Cisco Expressway X8.9.1

Release Notes

First Published: December 2016

Last Updated: September 2017

Contents

Preface

Change History

Table 1 Release Notes Change History

Date	Change	Reason
February 2017	Republished with clarification for scope of shared line/ multiple line feature.	Customer found issue.
January 2017	Add summary of X8.9.1 software and documentation enhancements. Update Resolved Issues section. Update Limitations section.	X8.9.1 maintenance release
December 2016	First publication.	X8.9

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.

Product Documentation

The following documents provide guidance on installation, initial configuration, and operation of the product:

For installing the Expressway, see:

- *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 general administration topics, reference, and maintenance, see:

- *Cisco Expressway Administrator Guide* on the Cisco Expressway Series maintain and operate guides page.
- *Cisco Expressway Serviceability Guide* on the Cisco Expressway Series maintain and operate guides page.

Other documents that may be relevant in your environment:

- Registrar:

  See *Cisco Expressway Registrar Deployment Guide* on the Expressway configuration guides page.
- Firewall Traversal:

  See *Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide* on the Expressway configuration guides page.
- Cisco Spark: Hybrid services knowledge base
- Clustering:

  See the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide*, for your version, on the Cisco Expressway Series configuration guides page.
- Certificates:

  See *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page.
- Unified Communications:

  See *Mobile and Remote Access Through Cisco Expressway* on the Expressway configuration guides page.
- Cisco Meeting Server:

  Cisco Expressway with Cisco Meeting Server Deployment Guide on the Expressway configuration guides page.

  See *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.
- Microsoft Infrastructure:

  See *Cisco Expressway with Microsoft Infrastructure Deployment Guide* on the Expressway configuration guides page.

  See *Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet* on the Expressway configuration guides page.

Changes and Features in X8.9.1

X8.9.1 is a maintenance release.

Important! We strongly recommend that you upgrade to this X8.9.1 software. The software includes a fix for an issue with the Call History table. This issue can in certain circumstances cause severe system problems (CDETS CSCvc58081 refers).

Software Enhancements in X8.9.1

Table 3 Feature History by Release Number

Feature / change	X8.9	X8.9.1
Apple Push Notifications Service Pass Through to Cisco Jabber for iPhone and iPad	Not supported	Supported
Edge Traversal of Microsoft SIP Traffic for Cisco Meeting Server	Supported	Supported
Web Proxy for Meeting Server	NOT SUPPORTED	NOT SUPPORTED
IM and Presence Service Federation With Skype for Business or Office 365 Organizations	Preview	Supported
Cisco Expressway as H.323 Gatekeeper	Supported	Supported
REST API Expansion	Supported	Supported
Allow Jabber for iPhone and iPad to Use Safari for SSO Over MRA	Supported	Supported
Shared Line / Multiple Line Support for MRA Endpoints	Preview	Supported
Smart Call Home	Preview	Preview
Secure Install Wizard	Supported	Supported
DiffServ Code Point Marking	Supported	Supported
Maintenance Mode For MRA	Supported	Supported
X8.9 Changes and Enhancements	Supported	Supported

Summary of changes

- If you have Cisco Jabber users with iOS devices, Expressway with Mobile and Remote Access now supports the Apple Push Notification Service. (Subject to the dependent systems being available.) See feature description below.
- The Install Wizard has these changes:
  - When deploying an OVA using the Install Wizard, a warning in relation to an RSA key being required has been removed. An RSA public key is only required if you wish to set the root and admin password through SSH – primarily used in automated deployments.
  - The serial number and release key, if available, now appear in the Install Wizard for reference purposes.
- For DCSP marking, traffic type "Video" is now assigned by default if the media type cannot be identified. (For example, if different media types are multiplexed on the same port.) Previously we assigned type "Audio" as the default.
- Miscellaneous security enhancements.

- A new alarm number 20021 exists, to warn about cluster communication failures.

Apple Push Notification Service Pass Through to Cisco Jabber for iPhone and iPad

If you have Cisco Jabber users with iOS devices, Expressway with Mobile and Remote Access is able to support the Apple Push Notification Service (APNs). This feature is subject to the dependent systems also being APNs-enabled.

