Cisco Expressway and Cisco Expressway Select Release Note for X15.2.x

(Includes X15.2 and X15.2.1 releases)

Published Date: 2024-11-05

Contents

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
November 2024	First publication for Cisco Expressway and Cisco Expressway Select - X15.2.1	X15.2.1 release
October 2024	First publication for Cisco Expressway and Cisco Expressway Select - X15.2	X15.2 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: Cisco Expressway pre-installed on UCS C220 M6S)**	52E5####	X14.3.1 onwards
CE1200 Hardware Revision 2 **(4th gen: Cisco Expressway pre-installed on UCS C220 M5L)**	52E1####	Supported (X12.5.5 onwards) End of Life Announcement: Link
CE1200 Hardware Revision 1 **(4th gen: Cisco Expressway pre-installed on UCS C220 M5L)**	52E0####	Supported (X8.11.1 onwards) End of Life Announcement: Link

Platform Name	Serial Number	Scope of Software Version Support
CE1100 (3rd gen: Cisco Expressway pre-installed on UCS C220 M4L)	52D#####	Not Supported 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 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 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. This means that Cisco Expressway can only support 1250 of these Jabber client registrations.

Important:

- Ensure that the limited number of encrypted signaling is **not** more than 2500 sessions per Cisco Expressway instance. 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.

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

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

Or

- Cisco Expressway Select –→ Cisco Expressway

For more information, see Appendix 3: Upgrade Path.

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.

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)

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).

Summary of Features and Bugs Fixed

Feature Enhancements	Status
Cisco Expressway supports TLS 1.3. There is an interface to set TLS 1.3 as a minimum protocol	Supported from X15.2
Deprecated Crypto Algorithm in Cisco Expressway	
An interface is provided to change the preference of the signature algorithm for SIP protocol over TLS 1.3. This applies to all outbound SIP communications	
Syncing the database has improved the administrator experience	
New Interfaces are introduced to configure MRA cookies. 1. HttpOnly Edge 2. X-Auth Cookie Expiry	
Cisco Expressway checks for poll validation fields (RFC 5905) in ntpd servers	
Default API access for Admin has been disabled on GUI and CLI	

Bugs Fixed	Status
Incorrectly formatted SIP message crashing the App	Supported from X15.2
IDP, CUCM, MRA, FW config not captured in Cisco Expressway backup	
Cisco Expressway Access Control in Web Interface	
Apache HTTP server 2.4.56 related vulnerabilities	
Cisco Expressway Series Privilege Escalation Vulnerability	

Bugs Fixed	Status
Cisco Expressway Edge Improper Authorization Vulnerability	Supported from X15.2
regreSSHion - CVE-2024-6387	
CMS call move fails sometimes	
Cisco Expressway dropping calls with Bandwidth Allocation Failure, link status issues	
Upgrade to 15.0.2 removed the external LAN interface from the firewall rule configuration	
Cisco Expressway does not reflect Africa/Cairo Egypt daylight savings time	
When tomcat is CA signed but CallManager is self-signed you cannot add CallManager to Cisco Expressway-C	
ACR: __pthread_kill_implementation Line: 0 (malloc(): unsorted double linked list corrupted)	
B2BUA incorrectly shows ciphers on unencrypted call leg	
An unexpected software error was detected in the Management framework.pyc: Detail=\"Failed to notify file system observer	
Cisco Expressway negotiates encryption ciphers currently considered weak	
Not able to add Static route from Web GUI using LAN2/LAN3	
Audit logging for Rest API commands	
Cisco Expressway PSIRT Verification for CVE-2023-48795	
Page Navigation broken links in Cisco Expressway WebUI	
Network instability after upgrade to X14.3.3 for CE/appliance	
TelePresence Room registration resource leak on SLR deployment	

