Cisco Expressway and Cisco Expressway Select Release Note for X14.3.x

(Includes X14.3, X14.3.1, X14.3.2, X14.3.3, X14.3.4, X14.3.5, and X14.3.6 releases)

Published Date: 2024-08-15

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
August 2024	First publication for Cisco Expressway and Cisco Expressway Select - X14.3.6	X14.3.6 release
July 2024	Republished the Cisco Expressway and Cisco Expressway Select Release Note - X14.3.x	X14.3.x release
March 2024	First publication for Cisco Expressway and Cisco Expressway Select - X14.3.5	X14.3.5 release
January 2024	First publication for Cisco Expressway and Cisco Expressway Select - X14.3.4	X14.3.4 release
November 2023	First publication for Cisco Expressway and Cisco Expressway Select - X14.3.3	X14.3.3 release
November 2023	First publication for Cisco Expressway and Cisco Expressway Select - X14.3.2	X14.3.2 release
August 2023	First publication for Cisco Expressway and Cisco Expressway Select - X14.3.1	X14.3.1 release
May 2023	First publication for Cisco Expressway and Cisco Expressway Select - X14.3	X14.3 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)

Platform Name	Serial Number	Scope of Software Version Support
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
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#####	Note 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.

- From X14.2 release and later versions, ESXi 6.5 Update 2a, ESXi 7.0 Update 3, ESXi 7.0 Update 3c, and ESXi 7.0 Update 3d are supported.

From the X14.2.6 release and later versions, ESXi 6.5 Update 2a, ESXi 7.0 Update 3c, ESXi 7.0 Update 3d, and ESXi 8.0 Update 1 are supported.

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: 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: 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

X14.3.6 release

This release fixes a defect, **CVE-2024-6387–Remote Unauthenticated Code Execution Vulnerability in OpenSSH Server (regreSSHion)**. For more information, see Issues resolved in X14.3.6.

X14.3.5 release

A few defects are fixed in this release. For more information, see Issues resolved in X14.3.5.

X14.3.4 release

A few defects are fixed in this release. For more information, see Issues resolved in X14.3.4.

X14.3.3 release

A few defects are fixed in this release. For more information, see Issues resolved in X14.3.3.

X14.3.2 release

A few defects are fixed in this release. For more information, see Issues resolved in X14.3.2.

X14.3.1 release

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.

The CAP of 2500 secured/crypto sessions is also applicable to the Cisco TelePresence Video Communication Server (VCS) Series.

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.

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).

X14.3 release

Smart Licensing Export Compliance – Unrestricted (Capped Version)

Signaling to no more than 2500 endpoints

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.

Expressway is a media gateway and must provide media encryption or encrypted signaling to **at most** 2500 endpoints. This restriction is effective from X14.2 release of the Cisco Expressway.

The CAP of 2500 secured/crypto sessions also applies to Cisco TelePresence Video Communication Server (VCS) Series.

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

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 instance of Expressway. A customer that needs to exceed this limit may deploy additional peers/clusters, if entitled, 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.

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. This image cannot exceed 2,500 encrypted signaling sessions. Users must submit a new $0 order (PID L-EXPWY-14.X-K9=) for an export-restricted image exceeding 2,500 encrypted signaling sessions.

For PID Details and Ordering Guide, see Appendix 1: Ordering Information.

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

The following upgrades are allowed.

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

For more information, see Appendix 3: Upgrade Path.

Deploying OVA with vSphere ESXi 7.0 U2

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

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

X14.3.1 and later releases

This section applies to hardware support services only.

CE1300 Appliance

X14.3.1 is the first factory-loaded and supported release on this appliance. For more information, see Virtualization for Cisco Expressway.

CE1200 Appliance

The Cisco Expressway X14.3.1 is supported on CE1200.

The End of Vulnerability/Security support is until November 30, 2023.

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 X14.3.1 is supported on CE1100.

The End of Vulnerability/Security support is until November 30, 2023 (as per the original End-of-Life bulletin), which is also the last date of support for those customers with a valid service contract.

The last date of support (Hardware) is November 30, 2023.

Although customers may run this release of software 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 X14.3.1 is **not** supported on CE500 and CE1000.

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

X14.3 release[2]

This section applies to hardware support services only.

CE1200 Appliance

Important: Supply issues with components used in the Expressway CE1200 delay orders. In light of the supply issues, we are extending the end of Vulnerability/Security support until November 30, 2023.

Please ignore the warning “unsupported hardware” in the User Interface.

[2] In Cisco Expressway and Cisco Expressway Select Release Note - X14.3, it was titled “Hardware Support for CE1200, CE1100, CE1000, and CE500 Appliances.” To maintain consistency, the title is changed.

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

Considering ongoing issues with component shortages that are affecting the timely supply of new Expressway appliances, to support those customers still using Cisco Expressway CE1100 appliances, Cisco has decided to extend the End of Vulnerability/Security Support from November 14, 2021 (as per the original End-of-Life bulletin) to November 30, 2023, in line with the last date of support, for those customers with a valid service contract.