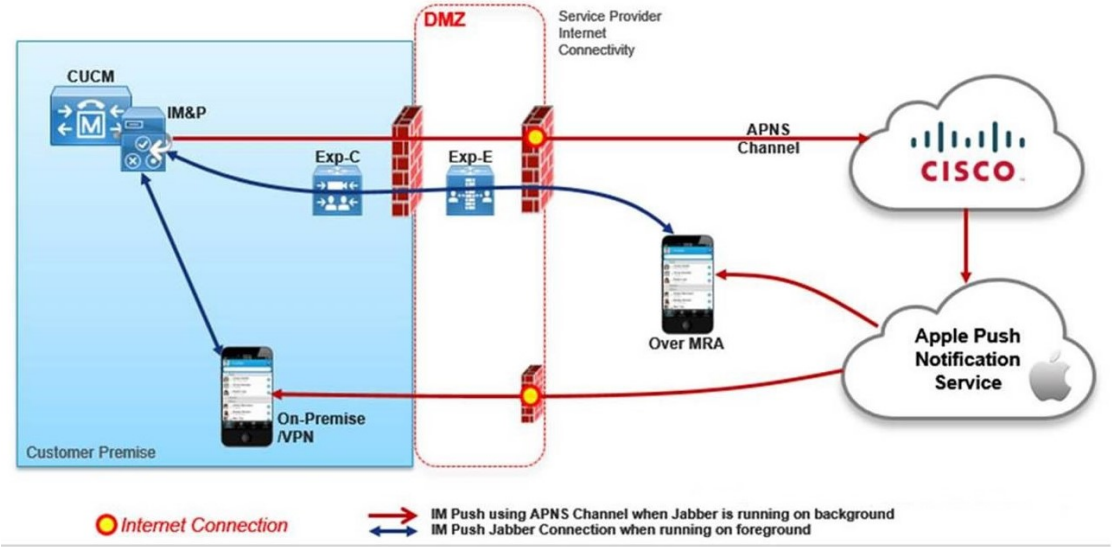
In X8.9.*n* this feature is used only for IM&P services, and not for video or voice calls.

No extra configuration is needed, assuming Expressway-E is already providing Mobile and Remote Access for Jabber iOS devices. The following requirements apply:

- Devices running an APNs-enabled Jabber for iOS software build.
- Cisco Unified Communications Manager IM and Presence Service running an APNs-enabled software version.

For more information, see *Deploying Apple Push Notifications for the IM and Presence Service* on the Cisco Unified Communications Manager IM and Presence Service Configuration and TechNotes page on Cisco.com

Figure 1 Example of Apple Push Notifications for CUCM IM&P and Jabber iOS



Documentation Changes in X8.9.1

The following sections in these notes have been updated:

- Limitations
- Notable Issues in this Version
- Resolved Issues list
- Cisco Expressway as H.323 Gatekeeper (endpoint software requirements corrected)

Changes to other documents include:

- The section "*What's New in this Version*" is now removed from the online help.
- The information about how to make backups and restore the system has been updated.
- We now clarify that we do not support downgrading an existing Expressway system to an earlier version.

- We now clarify that in paired configurations with a Expressway-C and a Expressway-E, the Expressway-E needs its own, separate public IP address. And if you use static NAT IP addressing, the Expressway-C must not use the same IP address as the Expressway-E.
- The *Mobile and Remote Access Deployment Guide* has new information about shared line and multiline support for endpoints connected through MRA. In section "*Unsupported Features When Using Mobile and Remote Access*".

