Cisco Expressway X8.5.3

Software Release Notes
June 2015

Contents

Product documentation

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

- Cisco Expressway Administrator Guide
- Cisco Expressway Cluster Creation and Maintenance Deployment Guide
- Cisco Expressway on Virtual Machine Installation Guide

The Cisco Expressway installation and configuration guides on Cisco.com cover topics such as basic configuration, Unified Communications mobile and remote access, certificate creation and use, ENUM dialing, external policy, integration with Cisco Unified Communications Manager and Microsoft Lync.

X8.5.n Feature support history

Table 1: Feature history by release number

Feature / change	X8.5.3	X8.5.2 (withdrawn)	X8.5.1	X8.5
KPML	Supported	Supported	Not supported	Not supported
Multiple Presence Domains via MRA	Preview	Preview	Preview	Not supported
SSO over MRA	Supported	Supported	Supported; SAML signing algorithm changed	Preview
CSR UI digest algorithm options	Supported	Supported	Supported	Not supported
Cisco DX Series endpoints over MRA	Preview (with KPML)	Preview (with KPML)	Preview (no KPML)	Preview (no KPML)
Cisco IP Phone 7800/8800 Series over MRA	Preview (with KPML)	Preview (with KPML)	Preview (no KPML)	Preview (no KPML)
Early media	Supported	Supported	Supported	Supported
Unsolicited NOTIFY pass-through	Supported	Supported	Supported	Supported
Multiple deployments	Supported	Supported	Supported	Supported
Secure connection checker	Supported	Supported	Supported	Supported
Syslog publish filter	Supported	Supported	Supported	Supported
Call Detail Records (CDRs)	Supported	Supported	Supported	Supported
Media statistics	Supported	Supported	Supported	Supported
Password change requires authorization	Supported	Supported	Supported	Supported
Static routes	Supported	Supported	Supported	Supported

Changes in X8.5.3

Version X8.5.3 is a maintenance release. The lists of Open and Resolved Issues [p.9] have been updated since the previous release.

Note: Version X8.5.3 supersedes the X8.5.2 release. The X8.5.2 software is no longer available for download and we strongly recommend that you upgrade to X8.5.3.

Changes in X8.5.2

Version X8.5.2 is a maintenance release. The lists of Open and Resolved Issues [p.9] have been updated since the previous release.

This maintenance release also builds on features introduced in previous X8.5 releases, as follows:

(Preview) MRA support for new endpoints

Note: This feature is implemented in this version for the purpose of previewing with dependent systems. It is not currently supported and should not be relied upon in your production environment. Full support for this feature is planned for future releases of the Expressway software and the interdependent systems below.

Mobile and Remote Access is extended in this release to include support for the Cisco DX Series endpoints, and the 8800 Series and 7800 Series IP phones, registering to Cisco Unified Communications Manager. A previous limitation of the support for these endpoints, in which KPML pass-through was not working in some circumstances, has been resolved in X8.5.2.

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

The DX Series must be running at least version 10.2.4, in which MRA support is described as "Unsupported Marketing Beta", to enable preliminary testing with MRA in your deployment. The Cisco IP Phone 78/8800 Series endpoints must be running version 10.3.1 or later if you want to use them for 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.

KPML pass-through

With Key Press Markup Language support, phone users outside the network can use endpoint-signaled Unified CM features like off-hook dial, group call pickup, abbreviated dial and others.

Updated language packs

The web interface and embedded webhelp are localized into the following languages. See *Installing language packs* for details of changing the language pack.

- Chinese
- French
- German

- Spanish
- Japanese
- Korean
- Russian

Note: These localizations apply to the X8.5.1 versions of UI and help.

Important behavior changes

MRA authorizations are now rate controlled by default, to reduce the load of unnecessary authorizations on the Expressway. Take care when you upgrade because your current endpoint software may be reauthorizing more often than necessary, which could result in the Expressway issuing HTTP 429 "Too Many Requests". If you routinely see this error after upgrade, you can edit the rate control settings at **Configuration > Unified Communications > Configuration > Advanced**.

Software enhancements

- This release introduces rate control for successful authorisations, via MRA, of users accessing collaboration services; this feature applies to SSO-authenticated users as well as non-SSO-authenticated users.
- The Single Sign-On feature introduced in X8.5.1 has been further improved in this release. The status information concerning user tokens has been improved. You can also purge tokens issued to a user, or to all users, if necessary. The UI for the SAML export feature has been improved.
- The cluster database (CDB) resiliency has been improved.

