



Cisco Expressway Release Note (X14.0.4)

First Published: 2021-12-01

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1

About the Documentation 1

Change History 1

Supported Platforms 2

Notices Relating to Deploying OVA with VMware 7.0 U2 3

Notices Relating to VCS Product Support 3

Notices Relating to Hardware Support for CE1200, CE1100, CE1000, and CE500 Appliances 3

Interoperability and Compatibility 3

Product Compatibility Information 3

Which Expressway Services Can Run Together? 4

Feature Summary for X14.0.4 4

Withdrawn or Deprecated Features and Software 5

No Support for Ray Baum's Act 6

Related Documentation 6

Features and Changes in X14.0.4 7

Security Enhancements 7

Preview Features 9

(Preview) Hardware Security Module (HSM) Support 9

(Preview) Headset Capabilities for Cisco Contact Center – MRA Deployments 10

(Preview) Push Notifications with Mobile Application Management clients - MRA Deployments 10

(Preview) Push Notifications with Android Devices – MRA Deployments 10

(Preview) KEM Support for Compatible Phones - MRA Deployments 10

REST API Changes 11

Other Changes 12

About Cisco Expressway Licensing 13

How Smart Licensing Works 15

Important Configuration Information for Smart Licensing	15
Open and Resolved Issues	16
Bug Search Tool Links	16
Notable Issues in this Version	16
Limitations	17
Some Expressway Features are Preview or Have External Dependencies	17
Unsupported Functionality	17
Expressway TURN does Not Operate as a STUN Server	17
Cisco Webex Hybrid Call Service	18
Product License Registration - Issue with Converting to Smart Licensing	18
Redirect URI Support	18
Static NAT for Clustered Systems	18
MRA Limitations	18
MRA SIP Registration Failover	19
MRA OAuth Token Authorization with Endpoints / Clients	19
Spurious Alarms when Adding or Removing Peers in a Cluster	20
Virtual Systems	20
CE1200 Appliance	20
Medium Appliances with 1 Gbps NIC - Demultiplexing Ports	20
Language Packs	21
XMPP Federation-Behavior on IM&P Node Failure	21
Cisco Webex Calling May Fail with Dual-NIC Expressway	21
Microsoft Federation with Dual Homed Conferencing-SIP Message Size	21
Intradomain Microsoft Interop with Expressway and Cisco Meeting Server	21
Licensing Behavior with Chained Expressway-Es	22
Smart Licensing not Available With Features that Use Option Keys (including HSM)	22
HSM Support	22
Option Keys Only Take Effect for 65 Keys or Fewer	23
TURN Servers	23
Upgrading Expressway to X14.0.4	23
Summary	23
Prerequisites and Software Dependencies	23
Upgrade Instructions	26
Before You Begin	26

Process to Upgrade a Standalone System	27
What Next?	28
Process to Upgrade a Clustered System	29
What Next?	30
Using Collaboration Solutions Analyzer	31
Getting Started	31
Using the Bug Search Tool	31
Obtaining Documentation and Submitting a Service Request	32
Appendix 1: Configuring HSM Devices on Expressway	32
Important: Read this First	32
How to Enable and Manage HSM	32
Task 1: Configure Prerequisites	32
Task 2: Enable HSM on Expressway	33
Task 3: Monitor HSM Status Check	34
Task 4: Next Steps - Generate and Install the HSM Private Key	35
How to Delete Modules	35
How to Disable HSM	35
Appendix 2: Post-Upgrade Tasks for MRA Deployments	36
To Reconfigure the MRA Access Control Settings	36
Settings for MRA Access Control	37
MRA Access Control Values Applied by the Upgrade	41



CHAPTER 1

About the Documentation

- [Change History](#), on page 1
- [Supported Platforms](#), on page 2
- [Interoperability and Compatibility](#), on page 3
- [Feature Summary for X14.0.4](#), on page 4
- [Withdrawn or Deprecated Features and Software](#), on page 5
- [No Support for Ray Baum's Act](#), on page 6
- [Related Documentation](#), on page 6
- [Features and Changes in X14.0.4](#), on page 7
- [About Cisco Expressway Licensing](#), on page 13
- [Open and Resolved Issues](#), on page 16
- [Limitations](#), on page 17
- [Upgrading Expressway to X14.0.4](#), on page 23
- [Using Collaboration Solutions Analyzer](#), on page 31
- [Using the Bug Search Tool](#), on page 31
- [Obtaining Documentation and Submitting a Service Request](#), on page 32
- [Appendix 1: Configuring HSM Devices on Expressway](#), on page 32
- [Appendix 2: Post-Upgrade Tasks for MRA Deployments](#), on page 36

Change History

Table 1: Change History

Date	Change	Reason
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

Date	Change	Reason
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
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)

Notices Relating to Deploying OVA with VMware 7.0 U2



Note This is a known issue in the current release. Deploying X14.0.4 OVA shows "Invalid Certificate" on vCenter 7.0 U2 version of VMware, though it shows "Trusted Certificate" in older versions. Refer to this [Knowledge Article](#) for more information about the issue.

Notices Relating to 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](#).

This notice does not affect the Cisco Expressway Series product.

Notices Relating to Hardware Support for CE1200, CE1100, CE1000, and CE500 Appliances

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



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 for the CE1100 by 3 months, that is, from November 14, 2021 to February 14, 2022.

Please ignore the warning “**unsupported hardware**” in the UI.

CE1100 appliance - end-of-sale and advance notice of hardware service support withdraw

As of 13 November 2018, you cannot order the CE1100 appliance from Cisco. Cisco will withdraw hardware support services for the appliance in a future release. See the [End-of-sale announcement](#) for important dates in the lifecycle of this 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 X14.0.4

Note This table is subject to change.

Table 3: Features by Release Number

Feature / Change	Status
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
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

Feature / Change	Status
Expressway Cluster load balancing not applicable to SIP Federation	Supported from X14.0
MRA SIP Registration Failover for Cisco Jabber	Supported from X14.0
Hardware Security Module (HSM) Support	Preview
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
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
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 MLTS (Multiline Telephone System). 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	<i>Cisco Expressway Virtual Machine Installation Guide</i> on the Expressway Installation Guides page.
Installation - physical appliances	<i>Cisco Expressway CE1200 Appliance Installation Guide</i> on the Expressway Installation Guides page.
Basic configuration for single-box systems	<i>Cisco Expressway Registrar Deployment Guide</i> on the Expressway Configuration Guides page.
Basic configuration for paired-box systems (firewall traversal)	<i>Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide</i> on the Expressway Configuration Guides page.
Administration and maintenance	<i>Cisco Expressway Administrator Guide</i> on the Expressway Maintain and Operate Guides page (includes Serviceability information).
Clustering	<i>Cisco Expressway Cluster Creation and Maintenance Deployment Guide</i> on the Expressway Configuration Guides page.
Certificates	<i>Cisco Expressway Certificate Creation and Use Deployment Guide</i> on the Expressway Configuration Guides page.
Ports	<i>Cisco Expressway IP Port Usage Configuration Guide</i> on the Expressway Configuration Guides page.
Mobile and Remote Access	<i>Mobile and Remote Access Through Cisco Expressway Deployment Guide</i> on the Expressway Configuration Guides page.
Cisco Meeting Server	<p><i>Cisco Meeting Server with Cisco Expressway Deployment Guide</i> on the Expressway Configuration Guides page.</p> <p><i>Cisco Meeting Server API Reference Guide</i> on the Cisco Meeting Server Programming Guides page.</p> <p>Other <i>Cisco Meeting Server Guides</i> are available on the Cisco Meeting Server Configuration Guides page.</p>

Cisco Webex Hybrid Services	Hybrid services knowledge base
Cisco Hosted Collaboration Solution (HCS)	HCS customer documentation
Microsoft infrastructure	<i>Cisco Expressway with Microsoft Infrastructure Deployment Guide</i> on the Expressway Configuration Guides page. <i>Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet</i> on the Expressway Configuration Guides page.
Rest API	<i>Cisco Expressway REST API Summary Guide</i> on the Expressway Configuration Guides page (high-level information only as the API is self-documented).
Multiway Conferencing	<i>Cisco TelePresence Multiway Deployment Guide</i> on the Expressway Configuration Guides page.

Features and Changes in X14.0.4

Security Enhancements

Various security-related improvements 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.

X14.0.4 release

RedSky E911 Location Services Support in Expressway: As part of this change, Expressway will passthrough SIP headers (needed for RedSky feature) - Geolocation, Geolocation-Routing, and RedSky-CustomerID. The SIP header value for Geolocation will be masked in all Expressway logs for security reasons.