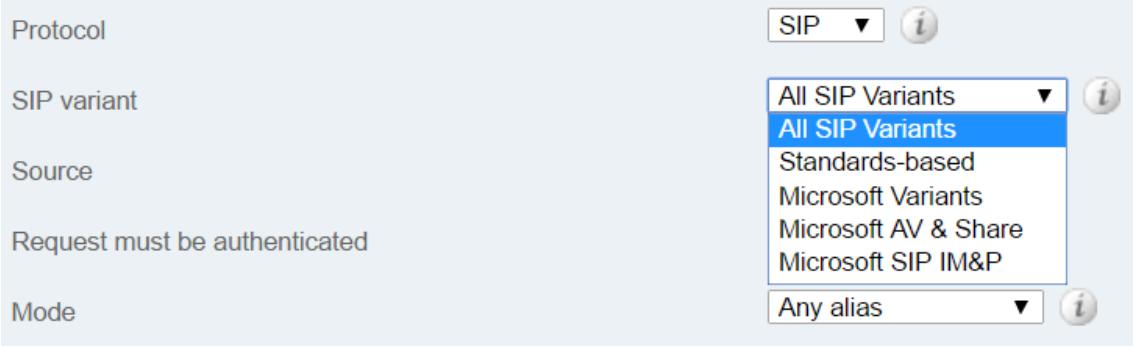
Features in X8.9

Edge Traversal Integration with Cisco Meeting Server

The Expressway pair at the edge of the network can now traverse Microsoft-variant SIP traffic to and from the Cisco Meeting Server. This allows your users to collaborate with people from external organizations that use Office 365 or Microsoft Skype for Business infrastructure. Users can meet in Meeting Server spaces, or make point-to-point calls between the organizations.

Two Expressway enhancements help you configure these collaboration scenarios:

- The DNS zone can do SRV lookups for the Microsoft federation service (`._sipfederationtls._tcp.example.com.`)
- Search rules now have the ability to route calls based on which variant of SIP is used on the call

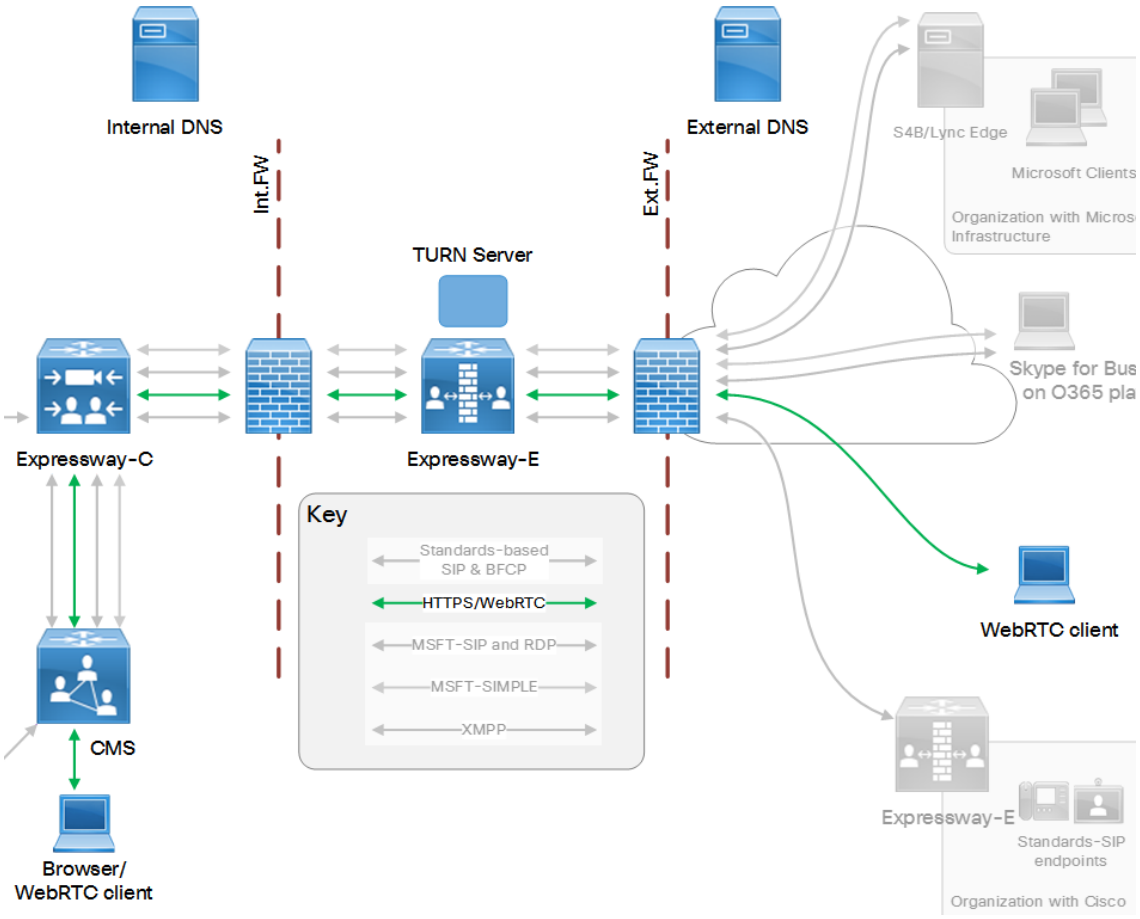


Cisco Expressway with Cisco Meeting Server Deployment Guide on the Expressway configuration guides page.

