# Cisco Expressway X8.11.4

## Release Notes

**First Published: July 2018**

**Last Updated: April 2019**

## 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 |
|---|---|---|
| April 2019 | Add mention to *Notable Issues* section of unexpected behavior in Overview page of web user interface when Expressway is registrar (no non-traversal call counting and no status display). | Documentation addition |

**Table 1 Release Notes Change History (continued)**

| Date | Change | Reason |
|---|---|---|
| March 2019 | Clarify that removal of a cluster peer deletes *all* configuration for the LAN2 interface in dual NIC deployments (*Factory Reset of Peer Leaving Cluster* section). | Documentation addition |
| February 2019 | Add licensing issue for Jabber Guest versions before 11.1.2, to *Open and Resolved Issues*. | Documentation correction |
| November 2018 | Update Limitation regarding chat/messaging services over MRA with OAuth refresh plus IM and Presence Service presence redundancy groups. | X8.11.4 |
| November 2018 | Updates for maintenance release. | X8.11.4 |
| October 2018 | Updates for maintenance release. | X8.11.3 |
| September 2018 | Update Limitations section to clarify demultiplexing ports behavior for Medium systems. | Clarification |
| September 2018 | Updates for maintenance release.<br><br>Add information that X8.11 software version is no longer available and should not be used. | X8.11.2<br><br>Software withdrawn |
| September 2018 | Updates for maintenance release.<br><br>Also clarify that MRA-connected chat/messaging services not supported in all cases if user authentication is by token refresh. | X8.11.1 |
| July 2018 | First publication | X8.11 |

# 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 |
| CE1200 (Expressway pre-installed on UCS C220 M5L) | 52E###### | X8.11.1 onwards |
| CE1100 (Expressway pre-installed on UCS C220 M4L) | 52D###### | X8.6.1 onwards |
| CE1000* (Expressway pre-installed on UCS C220 M3L) | 52B###### | X8.1.1 to X8.10.n<br><br>No support for any versions after X8.10.n on this hardware. |
| CE500* (Expressway pre-installed on UCS C220 M3L) | 52C###### | X8.1.1 to X8.10.n<br><br>No support for any versions after X8.10.n on this hardware. |

* 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 - Hardware Service Support for CE500 and CE1000 Appliances to be Withdrawn

Cisco will withdraw 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.

## Related Documents

**Table 3 Links to Related Documentation**

| | |
|---|---|
| Installation - virtual machines | *Cisco Expressway Virtual Machine Installation Guide* on the Expressway installation guides page |
| Installation - physical appliances | **For Expressway:** *Cisco Expressway CE1200 Appliance Installation Guide* on the Expressway installation guides page<br><br>**For VCS:***Cisco Video Communication Server CE1100 Appliance Installation Guide* on the VCS installation guides page |
| Basic configuration for registrar / single systems | **For Expressway:***Cisco Expressway Registrar Deployment Guide* on the Expressway configuration guides page<br><br>**For VCS:***Cisco Single VCS Control - Basic Configuration Deployment Guide* on the VCS configuration guides page |
| Basic configuration for firewall traversal / paired systems | **For Expressway:***Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide* on the Expressway configuration guides page<br><br>**For VCS:***Cisco TelePresence VCS Basic Configuration (Control with Expressway) Deployment Guide* on the VCS configuration guides page |
| Administration and maintenance | **For Expressway:**<br>*Cisco Expressway Administrator Guide* on the Cisco Expressway Series maintain and operate guides page<br>*Cisco Expressway Serviceability Guide* on the Cisco Expressway Series maintain and operate guides page<br><br>**For VCS:**<br>*Cisco TelePresence VCS Administrator Guide* on the Cisco TelePresence VCS maintain and operate guides page<br>*Cisco TelePresence VCS Serviceability Guide* on the Cisco TelePresence VCS maintain and operate guides page |
| 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 |
| Rest API | *Cisco Expressway REST API Reference 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 Meeting Server with Cisco Expressway Deployment Guide* on the Expressway configuration guides page<br><br>*Cisco Meeting Server API Reference Guide* on the Cisco Meeting Server programming guides page<br><br>Other Cisco Meeting Server guides are available on the Cisco Meeting Server configuration guides page |
| Cisco Webex Hybrid Services | Hybrid services knowledge base |

**Table 3 Links to Related Documentation (continued)**

| | |
|---|---|
| Microsoft infrastructure | *Cisco Expressway with Microsoft Infrastructure Deployment Guide* on the Expressway configuration guides page<br><br>*Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet* on the Expressway configuration guides page |
| Multiway Conferencing | Cisco TelePresence Multiway Deployment Guide on the Expressway configuration guides page |

# Feature History

**Table 4 Feature History by Release Number**

| Feature / change | X8.11 (withdrawn) | X8.11.1 (withdrawn) | X8.11.2 (withdrawn) | X8.11.3 (withdrawn) | X8.11.4 |
|---|---|---|---|---|---|
| System Size Selection for Appliances | – | – | – | Supported | Supported |
| Finesse Agent Support over MRA | – | – | Supported | Supported | Supported |
| First Software Release for the CE1200 Appliance | – | Supported | Supported | Supported | Supported |
| Device Registration to Expressway-E (SIP and H.323) | Supported | Supported | Supported | Supported | Supported |
| Changes to Cisco TMS Provisioning Access | Supported | Supported | Supported | Supported | Supported |
| Multiway Conferencing on Cisco Expressway Series | Supported | Supported | Supported | Supported | Supported |
| SIP Proxy to Multiple Meeting Server Conference Bridges (Support for Cisco Meeting Server Load Balancing) | Preview | Preview | Preview | Preview | Preview |
| Web Proxy to Multiple Meeting Server Web Bridges | Supported | Supported | Supported | Supported | Supported |
| Cisco Meeting App can use Expressway-E TURN Server | Preview | Preview | Preview | Preview | Preview |
| TURN on TCP 443 | Supported | Supported | Supported | Supported | Supported |
| TURN Port Multiplexing on Large Expressway-E | Supported | Supported | Supported | Supported | Supported |
| Improved Security of Data at Rest | Supported | Supported | Supported | Supported | Supported |
| Common Criteria Preparation | Supported | Supported | Supported | Supported | Supported |