Changes in X8.5.1

Version X8.5.1 is a maintenance release. The lists of Open and Resolved Issues [p.9] have been updated since the previous release.

This maintenance release also builds on features introduced in the X8.5 release, as follows:

SSO over MRA

Single Sign-On over MRA is released with X8.5.1; this feature was previewed in X8.5. The *Features in X8.5.n* section has been updated with information about SSO over MRA.

The Expressway-C now defaults to SHA-256 for signing SSO requests it gives to clients, and you can change it to use SHA-1 if required. In version X8.5, when the SSO feature was previewed, the Expressway-C defaulted to SHA-1 and there was no way to select a different algorithm.

Note: If you were using the SSO feature with X8.5, this change may cause it to stop working after upgrade to X8.5.1. You have two options to resolve this: leave the new default on the Expressway-C, and you may need to reconfigure the IdP to expect requests to be signed with SHA-256 (recommended for better security); the other option is to revert the Expressway-C's signing algorithm to SHA-1 for your IdP (go to **Configuration > Unified Communications > Identity Providers (IdP)**, locate your IdP row, then in **Actions** column click **Configure Digest**).

Jabber 10.6 File Transfer support

The Cisco Jabber file transfer over MRA limitation, which was previously documented in Expressway documents, has now changed as follows:

- 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.

(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 being previewed with Expressway X8.5.1, 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 preview 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 10 domains.

Features in X8.5.n

Feature previews

The following features are implemented in this version for the purpose of previewing with dependent systems. They are not currently supported and should not be relied upon in your production environment. Full support for these features is planned for a future release of the Expressway software.

(Preview) Single sign-on over MRA

Enables single sign-on (common identity) for SSO-capable clients that are accessing on-premises Unified Communications services from outside the network.

(Preview) MRA support for new endpoints

Mobile and Remote Access is extended in this release to include support for the Cisco DX Series endpoints, and the 8800 Series and 7800 Series IP phones, registering to Cisco Unified Communications Manager. Some features on the IP phones, particularly where they rely on DTMF/KPML pass-through, were not available in X8.5. This limitation was resolved in X8.5.2.

Single sign-on over MRA

Use this feature to enable single sign-on for endpoints accessing Unified Communications services from outside the network. Single sign-on over the edge relies on the secure traversal capabilities of the Expressway pair at the edge, and trust relationships between the internal service providers and the externally resolvable identity provider (IdP).

The endpoints do not need to connect via VPN; they use one identity and one authentication mechanism to access multiple Unified Communications services. Authentication is owned by the IdP, and there is no authentication at the Expressway, nor at the internal Unified CM services.

Supported endpoints

- Cisco Jabber 10.6 or later

Supported Unified Communications services

- Cisco Unified Communications Manager 10.5(2) or later
- Cisco Unity Connection 10.5(2) or later
- Cisco Unified Communications Manager IM and Presence Service 10.5(2) or later
- Other internal web servers, for example intranet

