

使用Expressway x15.5導航客戶端EKU日落

簡介

本文檔介紹使用Cisco Expressway x15.5導航客戶端EKU日落。

背景資訊

數位證書是由受信任的證書頒發機構(CA)頒發的電子憑證，通過確保身份驗證、資料完整性和機密性來保護伺服器 and 客戶端之間的通訊。這些證書包含定義其用途的擴展金鑰用法(EKU)欄位：

- 伺服器身份驗證EKU(id-kp-serverAuth)在伺服器出示證書以證明身份時使用。
- 客戶端身份驗證EKU(id-kp-clientAuth)在雙方TLS(mTLS)連線中使用，在該連線中雙方相互進行身份驗證。

傳統上，單個證書可以同時包含伺服器和客戶端身份驗證EKU，使其可用於雙重用途。這對於在不同連線場景中同時充當伺服器和客戶端的Cisco Expressway等產品尤為重要。

問題定義

Chrome根程式策略更改

自2026年6月起，Chrome根程式策略限制包含在Chrome根儲存中的根證書頒發機構(CA)證書，逐步停用多用途根來調整所有公共金鑰基礎結構(PKI)層次結構，以便僅使用TLS伺服器身份驗證使用案例。

主要政策要求

- 公共根CA必須宣告僅用於伺服器身份驗證(id-kp-serverAuth)的擴展金鑰使用(EKU)。
- 禁止在這些證書中包括客戶端身份驗證EKU。
- 沒有更多公共伺服器TLS證書的混合使用的根CA。
- 實施時間表：2026年6月

公共CA響應時間表

- 2025年10月：許多公共CA(DigiCert、Sectigo、SSL)預設開始頒發僅伺服器證書。
- 2026年5月：公共CA伺服器停止頒發客戶端身份驗證EKU證書
- 2026年6月：Chrome根計劃策略完全生效



附註：此策略僅適用於公共CA頒發的證書。私有PKI和自簽名證書不受此策略的影響。

如果您有興趣閱讀有關客戶端EKU設定對Expressway的影響，請參閱[在公共CA證書中準備Expressway客戶端身份驗證EKU失效。](#)

Expressway版本x15.5，帶解決方案

Expressway x15.5

Expressway x15.5提供了針對由於所有公共證書頒發機構對客戶端EKU的設定而引起的問題而提出的解決方案。這是一個全球性問題，影響選擇使用公共PKI證書的所有供應商/部署。

x15.4之前的版本中有一個CLI命令開關，允許管理員在Expressway E上上傳僅伺服器EKU證書（無客戶端EKU）。

xConfiguration XCP TLS證書CVS EnableServerEkuUpload:於



附註：此命令在x15.5上已棄用。

X15.5證書儲存新增

x15.5有兩個證書儲存區：

1. 伺服器證書儲存
2. 客戶端證書儲存

高速公路（單網絡卡或雙網絡卡）：兩個Expressway介面均可根據需要使用2個證書儲存。

範例：

- 當expressway在TLS握手期間充當客戶端時，將顯示客戶端證書。
- 當expressway在TLS握手期間充當伺服器時，將顯示伺服器證書。



附註：兩個證書儲存（客戶端和伺服器）使用相同的受信任CA庫。確保已在信任儲存上正確上載簽署伺服器和客戶端證書的CA。診斷日誌現在包含PEM檔案格式的伺服器證書和客戶端證書。

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

從X15.4或早期版本升級到X15.5

執行升級時，來自x15.4或早期版本的伺服器證書會複製到x15.5上的客戶端證書儲存中。x15.5上的客戶端和伺服器證書儲存具有相同的證書。

螢幕截圖示例

15.4上的Expressway伺服器，當前伺服器證書序列號46:df:76:aa:00:00:00:00:29

證書：

版本:3(0x2)

