

# Naviguer dans le coucher de soleil EKU client avec Expressway x15.5

## Introduction

Ce document décrit la navigation dans le coucher de soleil EKU du client avec Cisco Expressway x15.5.

## Informations générales

Les certificats numériques sont des informations d'identification électroniques émises par des autorités de certification (CA) de confiance qui sécurisent la communication entre les serveurs et les clients en garantissant l'authentification, l'intégrité des données et la confidentialité. Ces certificats contiennent des champs d'utilisation de clé étendue (EKU) qui définissent leur objectif :

- Server Authentication EKU (id-kp-serverAuth) est utilisé lorsqu'un serveur présente son certificat pour prouver son identité.
- L'EKU d'authentification client (id-kp-clientAuth) est utilisée dans les connexions TLS mutuelles (mTLS) où les deux parties s'authentifient l'une l'autre.

Traditionnellement, un seul certificat peut contenir à la fois des UEC d'authentification de serveur et de client, ce qui lui permet de remplir deux fonctions. Ceci est particulièrement important pour les produits tels que Cisco Expressway qui agissent à la fois comme serveur et comme client dans différents scénarios de connexion.

## Définition du problème

### Modification de la politique du programme racine Chrome

À compter de juin 2026, la politique du programme racine Chrome restreint les certificats de l'autorité de certification racine (CA) inclus dans le magasin racine Chrome, éliminant progressivement les racines polyvalentes pour aligner toutes les hiérarchies d'infrastructure à clé publique (PKI) afin de servir uniquement les cas d'utilisation d'authentification du serveur TLS.

## Principales exigences de stratégie

- Les autorités de certification racines publiques doivent affirmer l'utilisation de clé étendue (EKU) UNIQUEMENT pour l'authentification du serveur (id-kp-serverAuth).
- Il est interdit d'inclure l'EKU d'authentification client dans ces certificats.
- Plus d'autorités de certification racine à utilisation mixte pour les certificats TLS de serveur public.
- Délai d'application : Juin 2026

## Délai de réponse de l'AC publique

- Octobre 2025 : Par défaut, de nombreuses autorités de certification publiques (DigiCert, Sectigo, SSL) ont commencé à émettre des certificats de serveur uniquement.
- Mai 2026 : Les serveurs CA publics arrêtent d'émettre des certifications EKU d'authentification client
- Juin 2026 : La politique du programme racine de Chrome devient pleinement efficace



Remarque : Cette politique s'applique uniquement aux certificats émis par des autorités de certification publiques. L'ICP privée et les certificats auto-signés ne sont pas affectés par cette stratégie.

---

Si vous êtes intéressé à lire sur l'impact de la temporisation de l'EKU client sur Expressways, référez-vous à [Préparer Expressway pour l'authentification client EKU temporisation dans les certificats d'autorité de certification publique.](#)

## Expressway version x15.5 avec solution

### Expressway x15.5

Expressway x15.5 est livré avec une solution proposée pour un problème qui se pose en raison de la temporisation de l'EKU client par toutes les autorités de certification publiques. Il s'agit d'un problème global qui affecte tous les fournisseurs/déploiements qui choisissent d'utiliser des certificats PKI publics.

x15.4, une version antérieure, avait un commutateur de commande CLI qui permettait à l'administrateur de télécharger le certificat Server EKU only (pas d'EKU client présent) sur Expressway E.

xConfiguration Certificat XCP TLS CVS EnableServerEkuUpload : On (activé)



Remarque : Cette commande est déconseillée sur x15.5.

---

## Ajout au magasin de certificats X15.5

x15.5 possède deux magasins de certificats :

1. Magasin de certificats du serveur

2. Magasin de certificats client

Expressways (carte réseau simple ou double) : Les deux interfaces Expressway peuvent utiliser 2 magasins de certificats en fonction des besoins.


Exemple :


- Lorsqu'expressway agit en tant que client pendant la connexion TLS, le certificat client est présenté.
- Lorsque expressway agit en tant que serveur lors de la connexion TLS, le certificat de serveur est présenté.





Remarque : Les deux magasins de certificats (client et serveur) utilisent la même bibliothèque d'autorités de certification approuvées. Assurez-vous que l'autorité de certification qui a signé les certificats du serveur et du client est correctement téléchargée sur le magasin d'approbations. Les journaux de diagnostic incluent désormais le certificat du serveur et le certificat du client au format de fichier 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

Mise à niveau de X15.4 ou version antérieure vers X15.5

Lorsqu'une mise à niveau est effectuée, le certificat du serveur à partir de x15.4 ou d'une version antérieure, le magasin de certificats du serveur Expressway est copié dans le magasin de certificats du client sur x15.5. Les magasins de certificats du client et du serveur sur x15.5 ont le même certificat.

Exemple avec captures d'écran

Serveur Expressway sur 15.4, certificat de serveur actuel Numéro de série  
46:df:76:aa:00:00:00:00:29

Certificat:

Version : 3 (0x2)

Numéro de série:

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

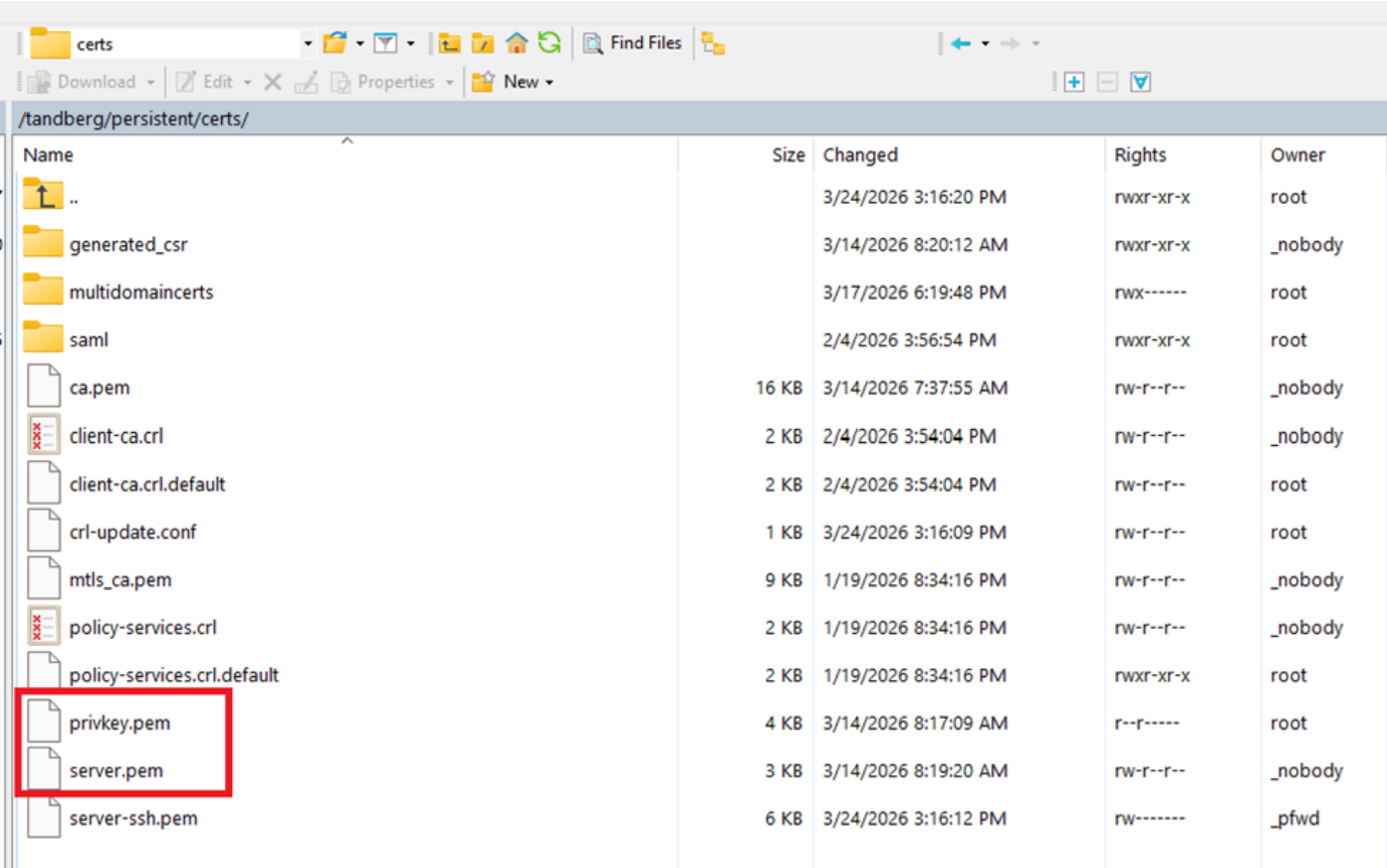
## Validité

Pas avant : 14 mars 02:37:40 2026 GMT

Pas après : 14 mars 02:47:40 2028 GMT

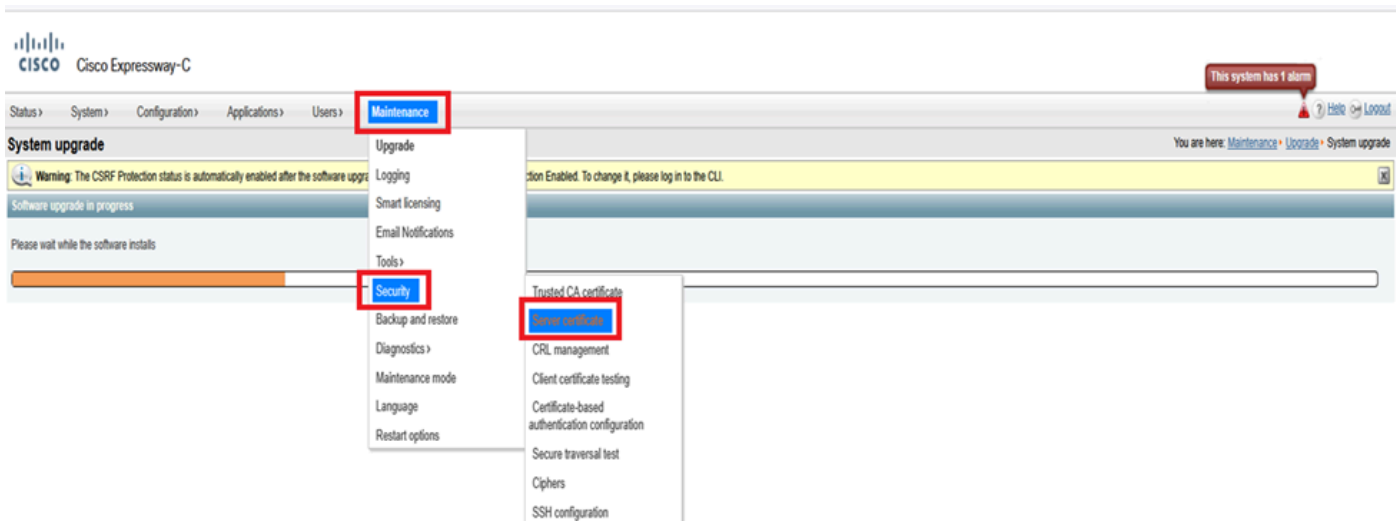
Objet : C = IN, ST = KA, L = KA, O = Cisco, OU = TAc, CN = cluster.s.com

Répertoire persistant/cert du système de fichiers Expressway sur x15.4 :



