

Expressway x15.5でクライアントEKU Sunsetに移動する

はじめに

このドキュメントでは、Cisco Expressway x15.5を使用したクライアントEKUサンセットのナビゲーションについて説明します。

バックグラウンド情報

デジタル証明書は、信頼できる認証局(CA)によって発行される電子証明書で、認証、データの整合性、機密性を確保することによってサーバとクライアント間の通信を保護します。これらの証明書には、その目的を定義する拡張キー使用法(EKU)フィールドが含まれています。

- サーバ認証EKU(id-kp-serverAuth)は、サーバが身元を証明するために証明書を提示する場合に使用されます。
- クライアント認証EKU(id-kp-clientAuth)は、両方のパーティが互いを認証する相互TLS(mTLS)接続で使用されます。

従来、1つの証明書にサーバ認証とクライアント認証の両方のEKUを含めることができるため、二重目的で使用できます。これは、異なる接続シナリオでサーバとクライアントの両方として機能するCisco Expresswayなどの製品にとって特に重要です。

問題の定義

Chromeルートプログラムポリシーの変更

2026年6月より、Chromeルートプログラムポリシーは、Chromeルートストアに含まれるルート認証局(CA)証明書を制限し、多用途ルートを段階的に廃止して、すべての公開キーインフラストラクチャ(PKI)階層を調整し、TLSサーバ認証のユースケースのみを提供します。

主要なポリシー要件

- パブリックルートCAは、サーバ認証(id-kp-serverAuth)に対してのみ拡張キー使用法

(EKU)をアサートする必要があります。

- これらの証明書にクライアント認証EKUを含めることは禁止されています。
- パブリックサーバのTLS証明書に使用するルートCAが混在する必要がなくなりました。
- 実施スケジュール：2026年6月

パブリックCA応答のタイムライン

- 2025年10月：多くのパブリックCA(DigiCert、Sectigo、SSL)が、デフォルトでサーバ専用証明書の発行を開始しました。
- 2026年5月：パブリックCAサーバがClient Authentication EKU証明書の発行を停止
- 2026年6月：Chromeルートプログラムポリシーが完全に発効



注：このポリシーは、パブリックCAによって発行された証明書にのみ適用されます。プライベートPKIおよび自己署名証明書は、このポリシーの影響を受けません。

ExpresswayでのクライアントEKUのサンセット設定の影響については、「[パブリックCA証明書でのクライアント認証EKUのサンセットに対するExpresswayの準備](#)」を参照してください。

Expresswayリリースx15.5およびソリューション

Expressway x15.5

Expressway x15.5には、すべての公開認証局によるクライアントEKUのサンセットが原因で発生する問題の修正案が付属しています。これはグローバルな問題であり、パブリックPKI証明書の使用を選択するすべてのベンダー/導入に影響を与えます。

以前のリリースのx15.4にはCLIコマンドスイッチがあり、管理者はExpressway EにサーバEKUのみの証明書 (クライアントEKUなし) をアップロードできました。

xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload : オン



注：このコマンドはx15.5では使用されなくなりました。

X15.5証明書ストアの追加

x15.5には2つの証明書ストアがあります。

1. サーバー証明書ストア

2. クライアント証明書ストア

Expressway (シングルNicまたはデュアルNic) : どちらのExpresswayインターフェイスも、必要に応じて2つの証明書ストアを使用できます。

例 :

- TLSハンドシェイク時にExpresswayがクライアントとして動作すると、クライアント証明書が提示されます。
- TLSハンドシェイク中にExpresswayがサーバとして動作すると、サーバ証明書が提示されます。



注 : 両方の証明書ストア (クライアントとサーバ) で、同じ信頼済みCAライブラリが使用されています。サーバ証明書とクライアント証明書に署名したCAが信頼ストアに正しくアップロードされていることを確認します。 診断ログに、サーバ証明書とクライアント証明書がPEMファイル形式で含まれるようになりました。

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

X15.4以前のバージョンからX15.5へのアップグレード

アップグレードを実行すると、x15.4以前のバージョンのサーバ証明書が、x15.5のクライアント証明書ストアにExpresswayサーバ証明書ストアがコピーされます。x15.5上のクライアント証明書ストアとサーバ証明書ストアは同じ証明書を持ちます。

スクリーンショットの例

15.4上のExpresswayサーバ、現在のサーバ証明書シリアル番号46:df:76:aa:00:00:00:00:00:29

証明書:

バージョン : 3(0x2)

シリアル番号:

