



# Cisco Expressway

## Administrator Guide

---

Software version: X8.5.2

April 2015

---

# Contents

|  |           |
|--|-----------|
| <b>Introduction</b> .....                                      | <b>9</b>  |
| About the Cisco Expressway .....                               | 10        |
| Expressway base applications .....                             | 11        |
| Standard features .....  | 11        |
| Optional features .....  | 12        |
| Appliance and virtual machine options .....                    | 13        |
| About this guide .....   | 14        |
| Related documentation .....                                    | 14        |
| Training .....   | 14        |
| Glossary .....   | 14        |
| Accessibility notice .....                                     | 14        |
| Using the web interface .....                                  | 15        |
| Using the command line interface (CLI) .....                   | 16        |
| Web page features and layout .....                             | 17        |
| What's new in this version? .....                              | 19        |
| Changes in X8.5.2 .....  | 19        |
| <b>Network and system settings</b> .....                       | <b>22</b> |
| Network settings .....   | 23        |
| Configuring Ethernet settings .....                            | 23        |
| Configuring IP settings .....                                  | 23        |
| Configuring DNS settings .....                                 | 25        |
| Configuring Quality of Service settings .....                  | 27        |
| Static routes .....  | 27        |
| Intrusion protection .....                                     | 29        |
| Configuring firewall rules .....                               | 29        |
| Current active firewall rules .....                            | 31        |
| Configuring automated intrusion protection .....               | 31        |
| Network services .....   | 35        |
| Configuring system name and access settings .....              | 35        |
| Configuring SNMP settings .....                                | 39        |
| Configuring time settings .....                                | 40        |
| Configuring the Login page .....                               | 42        |
| Configuring external manager settings .....                    | 43        |
| <b>Firewall traversal</b> .....                                | <b>44</b> |
| About firewall traversal .....                                 | 45        |
| The Expressway solution .....                                  | 45        |
| How does it work? .....  | 45        |
| H.323 firewall traversal protocols .....                       | 45        |
| SIP firewall traversal protocols .....                         | 46        |
| Media demultiplexing .....                                     | 46        |
| Firewall traversal configuration overview .....                | 47        |
| Configuring a traversal client and server .....                | 49        |
| Configuring ports for firewall traversal .....                 | 50        |
| Configuring the firewall .....                                 | 50        |
| Configuring traversal server ports .....                       | 50        |
| Configuring ports for connections from traversal clients ..... | 51        |
| Firewall traversal and authentication .....                    | 54        |

|   |            |
|---|------------|
| Authentication and NTP .....  | 54         |
| About ICE and TURN services .....   | 55         |
| About ICE .....   | 55         |
| About TURN .....  | 55         |
| Configuring TURN services .....   | 56         |
| <b>Unified Communications .....</b>   | <b>58</b>  |
| Unified Communications prerequisites .....  | 59         |
| Configuring a secure traversal zone connection for Unified Communications .....   | 59         |
| Server certificate requirements for Unified Communications .....                  | 61         |
| Mobile and remote access .....  | 64         |
| Mobile and remote access overview .....   | 64         |
| Configuring mobile and remote access on Expressway .....                          | 65         |
| Using deployments to partition Unified Communications services .....              | 71         |
| Single Sign-On (SSO) over the Collaboration Edge .....                            | 73         |
| Checking the status of Unified Communications services .....                      | 78         |
| Mobile and remote access port reference .....                                     | 78         |
| External XMPP federation .....  | 81         |
| Deploying Expressway for external XMPP federation .....                           | 81         |
| Configuring Expressway for external XMPP federation .....                         | 82         |
| DNS SRV records for XMPP federation .....   | 86         |
| Port usage for XMPP federation .....  | 87         |
| Checking XMPP federation status .....   | 87         |
| Troubleshooting external XMPP federation .....                                    | 88         |
| Cisco Jabber Guest .....  | 92         |
| Jabber Guest services overview .....  | 92         |
| Jabber Guest signaling and media flows in single-NIC deployment .....             | 92         |
| Jabber Guest licensing and call capacity .....                                    | 95         |
| Configuring Jabber Guest services on Expressway .....                             | 95         |
| Configuring your firewall for Jabber Guest traffic .....                          | 99         |
| Troubleshooting Jabber Guest services on Expressway .....                         | 100        |
| <b>Protocols .....</b>  | <b>102</b> |
| Configuring H.323 .....   | 103        |
| Configuring SIP .....   | 104        |
| SIP functionality and SIP-specific transport modes and ports .....                | 104        |
| Certificate revocation checking modes .....                                       | 104        |
| Configuring domains .....   | 106        |
| Configuring the supported services for Unified Communications .....               | 106        |
| Configuring SIP and H.323 interworking .....                                      | 107        |
| <b>Device authentication .....</b>  | <b>108</b> |
| About device authentication .....   | 109        |
| Controlling system behavior for authenticated and non-authenticated devices ..... | 109        |
| Authentication policy configuration options .....                                 | 110        |
| SIP authentication trust .....  | 111        |
| Configuring authentication to use the local database .....                        | 112        |
| Authenticating with external systems .....  | 112        |
| <b>Zones and neighbors .....</b>  | <b>113</b> |
| About zones .....   | 114        |
| Configuring media encryption policy .....   | 115        |

|   |            |
|---|------------|
| Configuring the B2BUA for media encryption .....                        | 115        |
| Configuring ICE messaging support .....                                 | 116        |
| The Default Zone .....  | 117        |
| Configuring the Default Zone .....                                      | 117        |
| Configuring Default Zone access rules .....                             | 118        |
| Configuring zones .....   | 119        |
| Configuring neighbor zones .....  | 119        |
| Configuring traversal client zones .....                                | 122        |
| Configuring traversal server zones .....                                | 124        |
| Configuring ENUM zones .....  | 127        |
| Configuring DNS zones .....   | 127        |
| Zone configuration: advanced settings .....                             | 128        |
| Zone configuration: pre-configured profile settings .....               | 132        |
| TLS certificate verification of neighbor systems .....                  | 133        |
| Configuring a zone for incoming calls only .....                        | 133        |
| <b>Clustering and peers .....</b>                                       | <b>134</b> |
| About clusters .....  | 135        |
| License usage within a cluster .....                                    | 136        |
| Managing clusters and peers .....                                       | 137        |
| Setting up a cluster .....  | 137        |
| Maintaining a cluster .....   | 138        |
| Specifying peer-specific items in clustered systems .....               | 139        |
| Sharing bandwidth across peers .....                                    | 140        |
| Cluster upgrades, backup and restore .....                              | 141        |
| Neighboring between Expressway clusters .....                           | 141        |
| Troubleshooting cluster replication problems .....                      | 143        |
| <b>Dial plan and call processing .....</b>                              | <b>144</b> |
| Call routing process .....  | 145        |
| Configuring hop counts .....  | 146        |
| Configuring dial plan settings .....                                    | 147        |
| About the fallback alias .....  | 147        |
| About transforms and search rules .....                                 | 148        |
| About pre-search transforms .....                                       | 148        |
| Configuring pre-search transforms .....                                 | 149        |
| Search and zone transform process .....                                 | 150        |
| Configuring search rules .....  | 151        |
| Example searches and transforms .....                                   | 154        |
| Filter queries to a zone without transforming .....                     | 154        |
| Always query a zone with original alias (no transforms) .....           | 155        |
| Query a zone for a transformed alias .....                              | 155        |
| Query a zone for original and transformed alias .....                   | 156        |
| Query a zone for two or more transformed aliases .....                  | 157        |
| Allowing calls to IP addresses only if they come from known zones ..... | 158        |
| Configuring search rules to use an external service .....               | 160        |
| About Call Policy .....   | 163        |
| Configuring Call Policy .....   | 163        |
| Configuring Call Policy rules using the web interface .....             | 164        |
| Configuring Call Policy using a CPL script .....                        | 164        |
| Configuring Call Policy to use an external service .....                | 165        |
| Supported address formats .....   | 167        |

|   |            |
|---|------------|
| Dialing by IP address .....                                   | 167        |
| Dialing by H.323 ID or E.164 alias .....                      | 167        |
| Dialing by H.323 or SIP URI .....                             | 167        |
| Dialing by ENUM .....   | 167        |
| Dialing by IP address .....                                   | 169        |
| About ENUM dialing .....                                      | 170        |
| ENUM dialing process .....                                    | 170        |
| Enabling ENUM dialing .....                                   | 170        |
| ENUM dialing for outgoing calls .....                         | 171        |
| Configuring zones and search rules for ENUM dialing .....     | 172        |
| ENUM dialing for incoming calls .....                         | 174        |
| Configuring DNS servers for ENUM and URI dialing .....        | 176        |
| Configuring call routing and signaling .....                  | 177        |
| Identifying calls .....                                       | 178        |
| Disconnecting calls .....                                     | 179        |
| <b>Bandwidth control .....</b>                                | <b>180</b> |
| About bandwidth control .....                                 | 181        |
| Configuring bandwidth controls .....                          | 181        |
| About subzones .....  | 183        |
| About the Traversal Subzone .....                             | 183        |
| Applying bandwidth limitations to the Traversal Subzone ..... | 185        |
| Links and pipes .....   | 186        |
| Configuring links .....                                       | 186        |
| Default links .....   | 186        |
| Configuring pipes .....                                       | 187        |
| Applying pipes to links .....                                 | 187        |
| <b>Applications .....</b>                                     | <b>188</b> |
| B2BUA (back-to-back user agent) overview .....                | 189        |
| Configuring B2BUA TURN servers .....                          | 189        |
| Microsoft Lync B2BUA .....                                    | 190        |
| <b>User accounts .....</b>                                    | <b>196</b> |
| About user accounts .....                                     | 197        |
| Account authentication .....                                  | 197        |
| Account types .....   | 197        |
| Configuring password security .....                           | 199        |
| Configuring administrator accounts .....                      | 201        |
| Viewing active administrator sessions .....                   | 203        |
| Configuring remote account authentication using LDAP .....    | 204        |
| Checking the LDAP server connection status .....              | 206        |
| Configuring administrator groups .....                        | 207        |
| Resetting forgotten passwords .....                           | 209        |
| Changing an administrator account password via GUI .....      | 209        |
| Resetting root or admin password via serial connection .....  | 209        |
| Resetting root or admin password via vSphere .....            | 209        |
| Using the root account .....                                  | 211        |
| Changing the root account password .....                      | 211        |
| Accessing the root account over SSH .....                     | 211        |
| Managing SSO tokens .....                                     | 212        |

|   |            |
|---|------------|
| <b>Maintenance</b> .....  | <b>213</b> |
| Enabling SSH access .....   | 214        |
| Enabling maintenance mode .....                                   | 215        |
| About upgrading software components .....                         | 216        |
| Upgrading Expressway software .....                               | 217        |
| Upgrading using secure copy (SCP/PSCP) .....                      | 218        |
| Configuring logging .....   | 219        |
| Changing Event log verbosity .....                                | 219        |
| Logging media statistics .....                                    | 220        |
| Publishing logs to remote syslog servers .....                    | 220        |
| Managing option keys .....  | 222        |
| About security certificates .....                                 | 223        |
| Managing the trusted CA certificate list .....                    | 223        |
| Managing the Expressway's server certificate .....                | 224        |
| Managing certificate revocation lists (CRLs) .....                | 227        |
| Configuring certificate-based authentication .....                | 230        |
| Testing client certificates .....                                 | 231        |
| Testing secure traversal .....                                    | 232        |
| Configuring language settings .....                               | 234        |
| Changing the language .....                                       | 234        |
| Installing language packs .....                                   | 234        |
| Removing language packs .....                                     | 235        |
| Backing up and restoring Expressway data .....                    | 236        |
| When to create a backup .....                                     | 236        |
| Content of the backup file .....                                  | 236        |
| Limitations .....   | 236        |
| Creating a system backup .....                                    | 236        |
| Restoring a previous backup .....                                 | 237        |
| Diagnostics tools .....   | 238        |
| Configuring diagnostic logging .....                              | 238        |
| Creating a system snapshot .....                                  | 239        |
| Configuring Network Log levels .....                              | 240        |
| Configuring Support Log levels .....                              | 240        |
| Incident reporting .....  | 241        |
| Incident reporting caution: privacy-protected personal data ..... | 241        |
| Enabling automatic incident reporting .....                       | 241        |
| Sending incident reports manually .....                           | 242        |
| Viewing incident reports .....                                    | 242        |
| Incident report details .....                                     | 243        |
| Checking the effect of a pattern .....                            | 244        |
| Locating an alias .....   | 245        |
| Port usage .....  | 246        |
| Local inbound ports .....   | 246        |
| Local outbound ports .....  | 246        |
| Remote listening ports .....                                      | 247        |
| Network utilities .....   | 248        |
| Ping .....  | 248        |
| Traceroute .....  | 248        |
| Tracepath .....   | 249        |
| DNS lookup .....  | 249        |

|   |            |
|---|------------|
| Restarting, rebooting and shutting down .....         | 252        |
| Developer resources .....                             | 254        |
| Debugging and system administration tools .....       | 254        |
| Experimental menu .....                               | 254        |
| <b>Overview and status information .....</b>          | <b>255</b> |
| Status overview .....                                 | 256        |
| System information .....                              | 257        |
| Ethernet status .....                                 | 258        |
| IP status .....                                       | 259        |
| Resource usage .....                                  | 260        |
| Call status .....                                     | 262        |
| Disconnecting calls .....                             | 263        |
| B2BUA calls .....                                     | 264        |
| Viewing B2BUA call media details .....                | 264        |
| Search history .....                                  | 265        |
| Search details .....                                  | 266        |
| Local Zone status .....                               | 267        |
| Zone status .....                                     | 268        |
| Bandwidth .....                                       | 269        |
| Link status .....                                     | 269        |
| Pipe status .....                                     | 269        |
| Policy server status and resiliency .....             | 270        |
| Viewing policy server status via the Expressway ..... | 270        |
| TURN relay usage .....                                | 271        |
| TURN relay summary .....                              | 271        |
| Unified Communications status .....                   | 272        |
| Checking SSO statistics .....                         | 272        |
| Lync B2BUA .....                                      | 273        |
| Lync B2BUA status .....                               | 273        |
| Managing alarms .....                                 | 274        |
| Logs .....  | 275        |
| Event Log .....                                       | 275        |
| Configuration Log .....                               | 276        |
| Network Log .....                                     | 277        |
| Hardware status .....                                 | 279        |
| <b>Reference material .....</b>                       | <b>280</b> |
| Performance capabilities .....                        | 281        |
| About Event Log levels .....                          | 282        |
| Event Log format .....                                | 282        |
| Administrator events .....                            | 283        |
| Message details field .....                           | 283        |
| Events and levels .....                               | 285        |
| CPL reference .....                                   | 291        |
| CPL address-switch node .....                         | 291        |
| otherwise .....                                       | 293        |
| not-present .....                                     | 293        |
| location .....  | 293        |
| rule-switch .....                                     | 294        |
| proxy .....   | 295        |
| reject .....  | 295        |

|   |     |
|---|-----|
| Unsupported CPL elements .....  | 295 |
| Changing the default SSH key .....  | 297 |
| Restoring default configuration (factory reset) .....   | 298 |
| Prerequisite files .....  | 298 |
| Performing a reset to default configuration .....   | 298 |
| Resetting via USB stick .....   | 299 |
| Password encryption .....   | 300 |
| Pattern matching variables .....  | 301 |
| Port reference .....  | 303 |
| Local Expressway inbound/outbound ports .....   | 303 |
| Remote listening ports .....  | 306 |
| Mobile and remote access port reference .....   | 308 |
| Microsoft Lync B2BUA port reference .....   | 310 |
| Regular expressions .....   | 312 |
| Supported characters .....  | 314 |
| Call types and licensing .....  | 315 |
| Call types .....  | 315 |
| What are traversal calls? .....   | 315 |
| Alarms .....  | 317 |
| Command reference — xConfiguration .....  | 332 |
| Command reference — xCommand .....  | 370 |
| Command reference — xStatus .....   | 383 |
| External policy overview .....  | 385 |
| Using an external policy server .....   | 385 |
| External policy request parameters .....  | 385 |
| Default CPL for policy services .....   | 386 |
| Flash status word reference table .....   | 388 |
| Supported RFCs .....  | 389 |
| Software version history .....  | 391 |
| X8.5.1 .....  | 391 |
| X8.5 .....  | 392 |
| Feature previews .....  | 392 |
| Single sign-on over MRA .....   | 392 |
| Improved line-side capabilities .....   | 393 |
| Multiple deployments for partitioning mobile and remote access to Unified Communications services | 393 |
| Serviceability improvements .....   | 394 |
| Other changes .....   | 395 |
| X8.2 .....  | 396 |
| X8.1.1 .....  | 398 |
| Related documentation .....   | 399 |
| Legal notices .....   | 401 |
| Intellectual property rights .....  | 401 |
| Copyright notice .....  | 401 |
| Patent information .....  | 402 |



# Introduction

---

This section provides an overview of the Cisco TelePresence Video Communication Server.

|                                   |    |
|-----------------------------------|----|
| About the Cisco Expressway .....  | 10 |
| About this guide .....            | 14 |
| What's new in this version? ..... | 19 |

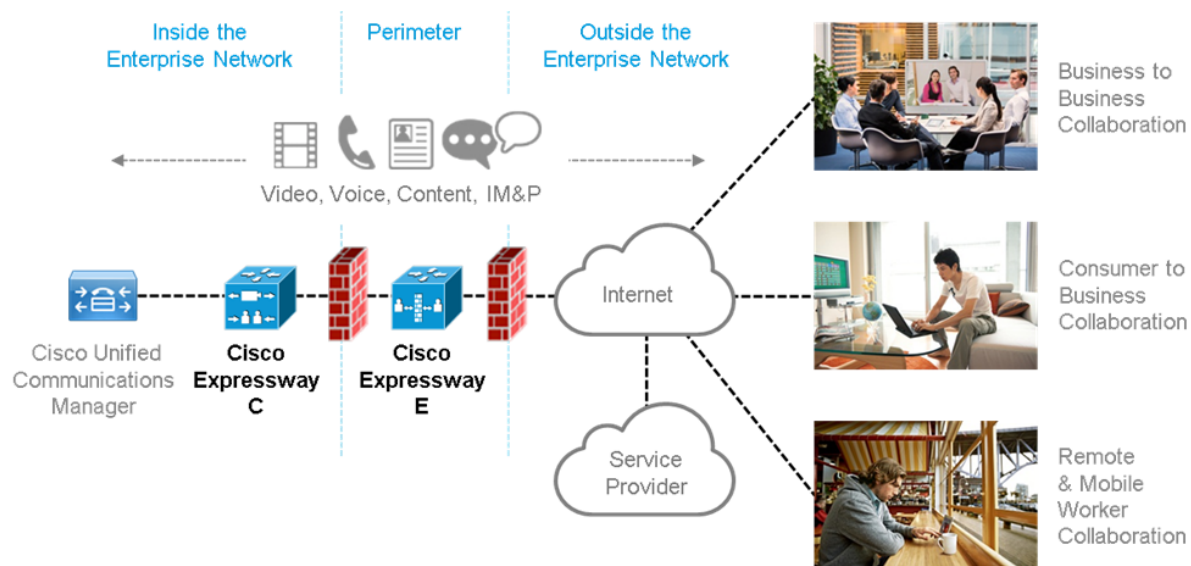
## About the Cisco Expressway

Cisco Expressway is designed specifically for comprehensive collaboration services provided through Cisco Unified Communications Manager. It features established firewall-traversal technology and helps redefine traditional enterprise collaboration boundaries, supporting our vision of any-to-any collaboration.

As its primary features and benefits, Cisco Expressway:

- Offers proven and highly secure firewall-traversal technology to extend your organizational reach.
- Helps enable business-to-business, business-to-consumer, and business-to-cloud-service-provider connections.
- Provides session-based access to comprehensive collaboration for remote workers, without the need for a separate VPN client.
- Supports a wide range of devices with Cisco Jabber for smartphones, tablets, and desktops.
- Complements bring-your-own-device (BYOD) strategies and policies for remote and mobile workers.

The Expressway is deployed as a pair: an Expressway-C with a trunk and line-side connection to Unified CM, and an Expressway-E deployed in the DMZ and configured with a traversal zone to an Expressway-C.



The Expressway is available on a dedicated CE Series appliance and also runs on VMware on a range of Cisco UCS servers. See [Expressway on Virtual Machine Installation Guide](#) for more information.

## Expressway base applications

The Expressway is available with alternative base applications as described below.

### Expressway-C

Expressway-C delivers any-to-any enterprise wide conference and session management and interworking capabilities. It extends the reach of telepresence conferences by enabling interworking between Session Initiation Protocol (SIP)- and H.323-compliant endpoints, interworking with third-party endpoints; it integrates with Unified CM and supports third-party IP private branch exchange (IP PBX) solutions. Expressway-C implements the tools required for creative session management, including definition of aspects such as routing, dial plans, and bandwidth usage, while allowing organizations to define call-management applications, customized to their requirements.

### Expressway-E

The Expressway-E deployed with the Expressway-C enables smooth video communications easily and securely outside the enterprise. It enables business-to-business video collaboration, improves the productivity of remote and home-based workers, and enables service providers to provide video communications to customers. The application performs securely through standards-based and secure firewall traversal for all SIP and H.323 devices. As a result, organizations benefit from increased employee productivity and enhanced communication with partners and customers.

It uses an intelligent framework that allows endpoints behind firewalls to discover paths through which they can pass media, verify peer-to-peer connectivity through each of these paths, and then select the optimum media connection path, eliminating the need to reconfigure enterprise firewalls.

The Expressway-E is built for high reliability and scalability, supporting multivendor firewalls, and it can traverse any number of firewalls regardless of SIP or H.323 protocol.

## Standard features

The primary purpose of the Expressway is to provide secure firewall traversal and session-based access to Cisco Unified Communications Manager for remote workers, without the need for a separate VPN client.

### Rich media session features

The following features are available when rich media session licenses are installed on the Expressway:

- SIP Proxy
- SIP / H.323 interworking
- IPv4 and IPv6 support, including IPv4 / IPv6 interworking
- QoS tagging
- Bandwidth management on both a per-call and a total usage basis
- Automatic downspeeding option for calls that exceed the available bandwidth
- URI and ENUM dialing via DNS, enabling global connectivity
- Up to 100 rich media sessions on a standard [Small/Medium](#) system and 500 rich media sessions on a Large system
- 1000 external zones with up to 2000 matches

- Flexible zone configuration with prefix, suffix and regex support
- Can be neighbored with other systems such as a Cisco VCS or other gatekeepers and SIP proxies
- n+1 redundancy, can be part of a cluster of up to 6 Expressways for increased capacity and redundancy
- Intelligent Route Director for single number dialing and network failover facilities
- Call Policy (also known as Administrator Policy) including support for CPL
- Support for external policy servers
- AD authentication for administrators of the Expressway
- Embedded setup wizard using a serial port for initial configuration
- System administration using a web interface or RS-232, SSH, and HTTPS
- Intrusion protection

Note that endpoints or other devices cannot register to the Expressway.

## Optional features

Some Expressway features are available by the purchase and installation of the appropriate option key:

### SIP to Microsoft Lync 2010 / 2013 gatewaying

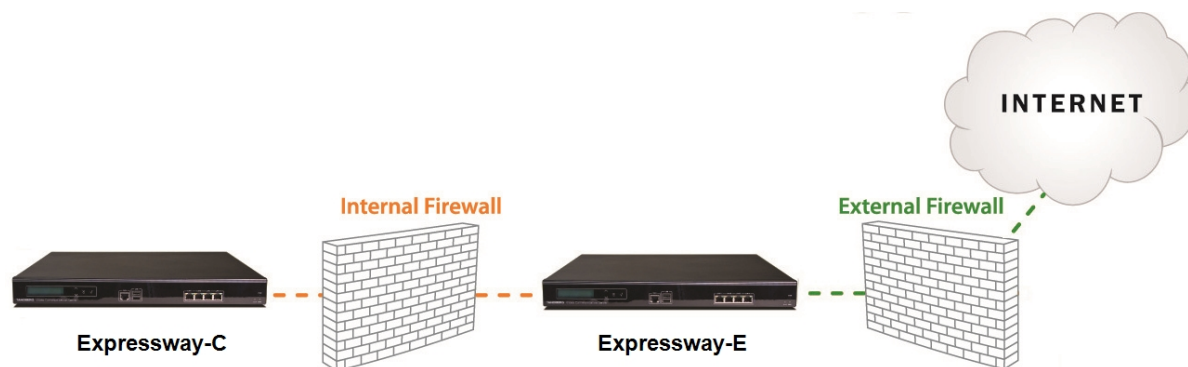
The Microsoft Lync back-to-back user agent (Lync B2BUA) on the Expressway can be used to route SIP calls between the Expressway and a Microsoft Lync Server. It provides interworking between Microsoft ICE (used by Lync clients) and media for communications with standard video endpoints.

The **Microsoft Interoperability** option key is required for all types of communication with Lync 2013.

### Advanced Networking

The Advanced Networking option enables the LAN 2 Ethernet port on the Expressway-E, allowing you to have a secondary IP address for your Expressway. This option also includes support for deployments where the Expressway-E is located behind a static NAT device, allowing it to have separate public and private IP addresses.

This configuration is intended for deployments where the Expressway-E is located in a DMZ between two separate firewalls on separate network segments.



## Appliance and virtual machine options

The Expressway supports on-premises and cloud applications and is available as a dedicated appliance or as a virtualized application on VMware, with additional support for Cisco Unified Computing System (Cisco UCS) platforms.

See [Performance capabilities \[p.281\]](#) for information about the capabilities of each type of appliance or virtual machine.

### Virtual machine options

The Expressway has 3 virtualized application deployment types:

- Small (for BE 6000 platform)
- Medium (standard installation)
- Large (extra performance and scalability capabilities)

See [Expressway on Virtual Machine Installation Guide](#) for more information.

### CE Series appliances

The Expressway is available as a dedicated CE Series appliance which is based on a UCS C220 M3L:

- CE500 appliance: used for standard installations and is equivalent to a Medium VM
- CE1000 appliance: offers extra performance and scalability capabilities and is equivalent to a Large VM

See the [CE Series appliance installation guides](#) for more information.

## About this guide

This guide has been divided into several sections, providing conceptual, configuration and reference information about the various features and capabilities of the Expressway. It describes a fully equipped version of the Expressway. Your version may not have all the described extensions installed.

Most configuration tasks on the Expressway can be performed by using either the web interface or a command line interface (CLI). This guide mainly describes how to use the web interface. Some Expressway features are only available through the CLI and these are described as appropriate, including the relevant CLI command.

In this guide, instructions for performing a task using the web interface are shown in the format **Menu > Submenu** followed by the **Name** of the page that you will be taken to.

Where command line interface (CLI) commands are included, they are shown in the format:

```
xConfiguration <Element> <SubElement>  
xCommand <Command>
```

## Related documentation

See [Related documentation \[p.399\]](#) for a full list of documents and web sites referenced in this guide.

## Training

Training is available online and at our training locations. For more information on all the training we provide and where our training offices are located, visit [www.cisco.com/go/telepresencetraining](http://www.cisco.com/go/telepresencetraining).

## Glossary

A glossary of TelePresence terms is available at: <https://tp-tools-web01.cisco.com/start/glossary/>.

## Accessibility notice

Cisco is committed to designing and delivering accessible products and technologies.

The Voluntary Product Accessibility Template (VPAT) for Cisco Expressway is available here:

[http://www.cisco.com/web/about/responsibility/accessibility/legal\\_regulatory/vpats.html#telepresence](http://www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html#telepresence)

You can find more information about accessibility here:

[www.cisco.com/web/about/responsibility/accessibility/index.html](http://www.cisco.com/web/about/responsibility/accessibility/index.html)

## Using the web interface

System configuration is normally carried out through the web interface.

To use the web interface:

1. Open a browser window and in the address bar type either:
  - the IP address of the system
  - the FQDN of the system
2. Enter a valid administrator **Username** and **Password** and click **Login** (see the [user accounts](#) section for details on setting up administrator accounts). You are presented with the **Overview** page.

Note that when logging in using the Expressway web interface, you may receive a warning message regarding the Expressway's security certificate. This can safely be ignored.

A [command line interface](#) is also available.

### Required fields

All mandatory fields on web pages are indicated by a red star .

### Supported browsers

The Expressway web interface is designed for use with Internet Explorer 8 or 9 (not in compatibility mode), Firefox 3 or later, or Chrome. Later versions of Internet Explorer may also work, but are not officially supported. It may work with Opera and Safari, but you could encounter unexpected behavior.

JavaScript and cookies must be enabled to use the Expressway web interface.

## Using the command line interface (CLI)

The Expressway can be configured through a web interface or via a command line interface (CLI).

The CLI is available by default over SSH and through the serial port. These settings are controlled on the [System administration](#) page.

To use the CLI:

1. Start an SSH session.
2. Enter the IP address or FQDN of the Expressway.
3. Log in with a username of **admin** and your system password.
4. You can now start using the CLI by typing the appropriate commands.

### Command types

Commands are divided into the following groups:

- **xStatus**: these commands return information about the current status of the system. Information such as current calls is available through this command group. See [Command reference — xStatus \[p.383\]](#) for a full list of **xStatus** commands.
- **xConfiguration**: these commands allow you to add and edit single items of data such as IP address and zones. See [Command reference — xConfiguration \[p.332\]](#) for a full list of **xConfiguration** commands.
- **xCommand**: these commands allow you to add and configure items and obtain information. See [Command reference — xCommand \[p.370\]](#) for a full list of **xCommand** commands.
- **xHistory**: these commands provide historical information about calls.
- **xFeedback**: these commands provide information about events as they happen, such as calls.

Note that:

- Typing an **xConfiguration** path into the CLI returns a list of values currently configured for that element (and sub-elements where applicable).
- Typing an **xConfiguration** path into the CLI followed by a ? returns information about the usage for that element and sub-elements.
- Typing an **xCommand** command into the CLI with or without a ? returns information about the usage of that command.



## Web page features and layout

This section describes the features that can be found on the Expressway web interface pages.

Figure 1: Example list page

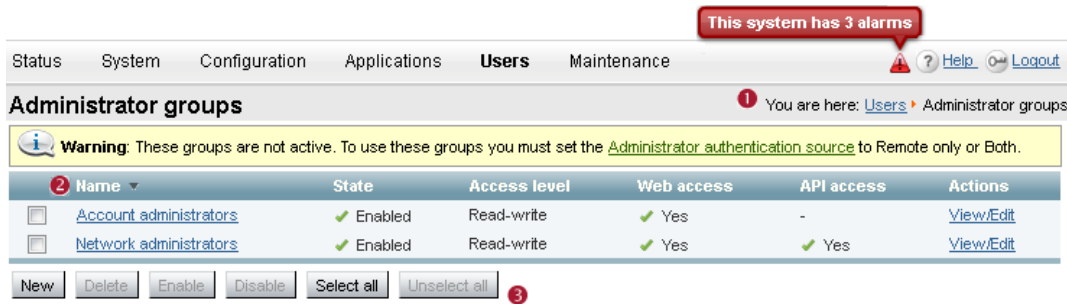
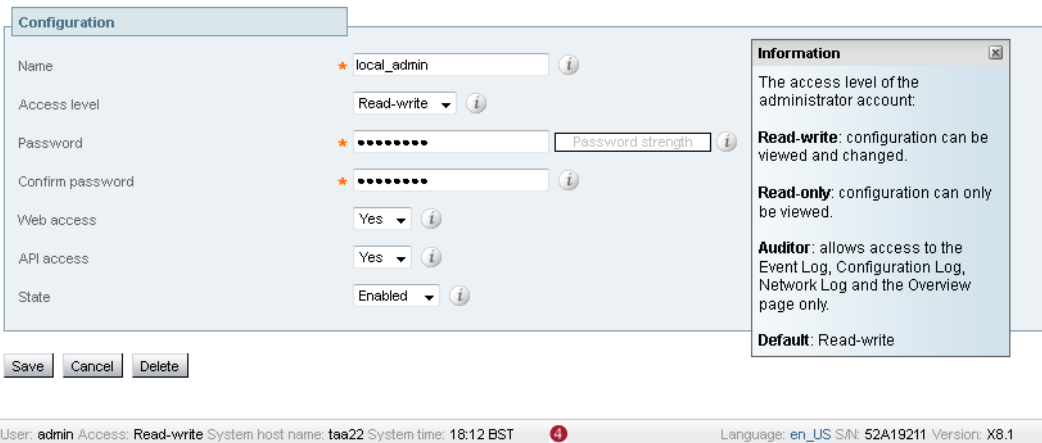









Figure 2: Example configuration page



The elements included in the example web pages shown here are described in the table below.

| Page element           |        | Description  |
|------------------------|--------|--|
| Page name and location | 1      | Every page shows the page name and the menu path to that page. Each part of the menu path is a link; clicking on any of the higher level menu items takes you to that page.  |
| System alarm           | !      | This icon appears on the top right corner of every page when there is a system alarm in place. Click on this icon to go to the Alarms page which gives information about the alarm and its suggested resolution.   |
| Help                   | ?      | This icon appears on the top right corner of every page. Clicking on this icon opens a new browser window with help specific to the page you are viewing. It gives an overview of the purpose of the page, and introduces any concepts configured from the page. |
| Log out                | Logout | This icon appears on the top right corner of every page. Clicking on this icon ends your administrator session.  |

| Page element                     |   | Description  |
|----------------------------------|---|--|
| Field level information          |  | An information box appears on the configuration pages whenever you either click on the Information icon or click inside a field. This box gives you information about the particular field, including where applicable the valid ranges and default value. To close the information box, click on the X at its top right corner. |
| Information bar                  |  | The Expressway provides you with feedback in certain situations, for example when settings have been saved or when you need to take further action. This feedback is given in a yellow information bar at the top of the page.   |
| Sorting columns                  |  | Click on column headings to sort the information in ascending and descending order.  |
| Select All and Unselect All      |  | Use these buttons to select and unselect all items in the list.  |
| Mandatory field                  |  | Indicates an input field that must be completed.   |
| Peer-specific configuration item |  | When an Expressway is part of a cluster, most items of configuration are applied to all peers in a cluster. However, items indicated with a † must be specified separately on each cluster peer.   |
| System Information               |  | The name of the user currently logged in and their access privileges, the system name (or LAN 1 IPv4 address if no system name is configured), local system time, currently selected language, serial number and Expressway software version are shown at the bottom of the page.  |

Note that you cannot change configuration settings if your administrator account has read-only privileges.

## What's new in this version?

The new features introduced in this release of Expressway software are listed below.

Table 1: Feature history by release number

| Feature / change   | X8.5.2    | X8.5.1  | X8.5          |
|--|-----------|---|---------------|
| <a href="#">KPML</a>                                     | Supported | Not supported                                   | Not supported |
| <a href="#">Multiple Presence Domains via MRA</a>        | Preview   | Preview   | Not supported |
| <a href="#">SSO over MRA</a>                             | Supported | Supported;<br>SAML signing<br>algorithm changed | Preview       |
| <a href="#">CSR UI digest algorithm options</a>          | Supported | Supported                                       | Not supported |
| <a href="#">Cisco DX Series endpoints over MRA</a>       | Preview   | Preview   | Preview       |
| <a href="#">Cisco IP Phone 7800/8800 Series over MRA</a> | Preview   | Preview   | Preview       |
| <a href="#">Early media</a>                              | Supported | Supported                                       | Supported     |
| <a href="#">Unsolicited NOTIFY pass-through</a>          | Supported | Supported                                       | Supported     |
| <a href="#">Multiple deployments</a>                     | Supported | Supported                                       | Supported     |
| <a href="#">Secure connection checker</a>                | Supported | Supported                                       | Supported     |
| <a href="#">Syslog publish filter</a>                    | Supported | Supported                                       | Supported     |
| <a href="#">Call Detail Records (CDRs)</a>               | Supported | Supported                                       | Supported     |
| <a href="#">Media statistics</a>                         | Supported | Supported                                       | Supported     |
| <a href="#">Password change requires authorization</a>   | Supported | Supported                                       | Supported     |
| <a href="#">Static routes</a>                            | Supported | Supported                                       | Supported     |

## Changes in X8.5.2

These are changes and developments to the X8.5 software during its maintenance cycle, as summarized above. See [Software version history \[p.391\]](#) for full descriptions of the features introduced in [X8.5 \[p.392\]](#) and the changes in [X8.5.1 \[p.391\]](#).

### (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.

- [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.

- Chinese
- French
- German
- Spanish

---

**Note:** These localizations apply to the X8.5.1 versions of UI and help. Additional language packs (for Japanese, Korean, and Russian) are currently being prepared.

---

### 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.



# Network and system settings

---

This section describes network services and settings related options that appear under the **System** menu of the web interface. These options enable you to configure the Expressway in relation to the network in which it is located, for example its IP settings, firewall rules, intrusion protection and the external services used by the Expressway (for example DNS, NTP and SNMP).

|   |    |
|---|----|
| Network settings .....                      | 23 |
| Intrusion protection .....                  | 29 |
| Network services .....                      | 35 |
| Configuring external manager settings ..... | 43 |

# Network settings

## Configuring Ethernet settings

Use the **Ethernet** page (**System > Network interfaces > Ethernet**) to configure the speed of the connections between the Expressway and the Ethernet networks to which it is connected. The speed and duplex mode must be the same at both ends of the connection. If you installed the **Advanced Networking** option, you can configure the speed and duplex mode for each Ethernet port.

The default **Speed** is *Auto*, which means that the Expressway and the connected switch will automatically negotiate the speed and duplex mode.

---

**Note:** We recommend *Auto* unless the connected switch is unable to auto-negotiate. A mismatch in speed/duplex mode between the two ends of the connection will cause packet loss and could make the system inaccessible.

---

## Configuring IP settings

The **IP** page (**System > Network interfaces > IP**) is used to configure the IP protocols and network interface settings of the Expressway.

### IP protocol configuration

You can configure whether the Expressway uses *IPv4*, *IPv6* or *Both* protocols. The default is *Both*.

- *IPv4*: it only takes calls between two endpoints communicating via IPv4. It communicates with other systems via IPv4 only.
- *IPv6*: it only takes calls between two endpoints communicating via IPv6. It communicates with other systems via IPv6 only.
- *Both*: it takes calls using either protocol. If a call is between an IPv4-only and an IPv6-only endpoint, the Expressway acts as an IPv4 to IPv6 gateway. It communicates with other systems via either protocol.

All IPv6 addresses configured on the Expressway are treated as having a /64 network prefix length.

### IPv4 to IPv6 gatewaying (interworking)

The Expressway can act as a gateway for calls between IPv4 and IPv6 devices. To enable this feature, select an **IP protocol** of *Both*.

### IP gateways

You can set the default **IPv4 gateway** and **IPv6 gateway** used by the Expressway. These are the gateways to which IP requests are sent for IP addresses that do not fall within the Expressway's local subnet.

- The default **IPv4 gateway** is 127.0.0.1, which should be changed during the commissioning process.
- The **IPv6 gateway**, if entered, must be a static global IPv6 address. It cannot be a link-local or a stateless auto-configuration (SLAAC) IPv6 address.

## LAN configuration

LAN 1 is the primary network port on the Expressway. You can configure the **IPv4 address** and **subnet mask**, the **IPv6 address** and the **Maximum transmission unit (MTU)** for this port.

- The Expressway is shipped with a default IP address of 192.168.0.100 (for both LAN ports). This lets you connect the Expressway to your network and access it via the default address so that you can configure it remotely.
- The **IPv6 address**, if entered, must be a static global IPv6 address. It cannot be a link-local or a stateless auto-configuration (SLAAC) IPv6 address.
- If you have **Advanced Networking** installed, you can also configure these options for the LAN 2 port.
- The **Maximum transmission unit (MTU)** defaults to 1500 bytes.

## About Advanced Networking

The **Advanced Networking** option key enables the LAN 2 port on an Expressway-E for both management and call signaling. This allows you to have a second IP address for your Expressway. The option key also enables static NAT functionality.

### Configuring dual network interfaces

Dual network interfaces are intended for deployments where the Expressway-E is located in a DMZ between two separate firewalls on separate network segments. In such deployments, routers prevent devices on the internal network from being able to route IP traffic to the public internet, and instead the traffic must pass through an application proxy such as the Expressway-E.

To enable the use of dual network interfaces:

1. Ensure that the **Advanced Networking** option key is installed on the Expressway-E.
2. Set **Use dual network interfaces** to Yes.
3. Set **External LAN interface** to LAN2.  
LAN 2 should be used as the public interface of the Expressway-E (if the Expressway-E is ever clustered, LAN 1 must be used for clustering, and the clustering interface must not be mapped through a NAT).  
This setting also determines the port from which TURN server relay allocations are made.

