Cisco Expressway X8.2.1

Software Release Notes
August 2014

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

Further Expressway deployment guides covering 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 are available on cisco.com.

Changes in X8.2.1

Expressway version X8.2.1 is a maintenance release and does not introduce any new features or major changes to behavior. See Resolved issues [p.4] and Open issues [p.8] for changes since the previous feature release.

New features in X8.2

Unified Communications: Jabber Guest

Cisco Jabber Guest is a consumer to business (C2B) solution that extends the reach of Cisco's enterprise telephony to people outside of a corporate firewall who do not have phones registered with Cisco Unified Communications Manager.

External XMPP federation

External XMPP federation enables users registered to Unified CM IM & Presence to communicate via the Expressway-E with users from a different XMPP deployment.

TURN media over TCP

The Expressway-E TURN server supports TURN media over TCP.

This allows clients to use TURN services in environments where UDP connections are not supported or blocked. Configuration of the supported protocols is available only through the CLI command **`xConfiguration Traversal Server TURN ProtocolMode`**.

New 'Unified Communications traversal' zone type

To simplify the configuration of secure traversal client and traversal server zones that are to be used for Unified Communications, you must now use the new zone type of *Unified Communications traversal* when configuring zones via the web interface.

This automatically configures an appropriate traversal zone (a traversal client zone when selected on a Expressway-C, or a traversal server zone when selected on an Expressway-E) that uses SIP TLS with **TLS verify mode** set to *On*, and **Media encryption mode** set to *Force encrypted*.

This replaces the previous **Unified Communications services** setting that was available when configuring traversal client and traversal server zones. Existing zones configured in previous software versions for **Unified Communications services** are automatically converted to use the new *Unified Communications traversal* zone type.

Note that this zone type applies to the web interface only, the underlying CLI configuration settings have not changed.

Support for `X-cisco-srtp-fallback`

Support has been added for the **`X-cisco-srtp-fallback`** package, allowing the Expressway's B2BUA to use Cisco Unified Communications Manager-style best effort media encryption for the automatically generated TLS neighbor zones.

RTP and RTCP media demultiplexing ports

In Small/Medium systems, 1 pair of RTP and RTCP media demultiplexing ports are used. These can now either be explicitly specified (**Configuration > Traversal > Ports**) or they can be allocated from the start of the general range of traversal media ports. In previous X8 releases they were always allocated from the start of the traversal media ports range.

In Large systems, 6 pairs of RTP and RTCP media demultiplexing ports are used. These are still always allocated from the start of the traversal media ports range.

After upgrading to X8.2, all existing traversal media port configurations / firewall requirements are maintained.

Diagnostic logging

The diagnostic logging feature has been extended to include:

- an xconfig file
- an xstatus file
- enabling the tcpdump (if requested) cluster-wide
- consolidating all of the files into a single downloadable diagnostic log archive (per peer)
- an indication on the web administration page of which user / IP address initiated the logging

The xconfig and xstatus files are taken at the start of the logging process.

SIP REFER support

The Expressway B2BUA has SIP REFER message support. A **SIP REFER mode** advanced zone configuration parameter has been introduced.

By default it will forward REFER messages, but it can be configured to terminate REFER messages and use the B2BUA to perform the transfer (typically to a bridge) on behalf of the far endpoint.

Other enhancements and usability improvements

- The **HTTP server allow list** page (used for mobile and remote access clients to access additional web services inside the enterprise) now displays any automatically configured entries.
- You can configure the timeout period for TLS socket handshake (**Configuration > Protocols > SIP**).
- The TURN relay status page (**Status > TURN relay usage**) now provides a summary list of all the clients that are connected to the TURN server. From there you can select a specific client to see all of the relays and ports that it is using.
- Ability to copy search rules. You can use the **Clone** action on the search rules listing page (**Configuration > Dial plan > Search rules**) to copy and then edit an existing search rule.
- The DNS lookup tool allows you to select which DNS servers (from the configured set of default DNS servers) to use for the lookup.
- The automated protection service now supports IPv6 addresses.

Changed functionality

Access to the systemunit.xml file is now protected. Only authenticated Expressway administrator accounts can access the file. This may affect the discovery of Expressway by Cisco TMS.

Call status and call history now indicates components routed through the B2BUA for encryption or ICE support with a component type of 'B2BUA' (formerly 'Encryption B2BUA').

