Configurar e solucionar problemas de certificados de borda de colaboração (MRA)

Contents

Introdução

Este documento descreve os certificados com relação às implantações de Acesso Remoto Móvel (MRA).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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

Autoridade de certificado (CA) pública vs. privada

Há diversas opções para assinar certificados nos servidores Expressway-C e E. Você pode optar por ter a CSR (Certificate Signing Request, Solicitação de assinatura de certificado) assinada por uma CA pública, como GoDaddy, Verisign ou outras, ou pode assiná-la internamente se usar sua própria Autoridade de certificação (pode ser autoassinada com OpenSSL ou uma CA corporativa interna, como um servidor Microsoft Windows). Para obter mais informações sobre como criar e assinar os CSRs usados por qualquer um desses métodos, consulte o Guia de Criação de Certificados do Video Communication Server (VCS).

O único servidor que exige a assinatura de uma CA pública é o Expressway-E. Este é o único servidor onde os clientes veem o certificado quando entram via MRA, portanto, use uma CA pública para garantir que os usuários não tenham que aceitar manualmente o certificado. O Expressway-E pode funcionar com um certificado interno assinado pela CA, mas os usuários iniciantes seriam solicitados a aceitar o certificado não confiável. O registro MRA dos telefones das séries 7800 e 8800 não funcionaria com certificados internos porque sua lista de certificados confiáveis não pode ser modificada. Para simplificar, sugere-se que seus certificados Expressway-C e Expressway-E sejam assinados pela mesma CA; no entanto, isso não é um requisito, desde que você tenha configurado corretamente as listas de CAs confiáveis em ambos os servidores.

Como funciona a cadeia de certificados

Os certificados são vinculados em uma cadeia de dois ou mais usados para verificar a origem que assinou o certificado do servidor. Há três tipos de certificados em uma cadeia: o certificado cliente/servidor, o certificado intermediário (em alguns casos) e o certificado raiz (também conhecido como CA raiz, pois esta é a autoridade de nível mais alto que assinou o certificado).

Os certificados contêm dois campos principais que criam a cadeia: o assunto e o emissor.

O assunto é o nome do servidor ou da autoridade representada por esse certificado. No caso de um Expressway-C ou Expressway-E (ou outros dispositivos de Unified Communications (UC)), isso é criado a partir do Fully Qualified Domain Name (FQDN).

O emissor é a autoridade que validou esse certificado específico. Como qualquer pessoa pode assinar um certificado (que inclui o servidor que criou o certificado, para começar, também conhecido como certificados autoassinados), os servidores e clientes têm uma lista de emissores ou CAs em que confiam como autênticos.

Uma cadeia de certificados sempre termina com um certificado raiz ou de nível superior autoassinado. À medida que você avança pela hierarquia de certificados, cada certificado tem um emissor diferente em relação ao assunto. Eventualmente, você encontrará a CA raiz onde o assunto e o emissor correspondem. Isso indica que é o certificado de nível superior e, portanto, aquele que precisa ser confiável para uma lista de CAs confiáveis de cliente ou servidor.

Resumo do handshake SSL

No caso da zona de passagem, o Expressway-C sempre atua como o cliente, enquanto o Expressway-E

sempre é o servidor. O intercâmbio simplificado funciona da seguinte forma:

Expressway-C Expressway-E

---------Hello do cliente-------->

<--------Olá servidor---------

<----Certificado do servidor-------

<----Solicitação de certificadoâ€”

------Certificado do cliente------>

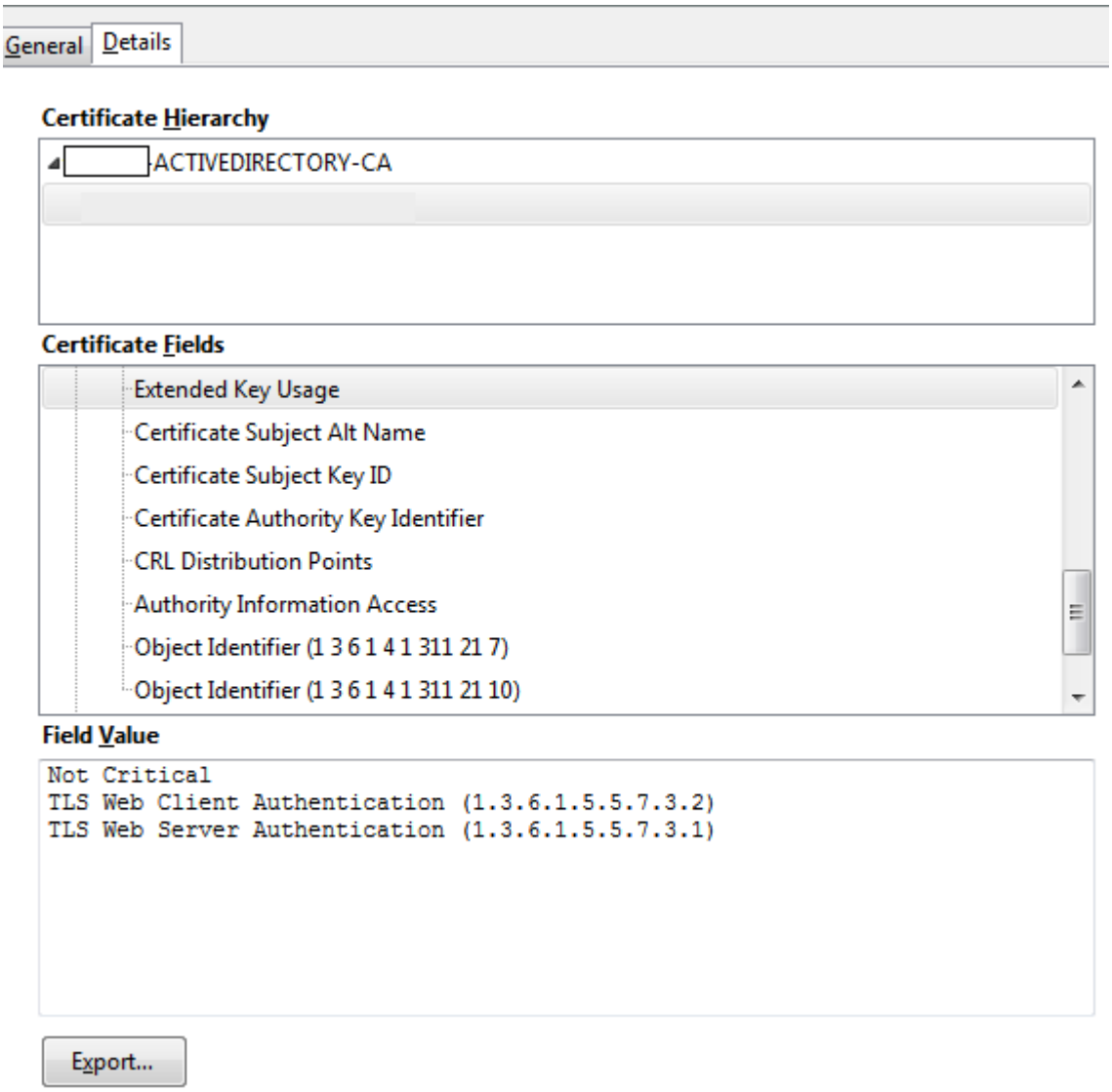
A chave aqui está na troca, pois o Expressway-C sempre inicia a conexão e, portanto, é sempre o cliente. O Expressway-E é o primeiro a enviar seu certificado. Se o Expressway-C não puder validar esse certificado, ele removerá o handshake e não poderá enviar o seu próprio para o Expressway-E.

Outro item importante a observar é a autenticação de cliente Web Transport Layer Security (TLS) e os atributos de autenticação de servidor Web TLS nos certificados. Esses atributos são determinados na CA que assinou o CSR (se uma CA do Windows for usada, isso é determinado pelo modelo selecionado) e indicam se o certificado é válido na função do cliente ou do servidor (ou ambos). Como para um VCS ou Expressway, ele pode ser baseado na situação (é sempre o mesmo para uma zona de passagem), e o certificado deve ter atributos de autenticação de cliente e servidor.

O Expressway-C e o Expressway-E geram um erro quando carregados em um novo certificado de servidor, se ambos não forem aplicados.

Se você não tiver certeza se um certificado tem esses atributos, poderá abrir os detalhes do certificado em um navegador ou no sistema operacional e verificar a seção Uso Estendido de Chave (consulte a imagem). O formato pode variar e depende de como você olha para o certificado.

Exemplo:



Configurar

Confiança/zona de passagem Expressway-C e Expressway-E

Gerar e assinar CSRs

Conforme descrito anteriormente, os certificados Expressway-C e Expressway-E devem ser assinados por uma CA interna ou externa ou pelo OpenSSL para que sejam assinados automaticamente.