Note that:

- You should configure the LAN 1 port and restart the Expressway before configuring the LAN 2 port.
- The LAN 1 and LAN 2 interfaces must be on different, non-overlapping subnets.
- If you have Advanced Networking enabled but only want to configure one of the Ethernet ports, you must use LAN 1.
- If the Expressway-E is in the DMZ, the outside IP address of the Expressway-E must be a public IP address, or if static NAT mode is enabled, the static NAT address must be publicly accessible.
- The Expressway-E may also be used to traverse internal firewalls within an enterprise. In this case the "public" IP address may not be publicly accessible, but is an IP address accessible to other parts of the enterprise.
- If you need to change the IP addresses on one or both interfaces, you can do it via the UI or the CLI. You can change both at the same time if required, and the new addresses take effect after a restart.



## Configuring static NAT

You can deploy the Expressway-E behind a static NAT device, allowing it to have separate public and private IP addresses. This feature is intended for use in deployments where the Expressway-E is located in a DMZ, and has the **Advanced Networking** feature enabled.

In these deployments, the externally-facing LAN port has static NAT enabled in order to use both a private and public IPv4 address; the internally facing LAN port does not have static NAT enabled and uses a single IPv4 (or IPv6) address.

In such a deployment, traversal clients should be configured to use the internally-facing IP address of the Expressway-E.

To enable the use of a static NAT:

1. Ensure that the **Advanced Networking** option key is installed.
2. For the externally-facing LAN port:
  - a. In the **IPv4 address** field, enter the Expressway-E's private IP address.
  - b. Set **IPv4 static NAT mode** to *On*.
  - c. In the **IPv4 static NAT address** field, enter the Expressway-E's public IP address - this is the IP address of the outside of the NAT.

---

**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.

---

## Configuring DNS settings

The **DNS** page (**System > DNS**) is used to configure the Expressway's DNS servers and DNS settings.

### Configuring the system host and domain name

The **System host name** defines the DNS host name that this Expressway is known by.

- It must be unique for each peer in a cluster.
- It is used to identify the Expressway on a remote log server (a default name of "TANDBERG" is used if the **System host name** is not specified).

The **Domain name** is used when attempting to resolve unqualified server addresses (for example **ldapservers**). It is appended to the unqualified server address before the query is sent to the DNS server. If the server address is fully qualified (for example **ldapservers.mydomain.com**) or is in the form of an IP address, the domain name is not appended to the server address before querying the DNS server.

It applies to the following configuration settings in the Expressway:

- LDAP server
- NTP server
- External Manager server
- Remote logging server

You are recommended to use an IP address or FQDN (Fully Qualified Domain Name) for all server addresses.

Note that the FQDN of the Expressway is the **System host name** plus the **Domain name**.

### Impact on SIP messaging

The **System host name** and **Domain name** are also used to identify references to this Expressway in SIP messaging, where an endpoint has configured the Expressway as its SIP proxy in the form of an FQDN (as opposed to an IP address, which is not recommended).

In this case the Expressway may, for example, reject an INVITE request if the FQDN configured on the endpoint does not match the **System host name** and **Domain name** configured on the Expressway. (Note that this check occurs because the SIP proxy FQDN is included in the route header of the SIP request sent by the endpoint to the Expressway.)

### DNS requests

By default, DNS requests use a random port from within the system's ephemeral port range.

If required, you can specify a custom port range instead by setting **DNS requests port range** to *Use a custom port range* and then defining the **DNS requests port range start** and **DNS requests port range end** fields. Note that setting a small source port range will increase your vulnerability to DNS spoofing attacks.

## Configuring DNS server addresses

You must specify at least one DNS server to be queried for address resolution if you want to:

- Use FQDNs (Fully Qualified Domain Names) instead of IP addresses when specifying external addresses (for example for LDAP and NTP servers, neighbor zones and peers).
- Use features such as URI dialing or [ENUM dialing](#).

### Default DNS servers

You can specify up to 5 default DNS servers.

- The Expressway only queries one server at a time; if that server is not available the Expressway will try another server from the list.
- The order that the servers are specified is not significant; the Expressway attempts to favor servers that were last known to be available.

### Per-domain DNS servers

In addition to the 5 default DNS servers, you can specify 5 additional explicit DNS servers for specified domains. This can be useful in deployments where specific domain hierarchies need to be routed to their explicit authorities.

For each additional per-domain DNS server address you can specify up to 2 **Domain names**. Any DNS queries under those domains are forwarded to the specified DNS server instead of the default DNS servers.

You can specify redundant per-domain servers by adding an additional per-domain DNS server address and associating it with the same **Domain names**. In this scenario, DNS requests for those domains will be sent in parallel to both DNS servers.

---

**Tip:** you can also use the [DNS lookup](#) tool (**Maintenance > Tools > Network utilities > DNS lookup**) to check which domain name server (DNS server) is responding to a request for a particular hostname.

---

## Caching DNS records

To improve performance, DNS lookups may be cached. This cache is flushed automatically whenever the DNS configuration is changed.

You can also force the cache to be flushed by clicking **Flush DNS cache**.

## Configuring Quality of Service settings

The **Quality of Service (QoS)** page (**System > Quality of Service**) is used to configure QoS options for outbound traffic from the Expressway.

This allows the network administrator to tag all signaling and media packets flowing through the Expressway with one specific QoS tag and hence provide the ability to prioritize video traffic over normal data traffic. Management traffic, for example SNMP messages, is not tagged.

### Supported mechanisms

The Expressway supports the *DiffServ* (Differentiated Services) mechanism which puts the specified **Tag value** in the TOS (Type Of Service) field of the IPv4 header or TC (Traffic Class) field of the IPv6 header.

## Static routes

You can define static routes from the Expressway to an IPv4 or IPv6 address range. Go to **System > Network interfaces > Static routes**.

On this page you can view, add, and delete static routes.

Static routes are sometimes required when using the **Advanced Networking** option and deploying the Expressway in a DMZ. They may also be required in other complex network deployments.

### To add a static route:

1. Enter the base destination address of the new static route from this Expressway  
For example, enter `203.0.113.0` or `2001:db8::`
2. Enter the prefix length that defines the range  
Extending the example, you could enter `24` to define the IPv4 range `203.0.113.0 - 203.0.113.255`, or `32` to define the IPv6 range `2001:db8::` to `2001:db8:ffff:ffff:ffff:ffff:ffff:ffff`.  
The address range field shows the range calculated by the Expressway from the IP address and Prefix length.
3. Enter the IP address of the gateway for your new route
4. Select an ethernet interface for your new route  
This option is only available if the second ethernet interface is enabled. Select *LAN 1* or *LAN 2* to force the route via that interface, or select *Auto* to allow the Expressway to make this route on either interface.
5. Click **Create route**  
The new static route is listed in the table. You can delete routes from this table if necessary.

### Notes

- IP routes can also be configured using the CLI, using [xCommand RouteAdd](#) and the [xConfiguration IP Route](#) commands.

- You can configure routes for up to 50 network and host combinations.
- Do not configure IP routes by logging in as `root` and using `ip route` statements.

# Intrusion protection

## Configuring firewall rules

Firewall rules provide the ability to configure IP table rules to control access to the Expressway at the IP level. On the Expressway, these rules have been classified into groups and are applied in the following order:

- **Dynamic system rules:** these rules ensure that all established connections/sessions are maintained. They also include any rules that have been inserted by the automated detection feature as it blocks specific addresses. Finally, it includes a rule to allow access from the loopback interface.
- **Non-configurable application rules:** this incorporates all necessary application-specific rules, for example to allow SNMP traffic and H.323 gatekeeper discovery.
- **User-configurable rules:** this incorporates all of the manually configured firewall rules (as described in this section) that refine — and typically restrict — what can access the Expressway. There is a final rule in this group that allows all traffic destined for the Expressway LAN 1 interface (and the LAN 2 interface if the **Advanced Networking** option key is installed).

There is also a final, non-configurable rule that drops any broadcast or multicast traffic that has not already been specifically allowed or denied by the previous rules.

By default any traffic that is destined for the specific IP address of the Expressway is allowed access, but that traffic will be dropped if the Expressway is not explicitly listening for it. You have to actively configure extra rules to lock down the system to your specifications.

Note that return traffic from outbound connections is always accepted.

### User-configured rules

The user-configured rules are typically used to restrict what can access the Expressway. You can:

- Specify the source IP address subnet from which to allow or deny traffic.
- Choose whether to drop or reject denied traffic.
- Configure well known services such as SSH, HTTP/HTTPS or specify customized rules based on transport protocols and port ranges.
- Configure different rules for the LAN 1 and LAN 2 interfaces (if the **Advanced Networking** option key is installed), although note that you cannot configure specific destination addresses such as a multicast address.
- Specify the priority order in which the rules are applied.



## Setting up and activating firewall rules

The **Firewall rules configuration** page is used to set up and activate a new set of firewall rules.

The set of rules shown will initially be a copy of the current active rules. (On a system where no firewall rules have previously been defined, the list will be empty.) If you have a lot of rules you can use the **Filter** options to limit the set of rules displayed. Note that the built-in rules are not shown in this list.

You can then change the set of firewall rules by adding new rules, or by modifying or deleting any existing rules. Any changes made at this stage to the current active rules are held in a pending state. When you have completed making all the necessary changes you can activate the new rules, replacing the previous set.

### To set up and activate new rules:

1. Go to **System > Protection > Firewall rules > Configuration**.
2. Make your changes by adding new rules, or by modifying or deleting any existing rules as required.  
You can change the order of the rules by using the up/down arrows  and  to swap the priorities of adjacent rules.
  - New or modified rules are shown as **Pending** (in the **State** column).
  - Deleted rules are shown as **Pending delete**.
3. When you have finished configuring the new set of firewall rules, click **Activate firewall rules**.
4. Confirm that you want to activate the new rules. This will replace the existing set of active rules with the set you have just configured.  
After confirming that you want to activate the new rules, they are validated and any errors reported.
5. If there are no errors, the new rules are temporarily activated and you are taken to the **Firewall rules confirmation** page.  
You now have 15 seconds to confirm that you want to keep the new rules:
  - Click **Accept changes** to permanently apply the rules.
  - If the 15 seconds time limit expires or you click **Rollback changes**, the previous rules are reinstated and you are taken back to the configuration page.

The automatic rollback mechanism provided by the 15 seconds time limit ensures that the client system that activated the changes is still able to access the system after the new rules have been applied. If the client system is unable to confirm the changes (because it can no longer access the web interface) then the rollback will ensure that its ability to access the system is reinstated.

When configuring firewall rules, you also have the option to **Revert all changes**. This discards all pending changes and resets the working copy of the rules to match the current active rules.

### Rule settings

The configurable options for each rule are:

| Field                               | Description   | Usage tips  |
|-------------------------------------|---|---|
| <b>Priority</b>                     | The order in which the firewall rules are applied.  | The rules with the highest priority (1, then 2, then 3 and so on) are applied first.<br><br>Firewall rules must have unique priorities. Rule activation will fail if there are multiple rules with the same priority.   |
| <b>Interface</b>                    | The LAN interface on which you want to control access.  | This only applies if the <b>Advanced Networking</b> option key is installed.  |
| <b>IP address and Prefix length</b> | These two fields together determine the range of IP addresses to which the rule applies.                                  | The <b>Address range</b> field shows the range of IP addresses to which the rule applies, based on the combination of the <b>IP address</b> and <b>Prefix length</b> .<br><br>The prefix length range is 0-32 for an IPv4 address, and 0-128 for an IPv6 address. |
| <b>Service</b>                      | Choose the service to which the rule applies, or choose <i>Custom</i> to specify your own transport type and port ranges. | Note that if the destination port of a service is subsequently reconfigured on the Expressway, for example from 80 to 8080, any firewall rules containing the old port number will not be automatically updated.  |
| <b>Transport</b>                    | The transport protocol to which the rule applies.   | Only applies if specifying a <i>Custom</i> service.   |

| Field                     | Description  | Usage tips   |
|---------------------------|--|--|
| <b>Start and end port</b> | The port range to which the rule applies.  | Only applies if specifying a UDP or TCP <i>Custom</i> service.   |
| <b>Action</b>             | <p>The action to take against any IP traffic that matches the rule.</p> <p><i>Allow</i>: Accept the traffic.</p> <p><i>Drop</i>: Drop the traffic without any response to the sender.</p> <p><i>Reject</i>: Reject the traffic with an 'unreachable' response.</p> | <p>Dropping the traffic means that potential attackers are not provided with information as to which device is filtering the packets or why.</p> <p>For deployments in a secure environment, you may want to configure a set of low priority rules (for example, priority 50000) that deny access to all services and then configure higher priority rules (for example, priority 20) that selectively allow access for specific IP addresses.</p> |
| <b>Description</b>        | An optional free-form description of the firewall rule.  | If you have a lot of rules you can use the <b>Filter</b> by description options to find related sets of rules.   |

## Current active firewall rules

The [Current active firewall rules](#) page ([System > Protection > Firewall rules > Current active rules](#)) shows the user-configured firewall rules that are currently in place on the system. There is also a set of built-in rules that are not shown in this list.

If you want to change the rules you must go to the [Firewall rules configuration](#) page from where you can set up and activate a new set of rules.

## Configuring automated intrusion protection

The automated protection service can be used to detect and block malicious traffic and to help protect the Expressway from dictionary-based attempts to breach login security.

It works by parsing the system log files to detect repeated failures to access specific service categories, such as SIP, SSH and web/HTTPS access. When the number of failures within a specified time window reaches the configured threshold, the source host address (the intruder) and destination port are blocked for a specified period of time. The host address is automatically unblocked after that time period so as not to lock out any genuine hosts that may have been temporarily misconfigured.

You can configure ranges of addresses that are exempted from one or more categories (see [Configuring exemptions \[p.33\]](#) below).

Automated protection should be used in combination with the [firewall rules](#) feature - use automated protection to dynamically detect and temporarily block specific threats, and use firewall rules to permanently block a range of known host addresses.

### About protection categories

The set of available protection categories on your Expressway are pre-configured according to the software version that is running. You can enable, disable or configure each category, but you cannot add additional categories.

The rules by which specific log file messages are associated with each category are also pre-configured and cannot be altered. You can view example log file entries that would be treated as an access failure/intrusion within a particular category by going to **System > Protection > Automated detection > Configuration** and clicking on the name of the category. The examples are displayed above the **Status** section at the bottom of the page.

## Enabling automated protection

To enable intrusion protection on your Expressway:

1. Go to **System > Administration**.
2. Set **Automated protection service** to *On*.
3. Click **Save**.
4. You must then ensure that the required protection categories are enabled and configured, and that any required exemptions are specified, as described below.  
All protection categories are disabled by default.

## Configuring protection categories

The **Automated detection overview** page (**System > Protection > Automated detection > Configuration**) is used to enable and configure the Expressway's protection categories, and to view current activity.

The page displays a summary of all available categories, showing:

- **Status:** this indicates if the category is configured to be *On* or *Off*. When *On*, it additionally indicates the state of the category: this is normally *Active*, but may temporarily display *Initializing* or *Shutting down* when a category has just been enabled or disabled. Check the alarms if it displays *Failed*.)
- **Currently blocked:** the number of addresses currently being blocked for this category.
- **Total failures:** the total number of failed attempts to access the services associated with this category.
- **Total blocks:** the total number of times that a block has been triggered. Note that:
  - The **Total blocks** will typically be less than the **Total failures** (unless the **Trigger level** is set to 1).
  - The same address can be blocked and released several times per category, with each occurrence counting as a separate block.
- **Exemptions:** the number of addresses that are configured as exempt from this category.

From this page, you can also view any currently blocked addresses or any exemptions that apply to a particular category.

### Enabling and disabling categories

To enable or disable one or more protection categories:

1. Go to **System > Protection > Automated detection > Configuration**.
2. Select the check box alongside the categories you want to enable or disable.
3. Click **Enable** or **Disable** as appropriate.



## Configuring a category's blocking rules

To configure a category's specific blocking rules:

1. Go to **System > Protection > Automated detection > Configuration**.
2. Click on the name of the category you want to configure.  
You are taken to the configuration page for that category.
3. Configure the category as required:
  - **State**: whether protection for that category is enabled or disabled.
  - **Description**: a free-form description of the category.
  - **Trigger level** and **Detection window**: these settings combine to define the blocking threshold for the category. They specify the number of failed access attempts that must occur before the block is triggered, and the time window in which those failures must occur.
  - **Block duration**: the period of time for which the block will remain in place.
4. Click **Save**.

## Configuring exemptions

The **Automated detection exemptions** page (**System > Protection > Automated detection > Exemptions**) is used to configure any IP addresses that are to be exempted always from one or more protection categories.

To configure exempted addresses:

1. Go to **System > Protection > Automated detection > Exemptions**.
2. Click on the **Address** you want to configure, or click **New** to specify a new address.
3. Enter the **Address** and **Prefix length** to define the range of IPv4 addresses you want to exempt.
4. Select the categories from which the address is to be exempted.
5. Click **Add address**.

Note that if you exempt an address that is currently blocked, it will remain blocked until its block duration expires (unless you unblock it manually via the **Blocked addresses** page).

## Managing blocked addresses

The **Blocked addresses** page (**System > Protection > Automated detection > Blocked addresses**) is used to manage the addresses that are currently blocked by the automated protection service:

- It shows all currently blocked addresses and from which categories those addresses have been blocked.
- You can unblock an address, or unblock an address and at the same time add it to the exemption list. Note that if you want to permanently block an address, you must add it to the set of configured [firewall rules](#).

If you access this page via the links on the **Automated detection overview** page it is filtered according to your chosen category. It also shows the amount of time left before an address is unblocked from that category.

## Investigating access failures and intrusions

If you need to investigate specific access failures or intrusion attempts, you can review all the relevant triggering log messages associated with each category. To do this:

1. Go to **System > Protection > Automated detection > Configuration**.
2. Click on the name of the category you want to investigate.
3. Click **View all matching intrusion protection triggers for this category**.  
The system will display all the relevant events for that category. You can then search through the list of triggering events for the relevant event details such as a user name, address or alias.

## Automated protection service and clustered systems

When the automated protection service is enabled in a clustered system:

- Each peer maintains its own count of connection failures and the trigger threshold must be reached on each peer for the intruder's address to be blocked by that peer.
- Addresses are blocked against only the peer on which the access failures occurred. This means that if an address is blocked against one peer it may still be able to attempt to access another peer (from which it may too become blocked).
- A blocked address can only be unblocked for the current peer. If an address is blocked by another peer, you must log in to that peer and then unblock it.
- Category settings and the exemption list are applied across the cluster.
- The statistics displayed on the **Automated detection overview** page are for the current peer only.

## Additional information

- When a host address is blocked and tries to access the system, the request is dropped (the host receives no response).
- A host address can be blocked simultaneously for multiple categories, but may not necessarily be blocked by all categories. Those blocks may also expire at different times.
- When an address is unblocked (either manually or after its block duration expires), it has to fail again for the full number of times as specified by the category's trigger level before it will be blocked for a second time by that category.
- A category is reset whenever it is enabled. All categories are reset if the system is restarted or if the automated protection service is enabled at the system level. When a category is reset:
  - Any currently blocked addresses are unblocked.
  - Its running totals of failures and blocks are reset to zero.
- You can view all Event Log entries associated with the automated protection service by clicking **View all intrusion protection events** on the **Automated detection overview** page.

# Network services

## Configuring system name and access settings

The **System administration** page (**System > Administration**) is used to configure the name of the Expressway and the means by which it is accessed by administrators.

### System settings

#### System name

The **System name** is used to identify the Expressway. It appears in various places in the web interface, and in the display on the front panel of the unit (so that you can identify it when it is in a rack with other systems). The **System name** is also used by Cisco TMS.

We recommend that you give the Expressway a name that allows you to easily and uniquely identify it.

#### Ephemeral port range

You can specify the **Ephemeral port range start** and **end** values. This defines the port range to use for ephemeral outbound connections not otherwise constrained by Expressway call processing.

The default range is 30000 to 35999.

#### Call detail records (CDRs)

The system can capture CDRs if you enable the service (which is off by default), and can publish them as syslog messages if you are using remote logging.

If you select *Service only* the system keeps the CDRs for 7 days, and these CDRs can only be read via the REST API to the Expressway. If you select *Service and logging*, the local data is exposed in the Event log, and the CDRs are also sent as INFO messages to your syslog host.

---

#### Notes:

- CDR reporting is best effort and the CDRs cannot be relied upon for accurate billing purposes.
  - The local 7 days worth of CDR data is written to disk. It is preserved over a system restart/reboot, and is included in the backup/restore process.
- 

## Administration access settings

While you can administer the Expressway via a PC connected directly to the unit via a serial cable, you may want to access the system remotely over IP. You can do this using either the web interface (via HTTPS) or through a command line interface (via SSH).

The configurable options are:

| Field                        | Description   | Usage tips  |
|------------------------------|---|---|
| <b>Services</b>              |   |   |
| <b>Serial port / console</b> | Whether the system can be accessed locally via the VMware console. Default is <i>On</i> . | Serial port / console access is always enabled for one minute following a restart, even if it is normally disabled. |

| Field                                  | Description   | Usage tips  |
|--|---|---|
| <b>SSH service</b>                     | Whether the Expressway can be accessed via SSH and SCP. Default is <i>On</i> .  |   |
| <b>Web interface (over HTTPS)</b>      | Whether the Expressway can be accessed via the web interface. Default is <i>On</i> .  | Cisco TMS accesses the Expressway via the web server. If HTTPS mode is turned off, Cisco TMS will not be able to access it.   |
| <b>Session limits</b>                  |   |   |
| <b>Session time out</b>                | The number of minutes that an administration session (serial port, HTTPS or SSH) may be inactive before the session is timed out. Default is 30 minutes.  |   |
| <b>Per-account session limit</b>       | The number of concurrent sessions that each individual administrator account is allowed on each Expressway.   | This includes web, SSH and serial sessions. Session limits are not enforced on the root account. A value of 0 turns session limits off.   |
| <b>System session limit</b>            | The maximum number of concurrent administrator sessions allowed on each Expressway.   | This includes web, SSH and serial sessions. Session limits are not enforced on the root account; however active root account sessions do count towards the total number of current administrator sessions. A value of 0 turns session limits off. |
| <b>System protection</b>               |   |   |
| <b>Automated protection service</b>    | Whether the <a href="#">automated protection service</a> is active. Default is <i>Off</i> .   | After enabling the service you must go and configure the specific <a href="#">protection categories</a> .   |
| <b>Automatic discovery protection</b>  | Controls how management systems such as Cisco TMS can discover this Expressway.<br><i>Off</i> : automatic discovery is allowed.<br><i>On</i> : Cisco TMS has to be manually configured to discover this Expressway and must provide administrator account credentials.<br>Default is <i>Off</i> . | You must restart the system for any changes to take effect.   |
| <b>Web server configuration</b>        |   |   |
| <b>Redirect HTTP requests to HTTPS</b> | Determines whether HTTP requests are redirected to the HTTPS port. Default is <i>On</i> .   | HTTPS must also be enabled for access via HTTP to function.   |

| Field  | Description  | Usage tips  |
|--|--|---|
| <b>HTTP Strict Transport Security (HSTS)</b> | <p>Determines whether web browsers are instructed to only ever use a secure connection to access this server. Enabling this feature gives added protection against man-in-the-middle (MITM) attacks.</p> <p><i>On:</i> the Strict-Transport-Security header is sent with all responses from the web server, with a 1 year expiry time.</p> <p><i>Off:</i> the Strict-Transport-Security header is not sent, and browsers work as normal.</p> <p>Default is <i>On</i>.</p>  | See below for more information about HSTS.  |
| <b>Client certificate-based security</b>     | <p>Controls the level of security required to allow client systems (typically web browsers) to communicate with the Expressway over HTTPS.</p> <p><i>Not required:</i> the client system does not have to present any form of certificate.</p> <p><i>Certificate validation:</i> the client system must present a valid certificate that has been signed by a trusted certificate authority (CA). Note that a restart is required if you are changing from <i>Not required</i> to <i>Certificate validation</i>.</p> <p><i>Certificate-based authentication:</i> the client system must present a valid certificate that has been signed by a trusted CA and contains the client's authentication credentials.</p> <p>Default: <i>Not required</i></p> | <p><b>Important:</b></p> <p>Enabling <i>Certificate validation</i> means that your browser (the client system) can use the Expressway web interface only if it has a valid (in date and not revoked by a CRL) client certificate that is signed by a CA in the Expressway's trusted CA certificate list.</p> <p>Ensure your browser has a valid client certificate before enabling this feature. The procedure for uploading a certificate to your browser may vary depending on the browser type and you may need to restart your browser for the certificate to take effect.</p> <p>You can upload CA certificates on the <a href="#">Managing the trusted CA certificate list [p.223]</a> page, and test client certificates on the <a href="#">Testing client certificates [p.231]</a> page.</p> <p>Enabling <i>Certificate-based authentication</i> means that the standard login mechanism is no longer available. You can log in only if your browser certificate is valid and the credentials it provides have the appropriate authorization levels. You can configure how the Expressway extracts credentials from the browser certificate on the <a href="#">Certificate-based authentication configuration</a> page.</p> <p>This setting does not affect client verification of the Expressway's server certificate.</p> |

| Field   | Description  | Usage tips   |
|---|--|--|
| <b>Certificate revocation list (CRL) checking</b> | <p>Specifies whether HTTPS client certificates are checked against certificate revocation lists (CRLs).</p> <p><i>None</i>: no CRL checking is performed.</p> <p><i>Peer</i>: only the CRL associated with the CA that issued the client's certificate is checked.</p> <p><i>All</i>: all CRLs in the trusted certificate chain of the CA that issued the client's certificate are checked.</p> <p>Default: <i>All</i></p> | Only applies if <b>Client certificate-based security</b> is enabled. |
| <b>CRL inaccessibility fallback behavior</b>      | <p>Controls the revocation checking behavior if the revocation status cannot be established, for example if the revocation source cannot be contacted.</p> <p><i>Treat as revoked</i>: treat the certificate as revoked (and thus do not allow the TLS connection).</p> <p><i>Treat as not revoked</i>: treat the certificate as not revoked.</p> <p>Default: <i>Treat as not revoked</i></p>                              | Only applies if <b>Client certificate-based security</b> is enabled. |

By default, access via HTTPS and SSH is enabled. For optimum security, disable HTTPS and SSH and use the serial port to manage the system. Because access to the serial port allows the password to be reset, we recommend that you install the Expressway in a physically secure environment.

## HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) provides a mechanism where a web server forces a web browser to communicate with it using secure connections only.

As of August 2014, this mechanism is supported by the following browsers:

- Chrome, versions 4.0.211.0 and later
- Firefox, versions 4 and later

When HSTS is enabled, a browser that supports HSTS will:

- Automatically turn any insecure links to the website into secure links (for example, `http://example.com/page/` is modified to `https://example.com/page/` before accessing the server).
- Only allow access to the server if the connection is secure (for example, the server's TLS certificate is valid, trusted and not expired).

Browsers that do not support HSTS will ignore the Strict-Transport-Security header and work as before. They will still be able to access the server.

Compliant browsers only respect Strict-Transport-Security headers if they access the server through its fully qualified name (rather than its IP address).

## Configuring SNMP settings

The **SNMP** page (**System > SNMP**) is used to configure the Expressway's SNMP settings.

Tools such as Cisco TelePresence Management Suite (Cisco TMS) or HP OpenView may act as SNMP Network Management Systems (NMS). They allow you to monitor your network devices, including the Expressway, for conditions that might require administrative attention.

The Expressway supports the most basic MIB-II tree (.1.3.6.1.2.1) as defined in [RFC 1213](#).

The information made available by the Expressway includes the following:

- system uptime
- system name
- location
- contact
- interfaces
- disk space, memory, and other machine-specific statistics

By default, SNMP is *Disabled*, therefore to allow the Expressway to be monitored by an SNMP NMS (including Cisco TMS), you must select an alternative **SNMP mode**. The configurable options are:

| Field                 | Description   | Usage tips   |
|-----------------------|---|--|
| <b>SNMP mode</b>      | Controls the level of SNMP support.<br><i>Disabled</i> : no SNMP support.<br><i>v3 secure SNMP</i> : supports authentication and encryption.<br><i>v3 plus TMS support</i> : secure SNMPv3 plus non-secure access to OID 1.3.6.1.2.1.1.2.0 only.<br><i>v2c</i> : non-secure community-based SNMP. | If you want to use secure SNMPv3 but you also use Cisco TMS as your external manager, you must select <i>v3 plus TMS support</i> . |
| <b>Description</b>    | Custom description of the system as viewed by SNMP. The default is to have no custom description (empty field).   | When you leave this field empty, the system uses its default SNMP description.   |
| <b>Community name</b> | The Expressway's SNMP community name. The default is <i>public</i> .  | Only applies when using <i>v2c</i> or <i>v3 plus TMS support</i> .   |
| <b>System contact</b> | The name of the person who can be contacted regarding issues with the Expressway. The default is <i>Administrator</i> .   | The <b>System contact</b> and <b>Location</b> are used for reference purposes by administrators when following up on queries.      |
| <b>Location</b>       | Specifies the physical location of the Expressway.  |  |
| <b>Username</b>       | The Expressway's SNMP username, used to identify this SNMP agent to the SNMP manager.   | Only applies when using <i>v3 secure SNMP</i> or <i>v3 plus TMS support</i>  |

**v3 Authentication** settings (only applicable to SNMPv3)

| Field  | Description  | Usage tips                     |
|--|--|--------------------------------|
| <b>Authentication mode</b>                             | Enables or disables SNMPv3 authentication.   |                                |
| <b>Type</b>  | The algorithm used to hash authentication credentials.<br><i>SHA</i> : Secure Hash Algorithm.<br><i>MD5</i> : Message-Digest algorithm 5.<br>The default is <i>SHA</i> .   |                                |
| <b>Password</b>  | The password used to encrypt authentication credentials.   | Must be at least 8 characters. |
| <b>v3 Privacy settings</b> (only applicable to SNMPv3) |  |                                |
| <b>Privacy mode</b>                                    | Enables or disables SNMPv3 encryption.   |                                |
| <b>Type</b>  | The security model used to encrypt messages.<br><i>DES</i> : Data Encryption Standard 56-bit encryption.<br><i>AES</i> : Advanced Encryption Standard 128-bit encryption.<br>If available, the default and recommended setting is <i>AES</i> . |                                |
| <b>Password</b>  | The password used to encrypt messages.   | Must be at least 8 characters. |

The Expressway does not support SNMP traps or SNMP sets, therefore it cannot be managed via SNMP.

**Note:** SNMP is disabled by default, because of the potentially sensitive nature of the information involved. Do not enable SNMP on a Expressway on the public internet or in any other environment where you do not want to expose internal system information.

## Configuring time settings

The **Time** page (**System > Time**) is used to configure the Expressway's NTP servers and to specify the local time zone.

An NTP server is a remote server with which the Expressway synchronizes in order to ensure its time is accurate. The NTP server provides the Expressway with UTC time.

Accurate time is necessary for correct system operation.

### Configuring the NTP servers

To configure the Expressway with one or more NTP servers to be used when synchronizing system time, enter the **Address** of up to five servers in one of the following formats, depending on the system's DNS settings (you can check these settings on the **DNS** page, **System > DNS**):

- if there are no **DNS servers** configured, you must use an IP address for the NTP server
- if there are one or more **DNS servers** configured, you can use an FQDN or IP address for the NTP server



- if there is a DNS **Domain name** configured in addition to one or more **DNS servers**, you can use the server name, FQDN or IP address for the NTP server

Three of the **Address** fields default to NTP servers provided by Cisco.

You can configure the **Authentication** method used by the Expressway when connecting to an NTP server. Use one of the following options for each NTP server connection:

| Authentication method | Description   |
|-----------------------|---|
| <i>Disabled</i>       | No authentication is used.  |
| <i>Symmetric key</i>  | Symmetric key authentication. When using this method a <b>Key ID</b> , <b>Hash</b> method and <b>Pass phrase</b> must be specified. The values entered here must match exactly the equivalent settings on the NTP server. You can use the same symmetric key settings across multiple NTP servers. However, if you want to configure each server with a different pass phrase, you must also ensure that each server has a unique key ID. |
| <i>Private key</i>    | Private key authentication. This method uses an automatically generated private key with which to authenticate messages sent to the NTP server.   |

### Displaying NTP status information

The synchronization status between the NTP server and the Expressway is shown in the **Status** area as follows:

- *Starting*: the NTP service is starting.
- *Synchronized*: the Expressway has successfully obtained accurate system time from an NTP server.
- *Unsynchronized*: the Expressway is unable to obtain accurate system time from an NTP server.
- *Down*: the Expressway's NTP client is not running.
- *Reject*: the NTP service is not accepting NTP responses.

Note that updates may take a few minutes to be displayed in the status table.

Other status information available includes:

| Field          | Description   |
|----------------|---|
| NTP server     | The actual NTP server that has responded to the request. This may be different to the NTP server in the NTP server address field.   |
| Condition      | Gives a relative ranking of each NTP server. All servers that are providing accurate time are given a status of <i>Candidate</i> ; of those, the server that the Expressway considers to be providing the most accurate time and is therefore using shows a status of <i>sys.peer</i> . |
| Flash          | A code giving information about the server's status. <i>00 ok</i> means there are no issues. See the <a href="#">Flash status word reference table [p.388]</a> for a complete list of codes.  |
| Authentication | Indicates the status of the current authentication method. One of <i>ok</i> , <i>bad</i> or <i>none</i> . <i>none</i> is specified when the <b>Authentication</b> method is <i>Disabled</i> .   |
| Event          | Shows the last event as determined by NTP (for example <i>reachable</i> or <i>sys.peer</i> )  |

| Field        | Description   |
|--------------|---|
| Reachability | Indicates the results of the 8 most recent contact attempts between the Expressway and the NTP server, with a tick indicating success and a cross indicating failure. The result of the most recent attempt is shown on the far right.<br><br>Each time the NTP configuration is changed, the NTP client is restarted and the <b>Reachability</b> field will revert to all crosses apart from the far right indicator which will show the result of the first connection attempt after the restart. However, the NTP server may have remained contactable during the restart process. |
| Offset       | The difference between the NTP server's time and the Expressway's time.   |
| Delay        | The network delay between the NTP server and the Expressway.  |
| Stratum      | The degree of separation between the Expressway and a reference clock. 1 indicates that the NTP server is a reference clock.  |
| Ref ID       | A code identifying the reference clock.   |
| Ref time     | The last time that the NTP server communicated with the reference clock.  |

For definitions of the remaining fields on this page, and for further information about NTP, see [Network Time Protocol website](#).

## Expressway time display and time zone

Local time is used throughout the web interface. It is shown in the system information bar at the bottom of the screen and is used to set the timestamp that appears at the start of each line in the Event Log.

Note that UTC timestamps are included at the end of each entry in the Event Log.

Internally, the Expressway maintains its system time in UTC. It is based on the Expressway's operating system time, which is synchronized using an NTP server if one is configured. If no NTP servers are configured, the Expressway uses its own operating system time to determine the time and date.

Specifying your local **Time zone** lets the Expressway determine the local time where the system is located. It does this by offsetting UTC time by the number of hours (or fractions of hours) associated with the selected time zone. It also adjusts the local time to account for summer time (also known as daylight saving time) when appropriate.

## Configuring the Login page

The **Login page configuration** page (**System > Login page**) is used to specify a message and image to appear on the login page.

The **Welcome message title** and **text** appears to administrators when attempting to log in using the CLI or the web interface.

You can upload an image that will appear above the welcome message on the login page when using the web interface.

- Supported image file formats are JPG, GIF and PNG.
- Images larger than 200x200 pixels will be scaled down.

Note that this feature is not configurable using the CLI.

## Configuring external manager settings

The **External manager** page (**System > External manager**) is used to configure the Expressway's connection to an external management system.

An external manager is a remote system, such as the Cisco TelePresence Management Suite (Cisco TMS), used to monitor events occurring on the Expressway, for example call attempts, connections and disconnections, and as a place for where the Expressway can send alarm information. The use of an external manager is optional.

| Field                                | Description   | Usage tips  |
|--------------------------------------|---|---|
| <b>Address and path</b>              | To use an external manager, you must configure the Expressway with the IP address or host name and path of the external manager to be used. | If you are using Cisco TMS as your external manager, use the default path of <b>tms/public/external/management/SystemManagementService.asmx</b> .   |
| <b>Protocol</b>                      | Determines whether communications with the external manager are over <i>HTTP</i> or <i>HTTPS</i> . The default is <i>HTTPS</i> .            |   |
| <b>Certificate verification mode</b> | Controls whether the certificate presented by the external manager is verified.   | If you enable verification, you must also add the certificate of the issuer of the external manager's certificate to the file containing the Expressway's trusted CA certificates. This is done from the <a href="#">Managing the trusted CA certificate list [p.223]</a> page ( <b>Maintenance &gt; Security certificates &gt; Trusted CA certificate</b> ). |

Note that:

- the Expressway will continue to operate without loss of service if its connection to Cisco TMS fails. This applies even if the Expressways are clustered. No specific actions are required as the Expressway and Cisco TMS will automatically start communicating with each other again after the connection is re-established.
- Cisco TMS identifies the Expressway as a "TANDBERG VCS".

# Firewall traversal

---

This section describes how to configure your Expressway-C and Expressway-E in order to traverse firewalls.

|   |    |
|---|----|
| About firewall traversal .....                  | 45 |
| Configuring a traversal client and server ..... | 49 |
| Configuring ports for firewall traversal .....  | 50 |
| Firewall traversal and authentication .....     | 54 |
| About ICE and TURN services .....               | 55 |

# About firewall traversal

The purpose of a firewall is to control the IP traffic entering your network. Firewalls will generally block unsolicited incoming requests, meaning that any calls originating from outside your network will be prevented. However, firewalls can be configured to allow outgoing requests to certain trusted destinations, and to allow responses from those destinations. This principle is used by Cisco's Expressway technology to enable secure traversal of any firewall.

## The Expressway solution

The Expressway solution consists of:

- An Expressway-E located outside the firewall on the public network or in the DMZ, which acts as the firewall traversal server.
- An Expressway-C or other traversal-enabled endpoint located in a private network, which acts as the firewall traversal client.

The two systems work together to create an environment where all connections between the two are outbound, i.e. established from the client to the server, and thus able to successfully traverse the firewall.

We recommend that both the Expressway-E and the Expressway-C run the same software version.

## How does it work?

The traversal client constantly maintains a connection via the firewall to a designated port on the traversal server. This connection is kept alive by the client sending packets at regular intervals to the server. When the traversal server receives an incoming call for the traversal client, it uses this existing connection to send an incoming call request to the client. The client then initiates the necessary outbound connections required for the call media and/or signaling.

This process ensures that from the firewall's point of view, all connections are initiated from the traversal client inside the firewall out to the traversal server.

For firewall traversal to function correctly, the Expressway-E must have one traversal server zone configured on it for each client system that is connecting to it. Likewise, each Expressway client must have one traversal client zone configured on it for each server that it is connecting to.

The ports and protocols configured for each pair of client-server zones must be the same. See the [Configuring a traversal client and server \[p.49\]](#) for a summary of the required configuration on each system. Because the Expressway-E listens for connections from the client on a specific port, you are recommended to create the traversal server zone on the Expressway-E before you create the traversal client zone on the Expressway-C.

Note that the traversal client and the traversal server must both be Expressway systems (neither can be a Cisco VCS).

## H.323 firewall traversal protocols

The Expressway supports two different firewall traversal protocols for H.323: Assent and H.460.18/H.460.19.

- Assent is Cisco’s proprietary protocol.
- H.460.18 and H.460.19 are ITU standards which define protocols for the firewall traversal of signaling and media respectively. These standards are based on the original Assent protocol.

A traversal server and traversal client must use the same protocol in order to communicate. The two protocols each use a different range of ports.

## SIP firewall traversal protocols

The Expressway supports the Assent protocol for SIP firewall traversal of media.

The signaling is traversed through a TCP/TLS connection established from the client to the server.

## Media demultiplexing

The Expressway-E uses media demultiplexing in the following call scenarios:

- Any H.323 or SIP call leg to/from an Expressway-C through a traversal zone configured to use Assent.
- Any H.323 call leg to/from an Expressway-C through a traversal server zone configured to use H460.19 in demultiplexing mode
- H.323 call legs between an Expressway-E and an Assent or H.460.19 enabled endpoint

The Expressway-E uses non-demultiplexed media for call legs directly to/from SIP endpoints (that is endpoints which do not support Assent or H.460.19), or if the traversal server zone is not configured to use H.460.19 in demultiplexing mode.

