Cisco Expressway and Cisco Expressway Select Release Note for X15.5.x release

(Includes X15.5, X15.5.1, X15.5.2, X15.5.3, X15.5.20, and X15.5.21 releases)

Published Date: 2026-10-26

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

About the Documentation 5
Change History 5
Supported Platforms 5
New Hypervisor Support for On-premises Calling Solutions 7
Supported virtualization environments 7
About the Hypervisors 8
VMware vSphere ESXi 8
Cisco NFVIS-for-UC (Network Function Virtualization Infrastructure Software-for-Unified Communications) 8
Nutanix AHV 9
Reference guides 9
Change Notices 9
Smart Licensing – Unrestricted Distribution (Capped Version) 9
Signaling to no more than 2500 sessions 9
Smart Licensing Export Compliance – Restricted Distribution (Uncapped Version) 10
Upgrade Approach 10
Interoperability and Compatibility 10
Product Compatibility Information 10
Detailed matrices 10
Mobile and Remote Access (MRA) 11
Which Expressway Services Can Run Together? 11
Summary of Features and Bugs Fixed 11
X15.5.21 release 11
Bug Fixed 11
X15.5.20 release 11
Bug Fixed 11
X15.5.3 release 12
Bugs Fixed 12
X15.5.2 release 13
Feature Enhancements 13
Bugs Fixed 13
X15.5.1 release 14
Feature Enhancements 14
Bugs Fixed 14

© 2026 Cisco and/or its affiliates. All rights reserved.

X15.5 release 15
Feature Enhancements 15
Bugs Fixed 15
Withdrawn or Deprecated Features and Software 16
Product Bulletin(s) 17
..... 17
No Support for Ray Baum's Act 17
Related Documentation 17
Features and Changes 19
X15.5.21 release 19
Security Management 19
X15.5.20 release 19
System Management 19
Feature Enhancement 19
Security Management 20
X15.5.3 release 22
Security Management 22
Issues Resolved 22
System Management 22
Issues Resolved 22
..... 24
X15.5.2 release 24
System Management 24
Feature Enhancements 24
Issues Resolved 24
X15.5.1 release 25
Security Enhancement 25
Feature Enhancements 25
System Management 25
Issues Resolved 26
X15.5 release 28
System Management 28
Feature Enhancements 28
Preview Features 29
REST API Changes 29

© 2026 Cisco and/or its affiliates. All rights reserved.

Software Downloads Folder Path 30
Smart Licensing Export Compliance for Cisco Expressway Select – 30
Restricted Distribution (Uncapped Version) 30
Open and Resolved Issues 31
Using the Bug Search Tool 31
Appendix 1: Ordering Information 33
PID Details 33
Ordering Guide 33
Appendix 2: Accessibility and Compatibility Features 35
Appendix 3: Upgrade Path 36

© 2026 Cisco and/or its affiliates. All rights reserved.

About the Documentation

- To find out what's new and changed for this release, refer to the Features and Changes.
- For information on the documentation that is available for this release, refer to Related Documentation.

Change History

Date	Change	Reason
October 2026	First publication for Cisco Expressway and Cisco Expressway Select - X15.5.21 release	X15.5.21 release
October 2026	First publication for Cisco Expressway and Cisco Expressway Select - X15.5.20 release	X15.5.20 release
September 2026	First publication for Cisco Expressway and Cisco Expressway Select - X15.5.3 release	X15.5.3 release
July 2026	First publication for Cisco Expressway and Cisco Expressway Select - X15.5.2 release	X15.5.2 release
June 2026	First publication for Cisco Expressway and Cisco Expressway Select - X15.5.1 release.	X15.5.1 release
April 2026	Updated “Summary of Features and Bugs Fixed” section with “External Manager interface must be over HTTP”.	Republished X15.5.x release
April 2026	First publication for Cisco Expressway and Cisco Expressway Select - X15.5.x release.	X15.5.x release

Supported Platforms

Platform Name	Serial Number	Scope of Software Version Support
Virtual Machine - Small Scale Deployment	(Auto-generated)	Supported (X8.1 onwards)

© 2026 Cisco and/or its affiliates. All rights reserved.

Platform Name	Serial Number	Scope of Software Version Support
Virtual Machine – Medium Scale Deployment	(Auto-generated)	Supported (X8.1 onwards)
Virtual Machine – Large Scale Deployment	(Auto-generated)	Supported (X8.1 onwards)
CE1300 Hardware Revision 2 **(5th gen: Cisco Expressway pre-installed on UCS C220 M6S)**	WZP#########	X15.2.2 onwards End-of-Sale and End-of-Life Announcement: Link **Note:** Downgrade to x15.2.1 version is not supported. TAC to engage BU via BEMS if any Customer wants to downgrade to an earlier released version.
CE1300 Hardware **(5th gen: Cisco Expressway pre-installed on UCS C220 M6S)**	52E5####	X14.3.1 onwards
Note: This is applicable only for CE1300 End-of-Sale and End-of-Life Announcement: Link		
CE1200 Hardware Revision 2 **(4th gen: Cisco Expressway pre-installed on UCS C220 M5L)**	52E1####	Supported (X12.5.5, X14.3.1 (X14.3.x), X15.0.x, X15.2.x, X15.3.x, X15.4.x, and X15.5.x)
CE1200 Hardware Revision 1 **(4th gen: Cisco Expressway pre-installed on UCS C220 M5L)**	52E0####	Supported (X8.11.1, X12.5.5, X14.3.1 (X14.3.x), X15.0.x, X15.2.x, X15.3.x, X15.4.x, and X15.5.x)
Note: This is applicable only for CE1200 The last date of support (Hardware) is October 31, 2028. End-of-Sale and End-of-Life Announcement: Link		
Note: This applies to appliances that have reached the end of life and the end of support. For Hardware that has reached the end of support, there is no support for either Hardware or Software issues (including Hardware-embedded Software such as BIOS, firmware, and drivers).		

© 2026 Cisco and/or its affiliates. All rights reserved.

New Hypervisor Support for On-premises Calling Solutions

The Cisco Expressway X15.4 release introduced support for additional virtualization options. In addition to VMware vSphere ESXi, X15.4 supports Cisco NFVIS-for-UC and Cisco Compute Hyperconverged with Nutanix (CCHN) for on-premises calling deployments. These additions allow on-premises customers to choose between traditional VMware support, a Cisco-native virtualization layer for appliances, or a robust hyperconverged infrastructure (HCI) solution.

