



Cisco Expressway

Release Note

First Published: July 2015

Last Updated: February 2016

Software version: X8.6

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](#)
- *Cisco Expressway Basic Configuration Deployment Guide* in [Cisco Expressway Series Configuration Guides](#)
- *Cisco Expressway Serviceability Guide* in [Cisco Expressway Series Maintain and Operate Guides](#)
- [Cloud Extensions knowledge base](#)
- *Cisco Expressway and Microsoft Lync Deployment Guide* in [Cisco Expressway Series Configuration Guides](#)

New Features in X8.6

Table 1 Feature history by release number

Feature / change	X8.6
Lync Desktop Sharing	Supported
Cloud Extensions	Supported
License bypass for calls to cloud-based Collaboration Meeting Rooms (CMRs)	Supported
New codec support: OPUS and H.265	Supported
System Metrics Collection	Supported
Cisco DX Series endpoints over MRA	Supported with endpoint version 10.2.4(99) or later

Table 1 Feature history by release number (continued)

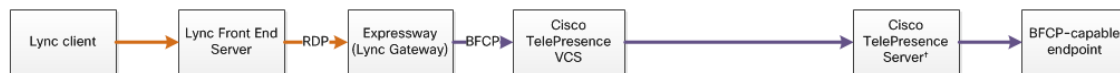
Feature / change	X8.6
Cisco IP Phone 7800/8800 Series over MRA	Preview with endpoint version 10.3.1 or later
Multiple Presence Domains via MRA	Preview
Japanese, Korean, Russian localizations	X8.5.1 UI
Changes and minor enhancements	Supported

Support for Desktop Sharing from Lync

The Expressway now supports desktop or application sharing from Lync clients with conference participants using Cisco Collaboration endpoints.

The Expressway does the transcoding of the Microsoft Remote Desktop Protocol (RDP), originating from the Lync client, into the Binary Floor Control Protocol (BFCP) used by many standards-based endpoints. The Expressway does not perform the reverse transcoding from BFCP to RDP, and presentation towards Lync will go in the video channel as in previous releases.

The following deployments support desktop sharing from Lync:

Figure 1: Lync environment to TelePresence Server conference registered to VCS**Figure 2: Lync environment to TelePresence Server conference managed by TelePresence Conductor neighbored to VCS****Figure 3: Lync environment to TelePresence Server conference managed by TelePresence Conductor trunked to Unified CM****Note:**

† If you are using the Optimize Resources feature with Lync desktop sharing, you need TelePresence Server version 4.2 or later

‡ If you are using the Optimize Resources feature with Lync desktop sharing, you need TelePresence Conductor version XC4.0

To configure your Cisco Collaboration environment to interoperate with Microsoft Lync, see the *Microsoft Lync and Cisco Expressway Deployment Guide* on the [Cisco Expressway Series Configuration Guides](#) page.

Cloud Extensions

What are Cloud Extensions and what do they do?

Cisco Cloud Extensions empower cloud-based and premises-based solutions to deliver a more capable, better

integrated collaboration user experience.

Note: "Cloud Extensions" is a temporary group name for a growing number of hybrid services. Forthcoming versions of Expressway software and documentation will use "Hybrid Services" in place of "Cloud Extensions".

Which services am I entitled to use?

When you purchase Cloud Extension services you get access to Cloud Collaboration Management—an administrative interface to the Cisco Collaboration Cloud. In Cloud Collaboration Management you can check your organization's service entitlements and enable features for your users.

What software do I need?

The on-premises components of Cloud Extensions are called "connectors", and the Expressway software contains a management connector to manage registration and other connectors.

The management connector is dormant until you register. When you register, the management connector is automatically upgraded if a newer version is available.

The Expressway then downloads any other connectors that you selected using Cloud Collaboration Management. They are not started by default and you need to do some configuration before they'll work.

How do I install, upgrade, or downgrade?

The connectors are not active by default, and will not do anything until you configure and start them. You can do this on new UI pages that the connectors install on the Expressway.

Connector upgrades are made available through Cloud Collaboration Management, and the management connector will download the new versions to Expressway when you have authorized the upgrade.

You can also deregister, which disconnects your Expressway from Collaboration Cloud and removes all connectors and related configuration.

Note: We do not normally advise downgrading Expressway, although we try to ensure that the interface remains accessible if you are forced to restore a previous version. However, we explicitly do not support a downgrade of the Expressway software from X8.6 versions while the Expressway is registered for Cloud Extensions. If you have to downgrade, **you must deregister from Cloud Extensions before you downgrade.**

Where can I read more about Cloud Extensions?

Cloud Extensions are continuously developed and may be published more frequently than Expressway. This means that information about Cloud Extensions is maintained on the [Cloud Extensions help site](#), and several Expressway interface pages link out to that site.

License Bypass for Calls to Collaboration Meeting Rooms (CMRs)

The Expressway no longer requires rich media session licenses for calls to and from cloud-based CMRs. This includes SIP calls between Collaboration Cloud and the CMR Hybrid solution.

