Cisco Expressway and Cisco Expressway Select Release Note for X15.3.x release

(Includes X15.3, X15.3.1, and X15.3.2 releases)

Published Date: 2026-01-07

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

Contents

About the Documentation 4
Change History 4
Supported Platforms 4
ESXi Requirements 5
Change Notices 6
Smart Licensing – Unrestricted Distribution (Capped Version) 6
Signaling to no more than 2500 sessions 6
Smart Licensing Export Compliance – Restricted Distribution (Uncapped Version) 6
Upgrade Approach 7
Interoperability and Compatibility 7
Product Compatibility Information 7
Detailed matrices 7
Mobile and Remote Access (MRA) 7
Which Expressway Services Can Run Together? 7
Summary of Features and Bugs Fixed 8
X15.3.2 release 8
X15.3.1 release 8
X15.3 release 9
Withdrawn or Deprecated Features and Software 11
No Support for Ray Baum's Act 12
Related Documentation 12
Features and Changes 13
Security Enhancement 13
X15.3.1 and X15.3.2 releases 13
X15.3 release 13
Deprecation of SHA1 Certificate 13
Enhance logging to capture the expiry date of the certificate 14
Key 3rd Party Software Package Upgrade 16
System Management Enhancement 16
X15.3.2 release 17
X15.3.1 release 17
Smart Licensing revocation on Expressway 17
Reset the CA certificates to their defaults at least once before resetting the server certificate. 17

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

X15.3 release 17
Add apache_access logs to Syslog 17
Factory support for 52 Serial number to be removed 17
Mobile Remote Access Enhancement 18
X15.3.1 and X15.3.2 releases 18
X15.3 release 18
40 second timeout delay for HTTP query to down Cisco Unified CM node 18
Preview Features 18
REST API Changes 19
Software Downloads Folder Path 19
Smart Licensing Export Compliance for Cisco Expressway Select – 19
Restricted Distribution (Uncapped Version) 19
Open and Resolved Issues 20
Using the Bug Search Tool 20
Appendix 1: Ordering Information 22
PID Details 22
Ordering Guide 22
Appendix 2: Accessibility and Compatibility Features 24
Appendix 3: Upgrade Path 25

© 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
January 2026	First publication for Cisco Expressway and Cisco Expressway Select - X15.3.2	X15.3.2 release
October 2025	First publication for Cisco Expressway and Cisco Expressway Select - X15.3.1	X15.3.1 release
August 2025	First publication for Cisco Expressway and Cisco Expressway Select - X15.3	X15.3 release

Supported Platforms

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

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

Platform Name	Serial Number	Scope of Software Version Support
CE1300: From February 26, 2025, X15.2.2 is the factory-loaded and supported release on this appliance. Prior releases are not supported. It supports the Cisco Expressway X15.2.2 and all subsequent releases. For more information, see Virtualization for Cisco Expressway. **Note:** If you want to install Cisco Expressway X14 on this appliance, please contact the Technical Assistance Centre (TAC).		
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, and X15.3.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, and X15.3.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		
CE1100 (3rd gen: Cisco Expressway pre-installed on UCS C220 M4L)	52D#####	Not Supported End-of-Sale and End-of-Life Announcement: Link
CE1000 (2nd gen: Cisco Expressway pre-installed on UCS C220 M3L)	52B#####	Not Supported End-of-Life Announcement: Link
CE500 (2nd gen: Cisco Expressway pre-installed on UCS C220 M3L)	52C#####	Not Supported End-of-Life Announcement: Link
Note: This applies to appliances that have reached the end-of-life and end-of-support. For Hardware that has reached the last day of support: There is no support for either Hardware or Software issues (which includes Hardware embedded Software like BIOS, firmware, and drivers).		

ESXi Requirements

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 later 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 is October 2025.

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

Important:

The following are the ESXi-end-of-support versions.

- ESXi 6.5 Update 2
  - ESXi 6.5 is the End of Technical Guidance.
  - The End of Technical Guidance for vSphere/EXXI 6.5 is 15-Nov-2023.
- ESXi 6.7 Update 3
  - ESXi 6.7 release is the End of Technical Guidance.
  - The End of Technical Guidance for vSphere/ESXi 6.7 is 15-Nov-2023.

There is no phone support or web support available from VMware.

There are no more bug/security fixes (so if the Application layer has a problem isolated to the ESXi driver or ESXi software, there is no fix). For more information, see Product Lifecycle Matrix.

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 to **no more than** 2500 sessions. This restriction became effective from the X14.2 release of the Cisco Expressway.

