

Navegar no cliente ECU Sunset com Expressway x15.5

Introdução

Este documento descreve a navegação no cliente ECU sunset com o Cisco Expressway x15.5.

Informações de Apoio

Os certificados digitais são credenciais eletrônicas emitidas por Autoridades de Certificação (CAs) confiáveis que protegem a comunicação entre servidores e clientes, garantindo a autenticação, a integridade dos dados e a confidencialidade. Estes certificados contêm campos de Uso Estendido de Chave (EQU) que definem sua finalidade:

- EQU de Autenticação do Servidor (id-kp-serverAuth) é usado quando um servidor apresenta seu certificado para comprovar a identidade.
- O EQU de autenticação do cliente (id-kp-clientAuth) é usado em conexões TLS mútuas (mTLS) onde ambas as partes se autenticam.

Tradicionalmente, um único certificado pode conter EQUs de Autenticação de Servidor e de Cliente, permitindo que ele sirva a duas finalidades. Isso é particularmente importante para produtos como o Cisco Expressway que atuam como servidor e cliente em diferentes cenários de conexão.

Definição do problema

Mudança de política do programa Chrome Root

A partir de junho de 2026, a Política do programa raiz do Chrome restringe os certificados de Autoridade de certificação raiz (CA) incluídos no Chrome Root Store, eliminando gradualmente as raízes multiuso para alinhar todas as hierarquias de infraestrutura de chave pública (PKI) para servir apenas casos de uso de autenticação de servidor TLS.

Principais requisitos da política

- As CAs de raiz públicas devem declarar Uso Estendido de Chave (EKU) SOMENTE para Autenticação de Servidor (id-kp-serverAuth).
- É proibido incluir EKU de Autenticação de Cliente nesses certificados.
- Não há mais CAs raiz de uso misto para certificados TLS de servidor público.
- Cronograma de aplicação: Junho de 2026

Cronograma de Resposta de CA Pública

- outubro de 2025: Muitas CAs públicas (DigiCert, Sectigo, SSL) começaram a emitir certificados somente de servidor por padrão.
- Maio de 2026: Os servidores públicos de CA param de emitir certificações EKU de Autenticação de Cliente
- Junho de 2026: A política do programa Chrome Root torna-se totalmente eficaz



Note: Esta política se aplica somente a certificados emitidos por autoridades de certificação públicas. PKI particular e certificados autoassinados não são afetados por esta política.

Se você estiver interessado em ler sobre o impacto do desligamento do EKU do cliente no Expressways, consulte [Preparar o Expressway para o Desligamento do EKU de Autenticação do Cliente em Certificados CA Públicos](#).

Expressway versão x15.5 com solução

Expressway x15.5

O Expressway x15.5 vem com uma correção proposta para um problema que surge devido ao desligamento do EKU do cliente por todas as autoridades de certificação públicas. Esse é um problema global e afeta todos os fornecedores/implantações que optam por usar certificados PKI públicos.

x15.4, uma versão anterior, tinha um switch de comando CLI que permitia que o administrador carregasse o certificado somente EKU de servidor (nenhum EKU de cliente presente) no Expressway E.

EnableServerEkuUpload de CVS de certificado TLS XCP xConfiguration: Ligado



Note: Este comando foi preterido em x15.5.

Adição de Repositório de Certificados X15.5

O x15.5 tem dois armazenamentos de certificados:

1. Repositório de certificados do servidor
2. Repositório de certificados do cliente


Expressways (Nic única ou Nic dupla): Ambas as interfaces Expressway podem usar 2 armazenamentos de certificados conforme necessário.


Exemplo:


- Quando o expressway atua como um cliente durante o handshake TLS, o certificado do cliente é apresentado.
- Quando o expressway atua como servidor durante o handshake TLS, o certificado do servidor é apresentado.





Note: Ambos os armazenamentos de certificados (Cliente e Servidor) usam a mesma biblioteca de CAs confiáveis. Verifique se a autoridade de certificação que assinou os certificados de servidor e cliente está carregada corretamente no repositório Confiável. Os logs de diagnóstico agora incluem o certificado do servidor e o certificado do cliente no formato de arquivo PEM.


 ca_vcs8c_2026-03-25_03_20_11.pem


 client_vcs8c_2026-03-25_03_20_11.pem


 eth0_diagnostic_logging_tcpdump00_vcs8c_2026-03-25_03_20_11.pcap

 loggingsnapshot_vcs8c_2026-03-25_03_20_11.txt

 server_vcs8c_2026-03-25_03_20_11.pem

 xconf_dump_vcs8c_2026-03-25_03_20_11.txt

 xconf_dump_vcs8c_2026-03-25_03_20_11.xml

 xstat_dump_vcs8c_2026-03-25_03_20_11.txt

 xstat_dump_vcs8c_2026-03-25_03_20_11.xml

Atualização de X15.4 ou versão anterior para X15.5

Quando uma atualização é executada, o certificado do servidor de x15.4 ou versão anterior, o armazenamento de certificados do servidor Expressway é copiado para o armazenamento de certificados do cliente em x15.5. Os armazenamentos de certificados do cliente e do servidor em x15.5 têm o mesmo certificado.

Exemplo com capturas de tela

Servidor Expressway na versão 15.4, Número de Série do certificado do servidor atual
46:df:76:aa:00:00:00:00:29

Certificado:

Versão: 3 (0x2)

Número de série:

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

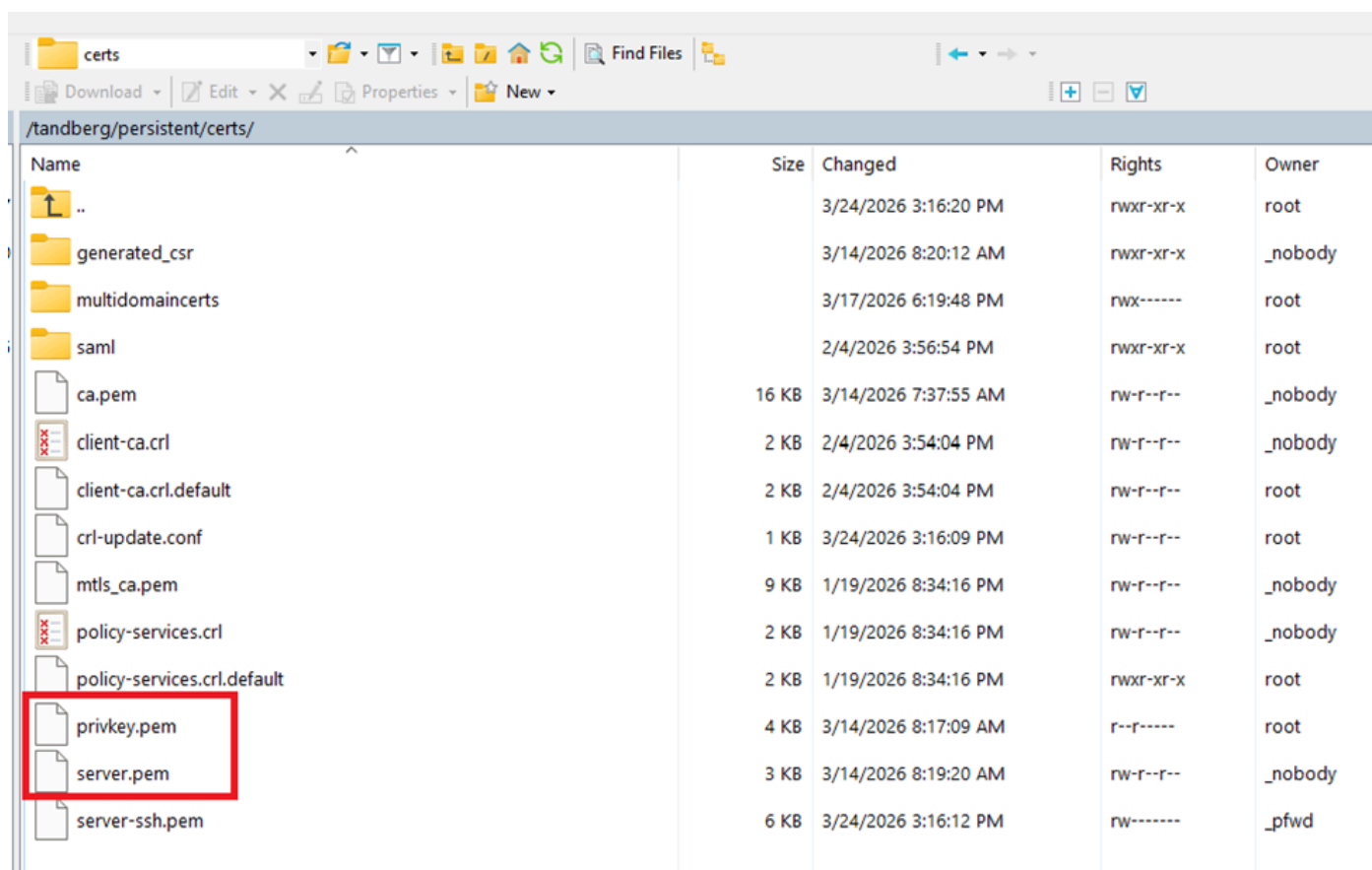
Validade

Não Antes: Mar 14 02:37:40 2026 GMT

Não depois de: Mar 14 02:47:40 2028 GMT

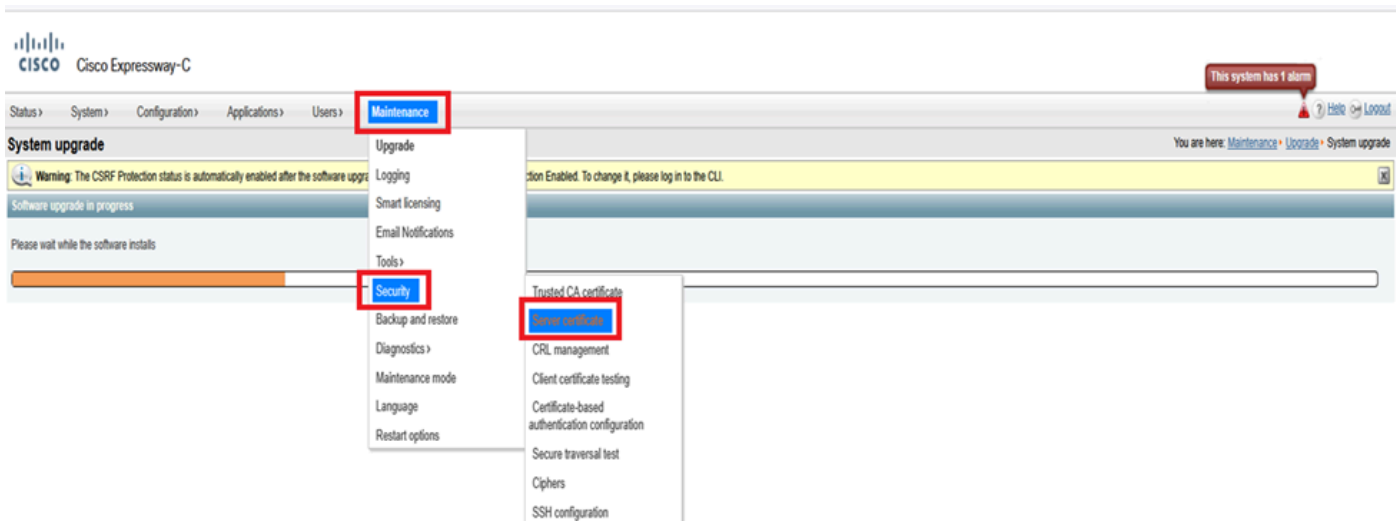
Assunto: C = IN, ST = KA, L = KA, O = Cisco, OU = TAc, CN = cluster.s.com

Diretório persistente/certificado do sistema de arquivos Expressway em x15.4:



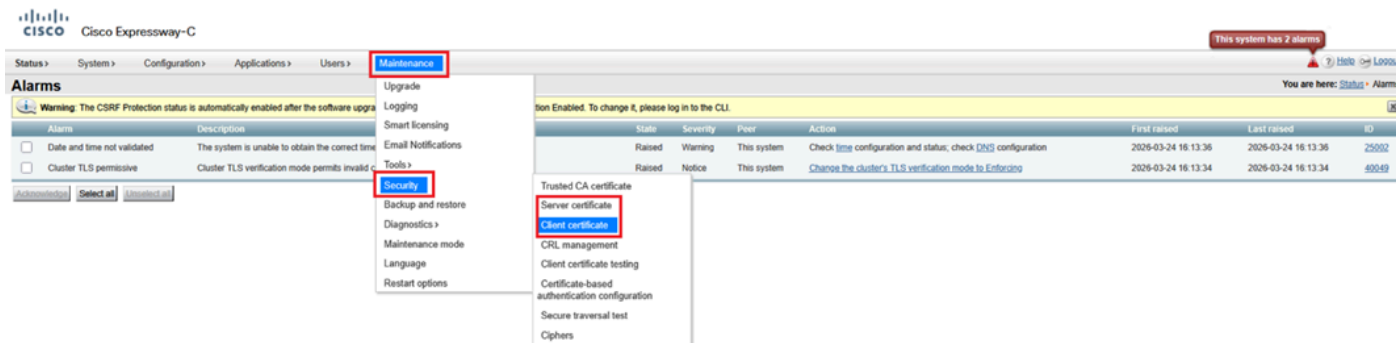
Name	Size	Changed	Rights	Owner
..		3/24/2026 3:16:20 PM	nwxr-xr-x	root
generated_csr		3/14/2026 8:20:12 AM	nwxr-xr-x	_nobody
multidomaincerts		3/17/2026 6:19:48 PM	nwx-----	root
saml		2/4/2026 3:56:54 PM	nwxr-xr-x	root
ca.pem	16 KB	3/14/2026 7:37:55 AM	nw-r--r--	_nobody
client-ca.crl	2 KB	2/4/2026 3:54:04 PM	nw-r--r--	_nobody
client-ca.crl.default	2 KB	2/4/2026 3:54:04 PM	nw-r--r--	root
crl-update.conf	1 KB	3/24/2026 3:16:09 PM	nw-r--r--	root
mtls_ca.pem	9 KB	1/19/2026 8:34:16 PM	nw-r--r--	_nobody
policy-services.crl	2 KB	1/19/2026 8:34:16 PM	nw-r--r--	_nobody
policy-services.crl.default	2 KB	1/19/2026 8:34:16 PM	nwxr-xr-x	root
privkey.pem	4 KB	3/14/2026 8:17:09 AM	r--r-----	root
server.pem	3 KB	3/14/2026 8:19:20 AM	nw-r--r--	_nobody
server-ssh.pem	6 KB	3/24/2026 3:16:12 PM	nw-----	_pfwd

Menu Expressway (Manutenção > Segurança > Certificado do servidor) em x15.4 (apenas campo de certificado do servidor presente):



Após a atualização bem-sucedida para x15.5

Aqui, você vê 2 opções de certificado em Manutenção > Segurança > certificado do cliente e certificados do servidor. Após a atualização para x15.5, os portais de certificado do servidor e do cliente na administração da Web mostram o mesmo certificado porque o certificado do servidor de x15.4 foi copiado para o armazenamento de certificados do cliente em x15.5.