Media demultiplexing ports on the Expressway-E are allocated from the general range of **traversal media ports**. This applies to all RTP/RTCP media, regardless of whether it is H.323 or SIP. 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).

For example, in a SIP call from within an enterprise to an endpoint at home through an Expressway-C/Expressway-E pair, the only demultiplexing that would occur would be on the Expressway-E ports facing the Expressway-C:



However, an H.323 call from within an enterprise to an Assent capable H.323 endpoint at home through the same Expressway-C/Expressway-E would perform demultiplexing on both sides of the Expressway-E:

| Enterprise endpoint | Expressway-C |             | Expressway-E |         | Home endpoint |
|---------------------|--------------|-------------|--------------|---------|---------------|
|                     | Non-demuxed  | Non-demuxed | Demuxed      | Demuxed |               |
| RTP ports           | 36002        | 36004       | 36000        | 36000   |               |
| RTCP ports          | 36003        | 36005       | 36001        | 36001   |               |

If the Expressway-E has Advanced Networking, it will still use the same port numbers as described above, but they will be assigned to the internal and external IP addresses.

## Firewall traversal configuration overview

This section provides an overview to how the Expressway can act as a traversal server or as a traversal client.

### Expressway as a firewall traversal client

The Expressway can act as a firewall traversal client on behalf of any systems that are neighbored with it. To act as a firewall traversal client, the Expressway must be configured with information about the systems that will act as its firewall traversal server.

You do this by adding a traversal client zone on the Expressway-C (**Configuration > Zones > Zones**) and configuring it with the details of the Expressway-E traversal server. See [Configuring traversal client zones \[p.122\]](#) for more information. You can create more than one traversal client zone if you want to connect to multiple traversal servers.

### Expressway as a firewall traversal server

The Expressway-E has all the functionality of an Expressway-C. However, its main feature is that it can act as a firewall traversal server for other Cisco systems. It can also provide TURN relay services to ICE-enabled endpoints.

#### Configuring traversal server zones

For the Expressway-E to act as a firewall traversal server for Cisco systems, you must create a traversal server zone on the Expressway-E (**Configuration > Zones > Zones**) and configure it with the details of the traversal client. See [Configuring traversal server zones \[p.124\]](#) for more information.

You must create a separate traversal server zone for every system that is its traversal client.

#### Configuring other traversal server features

- To enable TURN relay services and find out more about ICE, see [About ICE and TURN services \[p.55\]](#).
- To reconfigure the default ports used by the Expressway-E, see [Configuring ports for firewall traversal \[p.50\]](#).

### Firewall traversal and Advanced Networking

The Advanced Networking option key enables the LAN 2 interface on the Expressway-E (the option is not available on an Expressway-C). The LAN 2 interface is used in situations where the Expressway-E is

located in a DMZ that consists of two separate networks - an inner DMZ and an outer DMZ - and your network is configured to prevent direct communication between the two.

With the LAN 2 interface enabled, you can configure the Expressway with two separate IP addresses, one for each network in the DMZ. Your Expressway then acts as a proxy server between the two networks, allowing calls to pass between the internal and outer firewalls that make up your DMZ.

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.



# Configuring a traversal client and server

The basic steps in configuring a traversal client and server are as follows:

| Step | Description  |
|------|--|
| 1    | On the Expressway-E, create a traversal server zone (this represents the incoming connection from the Expressway-C). In the <b>Username</b> field, enter the Expressway-C's authentication username. |
| 2    | On the Expressway-E, add the Expressway-C's authentication username and password as credentials into the local authentication database.  |
| 3    | On the Expressway-C, create a traversal client zone (this represents the connection to the Expressway-E).  |
| 4    | Enter the same authentication <b>Username</b> and <b>Password</b> as specified on the Expressway-E.  |
| 5    | Configure all the modes and ports in the H.323 and SIP protocol sections to match identically those of the traversal server zone on the Expressway-E.  |
| 6    | Enter the Expressway-E's IP address or FQDN in the <b>Peer 1 address</b> field.  |

The image displays two configuration panels side-by-side, illustrating the steps for setting up a traversal client and server.

**VCS Expressway (server) - Create zone 1:**

- Configuration:** Name: to Traversal Client 1; Type: Traversal server; Hop count: 15.
- Connection credentials:** Username: client\_username; Password: Add/Edit local authentication database.
- H.323:** Mode: On; Protocol: Assent; Port: 6001; H.460.19 demultiplexing mode: Off.
- SIP:** Mode: On; Port: 7001; Transport: TLS; TLS verify mode: Off; Accept proxied registrations: Allow; Poison mode: Off.

**VCS Control (client) - Create zone 5:**

- Configuration:** Name: to Traversal Server; Type: Traversal client; Hop count: 15.
- Connection credentials:** Username: client\_username; Password: [Redacted].
- H.323:** Mode: On; Protocol: Assent; Port: 6001.
- SIP:** Mode: On; Port: 7001; Transport: TLS; TLS verify mode: Off; Accept proxied registrations: Allow; Poison mode: Off.
- Location:** Peer 1 address: traversalserver@example.com.

**Create credential 2:**

- Configuration:** Name: client\_username; Password: [Redacted].

Red arrows indicate the flow of configuration data: from the 'Create credential' panel to the 'Connection credentials' field of the 'VCS Control (client)' zone, and from the 'Connection credentials' field of the 'VCS Expressway (server)' zone to the 'Connection credentials' field of the 'VCS Control (client)' zone.

# Configuring ports for firewall traversal

Ports play a vital part in firewall traversal configuration. The correct ports must be set on the Expressway-E, traversal client and firewall in order for connections to be permitted.

Ports are initially configured on the Expressway-E by the Expressway-E administrator. The firewall administrator and the traversal client administrator should then be notified of the ports, and they must configure their systems to connect to these specific ports on the server. The only port configuration required on the traversal client is the range of ports it uses for outgoing connections; the firewall administrator may need to know this information so that if necessary they can configure the firewall to allow outgoing connections from those ports.

The [Port usage \[p.246\]](#) pages (under **Maintenance > Tools > Port usage**) list all the IP ports that are being used on the Expressway, both inbound and outbound. This information can be provided to your firewall administrator so that the firewall can be configured appropriately.

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.

The Expressway solution works as follows:

1. Each traversal client connects via the firewall to a unique port on the Expressway-E.
2. The server identifies each client by the port on which it receives the connection, and the authentication credentials provided by the client.
3. After the connection has been established, the client regularly sends a probe to the Expressway-E to keep the connection alive.
4. When the Expressway-E receives an incoming call for the client, it uses this initial connection to send an incoming call request to the client.
5. The client then initiates one or more outbound connections. The destination ports used for these connections differ for signaling and/or media, and depend on the protocol being used (see the following sections for more details).

## Configuring the firewall

For Expressway firewall traversal to function correctly, your firewall must be configured to:

- allow initial outbound traffic from the client to the ports being used by the Expressway-E
- allow return traffic from those ports on the Expressway-E back to the originating client

---

**Note:** we recommend that you turn off any H.323 and SIP protocol support on the firewall: these are not needed in conjunction with the Expressway solution and may interfere with its operation.

---

## Configuring traversal server ports

The Expressway-E has specific listening ports used for firewall traversal. Rules must be set on your firewall to allow connections to these ports. In most cases the default ports should be used. However, you have the option to change these ports if necessary by going to the **Ports** page (**Configuration > Traversal > Ports**).

The configurable ports for signaling are:

- **H.323 Assent call signaling port**; default is 2776
- **H.323 H.460.18 call signaling port**; default is 2777

## RTP and RTCP media demultiplexing ports

The port configuration options depend upon the [type of appliance or VM](#):

- Small/Medium systems: 1 pair of RTP and RTCP media demultiplexing ports are used. They can either be explicitly specified or they can be allocated from the start of the general range of traversal media ports.
- Large systems: 6 pairs of RTP and RTCP media demultiplexing ports are used. They are always allocated from the start of the traversal media ports range.

## Configuring ports for connections from traversal clients

Each traversal server zone specifies an H.323 port and a SIP port to use for the initial connection from the client. Each time you configure a new traversal server zone on the Expressway-E, you are allocated default port numbers for these connections:

- H.323 ports start at UDP/6001 and increment by 1 for every new traversal server zone.
- SIP ports start at TCP/7001 and increment by 1 for every new traversal server zone.

You can change these default ports if necessary but you must ensure that the ports are unique for each traversal server zone. After the H.323 and SIP ports have been set on the Expressway-E, matching ports must be configured on the corresponding traversal client. Note that:

- The default port used for the initial connections from MXP endpoints is the same as that used for standard RAS messages, that is UDP/1719. While you can change this port on the Expressway-E, most endpoints will not support connections to ports other than UDP/1719, therefore we recommend that you leave this as the default.
- You must allow outbound connections through your firewall to each of the unique SIP and H.323 ports that are configured on each of the Expressway-E's traversal server zones.

The following table shows the default ports used for connections to the Expressway-E.

Table 2: Default traversal port connections

| Protocol    | Call signaling   | Media  |
|-------------|--|--|
| Assent      | TCP/2776: listening port for H.225 and H.245 protocols                                     | The RTP and RTCP media demultiplexing ports in Large system are always allocated from the start of the general range of traversal media ports (UDP/36000-36011*). In Small/Medium systems the media demultiplexing ports can either be explicitly specified or they can be allocated from the start of the traversal media ports range.  |
| H.460.18/19 | TCP/1720: listening port for H.225 protocol<br>TCP/2777: listening port for H.245 protocol | The RTP and RTCP media demultiplexing ports in Large systems are always allocated from the start of the general range of traversal media ports (UDP/36000-36011*). In Small/Medium systems the media demultiplexing ports can either be explicitly specified or they can be allocated from the start of the traversal media ports range.<br>RTP and RTCP media non-demultiplexing ports are allocated from the remainder of the traversal media ports range: UDP/36002-59999*. |

Table 2: Default traversal port connections (continued)

|     |  |  |
|-----|--|--|
| SIP | SIP call signaling uses the same port as used by the initial connection between the client and server. | Where the traversal client is an Expressway, SIP media uses Assent to traverse the firewall. |
|-----|--|--|

\* 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).

The call signaling ports are configured via [Configuration > Traversal > Ports](#). The traversal media port range is configured via [Configuration > Traversal Subzone](#).

## Configuring TURN ports

The Expressway-E can be enabled to provide [TURN services](#) (Traversal Using Relays around NAT) which can be used by ICE-enabled SIP endpoints.

The ports used by these services are configurable via [Configuration > Traversal > TURN](#).

The ICE clients on each of the SIP endpoints must be able to discover these ports, either by using SRV records in DNS or by direct configuration.

## Configuring ports for connections out to the public internet

In situations where the Expressway-E is attempting to connect to an endpoint on the public internet, you will not know the exact ports on the endpoint to which the connection will be made. This is because the ports to be used are determined by the endpoint and advised to the Expressway-E only after the server has located the endpoint on the public internet. This may cause problems if your Expressway-E is located within a DMZ (where there is a firewall between the Expressway-E and the public internet) as you will not be able to specify in advance any rules that will allow you to connect out to the endpoint's ports.

You can however specify the ports on the Expressway-E that are used for calls to and from endpoints on the public internet so that your firewall administrator can allow connections via these ports. The ports that can be configured for this purpose are:

Table 3: Port connections out to the public internet

| H.323                      | SIP  | TURN                                      |
|----------------------------|--|---|
| TCP/1720: signaling        | TCP/5061: signaling  | UDP/3478 (default): TURN services<br>**   |
| UDP/1719: signaling        | UDP/5060 (default): signaling                                  |   |
| UDP/36000-59999: media*    | UDP/36000-59999: media*  | UDP/24000-29999 (default range):<br>media |
| TCP/15000-19999: signaling | TCP: a temporary port in the range<br>25000-29999 is allocated |   |

\* 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).

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

# Firewall traversal and authentication

The Expressway-E allows only authenticated client systems to use it as a traversal server.

Upon receiving the initial connection request from the traversal client, the Expressway-E asks the client to authenticate itself by providing its authentication credentials. The Expressway-E then looks up the client's credentials in its own authentication database. If a match is found, the Expressway-E accepts the request from the client.

The settings used for authentication depend on the type of traversal client:

| Traversal client   | Expressway-E traversal server   |
|--|---|
| <p><b>Expressway-C</b></p> <p>The Expressway client provides its <b>Username</b> and <b>Password</b>. These are set on the traversal client zone by using <a href="#">Configuration &gt; Zones &gt; Zones &gt; Edit zone</a>, in the <a href="#">Connection credentials</a> section.</p> | <p>The traversal server zone for the Expressway client must be configured with the client's authentication <b>Username</b>. This is set on the Expressway-E by using <a href="#">Configuration &gt; Zones &gt; Zones &gt; Edit zone</a>, in the <a href="#">Connection credentials</a> section.</p> <p>There must also be an entry in the Expressway-E's authentication database with the corresponding client username and password.</p> |
| <p><b>Endpoint</b></p> <p>The endpoint client provides its <b>Authentication ID</b> and <b>Authentication Password</b>.</p>  | <p>There must be an entry in the Expressway-E's authentication database with the corresponding client username and password.</p>  |

Note that all Expressway traversal clients must authenticate with the Expressway-E.

## Authentication and NTP

All Expressway traversal clients that support H.323 must authenticate with the Expressway-E. The authentication process makes use of timestamps and requires that each system uses an accurate system time. The system time on an Expressway is provided by a remote NTP server. Therefore, for firewall traversal to work, all systems involved must be configured with details of an [NTP server](#).

# About ICE and TURN services

## About ICE

ICE (Interactive Connectivity Establishment) provides a mechanism for SIP client NAT traversal. ICE is not a protocol, but a framework which pulls together a number of different techniques such as TURN and STUN.

It allows endpoints (clients) residing behind NAT devices to discover paths through which they can pass media, verify peer-to-peer connectivity via each of these paths and then select the optimum media connection path. The available paths typically depend on any inbound and outbound connection restrictions that have been configured on the NAT device. Such behavior is described in [RFC 4787](#).

An example usage of ICE is two home workers communicating via the internet. If the two endpoints can communicate via ICE the Expressway-E may (depending on how the NAT devices are configured) only need to take the signaling and not take the media. If the initiating ICE client attempts to call a non-ICE client, the call set-up process reverts to a conventional SIP call requiring NAT traversal via media latching where the Expressway also takes the media.

For more information about ICE, see [RFC 5245](#).

## About TURN

TURN (Traversal Using Relays around NAT) services are relay extensions to the STUN network protocol that enable a SIP or H.323 client to communicate via UDP or TCP from behind a NAT device.

For more information about TURN see [RFC 5766](#), and for detailed information about the base STUN protocol, see [RFC 5389](#).

Each ICE client requests the TURN server to allocate relays for the media components of the call. A relay is required for each component in the media stream between each client.

After the relays are allocated, each ICE client has 3 potential connection paths (addresses) through which it can send and receive media:

- its host address which is behind the NAT device (and thus not reachable from endpoints on the other side of the NAT)
- its publicly-accessible address on the NAT device
- a relay address on the TURN server

The endpoints then decide, by performing connectivity checks through ICE, how they are going to communicate. Depending upon how the NAT devices are configured, the endpoints may be able to communicate between their public-facing addresses on the NAT devices or they may have to relay the media via the TURN server. If both endpoints are behind the same NAT device they can send media directly between themselves using their internal host addresses.

After the media route has been selected, the TURN relay allocations are released if the chosen connection paths do not involve routing via the TURN server. Note that the signaling always goes via the Expressway, regardless of the final media communication path chosen by the endpoints.

### Capabilities and limitations

- [Small/Medium](#) systems support up to 1800 relay allocations. This is typically enough to support 100 calls but does depend on the network topology and the number of media stream components used for the call (for

example, some calls may use Duo Video, or other calls might be audio only).

- A [Large](#) system supports up to 6000 relays, spread evenly across 6 ports where each port is limited to handling 1000 relays. This limit is not strictly enforced, so we recommend adding an SRV record for each port to enable round robin.
- Clustered Expressways: if the requested TURN server's relays are fully allocated the server will respond to the requesting client with the details of an alternative server in the cluster (the TURN server currently with the most available resources).
- The Expressway's TURN services are supported over single and dual network interfaces (via the Advanced Networking option). For dual network interfaces, the TURN server listens on both interfaces but relays are allocated only on the Expressway's externally facing LAN interface.
- Microsoft ICE (which is not standards-based) is not supported by the Expressway-E's TURN server; to enable communications between the Expressway and Microsoft Lync clients that are registered through a Microsoft Edge Server you need to use the [B2BUA for Microsoft Lync](#).
- The TURN server does not support bandwidth requests. Traversal zone bandwidth limits do not apply.
- The Expressway-E TURN server supports TURN media over TCP and UDP. Configuration of the supported protocols is available only through the CLI command `xConfiguration Traversal Server TURN ProtocolMode`.
- The Expressway-E TURN server supports UDP relays over TCP; it does not currently support TCP relays.

## Configuring TURN services

TURN relay services are only available on the Expressway-E. To use [TURN services](#) you need the TURN Relay option key (this controls the number of TURN relays that can be simultaneously allocated by the TURN server).

The **TURN** page ([Configuration > Traversal > TURN](#)) is used to configure the Expressway-E's TURN settings.

The configurable options are:

| Field                | Description  | Usage tips |
|----------------------|--|------------|
| <b>TURN services</b> | Determines whether the Expressway offers TURN services to traversal clients. |            |



| Field                               | Description  | Usage tips  |
|-------------------------------------|--|---|
| <b>TURN requests port</b>           | <p>The listening port for TURN requests. The default is 3478.</p> <p>On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483.</p> | <p>To allow endpoints such as Jabber Video to discover TURN services, you need to set up DNS SRV records for <code>_turn._udp.</code> and <code>_turn._tcp</code> (either for the single port, or range of ports as appropriate).</p> <p>If you need to change the <b>TURN requests port</b> (o range, for Large systems) while the <b>TURN services</b> are already <i>On</i>:</p> <ol style="list-style-type: none"> <li>1. Change <b>TURN services</b> to <i>Off</i> and <b>Save</b></li> <li>2. Edit the port number/range</li> <li>3. Change <b>TURN services</b> to <i>On</i> and <b>Save</b></li> </ol> <p>This is because changes to the port numbers do not come into effect until the <b>TURN services</b> are restarted.</p> |
| <b>Authentication realm</b>         | This is the realm sent by the server in its authentication challenges.   | Ensure that the client's credentials are stored in the local authentication database.   |
| <b>Media port range start / end</b> | <p>The lower and upper port in the range used for the allocation of TURN relays.</p> <p>The default TURN relay media port range is 24000 – 29999.</p>                                  |   |

### TURN server status

A summary of the TURN server status is displayed at the bottom of the **TURN** page. When the TURN server is active, the summary also displays the number of active TURN clients and the number of active relays.

Click on the active relay links to access the [TURN relay usage](#) page, which lists all the currently active TURN relays on the Expressway. You can also review further details of each TURN relay including permissions, channel bindings and counters.

# Unified Communications

---

This section describes how to configure the Expressway-C and Expressway-E for Unified Communications functionality, a core part of the Cisco Collaboration Edge Architecture:

|  |    |
|--|----|
| Unified Communications prerequisites ..... | 59 |
| Mobile and remote access .....             | 64 |
| External XMPP federation .....             | 81 |
| Cisco Jabber Guest .....                   | 92 |

# Unified Communications prerequisites

## Configuring a secure traversal zone connection for Unified Communications

To support Unified Communications features (such as mobile and remote access or Jabber Guest), there must be a Unified Communications traversal zone connection between the Expressway-C and the Expressway-E. This involves:

- Installing suitable security certificates on the Expressway-C and the Expressway-E.
- Configuring a Unified Communications traversal zone between the Expressway-C and the Expressway-E

---

**Note:** You should configure only one *Unified Communications traversal zone* per Expressway.

---

### Installing Expressway security certificates

You must set up trust between the Expressway-C and the Expressway-E:

1. Install a suitable server certificate on both the Expressway-C and the Expressway-E.
  - The certificate must include the **Client Authentication** extension. The system will not allow you to upload a server certificate without this extension when Unified Communications features have been enabled.
  - The Expressway includes a built-in mechanism to generate a certificate signing request (CSR) and is the recommended method for generating a CSR:
    - Ensure that the CA that signs the request does not strip out the client authentication extension.
    - The generated CSR includes the client authentication request and any relevant subject alternate names for the Unified Communications features that have been enabled (see [Server certificate requirements for Unified Communications \[p.61\]](#) if appropriate).
  - To generate a CSR and /or to upload a server certificate to the Expressway, go to **Maintenance > Security certificates > Server certificate**. You must restart the Expressway for the new server certificate to take effect.
2. Install on both Expressways the trusted Certificate Authority (CA) certificates of the authority that signed the Expressway's server certificates.

There are additional trust requirements, depending on the Unified Communications features being deployed.

For mobile and remote access deployments:

  - The Expressway-C must trust the Unified CM and IM&P tomcat certificate.
  - If appropriate, both the Expressway-C and the Expressway-E must trust the authority that signed the endpoints' certificates.

For Jabber Guest deployments:

  - When the Jabber Guest server is installed, it uses a self-signed certificate by default. However, you can install a certificate that is signed by a trusted certificate authority. You must install on the Expressway-C either the self-signed certificate of the Jabber Guest server, or the trusted CA certificates of the authority that signed the Jabber Guest server's certificate.

To upload trusted Certificate Authority (CA) certificates to the Expressway, go to **Maintenance > Security certificates > Trusted CA certificate**. You must restart the Expressway for the new trusted CA certificate to take effect.

See [Certificate Creation and Use With Expressway Deployment Guide](#) for full information about how to create and upload the Expressway's server certificate and how to upload a list of trusted certificate authorities.

## Configuring encrypted Expressway traversal zones

To support Unified Communications features via a secure traversal zone connection between the Expressway-C and the Expressway-E:

- The Expressway-C and Expressway-E must be configured with a zone of type *Unified Communications traversal*. 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*.
- Both Expressways must trust each other's server certificate. As each Expressway acts both as a client and as a server you must ensure that each Expressway's certificate is valid both as a client and as a server.
- If an H.323 or a non-encrypted connection is also required, a separate pair of traversal zones must be configured.

To set up a secure traversal zone, configure your Expressway-C and Expressway-E as follows:

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.
3. Configure the fields as follows (leave all other fields with default values):

|                                       | Expressway-C                            | Expressway-E  |
|---------------------------------------|---|---|
| Name                                  | "Traversal zone" for example            | "Traversal zone" for example  |
| Type                                  | <i>Unified Communications traversal</i> | <i>Unified Communications traversal</i>   |
| <b>Connection credentials</b> section |   |   |
| Username                              | "exampleauth" for example               | "exampleauth" for example   |
| Password                              | "ex4mpl3.c0m" for example               | Click <b>Add/Edit local authentication database</b> , then in the popup dialog click <b>New</b> and enter the <b>Name</b> ("exampleauth") and <b>Password</b> ("ex4mpl3.c0m") and click <b>Create credential</b> .  |
| <b>SIP</b> section                    |   |   |
| Port                                  | 7001                                    | 7001  |
| TLS verify subject name               | Not applicable                          | Enter the name to look for in the traversal client's certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). If there is a cluster of traversal clients, specify the cluster name here and ensure that it is included in each client's certificate. |
| <b>Location</b> section               |   |   |

|                    | Expressway-C  | Expressway-E   |
|--------------------|---|----------------|
| Peer 1 address     | Enter the FQDN of the Expressway-E.<br><br>Note that if you use an IP address (not recommended), that address must be present in the Expressway-E server certificate. | Not applicable |
| Peer 2...6 address | Enter the FQDNs of additional peers if it is a cluster of Expressway-Es.  | Not applicable |

- Click **Create zone**.

## Server certificate requirements for Unified Communications

### Cisco Unified Communications Manager certificates

The two Cisco Unified Communications Manager certificates that are significant for Mobile and Remote Access are the *CallManager* certificate and the *tomcat* certificate. These are automatically installed on the Cisco Unified Communications Manager and by default they are self-signed and have the same common name (CN).

We recommend using externally-signed certificates for best end-to-end security between external endpoints and internal endpoints. However, if you do use self-signed certificates, the two certificates must have different common names. This is because the Expressway does not allow two self-signed certificates with the same CN. If the *CallManager* and *tomcat* self-signed certs have the same CN in the Expressway's trusted CA list, then it can only trust one of them. This means that either secure HTTP or secure SIP, between Expressway-C and Cisco Unified Communications Manager, will fail.

### Expressway certificates

The Expressway certificate signing request (CSR) tool prompts for and incorporates the relevant subject alternate name (SAN) entries as appropriate for the Unified Communications features that are supported on that Expressway.

The following table shows which CSR alternative name elements apply to which Unified Communications features:

| CSR SAN element  | Mobile and remote access | Jabber Guest | XMPP federation          |
|--|--------------------------|--------------|--------------------------|
| Unified CM registrations domains                         | ✓<br>(Expressway-E only) | X            | X                        |
| XMPP federation domains                                  | X                        | X            | ✓<br>(Expressway-E only) |
| IM and Presence chat node aliases (federated group chat) | X                        | X            | ✓                        |
| Unified CM phone security profile names                  | ✓<br>(Expressway-C only) | X            | X                        |

**Note:**

- A new Expressway-C certificate may need to be produced for the Expressway-C if chat node aliases are added or renamed, such as when an IM and Presence node is added or renamed, or if new TLS phone security profiles are added.
- A new Expressway-E certificate must be produced if new chat node aliases are added to the system, or if the Unified CM or XMPP federation domains are modified.
- You must restart the Expressway for any new uploaded server certificate to take effect.

More details about the individual feature requirements per Expressway-C / Expressway-E are described below.

**Expressway-C server certificate requirements**

The Expressway-C server certificate needs to include the following elements in its list of subject alternate names:

- **Unified CM phone security profile names:** the names of the **Phone Security Profiles** in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. Use the FQDN format and separate multiple entries with commas.  
Having the secure phone profiles as alternative names means that Unified CM can communicate via TLS with the Expressway-C when it is forwarding messages from devices that use those profiles.
- **IM and Presence chat node aliases (federated group chat):** the **Chat Node Aliases** (e.g. chatroom1.example.com) that are configured on the IM and Presence servers. These are required only for Unified Communications XMPP federation deployments that intend to support group chat over TLS with federated contacts.  
The Expressway-C automatically includes the chat node aliases in the CSR, providing it has discovered a set of IM&P servers.  
We recommend that you use DNS format for the chat node aliases when generating the CSR. You must include the same chat node aliases in the Expressway-E server certificate's alternative names.

Figure 3: Entering subject alternative names for security profiles and chat node aliases on the Expressway-C's CSR generator

The screenshot shows a web interface for generating a CSR. It has a title 'Alternative name' and four input fields with corresponding labels and information icons:

- Additional alternative names (comma separated):** An empty text input field.
- IM and Presence chat node aliases (federated group chat):** A text input field containing 'chatnode1.xmpp.example.com,chatnode2.xmpp.example.com' and a dropdown menu set to 'DNS'.
- Unified CM phone security profile names:** A text input field containing 'DX80TLSprofile.example.com'.
- Alternative name as it will appear:** A list of generated DNS entries: 'DNS:vcsc.example.com', 'DNS:chatnode1.xmpp.example.com', 'DNS:chatnode2.xmpp.example.com', and 'DNS:DX80TLSprofile.example.com'.

**Expressway-E server certificate requirements**

The Expressway-E server certificate needs to include the following elements in its list of subject alternate names:

- **Unified CM registrations domains:** all of the domains which are configured on the Expressway-C for Unified CM registrations. They are required for secure communications between endpoint devices and Expressway-E.

Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. You may select *CollabEdgeDNS* format instead, which simply adds the prefix `collab-edge.` to the domain that you enter. This format is recommended if you do not want to include your top level domain as a SAN (see example in following screenshot).

- **XMPP federation domains:** the domains used for point-to-point XMPP federation. These are configured on the IM&P servers and should also be configured on the Expressway-C as domains for XMPP federation.

Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. Do not use the *XMPPAddress* format as it may not be supported by your CA, and may be discontinued in future versions of the Expressway software.

- **IM and Presence chat node aliases (federated group chat):** the same set of **Chat Node Aliases** as entered on the Expressway-C's certificate. They are only required for voice and presence deployments which will support group chat over TLS with federated contacts.

Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. Do not use the *XMPPAddress* format as it may not be supported by your CA, and may be discontinued in future versions of the Expressway software.

Note that you can copy the list of chat node aliases from the equivalent **Generate CSR** page on the Expressway-C.

Figure 4: Entering subject alternative names for Unified CM registration domains, XMPP federation domains, and chat node aliases, on the Expressway-E's CSR generator

The screenshot shows a web interface for configuring subject alternative names. It includes several input fields and dropdown menus:

- Additional alternative names (comma separated):** An empty text input field with an information icon.
- Unified CM registrations domains:** A text input field containing "example.com" and a dropdown menu set to "CollabEdgeDNS" with an information icon.
- XMPP federation domains:** A text input field containing "xmpp.example.com" and a dropdown menu set to "DNS" with an information icon.
- IM and Presence chat node aliases (federated group chat):** A text input field containing "chatnode1.xmpp.example.com,chatnode2.xmpp.example.com" and a dropdown menu set to "DNS" with an information icon.
- Alternative name as it will appear:** A list of generated DNS entries:
  - DNS:vcse.example.com
  - DNS:collab-edge.example.com
  - DNS:xmpp.example.com
  - DNS:chatnode1.xmpp.example.com
  - DNS:chatnode2.xmpp.example.com

See [Certificate Creation and Use With Expressway Deployment Guide](#) for full information about how to create and upload the Expressway's server certificate and how to upload a list of trusted certificate authorities.

# Mobile and remote access

This section describes how to configure your Expressway to support Unified Communications mobile and remote access.

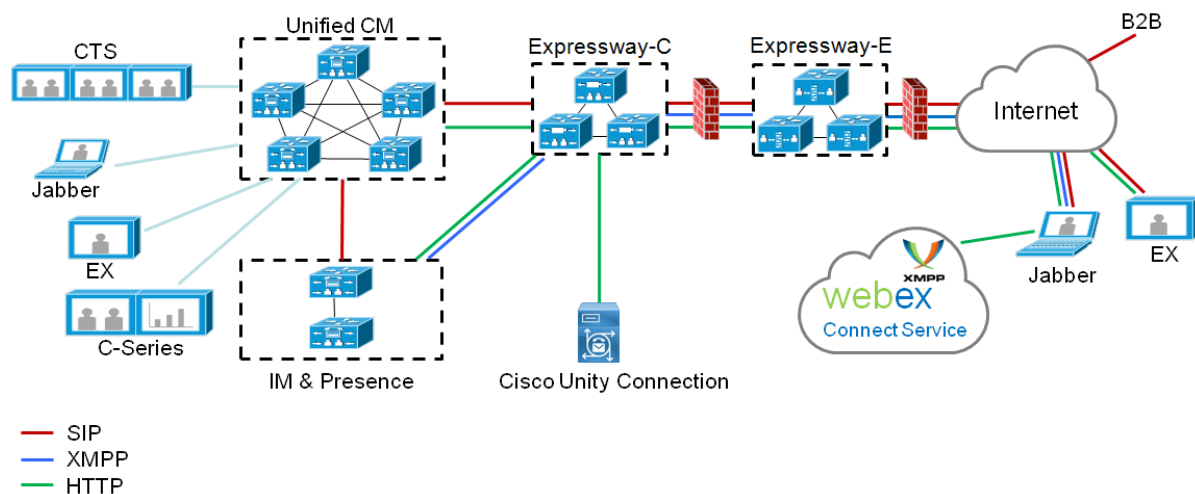
## Mobile and remote access overview

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.

The overall solution provides:

- **Off-premises access:** a consistent experience outside the network for Jabber and EX/MX/SX Series clients
- **Security:** secure business-to-business communications
- **Cloud services:** enterprise grade flexibility and scalable solutions providing rich WebEx integration and Service Provider offerings
- **Gateway and interoperability services:** media and signaling normalization, and support for non-standard endpoints

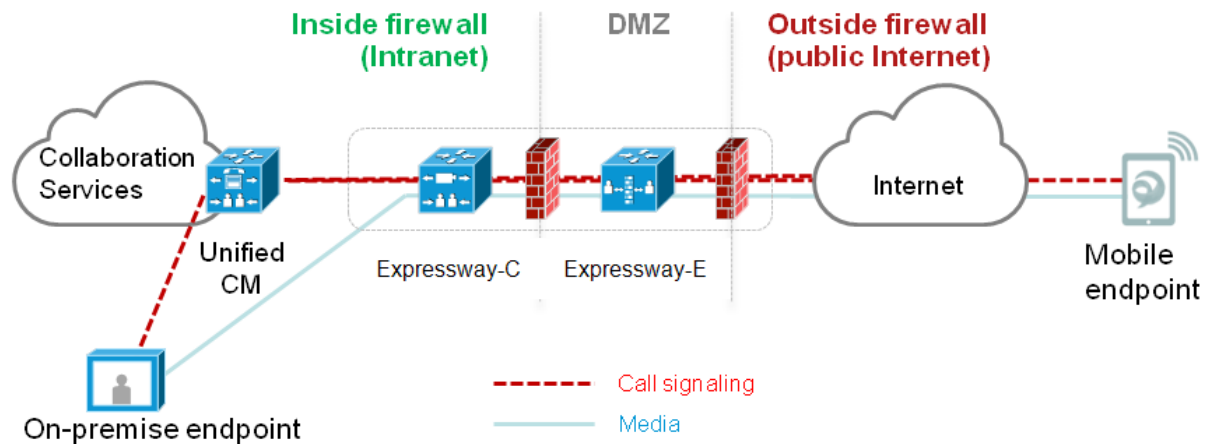
Figure 5: Unified Communications: mobile and remote access



Note that third-party SIP or H.323 devices can register to a Cisco VCS connected via a neighbor zone to a Cisco Expressway and, if necessary, interoperate with Unified CM-registered devices over a SIP trunk.



Figure 6: Typical call flow: signaling and media paths



- Unified CM provides call control for both mobile and on-premises endpoints.
- Signaling traverses the Expressway solution between the mobile endpoint and Unified CM.
- Media traverses the Expressway solution and is relayed between endpoints directly; all media is encrypted between the Expressway-C and the mobile endpoint.

## Jabber client connectivity without VPN

The mobile and remote access solution supports a hybrid on-premises and cloud-based service model, providing a consistent experience inside and outside the enterprise. It provides a secure connection for Jabber application traffic without having to connect to the corporate network over a VPN. It is a device and operating system agnostic solution for Cisco Jabber clients on Windows, Mac, iOS and Android platforms.

It allows Jabber clients that are outside the enterprise to:

- use instant messaging and presence services
- make voice and video calls
- search the corporate directory
- share content
- launch a web conference
- access visual voicemail

Note that Jabber Web and Cisco Jabber Video for TelePresence (Jabber Video) are not supported.

## Configuring mobile and remote access on Expressway

This section describes the steps required to enable and configure mobile and remote access features on Expressway-C and Expressway-E, and how to discover the Unified CM servers and IM&P servers used by the service.

### Installing Expressway security certificates and setting up a secure traversal zone

To support Unified Communications features (such as mobile and remote access or Jabber Guest), there must be a Unified Communications traversal zone connection between the Expressway-C and the

Expressway-E. This involves:

- Installing suitable security certificates on the Expressway-C and the Expressway-E.
- Configuring a Unified Communications traversal zone between the Expressway-C and the Expressway-E

For information about how to do this, see:

- [Configuring a secure traversal zone connection for Unified Communications \[p.59\]](#) (if your system does not already have a secure traversal zone in place)
- [Server certificate requirements for Unified Communications \[p.61\]](#)

Note that if XMPP federation is to be used, the IM&P servers need to be discovered on the Expressway-C for all the relevant information to be available when generating certificate signing requests.

## Setting up the Expressway-C

This section describes the configuration steps required on the Expressway-C.

### Configuring DNS and NTP settings

Check and configure the basic system settings on Expressway:

1. Ensure that **System host name** and **Domain name** are specified (**System > DNS**).
2. Ensure that local DNS servers are specified (**System > DNS**).
3. Ensure that all Expressway systems are synchronized to a reliable NTP service (**System > Time**). Use an **Authentication** method in accordance with your local policy.

If you have a cluster of Expressways you must do this for every peer.

### Enabling the Expressway-C for mobile and remote access

To enable mobile and remote access functionality:

1. Go to **Configuration > Unified Communications > Configuration**.
2. Set **Unified Communications mode** to *Mobile and remote access*.
3. Click **Save**.

Note that you must select *Mobile and remote access* before you can configure the relevant domains and traversal zones.

### Configuring the domains to route to Unified CM

You must configure the domains for which registration, call control, provisioning, messaging and presence services are to be routed to Unified CM.

1. On Expressway-C, go to **Configuration > Domains**.
2. Select the domains (or create a new domain, if not already configured) for which services are to be routed to Unified CM.
3. For each domain, turn *On* the services for that domain that Expressway is to support. The available services are:
  - **SIP registrations and provisioning on Unified CM:** Endpoint registration, call control and provisioning for this SIP domain is serviced by Unified CM. The Expressway acts as a Unified Communications gateway to provide secure firewall traversal and line-side support for Unified CM

registrations. The default is *On*.

- **IM and Presence Service:** Instant messaging and presence services for this SIP domain are provided by the Unified CM IM and Presence service. The default is *On*.
- **XMPP federation:** Enables XMPP federation between this domain and partner domains. The default is *On*.
- **Deployment:** Associates the domain with the selected deployment, if there are multiple deployments. This setting is absent if there is only one deployment (there is always at least one).

Turn *On* all of the applicable services for each domain.

Note that these settings are not entirely independent. You cannot disable SIP registration and provisioning while using IM and Presence. You can disable IM and Presence while **SIP registrations and provisioning on Unified CM** is *On*, but the reverse is not true. So, if you switch **IM and Presence Service** *On*, then your setting for SIP registrations and provisioning is ignored and the Expressway-C behaves as though it was *On*.

## Discovering Unified Communications servers and services

The Expressway-C must be configured with the address details of the Unified Communications services/nodes that are going to provide registration, call control, provisioning, voicemail, messaging, and presence services to MRA users.

IM and Presence Service configuration is not required if you're deploying the hybrid model, as these services are provided by the WebEx cloud.

---

**Note:** The connections configured in this procedure are static. You must refresh the configuration on the Expressway-C after you reconfigure or upgrade any of the discovered Unified Communications nodes. For more details, see [Why should I refresh the discovered nodes? \[p.70\]](#)

Go to **Configuration > Unified Communications > <UC server type>** and click **Refresh servers**.

---

### Trusting the certificates presented to the Expressway-C

If **TLS verify mode** is *On* when discovering Unified Communications services, then you must configure the Expressway-C to trust the certificates presented by the IM and Presence Service nodes and Unified CM servers.

1. Determine the relevant CA certificates to upload:
  - If the servers' tomcat and CallManager certificates are CA-signed, the Expressway-C's trusted CA list must include the root CA of the certificate issuer.
  - If the servers are using self-signed certificates, the Expressway-C's trusted CA list must include the self-signed certificates from all discovered IM and Presence Service nodes, Cisco Unity Connection servers, and Unified CM servers.
2. Upload the required certificates to the Expressway-C (**Maintenance > Security certificates > Trusted CA certificate**).
3. Restart the Expressway-C (**Maintenance > Restart options**).

### Discovering IM and Presence Service nodes

1. On Expressway-C, go to **Configuration > Unified Communications > IM and Presence Service nodes**.

The page lists any IM and Presence Service nodes that have already been discovered.

2. Add the details of an IM and Presence Service database publisher node:
  - a. Click **New**.
  - b. Enter the address of the **IM and Presence Service database publisher node**.  
You can enter an FQDN or an IP address, but we recommend using the FQDN when **TLS verify mode** is *On*.
  - c. Enter the **Username** and **Password** of an account that can access this server.

---

**Note:** These credentials are stored permanently in the Expressway database. The corresponding IM and Presence Service user must have the *Standard AXL API Access* role.