序列號：

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

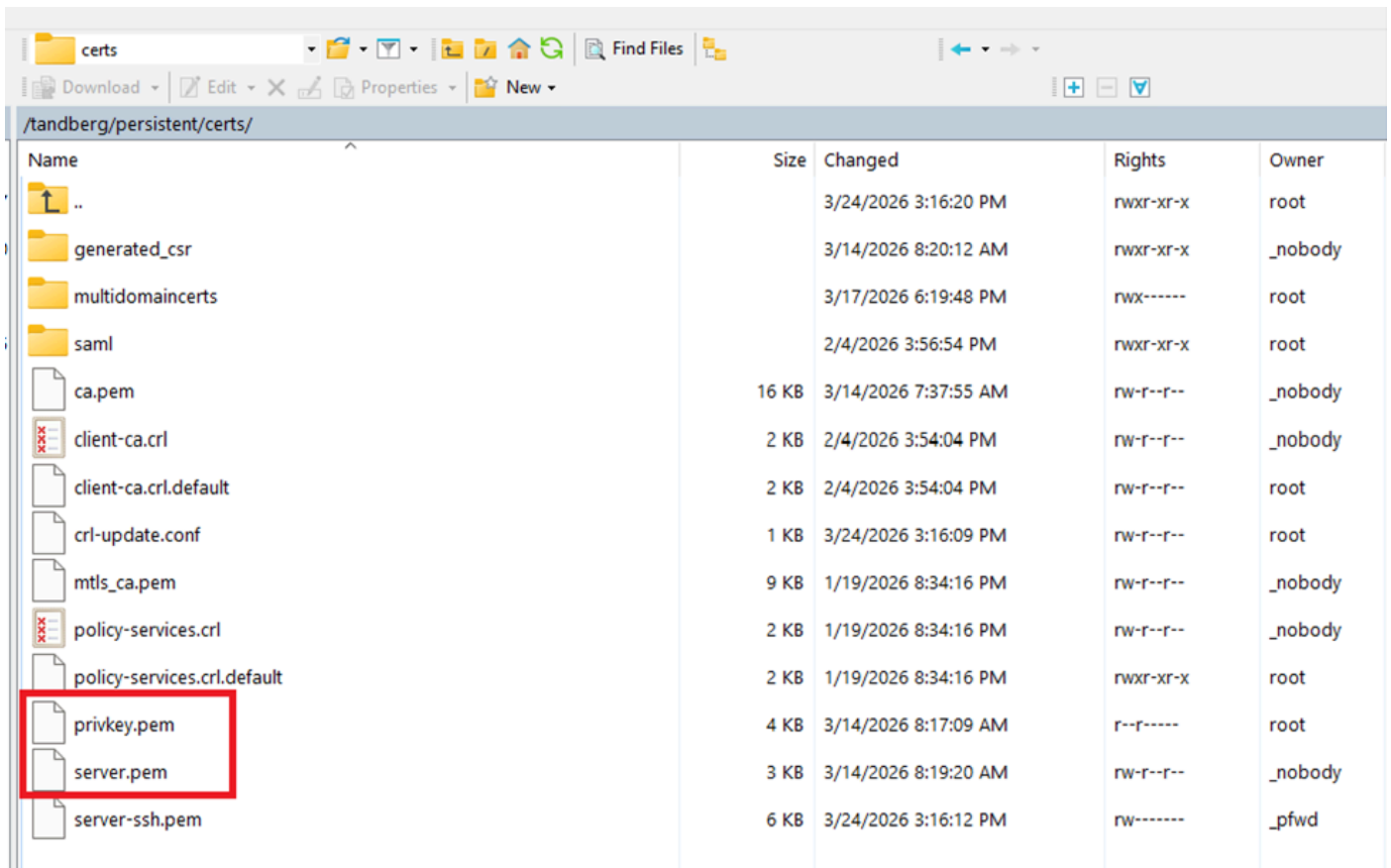
有效性

不早於：3月14日02:37:40 2026格林尼治標準時

不晚於：3月14日02:47:40 2028格林尼治標準時

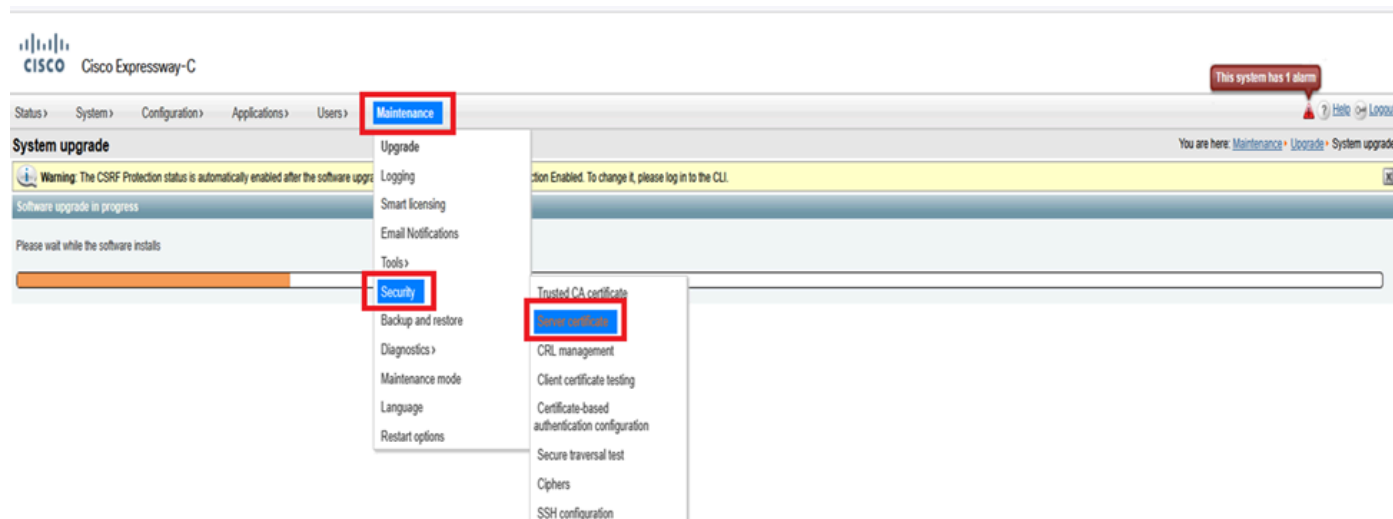
主題：C = IN、ST = KA、L = KA、O = Cisco、OU = TAc、CN = cluster.s.com

x15.4上的Expressway檔案系統永久/證書目錄：



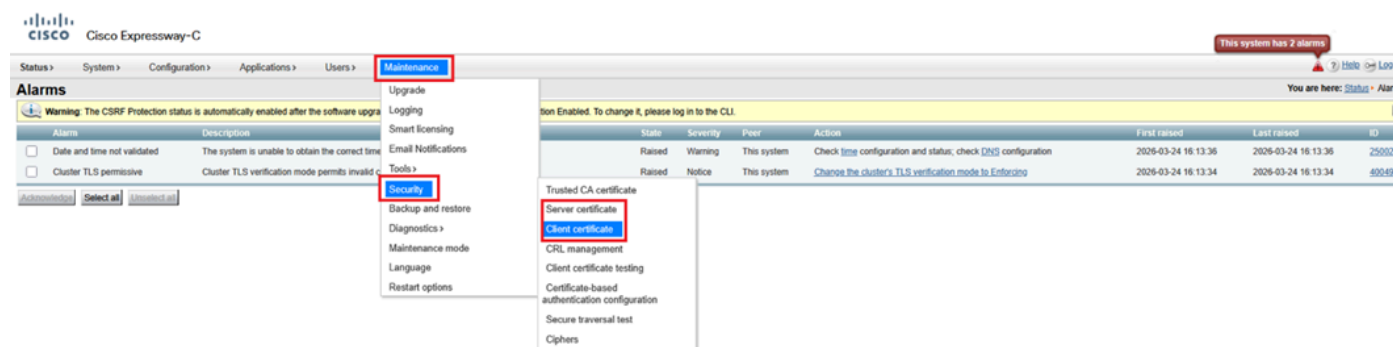
| Name | Size | Changed | Rights | Owner |
|-----------------------------|-------|----------------------|-----------|---------|
| .. | | 3/24/2026 3:16:20 PM | nwxr-xr-x | root |
| generated_csr | | 3/14/2026 8:20:12 AM | nwxr-xr-x | _nobody |
| multidomaincerts | | 3/17/2026 6:19:48 PM | nwx----- | 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 |

x15.4上的Expressway選單(「維護」>「安全」>「伺服器證書」)(僅存在伺服器證書欄位)：



成功升級到x15.5後

在此，您會看到維護>安全>客戶端證書和伺服器證書下有2個證書選項。升級到x15.5後，Web admin上的伺服器 and 客戶端證書門戶顯示相同的證書，因為來自x15.4的伺服器證書已複製到x15.5上的客戶端證書儲存中。