Although customers may run this release of software 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 Notice

Cisco no longer supports the Cisco Expressway CE500 and CE1000 appliance hardware platforms. For 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

X14.3.6 release

Feature / Change	Status
CVE-2024-6387–Remote Unauthenticated Code Execution Vulnerability in OpenSSH Server (regreSSHion)	Supported from X14.3.6

X14.3.x releases

Feature / Change	Status
NA	X14.3.5 X14.3.4 X14.3.3 X14.3.2 X14.3.1

X14.3 release

Feature / Change	Status
Support for Elliptic Curve Digital Signature Algorithm (ECDSA) certificate	Supported from X14.3
Route calls to US Suicide Prevention Hotline (988) without RMS licenses	Supported from X14.3

Withdrawn or Deprecated Features and Software

The Expressway product set is under continuous review and features are sometimes withdrawn from the product or deprecated to indicate that support for them 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
Cisco Jabber Video for TelePresence (Movi) **Note: This pertains 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 Management Suite Provisioning Extension (Cisco TMSPE)	Deprecated
Expressway Starter Pack	Deprecated
Smart Call Home preview feature	Withdrawn X12.6.2

Feature / Software	Status
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 Ray Baum's Act requirements should use the Cisco Unified Communication Manager in conjunction with the 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.
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.

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

Features and Changes

X14.3.6 release

Security Enhancement

CVE-2024-6387 - Remote Unauthenticated Code Execution Vulnerability in OpenSSH Server (regreSSHion)

From the Cisco Expressway X14.3.6 release onwards, this fix evaluates the product Expressway Series and TelePresence Video Communication Server (VCS) against the vulnerability in the OpenSSH server.

X14.3.5, X14.3.4, X14.3.3, and X14.3.2 releases

These releases (Including X14.3.5, X14.3.4, X14.3.3, and X14.3.2) do not include new features.

X14.3.1 release

We aim to provide new Expressway features as promptly 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.

There are no new functional enhancements or changes for this release.

X14.3 release

We aim to provide new Expressway features as promptly as possible. Sometimes, it is not possible to officially support a new feature because it may require updates to other Cisco products that are not yet available.

Security Enhancement

Various security-related improvement(s) apply 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.

Support for Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate

Earlier releases of Cisco Expressway supported RSA certificates only. However, from the Cisco Expressway X14.3 release onwards, the Elliptic Curve Digital Signature Algorithm (ECDSA) certificate and the existing RSA certificate have been added.

RSA and ECDSA have been added to the Publickeyalgorithm field. The Keysize depends on the selected Publickeyalgorithm.

Command Line Interface Updates

The settings can also be configured through the following commands in the Expressway CLI:

- xconfiguration Ciphers sshd_pfwd_pubkeyalgorithms
- xcommand Certs Command for Server CSR
- xcommand Certs Command for Domain CSR

For details, see the Cisco Expressway Administrator Guide (X14.3).

Configuration Details

For details, see the Cisco Expressway Certificate Creation and Use Deployment Guide (X14.3).

Management Enhancement

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

Route calls to US Suicide Prevention Hotline (988) without RMS licenses

Expressway supports 911, 933, and 988 calls without consuming Rich Media Session (RMS) licenses.

Set the Default Value of SIP TLS DH key size to 2048 for Fresh Install and Upgrade

There is a change in the default value after the fresh installation and upgrade.

```
"xConfiguration SIP Advanced SipTlsDhKeySize"
```

When Expressway is upgraded from X14.2.6 or a lower version to the X14.3 release, the value of the SipTlsDhKeySize configure will be set to 2048 if it is currently 1024.

Fresh Installation: When we install the Expressway X14.3 release fresh, the default value of SipTlsDhKeySize is 2048.

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 some 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 white paper Cisco Headset and Finesse Integration for Contact Center.

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 in view of the COVID-19 crisis, this may be useful information for customers who are 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 REST API for Expressway is available to simplify remote configuration. For example, by third party systems such as Cisco Prime Collaboration Provisioning. We add REST API access to configuration, commands, and status information as new features are added, and also selectively retrofit the REST API to some features that were added in earlier versions of Expressway.

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	X14.3.6 X14.3.5 X14.3.4 X14.3.3 X14.3.2

Other Changes

X14.3.6, X14.3.5, X14.3.4, and X14.3.3 releases

There are no changes in these releases.

X14.3.2 release

Common Criteria Changes

The following are the changes –

- **Audit Log for Login Banner** – Editing the Login Banner will now create an Event Log displaying the changes made, the user who made them, and the time they were made.
- **SSH Logging Enhancement** – SSH logs are added.

- **CLI Session Timeout** - Local CLI Sessions will now timeout as intended.
- **Event Logging - TLS Handshakes, Failed Connection, and many more –**
  - A new log level is included for the Apache Web Server called "developer.apache2"
  - Log Level change for "developer.apache2" will trigger the Apache Web Server to restart.
  - In the **Maintenance > Diagnostics > Advanced > Support Log configuration** section, the "Reset to info" button has been renamed to "Reset Defaults."