**Table 4 Feature History by Release Number (continued)**

| Feature / change | X8.11 (withdrawn) | X8.11.1 (withdrawn) | X8.11.2 (withdrawn) | X8.11.3 (withdrawn) | X8.11.4 |
|---|---|---|---|---|---|
| Mandatory Password on Backups | Supported | Supported | Supported | Supported | Supported |
| Custom Domain Search | Supported | Supported | Supported | Supported | Supported |
| Built-in-Bridge Recording over MRA<br>(Not new in X8.11. Included for information due to its former preview status)<br><br>Information about BiB over MRA is now available in the *Mobile and Remote Access Through Cisco Expressway* guide | Supported (formerly preview) | Supported | Supported | Supported | Supported |
| Access Policy Support over MRA<br>(Not new in X8.11. Included for information due to its former preview status) | Supported (formerly preview)<br><br>Requires Cisco Jabber 12.0 | As for X8.11 | As for X8.11 | As for X8.11 | As for X8.11 |
| Multiple Presence Domains over MRA<br>(Not new in X8.11. Included for information due to its preview status) | Preview | Preview | Preview | Preview | Preview |
| License Key Consolidation | Supported | Supported | Supported | Supported | Supported |
| Factory Reset of Peer Leaving Cluster | Supported | Supported | Supported | Supported | Supported |
| Smart Call Home<br>(Not new in X8.11. Included for information due to its preview status) | Preview | Preview | Preview | Preview | Preview |
| SRV Connectivity Tester Tool | Supported | Supported | Supported | Supported | Supported |
| REST API Expansion | Supported | Supported | Supported | Supported | Supported |

# Important Information About Versions X8.9 through X8.11.3

This X8.11.4 maintenance release supersedes all earlier versions of X8.11.x, X8.10.x and X8.9.x software, which are no longer available for download. **Cisco strongly recommends that you upgrade to this version**. (For clarity the feature lists in these release notes still reference X8.11, but the software is unavailable.)

# Changes in X8.11.4

### CAUTION - PLEASE READ THIS BEFORE YOU START

**Systems on X8.1.x or Earlier Need a Two-Stage Upgrade** **If you are upgrading a VCS system on X8.1.x or earlier software, you must do an intermediate upgrade to X8.10 first, before you upgrade to this release (see Upgrade Prerequisites and Software Dependencies, page 27 for details). Otherwise there is a risk of data corruption.**

Cisco Jabber 12.5 or later is needed if you want chat/messaging services over MRA with authentication using OAuth refresh (self-describing tokens) and you configure IM and Presence Service presence redundancy groups. With this release of Expressway, user login failures will occur in this scenario if Jabber versions before 12.5 are in use.

### Changes for security advisory

X8.11.4 is a maintenance release to address a security advisory, published by Cisco at https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181107-vcsd and tracked by CDETS CSCvn17278.

### Changes to other open issues

Some other issues are fixed in this maintenance release, and the search lists for Open and Resolved Issues, page 21 have been updated accordingly.

### MRA changes (customer documentation)

The customer documentation is now fixed to include these previously undocumented limitations for recording over Mobile and Remote Access (MRA) connections, including Built-in-Bridge (BiB) recording:

- Recording only works for direct person-to-person calls, and not for conferences.
- Recording is not currently supported for Silent Monitoring and Whisper Coaching features.

### Web Proxy for Cisco Meeting Server changes

This item applies if you use Expressway as a Web Proxy for Cisco Meeting Server, to support Cisco Meeting WebRTC Apps. Previously, the Expressway WebRTC socket timeout value caused WebRTC calls to drop after 1 hour (3600 seconds). The timeout is now extended to 12 hours (43,200 seconds). Currently this setting is not configurable (CDETS CSCvn28708 refers).

# Changes in X8.11.3

### Changes to open issues and limitations

X8.11.3 is a maintenance release. The search lists for Open and Resolved Issues, page 21 have been updated.

Some limitations are fixed or mitigated in this release:

- Previously we did not support dual-homed conferences for Microsoft-based users with a Meeting Server Call Bridge cluster, and Expressway as the edge for Meeting Server. This scenario is now supported.
- Medium sized appliance-based systems with a 1 Gbps NIC are automatically converted to a Large system on upgrade. The resulting demultiplexing port behavior by Expressway causes dropped calls unless the default demultiplexing ports for Large systems are opened on the firewall. In this release you can use the new system size selection setting to manually reset the default size to Medium (see next point).
- For Cisco Expressway CE1200 appliances configured as Expressway-E systems, previously you could not use any REST API commands that specifically apply to Expressway-E. The commands are now supported.

### System size selection for appliances

For CE1100 or CE1200 appliances, you can now manually change the system size to Medium or Large. To do this, go to the **System > Administration settings** page and select the required size from the **Deployment Configuration** list.

# Changes in X8.11.2

### Changes to open issues

X8.11.2 is a maintenance release. The search lists for Open and Resolved Issues, page 21 have been updated.

### MRA changes

The following change applies for deployments that use the Cisco Unified Communications Manager Mobile and Remote Access (MRA) feature:

- For supported devices, the Cisco Finesse agent and contact center thin-client desktop is now supported over MRA connections.

# Changes in X8.11.1

### New CE1200 appliance

A new CE1200 appliance is introduced in conjunction with this software maintenance release.

If you deploy existing CE500, CE1000, or CE1100 appliances, this section highlights some of the differences in the CE1200:

- The CE1200 is designed for use with the Cisco Expressway Series product range, and does not support the Cisco VCS product. It ships with the release key pre-installed.
- Unlike earlier appliances, the CE1200 is a single, multi-purpose server that can operate as a Cisco Expressway-C or a Cisco Expressway-E. By default it always ships with Expressway-C preinstalled. To deploy the server as an Expressway-E, you configure the **Type** option as *Expressway-E*, in the Service Setup Wizard (the wizard runs when you first launch the Expressway web user interface, or you can run it anytime from the **Status > Overview** page). The Traversal Server option key is no longer used to change to an Cisco Expressway-E.
- The CE1200 can support up to 5000 registrations for Mobile and Remote Access, an increase on the 2500 MRA registrations supported by other physical appliances or VM-based systems.

