Cisco Expressway X8.8.2

Release Notes

First Published: June 2016

Last Updated: September 2016

Contents

Preface

Change History

Table 1   Release Notes Change History

Date	Change	Reason
September 2016	Added list of X8.8.2 enhancements and updated lists of open / resolved issues	X8.8.2 maintenance release
August 2016	Improved upgrade warning with reverse DNS required for Expressway-E	Customer impact of X8.8 security improvement
August 2016	Terminology corrected	Document errata
July 2016	Updated lists of open / resolved issues	X8.8.1 maintenance release
July 2016	Updated with new notable issue	CSCva36208
July 2016	Updated Expressway registrar feature description	Detail requested
June 2016	First publication	X8.8 release

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:

- Cisco Expressway Installation Guides
- *Cisco Expressway Administrator Guide* in Cisco Expressway Series Maintain and Operate Guides
- Hybrid services knowledge base
- *Cisco Expressway Basic Configuration Deployment Guide* in Cisco Expressway Series Configuration Guides
- *Cisco Expressway Serviceability Guide* in Cisco Expressway Series Maintain and Operate Guides

- *Cisco Expressway and Microsoft Infrastructure Deployment Guide* in Cisco Expressway Series Configuration Guides

Changes in X8.8.2

X8.8.2 is a maintenance release. The lists of Open and Resolved Issues, page 13, have been updated, and the software has the following enhancements:

- The call policy rule editor now has more granular control. You can use the web interface to create policy rules to allow or reject calls from specific zones or callers. You can also choose whether the rule applies to authenticated or unauthenticated callers.
- The clustering page now gives better feedback on DNS resolution and peer certificate status during cluster configuration.
- Zone pages now show how many registrations were proxied by the zones.
- The online help has been updated.

Changes in X8.8.1

X8.8.1 is a maintenance release. There are no new features, but the lists of Open and Resolved Issues, page 13, have been updated.

- Cisco Expressway Series has been certified FIPS compliant.
- Several important bug fixes and security patches have been applied.
- The online help has been updated for Expressway registrations and MRA allow list features.

Features in X8.8

Table 3   Feature History by Release Number

Feature / change	X8.8
Registrations On Expressway	Supported
Skype for Business 2016 and Skype for Business Mobile Support	Supported
Broker for Microsoft SIP Traffic	Supported
Multistream Support	Supported
Service Setup Wizard	Supported
MRA Allow List Improvement	Supported
API for Remote Configuration of MRA	Supported
Large VM CPU Reservation Reduced	Supported
High Security Environment	Supported
Software Package Signing	Supported
SSL/TLS Support Restricted	Supported
Changes and Minor Enhancements	Supported

Registrations On Expressway

Expressway-C can now be used as a SIP registrar for telepresence room and desktop systems. We have also introduced a new licensing model for calls that go through the Expressway, to align more closely with the Unified CM licensing model.

When you configure the Expressway as a registrar, you must license it for concurrent systems (CUCM model), rather than for concurrent calls (VCS model). You can do that by adding either or both of the following license types to the Expressway-C:

- TelePresence Room System License
- Desktop System License

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

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

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, that is, Expressway-C peers can use each others' licenses. However, rooms cannot use desktop licenses, nor can desktop systems use room licenses.

- Registrations from outside the network are proxied to the Expressway-C by the Expressway-E. The Expressway-E cannot accept direct registrations.

- Device provisioning and FindMe are supported with Cisco TelePresence Management Suite.

- H.323 registrations are not currently supported.

- The Medium VM (or CE1100 with 1 GBps NIC) can support up to 2500 registrations. The Large VM (or CE1100 with 10 GBps NIC) can support up to 5000 registrations.

  Local registrations, proxy registrations (via Expressway-E), and MRA registrations (proxied to CUCM), 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 will use one RMS license, whenever those calls require the Expressway to process the media streams. 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 the *Cisco Expressway Administrator Guide* available at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html or the *Cisco Single Expressway-C Basic Configuration Deployment Guide* available at the Expressway configuration guides page.