Supported virtualization environments

Hypervisor	Expressway X15.4 requirements
VMware vSphere ESXi	Supported on Cisco or third-party hardware. The listed minimum versions are ESXi 7.0 Update 3 and 8.0 Update 1.
Cisco NFVIS-for-UC	Requires NFVIS-for-UC 4.18 (minimum 4.18.2a) and supported Cisco Calling Appliances.
Nutanix AHV	Requires CCHN hardware, AHV 10.0, AOS 7.0, and PrismCentral 2024.3. Nutanix on other hardware is not supported for this deployment

Note: Cisco NFVIS-for-UC is a special edition of NFVIS that introduces a new commercial offer with a separate product ID, distinct pricing, new licensing, and slightly different administrative User Interface.

- Cisco NFVIS-for-UC supports only select On-premises Calling Applications.
- Cisco NFVIS-for-UC supports only select Cisco Calling Appliances

Hypervisor	Scope of Version Support	Supported Hardware
Cisco NFVIS-for-UC	NFVIS 4.18 (minimum 4.18.2a)	PID CE1400V-M7-K9 For more information, see the "Virtualization Requirements" section in "Cisco Expressway Install and Upgrade Guide" and "Cisco Virtualization Guide for Cisco On-premises Calling Applications."
The following PIDs are supported.		
	BE7M-M7-K9	**BE7H-M7-K9**	**BE7M-M6-K9**	**BE7M-M6-K9**
	BE6K-M7-K9	**BE6K-M6-K9**	**BE6M-M5-K9**	**BE6H-M5-K9**
Nutanix AHV	• Nutanix AHV version 10.0 with AOS version 7.0 • PrismCentral version 2024.3	Cisco HCI Infrastructure, which supports Nutanix.

© 2026 Cisco and/or its affiliates. All rights reserved.

The compatibility table lists the minimum versions for X15.4. Support can vary by Expressway release and subsequent maintenance updates; see Cisco Expressway Install and Upgrade Guide before installing or upgrading.

About the Hypervisors

VMware vSphere ESXi

VMware ESXi (formerly named ESXi, now renamed back to ESX in version 9.0) is an enterprise-class, type-1 hypervisor developed by VMware and Broadcom. As a Type 1 hypervisor, ESXi runs directly on bare-metal hardware without requiring a host operating system, providing direct access to hardware resources for enhanced performance and efficiency.

Cisco on-premises applications are supported on VMware vSphere ESXi running on a broad spectrum of Cisco Calling Appliances, Cisco General-purpose Compute/Storage, and third-party General-purpose Compute/Storage.

The following are the ESXi-supported versions.

The X15.0 and later releases support ESXi 7.0 Update 1, ESXi 8.0 Update 1, and subsequent maintenance versions.

Note:

- VMware withdrew the following supported versions: ESXi 7.0 Update 3, 3a, and 3b due to critical issues identified with those builds.
- The End of General Support for ESXi 7.0 ended on October 2025.
- The End of General Support for ESXi 8.0 will be in October 2027.

For more information on ESXi support for older Cisco on-premises calling application releases (X14 and earlier), see Cisco Collaboration Virtualization.

For the latest Cisco Expressway compatibility and supported ESXi versions and hypervisor requirements, see the "Virtualization Requirements" section in the Cisco Expressway Install and Upgrade Guide for X15.4.

Cisco NFVIS-for-UC (Network Function Virtualization Infrastructure Software-for-Unified Communications)

Cisco NFVIS (Network Function Virtualization Infrastructure Software) is a hypervisor product from Cisco's Enterprise Network Function Virtualization (Enterprise NFV) portfolio. It is a special-purpose Linux/KVM-based virtualization layer for deploying select application workloads on select Cisco hardware.

For more information on the base Cisco NFVIS from Cisco Enterprise NFV, see the following:

- Optimize the virtualization layer
- Cisco Enterprise NFV Infrastructure Software

© 2026 Cisco and/or its affiliates. All rights reserved.

For more information on Cisco On-premises Calling Applications support on Cisco NFVIS-for-UC, see Virtualization Requirements for Cisco NFVIS-for-UC in Cisco Virtualization Guide for Cisco On-premises Calling Applications.

Nutanix AHV

Nutanix is a hyperconverged infrastructure (HCI) platform that integrates compute, storage, and networking into a single, software-defined system, providing a robust foundation for hybrid cloud deployments.

Acropolis Hypervisor (AHV) is a hypervisor from Nutanix that runs alongside Acropolis OS (AOS) hyperconvergence software and PrismCentral (PC), a web-based, centralized management software. These products are all part of Nutanix Cloud Infrastructure (NCI) or Nutanix Cloud Platform (NCP) portfolios.

Cisco Compute Hyperconverged with Nutanix (CCHN) is a joint solution that runs Nutanix software on Cisco hardware, with joint support from both companies.

Cisco on-premises applications are supported on Nutanix AHV, AOS, and PC with CCHN hardware.

For more information on Nutanix software, see the Nutanix Home page.

For more information on CCHN hardware, see Cisco Compute Hyperconverged with Nutanix

For more information on Cisco on-premises calling applications support on Cisco Compute Hyperconverged with Nutanix, see Virtualization Requirements for Nutanix AHV in Cisco Virtualization Guide for Cisco On-premises Calling Applications.

Reference guides

- **Installation Guide:** Cisco Expressway Install and Upgrade Guide
- **Virtualization Guide:** See Cisco Virtualization Guide for Cisco On-premises Calling Applications
- **Collaboration Installation Guides:**
  - Cisco Unified Communications Manager and the IM and Presence Service
  - Cisco Emergency Responder Administration Guide

Change Notices

Smart Licensing – Unrestricted Distribution (Capped Version)

Signaling to no more than 2500 sessions

Cisco Expressway is a media gateway and must provide media encryption or encrypted signaling for up to 2500 sessions. This restriction became effective from the X14.2 release of the Cisco Expressway.

Encrypted signaling to endpoints/sessions refers to SIP registrations or calls, H.323 registrations or calls, WebRTC calls, and XMPP registrations.

For example, a Jabber client registering over MRA will use two sessions if it uses both SIP and XMPP. Cisco Expressway can support only 1250 Jabber client registrations.

© 2026 Cisco and/or its affiliates. All rights reserved.

Important:

- Ensure that the limited number of encrypted signaling sessions per Cisco Expressway instance is not more than 2500. If a customer needs to exceed this limit, they may deploy additional peers/clusters to provide extra capacity.
- CCO does not perform a “license determination check.” So, existing customers will only have access to the limited/capped version.

Smart Licensing Export Compliance – Restricted Distribution (Uncapped Version)

The **Cisco Expressway Select** is an export-restricted image that supports more than 2500 encrypted signaling sessions.

