Cisco Expressway and Cisco TelePresence Video Communication Server Release Note (X14.2.2)

First Published: 2022-12-07

Last Modified: 2022-12-07

About the Documentation

This document lists the following topics -

Change History

Table 1: Change History

Date	Change	Reason
December 2022	First publication for X14.2.2	X14.2.2 release
November 2022	First publication for X14.0.10	X14.0.10 release
October 2022	First publication for X14.2.1	X14.2.1 release

Date	Change	Reason
September 2022	First publication for X14.0.9	X14.0.9 release
August 2022	Republished X14.2	X14.2 release Replaced Bug ID
August 2022	First publication for X14.2	X14.2 release
July 2022	First publication for X14.0.8	X14.0.8 release
May 2022	First publication for X14.0.7	X14.0.7 release
March 2022	First publication for X14.0.6	X14.0.6 release
February 2022	First publication for X14.0.5	X14.0.5 release
December 2021	First publication for X14.0.4	X14.0.4 release
August 2021	First publication for X14.0.3.	X14.0.3 release
August 2021	Added a new item on Traffic Server Enforces Certificate Verification in the section "Other Changes in this Release."	X14.0.2 release - Republished
July 2021	First publication for X14.0.2.	X14.0.2 release
June 2021	First publication for X14.0.1.	X14.0.1 release
May 2021	Included a limitation in MRA Limitations section.	X14.0 release - Republished
April 2021	First publication for X14.0.	X14.0 release
December 2020	First publication for X12.7.	X12.7 release
August 2020	Updates for maintenance release.	X12.6.2 release
July 2020	Remove misleading section about issues with software downgrade (which is not supported).	Document correction
July 2020	Updates for maintenance release. Also, clarification on endpoint requirements for OAuth token authorization.	X12.6.1 release
June 2020	First publication for X12.6.	X12.6 release

Supported Platforms

Table 2: Expressway Platforms Supported in this Release

Platform name	Serial Numbers	Scope of software version support
Small VM (OVA)	(Auto-generated)	X8.1 onwards
Medium VM (OVA)	(Auto-generated)	X8.1 onwards
Large VM (OVA)	(Auto-generated)	X8.1 onwards
CE1200 Hardware Revision 2 (pre-installed on UCS C220 M5L)	52E1####	X12.5.5 onwards
CE1200 Hardware Revision 1 (pre-installed on UCS C220 M5L)	52E0####	X8.11.1 onwards
CE1100 (Expressway pre-installed on UCS C220 M4L)	52D#####	Not supported (after X12.5.x) except limited support with X12.6.x versions for maintenance and bug fixing purposes only. Vulnerability/Security support is extended until November 30, 2023.
CE1000 (Expressway pre-installed on UCS C220 M3L)	52B#####	Not supported (after X8.10.x)
CE500 (Expressway pre-installed on UCS C220 M3L)	52C#####	Not supported (after X8.10.x)

Change Notices

Maximum Transmission Unit Size Defaulting to 1500 Upon Upgrading to X14.2

The Maximum Transmission Unit (MTU) size defaults to 1500 post upgrade to X14.2 (from a lower version) while customizing the 'Maximum Transmission Unit (MTU)'. You must set it back to the intended value after a successful upgrade. To ensure MTU is set correctly, navigate to **System** > **Network Interfaces** > **IP** and then the appropriate LAN Number to check the current value.

Note Restart the system for MTU size modification to take effect.

Smart Licensing Export Compliance

Signaling to no more than 2500 endpoints

Cisco is committed to maintaining 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 **no more than** 2500 endpoints. *This restriction will be effective in the X14.2 release of the Cisco Expressway.*

Note The CAP of 2500 secured/crypto sessions is also applicable to 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 instance of Expressway. A customer that needs to exceed this limit may deploy additional peers/clusters if entitled, to provide additional capacity.

