



Cisco Expressway X12.7.1

Release Notes

First Published: February 2021

Last Updated:

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.

Contents

Preface	3
Change History	3
Supported Platforms	5
Notices Relating to VCS Product Support	5
Notices Relating to Hardware Support for CE1 100, CE1000, and CE500 Appliances	5
Feature History Summary for X12.7.1	6
Withdrawn or Deprecated Features and Software	7
Related Documentation	8
Changes in X12.7.1	10
Server Name Indication (SNI) Support for Single-tenant Environments	10
Other Software Changes in X12.7.1	10
Features and Changes in X12.7	11
Security Enhancements	11
Dedicated Management Interface	11
Fast Path Registration for MRA (Caching Optimization for Registrations)	13
Webex VDI over MRA	13

Extension of TLS 1.2 as Default Minimum Version	13
TLS Changes - Impact for TMS and CMS	14
TLS Changes - Impact for LDAP	14
TLS Changes - Impact for SMTP	14
CBC Ciphers Removed from SSH Default Configuration	14
Virtualized Systems - VMware HA and DRS (Manual) Tested	15
Virtualized Systems - Later VM Hardware Version	15
Virtualized Systems - ESXi 7.0 for Large/Medium VMs	15
Virtualized Systems - ESXi 6.0 now Deprecated	15
LDAP Authentication Search Optimization	15
(Preview) Hardware Security Module (HSM) Support	16
(Preview) SIP Registration Failover for Cisco Jabber - MRA Deployments	16
(Preview) Headset Capabilities for Cisco Contact Center - MRA Deployments	17
(Preview) Push Notifications with Mobile Application Management clients- MRA Deployments	17
(Preview) Push Notifications with Android Devices - MRA Deployments	17
(Preview) KEM Support for Compatible Phones - MRA Deployments	18
Ongoing Removal of Unsupported Functions from UI	18
Other Changes in this Release	18
REST API Changes	18
About Cisco Expressway Licensing	20
How Smart Licensing Works	21
Important Configuration Information for Smart Licensing	21
Open and Resolved Issues	23
Bug Search Tool Links	23
Notable Issues in this Version	23
Limitations	24
Some Expressway Features are Preview or Have External Dependencies	24
Unsupported Functionality	24
Expressway TURN does Not Operate as a STUN Server	24
Cisco Webex Hybrid Call Service	24
Product License Registration - Issue with Converting to Smart Licensing	24
Static NAT for Clustered Systems	25
MRA Limitations	25
MRA OAuth Token Authorization with Endpoints / Clients	25
Spurious Alarms when Adding or Removing Peers in a Cluster	25
Virtual Systems	26

CE1200 Appliance	26
Medium Appliances with 1 Gbps NIC - Demultiplexing Ports	26
XMPP Federation-Behavior on IM&P Node Failure	26
Cisco Webex Calling May Fail with Dual-NIC Expressway	26
Interoperability and Compatibility	28
Which Expressway Services Can Run Together?	28
Upgrading Expressway to X12.7.1	29
Summary	29
Prerequisites and Software Dependencies	29
Upgrade Instructions	32
Process to Upgrade a Standalone System	33
Process to Upgrade a Clustered System	35
Using Collaboration Solutions Analyzer	37
Using the Bug Search Tool	37
Obtaining Documentation and Submitting a Service Request	38
Appendix 1: Configuring HSM Devices on Expressway	39
Important: Read this First	39
How to Enable and Manage HSM	39
How to Delete Modules	41
How to Disable HSM	41
Appendix 2: Post-Upgrade Tasks for MRA Deployments	42
Cisco Legal Information	47
Cisco Trademark	47

Preface

Change History

Table 1 Release Notes Change History

Date	Change	Reason
February 2021	Updates for maintenance release.	X12.7.1
December 2020	First publication of X12.7 release.	X12.7
October 2020	Updates for maintenance release.	X12.6.4
October 2020	Updates for maintenance release.	X12.6.3
August 2020	Updates for maintenance release.	X12.6.2

