Prepare Expressway for Client Auth EKU Sunset in Public CA Certificates

Contents

- Introduction
- Backgroup Information
- Problem Definition
  - Chrome Root Program Policy Change
  - Key Policy Requirements
  - Public CA Response Timeline
  - Related Cisco Documentation
- How It Impacts the Expressway Solution
  - Affected Products
  - Dual Role of Expressway
- Specific Affected Use Cases
- Recommendations
  - Audit Current Certificates (MANDATORY FIRST STEP)
  - Short-Term Workarounds (Before June 2026)
  - Option 1: Switch to Public Root CAs Providing Combined EKU Certificates
  - Option 2: Renew Current Certificates to Extend Their Validity
    - Renewal Strategy
    - Special Considerations forLet'sEncrypt Certificates
    - Action Items for Encrypting Users
  - Option 3: Evaluate and Migrate to Alternative CA Providers
    - Private PKI Approach
    - Long-Term Solution (Software Upgrades Required)
    - Cisco Expressway X15.4 Solution Details (February 2026)
    - Cisco Expressway X15.5 Solution Details (May 2026)
- Decision Tree
- Frequently Asked Questions (FAQ)
  - General Questions
  - Let'sEncrypt Specific
  - Upgrade Questions
  - MRA (Mobile and Remote Access) Specific
  - Certificate Management
  - Timeline Questions
- Additional Resources
  - Cisco Documentation
  - External References
  - Certificate Authority Resources
- Conclusion
- Key Takeaways

Introduction

This document describes Chrome Root Program Policy changes on Cisco Expressway and Client Authentication EKU sunset in public CA certificates after 6/26.

Backgroup Information

Digital certificates are electronic credentials issued by trusted Certificate Authorities (CAs) that secure communication between servers and clients by ensuring authentication, data integrity, and confidentiality. These certificates contain Extended Key Usage (EKU) fields that define their purpose:

- Server Authentication EKU (id-kp-serverAuth): Used when a server presents its certificate to prove identity
- Client Authentication EKU (id-kp-clientAuth): Used in mutual TLS (mTLS) connections where both parties authenticate each other

Traditionally, a single certificate could contain both Server and Client Authentication EKUs, allowing it to serve dual purposes. This is particularly important for products like Cisco Expressway that act as both server and client in different connection scenarios.

Problem Definition

Chrome Root Program Policy Change

Effective June 2026, the Chrome Root Program Policy restricts Root Certificate Authority (CA) certificates included in the Chrome Root Store, phasing out multi-purpose roots to align all public-key infrastructure (PKI) hierarchies to serve only TLS server authentication use cases.

Key Policy Requirements

- Public Root CAs must assert Extended Key Usage (EKU) ONLY for Server Authentication (id-kp-serverAuth)
- Certificates must include ONLY Server Authentication EKU to maintain trust from Google Chrome browser
- Including Client Authentication EKU in these certificates are prohibited
- Root CAs that continue to issue certificates with Client Authentication EKU are eventually removed from the Chrome Root Store
- No more mixed-use root CAs for public server TLS certificates
- Enforcement Timeline: June 2026

Public CA Response Timeline

- October 2025: Many public CAs (DigiCert, Sectigo, SSL) began issuing server-only certificates by default
- February 11, 2026: Let's Encrypt stops issuing certificates with Client Authentication EKU using the *classic* ACME profile
- May 2026: Public CA servers stop issuing Client Authentication EKU certifications
- June 2026: Chrome Root Program Policy becomes fully effective

Note: This policy applies only to certificates issued by public CAs. Private PKI and self-signed certificates are not affected by this policy.