> **Observação**: não é possível usar o certificado temporário que vem no servidor Expressway, pois ele não é suportado. Se você usar certificados curinga nos quais você tem um certificado de assinatura de CA e a linha de assunto não estiver definida especificamente, ele não será suportado.

A primeira etapa é gerar o CSR e que ele seja assinado pelo tipo de CA de preferência. Esse processo é fornecido especificamente no guia de criação de certificado. Ao criar o CSR, é importante ter em mente os Nomes Alternativos de Entidade (SANs) necessários que precisam ser incluídos nos certificados. Isso também está listado no guia de certificados e no guia de implantação de acesso remoto móvel. Verifique as versões mais recentes do guia à medida que mais recursos forem sendo adicionados. Lista de SANs comuns que precisam ser incluídas, com base nos recursos usados:

Expressway-C

- Qualquer domínio (interno ou externo) adicionado à lista de domínios.
- Qualquer alias de nó de bate-papo persistente se a federação XMPP for usada.
- Proteger nomes de perfil de dispositivo no CUCM se perfis de dispositivo seguros forem usados.

Expressway-E

- Qualquer domínio configurado no Expressway-C.
- Qualquer alias de nó de bate-papo persistente se a federação XMPP for usada.
- Qualquer domínio divulgado por federações XMPP.

> **Observação**: se o domínio base usado para pesquisas de registro de serviço (SRV) externo não estiver incluído como SAN no certificado Expressway-E (xxx.com ou collab-edge.xxx.com), os clientes Jabber ainda exigirão que o usuário final aceite o certificado na primeira conexão e os endpoints TC não conseguirão se conectar.

Configure o Expressway-C e o Expressway-E para confiar um no outro

Para que a zona de passagem do Unified Communications estabeleça uma conexão, o Expressway-C e o Expressway-E devem confiar nos certificados uns dos outros. Para este exemplo, suponha que o certificado Expressway-E foi assinado por uma CA pública que usa essa hierarquia.

Certificado 3

Emissor: CA raiz GoDaddy

Assunto: CA raiz GoDaddy

Certificado 2

Emissor: CA raiz GoDaddy

Assunto: Autoridade Intermédia GoDaddy

Certificado 1

Emissor: Autoridade Intermediária GoDaddy

Assunto: Expressway-E.lab

O Expressway-C precisa ser configurado com o certificado de confiança 1. Na maioria dos casos, com base nos certificados confiáveis aplicados ao servidor, ele envia apenas seu certificado de servidor de nível mais baixo. Isso significa que, para que o Expressway-C confie no certificado 1, você deve carregar os certificados 2 e 3 na lista de CAs confiáveis do Expressway-C (**Manutenção**> Segurança > Lista de CAs confiáveis). Se você deixar de fora o certificado intermediário 2 quando o Expressway-C receber o certificado Expressway-E, ele não poderá ter uma maneira de vinculá-lo à CA raiz GoDaddy confiável, portanto, ele seria rejeitado.

Certificado 3

Emissor: CA raiz GoDaddy

Assunto: CA raiz GoDaddy

Certificado 1

Emissor: Autoridade Intermediária GoDaddy - Não Confiável!

Assunto: Expressway-E.lab

Além disso, se você carregar apenas o certificado intermediário sem a raiz para a lista de CA confiável do Expressway-C, verá que a Autoridade Intermediária GoDaddy é confiável, mas é assinada por uma autoridade superior, nesse caso, a CA raiz GoDaddy que não é confiável, portanto, falhará.

Certificado 2

Emissor: CA raiz GoDaddy - Não confiável!

Assunto: Autoridade Intermédia GoDaddy

Certificado 1

Emissor: Autoridade Intermediária GoDaddy

Assunto: Expressway-E.lab

Com todos os intermediários e o raiz adicionado à lista de CA confiável o certificado pode ser verificado...

Certificado 3

Emissor: CA raiz GoDaddy - certificado de nível superior autoassinado é confiável e a cadeia está completa!