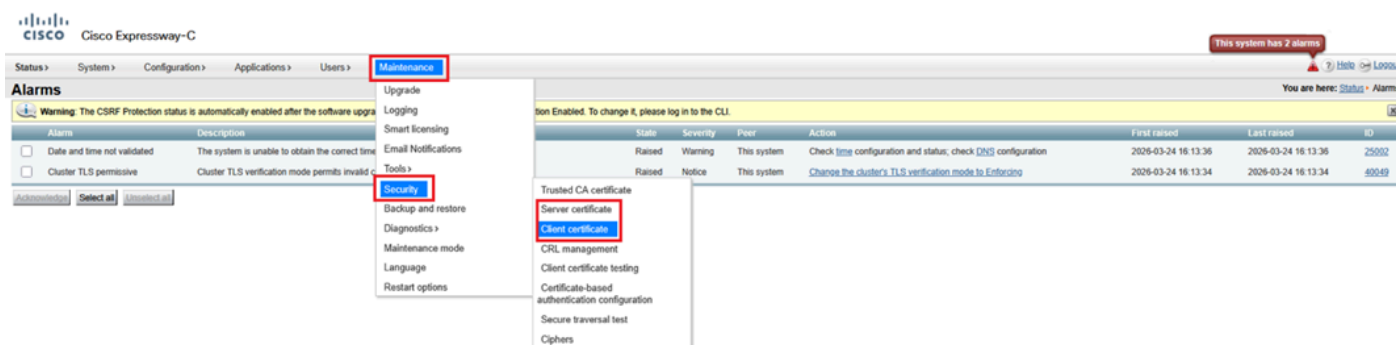
Name	Size	Changed	Rights	Owner
..		3/24/2026 3:16:20 PM	nwxr-xr-x	root
generated_csr		3/14/2026 8:20:12 AM	nwxr-xr-x	_nobody
multidomaincerts		3/17/2026 6:19:48 PM	nwx-----	root
saml		2/4/2026 3:56:54 PM	nwxr-xr-x	root
ca.pem	16 KB	3/14/2026 7:37:55 AM	nw-r--r--	_nobody
client-ca.crl	2 KB	2/4/2026 3:54:04 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 (Maintenance > Security > Server certificate) sur x15.4 (seul champ de certificat de serveur présent) :



Après une mise à niveau réussie vers x15.5

Ici, vous voyez 2 options de certificat sous Maintenance > Security > client certificate and server certificates. Après la mise à niveau vers x15.5, les portails de certificats Serveur et Client de l'administrateur Web affichent le même certificat, car le certificat du serveur de x15.4 a été copié dans le magasin de certificats client sur x15.5.



Une mise à niveau vers un certificat et une clé privée x15.5 existants a été copiée dans le magasin de certificats client.

Répertoire persistant/cert du système de fichiers Expressway sur 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

## Vérification de l'UKE X15.5 pendant la connexion TLS

Sur x15.5, une nouvelle commande CLI a été introduite pour vérifier l'utilisation de la clé étendue (EKU) pendant la connexion TLS. La valeur par défaut est « ON ». Le jeu de commandes est valide sur Expressway Core et Edge.

La commande set déclenche une vérification de toutes les connexions INBOUND SIP TLS dans Expressway. (hello/certificat client entrant présenté). Lorsque cette option est activée, elle vérifie si le certificat présenté par l'initiateur TLS contient ou non l'EKU client dans le certificat. S'il est désactivé, la vérification est ignorée ; cependant, l'UKE du serveur est vérifiée si elle est présente sur le certificat.

xconfiguration SIP TLS Certificate ExtendedKeyMode de vérification de l'utilisation :  
 ACTIVÉ/DÉSACTIVÉ :



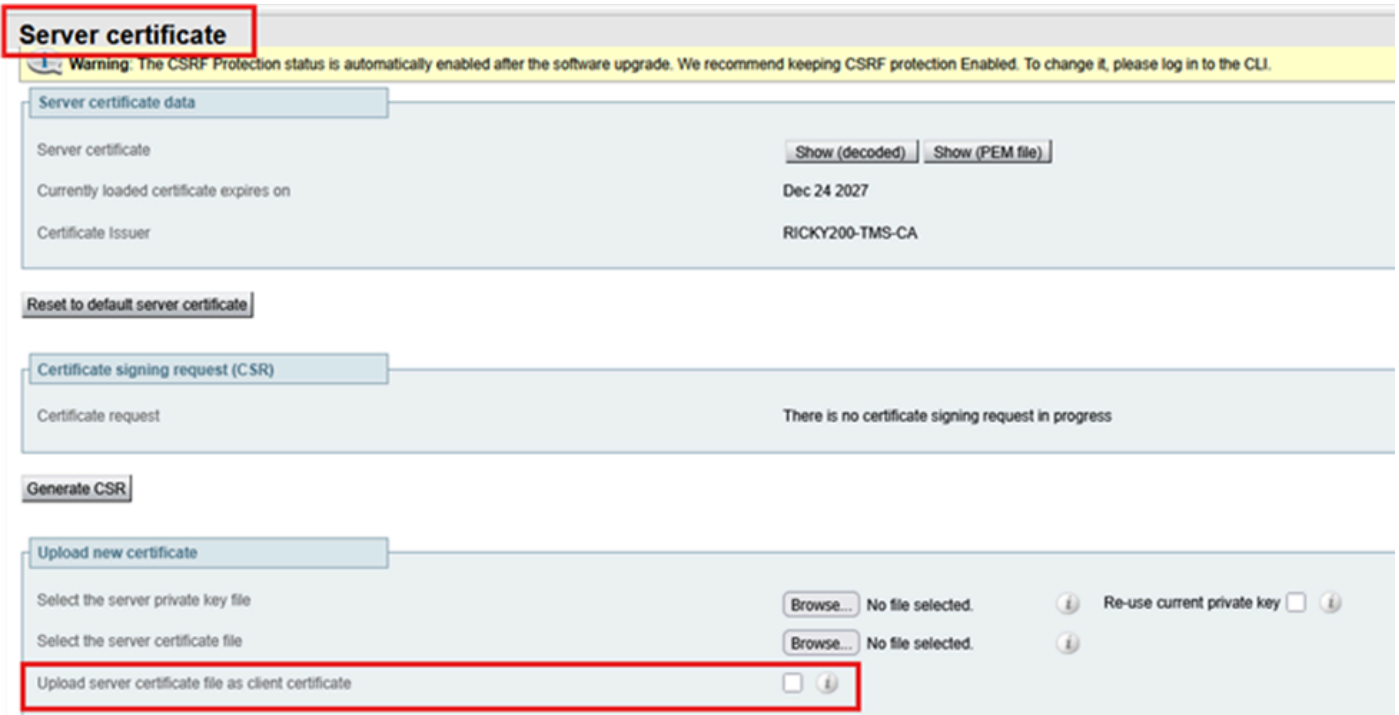
Remarque : Si vous générez un certificat client en signant un CSR qui ne contient pas l'EKU client (un exemple de certificat signé par une autorité de certification publique), vous ne pouvez pas télécharger ce certificat manuellement sur le magasin de certificats client. Vous devez donc vous assurer que les certificats générés par la signature d'un CSR contiennent toujours l'EKU client (une autorité de certification privée peut être utilisée pour insérer l'EKU client).