升級到x15.5的現有證書和私鑰已被複製到客戶端證書儲存中。

x15.5上的Expressway檔案系統永續性/證書目錄：

| 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 |

在TLS握手期間進行X15.5 EKU檢查

在x15.5上，引入了新的CLI命令來檢查TLS握手期間的擴展金鑰使用(EKU)。預設值為「ON」。命令集在Expressway核心和邊緣上有效。

命令集觸發檢查所有到Expressway的入站SIP TLS連線。(入站客戶端hello/提供的證書)。如果設定為「ON」，則檢查TLS發起方提供的證書在證書中是否包含客戶端EKU。如果關閉，則繞過檢查；但是，會檢查伺服器EKU是否存在於證書中。

xconfiguration SIP TLS Certificate ExtendedKeyUsage檢查模式：開/關：



附註：如果生成客戶端證書，並對不包含客戶端EKU的CSR進行簽名(公共CA簽名證書的

示例)，則無法在客戶端證書儲存上手動上載此證書。因此，您需要確保通過簽署CSR生成的證書始終包含客戶端EKU（可以使用專用CA插入客戶端EKU）。



提示：當您嘗試從客戶端證書儲存中上傳CSR簽名證書（缺少客戶端EKU）時，此錯誤變得明顯。

CISCO Cisco Expressway-E

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

Client certificate

Invalid certificate: The file provided does not have a client usage attribute. Services requiring mutual TLS may not work.

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.

Client certificate data

但是，如果選擇通過伺服器證書儲存上傳僅具有伺服器EKU（無客戶端EKU）的證書，並選擇上傳伺服器證書檔案作為客戶端證書，則證書將複製到客戶端證書儲存中。如果管理員不想在Expressway-Edge上使用私有CA簽名的證書，可以選擇僅將伺服器EKU從伺服器證書儲存複製到客戶端證書儲存。

Server certificate

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.

Server certificate data

Server certificate

Currently loaded certificate expires on Dec 24 2027

Certificate issuer RICKY200-TMS-CA

Certificate signing request (CSR)

Certificate request There is no certificate signing request in progress

Generate CSR

Upload new certificate

Select the server private key file No file selected. Re-use current private key

Select the server certificate file No file selected.

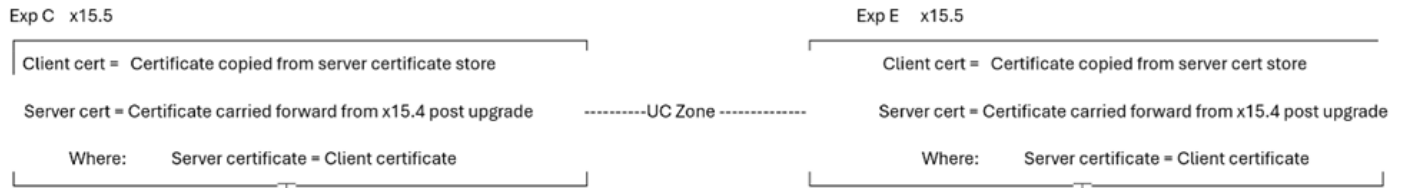
Upload server certificate file as client certificate

多個證書儲存，多個部署方案

由於現在在Expressway上有兩個證書儲存，因此存在多個證書儲存方案。

條件1:升級

當Expressway從x15.4或x15.5之前的版本升級時，此情況為真。x15.4版本的現有證書被複製到兩(2)個證書儲存中。在x15.5客戶端和伺服器上，證書是相同的。

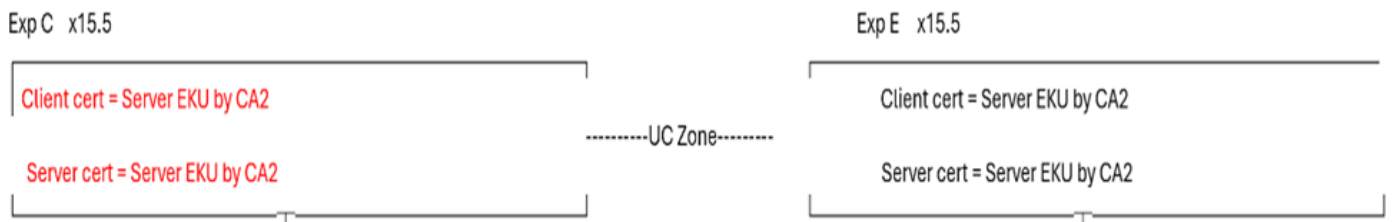


條件2:管理員在x15.5上安裝新證書時 (現有證書已過期)

CA 1 =內部CA

CA 2 =公共CA

在下一圖中，Expressway核心具有僅由CA 2簽署的伺服器EKU的客戶端證書 (公共CA) 和僅由CA 2簽署的伺服器EKU的伺服器證書 (公共CA)。同樣，Expressway E具有包含由CA2簽名的伺服器EKU的客戶端證書 (公共CA) 和包含僅由CA 2簽名的伺服器EKU的伺服器證書 (公共CA)。



如果Expressway核心伺服器證書沒有客戶端EKU、統一通訊遍歷區域、MRA，則WebRTC代理不起作用。確保Expressway核心伺服器證書具有客戶端EKU。這是使用者選擇對來自公共CA的所有憑證進行簽名的常見使用案例。由於公共CA在證書中不包括客戶端EKU，因此統一通訊遍歷區域將變為活動狀態。

要啟用UC區域，快速修復方法是關閉Expressway E上的EKU檢查。這將顯示UC區域。但是，SSH隧道保持非活動狀態。從今天起，2222上的SSH隧道通訊需要驗證客戶端EKU。