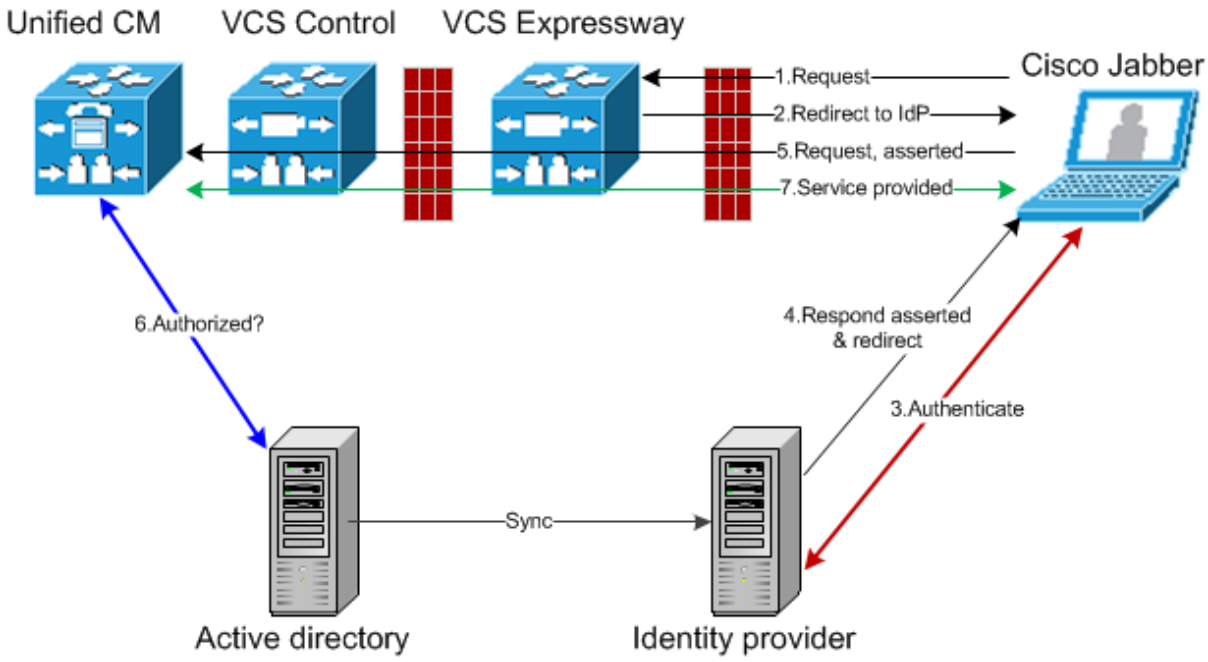
How it works

Cisco Jabber determines whether it is inside the organization's network before it requests a Unified Communications service. If it is outside the network, then it requests the service from the Expressway-E on the edge of the network. If single sign-on is enabled at the edge, the Expressway-E redirects Jabber to the IdP with a signed request to authenticate the user.

The IdP challenges the client to identify itself. When this identity is authenticated, the IdP redirects Jabber's service request back to the Expressway-E with a signed assertion that the identity is authentic.

The Expressway-E trusts the IdP, so it passes the request to the appropriate service inside the network. The Unified Communications service trusts the IdP and the Expressway-E, so it provides the service to the Jabber client.

Figure 1: Single sign-on for on-premises UC services



Improved line-side capabilities

The line-side SIP capabilities of the Expressway have been extended to improve the support that MRA offers for endpoints registering to Unified CM. The improvements are:

Early Media support over MRA

Support for this feature means that endpoint users can hear media from the far end before the call is fully established, to indicate call progress (eg. busy tone) or play interactive voice responder messages.

The MRA deployment now supports passing through the 183 provisional response to enable early media, but the feature is dependent on endpoint support. Early media is supported in recent software for TC series endpoints but is not supported in Jabber 10.6.

Unsolicited NOTIFY pass-through

The unsolicited NOTIFY between Unified CM and the endpoints provides support for features like Message Waiting Indicator (MWI).

Multiple deployments for partitioning mobile and remote access to Unified Communications services

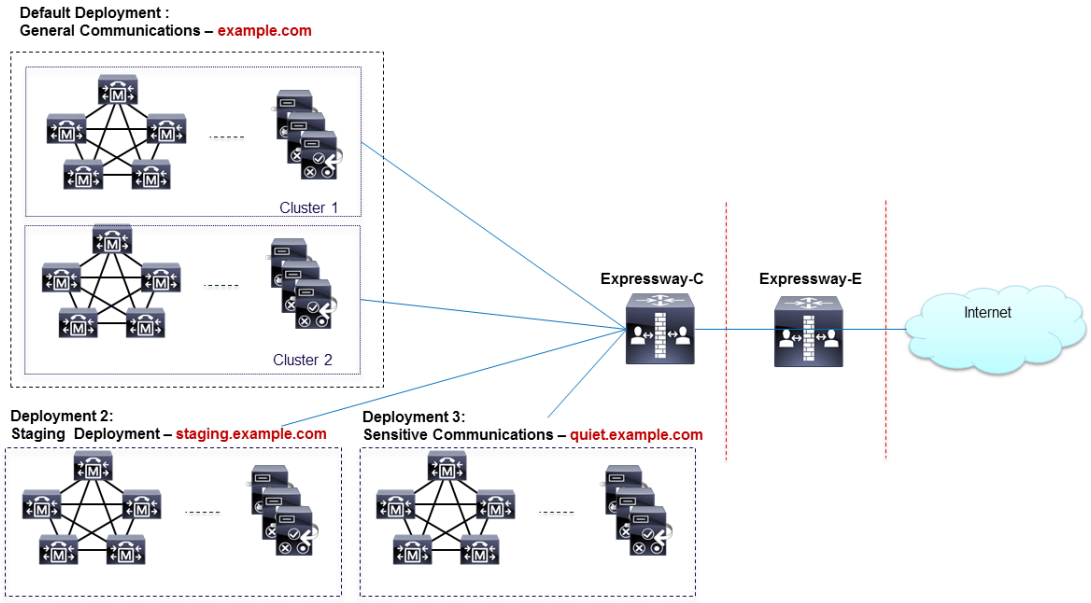
This release introduces the concept of "deployments" to the Expressway.