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

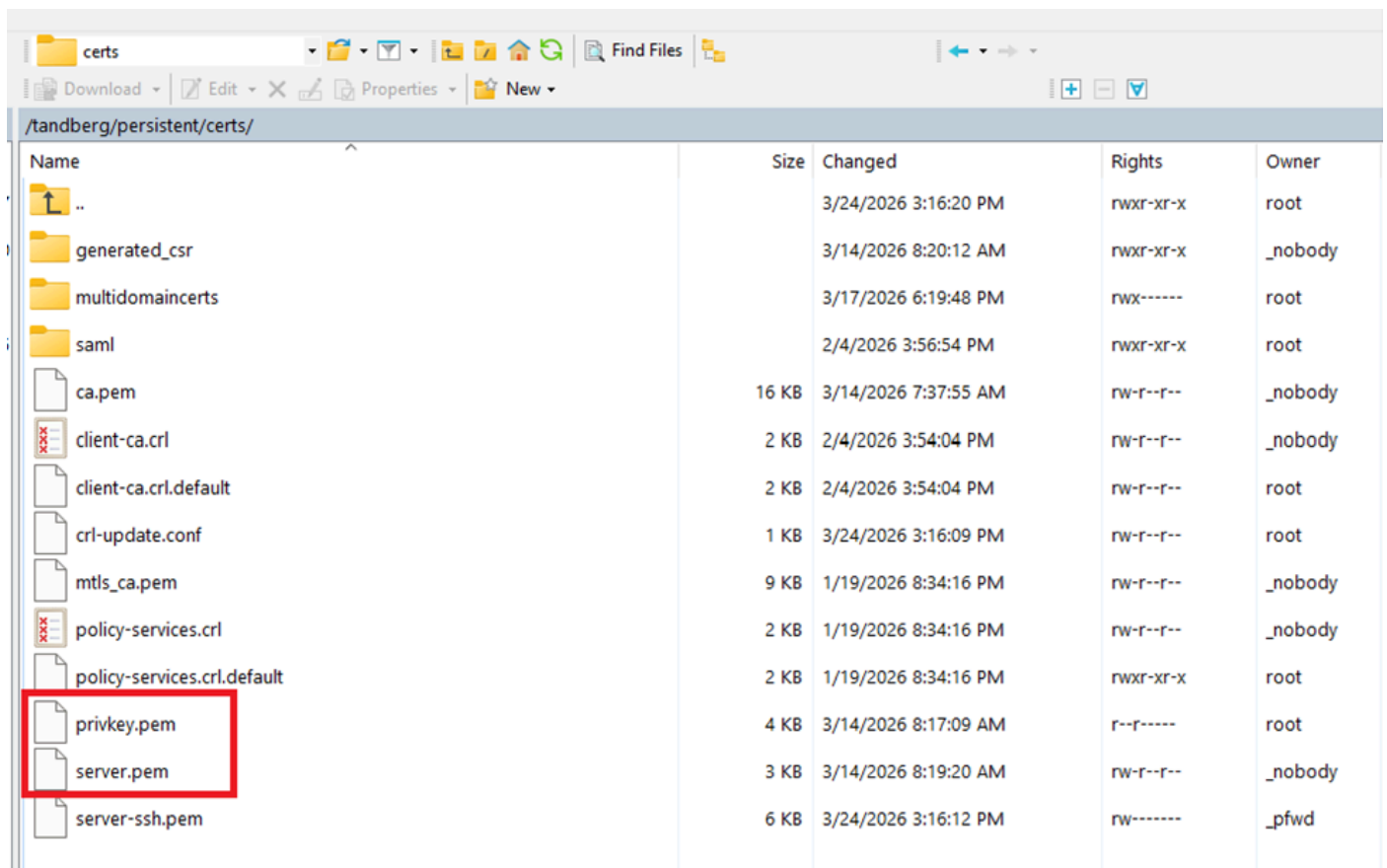
有効性

指定日以前 : 3月14日02:37:40 2026 GMT

Not After : 3月14日02:47:40 2028 GMT

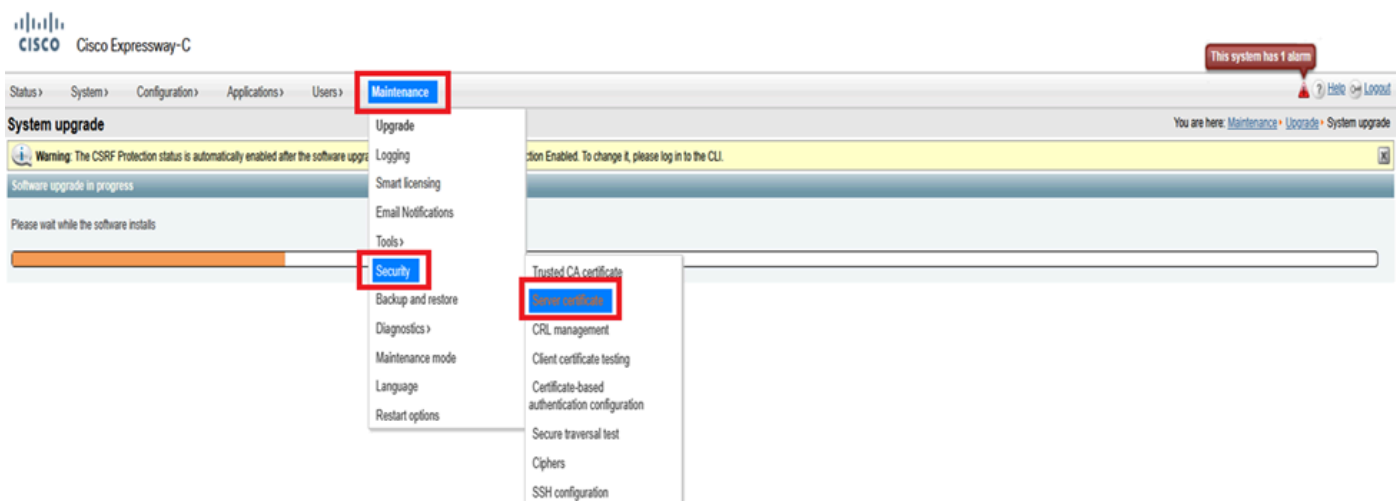
件名 : C = IN、ST = KA、L = KA、O = Cisco、OU = TAc、CN = cluster.s.com

x15.4上のExpresswayファイルシステムの永続的な/証明書ディレクトリ :



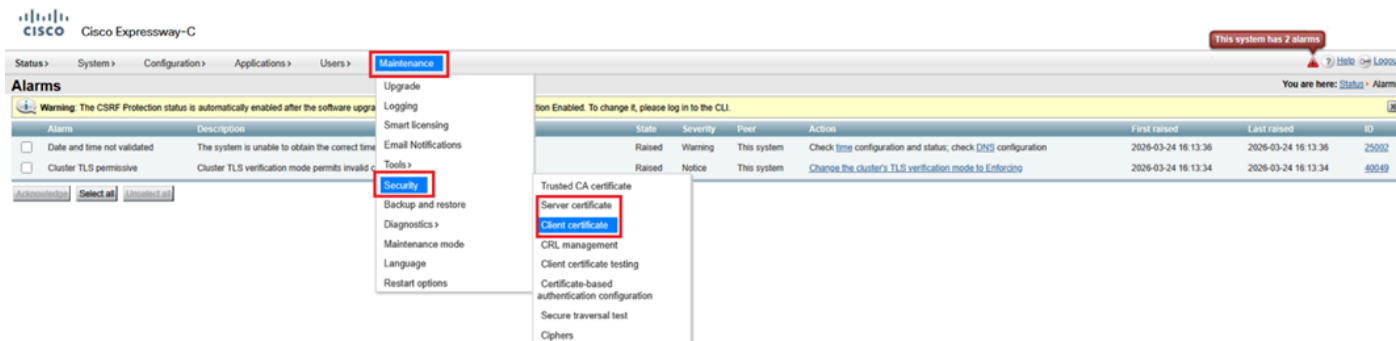
Name	Size	Changed	Rights	Owner
..		3/24/2026 3:16:20 PM	rw-r--r--	root
generated_csr		3/14/2026 8:20:12 AM	rw-r--r--	_nobody
multidomaincerts		3/17/2026 6:19:48 PM	rw-r--r--	root
saml		2/4/2026 3:56:54 PM	rw-r--r--	root
ca.pem	16 KB	3/14/2026 7:37:55 AM	rw-r--r--	_nobody
client-ca.crl	2 KB	2/4/2026 3:54:04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

