Cisco Expressway X8.10.4

Release Notes

First Published: July 2017

Last Updated: September 2018

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

Change History

Table 1 Release Notes Change History

Date	Change	Reason
September 2018	Update Limitations that Expressway does not support the IM and Presence Service subgroups feature over MRA connections.	Documentation
July 2018	Add caution not to use the built in Expressway forward proxy.	Documentation
April 2018	Fix incorrect port information for forward proxy in Changes to TLS and Cipher Suite Defaults	Documentation
February 2018	Update Limitations that interoperated Microsoft calls fail if clustered Expressway-E node placed in maintenance mode	Documentation
December 2017	Update Feature History, Open and Resolved Issues	X8.10.4 maintenance release

Table 1 Release Notes Change History (continued)

Date	Change	Reason
November 2017	Update Feature History, Open and Resolved Issues and Limitations	X8.10.3 maintenance release
October 2017	Added preview feature "Built-in-Bridge Recording over MRA"	New in X8.10.2
September 2017	Update Limitations with maximum of 65 option keys	Documentation
September 2017	Update Open and Resolved Issues and Limitations	X8.10.2 maintenance release
August 2017	Clarify information about TURN on port 443	Documentation
August 2017	Add summary of X8.10.1 software enhancements. Update Open and Resolved Issues	X8.10.1 maintenance release
July 2017	Update Notable Issues in this Version about licensing issues for Jabber Guest calls in Single NIC deployments	Documentation
July 2017	Update Prerequisites and Software Dependencies with information for deployments that interoperate with Microsoft environments	Documentation
July 2017	First publication	X8.10

Supported Platforms

Table 2 Expressway Software Versions Supported by Platform

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
CE500* (Expressway pre-installed on UCS C220 M3L)	52C######	X8.1.1 onwards
CE1000* (Expressway pre-installed on UCS C220 M3L)	52B######	X8.1.1 onwards
CE1100 (Expressway pre-installed on UCS C220 M4L)	52D######	X8.6.1 onwards

* As of 26th February 2016, you cannot order the CE500 and CE1000 appliances from Cisco. See the End-of-sale announcement for other important dates in the lifecycle of these platforms.

Advance Notice - Support for CE500 and CE1000 Appliances to be Withdrawn

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

Related Documents

Table 3 Links to Expressway User Documents

Installation	**For Expressway:** ■ *Cisco Expressway Virtual Machine Installation Guide* on the Expressway installation guides page. ■ *Cisco Expressway CE1100 Appliance Installation Guide* on the Expressway installation guides page. **For VCS:** *Cisco Video Communication Server CE1100 Appliance Installation Guide* on the VCS installation guides page.
Administration and maintenance (includes reference information)	**For Expressway:** *Cisco Expressway Administrator Guide* on the Cisco Expressway Series maintain and operate guides page. **For VCS:** *Cisco TelePresence VCS Administrator Guide* on the Cisco TelePresence VCS maintain and operate guides page. **For Expressway:** *Cisco Expressway Serviceability Guide* on the Cisco Expressway Series maintain and operate guides page. **For VCS:** *Cisco TelePresence VCS Serviceability Guide* on the Cisco TelePresence VCS maintain and operate guides page.
Registrar/ basic call control	**For Expressway:** *Cisco Expressway Registrar Deployment Guide* on the Expressway configuration guides page. **For VCS:** *Cisco Single VCS Control – Basic Configuration Deployment Guide* on the VCS configuration guides page.
Firewall traversal	**For Expressway:** *Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide* on the Expressway configuration guides page. **For VCS:** *Cisco TelePresence VCS Basic Configuration (Control with Expressway) Deployment Guide* on the VCS configuration guides page.
Cisco Spark	Hybrid services knowledge base
Clustering	*Cisco Expressway Cluster Creation and Maintenance Deployment Guide* on the Cisco Expressway Series configuration guides page.
Certificates	*Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page.
Unified Communications	*Mobile and Remote Access Through Cisco Expressway* on the Expressway configuration guides page.
Cisco Meeting Server	*Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure* on the Expressway configuration guides page. *Cisco Meeting Server API Reference Guide* on the Cisco Meeting Server programming guides page. Other Cisco Meeting Server configuration guides are available on the Cisco Meeting Server configuration guides page.

Table 3 Links to Expressway User Documents (continued)

Microsoft infrastructure	*Cisco Expressway with Microsoft Infrastructure Deployment Guide* on the Expressway configuration guides page. *Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet* on the Expressway configuration guides page.
Rest API	*Cisco Expressway REST API Reference Guide* on the Expressway installation guides page.

Feature History

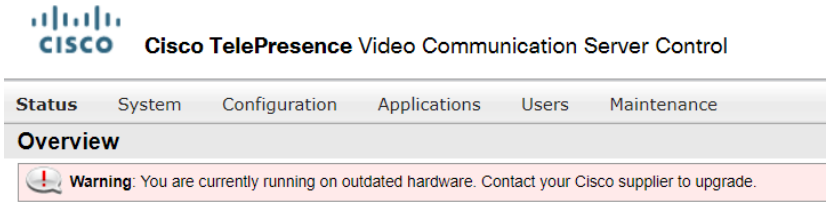
Table 4 Feature History by Release Number

Feature / change	X8.10	X8.10.1	X8.10.2	X8.10.3 (no change)	X8.10.4 (no change)
Built-in-Bridge Recording over MRA	Not supported	Not supported	Preview	Preview	Preview
Improved Push Notification Support for MRA	Preview	Supported	Supported	Supported	Supported
Self-Describing Tokens Support for MRA (OAuth tokens with refresh)	Preview	Supported	Supported	Supported	Supported
Access Control Configuration Changes for MRA	Supported	Supported	Supported	Supported	Supported
Access Policy Support for MRA	Preview	Preview	Preview	Preview	Preview
Changes to TLS and Cipher Suite Defaults	Supported	Supported	Supported	Supported	Supported
AES-GCM Cipher Mode for Media Encryption	Supported	Supported	Supported	Supported	Supported
Delayed Cisco XCP Router Restart for Multitenancy	Supported	Supported	Supported	Supported	Supported
Server Name Indication for Multitenancy	Supported	Supported	Supported	Supported	Supported
Session Identifier Support	Supported	Supported	Supported	Supported	Supported
REST API Expansion	Supported	Supported	Supported	Supported	Supported
Smart Call Home (Not new in X8.10. Included for information due to its preview status)	Preview	Preview	Preview	Preview	Preview
Multiple Presence Domains through MRA (Not new in X8.10. Included for information due to its preview status)	Preview	Preview	Preview	Preview	Preview

Changes in X8.10.4

- Various security enhancements to the Expressway software.
- CSCvg15240. Applies to deployments with IM and Presence Service federation, where the federation server is behind a NAT. Previous releases had an issue with missing presence status for a Jabber user added into a Skype for Business buddy list. The issue is now fixed.
- Clustered systems. The maximum supported round-trip delay / RTT has been tested and verified at 80ms (up from the previous verified figure of 30ms).