Assunto: CA raiz GoDaddy

Certificado 2

Emissor: CA raiz GoDaddy

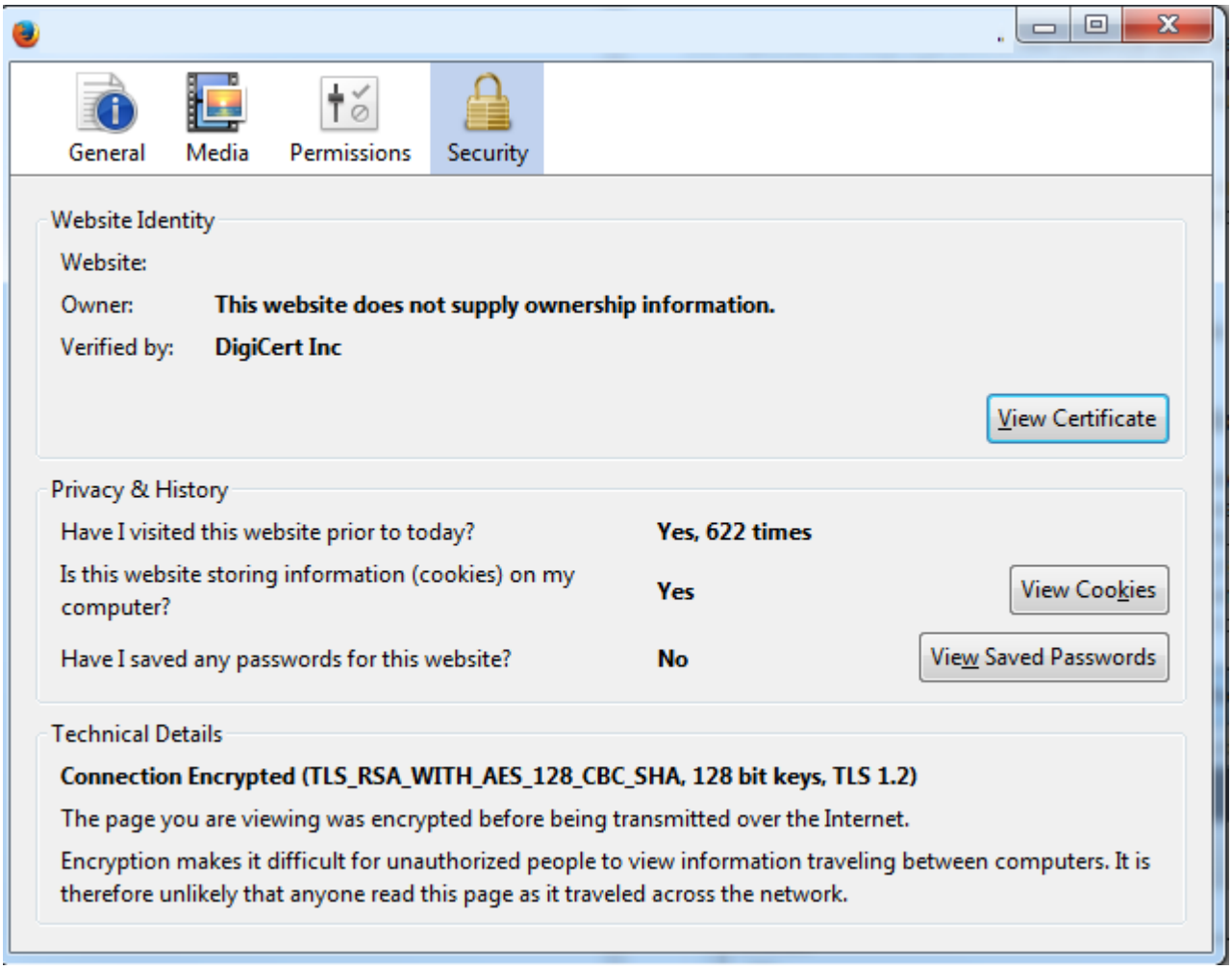
Assunto: Autoridade Intermédia GoDaddy

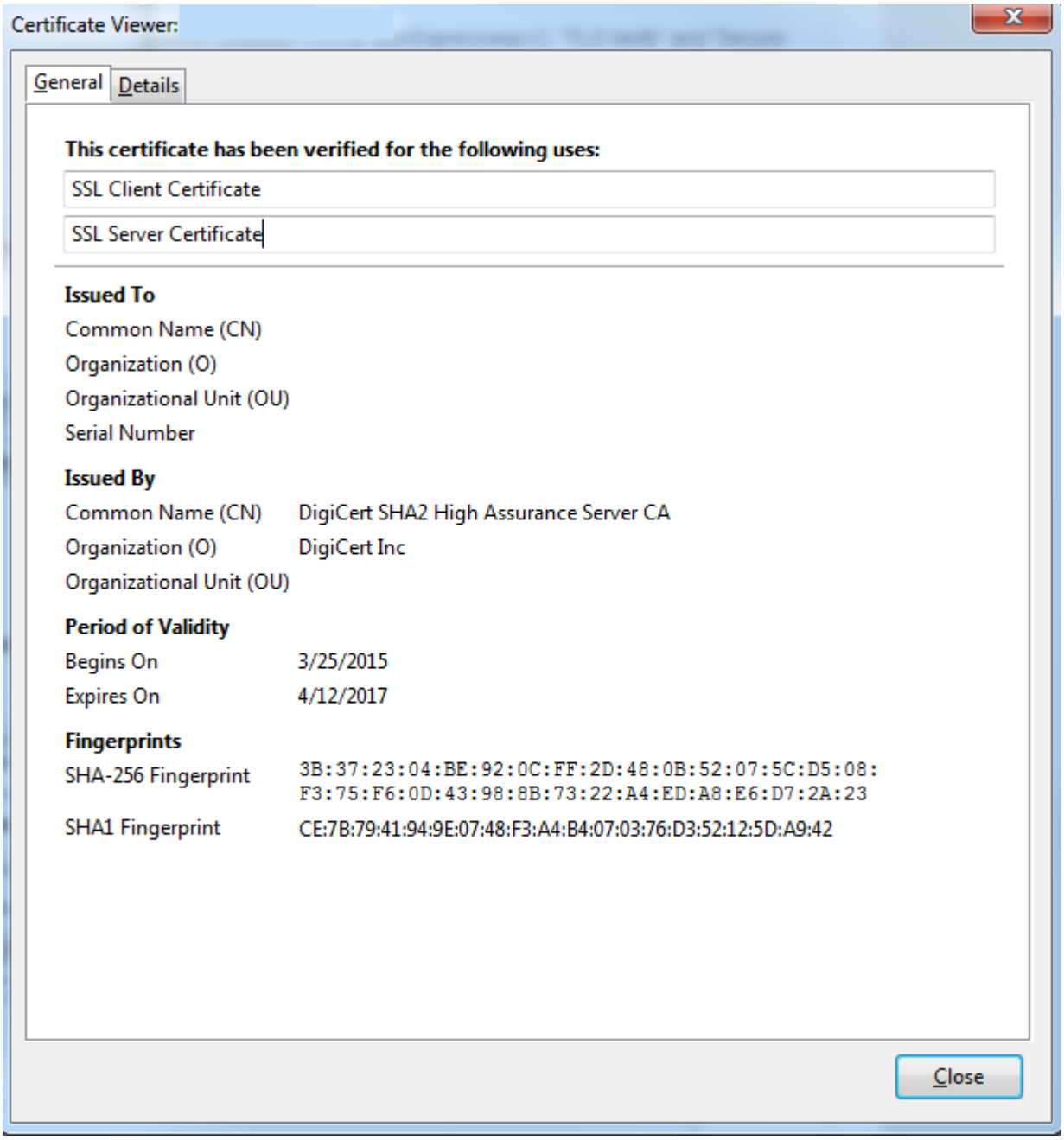
Certificado 1

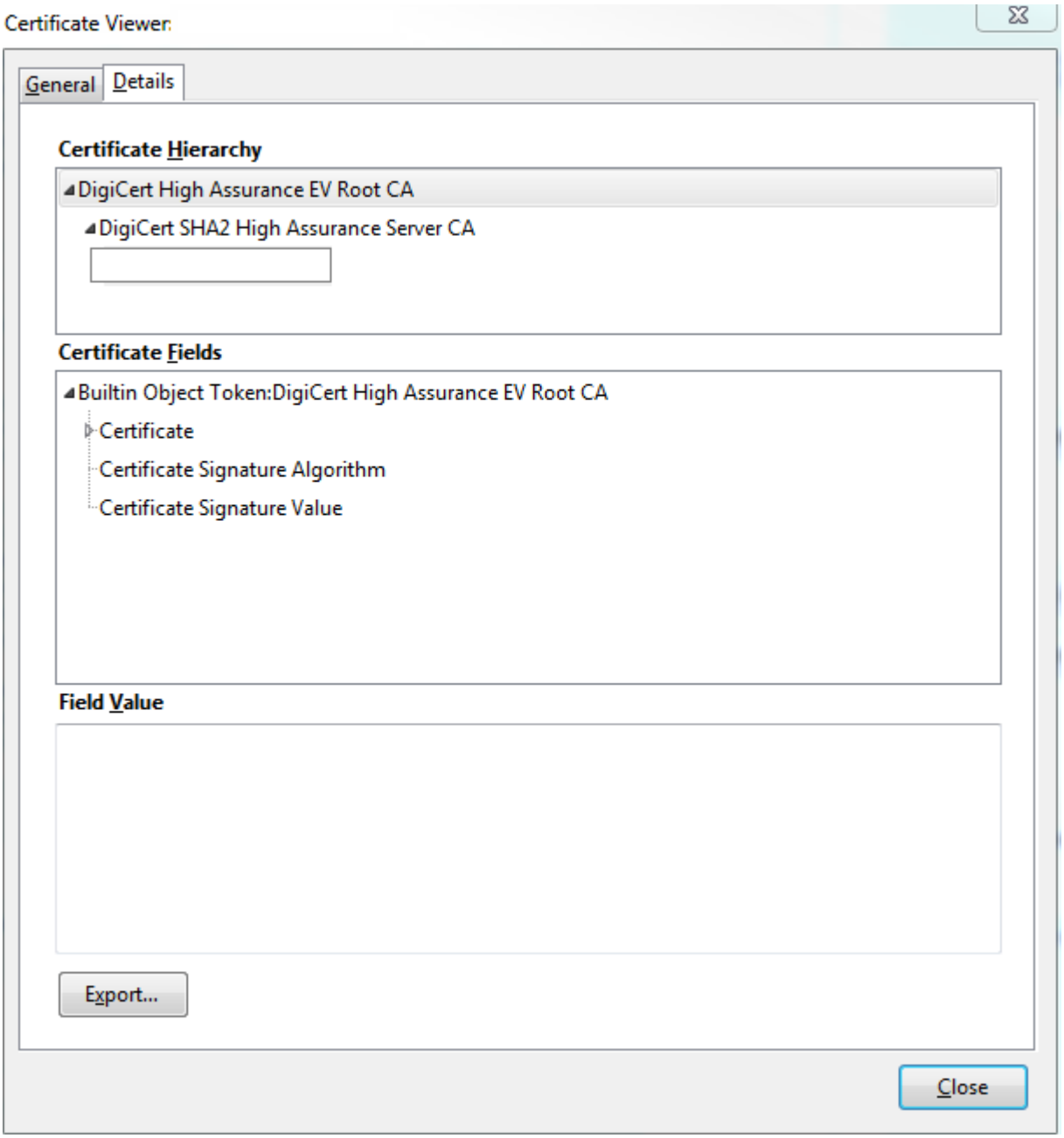
Emissor: Autoridade Intermediária GoDaddy

Assunto: Expressway-E.lab

Se você não tiver certeza de qual é a cadeia de certificados, poderá verificar seu navegador quando estiver conectado à interface da Web do Expressway específico. O processo varia levemente com base no navegador, mas no Firefox, você pode clicar no ícone de cadeado na extremidade esquerda da barra de endereços. No pop-up, clique em **Mais informações > Exibir certificado > Detalhes**. Se o seu navegador puder juntar toda a cadeia, você poderá ver a cadeia de cima para baixo. Se o certificado de nível superior não tiver um assunto e um emissor correspondentes, isso significa que a cadeia não foi concluída. Você também pode exportar cada certificado na cadeia sozinho, se clicar em **exportar** com o certificado desejado realçado. Isso é útil caso você não esteja 100% certo de que carregou os certificados corretos na lista de CAs confiáveis.


General
Media
Permissions
Security
Website Identity
Website:
Owner: This website does not supply ownership information.
Verified by: DigiCert Inc
View Certificate
Privacy & History
Have I visited this website prior to today? Yes, 622 times
Is this website storing information (cookies) on my computer? Yes
View Cookies
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.


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



Agora que o Expressway-C confia no certificado do Expressway-E, verifique se ele funciona na direção oposta. Se o certificado Expressway-C for assinado pela mesma CA que assinou o Expressway-E, o processo será simples. Carregue os mesmos certificados para a lista de CAs confiáveis no Expressway-E como você já fez no C. Se o C for assinado por uma CA diferente, você precisará usar o mesmo processo como mostrado na imagem, mas usar a cadeia do certificado assinado pelo Expressway-C.