Related Cisco Documentation

- Cisco bug ID: CSCwr73373- Support for separate server and client Certificate for Expressway
- Field Notice: FN74362
- Chrome Root Program Policy: Chrome Root Program Policy Documentation

How It Impacts the Expressway Solution

Affected Products

Per Field Notice FN74362, all Cisco Expressway versions are affected:

Product	Affected Releases	Impact
Expressway Core and Edge	X14 (All versions)	X14.0.0 through X14.3.7 - All releases affected
Expressway Core and Edge	X15 (Versions before X15.4)	X15.0.0 through X15.3.2 - All releases affected

Dual Role of Expressway

Cisco Expressway products (Expressway-C and Expressway-E) act as both server and client in various connection scenarios, requiring certificates with both Server and Client Authentication EKUs.

Expressway E as Server (Server Authentication EKU required):

- HTTPS browser access
- SIP UC Traversal connections
- Webex Edge Audio/MRA connectivity

Expressway E as Client (Client Authentication EKU required):

- B2B communications
- MRA (Mobile and Remote Access) connections
- XMPP Federation
- SIP Neighbor Zone/CMS connections
- Interactions with external entities
- Connection to Cisco Cloud (MRA Onboarding)

Specific Affected Use Cases

The Public CA-signed certificate with Client Authentication EKU currently used for mTLS connections in Cisco Expressway is the Expressway Server Certificate. This certificate is used for the these mTLS connections:

1. SIP B2B call over mTLS - Expressway E becomes client or server on mTLS connection, depending on session-initiated site
2. SIP IMP Federation over mTLS - Expressway E becomes client or server on mTLS connection, depending on session-initiated site
3. UC Traversal Zone - Expressway C presents Client Authentication EKU
4. Traversal Zone with mTLS configuration - Expressway C presents Client Authentication EKU
5. SIP Neighbour Zone with mTLS configuration - Expressway becomes client or server on mTLS connection, depending on session-initiated site, including connections with:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unity
- Cisco Unified Border Element (CUBE)
- Cisco Meeting Server (CMS)
- Connection to Cisco Cloud - MRA Onboarding (Expressway initiates the connection to Cisco Cloud and presents Client Authentication EKU)

Recommendations

Audit Current Certificates (MANDATORY FIRST STEP)

Per Field Notice FN74362, before considering workaround and solution options:

- Prepare an inventory of all public TLS certificates to identify which certificates contain the Client Authentication EKU
- Take a backup of your Cisco Expressway instance or manually copy the signed certificate and Private key
- Document certificate usage: Identify which certificates are used for mTLS connections
- Verify CA and root information: Document which CA and root issued each certificate
- Check expiration dates: Plan renewals strategically before policy enforcement

Short-Term Workarounds (Before June 2026)

Administrators can choose from one of these workaround options:

Option 1: Switch to Public Root CAs Providing Combined EKU Certificates

Some Public Root CAs (such as DigiCert and IdenTrust) issue certificates with combined EKU from an alternative root, which can not be included in the Chrome browser trust store.

Examples of Public Root CAs and EKU Types (per FN74362):

CA Vendor	**EKU Type**	**Root CA**	**Issuing/Sub CA**
IdenTrust	clientAuth + serverAuth	IdenTrust Public Sector Root CA 1	IdenTrust Public Sector Server CA 1
DigiCert	clientAuth + serverAuth	DigiCert Assured ID Root G2	DigiCert Assured ID CA G2

Prerequisites for this approach:

- Coordinate with your CA provider to check the availability of such certificates.
- Before deploying certificates, ensure that both the server presenting the certificate and all clients consuming it trust the corresponding Root CA.
- Exchange root certificate information with communication peers.
- This approach avoids immediate need for software upgrades.

Certificate Management References:

- Cisco Expressway Certificate Creation and Use Deployment Guide (X14.0)
- Cisco Expressway Certificate Creation and Use Deployment Guide (X15.0)

Option 2: Renew Current Certificates to Extend Their Validity

Certificates issued by Public Root CAs before May 2026 that have both Server and Client Authentication EKU continue to be honored until their term expires.