Cisco is committed to strict compliance with all global export laws and regulations.

Every software release must comply with all relevant Export Control legislation - the US and local country regulations that control the conditions under which certain software and technology may be exported or transferred to other countries and parties.

There is no encrypted session limit/capping on the number of registrations/calls/sessions (hardware limit still applies). For more information, see the Cisco Expressway Administrator Guide.

Important: CCO does not perform a “license determination check.” So existing customers will only have access to the Export Unrestricted image. Users must order a special $0 Product Identifier (PID) for the Cisco Expressway Select [1] (see Appendix 1: Ordering Information).

Upgrade Approach

The following upgrades are allowed. This applies to all X14.3.x and later releases.

- Cisco Expressway –→ Cisco Expressway Select

Or

- Cisco Expressway Select –→ Cisco Expressway

For more information, see Appendix 3: Upgrade Path.

Interoperability and Compatibility

Product Compatibility Information

Detailed matrices

Cisco Expressway is standards-based and interoperates with SIP and H.323 equipment from Cisco and third parties. For specific device interoperability questions, contact your Cisco representative.

[1] Export-restricted image exceeding 2500 encrypted signaling sessions.

© 2026 Cisco and/or its affiliates. All rights reserved.

Mobile and Remote Access (MRA)

The Mobile and Remote Access Through Cisco Expressway Deployment Guide provides information on compatible MRA products, including the “Version tables for endpoints and infrastructure products.”

For MRA to access the latest features and functionality, it's recommended that Cisco Expressway be deployed in conjunction with the latest version of Unified CM. However, Cisco Expressway is also backward compatible with earlier Unified CM releases. For more information, see the Cisco Collaboration Systems Release Compatibility Matrix.

Which Expressway Services Can Run Together?

The Cisco Expressway Administrator Guide details which Expressway services can coexist on the same Expressway system or cluster. See the “Services That Can be Hosted Together” table in the **Introduction** chapter. For example, the table indicates whether MRA can coexist with CMR Cloud (it can).

Summary of Features and Bugs Fixed

X15.5.21 release

Bug Fixed

Bug Fixed	Status
Security Management	
PHP2shell Vulnerabilities Affecting Cisco Expressway: October 2026	Fixed in X15.5.21

X15.5.20 release

Bug Fixed

Bug Fixed	Status
System Management	
During an HTTP tunnel abort, ATS passes a null buffer, which is dereferenced and causes a SIGSEGV. The fix was to handle the null pointer gracefully instead of crashing	Fixed in X15.5.20

© 2026 Cisco and/or its affiliates. All rights reserved.

X15.5.3 release

Bugs Fixed

Bugs Fixed	Status
Security Management	
Improved web UI security to help prevent cross-site scripting (XSS) vulnerabilities.	Fixed in X15.5.3
ACME certificate renewals now preserve the SSL configuration and prevent traffic server crashes.	
Improved SIP message framing by handling oversized Content-Length values consistently on Expressway TCP and TLS listeners.	
System Management	
Upgrades to X15.5.1 now preserve configured IP exemptions so trusted addresses remain excluded from automated intrusion protection.	Fixed in X15.5.3
Expressway now reports cluster status more reliably, reducing intermittent “Connection unexpectedly lost” alarms in the web interface.	
Expressway X15.5 now lets administrators delete External Manager configurations successfully.	
Improved Mobile and Remote Access call reliability by preventing unintended B2BUA engagement on Expressway-E.	
Improved Expressway recovery after an FSM watchdog event to help maintain port forwarding and MRA availability.	
Cisco Expressway now raises alarms for application failures, helping administrators identify issues quickly and maintain service reliability.	

© 2026 Cisco and/or its affiliates. All rights reserved.

X15.5.2 release

Feature Enhancements

Feature Enhancements	Status
System Enhancement	
Expressway now uses centralized cipher definitions, improving consistency and simplifying future cryptographic updates.	Supported from X15.5.2
Expressway now provides streamlined reset processing and no longer retains an unnecessary CA private key in persistent certificate storage.	

Bugs Fixed

Bugs Fixed	Status
System Management	
Expressway now handles transient fail2ban status responses without raising false alarm 40041.	Fixed in X15.5.2
Expressway now uses trusted server information for web redirects, improving protection against manipulated requests.	
tshell now remains available when routing status data is temporarily incomplete.	
Expressway-C now reliably releases UDP media ports after BiB-recorded MRA calls, helping prevent resource exhaustion and call failures.	
Expressway CLI now provides clear, actionable guidance for domain certificate and CSR operations.	
Users can now confirm and complete CPL file uploads without losing the selected file.	
BiB call recording over MRA now completes reliably when SIP signaling is load balanced across Expressway-C peers.	

© 2026 Cisco and/or its affiliates. All rights reserved.

X15.5.1 release

Feature Enhancements

Feature Enhancements	Status
Security Enhancement	
Improved security for system backup decryption.	Supported from X15.5.1
System Enhancement	
REST APIs added for EKU-related enhancements.	Supported from X15.5.1
Updated cipher suites for primary cryptographic requirements.	
New CLI Toggle to Enable or Disable the Client EKU (Extended Key Usage) Check for XMPP Federation.	

Bugs Fixed

Bugs Fixed	Status
System Management	
CE1300 Expressway Loses Configuration and Reverts to 'Cisco Expressway/VCS Base' after upgrading to X15.4.	Fixed in X15.5.1
Unable to access CMS Web App over WebRTC after upgrading to X15.	
Expressway HTTPS connection to external management server fails.	
Handled missing Contact header in REGISTER during maintenance mode.	
Updated Certificate Guidance for Let's Encrypt ACME.	

© 2026 Cisco and/or its affiliates. All rights reserved.

X15.5 release

Feature Enhancements

Feature Enhancements	Status
Security Enhancement	
A new option is added to disable Client EKU validation, giving you more flexibility and preventing service interruptions.	Supported from X15.5
TLS Server Certificates is updated by removing the Client Authentication EKU to better align with modern security standards.	

Bugs Fixed

Bugs Fixed	Status
System Management	
Memory issue in Smart Licensing is fixed to ensure the system stays stable and avoids crashes.	Fixed in X15.5
Optimized the management framework to prevent memory buildup and keep the system running fast.	
The "Filter" button in Call History is now fully functional, making it easy to find the records you need.	
Stabilized load balancing across Expressway-C nodes to ensure a smooth and reliable connection for all users.	
Unable to add IMP server node on Expressway-C with version X15.4.	
Unable to Delete IMP server node from web UI with version X15.4.	
Streamlined the local authentication database so that password updates are reflected accurately without creating duplicates.	
Upgrading from X15.2.2 to X15.3 now reliably preserves your settings, ensuring a smooth transition without a factory reset.	