Comunicação segura entre Cisco Unified Communications Manager (CUCM) e Expressway-C

Overview

Diferentemente da zona de passagem entre Expressway-C e Expressway-E, a sinalização segura NÃO é necessária entre Expressway-C e CUCM. A menos que não seja permitido por políticas de segurança internas, você deve sempre configurar o MRA para trabalhar com perfis de dispositivo não seguros no CUCM primeiro para confirmar se o restante da implantação está correto antes de continuar com esta etapa.

Há dois recursos de segurança principais que podem ser ativados entre o CUCM e o Expressway-C;

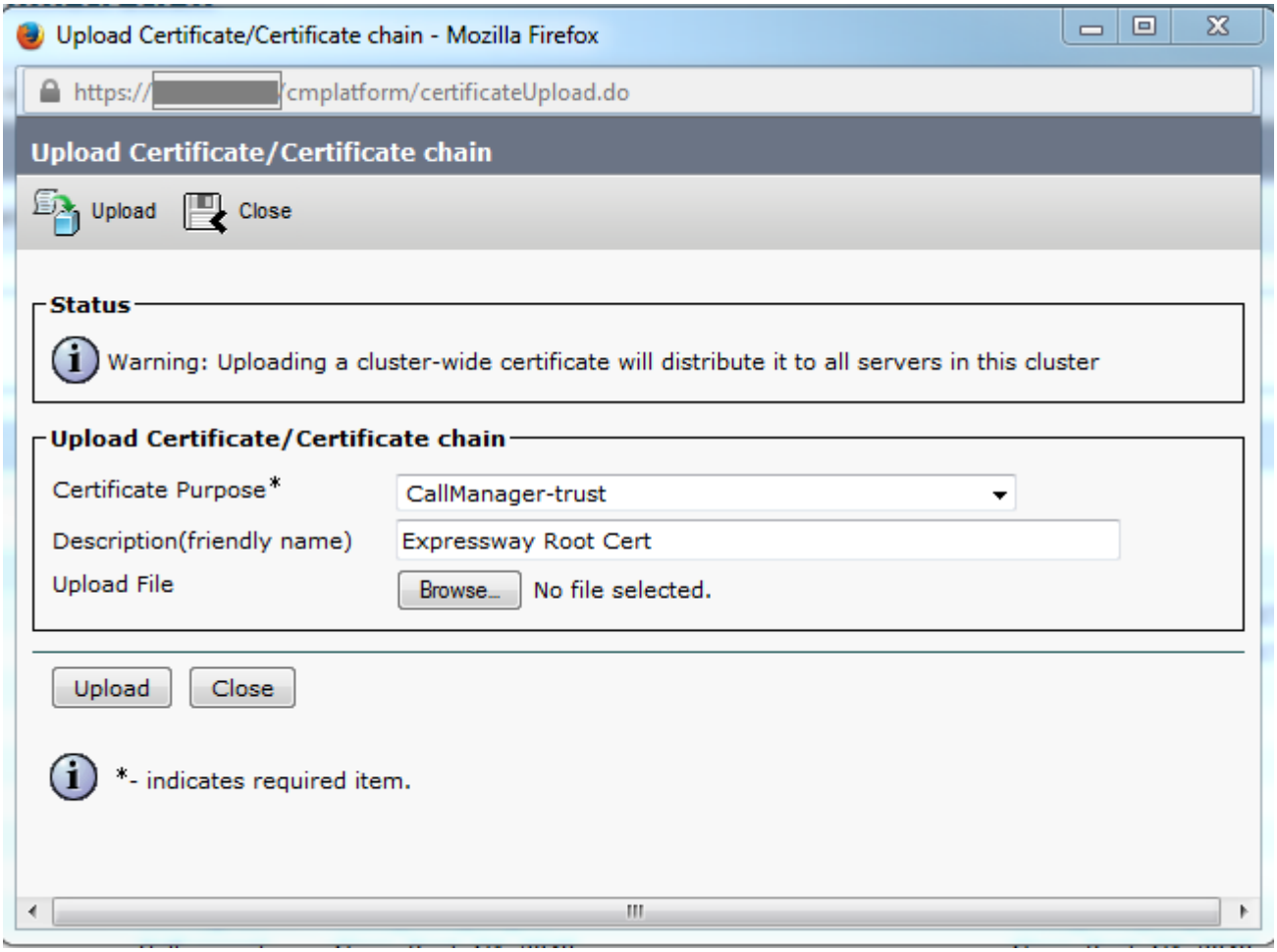
Verificação de TLS e Registros de dispositivo seguro. Há uma diferença importante entre esses dois, pois eles usam dois certificados diferentes no lado CUCM do handshake SSL.

Verificação TLS - certificado tomcat

Proteger registros SIP - certificado callmanager

Configurar confiança entre CUCM e Expressway-C

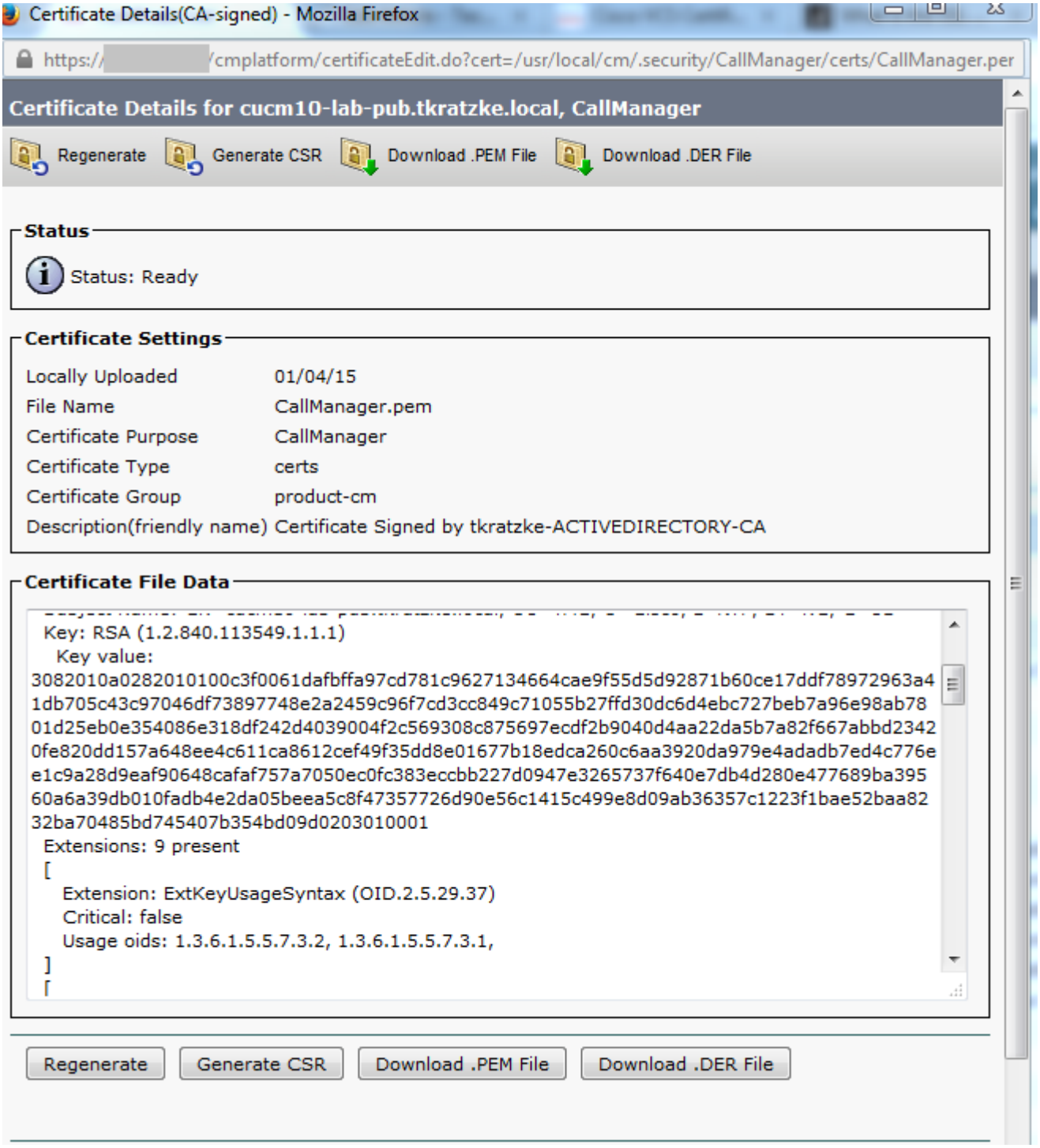
O conceito, neste caso, é exatamente o mesmo que entre Expressway-C e Expressway-E. O CUCM primeiro precisa confiar no certificado de servidor do Expressway-C. Isso significa que no CUCM, os certificados raiz e intermediários do Expressway-C precisam ser carregados como um certificado tomcat-trust para o recurso de verificação TLS e um CallManager-trust para registros de dispositivo seguro. Para conseguir isso, navegue até **Cisco Unified OS Administration** no canto superior direito da GUI da Web do CUCM e, em seguida, **Security**> **Certificate Management**. Aqui é possível clicar em **Carregar certificado/cadeia de certificados e selecione o formato confiável correto ou clique em Encontrar para ver uma lista dos certificados carregados no momento.**



Você precisa garantir que o Expressway-C confie na CA que assinou os certificados do CUCM. Isso pode ser feito se você adicioná-los à lista de CAs confiáveis. Em quase todos os casos, se você assinou os certificados CUCM com uma CA, os certificados tomcat e CallManager devem ser assinados pela mesma CA. Se forem diferentes, você precisará confiar em ambos se usar Verificação TLS e Registros seguros.

