Cisco Expressway and Cisco Expressway Select Release Note for X15.0.x release

(Includes X15.0, X15.0.1, X15.0.2, and X15.0.3 releases)

Published Date: 2024-07-31

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 endpoints 6
Smart Licensing Export Compliance – Restricted Distribution (Uncapped Version) 6
Upgrade Approach (Applicable for all X14.3.x and later releases) 6
Deploying OVA with vSphere ESXi 7.0 U2 7
VCS Product Support 7
Hardware Support for CE1x00 Appliances 7
Interoperability and Compatibility 8
Product Compatibility Information 8
Which Expressway Services Can Run Together? 8
Summary of Features and Bugs Fixed 8
X15.0.3 release 8
X15.0.2 release 8
X15.0.1 release 9
X15.0 release 9
Withdrawn or Deprecated Features and Software 9
No Support for Ray Baum's Act 10
Related Documentation 10
Features and Changes 12
Security Enhancement 12
X15.0.3 release 12
X15.0.2 release 12
X15.0.1 release 13
X15.0 release 13
Management Enhancement 15
X15.0.3 release 15
X15.0.2 release 15
X15.0.1 release 15
X15.0 release 16
Mobile Remote Access Enhancement 16

X15.0.3 release 16
X15.0.2 release 16
X15.0.1 release 17
X15.0 release 17
Preview Features 17
REST API Changes 18
Other Changes in this Release 18
X15.0 release 18
Software Downloads Folder Path 19
Smart Licensing Export Compliance for Expressway Select – Restricted Distribution (Uncapped Version) 19
Limitations 20
Open and Resolved Issues 20
Notable Issue Resolved 20
X15.0.1 release 20
Notable Issue 21
Using the Bug Search Tool 21
Appendix 1: Ordering Information 22
PID Details 22
Ordering Guide 22
Appendix 2: Accessibility and Compatibility Features 23
Appendix 3: Upgrade Path 24

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
July 2024	First publication for Cisco Expressway and Cisco Expressway Select - X15.0.3	X15.0.3 release
May 2024	First publication for Cisco Expressway and Cisco Expressway Select - X15.0.2	X15.0.2 release
March 2024	First publication for Cisco Expressway and Cisco Expressway Select - X15.0.1	X15.0.1 release
December 2023	First publication for Cisco Expressway and Cisco Expressway Select - X15.0	X15.0 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 **(5th gen: Expressway pre-installed on UCS C220 M6S)**	52E5####	X14.3.1 onwards
CE1200 Hardware Revision 2 **(4th gen: pre-installed on UCS C220 M5L)**	52E1####	Supported (X12.5.5 onwards) End of Life Announcement: Link

Platform Name	Serial Number	Scope of Software Version Support
CE1200 Hardware Revision 1 **(4th gen: pre-installed on UCS C220 M5L)**	52E0####	Supported (X8.11.1 onwards) End of Life Announcement: Link
CE1100 (3rd gen: Expressway pre-installed on UCS C220 M4L)	52D#####	Not Supported End of Life Announcement: Link
CE1000 (2nd gen: Expressway pre-installed on UCS C220 M3L)	52B######	Not Supported End of Life Announcement: Link
CE500 (2nd gen: 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 the 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. (**Reference:** Link).
- The End of General Support for ESXi 7.0 is 02-Apr-2025.

Important:

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

- ESXi 6.5 Update 2
  - ESXi 6.5 release 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 VMware Product Lifecycle Matrix.

Change Notices

Smart Licensing – Unrestricted Distribution (Capped Version)

Signaling to no more than 2500 endpoints

Expressway is a media gateway and must provide media encryption or encrypted signaling to **no more than** 2500 endpoints. This restriction is effective from the X14.2 release of the Cisco Expressway.

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

Important:

- Ensure that the limited number of encrypted signaling is **not** more than 2500 endpoints per Expressway instance. If a customer needs to exceed this limit, they may deploy additional peers/clusters to provide additional 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)

Cisco Expressway Select is an export-restricted image that can exceed 2,500 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.

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 Expressway Select[1] (see Appendix 1: Ordering Information.

Upgrade Approach (Applicable for all X14.3.x and later releases)

The following upgrades are allowed.

- Expressway –→ Expressway Select
  Or
- Expressway Select –→ Expressway

For more information, see Appendix 3: Upgrade Path.