O certificado e a chave privada existentes após a atualização para x15.5 foram copiados para o armazenamento de certificados do cliente.

Diretório persistente/certificado do sistema de arquivos Expressway em x15.5:

Name	Size	Changed
..		3/24/2026 4:13:44 PM
generated_csr		3/14/2026 8:20:12 AM
multidomaincerts		3/17/2026 6:19:48 PM
saml		3/24/2026 4:12:43 PM
ca.pem	16 KB	3/14/2026 7:37:55 AM
client.pem	3 KB	3/24/2026 4:12:46 PM
client-ca.crl	2 KB	2/4/2026 3:54:04 PM
client-ca.crl.default	2 KB	2/4/2026 3:54:04 PM
clientprivkey.pem	4 KB	3/24/2026 4:12:46 PM
client-ssh.pem	6 KB	3/24/2026 4:13:37 PM
crl-update.conf	1 KB	3/24/2026 4:13:34 PM
mtls_ca.pem	9 KB	1/19/2026 8:34:16 PM
policy-services.crl	2 KB	1/19/2026 8:34:16 PM
policy-services.crl.default	2 KB	1/19/2026 8:34:16 PM
privkey.pem	4 KB	3/14/2026 8:17:09 AM
server.pem	3 KB	3/14/2026 8:19:20 AM
server-ssh.pem	6 KB	3/24/2026 4:13:37 PM

Verificação de ECU X15.5 durante handshake TLS

Em x15.5, um novo comando CLI foi introduzido para verificar o uso estendido de chave (EKU - Extended Key Usage) durante o handshake TLS. O valor padrão é "LIGADO". O conjunto de comandos é válido em Expressway Core e Edge.

O conjunto de comandos aciona uma verificação de todas as conexões SIP TLS de ENTRADA no Expressway. (saudações/certificado de cliente de entrada apresentado). Quando ativada, esta opção verifica se o certificado apresentado pelo iniciador TLS contém ou não ECU de cliente no certificado. SE DESLIGADO, a verificação é ignorada; no entanto, o ECU do servidor é verificado se ele está presente no certificado.

Modo de Verificação ExtendedKeyUsage do Certificado TLS SIP do xconfiguration:
LIGAR/DESLIGAR:



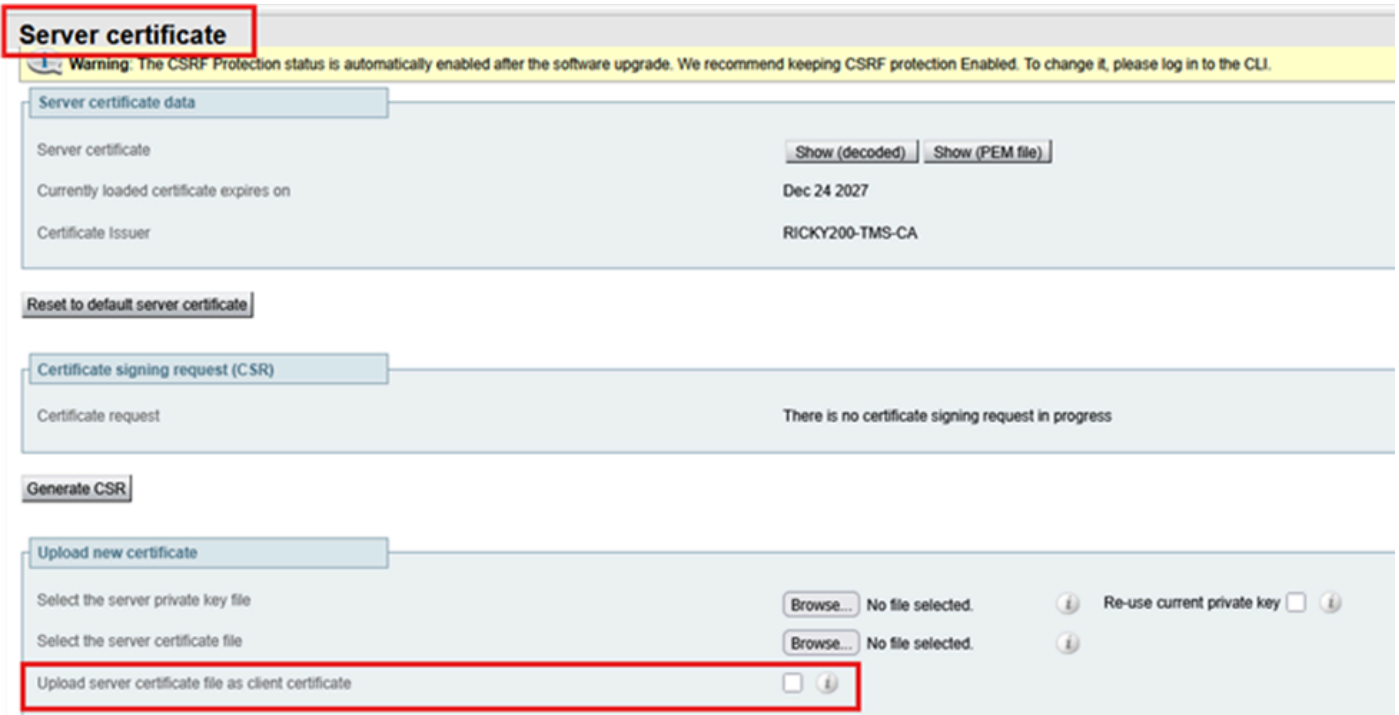
Note: Se você gerar um certificado de cliente, assinando um CSR que não contenha EKU de cliente (um exemplo de certificado assinado por uma CA pública), não será possível carregar esse certificado manualmente no armazenamento de certificados de cliente. Portanto, você precisa garantir que os certificados gerados pela assinatura de um CSR sempre contenham o EKU do cliente (uma CA privada pode ser usada para inserir o EKU do cliente).



Tip: Esse erro fica evidente quando você tenta carregar um certificado assinado CSR, que não tem o EKU do cliente, no repositório de certificados do cliente.

The screenshot shows the Cisco Expressway-E web interface. At the top left is the Cisco logo and the text "Cisco Expressway-E". Below this is a navigation menu with items: Status >, System >, Configuration >, Applications >, Users >, and Maintenance >. The main heading is "Client certificate". Below the heading, there is a yellow warning box with an information icon and the text: "Invalid certificate: The file provided does not have a client usage attribute. Services requiring mutual TLS may not work." Below this is another yellow warning box with an information icon and the text: "Warning: The CSRF Protection status is automatically enabled after the software upgrade. We recommend keeping CSRF protection Enabled. To change it, please log in to the CLI." At the bottom, there is a blue button labeled "Client certificate data".

No entanto, se você optar por carregar um certificado que tenha apenas um EKU de servidor (sem EKU de cliente) através do armazenamento de certificados do servidor e selecionar Carregar arquivo de certificado do servidor como certificado de cliente, o certificado será copiado para o armazenamento de certificados do cliente. Os administradores que não desejam usar um certificado assinado por uma CA privada no Expressway-Edge podem optar por copiar a EKU do servidor somente do armazenamento de certificados do servidor para o armazenamento de certificados do cliente.