x15.4上のExpresswayメニュー(Maintenance > Security > Server certificate) (サーバ証明書ファイルのみが存在する) :



x15.5へのアップグレードに成功した後

この例では、Maintenance > Security > client certificateおよびserver certificatesの下に2つの証明書オプションが表示されています。x15.5へのアップグレード後、x15.4からのサーバ証明書がx15.5のクライアント証明書ストアにコピーされたため、web adminのサーバ証明書ポータルとクライアント証明書ポータルの両方に同じ証明書が表示されます。



x15.5へのアップグレード後の既存の証明書と秘密キーがクライアント証明書ストアにコピーされました。

x15.5上のExpresswayファイルシステムの永続的な/証明書ディレクトリ：

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

TLSハンドシェイク時のX15.5 EKUチェック

x15.5では、新しいCLIコマンドが導入され、TLSハンドシェイク時に拡張キー使用法(EKU)をチェックできるようになりました。デフォルト値は「オン」です。コマンドセットはExpressway CoreおよびEdgeで有効です。

コマンドセットにより、Expresswayへのすべての着信SIP TLS接続のチェックがトリガーされます。(インバウンドクライアントhello/証明書が提示されます)。オンにすると、TLSイニシエータによって提示された証明書に証明書のクライアントEKUが含まれているかがチェックされます。オフにすると、チェックはバイパスされますが、サーバEKUが証明書に存在する場合はチェックされます。

xconfiguration SIP TLS Certificate ExtendedKeyUsageチェックモード：オン/オフ：



注：クライアント証明書を生成し、クライアントEKU（パブリックCA署名付き証明書の例）を含まないCSRに署名する場合は、この証明書をクライアント証明書ストアに手動でアップロードできません。そのため、CSRの署名によって生成された証明書に必ずクライアントEKUが含まれていることを確認する必要があります（プライベートCAを使用して、クライアントEKUを挿入できます）。



ヒント：このエラーは、クライアントのEKUが欠落しているCSR署名付き証明書をクライアント証明書ストアからアップロードしようとするとき明らかになります。

The screenshot shows the Cisco Expressway-E web interface. The top navigation bar includes 'Status >', 'System >', 'Configuration >', 'Applications >', 'Users >', and 'Maintenance >'. The main heading is 'Client certificate'. A yellow warning box contains the message: 'Invalid certificate: The file provided does not have a client usage attribute. Services requiring mutual TLS may not work.' Below this, another yellow warning box states: '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.' A blue tab labeled 'Client certificate data' is visible at the bottom of the error section.

ただし、サーバEKUのみ（クライアントEKUなし）が含まれている証明書をサーバ証明書ストア経由でアップロードし、Upload server certificate file as client certificateを選択すると、証明書はクライアント証明書ストアにコピーされます。Expressway-EdgeでプライベートCA署名付き証明書を使用しない管理者は、サーバ証明書ストアからクライアント証明書ストアにのみサーバEKUをコピーすることを選択できます。

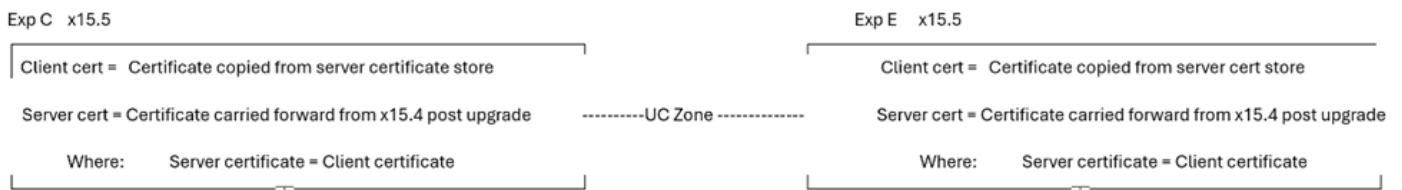
The screenshot shows the 'Server certificate' configuration page in the Cisco Expressway-E web interface. The page title 'Server certificate' is highlighted with a red box. A yellow warning box at the top reads: 'Warning: The CSRF Protection status is automatically enabled after the software upgrade. We recommend keeping CSRF protection Enabled. To change it, please log in to the CLI.' Below this is a section for 'Server certificate data' with fields for 'Server certificate', 'Currently loaded certificate expires on' (Dec 24 2027), and 'Certificate issuer' (RICKY200-TMS-CA). There are 'Show (decoded)' and 'Show (PEM file)' buttons. A 'Reset to default server certificate' button is also present. The 'Certificate signing request (CSR)' section shows 'There is no certificate signing request in progress'. The 'Generate CSR' section is partially visible. At the bottom, the 'Upload new certificate' section has three options: 'Select the server private key file' (Browse... No file selected.), 'Select the server certificate file' (Browse... No file selected.), and 'Upload server certificate file as client certificate' (checkbox), which is highlighted with a red box.