Note: The combination of having static NAT mode on and having the B2BUA engaged to do media encryption/decryption can cause the firewall outside the Expressway-E to mistrust packets originating from the Expressway-E. You can work around this by configuring the firewall to allow NAT reflection. If your firewall cannot allow this, you must configure the traversal path such that the B2BUA on the Expressway-E is not engaged.

Changes in X8.1.1

Unified Communications: mobile and remote access

Cisco Unified Communications mobile and remote access is a core part of the Cisco Collaboration Edge Architecture. It allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging and presence services provided by Cisco Unified Communications Manager (Unified CM) when the endpoint is not within the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations.

For more information including configuration recommendations and troubleshooting details, see *Unified Communications: Mobile and Remote Access via Expressway Deployment Guide*.

Support to modify Maximum transmission unit (MTU) size

You can configure the maximum transmission unit (MTU) for each network interface on the **System > IP** page.

Diagnostic logging

The tcpdump facility has been removed from the **Diagnostic logging** tool.

Jabber Guest

Jabber Guest support has been removed (it was previously provided as a feature preview in X8.1). It will be reintroduced in a future release of Expressway software.

Resolved issues

Resolved in X8.2.1

Table 1: Issues resolved in X8.2.1

Identifier	Description
CSCup29435	**Symptoms:** Expressway reports an application error, and the process restarts automatically. An alarm is raised reporting that an unexpected software error was detected. **Conditions:** Rare, under investigation. **Workaround:** None, the app process will automatically be restarted.
CSCup46518	**Symptoms:** A remote endpoint registered to UCM via Mobile and Remote Access may fail to register if an Expressway-C in the cluster is out of service (shutdown, or otherwise unreachable). **Conditions:** One Expressway-C in the cluster is out of service, and the route created by the endpoint happens to use that server. **Workaround:** Restart the endpoint, which will cause it to obtain updated information about the available Expressway-C servers, which will not include the one that is out of service.
CSCup01126	**Symptoms:**Expressway restart due to internal application crash with "An unexpected software error was detected in app[15225]: SIGSEGV (address not mapped to object) @0x0000000000000000" alarm message.

Table 1: Issues resolved in X8.2.1 (continued)

Identifier	Description
CSCup29484	**Symptoms:** For re-INVITE process, Expressway B2BUA reuse Max-Forwards value that it stored at the call establishment, therefore may see Max-Forward parameter reduced to an unexpected level. **Conditions:** Re-INVITE and call go through Expressway B2BUA application. **Workaround:** None.
CSCup75947	**Symptoms:** On Expressway running 8.2 in a WebEx Enabled TelePresence environment, B2BUA fails to process and forward on the ACK sent by an MCU in response to a WebEx 200OK. The results in a SIP negotiation failure where the connection ultimately times out on the WebEx side and WebEx sends a BYE. **Conditions:** WebEx Enabled TelePresence where MCU dials out to WebEx. **Workaround:** In WebEx Enabled TelePresence deployments you should: ■ Reconfigure the Expressway-E to not use static NAT, or ■ Recommended configuration for Expressway-C with Expressway-E deployments is to configure the media encryption policy setting on the traversal client zone on Expressway-C, the traversal server zone on Expressway-E, and every zone on Expressway-E, and to only use static NAT on the Expressway-E. With this configuration the encryption B2BUA will only be enabled on the Expressway-C.
CSCup25151	**Symptom:** The following Cisco products: Cisco Expressway include a version of openssl that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2010-5298 - SSL_MODE_RELEASE_BUFFERS session injection or denial of service CVE-2014-0076 - Fix for the attack described in the paper "Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack" CVE-2014-0195 - DTLS invalid fragment vulnerability CVE-2014-0198 - SSL_MODE_RELEASE_BUFFERS NULL pointer dereference CVE-2014-0221 - DTLS recursion flaw CVE-2014-0224 - SSL/TLS MITM vulnerability CVE-2014-3470 - Anonymous ECDH denial of service This bug has been opened to address the potential impact on this product. **Conditions:** Devices running an affected version of software. **Workaround:** None. **Further Problem Description:** Fix will be available with X8.2.1. **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 10/9.5: https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:U/RC:C The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product.
CSCup50593	**Symptoms:** Expressway reports an application error, an alarm is raised reporting that an unexpected software error was detected (getCallSerialNumbers Line: 41). **Conditions:** The Expressway application builds SIP message strings from null pointer. **Workaround:** None.