Vários armazenamentos de certificados, vários cenários de implantação

Como agora há dois armazenamentos de certificados no Expressway, há vários cenários de armazenamentos de certificados.

Condição 1: Atualização

Quando o Expressway é atualizado de x15.4 ou anterior a x15.5, essa condição é verdadeira. Os certificados existentes da versão x15.4 são copiados em dois (2) armazenamentos de certificados. No cliente e no servidor x15.5, os certificados são os mesmos.

Exp C x15.5

Client cert = Certificate copied from server certificate store
 Server cert = Certificate carried forward from x15.4 post upgrade
 Where: Server certificate = Client certificate

Exp E x15.5

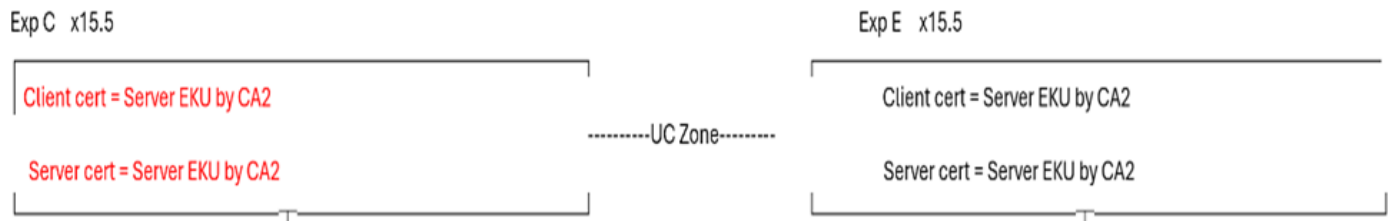
Client cert = Certificate copied from server cert store
 Server cert = Certificate carried forward from x15.4 post upgrade
 Where: Server certificate = Client certificate

Condição 2: Quando o administrador instala um novo certificado em x15.5 (certificados existentes expirados)

CA 1 = CA interna

CA 2 = CA pública

Na figura a seguir, o Expressway Core tem um certificado de cliente com EKU de servidor assinado somente por CA 2 (CA pública) e um certificado de servidor com EKU de servidor assinado somente por CA 2 (CA pública). Da mesma forma, o Expressway E tem um certificado de cliente com o servidor EKU assinado por CA2 (CA pública) e um certificado de servidor com o servidor EKU assinado somente por CA 2 (CA pública).



Se o certificado do servidor núcleo Expressway não tiver um EKU de cliente, zona de passagem de comunicações unificadas, MRA, o proxy WebRTC não funcionará. Certifique-se de que o certificado do servidor núcleo Expressway tenha um EKU cliente. Este é um caso de uso comum em que os usuários optam por assinar todos os certificados de uma CA pública. Como a CA pública não inclui o EKU do cliente em certificados, a zona de passagem de comunicações unificadas se torna ativa.

Para tornar a zona UC ativa, uma correção rápida é desativar a verificação de EKU no Expressway E. Isso ativa a zona de UC. No entanto, os túneis SSH permanecem inativos. A partir de hoje, a comunicação do túnel SSH no 2222 requer a validação do EKU cliente.

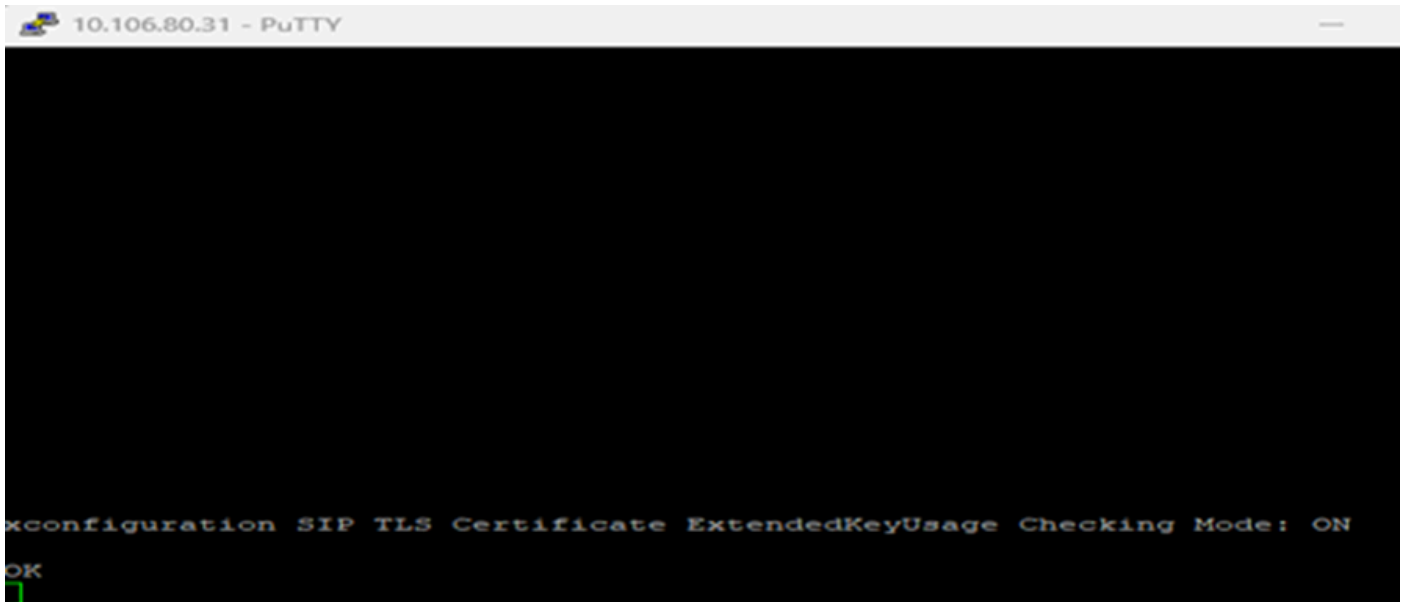
O logon do cliente MRA e as funções proxy WebRTC não funcionam. Você poderia ter que recorrer a CA privada.

Caso de teste 1

- Quando a verificação EKU está "ON" no Expressway E
- Quando o certificado de Cliente e Servidor no núcleo do Expressway tem somente EKU de Servidor
- O status da zona UC é FALHA

Em Expressway-Edge ExtendedKeyUsage, verifique ON.

Modo de Verificação ExtendedKeyUsage do Certificado TLS SIP do xconfiguration: Ligado:



Falha na zona de comunicação unificada:



Os logs do Expressway E mostram onde 10.106.80.16 = Expressway Core, 10.106.80.31 = Expressway Edge:



Caso de teste 2

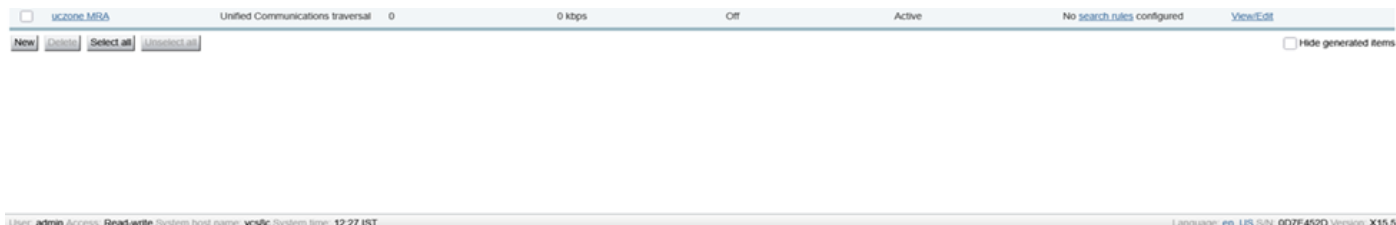
- Quando a verificação EKV está DESATIVADA no Expressway E
- Quando o certificado de Cliente e Servidor no Expressway Core tiver somente EKV de servidor
- O status da zona UC é ATIVO

Desative a verificação de EKV no Expressway E.