Bugs Fixed	Status
Cisco Expressway calls involving H323 are not capturing the Source in the Search History	Supported from X15.2
CollabEdge registration count becomes higher than the provisioned MRA client	
CollabEdge registration count is too high on the Cisco Expressway GUI	
Memory leak in Management framework leading ACR: _execute_child	
Cisco Expressway log rotation not Initiated post-upgrade	
An alarm was raised for concurrent non-traversal call limit unexpectedly	
Evaluation of VCS for HTTP/2 Rapid Reset Attack vulnerability	
SIP Registration Configuration is getting set as "Off" in EXWY-C after Upgrade	
Incorrect instructions for adding SSH public key to Cisco Expressway	
taa-chkpasswd randomly consuming high CPU for extended periods	
ClusterDB crashed (Erlang heap crash)	
ACR: __pthread_kill_implementation Line: 0	
STUN Keepalive feature is not disabled on Cisco Expressway-C when set to Off	
LDAP TLS support for different ports than 636	
Cisco Expressway/VCS OVA Presents as Other (32-Bit) under Guest OS of 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. This table lists the features that are currently in deprecated status or have been withdrawn since X12.5.

Feature / Software	Status
SHA1 Signed Certificate deprecation in the Cisco Expressway	Deprecated from X15.2
Support for Microsoft Lync Server	Withdrawn For more information, follow the 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
Cisco Jabber Video for TelePresence (Movi) **Note: This 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
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

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 Communication Manager in conjunction with Cisco Emergency Responder.

Related Documentation

Resource	Description
Support Videos	Videos provided by Cisco TAC engineers about certain common Cisco Expressway configuration procedures are available on the Cisco Expressway/VCS Screencast Video List page (search for "Cisco Expressway videos").

Resource	Description
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. 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 Cisco Expressway Configuration Guides page. Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet on the Cisco Expressway Configuration Guides page.

Resource	Description
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 X14.x - Guide & FAQ	Guide and FAQ
Interoperability Database	Interoperability Database
Cisco Collaboration Infrastructure Requirements	Cisco Collaboration Infrastructure Requirements

Features and Changes

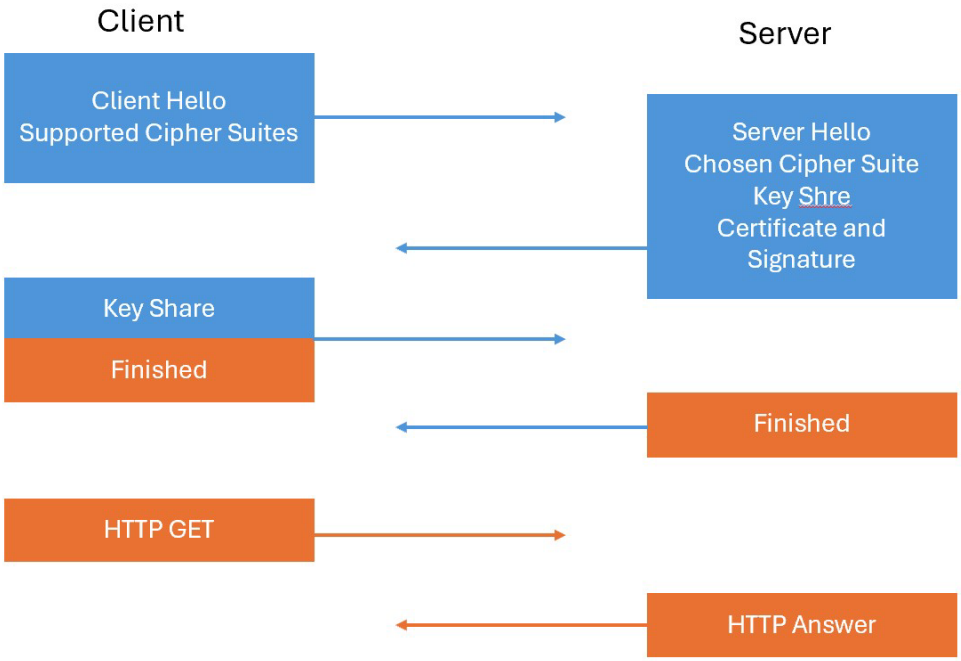
Security Enhancement

This release incorporates several security-related improvement(s) as part of the ongoing security enhancements. These may be behind the scenes, but a few changes affect the user interfaces or configuration.

TLS Operation Overview

TLS 1.3 is simpler, faster, and more secure. The cipher suite space is pruned, and all cipher suites that support TLS 1.3 use Authenticated Encryption with Associated Data (AEAD) algorithms.