[1] Export-restricted image exceeding 2,500 encrypted signaling sessions.

Deploying OVA with vSphere ESXi 7.0 U2

Note: This is a known issue in the current release. Deploying X14.2 OVA shows “Invalid Certificate” on the vCenter 7.0 U2 version of vSphere ESXi, though it shows “Trusted Certificate” in older versions. For more information about the issue, refer to the Knowledge Article.

VCS Product Support

Cisco has announced **end-of-sale** and **end-of-life** dates for the Cisco TelePresence Video Communication Server (VCS) (1st Generation) product. Details are available at the following Link/Link.

This notice does not affect the Cisco Expressway Series product.

Hardware Support for CE1x00 Appliances

This section applies to hardware support services only.

CE1300 Appliance

X14.3.1 is the first factory-loaded and supported release on this appliance. It also supports the Cisco Expressway X14.3.1 (X14.3.x), X15.x, and all subsequent releases. For more information, see Virtualization for Cisco Expressway.

CE1200 Appliance

The Cisco Expressway X14.3.1 (X14.3.x), X.15.x, and all subsequent releases are supported on CE1200.

The last date of support (Hardware) is October 31, 2028 (as per the End-of-Life bulletin).

CE1100 Appliance - End-of-Life and Advance Notice of Hardware Service Support withdraw

The Cisco Expressway X15.x release is **not** supported on CE1100.

For more information, see the End-of-Life bulletin. This is in line with the last date of support for those customers with a valid service contract.

Although customers may run this software release on the Expressway CE1100 and benefit from security improvements/vulnerability fixes, many new features require newer, more powerful hardware. As a result, new features/functionality added in this release of the Expressway software are not supported for use on the CE1100 platform.

CE500 and CE1000 Appliances - End-of-Sale and End-of-Life Notice

The Cisco Expressway X15.x release is **not** supported on CE500 and CE1000.

Cisco no longer supports the Cisco Expressway CE500 and CE1000 appliance hardware platforms. For more details, see the End-of-Life bulletin.

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)

Information about compatible products for MRA, specifically, is provided in version tables for endpoints and infrastructure products in the Mobile and Remote Access Through Cisco Expressway Deployment Guide.

For MRA to access the latest features and functionality, it's recommended that Expressway is deployed in conjunction with the latest version of UCM. However, Expressway is backward compatible with earlier UCM releases as well.

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, if you want to know if MRA can coexist with CMR Cloud (it can), the table will tell you.

Summary of Features and Bugs Fixed

X15.0.3 release

Feature(s) / Bug(s)	Status
Bug Fixed	
Remote Unauthenticated Code Execution Vulnerability in OpenSSH Server (regreSSHion)	Supported from X15.0.3

X15.0.2 release

Feature(s) / Bug(s)	Status
Bug Fixed	
Removal of Obsolete Cipher	Supported from X15.0.2
New RAML REST APIs introduced – **1. Resource Usage** **2. Cluster Peer Status** **3. Sys Key Status**	Supported from X15.0.2

X15.0.1 release

Feature(s) / Bug(s)	Status
Bug Fixed	
taa-chkpasswd randomly consuming high CPU beyond the normal duration while interacting with LDAP for user authentication	Supported from X15.0.1

X15.0 release

Feature(s) / Bug(s)	Status
Feature Enhancements	
LDAP TLS support for different ports other than 636 or 3269	Supported from X15.0
Removal of Banned Ciphers	
Cross Site Request Forgery Protection Header	
Webex Unified CM Calling Support Auto-extend Refresh Token	
WebRTC session counter on Web User Interface for Expressway-E	
Bug Fixed	
Log rotation stops in the Expressway	Supported from X15.0

Withdrawn or Deprecated Features and Software

The 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. This table lists the features that are currently in deprecated status or have been withdrawn since X12.5.