Modo de Verificação ExtendedKeyUsage do Certificado TLS SIP do xconfiguration: Off

```
10.106.80.31 - PuTTY
xconfiguration SIP TLS Certificate ExtendedKeyUsage Checking Mode: Off
OK
```

Zona de comunicação unificada ativa:



No entanto, os túneis ssh ainda falharam:

Unified Communications SSH tunnels status

Target	Domain	Status	Tunnel Created	Reason	Peer
smartslave.vikdutta.com	555.federation.com	Failed	29/03/2026 07:09:26	Permission denied	10.106.80.16
smartslave.vikdutta.com	tomcat.com	Failed	29/03/2026 07:09:26	Permission denied	10.106.80.16

Logs de eventos do Expressway:

Results

2026-03-29T12:33:12.384+05:30	ssh: Detail="ssh: connect to host smartslavsmarts 22222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:31:56.811+05:30	ssh: Detail="ssh: connect to host smartslavsmarts 22222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:28:56.519+05:30	ssh: Detail="ssh: connect to host smartslavsmarts 22222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:28:24.476+05:30	ssh: Detail="ssh: connect to host smartslavsmarts 22222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:27:52.445+05:30	ssh: Detail="ssh: connect to host smartslavsmarts 22222:port 2222: Connection timed out" Level="ERROR"

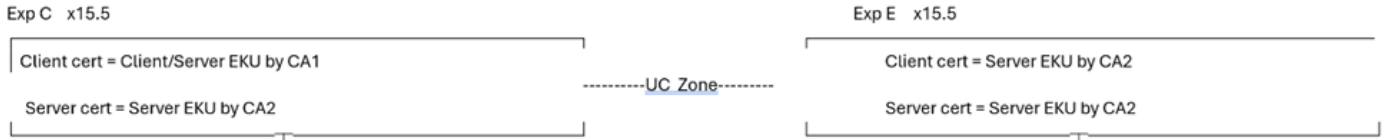
Condição 2.1: Caso de sucesso

CA 1 = CA interna

CA 2 = CA pública

- Onde o certificado de cliente principal do Expressway é assinado pela CA 1 (CA interna) e inclui, EKU cliente/servidor ambos.
- O certificado do servidor núcleo Expressway é assinado por CA 2 pública e inclui somente EKU de servidor.

- O certificado do Servidor de Borda do Expressway é assinado pela CA 2 pública e inclui somente a ECU do Servidor.
- O certificado do cliente de Borda do Expressway é assinado pela CA 2 pública e inclui somente ECU do Servidor.



Essa condição é um caso de sucesso. Independentemente de o modo de verificação ECU ser ON/OFF, a zona de Comunicação Unificada e o túnel SSH se tornam ativos. Os clientes MRA funcionam.

Não importa se a verificação de ECU de borda do Expressway está DESATIVADA ou ATIVADA. O certificado de cliente principal do Expressway contém ECU de cliente:

```
10.106.80.31 - PuTTY
xconfiguration SIP TLS Certificate ExtendedKeyUsage Checking Mode: Off
OK
```

```
10.106.80.31 - PuTTY
xConfiguration SIP TLS Certificate ExtendedKeyUsage Checking Mode: "On"
OK
```

Túneis SSH no núcleo do Expressway Ativos:

CISCO Cisco Expressway-C

Status > System > Configuration > Applications > Users > Maintenance >

Unified Communications SSH tunnels status

Warning: The CSRF Protection status is automatically enabled after the software upgrade. We recommend keeping CSRF protection Enabled. To change it, please log in to the CLI.

Target	Domain	Status	Tunnel Created
smartslave.vikdutta.com	tomcat.com	Active	29/03/2026 07:21:27
smartslave.vikdutta.com	555.federation.com	Active	29/03/2026 07:19:26

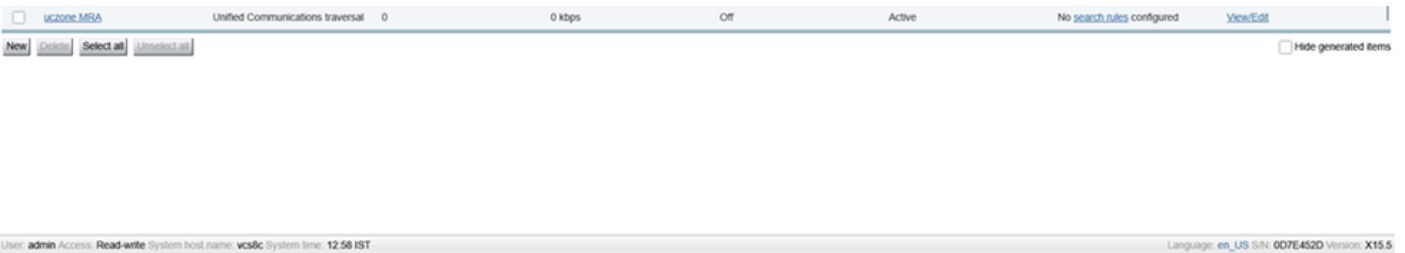
Túneis SSH na Borda do Expressway Ativos:

Unified Communications SSH tunnels status

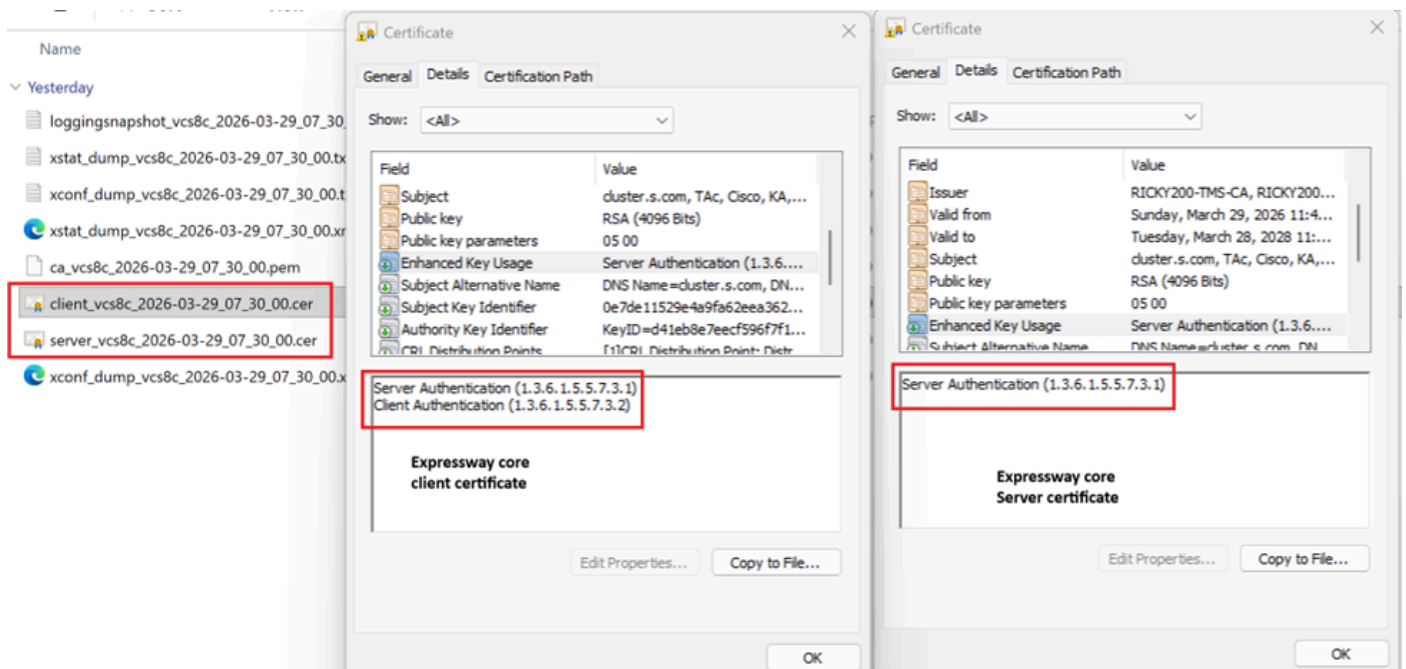
Warning: The CSRF Protection status is automatically enabled after the software upgrade. We recommend keeping CSRF protection Enabled. To change it, please log in to the CLI.