TLS v1.2



The first message a Client sends, the CLIENT HELLO, with CIPHER suites supported in the preferred order.

The Server receives it and answers with SERVER HELLO with the preferred CIPHER providing its key share.

The Server also sends its certificate.

The Client receives the Server information, generates its key share, and mixes it with the server key share to generate encryption keys.

The Client then sends its key share to the server, enables encryption, and sends a Finished message.

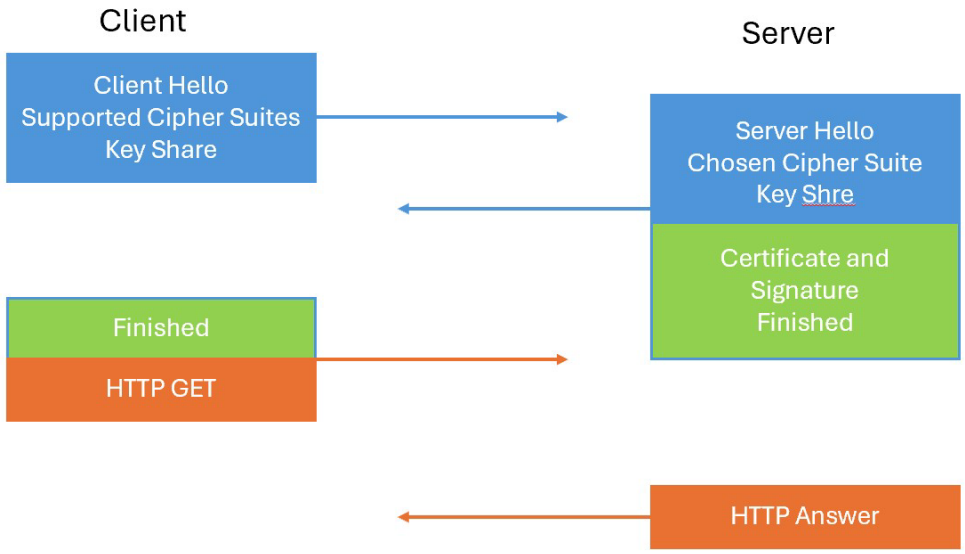
The Server does the same, mixes key share to get encryption keys, and sends a Finished message.

Encrypted Data flow is achieved at this point.

Note: For TLS v1.2, the server offers a certificate based on the preferred CIPHER.

For example, Unified CM can choose to offer an ECDSA or RSA certificate based on the CIPHER.

TLS v1.3



The Client sends the CLIENT HELLO, with CIPHER suites which it supports, but also guesses the Key Agreement Algorithm.

As soon as the Server selects the CIPHER and Key Agreement algorithm, it is ready to generate the Key since it has the client key share.

The Server sends a Finished message with its key share and certificate (Encrypted, since it has a key).

The Client receives all the information and generates its key share, checks the certificate, and Finished.

The Client is ready to share data now.

Note: Unlike the TLS v1.2 certificate, TLS v1.3 is selected based on signature algorithm.

Cisco Expressway supports TLS 1.3 as the minimum TLS version

Starting from X15.2, Cisco Expressway supports tlsv1.3 system-wide. Consider the following TLS communication between

1. Expressway-E and Clients
2. Expressway-C and On-Prem servers
3. Expressway-C and Expressway-E

Users can configure these to have its minimum TLS version as 1.3. This minimum TLS version can be configured per the component defined in the **Maintenance** –> **Security** –> **Cipher configuration** page.

Note:

- All Inbound/Outbound connections to support tlsv1.3.
- Unlike tlsv1.2, users cannot modify the Ciphers list in tlsv1.3.

- Below is the default cipher list supported with tlsv1.3
  - Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
  - Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
  - Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
- Presently, the system upgrade from an old version will continue to use the minimum TLS version as tlsv1.2.
- Systems on upgrade support tlsv1.3 ciphers, but no changes on the cipher list under Web User Interface.
- Any new installations on version X15.2 supports the minimum TLS version as tlsv1.2 by default.
- tlsv1.3 ciphers are added for new installs as well. However, there are no changes to the cipher list for tlsv1.2.

Configure TLS v1.3 as the minimum TLS version option for services

1 Remote Loggin (Syslog)

Remote Syslog now supports TLS v1.3 for message logging via the Syslog server.