© 2026 Cisco and/or its affiliates. All rights reserved.

Bugs Fixed	Status
Communication over External Manager interface is only supported over HTTP. It is not supported over HTTPS.	
Enhanced cluster stability by fixing a communication error, ensuring all six nodes work together securely and reliably.	

Withdrawn or Deprecated Features and Software

The Cisco Expressway product set is under continuous review. Features are sometimes withdrawn from the product or deprecated to indicate that support will be withdrawn in a subsequent release.

Feature / Software	Status
Jabber Guest Services	Deprecated from X15.3
SHA1 Signed Certificate deprecation in the Cisco Expressway	Deprecated from X15.2
Support for the Microsoft Lync Server	Withdrawn For more information, follow the link.
Hardware Security Module (HSM) Support	Withdrawn from X14.2
Support for the Microsoft Internet Explorer browser	Deprecated from X14.0.2
VMware ESXi 6.0 (VM-based deployments)	Deprecated
Cisco Jabber Video for TelePresence (Movi) **Note: This relates to Cisco Jabber Video for TelePresence (which works in conjunction with Cisco Expressway for video communication) and not to the Cisco Jabber soft client that works with Unified CM.**	Deprecated
FindMe device/location provisioning service - Cisco TelePresence FindMe/Cisco TelePresence Suite Provisioning Extension (Cisco TMSPE)	Deprecated
Cisco Expressway Starter Pack	Deprecated
Smart Call Home preview feature	Withdrawn X12.6.2
Cisco Expressway built-in forward proxy	Withdrawn X12.6.2
Cisco Advanced Media Gateway	Withdrawn X12.6
VMware ESXi 5.x (VM-based deployments)	Withdrawn X12.5

© 2026 Cisco and/or its affiliates. All rights reserved.

Product Bulletin(s)

H.323 protocol support has reached end of support. For more information, follow the link.

No Support for Ray Baum's Act

Cisco Expressway is not a Multiline Telephone System (MLTS). Customers who comply with the requirements of Ray Baum's Act should use Cisco Unified Communications Manager in conjunction with Cisco Emergency Responder.

Related Documentation

Resource	Description
Support Resources	Reference Guides about certain common Cisco Expressway configuration procedures are available on the Cisco Expressway Series List page.
Installation - Virtual Machines	Cisco Expressway Virtual Machine Installation Guide is available on the Cisco Expressway Installation Guides page.
Cisco Expressway Install and Upgrade Guide	Cisco Expressway Install and Upgrade Guide is available on the Cisco Expressway Installation Guides page.
Installation - Physical Appliances	Cisco Expressway CE1300 Appliance Installation Guide is listed on the Cisco Expressway Installation Guides page.
Basic Configuration for single-box systems	Cisco Expressway Registrar Deployment Guide is listed on the Cisco Expressway Configuration Guides page.
Basic Configuration for Paired box Systems (firewall traversal)	Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide is available on the Cisco Expressway Configuration Guides page.
Administration and Maintenance	Cisco Expressway Administrator Guide is available on the Cisco Expressway Maintain and Operate Guides page (includes Serviceability information).
Clustering	Cisco Expressway Cluster Creation and Maintenance Deployment Guide is listed on the Cisco Expressway Configuration Guides page.
Certificates	Cisco Expressway Certificate Creation and Use Deployment Guide is available on the Cisco Expressway Configuration Guides page.
Ports	Cisco Expressway IP Port Usage Configuration Guide is listed on the Cisco Expressway Configuration Guides page.

© 2026 Cisco and/or its affiliates. All rights reserved.

Resource	Description
Mobile and Remote Access	Mobile and Remote Access Through Cisco Expressway Deployment Guide is available on the Cisco Expressway Configuration Guides page.
Open Source Documentation	Open Source Documentation Cisco TelePresence Video Communication Server and Cisco Expressway Series Open Source Documentation is published on the Licensing Information page.
Cisco Meeting Server	Cisco Meeting Server with Cisco Expressway Deployment Guide is available on the Cisco Expressway Configuration Guides page. Cisco Meeting Server API Reference Guide is listed on the Cisco Meeting Server Programming Guides page. Other Cisco Meeting Server Guides are available on the Cisco Meeting Server Configuration Guides page.
Microsoft Infrastructure	Cisco Expressway with Microsoft Infrastructure Deployment Guide is available on the Cisco Expressway Configuration Guides page. Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet are listed on the Cisco Expressway Configuration Guides page.
REST API	Cisco Expressway REST API Summary Guide is available on the Cisco Expressway Configuration Guides page (high-level information only as the API is self-documented). This guide is no longer updated or published.
Multiway Conferencing	Cisco TelePresence Multiway Deployment Guide is listed on the Cisco Expressway Configuration Guides page.
Virtualization for Cisco Expressway Series	Cisco Expressway Physical Appliance Installation Guide
Cisco Collaboration Systems Release Compatibility Matrix	Compatibility Matrix
Upgrade of Video Communication Server (VCS) / Cisco Expressway for X14.x - Guide & FAQ	Guide and FAQ
Interoperability Database	Interoperability Database
Cisco Virtualization Guide for Cisco On-premises Calling Applications	Cisco Virtualization Guide for Cisco On-premises Calling Applications

© 2026 Cisco and/or its affiliates. All rights reserved.

Features and Changes

X15.5.21 release

Security Management

PHP2shell Vulnerabilities Affecting Cisco Expressway: October 2026

For more information, see bug ID CSCwx37062.

X15.5.20 release

How does X15.5.20 strengthen Cisco Expressway security?

As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Expressway Series Software engineering team conducted a comprehensive internal security review. The review led to a software hardening release that addresses multiple internally identified vulnerabilities. For more information, see Cisco Security Advisory at the following link- Cisco Expressway Series Security Hardening Release: October 2026.

System Management

Feature Enhancement
Upgrade readiness

Before you start the upgrade, verify the cluster configuration and certificate readiness on every Expressway peer. If any requirement is not met, the upgrade stops without changing the existing cluster configuration. Correct the reported issue, then retry the upgrade.

Cluster Upgrades Enforce TLS Verification

Systems attempting an upgrade must present a valid certificate containing the system FQDN in the SAN. The peer identity check will stop the upgrade if the certificate is invalid. Certificate readiness must be confirmed before the upgrade begins.

Note:

Before upgrading, switch clusters from Permissive to Enforced mode. This helps identify and resolve certificate issues ahead of time, reducing the risk of delays during the maintenance window.

Cluster peer identity format

All configured cluster members must use the same identity format:

- Identify all peers by FQDN.