To add a CE1200 appliance to an existing cluster that has CE1100 models in it, configure the Type option to match the other peers (Expressway-E or Expressway-C) through the service setup wizard on the **Status > Overview** page, *before* you add the CE1200 to the cluster.

### Jabber Guest license issue in single-NIC deployments resolved

Subject to running Jabber Guest 11.1.2 version or later, this maintenance release resolves a previous issue with RMS licenses for Jabber Guest calls being consumed on Expressway-C instead of on Expressway-E (CDETS CSCvf34525).

**Note:** A separate issue with Jabber Guest in single-NIC deployments still exists, concerning the Expressway-E failing to count an RMS license per Jabber Guest call (CDETS CSCva36208).

### MRA changes

These changes apply to deployments that use the Cisco Unified Communications Manager Mobile and Remote Access (MRA) feature:

- Hunt groups (including hunt pilots and hunt lists) are supported over MRA, if you are running Cisco Unified Communications Manager version 11.5(1)SU5 or a later version that has the relevant change.
- The Expressway CE1200 appliance is verified as supporting up to 5000 registrations for Mobile and Remote Access, up from 2500 verified for previous appliances. (This change does not apply to earlier physical appliance models, or VM systems, which remain at 2500 MRA registrations.)

# Features in X8.11 (now in X8.11.4)

## Device Registration Enhancements

### Registrations to Expressway-E

From X8.11 we support SIP registrar and H.323 Gatekeeper functionality on the Cisco Expressway-E, so you can now register SIP and H.323 endpoints directly to the Expressway-E.

**Licensing**

If you have existing licenses on the Expressway-C and want to register some or all of your existing licensed endpoints to the Expressway-E, you need to manually delete the relevant option key(s) from the Expressway-C and reload them on the Expressway-E.

**Information for H.323 devices**

- As with H.323 registrations to the Expressway-C, each H.323 device registered to Expressway-E consumes a TelePresence Room System License.
- Currently we do not support proxy registrations by remote H.323 devices to Expressway-C or Expressway-E.

### Changes to Cisco TMS Provisioning Access (Users, FindMe, Phone Book and Device Provisioning)

The Expressway can optionally access FindMe and other provisioning services hosted by Cisco TMS (through the Cisco TMSPE). Previously, this was enabled by default on Expressway if you had the necessary option keys.

From X8.11, the Cisco TMS-hosted provisioning services are enabled through the **System > Administration settings** page in the web user interface or the device provisioning CLI command (*xconfiguration Administration DeviceProvisoning*). You do not need special option keys or licenses to enable these services. The following device provisioning services are available:

- Users
- FindMe
- Phone Books
- Devices

For new installations all services are off by default. For existing systems your current service settings are preserved and remain unchanged after upgrading.

From X8.11, we support device provisioning on the Cisco Expressway-E, as well as on the Cisco Expressway-C as before. Although device provisioning is now supported on both components, for deployments with a paired Expressway-C and Expressway-E, we recommend that you use it on the Expressway-C.

## Multiway on Expressway

The Cisco Expressway Series now supports Multiway conferencing, which was previously only supported on the Cisco VCS product. Subject to Multiway-compliant endpoints and Cisco TelePresence Server or Cisco TelePresence MCU Series conference bridges, a video caller in a point-to-point call can manually add a third person to the call, to create an instant conference.

**Note:** Multiway conferencing relies on an underlying Cisco Expressway feature known as 'Conference Factory'. Because of this, some documentation, licensing, and user interface settings related to Multiway conferencing use the term Conference Factory.

**Licensing**

The Multiway conferencing feature requires a 'Conference System' licence on Cisco Expressway-C. This license is free, but it takes up one registration resource when you enable Conference Factory (that is, Multiway conferencing).

# Improved Integration with Cisco Meeting Server

## (Preview) SIP Proxy to Multiple Meeting Server Conference Bridges (Support for Meeting Server Load Balancing)

This feature is currently in preview status only. It is not supported with Cisco Meeting Server software version 2.3 or earlier. Also, a Limitation currently exists regarding support for dual-homed conferences with a Meeting Server cluster.

From X8.11, Cisco Expressway Series supports the mechanism that is used to load balance the calls between Meeting Servers that are in call bridge groups.

When Cisco Meeting Servers are in a call bridge group, and a participant tries to join a space on a server that has no capacity, that server rejects the call with the response code " 488 Not Acceptable Here" . This call is then rerouted to another server by the call control layer. That other server then sends a SIP INVITE to the call control layer, using the original call details. The participant is now in the correct space, on a different Meeting Server. In cases where there is capacity in the “second” server, but another Meeting Server has more capacity, it asks that Meeting Server in the group to send the SIP INVITE.

There is a new setting in the neighbor zone called Meeting Server load balancing which must be enabled (**Configuration > Zones > Zones > Zone Name > Advanced**). This setting allows the Cisco Expressway's B2BUA to process the INVITE from the " second" Meeting Server to enable the participant to connect.

We recommend that Meeting Server load balancing is set to *On* regardless of whether endpoints are registered with Expressway or with Unified CM.

### Known Supported Features and Limitations

- Cisco Expressway invokes its B2BUA to process the call replacement.
- Load balancing of calls from registered H.323 endpoints is also supported.
- Calls with DTLS-secured media are not supported.
- Different encryption modes can be applied on call legs to and from Cisco Expressway.

## Web Proxy to Multiple Meeting Server Web Bridges

Cisco Expressway now supports load balancing and redundancy of Meeting Server web bridges when it is acting as a proxy for the Cisco Meeting WebRTC App.

In earlier versions, the Cisco Expressway did support multiple web bridges in a limited way; it would attempt to distribute connections evenly across all the web bridge addresses returned by its DNS SRV query. However, if those addresses were not reachable, the Cisco Expressway did not adapt gracefully and the connection would fail.