複数の証明書ストア、複数の導入シナリオ

Expresswayには2つの証明書ストアがあるため、証明書ストアには複数のシナリオがあります。

条件1：アップグレード

Expresswayをx15.4またはx15.5より前のバージョンからアップグレードする場合、この条件は成立します。x15.4バージョンの既存の証明書が2つの証明書ストアにコピーされます。x15.5のクライアントとサーバでは、証明書は同じです。

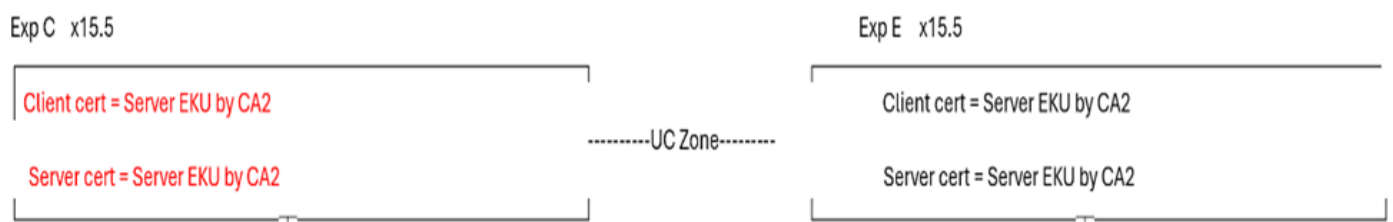


条件2：管理者がx15.5に新しい証明書をインストールしたとき（既存の証明書の有効期限が切れました）

CA 1 =内部CA

CA 2 =パブリックCA

次の図に示すように、Expressway Coreには、CA 2によってのみ署名されたサーバEKU（パブリックCA）を持つクライアント証明書と、CA 2によってのみ署名されたサーバEKU（パブリックCA）を持つサーバ証明書があります。同様に、Expressway Eには、CA 2によって署名されたサーバEKU（パブリックCA）を持つクライアント証明書と、CA 2によってのみ署名されたサーバEKU（パブリックCA）を持つサーバ証明書があります。



Expresswayコアサーバ証明書にクライアントEKU、ユニファイドコミュニケーショントラバーサルゾーン、MRAがない場合、WebRTCプロキシは機能しません。Expressway Coreサーバ証明書にクライアントEKUがあることを確認してください。これは、ユーザーがパブリックCAからすべての証明書への署名を選択する一般的な使用例です。パブリックCAは証明書にクライアントEKUを含めないため、ユニファイドコミュニケーショントラバーサルゾーンはアクティブになります。

UCゾーンをアクティブにするには、Expressway EでEKUチェックをオフにするという手っ取り早い方法があります。これにより、UCゾーンが起動します。ただし、SSHトンネルは非アクティブのままです。現在、2222でのSSHトンネル通信には、クライアントEKUの検証が必要です。

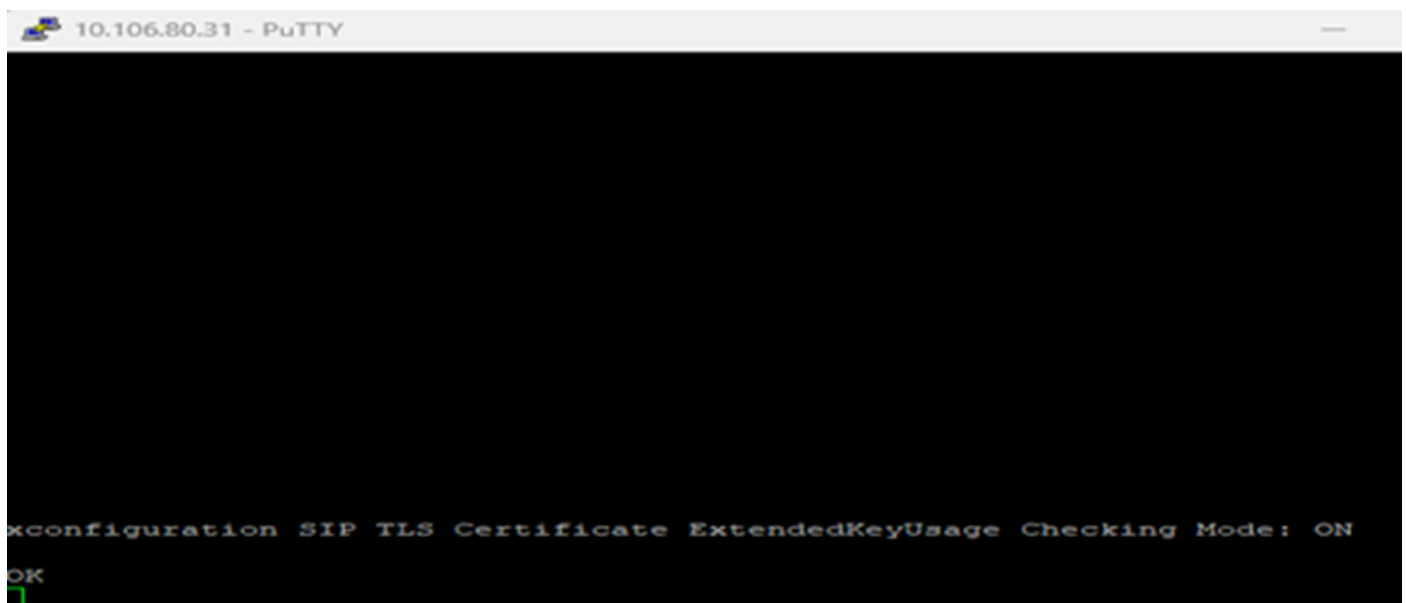
MRAクライアントログインおよびWebRTCプロキシ機能は機能しません。プライベートCAに頼らざるを得ない場合もあります。

テスト ケース 1

- Expressway EでEKUチェックが「ON」のとき
- Expressway Coreのクライアントおよびサーバ証明書にサーバEKUのみがある場合
- UCゾーンステータスがFAILED

Expressway-EdgeでExtendedKeyUsageをオンにします。

xconfiguration SIP TLS Certificate ExtendedKeyUsageチェックモード：オン：



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

ユニファイドコミュニケーションゾーン障害：

uczone.MSA Unified Communications traversal 0 0 kbps Off Failed No search rules configured View/Edit

New Delete Select all Unselect all Hide generated items

User: admin Access: Read-write System host name: vcs8c System time: 12:24 IST Language: en_US S/N: 007E452D Version: X15.5

Expressway Eのログには、10.106.80.16 = Expressway Core、10.106.80.31 = Expressway Edgeと記録されています。