X14.0.3 release

- Cisco has released software updates that addresses the following vulnerabilities.
 - **Remote Code Execution Vulnerability:** A vulnerability in the Web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) can allow an authenticated, remote attacker to execute arbitrary code on the underlying operating system as the *root* user.

This vulnerability occurs due to incorrect handling of certain crafted software images that are uploaded to the affected device. An attacker can authenticate the system as an administrative user and exploit this vulnerability. The attacker can then upload specific crafted software images to the affected device. A successful exploit can allow the attacker to execute arbitrary code on the underlying operating system as the *root* user.
 - **Image Verification Vulnerability:** A vulnerability in the image verification function of the Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) can allow an authenticated, remote attacker to execute code with internal user privileges on the underlying operating system.

The vulnerability occurs due to insufficient validation of the content of upgrade packages. An attacker can upload a malicious archive to the **Upgrade** page of the **Administrative Web Interface** and exploit this vulnerability. A successful exploit can allow the attacker to execute code with *user-level* privileges (the **_nobody** account) on the underlying operating system.

- Mobile and Remote Access (MRA) supports WiFi to LTE handoff and vice-versa on Webex App.

X14.0.2 release

- The Install Wizard can start SSH Service on port 22 (standard SSH port) to set the *root* and *admin* password.
- Alarm to indicate that certificates have expired.

X14.0.1 release

- Multiple Admin Accounts and Groups can have CLI access. For more information, see [About the administrator account and field references](#).
- Two new alarms have been introduced in the trust store and onboarding trust store to notify the administrator.
 - Alarm to indicate that certificate is going to expire in next 21 days.

X14.0 release

- Admins now have the flexibility to configure SSH ciphers on TCP port 22 which is configurable from the web interface, without needing to use CLI commands to update the Expressway SSH configuration.
- To meet Cisco Product Security Baseline, the cipher filters for the following services are updated:
 - SSL ciphers used by Reverse proxy
 - SSL ciphers used by Apache
 - SSL ciphers used by UC Service Discovery
 - SSL ciphers used by XMPP
 - SSL ciphers for LDAP
- To meet Cisco Product Security Baseline, the crypto algorithms of the SSH Key Configuration are updated. Some disallowed key exchange algorithms are removed:
 - ecdh-sha2-nistp521
 - ecdh-sha2-nistp384

The following key exchange algorithms are added:

- ecdh-sha2-nistp256
- diffie-hellman-group14-sha256
- diffie-hellman-group14-sh1

- Expressway-E is exposed to silent SIP scans (using SIP OPTIONS) and spam calls (using SIP INVITE). This is similar to a DoS attack. To protect from this SIP based DOS attack, SIP Authentication Failure on Fail2Ban is enabled by default for :
 - Fresh Expressway installations from X14.0 and later versions
 - Factory reset with X14.0 or later versions
- But, if you only upgrade SIP-Auth ban it will remain in the same enabled/disabled state as before your upgrade.
- You can configure the Rate Limits for SIP transaction. From the Web UI, you can enable/disable or change number of connections per second and Burst limit values. By default, the connections per second values is 100 and the Burst limit is 20.
 - Automated Protection or the SIP Registration failure detection system is now enhanced to cover the following conditions:
 - License limit exceeded
 - Maintenance mode
 - Not permitted by policy
 - Out of resource
 - Registration not allowed
 - When an Expressway VM is running on sub-spec hardware with a slow CPU and low memory, an unsupported/non-compliant hardware warning alarm is displayed.
 - As part of the enhancements to CUCM/Phone security feature support over MRA, port 6971 is added on the HTTPS allow list for OAuth enabled MRA client to download the configuration file.

Preview Features

Preview Features Disclaimer

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.

(Preview) Hardware Security Module (HSM) Support

From X12.6 release, Expressway supports HSM functionality, on a Preview basis only. 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. An HSM device comes as a plug-in card or an external device that attaches directly to your computer or network server. It prevents hardware and software tampering—by raising alarms or by making the HSM inoperable.

A new **Maintenance > Security > HSM configuration** page is added to the Expressway web user interface.

Expressway currently only supports the nShield Connect XC from Entrust as an HSM provider (on a Preview basis).



Important The “SafeNet Luna” network device from Gemalto is also referenced in the Expressway user interface but, **this device is not currently supported by Expressway.**

(Preview) 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](#).

(Preview) 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.

(Preview) 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.

(Preview) 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
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

Configuration APIs	API introduced in version
Domain certificates for Server Name Identification	X8.10
MRA expansion	X8.9
Business to business calling	X8.9
MRA	X8.8

Other Changes

X14.0.2 release

Prior to X14.0.2 showed 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.

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 X14.0.4, 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 - Upload the Complete Certificate Authority (CA) chain of trust including any Certificate Authority provided intermediate certificates 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](#).

About Cisco Expressway Licensing

Cisco Expressway supports two licensing modes:

- **PAK-based licensing.** The classic, traditional method uses option keys (also known as Product Activation Keys) to install licenses on Expressway. Option keys are not just used for licenses, but also to enable certain features and services.
- **Smart Licensing.** 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. In contrast, traditional PAK-based licensing “locks” the licenses to an individual node or cluster.

Only one licensing mode is supported at any time on any Expressway node or Expressway cluster.



Warning

Support for PAK-based licensing will be removed in an upcoming release of Expressway, along with a recommendation to plan its migration to Smart Licensing.

Expressway is set to PAK-based licensing by default. You switch to Smart Licensing from the web interface (**Maintenance > Smart licensing**). Switching back to PAK needs a factory reset.

The following options are supported in both PAK-based licensing mode and Smart License mode. You can convert these PAK-based options to Smart in the [License Registration Portal](#).

Table 7: Option Keys Supported in Either License Mode

PID	Key	Option
LIC-EXP-RMS * 1	116341Yn-m- #####	Rich Media Session licenses
LIC-EXP-DSK (includes LIC-EXP-DSK-EA)	116341Bn-m- #####	Expwy Desktop system registration licenses / UC Manager Enhanced licenses
LIC-EXP-ROOM (includes LIC-EXP-ROOM-EA)	116341An-m- #####	Expwy Room system registration licenses / UC Manager TP Room licenses

¹ Includes LIC-EXP-RMS-CPW, LIC-EXP-RMS-HCS, LIC-EXP-RMS-MIG, LIC-EXP-RMS-PMP, LIC-EXP-RMS-EA & LIC-EXP-RMS=

The following keys are not needed (from X12.5.4) and the functionality is enabled by default. If running in PAK based licensing mode they are not needed, but it will do no harm to apply the keys.



Note 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](#).

Table 8: Option Keys Not Needed in Either License Mode

PID	Key	Option
LIC-SW-EXP-K9	16 digit number	Release Key
LIC-EXP-SERIES	116341E00-m- #####	Expressway Series
LIC-EXP-TURN	116341In-m- #####	TURN relay licenses (Expressway-E only)
LIC-EXP-E	116341T00-m- #####	Traversal Server feature (Expressway-E only)
LIC-EXP-GW	116341G00-m- #####	Interworking Gateway feature
LIC-EXP-AN	116341L00-m- #####	Advanced Networking Feature (Expressway-E only)



Note If you use any of the following keys, **do not switch from PAK-based licensing to Smart License mode**, as the functionality is not yet supported in Smart License mode.

Table 9: Option Keys Currently Supported in PAK-based Mode Only

PID	Key	Option
LIC-EXP-JITC=	116341J00-m- #####	Advanced Account Security feature
LIC-EXP-HSM	116341H00-m- #####	Hardware Security Module feature (this is currently in Preview status only)
LIC-EXP-MSFT	116341C00-m- #####	Microsoft Interoperability

How Smart Licensing Works

Smart Licensing is available across multiple Cisco products. It simplifies licensing and makes license ownership and consumption clearer. Devices self-register and report license consumption, which removes the need to use option keys (Product Activation Keys). License entitlements are pooled in a single account that can be used across Expressways or across different clusters of Expressways. You can use a license on any compatible device owned by your company and move them around to meet the needs of your organization.

You use Smart Licensing to register/deregister Expressway with CSSM (or the Smart Software Manager On-Prem) to view license usage, count, and status per license type, and to renew license authorizations. CSSM is hosted on the [Cisco Software Manager](#) and allows product instances to register and report license consumption to it.