Table 1 Release Notes Change History (continued)

Date	Change	Reason
July 2020	Remove misleading section about issues with software downgrade (which is not supported).	Document correction
July 2020	Updates for maintenance release. Also clarify endpoint requirements for OAuth token authorization.	X12.6.1
June 2020	First publication.	X12.6

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. Expressway was supported from X8.6.1 to X12.5.9, and X12.6 for bug fixes 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 VCS Product Support

Cisco TelePresence Video Communication Server (VCS) product is now **end-of-sale**. For **end-of-life** dates and other details, refer <https://www.cisco.com/c/en/us/products/collateral/unified-communications/telepresence-video-communication-server-vcs/eos-eol-notice-c51-743969.html>

This notice does not affect the Cisco Expressway Series product.

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

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

CE500 and CE1000 appliances - advance notice of hardware service support to be withdrawn

Cisco will withdraw hardware support services for the Cisco Expressway CE500 and CE1000 appliance hardware platforms in a future release. More details are available in the [End-of-sale announcement](#).

CE1100 appliance - end of sale from 13th November 2018 and advance notice of hardware service support to be withdrawn

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 other important dates in the lifecycle of this platform.

Feature History Summary for X12.7.1

Table 3 Features by Release Number

Feature / change	Status
Support for SNI in single tenant environments	Supported from X12.7.1
Dedicated Management Interface	Supported from X12.7
Fast Path Registration for MRA (Caching Optimization for Registrations)	Supported from X12.7
Webex VDI for MRA	Supported from X12.7
Virtualized Systems - ESXi 7.0 Qualification	Supported from X12.7
Hardware Security Module (HSM) Support	Preview
MRA SIP Registration Failover for Cisco Jabber	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
VMware ESXi6.0 (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 virtual hardware versions ESXi5.x (VM-based deployments)	Withdrawn X12.5

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
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 registrar / single systems	<i>Cisco Expressway Registrar Deployment Guide</i> on the Expressway configuration guides page
Basic configuration for firewall traversal / paired systems	<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 <i>Cisco Expressway Serviceability Guide</i> on the Expressway maintain and operate guides page
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 (MRA)	<i>Mobile and Remote Access Through Cisco Expressway</i> on the Expressway configuration guides page
Cisco Meeting Server	<i>Cisco Meeting Server with Cisco Expressway Deployment Guide</i> on the Expressway configuration guides page <i>Cisco Meeting Server API Reference Guide</i> on the Cisco Meeting Server programming guides page Other Cisco Meeting Server guides are available on the Cisco Meeting Server configuration guides page
Cisco Webex Hybrid Services	Hybrid services knowledge base

Table 5 Links to Related Documents and Videos (continued)

Cisco Hosted Collaboration Solution (HCS)	HCS customer documentation
Microsoft infrastructure	<p><i>Cisco Expressway with Microsoft Infrastructure Deployment Guide</i> on the Expressway configuration guides page</p> <p><i>Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet</i> on the Expressway configuration guides page</p>
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

Changes in X12.7.1

Server Name Indication (SNI) Support for Single-tenant Environments

From X12.7.1, support for SNI is now extended to single-tenant environments, in addition to the multi-tenant HCS environments which were previously supported.

Other Software Changes in X12.7.1

From X12.7.1, in a clustered environment, if the status of an automated intrusion protection category is changed in a primary peer, the same will not reflect in other peers which was the case earlier. This unexpected behaviour is now corrected and expressway now works as per design.

Features and Changes in X12.7

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:

- More services are now configured by default on Expressway to require TLS 1.2 as the minimum TLS version (see below for details).
- SMTP mail-based services now require TLS certificate-based verification. This change primarily affects the alarm-based email notification feature (see below for details).
- An additional password check is now performed if the "Enforce strict passwords" feature is enabled **Users > Password security** (Users > Password security) page. From X12.7, if the account holder tries to use the same letters as their username in their password - in straight or reverse order, and in lower or upper case - an error message is displayed.
Note: The strict passwords feature applies to the local authentication database, and administrator accounts and FindMe user accounts managed locally in Expressway, but does not apply to LDAP and externally stored credentials.