Feature / Software	Status
Support for Microsoft Lync Server	Withdrawn For more information, see link.
Hardware Security Module (HSM) Support	Withdrawn from X14.2
Support for Microsoft Internet Explorer browser	Deprecated from X14.0.2
VMware ESXi 6.0 (VM-based deployments)	Deprecated

Feature / Software	Status
Cisco Jabber Video for TelePresence (Movi) **Note: Relates to Cisco Jabber Video for TelePresence (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 Management Suite Provisioning Extension (Cisco TMSPE)	Deprecated
Expressway Starter Pack	Deprecated
Smart Call Home preview feature	Withdrawn X12.6.2
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

No Support for Ray Baum's Act

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

Related Documentation

Resource	Description
Support Videos	Videos provided by Cisco TAC engineers about certain common Expressway configuration procedures are available on the Expressway/VCS Screencast Video List page (search for "Expressway videos").
Installation - Virtual Machines	Cisco Expressway Virtual Machine Installation Guide on the Expressway Installation Guides page.
Installation - Physical Appliances	Cisco Expressway CE1300 Appliance Installation Guide on the Expressway Installation Guides page.
Basic Configuration for single-box systems	Cisco Expressway Registrar Deployment Guide on the Expressway Configuration Guides page.
Basic Configuration for Paired box Systems **(firewall traversal)**	Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide on the Expressway Configuration Guides page.

Resource	Description
Administration and Maintenance	Cisco Expressway Administrator Guide on the Expressway Maintain and Operate Guides page (includes Serviceability information).
Clustering	Cisco Expressway Cluster Creation and Maintenance Deployment Guide on the Expressway Configuration Guides page.
Certificates	Cisco Expressway Certificate Creation and Use Deployment Guide on the Expressway Configuration Guides page.
Ports	Cisco Expressway IP Port Usage Configuration Guide on the Expressway Configuration Guides page.
Mobile and Remote Access	Mobile and Remote Access Through Cisco Expressway Deployment Guide on the Expressway Configuration Guides page.
Open Source Documentation	Open Source Documentation Cisco TelePresence Video Communication Server and Expressway Series Open Source Documentation on the Licensing Information page.
Cisco Meeting Server	Cisco Meeting Server with Cisco Expressway Deployment Guide on the Expressway Configuration Guides page. 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.
Cisco Webex Hybrid Services	Hybrid services knowledge base
Microsoft Infrastructure	Cisco Expressway with Microsoft Infrastructure Deployment Guide on the Expressway Configuration Guides page. Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet on the Expressway Configuration Guides page.
Rest API	Cisco Expressway REST API Summary Guide on the 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 Expressway Configuration Guides page.
Virtualization for Cisco Expressway Series	Virtualization for Cisco Expressway
Cisco Collaboration Systems Release Compatibility Matrix	Compatibility Matrix

Resource	Description
Upgrade of Video Communication Server (VCS) / Expressway X14.x - Guide & FAQ	Guide and FAQ
Interoperability Database	Interoperability Database
Cisco Collaboration Infrastructure Requirements	Cisco Collaboration Infrastructure Requirements

Features and Changes

Security Enhancement

Various security-related improvement(s) are applied in this release as part of ongoing security enhancements. Much of this is behind the scenes, but some changes affect the user interfaces or configuration.

X15.0.3 release

Default Cross-Site Request Forgery Protection Status to Enabled

From X15.0.3 and subsequent releases, the Cross-Site Request Forgery (CSRF) Protection status is automatically 'Enabled' as a new installation, factory reset, or system upgrade to x15.0.3, enabled by default.

Note: We recommend keeping it enabled. To change it, please log in to the CLI.

Due to this, the custom header must be added to the content header for all the post/put call requests in Expressway.

X15.0.2 release

Removal of Obsolete Cipher

The default cipher configuration is modified in the Expressway. The changes are as follows.

Fresh Installation

From (Existing) - "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH:!AES256+DH+AESCCM"

New cipher configuration-

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

The following ciphers have been removed with min TLSv1.2 configuration.

1. TLS_RSA_WITH_AES_256_CCM
2. TLS_RSA_WITH_AES_128_CCM

3. TLS_DHE_RSA_WITH_AES_256_CCM
4. TLS_DHE_RSA_WITH_AES_128_CCM
5. TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Upgrade

If the user is upgrading from another version and if the

- Default ciphers were used in the existing version; they would be modified to the newer cipher string.
- The user has already modified Ciphers; they will be retained as-is.
- The user has preferred RSA Ciphers using a prefix of ECDHE-RSA-AES256-GCM-SHA384, then the system will retain that prefix, and RSA will be preferred post-upgrade.

Information –

1. New VM deployment with X15.0.2 OVA file, cipher parameter will be set to the new recommended configuration.

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

2. Upgrade to X15.0.2 on systems with default cipher configuration; the cipher configuration will automatically update to the new recommended configuration.