Admin can select TLS version under **Maintenance** -> **Logging** -> **Remote Syslog servers** -> **Minimum TLS version**.

The ECDSA signature algorithm is preferred after configuring TLS v1.3. The admin must install the right certificates on the servers to set up the trust relation correctly.

If minimum version tlsv1.2 is enabled on Cisco Expressway, it offers both TLS 1.2 and TLS 1.3 under *Client Hello* with preferred CIPHERS for tlsv1.2 negotiations and preferred algorithm as ECDSA for tlsv1.3.

2 HTTPS

- TLS v1.3 is now supported for the Web Management of Cisco Expressway.
- Admin can select the TLS version under **Maintenance** -> **Security** -> **Ciphers** and set the TLS version for HTTPS.
- For incoming HTTPS connections, Cisco Expressway acts as a server.
- Cisco Expressway selects TLS v1.3 if the Client offers tlsv1.3 only or with other lower versions.
- If Cisco Expressway is set for minTLS v1.3, ensure that the Web client also supports TLS v1.3. Otherwise, the connection will fail.

3 LDAP

TLS v1.3 is now supported for connections to the LDAP server.

Admin can select the TLS version under Maintenance -> Security -> CIPHERS and set the minTLS version for LDAP.

4 Reverse Proxy

- TLS v1.3 now supports Logon services using Reverse proxy.
- Admin can select the TLS version and set the TLS version for Reverse Proxy under **Maintenance** -> **Security** -> **Ciphers**.
- Expressway acts as a client for outgoing HTTPS connections through Reverse proxy (remap, cms).
- Expressway acts as a server for incoming HTTPS connections.
- Expressway selects TLS v1.3 if the client offers tlsv1.3 only or with other lower versions.
- If Cisco Expressway is set for minTLS v1.3, ensure that the client also supports TLS v1.3. Otherwise, the connection will fail.

5 SIP

- TLS v1.3 now supports SIP communications on the Cisco Expressway.
- Admin can select the TLS version and set the TLS version for SIP under **Maintenance** -> **Security** -> **Ciphers**.
- Expressway acts as a client for outgoing SIP connections.
- Expressway acts as a server for incoming SIP connections.
- Expressway selects TLS v1.3 if the client offers tlsv1.3 only or with other lower versions.
- If Cisco Expressway is set for minTLS v1.3, ensure that the client also supports TLS v1.3. Otherwise, the connection will fail.
- Use this for traversal zones between Cisco Expressway E (as a server) and Cisco Expressway C (as a client).

6. TMS

TMS interface does not support TLS 1.3.

7 UC discovery

- TLS v1.3 supports Unified communication server discovery.
- Admin can select the TLS version and set the TLS version for UC Discovery under **Maintenance** -> **Security** -> **Ciphers**.
- Cisco Expressway acts as a client for outgoing HTTPS connections for AXL queries.

8 XMPP

- TLS v1.3 supports XMPP communications on the Cisco Expressway.
- Admin can select the TLS version and set the TLS version for XMPP under **Maintenance** -> **Security** -> **Ciphers**.
- Expressway acts as a client for outgoing XMPP connections.
- Expressway acts as a server for incoming XMPP connections
- You can use this for XMPP federation between Expressway E.

9 SMTP

- TLS v1.3 supports connections to the SMTP server.
- Admin can select the TLS version and set the minTLS version for SMTP under **Maintenance** -> **Security** -> **Ciphers**.

Enable support for TLS v1.3 in Cluster Database

- CDB supports TLS v1.3 with the upgrade to the Cisco Expressway X15.2. This is unlike other interfaces which offer both TLS v1.2 and TLS v1.3.
- There is no option to change the minimum TLS version from 1.3 for CDB connections. Only the following Cipher has been added as part of TLS v1.3.
  TLS_AES_128_GCM_SHA256

System Upgrade to X15.2

The CDB connection breaks due to TLS version mismatch raising a cluster replication alarm while upgrading the software version to X15.2.

Warning: This Expressway cluster is in a partitioned state. Do not make any configuration changes until the cluster is operating normally. See the Clustering page.

After upgrading the primary node, the upgraded node uses tlsv1.3 to connect, which other nodes will reject with a “protocol version” error.

