa 3. Siga o assistente e certifique-se de que Base-64 encoded esteja selecionado.



Seleção de formato do certificado

Etapa 4. Depois de salvo, carregue o novo arquivo no Expressway.



Cadeia de Certificados de Autoridade de Certificação Não Confiável

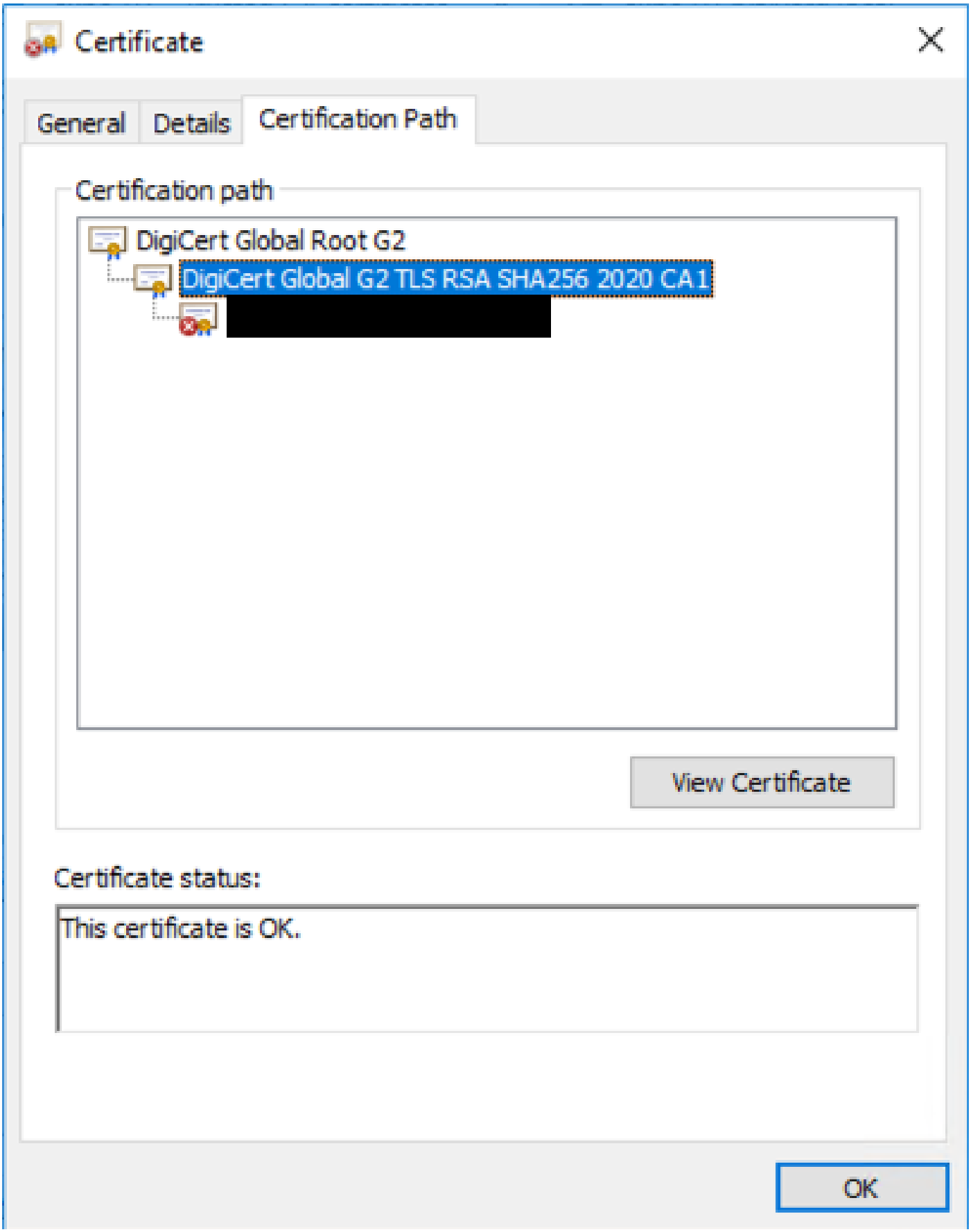
Este erro ocorre quando os Certificados de Autoridade de Certificação que assinaram o certificado do servidor não são confiáveis. Antes de carregar um certificado de servidor, o servidor deve confiar em todos os certificados CA na cadeia.