Dedicated Management Interface

From X12.7, Expressway supports the Dedicated Management Interface (DMI). This is a new network interface that uses the third LAN port (LAN3) to access Expressway for management-related activities. Instead of sharing a routing interface with other traffic, management traffic is sent and received through LAN3 and no other traffic uses that port.

The DMI is disabled by default. Enabling the DMI has two aspects:

1. Enabling the DMI function - this switches on the LAN3 port for management traffic. However, it is not exclusive and LAN1 (and LAN2 if configured) can also be used - Expressway continues to listen for management traffic on LAN1/LAN2 as well, not just on the LAN3 port.
2. If you want LAN3 to be the only interface for management traffic, you need to configure the individual management services in Expressway for DMI only. Note that if you have management servers outside the LAN3 subnet, currently you also need to configure static IP routes in order for their traffic to be directed to LAN3.

Server / client management traffic

Expressway management traffic can be classified as server-based or client-based.

Management traffic where Expressway is the server:

- HTTP(S) - for web UI administration and REST API
- ssh - for CLI (not for MRA tunnels)
- SNMP

Management traffic where Expressway is the client, for example:

- HTTP(S) for feedback events to external managers like Cisco TMS
- NTP
- directory (LDAP, Active Directory)
- remote syslog
- system metrics (collectd)

Prerequisites

The new DNS name for the DMI interface must be entered as a Subject Alternative Name (SAN) on the Expressway server certificate. If an IP address is used to access the interface (or a DNS that is not a SAN entry in the certificate) a certificate validation warning will be issued and access may be blocked.

CAUTION: It is essential to properly secure the DMI, as it provides access into the Expressway configuration.

Enable DMI

1. Go to **System > Network Interfaces > IP** and set Use Dedicated Management Interface to Yes
2. In the **LAN3 - DMI** section
 - a. Specify the IPv4 and/or IPv6 address of the LAN3 port.
 - b. For IPv4 also specify the subnet mask.
 - c. For IPv6 use a static, global address. It cannot be link-local or stateless SLAAC.
 - d. Optionally change the maximum Ethernet packet size that can be sent over the DMI by setting the **Maximum transmission unit (MTU)** for the port. The default is 1500 bytes.
3. Restart the system. These changes require a restart to take effect.

The DMI is now activated on LAN3 as an interface for management traffic. If you want the DMI to be the sole interface for management, go on to the next tasks.

Note: For Expressway VMs, the OVF template includes a customization option to define the DMI IP address.

(Optional) Make DMI sole interface - server management traffic

Use this task to make management traffic use the DMI, where Expressway is the server.

CAUTION: Before you do this, make sure that the required services are accessible on LAN3, else they won't have access after the change to DMI only. This is especially important for administration services, as the only way to recover them would be to turn off DMI using the console (serial/VMWare).

1. You can do this for administration services (web user interface, REST API, and command line interface) and/or for SNMP. Do either or both the following steps, depending on which services you want to configure for DMI only:
 - Go to System > SNMP and in the Configuration section set Use Dedicated Management Interface only to Yes.
 - Go to System > Administration settings and in the Services section set Use Dedicated Management Interface only (for administration) to Yes.
2. You need to restart the system for the changes to take effect for the web user interface and the API, which remain accessible from LAN1 / LAN2 until you restart. Changes take immediate effect for the command line interface (SSH) and SNMP service, regardless of restart.

The specified management services can now be accessed only from the DMI / LAN3 port.

Note: Expressway will not let you disable the DMI while a management service is configured to use it as the only interface.

(Optional) Make DMI sole interface - client management traffic outside subnet

For management traffic where Expressway acts as the client, the traffic will be directed to the DMI if the target server is in the same subnet as the DMI / LAN3 port. If it's not possible to deploy the server in the same subnet as LAN3, you can optionally force Expressway management traffic to use the DMI, by configuring static IP routes for LAN3 per service.