- The system warns you if you are on hardware that is no longer supported. Contact your Cisco supplier to find out about our migration program.



- CSCvd68778 is resolved in this release, which means that Extension Mobility works via MRA for those Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series phones that support MRA.

Changes in X8.10.3

Important! All Expressway software versions from X8.9 include a fix for an issue with the Call History table. In certain circumstances this issue may cause severe system problems (CDETS CSCvc58081 refers). If you are not already running a fixed version, then we strongly recommend that you upgrade to this X8.10.*n* release.

- Cisco Spark Hybrid Services. For new registrations of Expressways to Cisco Spark, the Expressway must be running X8.10.3 or later. Existing registrations still work with Expressway X8.9 or later, although we recommend that you always keep the host Expressway at the latest feature release.
- CSCvg09088. Applies to Mobile and Remote Access deployments with multiple IM and Presence Service clusters that are not all configured with the same OAuth capabilities. Previously, the Expressway-C XCP component did not always communicate with a user's home IM and Presence Service cluster. This could result in a mismatch of authorization support and cause Jabber client sign-ins to fail over MRA. The issue is now fixed.
- Added a SIP maximum message size setting. A new **SIP max size** setting in the Expressway user interface (**Configuration > Protocols > SIP > Advanced**) defines the maximum SIP message buffer on the Expressway. The default is 32,768 bytes, and the value is configurable up to 1 MB.
- CSCvf85709. From X8.10.2, dual-homed conferencing through Expressway and Meeting Server with an AVMCU invoked on the Microsoft side was limited to conferences with 10 or fewer participants. This limitation no longer exists from X8.10.3, providing the SIP maximum message size is set to 32,768 bytes or greater (see previous point).
- Removed the maximum SDP payload setting. The **SDP max size** setting is removed from the Expressway user interface (it used to be on **Configuration > Protocols > SIP > Advanced**). Now replaced by the new **SIP max size**.
- This release provides new Expressway language packs which reflect security changes since the previous packs were created, and the latest web user interface. Instructions for installing or updating the packs are in the *Expressway Administrator Guide*. The previous language packs do not work with this release.

Changes in X8.10.2

(Preview) Built-in-Bridge Recording over MRA

The Expressway supports Built-in-Bridge recording over MRA. This feature can help your organization to prepare for the telephone recording requirements of the European Union's *Markets in Financial Instruments Directive* (MiFID II), which comes into effect in January 2018.

When Built-in-Bridge (BiB) is enabled, Cisco Unified Communications Manager forks the call to/from the endpoint to a media recording server. BiB can be used to record calls that are made or received by users working off-premises.

BiB over MRA requires the following components:

- Any compatible clients:
  - Cisco Jabber for Windows 11.9
  - Cisco Jabber for Mac 11.9
  - Cisco Jabber for iPhone and iPad 11.9
  - Cisco Jabber for Android 11.9
  - Cisco IP Phone 7811, 7821, 7841, and 7861
  - Cisco IP Phone 8811, 8841, 8845, 8851, 8861, and 8865
- Registrar/call control agent: **Cisco Unified Communications Manager 11.5(1)SU3** (BiB is not supported on Expressway-registered endpoints)
- Edge traversal: **Expressway X8.10.2**
- Recording server: Out of scope for this document.

Other changes

- CSCvf50910 **XMPP Federation fails for multiple Expressway clusters**. This was previously highlighted in the *Notable Issues* section of these release notes, and is now fixed.
- CSCve41422 **MS Interop dual-homing feature fails through Expressway and Meeting Server**. This is now fixed to support up to **10 users**, providing the **SIP max size** value defined in your SIP settings is 32,768 bytes (the default) or greater.
- Various corrections to the user documentation.

Note: As well as these Expressway changes, you no longer need to use TLSv1.0 for calls to Webex via Expressway.

Changes in X8.10.1

- The Expressway-E TURN server can now optionally be configured on port 443 for use as a generic server – but is NOT currently supported for use with Cisco Meeting Server.

  We've done this so that clients can use TURN even in environments with restrictive firewall policies.

  Some limitations exist if you want to use port 443 for TURN:
  - Not currently supported with Cisco Meeting Server.
  - You must first change the web administrator port to a different port (**System > Administration**).
  - The option to use port 443 does not apply to large systems – Expressway-E Large OVAs or large scale appliances.
- Expressway virtual machines can now run on VMware ESXi 6.5.
- A new web interface control for the AES GCM media encryption mode is available for Mobile and Remote Access (MRA) deployments. When you add a Unified CM node (**Configuration > Unified Communications > Unified CM servers**) you can now set **AES GCM support** to *On*.
- In multitenant mode, the system hostname you configure on the **System > DNS** page of the Cisco Expressway-E and in DNS for Cisco Jabber clients to register for MRA is now case insensitive.
- These features for MRA deployments are now fully supported; previously they were in preview status:
  - Improved push notification support for Cisco Jabber users with iOS devices
  - Self-describing token authorization (OAuth tokens with refresh)

Note: The TURN on port 443 change was actually made in X8.10, but because it wasn't included in earlier versions of X8.10 Release Notes, for convenience it's also referenced here.

Features in X8.10

New Features for Deployments with Mobile and Remote Access

These changes are relevant if your Expressway is configured for MRA.

Improved Push Notification Support for MRA

We introduced this feature in X8.10 **in preview status only**. It's fully supported from **X8.10.1**.

This feature applies if you have Cisco Jabber users with iOS devices (Cisco Jabber for iPhone and iPad) who sign in remotely. Expressway deployments that are configured for MRA can support Apple's cloud-based Push Notification service. From X8.9.1, we supported Push Notifications for IM and Presence Service instant messages. From X8.10, we support them for voice and video calls too. Push Notifications are only used for Jabber for iPhone and iPad clients. Android, Windows, and Mac users are unaffected.

Note: If Unified CM detects a remote or mobile Jabber for iPhone and iPad connection, it always sends a Push Notification as well as a SIP Invite.