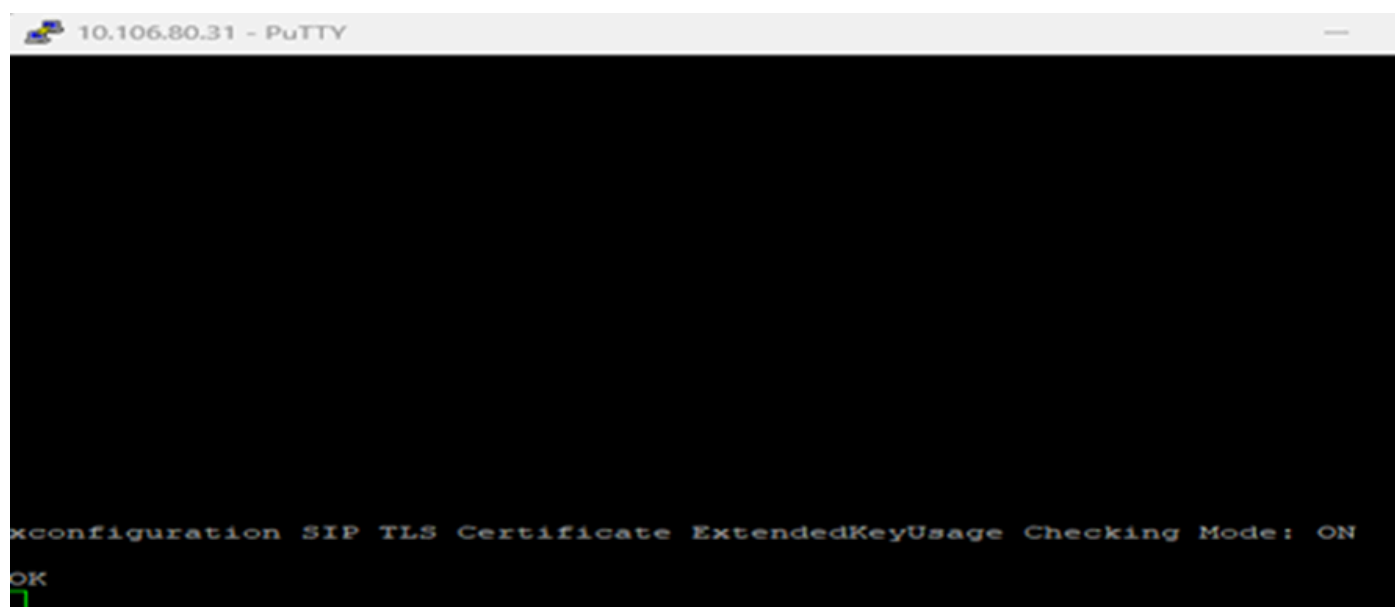
MRA客戶端登入和WebRTC代理功能無法正常工作。您可能不得不求助於私有CA。

測試用例1

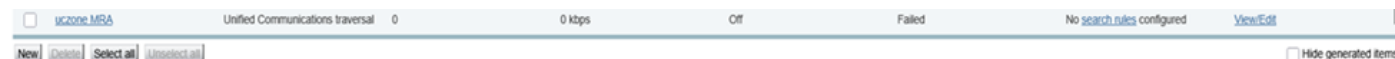
- 當Expressway E上的EKU檢查為「ON」時
- 當Expressway核心上的客戶端和伺服器證書僅具有伺服器EKU時
- UC區域狀態失敗

開啟Expressway-Edge ExtendedKeyUsage。

xconfiguration SIP TLS Certificate ExtendedKeyUsage檢查模式：於：



統一通訊區域故障：



User: admin Access: Read-write System host name: vcs8c System time: 12:24 IST

Language: en_US SIN: 007E452D Version: X15.5

Expressway E日誌顯示，其中10.106.80.16 = Expressway核心，10.106.80.31 = Expressway邊緣

：

| Results | |
|-------------------------------|--|
| 2026-03-29T12:24:39.839+05:30 | fvcs: 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 | fvcs: 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 | fvcs: 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 | fvcs: 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 | fvcs: 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" |

測試用例2

- Expressway E上的EKU檢查處於關閉狀態時
- 當Expressway核心上的客戶端和伺服器證書僅具有伺服器EKU時
- UC區域狀態為「活動」

關閉Expressway E上的EKU檢查。

xconfiguration SIP TLS Certificate ExtendedKeyUsage檢查模式 : Off

```

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

```

統一通訊區活動 :

但是，ssh隧道仍然失敗：

| 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事件日誌：

Results

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

條件2.1:成功案例

CA 1 =內部CA

CA 2 =公共CA

- 其中Expressway核心客戶端證書由CA 1 (內部CA) 簽名並包括，客戶端/伺服器EKU都包括。
 -
- Expressway核心伺服器證書由CA 2公共CA簽署，僅包括伺服器EKU。
- Expressway邊緣伺服器證書由CA 2公共CA簽署，僅包括伺服器EKU。
- Expressway邊緣客戶端證書由CA 2公共CA簽署，僅包括伺服器EKU。

Exp C x15.5

```
Client cert = Client/Server ECU by CA1
Server cert = Server ECU by CA2
```

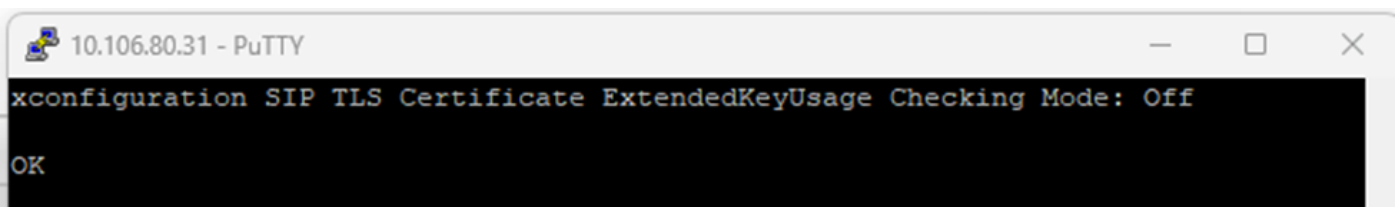
-----UC Zone-----

Exp E x15.5

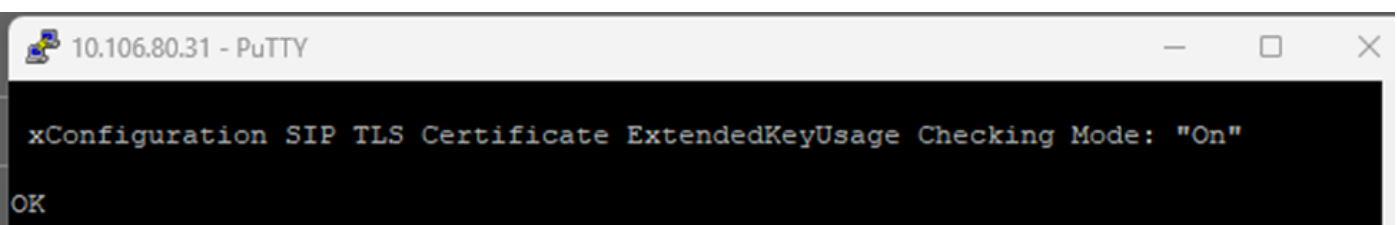
```
Client cert = Server ECU by CA2
Server cert = Server ECU by CA2
```