A deployment is an abstract boundary used to enclose a domain and one or more Unified Communications service providers, such as Unified CM, Cisco Unity Connection, and IM and Presence Service nodes.

The purpose of multiple deployments is to partition the Unified Communications services available to mobile and remote access (MRA) users. This enables different subsets of MRA users to access different sets of services over the same Expressway pair. We recommend that you do not exceed 10 deployments.

For example, consider an implementation of two sets of Unified Communications infrastructure to provide a live MRA environment and a staging environment, respectively. This implementation might also require an isolated environment for sensitive communications.

Figure 2: Multiple deployments to partition Unified Communications services accessed from outside the network



Serviceability improvements

Secure connection checker

This new utility enables you to test whether or not a secure connection can be made from the Expressway. It checks the validity of certificates presented by the transacting parties, looking for errors that would prevent the secure connection.

You simply enter an FQDN, hostname, or IP address to test the secure connection without otherwise affecting your configuration.

The feature can be used in the following circumstances:

- you are discovering Unified Communications servers / nodes while configuring Mobile and Remote Access, and wish to test whether TLS or HTTPS will be possible with the configured nodes
- you are configuring a Unified Communications traversal zone, or Secure Traversal zone, between the Expressway-C and the Expressway-E

Syslog publish filter

You can now filter the logs that Expressway sends to each remote syslog host by severity level.

For example, your syslog host is typically receiving syslog messages from multiple systems, so you may want to limit Expressway to sending only "Error" messages (and anything more severe) to this host. If you want to leave the host untouched while troubleshooting a Expressway problem, you could configure a second, temporary, host to receive "Debug" level (most verbose = messages of all severities). Then you could safely remove the configuration after resolving the issue, without risking your primary syslog host.

Call detail records (CDRs)

The Expressway now has the ability to record call connections and disconnections. There is a new service that allows short-lived CDRs to be read from the Expressway by an external system.

There is also an option to log the CDRs more permanently, in which case the CDRs are published as Informational messages to your syslog host. This option also keeps CDRs for a few days on the event log, but the local data could rotate quickly.

Note: CDR reporting is best effort and should not be relied upon for accurate billing purposes.

Media statistics

A media statistics logging service has been added to this release. When the service is active, up to 2GB of data is kept locally in a rotating log. The stats are also published as syslog messages for offline storage and analysis. For each call, the Expressway tracks statistics like packet counts, bitrates, and jitter.

Other changes

Enhancements and usability improvements

- You can add static IP routes via the web UI, where previously these could only be added by CLI . There is a new page **System > Network interfaces > Static routes** to provide this functionality.
- The Certificate Signing Request (CSR) generator now enables you to select the digest algorithm requested for your certificate. The options are SHA-1, SHA-256 (new default), SHA-384, and SHA-512. In Expressway versions prior to X8.5.1, the CSR page had no way to select the algorithm, and the CSR used SHA-1 by default.

Changed functionality

- When changing an administrator account password, the logged in administrator is now required to authorize the change by entering their own password.
- The IP and Ethernet configuration pages have a new menu location. Previously these were **System > IP** and **System > Ethernet**. These pages are now **System > Network interfaces > IP** and **System > Network interfaces > Ethernet**.
- The Expressway-C now defaults to SHA-256 for signing SSO requests it gives to clients, and you can change it to use SHA-1 if required. In version X8.5, when the SSO feature was previewed, the Expressway-C defaulted to SHA-1 and there was no way to select a different algorithm.