Target	Domain	Status	Tunnel Created
vcs8c	tomcat.com	Active	29/03/2026 07:21:27
vcs8c	555.federation.com	Active	29/03/2026 07:19:26

Status Ativo da Zona MRA de Comunicação Unificada:



- O certificado do cliente Expressway-Core tem ECU de servidor e ECU de cliente.
- O certificado do servidor central do Expressway tem somente ECU de servidor.



O cliente MRA faz logon e está registrado:

The screenshot shows the Cisco Jabber interface. The main window is titled "Cisco Jabber" and shows the user "hanu@". A search bar is visible. A "Connection Status" window is open, displaying the following information:

Cisco Jabber
Version 12.6.1 (284405)

✓ Softphone	Status: Connected
	Protocol: SIP
	Address: 10.106.79.162 (CCMCIP - Expressway) (IPv4)
	Device: CSFHanu
	Line: 7777
Deskphone	Status: Not connected
	Protocol: CTI
	Address: (CTI) (Unknown)
✓ Outlook address book	Status: Last connection successful.
	Protocol: MAPI
	Address: Outlook (Unknown)
✓ Directory	Status: Last connection successful.

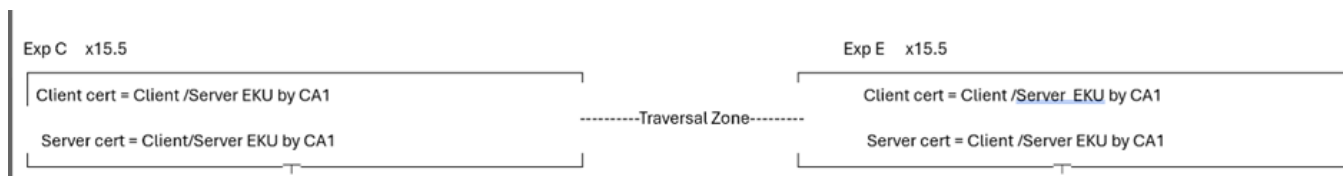


Note: Compare e anote as EKUs presentes nos certificados para que o proxy MRA e WebRTC funcionem. É uma comparação entre uma implantação funcional e uma não funcional.

Condição 3: Assina todos os certificados com uma AC privada

CA 1 = CA interna

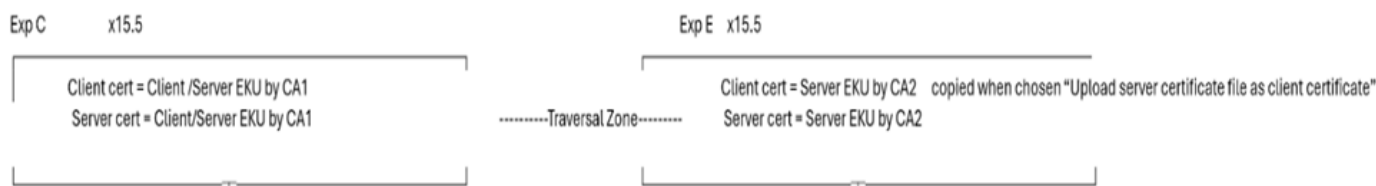
CA 2 = CA pública



Na condição 3, todos os certificados são assinados pela CA interna (CA1) .

- Quando o Expressway-E envia uma conexão TLS, a raiz/intermediário CA 1 precisa ser trocada com a entidade da extremidade oposta. Se a extremidade oposta não tiver capacidade ou não permitir que um certificado de CA privado seja carregado, a conexão TLS não será bem-sucedida.
- Os clientes MRA obtêm certificados para aceitar pop-ups se o certificado privado não estiver no armazenamento confiável do SO.

Condição 4: A Borda do Expressway tem Certificados Públicos com ECU de Servidor Somente



Na condição 4, os certificados de cliente e servidor núcleo do Expressway são (CA1) CA interna assinada e têm ECU de cliente e servidor presentes. O certificado do servidor Expressway E é uma CA pública assinada e tem somente ECU de servidor. O certificado do servidor é copiado para o repositório de certificados do cliente, escolhendo Carregar arquivo de certificado do servidor como certificado do cliente.

Na condição 4, quando a conexão TLS é feita à extremidade oposta, se o Expressway -E envia uma saudação de cliente TLS, a extremidade oposta precisa desabilitar a verificação de ECU do cliente (pois o certificado do cliente não tem ECU de autenticação do cliente) ou a conexão TLS não é bem-sucedida.

Pode haver muito mais condições ou cenários no campo com base na implantação de usuários e casos de uso, e todos não podem ser cobertos devido ao meu fluxo limitado de ideias. No entanto, os pontos a serem lembrados são:

- # SE o Expressway se tornar um cliente durante o handshake TLS, o certificado do cliente

será apresentado aos pares.

- #IF Expressway torna-se servidor durante o handshake TLS; o certificado do servidor é apresentado ao par.

Este raciocínio foi estabelecido com estes casos de testes.

Cenário 1

Para esse cenário, o Expressway apresenta o certificado do cliente durante o handshake MTLS com o Webex.

Uma chamada de vídeo para a reunião do Webex:

Exemplo de fluxo de chamada Jabber -à CUCM -à Exp Core —à Exp Edge —à Webex

10.106.80.31= Expressway Edge

163.129.37.33 = Webex

```
2026-03-24T11:54:26.106+00:00 tvcs smartslave: UTCTime="2026-03-24 11:54:26,106"  
Module="network.sip" Level="DEBUG": Action="Enviado" Local-ip="10.106.80.31" Local-  
port="25002" Dst-ip="163.129.37.33" Dst-port="5061"
```

Expressway Edge tem certificado de cliente com esse número de série
(2f0000004c869c77c8981becde0000000004c).

O Expressway Edge envia hello do cliente para o "Webex durante a negociação TLS e, em seguida, envia o certificado do cliente.

Número de série 2f0000004c869c77c8981becde0000000004c:

1. Expressway Edge envia hello do cliente (pkt= 13699) para 'Webex durante a negociação mTLS.
2. O Webex envia um hello de servidor para Expressway Edge (pkt=13701).
3. Webex envia seu certificado para Expressway Edge (pkt=13711).