此條件是一個成功案例。無論EKU檢查模式是否為ON/OFF，統一通訊區域和SSH隧道都變為活動狀態。MRA客戶端工作。

Expressway邊緣EKU檢查是關閉還是開啟並不重要。Expressway核心客戶端證書包含客戶端EKU:

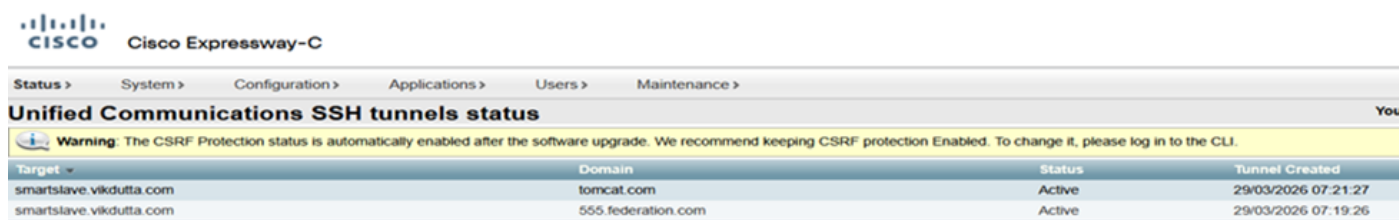


```
10.106.80.31 - PuTTY
xConfiguration SIP TLS Certificate ExtendedKeyUsage Checking Mode: Off
OK
```



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

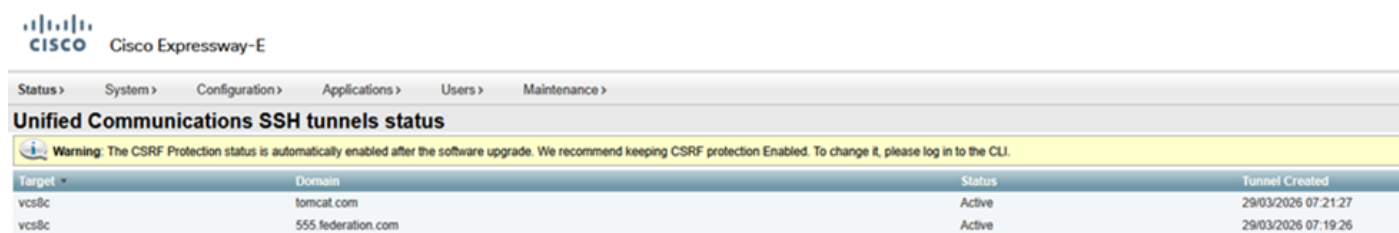
Expressway核心活動狀態上的SSH隧道：



The screenshot shows the Cisco Expressway-C management interface. At the top, there is a navigation bar with links for Status, System, Configuration, Applications, Users, and Maintenance. Below this is the title 'Unified Communications SSH tunnels status'. A yellow warning banner 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 the warning is a table with the following data:

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

Expressway邊緣上處於活動狀態的SSH隧道：



The screenshot shows the Cisco Expressway-E management interface. It has a similar layout to the Expressway-C interface, with a navigation bar and a title 'Unified Communications SSH tunnels status'. A yellow warning banner is present. Below the warning 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 |

統一通訊MRA區域狀態處於活動狀態：

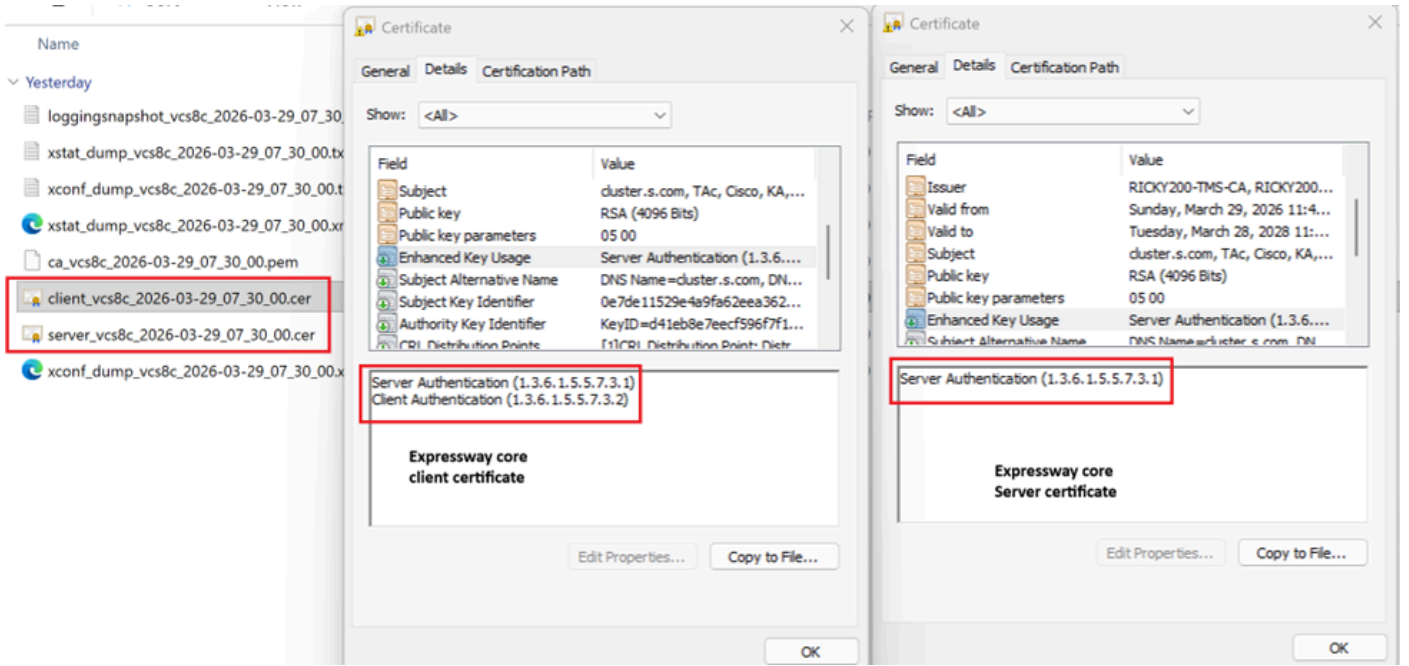


The screenshot shows the Cisco Expressway management interface for a Unified Communications MRA region. The region name is 'uczone_MRA'. The status is 'Active'. The table below shows the following data:

| Unified Communications traversal | 0 | 0 kbps | Off | Active | No search rules configured | View/Edit |
|----------------------------------|---|--------|-----|--------|----------------------------|-----------|
| <input type="checkbox"/> | | | | | | |

At the bottom of the interface, there is a footer with the following information: 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客戶端證書具有伺服器EKU和客戶端EKU。
- Expressway核心伺服器證書只有伺服器EKU。



MRA客戶端登入並註冊：

The screenshot shows the Cisco Jabber interface with a 'Connection Status' window open. The window title is 'Cisco Jabber' and the version is 'Version 12.6.1 (284405)'. The status is as follows:

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

The IP address '10.106.79.162 (CCMCIP - Expressway) (IPv4)' and the device name 'CSFHanu' are highlighted with a red box in the original image.

