Cisco Expressway X8.7.2

Release Note
March 2016

Preface

Change History

Table 1 Release Note Change History

Date	Change	Reason
March 2016	Updated resolved and open issues links. Listed minor changes in X8.7.2.	X8.7.2 maintenance release
February 2016	Updated resolved and open issues links. Listed minor changes in X8.7.1. Added Hybrid Services upgrade prerequisite.	X8.7.1 maintenance release
November 2015	Release notes for new version of Expressway.	X8.7 feature 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

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 Lync Deployment Guide* in Cisco Expressway Series Configuration Guides

Changes in X8.7.2

X8.7.2 is a maintenance release. There are no new features, but the lists of Open and Resolved Issues, page 6, have been updated.

- CiscoSSL has been upgraded to version 5.4.3 in this version of Expressway. This version of Cisco SSL rejects keys with fewer than 1024 bits when doing Diffie-Hellman (DH) key exchange.

  Note: This Expressway upgrade prevents SSL interoperability with versions 9.x and earlier of Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service, because those products generate 768 bit keys for D-H key exchange.

  Suggested workaround: Upgrade Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service to the latest version of 10.x or 11.x.

Changes in X8.7.1

X8.7.1 is a maintenance release. There are no new features, but the lists of Open and Resolved Issues, page 6, have been updated.

- Two parameters have been added to the DNS zone configuration. These parameters enable a manual override of the DNS request, to enable routing outbound calls to the Cisco Collaboration Cloud without modifying the SIP URI. The parameters are **Modify DNS request** (*On* or *Off*) and **Domain to search for** (accepts an FQDN).

  This option is primarily intended for use with Cisco Spark Call Service. See www.cisco.com/go/hybrid-services.
- The 2 * 2.4 GHz CPU reservation requirement of the Medium virtual Expressway has been relaxed to allow for slight variance in host clock speeds.

  These natural variations were preventing some correctly specified UCS hardware configurations, including some BE6000 options, from meeting the CPU requirement.

  See *Cisco Expressway Virtual Machine Installation Guide* on the Expressway installation guides page.
- The IP interface selection options have changed. On **System > Network interfaces > IP**, the **IP protocol** switch now has the options *IPv4 only*, *IPv6 only*, or *Both*.
- CiscoSSL has been upgraded to version 5.4.2 (based on OpenSSL v1.0.2e). This version does not allow TLS connections to use the RC4 cipher.

New Features in X8.7

Table 3 Feature History by Release Number

Feature / change	X8.7
Dial via Office-Reverse (DVO-R)	Supported
Lync Screen Sharing Through a Gateway Cluster	Supported
Mobile and Remote Access with Cisco IP Phone 78/8800 Series	Supported
Hybrid Services and Expressway/VCS Rebranding	Supported
Hosting on VMWare vSphere® 6.0	Supported
Keyword Filter for Syslog Output	Supported
Changes and Minor Enhancements	Supported

Dial via Office-Reverse through MRA

Your mobile workers need the same high quality, security and reliability that they experience when placing calls in the office. You can assure them of just that when you enable the Dial via Office-Reverse (DVO-R) feature and they are using Cisco Jabber on a dual-mode mobile device. DVO-R routes Cisco Jabber calls through the enterprise automatically.

DVO-R handles call signaling and voice media separately. All call signaling, including the signaling for Mobile and Remote Access on Expressway, traverses the IP connection between the client and Cisco Unified Communications Manager. Voice media traverses the cellular interface and hairpins at the enterprise Public Switched Telephone Network (PSTN) gateway.

Moving audio to the cellular interface ensures high-quality calls and securely maintained audio even when the IP connection is lost.

You can configure DVO-R so that, when a user makes a call, the return call from Cisco Unified Communications Manager goes to either:

- The user's Mobile Identity (mobile number).
- An Alternate Number for the user (such as a hotel room).

This feature is dependent on the following versions of related systems:

- Cisco Unified Communications Manager 11.0(1) or later
- Cisco Jabber 11.1 or later

You can read more about how this feature works in the *Mobile and Remote Access through Expressway Deployment Guide* on the Expressway Configuration Guides page.

Lync Screen Sharing Through a Gateway Cluster

Transcoding of Lync screen sharing was introduced in X8.6.

X8.7 extends this feature to work on a cluster of Gateway Expressway peers, so that a greater number of screen sharing sessions can be simultaneously transcoded.

You must configure the Lync B2BUA and the related transcoding parameters on the master peer. The number of transcoding sessions you enter is the per peer number.

The transcoding capacity of the cluster is approximately the number of sessions you choose multiplied by the number of peers, up to a maximum multiple of 4x.

For example, consider a cluster of four large VMs. If you set **Maximum RDP transcode sessions** to *20*, then the cluster would provide up to 80 simultaneous screen shares.

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.

Mobile and Remote Access with Cisco IP Phone 78/8800 Series

Mobile and Remote Access is now officially supported with the Cisco IP Phone 78/8800 Series, when the phones are running firmware version 11.0(1) or later. We recommend Expressway X8.7 or later for use with these phones.

- Cisco IP Phone 8800 Series
- Cisco IP Phone 7800 Series

MRA is officially supported with the Cisco DX Series endpoints running firmware version 10.2.4(99) or later. This support was announced with Expressway version X8.6.