Mixed configurations that use both IP addresses and FQDNs are unsupported. The X15.5.20 installer detects this configuration and blocks the upgrade before rebooting. The readiness check also fails if a

© 2026 Cisco and/or its affiliates. All rights reserved.

configured cluster has no peer configuration or an empty one. Standalone systems pass the peer-identity check.

Before retrying the upgrade, standardize peer identities so they all use FQDNs. Allow the configuration to replicate, then confirm that the cluster is healthy. Do not change the identity format during a rolling upgrade.

Security Management

TLS verification

Note:

For clustering in X15.5.20, TLS verification must be set to **Enforcing**.

Important:

Permissive mode is not supported.

Administrator action:

- The supported clustering state in X15.5.20 is TLS Verification: Enforcing.
- A legacy Permissive setting may still be visible for compatibility, but it does not bypass ClusterDB certificate trust or peer identity validation.
- Resolve certificate issues and verify cluster health in Enforcing mode before upgrading.

Match LDAP administrator groups exactly

LDAP administrator-role mapping now requires an exact match to the configured group name. A user no longer receives a role when one group name merely contains the configured group name as a substring.

Administrator impact: A deployment that relied on partial group-name matches may stop granting the expected administrator role.

Administrator action: Compare each configured Expressway administrator group with the exact group name returned by the LDAP directory.

Default credentials and first login

The shipped root account no longer has a factory-default password. A seeded default administrator credential must be reset.

Administrator impact: Update installation, factory-reset, recovery, and unattended-deployment procedures if they assume that a default password can be reused.

Administrator action: Use the supported first-login or recovery workflow to set a unique password. Update provisioning automation so it does not rely on a static factory credential.

© 2026 Cisco and/or its affiliates. All rights reserved.

Password validation and history

Empty administrator passwords are rejected. The default password-history depth is 12.

Administrator impact:

- Automation cannot create or update an administrator account with an empty password.
- A recently used password that could previously be reused may now be rejected.

Administrator action: Review password-generation and rotation automation. Ensure it can provide enough unique passwords to meet the configured history depth.

Stricter SAN and hostname validation

Certificate names that contain an embedded NUL character are rejected. If a certificate includes a Subject Alternative Name (SAN) extension, verification does not fall back to the Common Name (CN).

Administrator impact: A certificate may fail validation if it relies on the CN and includes an unrelated SAN. Matching for MRA UC client SANs also rejects overly broad or malformed values.

Administrator action: Reissue affected certificates with every required DNS name in the correct SAN type. Do not rely on CN fallback.

Restore H.323 endpoint registration after upgrading to Expressway x15.5.20

After an upgrade to Expressway x15.5.20, an authenticated H.323 endpoint that uses challenge credentials may stop registering on the default subzone. This can affect endpoints that register with multiple aliases, such as an H.323 ID and an E.164 number.

Administrator action: Assess the impact on your deployments and notify affected customers if they need to change their configuration.

Recommended fix: Map each endpoint alias

Configure a credential alias mapping for every alias the endpoint uses. For example:

xConfiguration Registration CredentialAliasMap 1 Credential: "h323"

xConfiguration Registration CredentialAliasMap 1 Pattern String: "ex90@domain.com"

xConfiguration Registration CredentialAliasMap 1 Pattern Type: Exact

xConfiguration Registration CredentialAliasMap 2 Credential: "h323"

xConfiguration Registration CredentialAliasMap 2 Pattern String: "2001"

xConfiguration Registration CredentialAliasMap 2 Pattern Type: Exact

These entries map the endpoint's H.323 ID (ex90@domain.com) and E.164 alias (2001). Add an entry for each alias used by the endpoint.

Alternative: Turn off credential alias binding

To turn off credential alias binding on the default subzone, use:

© 2026 Cisco and/or its affiliates. All rights reserved.

xconfiguration Zones LocalZone DefaultSubZone Authentication CredentialAliasBinding: "Off"

For a specific subzone, use its ID:

xConfiguration Zones LocalZone SubZones <SubZone ID> Authentication CredentialAliasBinding: Off

Note: Disabling credential alias binding may weaken your security posture.

X15.5.3 release

Security Management

Issues Resolved

Improved web UI protection against cross-site scripting vulnerabilities

Issue: The web UI has potential cross-site scripting (XSS) vulnerabilities that could allow malicious scripts to execute in a user's browser. The UI requires security hardening to reduce this risk and protect users and their data.

Resolution: This fix strengthens security controls throughout the web UI to reduce exposure to cross-site scripting (XSS) vulnerabilities.

Prevented traffic server crashes during ACME certificate renewal

Issue: During ACME certificate renewal, a race condition can leave the SSL configuration empty, causing the traffic server to crash and interrupt secure traffic.

Resolution: ACME certificate renewals now preserve the SSL configuration and prevent traffic server crashes.

Improved SIP Content-Length Handling on Expressway

Issue: An unauthenticated network attacker who can reach the Expressway SIP TCP or TLS listener on ports 5060 or 5061 can send a SIP message with a Content-Length value that overflows 32-bit arithmetic. This can cause Expressway to frame the message differently from an RFC 3261-compliant parser processing the same data stream, creating a SIP message-parsing inconsistency.

Resolution: Improved SIP message framing by handling oversized Content-Length values consistently on Expressway TCP and TLS listeners.

System Management

Issues Resolved

IP exemptions persist after upgrading to X15.5.1

Issue: During an upgrade to X15.5.1, configured IP exemptions were removed. As a result, trusted IP addresses were no longer excluded from automated intrusion protection and could be incorrectly blocked.

© 2026 Cisco and/or its affiliates. All rights reserved.

Resolution: Upgrades to X15.5.1 now preserve configured IP exemptions so trusted addresses remain excluded from automated intrusion protection.

Improved Expressway Cluster Status Reporting

Issue: In Expressway X15.5, the web interface intermittently displays cluster failure alarms, such as **"Connection unexpectedly lost,"** making it difficult for administrators to determine the actual health of the cluster.

Resolution: Expressway now reports cluster status more reliably, reducing intermittent "Connection unexpectedly lost" alarms in the web interface.

Administrators can now delete External Manager configurations

Issue: On Cisco Expressway X15.5, administrators may be unable to delete an existing External Manager configuration because the deletion operation fails. This prevents administrators from removing obsolete or incorrect External Manager settings.

Resolution: Expressway X15.5 now lets administrators delete External Manager configurations successfully.

Improved MRA call reliability on Expressway-E

Issue: Mobile and Remote Access (MRA) calls fail intermittently when the back-to-back user agent (B2BUA) is unintentionally engaged on Cisco Expressway-E.