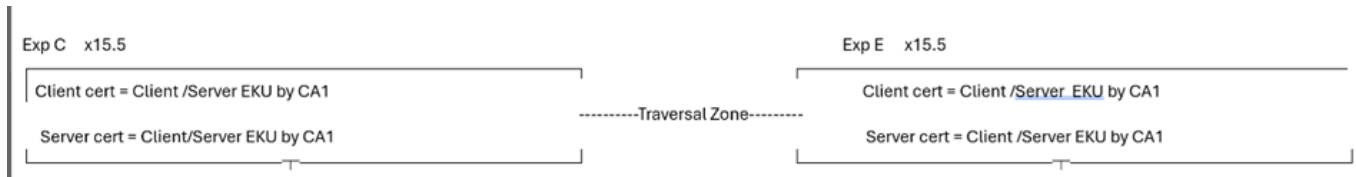


附註：比較並注意MRA和WebRTC代理在證書中存在的EKU。它是工作部署和非工作部署的比較。

條件3:使用私有CA簽署所有憑證

CA 1 =內部CA

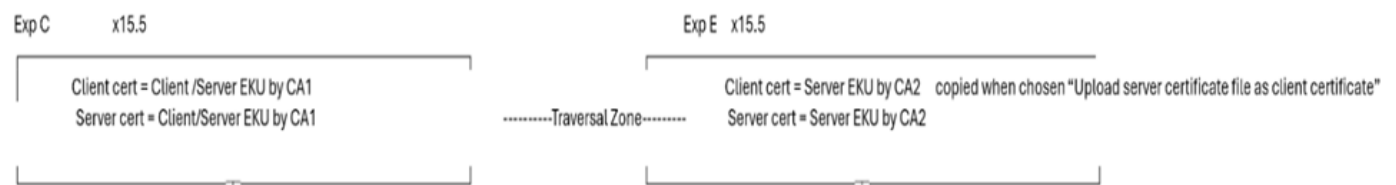
CA 2 = 公共CA



在條件3中，所有憑證皆由內部CA(CA1)簽署。

- 當Expressway-E發出TLS連線時，CA 1根/中間需要與遠端實體交換。如果遠端沒有功能或不允許上傳私有CA證書，則TLS連線不成功。
- 如果私有證書不在OS信任儲存中，MRA客戶端將獲得證書以接受彈出視窗。

條件4: Expressway邊緣具有公共證書 (僅包含伺服器EKU)



在條件4中，Expressway核心客戶端和伺服器證書是(CA1)內部CA簽名，並且客戶端和伺服器EKU都存在。Expressway E伺服器證書為公共CA簽名，並且只有伺服器EKU。將伺服器證書複製到客戶端證書儲存中，選擇上傳伺服器證書檔案作為客戶端證書。

在條件4中，當與遠端建立TLS連線時，如果Expressway -E傳送TLS客戶端hello，則遠端必須禁用客戶端EKU檢查（因為客戶端證書沒有客戶端身份驗證EKU），否則TLS連線不成功。

根據使用者部署和使用案例，在現場可以有更多的條件或情景，但由於我的思路有限，無法涵蓋所有情況。然而，需要記住的要點是：

- #如果在TLS握手期間Expressway成為客戶端，則客戶端證書將呈現給對等體。
- #IF Expressway在TLS握手期間成為伺服器；伺服器證書呈現給對等體。

該推理已結合這些測試用例進行確立。

案例 1

對於此情況，Expressway會在與Webex進行MTLS握手期間顯示客戶端證書。

Webex會議的視訊通話：

呼叫流Jabber -à CUCM -à Exp Core —à Exp Edge —à Webex示例

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邊緣具有使用此序列號(2f0000004c869c77c8981becde00000000004c)的客戶端證書。

Expressway Edge在TLS協商期間向'Webex'傳送客戶端hello，然後傳送客戶端證書。

序列號2f0000004c869c77c8981becde00000000004c:

1. 在mTLS協商期間，Expressway Edge將客戶端hello(pkt= 13699)傳送到「Webex」。
2. Webex向Expressway Edge(pkt=13701)傳送伺服器hello。
3. Webex將其憑證傳送到Expressway Edge(pkt=13711)。
4. Webex請求Expressway邊緣證書「CertificateRequest」(pkt=13715)。
5. Expressway Edge將其證書傳送到Webex(pkt=13718)。

(螢幕截圖)

Length: 2936
 Certificates Length: 2933
 Certificates (2933 bytes)
 Certificate Length: 2934

```

Certificate [..]: 308207ee308206d6a0030201020132f0000004c869c77c8981becde0000000004c300006092a864806f700101000500304f31133011000a0992260993f22c6401191603636fd3118301006
  signedCertificate
    version: v3 (2)
    serialNumber: 0x2f000004c869c77c8981becde0000000004c
    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)
  
```

來自Expressway邊緣的客戶端證書：

| 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 |
| loggingsnapshot_smartslave_2026-03-24_11_55... | ✓ | | | 718 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.bt | ✓ | | | 69 KB |
| xstat_dump_smartslave_2026-03-24_11_55_47.xml | ✓ | | | 120 KB |

| Field | Value |
|--------------------------|---------------------------------|
| Version | V3 |
| Serial number | 2f000004c869c77c8981becd... |
| 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, flk |