Prerequisites and recommendations

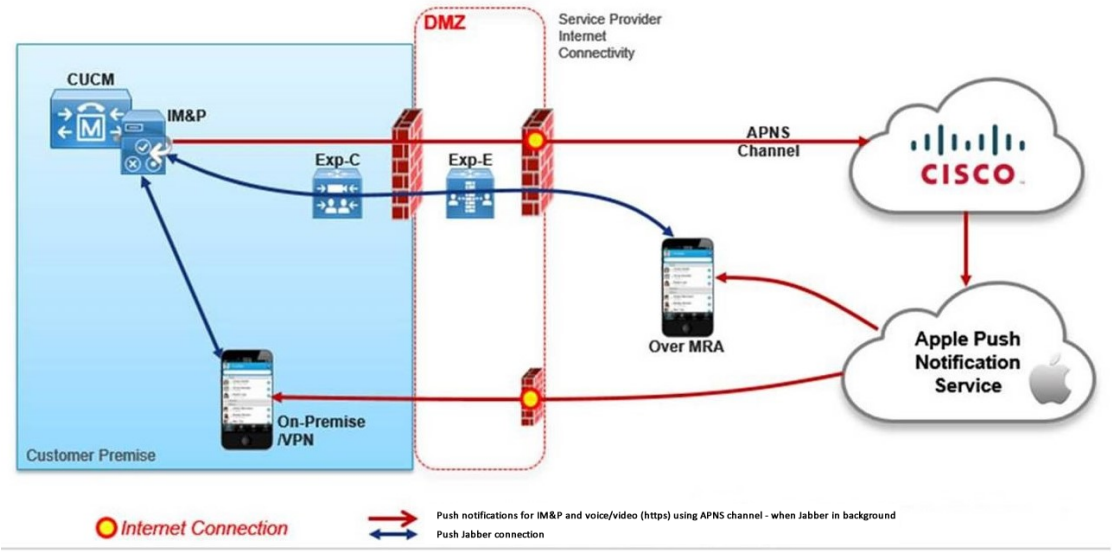
No specific configuration is needed on the Expressway for Push Notifications, assuming Expressway-E is already providing Mobile and Remote Access (MRA) for Jabber iOS devices. However, these prerequisites and recommendations apply:

- Push Notifications in the Expressway require a network connection between Expressway and the Cisco WebEx cloud, and between Cisco Jabber and the Push Notification servers in the Apple cloud. **They cannot work in a private network, with no internet connection.**
- Expressway is already providing Mobile and Remote Access for Jabber for iPhone and iPad. MRA must be fully configured (domain, zone, server settings).
- Depending on your Unified CM configuration, the Unified CM may need a forward proxy to send Push Notifications to the Cisco Collaboration Cloud.
- We recommend using self-describing token authorization.
- Expressway-E **restart required for Push Notifications with instant messages**. After you enable Push Notifications on the IM and Presence Service you need to restart the Expressway-E. Until the restart, Expressway-E can't recognize the push capability on IM and Presence Service, and does not send PUSH messages to the Jabber clients.
- You need the following Push Notification-enabled releases (or higher) on Cisco Unified Communications Manager, IM and Presence Service, and the Jabber devices:
  - Expressway X8.10.1 or later (preview status only in X8.10)
  - Cisco Jabber for iPhone and iPad iOS 11.9
  - Cisco Unified Communications Manager 11.5(SU3)
  - Cisco Unified Communications Manager IM and Presence Service 11.5(SU3)
  - Cisco Unity Connection 11.5(SU3)

Why have we implemented support for Push Notifications?

Apple now deprecates the VoIP Background Mode that allows Jabber iOS to keep a SIP session open even when the app is running in the background. Push Notifications allow Unified CM to tell Jabber about incoming calls and messages. Then Jabber can reconnect to Unified CM to retrieve the message or answer the call. Jabber uses the new self-describing token feature in this release to help it to do this quickly.

Figure 1 Push Notifications architecture



Information about Push Notifications in Unified Communications products

For information about Push Notifications in Unified CM and IM and Presence Service, see *Deploying Push Notifications for Cisco Jabber on iPhone and iPad* available from the Cisco Unified Communications Manager documentation pages on Cisco.com.

About the Expressway forward proxy service

CAUTION: At present the built-in Expressway forward proxy is not suitable for use with Cisco Unified Communications Manager and/or IM and Presence Service, and is not supported for those products. The forward proxy is in the Expressway user interface, but it should not be used. This means that if you require a forward proxy deployment, you need to use a suitable third-party HTTPS proxy.

Self-Describing Tokens Support for MRA (OAuth tokens with refresh)

We introduced this feature in X8.10 **in preview status only**. It's fully supported from **X8.10.1**.

Expressway supports using self-describing tokens as an MRA authorization option. (Set "**Authorize by OAuth token with refresh**" to *Yes*.) Self-describing tokens offer significant benefits:

- Token refresh capability, so users don't have to repeatedly re-authenticate.
- Fast authorization.
- Access policy support. The Expressway can enforce MRA access policy settings applied to users on the Unified CM.
- Roaming support. Tokens are valid on-premises and remotely, so roaming users don't need to re-authenticate if they move between on-premises and off-premises.

The Expressway uses self-describing tokens in particular to facilitate Cisco Jabber users. Jabber users who are mobile or work remotely, can authenticate while away from the local network (off-premises). If they originally authenticate on the premises, they don't have to re-authenticate if they later move off-premises. Similarly, users don't have to re-authenticate if they move on-premises after authenticating off-premises. Either case is subject to any configured access token or refresh token limits, which may force re-authentication.

For users with Jabber iOS devices, the high speeds supported by self-describing tokens optimize Expressway support for Apple Push Notifications (APNs).

We recommend self-describing token authorization for all deployments, assuming the necessary infrastructure exists to support it. Subject to proper Expressway configuration, if the Jabber client presents a self-describing token then the Expressway simply checks the token. No password or certificate-based authentication is needed. The token is issued by Unified CM (regardless of whether the configured authentication path is by external IdP or by the Unified CM). Self-describing token authorization is used automatically if all devices in the call flow are configured for it.

The Expressway-C performs token authorization. This avoids authentication and authorization settings being exposed on Expressway-E.

Prerequisites

- Expressway is already providing Mobile and Remote Access for Cisco Jabber.
- All other devices in the call flow are similarly enabled.
- You have the following minimum product versions installed, or later:
  - Expressway X8.10.1 (preview status only in X8.10)
  - Cisco Jabber 11.9 (on any/all client platforms)

    If you have a mix of Jabber devices, with some on an older software version, the older ones will use simple OAuth token authorization (assuming SSO and an IdP are in place).
  - Cisco Unified Communications Manager 11.5(SU3)
  - Cisco Unified Communications Manager IM and Presence Service 11.5(SU3)
  - Cisco Unity Connection 11.5(SU3)
- Make sure that self-describing authentication is enabled on the Cisco Expressway-C (" **Authorize by OAuth token with refresh**" setting) and on Unified CM and/or IM and Presence Service (" **OAuth with Refresh Login Flow**" enterprise parameter).
- You must refresh the Unified CM nodes defined on the Expressway. This fetches keys from the Unified CM that the Expressway needs to decrypt the tokens.

Limitations

Important: From X8.10.1, the Expressway fully supports the benefits of self-describing tokens (including token refresh, fast authorization, and access policy support). However, not all of the benefits are actually available throughout the wider solution. Depending on what other products you use (Unified CM, IM and Presence Service, Cisco Unity Connection) and what versions they are on, not all products fully support all benefits of self-describing tokens.

Note about automated intrusion protection

With OAuth token authentication, in some circumstances Cisco Jabber may trigger the automated intrusion protection on the Expressway-E. If this happens, a workaround is described in the Troubleshooting appendix of the *Mobile and Remote Access Via Expressway Deployment Guide* on Expressway configuration guides page.