Results

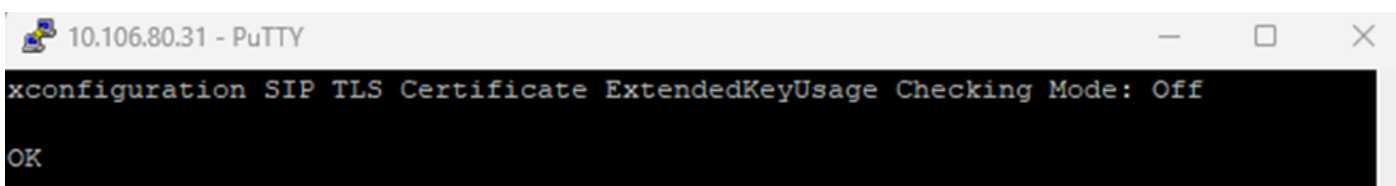
2026-03-29T12:24:39.839+05:30	tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-ip="10.106.80.16" Src-port="25046" Dst-ip="10.106.80.31" Dst-port="7001" Detail="unsupported certificate purpose" Protocol="TLS" Level="1" UTCTime="2026-03-29 06:54:39.839"
2026-03-29T12:24:39.819+05:30	tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-ip="10.106.80.16" Src-port="25045" Dst-ip="10.106.80.31" Dst-port="7001" Detail="unsupported certificate purpose" Protocol="TLS" Level="1" UTCTime="2026-03-29 06:54:39.819"
2026-03-29T12:23:59.591+05:30	tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-ip="10.106.80.16" Src-port="25044" Dst-ip="10.106.80.31" Dst-port="7001" Detail="unsupported certificate purpose" Protocol="TLS" Level="1" UTCTime="2026-03-29 06:53:59.591"
2026-03-29T12:23:59.569+05:30	tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-ip="10.106.80.16" Src-port="25043" Dst-ip="10.106.80.31" Dst-port="7001" Detail="unsupported certificate purpose" Protocol="TLS" Level="1" UTCTime="2026-03-29 06:53:59.569"
2026-03-29T12:23:19.426+05:30	tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-ip="10.106.80.16" Src-port="25042" Dst-ip="10.106.80.31" Dst-port="7001" Detail="unsupported certificate purpose" Protocol="TLS" Level="1" UTCTime="2026-03-29 06:53:19.426"

テスト ケース 2

- Expressway EでEKUチェックがオフのとき
- Expressway Coreのクライアント証明書とサーバ証明書にサーバのみのEKUがある場合
- UCゾーンステータスはACTIVE

Expressway EでEKUチェックをオフにします。

xconfiguration SIP TLS Certificate ExtendedKeyUsageチェックモード : オフ



10.106.80.31 - PuTTY

```
xconfiguration SIP TLS Certificate ExtendedKeyUsage Checking Mode: Off
```

OK

ユニファイドコミュニケーションゾーンアクティブ :

uczone.MSA Unified Communications traversal 0 0 kbps Off Active No search rules configured View/Edit

New Delete Select all Unselect all Hide generated items

User: admin Access: Read-write System host name: vcs8c System time: 12:27 IST Language: en_US S/N: 007E452D Version: X15.5

ただし、sshトンネルはまだ失敗しています。

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

Expresswayイベントログ :

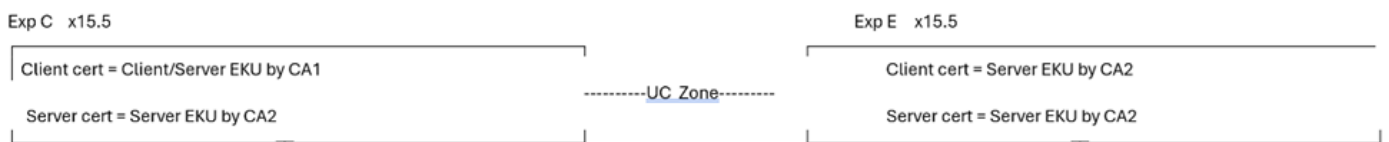
Results	
2026-03-29T12:33:12.384+05:30	ssh: Detail="ssh: connect to host smartslavsmarts 22222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:31:56.811+05:30	ssh: Detail="ssh: connect to host smartslavsmarts 22222:port 2222: Connection timed out" Level="ERROR"
2026-03-29T12:28:56.519+05:30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

条件2.1 : 成功事例

CA 1 =内部CA

CA 2 =パブリックCA

- Expresswayコアクライアント証明書がCA 1 (内部CA) によって署名され、クライアント/サーバEKUの両方が含まれている場合。
- Expresswayコアサーバ証明書はCA 2パブリックCAによって署名され、サーバEKUのみを含みます。
- Expressway Edge Server証明書はCA 2のパブリックCAによって署名されており、サーバEKUのみが含まれています。
- Expressway Edgeクライアント証明書はCA 2のパブリックCAによって署名されており、サーバEKUのみが含まれています。



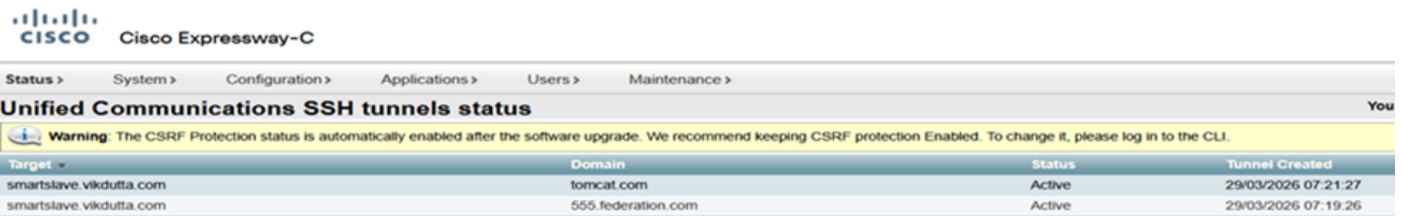
この条件は成功例です。 EKUチェックモードのオン/オフに関係なく、ユニファイドコミュニケーションゾーンとSSHトンネルの両方がアクティブになります。MRAクライアントは動作します。