On-premises approach - using Smart Software Manager On-Prem

If you do not want to manage Cisco products directly using Cisco Smart Software Manager, either for policy or network availability reasons, the Smart Software Manager On-Prem is available. Products register and report license consumption to the Smart Software Manager On-Prem in the same way as with Cisco Smart Software Manager.

Smart Software Manager On-Prem can be deployed in either Connected or Disconnected mode, depending on whether the satellite can connect directly to cisco.com.

- **Connected.** Used when there is direct connectivity to cisco.com. Smart account synchronization occurs automatically.
- **Disconnected.** Used when there is no direct connectivity to cisco.com. Smart Account synchronization must be manually uploaded and downloaded.

Important Configuration Information for Smart Licensing



Caution

After Smart Licensing is set to *On* you cannot reset to *Off* using the web interface. To go back to PAK-based licensing (or to change the system to a VCS) requires a factory reset. Because the reset will reinstall the software image and reset the Expressway configuration to the default, we strongly advise you to backup the Expressway data before you enable Smart Licensing.

- After Smart Licensing is enabled, you cannot use option keys on the Expressway. This means that you will not be able to apply option keys to use Advanced account security, Hardware Security Module (HSM), or Microsoft Interoperability (or to add licenses for RMS or room/desktop registrations).
- If you want to deploy HSM devices with the Expressway, you cannot currently use Smart Licensing.
- If a communication issue occurs with the registration server when you register the Expressway product instance, the registration fails with this message:

```
The last attempt to renew smart software licensing registration is in progress because of the following reason: HTTP Server Error 200: Operation timed out.
```

The product instance reattempts to register at 15-minute intervals. Refresh the page on your browser after each reattempt, to check current registration status. If the communication issue is resolved during

the reattempts, the product will be registered. If the product is not registered after multiple reattempts, verify if there is any communication issue with the registration server and manually reregister the product instance.

- When you restore a system, the Smart Licensing settings that are restored depends on whether you restore the backup onto the same system or on a different system.
 - If you restore on the same system, Smart Licensing will be enabled and the registration settings are restored on the restored system.
 - If you restore on a different system, Smart Licensing will be enabled on the restored system but you must register the product again with a registration key.

More details

For detailed product information about the Cisco Smart Software Manager, see [Cisco Smart Software Manager](#). Or for information about the on-prem manager, see [Smart Software Manager On-Prem](#).

For more information about how to configure Smart Licensing, see the *Cisco Expressway Administrator Guide*.

Open and Resolved Issues

Bug Search Tool Links

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 X14.0.4](#)
- [Issues resolved by X14.0.3](#)
- [Issues resolved by X14.0.2](#)
- [Issues resolved by X14.0.1](#)
- [Issues resolved by X14.0](#)

Notable Issues in this Version

Rich Media Session license is not consumed by Single NIC Expressway-E hosting Jabber Guest service

[CSCva36208](#)

Changes to the licensing model in X8.8 revealed an issue with licensing of the Jabber Guest service on the Expressway-E server. When the Expressway pair is part of the “Single NIC” Jabber Guest deployment, the Expressway-E should count one RMS license for each Jabber Guest call, but it does not. This issue may cause confusion about the server's load, because usage appears low even when the server is processing multiple calls.

We recommend the Dual NIC Jabber Guest deployment. If you are using single NIC deployment, make sure the Expressway-E is correctly licensed to ensure continuity of service with future upgrades.

Limitations

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). Occasionally we may recommend that a feature is not used until further updates are made to Expressway or other products. Expressway features which are provided in preview status only in this release, are listed in these notes.

Unsupported Functionality

Currently, if one Expressway node in a clustered deployment fails or loses network connectivity for any reason, or if the Unified CM restarts, all active calls going through the affected node will fail. The calls are not handed over to another cluster peer. This is not new behavior in X12.5.x, but due to an oversight it was not documented in previous releases. Bug ID [CSCtr39974](#) refers.

Expressway does not terminate DTLS. We do not support DTLS for securing media and SRTP is used to secure calls. Attempts to make DTLS calls through Expressway will fail. The DTLS protocol is inserted in the SDP but only for traversing the encrypted iX protocol.

From X12.5, Expressway provides limited SIP UPDATE support over MRA connections for session refresh purposes only, as specified by RFC [4028](#). However, you should not switch this on unless you have a specific requirement to use this capability. Any other use of SIP UPDATE is not supported and features that rely on this method will not work as expected.

Cisco VCS does not support the SIP UPDATE method ([RFC 3311](#)), and features that rely on this method will not work as expected.

Audio calls may be licensed as video calls in some circumstances. Calls that are strictly audio-ONLY consume fewer licenses than video calls. However, when audio calls include non-audio channels, such as the iX channel that enables ActiveControl, they are treated as video calls for licensing purposes.

Expressway TURN does Not Operate as a STUN Server

From X12.6.1, due to security enhancements, the Expressway-E TURN server no longer functions as a generic STUN server and will not accept unauthenticated STUN binding requests.

This leads to the following scenarios:

- **Scenario A:** If you use the B2BUA as a TURN client for Microsoft interoperability (as described in the *Cisco Expressway with Microsoft Infrastructure Deployment Guide*) the B2BUA will not send any STUN binding requests to the TURN server to check if it is alive or not. This means that from Expressway X12.6.1, the B2BUA may try to use a TURN server that is not reachable and hence that **calls may fail**.

- **Scenario B:** If you use Meeting Server WebRTC with Expressway (and Expressway-E is configured as a TURN server) before you install Expressway X12.6.1 or later, first upgrade the Meeting Server software to version 3.0 or to a compatible maintenance release in version 2.9.x or 2.8.x. Bug ID CSCvv01243 refers. This requirement is because other Meeting Server versions use STUN bind requests towards the TURN server on Expressway-E (For more information about Expressway-E TURN server configuration, see the *Cisco Expressway Web Proxy for Cisco Meeting Server Deployment Guide*).

Cisco Webex Hybrid Call Service

Expressway X12.6 and later does not work for hosting the Call Connector software that is required in a Hybrid Call Service deployment and you need to use an earlier supported version for the Expressway connector host. See the Hybrid Call Service known issues and Expressway version support documentation on <https://help.webex.com/> for more information.

Product License Registration - Issue with Converting to Smart Licensing

This item applies if you want to convert existing Expressway licenses (RMS, Desktop, or Room) to Smart Licensing entitlements. In this case do not use the option in the Cisco Product License Registration portal to partially convert just some of the licenses. Due to a known issue, if you opt to convert only some licenses, the system automatically forfeits/removes the remaining licenses as well. So the licenses that are not converted are also removed, and a licensing case will be required to retrieve them.

To avoid this happening, please ensure that the **Quantity to Convert** field is the same value as the **Quantity Available** field; this is the default when you open the page.

Redirect URI Support

This feature will not work when in a cluster deployment, Expressway-E observes two different source IP addresses. For example, Jabber or Webex client on mobile has an IP address different than that of the external browser on the mobile. This may be due to:

- There is change in IP address during mobile roaming
- If user is behind firewall configured for NAT with multiple public IP address
- Split VPN configuration

Static NAT for Clustered Systems

From X12.5.5, support for static NAT functionality on TURN is extended to clustered systems (support for standalone systems was introduced in X12.5.3). However, peers which are configured as TURN servers must be reachable using the private addresses for their corresponding public interfaces.

MRA Limitations

If you use Expressway for Mobile and Remote Access (MRA), some unsupported features and limitations currently exist. A list of key unsupported features that we know do not work with MRA is detailed in *Key Supported and Unsupported Features with Mobile and Remote Access* in the [Mobile and Remote Access Through Cisco Expressway Guide](#).

For details of which 7800/8800 Series phones and other endpoints support MRA, see the *MRA Requirements* section of the *Mobile and Remote Access Through Cisco Expressway Guide*.

SIP UPDATE for session refresh support over MRA has some limitations. For example, the following features that rely on the SIP UPDATE method ([RFC 3311](#)) will fail:

- Request to display the security icon on MRA endpoints for end-to-end secure calls.
- Request to change the caller ID to display name or number on MRA endpoints.

MRA SIP Registration Failover

OAuth Token Refresh will not happen when 7800/8800 series phones and other endpoints such as Jabber renew the OAuth Token on CUCM subscriber which issued the OAuth Token initially but is not reachable during Token Refresh.

To enable OAuth Token Refresh on -

- Jabber - Re-login to Jabber
- 7800/8000 Series phones - Reset the phones.

Expressway will not be able to load balance existing MRA registrations if more than 1 Expressway node in cluster is unreachable.