  Note: If you were using the SSO feature with X8.5, this change may cause it to stop working after upgrade to X8.5.1. You have two options to resolve this: leave the new default on the Expressway-C, and you may need to reconfigure the IdP to expect requests to be signed with SHA-256 (recommended for better security); the other option is to revert the Expressway-C's signing algorithm to SHA-1 for your IdP (go to **Configuration > Unified Communications > Identity Providers (IdP)**, locate your IdP row, then in **Actions** column click **Configure Digest**).

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 X8.5.3
- Issues resolved by X8.5.2
- Issues resolved by X8.5.1
- Issues resolved by X8.5

Notable open issues

The following issues are of particular concern for existing deployments at the time of this release.

CSCus47235 - CUCM 10.5.2 CN not duplicated into SAN for CSR

A behavior change in Unified Communications CSR 10.5.2 (Cisco Collaboration System Release) causes its *tomcat* certificates to fail validation on the Expressway. The impact on Expressway is that version 10.5.2 Unified Communications servers cannot successfully be discovered by Expressway-C when TLS verify mode is enabled. CSR 10.5.1 and earlier do not appear to be affected by this issue.

The following workarounds are available. Choose the one most suitable for your deployment:

- On Expressway, disable TLS verify mode when discovering Unified Communications nodes
  If you prefer not to disable TLS verify mode, you need to regenerate the tomcat certificate(s) for the nodes which fail validation. You could use the following approaches, referring to the Unified Communications security documentation for details:
- Use “Multi-server(SAN)” Distribution when generating Tomcat certificates on the Unified CM, IM & Presence Service or Unity Connection cluster.
  This will ensure the certificate presented by these servers to Expressway-C has a valid format, with the fully qualified domain name (FQDN) of each server in that cluster listed as a Subject Alternative Name.

- If you prefer single-server certificate distribution, modify the Common Name of the Tomcat certificate on each node so that the value differs from its fully qualified domain name (FQDN).
  This ensures that the FQDN of the server is correctly added as a Subject Alternate Name to that certificate.

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.
- 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 with X8.5.1, and we currently recommend that you do not exceed 10 domains.
- 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.
- NTLM authentication via the HTTP proxy.
- Maintenance mode; if an Expressway-C or 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

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

The DX Series must be running at least version 10.2.4, in which MRA support is described as "Unsupported Marketing Beta", to enable preliminary testing with MRA in your deployment. The Cisco IP Phone 78/8800 Series endpoints must be running version 10.3.1 or later if you want to use them for 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.

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.

Updating to X8.5.3

Upgrade instructions

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

If you are upgrading an Expressway that uses clustering, 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.

Upgrading 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, a traversal zone link to an Expressway system that is running the previous major release of Expressway software is supported. This means that you do not have to upgrade your Expressway-C and Expressway-E systems simultaneously.

Note that certain features introduced in the most recent software version (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. 0

DNS configuration on CUCM

- We strongly recommend that all CUCMs in clusters used for MRA have their records configured in DNS for both forward and reverse lookup.

Installing 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

Port Reference

The following tables list the IP ports and protocols used by Expressway for general services and functions.

For more information about ports, including those used for Unified Communications, device authentication, and the Microsoft Lync B2BUA see *Expressway IP Port Usage for Firewall Traversal*.

The tables show the generic defaults for each service, many of which are configurable. The actual services and ports used on your system will vary depending on its configuration, the option keys installed and features that have been enabled. A specific list of all the IP ports in use on a particular Expressway can be viewed via the port usage pages (**Maintenance > Tools > Port usage**).

When Advanced Networking is enabled, all ports configured on the Expressway, including those relating to firewall traversal, apply to both IP addresses; you cannot configure ports separately for each IP address.

Local Expressway Inbound/Outbound Ports

These are the IP ports on the Expressway used to receive (inbound) or send (outbound) communications with other systems.