Renewal Strategy

General recommendations are:

- Renew combined EKU certificates before policy sunsetting occurs
- For maximum certificate validity, plan to renew certificates before March 15, 2026.
- After this date, Public CA-issued certificates are valid only for 200 days.
- Cisco strongly recommends that you renew your certificates before this date if you wish to pursue this option.
- Public CA policy and implementation dates can vary.
- Some Public CAs have stopped issuing combined EKU certificates and can not provide one by default.
- To generate a certificate with a combined EKU, work with your CA authority and use a special profile provided by Public CAs.

Special Considerations for Let's Encrypt Certificates

Per FN74362, if you use Let's Encrypt certificates:

- Currently, Expressway uses a classic ACME profile that is hardcoded and cannot be modified by users
- This classic ACME profile is presently used for requesting certificates that include both Server and Client Authentication EKUs
- Starting February 11, 2026, certificate requests using this profile no longer include the Client Authentication EKU in certificates generated by Let's Encrypt
- For more information, see Ending TLS Client Authentication Certificate Support in 2026 - Let's Encrypt

Action Items for Encrypting Users

- Renew certificates before February 11, 2026 - ideally as close to this date as possible to maximize the 90-day validity period.
- Disable the ACME automated scheduler to prevent certificates from being automatically renewed

after February 11, 2026.
- This action helps avoid certificates being inadvertently overwritten with versions that contain only the Server Authentication EKU.
- If you do not renew before February 11, 2026 contact Cisco TAC for support.

Option 3: Evaluate and Migrate to Alternative CA Providers

This option is applicable to: Expressway C only; NOT applicable to Expressway E.

Private PKI Approach

- Evaluate the feasibility of transition to private PKI
- Set up a private CA to issue single certificates with combined EKU (server and client certificates with the required EKUs)
- When issuing a private CA-signed certificate, you need to share root certificate information with the peer.
- Before issuing or deploying a certificate, ensure that both the server presenting the certificate and all clients consuming it trust the corresponding Root CA.
- Private CAs are not subject to Chrome Root Program Policy
- Provides long-term control over certificate policies

⚠ **Caution**: This option is not viable for Expressway-E, which requires public CA certificates for external-facing services and browser trust.

Long-Term Solution (Software Upgrades Required)

Per Field Notice FN74362, Cisco is implementing product enhancements in fixed releases to address this issue comprehensively.

Fixed release schedule:

Product	Affected Release	Fixed Release	Purpose of Fix	Availability
Cisco Expressway	X14.x (All releases) X15.x (Earlier than X15.4)	**X15.4**	Intermittent solution: Allows additional upload of ServerAuth EKU-only signed certificate on Expressway E and certificate verification adjustment for MRA SIP signal between Expressway E and Expressway C	February 2026
Cisco Expressway	X14.x (All releases) X15.x (Earlier than X15.5)	**X15.5**	Comprehensive solution: Provides UI enhancement for segregating client and server certificates and provides options to administrators to disable EKU checking	May 2026

Note: Both Cisco Expressway E and Expressway C must be upgraded to the same version.

Cisco Expressway X15.4 Solution Details (February 2026)

Purpose: Intermittent solution to accommodate certificates with ServerAuth EKU only and to enable MRA registrations

Key enhancements are:

- **Removes restriction on certificate uploads**
- Allows administrators to upload certificates with only Server Authentication EKU via Web GUI on Expressway E
- Previously, Expressway rejected server-only certificates
- **Adjusts certificate verification for MRA**
- Modifies certificate verification for SIP signaling between Expressway-E and Expressway-C in MRA solutions
- Allows acceptance of server-only certificates from third-party applications

Who can upgrade to X15.4:

- if you deploy new or redeploy existing Expressway-E for MRA with server-only signed certificates.
- If you use ACME (Let's Encrypt) certificates after February 11, 2026.
- Existing deployments that need to upgrade signed certificates that only contains Server Authentication EKU.
- if you face certificate-related authentication issues in mTLS connections