There is no change to configuration for this feature. You enter a single address (called **Guest account client URI** in the Expressway UI). If there are multiple web bridges, Expressway-C discovers their IP addresses using DNS, then uses round-robin to distribute WebRTC connections evenly amongst those web bridges.

The X8.11 enhancement is that Expressway now maintains a dynamic list of IP addresses that it knows are web bridges. Specifically, the web proxy for Meeting Server feature has the following improvements:

- The Expressway-C regularly queries the DNS to detect any deliberate changes to your deployment; for example, host addresses being added to or removed from the SRV record.
- The Expressway-C probes the host addresses returned by DNS to check if they are reachable and that they are web bridges (using an API call).
- If an address is not reachable, or the host is not a web bridge, then the Expressway-C stops sending webRTC connections to that address.

- If the DNS SRV query is successful, the results, including weight and priority, are shown in the status area of the UI page.
- The UI also shows a "failed" or "active" status for each address.

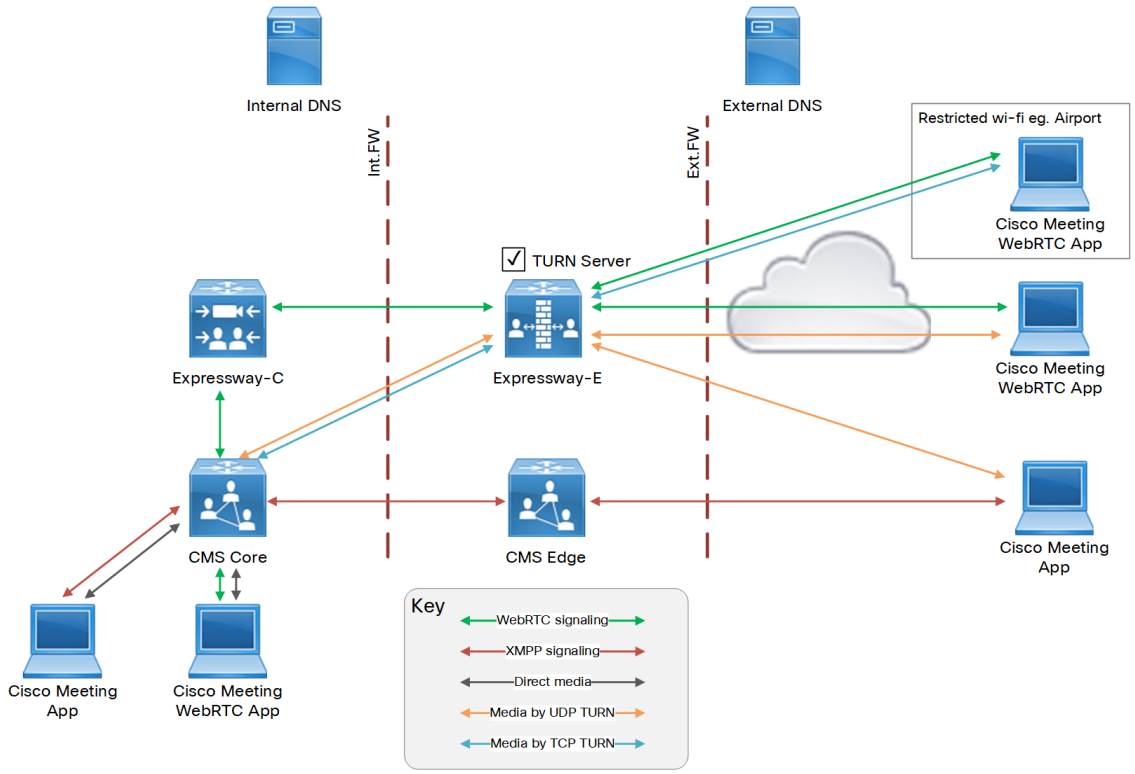
**Note:** Expressway-C does not maintain stateful connections from the Cisco Meeting WebRTC App to the Meeting Server web bridge. If a connection fails, for example a web bridge host goes down, the existing call to that host is lost and the client should attempt to re-establish the call to the web bridge. In this case, the Expressway would not proxy the new WebRTC connection to the failed host.

## (Preview) Cisco Meeting App Can Use Expressway-E TURN Server

This feature is currently in preview status only.

Owing to TURN server enhancements in X8.11, it is possible to use the Expressway-E TURN server for media path discovery and media relay between the Cisco Meeting App and the Cisco Meeting Server, even when that Expressway-E is being used to proxy WebRTC to the Meeting Server.

**Figure 1 Cisco Meeting WebRTC App and Cisco Meeting App sharing a TURN server**




In the diagram, the Expressway-E is configured to listen on TCP 443 for TURN requests and for WebRTC requests. The TURN clients (Meeting Server Core, Meeting App, and Cisco Meeting WebRTC App) will all try to use UDP 3478 for TURN requests.

If the WebRTC App cannot make the outbound connection to UDP 3478, it uses the TCP override port, which is 443 by default, to request media relays.

The Meeting Server Edge is still required to traverse the XMPP signalling for Cisco Meeting Apps. However, there is no need to use the TURN services of the Meeting Server Edge server.

# TURN Server Enhancements

## TURN on TCP 443

You can configure Expressway-E to listen to both TURN and Cisco Meeting Server requests on the TCP port 443. When Expressway-E receives a connection request through port 443, it forwards the request either to the TURN server or to the Meeting Server Web Proxy depending on the request type. This allows external users to use TURN services and join Meeting Server spaces from an environment with restricted firewall policies.

If the web administrator port is currently configured to listen for HTTPS requests on port 443, you must change it to a different port to listen to HTTP requests (**Web administrator port** setting on **System > Administration settings**). Expressway-E cannot listen for both web administration and TURN requests on the TCP port 443.

## TURN Port Multiplexing on Large Expressway

You can configure a Large Expressway-E TURN server to listen for TURN requests on a range of ports, from 3478 to 3483 by default. From X8.11, if TURN multiplexing is enabled, the Expressway-E accepts all TURN requests on the first port in the range (typically UDP 3478), and internally demultiplexes those requests onto the port range. TURN clients only need to know one of the ports, but the full capacity of the large Expressway-E TURN server is available.