Note In the future release of the Cisco Expressway, the restriction will remain in place for *ineligible* customers, who may not use export-controlled functionality, but *eligible* customers who are permitted to use export-controlled functionality must order a new SKU (when available) that will allow them to exceed this limit (if running on suitable hardware), thereby reducing the total number of Expressway instances needed for some customers.

For more information, see Cisco Expressway Administrator Guide (X14.2).

Deploying OVA with VMware 7.0 U2

Note This is a known issue in the current release. Deploying X14.2 OVA shows “Invalid Certificate” on vCenter 7.0 U2 version of VMware, though it shows “Trusted Certificate” in older versions. Refer to 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) product. Details are available at the following link.

Issues resolved in this software release are available to Cisco Expressway and Cisco TelePresence Video Communication Server users, however, new features added in this release are not supported on the Cisco TelePresence Video Communication Server (VCS) product.

This notice does not affect the Cisco Expressway Series product.

Hardware Support for CE1200, CE1100, CE1000, and CE500 Appliances

This section applies to **hardware** support services only.

CE1200 Appliance

Important Supply issues with components used in the Expressway CE1200 are delaying 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.

CE1100 Appliance - End-of-Life and Advance Notice of hardware service support withdraw

In light of 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 taken the decision to extend the End of Vulnerability/Security Support from November 14, 2021 (as per the original End-of-Life announcement) to November 30, 2023, in line with the last date of support, for those customers with a valid service contract.

Note 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 and 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

The Cisco Expressway CE500 and CE1000 appliance hardware platforms are no longer supported by Cisco. See the End-of-sale announcement for more details.

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 backwards 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 table "*Services That Can be Hosted Together*" 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.

Feature Summary for X14.2.2

Table 3: Features by Release Number

Feature / Change	Status
Enabling or Disabling CDB API Access	Supported from X14.2
TLS Verification Mode	Supported from X14.2
Upload files along /tmp/ path	Supported from X14.2
Smart Licensing Phase II	Supported from X14.2
MRA over IPv6	Supported from X14.2
XCP Routing Information	Supported from X14.2
Approved Cryptographic Primitives and Parameters	Supported from X14.2
Enable DOS Protection for TrafficServer	Supported from X14.2
Reduce Email Notifications	Supported from X14.2
Alternate Method of Using xCommand FIPS	Supported from X14.2
RedSky E911 Location Services	Supported from X14.0.4
Service Select Wizard	Supported from X14.0.3
Ban/Unban an IP Address	Supported from X14.0.3
Exempt an IP Address	Supported from X14.0.3
Call Detail Record (CDR) Configuration	Supported from X14.0.3
Multiple Admin Accounts and Groups can have CLI access.	Supported from X14.0.1
Ability to configure SNMP details in the new RAML REST API.	Supported from X14.0.1

Feature / Change	Status
Ability to view and acknowledge the alarms using command interface	Supported from X14.0.1
Redirect URI support for SSO/OAuth sign-in	Supported from X14.0
AV1 Support	Supported from X14.0
XCP support for “Jabber Zero Downtime”	Supported from X14.0
Escalation from P2P to Meeting	Supported from X14.0
Expressway Cluster load balancing not applicable to SIP Federation	Supported from X14.0
MRA SIP Registration Failover for Cisco Jabber	Supported from X14.0
MRA Mobile Application Management clients	Preview
Android Push Notifications for IM&P	Preview (disabled by default from X12.6.2)
Headset Capabilities for Cisco Contact Center	Preview

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.

Table 4: Deprecated and Withdrawn Features

Feature / Software	Status
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** 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

Feature / Software	Status
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 an Multiline Telephone System (MLTS). Customers that need to comply with the requirements of Ray Baum's Act should use Cisco Unified Communication Manager in conjunction with Cisco Emergency Responder.

Related Documentation

Table 5: Links to Related Documents and Videos

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 CE1200 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.

Mobile and Remote Access	*Mobile and Remote Access Through Cisco Expressway Deployment Guide* on the Expressway Configuration Guides 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
Cisco Hosted Collaboration Solution (HCS)	HCS customer documentation
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).
Multiway Conferencing	*Cisco TelePresence Multiway Deployment Guide* on the Expressway Configuration Guides page.