When an Expressway-E or Expressway-C node, where the Jabber client is registered goes out of service, then the Jabber MRA client automatically moves the registration to an alternate path. Also, when the Expressway-E or Expressway-C node comes back online, the existing load does not get distributed to the node. This would mean that some of Expressway node may be used higher than the other.

MRA OAuth Token Authorization with Endpoints / Clients

In standard MRA mode (no ICE) regardless of any MRA access policy settings configured on Unified CM, Cisco Jabber users will be able to authenticate by username and password or by traditional single sign-on in the following case:

- You have Jabber users running versions before 11.9 (no refresh token support) and Expressway is configured to allow non-token authentication.

In ICE passthrough mode, the ICE MRA call path must be encrypted end-to-end (see *Signaling Path Encryption Between Expressway-C and Unified CM* in the [Expressway MRA Deployment Guide](#)). Typically for end-to-end encryption, Unified CM must be in mixed mode for physical endpoints. For Jabber clients however, you can achieve the end-to-end encryption requirement by leveraging SIP OAuth with Unified CM clusters that are not in mixed mode.



Note You must enable SIP OAuth if the Unified CM is not in mixed mode, but SIP OAuth is not required for Jabber if you're able to register using standard secure profiles.

More information is in the *Configure MRA Access Control* section of the *Expressway MRA Deployment Guide* and in the *Deploying OAuth with Cisco Collaboration Solution Release 12.0* White Paper.

Spurious Alarms when Adding or Removing Peers in a Cluster

When a new peer is added to a cluster, the system may raise multiple 20021 Alarms (*Cluster communication failure: Unable to establish...*) even if the cluster is in fact correctly formed. The alarms appear on the existing peers in the cluster. The unnecessary alarms are typically lowered after at least 5 minutes elapses from the time that the new peer is successfully added.

These alarms also occur if a peer is removed from a cluster. This is generally valid alarm behavior in the case of removing a peer. However, as in the case of adding a peer, the alarms may not be lowered for 5 minutes or more.

Virtual Systems

- This issue applies to Expressways running as virtualized systems with certain ESXi versions using VMWare vCenter 7.0.x. It was found during testing using VMWare vCenter 7.0.1 with ESXi 6.7.0 to deploy an Expressway OVA. The *Ready to complete* final page of the *Deploy OVF Template* wizard displays template values instead of the actual values entered on the earlier wizard pages. The issue is cosmetic, and when you click “FINISH” the OVA will deploy as expected using the entered values. Bug ID CSCvw64883 refers.
- Video calling capacity may be restricted if the ESXi Side-Channel-Aware Scheduler is enabled, and CPU load exceeds 70%.
- With physical Expressway appliances, the **Advanced Networking** feature allows the speed and duplex mode to be set for each configured Ethernet port. You cannot set port speeds for virtual machine-based Expressway systems.

Also, virtual machine-based systems always show the connection speed between Expressway and Ethernet networks as 10000 Mb/s, regardless of the actual physical NIC speed. This is due to a limitation in virtual machines, which cannot retrieve the actual speed from the physical NIC(s).

CE1200 Appliance

- Specific requirements for the X710 firmware version exist, which may change depending on the current versions available. Please check the *Expressway CE1200 Installation Guide*, in the section “Required Firmware Version” for the latest details.
- The appliance requires the minimum Expressway software version detailed in the *Cisco Expressway CE1200 Installation Guide* (the version depends on the appliance revision). Although the system does not prevent downgrades to an earlier software version, Cisco does not support appliances on earlier versions.
- The Expressway allows you to add or delete Traversal Server or Expressway Series keys through the CLI, but in practice these keys have no effect in the case of CE1200 appliances (or for VM-based systems running X12.6 and later). The service setup web UI page now manages changes to the type (Expressway-C or Expressway-E) or the series (Cisco Expressway or Cisco VCS).

Medium Appliances with 1 Gbps NIC - Demultiplexing Ports

If you upgrade a Medium appliance with a 1 Gbps NIC to X8.10 or later, Expressway automatically converts the system to a Large system. This means that Expressway-E listens for multiplexed RTP/RTCP traffic on

the default demultiplexing ports for Large systems (36000 to 36011) and not on the demultiplexing ports configured for Medium systems. In this case, the Expressway-E drops the calls because ports 36000 to 36011 are not open on the firewall.

Workaround

From X8.11.4 you can manually change the system size back to Medium, through the **System > Administration settings** page (select *Medium* from the **Deployment Configuration** list).

Before X8.11.4, the workaround is to open the default demultiplexing ports for Large systems on the firewall.

Language Packs

If you translate the Expressway web user interface, new Expressway language packs are available from X8.10.3. Older language packs do not work with X8.10.n software (or X8.9.n). Instructions for installing or updating the packs are in the *Expressway Administrator Guide*.

XMPP Federation-Behavior on IM&P Node Failure

If you use XMPP external federation, be aware that if an IM and Presence Service node fails over to a different node after an outage, the affected users are not dynamically moved to the other node. Expressway does not support this functionality, and it has not been tested.

Cisco Webex Calling May Fail with Dual-NIC Expressway

This issue applies if you deploy Expressway with a dual-NIC Expressway-E. Cisco Webex Calling requests may fail if the same (overlapping) static route applies to both the external interface and the interface with the Expressway-C. This is due to current Expressway-E routing behavior, which treats Webex INVITES as non-NAT and therefore extracts the source address directly from the SIP via header.



Note We recommend that you make static routes as specific as possible, to minimize the risk of the routes overlapping.

Microsoft Federation with Dual Homed Conferencing-SIP Message Size

If you use dual homed conferencing through Expressway and Meeting Server with an AVMCU invoked on the Microsoft side, the maximum SIP message size must be set to 32768 bytes (the default) or greater. It's likely that you will need a greater value for larger conferences (that is, from around nine or more participants upwards). Defined via **SIP max size** on **Configuration > Protocols > SIP**.

Intradomain Microsoft Interop with Expressway and Cisco Meeting Server

If you use Meeting Server for Microsoft interoperability, a limitation currently applies to the following intradomain/intracompany scenario:

*You deploy separate Microsoft and standards-based SIP networks in a **single domain** and in a configuration that has an Expressway-E **directly facing** a Microsoft front end server (because you use internal firewalls*

between subnetworks, or for any other reason). For example, Cisco Unified Call Manager in one (sub)network and Microsoft in a second (sub)network, inside the same domain.

In this case we do not generally support Microsoft interoperability between the two networks, and calls between Meeting Server and Microsoft will be rejected.

Workaround

If you are not able to deploy the intradomain networks without an intervening Expressway-E (you cannot configure Meeting Server <> Expressway-C <> Microsoft), a workaround is to deploy an Expressway-C in each subnet, with an Expressway-E to traverse between them. That is:

Meeting Server <> Expressway-C <> Firewall <> Expressway-E <> Firewall <> Expressway-C <> Microsoft

Licensing Behavior with Chained Expressway-Es

If you chain Expressway-Es to traverse firewalls (from X8.10), be aware of this licensing behavior:

- If you connect through the firewall to the Cisco Webex cloud, each of the *additional* Expressway-Es which configure a traversal zone with the traversal client role, will consume a Rich Media Session license (per call). As before, the original Expressway-C and Expressway-E pair do not consume a license.
- If you connect through the firewall to a third-party organization (Business to Business call), *all* of the Expressway-Es in the chain, including the original one in the traversal pair, will consume a Rich Media Session license (per call). As before, the original Expressway-C does not consume a license.

Smart Licensing not Available With Features that Use Option Keys (including HSM)

The following Expressway features are enabled by option keys. Because option keys are incompatible with Smart Licensing, if you need these features, you must use PAK-based licensing and not Smart Licensing:

- Advanced account security
- HSM (Hardware Security Module)
- Microsoft Interoperability

HSM Support

As well as being one of the features that we currently provided in Preview status only, the following additional points apply to HSM support in Expressway:

- Like other features that are enabled by option keys (see previous section) you can't use HSM with Expressways that use Smart Licensing.
- Although the “SafeNet Luna” network device appears in the Expressway user interface, this device is not currently supported by Expressway at all and SafeNet Luna settings must not be configured.

Option Keys Only Take Effect for 65 Keys or Fewer

If you try to add more than 65 option keys (licenses), they appear as normal in the Expressway web interface (**Maintenance > Option keys**). However, only the first 65 keys take effect. Additional keys from 66 onwards appear to be added, but actually the Expressway does not process them. Bug ID [CSCvf78728](#) refers.