Conseil : Cette erreur devient évidente lorsque vous tentez de télécharger un certificat signé CSR, qui ne contient pas l'EKU client, à partir du magasin de certificats client.

The screenshot shows the Cisco Expressway-E web interface. At the top, there is a navigation menu with the following items: Status >, System >, Configuration >, Applications >, Users >, and Maintenance >. Below the navigation menu, the page title is "Client certificate". A red box highlights an error message: "Invalid certificate: The file provided does not have a client usage attribute. Services requiring mutual TLS may not work." Below the error message, there is a warning: "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 of the screenshot, there is a section titled "Client certificate data" which is currently empty.

Cependant, si vous choisissez de télécharger un certificat qui a une ECU serveur seulement (pas d'EKU client) via le magasin de certificats du serveur et sélectionnez Télécharger le fichier de certificat du serveur comme certificat client, le certificat est copié dans le magasin de certificats du client. Les administrateurs qui ne veulent pas utiliser un certificat signé par une autorité de certification privée sur Expressway-Edge peuvent choisir de copier l'EKE du serveur seulement du magasin de certificats du serveur vers le magasin de certificats du client.



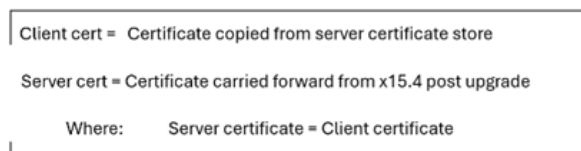
## Plusieurs magasins de certificats, plusieurs scénarios de déploiement

Étant donné qu'il existe maintenant deux magasins de certificats sur Expressway, il existe plusieurs scénarios de magasins de certificats.

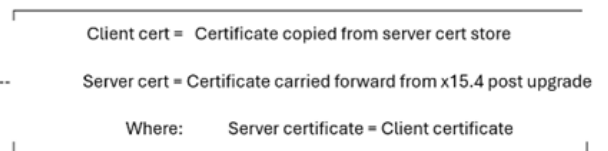
### Condition 1 : Mise à niveau

Lorsque Expressway est mis à niveau à partir de x15.4 ou avant x15.5, cette condition est vraie. Les certificats existants de la version x15.4 sont copiés dans deux (2) magasins de certificats. Sur le client et le serveur x15.5, les certificats sont identiques.

Exp C x15.5



Exp E x15.5

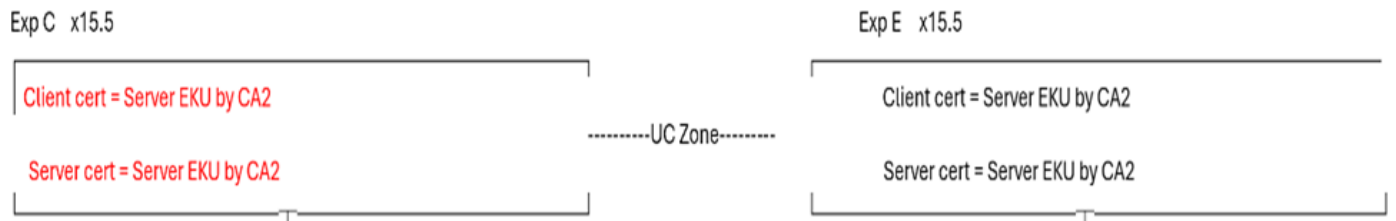


Condition 2 : Lorsque l'administrateur installe un nouveau certificat sur x15.5 (les certificats existants ont expiré)

CA 1 = CA interne

CA 2 = CA publique

Dans la figure ci-dessous, Expressway Core possède un certificat client avec l'EKU du serveur signé uniquement par CA 2 (Autorité de certification publique) et un certificat de serveur avec l'EKU du serveur signé uniquement par CA 2 (Autorité de certification publique). De même, Expressway E dispose d'un certificat client avec l'EKU serveur signé par CA2 (AC publique) et d'un certificat serveur avec l'EKU serveur signé uniquement par CA2 (AC publique).