Important requirements for X15.4:

- Both Expressway-E and Expressway-C must be upgraded to X15.4
- Plan upgrade during maintenance window to minimize service disruption

Limitations of X15.4 are:

- This is an intermittent solution that addresses immediate compatibility issues
- Does not provide full dual-certificate support
- Does not include service parameter to disable EKU checking
- mTLS connections can fail depending on session-initiated site

Cisco Expressway X15.5 Solution Details (May 2026)

Purpose: Comprehensive solution to meet global Google Chrome Root Program requirements

Key Product Enhancements:

- **Segregation of Client and Server Certificates**
- Enables support for two separate certificates on the same interface
- Expressway certificates with distinct Server Authentication EKU and Client Authentication EKU
- Facilitates proper mTLS connections with segregated certificate roles
- **UI and Backend Enhancements**
- New certificate management interfaces for individual management of both certificates

- Client Authentication EKU validation during certificate upload to avoid accidental MTLS connection drops
- Administrators can upload and manage server and client certificates separately
- **Options to Disable Client Authentication EKU Check**
- Service parameter allowing administrators to disable Client Authentication EKU check according to individual enterprise requirements
- Allows Cisco Expressway to ignore EKU from the remote peer (client) requesting a connection with only Server Authentication EKU certificates
- In the absence of a Client Authentication EKU certificate, allows Expressway to (re)use the Server Authentication EKU-only certificate as a Client certificate

