Securing the Edge: Collaboration Certificates and Ciphers



Jerson Gamboa
Technical Consulting Engineer,
@Linkedin jerson-gamboa-32812015

LT de Leon
Technical Consulting Engineer
@Linkedin ltdeleon

Cisco Webex App

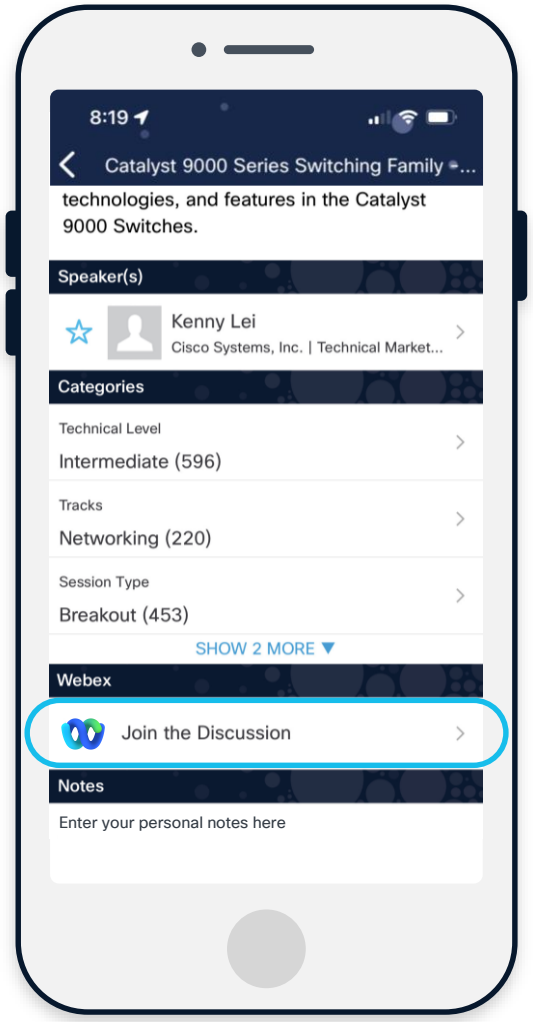
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 13, 2025.



© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Introduction

02 Reading Certificates

03 Certificate Extraction

04 MRA Certificates

05 TLS and Ciphers

06 Case Generator Scenarios

07 Upcoming!

© 2025 Cisco and/or its affiliates. All rights reserved.

Introduction

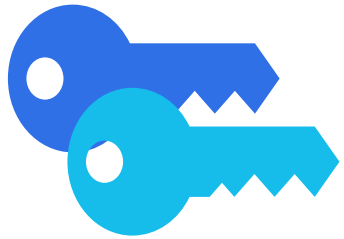
Acronym Glossary Slide

MRA = Mobile and Remote Access
PKI = Public Key Infrastructure
CSR = Certificate Signing Request
CA = Certificate Authority
CUCM = Cisco Unified Communications Manager
TLS = Transport Layer Security
ECDSA= Elliptic Curve Digital Signature Algorithm
EC= Elliptic Curve
RSA = Rivest–Shamir–Adleman

© 2025 Cisco and/or its affiliates. All rights reserved.

Public Key Infrastructure (PKI)

The PKI is a system allowing applications to interact securely using asymmetric encryption based on mathematically related public key/private key pairs.



Certificates are used to distribute public keys and establish the identity of the certificate owner.



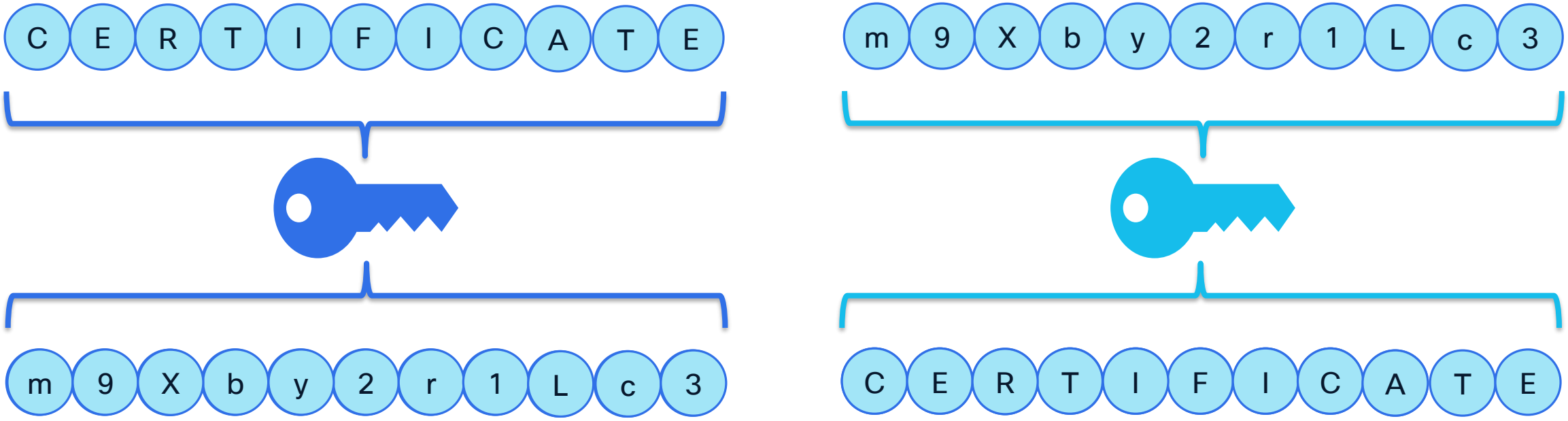
Certificate Authorities act as a trusted third-party mediator to validate that the party listed in the certificate owns the private key associated with the public key listed in the certificate.



© 2025 Cisco and/or its affiliates. All rights reserved.

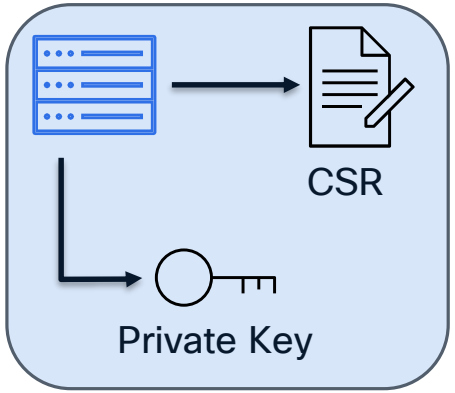
Public Key Infrastructure (PKI)

Information encrypted by a public key can only be decrypted using the corresponding Private Key, and information encrypted by a Private Key can only be decrypted by the corresponding Public Key.



© 2025 Cisco and/or its affiliates. All rights reserved.

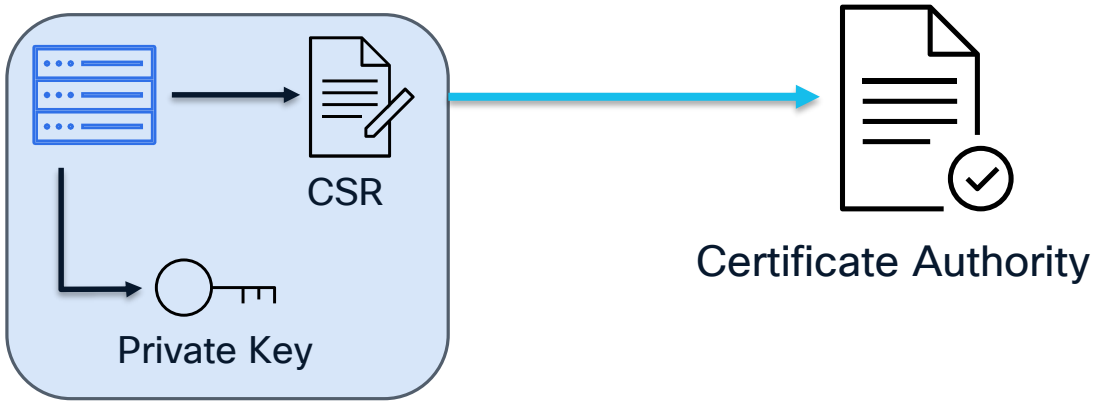
Certificate Signing Request (CSR)



- UC Server Generates the CSR which will be sent to a Certificate authority, and corresponding Private Key which will be store locally on the server

© 2025 Cisco and/or its affiliates. All rights reserved.

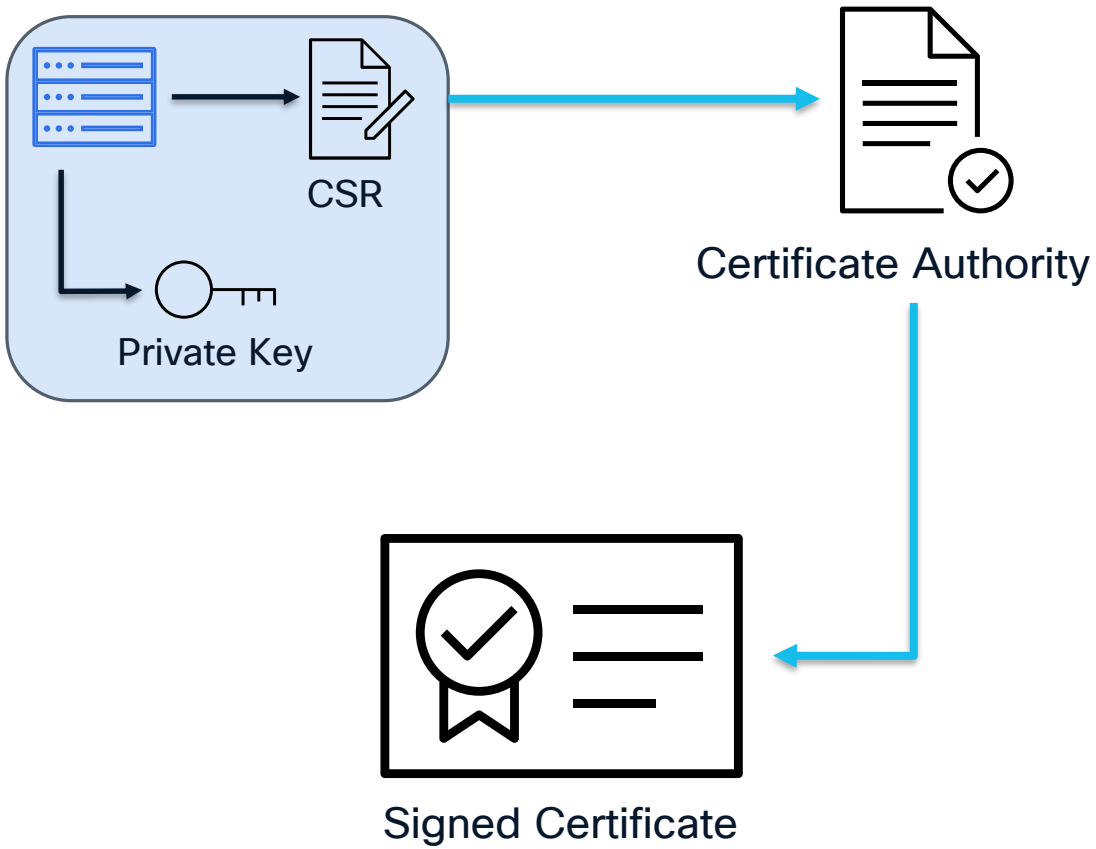
Certificate Signing Request (CSR)



- UC Server Generates the CSR which will be sent to a Certificate authority, and corresponding Private Key which will be store locally on the server
- The CSR is sent to the CA who verifies the signature in the CSR to prove the server possesses the private key that pairs with the public key provided

© 2025 Cisco and/or its affiliates. All rights reserved.

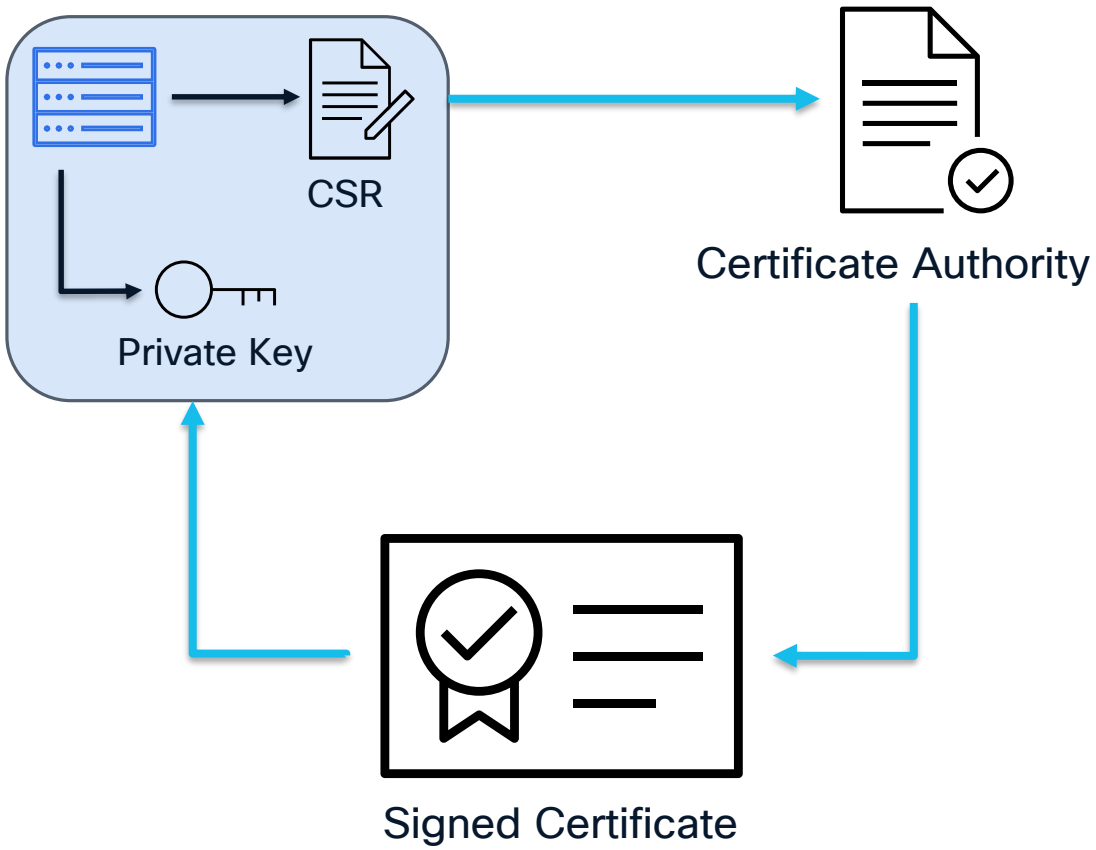
Certificate Signing Request (CSR)



- UC Server Generates the CSR which will be sent to a Certificate authority, and corresponding Private Key which will be store locally on the server
- The CSR is sent to the CA who verifies the signature in the CSR to prove the server possesses the private key that pairs with the public key provided
- The CA signs the certificate and provides the signed certificate back to the applicant

© 2025 Cisco and/or its affiliates. All rights reserved.

Certificate Signing Request (CSR)

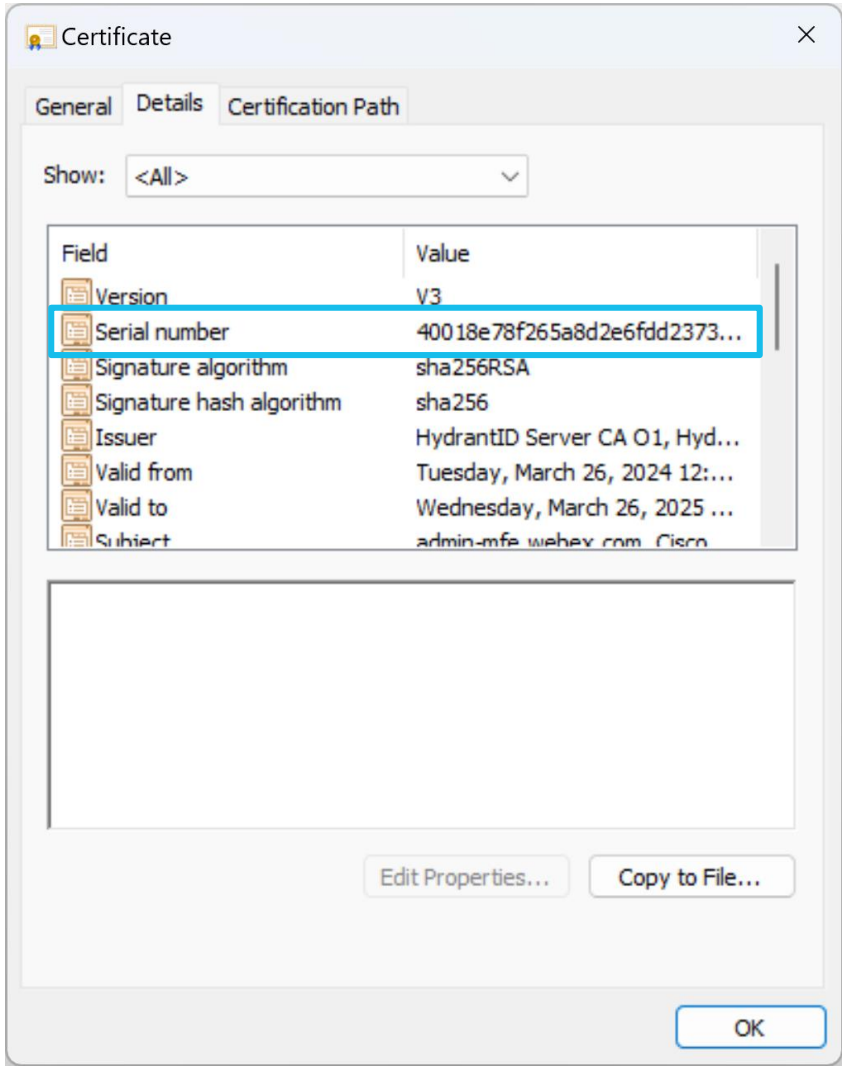


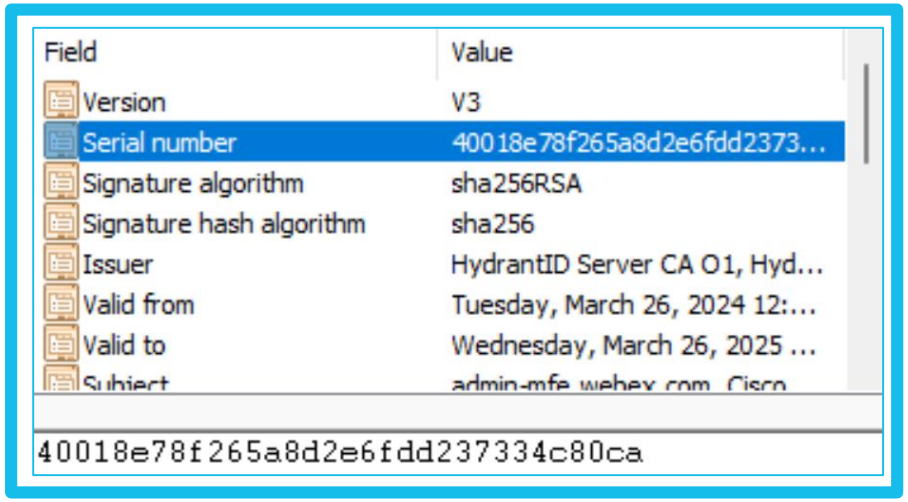
- UC Server Generates the CSR which will be sent to a Certificate authority, and corresponding Private Key which will be store locally on the server
- The CSR is sent to the CA who verifies the signature in the CSR to prove the certificate owner possesses the private key that pairs with the public key provided
- The CA signs the certificate and provides the signed certificate back to the applicant
- When loading the certificate back to the UC server the signed certificate is checked against the stored private key to ensure it is the appropriate certificate

© 2025 Cisco and/or its affiliates. All rights reserved.

Reading Certificates

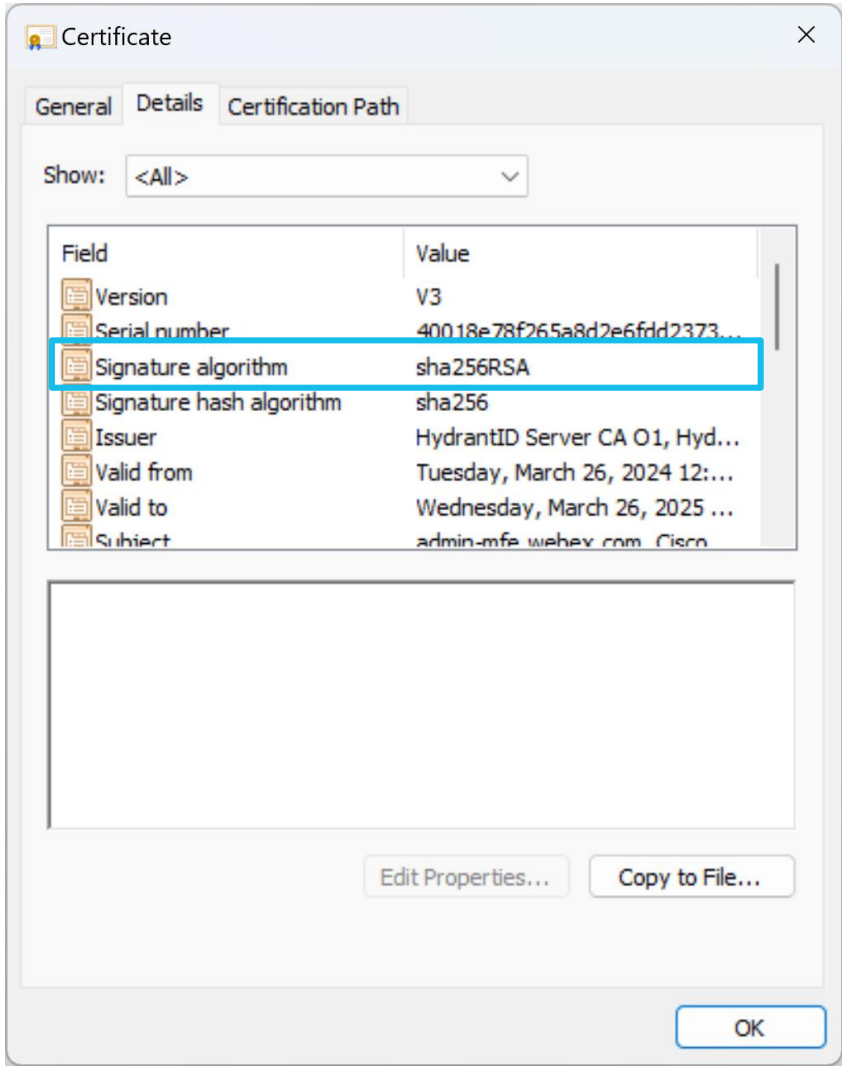
What's in a certificate? – Serial Number

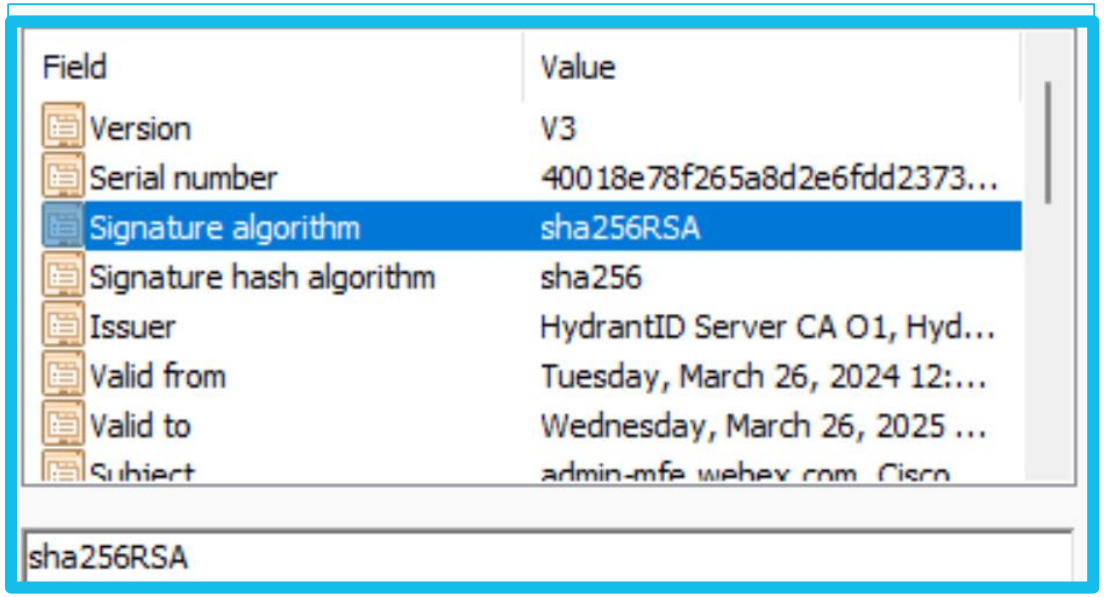




© 2025 Cisco and/or its affiliates. All rights reserved.