However, if TCP 443 TURN service is enabled, the external port does not multiplex the TCP TURN requests due to a technical limitation. So in this case, only 1000 TCP TURN relays are supported.

# Security Enhancements

## Improved Security of Data at Rest

From X8.11, every software installation has a unique root of trust. Each Expressway system, including hardware versions and VM versions has a unique key that is used to encrypt data local to that system. This improves the security of your data at rest in the following ways:

- The new key is created when you upgrade to X8.11, and is used to encrypt all data on the first restart.
- Only this key can be used to decrypt data from this system. No other Expressway key can decrypt this system's data.
- The key is never exposed on the UI. It is never logged, either locally or remotely.

## Common Criteria Preparation

In X8.11, the Expressway is configurable to meet the Common Criteria for Information Technology Security Evaluation (Common Criteria). The new security configurations in X8.11 are:

- The SSH tunnels between Expressway-C and Expressway-E have configurable cipher and key exchange algorithms.
- You can change **Ciphers** and **Public Key Algorithms** settings in the **Maintenance > Security > SSH configuration** web UI page.
- Logging can be set to a certification-compliant mode (on **Maintenance > Logging**, change the **Certification logging** mode).
- An option to force new administrators to reset their passwords. The option is on **Users > Administrator accounts**, when you add a new user.

**Note:** Also as part of Common Criteria work for Expressway, CA certificate checking now requires the *BasicConstraints* extension to be present.

### Mandatory Password on Backups

Backup files are now encrypted in all cases, and require you to specify a password for all backup and restore operations.

**Caution: To restore from a backup, you will need the password for the relevant backup file.**

## Mobile and Remote Access Deployments

These features and enhancements are relevant if your Expressway is configured for MRA (that is, deployments with mobile or remote devices that are registered to Cisco Unified Communications infrastructure).

### Custom Domain Search

X8.11 addresses a former limitation of MRA that applied when the DNS domain for the Unified Communications infrastructure was different from the DNS domain of the Expressway-C using AXL to connect to that infrastructure.

In earlier releases, you needed to enter the FQDN of the UC hosts when configuring the MRA connections. From X8.11, you can enter a custom domain and use only the hostnames to discover UC nodes. If the address you enter is not an FQDN or an IP address (for example, `yourhostname`) then the Expressway-C will search DNS for `yourhostname.Expressway-C-domain`. If that search does not return a host address, then Expressway-C queries DNS for `yourhostname.custom-domain`.

The Expressway-C then attempts the AXL connection to the hosts returned by DNS, as normal.

This is relevant if you connect to external nodes in a different sub-domain from the Expressway-C, and use non-qualified hostnames. Expressway can now resolve the hostnames into FQDNs, and you don't need to enter the host FQDNs when configuring connections between nodes.

**Note:** This change is a general system enhancement for Expressway and is not limited to MRA use.

### Intercom Support for IP Phones over MRA

Intercom support is now available over MRA, for IP phones that support the feature.

### Built-in-Bridge Recording Over MRA

Built-in-Bridge recording is now supported. Previously it was in preview status.

The Expressway supports Built-in-Bridge (BiB) recording over MRA. This feature can help organizations to comply with the phone recording requirements of the European Union's *Markets in Financial Instruments Directive* (MiFID II).

#### How it works

BiB can be used to record the audio portion of calls that are made or received by users working off-premises.

- BiB is always enabled on the Expressway.
- BiB is configurable on Cisco Unified Communications Manager. When BiB is enabled, Unified CM forks the call to/from the endpoint to a media recording server.

#### Prerequisites

BiB over MRA requires the following components, or later:

- 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 7800 Series or 8800 Series devices **which support MRA** (not all these phones are MRA-compatible)

    The 7800/8800 Series phones which currently support MRA are listed in the "Prerequisites" section of the latest *Mobile and Remote Access Through Cisco Expressway* guide on the Expressway configuration guides page, or ask your Cisco representative for details.
- Registrar/call control agent: **Cisco Unified Communications Manager 11.5(1)SU3**

  BiB is not supported on Expressway-registered endpoints.
- Edge traversal: **Expressway X8.11.1**
- Recording server: Out of scope for this document. (Information about configuring recording for Cisco Unified Communications Manager is available in the Feature Configuration Guide for Cisco Unified Communications Manager.)

Call recording for Cisco Jabber endpoints has some limitations, as follows. (These also apply on premises, and not just over MRA.)

- Cisco Unified Communications Manager does not allow Jabber mobile devices to be CTI-monitored.
- Jabber does not support injecting recording tones into the media stream.

### Access Policy Support over MRA

Access policy support over MRA is now supported. Previously it was in preview status.

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.

### (Preview) Multiple Presence Domains / Multiple IM Address Domains over MRA

This feature is currently in preview status only.

Jabber 10.6 and later can be deployed into an infrastructure where users are organized into more than one domain, or into domains with subdomains (subject to IM and Presence Service 10.0.x or later).

## Serviceability Improvements

### License Key Consolidation

The Expressway license now includes the following items as standard features, which were previously applied as separate option keys:

- *LIC-EXP-AN* Enable Advanced Networking (Expressway-E only)
- *LIC-EXP-TURN* Enable TURN Relay (Expressway-E only)
- *LIC-VCS-DEVPROV* Enable Device Provisioning
- *LIC-VCS-FINDME* Enable FindMe Service

**Note:** If you are upgrading an existing system that has these keys applied, for administrator convenience the keys remain visible in the web user interface after the upgrade, even though they are no longer needed.

## Factory Reset of Peer Leaving Cluster

From X8.11 we have modified the behavior of cluster peers when they are removed from the cluster or when the cluster is disbanded. This change is part of the unique root of trust improvement in X8.11. To remove a peer from a cluster you clear all peer address fields on that peer. When you do this, from X8.11, the Expressway **prepares itself to factory reset on the next restart** (and displays a banner to remind you that it is in this state).