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

For example, a Jabber client registering over MRA will use up two sessions if they are using both SIP and XMPP. Cisco Expressway can only support 1250 of these Jabber client registrations.

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 can exceed 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.

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

Note: 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 is applicable for 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 standards-based SIP and H.323 equipment, both from Cisco and third parties. For specific device interoperability questions, contact your Cisco representative.

Mobile and Remote Access (MRA)

The Mobile and Remote Access Through Cisco Expressway Deployment Guide provides information about compatible products for MRA, 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 provides information on whether MRA can coexist with CMR Cloud (it can).

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

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

Summary of Features and Bugs Fixed

X15.3.2 release

Bugs Fixed	Status
System Management Enhancement	
Expressway stops sending email notifications due to an invalid TLS protocol version on the SMTP server	Fixed in X15.3.2
Calls and registrations continue to be supported even after the SLR token has expired	
During an upgrade of Expressway from version X15.2.2 to X15.3, the server does not loose its configuration and does not revert to factory-reset mode	
IP phone over MRA fails to register with Expressway when network diagnostic log(network.http.edgeconfigprovisioning) is enabled	

X15.3.1 release

Bugs Fixed	Status
System Management Enhancement	
Smart Licensing revocation on Expressway	Fixed in X15.3.1
Reset the CA certificates to their defaults at least once before resetting the server certificate	
Expressway-C is repeatedly sending 'clusterUser' requests to Unified CM, causing about a 30-second delay in the MRA user login process	
The two-node Expressway cluster appears healthy in the User Interface, but the CLI shows reversed primary and secondary roles on both nodes	
Incident reports downloaded via the web user interface are corrupted with extra HTML fields and a truncated build section, though the original crash file remains intact	

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

Bugs Fixed	Status
Enabling both IPv4 and IPv6 causes duplicate Expressway-E entries (duplicate index/fedlet) in the exported IdP metadata, leading IdPs (for example, Azure) to reject the metadata	Fixed in X15.3.1
Cluster formation fails when operating in permissive mode using the default temporary certificate	
After moving the Expressway VM to a new host, an alarm appears stating that the master or peer configuration file could not be found, and a restart is required	
Expressway-C ↔ Expressway-E SIP OPTIONS probes consistently fail due to a “Failed to decrypt with system key” decryption error	
Expressway CDR (Call Detail Records) determines audio-only calls as video	
IPV4 gateway is not reachable from the LAN interface	
Basic Authentication responses vary based on administrative credential correctness, exposing validity	
sslh-select memory leaks when TCP TURN services are enabled on the Expressway-E	

X15.3 release

Feature Enhancements	Status
System Security Enhancement	
Deprecation of the SHA1 Certificate	Supported from X15.3
Enhance logging to capture the expiry date of the certificate	
Key 3rd Party Software Package Upgrade	
System Management Enhancement	
Add apache_access logs to Syslog	Supported from X15.3
Factory support for 52 serial numbers to be removed	

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

Feature Enhancements	Status
Mobile and Remote Access Enhancement	
40 second timeout delay for HTTP query to down the Cisco Unified CM node	Supported from X15.3

Bugs Fixed	Status
An internal software error occurred related to thread termination (__pthread_kill_implementation).	Fixed in X15.3
Configuration settings are intermittently lost when upgrading Expressways from version x15.0.3 to x15.2.2.	
The Provisioning API exhibits unexpected behavior when configuring DNS server settings.	
The Smart Licensing page becomes unresponsive if the Expressway Series setting is configured as "False."	
An internal software error occurred during a request operation (do_request).	
Changing user account passwords via REST API is only successful when authorized with local administrator credentials.	
An application crash occurs when processing a malformed SIP message.	
Critical vulnerabilities exist in Apache HTTP Server version 2.4.56; an upgrade to version 2.4.59 or later is required.	
Expressway drops calls due to "Bandwidth Allocation Failure" and related link status problems.	
The HSTS (HTTP Strict Transport Security) header is missing from responses sent on port 8443, as identified by security scans.	
Traffic Server crashes with an error indicating a plugin attempted to use a deleted continuation.	

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

Bugs Fixed	Status
The Expressway/VCS OVA is incorrectly identified as "Other (32-Bit)" in the Guest OS settings within ESXi.	

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
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.