Para registros SIP seguros, você também deve garantir que o nome do perfil do dispositivo seguro no CUCM que é aplicado ao dispositivo esteja listado como uma SAN no certificado Expressway-C. Se não contiver as mensagens de registro seguro, ele falhará com um 403 do CUCM, que indica uma falha de TLS.

Observação: quando o handshake SSL ocorre entre o CUCM e o Expressway-C para um registro SIP seguro, dois handshakes ocorrem. Primeiro, o Expressway-C atua como o cliente e inicia a conexão com o CUCM. Uma vez concluído com êxito, o CUCM inicia outro handshake como o cliente para responder. Isso significa que, assim como o Expressway-C, o certificado callmanager no CUCM precisa ter os atributos de cliente Web TLS e de autenticação de servidor Web aplicados. A diferença é que o CUCM permite que esses certificados sejam carregados sem ambos, e os registros internos seguros funcionariam bem se o CUCM tivesse apenas o atributo de autenticação de servidor. Você pode confirmar isso no CUCM se procurar o certificado do CallManager na lista e selecioná-lo. Lá, você pode ver os ids de uso na seção Ramal. Você pode ver 1.3.6.1.5.5.7.3.2 para a autenticação de cliente e 1.3.6.1.5.5.7.3.1 para a autenticação de servidor. Você também pode baixar o certificado nesta janela.



Observação: os certificados confiáveis aplicados ao publicador em um cluster devem ser replicados para os assinantes. É bom confirmar fazendo login neles separadamente em uma nova configuração.

Observação: para que o Expressway-C valide corretamente o certificado do CUCM, os servidores CUCM DEVEM ser adicionados ao Expressway-C com o FQDN, não o endereço IP. A única maneira de o endereço IP funcionar é se o IP de cada nó do CUCM for adicionado como uma SAN no certificado, o que quase nunca é feito.

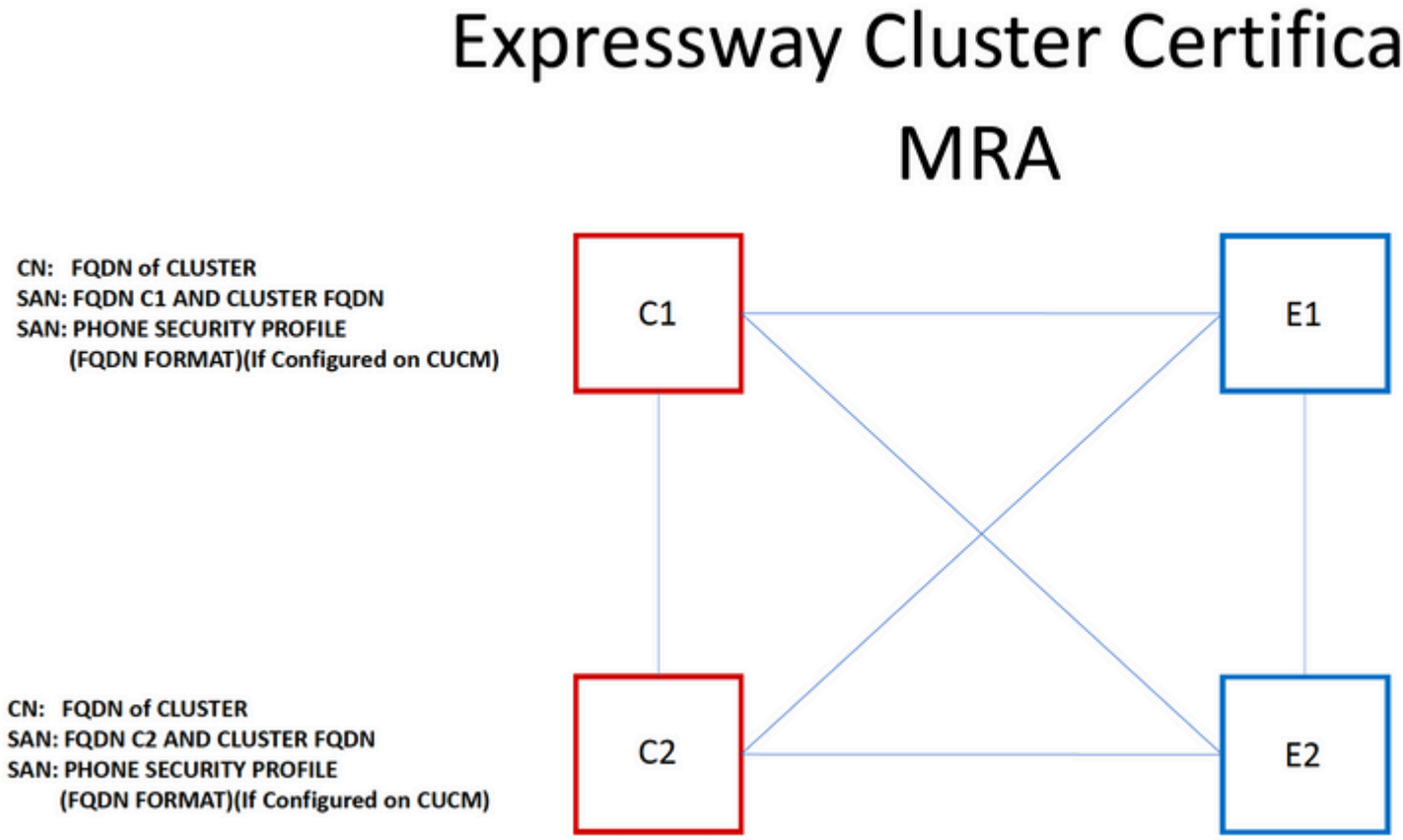
Servidores CUCM com certificados autoassinados

Por padrão, um servidor CUCM vem com certificados autoassinados. Se eles estiverem em vigor, não será possível usar os registros de verificação TLS e de dispositivo seguro ao mesmo tempo. Qualquer recurso pode ser usado sozinho, mas como os certificados são autoassinados, significa que os certificados Tomcat e CallManager autoassinados precisam ser carregados na lista de CAs confiáveis no Expressway-C. Quando o Expressway-C pesquisa sua lista de confiança para validar um certificado, ele para quando encontra um com um assunto correspondente. Por causa disso, o que estiver mais alto na lista de confiança, tomcat ou CallManager, esse recurso funcionará. O mais baixo falharia como se não estivesse presente. A solução para isso é assinar seus certificados CUCM com uma CA (pública ou privada) e confiar apenas nessa CA.