(NOT SUPPORTED) Web Proxy for Cisco Meeting Server

CAUTION: Do not use the Web Proxy for Meeting Server. This feature is not supported with this release of Expressway, due to known issues.

We've added a reverse https proxy for Cisco Meeting Server, which enables off-premises users to browse to a Meeting Server Web Bridge. Users can manage or join spaces without having any software other than a supported browser.



The proxy requires little extra configuration on the Expressway pair. Simply enter the Meeting Server listening address on the Expressway-C. Then the pair uses the existing traversal connection to proxy external https requests to that address.

You can enable the Web Proxy for Meeting Server on the same Expressway pair as MRA or other traversal features. However, you can't use it if the pair is configured for Jabber Guest.

More information

- List of supported browsers.
- *Cisco Expressway with Cisco Meeting Server Deployment Guide* on the Expressway configuration guides page.

You need Web Bridge version 2.1.2 or later to support this feature in Expressway.

IM and Presence Service Federation With Skype for Business or Office 365 Organizations

The Expressway pair at the edge of the network can now traverse messaging and presence traffic between IM and Presence Service and external organizations using Skype for Business or Office 365. For this feature to work, Cisco Unified Communications Manager IM and Presence Service must be running a compatible software version.

Cisco Expressway with Cisco Meeting Server Deployment Guide on the Expressway configuration guides page.

Cisco Expressway as H.323 Gatekeeper

X8.8 introduced the ability to use the Expressway-C as a SIP registrar, for TelePresence room and desktop systems. And a new licensing model with that feature.

X8.9 extends the feature to enable H.323 Gatekeeper functionality on the Expressway-C.

When you configure the Expressway as a SIP registrar or H.323 Gatekeeper, you must license it for concurrent systems (the Unified CM model), not for concurrent calls (the VCS model).

For SIP deployments, you can do this by adding either or both of the following license types to the Expressway-C:

- TelePresence Room System License
- Desktop System License

The following SIP devices register as desktop systems with all other devices considered room systems:

- Cisco TelePresence EX60
- Cisco TelePresence EX90
- Cisco DX70
- Cisco DX80

For H.323 deployments, all endpoints consume a TelePresence Room System License. This is due to a limitation in H.323, which does not determine the difference between desktop and room type endpoints.

We therefore recommend SIP as the preferred signaling protocol. H.323 is available as a fall back for endpoints that do not support SIP.

Note: DX systems must be running version CE8.2 or later and EX systems TC7.3.6 or later in order to register as desktop systems (for SIP only). DX and EX systems running earlier versions will still register for SIP but will consume a room system license.

Scope of the registrar feature:

- Option keys containing licenses for local registrations are installed on the Expressway-C.

  These licenses are pooled in a cluster, which means that Expressway-C peers can use each others' licenses. However, rooms cannot use desktop licenses, and desktop systems cannot use room licenses.
- Registrations from outside the network are proxied to Expressway-C by the Expressway-E. The Expressway-E cannot accept direct registrations.
- Proxy registration is possible with SIP endpoints only and does not apply to H.323 endpoints.
- Device provisioning and FindMe are supported with Cisco TelePresence Management Suite.
- The Large VM or CE1100 can support up to 5000 registrations, or 2500 MRA registrations (proxied to CUCM).

  Local registrations, proxy registrations (via Expressway-E), and MRA registrations, all count towards this number.

Implications of the new licensing model:

- Rich Media Session license usage has been reduced, following the principle that if you have already paid for a registration license you should not also pay for the Rich Media Session.
- Calls between registered systems do not use RMS licenses. Here, 'registered systems' means systems registered directly to the Expressway-C, by proxy to the Expressway-C through the Expressway-E, or by proxy through the Expressway pair (MRA) to neighbored Unified CMs.
- Calls from registered systems (as above) to Cisco infrastructure do not use RMS licenses. Currently, this extends only to Cisco Meeting Server, or to TelePresence Server when managed by TelePresence Conductor.
- Calls from registered systems (as above) to Cisco Collaboration Cloud do not use RMS licenses.