If you need to avoid the factory reset, restore the clustering peer address fields as they were. Replace the original peer addresses in the same order, and then save the configuration to clear the banner.

The factory reset is automatically triggered when the peer restarts, to remove sensitive data and clustering configuration. The reset clears all configuration except the following basic networking information, which is preserved for the LAN1 interface so that you can still access the Expressway. If you use the **dual-NIC option, be aware that any LAN2 configuration is removed completely by the reset**.

- IP addresses preserved
- Server certificate, associated private key, and CA trust store preserved
- Admin and root accounts and passwords preserved
- SSH keys preserved
- Option keys preserved
- HTTPS access enabled
- SSH access enabled

**CAUTION: You MUST follow the published clustering guidance when forming, changing, or upgrading Expressway clusters. Your cluster may be unrecoverable and you may lose data if you do not follow the correct sequence.** See the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide*, for your version, on the Cisco Expressway Series configuration guides page.

## (Preview) Smart Call Home

This feature is currently in preview status only.

Smart Call Home is an 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: ad hoc 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.

**Note:** Although the web user interface includes an option for SMTP with Smart Call Home, currently this is not actually implemented in the Expressway.

## SRV Connectivity Tester

The SRV connectivity tester is a network utility that tests whether the Expressway can connect to particular services on a given domain. You can use this tool to proactively test your connectivity while configuring Expressway-based solutions such as Cisco Webex Hybrid Call Service or business-to-business video calling.

You specify the DNS Service Record Domain and the Service Record Protocols you want to query for that domain. The Expressway does a DNS SRV query for each specified protocol, and then attempts TCP connections to the hosts returned by the DNS. If you specify TLS, the Expressway only attempts a TLS connection after the TCP succeeds.

The Expressway connectivity test page shows the DNS response and the connection attempts. For any connection failures, the reason is provided along with advice to help with resolving specific issues.

To troubleshoot connectivity, you can download the TCP data from your test in *.pcap* format. You can selectively download a dump of the DNS query, or a specific connection attempt, or you can get a single *.pcap* file showing the whole test.

### REST API Expansion

We continue to expand the REST API to simplify remote configuration. We are adding REST API access to configuration, commands, and status information when we add new features, but are also selectively retrofitting the REST API to features that were introduced in earlier versions.

For example, third party systems, such as Cisco Prime Collaboration Provisioning, can use the API to control the following features / services on the Expressway:

| Configuration APIs | API introduced in version |
|---|---|
| Clustering | X8.11 |
| Smart Call Home | X8.11 |
| Microsoft Interoperability | X8.11 |
| B2BUA TURN Servers | X8.10 |
| Admin account | X8.10 |
| Firewall rules | X8.10 |
| SIP configuration | X8.10 |
| Domain certificates for Server Name Identification | X8.10 |
| MRA expansion | X8.9 |
| Business to business calling | X8.9 |
| MRA | X8.8 |

The API is self-documented using RESTful API Modeling Language (RAML). You can access the RAML definitions for your system at `https://<ip address>/api/provisioning/raml`. A high-level summary of how to access and use the API is available in *Cisco Expressway REST API Summary Guide* on the Expressway installation guides page.

## Cisco Webex Hybrid Services with Expressway X8.11

- Some Expressway-based Hybrid Services require that you configure the connector host as a cluster, even if there is only one peer in the cluster ("cluster of one"). **Be very careful when modifying the Clustering configuration that you do not clear all Peer N address fields and Save the configuration**, unless you intend to factory reset the Cisco Expressway. You will lose your registration, all your connectors, and all associated configuration. See Factory Reset of Peer Leaving Cluster, page 17.
- 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.
- Expressways that will be used to host connectors for Cisco Webex Hybrid Services must be running a supported Expressway software version now, before you register them to Cisco Webex. (You can upgrade just the Management Connector component on the Expressway, without needing to upgrade the whole Expressway.)

  For details about which versions of Expressway are supported for hybrid connector hosting, see Connector Host Support for Cisco Webex Hybrid Services

- X8.11 introduces a new "Webex" zone type—a DNS zone that is specifically designed for connecting to Cisco Webex. This feature simplifies the configuration of Cisco Webex Hybrid Call Service. You can create or delete one Webex zone, but you cannot modify it. See Hybrid Call Service documentation for more detail.

## Other Software Changes and Enhancements

- You can manage how the Expressway handles malformed or corrupt SIP messages, using a new CLI command *RetainConnectionOnParseErrorMode*. By default Expressway closes the SIP connection if it receives a malformed or corrupt SIP message. This command lets you choose to have the connection maintained—for messages with non-mandatory headers only, or for all messages including mandatory headers.

  **Note:** Regardless of this setting, Expressway always closes the connection if it receives ten or more consecutive malformed messages, or if the *Content-Length* header is missing or malformed.
- We support firmware upgrades for Expressway appliances running on Cisco UCS C-Series servers, using the Cisco Host Upgrade Utility (HUU). The *Expressway Administrator Guide* now contains a link to the HUU user instructions.
- The DES encryption option is no longer in SNMP, but previously it still appeared in the Expressway user interface and documentation. This option has now been removed.
- The process to collect diagnostic logs is different. You use a new **Collect log** button to retrieve the generated log entries. Then use the **Download log** button as before. This change only affects diagnostic logging, not other log processes. You can download diagnostics logs repeatedly, by using the Collect log button again.

## Customer Documentation Changes

- **Two user guides are deprecated from X8.11.** These documents are deprecated from this release, and will no longer be maintained:• *Cisco Jabber and Microsoft Lync Interoperability Infrastructure Configuration Cheatsheet* (“SIP Broker” deployment) and *Cisco Expressway with Microsoft Infrastructure Deployment Guide* (“Lync Gateway” deployment).