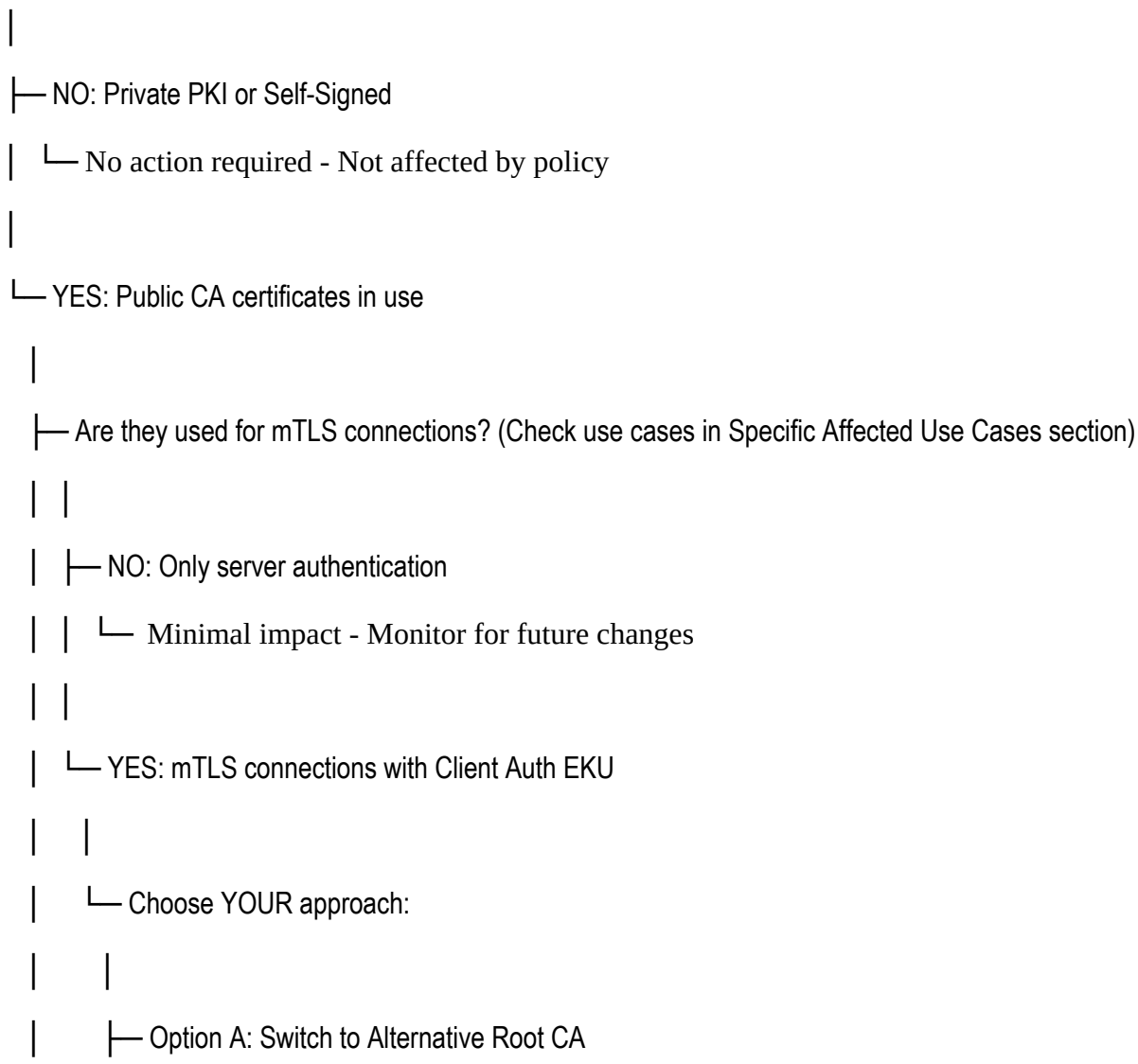
---

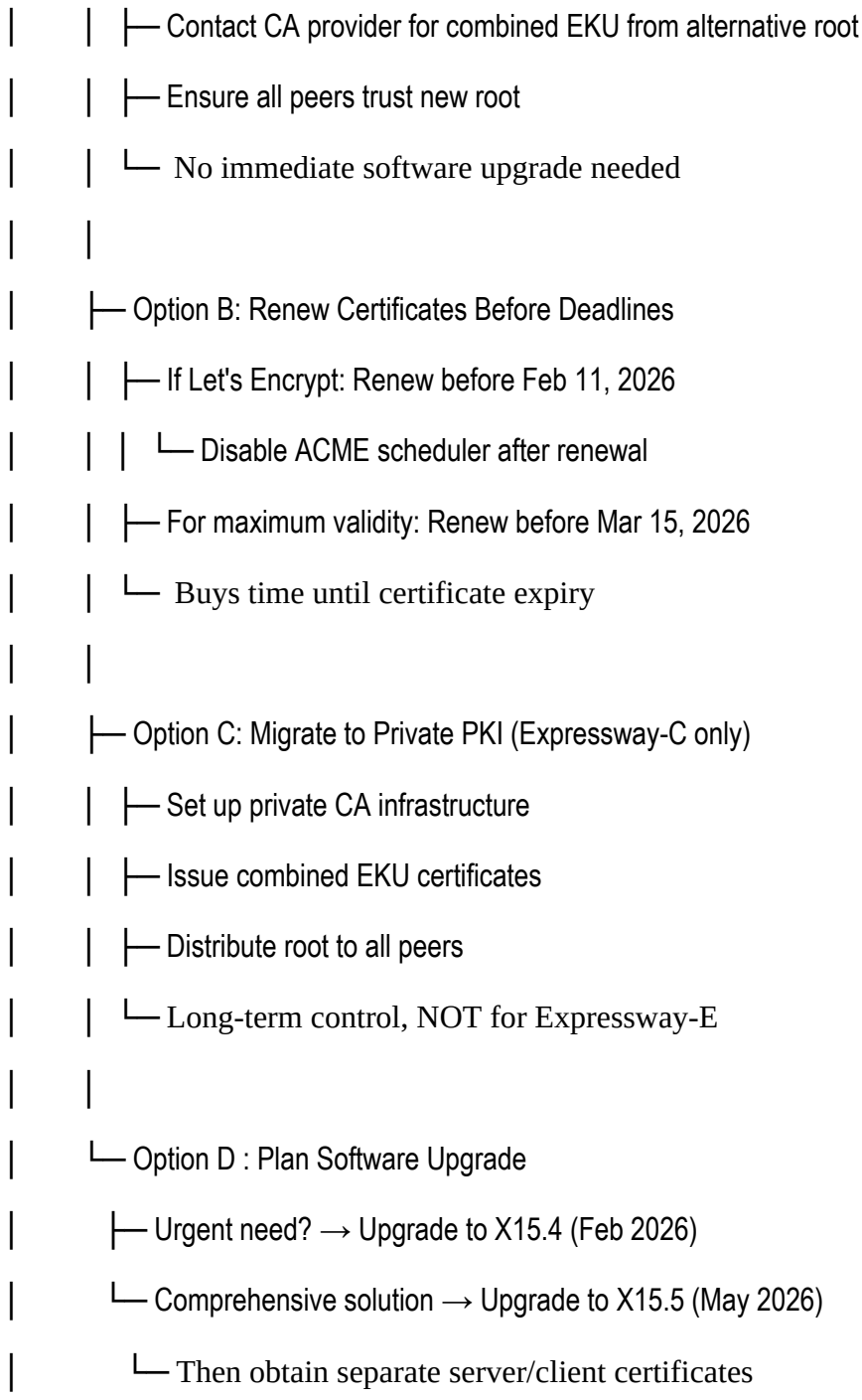
Note: In this case, the remote peer also has to support a similar Ignore Client Authentication EKU model