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 on the Cisco Expressway Installation Guides page.
Installation - Physical Appliances	Cisco Expressway CE1300 Appliance Installation Guide on the Cisco Expressway Installation Guides page.
Basic Configuration for single-box systems	Cisco Expressway Registrar Deployment Guide 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 on the Cisco Expressway Configuration Guides page.
Administration and Maintenance	Cisco Expressway Administrator Guide on the Cisco Expressway Maintain and Operate Guides page (includes Serviceability information).
Clustering	Cisco Expressway Cluster Creation and Maintenance Deployment Guide on the Cisco Expressway Configuration Guides page.
Certificates	Cisco Expressway Certificate Creation and Use Deployment Guide on the Cisco Expressway Configuration Guides page.
Ports	Cisco Expressway IP Port Usage Configuration Guide on the Cisco Expressway Configuration Guides page.
Mobile and Remote Access	Mobile and Remote Access Through Cisco Expressway Deployment Guide 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 on the Licensing Information page.
Cisco Meeting Server	Cisco Meeting Server with Cisco Expressway Deployment Guide on the Cisco Expressway Configuration Guides page.

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

Resource	Description
	Cisco Meeting Server API Reference Guide 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 on the Cisco Expressway Configuration Guides page. Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet on the Cisco Expressway Configuration Guides page.
Rest API	Cisco Expressway REST API Summary Guide on the Cisco Expressway Configuration Guides page (high-level information only as the API is self-documented). This guide is no longer updated and published.
Multiway Conferencing	Cisco TelePresence Multiway Deployment Guide on the Cisco Expressway Configuration Guides page.
Virtualization for Cisco Expressway Series	Virtualization for Cisco Expressway
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 Collaboration Infrastructure Requirements	Cisco Collaboration Infrastructure Requirements

Features and Changes

Security Enhancement

Note: This release incorporates several 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.

X15.3.1 and X15.3.2 releases

There are no new features or changes in these releases.

X15.3 release

Deprecation of SHA1 Certificate

SHA-1 algorithm-based certificates are no longer supported starting with version x15.2.

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

Issue: Even though the system currently allows uploading SHA-1 certificates after x15.2 is deployed, doing so can cause the Call Detail Record (CDB) to malfunction on the Expressway after a system upgrade.

Fresh Installation (x15.2.2 and later releases)

When performing a fresh installation of x15.2.2 or any later release, the system will prevent the upload of an SHA-1 certificate and will notify the failure.

Upgrade (x15.2.2 and later releases)

If you are upgrading to x15.2.2 or a later release from an older release, the upgrade process will stop immediately after the upgrade files are uploaded if an SHA-1 certificate is detected. You will receive an error, and the upgrade will not proceed.

Enhance logging to capture the expiry date of the certificate

Improved Certificate Expiration Visibility in Expressway (X15.3.0 Onwards)

Previously, on Expressway X15.2.4 and earlier releases, diagnosing issues related to expired certificates was challenging due to a lack of clear information in the user interface (WebUI) and diagnostic logs. Administrators often had to rely on packet captures for detailed investigation. This has been significantly improved in X15.3.0 and later releases.

General Improvements in X15.3.0

Starting with Expressway X15.3.0, the Expressway Web User Interface will display certificate expiration dates and diagnostic logs will provide specific details about certificate expiration. This makes it much easier to identify and troubleshoot SSL connection failures caused by expired certificates.

Adding Cluster with an Expired Certificate on Exp-C	Prior to X15.3.0 (X15.2.4 and earlier releases)	From X15.3.0 and later releases
Cisco Unified CM	**When attempting to add a Cisco Unified CM cluster with an expired certificate, the WebUI returned only generic error messages lacking specific details.**	The WebUI has been updated to explicitly show the certificate expiration date.
	Diagnostic logs lacked specific fault information, which hindered effective troubleshooting.	SSL failures resulting from certificate expiration will now be clearly visible to administrators.
		The diagnostic log will now capture the certificate expiration timestamp as displayed in the WebUI.
IMP	**The certificate expiration date is not displayed in the WebUI.**	The WebUI will present the certificate's expiration date for visibility.
	"Administrators observed an SSL failure, though no clear explanation or detailed error message is provided.	Administrators will be able to identify SSL failures, with the certificate's expiration date clearly indicated as the cause.