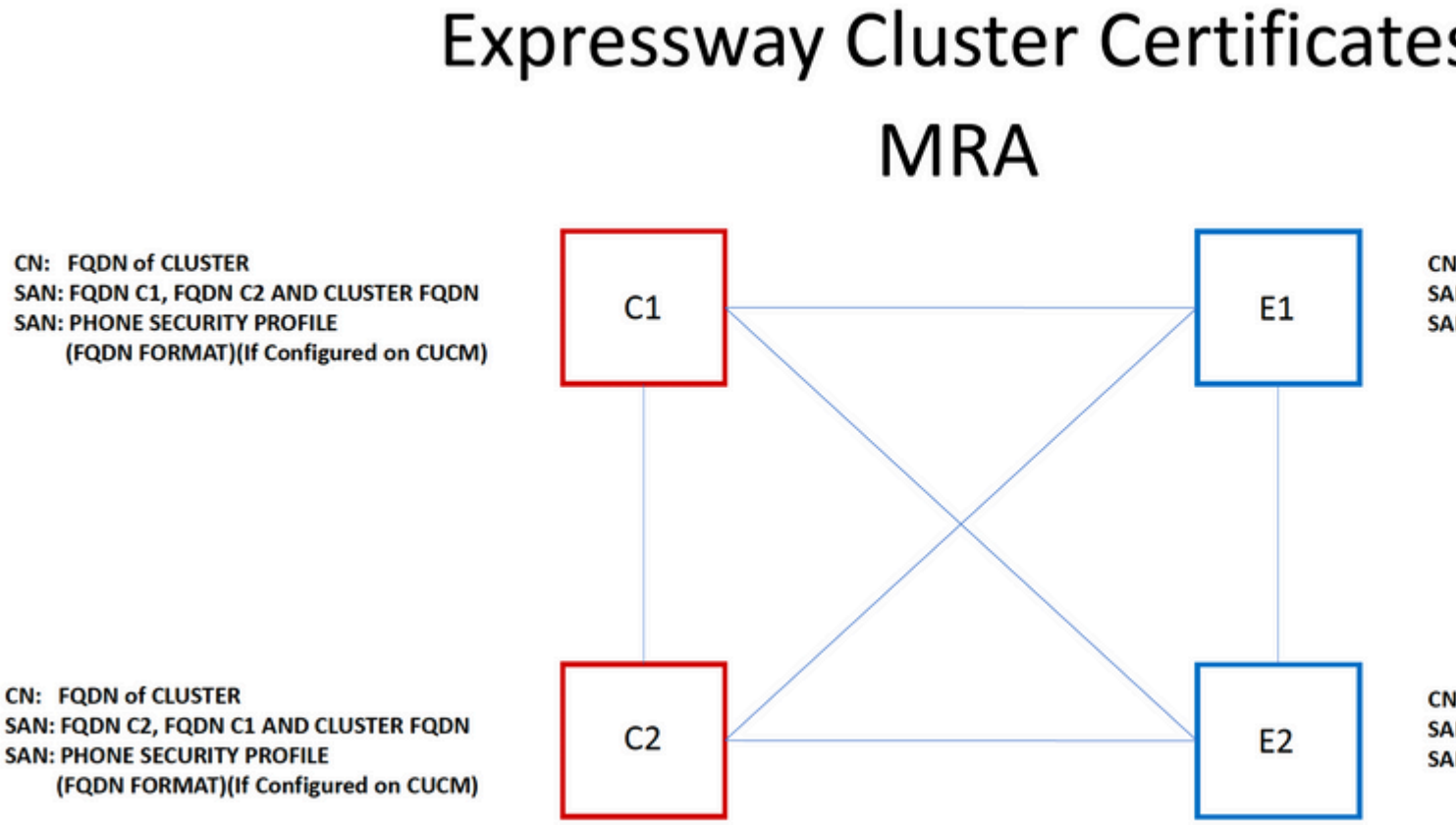
Considerações de cluster Expressway-C e Expressway-E

Certificados de cluster

É altamente recomendável que, se tiver um cluster dos servidores Expressway-C ou Expressway-E para redundância que um CSR separado seja gerado e assinado por uma CA. No cenário anterior, o Nome Comum (CN) de cada certificado de pares seria o mesmo FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) do cluster e as SANs seriam o FQDN do cluster e o respectivo FQDN de pares, como mostrado na imagem:



É possível usar o FQDN de cluster como o CN e cada FQDN de peers e o FQDN de cluster na SAN para usar o mesmo certificado para todos os nós no cluster e, portanto, evitar o custo de vários certificados assinados por uma CA pública.



> **Observação**: os nomes do perfil de segurança do telefone no certificado Cs só são necessários se você usar perfis de segurança do telefone seguro no UCM. O domínio externo ou collab-edge.example.com (onde example.com é o seu domínio) é um requisito somente para o registro de telefone IP e de terminal TC sobre MRA. Isso é opcional para o registro Jabber em MRA. Se não estiver presente, o jabber solicitará a aceitação do certificado quando o jabber efetuar login no MRA.

Se for absolutamente necessário, isso pode ser feito com o próximo processo ou você pode usar o OpenSSL para gerar a chave privada e o CSR manualmente:

Etapa 1. Gere um CSR no principal do cluster e configure-o para listar o alias do cluster como o CN. Adicione todos os pares no cluster como nomes alternativos, juntamente com todos os outros SANs obrigatórios.

Etapa 2. Assine este CSR e carregue-o no correspondente principal.

Etapa 3. Efetue login no principal como raiz e baixe a chave privada localizada em /Tandberg/persistent/certs.

Etapa 4. Carregue o certificado assinado e a chave privada correspondente um ao outro no cluster.

> **Observação**: isso não é recomendado pelas seguintes razões:
> 1. É um risco de segurança porque todos os pares usam a mesma chave privada. Se um estiver de alguma forma comprometido, um invasor poderá descriptografar o tráfego de qualquer um dos servidores.
> 2. Caso uma alteração precisar ser realizada no certificado, todo esse processo precisará ser seguido

---

novamente em vez de uma simples geração e assinatura de CSR.

Listas de CA confiáveis

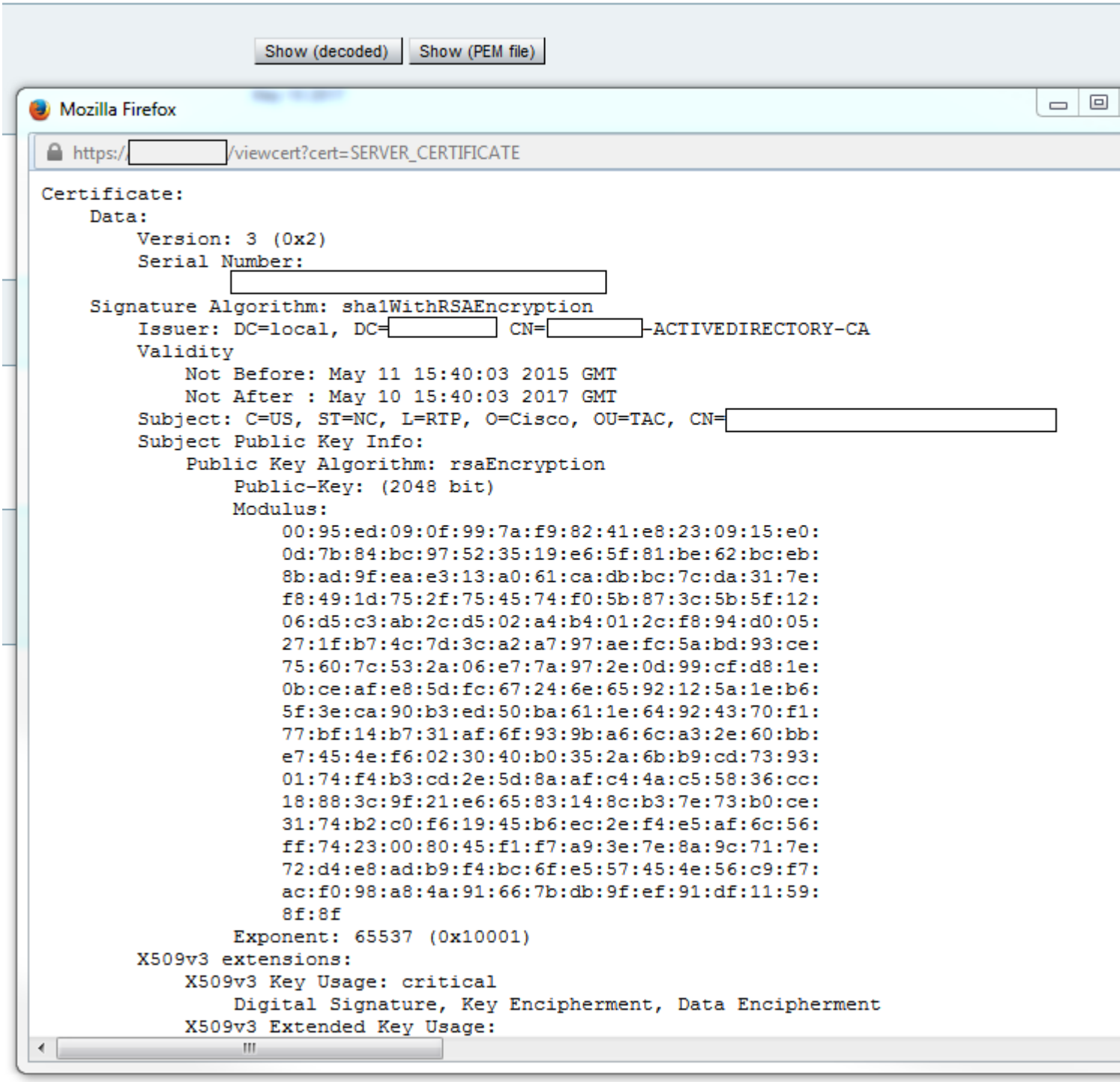
Diferentemente dos assinantes CUCM em um cluster, a lista de CAs confiáveis NÃO é replicada de um par para outro em um cluster Expressway ou VCS. Isso significa que, se você tiver um cluster, precisará carregar manualmente certificados confiáveis para a lista de CAs em cada peer.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verifique as informações do certificado atual

Há várias maneiras de verificar as informações em um certificado atual. A primeira opção é através do navegador da Web. Use o método descrito na seção anterior que também pode ser usado para exportar um certificado específico na cadeia. Se precisar verificar SANs ou outros atributos adicionados ao certificado de servidor Expressway, você pode fazer isso diretamente por meio da interface gráfica do usuário (GUI) da Web, navegue para **Manutenção > Certificados de segurança > Certificado de servidor** e clique em **Mostrar decodificado**.