Example

This example assumes an Expressway with these subnets:

- LAN3 subnet range: a.b.128.0 - a.b.191.255
- LAN1 subnet range: x.y.156.0 - x.y.159.255

Say you want to configure NTP with Expressway. The NTP server is in the LAN1 subnet. You want outgoing NTP traffic from Expressway and incoming responses from NTP to use the DMI / LAN3. This can be achieved by creating a static route for LAN3 (System > Network interfaces > Static routes select Add) with the following settings:

- IP address: x.y.151.0
- Prefix length: 24
- Gateway: 172.22.128.1 (*gateway of LAN3 subnet*)
- Interface: LAN3

More details about configuring static routes are in the *Expressway Administrator Guide*.

Fast Path Registration for MRA (Caching Optimization for Registrations)

From X12.7, Expressway supports Fast Path Registration for MRA-based devices. This optimizes routing processes, reducing the server workload, so leading to increased capacities. Expressway caches the initial routing calculation and then uses a Pre-Routed Route Header to forward subsequent packets to the destination using the cached routing result. This has the following benefits:

- Reduces the routing workload.
- Increases registration capacity.
- Ensures that each media packet follows the same route path.

IMPORTANT: This feature only applies to MRA deployments. The increased capacity and other benefits do not apply to non-MRA Expressway deployments.

Fast Path Registration is supported for the following SIP methods: REGISTER. Configuration is through the command line interface, and detailed instructions are provided in the latest *Expressway MRA Deployment Guide*.

The tested results for a standalone Expressway MRA deployment (Expressway-C + Expressway-E) when this feature is configured are:

Platform	MRA Registrations	MRA Video Calls	MRA Audio Calls
CE 1200	7000	500	1000
Large OVA	3500	500	1000
Medium OVA	3000	150	300
Small OVA	2500	100	200
Small OVA BE6K	2500	100	200

Webex VDI over MRA

This item applies if you deploy MRA. From X12.7, Expressway supports Webex for Virtual Desktop Infrastructure (VDI) with compatible MRA-connected clients, providing the deployed Unified Communications products are running compatible versions.

Extension of TLS 1.2 as Default Minimum Version

The default minimum TLS version is now TLS 1.2 for the additional services in X12.7, as listed in the table. The default version - and associated ciphers - can be configured to a lower version (not recommended) from the **Maintenance > Security > Ciphers** page.

Service	Configuration Setting
Certificate Checker	<i>HTTPS minimum TLS version</i>
Cisco Meeting Server discovery	<i>Reverse proxy minimum TLS version</i>
LDAP	<i>LDAP minimum TLS version</i>
SMTP mail client (TLS certificate-based authentication from X12.7)	<i>SMTP minimum TLS version</i>
TMS Provisioning Service	<i>TMS provisioning minimum TLS version</i>
UC server discovery (AXL query)	<i>UC server discovery minimum TLS version</i>

TLS Changes - Impact for TMS and CMS

From X12.7, Cisco TMS and Cisco Meeting Server are included in the services for which the default minimum TLS version is TLS 1.2. This means that if any Cisco TMS or Cisco Meeting Servers are deployed with TLS 1.1 or lower, the TLS handshake will fail.

TLS Changes - Impact for LDAP

From X12.7, LDAP is included in the services for which the default minimum TLS version is TLS 1.2. This means that if any LDAP servers are deployed with TLS 1.1 or lower, only local administrators will be able to sign in, and the TLS handshake will fail. **Remote administrators will be unable to sign in until such time as the LDAP server supports TLS 1.2** (and the **Ciphers** page is updated to match).

Configuration change on upgrade - "Remote-only" automatically set to "Both"

This change applies if you currently (before upgrading to this release) specify "Remote only" for the administrator authentication source setting on the **Users > LDAP configuration** page. To avoid remote administrators being unintentionally locked out of the Expressway, on upgrade to X12.7 or later, **this setting is automatically changed to "Both"**.