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

3. When upgrading to X15.0.2 on systems with customized cipher configurations, the cipher configuration is retained as-is after the software upgrade (it is not automatically updated).
4. Post upgrade and resetting the configuration to factory settings, automatically update the cipher parameter to a new recommended configuration.

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

X15.0.1 release

There are no new features or changes in this release.

X15.0 release

LDAP TLS support for different ports other than 636 or 3269

Expressway supports LDAPS for port 636 and LDAP over TLS (START_TLS)/LDAP Over TCP for port 389 or any other non-standard port.

While using SRV records, the LDAP communication port is assigned through DNS.

The Administrator can only select Encryption as TLS or OFF from the Web User Interface. Expressway uses “START_TLS” functionality on any non-standard port defined for LDAP over TLS. Expressway first checks

for “START_TLS” functionality even when Encryption is set to OFF. Otherwise, it proceeds with "LDAP Over TCP."

In the previous versions,

Port	Encryption	Server Certificate	Notes
636	TLS	Installed under the Trusted CA list at both ends	Communication in such case start by establishing TLS session towards LDAP and after successful TLS negotiation, the communication is encrypted.
389	OFF	--	Communication in such cases starts with Expressway establishing a TCP session towards the LDAP server and then checks for “START_TLS” functionality support from the LDAP side. If the response for “START_TLS” is a success, TLS is negotiated between the parties, and the session is encrypted.
			Communication is encrypted by “START_TLS” negotiation. If the session cannot be established using “START_TLS” functionality over TCP port 389 or a non-standard port, the LDAP session would be negotiated over TCP with "No Encryption." For example, the session fails to establish due to “Unknown CA” even after “START_TLS” is negotiated successfully. Communication with LDAP is established over TCP.

The following are the limitations of this behavior.

- Expressway used LDAP(S) only with well-defined LDAP port 636.
- For any other port, for example, 389 or a non-standard port, Expressway is hard-coded to always use the “Start_TLS” feature even if the encryption is set to OFF.
- Customers might not be aware that Expressway is using the” Start_TLS” feature in the background.

From X15.0 release,

Expressway supports LDAP port customization, and administrators will be able to set up desired encryption.

Administrator will be able to select Encryption as TLS, STARTTLS, or OFF from the Web User Interface.

After upgrading to X15.0 release, you must manually select an appropriate setting depending on the LDAP server configuration.

Note: Before upgrading to X15.0 release, you must manually set the “administration authentication source” as “Both” to avoid accidental locking out after upgrade.

Expressway is set up to use the following ports listed in the table.

Port	Encryption	Server Certificate	Notes
389	TLS	Installed under Trusted CA list on both ends	Earlier, it was only possible with default LDAP(S) port 636. In such cases, communication starts by establishing a TLS session with LDAP. After successful TLS negotiation, the communication is encrypted.
636	STARTTLS	Installed under Trusted CA list on both ends	A TCP session towards LDAP is established on port 636 (a well-known LDAP(S) port), which is also used for LDAP over TLS. After successful negotiation for “START_TLS,” the communication is encrypted.
Custom LDAP port 3636	OFF	--	Unlike the earlier implementation, Expressway uses TCP and does not look for “START_TLS” negotiation. Communication with LDAP is established over TCP.
3389	TLS	Installed under Trusted CA list on both ends	Earlier, it was only possible with default LDAP(S) port 636. Communication in such a case starts by establishing TLS session towards LDAP, and after successful TLS negotiation, the communication is encrypted

For more information, see the Cisco Expressway Administrator Guide.

Removal of Banned Ciphers

Expressway supports the following banned ciphers by default. Starting with the X15.0 release, it is recommended that you remove them from the **Maintenance** > **Security** > **Ciphers** page.

TLS_DHE_RSA_WITH_AES_128_CCM

TLS_RSA_WITH_AES_256_CCM

TLS_RSA_WITH_AES_128_CCM

For more information, see the Cisco Expressway Administrator Guide.

Management Enhancement

X15.0.3 release

Cross-Site Request Forgery Protection Header

Disabling or Enabling the Cross-Site Request Forgery Protection: CSRF Protection is Enabled by default.

X15.0.2 release

There are no new features or changes in this release.

X15.0.1 release

There are no new features or changes in this release.

X15.0 release

Cross-Site Request Forgery Protection Header

A new header has been included to prevent such attacks and must now be sent with XML Put, SOAP, and CDB Rest API requests whenever CSRF Protection is enabled. For the commands to enable or disable CSRF Header: X-CSRF-Header.