Resolved in X8.2

Table 2: Issues resolved in X8.2

Identifier	Description
CSCum90139	**Symptoms**: Expressway X8.1 uses the Ethernet 2 IP address for the media part in SDP rather than the configured Static NAT IP address. This results in calls failing on the media part. **Conditions**: Running Expressway X8.1 with Static NAT and encryption B2BUA enabled (a media encryption policy other than Auto). **Workaround**: Recommended configuration for Expressway-C with Expressway-E deployments is to configure the same media encryption policy setting on the traversal client zone on Expressway-C, the traversal server zone on Expressway-E, and every zone on Expressway-E, and to only use static NAT on the Expressway-E. With this configuration the encryption B2BUA will only be enabled on the Expressway-C.

Resolved in X8.1.1

Table 3: Issues resolved in X8.1.1

Identifier	Description
CSCuo16472	**Symptom**: Expressway includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160. This bug has been opened to address the potential impact on this product. **Conditions**: Device with default configuration, running one of the following versions: X7.2 X7.2.1 X7.2.2 X7.2.3 RC2 X8.1. Version X7.1 and all prior versions are NOT vulnerable to this issue. **Workaround**: Not currently available. **Further Problem Description**: Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html **PSIRT Evaluation**: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.4: https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector =AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:OF/RC:C The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product. CVE-2014-0160 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Table 3: Issues resolved in X8.1.1 (continued)

Identifier	Description
CSCul12855	**Symptom**: Expressway systems enable a number of SSL ciphers by default. The default configuration in X8.1 is: ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4-SHA:HIGH:!ADH:!aNULL. This means that suites that may be affected by issues such as the RC4 weakness (CVE-2013-2566), BEAST (CVE-2011-3389), or Lucky 13 (CVE-2013-0169). By default no GUI method is provided to allow the customization of these values to a customer's security policy. **Conditions**: Expressway systems running a version of Expressway software prior to X8.1.1. **Workaround**: Customers may modify the ssl.conf file of the device and modify the cipher list to that required to meet their security policy. Customers are advised to consult with Cisco TAC or their authorized support provider for assistance with this modification. **Further Problem Description**: This defect is opened as an enhancement to the current operation of the Expressway. Future versions of the product will be modified to remove all known affected ciphers. This may also include a migration to TSL 1.2, and the ability to modify the ciphers in use from the GUI. **PSIRT Evaluation**: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 2.6/2.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1 &version=2&vector=AV:N/AC:H/Au:N/C:N/I:P/A:N/E:U/RL:W/RC:C CVE-2013-2566, CVE-2011-3389 and CVE-2013-0169 have been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
CSCul83652	**Symptoms**: All endpoint registrations are lost. A kernel panic is logged in the kernel log. The system continues to run, but network traffic is affected for the Expressway application. The only way to recover is to reboot the system. **Conditions**: Occurs only on Expressway X8.1. On systems where it does occur, it happens very infrequently. Has only been seen on systems behind a GRE tunnel. **Workaround**: Use a cluster for registration resiliency.
CSCul93670	**Symptom**: Unified Communications services fail to start after a Expressway restart. Mobile and remote systems will not be able to register to Unified CM or make calls. This is an occasional issue. **Conditions**: Restart (or reboot) a Expressway that has Mobile and remote access enabled. **Workaround**: After a restart or reboot, wait 5 minutes and then go to **Status > Unified Communications** in the web interface. If any of the services are in an error state, go to **Configuration > Unified Communications > Configuration** and disable and then re-enable the **Mobile and remote access feature**.
CSCum48012	**Symptom**: Memory leak in the application which causes swap to be used. **Conditions**: Running Expressway X8.1. **Workaround**: Monitor memory usage and when usage of swap becomes high, reboot the Expressway.

Open issues

The following issues apply to this version of Cisco Expressway.