After the upgrade is complete, if you want to limit administrator sign ins again so that only remote administrators may authenticate:

1. Verify that the LDAP connection status is "Available".
2. On the Users > LDAP Configuration page, reconfigure the administrator authentication source back to "Remote only".

TLS Changes - Impact for SMTP

From X12.7, Expressway requires SMTP services to use TLS 1.2 certificate-based verification. These configuration prerequisites must be in place, else **alarm-based email notifications (and any other SMTP-based functions) will fail**:

- As the SMTP server certificate gets validated by the client, its IP address and/or FQDN must be in the certificate's CN/SAN.
- The SMTP server certificate issuer needs to be imported into the Expressway trusted CA certificate list (**Maintenance > Security > Trusted CA Certificate**).

CBC Ciphers Removed from SSH Default Configuration

As part of our ongoing security enhancements, CBC-mode ciphers are no longer included in the system's default cipher configuration for SSH. The upgrade will automatically change the default values to remove the CBC ciphers -

aes129-cbc, aes-256-cbc, aes192-cbc. If you need these ciphers (not recommended) you can use the `xconfiguration Ciphers sshd_ciphers` command to reconfigure them.

Virtualized Systems – VMware HA and DRS (Manual) Tested

Expressway version X12.7 was successfully tested with the following VMware features:

- **vSphere HA** (high availability). In tests using Expressway X12.7, VMware restarted the Expressway VM on an alternate host in the ESXi cluster. When the VM started, it successfully rejoined the cluster. Note that all active calls and registrations will drop when the Expressway VM is moved to the new host.
- **vSphere HA with DRS** (Distributed Resource Scheduler). Expressway is only tested and supported with DRS in **manual mode**. Carry out any recommended changes during a planned maintenance window.

Virtualized Systems – Later VM Hardware Version

This item applies to Expressways running as virtualized systems. Expressway X12.7 is compatible with VM hardware version 11.

Virtualized Systems – ESXi 7.0 for Large/Medium VMs

This item applies to Expressways running as virtualized systems. Expressway X12.7 is compatible with VMware ESXi version 7.0.

Virtualized Systems – ESXi 6.0 now Deprecated

This item applies to Expressways running as virtualized systems. VMware ESXi6.0 is now deprecated for Expressway systems.

LDAP Authentication Search Optimization

This item applies if you allow remote account authentication for Expressway administrators – they authenticate through an LDAP connection to a remote directory service. The LDAP search mechanism to verify that someone attempting to sign into Expressway is indeed a member of a permitted administrator group can take a long time and especially if a lot of subgroups are involved (bug ID [CSCvs44968](#) refers). X12.7 provides two new settings on the **Users > LDAP configuration** page, to optimize LDAP searching.

Nested Subgroup Search Depth

Used to limit the depth of groups for the LDAP search. For optimal search performance, define the top-level group for the remote administrator as an (administrator) group in Expressway and set the search depth to "1". The default is "16".

Skip Looking up all the Members

Used to disable or enable member lookup of an administrator group during the authentication search process. The default is "Yes" – skip the member lookup.

We recommend keeping this setting as "Yes" if the configured groups have relatively high numbers of members. However, for deployments where the configured groups have relatively few members, setting it to "No" (do member lookup) may help to reduce authentication latency.

Command line interface

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

- `xconfiguration Login Remote LDAP SearchOptimize NestedDepth: <1..16>`
- `xconfiguration Login Remote LDAP SearchOptimize SkipMembers: <Yes/No>`

(Preview) Hardware Security Module (HSM) Support

Expressway supports HSM functionality, on a Preview basis only, from X12.6.

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 supports the nShield Connect XC from Entrust as an HSM provider (on a Preview basis). Configuration instructions and some important caveats and limitations to be aware of, are detailed in [Appendix 1: Configuring HSM Devices on Expressway](#), page 39.