Features and Changes in X14.2.2

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 which are not yet available.

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

Security Enhancements

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.

Upload files along /tmp/ path

You must upload files along **/tmp/** path to keep the file upload process secure.

For example, Consider the following command. Use **/tmp/** at the beginning of the path:

```
xcommand Passworddictionarywrite /tmp/random_file
```

Enable DOS Protection for TrafficServer

There are default rate limits set for new connections on SIP and EDGE traffic categories Management category is also included in a monitoring capacity allowing visibility and logging of connection events above the configured level.

Approved Cryptographic Primitives and Parameters

Expressway does not support Anonymous Diffie Hellmen (ADH) cipher for SIP services, so TC/CE endpoints must enable certificate for SIP (Self-signed Certificate must be in *On* mode).

Management Enhancements

Smart Licensing

Cisco Smart Software Licensing is a new way to think about licensing.

Note Cisco Expressway Release X14.2 and later **only** supports Smart Licensing and is capped at 2500 encrypted signaling sessions to endpoints. It also includes changes in the trafficserver behavior (bug ID CSCwc69661 refers) that can lead to MRA failures - see here. For detailed information, see the *Cisco Expressway and Cisco TelePresence Video Communication Server Release Note (x14.2)* and *Cisco Expressway Administrator Guide (X14.2) before upgrading to X14.2*.

This method is typically managed with the cloud-based Cisco Smart Software Manager (CSSM). Alternatively, deployments that need an on-premises approach can use the Smart Software Manager On Prem product (formerly known as “Smart Software Manager Satellite”).

Smart Licensing provides customers with the flexibility to consume their licenses from any Expressway node or cluster that they have.

You can use Smart Licensing to:

- See the license usage and count.
- See the status of each license type.
- See the product licenses available on Cisco Smart Software Manager or Smart Software Manager On-Prem.
- Renew License Authorization with Cisco Smart Software Manager or Smart Software Manager On-Prem.
- Renew Registration
- Deregister with Cisco Smart Software Manager or Smart Software Manager On-Prem.
- Reregister License with Cisco Smart Software Manager

Important

- Product Activation Keys (PAK) Licensing (Option Keys) are removed from version X14.2.
- Smart License is default and the only licensing mode for Expressway-C and Expressway-E.
- In Smart License mode, the functionality is enabled by default and hence they are not needed or supported and may not be converted in the License Registration Portal.

Types of Cisco Smart License Reservation

Cisco Smart License Reservation is meant to reserve licenses and install them on the device. This process enables you to generate a unique reservation code from your Cisco device, which is then used to reserve a license type and quantity from your Cisco Smart Account's inventory.

The following are the license reservation types:

- **Permanent License Reservation (PLR):** All licenses are reserved.
- **Specific License Reservation (SLR):** Only specific licenses are reserved.

For details on the Cisco Smart License Reservation and Its Types, see the section on *About Cisco Smart License Reservation and Its Types* in Cisco Expressway Administrator Guide (X14.2).

Command Line Interface Updates

The following new CLI commands have been introduced to support this feature:

- `xconfiguration License Smart ReservationEnable: On`
- `xcommand License Smart Reservation Request`
- `xcommand License Smart Reservation Install <authorization code>`
- `xcommand License Smart Reservation Return`
- `xcommand License Smart Reservation ReturnAuthorization <auth code>`
- `xcommand License Smart Reservation Cancel`

Note The following commands are common for both Permanent License Reservation (PLR) and Specific License Reservation (SLR).

For details on the list of CLI Commands for PLR and SLR, see the section on *CLI Commands for PLR and SLR* in Cisco Expressway Administrator Guide (X14.2).