X14.3.1 release

Auto-renew of Refresh Token

The Webex App registered to Unified CM with OAuth authentication will automatically receive a Refresh token that is auto-renewed before it expires.

Expressway X14.3.1 will support this feature, and the Webex App will continue to receive Unified CM services without requiring a user to re-login after regular intervals.

The Jabber App behavior will not change. Its behavior will be similar to builds prior to X14.3.1.

X14.3 release

Unicode Character 2020 (dagger †) is removed from the Expressway Web User Interface

All occurrences of a specified Unicode Character 2020 (dagger †) in the current Web user interface are replaced with another specified Unicode Character “§” (U+00A7). This is a paragraph symbol, "§, "one of the standard footnote symbols.

Software Download Folder Path

The software download folder and path **apply** to both Unrestricted Distribution (Capped Version) and Restricted Distribution (Uncapped Version). This was implemented from X14.2.6 and 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 the Cisco Expressway Administrator Guide.

Smart Licensing Export Compliance – Restricted Distribution (Uncapped Version)

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

	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 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) is enabled by default in Expressway Select.
Smart Licensing	Yes		

For more information, see the Cisco Expressway Administrator Guide (X14.3).

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 recommend that a feature not be 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 X14.3.6

Notable Issues Resolved

The following notable issues are resolved.

1. STUN keepalive feature is not disabled on Expressway-C when set to OFF
2. Network instability after upgrading to Expressway X14.3.3 for the CE1200 Appliance
3. Expressway for Hybrid Services

Notable Issues

X14.3.5 release

STUN keepalive feature is not disabled on Expressway-C when set to OFF

Earlier, Expressway-C continued to send STUN keepalive to Cisco Unified CM even after disabling STUN keepalive feature on the **Expressway-C Unified Communications Configuration** page.

After the fix, Expressway-C does not send STUN keepalive to Cisco Unified CM after disabling STUN keepalive feature on the **Expressway-C Unified Communications Configuration** page.

This refers to bug ID CSCwc41663.

X14.3.3 and X14.3.4 release(s)

Network instability after upgrading to Expressway X14.3.3 for the CE1200 Appliance

The Expressway-E repeatedly raises a cluster communication alarm after upgrading to Expressway version X14.3.3. This prevents establishing a TCP connection with <IP Address> on ports 4371, 4372, 8443, 5061, and other ports.

Note: Ports 8443 and 5061 are related to MRA login flows.

Information: MRA login may fail when running X14.3.3 or X14.3.4 on a CE1200 appliance. Expressway drops packets destined for ports 8443 and 5061, which receive MRA login requests.

Workaround: A temporary **workaround** to resolve this issue is to reboot the Expressway-E devices for a short while (30 minutes to 1 hour) before the issue starts again (This refers to bug ID CSCwi75348).

X14.3 release

Expressway for Hybrid Services

In the current version of the Expressway, issues in the Hybrid Message and Serviceability Services are making the connectors non-operational. (This refers to bug IDs CSCwf34800 and CSCwf34878).

The Expressway X14.3 or later version will support Hybrid Services once the above defects are resolved.

Important: Before upgrading an Expressway used for Hybrid Services running on software version X14.2.x or earlier, ensure the running version of the Management Connector is 8.11-1.0.459 or later to be compatible with the upgrade.

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 search for a specific software version. The Bug Search Tool 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

- 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-14X-K9 and A-SW-EXPWY-14XU-K9 are found under A-FLEX-3 PID.

Product Identifier (PID)	Description	Path on CCO
A-SW-EXPWY-14X-K9	Restricted, can exceed 2500 signaling sessions	Products > Cisco Products > Unified Communications > Communications Gateways > Cisco Expressway Series > Cisco Expressway Select
A-SW-EXPWY-14XU-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-14.X-K9=	$0 Product Identifier (PID) for Expressway Select[3] 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

For details, see the Cisco Collaboration Flex Plan 3.0 (Flex 3.0) Ordering Guide.

- 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.

[3] 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.

For details, see the Current VPAT Documents → TelePresence.

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 the 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/X14.3.4/ X14.3.5/X14.3.6 unrestricted		
Option 1:	X14.0 restricted → 0$ PID → X14.3.1/X14.3.2/X14.3.3/X14.3.4/ X14.3.5/X14.3.6 unrestricted	
Option 2:	X14.0 restricted → 0$ PID → X14.0 unrestricted → X14.3.1/X14.3.2/X14.3.3/X14.3.4/ X14.3.5/X14.3.6 unrestricted	
From X12.x to any X14.x upgrade		
Any version of X14.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 X14.x unrestricted or later upgrade		
There is no restriction on upgrading from X12.x to X14.x. However, the customer should convert the licensing method (from the legacy PAK license method to the Smart Licensing method) before the X14.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 or later versions.		
Compatibility		
1. Upgrade from any version prior to X8.11.4 - Requires an intermediate upgrade to X8.11.4. 2. You can directly upgrade from version X8.11.4 or later to X14.x. No intermediate version is required.		

For more information, see Upgrade of Video Communication Server (VCS) / Expressway X14.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.