Table 3: Local inbound/outbound ports

Service/ function	Purpose	Expressway port (default)	Direction	Configurable via
SSH	Encrypted command line administration.	22 TCP	inbound	not configurable
HTTP	Unencrypted web administration.	80 TCP	inbound	not configurable
NTP	System time updates (and important for H.235 security).	123 UDP	outbound	not configurable
SNMP	Network management.	161 UDP	inbound	not configurable
HTTPS	Encrypted web administration.	443 TCP	inbound	not configurable
Clustering	IPsec secure communication between cluster peers.	500 UDP	inbound outbound	not configurable

Table 3: Local inbound/outbound ports (continued)

Service/ function	Purpose	Expressway port (default)	Direction	Configurable via
Clustering	IPsec secure communication between cluster peers.	IP protocol 51 (IPSec AH)	inbound outbound	not configurable
Reserved		636	inbound	not configurable
DNS	Sending requests to DNS servers.	1024 - 65535 UDP	outbound	**System > DNS**
Gatekeeper discovery	Multicast gatekeeper discovery. The Expressway does not listen on this port when **H.323 Gatekeeper Auto discover mode** is set to *Off* (this disables IGMP messages).	1718 UDP	inbound	not configurable
H.323 registration Clustering	Listens for inbound H.323 UDP registrations. If the Expressway is part of a cluster, this port is used for inbound and outbound communication with peers, even if H.323 is disabled.	1719 UDP	inbound outbound	**Configuration > Protocols > H.323**
H.323 call signaling	Listens for H.323 call signaling.	1720 TCP	inbound	**Configuration > Protocols > H.323**
Assent call signaling	Assent signaling on the Expressway-E.	2776 TCP	inbound	**Configuration > Traversal > Ports**
H.460.18 call signaling	H.460.18 signaling on the Expressway-E.	2777 TCP	inbound	**Configuration > Traversal > Ports**
Traversal server media demultiplexing RTP/RTCP	Optionally used on the Expressway-E for demultiplexing RTP/RTCP media on Small/Medium systems only.	2776/2777 UDP	inbound outbound	**Configuration > Traversal > Ports**
TURN services	Listening port for TURN relay requests on Expressway-E.	3478 UDP *	inbound	**Configuration > Traversal > TURN**
System database	Encrypted administration connector to the Expressway system database.	4444 TCP	inbound	not configurable
SIP UDP	Listens for incoming SIP UDP calls.	5060 UDP	inbound outbound	**Configuration > Protocols > SIP**
SIP TCP	Listens for incoming SIP TCP calls.	5060 TCP	inbound	**Configuration > Protocols > SIP**
SIP TLS	Listens for incoming SIP TLS calls.	5061 TCP	inbound	**Configuration > Protocols > SIP**
B2BUA	Internal ports used by the B2BUA. Traffic sent to these ports is blocked automatically by the Expressway's non-configurable firewall rules.	5071, 5073 TCP	inbound	not configurable
Traversal server zone H.323 Port	Port on the Expressway-E used for H.323 firewall traversal from a particular traversal client.	6001 UDP, increments by 1 for each new zone	inbound	**Configuration > Zones**

Table 3: Local inbound/outbound ports (continued)

Service/ function	Purpose	Expressway port (default)	Direction	Configurable via
Traversal server zone SIP Port	Port on the Expressway-E used for SIP firewall traversal from a particular traversal client.	7001 TCP, increments by 1 for each new zone	inbound	**Configuration > Zones**
H.225 and H.245 call signaling port range	Range of ports used for call signaling after a call is established.	15000 - 19999 TCP	inbound outbound	**Configuration > Protocols > H.323**
SIP TCP outbound port range	Range of ports used by outbound TCP/TLS SIP connections to a remote SIP device.	25000 - 29999 TCP	outbound	**Configuration > Protocols > SIP**
Ephemeral ports	Various purposes.	30000 – 35999	outbound	**System > Administration**
Multiplexed traversal media (Assent, H.460.19 multiplexed media)	Ports used for multiplexed media in traversal calls. RTP and RTCP media demultiplexing ports are allocated from the start of the traversal media ports range. The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at **Configuration > Traversal Subzone**. In Large Expressway systems the first 12 ports in the range – 36000 to 36011 by default – are always reserved for multiplexed traffic. The Expressway-E listens on these ports. You cannot configure a distinct range of demultiplex listening ports on Large systems: they always use the first 6 pairs in the media port range. On Small/Medium systems you can explicitly specify which 2 ports listen for multiplexed RTP/RTCP traffic, on the Expressway-E (**Configuration > Traversal > Ports**). If you choose not to configure a particular pair of ports (**Use configured demultiplexing ports** = *No*), then the Expressway-E will listen on the first pair of ports in the media traversal port range (36000 and 36001 by default).	36000 – 36001 UDP (Small / Medium systems) or 36000 – 36011 UDP (Large systems)	inbound outbound	**Configuration > Traversal Subzone**