Normalmente, a CA fornece os certificados de CA junto com o certificado de servidor assinado.

Se eles estiverem disponíveis, vá para a etapa 6 abaixo.

Se os certificados CA não estiverem disponíveis, eles poderão ser obtidos do certificado do servidor. Siga estes passos:

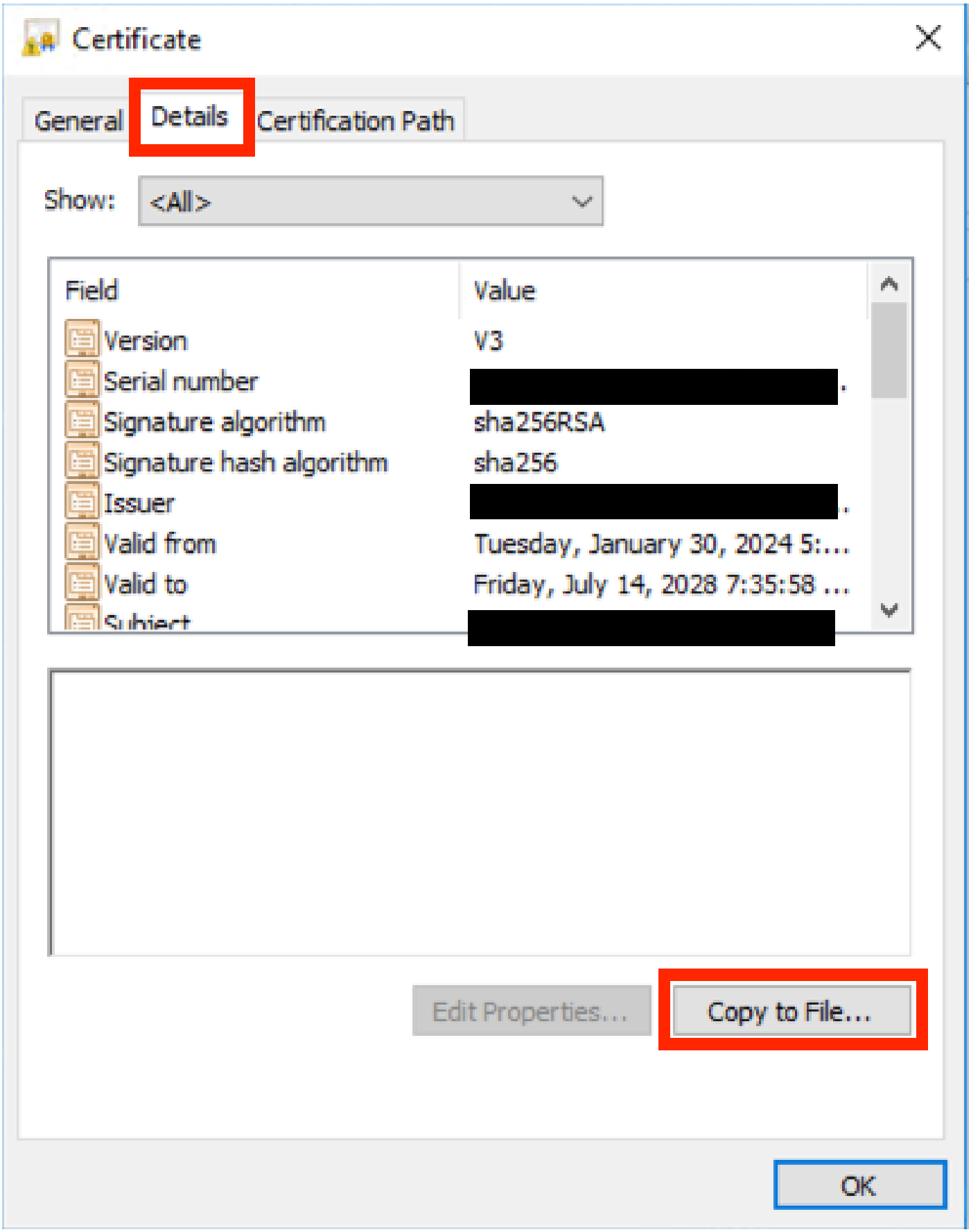
Etapa 1. Abra o certificado do servidor.
Etapa 2. Navegue até a guia Caminho de certificação. O certificado superior é considerado o certificado CA raiz. A parte inferior é o certificado do servidor e todos os intermediários são considerados certificados CA intermediários.
Etapa 3. Escolha um certificado CA e selecione Exibir certificado.