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

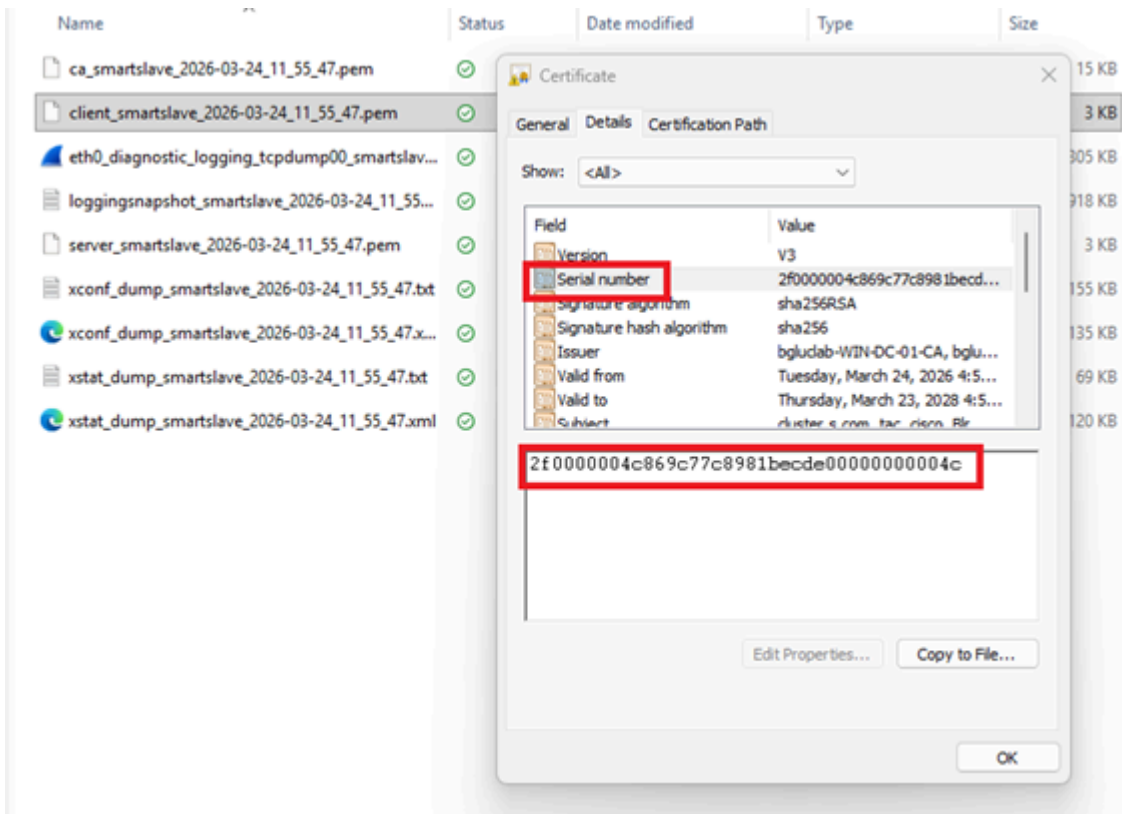
5. Expressway Edge envia seu certificado para o Webex (pkt=13718).

(captura de tela)

```
13698 2026-03-24 17:25:20.911700 10.106.80.31 163.129.37.32 TCP 66 25003 -> 5061 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=840949379 TSecr=3608271288
13699 2026-03-24 17:25:20.912773 10.106.80.31 163.129.37.32 TLSv1.2 503 Client Hello
13700 2026-03-24 17:25:20.956092 163.129.37.32 10.106.80.31 TCP 66 25003 -> 5061 [ACK] Seq=1 Ack=518 Win=28544 Len=0 TSval=3608271312 TSecr=840949380
13701 2026-03-24 17:25:20.956925 163.129.37.32 10.106.80.31 TLSv1.2 356 Server Hello
13702 2026-03-24 17:25:20.956963 10.106.80.31 163.129.37.32 TCP 66 25003 -> 5061 [ACK] Seq=518 Ack=91 Win=64512 Len=0 TSval=840949424 TSecr=3608271313
13703 2026-03-24 17:25:20.957044 163.129.37.32 10.106.80.31 TCP 1308 5061 -> 25003 [ACK] Seq=91 Ack=518 Win=28544 Len=1242 TSval=3608271313 TSecr=840949380 [TCP PDU reassembled in 13711]
13704 2026-03-24 17:25:20.957049 10.106.80.31 163.129.37.32 TCP 66 25003 -> 5061 [ACK] Seq=518 Ack=1333 Win=67584 Len=0 TSval=840949425 TSecr=3608271313
13705 2026-03-24 17:25:20.957163 163.129.37.32 10.106.80.31 TCP 1308 5061 -> 25003 [ACK] Seq=1333 Ack=518 Win=28544 Len=1242 TSval=3608271313 TSecr=840949380 [TCP PDU reassembled in 13711]
13706 2026-03-24 17:25:20.957170 10.106.80.31 163.129.37.32 TCP 66 25003 -> 5061 [ACK] Seq=518 Ack=2575 Win=70656 Len=0 TSval=840949425 TSecr=3608271313
13707 2026-03-24 17:25:20.957175 163.129.37.32 10.106.80.31 TCP 1308 5061 -> 25003 [ACK] Seq=2575 Ack=518 Win=28544 Len=1242 TSval=3608271313 TSecr=840949380 [TCP PDU reassembled in 13711]
13708 2026-03-24 17:25:20.957179 10.106.80.31 163.129.37.32 TCP 66 25003 -> 5061 [ACK] Seq=518 Ack=3817 Win=72704 Len=0 TSval=840949425 TSecr=3608271313
13709 2026-03-24 17:25:20.957184 163.129.37.32 10.106.80.31 TCP 1308 5061 -> 25003 [ACK] Seq=3817 Ack=518 Win=28544 Len=1242 TSval=3608271313 TSecr=840949380 [TCP PDU reassembled in 13711]
13710 2026-03-24 17:25:20.957188 10.106.80.31 163.129.37.32 TCP 66 25003 -> 5061 [ACK] Seq=518 Ack=5059 Win=71680 Len=0 TSval=840949425 TSecr=3608271313
13711 2026-03-24 17:25:20.957193 163.129.37.32 10.106.80.31 TLSv1.2 378 Certificate
13712 2026-03-24 17:25:20.957215 10.106.80.31 163.129.37.32 TCP 66 25003 -> 5061 [ACK] Seq=518 Ack=5371 Win=72704 Len=0 TSval=840949425 TSecr=3608271313
13713 2026-03-24 17:25:20.958101 163.129.37.32 10.106.80.31 TLSv1.2 404 Server Key Exchange
13714 2026-03-24 17:25:20.958110 10.106.80.31 163.129.37.32 TCP 66 25003 -> 5061 [ACK] Seq=518 Ack=5709 Win=73728 Len=0 TSval=840949426 TSecr=3608271314
13715 2026-03-24 17:25:20.958341 163.129.37.32 10.106.80.31 TLSv1.2 124 Certificate Request, Server Hello Done
13716 2026-03-24 17:25:20.958350 10.106.80.31 163.129.37.32 TCP 66 25003 -> 5061 [ACK] Seq=518 Ack=5767 Win=73728 Len=0 TSval=840949426 TSecr=3608271315
13717 2026-03-24 17:25:20.967607 10.106.80.31 163.129.37.32 TCP 2550 25003 -> 5061 [PSH, ACK] Seq=518 Ack=5767 Win=73728 Len=2484 TSval=840949435 TSecr=3608271315 [TCP PDU reassembled in 13718]
13718 2026-03-24 17:25:20.967797 10.106.80.31 163.129.37.32 TLSv1.2 1170 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
13719 2026-03-24 17:25:20.971327 10.106.80.31 10.106.80.31 TCP 66 5061 -> 25003 [ACK] Seq=5767 Ack=3002 Win=26112 Len=0 TSval=3608271365 TSecr=840949435
13720 2026-03-24 17:25:21.008884 163.129.37.32 10.106.80.31 TCP 66 5061 -> 25003 [ACK] Seq=5767 Ack=3002 Win=26112 Len=0 TSval=3608271365 TSecr=840949435
13721 2026-03-24 17:25:21.010881 163.129.37.32 10.106.80.31 TLSv1.2 72 Change Cipher Spec
```

```
Length: 2936
Certificates Length: 2933
Certificates (2933 bytes)
Certificate Length: 2834
Certificate [..]: 308207ee3082066de0030201020123f0000004c869c77c8981becde0000000004c300006092a864886f7000101000500304f31133011060e0992268993f22c6401191603636f6d3118301606
signedCertificate
  version: v3 (2)
  serialNumber: 0x2f0000004c869c77c8981becde0000000004c
  signature (sha256withRSAEncryption)
  issuer: rdnsSequence (0)
  rdnsSequence: 3 items (id-at-commonName=bgluclab-WIN-DC-01-CA,dc=bgluclab,dc=com)
    rdnsSequence item: 1 item (dc=com)
    rdnsSequence item: 1 item (dc=bgluclab)
    rdnsSequence item: 1 item (id-at-commonName=bgluclab-WIN-DC-01-CA)
  validity
    notBefore: utcTime (0)
    notAfter: utcTime (0)
  subject: rdnsSequence (0)
```