Si le certificat du serveur principal Expressway n'a pas d'EKU client, de zone de traversée des communications unifiées, de MRA, le proxy WebRTC ne fonctionne pas. Assurez-vous que le certificat du serveur Expressway Core a une unité d'évaluation du client. Il s'agit d'un cas d'utilisation courant où les utilisateurs choisissent de signer tous les certificats de l'autorité de certification publique. Puisque l'autorité de certification publique n'inclut pas l'EKU du client dans les certificats, la zone de traversée des communications unifiées devient active.

Pour rendre la zone UC active, une solution rapide consiste à désactiver la vérification ECU sur l'Expressway E. La zone UC s'affiche. Cependant, les tunnels SSH restent inactifs. À partir d'aujourd'hui, la communication du tunnel SSH sur le 2222 nécessite la validation de l'EKU client.

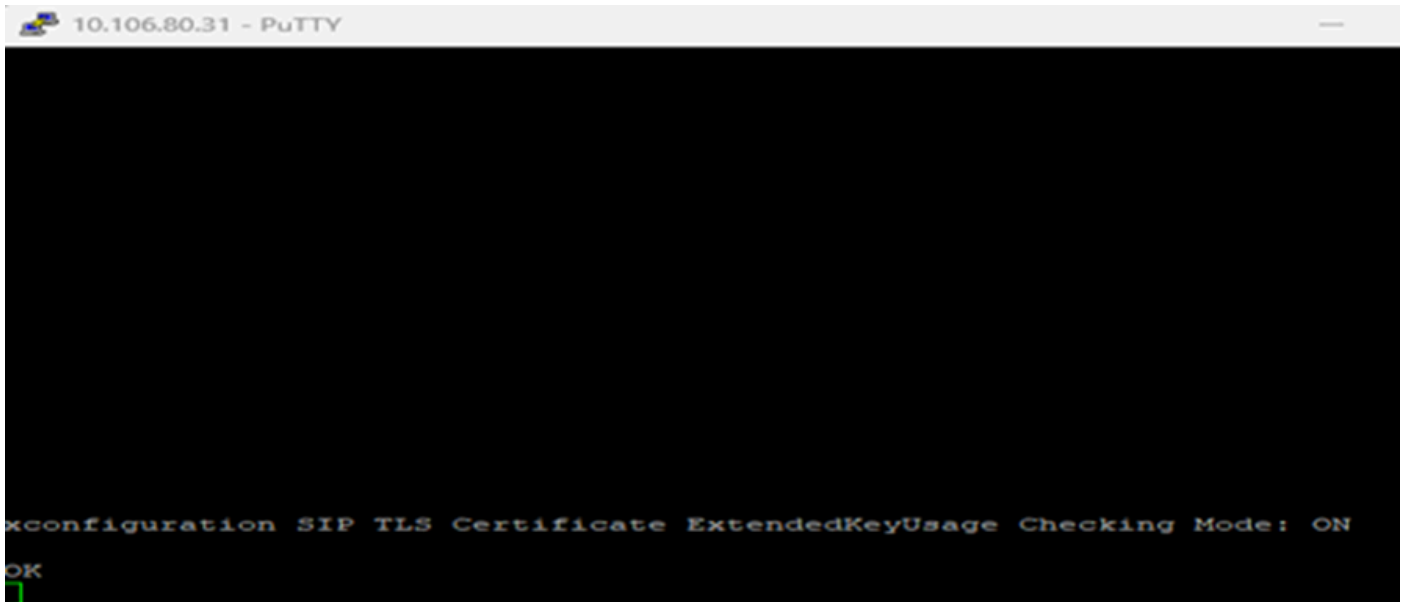
Les fonctions de connexion au client MRA et de proxy WebRTC ne fonctionnent pas. Vous pourriez devoir recourir à une autorité de certification privée.

#### Cas de test 1

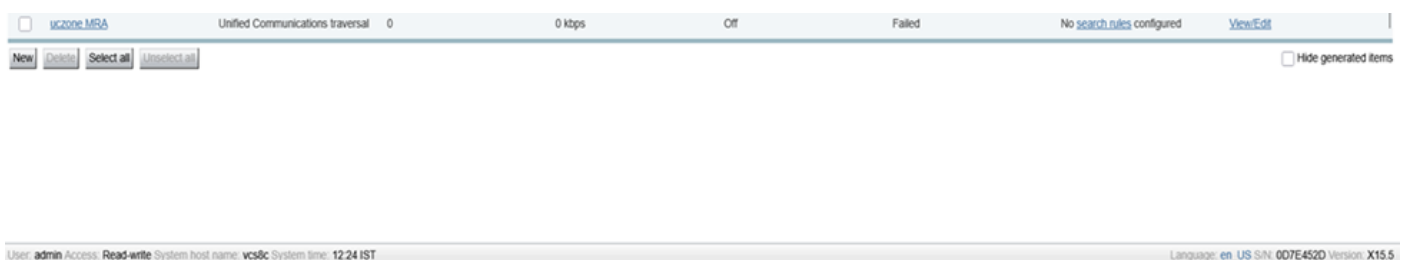
- Lorsque la vérification ECU est activée sur l'Expressway E
- Lorsque le certificat Client et Serveur sur Expressway Core a Server ECU seulement
- L'état de la zone UC est FAILED

Sur Expressway-Edge ExtendedKeyUsage, activez la case à cocher.

xconfiguration SIP TLS Certificate ExtendedKeyMode de vérification de l'utilisation : Activé:



Échec de la zone de communication unifiée :



Les journaux d'Expressway E indiquent où 10.106.80.16 = Expressway Core, 10.106.80.31 = Expressway Edge :