Caminho de certificação

Etapa 4. Navegue até a guia Detalhes e siga as etapas anteriores para salvar o certificado em um

arquivo separado.
Etapa 5. Repita essas etapas para todos os certificados CA presentes.



Guia Detalhes do certificado

Quando todos os certificados CA estiverem disponíveis, carregue-os na lista Certificado CA Confiável do Expressway:

Etapa 6. Navegue para Manutenção > Segurança > Certificado de CA confiável no servidor Expressway.
Passo 7. Selecione Escolher arquivo e carregue.
Etapa 8. Repita as etapas 7 para cada certificado CA.
Etapa 9. Quando todos os certificados CA forem carregados na lista confiável, carregue o certificado do servidor no servidor.

Zona de passagem inoperante com erro Erro de negociação TLS

Este erro ocorre quando o intercâmbio SSL entre o Expressway-C e o Expressway-E não é concluído com êxito. Alguns exemplos que podem causar isso:

- O nome de host não corresponde a um nome no certificado apresentado.
  - Verifique se o endereço de mesmo nível configurado na zona de passagem do Expressway-C corresponde a pelo menos um dos nomes no certificado do servidor Expressway-E
- O nome de verificação TLS não corresponde a um nome no certificado apresentado.
  - Certifique-se de que o nome de Verificação de TLS configurado na zona de passagem Expressway-E corresponda a um dos nomes no certificado do servidor Expressway-C. Se for uma configuração de cluster, é recomendável que o FQDN de cluster do Expressway-C seja configurado como TLS. Verifique o nome, pois ele deve estar presente em todos os nós do cluster.
- Os servidores não confiam nos certificados da autoridade de certificação
  - Assim como cada servidor deve confiar em seus próprios certificados CA antes de carregar o certificado de servidor nele, outros servidores também devem confiar nesses certificados CA para confiar no certificado de servidor. Para isso, certifique-se de que todos os certificados CA do caminho de certificação de ambos os servidores Expressway estejam presentes na lista CA confiável de todos os servidores envolvidos. Os certificados CA podem ser extraídos com as etapas fornecidas anteriormente neste documento.

Zona transversal ativa, mas SSH túneis desativados após uma renovação de certificado

Falha de túnel SSH

Esse erro geralmente ocorre após uma renovação de certificado quando um ou mais certificados CA intermediários não são confiáveis, a confiança do certificado CA raiz habilita a conexão de

zona de passagem, mas os túneis SSH são uma conexão mais detalhada e podem falhar quando a cadeia inteira não é confiável, os certificados CA intermediários são frequentemente alterados pelas autoridades de certificação, de modo que a renovação de um certificado pode disparar esse problema. Certifique-se de que todos os certificados intermediários de CA sejam carregados em todas as listas de confiança do Expressway.