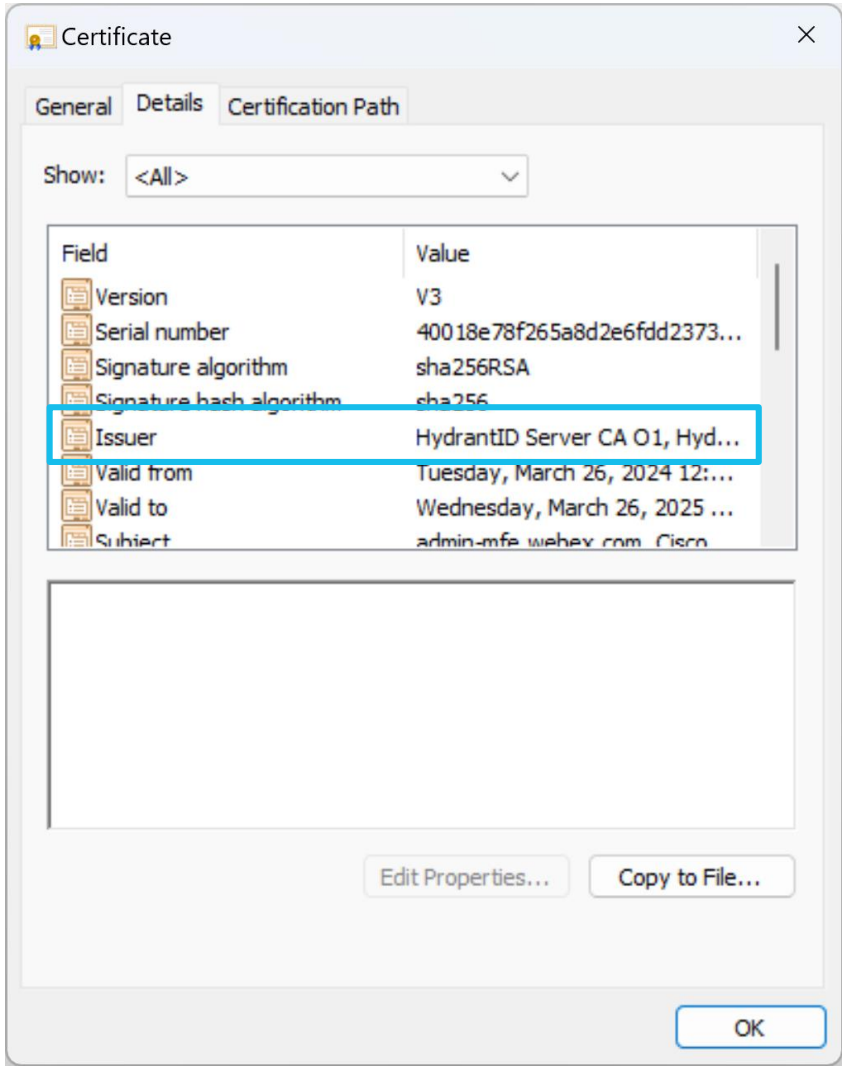
What's in a certificate? – Signature Algorithm

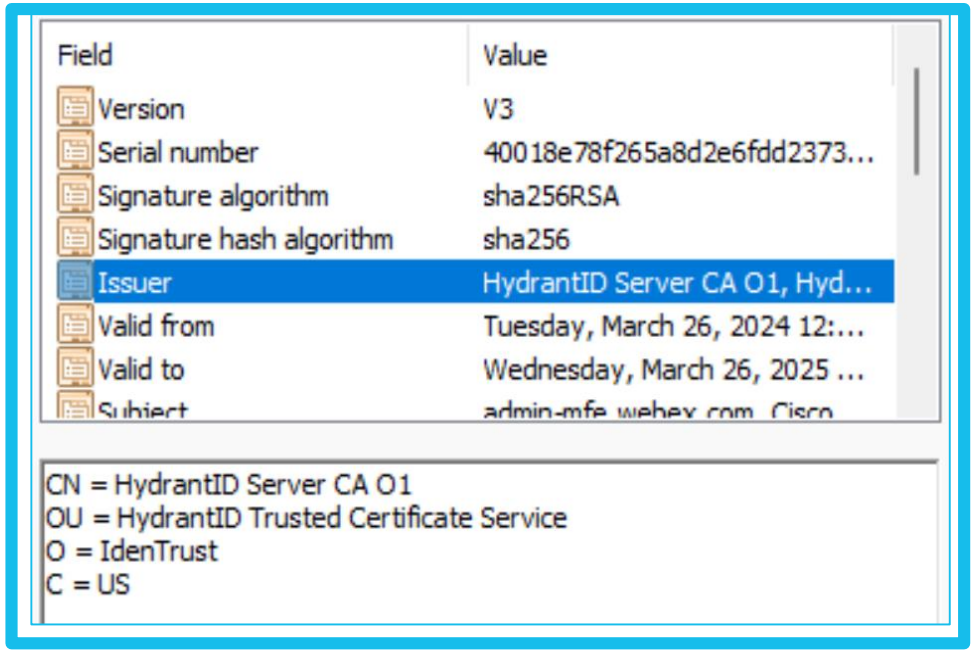




© 2025 Cisco and/or its affiliates. All rights reserved.

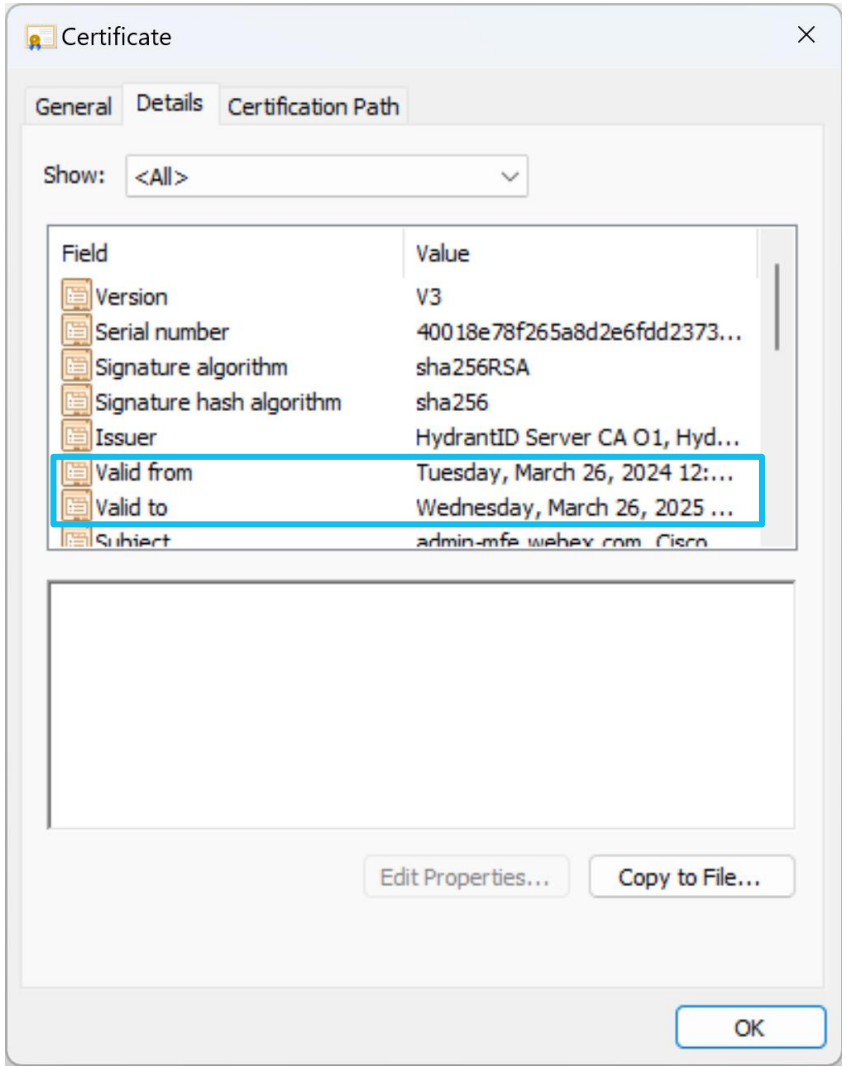
What's in a certificate? - Issuer

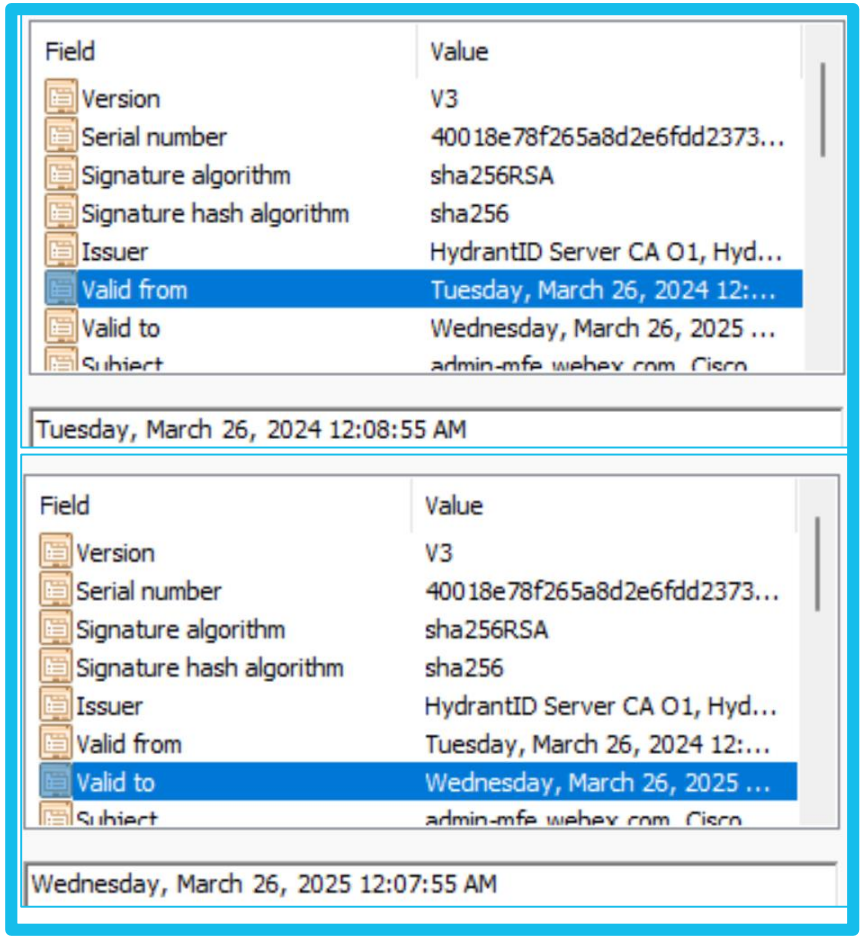




© 2025 Cisco and/or its affiliates. All rights reserved.

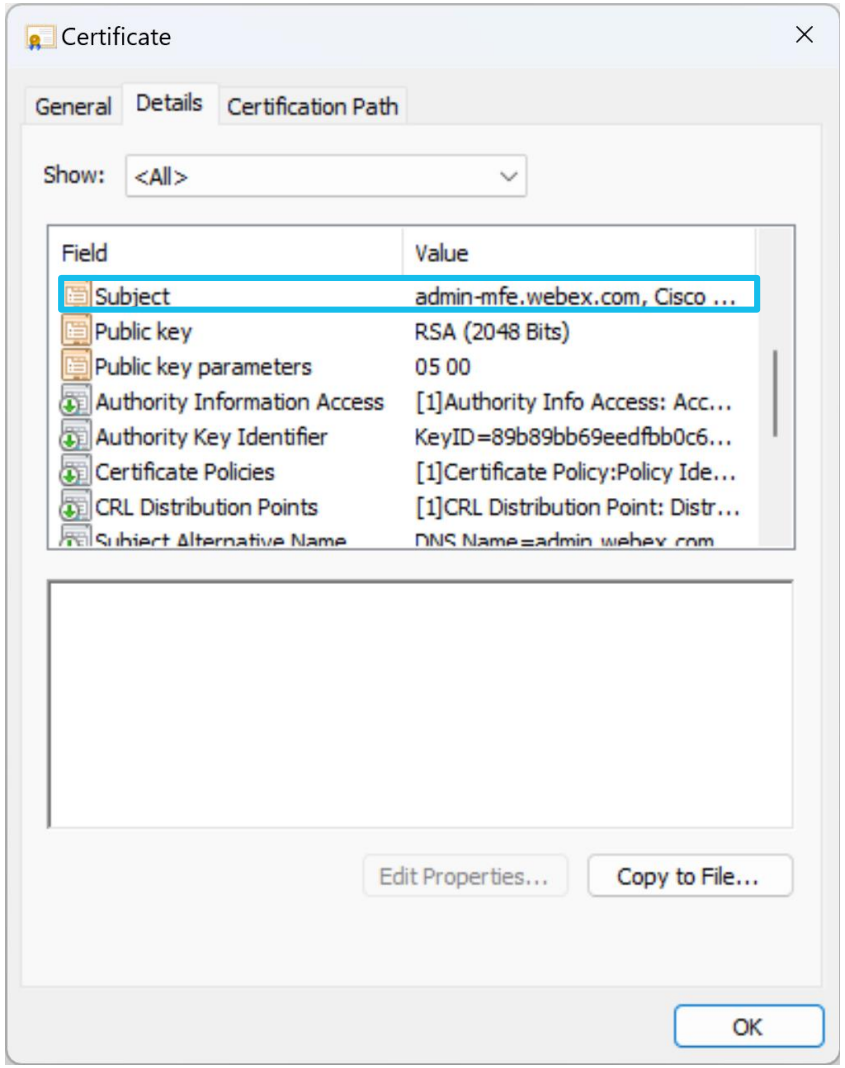
What's in a certificate? – Valid From/To

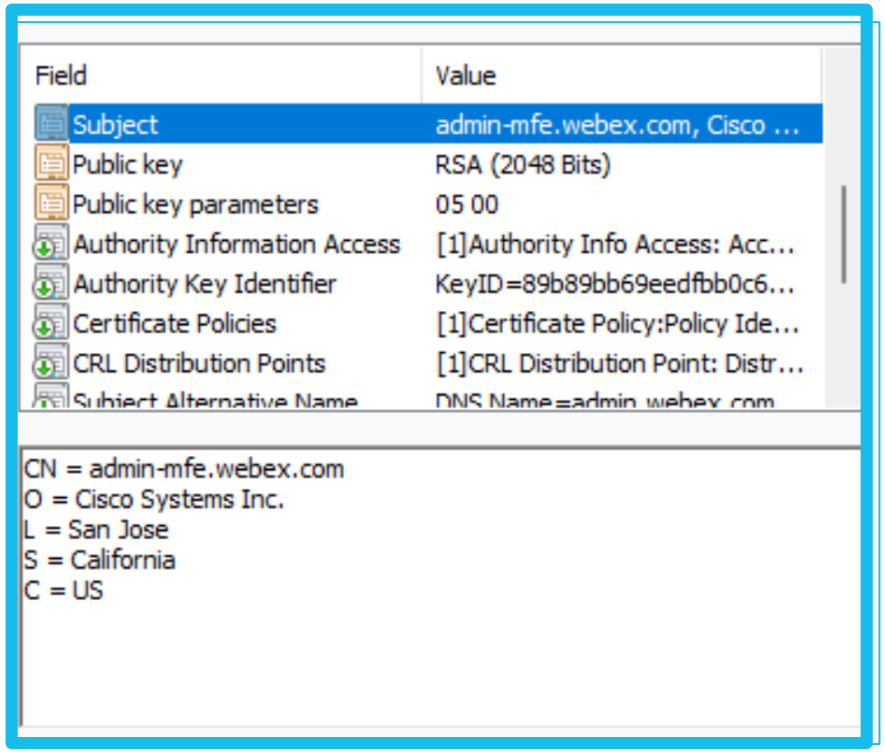




© 2025 Cisco and/or its affiliates. All rights reserved.

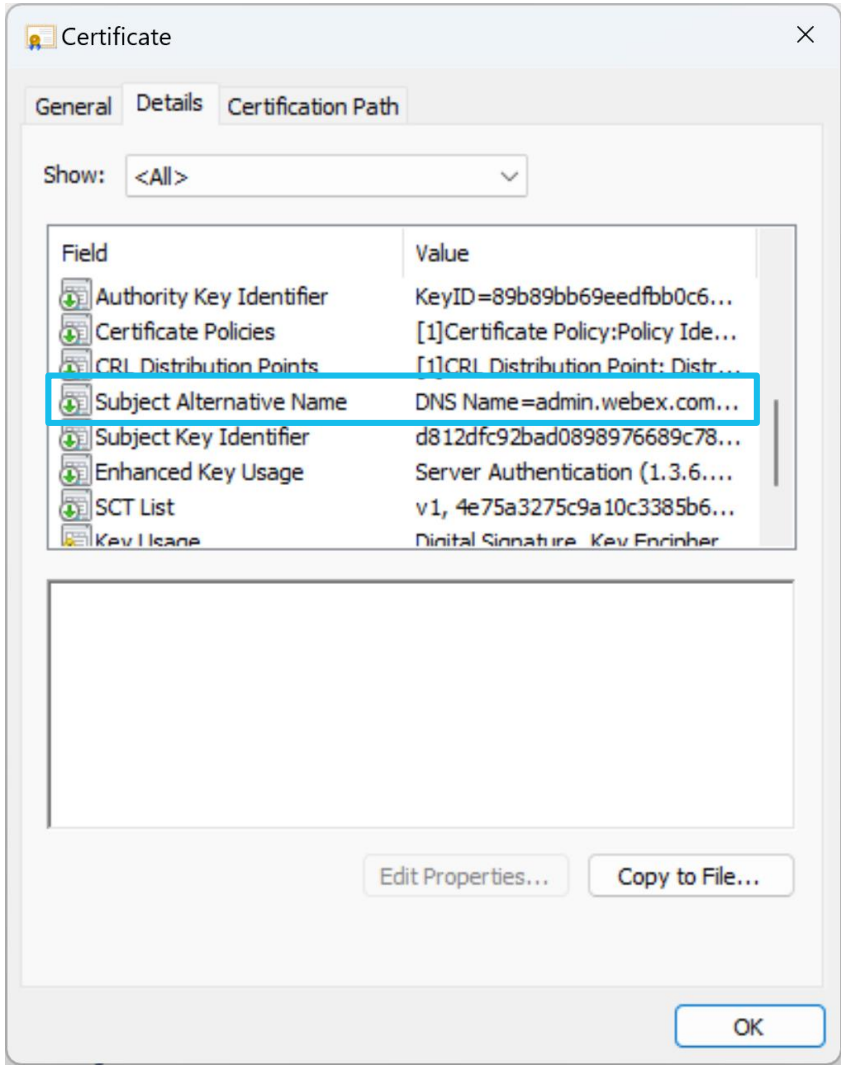
What's in a certificate? - Subject





© 2025 Cisco and/or its affiliates. All rights reserved.

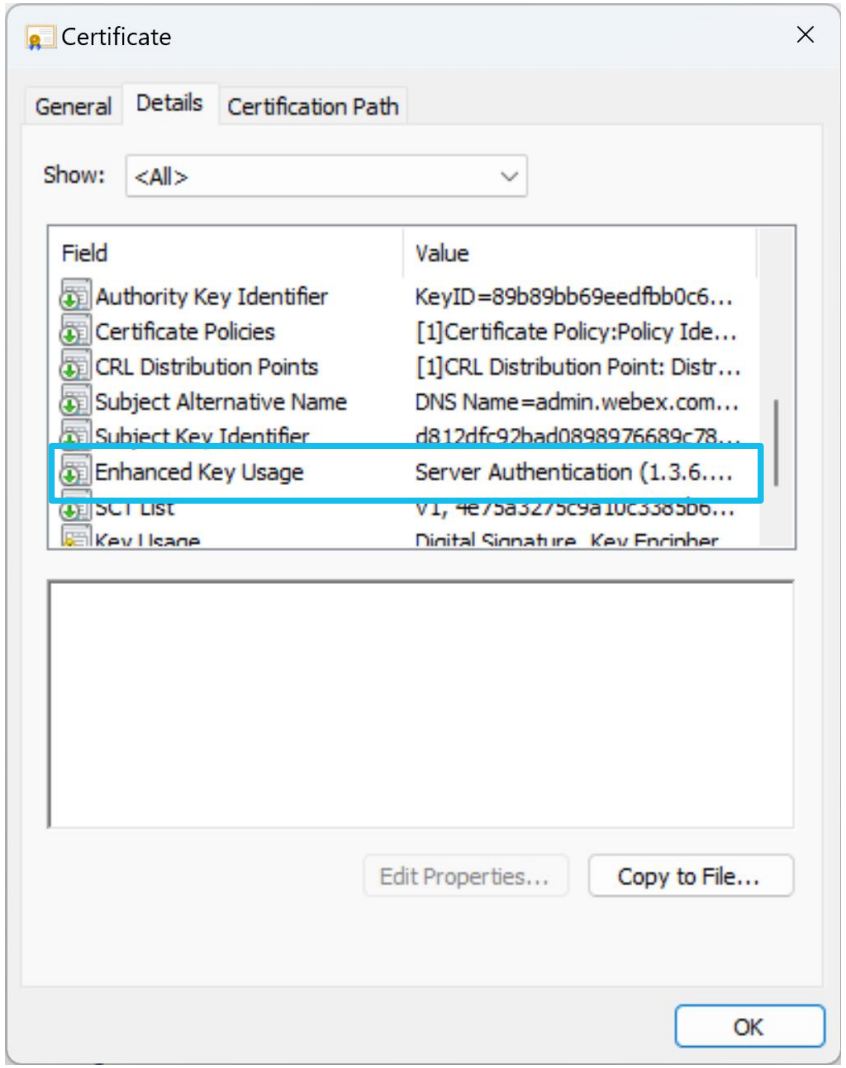
What's in a certificate? – Subject Alternative Name

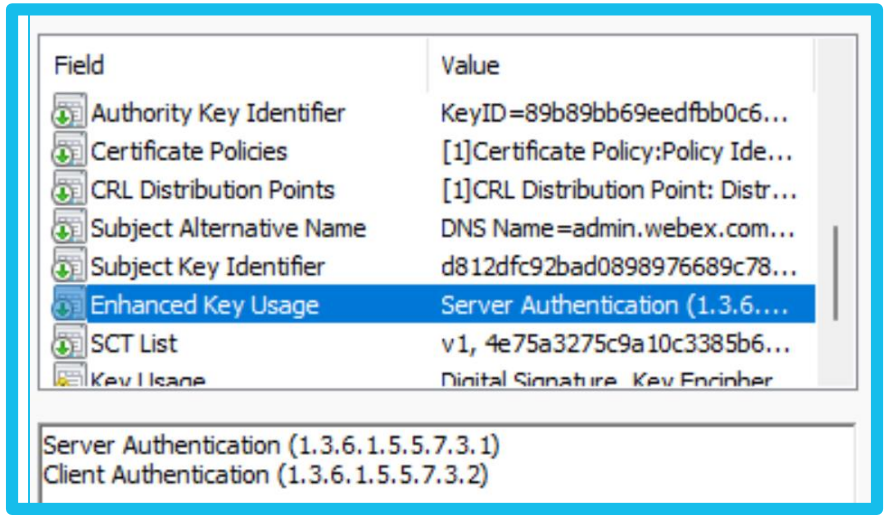




© 2025 Cisco and/or its affiliates. All rights reserved.

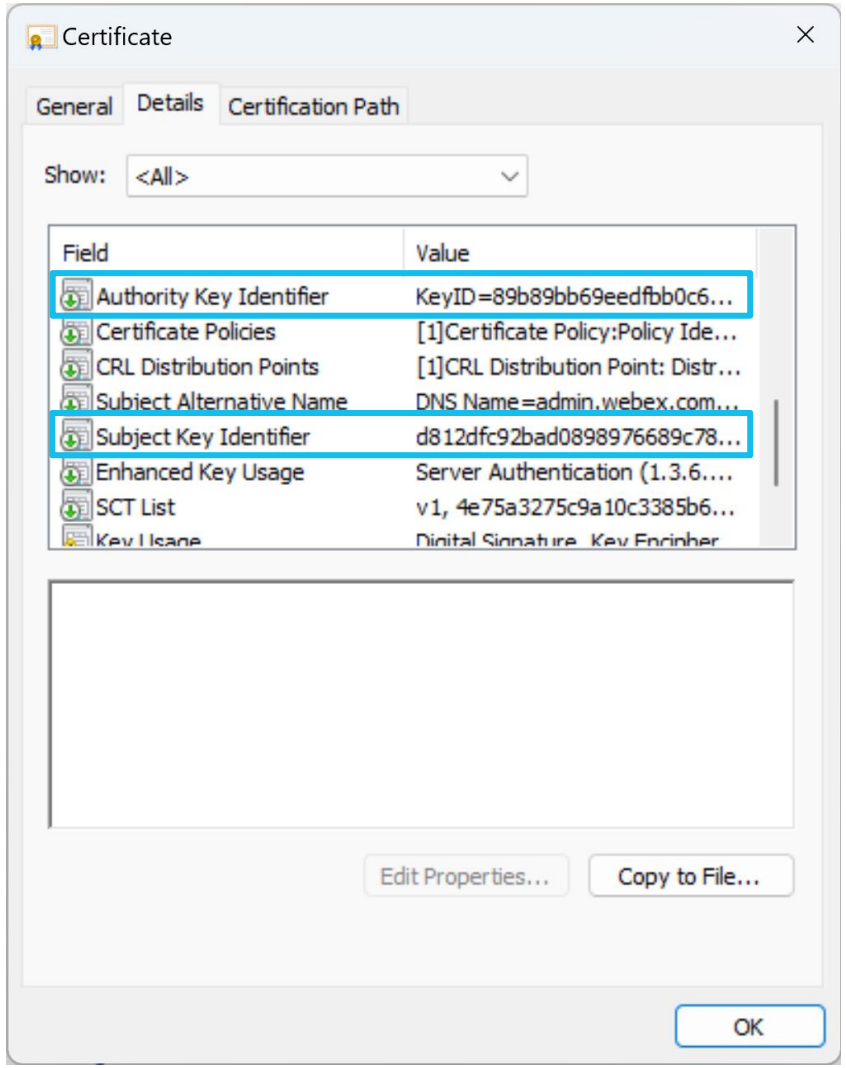
What's in a certificate? – Enhanced Key Usage

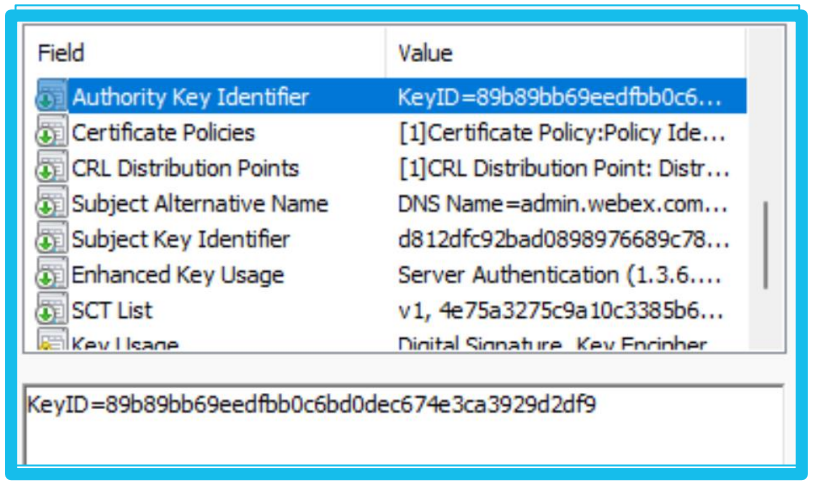


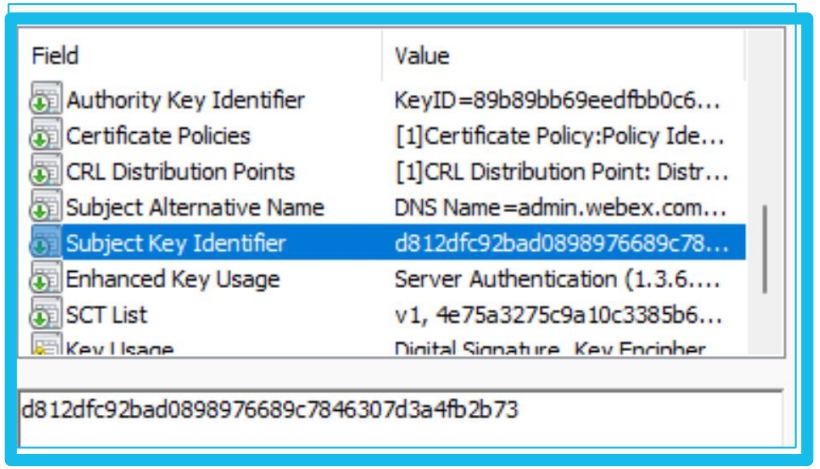


© 2025 Cisco and/or its affiliates. All rights reserved.