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

Skype for Business 2016 and Skype for Business Mobile Support

We have updated our support for Microsoft client and server combinations. The Gateway Expressway deployment is now interoperable with the following Microsoft collaboration products:

Table 4   Lync and Skype for Business Support Introduced in X8.8.2

Clients	On Lync Server 2013	On Skype for Business Server 2015
Skype for Business 2016 (Windows desktop)	Supported	Supported
Skype for Business 2015 (Windows desktop)	Supported	Supported
Skype for Business for iOS	Not supported	Limited support*
Skype for Business for Android	Not supported	Limited support*

* We do not support these clients in calls to MCU bridges. We do support them in other call scenarios, including calls to TelePresence Server bridges.

Broker for Microsoft SIP Traffic

In some previous versions of our *Cisco Expressway and Microsoft Interoperability Deployment Guide*, we published an appendix describing how to get Lync to Jabber messaging working using CPL on a "directory Expressway".

In X8.8, we have improved that deployment by creating an independent broker to perform the task of filtering and redirecting the messaging and presence traffic coming from the Microsoft infrastructure. This change has the following benefits:

- Maintains the robustness of the SDP parser, by not requiring it to process the non-standard SIP from Microsoft infrastructure
- No requirement for a directory Expressway, because the broker is hosted on the Gateway Expressway.
- The broker is abstracted from the rest of the software so you can disable it if you don't need it.
- If you were using the CPL deployment, you can now upgrade to X8.8 and benefit from the other features and improvements since X8.6.
- There is a new document to help you get Cisco Jabber integrated with Microsoft Skype for Business clients. Note that this integration relies on Lync Server 2013 or 2010; Skype for Business Server 2015 is not yet fully supported across all Cisco infrastructure in this deployment.

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

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

Multistream Support

The Expressway now supports passthrough of encrypted and unencrypted multistream calls. It also supports passthrough of the encrypted iX protocol required for the ActiveControl feature used by endpoints interacting with the TelePresence Server.

There is a new "Multistream mode" on all zone types that can potentially handle media. The mode is enabled by default, but it only applies when the zone passes media to or from the back to back user agent. The signaling of multistream calls is always passed through, irrespective of the zone's multistream mode setting.

Note:

- The Expressway does not encrypt the iX protocol on behalf of other entities; iX must either be encrypted from end to end, with the endpoints and TelePresence Server doing the encryption, or it must be unencrypted from end to end.

Service Setup Wizard

The Expressway can be used in different ways, some of which do not work together. Version X8.8 improves the user experience of configuring the Expressway for its chosen purpose in your environment.

When you first launch the user interface, you see a Service Setup Wizard instead of going straight into the menu. You can select the system series (VCS or Expressway) and type (*VCS Expressway/VCS Control* or *Expressway-E/Expressway-C*). These choices affect the list of services available.

Then you select from a number of popular Expressway services:

- Cisco Spark Hybrid Services
- Mobile and Remote Access
- Jabber Guest Services
- Microsoft Interoperability
- Registrar/ Proxy registrations (previously only possible on VCS, now also possible on Expressway)
- Collaboration Meeting Rooms (CMR) Cloud
- Business to Business Calling

When you have selected from the list, the wizard helps you to apply appropriate licenses for your selection, verify your basic configuration (network settings should have been configured previously), and then restart the system.

Following the restart, you'll only see the configuration pages and fields that are relevant for the service you selected. If you don't want to use the wizard you can skip through it, or you can go back to the start at any time.

Table 5   Services That Can Be Hosted Together

	Cisco Spark Hybrid Services (Connectors)	Mobile and Remote Access	Jabber Guest Services	Microsoft Interoperability	Registrar	CMR Cloud	Business to Business calling
Cisco Spark Hybrid Services (Connectors)	Y	N	N	N	N	N	N
Mobile and Remote Access	N	Y	N	N	Y	Y	Y
Jabber Guest Services	N	N	Y	N	Y	Y	Y
Microsoft Interoperability	N	N	N	Y	N	N	N
Registrar	N	Y	Y	N	Y	Y	Y
CMR Cloud	N	Y	Y	N	Y	Y	Y
Business to Business calling	N	Y	Y	N	Y	Y	Y