Access Control Configuration Changes for MRA

Configuration for MRA access control (authentication and authorization settings) is improved in this release.

- You can configure a more detailed, granular level of control than before.
- All configuration settings are collected onto the Expressway-C.
- Single sign-on authorization in previous releases is now simple OAuth token authorization. The web UI option is **Authorize by OAuth token**.
- The setting **Check for internal SSO availability** in previous releases is now **Check for internal authentication availability**.
- MRA access control previously defaulted to username and password authorization, which did not need explicit configuration. From X8.10, if you want username and password authorization you must manually configure it. The web UI option is **Authorize by user credentials**.

- For new customers, the MRA access control settings default to self-described token authorization, managed by the Unified CM (not an external IdP), with all other access control options off.
- Although you still enable MRA itself on Expressway-E, the MRA access control settings are now configured on Expressway-C.

Important: Information for existing MRA customers

If you already use the Expressway with MRA, the upgrade cannot preserve all of your existing settings. The X8.10 software **overwrites your currently configured MRA access control values**. The new upgrade values are detailed in the upgrade instructions later in these notes.

Because of these changes, we recommend some additional pre-upgrade checks and post-upgrade configuration for this release. The necessary steps are also described later in the upgrade instructions.

(Preview) Access Policy Support for MRA

This feature is currently in preview status only.

From X8.10, the Expressway will enforce MRA access policy settings specified on the Unified CM. These are optionally configured on the user profiles in Unified CM, to define which services individual users can access (None, IM&P, Voice & Video, or All). The Expressway only enforces MRA access policy if these conditions apply:

- The Expressway is configured to process self-describing tokens for MRA authorization (set **Authorize by OAuth token with refresh** to *On*).
- Other products in the call path also support self-describing tokens, including the access policy element of the tokens.

Note: As MRA access policy can only be enforced if the clients use self-describing tokens, it's most effective when self-describing token authorization is the *only* permitted authorization method for MRA.

Changes to TLS and Cipher Suite Defaults

From X8.10, Expressway defaults to TLS version 1.2 when establishing secure connections for the following services:

- HTTPS
- SIP
- XMPP
- UC server discovery
- Forward proxy
- Reverse proxy

For improved security, TLS 1.2 is recommended for all encrypted sessions. If required (typically for compatibility reasons with legacy equipment) the minimum TLS versions can be configured to use versions 1.0 or 1.1.

On upgrade, previous behavior and defaults persist so you won't be defaulted to TLS version 1.2. However, new installations will use the new defaults. So for new installations you should check that TLS version 1.2 is supported by all browsers and equipment that must connect to Expressway.

New cipher suites from X8.10

You can configure the cipher suite and minimum supported TLS version for each service on the new **Maintenance > Security > Ciphers** page, and they are also configurable via the CLI and the API. More information is provided in the online help and *Administrator Guide*.

These services and new cipher suites are shown in the table (cipher strings are in OpenSSL format):

Services	Cipher Suite Values (Defaults)
Forward proxy TLS ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
HTTPS ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
Reverse proxy TLS ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
SIP TLS ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH
UC server discovery TLS ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
XMPP TLS ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL

CLI cipher suite changes from X8.10

The cipher configuration changed from `xConfig Sip TLS CipherSuites` to `xConfig Ciphers SIPTLSCiphers Value`. This uses the same format as the new configuration for ciphers for the other services.

The maximum string length for cipher suites is now 2048 characters.

Known issues with TLS version 1.2 support

- Legacy endpoint version support:
  - MXP and TE Series devices do not support TLSv1.2.
  - TC < 7.3.3 does not support TLSv1.1 or TLSv1.2.
  - TC 7.3.6 removed support for TLSv1.0.
  - Jabber Video for TelePresence on Windows 7 does not support TLSv1.1/1.2 (supported from Windows 8.1).
- Windows:
  - Windows 7 and Windows Server 2008 R2 added TLSv1.1/1.2 support but **off** by default; post Windows 8.1 they are on by default. This impacts Jabber Video for TelePresence, TMS, Lync and other software and services running on Windows using the OS TLS APIs.
  - Windows OS 2003.does not support TLSv1.1 or TLSv1.2.
- Third-party endpoints:
  - Lifesize Icon 600 does not support TLSv1.2.
- Restarts:
  - SIP requires a restart after changing cipher suite configuration or TLS protocol version.
  - XCP requires a restart after changing cipher suite configuration or TLS protocol version.

Ports

The forward proxy destination port is 8445 and the source port is ephemeral. (The Expressway forward proxy is dependent on support by your Unified CM software.)

The reverse proxy listens on port 8443.

AES-GCM Cipher Mode for Media Encryption

As part of our ongoing security improvement work, from X8.10 we've improved the media encryption capabilities of the Expressway. All zones that can do media encryption now support the AES-GCM cipher mode for encrypting / decrypting SRTP media streams. (AES-GCM refers to the Galois/Counter Mode used with Advanced Encryption Standard cipher.)

This feature is off by default. If you know your endpoints can use GCM to encrypt media, then you may see a performance improvement by enabling this mode on the zones in the media path.

Notes:

- As the new media encryption mode is off by default, it is off for the CEtls zones that are automatically created for MRA. These zones are not editable through the web interface. To use AES GCM media encryption with MRA:
  - Zones that have not yet been auto-created. When you add the Unified CM server (**Configuration > Unified Communications > Unified CM servers**) set **AES GCM support** to *On*. (This web UI setting was introduced in X8.10.1.)
  - Zones that already exist. Configure the zones using the CLI command `xConfiguration Zones Zone index Neighbor SIP Media AesGcm Support: "On"`

    (Use `xstatus zone` to list the zones and their index numbers.)
- CE Series endpoints, and 7800 Series and 8800 Series phones don't know that they can offer AES GCM media encryption when they are in "edge" mode. They can offer this media encryption when they are directly registered to Unified CM (not through MRA).

  When these endpoints register through MRA, the Expressway-Cwill negotiate AES-128 media encryption with them instead.
- Cisco Jabber 11.9 can negotiate AES GCM, but it is not enabled by default when Jabber is in "edge" mode. You can modify the behavior using the *EnableNGEPolicy* parameter. See the *Parameters Reference Guide for Cisco Jabber* at the Jabber install and upgrade guides page.

Delayed Cisco XCP Router Restart for Multitenancy

The delayed Cisco XCP Router restart feature is part of Cisco Hosted Collaboration Solution (HCS), and is only available when the Expressway-E is in multitenant mode. The Expressway-E enters multitenant mode when you add a second Unified CM traversal zone with a new SIP domain.

Note: In multitenant mode, you must configure the system hostname on the **System > DNS** page of the Cisco Expressway-E to match the hostname configured in DNS (case-specific before X8.10.1, case insensitive from X8.10.1). Otherwise Cisco Jabber clients will be unable to register successfully for MRA.