What's in a certificate? – Authority/Subject Key Identifier

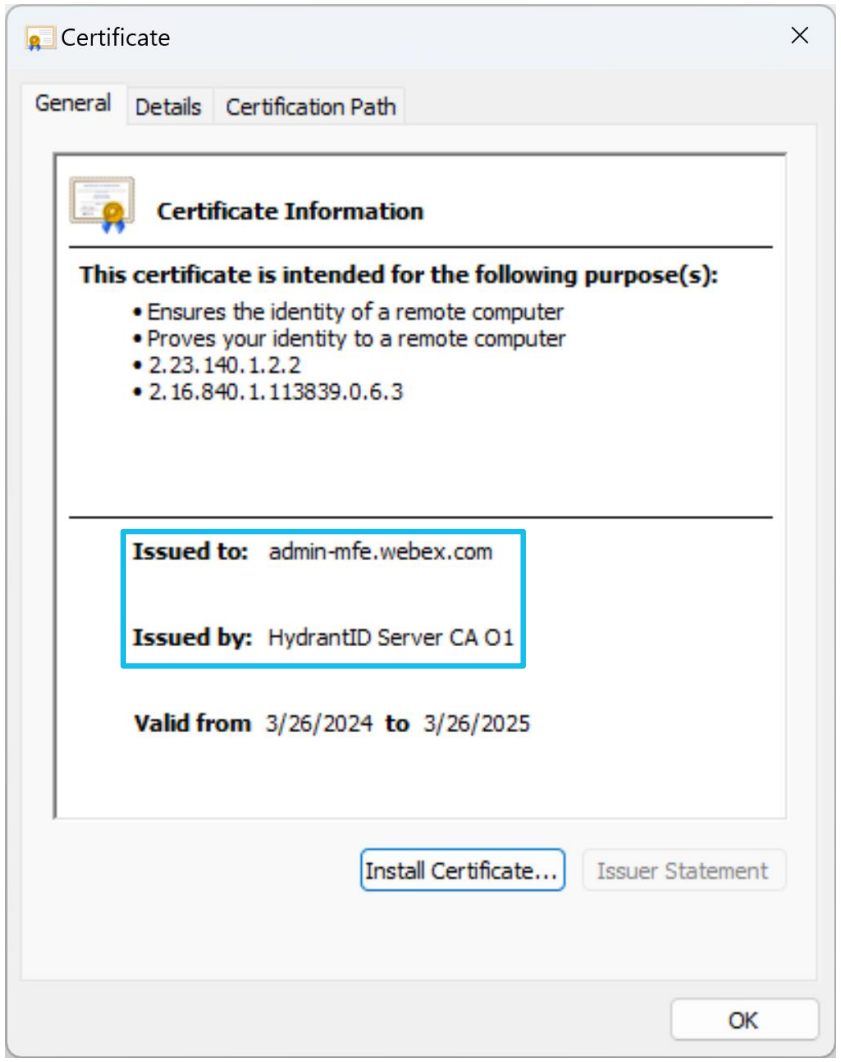


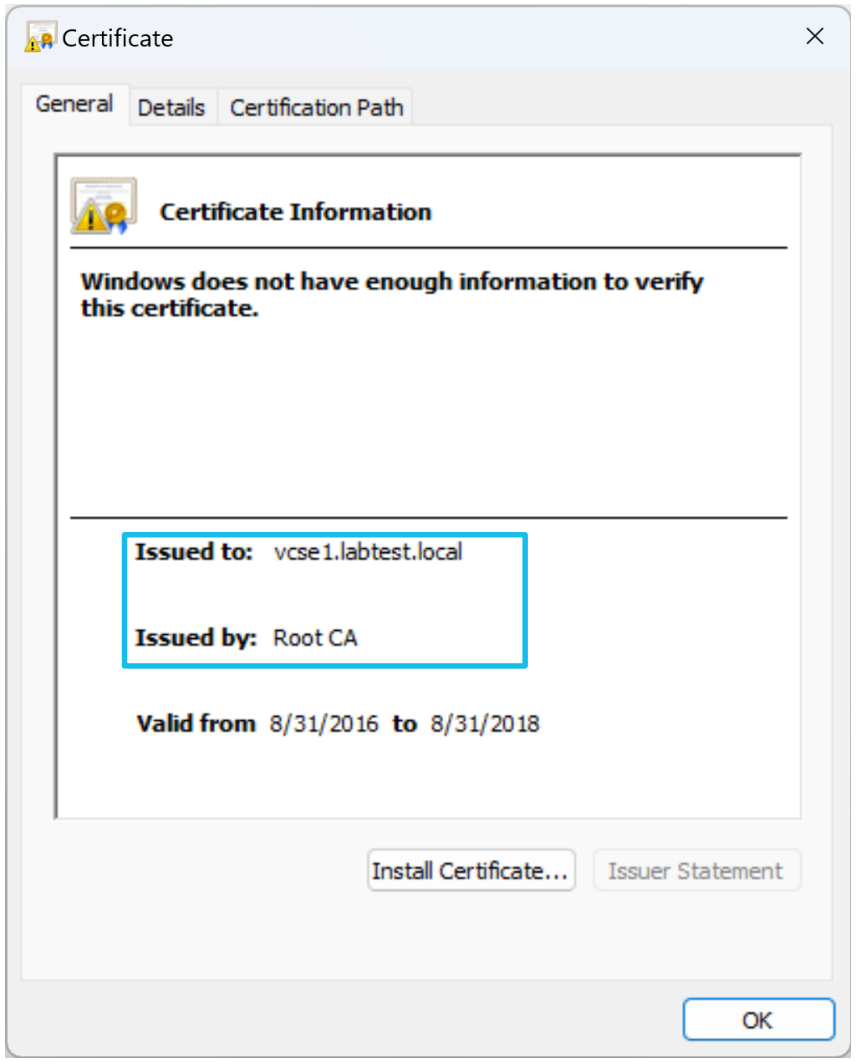




© 2025 Cisco and/or its affiliates. All rights reserved.

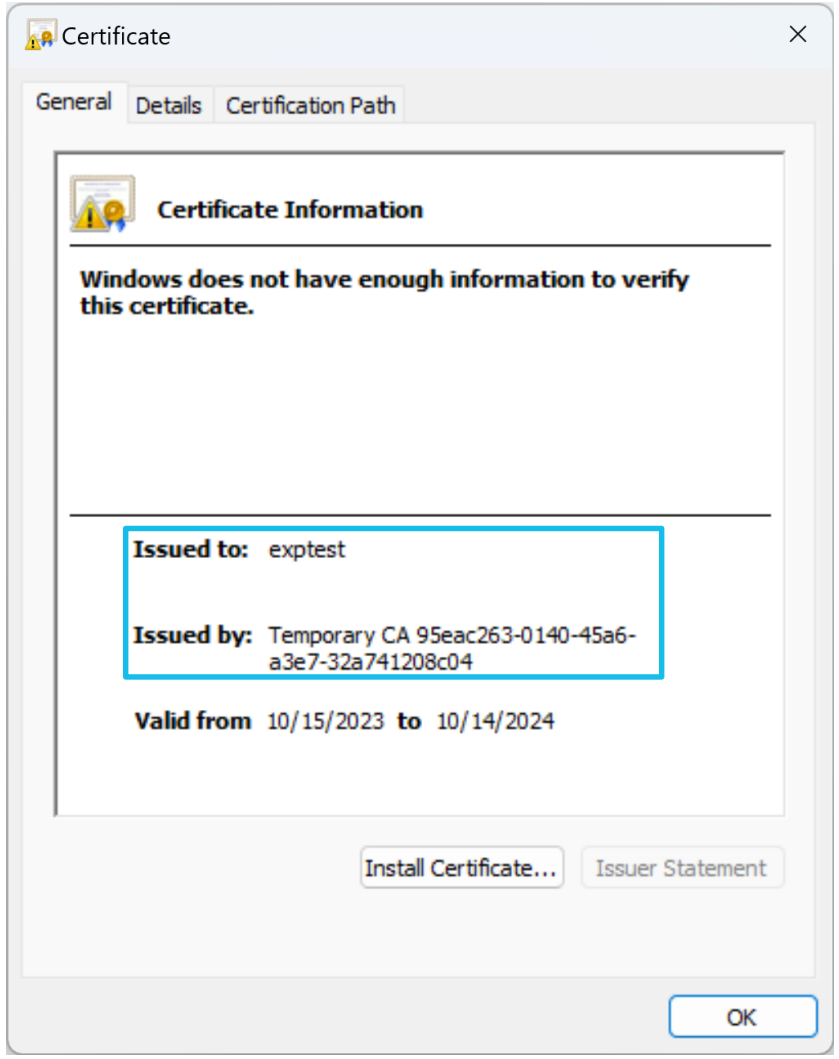
CA Signed Examples
(supported)

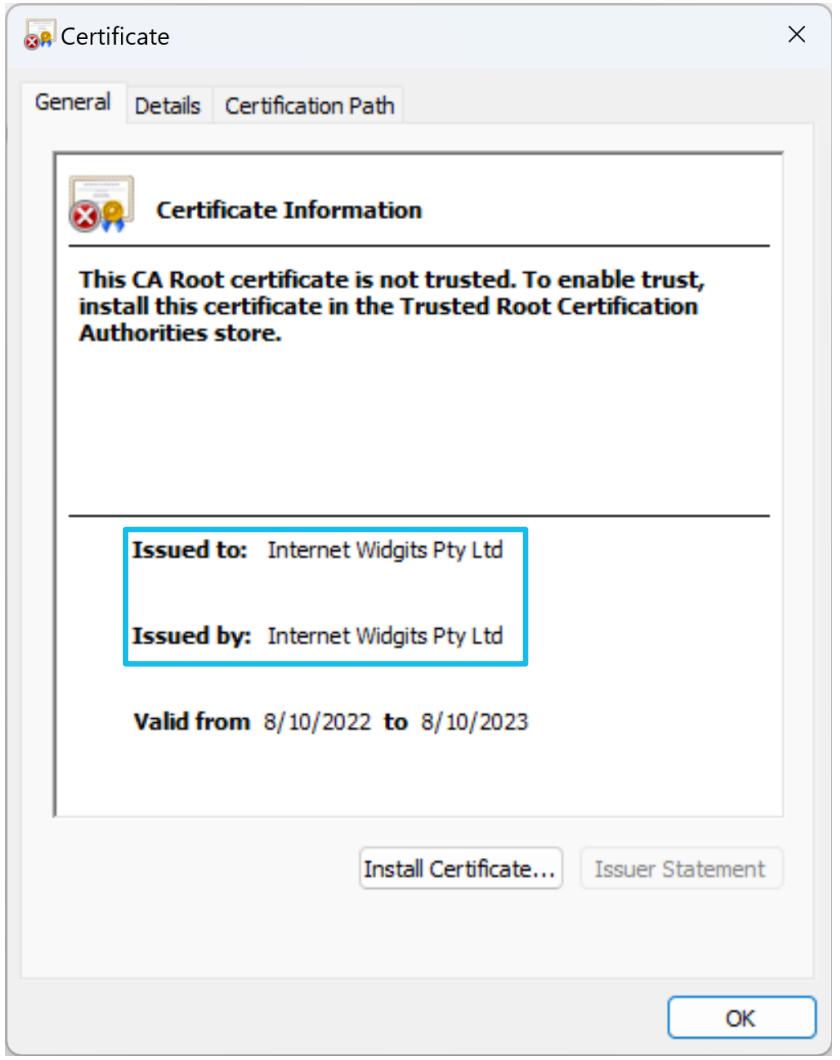




© 2025 Cisco and/or its affiliates. All rights reserved.

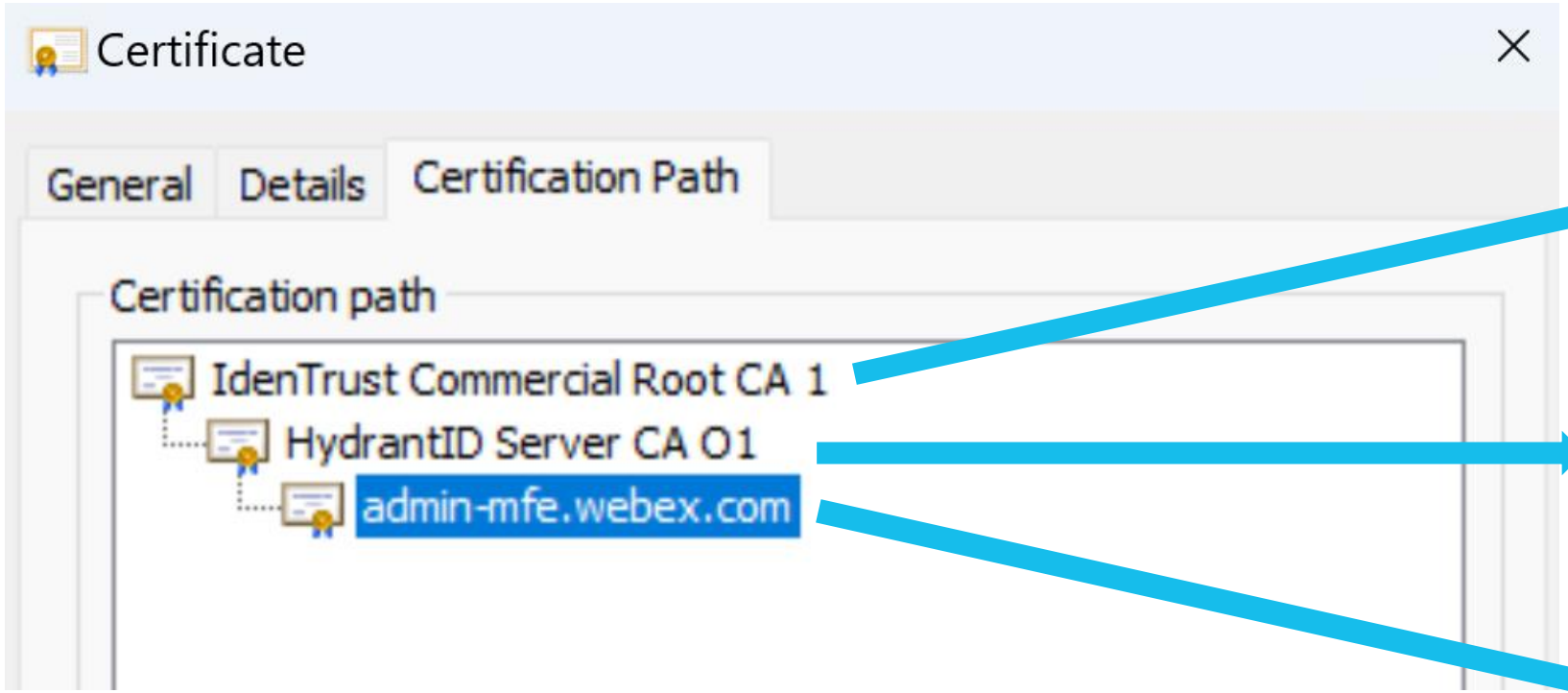
Temporary and Self-Signed Examples (unsupported)





© 2025 Cisco and/or its affiliates. All rights reserved.

What's in a certificate? - Certificate Chain



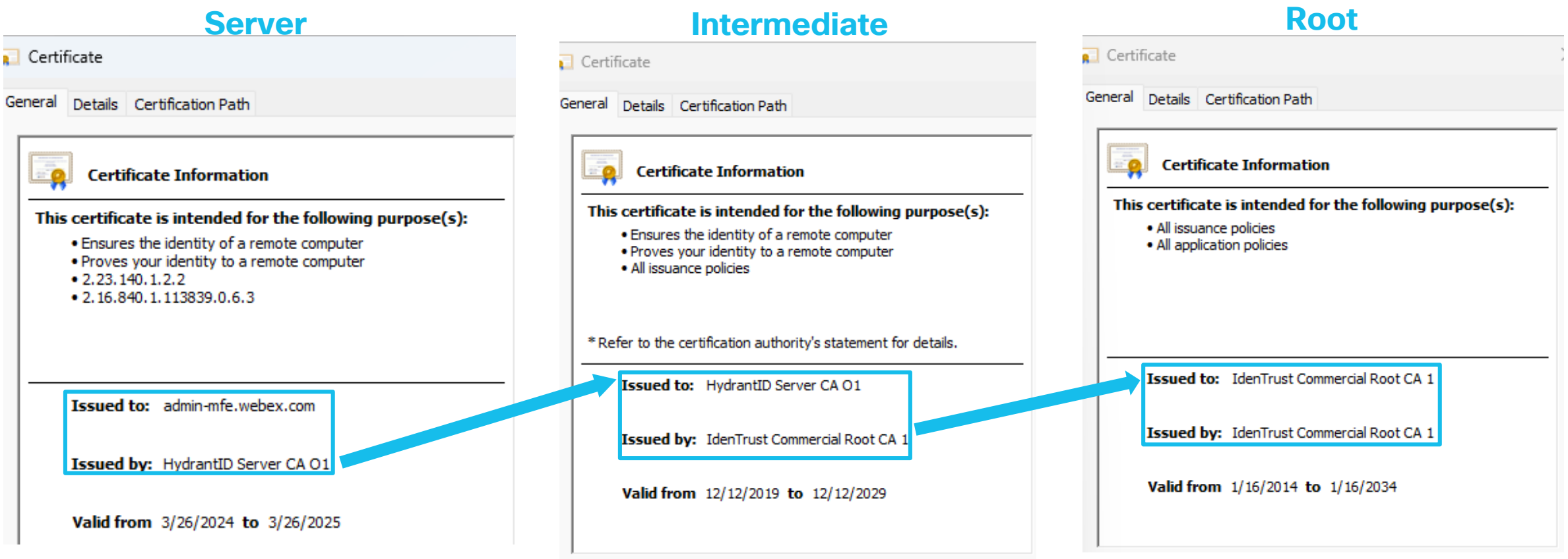
Root Certificate

Intermediate Certificate

Server Certificate

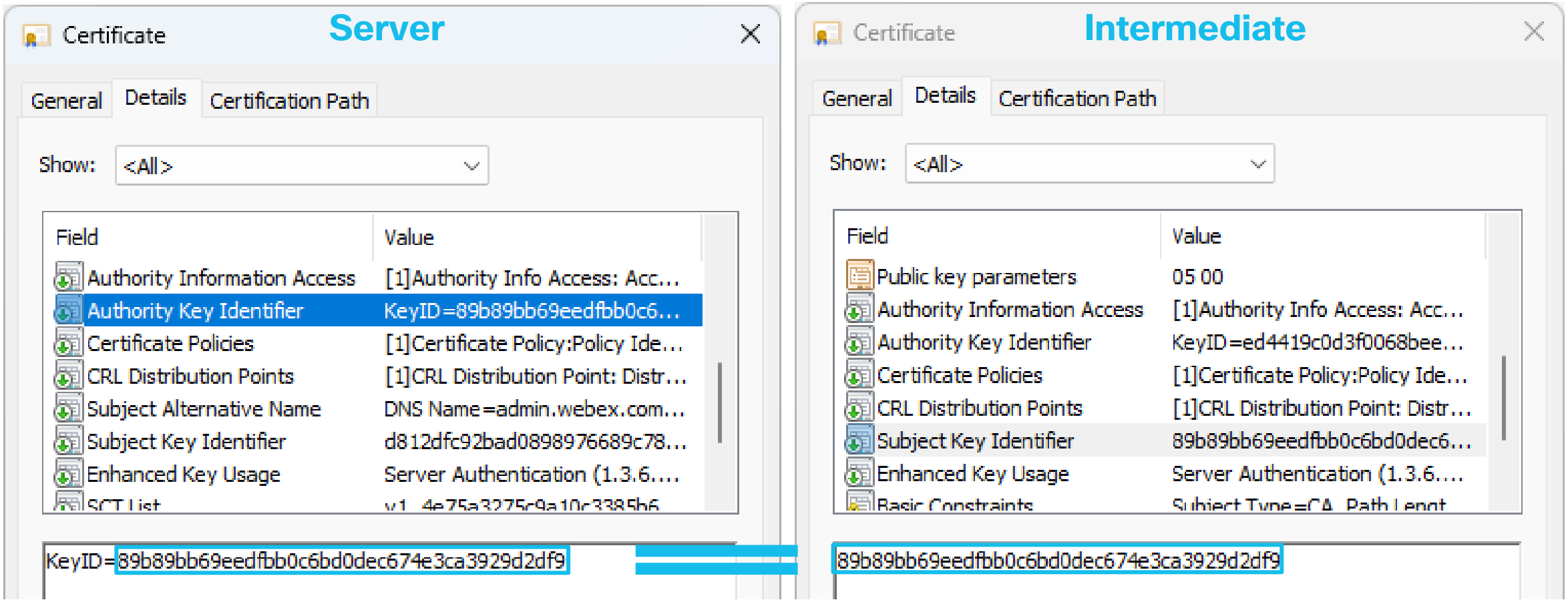
© 2025 Cisco and/or its affiliates. All rights reserved.

What's in a certificate? – Chain verification



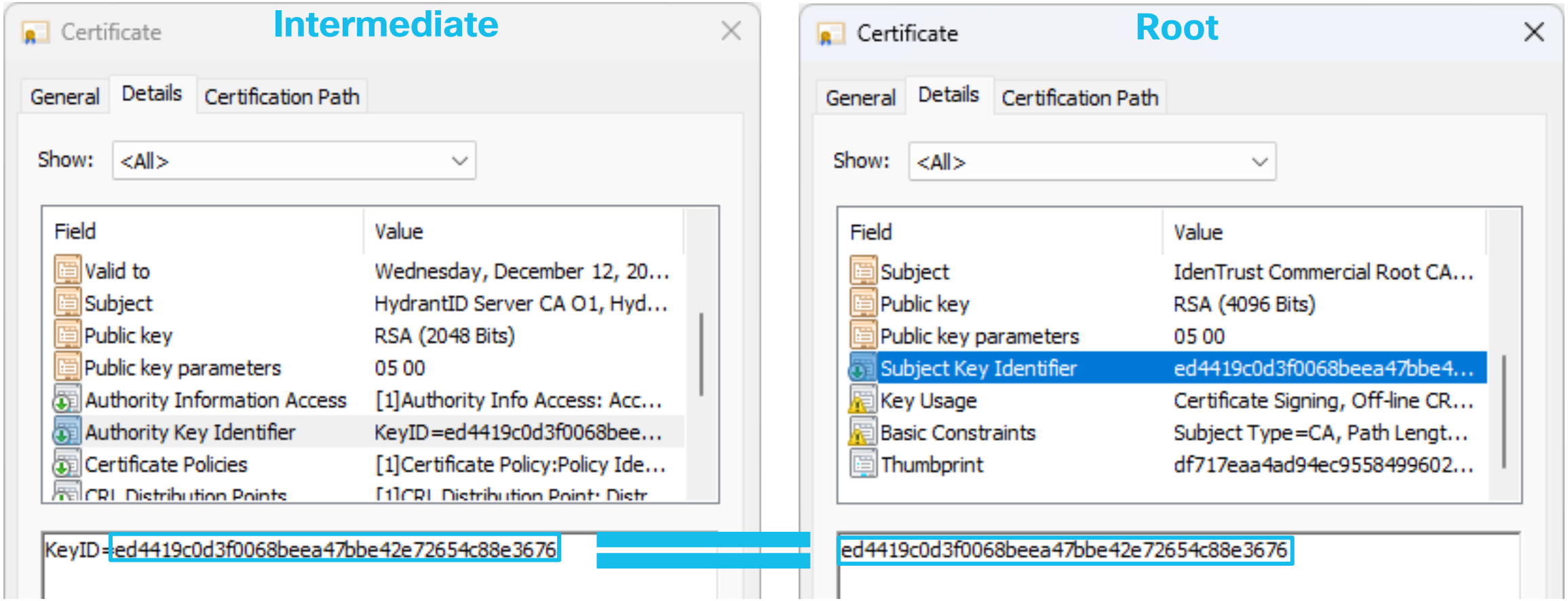
© 2025 Cisco and/or its affiliates. All rights reserved.

What's in a certificate? – Chain verification



© 2025 Cisco and/or its affiliates. All rights reserved.