Resolution: Improved Mobile and Remote Access call reliability by preventing unintended B2BUA engagement on Expressway-E.

Improved Expressway port forwarding recovery after FSM watchdog events

Issue: After an FSM watchdog event, Cisco Expressway can lose port-forwarding functionality and display an "Application failed" alert, disrupting Mobile and Remote Access (MRA) until the application restarts automatically.

Resolution: Improved Expressway recovery after an FSM watchdog event to help maintain port forwarding and MRA availability.

Improved application failure alarms in Cisco Expressway

Issue: Cisco Expressway does not reliably raise alarms when an application failure occurs, reducing administrator visibility and delaying troubleshooting.

Resolution: Cisco Expressway now raises alarms for application failures, helping administrators identify issues quickly and maintain service reliability.

© 2026 Cisco and/or its affiliates. All rights reserved.

X15.5.2 release

System Management

Feature Enhancements

Centralized cipher definitions for consistent security updates

Cipher-list definitions used across Expressway have been consolidated into shared constants. This improves consistency, reduces duplicated configuration, and simplifies future updates to approved cryptographic settings.

Streamlined certificate reset processing and storage

Server and client reset routines have been optimized, and an unnecessary CA private key is no longer copied to persistent certificate storage. This simplifies certificate handling and eliminates redundant key storage.

Issues Resolved

Improved handling of transient fail2ban status responses

A temporary empty response from fail2ban was incorrectly treated as a service failure, briefly raising alarm 40041 even though fail2ban remained healthy. Expressway now handles the response as a transient condition.

Strengthened validation for Expressway web redirects

A manipulated URL path and Host header could cause a redirect to use an untrusted destination. Redirects now use trusted server address and port information, with appropriate IPv4 and IPv6 handling.

Improved tshell resilience for routing status commands

The xstatus routinggraph command could terminate tshell if it read the routing XML file while the file was temporarily incomplete. The command now handles this condition without ending the administrative CLI session.

Reliable media-port cleanup for MRA call recording

Simultaneous teardown of BiB recording legs could leave calls in an incomplete state and prevent Expressway-C from releasing UDP media ports. Call cleanup now completes correctly and releases the associated resources.

© 2026 Cisco and/or its affiliates. All rights reserved.

Clearer CLI guidance for domain certificate operations

CLI help and error messages now clarify that domaincerts manages SNI domain records, while CSR and certificate lifecycle operations use the certs command with the domain parameter. Updated syntax and examples help users select the correct command.

Reliable CPL file upload confirmation

The CPL upload interface could clear the selected file before the replacement confirmation dialog was completed. The selection is now retained so users can confirm and complete the upload.

Reliable BiB recording across MRA load-balanced paths

A SIP route mismatch across Expressway-C cluster peers could leave the encryption mode undefined and cause the B2BUA to return a 500 error. Cluster-route handling has been corrected so BiB recording negotiation can complete over valid load-balanced paths.

X15.5.1 release

Security Enhancement

Feature Enhancements

Note: This release incorporates security-related improvements as part of the ongoing security enhancements. These may be behind the scenes, but a few changes affect the user interfaces or configuration.

Improved Security for System Backup Decryption

This release improves security for the **System Backup / Restore** feature.

The following changes are added:

- Strong password policy is now enforced for backup decryption.
- Rate limiting is now applied to backup/restore authentication failures using a fail2ban jail.
- New REST API endpoints were added to manage fail2ban jail handling for backup/restore authentication failures.

These changes help protect encrypted backups from brute-force attacks and improve reliability for REST-based automation.

System Management

The following are the System Management feature enhancements to improve the administrator's experience.

© 2026 Cisco and/or its affiliates. All rights reserved.

Feature Enhancements

REST APIs Added for EKU-related Enhancements

REST APIs are now available for the new EKU-related enhancements.

Key Updates

These APIs support the new certificate changes for Let's Encrypt and other CA providers.

The default setting to copy the server certificate is now **True** for both manual certificates and automatic certificates, including Let's Encrypt and other CAs.

Updated Cipher Suites for Primary Cryptographic Requirements

The cipher suites TLS_ECDHE_ECDSA_WITH_AES_128_CCM and TLS_ECDHE_ECDSA_WITH_AES_256_CCM have been removed.

This updated cipher suite configuration applies to fresh installations and to systems that use the default cipher list. The updated cipher suites will be visible after the upgrade.

New CLI Toggle to Enable or Disable the Client EKU (Extended Key Usage) Check for XMPP Federation

This release adds a CLI toggle that lets administrators turn the Client EKU check on or off during the XMPP federation mTLS handshake.

Why this change?

The CA/B Forum is removing the clientAuth EKU from publicly issued TLS certificates (effective May 2026). Without this toggle, XMPP federation mTLS connections on Expressway would fail once peers start using certificates issued under the new policy. This change keeps XMPP federation working smoothly.

Key Features & Enhancements

New CLI command:

xConfiguration XCP Federation ClientCertificateEKUCheck to control the EKU check (default: ON).

Default behavior is unchanged — the EKU check stays enabled after upgrade. Administrators only need to act if their federation peers begin presenting certificates without the clientAuth EKU.

Issues Resolved

The following are the issues found in features related to System Management. The issues are fixed to improve the administrator's experience.

CE1300 Expressway Loses Configuration and Reverts to 'Cisco Expressway/VCS Base' after upgrading to X15.4

Issue: When upgrading Expressway from X15.3.2 to X15.4, the server loses its configuration and returns to basic setup mode.

© 2026 Cisco and/or its affiliates. All rights reserved.

In X15.3.2, two nodes were successfully clustered for Expressway-E (dual NIC). After both nodes were upgraded to X15.4, the customer noticed that some settings were lost—for example, the LAN2 and cluster configurations. The Expressways also reverted to '**Cisco Expressway/VCS Base**'.

Resolution: Normalize the node serial by truncating it to valid hex digits before comparison, then match it with the CDB serial so tables restore correctly.

Unable to Access CMS Web App Over WebRTC After Upgrading to X15.5

Issue: After upgrading to X15.5, users may be unable to access the CMS Web App over WebRTC.

The issue is intermittent. It works on some X15.5 nodes but fails on others. In some cases, the same browser works at one time and fails at another.

When the issue occurs, users see a pop-up message, **“HTML processed with accessibility”**.

The issue has been reported across multiple browsers, including Chrome, Firefox, and Safari.

Resolution: Implemented a toggle to fix the header issue, allowing it to be turned ON or OFF as required during FCC.