Expressway EdgeのEKUチェックがOFFであるかONであるかは問題ではありません。 Expresswayコアクライアント証明書にクライアントEKUが含まれています。

```
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
```

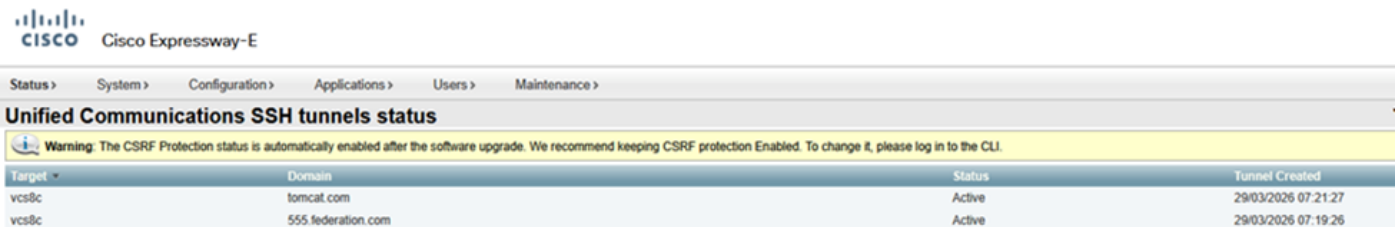
Expressway core ActiveのSSHトンネル :



The screenshot shows the Cisco Expressway-C web interface. The top navigation bar includes 'Status', 'System', 'Configuration', 'Applications', 'Users', and 'Maintenance'. The main heading is 'Unified Communications SSH tunnels status'. A warning message states: '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.' Below this is a table with the following data:

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

Expressway Edge ActiveのSSHトンネル :



The screenshot shows the Cisco Expressway-E web interface. The top navigation bar includes 'Status', 'System', 'Configuration', 'Applications', 'Users', and 'Maintenance'. The main heading is 'Unified Communications SSH tunnels status'. A warning message states: '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.' Below this is a table with the following data:

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

ユニファイドコミュニケーションMRAゾーンのステータスアクティブ :

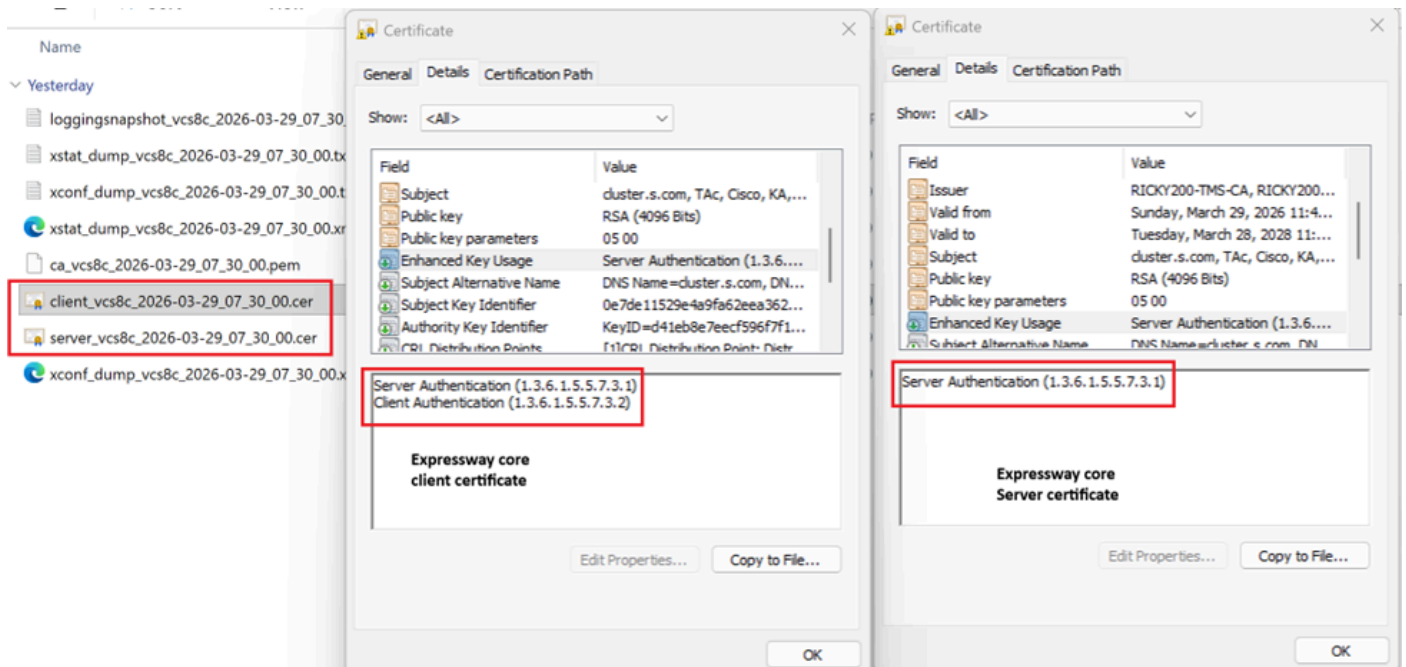


The screenshot shows the configuration page for the 'uczone.MRA' zone. The table below shows the zone's status:

Zone Name	Unified Communications traversal	Bandwidth	Traversal	Status	Search Rules	Action
uczone.MRA	0	0 kbps	Off	Active	No search rules configured	View/Edit

At the bottom, there are buttons for 'New', 'Delete', 'Select all', and 'Unselect all'. A footer bar shows 'User: admin Access: Read-write System host name: vcs8c System time: 12:58 IST Language: en_US S/N: 007E452D Version: X15.5'.

- Expressway-Coreクライアント証明書にサーバEKUとクライアントEKUがあります。
- Expressway Coreサーバ証明書にはサーバEKUのみがあります。



MRAクライアントがログインし、登録されます。

Cisco Jabber

hanu@

Search or call

All ▾

Connection Status

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.