What's in a certificate? – Chain verification

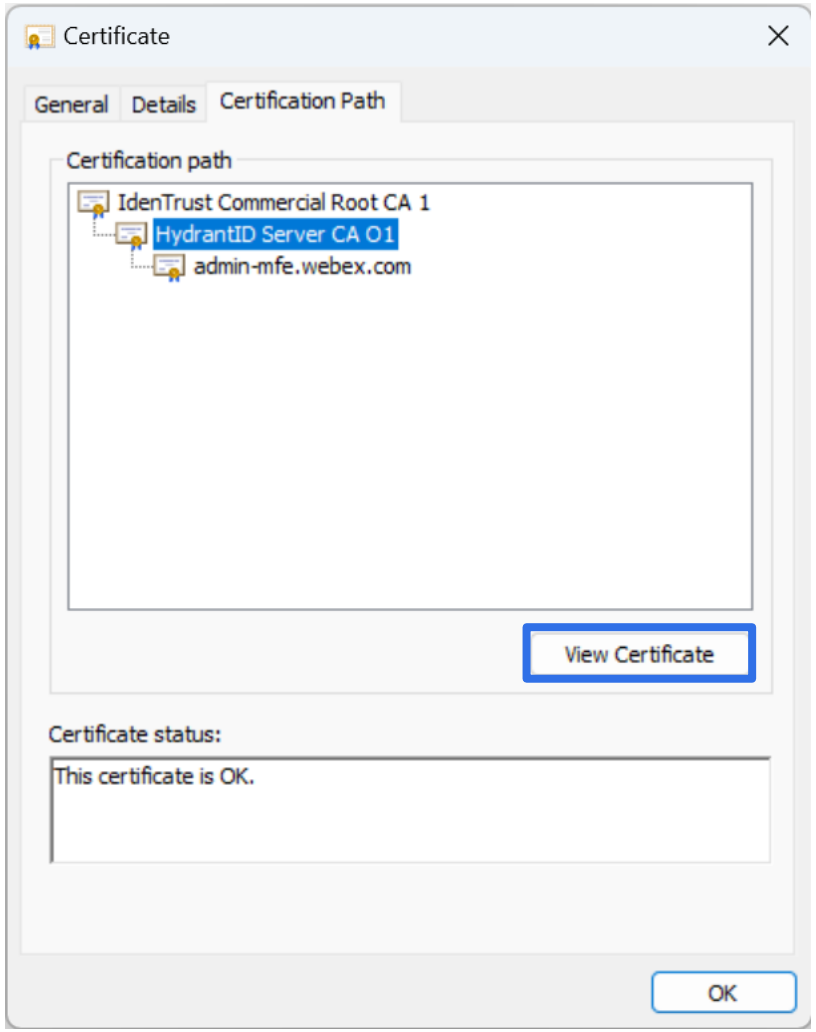


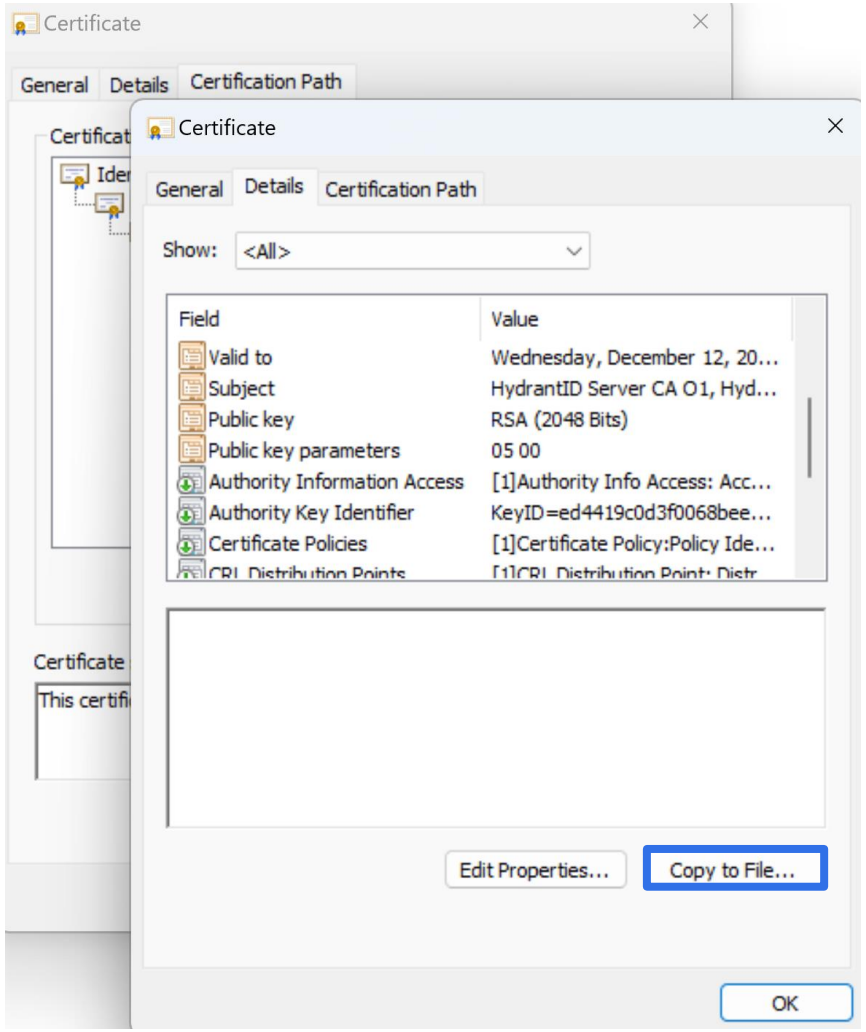
© 2025 Cisco and/or its affiliates. All rights reserved.

Certificate Extraction

Extracting CA Certificates – Extract from Certificate

TAC Tip

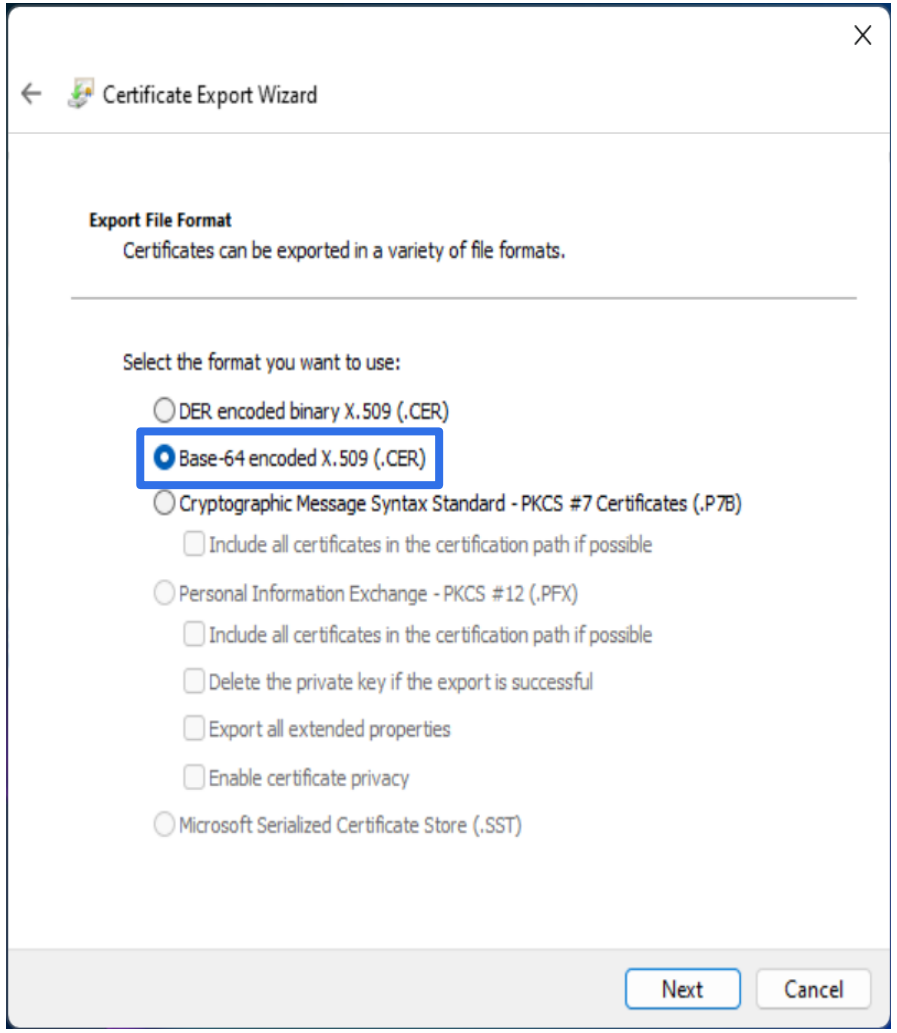


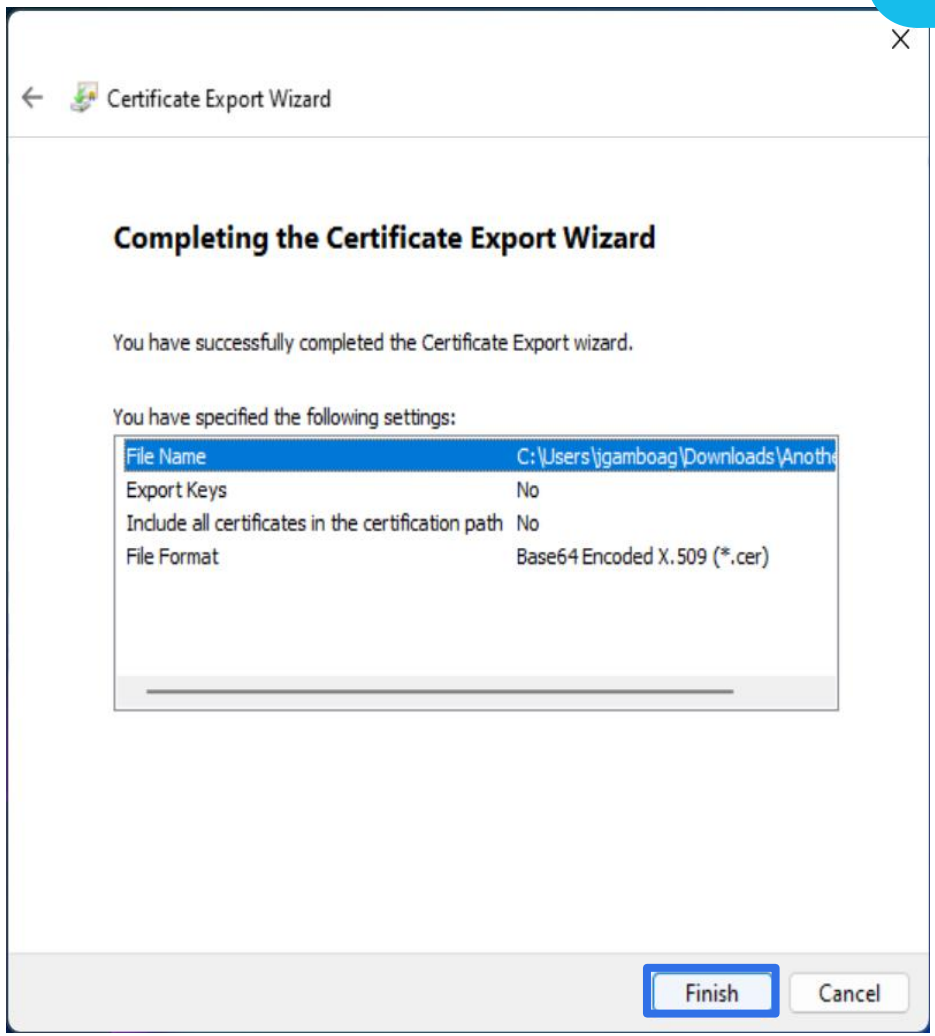


© 2025 Cisco and/or its affiliates. All rights reserved.

Extracting CA Certificates – Extract from Certificate

TAC Tip



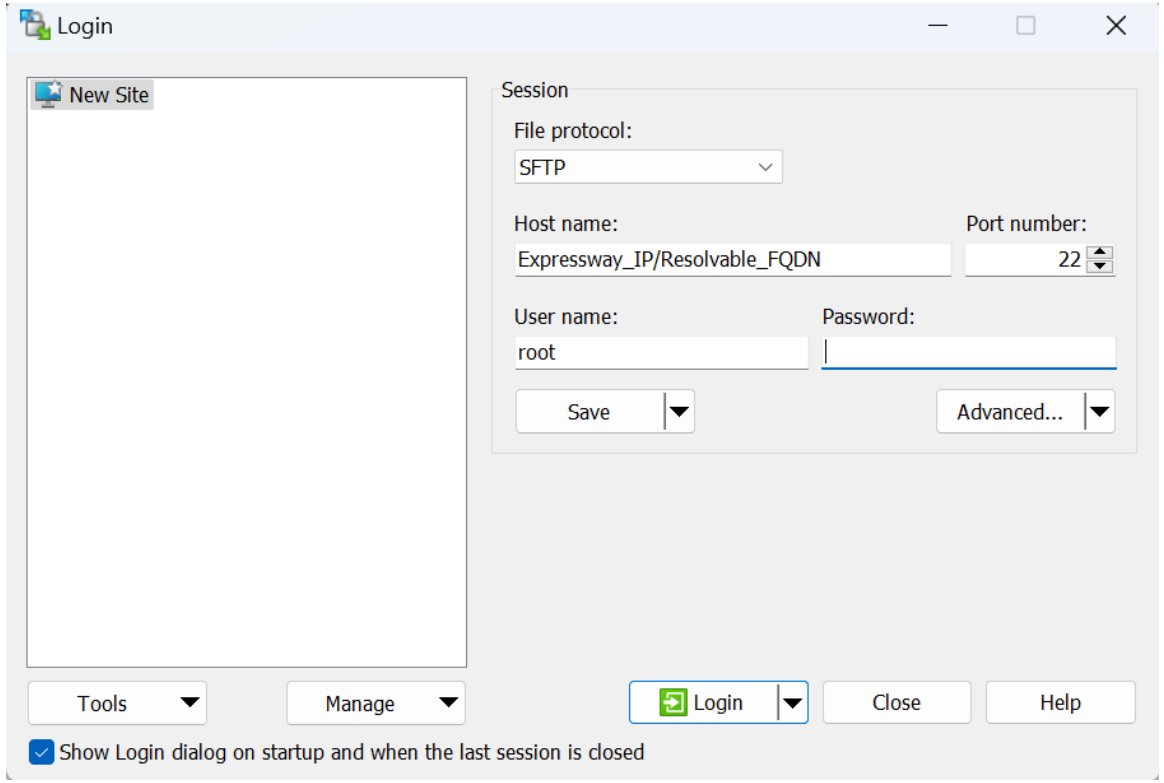


© 2025 Cisco and/or its affiliates. All rights reserved.

Extracting Expressway Certificates – SFTP/WinSCP

TAC Tip

Navigate to Tandberg/Persistent/Certs, collect certificates as required

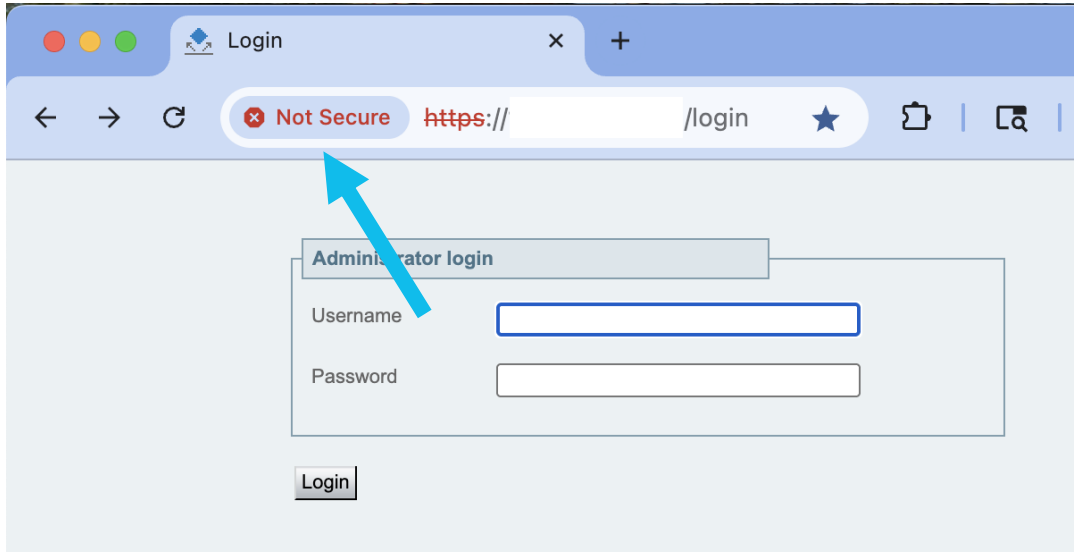


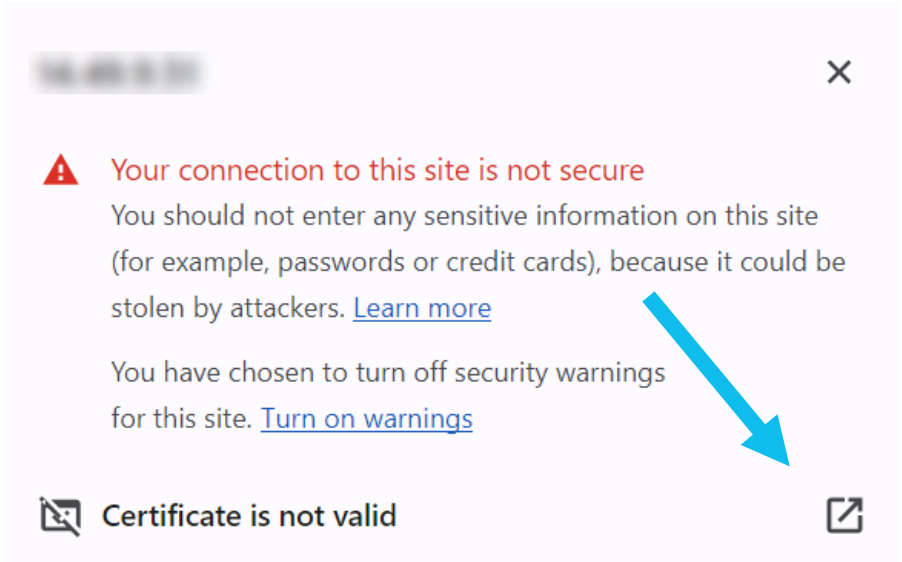
/tandberg/persistent/certs/

Name	Size	Changed	Rights	Owner
..		4/29/2024 1:22:59 PM	rwxr-xr-x	root
saml		12/6/2022 12:58:43 PM	rwxr-xr-x	_samlvfy
multidomaincerts		3/5/2023 6:40:54 AM	rwx------	root
generated_csr		12/6/2022 12:54:43 PM	rwxr-xr-x	_nobody
mtls_ca.pem	9 KB	7/14/2021 7:05:57 AM	rw-r--r--	_nobody
sch_server_cert.pem	6 KB	3/13/2023 10:47:12 AM	rw-r--r--	_nobody
ca.pem	6 KB	4/24/2023 7:24:06 AM	rw-r--r--	_nobody
server-ssh.pem	4 KB	3/11/2024 9:21:55 AM	rw-------	_pfwd
privkey.pem.default	2 KB	6/7/2023 9:24:01 AM	r--------	root
privkey.pem	2 KB	4/23/2023 4:27:00 PM	r---w----	root
server.pem.default	2 KB	6/7/2023 9:24:01 AM	r--r--r--	root
server.pem	2 KB	4/23/2023 4:27:00 PM	rw-r--r--	_nobody
ca.pem.default	2 KB	6/7/2023 9:24:01 AM	r--r--r--	root
client-ca.crl.default	2 KB	4/24/2023 7:22:13 AM	rw-r--r--	root
client-ca.crl	2 KB	4/24/2023 7:22:13 AM	rw-r--r--	_nobody
policy-services.crl.default	2 KB	7/14/2021 7:05:57 AM	rw-r--r--	root
policy-services.crl	2 KB	7/14/2021 7:05:57 AM	rw-r--r--	_nobody
crl-update.conf	1 KB	3/11/2024 9:21:54 AM	rw-r--r--	root

© 2025 Cisco and/or its affiliates. All rights reserved.

Extracting Expressway Certificates – Web Interface

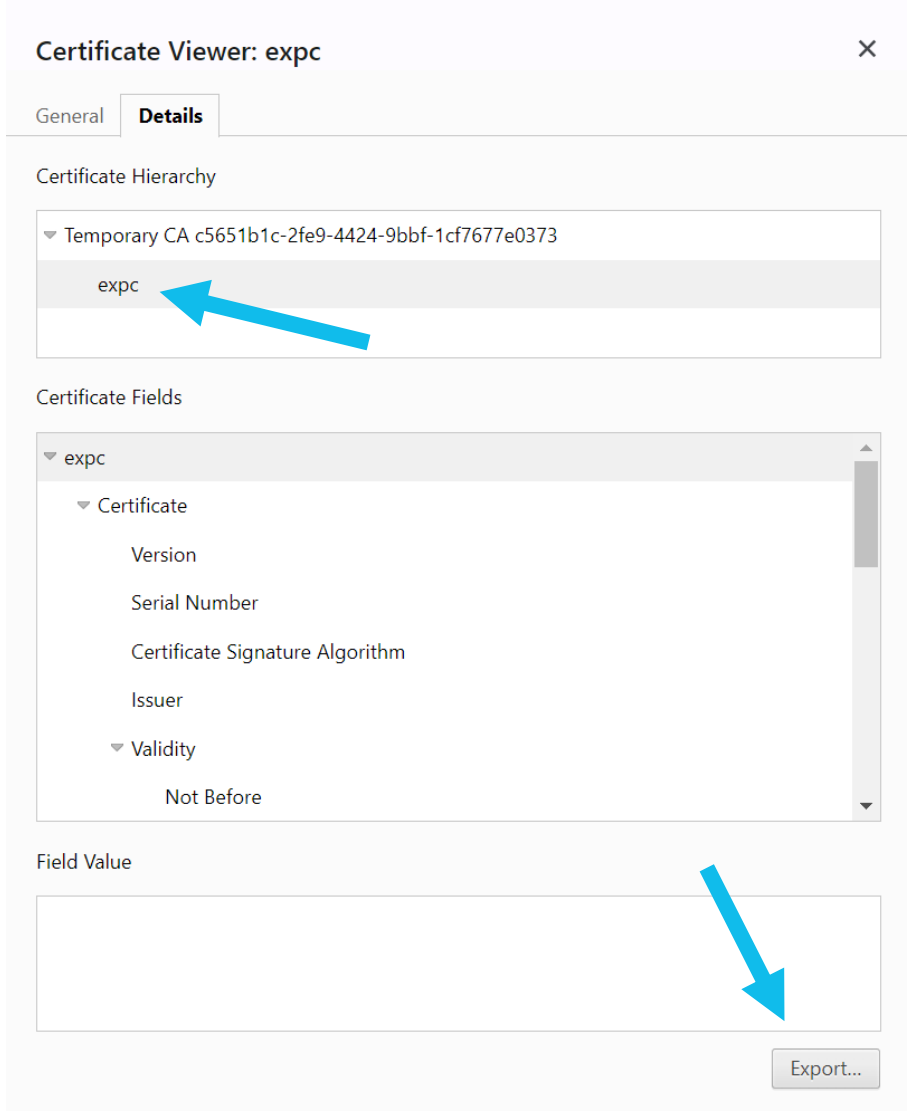




1. Navigate to the expressway web interface
2. Click on the padlock icon next to the URL
3. Select the certificate option

© 2025 Cisco and/or its affiliates. All rights reserved.

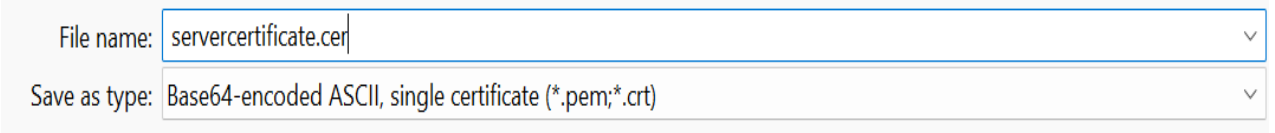
Extracting Expressway Certificates – Web Interface



4. While on details, select the server certificate

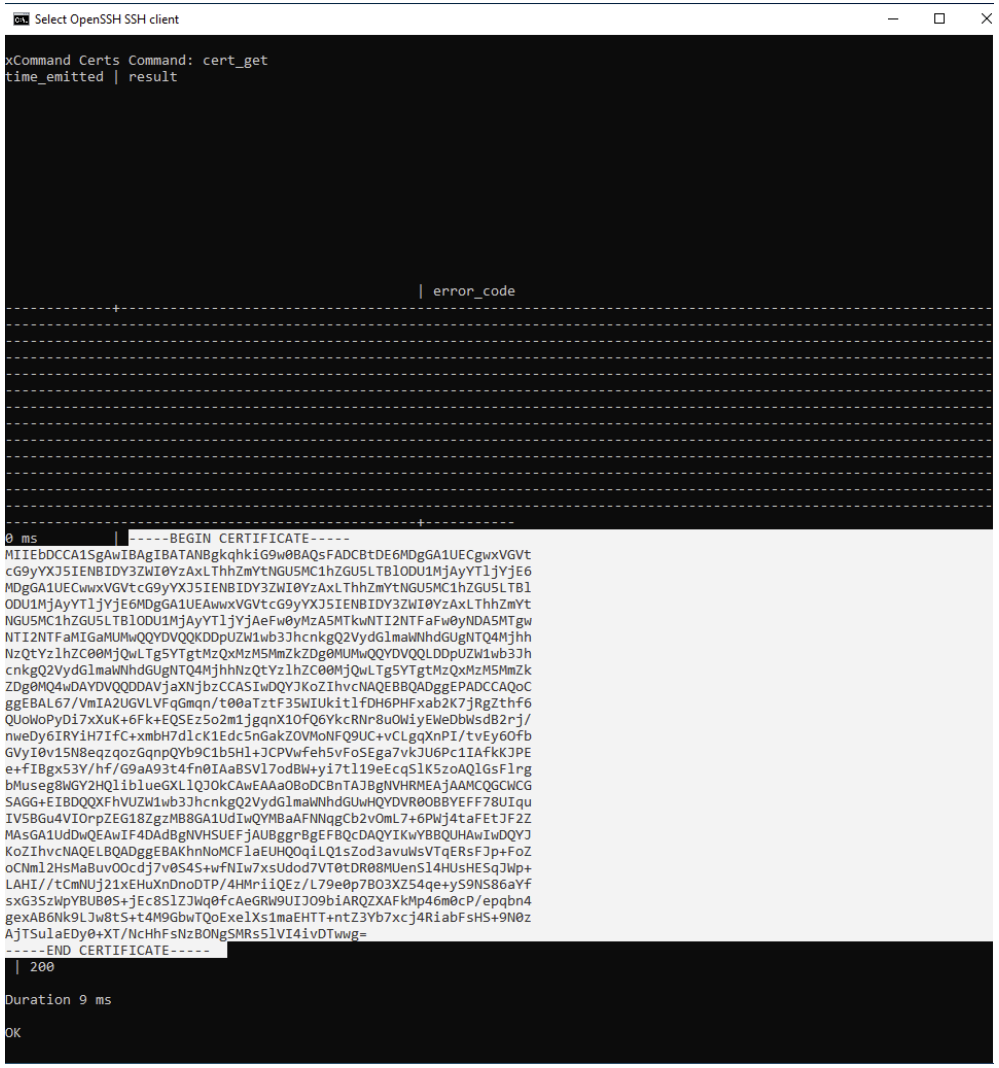
5. Click export

6. Browse and download the file on your desired folder



© 2025 Cisco and/or its affiliates. All rights reserved.