Multitenancy allows a service provider to share an Expressway-E cluster among multiple tenants. Each tenant has a dedicated Expressway-C cluster that connects to the shared Expressway-E cluster.

Certain configuration changes on the Expressway-E cluster, or a customer's Expressway-C cluster, require a restart of the Cisco XCP Router on each Expressway-E in the shared cluster. The restart is required for Cisco XCP Router configuration changes to take effect across all nodes in a multitenant Expressway-E cluster. The restart affects all users across all customers.

To reduce the frequency of this restart, and the impact on users, you can use the delayed Cisco XCP Router restart feature.

Note: Without the delayed restart feature enabled, the restart happens automatically and occurs each time you save any configuration change that affects the Cisco XCP Router. If multiple configuration changes are required, resulting in several restarts of the Cisco XCP Router, it can adversely affect users. We strongly recommend that multitenant customers enable the delayed Cisco XCP Router restart feature.

Server Name Indication for Multitenancy

Multitenancy is part of Cisco Hosted Collaboration Solution (HCS), and allows a service provider to share a Expressway-E cluster among multiple tenants.

Using the Server Name Indication (SNI) protocol extension within TLS, the Expressway can now store and use domain-specific certificates that can be offered to a client during the TLS handshake. This capability allows seamless integration of endpoints registering through MRA in a multitenant environment, and ensures the certificate domain name matches the client's domain. During a TLS handshake, the client includes an SNI field in the *ClientHello*

request. The Expressway looks up its certificate store and tries to find a match for the SNI hostname. If a match is found the domain-specific certificate is returned to the client.

Note: In multitenant mode, you must configure the system hostname on the **System > DNS** page of the Cisco Expressway-E to match the hostname configured in DNS (case-specific before X8.10.1, case insensitive from X8.10.1). Otherwise Cisco Jabber clients will be unable to register successfully for MRA.

See *Multitenancy with Cisco Expressway* on the Cisco Hosted Collaboration Solution page.

Session Identifier Support

From X8.10 the Expressway can support SIP "session identifiers". Assuming all devices in the call use session identifiers, the mechanism uses the *Session-ID* field in SIP headers to maintain a unique code through the entire transit of a call. Session identifiers are useful for investigating issues with calls that involve multiple components, as they can be used to find and track a specific call on the Expressway server. Support for session identifiers includes the SIP side of interworked SIP/H.323 calls, and calls to and from Microsoft systems. Session identifiers are defined in RFC 7989.

REST API Expansion

In X8.10, the API to simplify remote configuration has been expanded. Third party systems, such as Cisco Prime Collaboration Provisioning, can now use the API to configure the following features / services on the Expressway:

- Admin account
- Firewall rules
- SIP configuration
- TURN server configuration
- Domain certificates for Server Name Identification

The API is self-documented using REST API Markup Language (RAML).

See *Cisco Expressway REST API Reference Guide* on the Expressway installation guides page.

(Preview) Smart Call Home

This feature is currently in preview status only.

Smart Call Home is a free embedded support capability for Expressway. It offers proactive diagnostics and real-time alerts, enabling higher network availability and increased operational efficiency.

Smart Call Home notifies users of Schedule- and Event-based notifications.

- Schedule-based: inventory, telemetry and configuration messages used to generate a Device Report and improve hardware and software quality by identifying failure trends. You can find these notifications posted on the first day of every month.
- Event-based: asynchronous events already supported by Expressway such as alarms and ACRs. You will find these notifications posted to the Smart Call Home server as and when they occur.

You can opt to keep your organization's details anonymous. In this case Expressway sends reports to the Smart Call Home server as normal, but the server does not send out notifications.

Other Software Changes and Enhancements

- The upgrade process between major releases (for example, from X7.*n* to X8.*n*) has always needed a release key. The upgrade process now makes it clearer to administrators when a key is needed. And provides an opportunity to enter the key after you start the upgrade.

- You can now specify that anyone signing in to the Expressway must first acknowledge a customizable welcome message. The system displays an acceptance button, which users must click before they're allowed to continue.
- From X8.10, the Certificate Signing Request (CSR) generator no longer allows you to select the SHA-1 Digest algorithm for your certificate's signature. The remaining options are SHA-256, SHA-384, and SHA-512.
- The upload mechanism for server security certificates (**Maintenance > Security > Server certificate**) displays a warning if the certificate fails to meet certain criteria. Cases when the warning is displayed include:
  - Certificate does not have an acceptable level of security.
  - Certificate is missing a common name (CN) attribute.

    An alarm is also raised in this case, because some Expressway services don't work without the common name (MRA, Jabber Guest, and the Web Proxy for Cisco Meeting Server).
  - The certification authority (CA) or certificate revocation list (CRL) is not recognized.

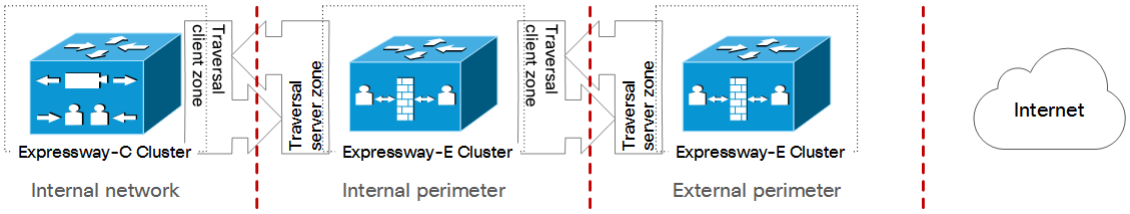
  The certificate upload is not prevented.
- For devices connected through MRA, the Expressway now provides passthrough support of Unified CM shared line features on Cisco Jabber clients running 11.9 or later, and on Collaboration Endpoint devices running CE8.3.0 or later. (The previous Expressway release already supported shared line for MRA-connected Cisco IP Phone 78xx and 8811, 8841, 8845, 8861 and 8865 devices with Path Header support enabled.)
- The Expressway-E TURN server can now optionally be configured on port 443 for use as a generic server - but is NOT currently supported for use with Cisco Meeting Server.

  We've done this so that clients can use TURN even in environments with restrictive firewall policies. Some limitations exist if you want to use port 443 for TURN:
  - Not currently supported with Cisco Meeting Server.
  - You must first change the web administrator port to a different port (**System > Administration**).
  - The option to use port 443 does not apply to large systems - Expressway-E Large OVAs or large scale appliances.
- From X8.10, the requirement to have a 10 Gbps NIC in order to achieve the scalability of a large system is removed. It is now possible to have the capacity of a large system with a 1 Gbps NIC subject to your bandwidth constraints.
  However, if you upgrade a Medium system with a 1 Gbps NIC to X8.10 or later, Expressway automatically converts the system to a Large system. As a result,Expressway-E listens for multiplexed RTP/RTCP traffic on default demultiplexing ports for Large systems (36000 to 36011); instead on demultiplexing ports that are configured for Medium systems. In this case, the Expressway-E drops the calls because these ports (36000 to 36011) are not open on the firewall. If you encounter this problem, open the default demultiplexing ports for Large systems on the firewall.
- Expressway **no longer supports ESXi 5.0 or ESXi 5.1 for virtual deployments**. You must use ESXi 5.5 or ESXi 6.0 (or ESXi6.5 if you have Expressway X8.10.1). See https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/product-lifecycle-matrix.pdf
- The IX filtering setting (**SIP UDP/IX filter mode**) defaults to *Off* for the preconfigured **Cisco Unified Communications Manager** zone profile. Previously the default was *On.* The default is still *On* for other preconfigured profiles, including **Cisco Unified Communications Manager (8.6.1 or later)**.