---

- d. [Recommended] Leave **TLS verify mode** switched *On* to ensure Expressway verifies the node's tomcat certificate (for XMPP-related communications).
- e. [Optional] Select which deployment this node/cluster will belong to.  
The **Deployment** field does not show if you have not created multiple deployments. All nodes belong to the default deployment if you choose not to use multiple deployments.
- f. Click **Add address**.  
If you enabled TLS verify mode, then the Expressway tests whether a secure connection can be established. It does this so you can find any TLS configuration errors before it continues the discovery process.  
If the secure connection test was successful, or if you did not enable TLS verify mode, then the system attempts to contact the publisher and retrieve details of its associated nodes.

---

**Note:** The status of the discovered node will be **Inactive** unless a valid traversal zone connection exists between the Expressway-C and the Expressway-E (may not yet be configured).

---

3. Repeat the discovery procedure for other IM and Presence Service nodes/clusters, if required.
4. Click **Refresh servers** to refresh all the node details after configuring multiple publisher addresses.

### Discovering Unified CM servers

1. On Expressway-C, go to **Configuration > Unified Communications > Unified CM servers**.  
The page lists any Unified CM nodes that have already been discovered.
2. Add the details of a Unified CM publisher node:
  - a. Click **New**.
  - b. Enter the **Unified CM publisher address**.  
You can enter an FQDN or an IP address, but we recommend using the FQDN when **TLS verify mode** is *On*.
  - c. Enter the **Username** and **Password** of an account that can access this server.

---

**Note:** These credentials are stored permanently in the Expressway database. The corresponding Unified CM user must have the *Standard AXL API Access* role.

---

- d. [Recommended] Leave **TLS verify mode** switched *On* to ensure Expressway verifies the node's certificates.  
The Unified CM node presents its tomcat certificate for AXL and UDS queries, and its CallManager certificate for subsequent SIP traffic. If the Unified CM server is using self-signed certificates, the Expressway-C's trusted CA list must include a copy of the tomcat certificate and the CallManager certificate from every Unified CM server.
- e. [Optional] Select which deployment this node/cluster will belong to.  
The **Deployment** field does not show if you have not created multiple deployments. All nodes belong to the default deployment if you choose not to use multiple deployments.
- f. Click **Add address**.

If you enabled TLS verify mode, then the Expressway tests whether a secure connection can be established. It does this so you can find any TLS configuration errors before it continues the discovery process.

If the secure connection test was successful, or if you did not enable TLS verify mode, then the system attempts to contact the publisher and retrieve details of its associated nodes.

3. Repeat the discovery procedure for other Unified CM nodes/clusters, if required.
4. Click **Refresh servers** to refresh all the node details after configuring multiple publisher addresses.

### Discovering Cisco Unity Connection servers

1. On Expressway-C, go to **Configuration > Unified Communications > Unity Connection servers**. The page lists any Cisco Unity Connection nodes that have already been discovered.
2. Add the details of a Cisco Unity Connection publisher node:
  - a. Click **New**.
  - b. Enter the **Unity Connection address**.  
You can enter an FQDN or an IP address, but we recommend using the FQDN when **TLS verify mode** is *On*.
  - c. Enter the **Username** and **Password** of an account that can access this server.

---

**Note:** These credentials are stored permanently in the Expressway database.

---

- d. [Recommended] Leave **TLS verify mode** switched *On* to ensure Expressway verifies the node's tomcat certificate.
  - e. [Optional] Select which deployment this node/cluster will belong to.  
The **Deployment** field does not show if you have not created multiple deployments. All nodes belong to the default deployment if you choose not to use multiple deployments.
  - f. Click **Add address**.  
If you enabled TLS verify mode, then the Expressway tests whether a secure connection can be established. It does this so you can find any TLS configuration errors before it continues the discovery process.  
If the secure connection test was successful, or if you did not enable TLS verify mode, then the system attempts to contact the publisher and retrieve details of its associated nodes.
3. Repeat the discovery procedure for other Cisco Unity Connection nodes/clusters, if required.
  4. Click **Refresh servers** to refresh all the node details after configuring multiple publisher addresses.

### Automatically generated zones and search rules

Expressway-C automatically generates non-configurable neighbor zones between itself and each discovered Unified CM node. A TCP zone is always created, and a TLS zone is created also if the Unified CM node is configured with a **Cluster Security Mode (System > Enterprise Parameters > Security Parameters)** of *1 (Mixed)* (so that it can support devices provisioned with secure profiles). The TLS zone is configured with its **TLS verify mode** set to *On* if the Unified CM discovery had **TLS verify mode** enabled. This means that the Expressway-C will verify the CallManager certificate for subsequent SIP communications. Each zone is created with a name in the format 'CEtcp-<node name>' or 'CEtls-<node name>'.

A non-configurable search rule, following the same naming convention, is also created automatically for each zone. The rules are created with a priority of 45. If the Unified CM node that is targeted by the search rule has a long name, the search rule will use a regex for its address pattern match.

Note that load balancing is managed by Unified CM when it passes routing information back to the registering endpoints.

## Why should I refresh the discovered nodes?

When the Expressway-C "discovers" a Unified Communications node, it establishes a connection to read the information required to create zones and search rules to proxy requests originating from outside of the network in towards that node.

**This configuration information is static.** That is, the Expressway only reads it when you manually initiate discovery of a new node, or when you refresh the configuration of previously discovered nodes. If any related configuration has changed on a node after you discover it, the mismatch between the new configuration and what the Expressway-C knows of that node will probably cause some kind of failure.

The information that the Expressway-C reads from the Unified Communications node is different for each node type and its role. The following list contains examples of UC configuration that you can expect to require a refresh from the Expressway. The list is not exhaustive; if you suspect that a configuration change on a node is affecting MRA services, you should refresh those nodes to eliminate one known source of potential problems.

- Changing cluster (e.g. adding or removing a node)
- Changing security parameters (e.g. Enabling Mixed Mode)
- Changing connection sockets (e.g. SIP port configuration)
- Changing TFTP server configuration
- Upgrading the software on the node

## Configuring the HTTP server allow list (whitelist) on Expressway-C

Jabber client endpoints may need to access additional web services inside the enterprise. This requires an "allow list" of servers to be configured to which the Expressway will grant access for HTTP traffic originating from outside the enterprise.

The features and services that may be required, and would need whitelisting, include:

- Visual Voicemail
- Jabber Update Server
- Custom HTML tabs / icons
- Directory Photo Host
- Advanced File Transfer (AFT)
- Problem Report Tool server

---

**Note:** In order for the AFT feature to work across Expressway you must ensure that all Unified CM IM and Presence Service nodes, across all Unified CM IM and Presence Service clusters, have been added to the whitelist either manually or automatically.

---

To configure the set of addresses to which HTTP access will be allowed:

1. On Expressway-C, go to **Configuration > Unified Communications > Configuration**.
2. Click **HTTP server allow list**.
3. Configure the hostnames or IP addresses of any HTTP servers that external Jabber clients are allowed to access.

Access is granted if the server portion of the client-supplied URI matches one of the names entered here, or if it resolves via DNS lookup to a specified IP address.

Expressway-C automatically whitelists the IP addresses of all discovered Unified CM nodes (that are running the CallManager and TFTP service), IM and Presence Service nodes, and Cisco Unity Connection nodes. These entries cannot be deleted. They are displayed in the **Auto-configured allow list** section of the **HTTP server allow list** page.

## Setting up the Expressway-E

This section describes the configuration steps required on the Expressway-E.

### Configuring DNS and NTP settings

Check and configure the basic system settings on Expressway:

1. Ensure that **System host name** and **Domain name** are specified (**System > DNS**).
2. Ensure that public DNS servers are specified (**System > DNS**).
3. Ensure that all Expressway systems are synchronized to a reliable NTP service (**System > Time**). Use an **Authentication** method in accordance with your local policy.

If you have a cluster of Expressways you must do this for every peer.

---

**Note:** The combination of <**System host name**>.<**Domain name**> is the FQDN of this Expressway-E. Ensure that this FQDN is resolvable in public DNS.

If you have a cluster of Expressway-Es, you must ensure that the **Domain name** is identical on each peer, and *it is case-sensitive*.

---

### Enabling the Expressway-E for mobile and remote access

To enable mobile and remote access functionality:

1. Go to **Configuration > Unified Communications > Configuration**.
2. Set **Unified Communications mode** to *Mobile and remote access*.
3. Click **Save**.

### Ensuring that TURN services are disabled on Expressway-E

You must ensure that TURN services are disabled on the Expressway-E used for mobile and remote access.

1. Go to **Configuration > Traversal > TURN**.
2. Ensure that **TURN services** are *Off*.

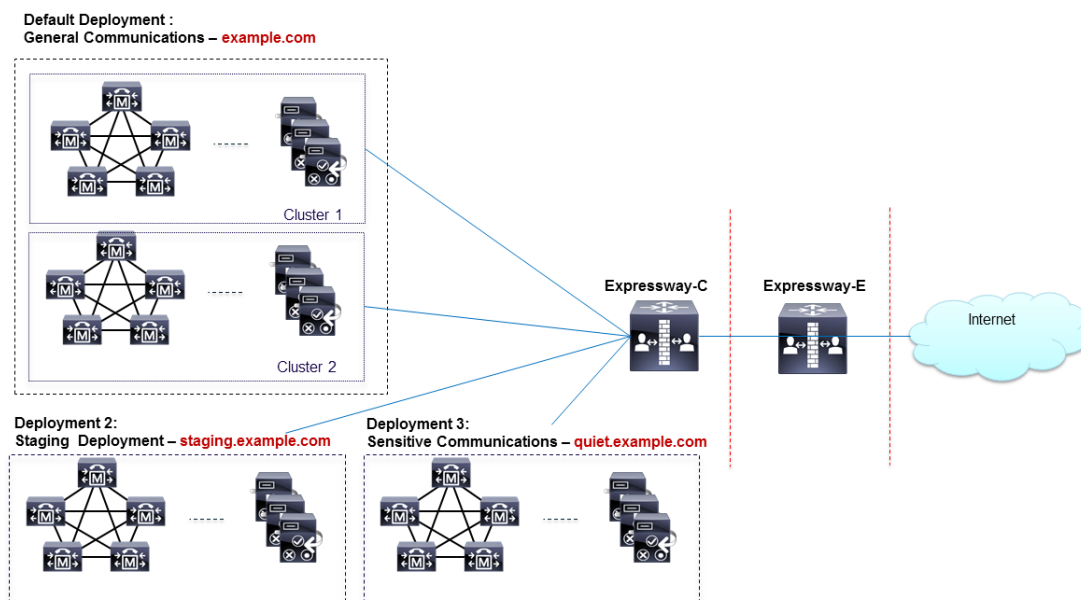
## Using deployments to partition Unified Communications services

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



Deployments and their associated domains and services are configured on the Expressway-C.

There is one primary deployment, called "Default deployment" unless you rename it, that automatically encloses all domains and services until you create and populate additional deployments. This primary deployment cannot be deleted, even if it is renamed or has no members.

To partition the services that you provide via mobile and remote access, create as many deployments as you need, associate a different domain with each, and then associate the required Unified Communications resources with each deployment.

You cannot associate one domain with more than one deployment. Similarly, each Unified Communications node may only be associated with one deployment.

#### To create a new deployment:

1. Log in to the Expressway-C.
2. Go to **Configuration > Unified Communications > Deployments** and click **New**.
3. Give the deployment a name and click **Create deployment**.  
The new deployment is listed on the **Deployments** page and is available to select when editing domains or UC services.

#### To associate a domain with a deployment:

1. Go to **Configuration > Domains**.  
The domains and their associated services are listed here. The deployment column shows where the listed domains are associated.



2. Click the domain name, or create a new domain (see [Configuring domains \[p.106\]](#)).
3. In the **Deployment** field, select the deployment which will enclose this domain.
4. Click **Save**.

#### To associate a Unified CM or other server/service with the deployment:

1. Go to **Configuration > Unified Communications >** and then **Unified CM servers**, or **IM and Presence Service nodes**, or **Unity Connection servers**.  
Any previously discovered service nodes of the selected type are listed here. The deployment column shows where the listed nodes are associated.  
If the list is not properly populated, see [Discovering Unified Communications servers and services \[p.67\]](#).
  2. Click the server / service node name.
  3. In the **Deployment** field, select which deployment will enclose this server / service node.
  4. Click **Save**.
- 
- Note:** When you save this change, the Expressway-C refreshes the connection to the node, which may temporarily disrupt the service to the connected users.
- 
5. Repeat for any other Unified Communications services that will belong to the deployment.

## Single Sign-On (SSO) over the Collaboration Edge

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

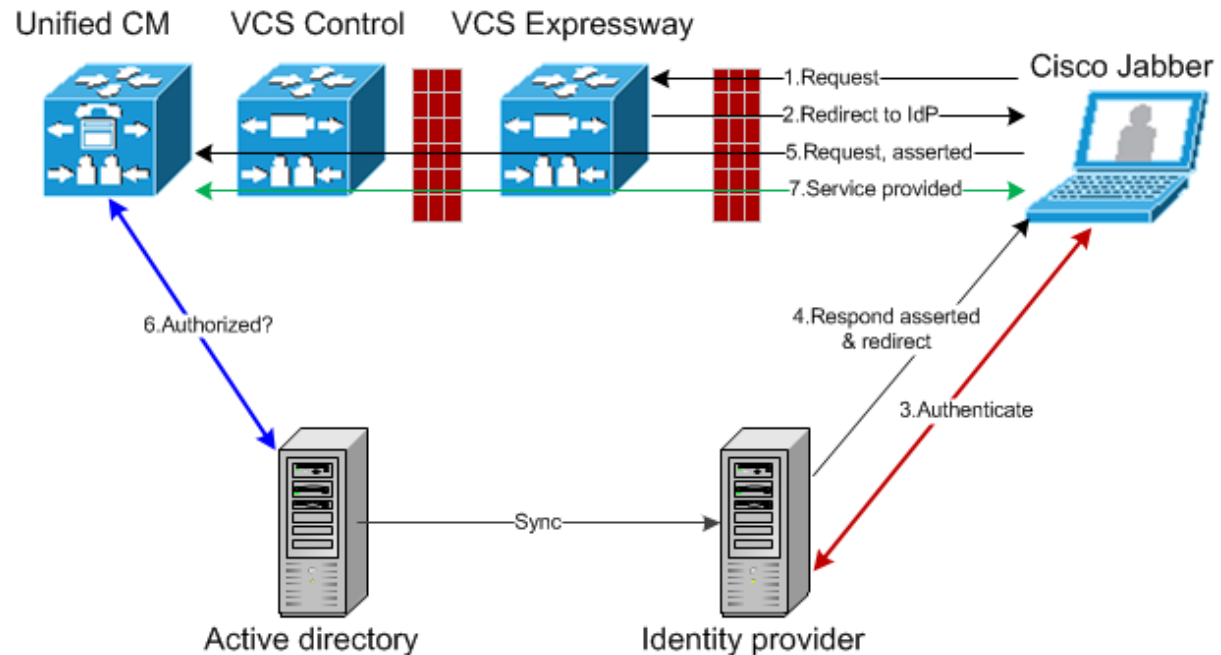
### How it works

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 8: Single sign-on for on-premises UC services



## Single Sign-On prerequisites

### On the Expressway pair:

- An Expressway-E and an Expressway-C are configured to work together at your network edge.
- A Unified Communications traversal zone is configured between the Expressway-C and the Expressway-E.
- The SIP domain that will be accessed via SSO is configured on the Expressway-C.
- The Expressway-C is in Mobile and remote access mode and has discovered the required Unified CM resources.
- The hostnames of the required Unified CM resources are added to the HTTP server allow list on the Expressway-C.
- If you are using multiple deployments, the Unified CM resources that will be accessed by SSO are in the same deployment as the domain that will be called from Jabber clients.

### On the Cisco Jabber clients:

- Clients are configured to request the internal services using the correct domain names / SIP URIs / Chat aliases.
- The default browser can resolve the Expressway-E and the IdP.

### On the Identity Provider:

The domain that is on the IdP certificate must be published in the DNS so that clients can resolve the IdP.

## Selecting an Identity Provider (IdP)

Cisco Collaboration solutions use SAML 2.0 (Security Assertion Markup Language) to enable SSO (single sign-on) for clients consuming Unified Communications services.

SAML-based SSO is an option for authenticating UC service requests originating from inside the enterprise network, and it is now extended to clients requesting UC services from outside via Mobile and Remote Access (MRA).

If you choose SAML-based SSO for your environment, note the following:

- SAML 2.0 is not compatible with SAML 1.1 and you must select an IdP that uses the SAML 2.0 standard.
- SAML-based identity management is implemented in different ways by vendors in the computing and networking industry, and there are no widely accepted regulations for compliance to the SAML standards.
- The configuration of and policies governing your selected IdP are outside the scope of Cisco TAC (Technical Assistance Center) support. Please use your relationship and support contract with your IdP Vendor to assist in configuring the IDP properly. Cisco cannot accept responsibility for any errors, limitations, or specific configuration of the IdP.

Although Cisco Collaboration infrastructure may prove to be compatible with other IdPs claiming SAML 2.0 compliance, only the following IdPs have been tested with Cisco Collaboration solutions:

- OpenAM 10.0.1
- Active Directory Federation Services 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4

## High level task list

1. Configure a synchronizable relationship between the identity provider and your on-premises directory such that authentication can securely be owned by the IdP. See *Directory Integration and Identity Management* in the [Cisco Collaboration System 10.x Solution Reference Network Designs \(SRND\)](#) document.
2. Export SAML metadata file from the IdP. Check the documentation on your identity provider for the procedure. For example, see *Enable SAML SSO through the OpenAM IdP* in the *SAML SSO Deployment Guide for Cisco Unified Communications Applications*.
3. Import the SAML metadata file from the IdP to the Unified CM servers and Cisco Unity Connection servers that will be accessed by single sign-on. See the Unified Communications documentation or help for more details.
4. Export the SAML metadata files from the Unified CM servers and Cisco Unity Connection servers. For example, see *High-Level Circle of Trust Setup* in the *SAML SSO Deployment Guide for Cisco Unified Communications Applications*.
5. Create the Identity Provider on the Expressway-C, by importing the SAML metadata file from the IdP.
6. Associate the IdP with SIP domain(s) on the Expressway-C.
7. Export the SAML metadata file(s) from the (master) Expressway-C; ensure that it includes the externally resolvable address of the (master) Expressway-E.  
The SAML metadata file from the Expressway-C contains the X.509 certificate for signing and encrypting SAML interchanges between the edge and the IdP, and the binding(s) that the IdP needs to redirect clients to the Expressway-E (peers).
8. Import the SAML metadata files from the Unified CM servers and Cisco Unity Connection servers to the IdP. An example using OpenAM is in the *SAML SSO Deployment Guide for Cisco Unified Communications Applications*.

9. Similarly, import the SAML metadata file from the Expressway-C to the IdP. See your IdP documentation for details.
10. Turn on SSO at the edge (on the Expressway-C and the Expressway-E).

## Importing the SAML metadata from the IdP

1. On the Expressway-C, go to **Configuration > Unified Communications > Identity providers (IdP)**. You only need to do this on the master peer of the cluster.
2. Click **Import new IdP from SAML**.
3. Use the **Import SAML file** control to locate the SAML metadata file from the IdP.
4. Set the **Digest** to the required SHA hash algorithm.  
The Expressway uses this digest for signing SAML authentication requests for clients to present to the IdP. The signing algorithm must match the one expected by the IdP for verifying SAML authentication request signatures.
5. Click **Upload**.  
The Expressway-C can now authenticate the IdP's communications and encrypt SAML communications to the IdP.

---

**Note:** You can change the signing algorithm after you have imported the metadata, by going to **Configuration > Unified Communications > Identity Providers (IdP)**, locating your IdP row then, in the **Actions** column, clicking **Configure Digest**.

---

## Associating domains with an IdP

You need to associate a domain with an IdP if you want the MRA users of that domain to authenticate via the IdP. The IdP adds no value until you associate at least one domain with it.

There is a many-to-one relationship between domains and IdPs. A single IdP can be used for multiple domains, but you may associate just one IdP with each domain.

### On the Expressway-C:

1. Open the IdP list (**Configuration > Unified Communications > Identity providers (IdP)**) and verify that your IdP is in the list.  
The IdPs are listed by their entity IDs. The associated domains for each are shown next to the ID.
2. Click **Associate domains** in the row for your IdP.  
This shows a list of all the domains on this Expressway-C. There are checkmarks next to domains that are already associated with this IdP. It also shows the IdP entity IDs if there are different IdPs associated with other domains in the list.
3. Check the boxes next to the domains you want to associate with this IdP.  
If you see (*Transfer*) next to the checkbox, checking it will break the domain's existing association and associate it with this IdP.
4. Click **Save**.  
The selected domains are associated with this IdP.

## Exporting the SAML metadata from the Expressway-C

---

**Note:** The Expressway-C must have a valid connection to the Expressway-E before you can export the Expressway-C's SAML metadata.

---

1. Go to **Configuration > Unified Communications > Export SAML data**.  
This page lists the connected Expressway-E, or all the Expressway-E peers if it's a cluster. These are listed because data about them is included in the SAML metadata for the Expressway-C.
2. [Conditional] If you have configured multiple deployments, you must select a deployment before you can export the SAML metadata.
3. Click **Download** or **Download all**.  
The page also lists all the Expressway-C peers, and you can download SAML metadata for each one, or export them all in a .zip file.
4. Copy the resulting file(s) to a secure location that you can access when you need to import SAML metadata to the IdP.

## Configuring IDPs

This topic covers any known additional configurations that are required when using a particular IDP for SSO over MRA.

These configuration procedures are required in addition to the prerequisites and high level tasks already mentioned, some of which are outside of the document's scope.

### Active Directory Federation Services 2.0

After creating Relying Party Trusts for the Expressway-Es, you must set some properties of each entity, to ensure that AD FS formulates the SAML responses as Expressway-E expects them.

These procedures were verified on AD FS 2.0, although the same configuration is required if you are using AD FS 3.0.

You need to:

- Sign the whole response (message and assertion)

#### To set these relying party trust properties for each entity:

In Windows PowerShell®, repeat the following command for each Expressway-E's *<EntityName>*:

```
Set-ADFSRelyingPartyTrust -TargetName "<EntityName>" -SAMLResponseSignature  
MessageAndAssertion
```

## Enabling Single Sign-On at the edge

### On the Expressway-C:

1. Go to **Configuration > Unified Communications > Configuration**
2. Locate **Single Sign-on support** and select *On*
3. Click **Save**

[Optional] Extend the time-to-live of SIP authorization tokens, by entering a number of seconds for **SIP token extra time-to-live (in seconds)**. This setting gives users a short window in which they can still accept calls after their credentials expire, but you should balance this convenience against the increased security exposure.

### On the Expressway-E:

1. Go to **Configuration > Unified Communications > Configuration**
2. Locate **Single Sign-on support** and select *On*
3. Click **Save**

[Optional] Choose how the Expressway-E reacts to `/get_edge_sso` requests by selecting whether or not the Expressway-C should check the home nodes.

The `/get_edge_sso` request from the client asks whether the client may try to authenticate the user by SSO. In this request, the client provides an identity of the user that the Expressway-C can use to find the user's home cluster:

- The default option is **Yes to Check for internal SSO availability**:  
The Expressway-E passes the request to the Expressway-C. The Expressway-C uses a round-robin algorithm to select a Unified CM node, and makes a UDS query for the supplied identity against that node. The Unified CM determines which node is the user's home node, and whether it is capable of doing SSO for the user, and then tells the Expressway-C the outcome. The Expressway-C then tells the Expressway-E which responds `true` or `false` to the client.
- If you select *No* to **Check for internal SSO availability**:  
The Expressway-E always responds `true` to `/get_edge_sso` requests. It does not make the inwards request to the user's home Unified CM, and thus cannot know whether SSO is really available there.

When the client receives a `true` response from Expressway-E, it will try to `/get_edge_config` via SSO. If it gets `false`, it will try `/get_edge_config` using whatever credentials it has - credentials which are independent from the identity managed by UDS inside the enterprise. If it gets `true` and SSO is not actually enabled on the user's home node, then `/get_edge_config` will fail and the client will not try the other authentication option.

The option you should choose depends entirely on your implementation. If you have a homogenous environment, in which all Unified CM nodes are capable of SSO, you can reduce response time and overall network traffic by selecting *No*. By contrast, if you want clients to use either mode of getting the edge configuration - during rollout or because you cannot guarantee that SSO is available on all nodes - you should select *Yes*.

## Checking the status of Unified Communications services

You can check the status of the Unified Communications services on both Expressway-C and Expressway-E.

1. Go to **Status > Unified Communications**.
2. Review the list and status of domains, zones and (Expressway-C only) Unified CM and IM&P servers. Any configuration errors will be listed along with links to the relevant configuration page from where you can address the issue.

## Mobile and remote access port reference

This section summarizes the ports that could potentially be used between your internal network (where the Expressway-C is located) and the DMZ (where the Expressway-E is located) and between the DMZ and the public internet.

**Outbound from Expressway-C (private) to Expressway-E (DMZ)**

| Purpose   | Protocol | Expressway-C (source) | Expressway-E (listening)   |
|---|----------|-----------------------|--|
| XMPP (IM and Presence)  | TCP      | Ephemeral port        | 7400   |
| SSH (HTTP/S tunnels)  | TCP      | Ephemeral port        | 2222   |
| Traversal zone SIP signaling  | TLS      | 25000 to 29999        | 7001   |
| Traversal zone SIP media<br>(for small/medium systems on X8.1 or later) | UDP      | 36000 to 59999*       | 36000 (RTP), 36001 (RTCP) (defaults)   |
| Traversal zone SIP media<br>(for large systems)                         | UDP      | 36000 to 59999*       | 36000 to 36011 (6 pairs of RTP and RTCP ports for multiplexed media traversal) |

**Outbound from Expressway-E (DMZ) to public internet**

| Purpose       | Protocol | Expressway-E (source)               | Internet endpoint (listening) |
|---------------|----------|-------------------------------------|-------------------------------|
| SIP media     | UDP      | 36002 to 59999 or<br>36012 to 59999 | >= 1024                       |
| SIP signaling | TLS      | 25000 to 29999                      | >= 1024                       |

**Inbound from public internet to Expressway-E (DMZ)**

| Purpose   | Protocol | Internet endpoint (source) | Expressway-E (listening)             |
|---|----------|----------------------------|--------------------------------------|
| XMPP (IM and Presence)  | TCP      | >= 1024                    | 5222                                 |
| HTTP proxy (UDS)  | TCP      | >= 1024                    | 8443                                 |
| Media   | UDP      | >= 1024                    | 36002 to 59999 or<br>36012 to 59999* |
| SIP signaling   | TLS      | >= 1024                    | 5061                                 |
| HTTPS (only required for external administrative access, which is strongly discouraged) | TCP      | >= 1024                    | 443                                  |

**From Expressway-C to Unified CM / Cisco Unity Connection**

| Purpose                             | Protocol | Expressway-C (source) | Unified CM (listening)         |
|-------------------------------------|----------|-----------------------|--------------------------------|
| XMPP (IM and Presence)              | TCP      | Ephemeral port        | 7400 (IM and Presence)         |
| HTTP proxy (UDS)                    | TCP      | Ephemeral port        | 8443 (Unified CM)              |
| HTTP proxy (SOAP)                   | TCP      | Ephemeral port        | 8443 (IM and Presence Service) |
| HTTP (configuration file retrieval) | TCP      | Ephemeral port        | 6970                           |

| Purpose   | Protocol | Expressway-C (source) | Unified CM (listening)  |
|---|----------|-----------------------|-------------------------|
| CUC (voicemail)                                       | TCP      | Ephemeral port        | 443 (Unity Connection)  |
| Message Waiting Indicator (MWI) from Unity Connection | TCP      | Ephemeral port        | 7080 (Unity Connection) |
| Media   | UDP      | 36000 to 59999*       | >= 1024                 |
| SIP signaling   | TCP      | 25000 to 29999        | 5060                    |
| Secure SIP signaling                                  | TLS      | 25000 to 29999        | 5061                    |

\* 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).

Note that:

- Ports 8191/8192 TCP and 8883/8884 TCP are used internally within the Expressway-C and the Expressway-E applications. Therefore these ports must not be allocated for any other purpose. The Expressway-E listens externally on port 8883; therefore we recommend that you create custom firewall rules on the external LAN interface to drop TCP traffic on that port.
- The Expressway-E listens on port 2222 for SSH tunnel traffic. The only legitimate sender of such traffic is the Expressway-C (cluster). Therefore we recommend that you create the following firewall rules for the SSH tunnels service:
  - one or more rules to allow all of the Expressway-C peer addresses (via the internal LAN interface, if appropriate)
  - followed by a lower priority (higher number) rule that drops all traffic for the SSH tunnels service (on the internal LAN interface if appropriate, and if so, another rule to drop all traffic on the external interface)



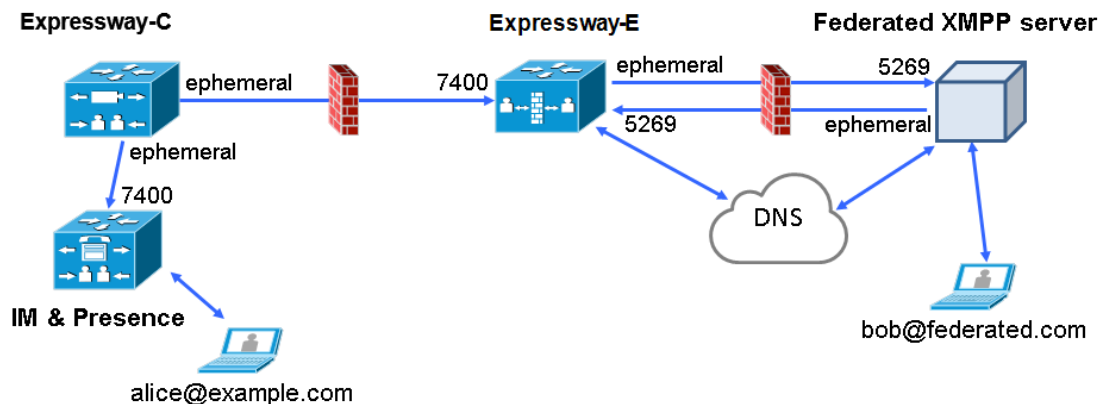
## External XMPP federation

This section describes how to configure your Expressway to support external XMPP federation.

### Deploying Expressway for 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.

The following diagram shows how XMPP messages are routed from your on-premises IM & Presence server via the Expressway-C and Expressway-E Collaboration Edge solution to the federated XMPP server. It also shows the ports and connections that are used as the messages traverse DMZ firewalls.



### Supported systems

- Expressway-E supports XMPP federation with:
  - Cisco Unified Communications Manager IM and Presence Service 9.1.1 or later
  - Cisco Webex Connect Release 6.x
  - other XMPP standards-compliant servers
- Cisco Jabber 9.7 or later
- Expressway-E does not support XMPP address translation (of email addresses, for example). External systems must federate with the Jabber IDs that are native to Unified CM IM & Presence. You can make the user's Unified CM IM&P Jabber ID resemble the user's email address, so that the federated partner can use email addresses for federation, by:
  - setting the Unified CM LDAP attribute for User ID to be the user's sAMAccountName
  - setting the Unified CM IM&P presence domain to be the same as the email domain
- Simultaneous internal federation managed by Unified CM IM&P and external federation managed by Expressway is not supported. If only internal federation is required then you must use Interdomain Federation on Unified CM IM&P. The available federation deployment configuration options are:
  - External federation only (managed by Expressway)
  - Internal federation only (managed by Unified CM IM&P)
  - Internal and external federation managed by Unified CM IM&P, but requires configuring your firewall to allow inbound connections

For more information see [Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager](#).

For information about configuring your system for external XMPP federation, see:

- [Configuring Expressway for external XMPP federation \[p.82\]](#)
- [DNS SRV records for XMPP federation \[p.86\]](#)
- [Port usage for XMPP federation \[p.87\]](#)
- [Checking XMPP federation status \[p.87\]](#)
- [Troubleshooting external XMPP federation \[p.88\]](#)

## Configuring Expressway for external XMPP federation

This section takes you through the steps required to configure your Expressway for external XMPP federation.

### Prerequisites

Ensure that you are running the following software versions:

- Expressway X8.2 or later
- Unified CM IM & Presence 9.1.1 or later

Note that XMPP federation can only be supported on a single Expressway cluster.

Before configuring your Expressway system for external XMPP federation:

- Ensure that Interdomain XMPP Federation has been **disabled** on Unified CM IM and Presence: Go to **Cisco Unified CM IM and Presence Administration > Presence > Inter Domain Federation > XMPP Federation > Settings** and ensure that **XMPP Federation Node Status** is set to *Off*. You must disable Interdomain Federation on Unified CM IM&P before enabling XMPP federation on Expressway.
- An Expressway-C (cluster) and Expressway-E (cluster) have been configured for Mobile and Remote Access to Unified Communications services, as described in *Mobile and Remote Access via Cisco Expressway Deployment Guide*. If only XMPP federation is required (video calls and remote registration to Unified CM are not required), the following items do not have to be configured:
  - domains that support *SIP registrations and provisioning on Unified CM* or that support *IM and Presence services on Unified CM*
  - Unified CM servers (you must still configure the IM&P servers)
  - HTTP server allow list

Note that federated communications are available to both on-premises clients (connected directly to Unified CM IM&P) and off-premises clients (connected to Unified CM IM&P via mobile and remote access).

- If you intend to use both TLS and group chat, the Expressway-C and Expressway-E server certificates must include in their list of subject alternate names (using either XMPPAddress or DNS formats) the **Chat Node Aliases** that are configured on the IM&P servers. Note that the Expressway-C automatically includes the chat node aliases in its certificate signing requests (CSRs), providing it has discovered a set of IM&P servers. When generating CSRs for the Expressway-E we recommend that you copy-paste the chat node aliases from the equivalent **Generate CSR** page on the Expressway-C. See [Server certificate requirements for Unified Communications \[p.61\]](#) for more information.

### Configuring local domains for XMPP federation on Expressway-C

You must configure your local domain names for which you want to provide XMPP federated services.

1. On Expressway-C, go to **Configuration > Domains**.
2. Click **New** (or click **View/Edit** if the required domain already exists).
3. Enter your local **Domain name** to be federated.
4. Set **XMPP federation** to *On*.
5. Click **Save**.
6. Repeat for any other local domains requiring federation.

## Configuring Expressway-E for XMPP federation

We recommend that XMPP federation configuration changes are made 'out of hours'. Enabling XMPP federation will restart the XCP router on all Expressway-E systems within the cluster. This will temporarily interrupt any existing mobile and remote access IM&P client sessions. Depending on the number of clients, full client reconnection may take several minutes. (See [Impact of configuration changes on a live system \[p.90\]](#) for more information.)

1. On Expressway-E, go to **Configuration > Unified Communications**.
2. Set **XMPP federation support** to *On*.  
When you apply this change, you may need to restart the XCP Routers on the IM&P server(s). The other settings on this page will not require a restart.
3. Configure the remaining fields as follows:

|  |  |
|--|--|
| <b>Use static routes</b>                         | Indicates whether a controlled list of static routes are used to locate the federated XMPP domains and chat node aliases, rather than DNS lookups. See <a href="#">Configuring how XMPP servers for federated domains and chat node aliases are located [p.84]</a> below.  |
| <b>Dialback secret</b>                           | Enter the dialback secret to use for identity verification with federated XMPP servers. If you have multiple Expressway-E systems in the same deployment, they must all be configured with the same dialback secret.<br><br>For more information about server dialback, see <a href="http://xmpp.org/extensions/xep-0220.html">http://xmpp.org/extensions/xep-0220.html</a> .  |
| <b>Security mode</b>                             | Indicates if a TLS connection to federated XMPP servers is required, preferred or not required.<br><i>TLS required</i> : the system guarantees a secure (encrypted) connection with the foreign domain.<br><i>TLS optional</i> : the system attempts to establish a TLS connection with the foreign domain. If it fails to establish a TLS connection, it reverts to TCP.<br><i>No TLS</i> : the system will not establish a TLS connection with the foreign domain. It uses a non-encrypted connection to federate with the foreign domain.<br><br>In all cases, server dialback is used to verify the identity of the foreign server. The foreign server must be configured to use server dialback. Note that SASL External is not a supported configuration on the local server. Foreign servers may be configured to use SASL, but SASL exchanges will not be supported by the local server.<br><br>The default, and recommended setting, is <i>TLS required</i> . |
| <b>Require client-side security certificates</b> | Controls whether the certificate presented by the external client is verified against the Expressway's current trusted CA list and, if loaded, the revocation list.<br><br>This setting does not apply if <b>Security mode</b> is <i>No TLS</i> .<br><br>Note that the federated domain name and any chat node aliases must be present in the certificate's subject alternate name, regardless of this setting.  |

|                     |   |
|---------------------|---|
| <b>Privacy mode</b> | <p>Controls whether restrictions are applied to the set of federated domains and chat node aliases.</p> <p><i>Off:</i> No restrictions are applied.</p> <p><i>Allow list:</i> Federation is allowed only with the domains and chat node aliases specified in the allow list.</p> <p><i>Deny list:</i> Federation is allowed with any domain or chat node alias except for those specified in the deny list.</p> <p>Note that any domains or chat node aliases that are configured as static routes are included automatically in the allow list.</p> <p>The default is <i>Allow list</i>.</p> <p>See <a href="#">Configuring the allow and deny lists for federated domains and chat node aliases [p.85]</a> below.</p> |
|---------------------|---|

4. Click **Save**

Your changes are applied. If you toggled **XMPP federation support**, you will be required to confirm that you want to restart the XCP router on the Expressway-C.

You may also need to restart the Unified CM IM&P XCP router services that are connected to the associated Expressway-C.
5. Log on to each IM and Presence server to check for notifications that you need to restart the XCP Routers. If you do need to restart them:
  - a. In **Cisco Unified IM and Presence Serviceability**, go to **Tools > Control Center - Network Services**.
  - b. Scroll down to the **IM and Presence Services** section and select **Cisco XCP Router**.
  - c. Click **Restart**.

This causes a restart of all XCP services on the IM and Presence Service.

The service restart may take several minutes.
  - d. Repeat on each IM and Presence server.

You could use the `utils service` CLI option (accessed via the Cisco Unified IM and Presence Operating System) to restart the services instead.

## Configuring how XMPP servers for federated domains and chat node aliases are located

You can use DNS lookups to locate the XMPP servers for federated domains and chat node aliases, or you can configure the addresses of specific XMPP servers.

**To use DNS lookups:**

1. On Expressway-E, go to **Configuration > Unified Communications**.
2. Set **Use static routes** to *Off*.
3. Click **Save**.

Note that all XMPP federated partners must publish in DNS the addresses of their XMPP servers as described in [DNS SRV records for XMPP federation \[p.86\]](#).

**To use static routes:**

1. If you want to use static routes for group chat, you must contact the partners with whom you are federating to get a list of their chat node aliases.
2. On Expressway-E, go to **Configuration > Unified Communications**.
3. Set **Use static routes** to *On* and click **Save**.
4. Click **Configure static routes for federated XMPP domains**.
5. On the **Federated static routes** page, click **New**.
6. Enter the details of the static route:

|                |  |
|----------------|--|
| <b>Domain</b>  | The federated XMPP domain or chat node alias.  |
| <b>Address</b> | The IP address or Fully Qualified Domain Name (FQDN) of an XMPP server for this federated domain or chat node alias. |

7. Click **Save**.
8. Add as many additional static routes as required.  
You can specify additional routes to alternative addresses for the same domain or chat node alias (all routes have an equal priority).

Note that:

- If there are no static routes defined for a federated domain or chat node alias, the system will use DNS instead.
- If static routes are defined for the federated domain or chat node alias, but the remote system cannot be contacted over those routes, the system will not fall back to DNS.
- If **Privacy mode** is set to *Allow list* and **Use static routes** is *On*, any domains (or chat node aliases) that are configured as static routes are included automatically in the allow list.

## Configuring the allow and deny lists for federated domains and chat node aliases

The allow and deny lists are used to control restrictions to the set of federated domains and chat node aliases. If **Privacy mode** is set to *Allow list* or *Deny list*, you must add the domains and chat node aliases with which you want to allow or deny federated connections.

This function manages restrictions at the domain / chat node alias level. Individual user-based privacy is controlled by each client / end-user.

The allow list and deny list modes are mutually exclusive. A domain/alias cannot be allowed and denied at the same time.

When federation is first enabled, **Privacy mode** is set to *Allow list* by default. In effect this puts the system in a 'lockdown' mode — you will not be allowed to connect with any federated domains or chat node aliases until you either add them to the allow list, configure static routes, or change the **Privacy mode** setting.