## Cas de test 2

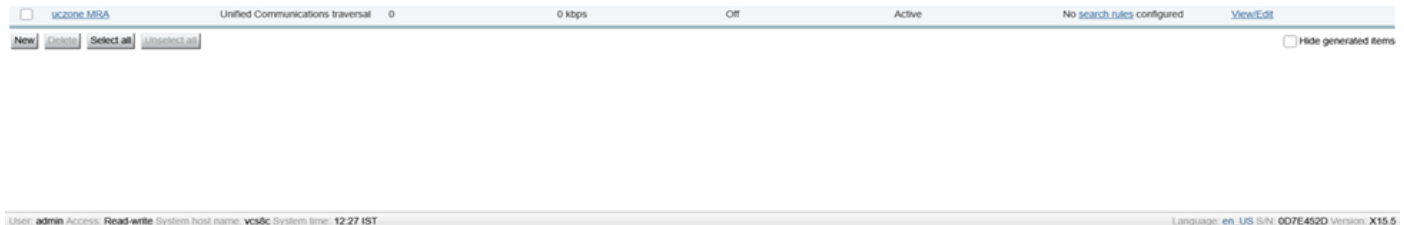
- Lorsque le contrôle ECU est désactivé sur l'Expressway E
- Lorsque le certificat Client et Serveur sur Expressway Core a une UER serveur seulement
- L'état de la zone UC est ACTIF

Désactivez le contrôle ECU sur l'Expressway E.

xconfiguration SIP TLS Certificate ExtendedKeyMode de vérification de l'utilisation : Off (désactivé)

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

Zone de communication unifiée active :



Cependant, les tunnels ssh ont toujours échoué :

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

Journaux des événements 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"

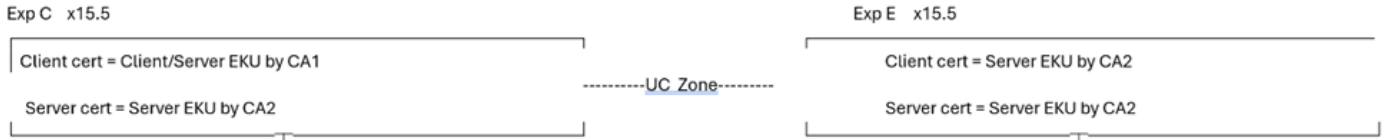
Condition 2.1 : Cas de réussite

CA 1 = CA interne

CA 2 = CA publique

- Où le certificat client principal d'Expressway est signé par CA 1 (CA interne) et inclut, Client/Server ECU les deux.
- Le certificat de serveur principal Expressway est signé par l'autorité de certification publique CA 2 et inclut l'unité de clé du serveur uniquement.

- Le certificat du serveur de périphérie Expressway est signé par l'autorité de certification publique CA2 et inclut l'unité de clé du serveur seulement.
- Le certificat client Expressway Edge est signé par l'autorité de certification publique CA 2 et inclut l'unité de clé du serveur uniquement.



Cette condition est un cas de réussite. Que le mode de vérification EKU soit ON/OFF ou non, la zone de communication unifiée et le tunnel SSH deviennent tous deux actifs. Les clients MRA fonctionnent.

Peu importe que la vérification EKU de l'Expressway Edge soit activée ou désactivée. Le certificat du client principal Expressway contient l'EKU du client :

```

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

```

Tunnels SSH sur le coeur Expressway actif :

**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

Tunnels SSH sur Expressway Edge Active :

### 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

État de la zone MRA Unified Communication Actif :

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

New Update Select all Unselect all Hide generated items

---

User: admin Access: Read-write System host name: vcs8c System time: 12:58 IST Language: en\_US S/N: 007E452D Version: X15.5

- Le certificat du client Expressway-Core a l'EKU du serveur et l'EKU du client.
- Le certificat Expressway Core Server comporte uniquement l'EKU du serveur.

The image shows two certificate detail windows side-by-side. The left window is for a client certificate, and the right is for a server certificate. Both have 'General' tabs selected.

Field	Value
Subject	duster.s.com, TAc, Cisco, KA,...
Public key	RSA (4096 Bits)
Public key parameters	05 00
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Alternative Name	DNS Name=duster.s.com, DN=...
Subject Key Identifier	0e7de11529e4a9fa62eea362...
Authority Key Identifier	KeyID=d41eb8e7eecf596f7f1...
Authority Distribution Points	f11c81 Distribution Point= Distr...

**Expressway core client certificate**

Field	Value
Issuer	RICKY200-TMS-CA, RICKY200...
Valid from	Sunday, March 29, 2026 11:4...
Valid to	Tuesday, March 28, 2028 11:...
Subject	duster.s.com, TAc, Cisco, KA,...
Public key	RSA (4096 Bits)
Public key parameters	05 00
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)
Subject Alternative Name	DNS Name=duster.s.com, DN=...

**Expressway core Server certificate**

Le client MRA se connecte et s'inscrit :

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.

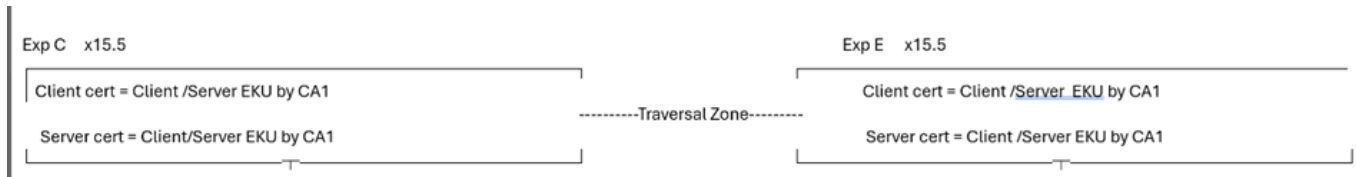


Remarque : Comparer et prendre note des unités ECU présentes dans les certificats pour que MRA et le proxy WebRTC fonctionnent. Il s'agit d'une comparaison entre un déploiement actif et un déploiement inactif.