Expressway HTTPS Connection to External Management Server Fails

Issue: Expressway could not connect to an external management server over HTTPS.

If External Manager was configured to use HTTPS and the address was reachable, the **FsmMain** process crashed within 8 seconds of every boot.

The crash happened because `httplib.cpp` passed `NULL` values for the client certificate parameters to `fsmsock_secureSocket()`. This then called `ttclib_strcpy()`, which fails when the input is `NULL`, causing a `SIGABRT` process crash.

Resolution: The issue was fixed by adding client certificate fields to the `HTTPS_params` structure, setting default certificate paths, and passing those values instead of `NULL`.

Handled Missing Contact Header in REGISTER During Maintenance Mode

Expressway now handles REGISTER messages that do not include a Contact header while the system is in **maintenance** mode.

Updated Certificate Guidance for Let’s Encrypt ACME

Let’s Encrypt now provides two versions of the **Root YR** certificate: one cross-signed by **ISRG Root X1** and one self-signed.

Users should install the **Root YR certificate that is cross-signed by ISRG Root X1** in the Expressway-E trust store. This allows Expressway to build a certificate chain that ends with **ISRG Root X1**, which is trusted by remote IP phones.

© 2026 Cisco and/or its affiliates. All rights reserved.

If the self-signed **Root YR** certificate is installed instead, Expressway may build a chain that ends with **Root YR**. Because some IP phones do not trust Root YR, MRA phone registration may fail after ACME certificate renewal.

X15.5 release

System Management

Feature Enhancements

Removal for Client EKU Authentication from TLS Server Certificates

In Expressway X15.5, Cisco has updated how security certificates are handled to comply with new Google Chrome security standards (**Announcement:** Link). Here is a simplified breakdown of what has changed:

The Main Change: Separate Certificates

Previously, a single certificate often handled both "Server" and "Client" roles. Because Google is pushing to remove "Client" information from Server certificates, Expressway X15.5 now lets you manage these two roles separately.

- **Server Certificates:** Used when other devices connect to the Expressway.
- **Client Certificates:** Used when the Expressway connects to other services (like Webex).

New Page

- **New Menu:** You will find a new "Client Certificate" page under **Maintenance → Security**.
- **Separate Storage:** Client certificates and their private keys are now stored in their own dedicated folder on the system.
- **No More Command-line:** You no longer need to use special command-line (like the one from Expressway X15.4) to upload these certificates; you can do it all through the web interface.

  xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload: Off

What Happens During an Upgrade?

- **Automatic Copy:** When you upgrade to Expressway X15.5, your existing Server certificate is automatically copied over to the new Client Certificate section so that your connection doesn't break.
- **Manual Option:** When uploading a new Server certificate, there is now a checkbox that allows you to "Copy to Client" automatically if you want to use the same certificate for both.

Important for ACME (Let's Encrypt) Users

- **The Issue:** Starting May 13, 2026, ACME will stop including "Client" data in the certificates they issue.
- **The Workaround:** Expressway X15.5 allows you to use an ACME Server certificate as a Client certificate. This works for services like Webex Edge Audio that don't strictly check for the "Client" tag.

© 2026 Cisco and/or its affiliates. All rights reserved.

- **The Recommendation:** Even though the "copy" feature works, it is best practice to eventually get a proper Client certificate from a provider that specifically supports it.

Disable Client EKU Validation for SIP Protocol

Starting with Expressway X15.5, we are adding a new setting that lets you turn OFF a specific security check for SIP TLS incoming connections.

What is changing?

Normally, when another device connects to the Expressway using a secure connection (TLS), the Expressway checks the device's certificate to make sure it has a "Client" label (known as Client EKU). By default, this check is **ON**.

The new option

You can now turn this check **OFF** if you need to. When turned OFF:

- The Expressway will stop looking for the "Client" label on certificates for incoming calls.
- It will still continue to check for the "Server" label to ensure the connection remains secure.

How to use it

You can use the following command on both Expressway-C and Expressway-E:
xconfiguration SIP TLS Certificate ExtendedKeyUsage Checking Mode: Off

Points to Remember:

- To upload a certificate to the client interface, it must include a valid "Client EKU." If you request a client certificate but your provider ignores that request and only gives you a "Server EKU," the certificate will not work.
- Some public certificate providers may not include the "Client EKU" feature in their certificates.
- We have removed the option to automatically copy a server certificate to the client interface if that certificate only contains server permissions. This ensures that certificates are used correctly for their intended purpose.

Preview Features

There are no preview features in this release.

REST API Changes

The Cisco Expressway REST API is available to simplify remote configuration by third-party systems. The plan is to add REST API access to configuration, commands, status information, and new features. The plan is to retrofit the REST API to support features added in earlier Cisco Expressway versions.

The API is self-documented using RAML, and you can access the RAML definitions at https://<ipaddress>/api/raml.

© 2026 Cisco and/or its affiliates. All rights reserved.

Configuration APIs	API Introduced in Version
NA	X15.5.21
NA	X15.5.20
NA	X15.5.3
NA	X15.5.2
Copy Server certificate as Client	X15.5.1
NA	X15.5

Software Downloads Folder Path

The software downloads folder and path apply to both Unrestricted Distribution (Capped Version) and Restricted Distribution (Uncapped Version). This change was implemented on X14.2.6 and X14.2.7 and applies to all X14.3.x and X15.x releases.

Important:

Cisco Expressway is available to download from software.cisco.com.

Path:

1. From the **Downloads Home** -> **Unified Communications** -> **Communications Gateways** -> **Expressway Series** -> **Expressway**.

   Or

   From the **Downloads Home** -> **Unified Communications** -> **Communications Gateways** -> **Expressway Series** -> **Expressway Select**.

2. Select a **Software Type** -> **Expressway Core and Edge**.

For more information, see the Cisco Expressway Administrator Guide.

Smart Licensing Export Compliance for Cisco Expressway Select – Restricted Distribution (Uncapped Version)

- Product Activation Keys (PAK) Licensing (Option Keys) was removed from the Cisco Expressway X14.2 release.
- Smart Licensing is the default and the only licensing mode for Expressway-C and Expressway-E.
- Export unrestricted images like "Expressway" are limited by default to 2500 encrypted signaling sessions.
- To exceed this limit, you need the export-restricted image "Expressway Select." To obtain this image, you must comply with export control requirements (U.S. and local regulations) and order a special $0 PID.

© 2026 Cisco and/or its affiliates. All rights reserved.