1. On Expressway-E, go to **Configuration > Unified Communications**.
2. Set **Privacy mode** as appropriate:
  - *Off*: No restrictions are applied.
  - *Allow list*: Federation is allowed only with the domains and chat node aliases specified in the allow list.
  - *Deny list*: Federation is allowed with any domain or chat node alias except for those specified in the deny list.
3. Click **Save**.
4. To manage the domains and chat node aliases in the allow or deny lists, click either **Federation allow list** or **Federation deny list** as appropriate.  
In the resulting page you can add, modify or delete the items in the allow/deny list. Wildcards or regexes are not allowed in the names; it must be an exact match.

All domains and chat node aliases that are configured as static routes are included automatically in the allow list.

## DNS SRV records for XMPP federation

If federating parties are **not** using static routes to access federated XMPP services, suitable DNS SRV records must be published.

### \_xmpp-server records

You must publish an \_xmpp-server DNS SRV record in DNS for your local domain so that remote enterprises can access your federated XMPP services. For example:

| Domain      | Service     | Protocol | Priority | Weight | Port | Target host      |
|-------------|-------------|----------|----------|--------|------|------------------|
| example.com | xmpp-server | tcp      | 0        | 0      | 5269 | vcse.example.com |

Similarly, to allow federating parties to discover a particular XMPP federated domain (if they are not using static routes), the federated enterprise must publish an \_xmpp-server DNS SRV record in its public DNS server. For example:

| Domain        | Service     | Protocol | Priority | Weight | Port | Target host              |
|---------------|-------------|----------|----------|--------|------|--------------------------|
| federated.com | xmpp-server | tcp      | 0        | 0      | 5269 | xmppserver.federated.com |

All enterprises must publish the service on port 5269. The published FQDNs must also be resolvable in DNS to an IP address.

## Group Chat

If you configure the Group Chat feature on a Unified CM IM&P server in an XMPP federation deployment, you must publish DNS SRV records for the federated chat node aliases.

To allow IM and Presence Service to discover a particular XMPP federated chat node alias, the federated enterprise must publish an \_xmpp-server DNS SRV record in its public DNS server. Similarly, IM and Presence Service must publish the same DNS SRV record in DNS for its domain. For example:

| Domain                | Service     | Protocol | Priority | Weight | Port | Target host      |
|-----------------------|-------------|----------|----------|--------|------|------------------|
| chatroom1.example.com | xmpp-server | tcp      | 0        | 0      | 5269 | vcse.example.com |

Both enterprises must publish the service on port 5269. The published FQDN must also be resolvable to an IP address in DNS.

Alternatively, to use group chat aliases on federated servers, you can configure static routes on the Expressway-E ([Configuration > Unified Communications > Federated static routes](#)) for each chat node alias.

Note that:

- The chat node aliases are configured on Unified CM IM&P Administration ([Messaging > Group Chat Server Alias Mapping](#)).
- Internal users do not need to use DNS to discover chat nodes; they get the chat room details from their local IM&P servers.

See [Chat configuration on IM and Presence](#) for more information about point-to-point instant messaging and group chat.

## Port usage for XMPP federation

This section summarizes the firewall ports that need to be opened for XMPP federation.

### Outbound from Expressway-C (private) to Expressway-E (DMZ)

| Purpose | Protocol | Expressway-C (source) | Expressway-E (listening) |
|---------|----------|-----------------------|--------------------------|
| XMPP    | TCP      | Ephemeral port        | 7400                     |

### Outbound from Expressway-E (DMZ) to public internet

| Purpose | Protocol | Expressway-E (source) | Federated XMPP server (listening) |
|---------|----------|-----------------------|-----------------------------------|
| XMPP    | TCP      | Ephemeral port        | 5269                              |

### Inbound from public internet to Expressway-E (DMZ)

| Purpose | Protocol | Federated XMPP server (source) | Expressway-E (listening) |
|---------|----------|--------------------------------|--------------------------|
| XMPP    | TCP      | Ephemeral port                 | 5269                     |

### From Expressway-C to IM and Presence Server

| Purpose | Protocol | Expressway-C (source) | IM and Presence Server (listening) |
|---------|----------|-----------------------|------------------------------------|
| XMPP    | TCP      | Ephemeral port        | 7400                               |

## Checking XMPP federation status

XMPP federation status information is available on the Expressway-E only.

You can go to **Status > Unified Communications** to check the primary status of the XMPP federation service. Normally, **XMPP Federation** should be *Active*.

If there are problems with the service, such as connectivity issues with the Expressway-C, the status will show as *Inactive*. In this case, you should also review the Unified Communications status page on the associated Expressway-C for more guidance as to what is causing the problem.

## Viewing federated connections

To view the current federated connections being managed by the Expressway-E:

1. On the Expressway-E, go to **Status > Unified Communications**.
2. Click **View federated connections** in the **Advanced status information** section.  
This shows all the current connections passing through that Expressway-E.  
It displays the IP **Address** of the client, and the **Direction** (*Incoming* or *Outgoing*) of the communication.  
Connections are closed after 10 minutes of inactivity.

Note that in clustered systems:

- An aggregated view is not displayed; only connections routed through the current peer are displayed.
- In 2-way connections, the inbound and outbound communications may be managed by different peers.

## Troubleshooting external XMPP federation

This section describes how to troubleshoot your external XMPP federation deployment and describes the impact of making configuration changes on a live system.

### Checking the basic status of your system

If you encounter issues with the XMPP federation status service, you should first check the **Status > Unified Communications** page on both the Expressway-C and the Expressway-E.

This will highlight any basic connection or configuration problems and provide information and links to help correct the problem.

### General configuration checklist

Ensure that the following Expressway configuration items have been specified correctly:

- Port 5269 is open in both directions between the internet and Expressway-E in the DMZ.
- DNS settings: host name, domain name and default DNS server (**System > DNS**).
- An accessible NTP server (**System > Time**).
- An active Unified Communications traversal zone on the Expressway-C and its associated Expressway-E (**Status > Zones**).
- **Unified Communications mode** is set to *Mobile and remote access* on both the Expressway-C and the Expressway-E (**Configuration > Unified Communications > Configuration**).
- **XMPP federation support** is *On* on the Expressway-E (**Configuration > Unified Communications > Configuration**).
- If static routes are enabled, ensure that the appropriate routes for the federated XMPP domains have been added to the Expressway-E (**Configuration > Unified Communications > Federated static routes**).



- At least one domain is configured on the Expressway-C with **XMPP federation** set to *On* (**Configuration > Domains**).
- IM & Presence servers have been discovered on the Expressway-C and have an active status (**Configuration > Unified Communications > IM and Presence servers**).

## Discovery, connectivity and firewall issues

- If using DNS lookup, check that `_xmpp-server` public DNS records exist for the domains and chat node aliases of all federated parties, and that they use port 5269.
- Check that port 5269 is open in both directions between the internet and Expressway-E in the DMZ.
- If the Expressway-C cannot connect to XCP on the Expressway-E remote host:
  - Check that the firewall has not blocked port 7400.
  - If the Expressway-E is running dual network interfaces, ensure that the traversal zone on the Expressway-C is connected to the internally-facing interface on the Expressway-E.
- Be aware that inbound and outbound connections can be routed through different cluster peers.

## Certificates and secure TLS connections

If you have configured secure TLS connections, ensure that:

- Valid server certificates are installed, they are in date and not revoked.
- Both the remote and local server certificates must contain a valid domain in the Subject Alternative Name (SAN). This applies even if **Require client-side security certificates** is disabled.
- If **Require client-side security certificates** is enabled, ensure that the server certificate is signed by a CA and is not locally signed.
- Certificate Authority (CA) certificates are installed.
- If you are using group chat over TLS, ensure that the Expressway-C and Expressway-E server certificates include in their list of subject alternate names (using either XMPPAddress or DNS formats) all of the **Chat Node Aliases** that are configured on the IM and Presence servers.
- Ensure that compatible security settings (TLS required, optional, no TLS) exist on your system and the remote federated system.

See [Server certificate requirements for Unified Communications \[p.61\]](#) for more information.

## Checking the Event Log

Check the Event Log on the Expressway-E for XMPP events.

Events related to XMPP federation are tagged with `Module="XMPPFederation"`. There are no XMPP-related logs on the Expressway-C.

## Performing diagnostic logging

When performing diagnostic logging (**Maintenance > Diagnostics > Diagnostic logging**), set the `develop.xcp.federation` support log (**Maintenance > Diagnostics > Advanced > Support Log configuration**) to debug level.

## Disabling Interdomain XMPP Federation on Unified CM IM&P

You must not enable both Interdomain XMPP Federation on Unified CM IM&P and XMPP federation on Expressway-E. One symptom of this incorrect configuration is that some users will have one-way federation.

If Interdomain Federation is enabled on Unified CM IM&P, perform the following operations in exactly the order shown:

1. Disable Interdomain Federation on the IM&P servers:
  - a. Go to **Cisco Unified CM IM and Presence Administration > Presence > Inter Domain Federation > XMPP Federation > Settings**.
  - b. Set **XMPP Federation Node Status** to *Off*.
2. Refresh the set of discovered IM&P servers on Expressway-C.
3. Restart all of the Unified CM IM&P XCP Router services that are connected to that Expressway-C.

## Impact of configuration changes on a live system

In general, we recommend that XMPP federation configuration changes are made 'out of hours'. This section describes the impact that configuration changes will have on current clients using XMPP federation and any Jabber clients using mobile and remote access.

### Expressway-C configuration changes

#### Domains

Any domain configuration changes, when one or more existing domains are configured for *IM and Presence services on Unified CM* or *XMPP Federation* will result in an automatic restart of the XCP router on both Expressway-C and Expressway-E.

The end-user impact is temporary loss of federation and any Jabber clients using mobile and remote access will be temporarily disconnected. The clients will automatically reconnect after a short period.

#### Unified Communications mode

Setting the **Unified Communications mode** to *Off* or to *Jabber Guest services* will stop the the XCP router on both Expressway-C and Expressway-E.

- This will remove the Expressway-E XMPP federation node from all discovered IM&P servers. A notification will appear on the IM&P administration interface to restart the XCP router on all affected IM&P nodes.
- The end-user impact is that all IM&P sessions will be disconnected. That is, there is a loss of federation, IM&P sessions over mobile and remote access will be disconnected, and sessions directly homed on the IM&P node will be dropped. When the XCP router is restarted on each IM&P node, all XCP functionality on that node will be disrupted.

#### Discovered IM & Presence Servers

Adding or deleting an IM & Presence publisher will require a restart of the XCP router on each IM & Presence node associated with that publisher only if **XMPP Federation** is enabled.

- This will cause a restart of the XCP router on Expressway-C.
- The end-user impact should be minimal. They will be unable to send or receive IM & Presence updates for a few seconds.

## Expressway-E configuration changes

### Unified Communications mode

Setting the **Unified Communications mode** to *Off* or to *Jabber Guest services* will stop the the XCP router on both Expressway-C and Expressway-E.

- This will remove the Expressway-E XMPP federation node from all discovered IM&P servers. A notification will appear on the IM&P administration interface to restart the XCP router on all affected IM&P nodes.
- The end-user impact is that all IM&P sessions will be disconnected. That is, there is a loss of federation, IM&P sessions over mobile and remote access will be disconnected, and sessions directly homed on the IM&P node will be dropped. When the XCP router is restarted on each IM&P node, all XCP functionality on that node will be disrupted.

Note that turning the **Unified Communications Mode** back to *On* will reinsert the XMPP federation node and have the same impact on the IM&P servers.

### XMPP federation support

Changing the **XMPP federation support** setting will restart the Expressway-E XCP router.

- This will result in the addition/removal of the Expressway-E XMPP federation node from all discovered IM & Presence servers. A notification will appear on the IM&P administration interface to restart the XCP router on all affected IM&P nodes.
- The end-user impact is that all IM&P sessions will be disconnected. That is, there is a loss of federation, IM&P sessions over mobile and remote access will be disconnected, and sessions directly homed on the IM&P node will be dropped. When the XCP router is restarted on each IM&P node, all XCP functionality on that node will be disrupted.

### Other XMPP federation settings

Changing any of the other XMPP federation settings, such as static routes, security and privacy settings, or the allow/deny lists, will only result in a restart of the XMPP Federation Connection Manager service on the Expressway-E.

End-users may notice a temporary disruption to federation; any mobile and remote access IM&P sessions will remain connected.

### Client reconnection times after loss of service

The time taken for a client to reconnect to the XMPP service depends on the re-login limits specified in the **Cisco Server Recovery Manager** service parameters on the IM&P server.

See the *High Availability Client Login Profiles* section in [Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager](#) for the IM&P version that you are running.

# Cisco Jabber Guest

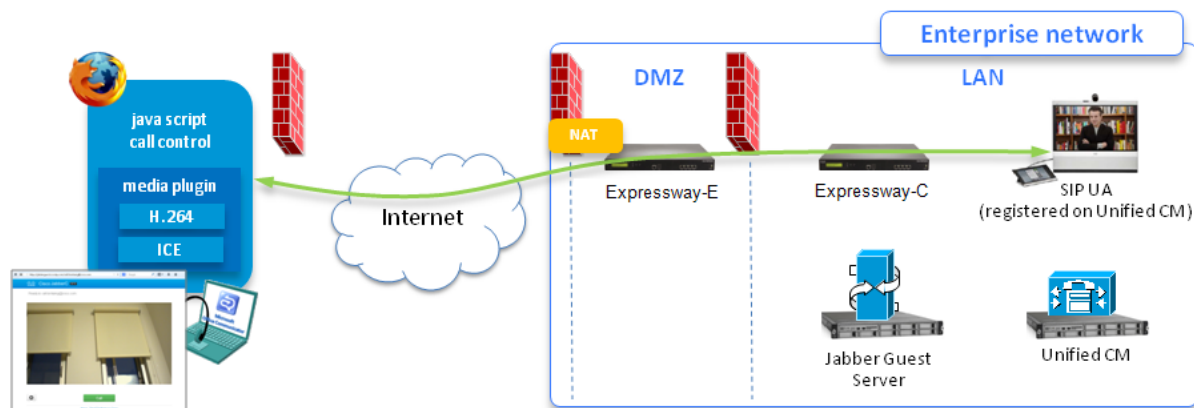
This section describes how to configure your Expressway for Cisco Jabber Guest services.

## Jabber Guest services overview

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.

It allows an external user to click on a hyperlink (in an email or a web page) that will download and install (on first use) a H.264 plugin into the user's browser. It then uses http-based call control to "dial" a URL to place a call to a predefined destination inside the enterprise. The user is not required to open an account, create a password, or otherwise authenticate.

To enable the call to be placed, it uses the Expressway solution (a secure traversal zone between the Expressway-C and Expressway-E) as a Unified Communications gateway to traverse the firewall between the Jabber Guest client in the internet and the Jabber Guest servers inside the enterprise to reach the destination user agent (endpoint).



## Jabber Guest signaling and media flows in single-NIC deployment

This topic summarizes the Jabber Guest traffic flow through the Expressway-E and Expressway-C deployment when the Expressway-E has only one network interface card (NIC) active.

The dual-NIC deployment is described in *Cisco Jabber Guest Server 10.0 Installation and Configuration Guide*.

### Single-NIC Expressway-E deployment summary

- The Expressway-E is in the DMZ with a single NIC enabled
- The Expressway-E is used for TURN services and reverse proxy
- SIP traffic goes from the Jabber Guest server to the Expressway-C. The Expressway-E does not do call control
- Media flows between the Expressway-E and Expressway-C using a port range and not a traversal zone

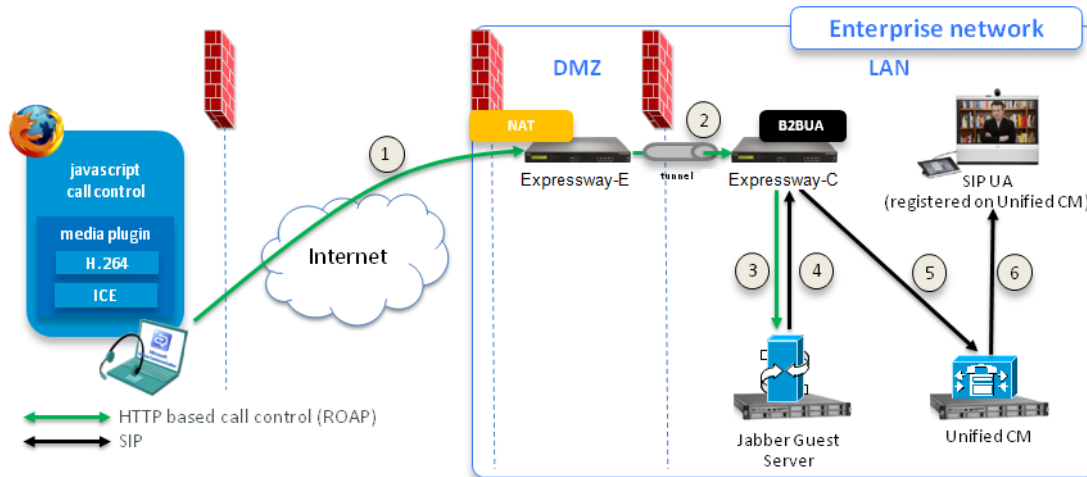
Note that the Expressway-E can optionally be configured to use static NAT mode. If you choose this mode, you must configure the Jabber Guest server with the static NAT address and DMZ external address of the Expressway-E. You need to do this so that media can go to the DMZ external address of the Expressway-E rather than being reflected off the outside firewall.

### Call flow summary in single-NIC deployment

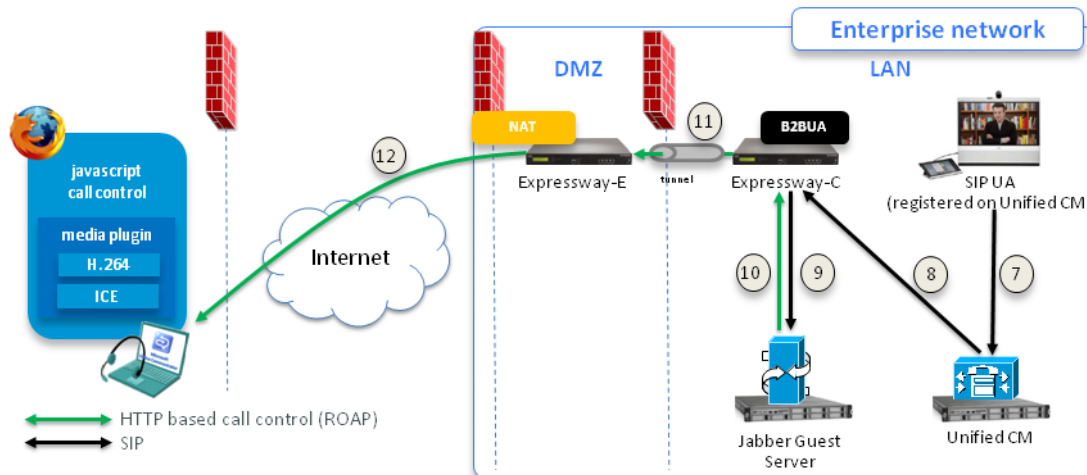
1. The Jabber Guest client sends an HTTP(S) request which is routed using HTTPS tunnels through the Expressway solution and on to the Jabber Guest server inside the enterprise.
2. The Jabber Guest server converts the HTTP(S) request into SIP and sends it to the Expressway-C.
3. The Expressway-C routes the call to the appropriate destination endpoint (typically via a SIP trunk to an endpoint registered to Unified CM) and uses its back-to-back user agent (B2BUA) to connect the call to the originating Jabber Guest client via the Expressway-E's TURN server.

### Call signaling flow

When the Jabber Guest client initiates the call, the following diagram shows how the signaling is typically routed through the Expressway, Jabber Guest server and Unified CM to the destination user agent.

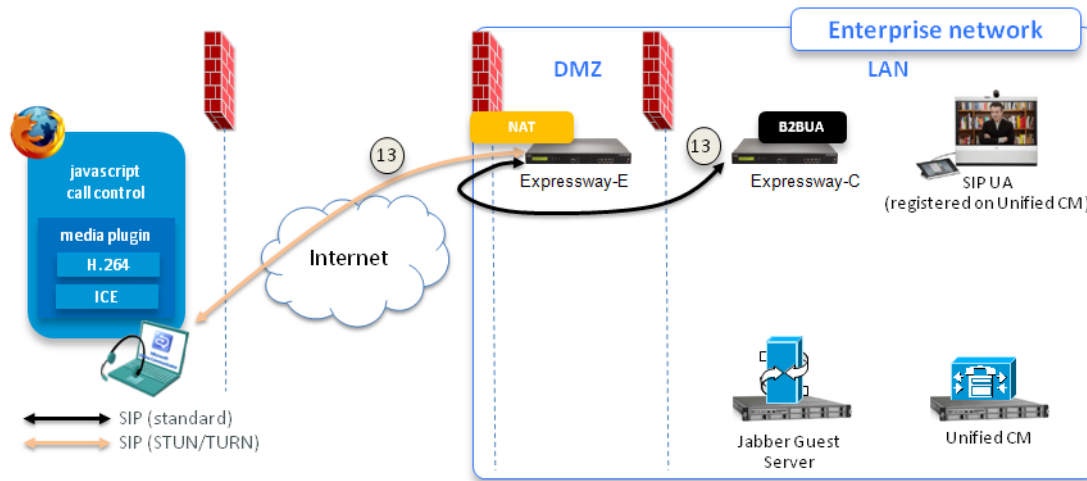


The return signaling from the user agent to the Jabber Guest client then follows the same route, but in reverse.



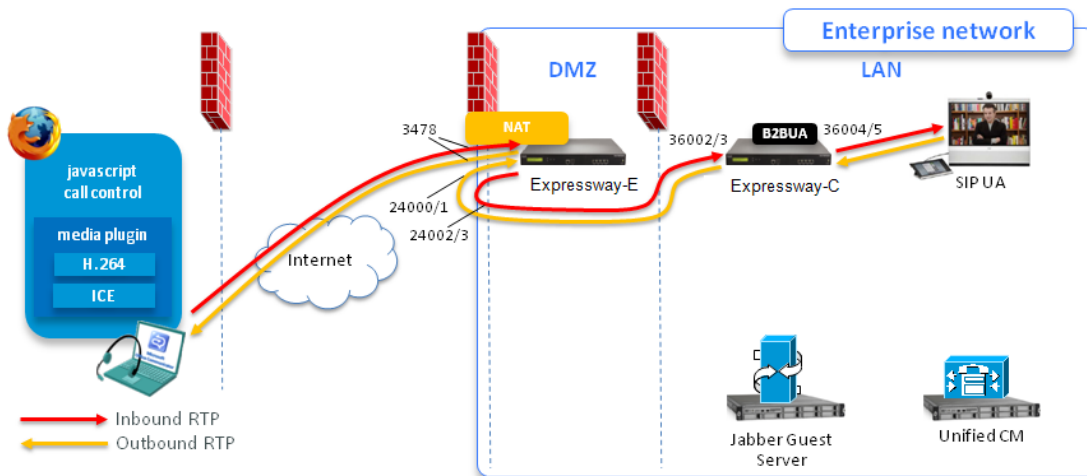
Media channels negotiation results in the allocation of TURN relays between the Jabber Guest client and the Expressway-E.

**Note:** Jabber Guest media does not go through the traversal link between Expressway-E and Expressway-C; media is sent from the Expressway-C to the externally-facing / NAT interface of the Expressway-E. You may need to configure your enterprise border firewall to reflect the media back in.



### RTP media flow

The following diagram shows the media flows and typical port usage on the Expressway-E and Expressway-C. The TURN server on the Expressway-E relays the media between the Jabber Guest client and the B2BUA on the Expressway-C, and the media also flows between the B2BUA and the internal endpoint.



See [Configuring your firewall for Jabber Guest traffic \[p.99\]](#) for full information about port requirements.

## Jabber Guest licensing and call capacity

The Expressway licensing requirements for Jabber Guest sessions are as follows:

- Each session typically uses 4 TURN server relays on the Expressway-E.
- 2 rich media session licenses are required per Cisco Jabber Guest session:
  - 1 rich media session license on the Expressway-E for each Cisco Jabber Guest session
  - 1 rich media session license on the Expressway-C for each Cisco Jabber Guest session

The maximum number of Jabber Guest sessions that can be supported through the Expressway depends on the type of [appliance / VM server](#), and whether they are deployed as a single Expressway-C and Expressway-E pair, or as a pair of clusters.

Table 4: Jabber Guest session limits

|   | Small / Medium systems | Large systems |
|---|------------------------|---------------|
| Single Expressway-C and Expressway-E pair   | 100                    | 500           |
| Pair of Expressway-C and Expressway-E clusters (4 or more peers per cluster for maximum capacity) | 400                    | 2000          |

## Configuring Jabber Guest services on Expressway

This guide primarily describes the Expressway configuration requirements. For information about configuring the Jabber Guest server and Jabber Guest client requirements, see:

- *Cisco Jabber Guest Server Installation and Configuration Guide*
- *Cisco Jabber Guest Administration and API Guide*
- *Cisco Jabber Guest Release Notes*

### Jabber Guest configuration summary

You must configure the Expressway with the domain that will support Jabber Guest services, associate that domain with one or more Jabber Guest servers, and set up the call routing to the destination endpoint.

In summary, the steps required to configure your Expressway system to support Jabber Guest are:

1. Install Expressway security certificates and set up a secure traversal zone for Unified Communications between Expressway-C and Expressway-E.
2. Configure the Expressway-E:
  - a. Enable Jabber Guest services.
  - b. Enable TURN services.
  - c. Lower the MTU size from 1500 to 1400 bytes.
3. Configure the Expressway-C:
  - a. Enable Jabber Guest services
  - b. Configure the domain that requires Jabber Guest support
  - c. Configure Jabber Guest servers and associate their addresses with the domain
  - d. Set up secure neighbor zones to the Jabber Guest servers

4. Configure the call routing, such as search rules, to route calls received from the Jabber Guest servers to the appropriate destinations e.g. Unified CM over a SIP trunk.
5. Configure the firewall to listen for and translate Jabber Guest traffic.

These steps are explained in detail below, using as an example a Jabber Guest client attempting to set up a call to the following URL: `https://expressway.example.com/call/8111@example.com`.

Note that:

- The Expressway-E domain must be the same as the domain used for Jabber Guest.
- You cannot use Jabber Guest services in conjunction with mobile and remote access calls and sessions.
- Media is sent from the Expressway-C to the externally-facing/NAT interface of the Expressway-E; you must ensure that your firewall allows this (see [Configuring your firewall for Jabber Guest traffic \[p.99\]](#)).

## Installing Expressway security certificates and setting up a secure traversal zone

To support Unified Communications features (such as mobile and remote access or Jabber Guest), there must be a Unified Communications traversal zone connection between the Expressway-C and the Expressway-E. This involves:

- Installing suitable security certificates on the Expressway-C and the Expressway-E.
- Configuring a Unified Communications traversal zone between the Expressway-C and the Expressway-E

See [Configuring a secure traversal zone connection for Unified Communications \[p.59\]](#) for instructions about how to do this if your system does not already have a secure traversal zone in place.

## Configuring the Expressway-E for Jabber Guest

You must enable Jabber Guest services:

1. On the Expressway-E, go to **Configuration > Unified Communications > Configuration**.
2. Set **Unified Communications mode** to *Jabber Guest services*.
3. Click **Save**.

You must enable the Expressway-E's TURN server to allow media routing from the Jabber Guest clients to the Expressway-C to be established via ICE:

1. Go to **Configuration > Traversal > TURN**.
2. Set **TURN services** to *On*.
3. Enter an **Authentication realm**.
4. Click **Save**.

You do not have to set up any TURN client credentials in the local authentication database.

In some call scenarios, such as when using VPN / SSL tunnels, the available Maximum Transmission Unit (MTU) can be reduced. The default MTU on Expressway-E of 1500 bytes can be too high and can cause packet loss. We recommended that you lower the MTU size on the relevant network interfaces to 1400 bytes:

1. Go to **System > Network interfaces > IP**.
2. In the **Maximum transmission unit (MTU)** field, enter 1400.



If you have multiple interfaces, you will typically want to do this on the externally-facing interface.

3. Click **Save**.

## Configuring the Expressway-C for Jabber Guest

### Task 1: Enable Jabber Guest services

1. On the Expressway-C, go to **Configuration > Unified Communications > Configuration**.
2. Set **Unified Communications mode** to *Jabber Guest services*.
3. Click **Save**.  
Jabber Guest services are enabled, but you cannot configure Jabber Guest servers yet; you need to enable Jabber Guest on a domain first.

### Task 2: Enable Jabber Guest on the required domain

1. Go to **Configuration > Domains**.
2. Select the domain that will support Jabber Guest services  
(If the domain does not yet exist, click **New** and enter the **Domain name**, in this case, **example.com**)
3. Set **Jabber Guest** to *On*
4. Click **Save**  
(The button reads **Create domain** if you are setting up the domain for the first time)

Note that only one Jabber Guest domain is supported per Expressway (cluster) deployment.

### Task 3: Configure Jabber Guest servers and associate their addresses with the Jabber Guest domain

1. Go back to **Configuration > Unified Communications > Configuration**.
2. Click the **Configure Jabber Guest servers** link.  
This takes you to the **Jabber Guest servers** page.
3. Click **New**.
4. Enter the details of the Jabber Guest server:
  - a. **Domain**: select the Jabber Guest domain that is to be mapped to a server hostname.
  - b. **Server hostname**: enter the FQDN of a Jabber Guest server to use for the selected domain.  
This must be an FQDN, not an unqualified hostname or an IP address.
  - c. **Priority**: this controls the order in which connections to this hostname are attempted for this domain.  
All priority 1 hostnames are attempted first, followed by priority 2 hostnames, and so on.
5. Click **Create entry**.
6. If required, add further Jabber Guest server addresses for the domain. You can give each server the same priority for even load balancing.

### Task 4: Create corresponding neighbor zones for each of the Jabber Guest servers

1. On the Expressway-C, go to **Configuration > Zones > Zones**.
2. Click **New**.
3. Configure the fields as follows (leave all other fields with default values):

|                              |  |
|------------------------------|--|
| <b>Name</b>                  | Enter the name you want to give this zone, for example “Jabber Guest server [name]”.   |
| <b>Type</b>                  | <i>Neighbor</i>  |
| <b>H.323 mode</b>            | <i>Off</i>   |
| <b>SIP mode</b>              | <i>On</i>  |
| <b>Transport</b>             | <i>TLS</i>   |
| <b>TLS verify mode</b>       | <p><i>On</i></p> <p>As these zones use a TLS verified connection you must ensure certificate trust between the Expressway and the Jabber Guest servers.</p> <ul style="list-style-type: none"> <li>When the Jabber Guest server is installed, it uses a self-signed certificate by default. However, you can install a certificate that is signed by a trusted certificate authority. You must install on the Expressway-C either the self-signed certificate of the Jabber Guest server, or the trusted CA certificates of the authority that signed the Jabber Guest server's certificate. To upload trusted Certificate Authority (CA) certificates to the Expressway, go to <a href="#">Maintenance &gt; Security certificates &gt; Trusted CA certificate</a>. You must restart the Expressway for the new trusted CA certificate to take effect.</li> <li>You must install on the Jabber Guest server the trusted CA certificates of the authority that signed the Expressway-C's server certificate. To manage certificates on the Jabber Guest server, go to <a href="#">Settings &gt; Local SSL Certificate</a>.</li> </ul> |
| <b>Media encryption mode</b> | <i>Force encrypted</i>   |
| <b>Location</b>              | Enter the same FQDN of the Jabber Guest server as configured on the <a href="#">Jabber Guest servers</a> page.   |
| <b>Zone profile</b>          | Default  |

- Click **Create zone**.
- Repeat this process for every Jabber Guest server.

Note that these neighbor zones are used to receive traffic **from** the Jabber Guest servers. Do not configure any search rules to route traffic **to** these zones.

## Configuring call routing

You must configure the call routing on the Expressway-C, such as search rules to route calls received by the Expressway-C from the Jabber Guest servers to the appropriate destinations.

In this example the destination address is `8111@example.com`. The call routing options could include:

- **Endpoints registered to Unified CM:** in this case you need to have configured a SIP trunk / neighbor zone between Unified CM and Expressway-C, and suitable search rules to route Jabber Guest calls (`8(\d{3})@example.com` for example) to Unified CM. See *Cisco Unified Communications Manager with Expressway (SIP Trunk) Deployment Guide*.
- **Endpoints registered to a neighbor system (such as a Cisco VCS):** in this case you need to have configured a neighbor zone between the neighbor system and Expressway-C, and suitable search rules to route calls for the Jabber Guest domain to the neighbor system.

## Configuring your firewall for Jabber Guest traffic

This section summarizes the ports that need to be opened for Jabber Guest traffic on the firewalls between your internal network (where the Expressway-C is located) and the DMZ (where the Expressway-E is located) and between the DMZ and the public internet.

### Inbound from public internet to Expressway-E (DMZ)

| Purpose                         | Protocol | Internet endpoint (source) | Expressway-E (listening)   |
|---------------------------------|----------|----------------------------|--|
| HTTPS traffic (see notes below) | TCP      | TCP source port            | 9443   |
| HTTP traffic (see notes below)  | TCP      | TCP source port            | 9980   |
| TURN server control / media     | UDP      | UDP source port            | 3478 (small/medium system)<br>3478-3483 (default range on large system)* |

Note that:

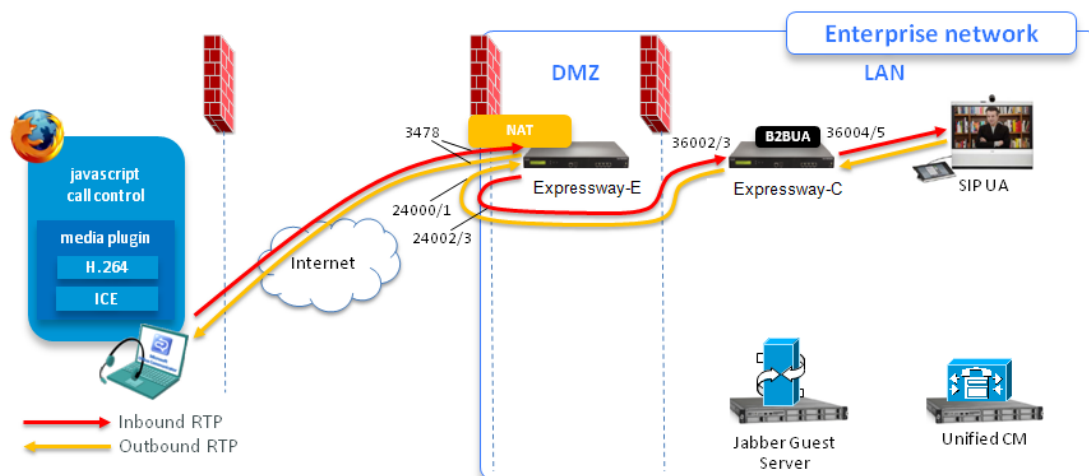
- HTTP and HTTPS traffic from Jabber Guest clients in the internet is sent to ports 80 and 443 TCP respectively. Therefore the firewall between the Expressway-E and the public internet must translate destination port 80 to 9980 and destination port 443 to 9443 for all TCP traffic that targets the Expressway-E address.
- 80/443 TCP are the standard HTTP/S administration interfaces on the Expressway. If the Expressway-E is administered from systems located in the internet, then the firewall translation must also distinguish by source address and must not translate the destination port of traffic arriving from those management systems.
- You also need to ensure that appropriate DNS records exist so that the Jabber Guest client can reach the Expressway-E. The FQDN of the Expressway-E in DNS must include the Jabber Guest domain, so in this case it could be `expressway.example.com`. Use round-robin DNS if it is a cluster of Expressway-Es. Note that this is public DNS configuration and it does not impose any configuration requirements on the Expressway-E itself (host name / domain name on the DNS page, or the cluster name etc.)

### Inbound from Expressway-E (external/NAT address) to Expressway-C (private)

| Purpose | Protocol | Expressway-E (source external/NAT address) | Expressway-C (listening) |
|---------|----------|--|--------------------------|
| Media   | UDP      | 24000 to 29999                             | 36002 to 59999 **        |

Jabber Guest media does not go through the traversal link between Expressway-E and Expressway-C. You may find that two way media can still be established even if the Expressway-E to Expressway-C rules described above are not applied. This is because the outbound media creates a pinhole in the firewall. However, these rules are required to support uni-directional media (that is, only from outside to inside).

The following diagram shows the media flows and typical port usage on the Expressway-E and Expressway-C. The TURN server on the Expressway-E relays the media between the Jabber Guest client and the B2BUA on the Expressway-C, and the media also flows between the B2BUA and the internal endpoint.



### Outbound from Expressway-C (private) to Expressway-E (external/NAT address)

| Purpose | Protocol | Expressway-C (source) | Expressway-E (listening external/NAT address) |
|---------|----------|-----------------------|---|
| Media   | UDP      | 36002 to 59999 **     | 24000 to 29999                                |

### Outbound from Expressway-C (private) to Expressway-E (DMZ internally-facing address)

| Purpose              | Protocol | Expressway-C (source) | Expressway-E (DMZ internal listening) |
|----------------------|----------|-----------------------|---------------------------------------|
| SSH (HTTP/S tunnels) | TCP      | Ephemeral port        | 2222                                  |

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

\*\* 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).

## Troubleshooting Jabber Guest services on Expressway

### Packet loss on calls

Check if the Maximum Transmission Unit (MTU) on Expressway-E is too high. We recommended that you lower the MTU size on the relevant network interfaces from 1500 to 1400 bytes.

**Jabber Guest client fails to connect and gets "Not Found on Accelerator" message**

This error can occur if:

- The Expressway-E domain is different from the Jabber Guest domain.
- The SIP trunk between the Jabber Guest server and the Expressway-C is not active.

**Jabber Guest client fails to connect and gets "Link Not Found" message**

This error can occur if:

- The URL being called is wrong.
- The correct URL is being called but it has not been enabled in the Jabber Guest server or it has expired.