Key to Table

Y: Yes, these services can be hosted on the same system or cluster

N: No, these services may not be hosted on the same system or cluster

Rules

- Hybrid Services requires a dedicated Expressway-C to host Connectors
- Microsoft Interoperability requires a dedicated VCS Control or Expressway-C (called Gateway VCS or Gateway Expressway in the help and documentation)
- Jabber Guest cannot work with MRA (technical limitation)
- MRA is currently not supported in IPv6 only mode. If you want IPv6 B2B calling to co-reside with IPv4 MRA on the same Expressway traversal pair, the Expressway-E and Expressway-C must both be in dual stack mode.

MRA Allow List Improvements

The MRA allow list feature is more specific in this release. When you add, discover, or refresh the Unified Communications nodes on the Expressway-C, the Expressway automatically adds the nodes to the allow list. We are now being a lot more specific by including the port and request path in the allow list rule.

We also improved the interface for manually adding rules, enabling you to accurately specify the URL and so restrict the scope of access. For example, instead of allowing `something.example.com`, now you can add `https://something.example.com:8443/pathto/resource.htm` instead.

You can also restrict which HTTP methods you allow for each of your rules.

Note: You should review your editable rules after you upgrade the Expressway-Cs in your MRA deployment. We advise this because any servers you previously added to the allow list are upgraded to prefix matching rules. These rules allow any path on that server, using the default ports for the originally entered protocol.

The automatically added entries are automatically upgraded to be more specific than in previous releases.

API for Remote Configuration of MRA

The Expressway has a new API to simplify remote configuration. Third party systems, such as Cisco Prime Collaboration Provisioning, can use the API to configure Mobile and Remote Access on the Expressway.

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

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

Large VM CPU Reservation Reduced

The Large Expressway VM CPU reservation requirement has been reduced from 25600 MHz to 16000 MHz. This means that two Large Expressway VMs can now comfortably co-reside on a UCS server with two eight-core 3.2 GHz processors, when hyperthreading is enabled. This was not previously possible because the higher reservation requirement, added to the CPU requirement for the hypervisor, exceeded the total processing power of the host.

The new reservation does not limit the maximum Expressway CPU speed; the Expressway can use the headroom provided by the higher specification host.

Security Improvements

High Security Environments

With this release we have improved security in a number of Expressway components, and have implemented new ways of testing and threat modelling, as part of an ongoing effort to improve security.

If you deploy Expressway into a high security environment, you must apply the *Advanced Account Security* option key, then enable **FIPS140-2 cryptographic mode** and acknowledge that you consent to the associated restrictions.

Software Package Signing

Starting with this release, we are signing Expressway software packages to give you confidence in their integrity and authenticity.

We now do an integrity check before you commit to an upgrade. This means you can't tell that the package is being verified on this particular upgrade, because your pre-upgrade version does not have this feature. During your next upgrade, you'll see package signing information, like this:

Upgrade confirmation

System information

Current software version	X8.8
New software version	X8.8.1
Serial number	52A19427
Release key	[redacted]
Signing Information	Cisco

Software package hashes

SHA-1 hash	[redacted]
SHA-512 hash	[redacted]

`Continue with upgrade` `Abort upgrade`

TLS Support Restricted

To improve security, the Expressway now only supports specific versions of TLS. The Expressway offers and accepts TLS versions 1.0, 1.1, and 1.2, when establishing secure connections.

Changes and Minor Enhancements

- From version X8.8 onwards, the Expressway does not create DSA host keys. It creates RSA or ECDSA keys instead, for improved security.

  If you upgrade a system that already has a DSA host key, the existing key will persist so that SSH client users do not have to verify the fingerprint again.

- From version X8.8 onwards, connections between cluster peers use TLS instead of IPSec. When you upgrade a cluster, the cluster comes up in TLS permissive mode.

- Multiple Device Messaging (a new feature in IM and Presence Service 11.5) is now supported for clients that connect through Expressway to IM and Presence Service in the cloud.