Note: This only applies when the dialed string does not need transformation on the Expressway (for example, user@sitename.webex.com).

Although untransformed SIP calls to cloud-based CMRs do not consume licenses, they do consume resources and may not progress if the Expressway is at full capacity.

There is no license bypass for CMR Premises calls. H.323 calls to cloud-based CMRs still consume licenses.

New Codec Support

The Expressway now supports the H.265 video and OPUS audio codecs. The codecs are supported in SIP traversal calls (that is, calls where the Expressway is handling the media streams).

These codecs are not supported on SIP - H.323 interworked or H.323 - H.323 calls.

System Metrics Collection

What is System Metrics Collection, and how does it work on Expressway?

System Metrics Collection is a feature on Expressway that publishes system performance statistics, enabling remote monitoring of performance.

The Expressway collects statistics about the performance of the hardware, OS, and the application, and publishes these statistics to a remote host (typically a data analytics server) that aggregates the data.

Where do I configure System Metrics Collection?

You can configure this feature on Expressway via the web interface or the command line. The configuration from one peer applies throughout the cluster, so we recommend that you configure it on the master peer if you are monitoring a cluster.

There is also some configuration required on the remote server; the collectd daemon should be running on the server, and should have the collectd network plugin configured to listen on an address that can be seen by the clients. Further details depend on your monitoring environment and are beyond the scope of this information.

How can I use this data?

You can use the data to generate graphs, aggregate statistics, and analyze performance, using tools such as Circonus and Graphite.

Where can I read more about System Metrics Collection?

For more details see the *Cisco VCS Serviceability Guide* on the [Cisco VCS Maintain and Operate Guides](#) page.

MRA Support for New Endpoints

Mobile and Remote Access is being expanded to include the following new endpoints.

The DX Series endpoints are officially supported via MRA if they are running version 10.2.4(99) or later. The Cisco IP Phone 78/8800 Series endpoints are not yet officially supported via MRA, but they must be running version 10.3.1 or later if you want to preview them with Mobile and Remote Access.

- [Cisco DX650](#)
- [Cisco DX80](#)
- [Cisco DX70](#)
- [Cisco IP Phone 8800 Series](#)
- [Cisco IP Phone 7800 Series](#)

When deploying DX Series or IP Phone 78/8800 Series endpoints to register with Cisco Unified Communications Manager via Mobile and Remote Access, you need to be aware of the following:

- **Phone security profile:** If the phone security profile for any of these endpoints has **TFTP Encrypted Config** checked, you will not be able to use the endpoint via Mobile and Remote Access. This is because the MRA solution does not support devices interacting with CAPF (Certificate Authority Proxy Function).

- **Trust list:** You cannot modify the root CA trust list on these endpoints. Make sure that the Expressway-E's server certificate is signed by one of the CAs that the endpoints trust, and that the CA is trusted by the Expressway-C and the Expressway-E.
- **Bandwidth restrictions:** The **Maximum Session Bit Rate for Video Calls** on the default region on Cisco Unified Communications Manager is 384 kbps by default. The **Default call bandwidth** on Expressway-C is also 384 kbps by default. These settings may be too low to deliver the expected video quality for the DX Series.

(Preview) Multiple Presence Domains / Multiple IM Address Domains via MRA

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

Limited testing has shown that this feature works via MRA. Hence this feature is in preview with Expressway X8.5.1 and later, pending further testing and full support in a future version of Expressway.

Note: This feature is distinct from the multiple deployments feature released in X8.5. That feature is limited to one domain per deployment, where all IM and Presence Service clusters within a deployment serve a single domain. This feature is different because it concerns MRA support for all IM and Presence Service clusters within a deployment serving a common set of one *or more* Presence domains.

Each new domain impacts the Expressway's performance. We currently recommend that you do not exceed 50 domains.

Updated Language Packs

Language packs are now available for the following languages. The packs include localized web interface and embedded webhelp. See *Install Language Packs* for details of changing the language pack.

- Japanese
- Russian
- Korean

Note: These localizations apply to the X8.5.1 versions of the UI and embedded help. They complete the set announced in the X8.5.3 release notes (Chinese, French, German, and Spanish).

Changes and Minor Enhancements

- The functionality provided by the Interworking option key is now included in the Expressway option key.
- There is a new option to modify the **SIP TCP connect timeout (Configuration > Protocols > SIP > Advanced)**. The default is 10 seconds.
- Mutual TLS authentication can now be configured for SIP calls (**Configuration > Protocols > SIP**). Two new parameters were added **Mutual TLS mode** (default Off) and **Mutual TLS port** (default 5062).
- A new zone parameter called **SIP parameter preservation** controls whether the SIP URI and Contact parameters are preserved between the zone and the B2BUA.
- A new zone parameter called **Preloaded SIP routes support** controls whether the zone processes SIP INVITE requests that contain the Route header.
- There is a new command line option to change the cipher suites used for SIP TLS connections. The command takes a colon-delimited string of cipher suites (see <https://www.openssl.org/docs/apps/ciphers.html#CIPHER-LIST-FORMAT>). For example, to set the current Expressway default suite, use:

```
xConfiguration SIP TLS CipherSuite: ALL:!EXP:!LOW:!MD5:@STRENGTH:+ADH
```
- The diagnostic log now includes two new .xml files, to record the xconfig and xstatus of the Expressway at the time the log was taken.