- Calls from registered systems to all other systems use one RMS license. This includes, but is not limited to, the following call types:
  - Business to business calls. Previously required two RMS licenses, now require one on Expressway-E.
  - Business to consumer calls (Jabber Guest). Previously required two RMS licenses, now require one on the Expressway-E.
  - Interoperability gateway calls (including Microsoft Lync / Skype for Business and third-party call control servers where interworking is required). Require one RMS license on the Expressway-C.

For more information:

See *Cisco Expressway Registrar Deployment Guide* on the Expressway configuration guides page.

Expressway Administrator Guide

To order registration licenses for the Expressway, see *Cisco Expressway X8.8 and Cisco TelePresence Video Communication Server (VCS) X8.8 Ordering Guide* at http://www.cisco.com/c/en/us/partners/tools/collaboration-ordering-guides.html

REST API Expansion

In X8.8, we introduced a new API to simplify remote configuration. Third party systems, such as Cisco Prime Collaboration Provisioning, can now use the API to configure the following features / services on the Expressway:

- Mobile and Remote Access (MRA)
- Business to business (B2B) calls

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

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

Allow Jabber on iOS to Use Safari for SSO Over MRA

This option applies if you use single sign-on (SSO) and have Cisco Jabber iOS endpoints that access Unified Communications services from outside the network. In this case, by default the identity provider's authentication page is displayed in an embedded web browser (not the Safari browser) on the iOS devices. That default browser is unable to access the iOS trust store, and so cannot use any certificates deployed to the devices. From X8.9, you can optionally configure Expressway-E to allow 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 SSO deployment.

Caveat

A potential security issue exists for this option. The mechanism to return browser control from Safari to Jabber after the identity provider 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.

Note: Make sure that you apply this option consistently in Expressway-E and in Unified CM. If you decide to enable or disable it in one application, do the same in the other. The relevant settings are:

- **Allow Jabber iOS clients to use embedded Safari browser** in Expressway-E (**Configuration > Unified Communications > Configuration > Single Signon** section)
- **SSO Login Behavior for iOS** in Unified CM (**System > Enterprise Parameters > SSO Configuration** section)

Supported endpoints

- Cisco Jabber for iOS 11.8 or later, on devices using iOS 9 or later

Supported Unified Communications services

- Cisco Unified Communications Manager 11.5(1)SU1 or later
- Cisco Unity Connection 11.5(1) or later

Shared Line / Multiple Line Support for MRA Endpoints

Expressway now supports pass through of Unified CM shared line and multiple line features for endpoints that are connecting by Mobile and Remote Access.

The benefit of this feature is that remote and mobile endpoint users can use features, like barge, conference barge, hold on one device and resume on another, in the same way as they would when they are on the premises.

You need to configure multiple and shared lines for users and their MRA devices on Unified CM.

Required versions:

- Unified CM 11.5(1)SU2 or later
- Expressway X8.9 or later
- Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series phones, with firmware version 11.5(1) or later

Note: This feature is disabled by default, because it impacts some features on earlier versions of Unified CM.

If you are using a Unified CM version before 11.5(1)SU2, and you enable SIP Path headers on Expressway-C, the following Unified CM features will *report the MRA devices' IP addresses instead of the Expressway's IP address*:

- Device Mobility
- Real-Time Monitoring Tool (RTMT)
- Cisco Emergency Responder (CER)

Other features may also be affected by this change. The devices' IP addresses are not useful for determining their location, as they are typically from reserved private ranges and could overlap with your organization's internal range.

(Preview) Smart Call Home

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.

Secure Install Wizard

The Expressway now includes an Install Wizard that helps make the deployment and configuration of your system easier and more secure.

The Install Wizard guides you through the initial configuration required to get your system up and running securely. Any further configuration is then possible using the web interface or CLI.

Only the person authorized to complete the system installation can access and complete the initial setup on the system console (or VM equivalent). All accounts on the Expressway are disabled upon first boot until the installation is complete. The system is also not accessible over the network interface until the installation has been completed and secured.