---

Decision Tree

START: Do you use Public CA certificates on Expressway?





Frequently Asked Questions (FAQ)

General Questions

Q: Do I need to worry about this if I use private PKI?

A: No. This policy only affects certificates issued by Public Root CAs. Private PKI and self-signed certificates are not impacted.

Q: What if I do not use mTLS connections?

A: If you only use standard TLS (server authentication), you are not affected by this policy. Your server-

only certificates continue to work. However, verify your use cases against the list in Specific Affected Use Cases section as some of use cases default uses mTLS.

Q: Will my standard HTTPS web connections to Expressway stop working?

A: No. Standard TLS connections are not affected. Web browser access to Expressway continues to work normally even with server-only EKU certificates.

Q: Can I continue using my existing certificates?

A: Yes, existing certificates with combined EKU remain valid until they expire. The issue arises when you need to renew. They work for both TLS and mTLS connections until expiry.

Q: How do I know if I am using mTLS or standard TLS?

A: Review***Specific Affected Use Cases***section.

Q. What can I do right now?

A: Cisco strongly recommends these immediate actions:

- **Audit your certificates**

  Identify public TLS certificates used for mTLS

- **Renew certificates early**

  Renew before **March 15, 2026** to maximize validity

- **Control ACME automation**

  Disable automated renewals that can replace certificates unexpectedly

- **Coordinate with your CA**

  Some CAs offer temporary or alternative certificate profiles

Q: Is CUCM SU3(a) compatible with X15.4 and X15.5

A: Yes

Q: Is there a security vulnerability with disabling Client EKU check in Cisco Expressway E (with X15.5 release)

A: Certificate still check CN/SAN to verify connection source is valid, only bypass EKU validation (certificate for client role purpose) which was included by default till Google raise security concern, therefore must not have security issue compare to before.

Let's Encrypt Specific

Q: I use Let's Encrypt with ACME on Expressway. What can I do?

A:

1. Renew your certificate before February 11, 2026 (as close to that date as possible)
2. Disable the ACME automated scheduler immediately after renewal

3. Plan to upgrade to X15.5 for long-term solution

Q: Can I modify the ACME profile to continue getting combined EKU certificates?