The CSRF Protection Header is introduced for CDB, XMLPut, and SOAP APIs.

Disabling or Enabling the Cross-Site Request Forgery Protection: CSRF Protection is Disabled by default.

The following CLI commands are introduced to enable or disable the custom header.

- xConfiguration Security CSRFProtection Status: "Disabled"
- xConfiguration Security CSRFProtection Status: "Enabled"

For more information, see the Cisco Expressway Administrator Guide (see the chapter "Reference Material - xConfiguration Commands").

Mobile Remote Access Enhancement
X15.0.3 release

TCP_NODELAY socket option for Expressway's SIP Register Message

Issue: MRA endpoints are not receiving 200 OK as the refresh register message

The issue observed on the Unified CM side was that when they receive the STUN request, and SIP REGISTER request messages, they can only parse the STUN request message. They cannot send the response to the Expressway side for the SIP REGISTER request. Hence, the MRA end-point is not sending the 200 OK response to the SIP Register.

Recommendation: TCP_NODELAY can reduce latency and increase the number of packets sent across the network since the data is sent as soon as it is written to the socket without waiting to fill a larger packet. So, we can enable the TCP no-delay option only when needed and have its default value set to OFF. Hence, CLI is recommended to enable the TCP no-delay option.

CLI Command:

xConfiguration SIP Advanced SipSocketTcpNoDelayEnabled: Off/On

Default value: Off

The default value for this CLI command is OFF.

Set the flag 'SipSocketTcpNoDelayEnabled' ON to set the TCP_NODELAY Socket option for SIP register messages.

This command is removed for Expressway-E, VCS-C, and VCS-E, and it is now available only for Expressway-C.

X15.0.2 release

There are no new features or changes in this release.

X15.0.1 release

There are no new features or changes in this release.

X15.0 release

Webex Unified CM Calling Support Auto-extend Refresh Token

The Webex App (Unified CM Registered) prompts users to log in every 60 days to maintain phone service. Administrators can configure the periodicity of these prompts. The default timing is 60 days.

Users can cancel their login to the Webex App. However, they will still have access to messaging, meetings, and internal calls. If the calls are not properly authenticated, then users will experience phone service disconnects and missed calls. Additionally, the User Experience can become confusing where internal (Call on Webex) calls may work, but PSTN calls will fail.

Set up the automatic Webex Application Refresh Token renewal for an improved user calling experience. This feature and Unified CM 15 have been available since November 2023. The Expressway X15 and Webex App 6.8 also support this feature.

This feature's benefits include end users not missing calls on the Webex App and experiencing calls on Webex only when PSTN calls fail.

Preview Features

Some features in this release are provided in “preview” status only because they have known limitations or incomplete software dependencies. Cisco reserves the right to disable preview features at any time without notice.

Preview features should not be relied on in your production environment. Cisco Technical Support will provide limited assistance (Severity 4) to customers who want to use preview features.

Headset Capabilities for Cisco Contact Center – MRA Deployments

This feature applies if you deploy Expressway with Mobile and Remote Access. It is currently provided in Preview status only.

New demonstration software now provides Cisco Contact Center functions on compatible Cisco headsets. From X12.6, Expressway automatically supports these new headset capabilities as a preview feature if the involved endpoint, headset, and Unified CM run the necessary software versions. The feature is enabled from the Unified CM interface, and you do not need to configure anything on Expressway.

More information is available in the Cisco Headset and Finesse Integration for Contact Center white paper.

KEM Support for Compatible Phones - MRA Deployments

We have not officially tested and verified support over MRA for the Key Expansion Module (KEM) accessory for Cisco IP Phone 8800 Series devices. However, we have observed that KEMs with multiple DNs work satisfactorily over MRA under lab conditions. These are not official tests, but given the COVID-19 crisis, this may be useful information for customers willing to use an unsupported preview feature.

SIP path headers must be enabled on Expressway, and you need a Unified CM software version that supports path headers (release 11.5(1)SU4 or later is recommended).