- Hybrid Services changes:
  - From version X8.10, the connectors used for some Cisco Spark Hybrid Services may co-reside with the Expressway-C that is used with Call Service. This co-residency is subject to limitations on user numbers as described in the relevant Hybrid Services documentation. Previously we recommended a dedicated Expressway-C for hosting the connectors. See Hybrid Services documentation for more detail.
  - Expressways that will be used to host connectors for Cisco Spark Hybrid Services, must be on version X8.10.3 or later before you register them to Cisco Spark.

    If the connector host Expressway is already registered to Cisco Spark then we still support X8.9. However, to maintain compatibility we recommend that you keep the host Expressway up to date with the latest feature release. The Expressway-based connectors check the host version and warn if it's more than one feature release behind. For example, when X8.10 is the latest feature release, the connectors will work with X8.9 and X8.10. We cannot guarantee compatibility with older versions of the host Expressway.
- For business-to-business Expressway deployments, you can configure firewall traversal chaining. As well as acting as a traversal server, Expressway-E can act as a traversal client to another Expressway-E.

Figure 2 Example of Two Chained Expressway-Es



If you chain two Expressway-Es for example (pictured), the first Expressway-E is a traversal server for the Expressway-C. That first Expressway-E is also a traversal client of the second Expressway-E. The second Expressway-E is a traversal server for the first Expressway-E.

Note:

- Traversal chaining is not supported for Mobile and Remote Access deployments.
- This capability was formally introduced to the Cisco Expressway Series in version X8.10. It has been possible with the Cisco TelePresence VCS since firewall traversal was introduced.

User Interface Menu Changes

Some menu names in the Web UI are different in this release, as follows:

- **Maintenance > Security Certificates** is now just **Maintenance > Security**
- **Status > Unified Communications > SSO Statistics** is now **Status > Unified Communications > MRA Authentication Statistics**
- **HTTP allow list > Editable rules** is now **HTTP allow list > Editable inbound rules**
- **HTTP allow list > Automatically added rules** is now **HTTP allow list > Automatic inbound rules**
- **HTTP allow list > Automatic outbound rules** is new in this release
- Various other new menus are added to support the features introduced by this release

Documentation Changes

We continue to phase out Cisco VCS documentation. Previously we provided two separate variants of most customer support documents, for the VCS and the Expressway. From X8.10 we begin to provide Expressway versions

only. The Expressway versions will include any relevant VCS-specific information. This change will happen gradually over time.

- Cisco Expressway documents: http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html
- Cisco VCS documents: http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/tsd-products-support-series-home.html

MRA limitations removed from Release Notes. We've removed the lists of unsupported items in Mobile and Remote Access from the Limitations section of these notes. This information is available in the *Mobile and Remote Access Through Cisco Expressway Deployment Guide* on the Expressway Configuration Guides page.

Minor enhancements to the documents. As well as adding the release features, we've made some minor documentation corrections and changes.

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 X8.10.4
- Issues resolved by X8.10.3
- Issues resolved by X8.10.2
- Issues resolved by X8.10.1
- Issues resolved by X8.10

Notable Issues in this Version

Licensing issues with Jabber Guest calls in Single NIC deployments

Currently the software has some unexpected rich media session (RMS) licensing behavior for Jabber Guest calls in Single NIC deployments, as follows:

- Each Jabber Guest call ought to consume an RMS license on the Cisco Expressway-E. In reality, the RMS licenses are currently consumed on the Cisco Expressway-C. This issue was identified in X8.10. CDETS CSCvf34525 refers. Contact your Cisco representative if you are affected by this issue.
- An earlier, related issue was identified from X8.8. 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. CDETS CSCva36208 refers.

Note that we recommend the Dual NIC Jabber Guest deployment.

Expressway B2BUA drops some RTCP multistreaming Refresh packets during decryption in Cisco WebEx calls CSCvc47502 and CSCvc34689

Note: This software version is only vulnerable to this issue **if** the other end of the call involves a VCS or Expressway running X8.7*x* or earlier.

This issue affects certain TelePresence configurations with Cisco VCS or Cisco Expressway software versions X8.7x.

Affected components

- Cisco TelePresence IX5000 Series immersive endpoint (all versions)
- Cisco VCS or Cisco Expressway versions X8.7.x and earlier
- Cisco TelePresence Server versions 4.3, 4.4(1.9), 4.2 or earlier
- Cisco TelePresence Server versions 4.4(1.16) or later
- Cisco TelePresence TX9000 Series
- Cisco TelePresence System (CTS)
- Other video endpoints

Description

The issue affects calls from immersive TelePresence systems operating in TIP/MUX mode, or other TelePresence systems operating in multistreaming mode, when encrypted/decrypted by VCS or Expressway X8.7.x. The symptoms are pixelated video which gets progressively worse, then the endpoint terminates the call (because problems with decoding received media lead to perceived packet loss). Other video and quality issues may also occur.

With the TelePresence Server, the following behavior may trigger the issue:

- Versions 4.3 or 4.4(1.9): sharing for more than the session refresh.
- Versions 4.2 or earlier, or 4.4(1.16) or later: starting and stopping sharing multiple times.

Note: This issue does not occur if any of the following cases apply:

- Encryption to / from the VCS / Expressway is disabled.
- TIP/MUX is disabled (immersive systems).
- Multistream is disabled.
- If Cisco WebEx is involved, and WebEx video callback (Call My Video System) is used.

Background

The mechanism for session state maintenance in X8.7.x is susceptible to issues when a high number of SSRC IDs are present in encrypted calls. These include calls from immersive endpoints that use TIP, or from endpoints operating in multistream mode. This issue was resolved by Expressway X8.8.x and later. However, this issue can affect encrypted calls where one of the VCS / Expressways at either end of the call leg is still on X8.7.x while the other is on X8.8.x or later.

Recommendation - Upgrade X8.7.x systems

The CMR Cloud infrastructure (Cisco WebEx) was upgraded from X8.7 to resolve the issue for customers that have VCS or Expressway X8.8.x on-premises. This means that other customers using CMR Hybrid, who have VCS / Expressway X8.7.x on-premises, could now see this issue. We strongly recommend that you upgrade your Cisco VCS / Expressway X8.7.x if you are using multistream/immersive endpoints for encrypted calls with other Cisco infrastructure, like CMR Cloud or third-party partners.