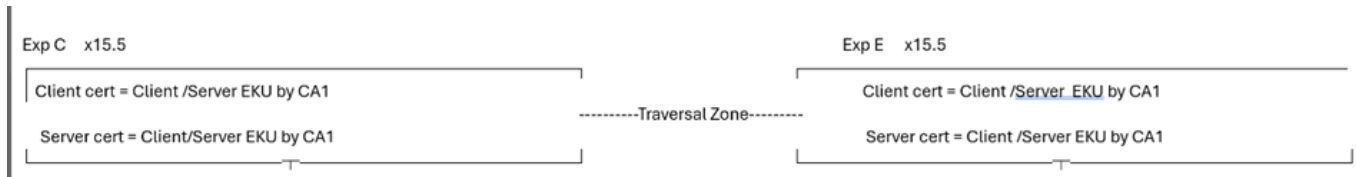


注:MRAおよびWebRTCプロキシが機能するように、証明書に含まれるEKUを比較してメモします。これは、正常に動作する導入と動作しない導入の比較です。

条件3 : プライベートCAですべての証明書に署名する

CA 1 =内部CA

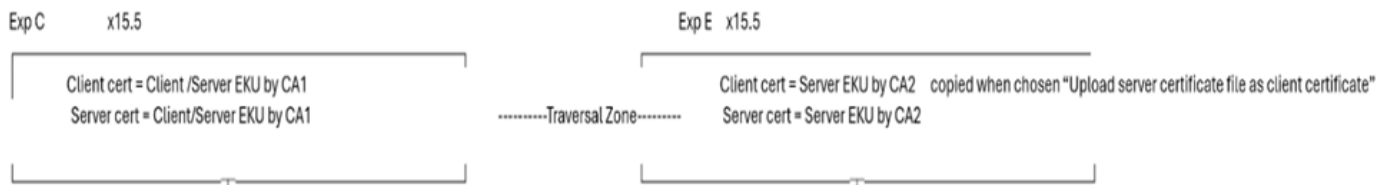
CA 2 =パブリックCA



条件3では、すべての証明書が内部CA(CA1)によって署名されます。

- Expressway-EがTLS接続を送信する場合、CA 1ルート/中間を遠端エンティティと交換する必要があります。遠端に機能がないか、プライベートCA証明書のアップロードが許可されていない場合、TLS接続は失敗します。
- プライベート証明書がOS信頼ストアにない場合、MRAクライアントはポップアップを受け入れるように証明書を取得します。

条件4: Expressway EdgeにサーバEKUのみの公開証明書がある



条件4では、Expresswayのコアクライアント証明書とサーバ証明書は(CA1)内部CAによって署名され、クライアントとサーバの両方のEKUが存在します。Expressway Eのサーバ証明書はパブリックCA署名付きで、サーバEKUのみを含んでいます。サーバ証明書がクライアント証明書ストアにコピーされます。「サーバ証明書ファイルをクライアント証明書としてアップロード」を選択します。

条件4では、TLS接続が遠端に対して行われる場合、Expressway-EがTLSクライアントhelloを送信すると、遠端は(クライアント証明書にクライアント認証EKUがないため)クライアントEKUチェックを無効にする必要があります、そうでない場合はTLS接続が失敗します。

ユーザの導入とユースケースに基づいて、フィールドにはさらに多くの条件やシナリオが存在する可能性があり、私の限られた思考の流れのためにすべてをカバーすることはできません。ただし、次の点に注意してください。

- # TLSハンドシェイク中にExpresswayがクライアントになると、クライアント証明書がピアに提示されます。
- #IF ExpresswayはTLSハンドシェイク時にサーバになります。サーバ証明書はピアに提示さ