Extracting Expressway Certificates – Command Line

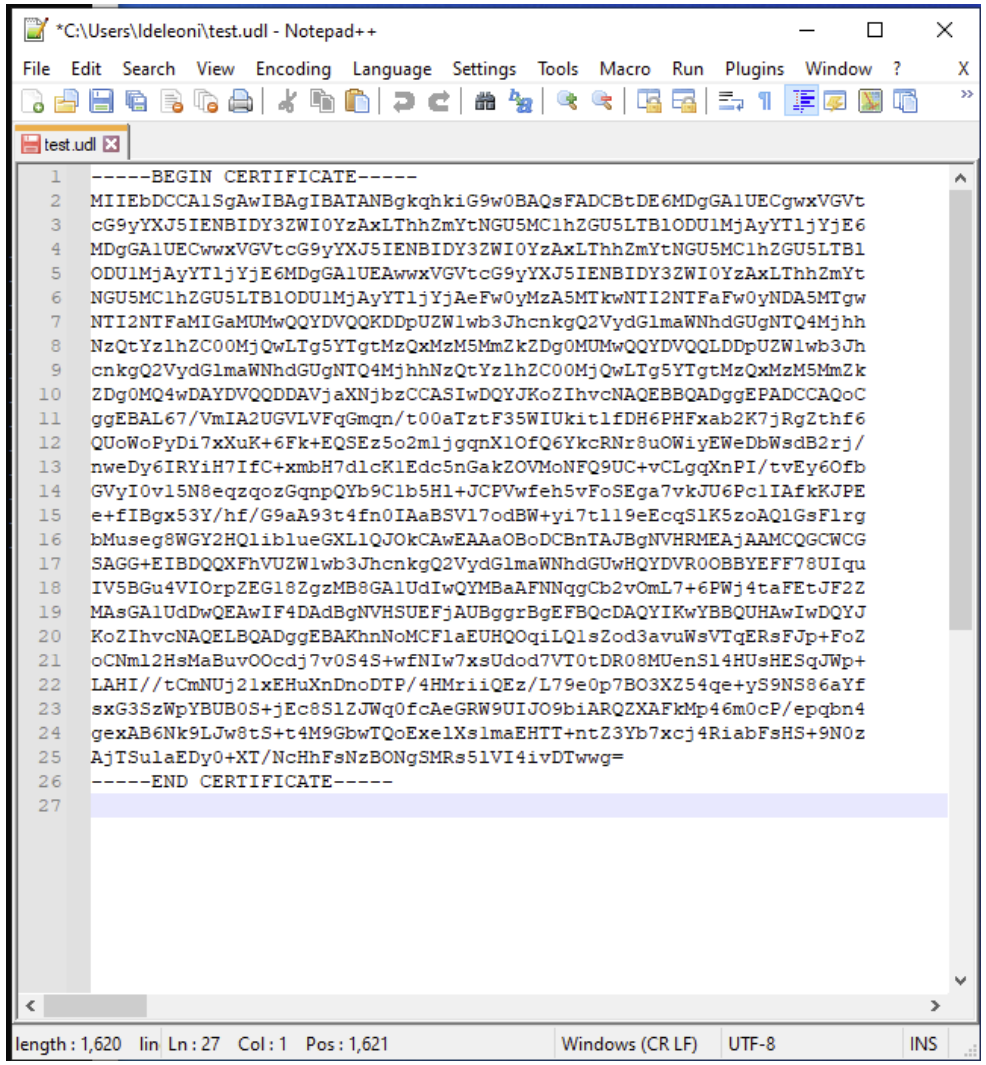


TAC Tip

1. Log into the Expressway CLI with admin credentials
2. Run the command 'xCommand Certs Command: cert_get'
3. Copy the certificate output from ----BEGIN CERTIFICATE----- through -----END CERTIFICATE-----

© 2025 Cisco and/or its affiliates. All rights reserved.

Extracting Expressway Certificates – Command Line



4. Paste the certificate into a notepad application like Notepad++

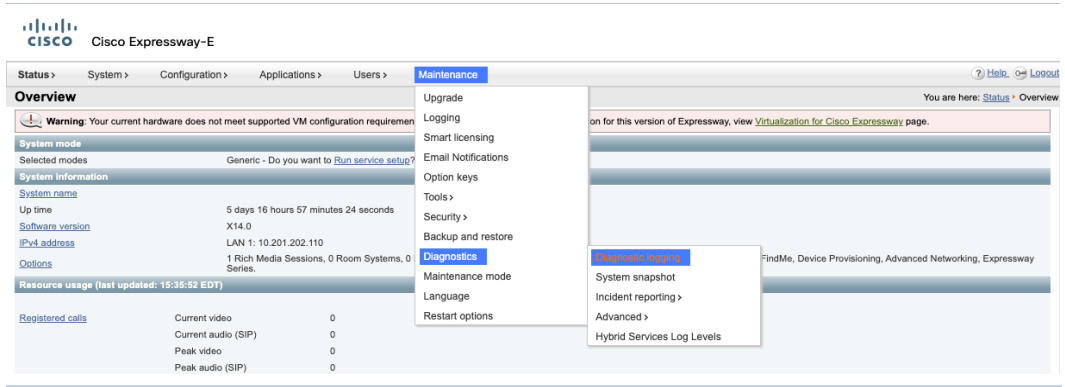
5. Make sure that there is a carriage return after -----END CERTIFICATE-----

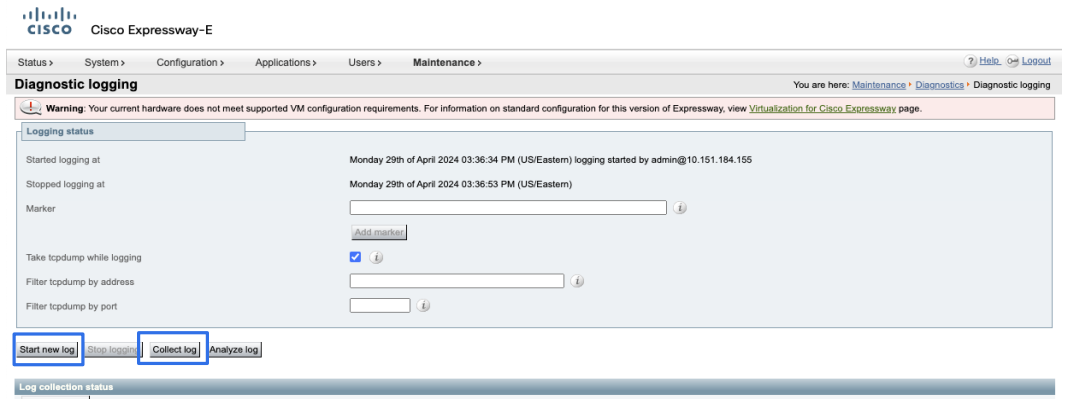
6. Save file as <certname>.pem*
   * When saving make sure the Save as type is set to All types (*.*)

© 2025 Cisco and/or its affiliates. All rights reserved.

Extracting Expressway Certificates – Log Bundle

TAC Tip





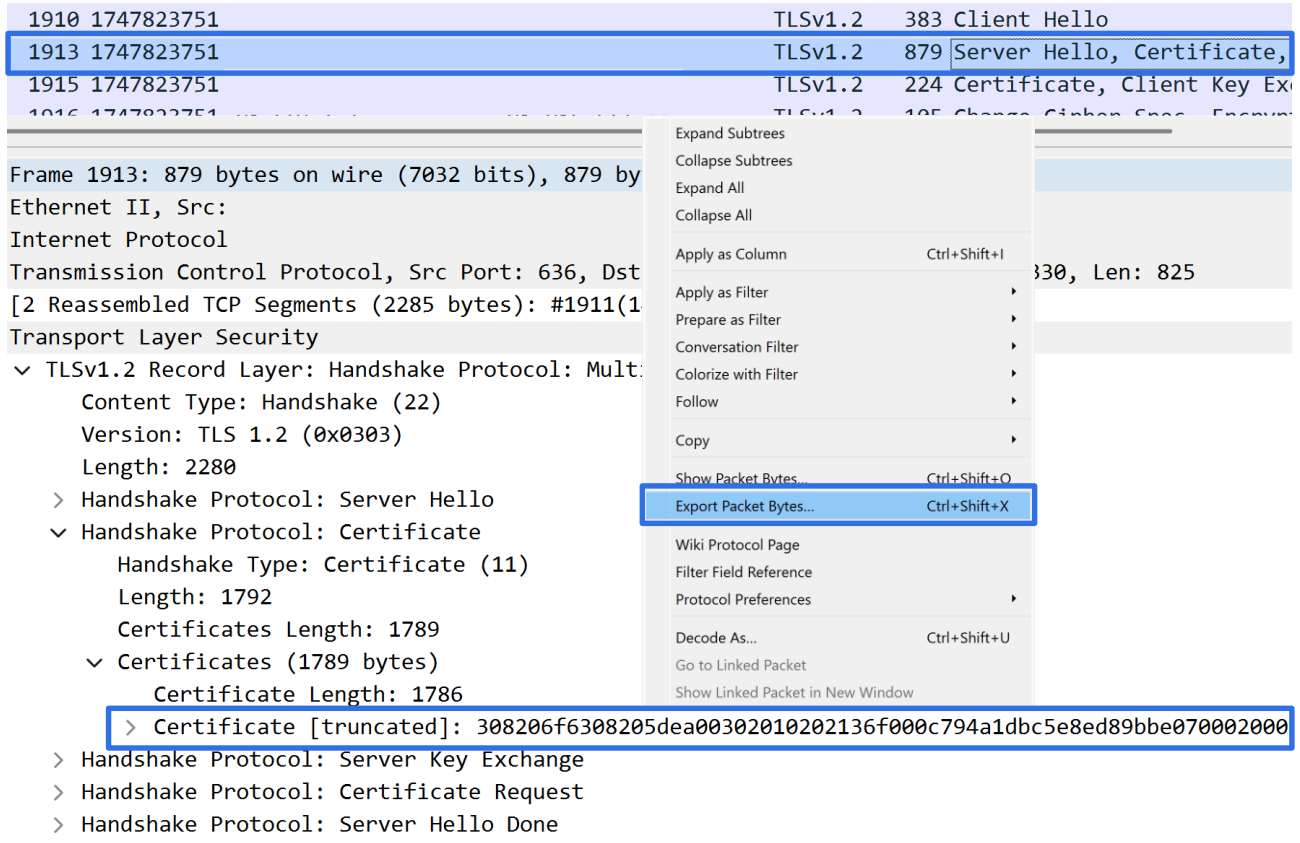
ca-EXP-E_2025-04-17_18:28:59.pem	11 300	11 776	2025-04-17 14:26
eth0_diagnostic_logging_tcpdump00_EXP-E_2025-04-17_18:28:59.pcap	1 760 197	1 760 256	2025-04-17 14:28
eth1_diagnostic_logging_tcpdump00_-EXP-E_2025-04-17_18:28:59.pcap	222 139	222 208	2025-04-17 14:29
loggingsnapshot_-EXP-E_2025-04-17_18:28:59.txt	361 987	362 496	2025-04-17 14:29
server_-EXP-E_2025-04-17_18:28:59.pem	2 610	3 072	2025-04-17 14:26
xconf_dump-EXP-E_2025-04-17_18:28:59.xml	92 175	92 672	2025-04-17 14:26
xconf_dump_-EXP-E_2025-04-17_18:28:59.txt	121 942	122 368	2025-04-17 14:26
xstat_dump_EXP-E_2025-04-17_18:28:59.xml	105 645	105 984	2025-04-17 14:26
xstat_dump_EXPE_2025-04-17_18:28:59.txt	121 704	121 856	2025-04-17 14:26

1. Log into the web UI
2. Navigate to Maintenance > Diagnostics > Diagnostic Logging
3. Click Start new log > Stop logging > Collect log > Download log
4. The server .pem certificate file will be included in the tar.gz log bundle

© 2025 Cisco and/or its affiliates. All rights reserved.

Extracting Expressway Certificates – Packet Capture

TAC Tip

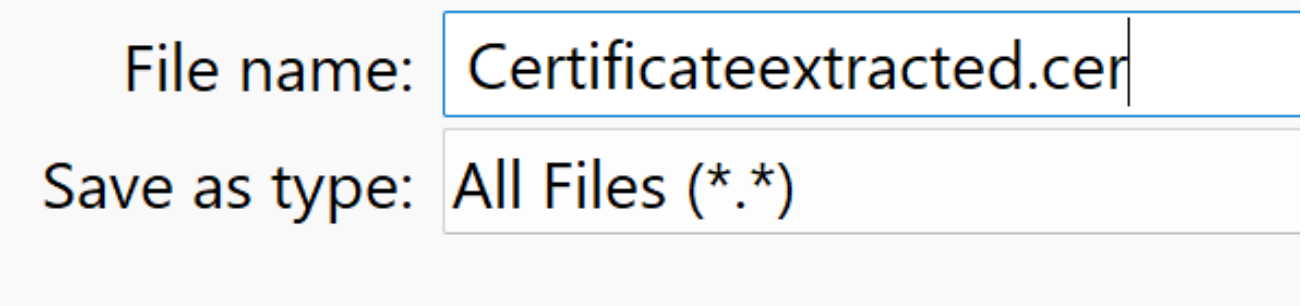


1. Select the packet containing the certificate
2. Expand the Transport Layer Security fields
3. Locate the certificate to be extracted
4. Right click on the certificate and select Export Packet Bytes
5. Name the file <filename>.cer with Save as type set to All Files (*.*)
6. Save

© 2025 Cisco and/or its affiliates. All rights reserved.

Extracting Expressway Certificates – Packet Capture

TAC Tip

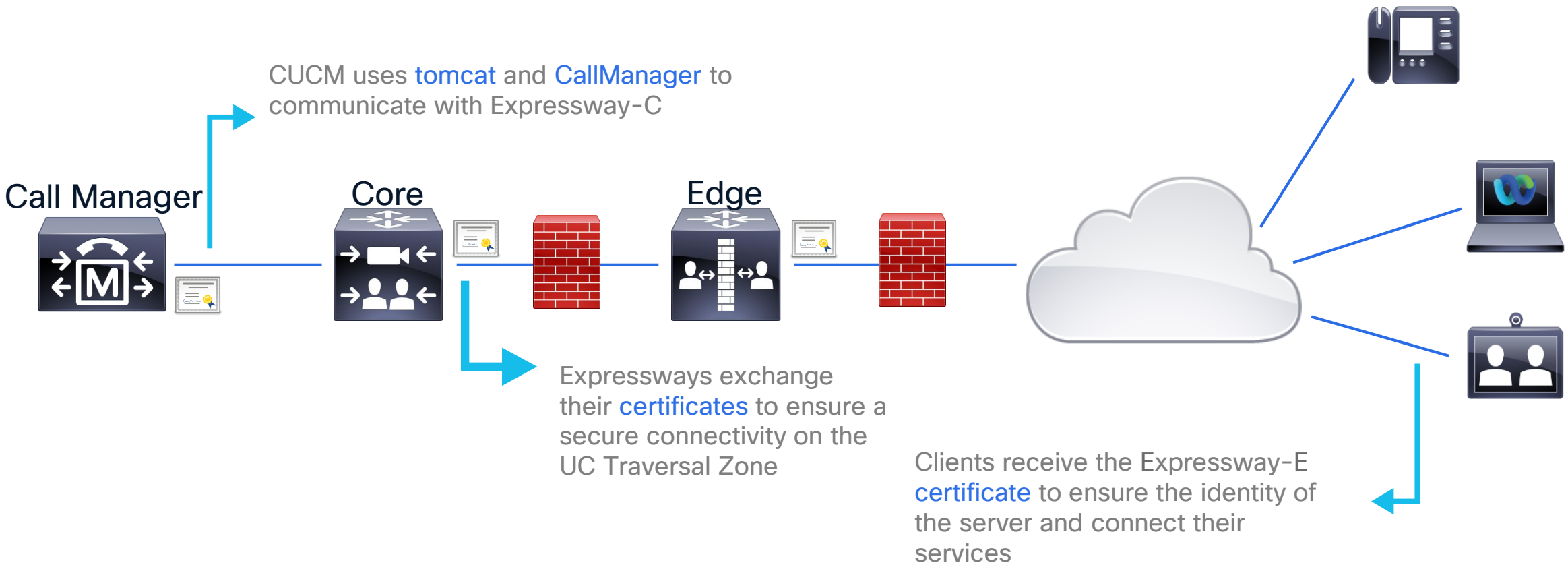


1. Select the packet containing the certificate
2. Expand the Transport Layer Security fields
3. Locate the certificate to be extracted
4. Right click on the certificate and select Export Packet Bytes
5. Name the file <filename>.cer with Save as type set to All Files (*.*)
6. Save

© 2025 Cisco and/or its affiliates. All rights reserved.

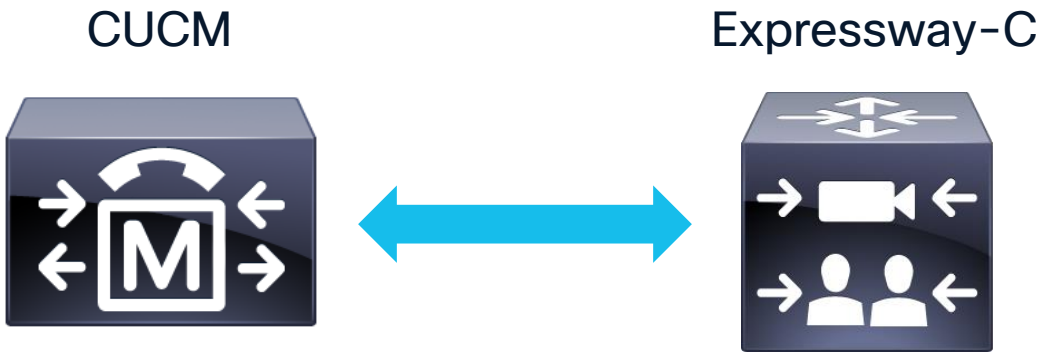
MRA Certificates

Significant Certificates in an MRA Deployment



© 2025 Cisco and/or its affiliates. All rights reserved.

UC Certificate Exchange: Establishing Trust

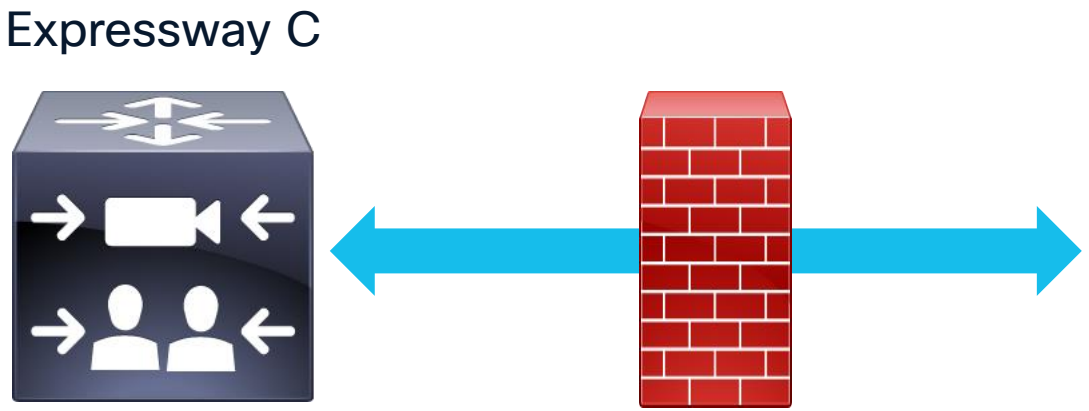


Just as the CA certificates that signed the Expressway-C certificate are uploaded to the Expressway-E, they must be uploaded to the CUCM in the tomcat-trust and CallManager-trust.

The Expressway-C must also trust the CUCM tomcat and CallManager certificates.

© 2025 Cisco and/or its affiliates. All rights reserved.

UC Certificate Exchange: Establishing Trust



Expressway-E signing CA certificate must be installed in Expressway-C Trusted CA list



Expressway-C signing CA certificate must be installed in Expressway-E Trusted CA list



© 2025 Cisco and/or its affiliates. All rights reserved.

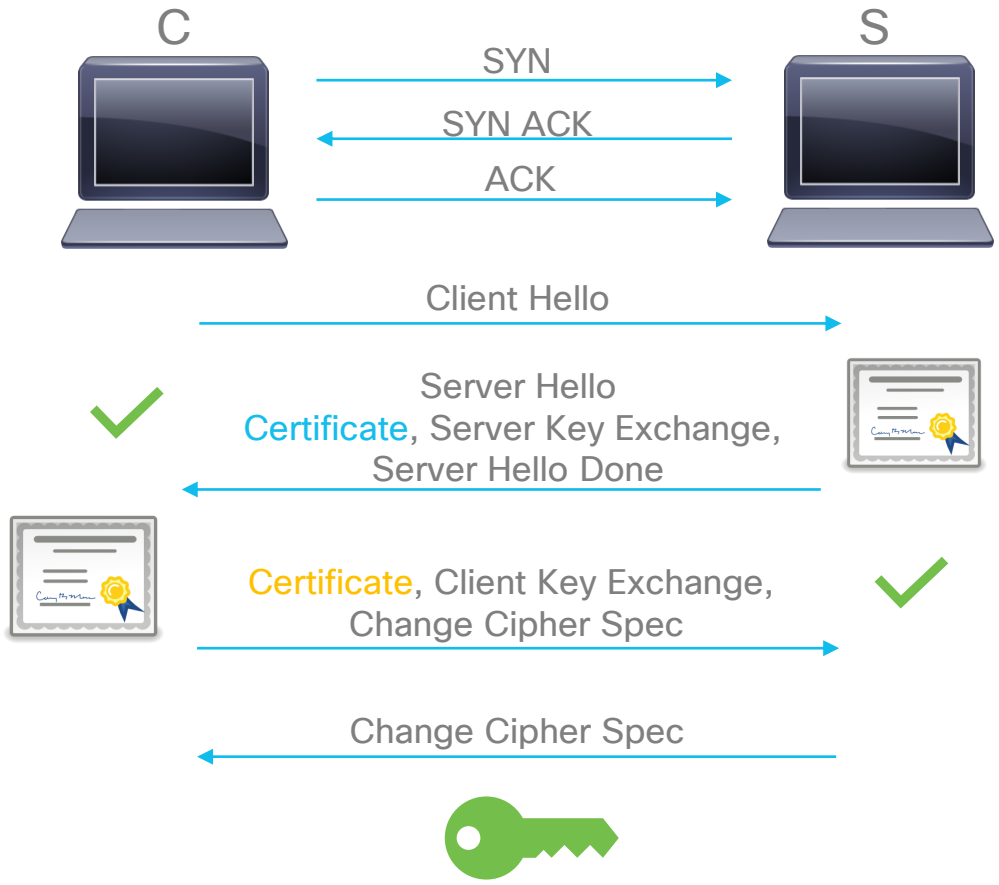
Expressway SAN Requirements

Add these items as subject alternative names	When generating a CSR for these purposes			
	Mobile and Remote Access	Jabber Guest	XMPP Federation	Business to Business Calls
Unified CM registrations domains (despite their name, these have more in common with service discovery domains than with Unified CM SIP registration domains)	Required on Expressway-E only	–	–	–
XMPP federation domains	–	–	Required on Expressway-E only	–
IM and Presence chat node aliases (federated group chat)	–	–	Required	–
Unified CM phone security profile names	Required on Expressway-C only	–	–	–
(Clustered systems only) Expressway Cluster name	Required on Expressway-C only	Required on Expressway-C only	Required on Expressway-C only	–

© 2025 Cisco and/or its affiliates. All rights reserved.