- Cisco DX650
- Cisco DX80
- Cisco DX70

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.

Hybrid Services and Expressway/VCS Rebranding

We have changed some terminology in this release:

- **Expressway/VCS base**

  In previous versions of the Cisco Expressway Series and the Cisco TelePresence Video Communication Server, the software was always branded as "VCS Control" before you activated it with a release key.

  In X8.7, the product is now called "Expressway/VCS base" when it is in this pre-activation state, which shows that it can be activated as an Expressway or as a VCS.

  These changes prepare us for a future release that will change the user experience of defining the purpose of your Expressway.

- **Hybrid Services**

  Version X8.6.1 included support for a feature called "Cloud Extensions". That feature has been renamed to "Hybrid Services" in the UI, documentation, and Cloud Collaboration Management.

  Hybrid Services is a group name for a family of user services that are delivered in part by the Cisco Collaboration Cloud and in part by your on-premises equipment.

  The Expressway/VCS base does not need a release key to register for Hybrid Services. After you register the Expressway/VCS base, it will be branded "Cisco Expressway base". You don't need to apply a release key for subsequent upgrades.

Note: For these reasons, we are requiring new Hybrid Services customers to use version X8.7. If you are using X8.6.1 for Hybrid Services, we strongly recommend upgrading to X8.7.

Hosting on VMWare vSphere 6.0

Expressway virtual machines can now run on VMware vSphere® version 6.0. Please be aware that we have noticed a known issue in ESXi 6.0 during our testing. We recommend that you read http://kb.vmware.com/kb/2124669 before you upgrade.

You can install new Expressway OVAs on the ESXi 6.0 host, or you can migrate existing VMs. If you migrate a virtual Expressway to a different host, you must shut it down before you move it.

See the *Cisco Expressway on Virtual Machine Installation Guide* on the Expressway Install and Upgrade Guides page.

Note: The virtual Expressway now has virtual hardware version 8. This means that new installations of virtual Expressway require ESXi 5.0 or later, and will not run on ESX/ESXi 4.x or earlier.

Keyword Filter for Syslog Output

You can now use keywords to filter the logs that Expressway sends to each remote syslog host. You can enter comma delimited words or phrases, and the syslog daemon will only forward log messages that match at least one of those keywords.

The keyword filter gives you more control over the types of messages that are published. You may only be interested in some types of messages, or you may not be allowed to send potentially sensitive information over the channel to the syslog server.

The user interface has also been improved as part of this change. In addition to the new keyword filter field, we've added more granular control over the message format and transport connection. Previously, these options were grouped into a "Mode" field and you could not configure them unless you chose the "Custom" mode.

Changes and Minor Enhancements

- Multistream support is disabled in this release, pending a complete implementation in a future release.
- A new CLI command allows you to set the cipher suites used when the Expressway authenticates with the AD domain for LDAP queries. The command is `xconfiguration Authentication ADS CipherSuite`.
- A Hybrid Services menu item has been added to the Expressway-E, to support Expressway-based hybrid services that are currently in development. The new menu item (**Applications > Hybrid Services > Certificate management**) has no explicit purpose for X8.7.
- A new system metric has been added to monitor each CPU core independently.
- New parameters have been added to the .ova file so you can configure the VM's network properties when deploying through vCenter.

  See *Cisco Expressway Virtual Machine Installation Guide* on the Expressway installation guides page.

  There is a delay when you deploy virtual machines with pre-configured network parameters. The deployment will take a few minutes longer than deploying the VM without pre-configured network parameters.
- The Expressway deployment guide now warns against choosing a single NIC, static NAT deployment of the Expressway-E. The preferred option for deploying the Expressway-E in the DMZ is to use both NICs.

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

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 modified (recent first)
- Issues resolved by X8.7.2
- Issues resolved by X8.7.1
- Issues resolved by X8.7

Notable Issues in this Version

CSCuy59366: Upgrading Expressway to X8.7.2 breaks SSL Handshake with CUCM or IM&P 9.x

An upgrade of CiscoSSL in this version of Expressway prevents it from accepting weak DH keys. If you have not yet applied this security improvement to your Cisco Unified Communications Manager or Cisco Unified Communications Manager IM and Presence Service infrastructure, they may not be able to communicate securely with Expressway. This could prevent your MRA deployment from working as expected.

We strongly recommend that you upgrade Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service to the latest version of 10.x or 11.x .

CSCuw95309: DTMF mid-call features not supported for Mobility-enabled Users

(This issue is present in Cisco Unified Communications Manager version 11.0)

For end users who have mobility enabled, DTMF-based mid-call features (for example, *81 - Hold, *83 - Resume) are not supported, regardless of the DTMF Signaling Method setting for the SIP trunk. This issue is present for all SIP trunks due to issues with SIP signaling and MTP allocation. There is no workaround for this issue.

Note: DTMF for User Controlled Voicemail avoidance and for navigating IVRs at the far-end are both supported.

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

This issue in X8.6 and X8.7 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 yet.

The affected deployment is documented in *Appendix 1: Federation*, of the X8.5 version of *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 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).

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.

Upgrading to X8.7.2

Prerequisites and Software Dependencies

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.

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 Lync B2BUA to route SIP calls between the Expressway and a

Microsoft Lync Server. See *VCS and Microsoft Lync 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 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.

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

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