  Guidelines for interworking with Microsoft environments using Meeting Server are provided in the *Cisco Meeting Server with Cisco Expressway Deployment Guide*.
- **We have phased out some Cisco VCS documentation.** Previously we provided two separate variants of most customer support documents, for the VCS and the Expressway. From X8.10 we began to provide Expressway versions only for certain guides. In such cases the Expressway versions include any relevant VCS-specific information.
  - Cisco Expressway documents are available here: http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html
  - Cisco VCS documents are available here: http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/tsd-products-support-series-home.html
- **What's New and Software Version History information is now in summary format in the Administrator Guide and online help.** We have restructured the "What's New" and "Software Version History" information in the Expressway Administrator Guide and online help. It's now a summary list of features and the releases in which they were introduced, with links out to the relevant release notes for detailed feature information.
- **REST API Guide no longer details individual calls.** As the Expressway API is self-documented using RAML, we have removed details about individual calls from the *Expressway REST API Reference Guide*. This document now provides summary information only, about how to access and use the API interface.
- **Cisco Meeting Server with Expressway.** The *Cisco Expressway Session Classification Deployment Guide* is now renamed to *Cisco Meeting Server with Cisco Expressway Deployment Guide*.

  The scenario for "Video Calls Between Two Standards-based Organizations (B2B)" is now in the *Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide*.

  The scenario for "IM&P Federation With Microsoft-based Organizations" is now in the *Chat and Presence Federation Using Cisco Expressway Deployment Guide*.

- **XMPP Federation with Expressway.** The *Cisco Unified Communications XMPP Federation Deployment Guide* for Expressway is now renamed to *Chat and Presence Federation Using Cisco Expressway*.
- **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 X8.11.4
- Issues resolved by X8.11.3
- Issues resolved by X8.11.2
- Issues resolved by X8.11.1
- Issues resolved by X8.11

## Notable Issues in this Version

**Unexpected behavior of active call counter and registered calls link in Overview page of the web user interface, when endpoints are registered to Expressway**

Two call-related issues do not currently work properly on the **Overview** page when Expressway is the registrar:

- Non-traversal calls (both endpoints registered to Expressway-C) do not increment the active call counter.
- If you click the "Registered calls" link, it unexpectedly displays the Unified Communications status page.

**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.

- 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.
- **This issue only applies to users who have a Jabber Guest version earlier than release 11.1(2)**, users with 11.1(2) and later are not affected. In affected cases, although each Jabber Guest call ought to consume an RMS license on the Cisco Expressway-E, in reality the RMS licenses are consumed on the Cisco Expressway-C. This issue was identified in X8.10 and CDETS CSCvf34525 refers. Contact your Cisco representative if you are affected by it.

Note that we recommend the Dual NIC Jabber Guest deployment.

# 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. If customers may 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

- 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 DTLS protocol is inserted in the SDP, but only for 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.

## Mobile and Remote Access Limitations

**Important: If you use Expressway for Mobile and Remote Access (MRA), various unsupported features and limitations currently exist.** These are detailed in *Supported and Unsupported Features with Mobile and Remote Access* in the X8.11 *Mobile and Remote Access Through Cisco Expressway* guide.

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

Limitations which are new for this release, or were not included in earlier documentation, include the following:

Cisco Jabber 12.5 or later is needed if you want chat/messaging services over MRA with authentication using OAuth refresh (self-describing tokens) and you configure IM and Presence Service presence redundancy groups. With this release of Expressway, user login failures will occur in this scenario if Jabber versions before 12.5 are in use.

These limitations exist for recording over MRA connections, including for BiB recording:

- Recording only works for direct person-to-person calls, and not for conferences.
- Recording is not currently supported for Silent Monitoring and Whisper Coaching features.

## 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.

# CE1200 Appliance

- In certain scenarios, issues exist with restores of an Expressway-E onto a CE1200 appliance from a CE1100 or earlier appliance backup. More details are provided in the upgrade instructions, including how to resolve each issue:
  - The CE1200 appliance may restore as an Expressway-C.
  - An incorrect banner may display in the web user interface.
- The CE1200 appliance requires Expressway software version X8.11.1 or later. Although the system does not prevent downgrades to an earlier software version, Cisco does not support appliances that are running 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. The service setup wizard (Type setting) manages whether the appliance is an Expressway-C or an Expressway-E, rather than the Traversal Server key as for earlier appliances.

## 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).

## 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. As a result, Expressway-E listens for multiplexed RTP/RTCP traffic on the default demultiplexing ports for Large systems (36000 to 36011); instead of on the demultiplexing ports that are configured for Medium systems. In this case, the Expressway-E drops the calls because ports 36000 to 36011 are not open on the firewall. From X8.11.3 you can manually change the system size back to Medium, through the **System > Administration settings** page (select *Medium* from the **Deployment Configuration** list). If you encounter this issue in a release earlier than X8.11.3, the workaround is to open the default demultiplexing ports for Large systems on the firewall.

## Language Packs

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

## 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.

## 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.

## Microsoft Federation with Dual Homed Conferencing-SIP Message Size

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

## Intradomain Microsoft Interop with Expressway and Cisco Meeting Server

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

*You deploy separate Microsoft and standards-based SIP networks in a **single domain** and in a configuration that has an Expressway-E **directly facing** a Microsoft front end server (because you use internal firewalls between subnetworks, or for any other reason). For example, Cisco Unified Call Manager in one (sub)network and Microsoft in a second (sub)network, inside the same domain.*