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) SIP Registration Failover for Cisco Jabber - MRA Deployments

This feature applies if you deploy Expressway with Mobile and Remote Access (MRA). It is currently provided in Preview status only due to pending software dependencies.

Expressway X12.7 builds on existing failover capabilities for clustered Expressways with a number of MRA failover updates that improve substantially the failover time for Cisco Jabber clients that connect over MRA. Among the updates include adaptive routing, STUN keepalive support and improved error reporting.

These new capabilities will allow Jabber clients to support MRA High Availability (failover) for voice and video.

Adaptive routing

Adaptive routing updates in Expressway X12.7 let Expressway alter the routing path dynamically. If a node failure is detected, packets are rerouted to a peer node that is up and running. For example, assume that a remote Jabber client sends a SIP REGISTER that is intended to be routed through a specific Expressway-E (EXWY-E1), Expressway-C (EXWY-C1) and Unified CM (CUCM1) combination, but the designated Expressway-C node is either down or is in maintenance mode. In this case, the message is rerouted to a peer Expressway-C node (EXWY-C2) and then on to the intended Unified CM destination. After the registration, Cisco Jabber also updates its routing table so that future SIP messages use the registration path.

Note: Failover does not include call preservation. The Jabber registration fails over to the new registration path, but active calls at the time of the failure are dropped.

STUN keepalive support

In addition to adaptive routing, Expressway X12.7 supports the use of STUN keepalives by MRA-connected Jabber clients. Remote Jabber clients send STUN keepalives into the enterprise network via Expressway-E to learn of connection issues ahead of time. As a result, if a node in the registration path fails, Jabber will learn of the failure after receiving the STUN response and can select a different route path for future SIP messages.

Requirements

No specific configuration is required (subject of course to the necessary clustering/backup nodes existing). However, you must be running the following minimum releases:

Routing Feature	Minimum Releases
Adaptive routing	Expressway X12.7 Cisco Jabber 12.9 MR

STUN keepalives	Expressway X12.7 Cisco Unified Communications Manager 14 Cisco Jabber 12.9MR
-----------------	--

Full benefits with all software requirements

When all three components – clients, Expressway, Unified CM – are running updated software with MRA registration failover capabilities, the following benefits apply:

- No user action required for failover
- Faster failover times—down to 30–60 seconds from the previous standard of 120 seconds
- Route path updates dynamically to handle server failures
- More routes are available to reach the intended destination
- Remote Jabber clients can learn of server failures via STUN keepalives and adjust routing ahead of time

Adaptive routing benefit without Unified CM upgrade

Even without new Unified CM software (but with new Expressway and Jabber software), this feature has the benefit of allowing Jabber clients to detect path failures. Note that this action will take over 2 minutes, and Expressway may flag Unified CM servers as inactive in some scenarios where actually the server is just idle or has low use at the time.

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

This feature applies if you deploy Expressway with Mobile and Remote Access (MRA). 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 don't need to configure anything on Expressway.

More information is available in the white paper *Cisco Headset and Finesse Integration for Contact Center* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucm/whitePaper/CUCM_Headsets_for_ContactCenter_WP.pdf

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

This feature applies if you deploy Expressway with MRA. It is currently provided in Preview status only.

With this feature, push notification support over MRA now includes support for Mobile Application Management (MAM) clients like Jabberintune and Jabberblackberry. As a result, the push notification service is available for all devices that are running Jabberintune and Jabberblackberry 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 CSCv12541 refers).

In X12.7, bug ID CSCv12541 is 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).

Ongoing Removal of Unsupported Functions from UI

To enhance usability and consistency we are removing discontinued functions and features from the user interface. Details per release are in [Withdrawn or Deprecated Features and Software, page 7](#)

Other Changes in this Release

The Connection Manager log has been improved.

The layout and content of the *Expressway MRA Deployment Guide* has been enhanced.