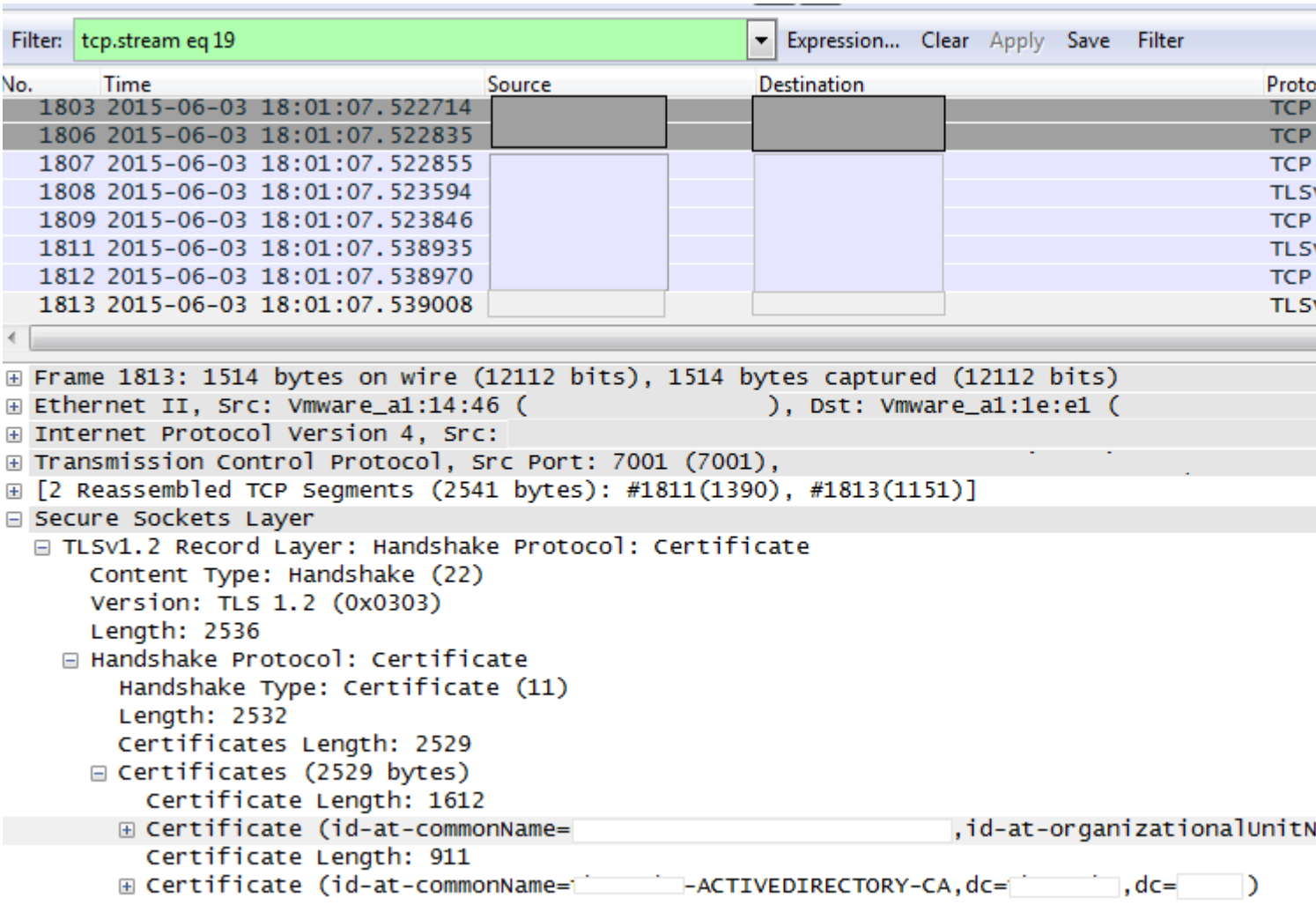


Aqui você pode ver todos os detalhes específicos do certificado sem a necessidade de baixá-lo. Você também pode fazer o mesmo em um CSR ativo, caso o certificado assinado associado ainda não tenha sido carregado.

Ler/exportar um certificado no Wireshark

Se você tiver uma captura Wireshark do handshake SSL que inclua a troca de certificados, o Wireshark pode realmente decodificar o certificado para você, e você pode realmente exportar qualquer certificado na cadeia (se a cadeia completa for trocada) de dentro. Filtre a captura de pacotes pela porta específica da troca de certificados (normalmente 7001 no caso da zona de passagem). Em seguida, se você não vir os pacotes hello do cliente e do servidor junto com o handshake SSL, clique com o botão direito do mouse em um dos

pacotes no fluxo TCP e selecione **decode as**. Aqui, selecione **SSL** e clique em **aplicar**. Agora, se você capturou o tráfego correto, você deve ver a troca de certificado. Localize o pacote do servidor correto que contém o certificado na carga. Expanda a seção SSL no painel inferior até ver a lista de certificados como mostrado na imagem:



Aqui você pode expandir qualquer um dos certificados para ver todos os detalhes. Se você quiser exportar o certificado, clique com o botão direito do mouse no certificado desejado na cadeia (se houver vários) e selecione **Exportar bytes de pacotes selecionados**. Insira um nome para o certificado e clique em **salvar**. Agora, você deve ser capaz de abrir o certificado no Visualizador de Certificados do Windows (se você lhe der uma extensão .cer), ou carregá-lo em qualquer outra ferramenta para análise.