Table 3: Local inbound/outbound ports (continued)

Service/ function	Purpose	Expressway port (default)	Direction	Configurable via
Non-multiplexed media port range	Range of ports used for non-multiplexed media. Ports are allocated from this range in pairs, with the first port number of each pair being an even number. The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at **Configuration > Traversal Subzone**. In Large Expressway systems the first 12 ports in the range – 36000 to 36011 by default – are always reserved for multiplexed traffic. The Expressway-E listens on these ports. You cannot configure a distinct range of demultiplex listening ports on Large systems: they always use the first 6 pairs in the media port range. On Small/Medium systems you can explicitly specify which 2 ports listen for multiplexed RTP/RTCP traffic, on the Expressway-E (**Configuration > Traversal > Ports**). If you choose not to configure a particular pair of ports (**Use configured demultiplexing ports** = *No*), then the Expressway-E will listen on the first pair of ports in the media traversal port range (36000 and 36001 by default).	36002 – 59999 UDP (Small / Medium systems) or 36012 – 59999 UDP (Large systems)	inbound outbound	**Configuration > Traversal Subzone**
TURN relay media port range	Range of ports available for TURN media relay.	24000 – 29999 UDP	inbound outbound	**Configuration > Traversal > TURN**

Note that two services or functions cannot share the same port and protocol; an alarm will be raised if you attempt to change an existing port or range and it conflicts with another service.

* On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483.

Remote Listening Ports

These tables show the default listening (destination) ports on the remote systems with which the Expressway communicates.

The source port on the Expressway for all of these communications is assigned from the Expressway's ephemeral range.

Table 4: Remote listening ports

Service/ function	Purpose	Destination port (default)	Configurable via
DNS	Requests to a DNS server.	53 UDP	**System > DNS**
External manager	Outbound connection to an external manager, for example Cisco TMS.	80 TCP	**System > External manager**
NTP	System time updates.	123 UDP	**System > Time**
LDAP account authentication	LDAP queries for login account authentication.	389 / 636 TCP	**Users > LDAP configuration**
Incident reporting	Sending application failure details.	443 TCP	**Maintenance > Diagnostics > Incident reporting > Configuration**
Remote logging	Sending messages to the remote syslog server.	514 UDP 6514 TCP	**Maintenance > Logging**
Neighbors (H.323)	H.323 connection to a neighbor zone.	1710 UDP	**Configuration > Zones**
Neighbors (SIP)	SIP connection to a neighbor zone.	5060 / 5061 TCP	**Configuration > Zones**
Traversal zone (H.323)	H.323 connection to a traversal server.	6001 UDP	**Configuration > Zones**
Traversal zone (SIP)	SIP connection to a traversal server.	7001 TCP	**Configuration > Zones**
TURN media relay	Range of ports available for TURN media relay.	24000 – 29999 UDP	**Configuration > Traversal > TURN** (on Expressway-E)

Additional information

Software filenames

The Expressway software filenames are in the format s42700x<y_y_y> where x<y_y_y> represents the software version (for example x8_5_0 represents X8.5).

Secure communications

As of version X8.1, new installations of Expressway ship with a default server certificate and trusted CA list.

For secure communications (HTTPS and SIP/TLS), we strongly recommend that you replace the Expressway default certificate with a certificate generated by a trusted certificate authority. See *Expressway Certificate Creation and Use Deployment Guide* for more information about to how to generate certificate signing requests and install certificates.

When you are upgrading your software, the upgrade does not generally affect your existing server certificate or trust store: these are retained after upgrade. However, we may occasionally recommend applying a new certificate or modifying your trusted CA list to improve security on your Expressway.

Restricting access to ISDN gateways (toll-fraud prevention)

Expressway-E users should take appropriate action to restrict unauthorized access to ISDN gateway resources. See *Expressway Basic Configuration Deployment Guide* for information about how to do this.