REST API Changes

The Expressway REST API is available to simplify remote configuration, for example, by third-party systems. As new features are added, we add REST API access to configuration, commands, and status information. We also selectively retrofit the REST API to some features added in earlier 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	X15.0.3
Resource Usage	X15.0.2
Cluster Peer Status	X15.0.2
Sys Key Status	X15.0.2
NA	X15.0.1
NA	X15.0

Other Changes in this Release

X15.0 release

Expressway supports proxy TFTP deployment

The TFTP (Trivial File Transfer Protocol) Proxy setup now supports the endpoint registration using activation code Onboarding and MRA.

A few other changes in this release:

- You can only enable **PreRoutedRouteHeader (PRRH)** on the Expressway Select image. In the Expressway image, PRRH is disabled, and the Command Line Interface (CLI) option is unavailable.
- A new parameter, “Webrtc Sessions,” is added to the Expressway-E **Overview** page.
- **Log rotation stops in the Expressway**

  Issue Description: Developer/Network/Sensors/Messages/Kernel logs stop rotating whenever there is a crash on the Expressway.

  Cause: This is caused by creating new crash log files (hard-linked to existing log files) under **/mnt/harddisk/log**. The size of the logs increases and fails to rotate.
  Example of files created:

  - crash-XXXX-XX-XXXX-messages
  - crash-XXXX-XX-XXXX-developer_log

- crash-XXXX-XX-XXXX-network_log

Solution: Delete all files of the form **crash-XXXX-XX-XXXX-messages/developer_log/network_log/sensors/kernel**

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 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 Cisco Expressway Administrator Guide.

Smart Licensing Export Compliance for 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.
- Export unrestricted images like "Expressway" are limited to 2500 encrypted signaling sessions by default.
- 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	X14.3.1 and Expressway Select X14.3.1 is not supported on the Cisco TelePresence Video Communication Server	
Support Advanced Account Security (AAS)	Yes		AAS and FIPS140-2 feature(s) is enabled by

	Cisco Expressway Select	Cisco TelePresence Video Communication Server (VCS)	Notes
and FIPS140-2 Cryptographic Mode		(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. Details are available at the following link.	default in Expressway Select.
Smart Licensing	Yes		

For more information, see the Cisco Expressway Administrator Guide.

Limitations

Some Expressway Features are Preview or Have External Dependencies

We aim to provide new Expressway features as speedily as possible. Sometimes, it is impossible to officially support a new feature because it may require updates to other Cisco products that are not yet available, or known issues or limitations affect some deployments of the feature. If customers might still benefit from using the feature, we mark it as a “preview” in the release notes. Preview features may be used, **but you should not rely on them in production environments (see Preview Features Disclaimer**). Occasionally we may recommend that a feature is not used until further updates are made to Expressway or other products.

Open and Resolved Issues

Follow the links below to read the most recent information about this release's open and resolved issues.

- All open issues, sorted by date modified (recent first)
- Issues resolved in X15.0.3
- Issues resolved in X15.0.2
- Issues resolved in X15.0.1
- Issues resolved in X15.0

Notable Issue Resolved

X15.0.1 release

The following notable issue is resolved.

taa-chkpasswd randomly consuming high CPU beyond the normal duration while interacting with LDAP for user authentication

Earlier, taa-chkpasswd randomly consumed a high CPU beyond the normal duration while interacting with LDAP for user authentication.

This behavior was observed while connecting to the Active Directory (AD). Connectivity issues must generate error responses and not lead to high CPU utilization.

After the Fix, CPU consumption is in the minimal range, even if connectivity issues persist.

This refers to bug ID CSCwh76084.

Notable Issue

None

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.
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 either *Keyword*, *Modified Date*, *Severity*, *Status*, or *Technology*.

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

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.

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.
- Ensure the Quantity of 0$ PID should equal the number of nodes.

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

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.

Appendix 3: Upgrade Path

Purpose – This section is to guide you through the Expressway upgrade process.

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 X14.3.1/X14.3.2/X14.3.3/X15.0/X15.0.1/X15.0.2/X15.0.3 unrestricted	
Option 1:	X14.0 restricted → 0$ PID → X14.3.1/X14.3.2/X14.3.3/X15.0/X15.0.1/X15.0.2/X15.0.3 unrestricted
Option 2:	X14.0 restricted → 0$ PID → X14.0 unrestricted → X14.3.1/X14.3.2/X14.3.3/X15.0/X15.0.1/X15.0.2/X15.0.3 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) prior to 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.	

For more information, see Upgrade of Video Communication Server (VCS) / Expressway X15.x - Guide & FAQ.

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.