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://<ip address>/api/raml`. A high-level summary of how to access and use the API is provided in the *Cisco Expressway REST API Summary Guide* on the [Expressway installation guides page](#).

Configuration APIs	API introduced in version
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

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

About Cisco Expressway Licensing

Cisco Expressway supports two licensing modes from X12.6:

- 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.

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 6 Option Keys Supported in Either License Mode

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

* 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 with Expressway X12.5.4 or later – the functionality is enabled by default. If running in PAK-based licensing mode they are not needed, and recommended that they should not be applied. **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 7 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)

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 8 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 *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 is enabled and the registration settings are restored on the restored system.
 - If you restore on a different system, Smart Licensing is 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 *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 X12.7.1](#)
- [Issues resolved by X12.7](#)

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 the 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 [Preview Features Disclaimer, page 1](#)). 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 the [Feature History table](#) earlier in these notes.

Unsupported Functionality

- 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.
- 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 of the licenses, the system automatically forfeits/removes the remaining licenses - that is, 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.

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. Details are provided in *Key Supported and Unsupported Features with Mobile and Remote Access* in the [Mobile and Remote Access Through Cisco Expressway](#) guide.

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.

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 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 that 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.

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.

We recommend that you make static routes as specific as possible, to minimize the risk of the routes overlapping, and this issue occurring.

Interoperability and Compatibility

Detailed Matrices

Interoperability test results for Expressway and other Cisco Telepresence products are available here <https://tp-tools-web01.cisco.com/interop/>.

A compatibility matrix for products in the Cisco Collaboration Systems Release (CSR) set is available here: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/CSR-Compatibility-Matrix-InteractiveHTML.html Entries for Expressway are in the "Enterprise Edge" section.

Mobile and Remote Access

Information about compatible products for MRA specifically, is provided in version tables for infrastructure products and for endpoints in the *Expressway MRA Deployment Guide*.

Which Expressway Services Can Run Together?

The *Cisco Expressway Administrator Guide* on the [Cisco Expressway Series maintain and operate guides](#) page 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 section. For example, if you want to know if MRA can coexist with CMR Cloud (it can) the table will tell you.

Upgrading Expressway to X12.7.1

This section describes how to install the software on Expressway using the web user interface, which is the method we recommend. If you prefer to use a secure copy program such as SCP or PSCP to do the install, please use the *Administrator Guide* instead.

Summary

Table 9 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 X12.7.1 software (this requirement applies to all upgrades to 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 X12.7.1 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, please note that 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 that 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, also 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, page 29](#) 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

Do not use this process if you are upgrading a clustered Expressway; instead use the [process to upgrade a clustered system](#).

1. Sign in to the Expressway web user interface as *admin*.
2. Back up the Expressway system before you upgrade (**Maintenance > Backup and restore**).
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.
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.
5. Go **Maintenance > Upgrade** to access the **Upgrade** page.
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.
7. Click **Upgrade**. This step uploads the software file but does not install it. The upload may take a few minutes to finish.
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.
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, page 42](#)

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:

1. Sign in to the Expressway web user interface as *admin*.
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.
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.
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.
5. Go **Maintenance > Upgrade** to access the **Upgrade** page.
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.
7. Click **Upgrade**. This step uploads the software file but does not install it. The upload may take a few minutes to finish.
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.

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.
9. For upgrades to other components (not the System platform) the software is automatically installed and no reboot is required.
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, page 42](#)
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

1. If you plan to use the log analysis tool, first collect the Expressway logs.
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.
3. Click the tool you want to use. For example, to work with logs:
 - a. Click **Log analysis**.
 - b. Upload the log file(s).
 - c. Select the files you want to analyze.
 - d. 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:

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

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

1. Type the product name in the **Search** field and click **Search**.
2. From the list of bugs that appears, use the **Filter** drop-down list to filter on either *Keyword*, *Modified Date*, *Severity*, *Status*, or *Technology*.

Use **Advanced Search** on the Bug Search Tool home page to search on a specific software version.