# Protocols

---

This section provides information about how to configure the Expressway to support the SIP and H.323 protocols.

|  |     |
|--|-----|
| Configuring H.323 .....                      | 103 |
| Configuring SIP .....                        | 104 |
| Configuring domains .....                    | 106 |
| Configuring SIP and H.323 interworking ..... | 107 |

## Configuring H.323

The **H.323** page (**Configuration > Protocols > H.323**) is used to configure the H.323 settings on the Expressway, including:

- whether H.323 is enabled or not
- whether to insert the prefix of the ISDN gateway into the caller's E.164 number presented on the destination endpoint

The configurable options are:

| Field  | Description  | Usage tips   |
|--|--|--|
| <b>H.323 mode</b>                              | Enables or disables H.323 on the Expressway. H.323 support is <i>On</i> by default.  |  |
| <b>Call signaling TCP port</b>                 | The listening port for H.323 call signaling. Default is 1720.  |  |
| <b>Call signaling port range start and end</b> | Specifies the lower port in the range used by H.323 calls after they are established. Default is 15000.                                    | The call signaling port range must be great enough to support all the required concurrent calls. |
| <b>Call time to live</b>                       | The interval (in seconds) at which the Expressway polls the endpoints in a call to verify that they are still in the call. Default is 120. | If the endpoint does not respond, the call will be disconnected.                                 |
| <b>Auto discover</b>                           | Determines whether it will respond to Gatekeeper Discovery Requests sent out by endpoints. The default is <i>On</i> .                      |  |

# Configuring SIP

The **SIP** page (**Configuration > Protocols > SIP**) is used to configure the SIP settings on the Expressway, including:

- SIP functionality and SIP-specific transport modes and ports
- certificate revocation checking modes for TLS connections

## SIP functionality and SIP-specific transport modes and ports

This section contains the basic settings for enabling SIP functionality and for configuring the various SIP-specific transport modes and ports. The configurable options are:

| Field                                | Description   | Usage tips   |
|--------------------------------------|---|--|
| <b>SIP mode</b>                      | Enables and disables SIP functionality on the Expressway. Default is <i>On</i> .  |  |
| <b>SIP protocols and ports</b>       | <p>The Expressway supports SIP over <b>UDP</b>, <b>TCP</b> and <b>TLS</b> transport protocols. Use the <b>Mode</b> and <b>Port</b> settings for each protocol to configure whether or not incoming and outgoing connections using that protocol are supported, and if so, the ports on which the Expressway listens for such connections.</p> <p>By default UDP is <i>Off</i>, and TCP and TLS are <i>On</i>. The default ports are:</p> <ul style="list-style-type: none"> <li>■ UDP port: 5060</li> <li>■ TCP port: 5060</li> <li>■ TLS port: 5061</li> </ul> | At least one of the transport protocols must be set to a <b>Mode</b> of <i>On</i> for SIP functionality to be supported.   |
| <b>TCP outbound port start / end</b> | The range of ports the Expressway uses when TCP and TLS connections are established. The default range is 25000 to 29999.   | The range must be sufficient to support all required concurrent connections.   |
| <b>TLS handshake timeout</b>         | The timeout period for TLS socket handshake. Default is 5 seconds.  | You may want to increase this value if TLS server certificate validation is slow (e.g. if OCSP servers do not provide timely responses) and thus cause connection attempts to timeout. |

## Certificate revocation checking modes

This section controls the certificate revocation checking modes for SIP TLS connections. The configurable options are:

| Field                                       | Description   | Usage tips  |
|---|---|---|
| <b>Certificate revocation checking mode</b> | Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment. | We recommend that revocation checking is enabled. |



| Field                                | Description   | Usage tips   |
|--------------------------------------|---|--|
| <b>Use OCSP</b>                      | Controls whether the Online Certificate Status Protocol (OCSP) may be used to perform certificate revocation checking.  | To use OCSP, the X.509 certificate to be checked must contain an OCSP responder URI.   |
| <b>Use CRLs</b>                      | Controls whether Certificate Revocation Lists (CRLs) are used to perform certificate revocation checking.   | <p>CRLs can be used if the certificate does not support OCSP.</p> <p>CRLs can be loaded manually onto the Expressway, downloaded automatically from preconfigured URIs (see <a href="#">Managing certificate revocation lists (CRLs) [p.227]</a>), or downloaded automatically from a CRL distribution point (CDP) URI contained in the X.509 certificate.</p> |
| <b>Allow CRL downloads from CDPs</b> | Controls whether the download of CRLs from the CDP URIs contained in X.509 certificates is allowed.   |  |
| <b>Fallback behavior</b>             | <p>Controls the revocation checking behavior if the revocation status cannot be established, for example if the revocation source cannot be contacted.</p> <p><i>Treat as revoked</i>: treat the certificate as revoked (and thus do not allow the TLS connection).</p> <p><i>Treat as not revoked</i>: treat the certificate as not revoked.</p> <p>Default: <i>Treat as not revoked</i></p> | <p><i>Treat as not revoked</i> ensures that your system continues to operate in a normal manner if the revocation source cannot be contacted, however it does potentially mean that revoked certificates will be accepted.</p>   |

# Configuring domains

The **Domains** page ([Configuration > Domains](#)) lists the domains managed by this Expressway for Unified Communications services.

A domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is `100.example-name.com`.

Note that values shown in the **Index** column correspond to the numeric elements of the `%localdomain1%`, `%localdomain2%`, ... `%localdomain200%` [pattern matching variables](#).

You can configure up to 200 domains. (Note that you cannot configure domains on an Expressway-E.)

## Configuring the supported services for Unified Communications

When the Expressway-C has been enabled for [Unified Communications](#) mobile and remote access, you must select the services that each domain will support. The options are:

- **SIP registrations and provisioning on Unified CM:** Endpoint registration, call control and provisioning for this SIP domain is serviced by Unified CM. The Expressway acts as a Unified Communications gateway to provide secure firewall traversal and line-side support for Unified CM registrations. The default is *On*.
- **IM and Presence Service:** Instant messaging and presence services for this SIP domain are provided by the Unified CM IM and Presence service. The default is *On*.
- **XMPP federation:** Enables XMPP federation between this domain and partner domains. The default is *On*.
- **Deployment:** Associates the domain with the selected deployment, if there are multiple deployments. This setting is absent if there is only one deployment (there is always at least one).

Any domain configuration changes, when one or more existing domains are configured for *IM and Presence services on Unified CM* or *XMPP Federation* will result in an automatic restart of the XCP router on both Expressway-C and Expressway-E.

The end-user impact is temporary loss of federation and any Jabber clients using mobile and remote access will be temporarily disconnected. The clients will automatically reconnect after a short period.

# Configuring SIP and H.323 interworking

The **Interworking** page ([Configuration > Protocols > Interworking](#)) lets you configure whether or not the Expressway acts as a gateway between SIP and H.323 calls. The translation of calls from one protocol to the other is known as “interworking”.

The Expressway always takes the media for SIP–H.323 interworked calls so that it can independently negotiate payload types on the SIP and H.323 sides and Expressway will re-write these as the media passes.

Also in a SIP SDP negotiation, multiple codec capabilities can be agreed (more than one video codec can be accepted) and the SIP device is at liberty to change the codec it uses at any time within the call. If this happens, because Expressway is in the media path it will close and open logical channels to the H.323 device as the media changes (as required) so that media is passed correctly.

## Searching by protocol

When searching a zone, the Expressway first performs the search using the protocol of the incoming call. If the search is unsuccessful the Expressway may then search the zone again using the alternative protocol, depending on where the search came from and the **Interworking mode**. Note that the zone must also be configured with the relevant protocols enabled (SIP and H.323 are enabled on a zone by default).

## Enabling SIP endpoints to dial H.323 numbers

SIP endpoints can only make calls in the form of URIs — such as `name@domain`. If the caller does not specify a domain when placing the call, the SIP endpoint automatically appends its own domain to the number that is dialed.

So if you dial `123` from a SIP endpoint, the search will be placed for `123@domain`. If the H.323 endpoint being dialed is just registered as `123`, the Expressway will not be able to locate the alias `123@domain` and the call will fail. The solutions are to either:

- Ensure all your endpoints, both H.323 and SIP, register with an alias in the form `name@domain`.
- Create a pre-search transform on the Expressway that strips the `@domain` portion of the alias for those URIs that are in the form of `number@domain`.  
See the [pre-search transforms](#) section for information about how to configure pre-search transforms, and the [stripping @domain for dialing to H.323 numbers](#) section for an example of how to do this.

# Device authentication

---

This section provides information about the Expressway's authentication policy and the pages that appear under the **Configuration > Authentication** menu.

|                                   |     |
|-----------------------------------|-----|
| About device authentication ..... | 109 |
|-----------------------------------|-----|

# About device authentication

Device authentication is the verification of the credentials of an incoming request to the Expressway from a device or external system. It is used so that certain functionality may be reserved for known and trusted users.

## Unified Communications mobile and remote access devices

You do not have to make any explicit configuration on the Expressway regarding the authentication of devices that are registering to Unified CM via the Expressway. The Expressway automatically handles the authentication of these devices against its home Unified CM cluster.

## Rich media sessions

Devices communicating with the Expressway that are participating in rich media sessions are subject to the Expressway's configurable authentication policy.

When device authentication is enabled, any device that attempts to communicate with the Expressway is challenged to present its credentials (typically based on a username and password). The Expressway will then verify those credentials against its [local authentication database](#).

Expressway authentication policy can be configured separately for each zone. This means that both authenticated and unauthenticated devices could be allowed to communicate with the same Expressway if required. Subsequent call routing decisions can then be configured with different rules based upon whether a device is authenticated or not.

# Controlling system behavior for authenticated and non-authenticated devices

How calls and other messaging from authenticated and non-authenticated devices are handled depends on how search rules, external policy services and CPL are configured.

## Search rules

When configuring a search rule, use the **Request must be authenticated** attribute to specify whether the search rule applies only to authenticated search requests or to all requests.

## External policy services

External policy services are typically used in deployments where policy decisions are managed through an external, centralized service rather than by configuring policy rules on the Expressway itself. You can configure the Expressway to use policy services in the following areas:

- [Search rules \(dial plan\)](#)
- [Call Policy](#)

When the Expressway uses a policy service it sends information about the call request to the service in a POST message using a set of name-value pair parameters. Those parameters include information about whether the request has come from an authenticated source or not.

More information about policy services, including example CPL, can be found in *External Policy on Expressway Deployment Guide*.

## CPL

If you are using the Call Policy rules generator on the Expressway, source matches are carried out against authenticated sources. To specify a match against an unauthenticated source, just use a blank field. (If a source is not authenticated, its value cannot be trusted).

If you use uploaded, handcrafted local CPL to manage your Call Policy, you are recommended to make your CPL explicit as to whether it is looking at the authenticated or unauthenticated origin.

- If CPL is required to look at the unauthenticated origin (for example, when checking non-authenticated callers) the CPL must use `unauthenticated-origin`. (However, if the user is unauthenticated, they can call themselves whatever they like; this field does not verify the caller.)
- To check the authenticated origin (only available for authenticated or “treat as authenticated” devices) the CPL should use `authenticated-origin`.

Note that due to the complexity of writing CPL scripts, you are recommended to use an external policy service instead.

## Authentication policy configuration options

Authentication policy behavior varies for H.323 and SIP messages.

The primary authentication policy configuration options and their associated behavior are as follows:

- **Check credentials:** verify the credentials using the relevant authentication method. Note that in some scenarios, messages are not challenged, see below.
- **Do not check credentials:** do not verify the credentials and allow the message to be processed.
- **Treat as authenticated:** do not verify the credentials and allow the message to be processed as if it has been authenticated. This option can be used to cater for endpoints from third-party suppliers that do not support authentication within their registration mechanism. Note that in some scenarios, messages are allowed but will still be treated as though they are unauthenticated, see below.

Authentication policy is selectively configurable for different zone types, based on whether they receive messaging:

- The Default Zone, Neighbor zones, traversal client zones, traversal server zones and Unified Communications traversal zones all allow configuration of authentication policy
- DNS and ENUM zones do not receive messaging and so have no authentication policy configuration.

To edit a zone's **Authentication policy**, go to **Configuration > Zones > Zones** and click the name of the zone. The policy is set to *Do not check credentials* by default when you create a new zone.

The behavior varies for H.323 and SIP messages as shown in the tables below:

### H.323

| Policy                   | Behavior  |
|--------------------------|---|
| Check credentials        | Messages are classified as either authenticated or unauthenticated depending on whether any credentials in the message can be verified against the authentication database.<br>If no credentials are supplied, the message is always classified as unauthenticated. |
| Do not check credentials | Message credentials are not checked and all messages are classified as unauthenticated.   |

| Policy                 | Behavior  |
|------------------------|---|
| Treat as authenticated | Message credentials are not checked and all messages are classified as authenticated. |

## SIP

The behavior for SIP messages at the zone level depends upon the [SIP authentication trust mode](#) setting (meaning whether the Expressway trusts any pre-existing authenticated indicators - known as P-Asserted-Identity headers - within the received message).

| Policy                   | Trust | Behavior  |
|--------------------------|-------|---|
| Check credentials        | Off   | Messages are not challenged for authentication.<br>All messages are classified as unauthenticated.<br>Any existing P-Asserted-Identity headers are removed.   |
|                          | On    | Messages are not challenged for authentication.<br>Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged.<br>Messages without an existing P-Asserted-Identity header are classified as unauthenticated. |
| Do not check credentials | Off   | Messages are not challenged for authentication.<br>All messages are classified as unauthenticated.<br>Any existing P-Asserted-Identity headers are removed.   |
|                          | On    | Messages are not challenged for authentication.<br>Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged.<br>Messages without an existing P-Asserted-Identity header are classified as unauthenticated. |
| Treat as authenticated   | Off   | Messages are not challenged for authentication.<br>All messages are classified as unauthenticated.<br>Any existing P-Asserted-Identity headers are removed.   |
|                          | On    | Messages are not challenged for authentication.<br>Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged.<br>Messages without an existing P-Asserted-Identity header are classified as unauthenticated. |

## SIP authentication trust

If the Expressway is configured to use [device authentication](#) it will authenticate incoming SIP INVITE requests. If the Expressway then forwards the request on to a neighbor zone such as another Expressway, that receiving system will also authenticate the request. In this scenario the message has to be authenticated at every hop.

To simplify this so that a device's credentials only have to be authenticated once (at the first hop), and to reduce the number of SIP messages in your network, you can configure neighbor zones to use the **Authentication trust mode** setting.

This is then used in conjunction with the zone's authentication policy to control whether pre-authenticated SIP messages received from that zone are trusted and are subsequently treated as authenticated or unauthenticated within the Expressway. Pre-authenticated SIP requests are identified by the presence of a P-Asserted-Identity field in the SIP message header as defined by [RFC 3325](#).

The **Authentication trust mode** settings are:

- **On**: pre-authenticated messages are trusted without further challenge and subsequently treated as authenticated within the Expressway. Unauthenticated messages are challenged if the **Authentication policy** is set to *Check credentials*.
- **Off**: any existing authenticated indicators (the P-Asserted-Identity header) are removed from the message. Messages from a local domain are challenged if the **Authentication policy** is set to *Check credentials*.

Note:

- We recommend that you enable authentication trust only if the neighbor zone is part of a network of trusted SIP servers.
- Authentication trust is automatically implied between traversal server and traversal client zones.

## Configuring authentication to use the local database

The local authentication database is included as part of your Expressway system and does not require any specific connectivity configuration. It is used to store user account authentication credentials. Each set of credentials consists of a **name** and **password**.

The credentials in the local database can be used for device (SIP and H.323), traversal client and TURN client authentication.

### Adding credentials to the local database

To enter a set of device credentials:

1. Go to **Configuration > Authentication > Local database** and click **New**.
2. Enter the **Name** and **Password** that represent the device's credentials.
3. Click **Create credential**.

Note that the same credentials can be used by more than one device.

## Authenticating with external systems

The **Outbound connection credentials** page (**Configuration > Authentication > Outbound connection credentials**) is used to configure a username and password that the Expressway will use whenever it is required to authenticate with external systems.

For example, when the Expressway is forwarding an invite from an endpoint to another Expressway, that other system may have authentication enabled and will therefore require your local Expressway to provide it with a username and password.

Note that these settings are not used by traversal client zones. Traversal clients, which must always authenticate with traversal servers before they can connect, configure their connection credentials per traversal client zone.



# Zones and neighbors

---

This section describes how to configure zones and neighbors on the Expressway (**Configuration > Zones**).

|   |     |
|---|-----|
| About zones .....                           | 114 |
| Configuring media encryption policy .....   | 115 |
| Configuring ICE messaging support .....     | 116 |
| The Default Zone .....                      | 117 |
| Configuring Default Zone access rules ..... | 118 |
| Configuring zones .....                     | 119 |

# About zones

A zone is a collection of endpoints, either all registered to a single system or located in a certain way such as via an ENUM or DNS lookup. Zones are used to:

- control through links whether calls can be made between these zones
- manage the bandwidth of calls
- search for aliases
- control the services available to endpoints within that zone by setting up its [authentication policy](#)
- control the [media encryption](#) and [ICE](#) capabilities for SIP calls to and from a zone

You can configure up to 1000 zones. Each zone is configured as one of the following zone types:

- [Neighbor](#): a connection to a neighbor system of the local Expressway.
- [Traversal client](#): the local Expressway is a traversal client of the system being connected to, and there is a firewall between the two.
- [Traversal server](#): the local Expressway is a traversal server for the system being connected to, and there is a firewall between the two.
- [ENUM](#): the zone contains endpoints discoverable by ENUM lookup.
- [DNS](#): the zone contains endpoints discoverable by DNS lookup.
- [Unified Communications traversal](#): a traversal client or traversal server zone used for Unified Communications features such as mobile and remote access or Jabber Guest. Note that this zone type applies to the web interface only; the underlying CLI configuration uses *traversal client* and *traversal server* zone types.

The Expressway also has a pre-configured [Default Zone](#).

- See the [Zone configuration](#) section for information about the configuration options available for all zone types.
- See the [Configuring search and zone transform rules](#) section for information about including zones as targets for search rules.

## Automatically generated neighbor zones

The Expressway may automatically generate some non-configurable neighbor zones:

- An Expressway-C automatically generates neighbor zones between itself and each discovered Unified CM node when the system is configured for [mobile and remote access](#).
- An Expressway automatically generates a neighbor zone named "To Microsoft Lync server via B2BUA" when the [Lync B2BUA](#) is enabled.

## Configuring media encryption policy

The media encryption policy settings allow you to selectively add or remove media encryption capabilities for SIP calls flowing through the Expressway. This allows you to configure your system so that, for example, all traffic arriving or leaving an Expressway-E from the public internet is encrypted, but is unencrypted when in your private network.

- The policy is configured on a per zone basis and applies only to that leg of the call in/out of that zone.
- Encryption is applied to the SIP leg of the call, even if other legs are H.323.

Media encryption policy is configured through the **Media encryption mode** setting on each zone, however the resulting encryption status of the call is also dependent on the encryption policy settings of the target system (such as an endpoint or another Expressway).

The encryption mode options are:

- *Force encrypted*: all media to and from the zone must be encrypted. If the target system/endpoint is configured to not use encryption, then the call will be dropped.
- *Force unencrypted*: all media must be unencrypted. If the target system/endpoint is configured to use encryption, then the call may be dropped; if it is configured to use *Best effort* then the call will fall back to unencrypted media.
- *Best effort*: use encryption if available, otherwise fall back to unencrypted media.
- *Auto*: no specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on the target system/endpoint requests. This is the default behavior and is equivalent to how the Expressway operated before this feature was introduced.

Encryption policy (any encryption setting other than *Auto*) is applied to a call by routing it through a back-to-back user agent (B2BUA) hosted on the Expressway.

When configuring your system to use media encryption you should note that:

- Any zone with an encryption mode of *Force encrypted* or *Force unencrypted* must be configured as a SIP-only zone (H.323 must be disabled on that zone).
- TLS transport must be enabled if an encryption mode of *Force encrypted* or *Best effort* is required.
- The call component routed through the B2BUA can be identified in the call history details as having a component type of *B2BUA*.
- There is a limit per Expressway of 100 simultaneous calls (500 calls on [Large systems](#)) that can have a media encryption policy applied.
- The B2BUA can also be invoked when [ICE messaging support](#) is enabled.

## Configuring the B2BUA for media encryption

The B2BUA used for encryption (and ICE support) is a different instance to the B2BUA used for Microsoft Lync integration. Whereas the Lync B2BUA has to be manually configured and enabled, the B2BUA used for encryption is automatically enabled whenever an encryption policy is applied.

## Configuring ICE messaging support

The **ICE support** option is a per-zone configuration setting that controls how the Expressway supports ICE messages to and from SIP devices within that zone.

The behavior depends upon the configuration of the **ICE support** setting on the incoming (ingress) and outgoing (egress) zone. When there is a mismatch of settings i.e. *On* on one side and *Off* on the other side, the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host.

All zones have **ICE support** set to *Off* by default.

When the B2BUA performs ICE negotiation with a host, it can offer TURN relay candidate addresses. To do this, the B2BUA must be configured with the addresses of the TURN servers to offer (via [Applications > B2BUA > B2BUA TURN servers](#)).

The following matrix shows the Expressway behavior for the different possible combinations of the **ICE support** setting when handling a call between, for example, zone A and zone B:

| ICE support setting |     | Zone A   |  |
|---------------------|-----|--|--|
|                     |     | Off  | On   |
| Zone B              | Off | Standard Expressway proxying behavior.<br>B2BUA is not normally invoked (however, see the note below regarding media encryption policy). | B2BUA is invoked.<br>B2BUA includes ICE candidates in messages to hosts in Zone A.   |
|                     | On  | B2BUA is invoked.<br>B2BUA includes ICE candidates in messages to hosts in Zone B.   | Standard Expressway proxying behavior.<br>B2BUA is not normally invoked (however, see the note below regarding media encryption policy). |

### Effect of media encryption policy when combined with ICE support

The Expressway also invokes the B2BUA if it has to apply a [media encryption policy](#) (any encryption setting other than *Auto*). This table shows the effect on ICE negotiation behavior depending on the ICE support and media encryption modes of the ingress and egress zones:

| ICE support             | Media encryption mode                | B2BUA invoked | Effect on ICE negotiation   |
|-------------------------|--------------------------------------|---------------|---|
| Both zones = <i>Off</i> | At least one zone is <b>not Auto</b> | Yes           | The B2BUA will not perform any ICE negotiation with either host.  |
| Both zones = <i>On</i>  | At least one zone is <b>not Auto</b> | Yes           | The B2BUA will perform ICE negotiation with both hosts.   |
| Both zones = <i>On</i>  | Both zones = <i>Auto</i>             | No            | The Expressway will not offer any TURN relay candidate addresses to either of the ICE capable hosts. However, note that each host device may have already been provisioned with TURN relay candidate addresses. |

Note that:

- B2BUA routed calls are identified in the call history by a component type of *B2BUA*.
- There is a limit of 100 concurrent calls (500 calls on [Large systems](#)) that can be routed via the B2BUA.

## The Default Zone

The Default Zone represents any incoming calls from endpoints or other devices that are not recognized as belonging to any of the existing configured zones.

The Expressway comes pre-configured with the Default Zone and [default links](#) between it and the Traversal Subzone. Note that the Default Zone cannot be deleted.

## Configuring the Default Zone

By configuring the Default Zone you can control how the Expressway handles calls from unrecognized systems and endpoints. To configure the Default Zone, go to **Configuration > Zones > Zones** and click on **DefaultZone**.

The configurable options are:

| Field                                | Description  | Usage tips   |
|--------------------------------------|--|--|
| <b>Authentication policy</b>         | The <b>Authentication policy</b> setting controls how the Expressway challenges incoming messages to the Default Zone.                                       | See <a href="#">Authentication policy configuration options [p.110]</a> for more information.  |
| <b>Media encryption mode</b>         | The <b>Media encryption mode</b> setting controls the media encryption capabilities for SIP calls flowing through the Default Zone.                          | See <a href="#">Configuring media encryption policy [p.115]</a> for more information.  |
| <b>ICE support</b>                   | Controls whether ICE messages are supported by the devices in this zone.   | See <a href="#">Configuring ICE messaging support [p.116]</a> for more information.  |
| <b>Use Default Zone access rules</b> | The <b>Use Default Zone access rules</b> setting controls which external systems are allowed to connect over SIP TLS to the Expressway via the Default Zone. | If the access rules are enabled, then by default no systems will be allowed to connect over SIP TLS via the Default Zone; you must set up the <a href="#">access rules</a> for the systems you want to grant access. In essence, it enables <b>TLS verify mode</b> on the Default Zone.<br><br>Note that this setting does not affect other connections to the Default Zone (H.323 and SIP UDP/TCP). |

## Using links and pipes to manage access and bandwidth

You can also manage calls from unrecognized systems and endpoints by configuring the [links](#) and [pipes](#) associated with the Default Zone. For example, you can:

- delete the default links to prevent any incoming calls from unrecognized endpoints
- apply pipes to the default links to control the bandwidth consumed by incoming calls from unrecognized endpoints

## Configuring Default Zone access rules

The Default Zone access rules ([Configuration > Zones > Default Zone access rules](#)) control which external systems are allowed to connect over SIP TLS to the Expressway via the Default Zone.

Each rule specifies a pattern type and string that is compared to the identities (Subject Common Name and any Subject Alternative Names) contained within the certificate presented by the external system. You can then allow or deny access to systems whose certificates match the specified pattern. Up to 10,000 rules can be configured.

To use the rules, **Use Default Zone access rules** on the [Default Zone](#) page must be set to Yes. If the access rules are enabled, then by default no systems will be allowed to connect over SIP TLS to the Default Zone; you must set up the access rules for the systems you want to grant access. Note that the access rules do not affect other connections to the Default Zone (H.323 and SIP UDP/TCP).

The configurable options are:

| Field                 | Description  | Usage tips  |
|-----------------------|--|---|
| <b>Name</b>           | The name assigned to the rule.   |   |
| <b>Description</b>    | An optional free-form description of the rule.   |   |
| <b>Priority</b>       | Determines the order in which the rules are applied if the certificate names match multiple rules. The rules with the highest priority (1, then 2, then 3 and so on) are applied first. Multiple rules with the same priority are applied in configuration order.  |   |
| <b>Pattern type</b>   | The way in which the <b>Pattern string</b> must match the Subject Common Name or any Subject Alternative Names contained within the certificate.<br><i>Exact</i> : the entire string must exactly match the name, character for character.<br><i>Prefix</i> : the string must appear at the beginning of the name.<br><i>Suffix</i> : the string must appear at the end of the name.<br><i>Regex</i> : treats the string as a <a href="#">regular expression</a> . | You can test whether a pattern matches a particular name by using the <a href="#">Check pattern</a> tool ( <a href="#">Maintenance &gt; Tools &gt; Check pattern</a> ). |
| <b>Pattern string</b> | The pattern against which the name is compared.  |   |
| <b>Action</b>         | The action to take if the certificate matches this access rule.<br><i>Allow</i> : allows the external system to connect via the Default Zone.<br><i>Deny</i> : rejects any connection requests received from the external system.  |   |
| <b>State</b>          | Indicates if the rule is enabled or not.   | Use this setting to test configuration changes, or to temporarily disable certain rules. Any disabled rules still appear in the rules list but are ignored.             |

# Configuring zones

The **Zones** page (**Configuration > Zones > Zones**) lists all the zones that have been configured on the Expressway, and lets you create, edit and delete zones.

It also displays the zone's H.323 or SIP connection status:

- *Off*: the protocol is disabled at either the zone or system level
- *Active*: the protocol is enabled for that zone and it has at least one active connection; if multiple connections are configured and some of those connections have failed, the display indicates how many of the connections are *Active*
- *On*: applies to DNS and ENUM zones only and indicates that the protocol is enabled for that zone
- *Failed*: the protocol is enabled for that zone but its connection has failed
- *Checking*: the protocol is enabled for that zone and the system is currently trying to establish a connection

To neighbor with another system (such as another Expressway or gatekeeper), create a connection over a firewall to a traversal server or traversal client, or discover endpoints via an ENUM or DNS lookup, you must configure a zone on the local Expressway. The available zone types are:

- *Neighbor*: connects the local Expressway to a neighbor system
- *Traversal client*: connects the local Expressway to a traversal server
- *Traversal server*: connects the local Expressway-E to a traversal client
- *ENUM*: enables ENUM dialing via the local Expressway
- *DNS*: enables the local Expressway to locate endpoints and other systems by using DNS lookups

The zone type indicates the nature of the connection and determines which configuration options are available. For traversal server zones, traversal client zones and neighbor zones this includes providing information about the neighbor system such as its IP address and ports.

The Expressway also has a pre-configured **Default Zone**. The Default Zone represents any incoming calls from endpoints or other devices that are not recognized as belonging to any of the existing configured zones.

Note that connections between the Expressway and neighbor systems must be configured to use the same SIP transport type, that is they must both be configured to use TLS or both be configured to use TCP. Any connection failures due to transport type mismatches are recorded in the Event Log.

After creating a zone you would normally make it a target of at least one of your zone policy [search rules](#) (**Configuration > Dial plan > Search rules**) otherwise search requests will not be sent to that zone.

## Configuring neighbor zones

A neighbor zone could be a collection of endpoints registered to another system (such as a Cisco VCS), or it could be a SIP device (for example Cisco Unified Communications Manager). The other system or SIP device is referred to as a neighbor. Neighbors can be part of your own enterprise network, part of a separate network, or even standalone systems.

You create a neighbor relationship with the other system by adding it as a neighbor zone on your local Expressway. After you have added it, you can:

- query the neighbor about its endpoints
- apply transforms to any requests before they are sent to the neighbor

- control the bandwidth used for calls between your local Expressway and the neighbor zone

Note that:

- neighbor zone relationship definitions are one-way; adding a system as a neighbor to your Expressway does not automatically make your Expressway a neighbor of that system
- inbound calls from any configured neighbor are identified as coming from that neighbor
- systems that are configured as cluster peers (formerly known as Alternates) must not be configured as neighbors to each other

The configurable options for a neighbor zone are:

| Field                         | Description  | Usage tips  |
|-------------------------------|--|---|
| <b>Configuration</b> section: |  |   |
| <b>Name</b>                   | The name acts as a unique identifier, allowing you to distinguish between zones of the same type.  |   |
| <b>Type</b>                   | The nature of the specified zone, in relation to the local Expressway. Select <i>Neighbor</i> .  | After a zone has been created, the <b>Type</b> cannot be changed.   |
| <b>Hop count</b>              | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the <a href="#">Hop counts</a> section for more information). This field specifies the hop count to use when sending a search request to this particular zone. | If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used.   |
| <b>H.323</b> section:         |  |   |
| <b>Mode</b>                   | Determines whether H.323 calls are allowed to and from the neighbor system.  |   |
| <b>Port</b>                   | The port on the neighbor system used for H.323 searches initiated from the local Expressway.   | This must be the same port number as that configured on the neighbor system as its H.323 UDP port.  |
| <b>SIP</b> section:           |  |   |
| <b>Mode</b>                   | Determines whether SIP calls are allowed to and from the neighbor system.  |   |
| <b>Port</b>                   | The port on the neighbor system used for outgoing SIP messages initiated from the local Expressway.  | This must be the same port number as that configured on the neighbor system as its SIP TCP, SIP TLS or SIP UDP listening port (depending on which SIP <b>Transport</b> mode is in use).   |
| <b>Transport</b>              | Determines which transport type is used for SIP calls to and from the neighbor system. The default is <i>TLS</i> .   |   |
| <b>TLS verify mode</b>        | Controls whether the Expressway performs X.509 certificate checking against the neighbor system when communicating over TLS.   | If the neighbor system is another Expressway, both systems can verify each other's certificate (known as mutual authentication). See <a href="#">TLS certificate verification of neighbor systems [p.133]</a> for more information. |



| Field                                    | Description   | Usage tips  |
|--|---|---|
| <b>Media encryption mode</b>             | Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone.   | See <a href="#">Configuring media encryption policy [p.115]</a> for more information.   |
| <b>ICE support</b>                       | Controls whether ICE messages are supported by the devices in this zone.  | See <a href="#">Configuring ICE messaging support [p.116]</a> for more information.   |
| <b>Authentication</b> section:           |   |   |
| <b>Authentication policy</b>             | Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected.  | The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. See <a href="#">Authentication policy configuration options [p.110]</a> for more information.   |
| <b>SIP authentication trust mode</b>     | Controls whether authenticated SIP messages (ones containing a P-Asserted-Identity header) from this zone are trusted without further challenge.  | See <a href="#">SIP authentication trust [p.111]</a> for more information.  |
| <b>Location</b> section:                 |   |   |
| <b>Location Peer 1 to Peer 6 address</b> | <p>The IP address or FQDN of the neighbor system. Enter the addresses of additional peers if:</p> <ul style="list-style-type: none"> <li>■ the neighbor is an Expressway cluster, in which case you must specify all of the peers in the cluster</li> <li>■ the neighbor is a resilient non-Expressway system, in which case you must enter the addresses of all of the resilient elements in that system</li> </ul>  | <p>Calls to an Expressway cluster are routed to whichever peer in that neighboring cluster has the lowest resource usage. See <a href="#">Neighboring between Expressway clusters [p.141]</a> for more information.</p> <p>For connections to non-Expressway systems, the Expressway uses a round-robin selection process to decide which peer to contact if no resource usage information is available.</p>                          |
| <b>Advanced</b> section:                 |   |   |
| <b>Zone profile</b>                      | <p>Determines how the zone's advanced settings are configured.</p> <p><i>Default:</i> uses the factory default profile.</p> <p><i>Custom:</i> allows you to configure each setting individually.</p> <p>Alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. The options include:</p> <ul style="list-style-type: none"> <li>■ <i>Cisco Unified Communications Manager</i></li> <li>■ <i>Cisco Unified Communications Manager (8.6.1 or later)</i></li> <li>■ <i>Nortel Communication Server 1000</i></li> <li>■ <i>Infrastructure device</i> (typically used for non-gatekeeper devices such as an MCU)</li> </ul> | <p>See <a href="#">Zone configuration: advanced settings [p.128]</a> for details on the advanced settings.</p> <p>Only use the <i>Custom</i> profile to configure the individual advanced settings on the advice of Cisco customer support.</p> <p>See <a href="#">Cisco Unified Communications Manager with Expressway Deployment Guide</a> for more information about the <i>Cisco Unified Communications Manager</i> profiles.</p> |

## Configuring traversal client zones

To traverse a firewall, the Expressway must be connected with a traversal server (typically, an Expressway-E).

In this situation your local Expressway is a traversal client, so you create a connection with the traversal server by creating a traversal client zone on your local Expressway. You then configure the client zone with details of the corresponding zone on the traversal server. (The traversal server must also be configured with details of the Expressway client zone.)

After you have neighbored with the traversal server you can:

- use the neighbor as a traversal server
- query the traversal server about its endpoints
- apply transforms to any queries before they are sent to the traversal server
- control the bandwidth used for calls between your local Expressway and the traversal server

For full details on how traversal client zones and traversal server zones work together to achieve firewall traversal, see [About firewall traversal \[p.45\]](#).

An [NTP server](#) must be configured for traversal zones to work.

The configurable options for a traversal client zone are:

| Field                                  | Description  | Usage tips  |
|--|--|---|
| <b>Configuration</b> section:          |  |   |
| <b>Name</b>                            | The name acts as a unique identifier, allowing you to distinguish between zones of the same type.  |   |
| <b>Type</b>                            | The nature of the specified zone, in relation to the local Expressway. Select <i>Traversal client</i> .  | After a zone has been created, the <b>Type</b> cannot be changed.   |
| <b>Hop count</b>                       | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the <a href="#">Hop counts</a> section for more information). This field specifies the hop count to use when sending a search request to this particular zone. | If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used. |
| <b>Connection credentials</b> section: |  |   |
| <b>Username and Password</b>           | Traversal clients must always authenticate with traversal servers by providing their authentication credentials. Each traversal client zone must specify a <b>Username</b> and <b>Password</b> to be used for authentication with the traversal server.                | Multiple traversal client zones can be configured, each with distinct credentials, to connect to one or more service providers. |
| <b>H.323</b> section:                  |  |   |
| <b>Mode</b>                            | Determines whether H.323 calls are allowed to and from the traversal server.   |   |
| <b>Protocol</b>                        | Determines which of the two firewall traversal protocols ( <i>Assent</i> or <i>H.460.18</i> ) to use for calls to the traversal server.  | See <a href="#">Configuring ports for firewall traversal [p.50]</a> for more information.                                       |

| Field                                  | Description  | Usage tips  |
|--|--|---|
| <b>Port</b>                            | The port on the traversal server to use for H.323 calls to and from the local Expressway.  | For firewall traversal to work via H.323, the traversal server must have a traversal server zone configured on it to represent this Expressway, using this same port number.  |
| <b>SIP</b> section:                    |  |   |
| <b>Mode</b>                            | Determines whether SIP calls are allowed to and from the traversal server.   |   |
| <b>Port</b>                            | The port on the traversal server to use for SIP calls to and from the Expressway.<br><br>This must be different from the listening ports used for incoming TCP, TLS and UDP SIP calls (typically 5060 and 5061).   | For firewall traversal to work via SIP, the traversal server must have a traversal server zone configured on it to represent this Expressway, using this same transport type and port number.                               |
| <b>Unified Communications services</b> | Controls whether this traversal zone provides Unified Communications services, such as mobile and remote access.   | If enabled, this zone must also be configured to use TLS with <b>TLS verify mode</b> enabled.<br><br>This setting only applies when <a href="#">Unified Communications mode</a> is set to <i>Mobile and remote access</i> . |
| <b>Transport</b>                       | Determines which transport type is used for SIP calls to and from the traversal server. The default is <i>TLS</i> .  |   |
| <b>TLS verify mode</b>                 | Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal server when communicating over TLS.  | See <a href="#">TLS certificate verification of neighbor systems [p.133]</a> for more information.  |
| <b>Media encryption mode</b>           | Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone.  | See <a href="#">Configuring media encryption policy [p.115]</a> for more information.   |
| <b>ICE support</b>                     | Controls whether ICE messages are supported by the devices in this zone.   | See <a href="#">Configuring ICE messaging support [p.116]</a> for more information.   |
| <b>Poison mode</b>                     | Determines if SIP requests sent to systems located via this zone are "poisoned" such that if they are received by this Expressway again they will be rejected.   |   |
| <b>Authentication</b> section:         |  |   |
| <b>Authentication policy</b>           | Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. | See <a href="#">Authentication policy configuration options [p.110]</a> for more information.   |
| <b>Client settings</b> section:        |  |   |

| Field                           | Description  | Usage tips  |
|---------------------------------|--|---|
| <b>Retry interval</b>           | The interval in seconds with which a failed attempt to establish a connection to the traversal server should be retried.                     |   |
| <b>Location</b> section:        |  |   |
| <b>Peer 1 to Peer 6 address</b> | The IP address or FQDN of the traversal server.<br>If the traversal server is an Expressway-E cluster, this should include all of its peers. | See <a href="#">Neighboring between Expressway clusters [p.141]</a> for more information. |

## Configuring traversal server zones

An Expressway-E can act as a traversal server, providing firewall traversal on behalf of traversal clients (an Expressway-C).

For firewall traversal to work, the traversal server (Expressway-E) must have a special type of two-way relationship with each traversal client. To create this connection between a Expressway-E and a Expressway-C, see [Configuring a traversal client and server \[p.49\]](#). For full details on how traversal client zones and traversal server zones work together to achieve firewall traversal, see [About firewall traversal \[p.45\]](#).

**Note:** You must synchronize with an [NTP server](#) to make sure that traversal zones to work.

After you have neighbored with the traversal client you can:

- provide firewall traversal services to the traversal client
- query the traversal client about its endpoints
- apply transforms to any queries before they are sent to the traversal client
- control the bandwidth used for calls between your local Expressway and the traversal client
- view zone status information, including the connection addresses

**Note:** Connection addresses listed in the status information may have been translated by a NAT element between the traversal server zone and the originating device.

Table 5: Traversal server zone configuration reference

| Field                                  | Description  | Usage tips  |
|--|--|---|
| <b>Configuration</b> section:          |  |   |
| <b>Name</b>                            | The name acts as a unique identifier, allowing you to distinguish between zones of the same type.  |   |
| <b>Type</b>                            | The nature of the specified zone, in relation to the local Expressway. Select <i>Traversal server</i> .  | After a zone has been created, the <b>Type</b> cannot be changed.   |
| <b>Hop count</b>                       | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the <a href="#">Hop counts</a> section for more information). This field specifies the hop count to use when sending a search request to this particular zone. | If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used. |
| <b>Connection credentials</b> section: |  |   |

Table 5: Traversal server zone configuration reference (continued)

| Field                                  | Description   | Usage tips  |
|--|---|---|
| <b>Username</b>                        | <p>Traversal clients must always authenticate with traversal servers by providing their authentication credentials.</p> <p>The authentication username is the name that the traversal client must provide to the Expressway-E. (It is configured as the connection credentials <b>Username</b> in its traversal client zone.)</p> | <p>There must also be an entry in the Expressway-E's local authentication database for the client's authentication username and password. To check the list of entries and add it if necessary, go to the <a href="#">Local authentication database</a> page. Either:</p> <ul style="list-style-type: none"> <li>■ click on the <a href="#">Add/Edit local authentication database</a> link</li> <li>■ go to <a href="#">Configuration &gt; Authentication &gt; Local database</a></li> </ul> |
| <b>H.323</b> section:                  |   |   |
| <b>Mode</b>                            | Determines whether H.323 calls are allowed to and from the traversal client.  |   |
| <b>Protocol</b>                        | Determines the protocol ( <i>Assent</i> or <i>H.460.18</i> ) to use to traverse the firewall/NAT.   | See <a href="#">Configuring ports for firewall traversal [p.50]</a> for more information.   |
| <b>Port</b>                            | The port on the local Expressway-E to use for H.323 calls to and from the traversal client.   |   |
| <b>H.460.19 demultiplexing mode</b>    | <p>Determines whether or not the same two ports are used for media by two or more calls.</p> <p><i>On</i>: all calls from the traversal client use the same two ports for media.</p> <p><i>Off</i>: each call from the traversal client uses a separate pair of ports for media.</p>  |   |
| <b>SIP</b> section:                    |   |   |
| <b>Mode</b>                            | Determines whether SIP calls are allowed to and from the traversal client.  |   |
| <b>Port</b>                            | The port on the local Expressway-E to use for SIP calls to and from the traversal client.   | This must be different from the listening ports used for incoming TCP, TLS and UDP SIP calls (typically 5060 and 5061).   |
| <b>Transport</b>                       | Determines which transport type is used for SIP calls to and from the traversal client. The default is <i>TLS</i> .   |   |
| <b>Unified Communications services</b> | Controls whether this traversal zone provides Unified Communications services, such as mobile and remote access.  | <p>If enabled, this zone must also be configured to use TLS with <b>TLS verify mode</b> enabled.</p> <p>This setting only applies when <a href="#">Unified Communications mode</a> is set to <i>Mobile and remote access</i>.</p>   |

Table 5: Traversal server zone configuration reference (continued)

| Field                                   | Description  | Usage tips  |
|---|--|---|
| <b>TLS verify mode and subject name</b> | Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client.<br><br>If <b>TLS verify mode</b> is enabled, a <b>TLS verify subject name</b> must be specified. This is the certificate holder's name to look for in the traversal client's X.509 certificate.          | If the traversal client is clustered, the <b>TLS verify subject name</b> must be the FQDN of the cluster.<br><br>See <a href="#">TLS certificate verification of neighbor systems [p.133]</a> for more information. |
| <b>Media encryption mode</b>            | Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone.  | See <a href="#">Configuring media encryption policy [p.115]</a> for more information.   |
| <b>ICE support</b>                      | Controls whether ICE messages are supported by the devices in this zone.   | See <a href="#">Configuring ICE messaging support [p.116]</a> for more information.   |
| <b>Poison mode</b>                      | Determines if SIP requests sent to systems located via this zone are "poisoned" such that if they are received by this Expressway again they will be rejected.   |   |
| <b>Authentication</b> section:          |  |   |
| <b>Authentication policy</b>            | Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. | See <a href="#">Authentication policy configuration options [p.110]</a> for more information.   |
| <b>UDP / TCP probes</b> section:        |  |   |
| <b>UDP retry interval</b>               | The frequency (in seconds) with which the client sends a UDP probe to the Expressway-E if a keep alive confirmation has not been received.   | The default UDP and TCP probe retry intervals are suitable for most situations. However, if you experience problems with NAT bindings timing out, they may need to be changed.                                      |
| <b>UDP retry count</b>                  | The number of times the client attempts to send a UDP probe to the Expressway-E during call setup.   |   |
| <b>UDP keep alive interval</b>          | The interval (in seconds) with which the client sends a UDP probe to the Expressway-E after a call is established, in order to keep the firewall's NAT bindings open.  |   |
| <b>TCP retry interval</b>               | The interval (in seconds) with which the traversal client sends a TCP probe to the Expressway-E if a keep alive confirmation has not been received.  |   |
| <b>TCP retry count</b>                  | The number of times the client attempts to send a TCP probe to the Expressway-E during call setup.   |   |
| <b>TCP keep alive interval</b>          | The interval (in seconds) with which the traversal client sends a TCP probe to the Expressway-E when a call is in place, in order to maintain the firewall's NAT bindings.   |   |

## Configuring ENUM zones

ENUM zones allow you to locate endpoints via an ENUM lookup. You can create one or more search rules for ENUM zones based on the ENUM DNS suffix used and/or by pattern matching of the endpoints' aliases.