TURN Servers

Currently, the TCP 443 TURN service and TURN Port Multiplexing are not supported through the CLI. Use the Expressway web interface to enable these functions (**Configuration > Traversal > TURN**).

Upgrading Expressway to X14.0.4

Summary

Table 10: Summary of tasks in a typical upgrade process

Stage	Task	Where
1	Review the <i>Prerequisites and Software Dependencies</i> and <i>Before You Begin</i> sections below	Release Notes
2	Back up the system	Maintenance > Backup and restore
3	Enable maintenance mode and wait for current calls and registrations to end	Maintenance > Maintenance mode
4	Upload the new software image (“ Upgrade ” option)	Maintenance > Upgrade
5	Install the new software (“ Continue with upgrade ” option)	Maintenance > Upgrade
6	Reboot	From the Upgrade page
7	In clustered deployments repeat for each peer in sequence	-

Prerequisites and Software Dependencies

This section has important information about issues that may prevent the system working properly after an upgrade. Before you upgrade, please review this section and complete any tasks that apply to your deployment.

Expressway systems before X8.11.4 need a two-stage upgrade

If you are upgrading a system which is running software earlier than version X8.11.4, you must first upgrade to an **intermediate release** before you install X14.0.4 software (this requirement applies to all upgrades X8.11.x and later versions). Depending on the existing system version, the upgrade will fail. We recommend upgrading to X8.11.4 as the intermediate release.

Is a release key needed?

A release key is not required to upgrade an Expressway on X8.6.x or later software to this release (from X8.11.4 to X14.0.4 for example). This change was introduced in X12.5.4. (Release keys are still used for Cisco VCS systems.)

All deployments

If you are upgrading from X12.6 or X12.6.1 and use the alarm-based email notifications feature



Note In X12.6.2 the email ID length is limited to 254 characters maximum. Before you upgrade make sure that all destination email IDs are no longer than 254 characters.

We do not support downgrades. Do not install a previous Expressway version onto a system that is running a newer version; the system configuration will be lost.



Note From X8.11.x, when the system restarts after the upgrade it uses a new encryption mechanism. This is due to a unique root of trust for every software installation that was introduced in that release.

X8.8 and later versions are more secure than earlier versions. Upgrading could cause your deployments to stop working as expected, and you must check for the following environmental issues before you upgrade to X8.8 or later:

- **Certificates:** Because certificate validation was tightened up in X8.8, you must verify the following items to avoid validation failures:
 - Try the secure traversal test before and after upgrade (**Maintenance > Security > Secure traversal test**) to validate TLS connections.
 - If Unified Communications nodes are deployed, do they use valid certificates that were issued by a CA in the Expressway-C trust list?
 - If you use self-signed certificates, are they unique? Does the trusted CA list on Expressway have the self-signed certificates of all the nodes in your deployment?
 - Are all entries in the Expressway trusted CA list unique? Remove any duplicates.
 - If **TLS verify mode** is enabled on connections to other infrastructure (always on by default for Unified Communications traversal zone, and optional for zones to Unified Communications nodes), make sure that the hostname is present in the CN or SAN field of the host's certificate. We do not recommend disabling TLS verify mode, even though it may be a quick way to resolve a failing deployment.
- **DNS entries:** Do you have forward and reverse DNS lookups for all infrastructure systems that the Expressway interacts with? From X8.8, you need forward and reverse DNS entries for all Expressway-E systems, so that systems making TLS connections to them can resolve their FQDNs and validate their certificates. If the Expressway cannot resolve system hostnames and IP addresses, complex deployments like MRA may not work as expected after the upgrade.
- **Cluster peers:** Do they have valid certificates? If they are using default certificates you should replace them with (at least) internally generated certificates and update the peers trust lists with the issuing CA.

From X8.8, clustering communications use TLS connections between peers instead of IPSec. By default, TLS verification is not enforced after the upgrade, and an alarm will remind you to enforce it.

How and when rebooting is necessary as part of the upgrade

Upgrading the *System platform* component is a two-stage process. First, the new software image is uploaded onto the Expressway. At the same time, the current configuration of the system is recorded, so that this can be restored after the upgrade. During this initial stage the system will continue running on its existing software version, and all normal system processes will continue.

The second part of the upgrade involves rebooting the system. It is only during the reboot that the Expressway installs the new software version and restores the previous configuration. Rebooting causes all current calls to terminate, and all current registrations to be ended. This means that you can upload the new software at any time, and then wait until a convenient moment (for example, when no calls are taking place) to switch to the new version by rebooting the system. Any **configuration changes made between the software upload and the reboot will be lost when the system restarts** with the new software version.

Upgrades for components other than the *System platform* do not involve a system reboot, although the services provided by that component are temporarily stopped while the upgrade process completes.

Deployments that use MRA

This section only applies if you use the Expressway for MRA (mobile and remote access with Cisco Unified Communications products).

- Minimum versions of Unified Communications infrastructure software apply - some versions of Unified CM, IM and Presence Service, and Cisco Unity Connection have been patched with CiscoSSL updates. Before you upgrade Expressway check that you are running the minimum versions listed in the *Mobile and Remote Access Through Expressway Deployment Guide*.

IM and Presence Service 11.5 is an exception. You must upgrade Expressway to X8.8 or later before you upgrade IM and Presence Service to 11.5.

- Expressway-C and Cisco Expressway-E **should both be upgraded** in the same upgrade “window”/timescale (this is also a general recommendation for non-MRA deployments). We don't recommend operating with Expressway-C and Expressway-E on different versions for an extended period.
- This item applies if you are upgrading a Expressway that is used for MRA, with clustered Unified CMs and endpoints running TC or Collaboration Endpoint (CE) software. In this case you must install the relevant TC or CE maintenance release listed below (or later) before you upgrade the Expressway. This is required to avoid a known problem with failover. If you do not have the recommended TC/CE maintenance release, an endpoint will not attempt failover to another Unified CM if the original Unified CM to which the endpoint registered fails for some reason. Bug ID [CSCvh97495](#) refers.
 - TC7.3.11
 - CE8.3.3
 - CE9.1.2

From X8.10.x, the MRA authentication (access control) settings are configured on Expressway-C and not on Expressway-E as in earlier releases, and default values are applied if it is not possible to retain the existing settings. To ensure correct system operation, after the upgrade reconfigure the access control settings on the Expressway, as described later in these instructions.

Deployments that use FIPS mode cryptography

If the Expressway has FIPS mode enabled, after the upgrade, manually change the default SIP TLS Diffie-Hellman key size from the default 1024 bits, to 2048 or greater, as described later in these instructions.

Deployments that use X8.7.x or earlier with Cisco Unified Communications Manager IM and Presence Service 11.5(1)

X8.7.x (and earlier versions) of Expressway are not interoperable with Cisco Unified Communications Manager IM and Presence Service 11.5(1) and later. This is caused by a deliberate change in that version of IM and Presence Service, which has a corresponding change in Expressway X8.8 and later. To ensure continuous interoperability, upgrade the Expressway systems before you upgrade the IM and Presence Service systems. The following error on Expressway is a symptom of this issue: *Failed Unable to Communicate with <IM&P node address>. AXL query HTTP error "'HTTPError:500'"*

Deployments that use Cisco Webex Hybrid Services

The Management Connector must be up to date before you upgrade Expressway. Authorize and accept any Management Connector upgrades advertised by the Cisco Webex cloud before you try to upgrade Expressway. Failure to do so may cause issues with the connector after the upgrade. For details about which versions of Expressway are supported for hybrid connector hosting, see [Connector Host Support for Cisco Webex Hybrid Services](#).

Upgrade Instructions

Before You Begin

- Do the upgrade when the system has low levels of activity.
- A system upgrade needs a system reboot to complete the process. The reboot will terminate any active calls and registrations.
- For clustered systems, allocate enough time to upgrade all peers in the same upgrade “window”. The cluster will not re-form correctly until the software versions match on all peers.
- Check the **Alarms** page (**Status > Alarms**) and make sure that all alarms are acted upon and cleared. Do this for each peer if you are upgrading a cluster.
- If you are upgrading a VM-based system, use the standard *.tar.gz* software image file. The *.ova* file is only needed for the initial install of Expressway software onto VMware.
- If you use the Expressway for MRA and you upgrade from X8.9.x or earlier to X8.10 or later, note your MRA authentication settings before you upgrade. From version X8.10 the MRA authentication (access control) settings moved from the Expressway-E to the Expressway-C. The upgrade does not preserve the existing Cisco Expressway-E settings, so after the upgrade you need to review them on the Expressway-C and adjust as necessary for your deployment. To access existing MRA authentication settings:
 - a. On the Expressway-E, go to **Configuration > Unified Communications > Configuration** and locate **Single Sign-on support**.