Table 4: Open issues

Identifier	Description
CSCuo82382	**Symptoms**: Encrypted H.323 call in ad-hoc conference, get black screen after session refresh (with default configuration, after approximately 15 minutes of conference call). **Conditions**: In some instances, under investigation, ad-hoc conference call with encrypted H.323 call. **Workarounds**: Perform a Hold / Resume. Alternatively, use SIP as call protocol instead of H.323. Alternatively, disable encryption call.
CSCuo75250	**Symptoms**: Expressway restart due to internal application crash with “An unexpected software error was detected in app[13484]: SIGSEGV (address not mapped to object) @0x0000000000000008” alarm message. **Conditions**: Rare, possibly related to interworking, under investigation. **Workaround**: None, the app process will automatically be restarted.
CSCum47768	**Symptoms:** Media stream fails to work. (e.g. slide content) **Conditions:** This occurs if re-invite updates the SDP, adding media lines for example, and a SIP ACK/200 message for a previous re-invite sequence is lost in transit. **Workaround:** None.
CSCup09760	**Symptoms:** Alarm raised in system, "Application failed - An unexpected software error was detected in app[13650]: SIGSEGV (Sent by the kernel) @0x0000000000000000" **Conditions:** Unknown. **Workaround:** None required, the service automatically recovers within a few seconds.
CSCup12382	**Symptoms:** Interworking call where received profile-level-id and max-br value defined in the SDP are not being mapped to the correct value in the outgoing capset. **Conditions:** SIP to H.323 interworking.
CSCup73726	**Symptoms:** An alarm is raised reporting that an unexpected software error was detected (parseViaHeader Line: 343). **Conditions:** There is an invalid SIP version of SIP/2./UDP in the Via header.
CSCup83131	**Symptoms:** An alarm is raised on the Expressway reporting a crash that: An unexpected software error was detected in managementframework.pyc: Detail="Stopping periodic timer callback." Not completed within="60.000000" **Conditions:** High resource use.
CSCup89654	**Symptoms:** Video call through Expressway experiences one-way audio/video, resulting as well in DTMF not being passed which in turn can fail IVR systems. **Conditions:** Expressway X8.1.1 with following topology: CUCM -- SIP -- Expressway -- H.323 -- H.323 MCU with IVR

Limitations

Unsupported features (general)

- DTLS is not supported through the Expressway-C/Expressway-E; attempts to make secure calls will fail
- SIP Early Media
- SIP KeyPad Markup Language (KPML)
- 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 Jabber features when using mobile and remote access

- Directory access mechanisms other than UDS
- Certificate provisioning to remote endpoints e.g. CAPF
- File transfer (except when operating in hybrid Webex mode)
- Deskphone control (QBE/CTI)
- Additional mobility features including DVO-R, GSM handoff and session persistency
- 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 features and limitations when using mobile and remote access

- 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; each Expressway deployment supports only one IM&P domain (even though IM & Presence 10.0 or later supports multiple IM&P 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

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 X8.2.1

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.
- Early field trial customers who have configured a previous X8.1 or X8.1.1 system for external XMPP federation must reconfigure their XMPP federation settings after upgrading to X8.2.

If you are upgrading an Expressway that uses clustering, you must follow the directions in *Expressway Cluster Creation and Maintenance Deployment Guide* for X8.2.1.

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.

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 5: 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
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

Table 5: Local inbound/outbound ports (continued)

Service/ function	Purpose	Expressway port (default)	Direction	Configurable via
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**
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**

Table 5: Local inbound/outbound ports (continued)

Service/ function	Purpose	Expressway port (default)	Direction	Configurable via
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 port range is 36000 to 59999. In Large systems the first 12 ports in the range – 36000 to 36011 – are used for multiplexed traffic only. In Small/Medium systems you can either explicitly specify the 2 ports to use for multiplexed traffic or use the first 2 ports from the media port range.	36000 – 36001 UDP (Small / Medium systems) or 36000 – 36011 UDP (Large systems)	inbound outbound	**Configuration > Traversal Subzone**
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 port range is 36000 to 59999. In Large systems the first 12 ports in the range – 36000 to 36011 – are used for multiplexed traffic only. In Small/Medium systems you can either explicitly specify the 2 ports to use for multiplexed traffic or use the first 2 ports from the media port range.	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 6: 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_1_0 represents X8.1).

Secure communications

For secure communications (HTTPS and SIP/TLS) we 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.

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 X8.2.1 release:

Table 7: 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
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
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

Table 7: Supported RFCs (continued)

RFC	Description
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	Revision	Description
August 2014	07	Note about NAT reflection added to X8.2 changed behavior, republished for X8.2.1.
August 2014	06	Note about NAT reflection added to X8.2 changed behavior, republished for X8.2.
July 2014	05	X8.2.1 maintenance release.
June 2014	04	X8.2 initial release.
July 2014	03	X8.1.1 release notes republished to remove limitation about Webex-enabled TelePresence.
April 2014	02	X8.1.1 maintenance release, including mobile and remote access features.
December 2013	01	X8.1 initial release. [Revised April 2014 to include issue CSCum90139.]