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

### Workaround

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

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

## Licensing Behavior with Chained Expressway-Es

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

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

## 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.

## Expressway Forward Proxy

**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.**

## TURN Servers

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

# Interoperability

## Test Results

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.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, you must 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'"
```

# 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 X8.11.4

## Upgrade Prerequisites and Software Dependencies

**CAUTION: 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 on X8.1.x or Earlier Need a Two-Stage Upgrade

If you are upgrading a system which is running software older than version X8.2, **you must first upgrade to an intermediate release before you install this X8.11.4 software.** Otherwise there is a **risk of data corruption**, due to database format changes in our later software versions. We recommend upgrading to X8.10.x (latest maintenance release) as the intermediate release. However, if you have specific reasons to prefer an earlier software version, you can upgrade to any version from and including X8.2, before you install this X8.11.4 software. (Version X8.2 is not affected by this issue—only versions from X8.1.x and earlier.)

- Version X8.10.n release notes are available here: https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-release-notes-list.html
- Version X8.10.n software is available here:https://software.cisco.com/download/type.html?mdfid=286255326&flowid=77866

### 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.

From X8.11.1, when the system restarts after the upgrade it uses a new encryption mechanism. This is due to the unique root of trust for every software installation, introduced in X8.11.1.

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 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'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.

### Deployments that use CE1200 appliances

When you restore an Expressway-E onto a CE1200 appliance from a CE1100 or earlier appliance backup, the CE1200 appliance may restore as an Expressway-C. This issue occurs if the service setup wizard was used in the CE1100 or earlier appliance to change the type to Expressway-C, and the wizard was not completed for the entire configuration. To avoid this issue, do the following before you back up the appliance:

1. Run the service setup wizard and change the type to Expressway-E.
2. Complete the wizard to the end.

Also, if you restore the Expressway-E configuration onto a CE1200 appliance from a CE1100 backup, the CE1200 appliance restores as an Expressway-E (as expected). However, depending on how the CE1100 type was previously configured, the web interface banner may display as Expressway-C. If you encounter this issue, go to the service setup wizard (**Status > Overview** page) and change **Type** to *Expressway-E*, then restart the system. This issue only occurs if the Traversal Server option key was used on the CE1100 to change the type to Expressway-E. If you used the service setup wizard, you will not encounter the issue.

### 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. Check that you are running the minimum versions described in the Expressway MRA 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.
- 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.
- 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. CDETS CSCvh97495 refers.

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

**Note:** Versions from X8.10.n move the MRA authentication (access control) settings from Expressway-E to Expressway-C, and apply 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 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. And you must upgrade the Expressway software before the IM and Presence Service software. More details are in Interoperability, page 26.

### 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.
- Make sure all relevant tasks in Upgrade Prerequisites and Software Dependencies, page 27 are complete.
- Note your MRA authentication settings before upgrading. This item only applies if you use the Expressway for MRA and you upgrade from X8.9.x 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. The upgrade does not preserve the existing Cisco Expressway-E settings, so 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:
  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**

### Clustered systems

To upgrade a clustered system, you should use the upgrade instructions in the *Expressway Cluster Creation and Maintenance Deployment Guide* on the Cisco Expressway Series configuration guides page. The following important requirement for upgrading clusters is explained in that guide, but for convenience it is also repeated here:

**CAUTION: For clustered systems, to avoid the risk of configuration data being lost and to maintain service continuity, it is ESSENTIAL TO UPGRADE THE PRIMARY PEER FIRST and then upgrade the subordinate peers ONE AT A TIME IN SEQUENCE.**

## Process

This process does not apply if you are upgrading a clustered system, or a Expressway that uses device provisioning (Cisco TMSPE), or FindMe (with Cisco TMS managing Expressway). In those cases, 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.x to X8.x, 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 feature release of Expressway (for example, from an X8.11 system to an X8.10 system). 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.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 5 Settings for MRA access control**

| Field | Description | Default |
|---|---|---|
| Authentication path | Hidden field until MRA is enabled. Defines how MRA authentication is controlled.<br><br>*SAML SSO authentication*: Clients are authenticated by an external IdP.<br><br>*UCM/LDAP basic authentication*: Clients are authenticated locally by the Unified CM against their LDAP credentials.<br><br>*SAML SSO and UCM/LDAP*: Allows either method.<br><br>*None*: 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.** | None before MRA turned on<br><br>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.<br><br>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.<br>(missing or bad snippet) | On |
| Authorize by OAuth token (previously SSO Mode) | Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*.<br><br>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*.<br><br>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.<br><br>The default is No, for optimal security and to reduce network traffic.<br><br>Controls how the Expressway-E reacts to remote client authentication requests by selecting whether or not the Expressway-C should check the home nodes.<br><br>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:<br><br>*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.<br><br>*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.<br><br>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.<br><br>**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*.<br><br>**Selecting an Identity Provider**<br><br>Cisco Collaboration solutions use SAML 2.0 (Security Assertion Markup Language) to enable SSO (single sign-on) for clients consuming Unified Communications services.<br><br>If you choose SAML-based SSO for your environment, note the following:<br><br>■ SAML 2.0 is not compatible with SAML 1.1 and you must select an IdP that uses the SAML 2.0 standard.<br>■ 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.<br>■ 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.<br><br>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:<br><br>■ OpenAM 10.0.1<br>■ Active Directory Federation Services 2.0 (AD FS 2.0)<br>■ PingFederate® 6.10.0.4 | – |
| Identity providers: Export SAML data | Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*.<br><br>For details about working with SAML data, see SAML SSO Authentication Over the Edge, page 1. | – |
| 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.<br><br>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.<br><br>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.<br><br>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 |

**Table 5 Settings for MRA access control (continued)**

| Field | Description | Default |
|---|---|---|
| SIP token extra time to live | Available if **Authorize by OAuth token** is *On*.<br><br>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<br><br>**Notes:**<br><br>**SSO mode**=*Off* in X8.9 is two settings in X8.10:<br><br>■ **Authentication path**=*UCM/LDAP*<br>■ **Authorize by user credentials**=*On*<br><br>**SSO Mode**=*Exclusive* in X8.9 is two settings in X8.10:<br><br>■ **Authentication path**=*SAML SSO*<br>■ **Authorize by OAuth token**=*On*<br><br>**SSO Mode**=*On* in X8.9 is three settings in X8.10:<br><br>■ **Authentication path**=*SAML SSO/and UCM/LDAP*<br>■ **Authorize by OAuth token**=*On*<br>■ **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) |

**Table 6 MRA access control values applied by the upgrade (continued)**

| Option | Value after upgrade | Previously on… | Now on… |
|---|---|---|---|
| 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 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.

**Note:** You need a customer or partner account to use Collaboration Solutions Analyzer.

**Getting started**

1. If you plan to use the log analysis tool, first collect the logs from your Expressway.
2. Sign in to https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/
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.

# Cisco Legal Information



# Cisco Trademark