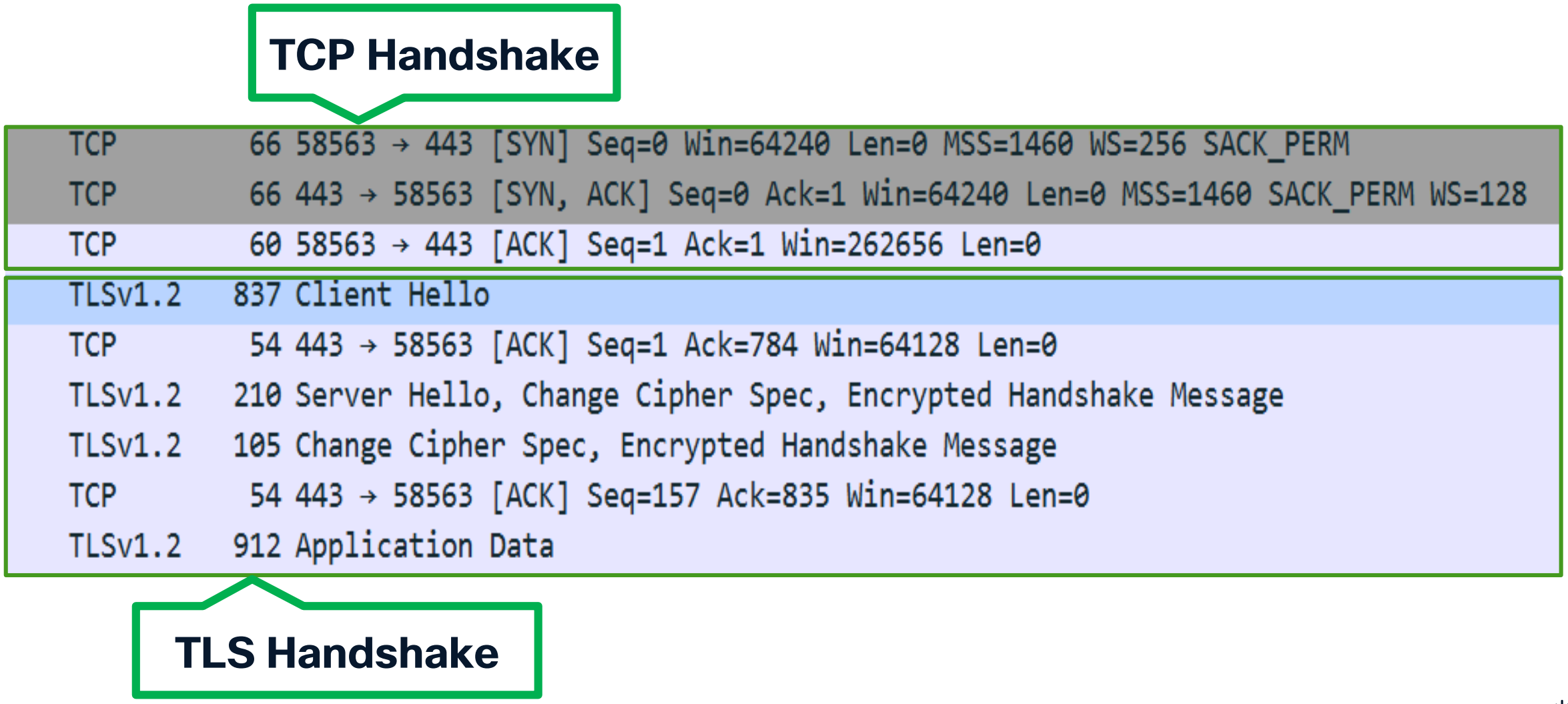
TLS and Ciphers

TLS Handshake



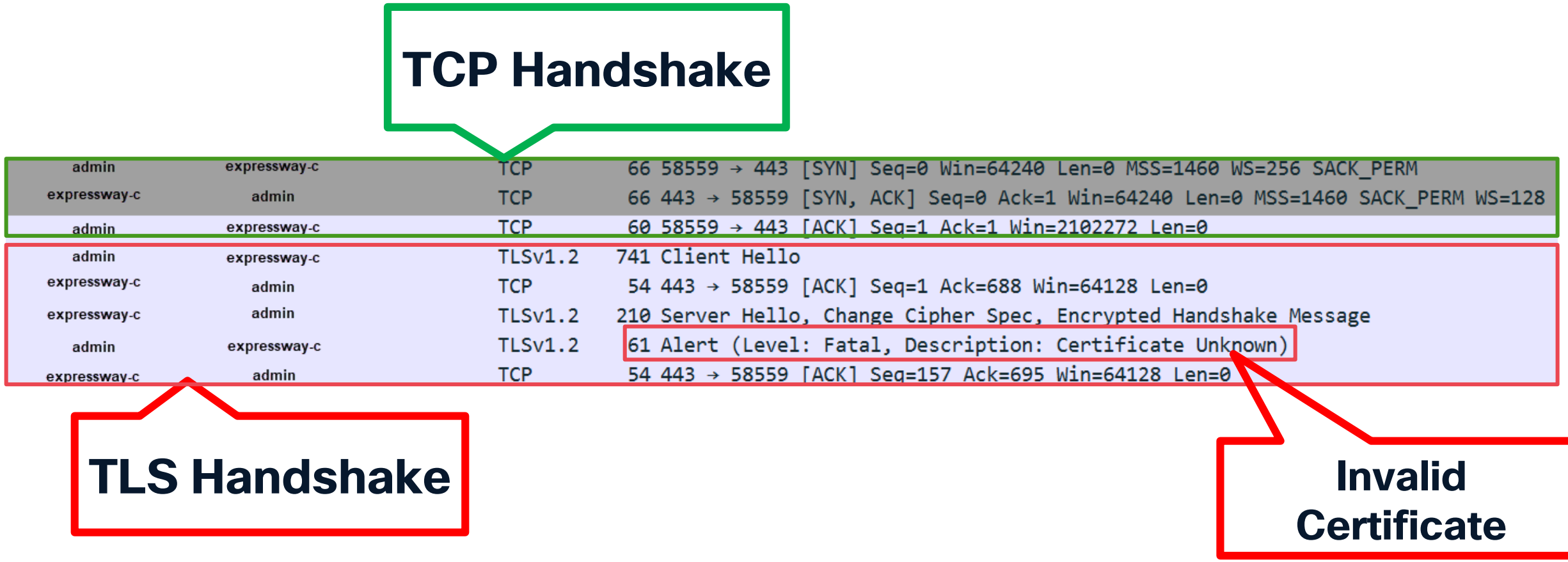
© 2025 Cisco and/or its affiliates. All rights reserved.

TLS Handshake Failures and Verification



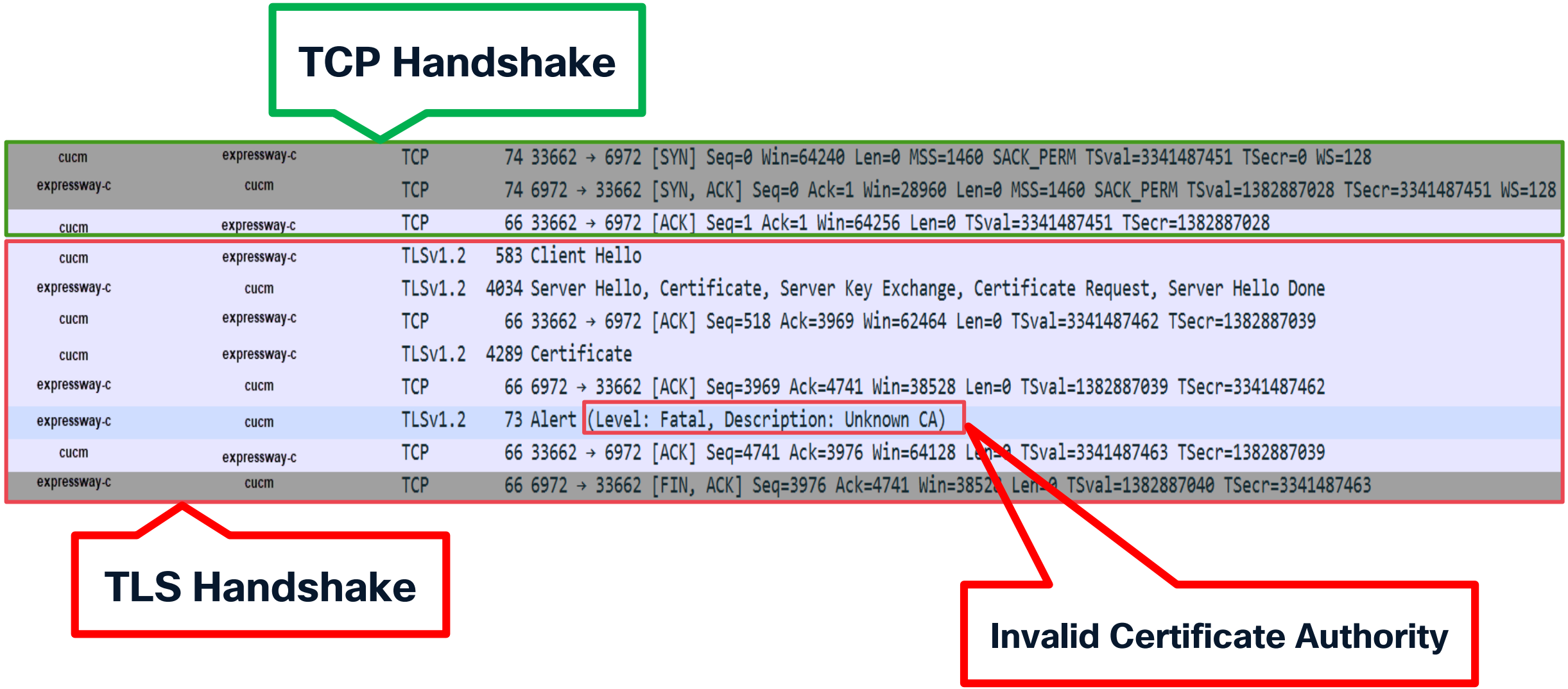
© 2025 Cisco and/or its affiliates. All rights reserved.

TLS Handshake Failures and Verification



© 2025 Cisco and/or its affiliates. All rights reserved.

TLS Handshake Failures and Verification



© 2025 Cisco and/or its affiliates. All rights reserved.

TLS Handshake Failures and Verification

TCP Handshake

Source	Destination	Protocol	Length	Info
expressway-c	expressway-e	TCP	74	27088 → 7002 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=270645594 TSecr=0 WS=128
expressway-e	expressway-c	TCP	74	7002 → 27088 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2585994536 TSecr=270645594 WS=128
expressway-c	expressway-e	TCP	66	27088 → 7002 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4291755130 TSecr=2585994536
expressway-c	expressway-e	TLSv1.2	260	Client Hello
expressway-c	expressway-e	TCP	74	27089 → 7002 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=270645594 TSecr=0 WS=128
expressway-e	expressway-c	TCP	66	7002 → 27088 [ACK] Seq=1 Ack=195 Win=65024 Len=0 TSval=2585994536 TSecr=4291755130
expressway-e	expressway-c	TLSv1.2	73	Alert (Level: Fatal, Description: Handshake Failure)
expressway-c	expressway-e	TCP	66	27088 → 7002 [ACK] Seq=195 Ack=8 Win=64256 Len=0 TSval=4291755131 TSecr=2585994536
expressway-c	expressway-e	TCP	66	27088 → 7002 [FIN, ACK] Seq=195 Ack=8 Win=64256 Len=0 TSval=4291755131 TSecr=2585994536
expressway-e	expressway-c	TCP	66	7002 → 27088 [FIN, ACK] Seq=8 Ack=196 Win=65024 Len=0 TSval=2585994537 TSecr=4291755131
expressway-c	expressway-e	TCP	66	27088 → 7002 [ACK] Seq=196 Ack=9 Win=64256 Len=0 TSval=4291755131 TSecr=2585994537

```
▾ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 189
  ▾ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 185
      Version: TLS 1.2 (0x0303)
    › Random: 4c1cc930681ad11dd228b3531e97c2f535191c0ed66156ddc0042c21c713f3d5
      Session ID Length: 0
      Cipher Suites Length: 82
    ▾ Cipher Suites (41 suites)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
```

TLS Handshake

© 2025 Cisco and/or its affiliates. All rights reserved.

TLS Handshake Failures and Verification

TCP Handshake

Source	Destination	Protocol	Length	Info
expressway-c	expressway-e	TCP	74	27088 → 7002 [SYN] Seq=0 Win=64240 Len=0 MS
expressway-e	expressway-c	TCP	74	7002 → 27088 [SYN, ACK] Seq=0 Ack=1 Win=651 1 WS=128
expressway-c	expressway-e	TCP	66	27088 → 7002 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4291755052 TSecr=2585994437
expressway-c	expressway-e	TLSv1.2	260	Client Hello
expressway-c	expressway-e	TCP	74	27089 → 7002 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=270645594 TSecr=0 WS=128
expressway-e	expressway-c	TCP	66	7002 → 27088 [ACK] Seq=1 Ack=195 Win=65024 Len=0 TSval=2585994536 TSecr=4291755130
expressway-e	expressway-c	TLSv1.2	73	Alert (Level: Fatal, Description: Handshake Failure)
expressway-c	expressway-e	TCP	66	27088 → 7002 [ACK] Seq=195 Ack=8 Win=64256 Len=0 TSval=4291755131 TSecr=2585994536
expressway-c	expressway-e	TCP	66	27088 → 7002 [FIN, ACK] Seq=195 Ack=8 Win=64256 Len=0 TSval=4291755131 TSecr=2585994536
expressway-e	expressway-c	TCP	66	7002 → 27088 [FIN, ACK] Seq=8 Ack=196 Win=65024 Len=0 TSval=2585994537 TSecr=4291755131
expressway-c	expressway-e	TCP	66	27088 → 7002 [ACK] Seq=196 Ack=9 Win=64256 Len=0 TSval=4291755131 TSecr=2585994537

```
▾ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 189
  ▾ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 185
      Version: TLS 1.2 (0x0303)
    › Random: 4c1cc930681ad11dd228b3531e97c2f535191c0ed66156ddc0042c21c713f3d5
      Session ID Length: 0
      Cipher Suites Length: 82
    ▾ Cipher Suites (41 suites)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
```

TLS Handshake

Cipher incompatibility

© 2025 Cisco and/or its affiliates. All rights reserved.

Case Generator Scenarios

After upgrading my server to x14.0.2, my devices are unable to connect over MRA

Expressway-C Traffic Server Enforces Certificate Verification

© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

As of x14.0.2, Expressway will send its client certificate whenever a server (CUCM) requests it, for services running on ports other than 8443 (e.g. 6971,6972) even if CUCM is in non-secure mode.

Expressway-C:
CA Certificates
(root and all intermediates)

Call Manager Trust Stores:
CallManager-trust
tomcat-trust



© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

The identifying signature for this issue is the Expressway's connections to CUCM over port 6972 failing with "tlsv1 alert unknown ca" and "502 connect failed" response.

In the client logs if you filter for 'HTTP response code' you will see 200 OK responses to the initial HTTP messages and then a 502 when the client requests the CSF configuration file:

```
2023-12-12 18:05:24,011 INFO  [0x00006d3c] [ls\src\http\BasicHttpClientImpl.cpp(675)] [csf.httpclient]
[csf::http::performRequest] - *-----* HTTP response code 200 connect code 0 for request #13 to
https://jabber.clus2024.com:8443/Y2x1czIwMjQuY29tCg/get_edge_config?service_name=_cisco-uds
2023-12-12 18:05:24,359 INFO  [0x00006d3c] [ls\src\http\BasicHttpClientImpl.cpp(675)] [csf.httpclient]
[csf::http::performRequest] - *-----* HTTP response code 200 connect code 0 for request #14 to
https://jabber.clus2024.com:8443/Y2x1czIwMjQuY29tL2h0dHBzL2NsdXNwdWIuY2lzY28udGVzdC84NDQz/cucm-uds/version
2023-12-12 18:05:24,493 INFO  [0x00006d3c] [ls\src\http\BasicHttpClientImpl.cpp(675)] [csf.httpclient]
[csf::http::performRequest] - *-----* HTTP response code 200 connect code 0 for request #16 to
https://jabber.clus2024.com:8443/Y2x1czIwMjQuY29tL2h0dHBzL2NsdXNwdWIuY2lzY28udGVzdC84NDQz/cucm-uds/servers
2023-12-12 18:05:24,843 INFO  [0x00006d3c] [ls\src\http\BasicHttpClientImpl.cpp(675)] [csf.httpclient]
[csf::http::performRequest] - *-----* HTTP response code 502 connect code 0 for request #19 to
https://jabber.clus2024.com:8443/Y2x1czIwMjQuY29tL2h0dHBzL2NsdXNwdWIuY2lzY28udGVzdC82OTcy/CSFuser.cnf.xml
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

Looking at the Expressway C logs we see the Expressway C sending the CSFuser.cnf.xml configuration request to the CUCM on port 6972 used for TFTP:

```
2023-12-12T11:14:56.307-07:00 clus2025expc traffic_server[22698]: UTCTime="2023-12-12 18:14:56,307"
Module="network.http.trafficserver" Level="DEBUG": Detail="Sending Request" Txn-id="1410111"
TrackingID="8d1b73e1-cfee-4066-8432-be78a1d1c000" Dst-ip="0.0.0.8" Dst-port="6972"
HTTPMSG:
|GET /CSFuser.cnf.xml HTTP/1.1
Host: 0.0.0.8:6972
Accept: */*
Cookie:<CONCEALED>
User-Agent: WebEx/1.0.0.2 (Windows;)
TrackingID: 8d1b73e1-cfee-4066-8432-be78a1d1c000
Client-ip: 0.0.0.3
X-Forwarded-For: 0.0.0.3, 127.0.0.1
Via: https/1.1 vcs[793cc42c-a89c-4d85-bfac-abef6ee56000] (ATS), http/1.1 vcs[e00de37e-99fa-4ea8-aad9-
f92e1b306000] (ATS)
 |
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

We then see the SSL connection to the CUCM fail with the tlsv1 alert unknown ca failure followed by the 502 connect failed response:

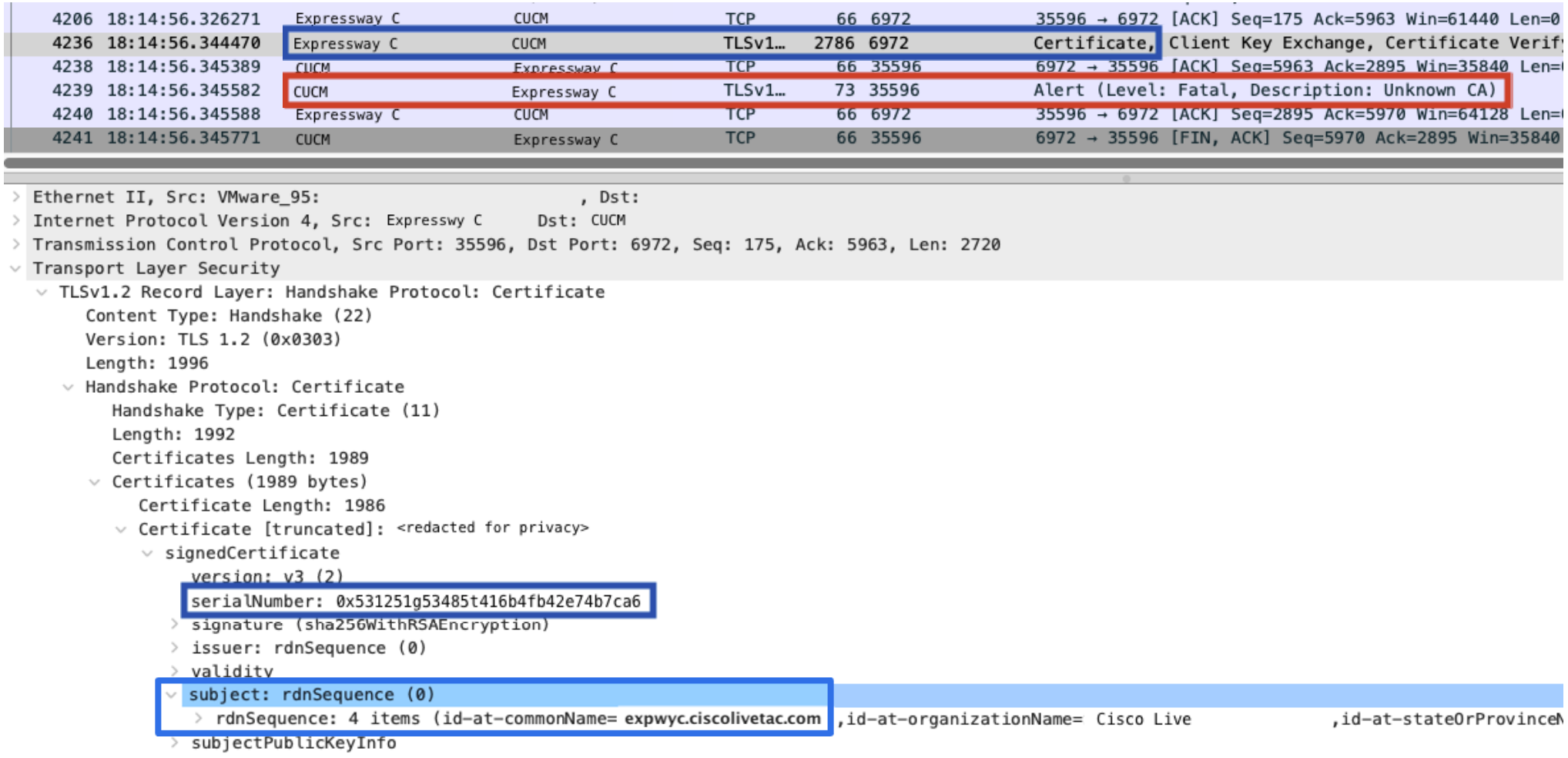
```
2023-12-12T11:14:56.345-07:00 clus2025expc traffic_server[22698]: [ET_NET 1] ERROR: SSL connection failed
for '0.0.0.8': error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca

2023-12-12T11:14:56.382-07:00 clus2025expc traffic_server[22698]: UTCTime="2023-12-12 18:14:56,382"
Module="network.http.trafficserver" Level="DEBUG": Detail="Sending Response" Txn-id="1410111" TrackingID=""
Dst-ip="127.0.0.1" Dst-port="32794"
HTTPMSG:
|HTTP/1.1 502 connect failed
Date: Tue, 12 Dec 2023 18:14:56 GMT
Connection: keep-alive
Server: CE_C
Cache-Control: no-store
Content-Type: text/html
Content-Language: en
Content-Length: 247
 |
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

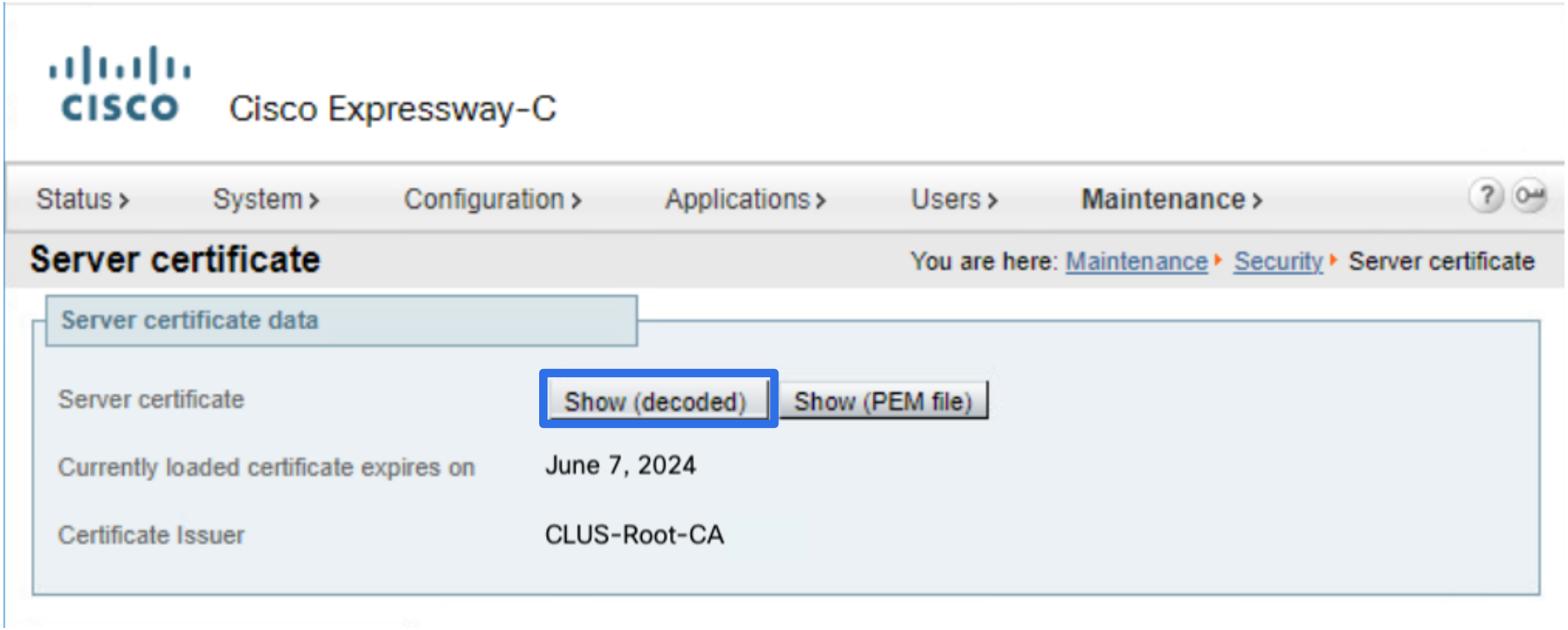
Confirm the serial number of the problematic certificate from the Expressway-C packet capture.



© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

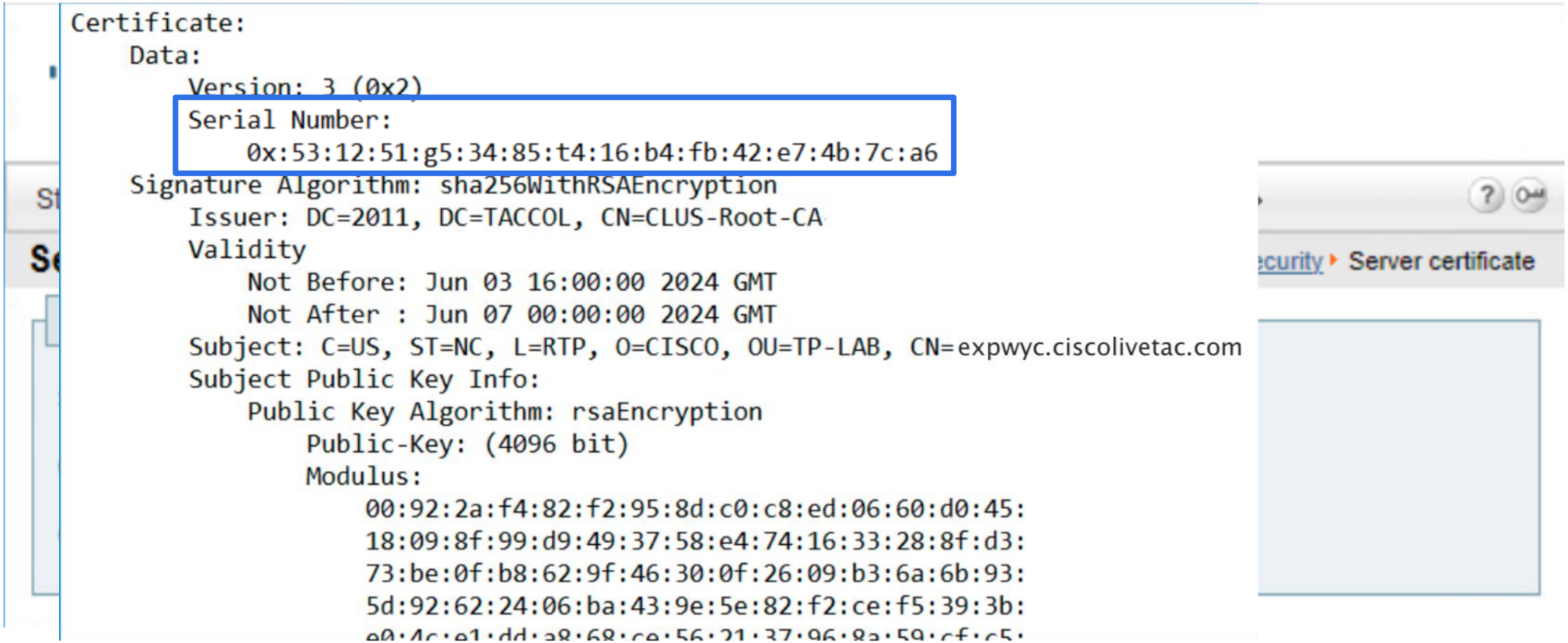
Check the installed Expressway-C certificate and check the serial number to make sure it matches the serial number identified in the logs



© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

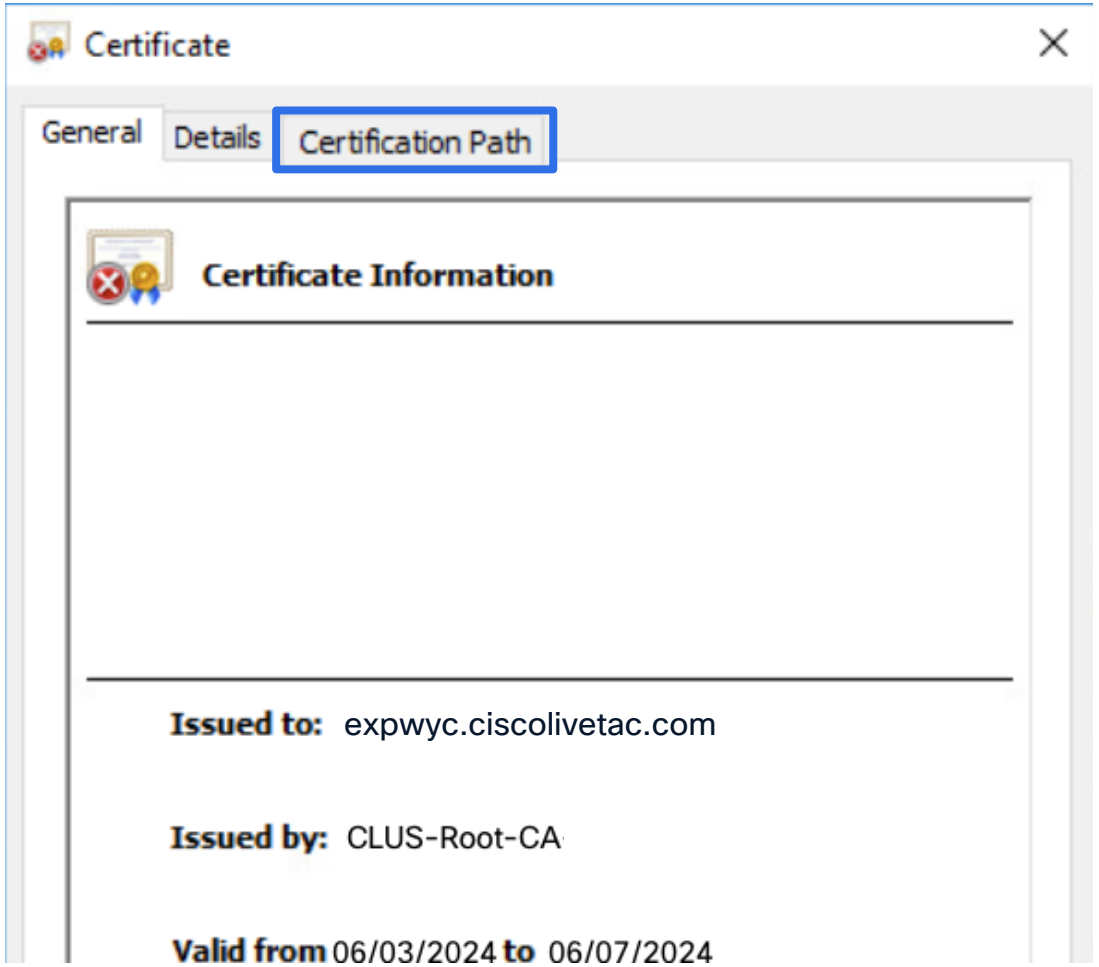
Check the installed Expressway-C certificate and check the serial number to make sure it matches the serial number identified in the logs



© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

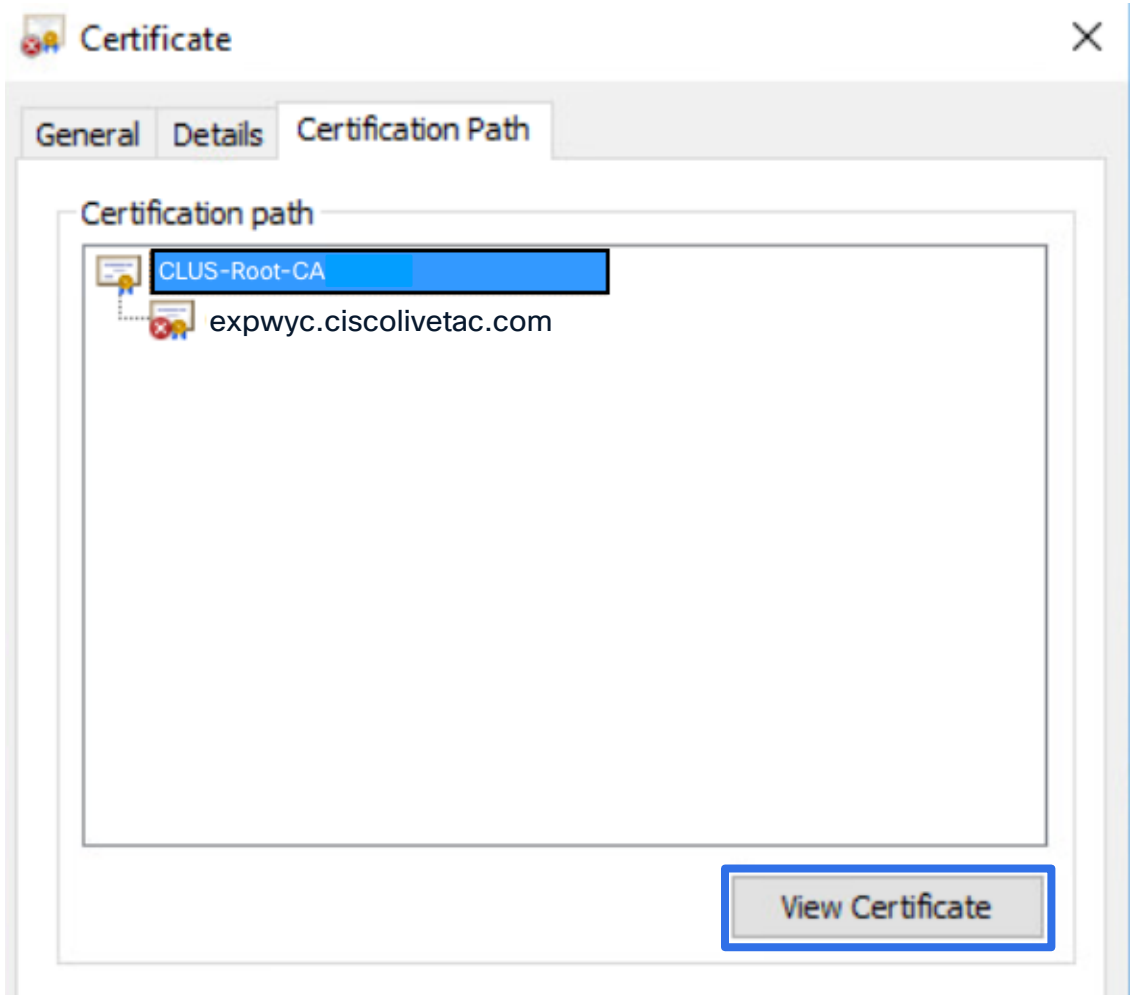
Open the certificate and use the “Certification Path” to view the Intermediate and Root certificates and confirm their respective serial numbers



© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

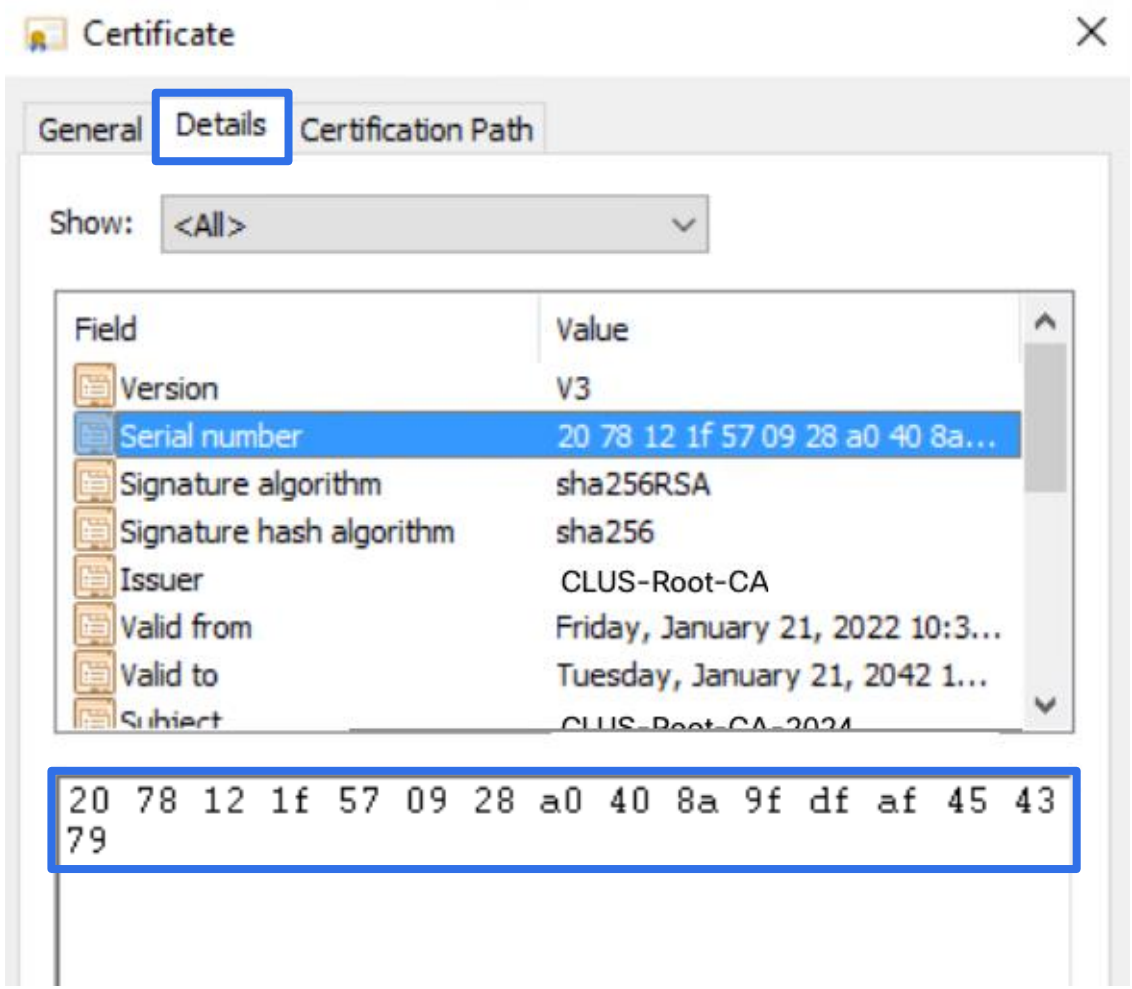
Open the certificate and use the “Certification Path” to view the Intermediate and Root certificates and confirm their respective serial numbers



© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

Open the certificate and use the “Certification Path” to view the Intermediate and Root certificates and confirm their respective serial numbers



© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

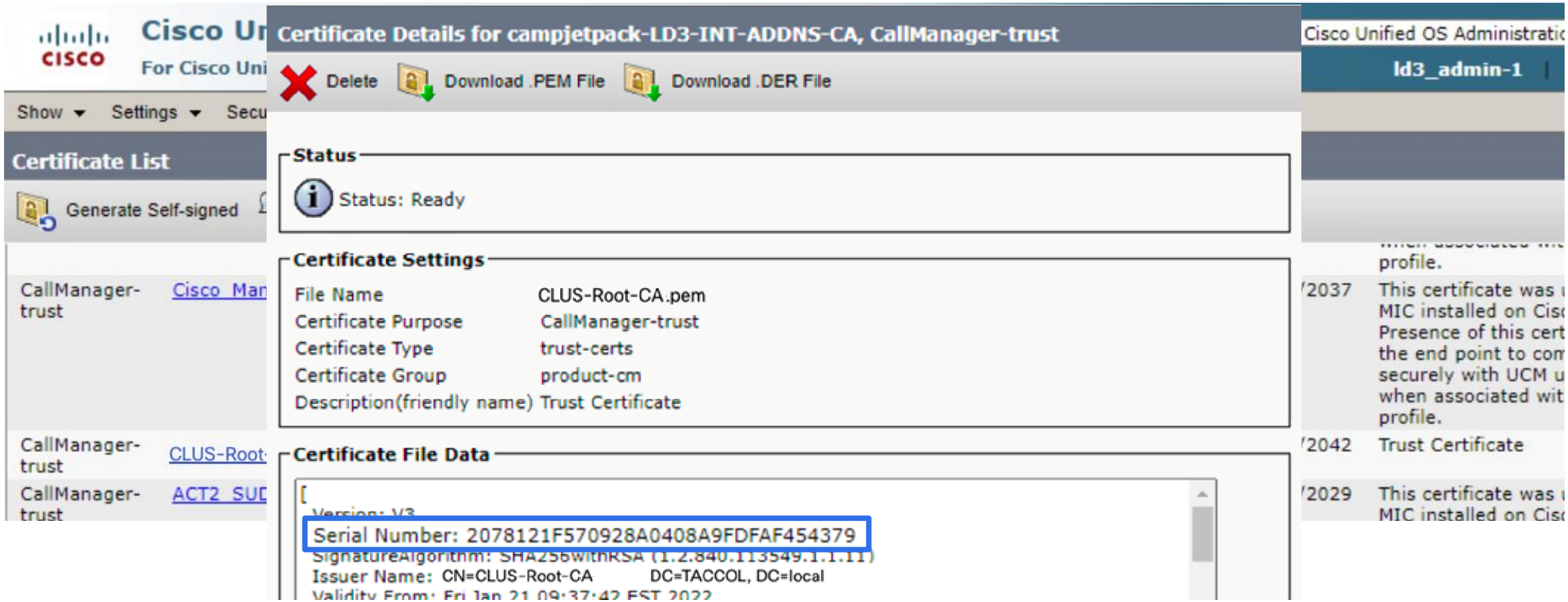
Check the CUCM CallManager-trust and tomcat-trust stores to confirm the Expressway-C Intermediate and Root CA certificates are installed



© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

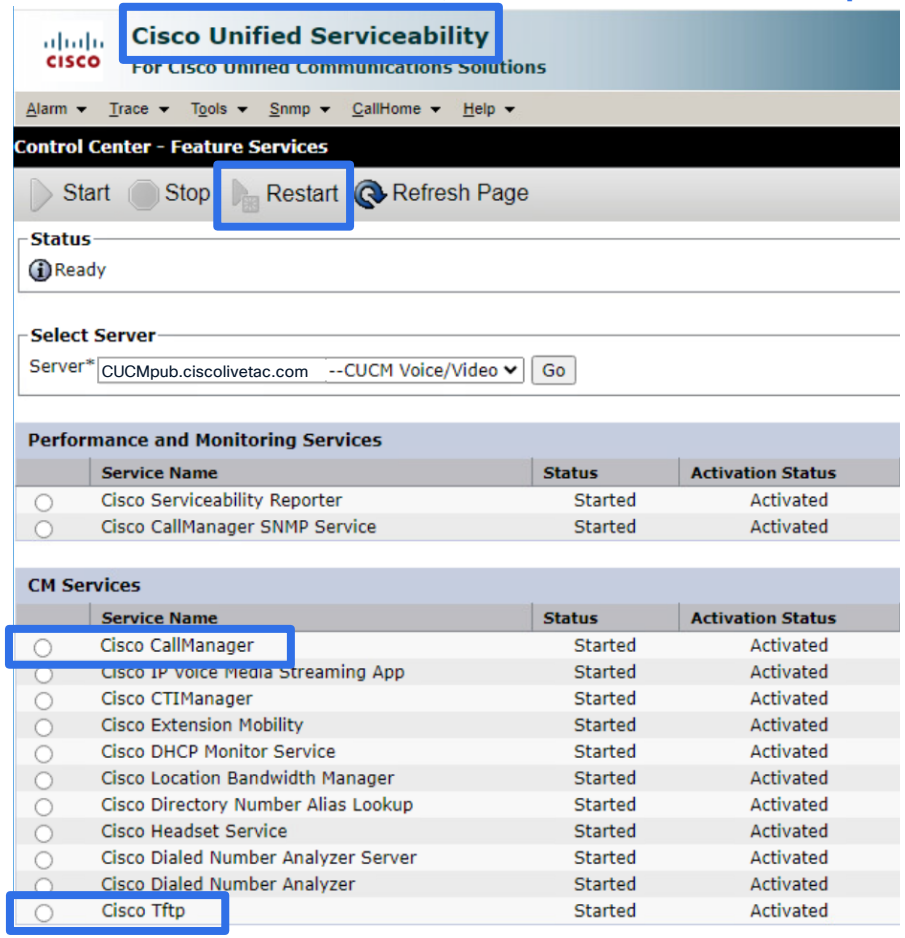
If the Expressway C Intermediate and Root CA certificates are already installed, check the Serial Number of the certificates in CUCM to confirm they are the same as identified from the Expressway C certificate chain



© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

If the Expressway-C CA certificates are uploaded to the CUCM trust stores and the serial numbers have been validated, then the next step would be to restart CallManager, TFTP, and tomcat services



CallManager and TFTP can be restarted from the web UI.

Tomcat can only be restarted from the CLI

```
admin:utils service restart Cisco Tomcat
Do not press Ctrl+C while the service is restarting.
arted properly, execute the same command again.
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Traffic Server Enforces Certificate Verification

This improvement requires the Expressway-C certificate signing CAs (root and intermediates) to be added in CUCM tomcat-trust and CallManager-trust list. After adding these certificates, ***you must also restart TFTP, CallManager and Tomcat services on each CUCM node in the cluster***.

Expressway C:
CA Certificates
(root and all intermediates)

Call Manager Trust Stores:
CallManager-trust
tomcat-trust



© 2025 Cisco and/or its affiliates. All rights reserved.

Impact of CUCM Service Restarts

CallManager Restart:
- High impact
- Will impact endpoints, device registration, and call management during the restart
- Restart can take 5-15 minutes depending on the size of the UCM cluster
- Change window or after hours is recommended

Tomcat Restart:
- Medium-Low impact
- Impacts web UI access, new SSO logins, and Extension Mobility logins during the restart
- Restart can take 20-30 minutes
- Change window or after hours at the customer's discretion

TFTP Restart:
- Low impact
- TFTP requests during the restart will fail, and can trigger update for phones not running the most recent phone load
- Restart during production hours typically OK but at the customer's discretion

When in doubt, restart in a change window or after hours

© 2025 Cisco and/or its affiliates. All rights reserved.

“When I try to upload a CA certificate into my expressway trust store, I’m getting a duplicate certificate error”

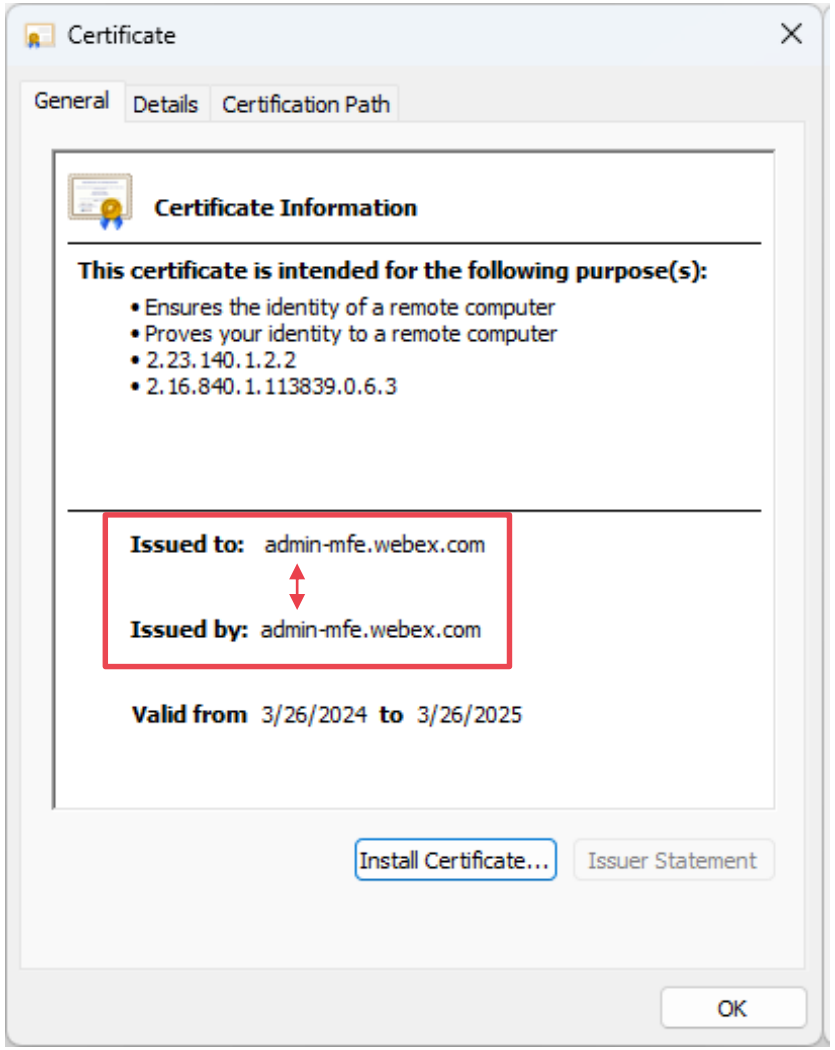
Expressway prevents duplicate self-signed certificates with the same Common Name

© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway prevents duplicate self-signed certificates with the same Common Name

Expressway previously allowed the upload of two self-signed certificates with identical Common Names (CN) to its trusted CA store, despite the underlying restriction preventing the use of two self-signed certificates with the same CN.

This limitation has been addressed in subsequent versions, including x14.2 and x14.0.7 and upwards. Expressway now prevents the upload of a second self-signed certificate if a certificate with a matching CN already exists in the trusted CA store.

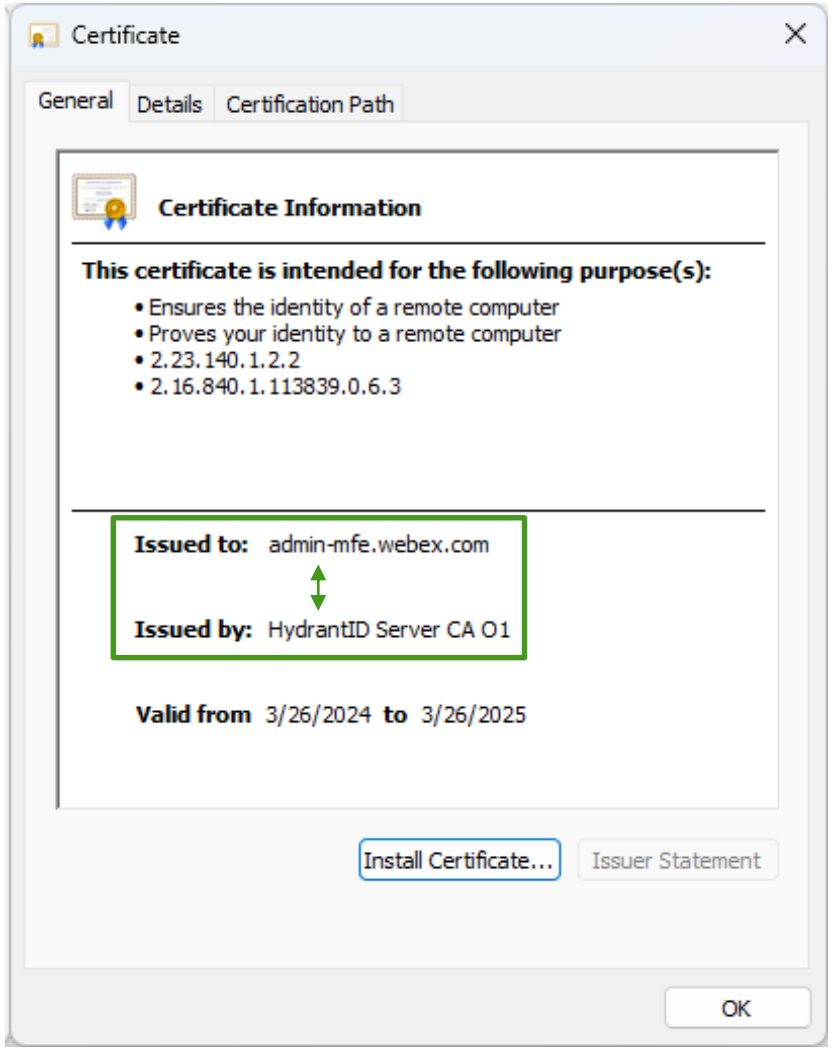


© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway prevents duplicate self-signed certificates with the same Common Name

Expressway previously allowed the upload of two self-signed certificates with identical Common Names (CN) to its trusted CA store, despite the underlying restriction preventing the use of two self-signed certificates with the same CN.

This limitation has been addressed in subsequent versions, including x14.2 and x14.0.7 and upwards. Expressway now prevents the upload of a second self-signed certificate if a certificate with a matching CN already exists in the trusted CA store.



© 2025 Cisco and/or its affiliates. All rights reserved.

“After upgrading my expressways to version x14.2, I’m unable to login over MRA”

Expressway-C Certificate Validation Change

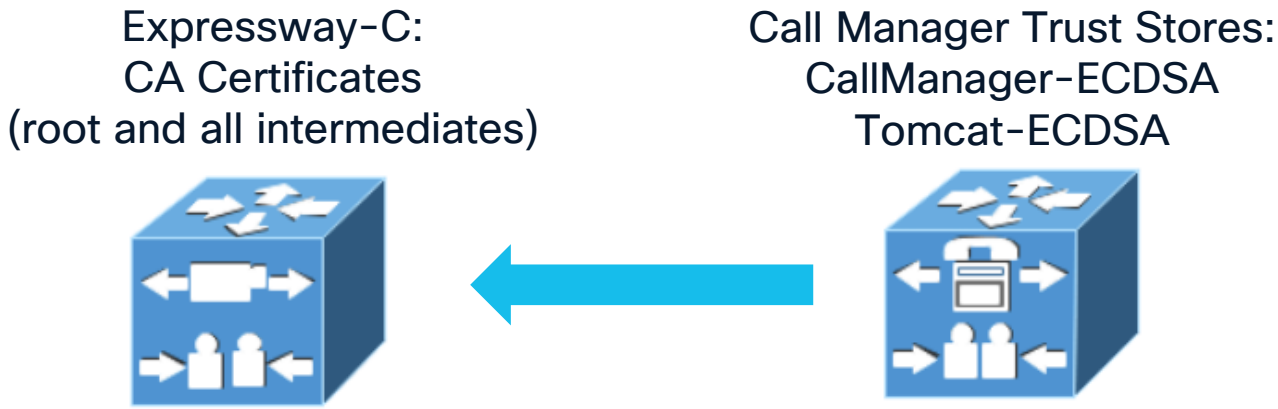
© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Certificate Validation Change

Starting with version x14.2, Expressway now verifies the certificate from UC servers and prioritizes cipher lists differently. This change may lead to unexpected TLS connections following a software upgrade.