- The **Call Detail Records (CDR)** switch has moved from the **System > Administration** page to the **Maintenance > Logging** page.
- The CLI commands `xCommand LoginUserAdd` and `xCommand LoginUserDelete` have been replaced by `xCommand CredentialAdd` and `xCommand CredentialDelete`.
- The hop count logic has changed so that internal hops between the Expressway application and its B2BUA do not decrement the hop count.
- Several advanced zone parameters have been removed because they are no longer required. These are **SIP SDP attribute line limit mode**, **SIP SDP attribute line limit length**, and **SIP Duo Video filter mode**.
- The **Maximum authorizations per period** default has increased to 8.

Open and Resolved issues

Follow the links below to read the most recent information about the open and resolved issues in this release. You need to refresh your browser after you log in to the Cisco Bug Search Tool.

- [All open issues, sorted by date modified \(recent first\)](#)
- [Issues resolved by X8.6](#)

Notable Issues in this Version

CSCuv47574: SDP Decode Fails when Trying to Split IM&P and Video From Lync

This issue in X8.6 prevents a previously published Lync federation deployment from working as it did in X8.5. If you are using the affected deployment, we recommend that you do not upgrade to X8.6.

The affected deployment is documented in *Appendix 1: Federation*, of the *Microsoft Lync and Cisco Expressway Deployment Guide*, on the [Cisco Expressway Series Configuration Guides page](#).

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.

- 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
- Deskphone control (QBE/CTI)
- Additional mobility features including DVO-R, GSM handoff and session persistency
- Hunt group/hunt pilot/hunt list
- Self-care portal
- Support for Jabber SDK
- Shared lines are supported in a limited way. Multiple endpoints can share a line but in-call features (like hold/resume) only work on the first endpoint that answers. Endpoints sharing the line may not correctly recognise the state of the call.

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 as a Lync 2013 gateway (if required, this must be configured on a stand-alone Expressway-C).
- Secure XMPP traffic between Expressway-C and IM&P servers (XMPP traffic is secure between Expressway-C and Expressway-E, and between Expressway-E and remote endpoint).
- 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).

Supported Clients When Using Mobile and Remote Access

- Cisco Jabber for Windows 9.7 or later
- Cisco Jabber for iPhone and iPad 9.6.1 or later
- Cisco Jabber for Android 9.6 or later
- Cisco Jabber for Mac 9.6 or later
- Cisco TelePresence endpoints/codecs running TC7.0.1 or later firmware

MRA Support for New Endpoints

The Cisco IP Phone 78/8800 Series endpoints are not yet officially supported via MRA, but they must be running version 10.3.1 or later if you want to preview them with Mobile and Remote Access.

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.

Upgrade to X8.6

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 features introduced in recent software versions (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.

Install Language Packs

You can install new language packs or install an updated version of an existing language pack.

Language packs are downloaded from the same area on cisco.com from where you obtain your Expressway software files. All available languages are contained in one language pack zip file. Download the appropriate language pack version that matches your software release.

After downloading the language pack, unzip the file to extract a set of .tlp files, one per supported language.

To install a .tlp language pack file:

1. Go to **Maintenance > Language**.
2. Click **Browse** and select the **.tlp** language pack file you want to upload.
3. Click **Install**.

The selected language pack is then verified and uploaded. This may take several seconds.

4. Repeat steps 2 and 3 for any other languages you want to install.

After upgrading to this software release, if you have previous language packs installed, you will see a "Language pack mismatch" alarm. Updated language packs for this release will be made available soon. In the meantime you will see a mixture of some text in your chosen language and some text (predominantly text related to new features) in English.

Note that:

- English (en_us) is installed by default and is always available.
- You cannot create your own language packs. Language packs can be obtained only from Cisco.

Available languages

The following table lists the set of languages currently available and the .tlp filename used to refer to that language.

Table 2 Available language packs

Language	.tlp filename format
Chinese (Simplified)	vcs-lang-zh-cn_<ver>.tlp
French	vcs-lang-fr-fr_<ver>.tlp
German	vcs-lang-de-de_<ver>.tlp
Japanese	vcs-lang-ja-jp_<ver>.tlp
Korean	vcs-lang-ko-kr_<ver>.tlp
Russian	vcs-lang-ru-ru_<ver>.tlp
Spanish	vcs-lang-es-es_<ver>.tlp

Use 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.

Obtain Documentation and Submit a Service Request

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* at: www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Document revision history

Table 3 Expressway release notes revisions

Date	Revision	Description
August 2015	Feature update	Republished post DX Series 10.2.4(99) release; those endpoints now officially support MRA
July 2015	First publication	X8.6 Release



Cisco Legal Information

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

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

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

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

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

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

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

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

© 2015 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

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