Note The existing value (On, Exclusive, or Off)

- b. If **Single Sign-on support** is set to *On* or *Exclusive*.



Note The current values of these related fields:

- Check for internal authentication availability.
 - Allow Jabber iOS clients to use embedded Safari.
-
- Make sure that all relevant tasks in [Prerequisites and Software Dependencies](#) are complete.

Upgrading Expressway-C and Expressway-E systems connected over a traversal zone

In all cases we recommend that Expressway-C (traversal client) and Expressway-E (traversal server) systems that are connected over a traversal zone **both run the same software version**. For some services such as Mobile and Remote Access, we *require* both systems to run the same version.

However, we do support a traversal zone link from one Expressway system to another that is running the previous feature release of Expressway (for example, from an X12.6 system to an X12.5 system). This means that you do not have to simultaneously upgrade your Expressway-C and Expressway-E systems.

Process to Upgrade a Standalone System



Note Do not use this process if you are upgrading a clustered Expressway; instead use the [Process to Upgrade a Clustered System](#).

Procedure

- Step 1** Sign in to the Expressway web user interface as *admin*.
- Step 2** Back up the Expressway system before you upgrade (**Maintenance** > **Backup and restore**).
- Step 3** Enable maintenance mode so that Expressway does not process any new incoming calls (**Maintenance** > **Maintenance mode**). Existing calls continue until the call is terminated.
- Step 4** Wait for all calls to clear and registrations to timeout.
- To manually remove any calls or registrations that don't clear automatically, use the **Status** > **Calls** page or the **Status** > **Registrations** > **By device** page respectively (SIP calls may not clear immediately).
- Note** You can leave the registration for Conference Factory (if enabled) – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration.
- Step 5** Go to **Maintenance** > **Upgrade** to access the **Upgrade** page.
- Step 6** Click **Browse** and select the software image file for the component you want to upgrade.
- The Expressway automatically detects which component you are upgrading based on the selected software image file.

- Step 7** Click **Upgrade**. This step uploads the software file but does not install it. The upload may take a few minutes to finish.
- Step 8** For upgrades to the **System platform** component, the **Upgrade confirmation** page is displayed:
- a. Check the following details:
 - **New software version** number is as expected.
 - **MD5 hash** and **SHA1 hash** values match the values displayed on the cisco.com page, where you downloaded the software image file.
 - b. Click **Continue with upgrade**. This step installs the new software.

The **System upgrade** page opens and displays a progress bar while the software installs.

A summary of any active calls and registrations is displayed when the software completes installing (the calls and registrations will be lost when you reboot the system in the next step).
 - c. Click **Reboot system**. Any configuration changes made between uploading the software tar file and rebooting, will be lost when the system restarts.

Sometimes the web browser interface times out during the restart process, after the progress bar reaches the end. This may occur if the Expressway carries out a disk file system check – approximately once every 30 restarts.

After the reboot is complete the **Login** page is displayed.
- Step 9** For upgrades to other components (not System platform) the software is automatically installed and no reboot is required.
-

What Next?

If you don't use MRA, the upgrade is now complete, and the Expressway configuration should be as expected. The **Overview** and **Upgrade** pages show the upgraded software version numbers.

If you do use MRA, and you are upgrading from X8.9.x or earlier, reconfigure your MRA access control settings as described in [Appendix 2: Post-Upgrade Tasks for MRA Deployments](#).

If you have components that require option keys to enable them, do this from the **Maintenance > Option keys** page.

If the Expressway has FIPS mode enabled (that is, it's a FIPS140-2 cryptographic system) then from X12.6 you must manually change the default SIP TLS Diffie-Hellman key size from the default 1024 bits, to 2048 or greater. To do this type the following command in the Expressway command line interface (change the value in the final element if you want a key size higher than 2048): *xconfiguration SIP Advanced SipTlsDhKeySize: "2048"*

This step does **not** apply to most systems. It only affects systems with advanced account security configured and FIPS enabled.

Process to Upgrade a Clustered System



Caution To avoid the risk of configuration data being lost and to maintain service continuity, UPGRADE THE PRIMARY PEER FIRST and then upgrade the subordinate peers ONE AT A TIME in sequence.

We recommend upgrading the Expressway-E cluster first, followed by the Expressway-C (in each case start with the primary peer). This ensures that when Expressway-C starts a new traversal session toward Expressway-E, the Expressway-E is ready to process it. Starting with the primary peer, upgrade the cluster peers in sequence as follows:

Procedure

- Step 1** Sign in to the Expressway web user interface as *admin*.
- Step 2** Back up the Expressway before you upgrade (**Maintenance > Backup and restore**).
- Note** If the cluster peers are running different versions of the Expressway, do not make any configuration changes other than the settings required to upgrade. The cluster does not replicate any configuration changes to the subordinate peers that are running on different versions from the primary Expressway.
- Step 3** Enable maintenance mode so that the peer does not process any new incoming calls (**Maintenance > Maintenance mode**). Existing calls continue until the call is terminated. Other peers in the cluster continue to process calls.
- Step 4** Wait for all calls to clear and registrations to timeout.
- To manually remove any calls or registrations that don't clear automatically, use the **Status > Calls** page or the **Status > Registrations > By device** page respectively (SIP calls may not clear immediately).
- Note** You can leave the registration for Conference Factory (if enabled) – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration.
- Step 5** Go to **Maintenance > Upgrade** to access the **Upgrade** page.
- Step 6** Click **Browse** and select the software image file for the component you want to upgrade. The Expressway automatically detects which component you are upgrading based on the selected software image file.
- Step 7** Click **Upgrade**. This step uploads the software file but does not install it. The upload may take a few minutes to finish.
- Step 8** For upgrades to the **System platform** component, the **Upgrade confirmation** page is displayed:
- Check the following details:
 - New software version** number is as expected.
 - MD5 hash** and **SHA1 hash** values match the values displayed on the cisco.com page, where you downloaded the software image file.
 - Click **Continue with upgrade**. This step installs the new software.
The **System upgrade** page opens and displays a progress bar while the software installs.

A summary of any active calls and registrations is displayed when the software completes installing (the calls and registrations will be lost when you reboot the system in the next step).

- c. Click **Reboot system**. Any configuration changes made between uploading the software tar file and rebooting, will be lost when the system restarts.

Sometimes the web browser interface times out during the restart process, after the progress bar reaches the end. This may occur if the Expressway carries out a disk file system check – approximately once every 30 restarts.

Ignore any cluster-related alarms and warnings that occur during the upgrade process, such as cluster communication failures or cluster replication errors. These are expected and will resolve when all cluster peers are upgraded and after cluster data synchronization (typically within 10 minutes of the complete upgrade).

After the reboot is complete the **Login** page displays.

Step 9 For upgrades to other components (not the System platform) the software is automatically installed and no reboot is required.

Step 10 Repeat the previous steps for each peer in sequence until all peers are on the new software version.

What Next?

1. Verify the new status of each Expressway (including the primary):
 - a. Go to **System > Clustering** and check that the cluster database status reports as **Active**.
 - b. Check the configuration for items from the System, Configuration, and Application menus.
2. Backup the Expressway again (**Maintenance > Backup and restore**).
3. If you use MRA, and you are upgrading from X8.9.x or earlier, reconfigure the MRA access control settings as described in [Appendix 2: Post-Upgrade Tasks for MRA Deployments](#).
4. If you have components that require option keys to enable them, do this from the **Maintenance > Option keys** page.
5. If the Expressway has FIPS mode enabled (that is, it's a FIPS140-2 cryptographic system) then from X12.6 you must manually change the default SIP TLS Diffie-Hellman key size from the default 1024 bits, to 2048 or greater. To do this type the following command in the Expressway command line interface (change the value in the final element if you want a key size higher than 2048): ***xconfiguration SIP Advanced SipTlsDhKeySize: "2048"***

This step does **not** apply to most systems. It only affects systems with advanced account security configured and FIPS enabled.
6. (Optional) If for any reason you want to change the default TLS version, the *Cisco Expressway Certificate Creation and Use Deployment Guide* explains how to set the TLS version on each peer.

The software upgrade on the Expressway cluster is now complete.

Using Collaboration Solutions Analyzer

The *Collaboration Solutions Analyzer* is created by Cisco Technical Assistance Center (TAC) to help you with validating your deployment, and to assist with troubleshooting by analyzing Expressway log files. For example, you can use the Business to Business Call Tester to validate and test calls, including Microsoft interworked calls.