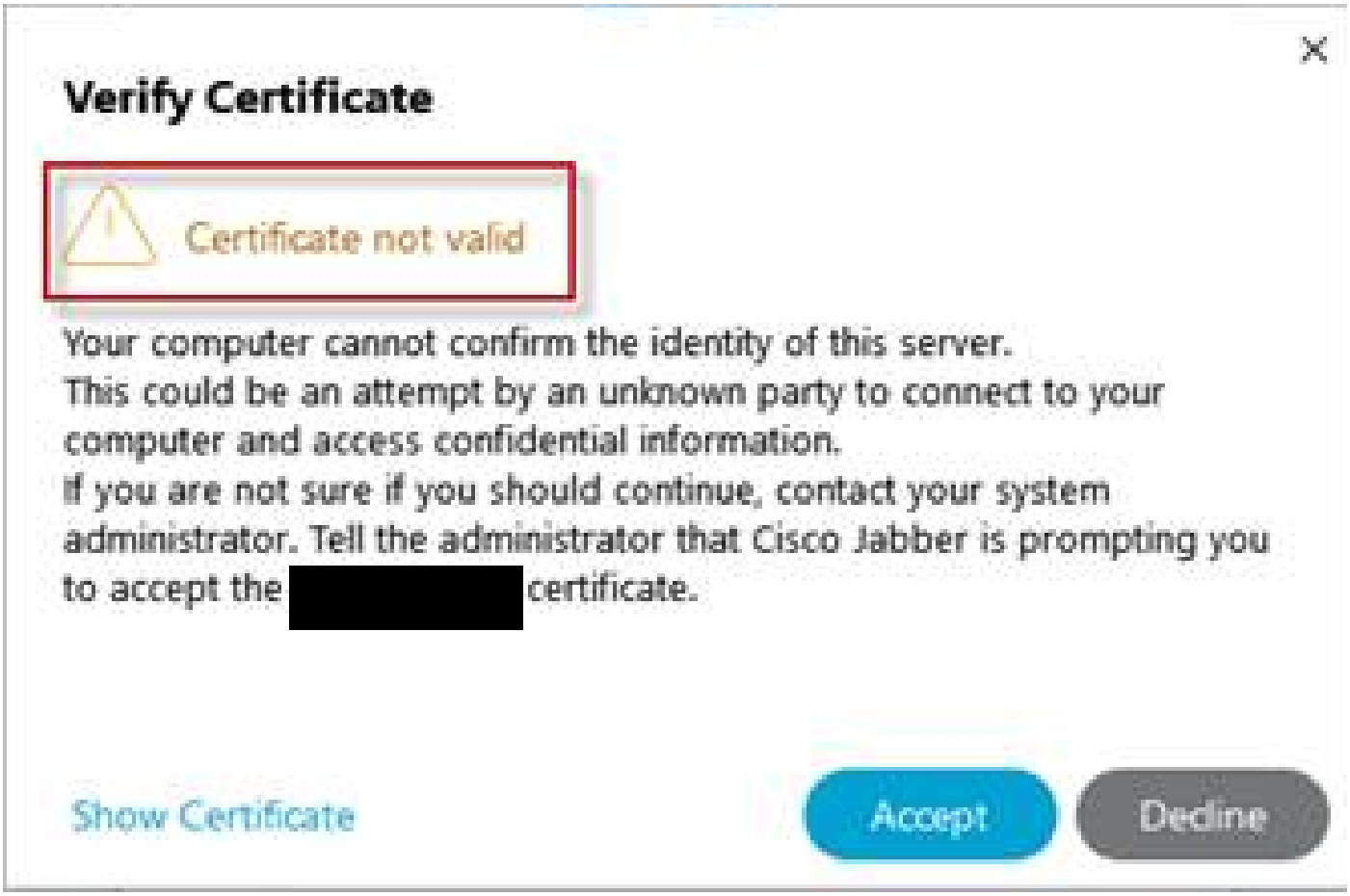
O logon de Acesso Móvel e Remoto falha após uma atualização ou renovação de certificado

Há muitas maneiras pelas quais um login pode falhar devido a certificados, mas em versões posteriores do software Expressway algumas alterações de software foram implementadas que, por razões de segurança, forçam a verificação de certificado onde ela não foi feita antes.

Isso é melhor explicado aqui: O servidor de tráfego impõe a verificação de certificado

Como diz a solução alternativa, certifique-se de que os certificados CA Expressway-C sejam carregados no Cisco Unified Communications Manager como tomcat-trust e callmanager-trust e reinicie os serviços necessários.

Alarme de certificado no Jabber no login de acesso móvel e remoto



Aviso de certificado não confiável Jabber

Esse comportamento ocorre quando o domínio usado no aplicativo não corresponde a um nome alternativo de requerente no certificado do servidor Expressway-E.

Certifique-se de que o exemplo .com ou o collab-edge.example .com alternativo seja um dos nomes alternativos presentes no certificado.

Informações Relacionadas

Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.