In a VM deployment, any preconfigured data gets imported when the VM boots for the first time and you are not required to re-enter data.

The Install Wizard does not affect the upgrade procedure for an existing system, as the system maintains any data that you have already configured.

Improved DiffServ Code Point Marking

From X8.9, the Expressway supports improved DSCP (Differentiated Service Code Point) packet marking for traffic passing through the firewall, including Mobile and Remote Access. DSCP is a measure of the Quality of Service level of the packet. To provide more granular control of traffic prioritization, DSCP values are set (marked) for these individual traffic types:

Traffic type	Supplied default value	Web UI field
Video	34	QoS Video
Audio	46	QoS Audio
XMPP	24	QoS XMPP
Signaling	24	QoS Signaling

Before X8.9 you had to apply DSCP values to all signaling and media traffic collectively.

You can optionally change the default DSCP values from the **System > Quality of Service** web UI page (or the CLI).

Notes:

- DSCP value "0" specifies standard best-effort service.
- DSCP marking is applied to SIP and H.323 traffic.
- DSCP marking is applied to TURN media, providing the TURN traffic is actually handled by the Expressway.
- Traffic type "Video" is assigned by default if the media type cannot be identified. (For example, if different media types are multiplexed on the same port.)

Existing QoS/DSCP Commands and API are Discontinued

From X8.9 we no longer support the previous methods to specify QoS/DSCP values. The former Web UI settings QoS Mode and QoS Value, CLI commands `xConfiguration IP QoS Mode` and `xConfiguration IP QoS Value` and corresponding API are now discontinued. Do not use these commands.

What if I currently use these commands?

When you upgrade the Expressway, any existing QoS value you have defined is automatically applied to the new fields and replaces the supplied defaults. For example, if you had a value of 20 defined, all four DSCP settings (QoS Audio, QoS Video, QoS XMPP, QoS Signaling) are set to 20 also.

We don't support downgrades. If you need to revert to your pre-upgrade software version, the QoS settings are reset to their original supplied defaults. So QoS Mode is set to *None* and QoS Value is set to *0*. You will need to manually redefine the values you want to use.

Improved Maintenance Mode

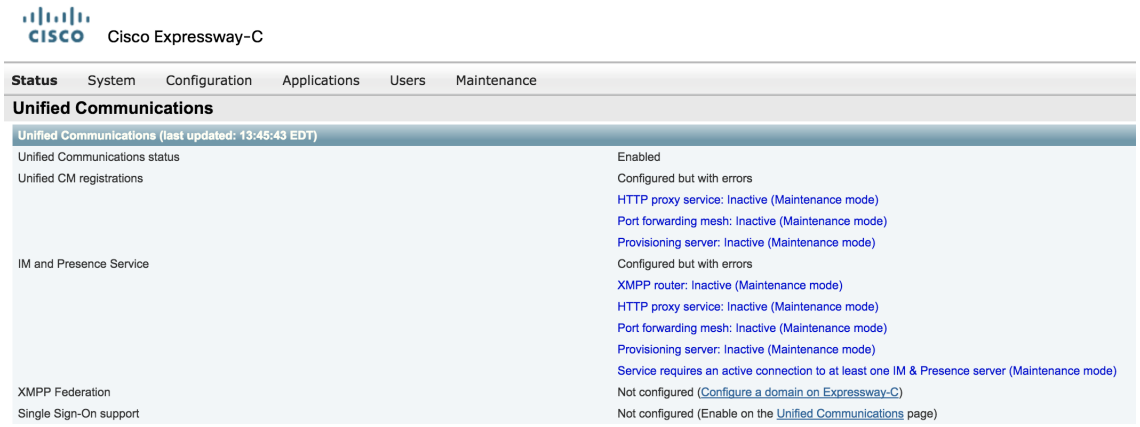
Maintenance mode on the Expressway has been enhanced so that you can bring an MRA system down in a managed way.

When you engage maintenance mode, the Expressway stops accepting new calls or proxy (MRA) traffic. Existing calls and chat sessions are not affected.

As users end their sessions normally, the system comes to a point when it is not processing any traffic of a certain type, and then it shuts that service down.