Prior to the upgrade, it may have been configured to request the Cisco Tomcat or Cisco CallManager RSA certificate from CUCM (or any other product with a separate certificate for the ECDSA algorithm).

However, post-upgrade, it might prioritize the ECDSA variant, which is more secure than RSA.



© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Certificate Validation Change

The identifying signature for this issue is Expressway connections to CUCM fails after establishing a TLS connection with errors “self signed certificate server” and “502 connect failed”

```
2024-01-05T12:33:14.901-05:00 clus2025expresswayc traffic_server[10907]: [ET_NET 2] WARNING: Core server certificate verification failed for (cucm.clus2025). Action=Terminate Error=self signed certificate server=cucm.clus2025(0.0.0.10) depth=0
2024-01-05T12:33:14.901-05:00 clus2025expresswayc traffic_server[10907]: [ET_NET 2] ERROR: SSL connection failed for 'cucm.clus2025': error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed
2024-01-05T12:33:14.902-05:00 clus2025expresswayc traffic_server[10907]: UTCTime="2024-01-05 17:33:14,902" Module="network.http.trafficserver" Level="INFO": Detail="Sending Response" Txn-id="56" TrackingID="" Dst-ip="127.0.0.1" Dst-port="32790" Msg="HTTP/1.1 502 connect failed"
2024-01-05T12:33:14.902-05:00 clus2025expresswayc traffic_server[10907]: UTCTime="2024-01-05 17:33:14,902" Module="network.http.trafficserver" Level="DEBUG": Detail="Sending Response" Txn-id="56" TrackingID="" Dst-ip="127.0.0.1" Dst-port="32790"
HTTPMSG:
|HTTP/1.1 502 connect failed
Date: Fri, 05 Jan 2024 17:33:14 GMT
Connection: keep-alive
Server: CE_C
Cache-Control: no-store
Content-Type: text/html
Content-Language: en
Content-Length: 247
```

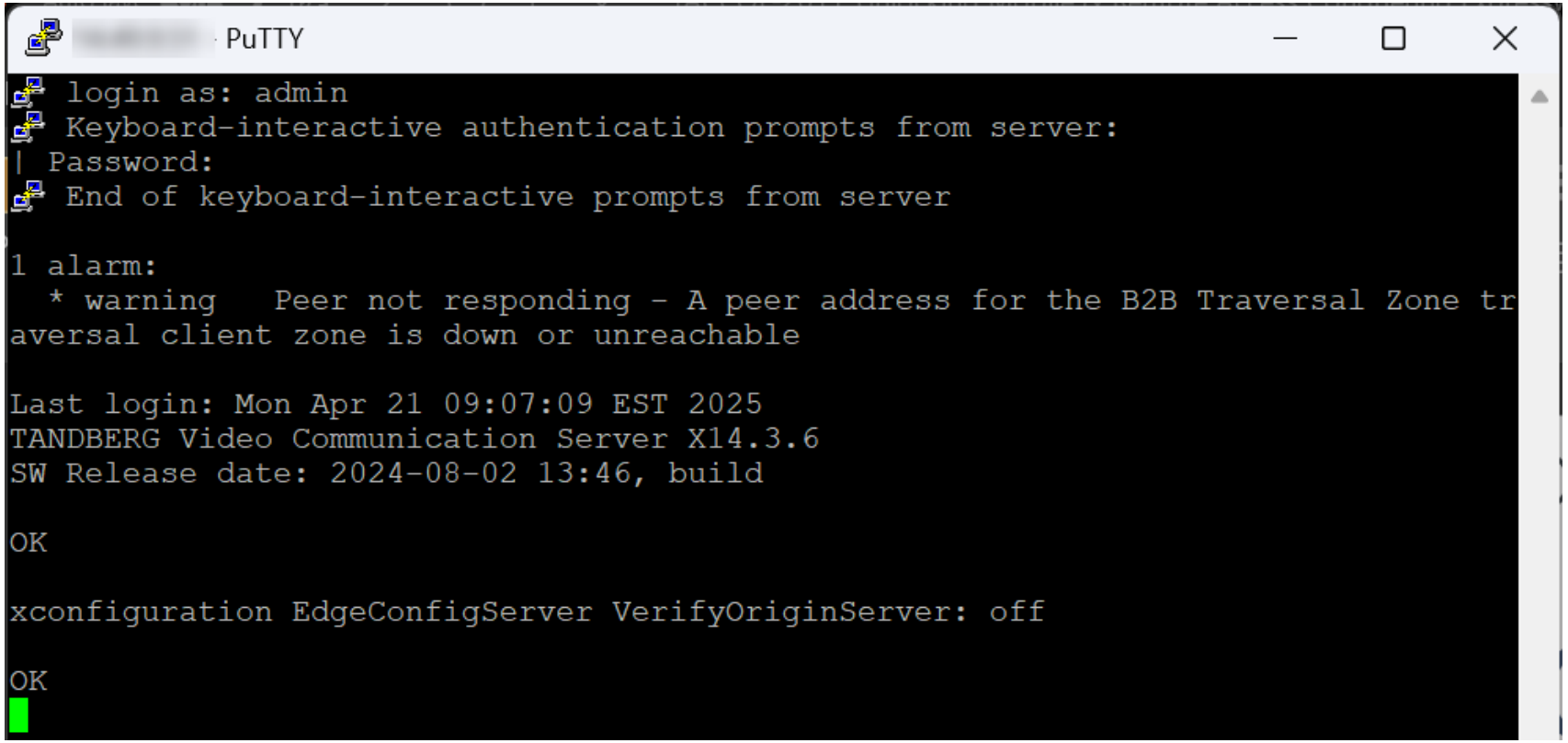
© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Certificate Validation Change

Workaround

TAC Tip

Apply command “*xConfiguration EdgeConfigServer VerifyOriginServer: Off*” on Expressway-C to stop certificate verification against CUCM, IMP and Unity in order to regain MRA services while fix is applied



© 2025 Cisco and/or its affiliates. All rights reserved.

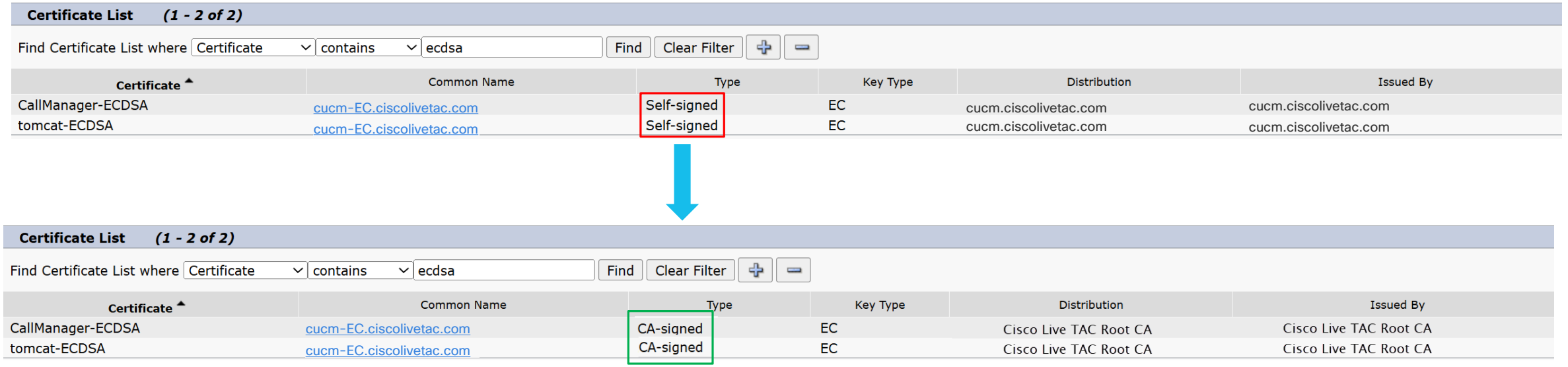
Expressway-C Certificate Validation Change

Fix #1 (recommended)

Uploading self-signed certificates to the Expressway-C Trusted CA database isn't feasible due to identical common names.

Cisco Tomcat-ECDSA and Cisco CallManager-ECDSA certificates need to be signed by a CA.

By doing this, we can upload the CA that signed the ECDSA certificates into the expressway-c and re-establish the TLS connectivity between the two servers

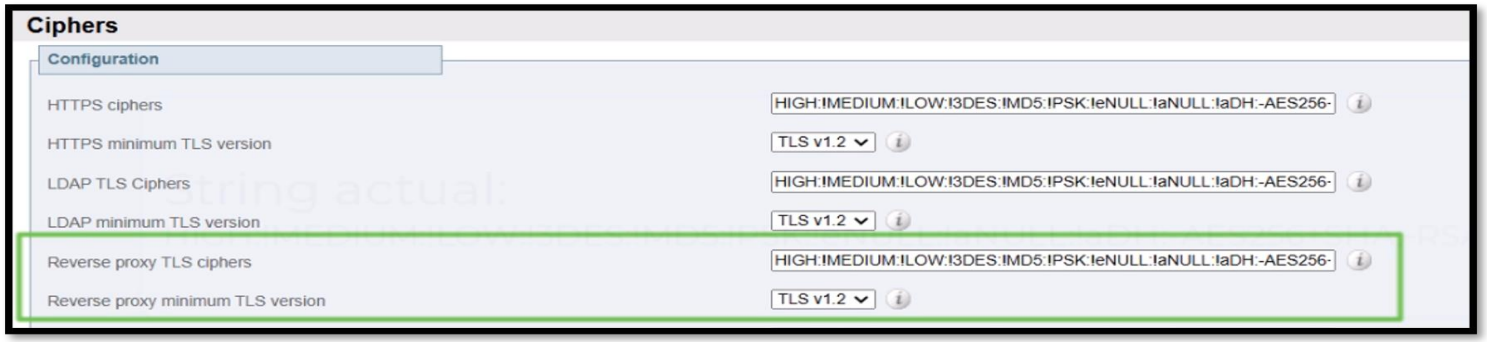


© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway-C Certificate Validation Change

Fix #2

Modify the reverse proxy cipher string so that Expressway-C requests Tomcat to present the RSA certificate, signed by an authority that C trusts.



Original string:

HIGH:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH:-AES256+SHA:-RSA+AESCCM:-DHE+AESCCM:-DHE+CHACHA20

Modified string:

ECDHE-RSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH:-AES256+SHA:-RSA+AESCCM:-DHE+AESCCM:-DHE+CHACHA20

© 2025 Cisco and/or its affiliates. All rights reserved.

“Our security scans found the following weak ciphers that need to be disabled...”

Disabling Ciphers

© 2025 Cisco and/or its affiliates. All rights reserved.

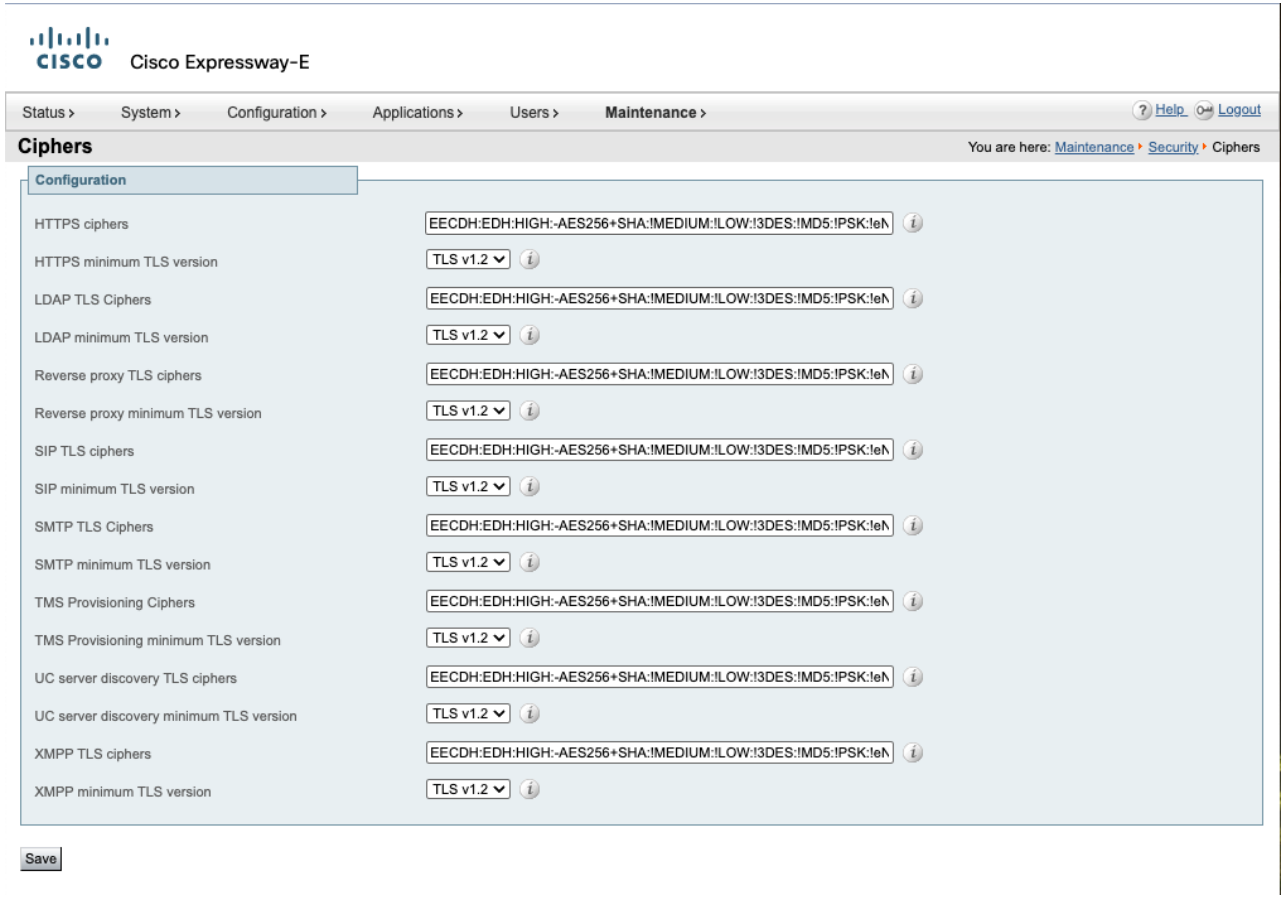
Configuring Ciphers in Expressway

Expressway ciphers can be modified from the Maintenance > Security > Cipher page.

Expressway uses OpenSSL formatted cipher names in the cipher configuration.

ie. TLS_RSA_WITH_AES_128_CCM (IANA) = AES128-CCM (OpenSSL)

Ciphers can be configured for HTTPS, LDAP, Reverse Proxy, SIP, SMTP, TMS provisioning, UC server discovery, and XMPP.



© 2025 Cisco and/or its affiliates. All rights reserved.

Configuring Ciphers in Expressway

```
~ # openssl ciphers -V "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH:!AES256+DH+AESCCM
"
         0x13,0x02 - TLS_AES_256_GCM_SHA384  TLSv1.3 Kx=any      Au=any  Enc=AESGCM(256) Mac=AEAD
         0x13,0x03 - TLS_CHACHA20_POLY1305_SHA256 TLSv1.3 Kx=any      Au=any  Enc=CHACHA20/POLY1305(256) Mac=AEAD
         0x13,0x01 - TLS_AES_128_GCM_SHA256  TLSv1.3 Kx=any      Au=any  Enc=AESGCM(128) Mac=AEAD
         0xC0,0x2C - ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AESGCM(256) Mac=AEAD
         0xC0,0x30 - ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AESGCM(256) Mac=AEAD
         0xCC,0xA9 - ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
         0xCC,0xA8 - ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH     Au=RSA  Enc=CHACHA20/POLY1305(256) Mac=AEAD
         0xC0,0xAD - ECDHE-ECDSA-AES256-CCM  TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AESCCM(256) Mac=AEAD
         0xC0,0x2B - ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AESGCM(128) Mac=AEAD
         0xC0,0x2F - ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AESGCM(128) Mac=AEAD
         0xC0,0xAC - ECDHE-ECDSA-AES128-CCM  TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AESCCM(128) Mac=AEAD
         0xC0,0x24 - ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES(256)  Mac=SHA384
         0xC0,0x28 - ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(256)  Mac=SHA384
         0xC0,0x23 - ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES(128)  Mac=SHA256
         0xC0,0x27 - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(128)  Mac=SHA256
         0xC0,0x09 - ECDHE-ECDSA-AES128-SHA  TLSv1 Kx=ECDH     Au=ECDSA Enc=AES(128)  Mac=SHA1
         0xC0,0x13 - ECDHE-RSA-AES128-SHA    TLSv1 Kx=ECDH     Au=RSA  Enc=AES(128)  Mac=SHA1
         0x00,0xA3 - DHE-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH       Au=DSS  Enc=AESGCM(256) Mac=AEAD
         0x00,0x9F - DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH       Au=RSA  Enc=AESGCM(256) Mac=AEAD
         0xCC,0xAA - DHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=DH       Au=RSA  Enc=CHACHA20/POLY1305(256) Mac=AEAD
         0x00,0xA2 - DHE-DSS-AES128-GCM-SHA256 TLSv1.2 Kx=DH       Au=DSS  Enc=AESGCM(128) Mac=AEAD
         0x00,0x9E - DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH       Au=RSA  Enc=AESGCM(128) Mac=AEAD
         0xC0,0x9E - DHE-RSA-AES128-CCM      TLSv1.2 Kx=DH       Au=RSA  Enc=AESCCM(128) Mac=AEAD
         0x00,0x6B - DHE-RSA-AES256-SHA256   TLSv1.2 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA256
         0x00,0x6A - DHE-DSS-AES256-SHA256   TLSv1.2 Kx=DH       Au=DSS  Enc=AES(256)  Mac=SHA256
         0x00,0x67 - DHE-RSA-AES128-SHA256   TLSv1.2 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA256
         0x00,0x40 - DHE-DSS-AES128-SHA256   TLSv1.2 Kx=DH       Au=DSS  Enc=AES(128)  Mac=SHA256
         0x00,0x33 - DHE-RSA-AES128-SHA      SSLv3 Kx=DH     Au=RSA  Enc=AES(128)  Mac=SHA1
         0x00,0x32 - DHE-DSS-AES128-SHA      SSLv3 Kx=DH     Au=DSS  Enc=AES(128)  Mac=SHA1
         0x00,0x9D - AES256-GCM-SHA384       TLSv1.2 Kx=RSA      Au=RSA  Enc=AESGCM(256) Mac=AEAD
         0xC0,0x9D - AES256-CCM              TLSv1.2 Kx=RSA      Au=RSA  Enc=AESCCM(256) Mac=AEAD
         0x00,0x9C - AES128-GCM-SHA256       TLSv1.2 Kx=RSA      Au=RSA  Enc=AESGCM(128) Mac=AEAD
         0xC0,0x9C - AES128-CCM              TLSv1.2 Kx=RSA      Au=RSA  Enc=AESCCM(128) Mac=AEAD
         0x00,0x3D - AES256-SHA256           TLSv1.2 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA256
         0x00,0x3C - AES128-SHA256           TLSv1.2 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA256
         0x00,0x2F - AES128-SHA              SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
~ #
```

Log into the CLI with root credentials and run the following command to validate the list of currently available ciphers:

~ # openssl ciphers -V “<cipher string>”

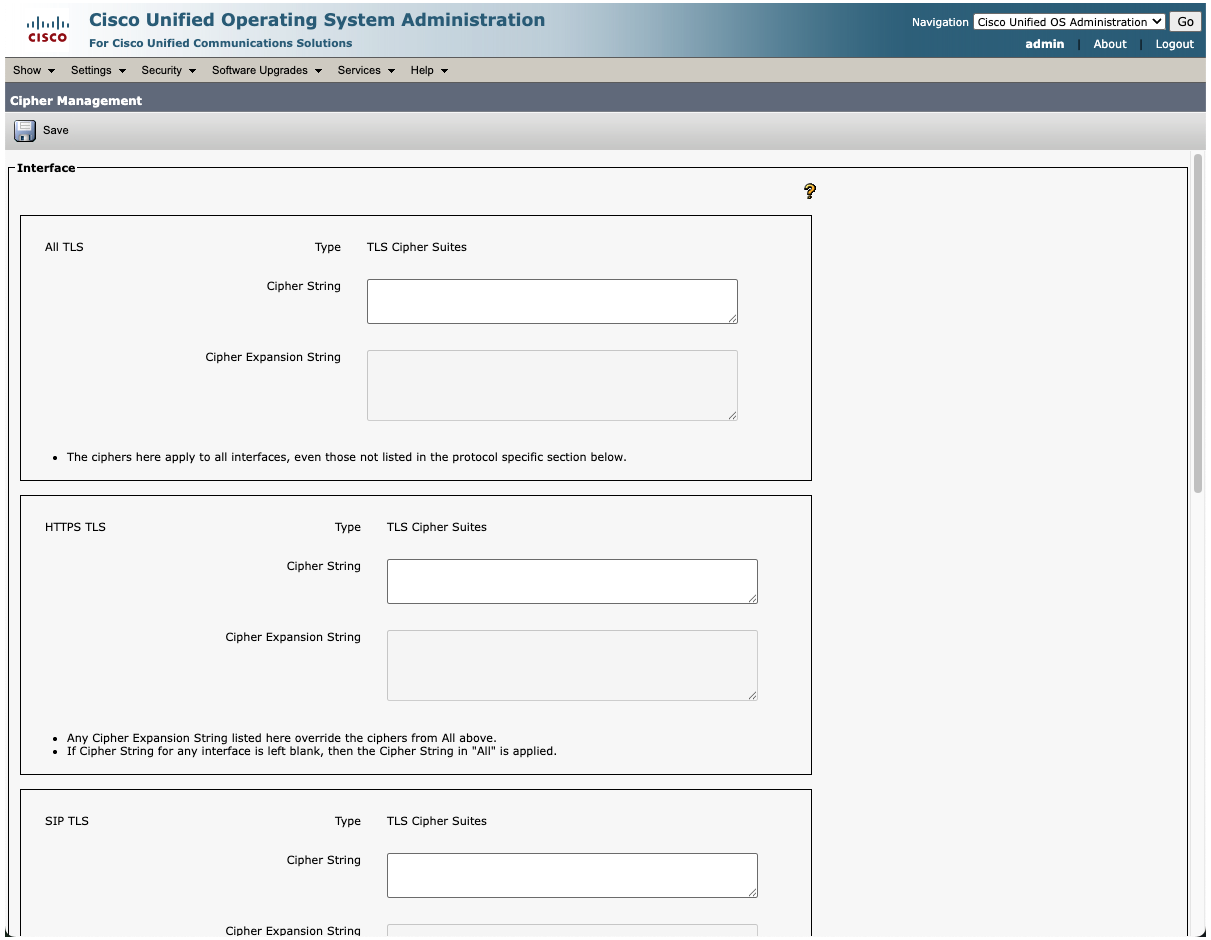
On the Expressway cipher page, append the cipher you would like to disable to the cipher string using the : separator and the ! or – symbol before the OpenSSL cipher name:

<cipher string>:!AES128-CCM

After disabling the cipher from the cipher configuration page, an Expressway restart is required for the change to take effect.

© 2025 Cisco and/or its affiliates. All rights reserved.

Configuring Ciphers in CUCM



CUCM ciphers can be configured from Cisco Unified OS Administration > Security > Cipher Management.

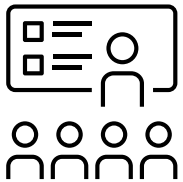
CUCM cipher configuration uses OpenSSL formatting.

Any cipher string configured in the HTTPS TLS or SIP TLS field overrides what is configured in the All TLS field.

© 2025 Cisco and/or its affiliates. All rights reserved.

Upcoming!

Move to 47 Day Certificates



The Change

On April 11, 2025 the CA/Browser Forum voted to amend the TLS Baseline Requirements to shorten the lifetime of TLS certificates, and the time in which domain validation information can be reused.

The aim is to enhance security and drive adoption of automated certificate management.



The Timeline

- As of March 15, 2026 max lifetime of a TLS certificate is 200 Days, domain validation info can be reused for 200 days
- As of March 15, 2027 max lifetime of a TLS certificate is 100 Days, domain validation info can be reused for 100 days
- As of March 15, 2029 max lifetime of a TLS certificate is 47 Days, domain validation info can be reused for 10 days

© 2025 Cisco and/or its affiliates. All rights reserved.

ACME Certificates for Expressway

Automated

The ACME service is an optional service on the Expressway E that automates the certificate renewal and deployment process using the Let's Encrypt CA to sign Expressway certificates.

Frequent Expiry

For increased security, certificates expire in 90 days (compared to the typical 1-year certificate) and new certificates are automatically fetched at 60 days.

No Impact Renewal

Automated renewal does not require an Expressway restart. Existing TLS connections are not dropped, and the new certificate is used for new connections.
No impact to MRA connectivity.

© 2025 Cisco and/or its affiliates. All rights reserved.

Expressway ACME Configuration

Cisco Expressway Certificate Creation and Use Deployment Guide (X14.3)
Chapter: Using ACME on Expressway-E

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-3/cert_creation_use/exwy_b_cisco-expressway-certificate-creation-and-use-deployment-guide-x14-3/exwy_m_using-acme-on-expressway-e.html

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you

cisco Live !

Q & A

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



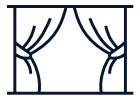
Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live mobile app.

© 2025 Cisco and/or its affiliates. All rights reserved.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting



Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact us at: jgamboag@cisco.com & ldeleoni@cisco.com

© 2025 Cisco and/or its affiliates. All rights reserved.


CISCO