Certificado de cliente da Borda do Expressway:



Cenário 2

O Expressway torna-se uma entidade de servidor durante o handshake mTLS e apresenta seu certificado de servidor:

Onde o Expressway apresenta o certificado do servidor, o Expressway tem uma zona de vizinho segura sobre 5061 com o nome de verificação LIGADO.

Zona vizinha segura entre o nó Expressway x15.5 e o nó Expressway x8.11.4:

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)

732	2026-03-25 15:10:17.833251	10.106.80.16	10.106.80.15	TCP	74 5061 → 29457 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=4070042683 TSecr=2013756904 WS=512
733	2026-03-25 15:10:17.833259	10.106.80.15	10.106.80.16	TCP	66 29457 → 5061 [ACK] Seq=1 Ack=1 Min=29312 Len=0 TSval=2013756905 TSecr=4070042683
736	2026-03-25 15:10:17.870548	10.106.80.15	10.106.80.16	TLSv1.2	276 Client Hello
737	2026-03-25 15:10:17.871031	10.106.80.16	10.106.80.15	TCP	66 5061 → 29457 [ACK] Seq=1 Ack=211 Min=65024 Len=0 TSval=4070042721 TSecr=2013756942
738	2026-03-25 15:10:17.878936	10.106.80.16	10.106.80.15	TLSv1.2	1514 Server Hello
739	2026-03-25 15:10:17.878955	10.106.80.15	10.106.80.16	TCP	66 29457 → 5061 [ACK] Seq=211 Ack=1449 Min=32128 Len=0 TSval=2013756950 TSecr=4070042729
740	2026-03-25 15:10:17.878964	10.106.80.16	10.106.80.15	TCP	1514 5061 → 29457 [ACK] Seq=1449 Ack=211 Min=65024 Len=1448 TSval=4070042729 TSecr=2013756942 [TCP PDU reassembled in 742]
741	2026-03-25 15:10:17.878968	10.106.80.15	10.106.80.16	TCP	66 29457 → 5061 [ACK] Seq=211 Ack=2097 Min=32128 Len=0 TSval=2013756950 TSecr=4070042729
742	2026-03-25 15:10:17.878969	10.106.80.16	10.106.80.15	TLSv1.2	830 Certificate, Server Key Exchange, Certificate Request, Server Hello Done
743	2026-03-25 15:10:17.878972	10.106.80.15	10.106.80.16	TCP	66 29457 → 5061 [ACK] Seq=211 Ack=3601 Min=37888 Len=0 TSval=2013756950 TSecr=4070042729
744	2026-03-25 15:10:17.887137	10.106.80.15	10.106.80.16	TLSv1.2	3560 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
745	2026-03-25 15:10:17.887300	10.106.80.16	10.106.80.15	TCP	66 5061 → 29457 [ACK] Seq=3661 Ack=3705 Win=69632 Len=0 TSval=4070042737 TSecr=2013756958
746	2026-03-25 15:10:17.888041	10.106.80.16	10.106.80.15	TCP	1514 5061 → 29457 [ACK] Seq=3661 Ack=3705 Win=69632 Len=1448 TSval=4070042738 TSecr=2013756958 [TCP PDU reassembled in 747]
747	2026-03-25 15:10:17.888048	10.106.80.16	10.106.80.15	TLSv1.2	764 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
748	2026-03-25 15:10:17.888053	10.106.80.15	10.106.80.16	TCP	66 29457 → 5061 [ACK] Seq=3705 Ack=5807 Win=43776 Len=0 TSval=2013756959 TSecr=4070042738
749	2026-03-25 15:10:17.888437	10.106.80.15	10.106.80.16	TLSv1.2	498 Application Data


```

Length: 2923
  Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 2919
    Certificates Length: 2916
  Certificates (2916 bytes)
    Certificate Length: 2005
  Certificate [-]: 308207d1308206b9a003020102020a46df76aa00000000029300006092a864886f70d01010c0500304931133011060a0992268993f22c64011916036f6d31183016060a0992268993f22c...
  signedCertificate
    version: v3 (2)
    serialNumber: 0x46df76aa000000000029
    signature (sha384withRSAEncryption)
      Algorithm Id: 1.3.6.1.4.1.311.1.17 (sha384withRSAEncryption)
    issuer: rdnSequence (0)
      rdnSequence: 3 items (id-at-commonName=RICKY200-TMS-CA,dc=RICKY200,dc=com)
    validity
  
```

Esta captura de tela mostra o certificado do servidor quando o número de série corresponde a:

The screenshot shows a Windows File Explorer window with a list of files including 'ca_vcs8c_2026-03-25_03_20_11.pem', 'client_vcs8c_2026-03-25_03_20_11.pem', 'eth0_diagnostic_logging_tcpdump00_vcs8c_2026-03-25_03_20_11.txt', 'loggingsnapshot_vcs8c_2026-03-25_03_20_11.txt', 'server_vcs8c_2026-03-25_03_20_11.pem', 'xconf_dump_vcs8c_2026-03-25_03_20_11.txt', 'xconf_dump_vcs8c_2026-03-25_03_20_11.xml', and 'xstat_dump_vcs8c_2026-03-25_03_20_11.txt'. A 'Certificate' dialog box is open, showing the 'General' tab. The 'Serial number' field is highlighted with a red box and contains the value '46df76aa0000000000029'. Below the dialog box, the same serial number is also highlighted with a red box.

Caso de teste 3: o cliente MRA é provisionado para login e o fluxo de trabalho inclui verificação de certificado do servidor de tráfego entre o Expressway Core e o CUCM.

10.106.80.16 = Expressway Core x15.5

10.106.80.38 = CUCM

- O Exp C 16 envia uma saudação de cliente em 6972 TFTP.

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.