  This feature is not supported through any versions of Expressway before X8.8.

Open and Resolved Issues

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 modifed (recent first)
- Issues resolved by X8.8.2
- Issues resolved by X8.8.1
- Issues resolved by X8.8

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 release have 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 could cause confusion about the server's load because the usage appears low, even when the server is processing multiple calls. We recommend the Dual NIC Jabber Guest deployment.

If you are using the single NIC deployment, make sure your Expressway-E is correctly licensed to ensure continuity of service when upgrading in future.

CSCva18731: **Calls to/from Skype for Business Android v6.4.0.5 fail due to ICE (internal/external)**

Skype for Business for Android version 6.4.0.5 cannot make or receive calls with standards-based endpoints (via Expressway configured for Microsoft interoperability) when the calls have both audio and video streams.

You can work around this issue in one of these ways:

- Using Skype for Business for Android 6.4.0.5 (or later): Make or answer calls as audio-only, and then add video after the audio call is established.
- Use an earlier release of Skype for Business for Android: For example, versions 6.0.0.8, 6.2.0.3, or 6.3.0.2 do not have this issue. Note that these versions are no longer available through the official channels.

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 Mobile and Remote Access

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.

Limitations

- Calls to/from additional lines on IP phones and endpoints that support multiple lines; only the primary line is supported via Mobile and Remote Access.
- Directory access mechanisms other than UDS.
- Certificate provisioning to remote endpoints e.g. CAPF.
- 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, CUCM and endpoints use UPDATE to implement blind transfer, which does not work correctly via MRA.
- Peer-to-peer file transfer when using IM and Presence Service and Jabber is unsupported via MRA
  - Managed File Transfer (MFT) with IM and Presence Service 10.5.2 (and later) and Jabber 10.6 (and later) clients is supported via MRA
  - File transfer with WebEx Messenger Service and Cisco Jabber is supported via MRA
- Jabber SDK, Jabber for Mac, and Jabber for Windows are not capable of deskphone control when they are connected over MRA, because the CTI-QBE protocol is not traversed by the Expressway pair. When these Jabber applications, or other CTI applications, can connect to CUCM CTIManager (on-premises or VPN) then they can deskphone control endpoints and clients that are connected over MRA.
- Additional mobility features including GSM handoff and session persistency.
- Hunt group/hunt pilot/hunt list.
- Self-care portal.
- Support for Jabber SDK.
- Shared lines are not supported on endpoints connected over MRA.

  Some shared line features may work but are not supported.

Unsupported Expressway Features and Limitations When Using Mobile and Remote Access

- The Expressway cannot be used for Jabber Guest when it is used for MRA.
- The Expressway-C used for Mobile and Remote Access cannot also be used for Microsoft Interoperability. Microsoft Interoperability 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.
- NTLM authentication via the HTTP proxy.
- Maintenance mode; if the Expressway-C or the Expressway-E is placed into maintenance mode, any existing calls passing through that Expressway will be dropped.
- The Expressway-E must not have TURN services enabled.
- Deployments on Large VM servers are limited to 2500 proxied registrations to Unified CM (the same limit as Small / Medium VM servers).

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.

To ensure continuous interoperability, you must upgrade your Expressway systems to X8.8 *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 X8.8.2

Prerequisites and Software Dependencies

Upgrade Caution, PLEASE READ: X8.8 is 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:

- Minimum versions of Unified Communications infrastructure: Unified CM, IM and Presence Service, and Cisco Unity Connection have all 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 to X8.8.

  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 before you upgrade IM and Presence Service to 11.5.

- Certificates: Certificate validation has been 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, 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.

Hybrid Services

Your Management Connector must be up to date before you upgrade your Expressway. You must authorize and accept any upgrades advertised by the Cisco Collaboration Cloud before attempting to upgrade.

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

When maintenance mode is enabled on Expressway, existing calls passing through it may be dropped. We recommend that you upgrade Expressway components while the system is inactive.

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

To upgrade a non-clustered Expressway:

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

   You should backup your system before upgrading. If you later need to downgrade to an earlier release you will have to restore a backup made against that previous release.

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