A: No. Currently, Expressway uses a hardcoded "classic" ACME profile that cannot be modified by users, please contact Cisco TAC for ACME certificate profile support.

Upgrade Questions

Q: Do I need to upgrade both Expressway-E and Expressway-C?

A: Yes, absolutely. Both must be upgraded to the same version (X15.4 or X15.5) for proper operation.

Q: can I upgrade to X15.4 or wait for X15.5?

A:

- Upgrade to X15.4 if you have urgent issues or need to accept server-only certificates now
- If possible, wait for X15.5 (May 2026) for the comprehensive solution with dual-certificate support

Q: My cluster replication is broken after certificate renewal. What happened?

A: Most likely your new certificate only has Server Authentication EKU, but:

- If on version before X15.4 with TLS Verify = Enforcing: Cluster peers cannot establish mTLS connections without Client Authentication EKU
- Solution options (Either one):

  Set TLS verification mode to "Permissive" (less secure)

  Obtain certificates with combined EKU from alternative CA root

  Upgrade to X15.4 or later, which bypasses Client Auth EKU verification for ClusterDB

Q: After upgrading to X15.4, can I use Enforcing mode with server-only certificates in my cluster?

A: **Yes.** Starting from X15.4, Expressway bypasses Client Auth EKU verification for mTLS ClusterDB connections. Therefore, TLS Verify can be set to "Enforcing" even if one or more cluster nodes only have Server Auth EKU.

Q: Why can't I upload my certificate through the Expressway Web GUI?

A: **Before X15.4**, the Web GUI enforces a hardcoded validation that requires certificates to have Client Authentication EKU. If your certificate only has Server Authentication EKU, you have two options:

- Use SCP (Secure Copy Protocol) to upload the certificate directly to the server (/persistent/Certs folder)
- Upgrade to X15.4 or later (Expressway-E only), which removes this restriction

Q: After upgrading to X15.4, I still cannot upload server-only certificates to Expressway-E

A: Once upgraded, ensure that this command is enabled

xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload: On

Q: I upgraded to X15.4. Can I now upload server-only certificates on both Expressway-E and Expressway-C?

A: **No. X15.4 only removes the upload restriction for Expressway-E.** Expressway-C still requires combined EKU certificates for upload via Web GUI. This is because Expressway-C frequently acts as a TLS client in UC Traversal Zones and requires Client Authentication EKU. Ensure that you run this command on Expressway-E. This command does not run on Expressway-C

xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload: On

Q: I can not register Smart License after certificate renewal. Why?

A: Smart Licensing failure after certificate renewal is usually NOT related to EKU:

- Check if Expressway can reach tools.cisco.com (CSSM)
- Verify firewall rules allow HTTPS outbound (port 443)
- Check if proxy configuration is correct (if using HTTP proxy)
- Verify CSSM server certificate is trusted in the Expressway trust store
- Smart Licensing does not require clientAuth, so this policy change does nott affect it

MRA (Mobile and Remote Access) Specific

Q: Does MRA require Client Authentication EKU on Expressway-E?

A: **It depends on the Expressway version:**

- Before X15.4: Yes, indirectly required

  During MRA SIP signaling, Expressway-E sends its signed certificate in a SIP SERVICE message to Expressway-C

  Expressway-C validates the certificate, requiring both Client Authentication and Server Authentication EKUs

  Without combined EKU, MRA SIP registration fails

- X15.4 and later: No

  Expressway-C no longer validates Client Authentication EKU in the SIP SERVICE message

  Expressway-E only needs Server Authentication EKU for MRA

  UC Traversal Zone operates unidirectionally (Expressway-C validates Expressway-E server certificate only)

Q: Why my Neighbor Zones are failing after uploading theServer Authentication EKU on Expresswayx15.4

A: If you set the TLS verification mode to “on”, it requires to have a client authentication EKU. So You can disable TLS verification in the Neighbor Zone configuration

Q: What certificates are needed for MRA to work properly?