After you have configured one or more ENUM zones, you can:

- apply transforms to alias search requests directed to that group of endpoints
- control the bandwidth used for calls between your local Expressway and each group of ENUM endpoints

Full details of how to use and configure ENUM zones are given in the [About ENUM dialing \[p.170\]](#) section.

The configurable options for an ENUM zone are:

| Field             | Description  | Usage tips  |
|-------------------|--|---|
| <b>Name</b>       | The name acts as a unique identifier, allowing you to distinguish between zones of the same type.  |   |
| <b>Type</b>       | The nature of the specified zone, in relation to the local Expressway. Select <i>ENUM</i> .  | After a zone has been created, the <b>Type</b> cannot be changed.   |
| <b>Hop count</b>  | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the <a href="#">Hop counts</a> section for more information). This field specifies the hop count to use when sending a search request to this particular zone. | If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used. |
| <b>DNS suffix</b> | The domain to be appended to the transformed E.164 number to create an ENUM domain for which this zone is queried.   |   |
| <b>H.323 mode</b> | Determines whether H.323 records are looked up for this zone.  |   |
| <b>SIP mode</b>   | Determines whether SIP records are looked up for this zone.  |   |

## Configuring DNS zones

DNS zones allow you to locate endpoints via a DNS lookup. You can create one or more search rules for DNS zones based on pattern matching of the endpoints' aliases.

After you have configured one or more DNS zones, you can:

- apply transforms to alias search requests directed to that group of endpoints
- control the bandwidth used for calls between your local Expressway and each group of DNS endpoints

The configurable options for a DNS zone are:

| Field       | Description   | Usage tips  |
|-------------|---|---|
| <b>Name</b> | The name acts as a unique identifier, allowing you to distinguish between zones of the same type. |   |
| <b>Type</b> | The nature of the specified zone, in relation to the local Expressway. Select <i>DNS</i> .        | After a zone has been created, the <b>Type</b> cannot be changed. |

| Field                                   | Description  | Usage tips  |
|---|--|---|
| <b>Hop count</b>                        | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the <a href="#">Hop counts</a> section for more information). This field specifies the hop count to use when sending a search request to this particular zone.   | If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used.   |
| <b>H.323 mode</b>                       | Determines whether H.323 calls are allowed to systems and endpoints located using DNS lookups via this zone.   |   |
| <b>SIP mode</b>                         | Determines whether SIP calls are allowed to systems and endpoints located using DNS lookups via this zone.   |   |
| <b>TLS verify mode and subject name</b> | Controls whether the Expressway performs X.509 certificate checking against the destination system server returned by the DNS lookup.<br><br>If <b>TLS verify mode</b> is enabled, a <b>TLS verify subject name</b> must be specified. This is the certificate holder's name to look for in the destination system server's X.509 certificate. | This setting only applies if the DNS lookup specifies TLS as the required protocol. If TLS is not required then the setting is ignored.<br>See <a href="#">TLS certificate verification of neighbor systems [p.133]</a> for more information. |
| <b>TLS verify subject name</b>          | The certificate holder's name to look for in the destination system server's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes).   |   |
| <b>Fallback transport protocol</b>      | The transport type to use for SIP calls from the DNS zone, when DNS NAPTR records and SIP URI parameters do not provide the preferred transport information.<br><br>The default is <i>UDP</i> (if enabled).  |   |
| <b>Media encryption mode</b>            | Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to the internet.  | See <a href="#">Configuring media encryption policy [p.115]</a> for more information.   |
| <b>ICE support</b>                      | Controls whether ICE messages are supported by the devices in this zone.   | See <a href="#">Configuring ICE messaging support [p.116]</a> for more information.   |
| <b>Zone profile</b>                     | Determines how the zone's advanced settings are configured.<br><br><i>Default:</i> uses the factory default profile.<br><br><i>Custom:</i> allows you to configure each setting individually.  | See <a href="#">Zone configuration: advanced settings [p.128]</a> for details on the advanced settings.<br><br>Only use the <i>Custom</i> profile to configure the individual advanced settings on the advice of Cisco customer support.      |

## Zone configuration: advanced settings

The table below describes the advanced zone configuration options for the *Custom* zone profile. Some of these settings only apply to specific zone types.



| Setting  | Description   | Default | Zone types      |
|--|---|---------|-----------------|
| <b>Monitor peer status</b>                     | Specifies whether the Expressway monitors the status of the zone's peers. If enabled, H.323 LRQs and/or SIP OPTIONS are periodically sent to the peers. If a peer fails to respond, that peer is marked as inactive. If all peers fail to respond the zone is marked as inactive.   | Yes     | Neighbor        |
| <b>Call signaling routed mode</b>              | Specifies how the Expressway handles the signaling for calls to and from this neighbor.<br><br><i>Auto</i> : signaling is taken as determined by the <b>Call signaling optimization (Configuration &gt; Call routing)</b> configuration.<br><br><i>Always</i> : signaling is always taken for calls to or from this neighbor, regardless of the <b>Call signaling optimization</b> configuration.<br><br>Calls via traversal zones or the B2BUA always take the signaling.  | Auto    | Neighbor        |
| <b>Automatically respond to H.323 searches</b> | Determines what happens when the Expressway receives an H.323 search, destined for this zone.<br><br><i>Off</i> : an LRQ message is sent to the zone.<br><br><i>On</i> : searches are responded to automatically, without being forwarded to the zone.  | Off     | Neighbor        |
| <b>H.323 call signaling port</b>               | Specifies the port on the neighbor to be used for H.323 calls to and from this Expressway.<br><br>This setting only applies if <b>Automatically respond to H.323 searches</b> is <i>On</i> (which includes when the <i>Infrastructure device</i> profile is selected), as the search process normally identifies which call signaling port to use.  | 1720    | Neighbor        |
| <b>Automatically respond to SIP searches</b>   | Determines what happens when the Expressway receives a SIP search that originated as an H.323 search.<br><br><i>Off</i> : a SIP OPTIONS or SIP INFO message is sent.<br><br><i>On</i> : searches are responded to automatically, without being forwarded.<br><br>This should normally be left as the default <i>Off</i> . However, some systems do not accept SIP OPTIONS messages, so for these zones it must be set to <i>On</i> . If you change this to <i>On</i> , you must also configure pattern matches to ensure that only those searches that actually match endpoints in this zone are responded to. If you do not, the search will not continue to other lower-priority zones, and the call will be forwarded to this zone even if it cannot support it. | Off     | Neighbor<br>DNS |

| Setting  | Description  | Default | Zone types  |
|--|--|---------|---|
| <b>Send empty INVITE for interworked calls</b> | <p>Determines whether the Expressway generates a SIP INVITE message with no SDP to send via this zone. INVITES with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323.</p> <p><i>On:</i> SIP INVITES with no SDP are generated.</p> <p><i>Off:</i> SIP INVITES are generated and a pre-configured SDP is inserted before the INVITES are sent.</p> <p>In most cases this option should normally be left as the default <i>On</i>. However, some devices do not accept invites with no SDP, so for these zones this should be set to <i>Off</i>.</p> <p>Note that the settings for the pre-configured SDP are configurable via the CLI using the <code>xConfiguration Zones Zone [1..1000] [Neighbor/DNS] Interworking SIP</code> commands. They should only be changed on the advice of Cisco customer support.</p> | On      | Neighbor<br>DNS   |
| <b>SIP poison mode</b>                         | <p><i>On:</i> SIP requests sent to systems located via this zone are "poisoned" such that if they are received by this Expressway again they will be rejected.</p> <p><i>Off:</i> SIP requests sent out via this zone that are received by this Expressway again will not be rejected; they will be processed as normal.</p>   | Off     | Neighbor<br>Traversal client<br>Traversal server<br>DNS |
| <b>SIP encryption mode</b>                     | <p>Determines whether or not the Expressway allows encrypted SIP calls on this zone.</p> <p><i>Auto:</i> SIP calls are encrypted if a secure SIP transport (TLS) is used.</p> <p><i>Microsoft:</i> SIP calls are encrypted using MS-SRTP.</p> <p><i>Off:</i> SIP calls are never encrypted.</p> <p>This option should normally be left as the default <i>Auto</i>.</p>   | Auto    | Neighbor  |
| <b>SIP REFER mode</b>                          | <p>Determines how SIP REFER requests are handled.</p> <p><i>Forward:</i> SIP REFER requests are forwarded to the target.</p> <p><i>Terminate:</i> SIP REFER requests are terminated by the Expressway.</p>   | Forward | Neighbor  |
| <b>SIP SDP attribute line limit mode</b>       | <p>Determines whether requests containing SDP sent out to this zone have the length of <code>a=fmtp</code> lines restricted.</p> <p><i>On:</i> the length is truncated to the maximum length specified by the SIP SDP attribute line limit length setting.</p> <p><i>Off:</i> the length is not truncated.</p> <p>The <b>SIP SDP attribute line limit</b> option should normally be left as the default of <i>Off</i>. However, some systems cannot handle attribute lines longer than 130 characters, so it must be set to <i>On</i> for connections to these systems.</p>  | Off     | Neighbor<br>DNS   |
| <b>SIP SDP attribute line limit length</b>     | <p>If <b>SIP SDP attribute line limit mode</b> is set to <i>On</i>, sets the maximum line length of <code>a=fmtp</code> SDP lines.</p>   | 130     | Neighbor<br>DNS   |
| <b>SIP multipart MIME strip mode</b>           | <p>Controls whether or not multipart MIME stripping is performed on requests from this zone.</p> <p>This option should normally be left as the default <i>Off</i>.</p>   | Off     | Neighbor  |

| Setting                                 | Description  | Default | Zone types      |
|---|--|---------|-----------------|
| <b>SIP UPDATE strip mode</b>            | <p>Controls whether or not the Expressway strips the UPDATE method from the Allow header of all requests and responses received from, and sent to, this zone.</p> <p>This option should normally be left as the default <i>Off</i>. However, some systems do not support the UPDATE method in the Allow header, so for these zones this should be set to <i>On</i>.</p>  | Off     | Neighbor        |
| <b>Interworking SIP search strategy</b> | <p>Determines how the Expressway searches for SIP endpoints when interworking an H.323 call.</p> <p><i>Options</i>: the Expressway sends an OPTIONS request.</p> <p><i>Info</i>: the Expressway sends an INFO request.</p> <p>This option should normally be left as the default <i>Options</i>. However, some endpoints cannot respond to OPTIONS requests, so this must be set to <i>Info</i> for such endpoints.</p>  | Options | Neighbor        |
| <b>SIP UDP/BFCP filter mode</b>         | <p>Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol.</p> <p><i>On</i>: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled.</p> <p><i>Off</i>: INVITE requests are not modified.</p>   | Off     | Neighbor<br>DNS |
| <b>SIP UDP/IX filter mode</b>           | <p>Determines whether INVITE requests sent to this zone filter out UDP/UDT/IX or UDP/DTLS/UDT/IX. This option may be required to enable interoperability with SIP devices that do not support the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol.</p> <p><i>On</i>: any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled.</p> <p><i>Off</i>: INVITE requests are not modified.</p> <p>We recommend that <b>SIP UDP/IX filter mode</b> is set to <i>On</i> for:</p> <ul style="list-style-type: none"> <li>■ business-to-business calls routed through neighbor zones that connect to external networks / non-Cisco infrastructure</li> <li>■ calls that connect internally to Unified CM 8.x or earlier (use <i>Off</i> for 9.x or later)</li> </ul> | Off     | Neighbor<br>DNS |
| <b>SIP Duo Video filter mode</b>        | <p>Determines whether INVITE requests sent to this zone filter out Duo Video. This option may be required to enable interoperability with SIP devices that do not support Duo Video.</p> <p><i>On</i>: the second video line in any outgoing INVITE request is removed.</p> <p><i>Off</i>: INVITE requests are not modified.</p>   | Off     | Neighbor<br>DNS |
| <b>SIP record route address type</b>    | <p>Controls whether the Expressway uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone.</p> <p><i>IP</i>: uses the Expressway's IP address.</p> <p><i>Hostname</i>: uses the Expressway's <b>System host name</b> (if it is blank the IP address is used instead).</p>  | IP      | Neighbor<br>DNS |

| Setting                                    | Description  | Default | Zone types |
|--|--|---------|------------|
| <b>SIP Proxy-Require header strip list</b> | A comma-separated list of option tags to search for and remove from Proxy-Require headers in SIP requests received from this zone.   | None    | Neighbor   |
| <b>Include address record</b>              | <p>Determines whether, if no NAPTR (SIP) or SRV (SIP and H.323) records have been found for the dialed alias via this zone, the Expressway will then query for A and AAAA DNS records before moving on to query lower priority zones. If A and AAAA records exist at the same domain for systems other than those that support SIP or H.323, this may result in the Expressway believing the search was successful and forwarding calls to this zone, and the call will fail.</p> <p><i>On:</i> the Expressway queries for A or AAAA records. If any are found, the Expressway will not then query any lower priority zones.</p> <p><i>Off:</i> the Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.</p> | Off     | DNS        |

## Zone configuration: pre-configured profile settings

The table below shows the advanced zone configuration option settings that are automatically applied for each of the pre-configured profiles.

| Setting                                 | Cisco Unified Communications Manager | Cisco Unified Communications Manager (8.6.1 or later) | Nortel Communication Server 1000 | Infrastructure device | Default |
|---|--------------------------------------|---|----------------------------------|-----------------------|---------|
| Monitor peer status                     | Yes                                  | Yes   | Yes                              | No                    | Yes     |
| Call signaling routed mode              | Always                               | Always  | Auto                             | Always                | Auto    |
| Automatically respond to H.323 searches | Off                                  | Off   | Off                              | On                    | Off     |
| H.323 call signaling port               | 1720                                 | 1720  | 1720                             | 1720                  | 1720    |
| Automatically respond to SIP searches   | Off                                  | Off   | Off                              | On                    | Off     |
| Send empty INVITE for interworked calls | On                                   | On  | On                               | On                    | On      |
| SIP poison mode                         | Off                                  | Off   | Off                              | Off                   | Off     |
| SIP encryption mode                     | Auto                                 | Auto  | Auto                             | Auto                  | Auto    |
| SIP REFER mode                          | Forward                              | Forward   | Forward                          | Forward               | Forward |
| SIP SDP attribute line limit mode       | Off                                  | Off   | Off                              | Off                   | Off     |
| SIP SDP attribute line limit length     | 130                                  | 130   | 130                              | 130                   | 130     |
| SIP multipart MIME strip mode           | Off                                  | Off   | Off                              | Off                   | Off     |

| Setting                             | Cisco Unified Communications Manager | Cisco Unified Communications Manager (8.6.1 or later) | Nortel Communication Server 1000 | Infrastructure device | Default |
|-------------------------------------|--------------------------------------|---|----------------------------------|-----------------------|---------|
| SIP UPDATE strip mode               | Off                                  | Off   | On                               | Off                   | Off     |
| Interworking SIP search strategy    | Options                              | Options   | Options                          | Options               | Options |
| SIP UDP/BFCP filter mode            | On                                   | Off   | Off                              | Off                   | Off     |
| SIP UDP/IX filter mode              | On                                   | On  | On                               | On                    | Off     |
| SIP Duo Video filter mode           | Off                                  | Off   | Off                              | Off                   | Off     |
| SIP record route address type       | IP                                   | IP  | IP                               | IP                    | IP      |
| SIP Proxy-Require header strip list | <blank>                              | <blank>   | "com.nortelnetworks.firewall"    | <blank>               | <blank> |

For more information about configuring a SIP trunk between Expressway and Unified CM, see [Cisco Unified Communications Manager with Expressway Deployment Guide](#).

## TLS certificate verification of neighbor systems

When a SIP TLS connection is established between an Expressway and a neighbor system, the Expressway can be configured to check the X.509 certificate of the neighbor system to verify its identity. You do this by configuring the zone's **TLS verify mode** setting.

If **TLS verify mode** is enabled, the neighbor system's FQDN or IP address, as specified in the **Peer address** field of the zone's configuration, is used to verify against the certificate holder's name contained within the X.509 certificate presented by that system. (The name has to be contained in either the Subject Common Name or the Subject Alternative Name attributes of the certificate.) The certificate itself must also be valid and signed by a trusted certificate authority.

Note that for traversal server and DNS zones, the FQDN or IP address of the connecting traversal client is not configured, so the required certificate holder's name is specified separately.

If the neighbor system is another Expressway, or it is a traversal client / traversal server relationship, the two systems can be configured to authenticate each other's certificates. This is known as mutual authentication and in this case each Expressway acts both as a client and as a server and therefore you must ensure that each Expressway's certificate is valid both as a client and as a server.

See [About security certificates \[p.223\]](#) for more information about certificate verification and for instructions on uploading the Expressway's server certificate and uploading a list of trusted certificate authorities.

## Configuring a zone for incoming calls only

To configure a zone so that it is never sent an alias search request (for example if you only want to receive incoming calls from this zone), do not define any search rules that have that zone as its target.

In this scenario, when viewing the zone, you can ignore the warning indicating that search rules have not been configured.

# Clustering and peers

---

This section describes how to set up a cluster of Expressway peers. Clustering is used to increase the capacity of your Expressway deployment and to provide resiliency.

|  |     |
|--|-----|
| About clusters .....                               | 135 |
| License usage within a cluster .....               | 136 |
| Managing clusters and peers .....                  | 137 |
| Troubleshooting cluster replication problems ..... | 143 |

## About clusters

An Expressway can be part of a cluster of up to six Expressways. Each Expressway in the cluster is a peer of every other Expressway in the cluster. When creating a cluster, you define a cluster name and nominate one peer as the master from which all relevant configuration is replicated to the other peers in the cluster. Clusters are used to:

- Increase the capacity of your Expressway deployment compared with a single Expressway.
- Provide redundancy in the rare case that an Expressway becomes inaccessible (for example, due to a network or power outage) or while it is in [maintenance mode](#) (for example, during a software upgrade).

### About the configuration master

All peers in a cluster must have identical configuration for subzones, zones, links, pipes, authentication, bandwidth control and Call Policy. To achieve this, you define a cluster name and nominate one peer as the configuration master. Any configuration changes made to the master peer are then automatically replicated across all the other peers in the cluster.

You should only make configuration changes on the master Expressway. Any changes made on other peers are not reflected across the cluster, and will be overwritten the next time the master's configuration is replicated across the peers. The only exceptions to this are some [peer-specific configuration items](#).

You may need to wait up to one minute before changes are updated across all peers in the cluster.

### Secure communication between peers

The Expressway uses IPsec (Internet Protocol Security) to enable secure communication between each cluster peer. Authentication is carried out through the use of a pre-shared access key.

Each peer in the cluster must be individually configured with the IP address and associated access key of every other peer in that cluster.

## License usage within a cluster

The following types of licenses are pooled for use by any peer in a cluster, irrespective of which peer the licenses are installed on:

- Rich media session licenses
- TURN relay licenses

The maximum number of licenses that each Expressway system can use depends on the [type of appliance or VM](#):

Table 6: Maximum licenses that a peer can use

|                     | Small / Medium / CE500 systems | Large / CE1000 systems |
|---------------------|--------------------------------|------------------------|
| Rich media sessions | 150                            | 500                    |
| TURN relays *       | 1800                           | 6000                   |

\* On a Large system, the total TURN capacity of 6000 relays is spread evenly across 6 ports; each port is limited to handling 1000 relays. On a Small/Medium system, there is a single TURN port that handles up to 1800 relays.

You can cluster up to 6 Expressway systems to increase capacity by a maximum factor of 4 (see [Performance capabilities \[p.281\]](#) for more information).

If a cluster peer becomes unavailable, the shareable licenses installed on that peer remain available to the rest of the cluster peers for two weeks from the time the cluster lost contact with the peer. This will maintain the overall license capacity of the cluster — however, note that each peer is limited by its physical capacity. After this two week period, the licenses associated with the unavailable peer are removed from the cluster. To maintain the same capacity for your cluster, you should ensure that either the problem with the peer is resolved or new option keys are installed on another peer in the cluster.

You can see a summary of all of the call and TURN relay licenses installed on each cluster peer by going to the [Option keys](#) page and scrolling down to the [Current licenses](#) section.

Capacity alarms are raised if either of the following usage thresholds are reached:

- the number of concurrent calls reaches 90% of the capacity of the cluster
- the number of concurrent calls on any one unit reaches 90% of the physical capacity of the unit



# Managing clusters and peers

## Setting up a cluster

Before setting up a cluster of X8.5.2 Expressway peers or adding an X8.5.2 Expressway to a cluster, ensure that:

- All clusters peers are running the same version of code. The only occasion where different peers are allowed to run different versions of code is for the short period of time while a cluster is being upgraded from one version of code to another, during which time the cluster will operate in a partitioned fashion.
- A DNS SRV record is available for the cluster which contains A or AAAA records for each peer of the cluster.
- Each peer has a different LAN configuration (a different IPv4 address and a different IPv6 address, where enabled).
- Each peer in a cluster is within a 15ms hop (30ms round trip delay) of each and every other Expressway in or to be added to the cluster.
- Each peer in a cluster is directly routable to each and every other Expressway in or to be added to the cluster. (There must be no NAT between cluster peers – if there is a firewall ensure that the required ports are opened.)
- Each peer is using a hardware platform (appliance or virtual machine) with equivalent capabilities; for example, you can cluster peers that are running on standard appliances with peers running on 2 core Medium VMs, but you cannot cluster a peer running on a standard appliance with peers running on 8 core Large VMs.
- All peers have the same set of option keys installed:
  - The number of call license keys may be different on different peers; all other license keys must be identical on each peer.
  - The Expressway must be restarted after installing some option keys in order to fully activate them.
- Each peer has a different system name.
- H.323 mode is enabled on each peer (**Configuration > Protocols > H.323**, and for **H.323 mode** select *On*); even if all endpoints in the cluster are SIP only, H.323 signaling is used for endpoint location searching and sharing bandwidth usage information with other peers in the cluster.
- The Expressway cluster has a DNS SRV record that defines all cluster peers.
- The DNS servers used by the Expressway peers must support both forward and reverse DNS lookups of all Expressway peer addresses; the DNS servers must also provide address lookup for any other DNS functionality required, such as:
  - NTP servers or the external manager if they configured using DNS names
  - Microsoft Lync Server FQDN lookup
  - LDAP server forward and reverse lookup (reverse lookups are frequently provided through PTR records).Note that DNS server configuration is specific to each peer.

Then, to create your cluster you must first configure a master peer and then add the other peers into the cluster one-by-one.

You are recommended to backup your Expressway data before setting up a cluster.

A full step-by-step guide to setting up and configuring clusters is available in the [Expressway Cluster Creation and Maintenance Deployment Guide](#).

## Maintaining a cluster

The **Clustering** page (**System > Clustering**) lists the IP addresses of all the peers in the cluster, to which this Expressway belongs, and identifies the master peer.

### Cluster name

The **Cluster name** is used to identify one cluster of Expressways from another. Set it to the fully qualified domain name (FQDN) used in SRV records that address this Expressway cluster, for example `cluster1.example.com`.

The FQDN can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter.

### Cluster pre-shared key

The Expressway uses IPsec (Internet Protocol Security) to enable secure communication between each cluster peer.

The **Cluster pre-shared key** is the common IPsec access key used by each peer to access every other peer in the cluster.

---

**Note:** each peer in the cluster must be configured with the same **Cluster pre-shared key**.

---

### Setting configuration for the cluster

You should only make configuration changes on the master Expressway. Any changes made on other peers are not reflected across the cluster, and will be overwritten the next time the master's configuration is replicated across the peers. The only exceptions to this are some [peer-specific configuration items](#).

You may need to wait up to one minute before changes are updated across all peers in the cluster.

## Adding and removing peers from a cluster

After a cluster has been set up you can add new peers to the cluster or remove peers from it.

Note that:

- Systems that are configured as peers must not also be configured as neighbors to each other, and vice versa.
- If peers are deployed on different LANs, there must be sufficient connectivity between the networks to ensure a low degree of latency between the peers - a maximum delay of 15ms one way, 30ms round-trip.
- Cluster peers can be in separate subnets. Peers communicate with each other using H.323 messaging, which can be transmitted across subnet boundaries.
- Deploying all peers in a cluster on the same LAN means they can be configured with the same routing information such as local domain names and local domain subnet masks.

## Changing the master peer

You should only need to change the **Configuration master** when:

- the original master peer fails
- you want to take the master Expressway unit out of service

Note that if the master fails, the remaining peers will continue to function normally, except they are no longer able to copy their configuration from the master so they may become out of sync with each other.

To change the master peer you must log in to every other Expressway in the cluster and change the configuration master on each peer:

1. Log in to the Expressway and go to **System > Clustering**.
2. Change the **Configuration master** to the peer you want to set as the new master (the numbers match against the **Peer IP address** fields underneath).
3. Click **Save**.
4. Repeat this for every peer in the cluster, ensuring that you select the same new master on each peer.

Note that during this process you may see alarms raised on some peers about inconsistent master peer configuration. These alarms will be lowered when every peer in the cluster is configured with the new master.

## Monitoring the status of the cluster

The status sections at the bottom of the **Clustering** page show you the current status of the cluster, and the time of the previous and next synchronization.

## Specifying peer-specific items in clustered systems

Most items of configuration are applied via the master peer to all peers in a cluster. However, the following items (marked with a † on the web interface) must be specified separately on each cluster peer.

---

**Note:** You should not modify configuration data that applies to all peers on any peer other than the master peer. At best it will result in the changes being overwritten from the master; at worst it will cause cluster replication to fail.

---

### Cluster configuration (System > Clustering)

The list of **Peer IP addresses** (including the peer's own IP address) that make up the cluster has to be specified on each peer and they must be identical on each peer.

The **Cluster name** and **Cluster pre-shared key** have to be specified on each peer and must be identical for all peers.

### Ethernet speed (System > Network interfaces > Ethernet)

The **Ethernet speed** is specific to each peer. Each peer may have slightly different requirements for the connection to their Ethernet switch.

### IP configuration (System > Network interfaces > IP)

LAN configuration is specific to each peer.

- Each peer must have a different **IPv4 address** and a different **IPv6 address**.
- **IP gateway** configuration is peer-specific. Each peer can use a different gateway.

Note that the IP protocol is applied to all peers, because each peer must support the same protocols.

### IP static routes (System > Network interfaces > Static routes)

Any static routes you add are peer-specific and you may create different routes on different peers if required. If you want all peers in the cluster to be able to use the same static route, you must create the route on each

peer.

### System name (System > Administration)

The **System name** must be different for each peer in the cluster.

### DNS servers and DNS host name (System > DNS)

DNS servers are specific to each peer. Each peer can use a different set of DNS servers.

The **System host name** and **Domain name** are specific to each peer.

### NTP servers and time zone (System > Time)

The **NTP servers** are specific to each peer. Each peer may use one or more different NTP servers.

The **Time zone** is specific to each peer. Each peer may have a different local time.

### SNMP (System > SNMP)

SNMP settings are specific to each peer. They can be different for each peer.

### Logging (Maintenance > Logging)

The Event Log and Configuration Log on each peer only report activity for that particular Expressway. The **Log level** and the list of **Remote syslog servers** are specific to each peer. We recommend that you set up a remote syslog server to which the logs of all peers can be sent. This allows you to have a global view of activity across all peers in the cluster. See the [logging](#) section for further details.

### Security certificates (Maintenance > Security certificates)

The trusted CA certificate, server certificate and certificate revocation lists (CRLs) used by the Expressway must be uploaded individually per peer.

### Administration access (System > Administration)

The following system administration access settings are specific to each peer:

- Serial port / console
- SSH service
- Web interface (over HTTPS)
- Redirect HTTP requests to HTTPS
- Automated protection service

### Option keys (Maintenance > Option keys)

Option keys are specific to each peer. Each peer must have an identical set of option keys installed, but you must purchase these separately for each peer in the cluster. However, this does not apply to rich media session and TURN relay licenses; these licenses can be installed on any cluster peer and are available for use by any peer in the cluster.

## Sharing bandwidth across peers

When clustering has been configured, all peers share the bandwidth available to the cluster.

For general information on how the Expressway manages bandwidth, see the [bandwidth control](#) section.

## Cluster upgrades, backup and restore

### Upgrading a cluster

Instructions for upgrading and downgrading clusters are contained in [Expressway Cluster Creation and Maintenance Deployment Guide](#).

### Backing up a cluster

The [backup and restore](#) process can be used to save and restore cluster configuration information.

The backup process saves all configuration information for the cluster, regardless of the Expressway used to make the backup.

### Restoring a cluster

You cannot restore data to an Expressway that is a part of a cluster.

To restore previously backed up cluster configuration data you must follow this process:

1. Remove the Expressway peer from the cluster so that it becomes a standalone Expressway.
2. Restore the configuration data to the standalone Expressway.
3. Build a new cluster using the Expressway that now has the restored data.
4. Take each of the other peers out of their previous cluster and add them to the new cluster. See [Setting up a cluster \[p.137\]](#) for more information about adding and removing cluster peers.

## Neighboring between Expressway clusters

You can neighbor your local Expressway (or Expressway cluster) to a remote Expressway cluster; this remote cluster could be a neighbor, traversal client, or traversal server to your local Expressway. In this case, when a call is received on your local Expressway and is passed via the relevant zone to the remote cluster, it will be routed to whichever peer in that neighboring cluster has the lowest resource usage. That peer will then forward the call as appropriate to one of its external zones.

Lowest resource usage is determined by comparing the number of available media sessions (maximum - current use) on the peers, and choosing the peer with the highest number. Peers that are in maintenance mode are not considered.

When configuring a connection to a remote cluster, you create a single zone and configure it with details of all the peers in the cluster. Adding this information to the zone ensures that the call is passed to that cluster regardless of the status of the individual peers.

You also need to enter the IP address of all peers in the remote cluster when the connection is via a **neighbor** or **traversal client** zone. You do not do this for **traversal server** zones, as these connections are not configured by specifying the remote system's IP address.

---

**Note:** Systems that are configured as peers must **not** also be configured as neighbors to each other, and vice versa.

---

### Neighboring your clusters

To neighbor your local Expressway (or Expressway cluster) to a remote Expressway cluster, you create a single zone to represent the cluster and configure it with the details of all the peers in that cluster:

1. On your local Expressway (or, if the local Expressway is a cluster, on the master peer), create a zone of the appropriate type. This zone will represent the connection to the cluster.
2. In the **Location** section, enter the IP address or FQDN of each peer in the remote cluster in the **Peer 1** to **Peer 6** address fields.

Note that:

- Ideally you should use IP addresses in these fields. If you use FQDNs instead, each FQDN must be different and must resolve to a single IP address for each peer.
- The order in which the peers in the remote Expressway cluster are listed here does not matter.
- Whenever you add an extra Expressway to a cluster (to increase capacity or improve redundancy, for example) you will need to modify any Expressways which neighbor to that cluster to let them know about the new cluster peer.

# Troubleshooting cluster replication problems

Cluster replication can fail for a variety of reasons. This section describes the most common problems and how to resolve them.

More comprehensive information is available in [Expressway Cluster Creation and Maintenance Deployment Guide](#).

## Some peers have a different master peer defined

1. For each peer in the cluster, go to the **System > Clustering** page.
2. Ensure each peer identifies the same **Configuration master**.

## Unable to reach the cluster configuration master peer

The Expressway operating as the master peer could be unreachable for many reasons, including:

- network access problems
- Expressway unit is powered down
- incorrectly configured IP addresses
- incorrectly configured IPsec keys - ensure each peer is configured with the same **Cluster pre-shared key** value
- different software versions

## "Manual synchronization of configuration is required" alarms are raised on peer Expressways

1. Log in to the peer as **admin** through the CLI (available by default over SSH and through the serial port).
2. Type `xCommand ForceConfigUpdate`.

This will delete the non-master Expressway configuration and force it to update its configuration from the master Expressway.

---

**CAUTION:** never issue this command on the master Expressway, otherwise all configuration for the cluster will be lost.

---

# Dial plan and call processing

---

This section provides information about the pages that appear under the Calls, Dial plan, Transforms and Call Policy sub-menus of the **Configuration** menu. These pages are used to configure the way in which the Expressway receives and processes calls.

|   |     |
|---|-----|
| Call routing process .....                                | 145 |
| Configuring hop counts .....                              | 146 |
| Configuring dial plan settings .....                      | 147 |
| About transforms and search rules .....                   | 148 |
| Example searches and transforms .....                     | 154 |
| Configuring search rules to use an external service ..... | 160 |
| About Call Policy .....                                   | 163 |
| Supported address formats .....                           | 167 |
| Dialing by IP address .....                               | 169 |
| About ENUM dialing .....                                  | 170 |
| Configuring DNS servers for ENUM and URI dialing .....    | 176 |
| Configuring call routing and signaling .....              | 177 |
| Identifying calls .....                                   | 178 |
| Disconnecting calls .....                                 | 179 |



# Call routing process

One of the functions of the Expressway is to route calls to their appropriate destination. It does this by processing incoming search requests in order to locate the given target alias. These search requests are received from:

- neighboring systems, including neighbors, traversal clients and traversal servers
- endpoints on the public internet

There are a number of steps involved in determining the destination of a call, and some of these steps can involve transforming the alias or redirecting the call to other aliases.

It is important to understand the process before setting up your dial plan so you can avoid circular references, where an alias is transformed from its original format to a different format, and then back to the original alias. The Expressway is able to detect circular references. If it identifies one it will terminate that branch of the search and return a “policy loop detected” error message.

## How the Expressway determines the destination of a call

The process followed by the Expressway when attempting to locate a destination endpoint is described below.

1. The caller enters into their endpoint the alias or address of the destination endpoint. This alias or address can be in a number of [different address formats](#).
2. The destination address is received by the Expressway.
3. Any [pre-search transforms](#) are applied to the alias.
4. Any [Call Policy](#) is applied to the (transformed) alias. If this results in one or more new target aliases, the process starts again with the new aliases checked against the pre-search transforms.
5. The Expressway then searches for the alias according to its search rules:
  - A matching rule may apply a zone transform to the alias before sending the query on to its **Target**. A **Target** can be one of the following types:
    - **Neighbor zone**: one of the Expressway's configured external neighbor zones, or a DNS or ENUM lookup zone.
    - **Policy service**: an external service or application. The service will return some CPL which could, for example, specify the zone to which the call should be routed, or it could specify a new destination alias.
6. If the search returns a new URI or alias (for example, due to a DNS or ENUM lookup, or the response from a policy service), the process starts again: the new URI is checked against any pre-search transforms, Call Policy is applied and a new Expressway search is performed.
7. If the alias is found within one of the external zones, or a routing destination is returned by the policy service, the Expressway attempts to place the call.
8. If the alias is not found, it responds with a message to say that the call has failed.

# Configuring hop counts

Each search request is assigned a hop count value by the system that initiates the search. Every time the request is forwarded to another neighbor gatekeeper or proxy, the hop count value is decreased by a value of 1. When the hop count reaches 0, the request will not be forwarded on any further and the search will fail.

For search requests initiated by the local Expressway, the hop count assigned to the request is configurable on a zone-by-zone basis. The zone's hop count applies to all search requests originating from the local Expressway that are sent to that zone.

Search requests received from another zone will already have a hop count assigned. When the request is subsequently forwarded on to a neighbor zone, the lower of the two values (the original hop count or the hop count configured for that zone) is used.

For H.323, the hop count only applies to search requests. For SIP, the hop count applies to all requests sent to a zone (affecting the Max-Forwards field in the request).

The hop count value can be between 1 and 255. The default is 15.

---

**Note:** if your hop counts are set higher than necessary, you may risk introducing loops into your network. In these situations a search request will be sent around the network until the hop count reaches 0, consuming resources unnecessarily. This can be prevented by setting the [Call loop detection mode](#) to *On*.

---

When dialing by URI or ENUM, the hop count used is that for the associated DNS or ENUM zone via which the destination endpoint (or intermediary SIP proxy or gatekeeper) was found.

## Configuring hop counts for a zone

Hop counts are configured on a zone basis. To configure the hop count for a zone:

1. Go to the **Zones** page (**Configuration > Zones > Zones**).
2. Click on the name of the zone you want to configure. You are taken to the **Edit zone** page.
3. In the **Configuration** section, in the **Hop count** field, enter the hop count value you want to use for this zone.

For full details on other zone options, see the [Configuring zones \[p.119\]](#) section.

# Configuring dial plan settings

The **Dial plan configuration** page (**Configuration > Dial plan > Configuration**) is used to configure how the Expressway routes calls in specific call scenarios.

The configurable options are:

| Field                                | Description  | Usage tips   |
|--------------------------------------|--|--|
| <b>Calls to unknown IP addresses</b> | <p>Determines the way in which the Expressway attempts to call systems which are not registered with one of its neighbors.</p> <p><i>Direct:</i> allows an endpoint to make a call to an unknown IP address without the Expressway querying any neighbors.</p> <p><i>Indirect:</i> upon receiving a call to an unknown IP address, the Expressway queries its neighbors for the remote address and if permitted routes the call through the neighbor.</p> <p><i>Off:</i> calls to unknown IP addresses are not allowed.</p> <p>The default is <i>Indirect</i>.</p> | <p>This setting applies to the call's destination address prior to any zone transforms, but after any pre-search transforms or Call Policy rules have been applied.</p> <p>See <a href="#">Dialing by IP address [p.169]</a> for more information.</p> |
| <b>Fallback alias</b>                | <p>The alias to which incoming calls are placed for calls where the IP address or domain name of the Expressway has been given but no callee alias has been specified.</p>   | <p>If no fallback alias is configured, calls that do not specify an alias will be disconnected. See below for more information.</p>  |

## About the fallback alias

The Expressway could receive a call that is destined for it but which does not specify an alias. This could be for one of the following reasons:

- the caller has dialed the IP address of the Expressway directly
- the caller has dialed a domain name belonging to the Expressway (either one of its configured SIP domains, or any domain that has an SRV record that points at the IP address of the Expressway), without giving an alias as a prefix

Normally such calls would be disconnected. However, such calls will be routed to the **Fallback alias** if it is specified. Note that some endpoints do not allow users to enter an alias and an IP address to which the call should be placed.