You need a customer or partner account to use the Collaboration Solutions Analyzer.

Getting Started

Procedure

- Step 1** If you plan to use the log analysis tool, first collect the Expressway logs.
- Step 2** Sign in to <https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/>
- From X12.6 you can use the **Analyze log** button on the **Diagnostic logging** page (**Maintenance > Diagnostics**) to open a link to the Collaboration Solutions Analyzer troubleshooting tool.
- Step 3** Click the tool you want to use. For example, to work with logs:
- Click **Log analysis**.
 - Upload the log file(s).
 - Select the files you want to analyze.
 - Click **Run Analysis**.

The tool analyzes the log files and displays the information in a format which is much easier to understand than the raw logs. For example, you can generate ladder diagrams to show SIP calls.

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:

- Using a web browser, go to the [Bug Search Tool](#).
- Sign in with a cisco.com username and password.
- Enter the bug identifier in the **Search** field and click **Search**.

To look for information when you do not know the identifier:

- 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.

Appendix 1: Configuring HSM Devices on Expressway

Important: Read this First

HSM failure. If an Expressway is configured to use HSM and the HSM subsequently fails, **all services that require encryption will become unavailable**. This includes MRA, calls, web access, and so on.

Factory reset. If the HSM is permanently unavailable for any reason, **you will need to do a factory reset** for the Expressway and then configure a new HSM on the Expressway. A factory reset **reinstalls the software image and resets the Expressway configuration** to the default, functional minimum (see the *Expressway Administrator Guide* for instructions about doing a reset.)

How to Enable and Manage HSM

Use the **HSM configuration** page (**Maintenance > Security > HSM configuration**) to configure the information needed for Expressway.

Settings are replicated across a cluster.

The **HSM configuration** page settings replicate across all peers in an Expressway cluster. So if you add or remove any settings on one peer, the change replicates to all other peers.

Task 1: Configure Prerequisites

Do the following before you enable Hardware Security Module (HSM) functionality on Expressway:

a.	Add an HSM option key.	<ol style="list-style-type: none"> i. Go to Maintenance > Option keys. ii. In the Software option section, enter the option key. iii. Click Add option. The key appears in the list at the top of the page.
----	------------------------	--

b.	<p>Install the HSM TLP package. You can get this from the same download site as the Expressway software image.</p> <p>The HSM TLP is an archive of HSM provider-specific binaries that are needed for the Expressway to use the HSM.</p>	<p>i. Go to Maintenance > Upgrade.</p> <p>ii. In the Upgrade component section, click Choose File to select the TLP file from your local machine.</p> <p>iii. Click Upgrade. A message, <i>Component installation succeeded</i>, appears at the top of the page and the HSM TLP also appears at the top of the page. You can check the list of all installed modules in the drop-down.</p> <p>Note You must add the option key and install the TLP on each peer in the cluster. You cannot enable HSM Mode on a cluster unless all peers have the option key and the TLP.</p>
c.	Deploy an HSM box on the Expressway	<p>To configure an nShield Connect XC HSM:</p> <p>i. Set up a Security World and Remote File System (RFS) according to the <i>nShield Connect User Guide</i>.</p> <p>ii. Configure RFS to an nShield Connect that contains master copies of all the files that the HSM needs. RFS normally resides on a client computer, but it can be located on any computer that is accessible on the network.</p> <p>iii. After you deploy RFS and the nShield Connect box, run the following command on RFS: <code>/opt/nfast/bin/rfs-setup --gang-client --write-noauth <Expressway_ip_address></code></p> <p>HSM certificate management will not work properly on the Expressway if this command is not run.</p>
d.	Have access to a certificate signing authority.	-
e.	Create an HSM-compatible certificate.	See the <i>Expressway Administrator Guide, Security</i> chapter for instructions.

Task 2: Enable HSM on Expressway

This is the recommended procedure to enable HSM use on Expressway:

Procedure

-
- Step 1** Go to **Maintenance > Security > HSM configuration**.
- Step 2** In **HSM Settings**, choose the HSM provider from the **HSM Mode** drop-down list.
- Step 3** Configure the nShield settings:
- a.** Enter the RFS IP address and RFS Port. The default port is 9004.
 - b.** Click **Save Configuration**.

The following message is displayed at the top of the page.

```
An HSM Settings updated
```

- c. In the **Add Module** section, enter the IP address, Port, ESN (Electronic Serial Number), and KNETI (Network Integrity Key) of the device.
- d. Click **Add Module**.

The following message is displayed at the top of the page.

```
An HSM Module successfully added
```

- e. The device is now displayed in a table below the **HSM Mode** tab.
- f. Repeat the Add Module steps to add more devices.

Step 4 Set the **HSM Mode** to *On* and click **Set Mode**.

The following message is displayed at the top of the page.

```
An HSM Mode successfully updated
```

Note Toggling the HSM Mode to *On/Off* may cause the web to become unavailable. If this happens, reload the browser page.

Results: HSM use is now enabled on the Expressway.

What to do next

To check the HSM operating status see the next section [Task 3: Monitor HSM Status Check](#).

Task 3: Monitor HSM Status Check

After you enable HSM mode, an **HSM Status check** section displays on the **HSM configuration** page. This section displays information about the HSM server and HSM certificate for all Expressway cluster peers, and for all modules on each peer:

HSM server running

1. **TRUE**, after HSM mode is enabled on Expressway, if processes responsible for communicating with the HSM boxes are running on the Expressway.
2. **FALSE**, if processes are not running on the Expressway and an HSM failure alarm is raised.

HSM certificate in use

1. **TRUE**, when an HSM certificate and private key are in use by Expressway.
2. **FALSE**, when an HSM certificate and private key are not being used by Expressway. Default state is **FALSE**. An alarm, *HSM certificate is not used*, is raised on the Expressway - to warn that you are not using an HSM certificate and private key.

After the HSM certificate and private key are deployed to the Expressway, this alarm is lowered and the displayed status changes to TRUE.

The ESN section lists HSM modules that are added during the HSM configuration and are distinguished by their ESN. The other columns define **Connection Status** and **Hardware Status**.

Connection Status

1. OK, if no network issues exist between the Expressway and HSM module.
2. Failed, if network or HSM server connectivity issues exist and an alarm is raised.

Hardware Status

1. OK, if no hardware issues are detected on the HSM box itself.
2. Failed, if there are any hardware or an HSM box configuration issue and an alarm is raised.

Task 4: Next Steps - Generate and Install the HSM Private Key

When HSM is enabled and operating properly, you need to generate and install the HSM private key and certificate on Expressway. For details, see *Managing the Expressway Server Certificate with HSM*, in the *Expressway Administrator Guide*.

How to Delete Modules



Note You cannot remove the last device while HSM mode is enabled. You first need to disable HSM mode.

To optionally delete devices (modules) from the Expressway HSM configuration:

Procedure

- Step 1** Go to **Maintenance > Security > HSM configuration**.
- Step 2** Choose the required device from the list and click **Delete**.
-

How to Disable HSM

If you decide to disable HSM for any reason, the recommended procedure is:

Procedure

- Step 1** Go to **Maintenance > Security > HSM configuration**.
- Step 2** Set **HSM Mode** to *Off* and click **Set Mode**. This disables HSM usage on the Expressway.

- Step 3** Check an individual device or click **Select all** to choose all the modules in the table to delete. (Click **Unselect all** to de-select all devices in the table.)
- Step 4** Click **Delete** and then **OK** in the confirmation dialog.
-

Appendix 2: Post-Upgrade Tasks for MRA Deployments

This section only applies if you use the Expressway for Mobile and Remote Access and you upgrade from X8.9.x or earlier to X8.10 or later. After the system restarts you need to reconfigure the MRA access control settings.

To Reconfigure the MRA Access Control Settings



Important

- The **Check for internal authentication availability** setting will be off after the upgrade. Depending on the authentication settings on the Unified CM, this may prevent remote login by some Cisco Jabber users.
 - The *Exclusive* option in X8.9 is now configured by setting **Authentication path** to *SAML SSO authentication*. This has the effect of prohibiting authentication by username and password.
-

Before you begin

After the system restarts you need to reconfigure the MRA access control settings.