A: For a typical MRA deployment:

Component	Certificate Requirements	EKU Required	Notes
Expressway-E (before X15.4)	serverAuth + clientAuth	Both	For SIP SERVICE validation by Exp-C
Expressway-E (X15.4+)	serverAuth only	Server only	Client EKU check bypassed
Expressway-C	clientAuth + serverAuth	Both	Always acts as client in UC Traversal
UC Traversal Zone	Unidirectional validation	Exp-E: serverAuth Exp-C: clientAuth	Exp-C validates Exp-E server cert

Q: My MRA was working fine, but after renewing my Expressway-E certificate with server-only EKU, SIP registration fails. What is wrong?

A: **If you are running a version before X15.4**, MRA SIP signaling requires Expressway-E to present both Server and Client Authentication EKUs in the SIP SERVICE message. Your options:

- Obtain a certificate with combined EKU
- Switch to an alternative CA root that issues combined EKU
- Upgrade both Expressway-E and Expressway-C to X15.4 or later (recommended)

Certificate Management

Q: How do I get a certificate with combined EKU from DigiCert or IdenTrust?

A: Contact your CA provider and request a certificate from their alternative root that still issues combined EKU.

Q: My CA says they can only provide server-only certificates. What can I do?

A: You have several options:

- Check for alternative roots: Ask your CA if they have alternative roots that issue combined EKU (like DigiCert Assured ID or IdenTrust Public Sector)
- Switch CA providers: Look for CAs offering combined EKU from non-Chrome-trusted roots
- Use private PKI: Set up internal CA for combined EKU certificates (Expressway-C deployments only)
- Upgrade to X15.4: Intermittent solution to accommodate certificates with ServerAuth EKU only and to enable MRA registrations
- Upgrade to X15.5 once available: Plan for dual-certificate architecture where server-only certs are acceptable and Comprehensive solution to meet global Google Chrome Root Program requirements

Timeline Questions

Q: What happens on June 15, 2026?

A: Chrome stops trusting public TLS certificates containing both Server and Client Authentication EKUs. Services using such certificates can fail.

Q: Why do I have to I renew before March 15, 2026?

A: After March 15, 2026, certificate validity is reduced from 398 days to 200 days. Renewing before this date gives you maximum certificate lifetime.

Q: What is the deadline for action?

A: There are multiple deadlines:

- February 11, 2026: Let's Encrypt stops combined EKU via classic ACME
- March 15, 2026: Certificate validity reduced to 200 days
- May 2026: Most public CAs stop issuing combined EKU entirely
- June 2026: Chrome policy fully enforced

Additional Resources

Cisco Documentation

- Field Notice FN74362: Cisco Expressway Impact on Secure Communication due to Upcoming Changes to TLS Certificates
- Cisco bug ID CSCwr73373: Support for separate server and client Certificate for Expressway

External References

- Chrome Root Program Policy
- Let's Encrypt: Ending TLS Client Authentication Certificate Support in 2026
- CA/Browser Forum Baseline Requirements

Certificate Authority Resources

- DigiCert Support Portal
- IdenTrust Certificate Services
- Let's Encrypt Community Forum
- Sectigo Knowledge Base

Conclusion

The sunsetting of Client Authentication EKU in public CA certificates represent a significant security policy shift that impacts Cisco Expressway deployments using mTLS connections. While this is an industry-wide change, the impact rating is CRITICAL per Field Notice FN74362, and immediate action is required to prevent service disruptions.

Key Takeaways

- This affects ALL Expressway versions (X14 and X15 before X15.4)
- Audit your certificates NOW - This is the mandatory first step
- Multiple workarounds are available - Choose the best fit for your environment
- Software upgrades are required for long-term solution - Plan for X15.5
- Both Expressway-E and Expressway-C must be upgraded together
- Let's Encrypt users have the earliest deadline - February 11, 2026