2f000004c869c77c8981becde0000000004c

案例 2

Expressway在mTLS握手期間成為伺服器實體，並顯示其伺服器證書：

當Expressway提供伺服器證書時，Expressway具有超過5061的安全鄰居區域，其驗證名稱為ON。

Expressway節點x15.5和Expressway節點x8.11.4之間的安全鄰居區域：

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

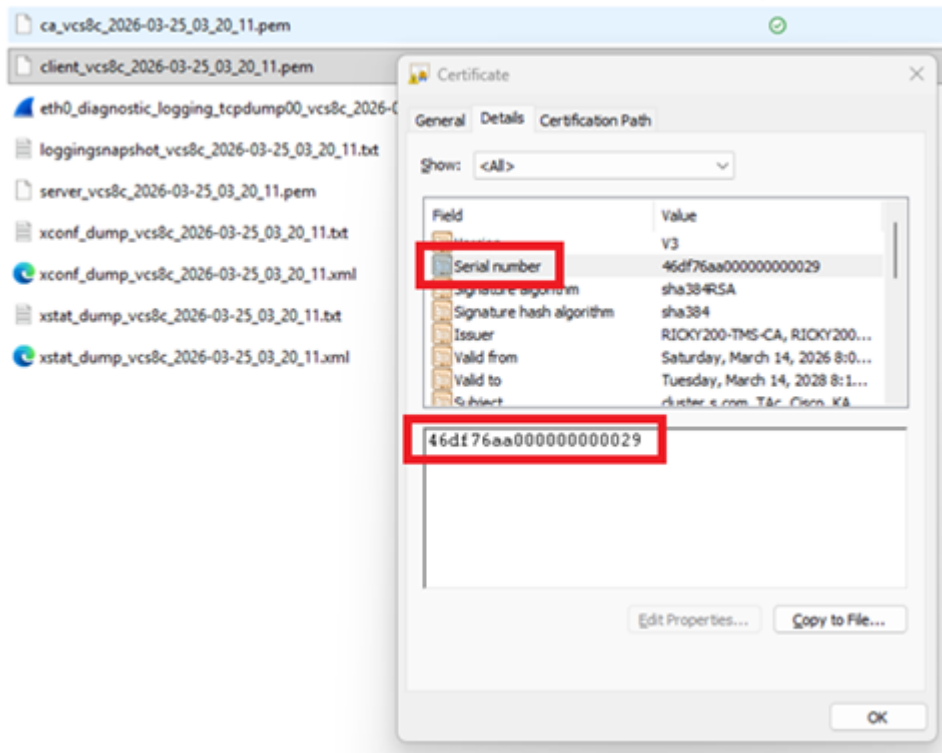
10.106.80.15 (x8.11.4) sends client certificate (pkt=744)

```
732 2026-03-25 15:10:17.83251 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 15:10:17.83259 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 29457 → 5061 [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=4070042729
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=2092 Win=32096 Len=0 TSval=2013756950 TSecr=4070042729
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=3681 Win=32096 Len=0 TSval=2013756959 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 [-]: 308207d13082069a003020102020a46d76aa0000000002330006092a864886f78d01010c050030493113301060a0992268993f22c6401191603636f6d3118301606a0992268993f22c...
signedCertificate
version: v3 (2)
serialNumber: 0x46df76aa000000000029
signature (sha1WithRSAEncryption)
algorithm: id-1.2.840.113549.1.1.12 (sha1WithRSAEncryption)
issuer: rdnSequence (0)
rdnSequence: 3 items (id-at-commonName=RICKY200-THS-CA,dc=RICKY200,dc=com)
validity