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

Adding Cluster with an Expired Certificate on Exp-C	Prior to X15.3.0 (X15.2.4 and earlier releases)	From X15.3.0 and later releases
	Although the diagnostic log may indicate a 'certificate expired' error, it does not specify the exact expiration date.	The diagnostic log will include the certificate expiration timestamp as displayed in the WebUI.
Unity Connection	**The certificate expiration date is not displayed in the WebUI.**	The certificate expiration date will be shown on the WebUI.
	Administrators may encounter SSL failures that lack a specific error message or identifiable cause."	SSL connection failures will be presented to administrators along with the corresponding certificate expiration date.
	Diagnostic logs report a 'certificate expired' error, but do not provide the actual expiration date.	The diagnostic log will also record the certificate expiration timestamp.
Cisco Meeting Server	**The Web user interface does not display the certificate expiration date.**	The WebUI will show the certificate expiration date and clearly indicate 'expired certificate' as the reason for the failure.
	Administrators may encounter SSL failures without any explicit error details or identifiable cause.	Administrators will encounter a TLS connection failure accompanied by the message 'expired certificate.
	Diagnostic logs report only an 'SSL handshake error' message, without providing any additional context or detailed information.	Diagnostic logs will now record both the certificate expiration date and the associated SSL handshake error
Traversal Zone	**Certificate expiration dates are not displayed in the WebUI.**	Administrators will continue to encounter the 'TLS negotiation failure' error message when attempting to save Zone settings.
	The UC/Traversal Zone reported a generic 'TLS negotiation failure' error, with no additional diagnostic details available.	Initiating the test via the 'Check Certificates' option will now display a clear warning stating that the certificate has expired.
	Selecting the 'Check Certificates' option results in a generic error message stating, 'An operation error occurred,' without further context or diagnostic information.	--
LDAP Server	**The WebUI did not alert administrators to any certificate issues when configuring LDAP via a secure port.**	When configuring LDAP settings, the WebUI will display the certificate expiration date.
	The system would only display a generic "connection failure" to the LDAP server.	Administrators will encounter a TLS connection failure error explicitly citing 'expired certificate' as the cause.

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

Adding Cluster with an Expired Certificate on Exp-C	Prior to X15.3.0 (X15.2.4 and earlier releases)	From X15.3.0 and later releases
	The diagnostic logs recorded the connection failure but did not provide information about a "certificate expired" event.	The diagnostic log will capture the certificate expiration timestamp as displayed in the WebUI.
SMTP Server	**No error warning was displayed when adding the SMTP server information for email notifications.**	While configuring email notifications, the WebUI will display the certificate expiration date.
	System records did not include the certificate expiration date.	Administrators will encounter a TLS connection failure error, accompanied by the reason 'expired certificate.'
	The diagnostic logs did not capture any errors related to the certificate.	Diagnostic logs will now include both the certificate expiration date and the corresponding SSL error.
Syslog Server	**A warning or error was not reported when adding a Syslog server.**	During Syslog configuration, the WebUI will display the certificate expiration date.
	There is no record of the certificate's expiration date.	Administrators will receive a TLS connection failure error, clearly indicating 'expired certificate' as the cause.
	Certificate expiration was not captured in diagnostic logs.	Diagnostic logs will now record both the certificate expiration date and the associated SSL error.

Key 3rd Party Software Package Upgrade

Software Version: X15.3.0 RC1

Kernel Version: 6.12.9

Cisco SSL/Open SSL version: CiscoSSL 1.1.1zb.7.3.416

NTPd version: 4.2.8p18

Apache: 2.4.62

glibc: 2.35

python: 3.11.11

php: 7.4.33

e2fs: 1.47.1 (20-May-2024)

System Management Enhancement

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

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

X15.3.2 release

There is no change in this release.

X15.3.1 release

Smart Licensing revocation on Expressway

Issue: Smart Licensing revocation cannot be enforced on Expressway. Expressway continues to show a Registration status of **Registered** and a License authorization status of **Authorized**.

Solution: Once the Expressway is successfully registered with the Smart License server, you can revoke the license by removing the associated registration token and deleting the Expressway node from the Product Instances menu.

This action will trigger the Expressway to deregister from the Smart License server automatically.

Reset the CA certificates to their defaults at least once before resetting the server certificate.

Doing so ensures the system generates the default server certificate after the reset.

X15.3 release

Add apache_access logs to Syslog

Previously, only Apache error logs were sent to the Syslog server. Starting with version X15.3.0, Apache access logs will also be sent to Syslog, tagged with "apache." For instance, this includes logs generated when enabling MRA services. Administrators who do not wish to send these Apache access logs to Syslog can filter them out using the "apache" keyword.

Factory support for 52 Serial number to be removed

Licensing and Hardware Revisions for Expressway CE1300 Series

Previously, the "52" range of numbers was used to identify hardware appliances. However, with the transition to Smart Licensing, this specific numbering range is no longer required for product licensing.

The Expressway CE1300 Series will now have two distinct hardware revisions:

- **Revision 1:** Supported from Expressway X14.3.1 onwards. This revision is identified and mapped using a "52E5####" identifier, which is tied to the Eth2 MAC address.
- **Revision 2:** Supported from Expressway X15.2.2 onwards. This revision is identified and mapped using the chassis serial number (WZP########) and the Eth2 MAC address.