Limitations

Some Expressway Features are Preview or Have External Dependencies

Important! 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. Where customers may still benefit from using the feature, it will be marked 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.

The following Expressway features are currently provided in preview status only, or depend on other product software versions which are not yet available

- Built-in-Bridge Recording over MRA
- Access Policy Support for MRA
- Smart Call Home
- Multiple Presence Domains through MRA

Unsupported Functionality

- The Expressway does not terminate DTLS. We do not support DTLS for securing media. SRTP is used to secure calls instead, and attempts to make DTLS calls through Expressway will fail.

  The Expressway does insert the DTLS protocol in the SDP, but only for the purpose of traversing the encrypted iX protocol.
- The Expressway does not support the SIP UPDATE method (RFC 3311). Features that rely on this method will not work as expected.
- Audio calls may be licensed as video calls in some circumstances. Calls that are strictly audio-ONLY consume fewer licenses than video calls. However, when audio calls include non-audio channels, such as the iX channel that enables ActiveControl, they are treated as video calls for licensing purposes.
- **CAUTION: At present the built-in Expressway forward proxy is not suitable for use with Cisco Unified Communications Manager and/or IM and Presence Service, and is not supported for those products. The forward proxy is in the Expressway user interface, but it should not be used. This means that if you require a forward proxy deployment, you need to use a suitable third-party HTTPS proxy.**

Virtual Systems

With physical Expressway appliances, the **Advanced Networking** option 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).

Language Packs

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

Option Keys Only Take Effect for 65 Keys or Fewer

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

CDETS CSCvf78728 refers.

MS Lync / Office 365 Calls Fail if a Expressway-E Cluster Node is Placed in Maintenance Mode

This applies if you have clustered Expressway-E nodes and interoperate with Microsoft environments. If you place one of the Cisco Expressway-Es in maintenance mode, Lync or Office365 calls fail. This is because current lookup behavior by the Lync Edge server / Office 365 cloud is to fetch the FQDN of the *non-active* (maintenance mode) Expressway-E. Hence the call requests always fail.

MS Federation with Dual Homed Conferencing

If you use dual homed conferencing through Expressway and Meeting Server with an AVMCU invoked on the Microsoft side, the maximum SIP message size must be set to 32768 bytes (the default) or greater. Defined via **SIP max size** on **Configuration > Protocols > SIP**.

Conference Factory

If you have device registration licenses (room or desktop) on the Cisco Expressway-C, then some settings relating to the "Conference Factory" feature will appear in the Cisco Expressway-C user interface. This is an error, and the Conference Factory is not supported on Expressway. Please ignore these settings if you see them.

Licensing Behavior with Chained Expressway-Es

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

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

OAuth Token Authorization (Jabber)

For Jabber users, some limitations may exist with enforcing OAuth authorization by self-describing token as the only allowed authentication method. Users on older versions of Jabber can still authenticate by username and password, or traditional single sign-on.

Mobile and Remote Access

- Feature Limitations

  If you use Expressway for Mobile and Remote Access (MRA), some unsupported features and limitations currently exist. These are detailed in the *Mobile and Remote Access Through Cisco Expressway Deployment Guide* on the Expressway Configuration Guides page. Note that the following item was added to that guide after its initial publication for X8.10.x:

In this release, Expressway does not support the IM and Presence Service subgroups feature. If you use subgroups over MRA, Cisco Jabber logins will fail, or will fail intermittently.

- Endpoint Limitations

  Some recent Cisco IP Phones in both the 8800 Series and 7800 Series do not currently support MRA. For details of which 7800/8800 Series phones support MRA, see the "Prerequisites" section of the latest *Mobile and Remote Access Through Cisco Expressway* guide, or ask your Cisco representative.

Interoperability

The interoperability test results for this product are posted to http://www.cisco.com/go/tp-interop, where you can also find interoperability test results for other Cisco TelePresence products.

Notable Interoperability Concerns

X8.7.n (and earlier versions) of Expressway are not interoperable with Cisco Unified Communications Manager IM and Presence Service 11.5(1). This is caused by a deliberate change in that version of IM and Presence Service, and there is a corresponding change in Expressway X8.8 (and later).

To ensure continuous interoperability, you must upgrade your Expressway systems to X8.10 *before* you upgrade your IM and Presence Service systems to 11.5(1).

The symptom of the issue is an error on Expressway as follows:

```
Failed Unable to Communicate with <IM&P node address>. AXL query HTTP error "'HTTPError:500'"
```

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 to X8.10.4

Prerequisites and Software Dependencies

CAUTION: This section has important information about upgrade 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.

All Deployments

We do not support downgrades. Do not install a previous Expressway version onto a system that is running a newer version. If you do so, the system configuration will not be preserved.

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: Certificate validation was tightened up in X8.8.
  - Try the secure traversal test before and after upgrade (**Maintenance > Security > Secure traversal test**) to validate TLS connections.
  - Are your Unified Communications nodes using valid certificates that were issued by a CA in the Expressway-Cs' trust list?
  - If you are using 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's trusted CA list unique? You must remove any duplicates.
  - If you have TLS verify enabled on connections to other infrastructure (always on by default for Unified Communications traversal zone, and optional for zones to Unified Communications nodes) you must ensure 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 onward, you must create 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 hostnames and IP addresses of systems, your complex deployments (eg. MRA) could stop working as expected after you 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. TLS verification is not enforced (by default) after you upgrade, and you'll see an alarm reminding you to enforce TLS verification.
- (If you use the Expressway for Mobile and Remote Access) Minimum versions of Unified Communications infrastructure: Some versions of Unified CM, IM and Presence Service, and Cisco Unity Connection have been patched with CiscoSSL updates. Check that you're running the minimum versions described in the Mobile and Remote Access deployment guide, before you upgrade Expressway.

  See *Mobile and Remote Access Through Cisco Expressway* on the Expressway configuration guides page.

  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.

Deployments that Use the Expressway for Mobile and Remote Access

- **Expressway-C and Cisco Expressway-E should be upgraded together**. We don't recommend operating with Expressway-C and Expressway-E on different versions for an extended period.

- X8.10.*n* moves the MRA authentication (access control) settings from Expressway-E to Expressway-C, **and applies default values where it is not possible to retain your existing settings.** For correct system operation, after you upgrade you must reconfigure the access control settings on the Expressway, as described later in these upgrade instructions.

Deployments that Use Cisco Spark Hybrid Services

The Management Connector must be up to date before you upgrade Expressway. You must authorize and accept any Management Connector upgrades advertised by the Cisco Collaboration Cloud before you try to upgrade Expressway. Failure to do so may cause issues with the connector after the upgrade.

For new registrations of Expressways to Cisco Spark, the Expressway must be running X8.10.3 or later. Existing registrations still work with Expressway X8.9 or later, although we recommend that you always keep the host Expressway at the latest feature release.