```
0030 f7 0d 01 01 0c 05 00 30 49 31 13 30 11 06 0a 09 ..
0040 92 26 89 93 f2 2c 64 01 19 16 03 63 6f 6d 31 18 -I
0050 30 16 06 0a 09 92 26 89 93 f2 2c 64 01 19 16 08 0-
0060 52 49 43 4b 59 32 30 30 31 18 30 16 06 03 55 0a R1
0070 03 13 0f 52 49 43 4b 59 32 30 30 2d 54 4d 53 2d ..
0080 43 41 30 1e 17 0d 32 36 30 33 31 34 30 32 33 37 G
0090 34 30 5a 17 0d 32 38 30 33 31 34 30 32 34 37 34 4e
00a0 30 5a 30 5d 31 0b 30 09 06 03 55 04 06 13 02 49 0i
00b0 4e 31 0b 30 09 06 03 55 04 06 13 02 4b 41 31 0b NI
00c0 30 09 06 03 55 04 07 13 02 4b 41 31 0e 30 0c 06 0-
00d0 03 55 04 0a 13 05 43 69 73 63 6f 31 0c 30 0a 06 -L
00e0 03 55 04 0b 13 03 54 41 63 31 16 30 14 06 03 55 -L
00f0 04 03 13 0d 63 6c 75 73 74 65 72 2e 73 2e 63 6f ..
0100 6d 30 82 02 22 30 0d 06 09 2a 86 48 86 f7 0d 01 mE
0110 01 01 05 00 03 82 02 0f 00 30 82 02 0a 02 82 02 ..
0120 01 00 bb b8 6e df 38 83 82 57 37 17 1f c1 33 37 ..
0130 bc e7 60 2a 04 9a 7c f2 93 e5 ab 21 97 18 5d ..
0140 90 89 46 67 56 b3 e1 68 01 8c b1 98 f2 dc f7 2b ..
0150 1c 7d a6 03 13 aa e5 b8 b8 21 90 7c ec 95 e0 34 -I
```

此螢幕截圖顯示序列號匹配的伺服器證書：



測試案例3:MRA客戶端已設定為登入， workflow包括Expressway核心與CUCM之間的流量伺服器證書驗證。

10.106.80.16 = Expressway核心x15.5

10.106.80.38 = CUCM

- Exp C 16在6972 TFTP上傳送客戶端hello。
- Exp C 16在TLS握手期間傳送客戶端證書。

The image shows a Wireshark capture of a TLS handshake. The packet list pane highlights the Certificate (3643) and Certificate Verify (3645) packets. The packet details pane shows the structure of the Certificate, including the serial number 46d176aa0000000029.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|--------------|--------------|----------|--------|--|
| 552 | 2026-03-25 17:21:14.861118 | 10.106.80.16 | 10.106.80.16 | TCP | 74 | 33302 → 6972 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2511750974 TSecr=0 WS=12 |
| 553 | 2026-03-25 17:21:14.861536 | 10.106.80.16 | 10.106.80.16 | TCP | 74 | 6972 → 33302 [SYN, ACK] Seq=60 Ack=2898 Len=0 MSS=1460 SACK_PERM TSval=2511750974 TSecr=2511750974 WS=12 |
| 554 | 2026-03-25 17:21:14.861558 | 10.106.80.16 | 10.106.80.16 | TCP | 66 | 33302 → 6972 [ACK] Seq=508 Ack=2897 Win=78656 Len=0 TSval=2511750974 TSecr=2511750974 |
| 555 | 2026-03-25 17:21:14.861576 | 10.106.80.16 | 10.106.80.16 | TLSv1.2 | 583 | Client Hello (SHA-256, TLSv1.2) |
| 556 | 2026-03-25 17:21:14.861595 | 10.106.80.16 | 10.106.80.16 | TLSv1.2 | 2324 | Server Hello |
| 557 | 2026-03-25 17:21:14.861617 | 10.106.80.16 | 10.106.80.16 | TCP | 66 | 33302 → 6972 [ACK] Seq=508 Ack=1449 Win=67584 Len=0 TSval=2511750974 TSecr=2511750974 |
| 558 | 2026-03-25 17:21:14.861624 | 10.106.80.16 | 10.106.80.16 | TLSv1.2 | 3524 | Certificate, Server Key Exchange |
| 559 | 2026-03-25 17:21:14.861628 | 10.106.80.16 | 10.106.80.16 | TCP | 66 | 33302 → 6972 [ACK] Seq=508 Ack=2897 Win=78656 Len=0 TSval=2511750974 TSecr=2511750974 |
| 560 | 2026-03-25 17:21:14.861631 | 10.106.80.16 | 10.106.80.16 | TLSv1.2 | 690 | Certificate Request, Server Hello Done |
| 561 | 2026-03-25 17:21:14.861634 | 10.106.80.16 | 10.106.80.16 | TCP | 66 | 33302 → 6972 [ACK] Seq=508 Ack=1531 Win=71216 Len=0 TSval=2511750974 TSecr=2511750974 |
| 562 | 2026-03-25 17:21:14.861639 | 10.106.80.16 | 10.106.80.16 | TLSv1.2 | 3643 | Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message |
| 563 | 2026-03-25 17:21:14.861700 | 10.106.80.16 | 10.106.80.16 | TCP | 66 | 6972 → 33302 [ACK] Seq=579 Ack=6573 Win=48544 Len=0 TSval=2511750998 TSecr=2511750998 |
| 564 | 2026-03-25 17:21:14.861638 | 10.106.80.16 | 10.106.80.16 | TCP | 1524 | 6972 → 33302 [ACK] Seq=3521 Ack=4897 Win=18784 Len=1448 TSval=2511750985 TSecr=2511750985 [TCP PDU reassembled in 565] |
| 565 | 2026-03-25 17:21:14.861671 | 10.106.80.16 | 10.106.80.16 | TLSv1.2 | 876 | New Session Ticket, Change Cipher Spec, Encrypted Handshake Message |
| 566 | 2026-03-25 17:21:14.861678 | 10.106.80.16 | 10.106.80.16 | TCP | 66 | 33302 → 6972 [ACK] Seq=4897 Ack=5779 Win=79360 Len=0 TSval=2511750988 TSecr=2511750988 |
| 567 | 2026-03-25 17:21:14.861691 | 10.106.80.16 | 10.106.80.16 | TLSv1.2 | 2542 | Application Data |
| 568 | 2026-03-25 17:21:14.861623 | 10.106.80.16 | 10.106.80.16 | TCP | 66 | 6972 → 33302 [ACK] Seq=5779 Ack=6573 Win=48544 Len=0 TSval=2511750994 TSecr=2511750994 |
| 569 | 2026-03-25 17:21:14.861692 | 10.106.80.16 | 10.106.80.16 | TLSv1.2 | 181 | Application Data |
| 570 | 2026-03-25 17:21:14.861706 | 10.106.80.16 | 10.106.80.16 | TCP | 1524 | 6972 → 33302 [ACK] Seq=5894 Ack=6573 Win=48544 Len=1448 TSval=2511750997 TSecr=2511750997 [TCP PDU reassembled in 569] |
| 571 | 2026-03-25 17:21:14.861713 | 10.106.80.16 | 10.106.80.16 | TCP | 66 | 33302 → 6972 [ACK] Seq=6573 Ack=7342 Win=83200 Len=0 TSval=2511750999 TSecr=2511750999 |
| 572 | 2026-03-25 17:21:14.861723 | 10.106.80.16 | 10.106.80.16 | TCP | 1524 | 6972 → 33302 [ACK] Seq=7342 Ack=6573 Win=48544 Len=1448 TSval=2511750997 TSecr=2511750997 [TCP PDU reassembled in 569] |
| 573 | 2026-03-25 17:21:14.861725 | 10.106.80.16 | 10.106.80.16 | TCP | 1524 | 6972 → 33302 [ACK] Seq=8790 Ack=6573 Win=48544 Len=1448 TSval=2511750998 TSecr=2511750998 [TCP PDU reassembled in 569] |
| 574 | 2026-03-25 17:21:14.861728 | 10.106.80.16 | 10.106.80.16 | TCP | 66 | 33302 → 6972 [ACK] Seq=6573 Ack=83200 Win=83200 Len=0 TSval=2511750999 TSecr=2511750999 |

Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 2923
 Handshake Protocol: Certificate
 Handshake Type: Certificate (11)
 Length: 2918
 Certificates Length: 2916
 Certificates (2916 bytes)
 Certificate Length: 2905
 Certificate [..]: 46d176aa0000000029
 signedCertificate
 version: v3 (2)
 serialNumber: 46d176aa0000000029
 signatureAlgorithm: sha384-RSA
 signature: sha384-RSA(Encryption)
 issuer: rdnSequence (0)
 issuer: rdnSequence (0) [..]: 1d-at-comonsec-RIOOY200-TS-CA,dc=RIOOY200,dc=com
 rdnSequence Item: 1 [..]: dc=com
 rdnSequence Item: 1 [..]: dc=RIOOY200
 rdnSequence Item: 1 [..]: 1d-at-comonsec-RIOOY200-TS-CA
 validFrom: notBefore: utcTime (0)
 validTo: notAfter: utcTime (0)

Expressway核心客戶端證書：

The image shows a Windows File Explorer window with a folder named 'ca_vcslc_2026-03-25_03_20_11.pem'. A 'Certificate' dialog box is open, displaying the details of a certificate. The 'Serial number' field is highlighted with a red box and contains the value '46d176aa0000000029'.

| Field | Value |
|--------------------------|---------------------------------|
| Version | v3 |
| Serial number | 46d176aa0000000029 |
| Signature algorithm | sha384-RSA |
| Signature hash algorithm | sha384 |
| Issuer | RIOOY200-TS-CA, RIOOY200... |
| Valid from | Saturday, March 14, 2026 8:0... |
| Valid to | Tuesday, March 14, 2026 8:1... |
| Subject | *.cn=*.com,*.cn=*.com,*.cn=... |

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。