Condition 3 : Signer tous les certificats avec une autorité de certification privée

CA 1 = CA interne

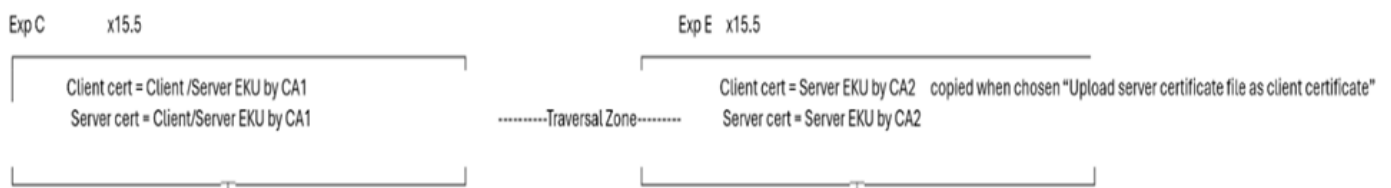
## CA 2 = CA publique



Dans la condition 3, tous les certificats sont signés par l'autorité de certification interne (CA1) .

- Lorsque Expressway-E envoie une connexion TLS, la racine/l'intermédiaire CA1 doit être échangée avec l'entité distante. Si l'extrémité distante n'a pas la capacité ou ne permet pas le téléchargement du certificat d'autorité de certification privée, la connexion TLS échoue.
- Les clients MRA obtiennent des certificats pour accepter les fenêtres intempestives si le certificat privé ne se trouve pas dans le magasin d'approbation du système d'exploitation.

Condition 4 : L'Expressway Edge possède des certificats publics avec une clé d'activation de serveur uniquement



Dans la condition 4, les certificats de client et de serveur principaux d'Expressway sont signés par l'autorité de certification interne (CA1) et comportent l'unité ECU du client et du serveur. Le certificat du serveur Expressway E est signé par une autorité de certification publique et ne comporte que l'unité ECU du serveur. Le certificat du serveur est copié dans le magasin de certificats client en choisissant Upload server certificate file as client certificate.

Dans la Condition 4, quand la connexion TLS est faite à l'extrémité distante, si Expressway -E envoie un bonjour client TLS, l'extrémité distante doit désactiver la vérification de l'ECU du client (car le certificat client n'a pas d'ECU d'authentification du client) sinon la connexion TLS échoue.

Il peut y avoir beaucoup plus de conditions ou de scénarios sur le terrain en fonction du déploiement de l'utilisateur et des cas d'utilisation et tous ne peuvent pas être couverts en raison de mon flux de pensée limité. Cependant, les points à retenir sont les suivants :

- # Si Expressway devient un client pendant la connexion TLS, le certificat client est présenté aux homologues.

- #IF Expressway devient serveur pendant la connexion TLS ; le certificat du serveur est présenté à l'homologue.

Ce raisonnement a été établi avec ces scénarios de tests.

## Scénario 1

Pour ce scénario, Expressway présente le certificat client lors de la connexion MTLs avec Webex.

Un appel vidéo à une réunion Webex :

Exemple de flux d'appels Jabber -à CUCM -à Exp Core —à Exp Edge —à Webex

10.106.80.31= Périphérie Expressway

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="Envoyé" Local-ip="10.106.80.31" Local-  
port="25002" Dst-ip="163.129.37.33" Dst-port="5061"
```

Expressway Edge possède un certificat client portant ce numéro de série  
(2f0000004c869c77c8981becde00000000004c).

Expressway Edge envoie un Hello client à « Webex » pendant la négociation TLS, puis envoie un certificat client.

Numéro de série 2f0000004c869c77c8981becde00000000004c :

1. Expressway Edge envoie un message Hello client (pkt= 13699) à « Webex » pendant la négociation mTLS.
2. Webex envoie un paquet Hello de serveur à Expressway Edge (pkt=13701).
3. Webex envoie son certificat à Expressway Edge (pkt=13711).
4. Webex demande un certificat de périphérie Expressway « CertificateRequest » (pkt=13715).

5. Expressway Edge envoie son certificat à Webex (pkt=13718).

(capture d'écran)

Network traffic capture showing TLS handshake between 10.106.00.31 and 163.129.37.32. Packet 13718 is highlighted, showing a Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, and Encrypted Handshake Message.