Permanent License Reservation

Permanent License Reservation (PLR) is a part of Cisco smart licensing solution. Smart Licensing needs a smart account. The product must connect to the Cisco Smart Software Management (CSSM) or Smart Software Manage (SSM On-Prem) in order to reactivate and report the most recent license status. You will use Cisco Permanent License Reservation or PLR license if you have extremely secured inner networks with restricted internet access.

You can apply Permanent licenses over evaluation licenses, and also apply it incrementally (that is, you can have multiple permanent licenses, and so on). Its capabilities are designed for highly secure environments, where communication with outside environment is impossible.

For details on how to configure Cisco Permanent License Reservation, see the section on *Permanent License Reservation* in Cisco Expressway Administrator Guide (X14.2).

Specific License Reservation

Specific License Reservation is a feature that is used in highly secure networks with no ability at any time to connect to Cisco Smart Software Manager or Cisco Smart Software Manager On-Prem. It provides a method

for customers to deploy a software license on a device (Product Instance - Expressway) without communicating usage information.

Specific License Reservation allows entitlements, perpetual or term, to be reserved for Cisco Expressway product Instance. A generated authorization code from Cisco Smart Software Manager can be installed on the Expressway product and no regular synchronization is needed if product runs within specified license consumption.

Ability to reserve license on Cisco Smart Software Manager is through Smart Account profile.

For details on how to configure Cisco Specific License Reservation, see the section on *Specific License Reservation* in Cisco Expressway Administrator Guide (X14.2).

Additional Information and Limitations

Expressway in *Specific License Reservation* mode implements the following:

- The licenses are shared across the Expressway nodes in a Cluster.
- License usage is reported to local Smart Agent in the Expressway.

For details on how to configure Cisco Smart Licensing, see the chapter on *Smart Licensing*, section *Additional Information*, *Limitation* in Cisco Expressway Administrator Guide (X14.2).

Configuration Details

For details on how to configure Cisco Smart Licensing, see the chapter on *Smart Licensing* in Cisco Expressway Administrator Guide (X14.2).

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.

Hardware Security Module (HSM) Support - Withdrawn from X14.2 release

The Expressway X12.6 release has added HSM functionality, as a **Preview** feature. (HSM safeguards and manages digital keys for strong authentication and provides crypto-processing for critical functions such as encryption, decryption, and authentication for the use of applications, identities, and databases.)

Although the **Maintenance** > **Security** > **HSM configuration** page is still visible in the Expressway User Interface in this version of Expressway software, this functionality is withdrawn and will be removed from the user interface in the future software releases.

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 are running 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.

Push Notifications with Mobile Application Management Clients - MRA Deployments

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

With this feature, push notification support over Mobile and Remote Access now includes support for Mobile Application Management (MAM) clients like Jabber Intune and Jabber BlackBerry. As a result, the push notification service is available for all devices that are running Jabber Intune and Jabber BlackBerry clients.

Push Notifications with Android Devices – MRA Deployments

This feature applies if you deploy Expressway with MRA. In X12.6 it was introduced in Preview status only, due to external product version dependencies.

In X12.6.2, the feature was switched off by default due to a known issue (bug ID CSCvv12541 refers).

In X12.7, bug ID CSCvv12541 was fixed. However, this feature remains in Preview status for now, due to pending software dependencies.

How to enable push notifications for Android devices

This feature is enabled through the Expressway command line interface. Only do this **if all IM and Presence Service nodes that service Android users are also running a supported release**.

The CLI command is: *xConfiguration XCP Config FcmService: On*

Note IM and Presence services for users who are currently signed in over MRA will be disrupted when this command is used, so those users will need to sign in again.

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 under lab conditions that KEMs with multiple DNs work satisfactorily over MRA. 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`.