Procedure

- Step 1** On the Expressway-C, go to **Configuration > Unified Communications > Configuration > MRA Access Control**.
- Step 2** Do one of the following:
- To take advantage of the new MRA access control methods from X8.10, set the appropriate values on this page for your chosen methods. See the first table below for help about which values to apply.
 - Or to retain your pre-upgrade authentication approach, set the appropriate values on this page to match your previous settings on the Expressway-E. See the second table below for help about how to map the old Expressway-E settings to their new equivalents on the Expressway-C.
- Step 3** If you configure self-describing tokens (**Authorize by OAuth token with refresh**), refresh the Unified CM nodes: Go to **Configuration > Unified Communications > <UC server type>** and click **Refresh servers**.
-

Settings for MRA Access Control

The fields you actually see in the Web UI depend on whether MRA is enabled (**Unified Communications mode** set to *Mobile and remote access*) and on the selected authentication path. Not all the fields in the table are necessarily displayed.

Table 11: Settings for MRA access control

Field	Description	Default
Authentication path	<p>Hidden field until MRA is enabled. Defines how MRA authentication is controlled.</p> <p><i>SAML SSO authentication:</i> Clients are authenticated by an external IdP.</p> <p><i>UCM/LDAP basic authentication:</i> Clients are authenticated locally by the Unified CM against their LDAP credentials.</p> <p><i>SAML SSO and UCM/LDAP:</i> Allows either method.</p> <p><i>None:</i> No authentication is applied. This is the default setting until MRA is first enabled. The “None” option is needed (rather than just leaving MRA turned off) because some deployments must turn on MRA to allow functions which are not actually MRA. (Such as the Web Proxy for Meeting Server, or XMPP Federation.) Only these customers should use “None”.</p> <p>Note Do not use it in other cases.</p>	None before MRA turned on UCM/LDAP after MRA turned on
Authorize by OAuth token with refresh	<p>This option requires self-describing tokens for authorization. It's our recommended authorization option for all deployments that have the infrastructure to support them.</p> <p>Only Jabber clients are currently capable of using this authorization method. Other MRA endpoints do not currently support it. The clients must also be in OAuth token with refresh authorization mode.</p>	On
Authorize by OAuth token (previously SSO Mode)	<p>Available if Authentication path is <i>SAML SSO</i> or <i>SAML SSO and UCM/LDAP</i>.</p> <p>This option requires authentication through the IdP. Currently, only Jabber clients are capable of using this authorization method, which is not supported by other MRA endpoints.</p>	Off

Field	Description	Default
Authorize by user credentials	<p>Available if Authentication path is <i>UCM/LDAP</i> or <i>SAML SSO and UCM/LDAP</i>.</p> <p>Clients attempting to perform authentication by user credentials are allowed through MRA. This includes Jabber, and supported IP phone and TelePresence devices.</p>	Off
Check for internal authentication availability	<p>Available if Authorize by OAuth token with refresh or Authorize by OAuth token is enabled.</p> <p>The default is No, for optimal security and to reduce network traffic.</p> <p>Controls how the Expressway-E reacts to remote client authentication requests by selecting whether or not the Expressway-C should check the home nodes.</p> <p>The request asks whether the client may try to authenticate the user by OAuth token, and includes a user identity with which the Expressway-C can find the user's home cluster:</p> <p><i>Yes</i>: The <i>get_edge_sso</i> request will ask the user's home Unified CM if OAuth tokens are supported. The home Unified CM is determined from the identity sent by the Jabber client's <i>get_edge_sso</i> request.</p> <p><i>No</i>: If the Expressway is configured not to look internally, the same response will be sent to all clients, depending on the Edge authentication settings.</p> <p>The option to choose depends on your implementation and security policy. If all Unified CM nodes support OAuth tokens, you can reduce response time and overall network traffic by selecting <i>No</i>. Or select <i>Yes</i> if you want clients to use either mode of getting the edge configuration - during rollout or because you can't guarantee OAuth on all nodes.</p> <p>Caution Setting this to <i>Yes</i> has the potential to allow rogue inbound requests from unauthenticated remote clients. If you specify <i>No</i> for this setting, the Expressway prevents rogue requests.</p>	No

Field	Description	Default
Identity providers: Create or modify IdPs	<p>Available if Authentication path is <i>SAML SSO</i> or <i>SAML SSO and UCM/LDAP</i>.</p> <p>Selecting an Identity Provider</p> <p>Cisco Collaboration solutions use SAML 2.0 (Security Assertion Markup Language) to enable SSO (single sign-on) for clients consuming Unified Communications services.</p> <p>If you choose SAML-based SSO for your environment, note the following:</p> <ul style="list-style-type: none"> • SAML 2.0 is not compatible with SAML 1.1 and you must select an IdP that uses the SAML 2.0 standard. • SAML-based identity management is implemented in different ways by vendors in the computing and networking industry, and there are no widely accepted regulations for compliance to the SAML standards. • The configuration of and policies governing your selected IdP are outside the scope of Cisco TAC (Technical Assistance Center) support. Please use your relationship and support contract with your IdP Vendor to assist in configuring the IdP properly. Cisco cannot accept responsibility for any errors, limitations, or specific configuration of the IdP. <p>Although Cisco Collaboration infrastructure may prove to be compatible with other IdPs claiming SAML 2.0 compliance, only the following IdPs have been tested with Cisco Collaboration solutions:</p> <ul style="list-style-type: none"> • OpenAM 10.0.1 • Active Directory Federation Services 2.0 (AD FS 2.0) • PingFederate®6.10.0.4 	-
Identity providers: Export SAML data	<p>Available if Authentication path is <i>SAML SSO</i> or <i>SAML SSO and UCM/LDAP</i>.</p> <p>For details about working with SAML data, see <i>SAML SSO Authentication Over the Edge</i>.</p>	-

Field	Description	Default
Allow Jabber iOS clients to use embedded Safari	<p>By default the IdP or Unified CM authentication page is displayed in an embedded web browser (not the Safari browser) on iOS devices. That default browser is unable to access the iOS trust store, and so cannot use any certificates deployed to the devices.</p> <p>This setting optionally allows Jabber on iOS devices to use the native Safari browser. Because the Safari browser is able to access the device trust store, you can now enable password-less authentication or two factor authentication in your OAuth deployment.</p> <p>A potential security issue exists for this option. The mechanism to return browser control from Safari to Jabber after the authentication completes, uses a custom URL scheme that invokes a custom protocol handler. It's possible that another application other than Jabber could intercept the scheme and gain control from iOS. In that case, the application would have access to the OAuth token in the URL.</p> <p>If you are confident that your iOS devices will not have other applications that register the Jabber custom URL scheme, for example because all mobile devices are managed, then it's safe to enable the option. If you are concerned about the possibility of another app intercepting the custom Jabber URL, then do not enable the embedded Safari browser.</p>	No
SIP token extra time to live	<p>Available if Authorize by OAuth token is <i>On</i>.</p> <p>Optionally extends the time-to-live for simple OAuth tokens (in seconds). Gives users a short window to accept calls after their credentials expire. However, it increases the potential security exposure.</p>	0 seconds

MRA Access Control Values Applied by the Upgrade

Table 12: MRA access control values applied by the upgrade

Option	Value after upgrade	Previously on...	Now on...
Authentication path	<p>Pre-upgrade setting is applied</p> <p>Note SSO mode=Off in X8.9 is two settings in X8.10:</p> <ul style="list-style-type: none"> • Authentication path=UCM/LDAP • Authorize by user credentials=On <p>SSO Mode=Exclusive in X8.9 is two settings in X8.10:</p> <ul style="list-style-type: none"> • Authentication path=SAML SSO • Authorize by OAuth token=On <p>SSO Mode=On in X8.9 is three settings in X8.10:</p> <ul style="list-style-type: none"> • Authentication path=SAML SSO/and UCM/LDAP • Authorize by OAuth token=On • Authorize by user credentials=On 	Both	Expressway-C
Authorize by OAuth token with refresh	On	-	Expressway-C
Authorize by OAuth token (previously SSO Mode)	Pre-upgrade setting is applied	Both	Expressway-C
Authorize by user credentials	Pre-upgrade setting is applied	Both	Expressway-C
Check for internal authentication availability	No	Expressway-E	Expressway-C
Identity providers: Create or modify IdPs	Pre-upgrade setting is applied	Expressway-C	Expressway-C (no change)

Option	Value after upgrade	Previously on...	Now on...
Identity providers: Export SAML data	Pre-upgrade setting is applied	Expressway-C	Expressway-C (no change)
Allow Jabber iOS clients to use embedded Safari	No	Expressway-E	Expressway-C
SIP token extra time to live	Pre-upgrade setting is applied	Expressway-C	Expressway-C (no change)