れます。

この理由は、これらのテストケースで確立されています。

シナリオ 1

このシナリオでは、ExpresswayはWebexとのMTLSハンドシェイク中にクライアント証明書を提示します。

Webex会議へのビデオ通話：

サンプルコールフロー 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 smartslave tvcs: UTCTime="2026-03-24 11:54:26,106"  
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="10.106.80.31" Local-port="25002"  
Dst-IP 「163.129.37.33」 Dst-port= 「5061」
```

Expressway Edgeには、このシリアル番号(2f0000004c869c77c8981becde00000000004c)のクライアント証明書があります。

Expressway EdgeはTLSネゴシエーション中に「Webex」にclient helloを送信し、クライアント証明書を送信します。

シリアル番号2f0000004c869c77c8981becde00000000004c:

1. Expressway EdgeはmTLSネゴシエーション中に、client hello(pkt= 13699)を「Webex」に送信します。
2. WebexがExpressway Edgeにサーバhello(pkt=13701)を送信します。
3. Webexが証明書をExpressway Edge(pkt=13711)に送信します。
4. WebexがExpresswayエッジ証明書「CertificateRequest」(pkt=13715)を要求します。

5. Expressway Edgeが自身の証明書をWebexに送信します(pkt=13718)。

(screenshot)

The screenshot displays a network traffic capture with the following details:

- Packet 13718:** 10.106.00.31 to 163.129.37.32, TLSv1.2, 1178 bytes. Content: Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message.
- Certificate Details:**
 - Version: v3 (2)
 - serialNumber: 2f0000004c869c77c8981becde000000004c
 - Signature: sha256WithRSAEncryption
 - Issuer: rdnsSequence (0)
 - Validity: notBefore: utcTime (0), notAfter: utcTime (0)
 - Subject: rdnsSequence (0)

Expressway Edgeからのクライアント証明書 :

The screenshot shows a file explorer window with the following files:

- ca_smartslave_2026-03-24_11_55_47.pem (15 KB)
- client_smartslave_2026-03-24_11_55_47.pem (3 KB)
- eth0_diagnostic_logging_tcpdump00_smartslav... (305 KB)
- loggingnsnapshot_smartslave_2026-03-24_11_55... (918 KB)
- server_smartslave_2026-03-24_11_55_47.pem (3 KB)
- xconf_dump_smartslave_2026-03-24_11_55_47.bt (155 KB)
- xconf_dump_smartslave_2026-03-24_11_55_47.x... (135 KB)
- xstat_dump_smartslave_2026-03-24_11_55_47.txt (69 KB)
- xstat_dump_smartslave_2026-03-24_11_55_47.xml (120 KB)

The 'client_smartslave_2026-03-24_11_55_47.pem' file is selected, and its properties dialog is open, showing the following details:

- Field: Version, Value: V3
- Field: Serial number, Value: 2f0000004c869c77c8981becde000000004c
- Field: Signature algorithm, Value: sha256RSA
- Field: Signature hash algorithm, Value: sha256
- Field: Issuer, Value: bgluclab-WIN-DC-01-CA, bglu...
- Field: Valid from, Value: Tuesday, March 24, 2026 4:5...
- Field: Valid to, Value: Thursday, March 23, 2028 4:5...
- Field: Subject, Value: cluster.s.com, fac, rison, BL

シナリオ 2

ExpresswayはmTLSハンドシェイク中にサーバエンティティになり、そのサーバ証明書を提示します。

Expresswayがサーバ証明書を提示する場合、Expresswayには名前の確認がオンの5061を介したセキュアなネイバーゾーンがあります。

Expresswayノードx15.5とExpresswayノードx8.11.4の間のセキュアネイバーゾーン：

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)

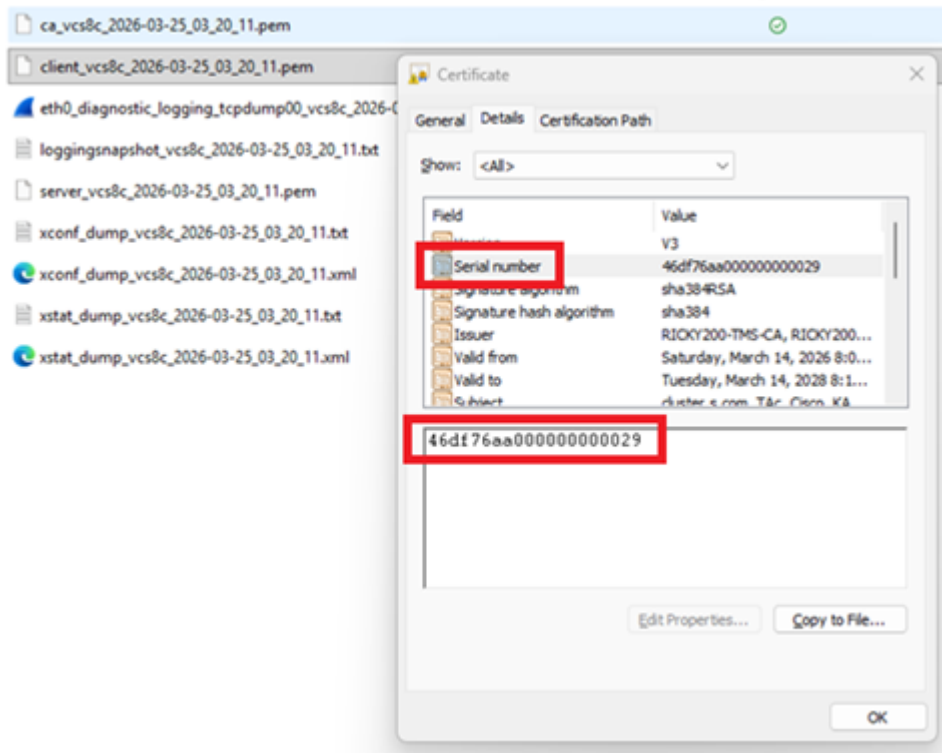
10.106.80.16 (x15.5) presents its server cert during TLS handshake (pkt=742) and requests client's cert

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=65168 Len=0 MSS=1460 SACK_PERM TSval=4070042683 TSecr=2013756904 WS=112
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 Win=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 2003 → 29457 [ACK] Seq=1 Ack=211 Win=65024 Len=0 TSval=4070042721 TSecr=2013756942
738 2026-03-25 15:10:17.870936 10.106.80.16 10.106.80.15 TLSv1.2 1514 Server Hello
739 2026-03-25 15:10:17.870955 10.106.80.15 10.106.80.16 TCP 66 29457 → 5061 [ACK] Seq=211 Ack=1449 Win=32128 Len=0 TSval=2013756950 TSecr=4070042720
740 2026-03-25 15:10:17.870964 10.106.80.16 10.106.80.15 TCP 1514 5061 → 29457 [ACK] Seq=1449 Ack=211 Win=65024 Len=1448 TSval=4070042729 TSecr=2013756942 [TCP PDU reassembled in 742]
741 2026-03-25 15:10:17.870968 10.106.80.15 10.106.80.16 TCP 66 29457 → 5061 [ACK] Seq=211 Ack=2003 Win=36896 Len=0 TSval=2013756950 TSecr=4070042720
742 2026-03-25 15:10:17.870969 10.106.80.16 10.106.80.15 TLSv1.2 830 Certificate, Server Key Exchange, Certificate Request, Server Hello Done
743 2026-03-25 15:10:17.870972 10.106.80.15 10.106.80.16 TCP 66 29457 → 5061 [ACK] Seq=211 Ack=3661 Win=37058 Len=0 TSval=2013756950 TSecr=4070042720
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 [..]: 308207d13082069a003020102020a46df76aa00000000029300006092a864886f76d01010c050030493113011060a0992268993f2c6401191603636f6d31183016060a0992268993f2c..
signedCertificate
version: v3 (2)
serialNumber: 0x46df76aa00000000029
signature (sha256withRSAEncryption)
Algorithm: Id. 1.2.840.113549.1.1.12 (sha256withRSAEncryption)
Issuer: rdnSequence (0)
rdnSequence: 3 items (id-at-commonName=RICKY200-THS-CA,dc=RICKY200,dc=com)
validity

次のスクリーンショットは、シリアル番号が一致するサーバ証明書を示しています。



テストケース3:MRAクライアントがログイン用にプロビジョニングされ、ワークフローに Expressway CoreとCUCM間のトラフィックサーバ証明書の検証が含まれています。

10.106.80.16 = Expressway Core x15.5

10.106.80.38 = CUCM

- Exp C 16は6972 TFTPでクライアントhelloを送信します。
- Exp C 16は、TLSハンドシェイク中にクライアント証明書を送信します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。