Upgrade Instructions

Before You Begin

Make sure all relevant tasks in Prerequisites and Software Dependencies, page 24 are complete.

We recommend that you upgrade Expressway components while the system has low levels of activity.

(If you use MRA) Note your MRA authentication settings before upgrading

This section only applies if you use the Expressway for Mobile and Remote Access and you upgrade from X8.9*n* or earlier to X8.10 or later. From version X8.10 we moved the MRA authentication (access control) settings from the Expressway-E to the Expressway-C. As the upgrade does not preserve the existing Cisco Expressway-E settings, after the upgrade you need to review the MRA access control settings on the Expressway-C and adjust them as necessary for your deployment.

To access existing MRA authentication settings:

1. On the Expressway-E, go to **Configuration > Unified Communications > Configuration** and locate **Single Sign-on support**. Note the existing value (On, Exclusive, or Off)
2. If **Single Sign-on support** is set to On or Exclusive, also note the current values of these related fields:
   a. **Check for internal authentication availability**
   b. **Allow Jabber iOS clients to use embedded Safari**

(If you use MRA with clustered Unified CMs) Install latest maintenance release on TC/CE endpoints

This section only 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. CDETS CSCvh97495 refers.

- TC7.3.11
- CE8.3.3
- CE9.1.2

Process

Only use this process if you have a single (non-clustered) Expressway. If you have a clustered system, follow the directions in the *Expressway Cluster Creation and Maintenance Deployment Guide* instead.

1. Backup the Expressway system before you upgrade (**Maintenance > Backup and restore**).
2. Enable maintenance mode:
   a. Go to **Maintenance > Maintenance mode**.
   b. Set **Maintenance mode** to *On*.
   c. Click **Save** and click **OK** on the confirmation dialog.
3. Wait for all calls to clear and registrations to timeout.
   - If necessary, manually remove any calls that do not clear automatically (**Status > Calls**, click **Select all** and then click **Disconnect**).
   - If necessary, manually remove any registrations that do not clear automatically (**Status > Registrations > By device**, click **Select all** and then click **Unregister**).

4. Upgrade and restart the Expressway (**Maintenance > Upgrade**).

   If you are upgrading to a new *major* release, for example from X7.n to X8.n, you first need to obtain a new release key from Cisco. The key is required during the upgrade process.

   The web browser interface may timeout during the restart process, after the progress bar has reached the end. This may occur if the Expressway carries out a disk file system check – which it does approximately once every 30 restarts.
5. This step depends on whether or not you use the Expressway for MRA:
   - If you don't use MRA, the upgrade is now complete and all Expressway configuration should be as expected.
   - If you do use MRA, go on to the next section and reconfigure your MRA access control settings.

Upgrade Expressway-C and Expressway-E Systems Connected Over a Traversal Zone

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.

However, we do support a traversal zone link from one Expressway system to another that is running the previous major release of Expressway. This means that you do not have to simultaneously upgrade your Expressway-C and Expressway-E systems.

Some services, like Mobile and Remote Access, require both the Expressway-C and Expressway-E systems to be running the same software version.

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*n* 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 5 Settings for MRA access control

Field	Description	Default
Authentication path	Hidden field until MRA is enabled. Defines how MRA authentication is controlled. *SAML SSO authentication*: Clients are authenticated by an external IdP. *UCM/LDAP basic authentication*: Clients are authenticated locally by the Unified CM against their LDAP credentials. *SAML SSO and UCM/LDAP*: Allows either method. *None*: No authentication is applied. The default until MRA is first enabled. The "None" option is required (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". **It is not recommended in other cases.**	None before MRA turned on UCM/LDAP after MRA turned on
Authorize by OAuth token with refresh	This option requires self-describing tokens for authorization. It's our recommended authorization option for all deployments that have the infrastructure to support them. 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. **Important:** From X8.10.1, the Expressway fully supports the benefits of self-describing tokens (including token refresh, fast authorization, and access policy support). However, not all of the benefits are actually available throughout the wider solution. Depending on what other products you use (Unified CM, IM and Presence Service, Cisco Unity Connection) and what versions they are on, not all products fully support all benefits of self-describing tokens.	On
Authorize by OAuth token (previously SSO Mode)	Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*. 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 *UCM/LDAP* or *SAML SSO and UCM/LDAP*. Clients attempting to perform authentication by user credentials are allowed through MRA. This includes Jabber, and supported IP phone and TelePresence devices.	Off

Table 5 Settings for MRA access control (continued)

Field	Description	Default
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: *Yes*: The *get_edge_sso* 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 *get_edge_sso* request. *No*: 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 *No*. Or select *Yes* 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 5 Settings for MRA access control (continued)

Field	Description	Default
Identity providers: Create or modify IdPs	Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*. **Selecting an Identity Provider** Cisco Collaboration solutions use SAML 2.0 (Security Assertion Markup Language) to enable SSO (single sign-on) for clients consuming Unified Communications services. If you choose SAML-based SSO for your environment, note the following: ■ 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. 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: ■ OpenAM 10.0.1 ■ Active Directory Federation Services 2.0 (AD FS 2.0) ■ PingFederate® 6.10.0.4	–
Identity providers: Export SAML data	Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*. For details about working with SAML data, see SAML SSO Authentication Over the Edge, page 1.	–

Table 5 Settings for MRA access control (continued)

Field	Description	Default
Allow Jabber iOS clients to use embedded Safari	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. This setting optionally allows Jabber on iOS devices to use the native Safari browser. Because the Safari browser *is* able to access the device trust store, you can now enable password-less authentication or two-factor authentication in your OAuth deployment. 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. 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.	No
SIP token extra time to live	Available if **Authorize by OAuth token** is *On*. 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.	0 seconds

Table 6 MRA access control values applied by the upgrade

Option	Value after upgrade	Previously on…	Now on…
Authentication path	Pre-upgrade setting is applied **Notes:** **SSO mode**=*Off* in X8.9 is two settings in X8.10: ▪ **Authentication path**=*UCM/LDAP* ▪ **Authorize by user credentials**=*On* **SSO Mode**=*Exclusive* in X8.9 is two settings in X8.10: ▪ **Authentication path**=*SAML SSO* ▪ **Authorize by OAuth token**=*On* **SSO Mode**=*On* in X8.9 is three settings in X8.10: ▪ **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	Off	–	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)

Using Collaboration Solutions Analyzer

Collaboration Solutions Analyzer is a tool created by Cisco Technical Assistance Center (TAC) to help you with troubleshooting, by analyzing log files from your Cisco Expressway.

To get started:

1. Collect the logs from your Cisco Expressway.
2. Sign in to https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/.

   (You need a customer or partner account to sign in).
3. Select **Log analysis**.
4. Upload your log file(s).
5. Select the log files you want to analyze.
6. Click **Run Analysis**.

The tool analyzes the log file and displays the information in a format that 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.

Cisco Legal Information

Cisco Trademark