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

Obtaining Documentation and Submitting a Service Request

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

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

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

Appendix 1: Configuring HSM Devices on Expressway

Important: Read this First	39
How to Enable and Manage HSM	39
How to Delete Modules	41
How to Disable HSM	41

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.	<ul 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>	<ul style="list-style-type: none"> i. Go to Maintenance > Upgrade. ii. In the Upgrade component section, click Choose File to select the TLP file from your local machine. 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>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> <ul style="list-style-type: none"> i. Set up a Security World and Remote File System (RFS) according to the nShield Connect user guide. 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. iii. After you deploy RFS and the nShield Connect box, run the following command on RFS: <pre>/opt/nfast/bin/rfs-setup --gang-client --write-noauth <Expressway_ip_address></pre> HSM certificate management will not work properly on the Expressway if this command is not run.
d.	Have access to a certificate signing authority	
e.	Create an HSM-compatible certificate	See the <i>Expressway Administrator Guide</i> security chapter for instructions.

Task 2: Enable HSM on Expressway

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

1. Go to **Maintenance > Security > HSM configuration**.
2. In **HSM Settings**, choose the HSM provider from the **HSM Mode** drop-down list.
3. Configure the nShield settings:
 - a. Enter the RFS IP address and RFS Port. The default port is 9004.
 - b. Click **Save Configuration**.
An *HSM Settings updated* message is displayed at the top of the page.
 - 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**.
An *HSM Module successfully added* message is displayed at the top of the page.
 - e. The device is now displayed in a table below the **HSM Mode** tab.
 - f. Repeat the Add Module steps to add more devices.
4. a. Set the **HSM Mode** to *On* and click **Set Mode**.
An *HSM Mode successfully updated* message is displayed (top of page).
Note: Toggling the HSM Mode to On/Off may cause the web to become unavailable. If this happens, reload the browser page.

Result: HSM use is now enabled on the Expressway. To check the HSM operating status see the next section [Task 3: Monitor HSM Status Check, page 40](#).

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

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

HSM certificate in use

- a. **TRUE**, when an HSM certificate and private key are in use by Expressway.
- b. **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

- a. **OK**, if no network issues exist between the Expressway and HSM module.
- b. **Failed**, if network or HSM server connectivity issues exist and an alarm is raised.

Hardware Status

- a. **OK**, if no hardware issues are detected on the HSM box itself.
- b. **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

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

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

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

How to Disable HSM

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

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

1. On the Expressway-C, go to **Configuration > Unified Communications > Configuration > MRA Access Control**.
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.
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**.

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.

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 10 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". Do not use it in other cases.</p>	<p>None before MRA turned on</p> <p>UCM/LDAP after MRA turned on</p>
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

Table 10 Settings for MRA access control (continued)

Field	Description	Default
Authorize by OAuth token (previously SSO Mode)	Available if Authentication path is <i>SAML SSO</i> or <i>SAML SSO and UCM/LDAP</i> . 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.	Off
Authorize by user credentials	Available if Authentication path is <i>UCM/LDAP</i> or <i>SAML SSO and UCM/LDAP</i> . Clients attempting to perform authentication by user credentials are allowed through MRA. This includes Jabber, and supported IP phone and TelePresence devices.	Off
Check for internal authentication availability	Available if Authorize by OAuth token with refresh or Authorize by OAuth token is enabled. The default is No, for optimal security and to reduce network traffic. Controls how the Expressway-E reacts to remote client authentication requests by selecting whether or not the Expressway-C should check the home nodes. 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: <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. <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. 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. Caution: Setting this to Yes has the potential to allow rogue inbound requests from unauthenticated remote clients. If you specify No for this setting, the Expressway prevents rogue requests.	No

Table 10 Settings for MRA access control (continued)

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 SAML SSO Authentication Over the Edge, page 1.</p>	–

Table 10 Settings for MRA access control (continued)

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 <i>is</i> 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

Table 11 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>Notes:</p> <p>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)
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)

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2021 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)