After upgrading the remaining nodes to the X15.2 version, the TLS v1.3 protocol establishes TLS.

Deprecated Crypto Algorithm in Cisco Expressway

From the Cisco Expressway X15.2 release, Expressway certificates will NOT support deprecated signature algorithms such as Signature Algorithm: sha1WithRSAEncryption or ecdsa-with-SHA1>. This is after updating Erlang-OTP to 26.2.2 in X15.2.

Customers must regenerate the server certificate using supported algorithms for Cisco Expressway upgrades.

If the sha1 certificate is installed and upgraded to X15.2 then the upgrade fails with an error message,

Certificates signed with Signature Algorithm: <sha1WithRSAEncryption or ecdsa-with-SHA1> is no longer supported. Update the Expressway Certificate before upgrading the Expressway Server. For more information, see the Cisco Expressway Administrator Guide.

Mobile Remote Access Enhancement

The following are the Mobile Remote Access management feature enhancements for improving administrator experience.

An interface is provided to change the preference of the signature algorithm for SIP protocol over TLS 1.3. This applies to all outbound SIP communications

A new xConfiguration command is introduced to enable or disable the preference for the RSA signature algorithm in Expressway-C for SIP protocol communication over TLS 1.3.

xConfiguration SIP Advanced TlsSignatureAlgoPrefRsa: <On/Off>

Default: On

For more information, see the Cisco Expressway Administrator Guide.

Optimize OAuth Flow for better CDB sync

Syncing the database has improved the administrator experience.

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. There is a plan 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	X15.2

Other Changes in this Release

New Interfaces are introduced to configure MRA cookies.

1. HttpOnly Edge Cookie is enabled by default. It supports Jabber 12.7 and later versions

   A new xConfiguration command is introduced.

   xConfiguration MRACookieConfig Httponly: <Enabled/Disabled>

   For more information, see the Cisco Expressway Administrator Guide.

2. X-Auth Cookie Expiry Config Changes

   A new xConfiguration command is introduced.

   xConfiguration MRACookieConfig Expiry: <Enabled/Disabled>

   For more information, see the Cisco Expressway Administrator Guide.

Cisco Expressway checks for poll validation fields (RFC 5905) in ntpd servers

Starting from the Cisco Expressway X15.2 release, Expressway will adhere to strict poll validation checks defined in RFC 5905. Expressway will reject any NTP server with invalid poll field values outside the range of MINPOLL (4) and MAXPOLL (17). This validation check is to maintain subnet dynamic behavior and protect against protocol errors.

Default API access for Admin has been disabled on GUI and CLI

All hosted API resources (web services) that accept client application connections MUST use authentication and authorization to protect API functionality. This applies to accessing data commensurate with the API's data sensitivity.

Earlier API access was 'Enabled' by default, and now it is 'Disabled'.

Note: This feature is applicable ONLY for new users.

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.
- 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	**X15.x and Cisco Expressway Select X15.x are not supported on 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. Details are available at the following link.**	
Support Advanced Account Security (AAS) and FIPS140-2 Cryptographic Mode	Yes		AAS and FIPS140-2 feature(s) are enabled by default in 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 most recent information about this release's open and resolved issues.

- All open issues, sorted by date modified (recent first)
- Issues resolved in X15.2.1
- Issues resolved in X15.2

Notable Issue

Ensure to use calendar connector version 8.11-1.0.8858 or later. Do this to avoid issues when creating new Microsoft Exchange or Cisco Conferencing Services configurations for the Hybrid Services calendar connector running on the Cisco Expressway X15.2.1 or later.

Notable Issue Resolved

Notice the following banner on the CCO page before performing an upgrade to Cisco Expressway X15.2. Customers using Expressway for Hybrid Services should NOT upgrade to Cisco Expressway X15.2. This refers to bug ID CSCwm90275.

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.

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 Deprecated Crypto Algorithm in Expressway.

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 unrestricted	
Option 1:	X14.0 restricted → 0$ PID → X14.3.x/X15.0.x/X15.2.x unrestricted
Option 2:	X14.0 restricted → 0$ PID → X14.0 unrestricted → X14.3.x/X15.0.x/X15.2.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.	

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.