Table 6: List of REST API(s)

Configuration APIs	API Introduced In Version
CDB Rest API Access - Enable/Disable CDB REST API Access	X14.2
Service Select Wizard	X14.0.3
Ability to acknowledge active Alarms	X14.0.3
Ban/Unban an IP Address	X14.0.3
Exempt an IP Address	X14.0.3
Call Detail Record (CDR) Configuration	X14.0.3
Status - fail2banbannedaddress	X14.0.2
SNMP Configuration	X14.0.1
Alarms - view and acknowledge	X14.0.1
Dedicated Management Interface (DMI)	X12.7
Diagnostic Logging	X12.6.3
Smart Licensing	X12.6
Clustering	X8.11
Smart Call Home	X8.11
Microsoft Interoperability	X8.11
B2BUA TURN Servers	X8.10
Admin account	X8.10
Firewall rules	X8.10
SIP configuration	X8.10
Domain certificates for Server Name Identification	X8.10
MRA expansion	X8.9
Business to business calling	X8.9
MRA	X8.8

Other Changes in this Release

X14.0.9 and X14.2.1 release(s)

Jabber Over MRA intermittently plays Ringing Tone instead of Busy, when called Extension is Busy

A new CLI command is added that specifies the maximum delay of a SIP REFER message . It contains DtLineBusyTone during initial call dialog (ensure SIP messages proceeds in a sequence) that the server can handle (in milliseconds).

Expressway processes and sends SIP messages (REFER contain DtLineBusyTone parameter and 183 Session Progress), which causes Jabber Over MRA to intermittently play Ringing Tone instead of Busy Tone (bug ID CSCwc27302 refers).

Recommend adjust delay between 100-200 milliseconds.

The CLI command is: **xConfiguration SIP Advanced BusytoneReferDelay: <0..2000>**

X14.2 release

TLS Verification Mode

We have enabled server certificate verification by default when communication happens between VCS(ATS) and CUCM/CUP/JabberGuest/UNITY/CMS. When the customer upgrades to release 14.2, CA of CUCM/CUP/JabberGuest/UNITY/CMS server certificate should be present in VCS CA trust store. If the customer wishes to disable/enable server certificate verification, following is the command.

```
xConfiguration EdgeConfigServer VerifyOriginServer: OFF/ON
```

Smart Licensing Export Compliance

Signaling to no more than 2500 endpoints

Note

- The Export Limit of 2500 registrations/calls/sessions is *On* by default for all customers. This means that now every customer will **not** be able to create more than 2500 encrypted connections.
- Encrypted signaling sessions to endpoints' is capped at 2500.
- 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.

Important There are cases where Expressway does not have sufficient information available to determine if 2 encrypted signaling sessions are from the same endpoint. For example, with Jabber where Expressway sees separate SIP and XMPP registrations (separate encrypted signaling sessions) and is unable to determine if they are from a single endpoint. This is double counted.

So a customer with 2200 Jabber users may think that it is fine to upgrade. But, after upgrading to X14.2, this will be seen as 4400 signaling sessions and they will get registration and calls rejected.

Table 7: Comparison of the Smart Licensing Features Supported in the Product

	Cisco Expressway	Cisco TelePresence Video Communication Server (VCS)	Notes
CAP of 2500 secured/crypto sessions	Yes	Yes	For both platforms regardless of the licensing model (Smart Licensing or PAK) a CAP of 2500 secured/crypto sessions is applicable when upgraded to X14.2 release.
Support Advanced Account Security (AAS) and FIPS140-2 Cryptographic Mode	No	Yes By adding/installing appropriate Option keys you have an option to **enable** AAS and FIPS140-2 feature(s).	
Smart Licensing	Yes	No	For Cisco VCS, Option keys /PAK license mode only

For more information, see Cisco Expressway Administrator Guide (X14.2).

Enabling or Disabling CDB API Access

Considering the Security of the Expressway product, access to CDB API has been disabled by default. They can be enabled or disabled using the Web User Interface or through REST API. You can enable or disable access to CDB REST API using the following REST API: https://%3CIP%20address%3E/api/provisioning/common/cdbrestapiaccess.

For more information, see Cisco Expressway Administrator Guide (X14.2).

Support for 4+1 and 5+1 Redundancy Models

Expressway supports the 4+1 and 5+1 redundancy models. Each cluster can have up to four or five Expressway nodes and a maximum of N+1 physical redundancy.