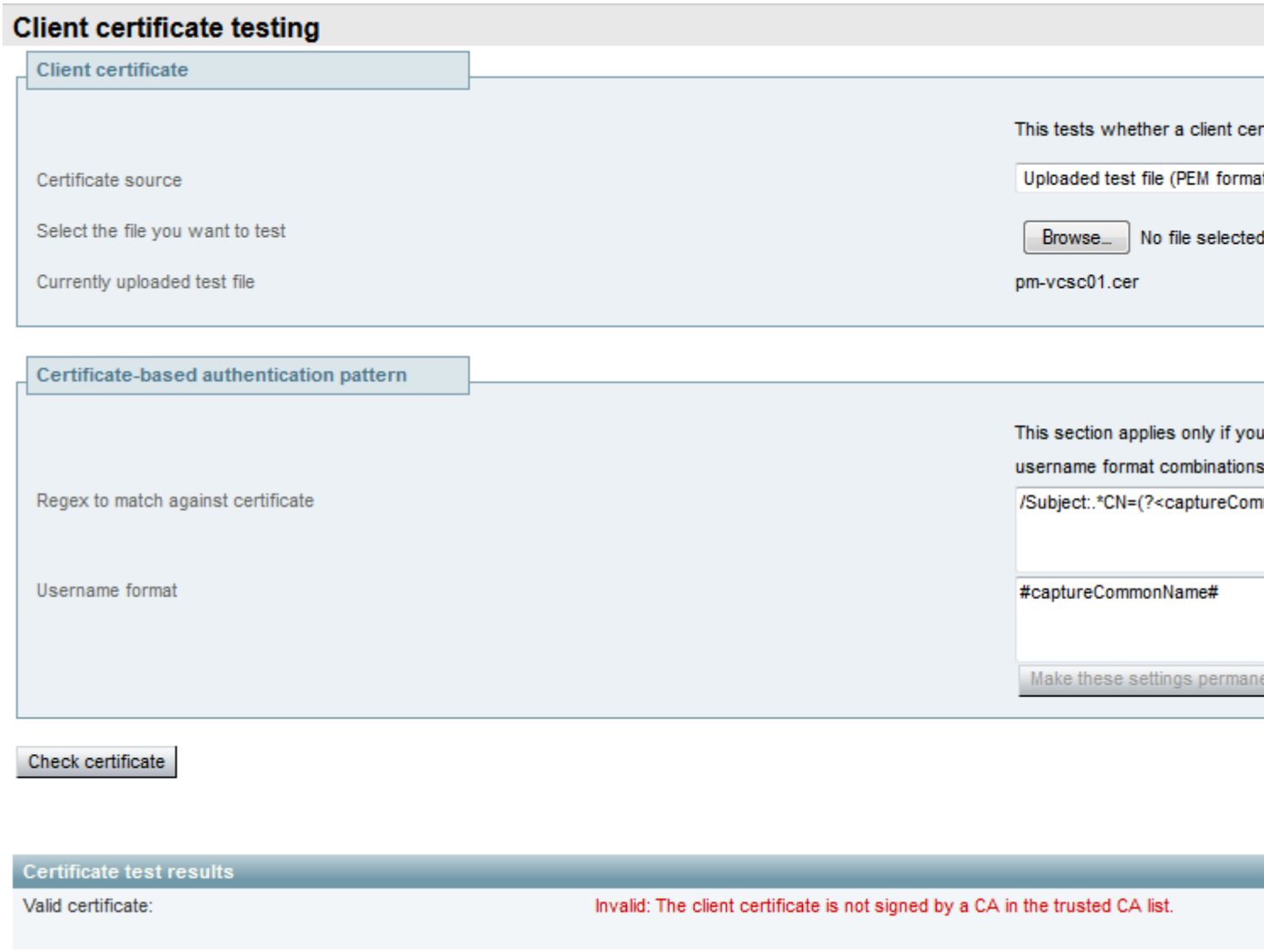
Troubleshooting

Esta seção fornece as informações que você pode usar para solucionar problemas da sua configuração.

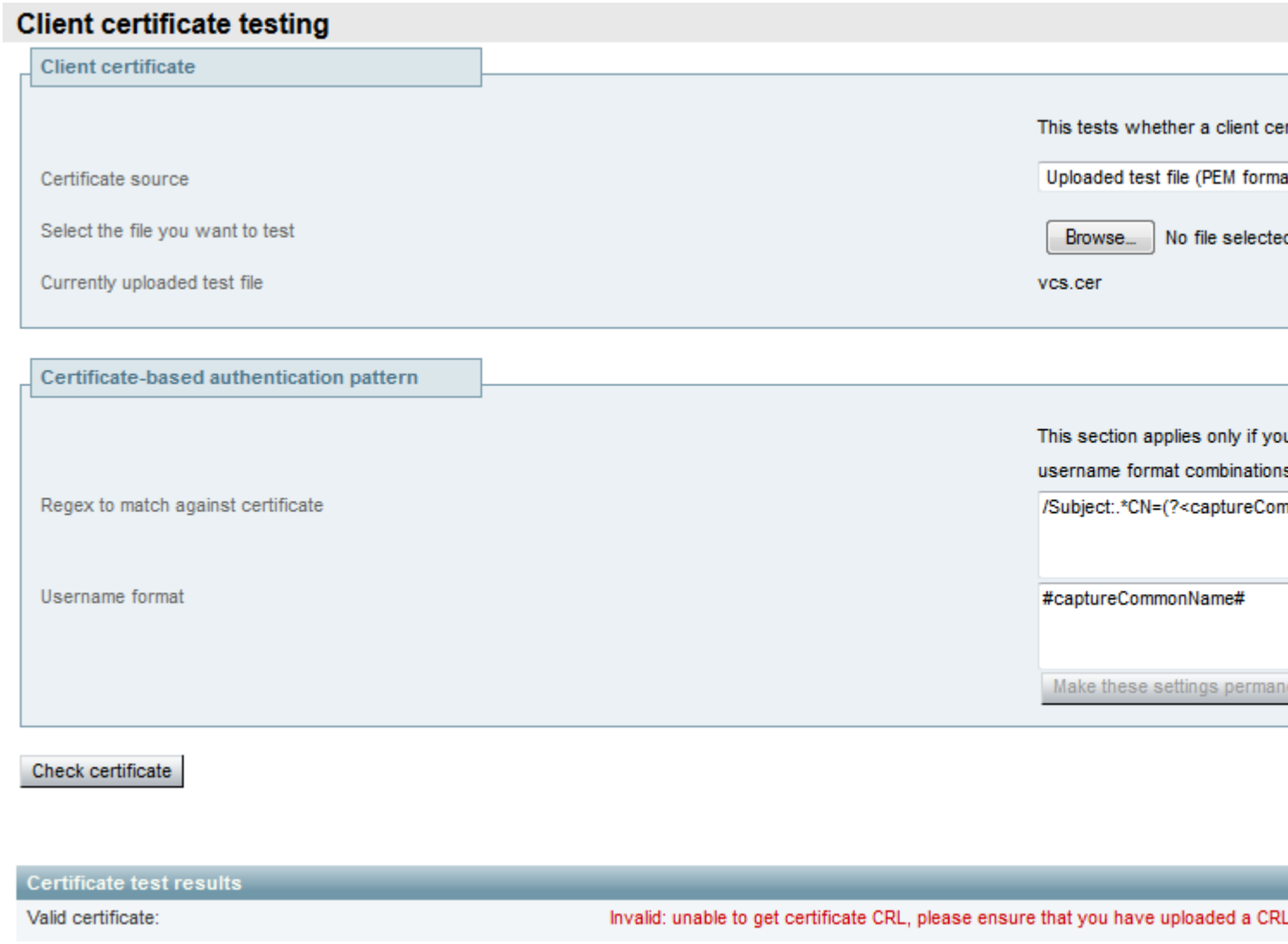
Testar Para Saber Se Um Certificado É Confiável No Expressway

Embora o melhor método seja verificar manualmente a cadeia de certificados e garantir que todos os membros estejam incluídos na lista de CAs confiáveis do Expressway, você pode verificar rapidamente se o Expressway confia em um certificado de cliente específico com a ajuda do **Teste de Certificado de Cliente** em **Manutenção** > Certificados de Segurança na GUI da Web. Mantenha todas as configurações padrão iguais. Selecione **Upload Test File** (formato pem) no menu suspenso e selecione o certificado do cliente que deseja verificar. Se o certificado não for confiável, você receberá um erro, como mostrado na imagem, que

explica o motivo da rejeição. O erro que você vê são as informações decodificadas do certificado carregado para referência.



Se você receber um erro que alegue que o Expressway não pode obter a CRL de certificado, mas o Expressway não usa a verificação de CRL, isso significa que o certificado seria confiável e passou em todas as outras verificações.



Endpoints Synergy Light (telefones 7800/8800 Series)

Esses novos dispositivos vêm com uma lista de certificados confiáveis pré-preenchida, que inclui um grande número de CAs públicas bem conhecidas. Esta lista confiável não pode ser modificada, o que significa que seu certificado do Expressway-E DEVE ser assinado por uma dessas CAs públicas correspondentes para funcionar com esses dispositivos. Se ele for assinado por uma CA interna ou uma CA pública diferente, a conexão falhará. Não há opção para o usuário aceitar manualmente o certificado como há com os clientes Jabber.

> **Observação**: em algumas implantações, descobriu-se que o uso de um dispositivo, como um Citrix NetScaler com uma CA da lista incluída nos 7800/8800 Series Phones, pode ser registrado em MRA, mesmo que o Expressway-E use uma CA interna. A CA raiz do NetScalers precisa ser carregada para o Expressway-E, e a CA raiz interna precisa ser carregada para o Netscaler para que a autenticação SSL funcione. Demonstrou-se que isso funciona e é o suporte de melhor esforço.

> **Observação**: se a lista de CAs confiáveis parecer ter todos os certificados corretos, mas ainda assim for rejeitada, verifique se não há outro certificado no topo da lista com o mesmo assunto que possa entrar em conflito com o correto. Quando tudo falhar, você sempre poderá exportar a cadeia diretamente do navegador ou do Wireshark e carregar todos os certificados para a lista de CAs dos

---

servidores opostos. Isso garantiria que ele fosse o certificado confiável.

Observação: quando você soluciona um problema de zona de passagem, às vezes o problema pode parecer relacionado a um certificado, mas na verdade é algo do lado do software. Certifique-se de que o nome de usuário e a senha usada na passagem estão corretos.

Observação: o VCS ou Expressway não suporta mais de 999 caracteres no campo SAN de um certificado. Todas as SANs que ultrapassarem esse limite (o que requer vários nomes alternativos) serão ignoradas como se não estivessem lá.

Recursos de vídeo

Esta seção fornece informações no vídeo que podem guiá-lo por todos os processos de configuração do Certificado.

Gerar um CSR para MRA ou Expressways em cluster

Instalar Certificado de Servidor no Expressway

Como configurar a confiança de certificado entre Expressways

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.