Important: Downgrading to Expressway X15.2.1 is not supported. If a customer requires a downgrade to an earlier released version, contact the Technical Assistance Center (TAC).

Pre-requisites to raise BEMS case for downgrade of CE1300.

Before the TAC Engineer can raise the BEMS case, the following information must be collected from the Expressway:

- **Serial Number:** Log in to the Expressway as *root* and run the command **serialno**. Save the output from the console to a file.
- **LAN3 (eth2) MAC Address:** Log in to the Expressway as *root* and run the command **ifconfig eth2**.

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

Login Expressway as *root* and check LAN3 (eth2) MAC address, by running **ifconfig eth2** command.

For example,

```
~ # ifconfig eth2

eth2      Link encap:Ethernet  HWaddr A0:EC:F9:38:D4:48

          BROADCAST MULTICAST  MTU:1500  Metric:1

          RX packets:0 errors:0 dropped:0 overruns:0 frame:0

           TX packets:0 errors:0 dropped:0 overruns:0
carrier:0
```

Note: Ensure the information is provided as an attachment when the BEMS case is raised.

Mobile Remote Access Enhancement

The following are the Mobile Remote Access management feature enhancements to improve the administrator's experience.

X15.3.1 and X15.3.2 releases

There are no new features or changes in these releases.

X15.3 release

40 second timeout delay for HTTP query to down Cisco Unified CM node

Issue: A customer-reported defect revealed an inadequacy in the Mobile and Remote Access (MRA) solution's handling of HTTP timeout values. Specifically, Jabber was configured with a 30-second timeout, while Expressway used 40 seconds.

In Expressway X15.2.x and earlier releases, a bug existed in ATS 8.11. This bug caused HTTP requests to time out incorrectly. Instead of timing out due to failed connection attempts, they timed out after 40 seconds because of "no activity." This happened specifically when Expressway-C couldn't determine if Cisco Unified CM (CUCM) was online using ARP.

This led to Expressway-C returning a 502 error to Expressway-E and significantly delaying the Jabber login process, especially when multiple Unified CM nodes were down, as each added a 40-second delay.

Solution: The timeout issues have been resolved in the latest ATS version, with Expressway X15.3.0 upgrading to ATS 9.2.6. This new version sets the "connect attempts timeout" to 10 seconds with a maximum of 1 retry. Customers on previous versions experiencing this issue can manually apply these values using "dbxsh".

Preview Features

There are no preview features in this release.

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

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. A plan is to retrofit REST API into some 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.

Configuration APIs	API Introduced in Version
NA	X15.3.2, X15.3.1, and X15.3

Software Downloads Folder Path

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

Important:

Cisco Expressway is available in the software download folder on 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)

Note:

- Product Activation Keys (PAK) Licensing (Option Keys) are removed from the Cisco Expressway X14.2 release.
- Smart License is the default and the only licensing mode for Expressway-C and Expressway-E.

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

- Export unrestricted images like "Expressway" are default limited to 2500 encrypted signaling sessions.
- For more, you need the export-restricted image "Expressway Select." To obtain this image, you must meet the export control requirements (US and local regulations, etc.) and order a special $0 PID.

	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 FIPS140-2 Cryptographic Mode	Yes		AAS and FIPS140-2 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 about this release's open and resolved issues.

- All open issues, sorted by date modified (recent first)
- Issues resolved in X15.3.2
- Issues resolved in X15.3.1
- Issues resolved in X15.3

Using the Bug Search Tool

The Bug Search Tool contains information about open and resolved issues for this release and previous releases, including descriptions of the problems and available workarounds. The identifiers listed in these release notes will take you 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.

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

2. Sign in with a cisco.com username and password.
3. Enter the bug identifier in the **Search** field and click **Search**.

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 **Advanced Search** on the Bug Search Tool home page 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 to get help and find more information.

PID Details

Note:

- 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.

Note:

- 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 the Quantity of 0$ PID should equal 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 is to guide you through the Expressway upgrade process.

Note: 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 path(s) 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 unrestricted	
Option 1:	X14.0 restricted → 0$ PID → X14.3.x/X15.0.x/X15.2.x/X15.3.x unrestricted
Option 2:	X14.0 restricted → 0$ PID → X14.0 unrestricted → X14.3.x/X15.0.x/X15.2.x/X15.3.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 – It is a two-stage upgrade approach. **Path:** X8.10 → X8.11 → X12.x → X14.x -> X15.x or later versions.	
Compatibility	
Note: 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.