XCP Routing Table

This improvement displays content of the Extensible Communications Platform (XCP) routing table. This content is a complete data dump of the XCP routing information contained in Cisco Jabber. This information is useful for debugging from the XCP point of view. It is made available both in the **routing.xml** file on the VCS device and in the **developer.xcp.jabber logs**.

Additionally, the ConnectionManager information is also available as a data dump through developer logs. This information displays the state of ConnectedSockets and FailedRequests counters.

All this information will help administrators to check the routing information, the number of connections, and details of each Jabber client connection.

Reducing Email Notifications

The purpose of this improvement is to stop spamming the administrator with emails if, for some reason, multiple alarms are raised over a short period.

If the same alarm is raised two or more times within an hour, emails will be sent only once. If the same alarm gets lowered, and raised again, email will be sent, regardless of the time passed. Obviously, this only applies when the administrator has configured to receive email notifications on a device.

Alternate Method of Using xCommand FIPS

- **Expressway Series**: FIPS functionality is not supported through CLI command and Web User Interface.
- **Cisco VCS**: You must add J00 Option Key in **Maintenance** > **Option keys** in **Add option key** field (or using CLI command). The options available for FIPS (<*leave/enter/status*>) are only visible before adding the JOO Option Key. You can use the JOO Option Key only after it is added.

Note Smart Licensing is FIPS compliant.

Cipher Preferences - ECDSA Cipher Preference Over RSA

ECDSA certificates are preferred over RSA.

Important The following points lists the various upgrade path(s) that are mandatory for upgrading ciphers.

1. When upgrading from version lower than 14.0 to 14.2, the ECDSA would be preferred. If you prefer RSA certificates over ECDSA, then prefix the cipher string with “ECDHE-RSA-AES256-GCM-SHA384:” using either Web User Interface (**Maintenance** > **Security** > **Ciphers**) or CLI command (**xConfiguration Ciphers**).
2. When upgrading from version equal or higher than 14.0 to 14.2 or higher version, you have appended “ECDHE-RSA-AES256-GCM-SHA384:” to the default Ciphers List to prefer RSA certificates over ECDSA. If you prefer ECDSA certificates over RSA, then remove “ECDHE-RSA-AES256-GCM-SHA384:” from the cipher string using Web User Interface (**Maintenance** > **Security** > **Ciphers**) or CLI command (**xConfiguration Ciphers**).
3. Any customer has a fresh install X14.2 image, ECDSA is being preferred. If you prefer RSA certificates over ECDSA, then prefix the cipher string with “ECDHE-RSA-AES256-GCM-SHA384:” using either Web User Interface (**Maintenance** > **Security** > **Ciphers**) or CLI command (**xConfiguration Ciphers**).

TLS 1.3 Support

From X14.2 release onwards, Expressway supports TLS 1.3 for SIP and Reverse proxy functionality.

Auto Created CE Zone Status

Expressway versions prior to X14.0.2 show a status of **Active** for CE zones where the Zone Profile had Monitor Peer status / Neighbor Monitor set to **No** - since the Expressway is not monitoring the peer status for the CE zones, the more accurate status of **Address Resolvable** is indicated.

Auto-created UC zones and associated Unified Communications zone profile are not customizable and Neighbor Monitor set to **No** is by design.

Starting with Expressway X14.0.2, auto-created CE (tcp/tls/OAuth) Zone destined for the UC node will show status as **Address Resolvable** as per a fix for CSCup29823.

Traffic Server Enforces Certificate Verification

Important Before upgrading from pre-X14.0.2 release to X14.2, make sure the following certificate requirement is met.

Due to improvements in the traffic server service in Expressway, beginning in X14.0.2, the following must be in place for MRA.