If users try to make new calls or start new chat sessions while the Expressway is in maintenance mode, the clients will receive a service unavailable response, and they might then choose to use another peer (if they are capable). This fail-over behavior depends on the client, but restarting the client should resolve any connection issues if there are active peers in the cluster.

The Unified Communications status pages also show (Maintenance Mode) in any places where MRA services are affected.



Other Changes and Enhancements

- The Expressway now supports advanced account security mode.
- You can nominate an administrator account as an emergency account. In case the Expressway disallows local authentication but is unable to connect to a remote authentication service.
- We have removed the limitation that TURN services should not be enabled on a system that is being used for MRA. We did this to allow services that require TURN to coexist with MRA. One example is edge traversal for Cisco Meeting Server.

  Note: This change does not make Jabber Guest compatible with MRA. It also does not mean that TURN can be used for MRA. The change simply means that MRA is not impacted if you enable TURN services (for other reasons).
- We have discontinued the pre-X8.9 API and CLI commands for defining QoS/DSCP values: `xConfiguration IP QoS Mode` and `xConfiguration IP QoS Value`. They are replaced by new commands / web UI settings.
- The web administration port is now configurable, on the **System > Administration** page. The default port is still 443.

- From X8.9 onwards, automated intrusion protection is enabled, by default, for the following categories:
  - http-ce-auth
  - http-ce-intrusion
  - sshpfwd-auth
  - sshpfwd-intrusion
  - xmpp-intrusion

  This change affects new systems. Upgraded systems keep their existing protection configuration.

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 X8.9.1
- Issues resolved by X8.9

Notable Issues in this Version

CSCva36208: **Rich Media Session license is not consumed by Single NIC Expressway-E hosting Jabber Guest service**

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

We recommend the Dual NIC Jabber Guest deployment.

If you use the single NIC deployment, make sure your Expressway-E is correctly licensed to ensure continuity of service with future upgrades.

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

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

Unsupported Features (General)

- DTLS is not supported through the Expressway-C/Expressway-E. SRTP is used to secure calls instead; attempts to make DTLS calls will fail.
- SIP UPDATE method. Features that rely on the SIP UPDATE method (RFC 3311) will not work as expected because the Expressway does not support this method.
- 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.

Unsupported Endpoint Features When Using MRA

Note: This list contains known limitations and is not exhaustive. The MRA deployment does not necessarily support pass through of line-side features provided by Cisco Unified Communications Manager. Absence of such items from this list does not imply that they are supported.

- Call recording for Cisco Jabber endpoints connected over Mobile and Remote Access (MRA).
- Cisco IP Phone 88xx and 78xx series support shared line or multiline features when connected through MRA (if Path Header support is enabled). We do not support shared line or multiline over MRA for other endpoints, phones, and soft clients.
- Custom embedded tabs for Cisco Jabber endpoints connected over MRA.
- Directory access mechanisms other than the Cisco User Data Service (UDS).
- Certificate provisioning to remote endpoints. For example, the Certificate Authority Proxy Function (CAPF). If you can do the first-time configuration on premises (inside the firewall) then you can support endpoints that use CAPF. After that you can use them over MRA - but you can't do the initial configuration over MRA.
- Features that rely on the SIP UPDATE method (RFC 3311) will not work as expected, because the Expressway does not support this method. For example, Unified CM and endpoints use UPDATE to implement blind transfer, which does not work correctly over MRA.
- Peer-to-peer file transfer when using IM and Presence Service and Jabber is unsupported over MRA.
  - Managed File Transfer (MFT) with IM and Presence Service 10.5.2 (and later) and Jabber 10.6 (and later) clients is supported over MRA.
  - File transfer with WebEx Messenger Service and Cisco Jabber is supported over MRA.
- Additional mobility features including GSM handoff and session persistency.
- Hunt group/hunt pilot/hunt list.
- Self-care portal.
- Jabber SDK is not supported over MRA.