```

Length: 2936
Certificates Length: 2933
Certificates (2933 bytes)
Certificate length: 2934
Certificate [-]: 308207e308206d6a0030201020132f0000004c869c77c8981becde0000000004c300006092a8486f7000101000500304f31133011000a0992268993f22c6401191603636f6d3118301606
  signedCertificate
    version: v3 (2)
    serialNumber: 0x2f0000004c869c77c8981becde000000004c
    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)
  
```

Certificat client d'Expressway Edge :

File explorer showing a list of certificates. The 'client\_smartslave\_2026-03-24\_11\_55\_47.pem' file is selected, and its properties dialog is open, showing the serial number 2f0000004c869c77c8981becde000000004c.

Name	Status	Date modified	Type	Size
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

Certificate Properties:

Field	Value
Version	V3
Serial number	2f0000004c869c77c8981becd...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	bgluclab-WIN-DC-01-CA, bglu...
Valid from	Tuesday, March 24, 2026 4:5...
Valid to	Thursday, March 23, 2028 4:5...
Subject	cluster.s.com, bar, rison, BL

Serial number: 2f0000004c869c77c8981becde000000004c

## Scénario 2

Expressway devient une entité de serveur lors de la connexion mTLS et présente son certificat de serveur :

Lorsque Expressway présente un certificat de serveur, Expressway a une zone de voisinage sécurisée sur 5061 avec le nom de vérification ON.

Zone de voisinage sécurisée entre les noeuds Expressway x15.5 et 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)

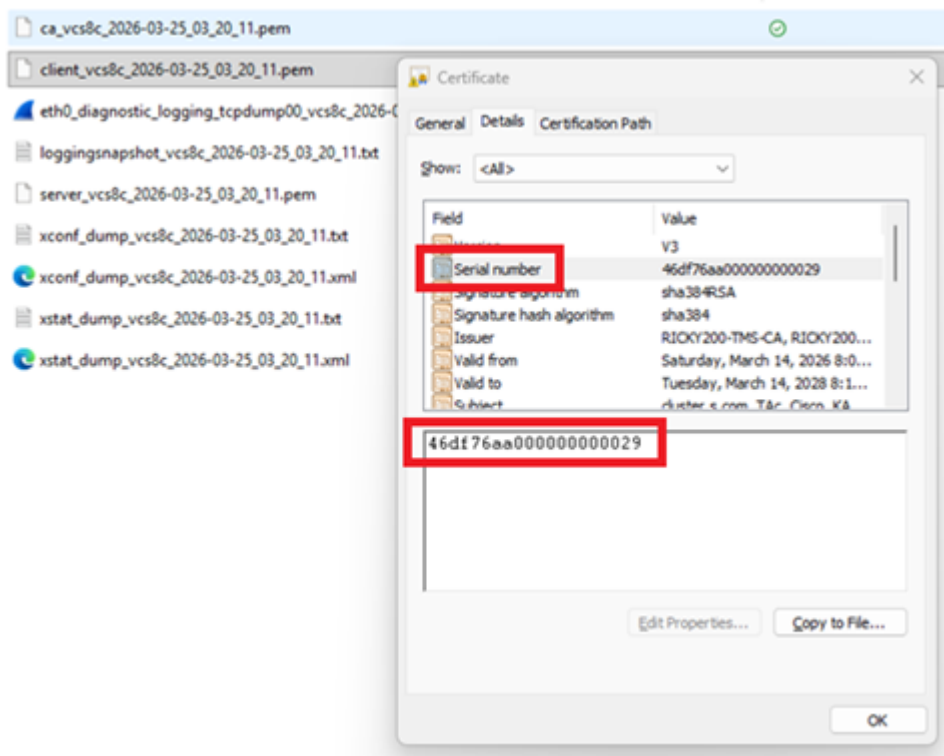
The screenshot displays a network traffic capture of a TLS handshake. The top section shows a list of packets with the following details:

- 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=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 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=2002 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

The bottom section shows a detailed view of the Certificate packet (742) with the following structure:

- Length: 2923
- Handshake Protocol: Certificate
- Handshake Type: Certificate (11)
- Length: 2919
- Certificates Length: 2916
- Certificates (2916 bytes)
- ▼ Certificate Length: 2005
- ▼ Certificate [..]: 308207d1308206b9a003020102020a46df76aa00000000029300606092a864886f76d01010c050030491133011060a0992268993f22c64011916036f6d31183016060a0992268993f22c...
- ▼ 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

Cette capture d'écran montre le certificat du serveur comme correspondant au numéro de série :



Cas de test 3 : le client MRA est configuré pour la connexion et le workflow inclut la vérification du certificat du serveur de trafic entre Expressway Core et CUCM.

10.106.80.16 = Expressway Core x15.5

10.106.80.38 = CUCM

- L'exp C 16 envoie un hello client sur TFTP 6972.
- Exp C 16 envoie un certificat client pendant la connexion TLS.

Content Type: Handshake (22)  
 Version: TLS 1.3 (0x0303)  
 Length: 2923

- Handshake Protocol: Certificate
  - Handshake Type: Certificate (11)
    - Length: 2918
    - Certificates Length: 2916
    - Certificates (2916 bytes)
      - Certificate Length: 2905
      - Certificate [1]: 46d176aa0000000029...
        - signedCertificate
          - version: v3 (2)
            - serialNumber: 46d176aa0000000029
            - signature (sha384/sha384/encryption)
            - issuer: rdSequence (0)
              - rdSequence: 3 items (1d-at-comonlaw-RIOOY200-THS-CA,4c-RIOOY200,4c-com)
                - rdSequence Item: 1 item (4c-com)
                - rdSequence Item: 1 item (4c-RIOOY200)
                - rdSequence Item: 1 item (1d-at-comonlaw-RIOOY200-THS-CA)
              - notBefore: utc15ae (0)
              - notAfter: utc15ae (0)

Certificat du client principal Expressway :

ca\_vcs1c\_2026-03-25\_03\_20\_11.pem  
 client\_vcs1c\_2026-03-25\_03\_20\_11.pem

eth0\_diagnostic\_logging\_tcpdump00\_vcs1c\_2026-03-25\_03\_20\_11.txt  
 loggingnapshot\_vcs1c\_2026-03-25\_03\_20\_11.txt  
 server\_vcs1c\_2026-03-25\_03\_20\_11.pem  
 xconf\_dump\_vcs1c\_2026-03-25\_03\_20\_11.txt  
 xconf\_dump\_vcs1c\_2026-03-25\_03\_20\_11.xml  
 vstat\_dump\_vcs1c\_2026-03-25\_03\_20\_11.txt  
 vstat\_dump\_vcs1c\_2026-03-25\_03\_20\_11.xml

General Details Certification Path

Show: <All>

Field	Value
Serial number	46d176aa0000000029
Signature algorithm	sha384-RSA
Signature hash algorithm	sha384
Issuer	RIOOY200-THS-CA, RIOOY200...
Valid from	Saturday, March 14, 2026 8:0...
Valid to	Tuesday, March 14, 2028 8:1...
Subject	cn=*.com, o=*.com, ou=*.com, c=*.com, CA

46d176aa0000000029

Edit Properties... Copy to File... OK

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.