Requirement - The Certificate Authority (CA) which signed the Expressway-C certificate must be added to the *Tomcat*-trust and *CallManager*-trust list of Cisco Unified Communications Manager (UCM), even if the UCM is in **non-secure** mode. And, restart the following services on CUCM side:

- Tomcat Service
- CallManager Service
- HA Proxy Service (if using TLS on Tomcat)

Reason - The traffic server service in Expressway sends its certificate whenever a server (UCM) requests it. These requests are for services running on ports other than 8443 (for example, ports 6971, 6972, and so on). This enforces certificate verification even if UCM is in non-secure mode.

For more information, see Mobile and Remote Access Through Expressway Deployment Guide.

Known Issue(s) and Workaround(s)

Upgrade failure due to "Unique index collision" error

From X14.2.1 release, duplicate entries are not allowed in the CDB table **serviceConfiguration**. Due to this, upgrades from a previous version (which have duplicate entries in 'serviceConfiguration' table) fail with the below error.

Error: Upgrade fails with the following error in developer logs.

```
"Unique index collision: The value already exists in the table"
Table="serviceConfiguration""
```

Cause: A 'UNIQUE' qualifier is introduced on the 'name' field of the table.

Due to this, upgrades from any previous version (which have duplicate entries in the 'serviceConfiguration' table) to a version higher or equal to X14.2.1 fails with a unique index collision error.

Solution: For technical assistance, contact Cisco Technical Assistance Center (TAC) team for a workaround script to delete duplicate entries before retrying the upgrade (bug ID CSCwd38155 refers).

Troubleshooting

CUCM Cipher Interop with Expressway

Servers during Transport Layer Security (TLS) handshake send Rivest Shamir Adleman (RSA)/Elliptic Curve Digital Signature Algorithm (ECDSA) ciphers. Expressway, as a client, can accept these ciphers.

Note Fresh install of Expressway comes default with ECDSA ciphers.

Expressway can negotiate an ECDSA cipher request.

Remember

- Certificate cipher with RSA, UCM sends either a *CallManager* or a *Tomcat* certificate.
- Certificate cipher with ECDSA, UCM sends either a *CallMananager-ECDSA* or a *Tomcat-ECDSA* certificate.
- Users must sequentially upload, to Expressway-C, signed Unified Call Manager (UCM) certificates as trusted Certificate Authority (CA) to verify the received certificate from UCM.

Reference Information

- **For Cipher Configuration:** Configuring ECDSA followed by RSA ciphers.

```
ECDHE-ECDSA-AES128-GCM-SHAdefault:ECDHE-ECDSA-AES128-SHAdefault:ECDHE-ECDSA-
AES128-SHA:ECDHE-ECDSA-AESdefault-GCM-SHA384:ECDHE-ECDSA-AESdefault-
AES128-SHA:ECDHE-ECDSA-AESdefault-GCM-SHA384:ECDHE-ECDSA-AESdefault-
GCM-SHA384
```

- **For Configuration in Expressway**

  Add the below Ciphers under **Maintenance** > **Security** > **Ciphers**.

Note The following cipher change is required to send ECDSA as a high preference.

```
EECDH:EDH:HIGH:-
AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH
```

Limitations

Smart Licensing Export Compliance

Export Restricted Functionality - Signaling to more than 2500 endpoints

Note The following aspects is in context of the Cisco Expressway X14.2 release.

Cisco Expressway X14.2 release is a **Unlimited** and **Capped** version with a CAP of 2500 secured sessions.

Note: CAP of 2500 secured sessions is also applicable to Cisco TelePresence Video Communication Server (VCS) Series.

Some Expressway Features are Preview or Have External Dependencies

We aim to provide new Expressway features as speedily as possible. Sometimes it is not possible to officially support a new feature because it may require updates to other Cisco products which 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 "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 the open and resolved issues in this release.

- All open issues, sorted by date modified (recent first)
- Issues resolved by X14.2.2
- Issues resolved by X14.2.1
- Issues resolved by X14.2

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 appears, 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 on a specific software version.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

Obtaining Documentation and Submitting a Service Request

Use the Cisco Notification Service to create customized flexible notification alerts to be sent to you via email or by RSS feed.

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.