	Cisco Expressway Select	Cisco TelePresence Video Communication Server (VCS)	Notes
CAP of 2500 No secured/crypto sessions	No	**X15.x and Cisco Expressway Select X15.x are not supported in the Cisco TelePresence Video Communication Server (VCS) series. The end of the software maintenance release date was 29 December 2022. Cisco has announced end-of-sale and end-of-life dates for the Cisco TelePresence Video Communication Server (VCS) product.**	
Support Advanced Account Security (AAS) and FIPS 140-2 Cryptographic Mode	Yes		AAS and FIPS 140-2 feature(s) are enabled by default in the Cisco Expressway Select.
Smart Licensing	Yes		

For more information, see the Cisco Expressway Administrator Guide.

Open and Resolved Issues

Follow the links below to read the latest information on the open and resolved issues for this release.

- All open issues, sorted by date modified (recent first)
- Issues resolved on X15.5.21
- Issues resolved on X15.5.20
- Issues resolved on X15.5.3
- Issues resolved on X15.5.2
- Issues resolved on X15.5.1
- Issues resolved on X15.5

Using the Bug Search Tool

The Bug Search Tool contains information on open and resolved issues for this release and previous releases, including problem descriptions and available workarounds. The identifiers listed in these release notes link directly to a description of each issue.

To look for information about a specific problem mentioned in this document:

1. Using a web browser, go to the Bug Search Tool.
2. Sign in with a cisco.com username and password.
3. Enter the bug identifier in the **Search** field and click **Search**.

© 2026 Cisco and/or its affiliates. All rights reserved.

To look for information when you do not know the identifier:

1. Type the product name in the **Search** field and click **Search**.
2. From the list of bugs that appear, use the **Filter** drop-down list to filter on *Keyword*, *Modified Date*, *Severity*, *Status*, or *Technology*.

Use **the Advanced Search on the Bug Search Tool home page to search** for a specific software version. The help pages have further information on using the Bug Search Tool.

© 2026 Cisco and/or its affiliates. All rights reserved.

Appendix 1: Ordering Information

You can access additional resources for help and more information.

PID Details

- The list of PIDs in the table below applies to both Unrestricted Distribution (Capped Version) and Restricted Distribution (Uncapped Version).
- The following PIDs A-SW-EXPWY-15X-K9 and A-SW-EXPWY-15XU-K9 are found under A-FLEX-3 PID.

Product Identifier (PID)	Description	Path on CCO
A-SW-EXPWY-15X-K9	Restricted, can exceed 2500 signaling sessions	Products > Cisco Products > Unified Communications > Communications Gateways > Cisco Expressway Series > Cisco Expressway Select
A-SW-EXPWY-15XU-K9	Unrestricted has a cap of 2500 signaling sessions. This applies to new customers who want to purchase Expressway Select.	Products > Cisco Products > Unified Communications > Communications Gateways > Cisco Expressway Series > Cisco Expressway
L-EXPWY-15.X-K9=	$0 Product Identifier (PID) for Expressway Select [2] This applies to existing customers who want to upgrade to the Expressway Select image.	Products > Cisco Products > Unified Communications > Communications Gateways > Cisco Expressway Series > Cisco Expressway Select
L-EXPWY-PLR-K9=	PLR for Expressway	Products > Cisco Products > Unified Communications > Communications Gateways > Cisco Expressway Series > Cisco Expressway Select

Ordering Guide

See the Cisco Collaboration Flex Plan 3.0 (Flex 3.0) Ordering Guide for details.

[2] Restricted, can exceed 2500 signaling sessions for existing customers who need to upgrade to uncapped images.

© 2026 Cisco and/or its affiliates. All rights reserved.

- On CSSM, on the **Create Registration Token** page, the **Allow export-controlled functionality on the products registered with this token**. The check box does not apply to Expressway images.
- In Cisco Smart Software Manager (CSSM), if the registration token is revoked from the **Inventory** > **General** > **Token Actions** menu and the Expressway node is deleted from the **Product Instances** menu, the Expressway Smart Licensing registration will be automatically deregistered, and its status will change to “Deregistered.”
- Ensure that the Quantity of $0 PID equals the number of nodes.

© 2026 Cisco and/or its affiliates. All rights reserved.

Appendix 2: Accessibility and Compatibility Features

A Voluntary Product Accessibility Template (VPAT®) is a document that explains how information and communication technology (ICT) products, such as software, hardware, electronic content, and support documentation, meet (conform to) the Revised 508 Standards for IT accessibility.

See Current VPAT Documents → TelePresence for details.

© 2026 Cisco and/or its affiliates. All rights reserved.

Appendix 3: Upgrade Path

Purpose - This section guides you through the Expressway upgrade process.

Important: Before you start the upgrade, verify the cluster configuration and certificate readiness on every Expressway peer. If any requirement is not met, the upgrade stops without changing the existing cluster configuration. Correct the reported issue, then retry the upgrade.

From the Cisco Expressway X15.2 release, Expressway certificates will NOT support deprecated signature algorithms such as Signature Algorithm: sha1WithRSAEncryption or ecdsa-with-SHA1. For more information, see the Cisco Expressway Administrator Guide.

The following table lists the various upgrade paths for Cisco Expressway and Cisco Expressway Select.

Expressway Core and Edge Releases	
From X14.0 restricted to X14.3.x/X15.0.x/X15.2.x/X15.3.x/X15.4.x/X15.5.x unrestricted	
Option 1:	X14.0 restricted → $0 PID → X14.3.x/X15.0.x/X15.2.x/X15.3.x/X15.4.x/X15.5.x unrestricted
Option 2:	X14.0 restricted → $0 PID → X14.0 unrestricted → X14.3.x/X15.0.x/X15.2.x/X15.3.x/X15.4.x/X15.5.x unrestricted
From X12.x to any X15.x upgrade	
Any version of X15.x can be migrated to both restricted and unrestricted images.	
From X12.x to any X14.x or later release upgrade / From X12.x restricted to any X15.x unrestricted or later upgrade	
There is no restriction on upgrading from X12.x to X15.x. However, the customer should convert the licensing method (from the legacy PAK license method to the Smart Licensing method) before the X15.x upgrade to avoid any Smart Licensing registration/account/license issues after the upgrade.	
Two-stage upgrades	
Upgrade from X8.x to X12.x: a two-stage approach. **Path:** X8.10 → X8.11 → X12.x → X14.x -> X15.x or later versions.	
Compatibility	
1. Upgrade from any version prior to X8.11.4 - Requires an intermediate upgrade to X8.11.4. 2. You can directly upgrade from version X8.11.4 or later to X15.x. No intermediate version is required.	

© 2026 Cisco and/or its affiliates. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte, Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at http://www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **https://www.cisco.com/c/en/us/about/legal/trademarks.html**. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco and/or its affiliates. All rights reserved.