Supported RFCs

The following RFCs are supported within the Expressway X8.5.3 release:

Table 5: Supported RFCs

RFC	Description
791	Internet Protocol
1213	Management Information Base for Network Management of TCP/IP-based internets
1305	Network Time Protocol (Version 3) Specification, Implementation and Analysis
2327	SDP: Session Description Protocol
2460	Internet Protocol, Version 6 (IPv6) Specification (partial, static global addresses only)
2464	Transmission of IPv6 Packets over Ethernet Networks
2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
2782	A DNS RR for specifying the location of services (DNS SRV)
2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
2915	The Naming Authority Pointer (NAPTR) DNS Resource Record
2976	SIP INFO method
3164	The BSD syslog Protocol
3261	Session Initiation Protocol
3263	Locating SIP Servers
3264	An Offer/Answer Model with the Session Description Protocol (SDP)
3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
3326	The Reason Header Field for the Session initiation Protocol (SIP)
3265	Session Initiation Protocol (SIP) – Specific Event Notification
3327	Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
3489	STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
3515	The Session Initiation Protocol (SIP) Refer Method
3550	RTP: A Transport Protocol for Real-Time Applications
3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
3596	DNS Extensions to Support IP Version 6
3761	The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)
3880	Call Processing Language (CPL): A Language for User Control of Internet Telephony Services

Table 5: Supported RFCs (continued)

RFC	Description
3891	Replaces header
3892	Referred-by header
3903	Session Initiation Protocol (SIP) Extension for Event State Publication
3944	H.350 Directory Services
3986	Uniform Resource Identifier (URI): Generic Syntax
4028	Session Timers in the Session Initiation Protocol
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers
4291	IP Version 6 Addressing Architecture
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
4480	RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)
4787	Network Address Translation (NAT) Behavioral Requirements for Unicast UDP
4861	Neighbor Discovery for IP version 6 (IPv6)
5095	Deprecation of Type 0 Routing Headers in IPv6
5104	Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF): Temporary Maximum Media Stream Bit Rate Request (TMMBR)
5245	Interactive Connectivity Establishment (ICE)
5389	Session Traversal Utilities for NAT (STUN)
5424	The Syslog Protocol
5626	Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
5627	Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP). Note that this RFC is only partially supported: Public GRUU is supported; Temporary GRUU is not supported.
5766	Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
5806	Diversion Indication in SIP
6156	Traversal Using Relays around NAT (TURN) Extension for IPv6

Virtual machine

Before you can order your release key and any option keys, you must first download and install the .ova file in order to obtain your hardware serial number. The Expressway provides limited capacity until a valid release key is entered.

Note that the .ova file is only required for the initial install of the Expressway software on VMware. Subsequent upgrades should use the .tar.gz file.

See *Expressway on Virtual Machine Installation Guide* for full installation instructions.

Third-party software

This product includes copyrighted software licensed from others. A list of the licenses and notices for open source software used in this product can be found at: http://www.cisco.com/en/US/products/ps11337/products_licensing_information_listing.html.

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.

Technical support

If you cannot find the answer you need in the documentation, check the website at www.cisco.com/cisco/web/support/index.html where you will be able to:

- Make sure that you are running the most up-to-date software.
- Get help from the Cisco Technical Support team.

Make sure you have the following information ready before raising a case:

- Identifying information for your product, such as model number, firmware version, and software version (where applicable).
- Your contact email address or telephone number.
- A full description of the problem.

To view a list of Cisco TelePresence products that are no longer being sold and might not be supported, visit: www.cisco.com/en/US/products/prod_end_of_life.html and scroll down to the TelePresence section.

Document revision history

Date	Description
June 2015	X8.5.3 Maintenance release.
April 2015	X8.5.2 Maintenance release.
April 2015	X8.5.1 Release note re-issued with Multiple Presence Domains (preview) limited to 10 domains.
February 2015	X8.5.1 Release note re-issued with multiple presence domains feature preview, qualified Jabber file transfer limitation, and feature support history table.
January 2015	X8.5.1 Maintenance release.
December 2014	Re-issued with MRA endpoint clarification.
December 2014	X8.5 release.
October 2014	X8.2.2 maintenance release.
August 2014	Note about NAT reflection added to X8.2 changed behavior, republished for X8.2.1.
August 2014	Note about NAT reflection added to X8.2 changed behavior, republished for X8.2.
July 2014	X8.2.1 maintenance release.
June 2014	X8.2 initial release.
July 2014	X8.1.1 release notes republished to remove limitation about Webex-enabled TelePresence.
April 2014	X8.1.1 maintenance release, including mobile and remote access features.
December 2013	X8.1 initial release. [Revised April 2014 to include issue CSCum90139.]