Unsupported Expressway Features and Limitations When Using MRA

- The Expressway cannot be used for Jabber Guest when it is used for Mobile and Remote Access (MRA).
- The Expressway-C used for MRA cannot also be used for Microsoft gateway service. Microsoft gateway service requires a dedicated Expressway-C.
- MRA is not supported in IPv6 only mode.
- Endpoint management capability (SNMP, SSH/HTTP access).
- Multi-domain and multi-customer support is limited as follows:
  - Prior to X8.5, each Expressway deployment supported only one IM&P domain (even though IM and Presence Service 10.0 or later supports Multiple Presence Domains).
  - As of X8.5, you can create multiple deployments on the Expressway-C, but this feature is still limited to one domain per deployment.
  - As of X8.5.1, a deployment can have Multiple Presence Domains. This feature is in preview, and we currently recommend that you do not exceed 50 domains.
- Deployments on Large VM servers are limited to 2500 proxied registrations to Unified CM (the same limit as Small / Medium VM servers).
- Not all contact center features are supported by Expressway when connected through MRA.

Unsupported Contact Center Features When Using MRA

This section applies if you use the Cisco Unified Contact Center Express (Unified CCX) solution through Mobile and Remote Access (MRA).

Expressway does not support some Unified CCX features for contact center agents or other users who connect over MRA. Unsupported features include:

- Deskphone control functions (due to no support for CTI-QBE protocol).
- Built in Bridge (BIB) functions, which means that silent monitoring and recording, and agent greeting are not available.
- Shared line and multiline support for 78xx and 88xx series phones is available from X8.9 but is not in earlier Expressway versions.

Notes:

- Jabber for Mac and Jabber for Windows are not capable of deskphone control when they are connected over MRA. This is because the Expressway pair does not traverse the CTI-QBE protocol.
- If these Jabber applications, or other CTI applications, can connect to CUCM CTIManager (directly or through the VPN) they *can* provide deskphone control of clients that are connected over MRA.

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 X8.9 *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'"
```

Upgrading to X8.9.1

Prerequisites and Software Dependencies

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

- 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.

- Certificates: Certificate validation was tightened up in X8.8.
  - Try the secure traversal test before and after upgrade (**Maintenance > Security certificates > 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?

  Important! From version 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.

  Note: If you are upgrading to X8.8 or later from an earlier version, clustering communications changed in X8.8 to 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.

Downgrading to an Earlier Version is Not Supported

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.

Hybrid Services

Important! Your Management Connector must be up to date before you upgrade your Expressway. You must authorize and accept any Management Connector upgrades advertised by the Cisco Collaboration Cloud before attempting to upgrade your Expressway. Failure to do so may cause issues with the connector once you have upgraded your Expressway.

Note: X8.7.1 is now the minimum version required for Hybrid Services. If you are using Hybrid Services with X8.7, you must upgrade to X8.7.1 or later.

Existing TMS Agent (Legacy Mode) Provisioning Deployments

Expressway X8.1 and later no longer supports TMS Agent (legacy mode) provisioning. **Before you upgrade to X8 or later**, if you are using TMS Agent (legacy mode) for provisioning you must first migrate to Cisco TelePresence Management Suite Provisioning Extension which requires TMS 13.2.x. See *Cisco TMS Provisioning Extension Deployment Guide* for instructions about how to migrate.

Existing OCS Relay Deployments

Expressway X8.1 and later no longer supports OCS Relay integration with Microsoft Lync 2010 / OCS 2007 R2. If you use OCS Relay you must migrate to using the Microsoft Interoperability B2BUA to route SIP calls between the Expressway and Microsoft infrastructure. See *Cisco VCS and Microsoft Infrastructure Deployment Guide* for information about this deployment.

Upgrade Instructions

Before You Begin

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

If you are upgrading a clustered Expressway, you must follow the directions in *Expressway Cluster Creation and Maintenance Deployment Guide*.

Process

To upgrade a non-clustered Expressway:

1. Backup the Expressway (**Maintenance > Backup and restore**).

   You should backup your system before upgrading.
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 (**Status > Calls**).
4. Upgrade and restart the Expressway (**Maintenance > Upgrade**).

   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.

The upgrade is now complete and all Expressway configuration should be as expected.

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.

Note that certain services (such as Mobile and Remote Access) require both the Expressway-C and Expressway-E systems to be running the same software version.

- We strongly recommend installing a new server certificate if you are upgrading from any version of Expressway released prior to X8.1.1.

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. Paste or drag in your log file.
4. Click **Run**.

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