### Example usage

You may want to configure your fallback alias to be that of your receptionist, so that all calls that do not specify an alias are still answered personally and can then be redirected appropriately.

For example, Example Inc has the domain of **example.com**. The endpoint at reception has the alias **reception@example.com**. They configure their Expressway with a fallback alias of **reception@example.com**. This means that any calls made directly to **example.com** (that is, without being prefixed by an alias), are forwarded to **reception@example.com**, where the receptionist can answer the call and direct it appropriately.

# About transforms and search rules

The Expressway can be configured to use transforms and search rules as a part of its call routing process.

## Transforms

Transforms are used to modify the alias in a search request if it matches certain criteria. You can transform an alias by removing or replacing its prefix, suffix, or the entire string, and by the use of regular expressions.

This transformation can be applied to the alias at two points in the routing process: as a pre-search transform, and as a zone transform.

- **Pre-search transforms** are applied before any Call Policy is applied and before the search process is performed (see [About pre-search transforms \[p. 148\]](#) for more details).
- **Zone transforms** are applied during the search process by each individual search rule as required. After the search rule has matched an alias they can be used to change the target alias before the search request is sent to a target zone or policy service (see [Search and zone transform process \[p. 150\]](#) for more details).

## Search rules

Search rules are used to route incoming search requests to the appropriate target zones or policy services.

The Expressway's search rules are highly configurable. You can:

- define alias, IP address and pattern matches to filter searches to specific zones or policy services
- define the priority (order) in which the rules are applied and stop applying any lower-priority search rules after a match is found; this lets you reduce the potential number of search requests sent out, and speed up the search process
- set up different rules according to the protocol (SIP or H.323) or the source of the query
- limit the range of destinations or network services available to unauthenticated devices by making specific search rules applicable to [authenticated requests](#) only
- use zone transforms to modify an alias before the query is sent to a target zone or policy service

Note that multiple search rules can refer to the same target zone or policy service. This means that you can specify different sets of search criteria and zone transforms for each zone or policy service.

The Expressway uses the protocol (SIP or H.323) of the incoming call when searching a zone for a given alias. If the search is unsuccessful the Expressway may then search the same zone again using the alternative protocol, depending on where the search came from and the **Interworking mode** ([Configuration > Protocols > Interworking](#)).

## About pre-search transforms

The pre-search transform function allows you to modify the alias in an incoming search request. The transformation is applied by the Expressway before any Call Policy is applied and before any searches take place.

- It applies to all incoming search requests received from neighbor, traversal client and traversal server zones, and endpoints on the public internet.
- It does not apply to requests received from peers (which are configured identically and therefore will have already applied the same transform).

Each pre-search transform defines a string against which an alias is compared, and the changes to make to the alias if it matches that string.

After the alias has been transformed, it remains changed and all further call processing is applied to the new alias.

### Pre-search transform process

Up to 100 pre-search transforms can be configured. Each transform must have a unique priority number between 1 and 65534.

Every incoming alias is compared with each transform in order of priority, starting with that closest to 1. If and when a match is made, the transform is applied to the alias and no further pre-search checks and transformations of the new alias will take place. The new alias is then used for the remainder of the [call routing process](#).

- Further transforms of the alias may take place during the remainder of the search process as a result of [Call Policy](#) (also known as Administrator Policy). If this is the case, the pre-search transforms are re-applied to the new alias.
- If you add a new pre-search transform that has the same priority as an existing transform, all transforms with a lower priority (those with a larger numerical value) will have their priority incremented by one, and the new transform will be added with the specified priority. However, if there are not enough “slots” left to move all the priorities down, you will get an error message.

## Configuring pre-search transforms

The [Transforms](#) page ([Configuration > Dial plan > Transforms](#)) lists all the [pre-search transforms](#) currently configured on the Expressway. It is used to create, edit, delete, enable and disable transforms.

Aliases are compared against each transform in order of **Priority**, until a transform is found where the alias matches the **Pattern** in the manner specified by the pattern **Type**. The alias is then transformed according to the **Pattern behavior** and **Replace string** rules before the search takes place (either locally or to external zones).

After the alias has been transformed, it remains changed. and all further call processing is applied to the new alias.

Note that transforms also apply to any [Unified Communications](#) messages.

The configurable options are:

| Field              | Description   | Usage tips   |
|--------------------|---|--|
| <b>Priority</b>    | The priority of the transform. Priority can be from 1 to 65534, with 1 being the highest priority. Transforms are applied in order of priority, and the priority must be unique for each transform. |  |
| <b>Description</b> | An optional free-form description of the transform.   | The description appears as a tooltip if you hover your mouse pointer over a transform in the list. |

| Field                   | Description   | Usage tips  |
|-------------------------|---|---|
| <b>Pattern type</b>     | <p>How the <b>Pattern string</b> must match the alias for the rule to be applied. Options are:</p> <p><i>Exact</i>: the entire string must exactly match the alias character for character.</p> <p><i>Prefix</i>: the string must appear at the beginning of the alias.</p> <p><i>Suffix</i>: the string must appear at the end of the alias.</p> <p><i>Regex</i>: treats the string as a <a href="#">regular expression</a>.</p> | <p>You can test whether a pattern matches a particular alias and is transformed in the expected way by using the <a href="#">Check pattern</a> tool (<b>Maintenance &gt; Tools &gt; Check pattern</b>).</p> |
| <b>Pattern string</b>   | <p>Specifies the pattern against which the alias is compared.</p>   | <p>The Expressway has a set of predefined <a href="#">pattern matching variables</a> that can be used to match against certain configuration elements.</p>  |
| <b>Pattern behavior</b> | <p>Specifies how the matched part of the alias is modified. Options are:</p> <p><i>Strip</i>: the matching prefix or suffix is removed.</p> <p><i>Replace</i>: the matching part of the alias is substituted with the text in the Replace string.</p> <p><i>Add Prefix</i>: prepends the <b>Additional text</b> to the alias.</p> <p><i>Add Suffix</i>: appends the <b>Additional text</b> to the alias.</p>                      |   |
| <b>Replace string</b>   | <p>The string to substitute for the part of the alias that matches the pattern.</p>   | <p>Only applies if the <b>Pattern behavior</b> is <i>Replace</i>.</p> <p>You can use regular expressions.</p>   |
| <b>Additional text</b>  | <p>The string to add as a prefix or suffix.</p>   | <p>Only applies if the <b>Pattern behavior</b> is <i>Add Prefix</i> or <i>Add Suffix</i>.</p>   |
| <b>State</b>            | <p>Indicates if the transform is enabled or not.</p>  | <p>Use this setting to test configuration changes, or to temporarily disable certain rules. Any disabled rules still appear in the rules list but are ignored.</p>  |

Click on the transform you want to configure (or click **New** to create a new transform, or click **Delete** to remove a transform).

## Search and zone transform process

The search rules and zone transform process is applied after all [pre-search transforms](#), and [Call Policy](#) have been applied.

The process is as follows:

1. The Expressway applies the search rules in priority order (all rules with a priority of 1 are processed first, then priority 2 and so on) to see if the given alias matches the rules criteria based on the **Source** of the query and the rule **Mode**.

2. If the match is successful, any associated zone transform (where the **Mode** is *Alias pattern match* and the **Pattern behavior** is *Replace* or *Strip*) is applied to the alias.
3. The search rule's **Target** zone or policy service is queried (with the revised alias if a zone transform has been applied) using the same protocol (SIP or H.323) as the incoming call request. Note that if there are many successful matches for multiple search rules at the same priority level, every applicable **Target** is queried.
  - If the alias is found, the call is forwarded to that zone. If the alias is found by more than one zone, the call is forwarded to the zone that responds first.
  - If the alias is not found using the native protocol, the query is repeated using the interworked protocol, depending on the [interworking mode](#).
  - If the search returns a new URI or alias (for example, due to an ENUM lookup, or the response from a policy service), the entire [Call routing process \[p. 145\]](#) starts again
4. If the alias is not found, the search rules with the next highest priority are applied (go back to step 1) until:
  - the alias is found, or
  - all target zones and policy services associated with search rules that meet the specified criteria have been queried, or
  - a search rule with a successful match has an **On successful match** setting of *Stop searching*

Note the difference between a successful match (where the alias matches the search rule criteria) and an alias being found (where a query sent to a target zone is successful). The *Stop searching* option provides better control over the network's signaling infrastructure. For example, if searches for a particular domain should always be routed to a specific zone this option lets you make the search process more efficient and stop the Expressway from searching any other zones unnecessarily.

## Configuring search rules

The [Search rules](#) page ([Configuration > Dial plan > Search rules](#)) is used to configure how the Expressway routes incoming search requests to the appropriate target zones (including the Local Zone) or policy services.

The page lists all the currently configured search rules and lets you create, edit, delete, enable and disable rules. You can click on a column heading to sort the list, for example by **Target** or **Priority**. If you hover your mouse pointer over a search rule, the rule description (if one has been defined) appears as a tooltip.

You can also copy and then edit any existing search rule by clicking **Clone** in the [Actions](#) column.

Up to 2000 search rules can be configured. Priority 1 search rules are applied first, followed by all priority 2 search rules, and so on.

The configurable options are:

| Field              | Description   | Usage tips  |
|--------------------|---|---|
| <b>Rule name</b>   | A descriptive name for the search rule.               |   |
| <b>Description</b> | An optional free-form description of the search rule. | The description appears as a tooltip if you hover your mouse pointer over a rule in the list. |

| Field                                | Description   | Usage tips   |
|--------------------------------------|---|--|
| <b>Priority</b>                      | The order in the search process that this rule is applied, when compared to the priority of the other search rules. All Priority 1 search rules are applied first, followed by all Priority 2 search rules, and so on. More than one rule can be assigned the same priority, in which case any matching target zones are queried simultaneously. The default is 100.  | The default configuration means that the Local Zone is searched first for all aliases. If the alias is not found locally, all neighbor, traversal client and traversal server zones are searched, and if they cannot locate the alias the request is sent to any DNS and ENUM zones. |
| <b>Protocol</b>                      | The source protocol for which the rule applies. The options are <i>Any</i> , <i>H.323</i> or <i>SIP</i> .   |  |
| <b>Source</b>                        | The sources of the requests for which this rule applies.<br><i>Any</i> : neighbor or traversal zones, and any non-registered devices.<br><i>All zones</i> : neighbor or traversal zones.<br><i>Named</i> : a specific source zone for which the rule applies.   | Named sources creates the ability for search rules to be applied as dial plan policy for specific zones.   |
| <b>Source name</b>                   | The specific source zone for which the rule applies. Choose from the Default Zone, Default Subzone or any other configured zone.  | Only applies if the <b>Source</b> is set to <i>Named</i> .   |
| <b>Request must be authenticated</b> | Specifies whether the search rule applies only to authenticated search requests.  | This can be used in conjunction with the Expressway's <a href="#">Authentication Policy</a> to limit the set of services available to unauthenticated devices.   |
| <b>Mode</b>                          | The method used to test if the alias applies to the search rule.<br><i>Alias pattern match</i> : the alias must match the specified <b>Pattern type</b> and <b>Pattern string</b> .<br><i>Any alias</i> : any alias (providing it is not an IP address) is allowed.<br><i>Any IP Address</i> : the alias must be an IP address.   |  |
| <b>Pattern type</b>                  | How the <b>Pattern string</b> must match the alias for the rule to be applied. Options are:<br><i>Exact</i> : the entire string must exactly match the alias character for character.<br><i>Prefix</i> : the string must appear at the beginning of the alias.<br><i>Suffix</i> : the string must appear at the end of the alias.<br><i>Regex</i> : treats the string as a <a href="#">regular expression</a> . | Applies only if the <b>Mode</b> is <i>Alias Pattern Match</i> .<br>You can test whether a pattern matches a particular alias and is transformed in the expected way by using the <a href="#">Check pattern</a> tool ( <b>Maintenance &gt; Tools &gt; Check pattern</b> ).            |



| Field                      | Description  | Usage tips   |
|----------------------------|--|--|
| <b>Pattern string</b>      | The pattern against which the alias is compared.   | Applies only if the <b>Mode</b> is <i>Alias Pattern Match</i> .<br><br>The Expressway has a set of predefined <a href="#">pattern matching variables</a> that can be used to match against certain configuration elements.   |
| <b>Pattern behavior</b>    | Determines whether the matched part of the alias is modified before being sent to the target zone or policy service<br><br><i>Leave</i> : the alias is not modified.<br><br><i>Strip</i> : the matching prefix or suffix is removed from the alias.<br><br><i>Replace</i> : the matching part of the alias is substituted with the text in the <b>Replace string</b> . | Applies only if the <b>Mode</b> is <i>Alias Pattern Match</i> .<br><br>If you want to transform the alias before applying search rules you must use <a href="#">pre-search transforms</a> .  |
| <b>Replace string</b>      | The string to substitute for the part of the alias that matches the pattern.   | Only applies if the <b>Pattern behavior</b> is <i>Replace</i> .<br><br>You can use regular expressions.  |
| <b>On successful match</b> | Controls the ongoing search behavior if the alias matches the search rule.<br><br><i>Continue</i> : continue applying the remaining search rules (in priority order) until the endpoint identified by the alias is found.<br><br><i>Stop</i> : do not apply any more search rules, even if the endpoint identified by the alias is not found in the target zone.       | If <i>Stop</i> is selected, any rules with the same priority level as this rule are still applied.   |
| <b>Target</b>              | The zone or policy service to query if the alias matches the search rule.  | You can configure external <a href="#">policy services</a> to use as a target of search rules. This could be used, for example, to call out to an external service or application, such as a TelePresence Conductor. The service will return some CPL which could, for example, specify a new destination alias which would start the search process over again. |
| <b>State</b>               | Indicates if the search rule is enabled or not.  | Use this setting to test configuration changes, or to temporarily disable certain rules. Any disabled rules still appear in the rules list but are ignored.  |

Click on the rule you want to configure (or click **New** to create a new rule, or click **Delete** to remove a rule).

### Useful tools to assist in configuring search rules

- You can test whether the Expressway can find an endpoint identified by a given alias, without actually placing a call to that endpoint, by using the [Locate](#) tool (**Maintenance > Tools > Locate**).
- You can test whether a pattern matches a particular alias and is transformed in the expected way by using the [Check pattern](#) tool (**Maintenance > Tools > Check pattern**).

## Example searches and transforms

You can use pre-search transforms and search rules separately or together. You can also define multiple search rules that use a combination of **Any alias** and **Alias pattern match** modes, and apply the same or different priorities to each rule. This will give you a great deal of flexibility in determining if and when a target zone is queried and whether any transforms are applied.

This section gives the following examples that demonstrate how you might use pre-search transforms and search rules to solve specific use cases in your deployment:

- [Filter queries to a zone using the original alias](#)
- [Always query a zone using the original alias](#)
- [Always query a zone using a transformed alias](#)
- [Query a zone using both the original and transformed alias](#)
- [Query a zone using two or more different transformed aliases](#)
- [Allow calls to IP addresses only if they come from known zones](#)

## Filter queries to a zone without transforming

You can filter the search requests sent to a zone so that it is only queried for aliases that match certain criteria. For example, assume all endpoints in your regional sales office are registered to their local Cisco VCS with a suffix of `@sales.example.com`. In this situation, it makes sense for your Head Office Expressway to query the Sales Office VCS only when it receives a search request for an alias with a suffix of `@sales.example.com`. Sending any other search requests to this particular VCS would take up resources unnecessarily. It would also be wasteful of resources to send search requests for aliases that match this pattern to any other zone (there may be other lower priority search rules defined that would also apply to these aliases). In which case setting **On successful match** to *Stop* means that the Expressway will not apply any further (lower priority) search rules.

To achieve the example described above, on your Head Office Expressway create a zone to represent the Sales Office VCS, and from the **Create search rule** page (**Configuration > Dial plan > Search rules > New**) set up an associated search rule as follows:

| Field                         | Value  |
|-------------------------------|--|
| Rule name                     | Regional sales office                                |
| Description                   | Calls to aliases with a suffix of @sales.example.com |
| Priority                      | 100  |
| Source                        | Any  |
| Request must be authenticated | No   |
| Mode                          | Alias pattern match                                  |
| Pattern type                  | Suffix   |
| Pattern string                | @sales.example.com                                   |
| Pattern behavior              | Leave  |
| On successful match           | Stop   |

| Field  | Value        |
|--------|--------------|
| Target | Sales office |
| State  | Enabled      |

## Always query a zone with original alias (no transforms)

To configure a zone so that it is always sent search requests using the original alias, from the [Create search rule](#) page ([Configuration > Dial plan > Search rules > New](#)), set up a search rule for that zone with a **Mode** of *Any alias*:

| Field                         | Value   |
|-------------------------------|---|
| Rule name                     | Always query with original alias              |
| Description                   | Send search requests using the original alias |
| Priority                      | 100   |
| Source                        | Any   |
| Request must be authenticated | No  |
| Mode                          | Any alias                                     |
| On successful match           | Continue                                      |
| Target                        | Head office                                   |
| State                         | Enabled                                       |

## Query a zone for a transformed alias

Note that the *Any alias* mode does not support alias transforms. If you want to always query a zone using a different alias to that received, you need to use a mode of *Alias pattern match* in combination with a regular expression.

You may want to configure your dial plan so that when a user dials an alias in the format `name@example.com` the Expressway queries the zone for `name@example.co.uk` instead.

To achieve this, from the [Create search rule](#) page ([Configuration > Dial plan > Search rules > New](#)) set up a search rule as follows:

| Field                         | Value                                  |
|-------------------------------|--|
| Rule name                     | Transform to example.co.uk             |
| Description                   | Transform example.com to example.co.uk |
| Priority                      | 100                                    |
| Source                        | Any                                    |
| Request must be authenticated | No                                     |
| Mode                          | Alias pattern match                    |

| Field               | Value         |
|---------------------|---------------|
| Pattern type        | Suffix        |
| Pattern string      | example.com   |
| Pattern behavior    | Replace       |
| Replace string      | example.co.uk |
| On successful match | Continue      |
| Target zone         | Head office   |
| State               | Enabled       |

## Query a zone for original and transformed alias

You may want to query a zone for the original alias at the same time as you query it for a transformed alias. To do this, configure one search rule with a **Mode** of *Any alias*, and a second search rule with a **Mode** of *Alias pattern match* along with details of the transform to be applied. Both searches must be given the same **Priority** level.

For example, you may want to query a neighbor zone for both a full URI and just the name (the URI with the domain removed). To achieve this, on your local Expressway from the [Create search rule](#) page ([Configuration > Dial plan > Search rules > New](#)) set up two search rules as follows:

### Rule #1

| Field                         | Value   |
|-------------------------------|---|
| Rule name                     | Overseas office - original alias              |
| Description                   | Query overseas office with the original alias |
| Priority                      | 100   |
| Source                        | Any   |
| Request must be authenticated | No  |
| Mode                          | Any alias                                     |
| On successful match           | Continue                                      |
| Target zone                   | Overseas office                               |
| State                         | Enabled                                       |

### Rule #2

| Field       | Value                                     |
|-------------|---|
| Rule name   | Overseas office - strip domain            |
| Description | Query overseas office with domain removed |
| Priority    | 100                                       |
| Source      | Any                                       |

| Field                         | Value               |
|-------------------------------|---------------------|
| Request must be authenticated | No                  |
| Mode                          | Alias pattern match |
| Pattern type                  | Suffix              |
| Pattern string                | @example.com        |
| Pattern behavior              | Strip               |
| On successful match           | Continue            |
| Target zone                   | Overseas office     |
| State                         | Enabled             |

## Query a zone for two or more transformed aliases

Zones are queried in order of priority of the search rules configured against them.

It is possible to configure multiple search rules for the same zone each with, for example, the same **Priority** and an identical **Pattern string** to be matched, but with different replacement patterns. In this situation, the Expressway queries that zone for each of the new aliases simultaneously. (Any duplicate aliases produced by the transforms are removed prior to the search requests being sent out.) If any of the new aliases are found by that zone, the call is forwarded to the zone. It is then up to the controlling system to determine the alias to which the call will be forwarded.

For example, you may want to configure your dial plan so that when a user dials an alias in the format **name@example.com**, the Expressway queries the zone simultaneously for both **name@example.co.uk** and **name@example.net**.

To achieve this, from the **Create search rule** page (**Configuration > Dial plan > Search rules > New**) set up two search rules as follows:

### Rule #1

| Field                         | Value                                  |
|-------------------------------|--|
| Rule name                     | Transform to example.co.uk             |
| Description                   | Transform example.com to example.co.uk |
| Priority                      | 100                                    |
| Source                        | Any                                    |
| Request must be authenticated | No                                     |
| Mode                          | Alias pattern match                    |
| Pattern type                  | Suffix                                 |
| Pattern string                | example.com                            |
| Pattern behavior              | Replace                                |
| Replace string                | example.co.uk                          |

| Field               | Value       |
|---------------------|-------------|
| On successful match | Continue    |
| Target zone         | Head office |
| State               | Enabled     |

## Rule #2

| Field                         | Value                                |
|-------------------------------|--------------------------------------|
| Rule name                     | Transform to example.net             |
| Description                   | Transform example.com to example.net |
| Priority                      | 100                                  |
| Source                        | Any                                  |
| Request must be authenticated | No                                   |
| Mode                          | Alias pattern match                  |
| Pattern type                  | Suffix                               |
| Pattern string                | example.com                          |
| Pattern behavior              | Replace                              |
| Replace string                | example.net                          |
| On successful match           | Continue                             |
| Target zone                   | Head office                          |
| State                         | Enabled                              |

## Allowing calls to IP addresses only if they come from known zones

In addition to making calls to aliases, calls can be made to specified IP addresses. To pass on such calls to the appropriate target zones you must set up search rules with a **Mode** of *Any IP address*. To provide extra security you can set the rule's **Source** option to *All zones*. This means that the query is only sent to the target zone if it originated from any configured zone or the Local Zone.

To achieve the example described above, from the [Create search rule](#) page ([Configuration > Dial plan > Search rules > New](#)) set up a search rule as follows:

| Field       | Value  |
|-------------|--|
| Rule name   | IP addresses from known zones                      |
| Description | Allow calls to IP addresses only from a known zone |
| Priority    | 100  |
| Source      | All zones  |

| <b>Field</b>                  | <b>Value</b>    |
|-------------------------------|-----------------|
| Request must be authenticated | No              |
| Mode                          | Any IP address  |
| On successful match           | Continue        |
| Target zone                   | Overseas office |
| State                         | Enabled         |

# Configuring search rules to use an external service

The configuration process to set up the Expressway to use an external policy service for search rules (dial plan) is broken down into the following steps:

- Configure the policy service to be used by search rules.
- Configure the relevant search rules to direct a search to the policy service.

## Configuring a policy service to be used by search rules

1. Go to **Configuration > Dial plan > Policy services**.
2. Click **New**.
3. Configure the fields on the **Create policy service** page as follows:

| Field   | Description   | Usage tips   |
|---|---|--|
| <b>Name</b>   | The name of the policy service.   |  |
| <b>Description</b>                                      | An optional free-form description of the policy service.  | The description appears as a tooltip if you hover your mouse pointer over a policy service in the list.  |
| <b>Protocol</b>   | The protocol used to connect to the policy service.<br>The default is <i>HTTPS</i> .  | The Expressway automatically supports HTTP to HTTPS redirection when communicating with the policy service server.   |
| <b>Certificate verification mode</b>                    | When connecting over HTTPS, this setting controls whether the certificate presented by the policy server is verified.<br><br>If <i>On</i> , for the Expressway to connect to a policy server over HTTPS, the Expressway must have a root CA certificate loaded that authorizes that server's server certificate. Also the certificate's Subject Common Name or Subject Alternative Name must match one of the <b>Server address</b> fields below. | The Expressway's root CA certificates are loaded via ( <b>Maintenance &gt; Security certificates &gt; Trusted CA certificate</b> ).  |
| <b>HTTPS certificate revocation list (CRL) checking</b> | Enable this option if you want to protect certificate checking using CRLs and you have manually loaded CRL files, or you have enabled automatic CRL updates.  | Go to <b>Maintenance &gt; Security certificates &gt; CRL management</b> to configure how the Expressway uploads CRL files.   |
| <b>Server address 1 - 3</b>                             | Enter the IP address or Fully Qualified Domain Name (FQDN) of the server hosting the service. You can specify a port by appending <code>:&lt;port&gt;</code> to the address.  | If an FQDN is specified, ensure that the Expressway has an appropriate DNS configuration that allows the FQDN to be resolved.<br><br>For resiliency, up to three server addresses can be supplied. |
| <b>Path</b>   | Enter the URL of the service on the server.   |  |



| Field              | Description   | Usage tips   |
|--------------------|---|--|
| <b>Status path</b> | The <b>Status path</b> identifies the path from where the Expressway can obtain the status of the remote service.<br>The default is <i>status</i> . | The policy server must supply return status information, see <a href="#">Policy server status and resiliency [p.270]</a> .   |
| <b>Username</b>    | The username used by the Expressway to log in and query the service.  |  |
| <b>Password</b>    | The password used by the Expressway to log in and query the service.  | The maximum plaintext length is 30 characters (which is subsequently encrypted).   |
| <b>Default CPL</b> | This is the fallback CPL used by the Expressway if the service is not available.  | You can change it, for example, to redirect to an answer service or recorded message.<br>For more information, see <a href="#">Default CPL for policy services [p.386]</a> . |

4. Click **Create policy service**.

### Configuring a search rule to direct a search to the policy service

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the fields on the **Create search rule** page as appropriate for the searches you want to direct to the external policy server.

This example shows how to divert calls to aliases ending in *.meet* to the external policy server:

|                                      |  |
|--------------------------------------|--|
| <b>Rule name</b>                     | A short name that describes the rule.  |
| <b>Description</b>                   | A free-form description of the rule.   |
| <b>Priority</b>                      | As required, for example 10.   |
| <b>Protocol</b>                      | As required, for example <i>Any</i> .  |
| <b>Source</b>                        | As required, for example <i>Any</i> .  |
| <b>Request must be authenticated</b> | Configure this setting according to your authentication policy.  |
| <b>Mode</b>                          | As required, for example <i>Alias pattern match</i> .  |
| <b>Pattern type</b>                  | As required, for example <i>Regex</i> .  |
| <b>Pattern string</b>                | As required, for example <i>*\meet@example.com</i>   |
| <b>Pattern behavior</b>              | As required, for example <i>Leave</i> .  |
| <b>On successful match</b>           | As required.<br>Note that if <i>Stop</i> is selected the Expressway will not process any further search rules for the original alias, but will restart the full call processing sequence if any new aliases are returned in the CPL. |
| <b>Target</b>                        | Select the policy service that was created in the previous step.   |

---

|              |                |
|--------------|----------------|
| <b>State</b> | <i>Enabled</i> |
|--------------|----------------|

---

To divert all searches to the policy server you could set up 2 search rules that both target the policy service:

- The first search rule with a **Mode** of *Any alias*.
- The second search rule with a **Mode** of *Any IP address*.

4. Click **Create search rule**.

The Expressway will direct all searches that match the specified pattern to the policy service server.

Your search rules must be configured in such a way that they will result in a match for the initial alias, and then either not match or not return a reject for any aliases to which the policy server has routed the call.

# About Call Policy

You can set up rules to control which calls are allowed, which calls are rejected, and which calls are to be redirected to a different destination. These rules are known as Call Policy (or Administrator Policy).

If Call Policy is enabled and has been configured, each time a call is made the Expressway will execute the policy in order to decide, based on the source and destination of the call, whether to:

- proxy the call to its original destination
- redirect the call to a different destination or set of destinations
- reject the call

---

**Note:** when enabled, Call Policy is executed for all calls going through the Expressway.

---

You should use Call Policy to determine which callers can make or receive calls via the Expressway.

## Configuring Call Policy

The **Call Policy configuration** page (**Configuration > Call Policy > Configuration**) is used to configure the Expressway's [Call Policy](#) mode and to upload local policy files.

### Call Policy mode

The **Call Policy mode** controls from where the Expressway obtains its Call Policy configuration. The options are:

- *Local CPL*: uses locally-defined Call Policy.
- *Policy service*: uses an external policy service.
- *Off*: Call Policy is not in use.

Each of these options are described in more detail below:

#### Local CPL

The *Local CPL* option uses the Call Policy that is configured locally on the Expressway. If you choose *Local CPL* you must then either:

- [configure basic Call Policy](#) through the **Call Policy rules** page (**Configuration > Call Policy > Rules**) — note that this only lets you allow or reject specified calls, or
- [upload a Call Policy file](#) that contains CPL script; however, due to the complexity of writing CPL scripts you are recommended to use an external policy service instead

Only one of these two methods can be used at any one time to specify Call Policy. If a CPL script has been uploaded, this takes precedence and you will not be able to use the **Call Policy rules** page; to use the page you must first delete the CPL script that has been uploaded.

If *Local CPL* is enabled but no policy is configured or uploaded, then a default policy is applied that allows all calls, regardless of source or destination.

The *Policy service* option is used if you want to refer all Call Policy decisions out to an external service. If you select this option an extra set of configuration fields appear so that you can specify the connection details of the external service. See [Configuring Call Policy to use an external service \[p.165\]](#) .

## Configuring Call Policy rules using the web interface



The **Call Policy rules** page ([Configuration > Call Policy > Rules](#)) lists the web-configured (rather than uploaded via a CPL file) Call Policy rules currently in place and allows you to create, edit and delete rules. It provides a mechanism to set up basic Call Policy rules without having to write and upload a CPL script.

You cannot use the Call Policy rules page to configure Call Policy if a CPL file is already in place. If this is the case, on the **Call Policy configuration** page ([Configuration > Call Policy > Configuration](#)) you will have the option to **Delete uploaded file**. Doing so will delete the existing Call Policy that was put in place using a CPL script, and enable use of the **Call Policy rules** page for Call Policy configuration.

Each rule specifies the **Action** to take for all calls from a particular **Source** alias to a particular **Destination** alias. If you have more than one rule, you can **Rearrange** the order of priority in which these rules are applied.

If rules are not configured, the default policy is to allow all calls, regardless of source or destination.

The configurable options are:

| Field                      | Description   | Usage tips  |
|----------------------------|---|---|
| <b>Source pattern</b>      | The alias or IP address that the calling endpoint used to identify itself when placing the call. If this field is blank, the policy rule applies to all incoming calls from unauthenticated users, meaning calls where the endpoint making the call is <b>not</b> registered and authenticated to a neighbor which in turn has authenticated with the local Expressway.   | This field supports <a href="#">regular expressions</a> . |
| <b>Destination pattern</b> | The alias or IP address that the endpoint dialed to make the call.  | This field supports <a href="#">regular expressions</a> . |
| <b>Action</b>              | Whether or not a call that matches the source and destination is permitted.<br><i>Allow</i> : if both the <b>Source</b> and <b>Destination</b> aliases match those listed, call processing will continue.<br><i>Reject</i> : if both the <b>Source</b> and <b>Destination</b> aliases match those listed, the call will be rejected.  |   |
| <b>Rearrange</b>           | Each combination of <b>Source</b> and <b>Destination</b> is compared, in the order shown on the <b>Call Policy rules</b> page, with the details of the call being made until a match is found, at which point the call policy is applied. To move a particular item to higher or lower in the list, thus giving the rule a higher or lower priority, click on the  and  icons respectively. |   |

Click on the rule you want to configure (or click **New** to create a new rule, or click **Delete** to remove a rule).

## Configuring Call Policy using a CPL script

You can use CPL scripts to configure advanced Call Policy. To do this, you must first create and save the CPL script as a text file, after which you upload it to the Expressway. However, due to the complexity of writing CPL scripts you are recommended to use an external [policy service](#) instead.

For information on the CPL syntax and commands that are supported by the Expressway, see the [CPL reference \[p.291\]](#) section.

## Viewing existing CPL script

To view the Call Policy that is currently in place as an XML-based CPL script, go to the [Call Policy configuration](#) page (**Configuration > Call Policy > Configuration**) and click **Show Call Policy file**.

- If Call Policy is configured to use a CPL script, this shows you the script that was uploaded.
- If Call Policy is configured by the **Call Policy rules** page, this shows you the CPL version of those call policy rules.
- If **Call Policy mode** is *On* but a policy has not been configured, this shows you a default CPL script that allows all calls.

You may want to view the file to take a backup copy of the Call Policy, or, if Call Policy has been configured using the Call Policy rules page you could take a copy of this CPL file to use as a starting point for a more advanced CPL script.

If Call Policy has been configured using the **Call Policy rules** page and you download the CPL file and then upload it back to the Expressway without editing it, the Expressway will recognize the file and automatically add each rule back into the **Call Policy rules** page.

## About CPL XSD files

The CPL script must be in a format supported by the Expressway. The **Call Policy configuration** page allows you to download the XML schemas which are used to check scripts that are uploaded to the Expressway. You can use the XSD files to check in advance that your CPL script is valid. Two download options are available:

- **Show CPL XSD file**: displays in your browser the XML schema used for the CPL script.
- **Show CPL Extensions XSD file**: displays in your browser the XML schema used for additional CPL elements supported by the Expressway.

## Uploading a CPL script

To upload a new CPL file:

1. Go to **Configuration > Call Policy > Configuration**.
2. From the **Policy files** section, in the **Select the new Call Policy file** field, enter the file name or **Browse** to the CPL script you want upload.
3. Click **Upload file**.

The Expressway polls for CPL script changes every 5 seconds, so the Expressway will almost immediately start using the updated CPL script. CPL scripts cannot be uploaded using the command line interface.

## Deleting an existing CPL script

If a CPL script has already been uploaded, a **Delete uploaded file** button will be visible. Click it to delete the file.

# Configuring Call Policy to use an external service

To configure Call Policy to refer all policy decisions out to an external service:

1. Go to **Configuration > Call policy > Configuration**.
2. Select a **Call Policy mode** of *Policy service*.
3. Configure the fields that are presented as follows:

| Field   | Description   | Usage tips   |
|---|---|--|
| <b>Protocol</b>   | The protocol used to connect to the policy service.<br>The default is <i>HTTPS</i> .  | The Expressway automatically supports HTTP to HTTPS redirection when communicating with the policy service server.   |
| <b>Certificate verification mode</b>                    | When connecting over HTTPS, this setting controls whether the certificate presented by the policy server is verified.<br><br>If <i>On</i> , for the Expressway to connect to a policy server over HTTPS, the Expressway must have a root CA certificate loaded that authorizes that server's server certificate. Also the certificate's Subject Common Name or Subject Alternative Name must match one of the <b>Server address</b> fields below. | The Expressway's root CA certificates are loaded via ( <a href="#">Maintenance &gt; Security certificates &gt; Trusted CA certificate</a> ).   |
| <b>HTTPS certificate revocation list (CRL) checking</b> | Enable this option if you want to protect certificate checking using CRLs and you have manually loaded CRL files, or you have enabled automatic CRL updates.  | Go to <a href="#">Maintenance &gt; Security certificates &gt; CRL management</a> to configure how the Expressway uploads CRL files.  |
| <b>Server address 1 - 3</b>                             | Enter the IP address or Fully Qualified Domain Name (FQDN) of the server hosting the service. You can specify a port by appending <code>:&lt;port&gt;</code> to the address.  | If an FQDN is specified, ensure that the Expressway has an appropriate DNS configuration that allows the FQDN to be resolved.<br><br>For resiliency, up to three server addresses can be supplied. |
| <b>Path</b>   | Enter the URL of the service on the server.   |  |
| <b>Status path</b>                                      | The <b>Status path</b> identifies the path from where the Expressway can obtain the status of the remote service.<br><br>The default is <i>status</i> .   | The policy server must supply return status information, see <a href="#">Policy server status and resiliency [p.270]</a> .   |
| <b>Username</b>   | The username used by the Expressway to log in and query the service.  |  |
| <b>Password</b>   | The password used by the Expressway to log in and query the service.  | The maximum plaintext length is 30 characters (which is subsequently encrypted).   |
| <b>Default CPL</b>                                      | This is the fallback CPL used by the Expressway if the service is not available.  | You can change it, for example, to redirect to an answer service or recorded message.<br><br>For more information, see <a href="#">Default CPL for policy services [p.386]</a> .                   |

4. Click **Save**.

The Expressway should connect to the policy service server and start using the service for Call Policy decisions.

Any connection problems will be reported on this page. Check the **Status** area at the bottom of the page and check for additional information messages against the **Server address** fields.

## Supported address formats

The destination address that is entered using the caller's endpoint can take a number of different formats, and this affects the specific process that the Expressway follows when attempting to locate the destination endpoint. The address formats supported by the Expressway are:

- IP address, for example `10.44.10.1` or `3ffe:80ee:3706::10:35`
- H.323 ID, for example `john.smith` or `john.smith@example.com` (note that an H.323 ID can be in the form of a URI)
- E.164 alias, for example `441189876432` or `6432`
- URI, for example `john.smith@example.com`
- ENUM, for example `441189876432` or `6432`

Each of these address formats may require some configuration of the Expressway in order for them to be supported. These configuration requirements are described below.

### Dialing by IP address

Dialing by IP address is necessary when the destination IP endpoint is not registered with any system. See the [Dialing by IP address \[p. 169\]](#) section for more information.

### Dialing by H.323 ID or E.164 alias

No special configuration is required to place a call using an H.323 ID or E.164 alias.

The Expressway follows the usual [call routing process](#), applying any transforms and then searching the external zones for the alias, according to the search rules.

Note that SIP endpoints always register using an AOR in the form of a URI. You are recommended to ensure that H.323 endpoints also register with an H.323 ID in the form of a URI to facilitate interworking.

### Dialing by H.323 or SIP URI

When a user places a call using URI dialing, they will typically dial `name@example.com`.

If the destination endpoint is registered to a neighbor system, no special configuration is required for the call to be placed. The Expressway follows the usual [search process](#), applying any transforms and then searching the external zones for the alias, according to the search rules.

URI dialing may make use of DNS to locate the destination endpoint. To support URI dialing via DNS, you must configure the Expressway with at least one DNS server and at least one DNS zone.

Full instructions on how to configure the Expressway to support URI dialing via DNS (both outbound and inbound) are given in the URI dialing section.

### Dialing by ENUM

ENUM dialing allows an endpoint to be contacted by a caller dialing an E.164 number - a telephone number - even if that endpoint has registered using a different format of alias. The E.164 number is converted into a URI by the DNS system, and the rules for URI dialing are then followed to place the call.

The ENUM dialing facility allows you to retain the flexibility of URI dialing while having the simplicity of being called using just a number - particularly important if any of your callers are restricted to dialing using a numeric keypad.

To support ENUM dialing on the Expressway you must configure it with at least one DNS server and the appropriate ENUM zones.

Full instructions on how to configure the Expressway to support ENUM dialing (both outbound and inbound) are given in the [ENUM dialing](#) section.



# Dialing by IP address

Dialing by IP address is necessary when the destination endpoint is not registered with any system.

## Calls to unknown IP addresses

Although the Expressway supports dialing by IP address, it is sometimes undesirable for the Expressway to be allowed to place a call directly to an IP address that is not local. Instead, you may want a neighbor to place the call on behalf of the Expressway, or not allow such calls at all. The **Calls to unknown IP addresses** setting (on the [Dial plan configuration](#) page) configures how the Expressway handles calls made to IP addresses which are not on its local network, or registered with one of its neighbors:

- *Direct*: the Expressway attempts to place the call directly to the unknown IP address without querying any neighbors.
- *Indirect*: the Expressway forwards the search request to its neighbors in accordance with its normal search process, meaning any zones that are the target of search rules with an *Any IP Address* mode. If a match is found and the neighbor's configuration allows it to connect a call to that IP address, the Expressway will pass the call to that neighbor for completion.
- *Off*: the Expressway will not attempt to place the call, either directly or indirectly to any of its neighbors.

The default setting is *Indirect*.

This setting applies to the call's destination address prior to any zone transforms, but after any pre-search transforms or Call Policy rules have been applied.

## Calling unregistered endpoints

An unregistered endpoint is any device that is not registered with an H.323 gatekeeper or SIP registrar. Although most calls are made between endpoints that are registered with such systems, it is sometimes necessary to place a call to an unregistered endpoint.

There are two ways to call to an unregistered endpoint:

- by dialing its URI (this requires that the local Expressway is configured to support URI dialing, and a DNS record exists for that URI that resolves to the unregistered endpoint's IP address)
- by dialing its IP address

## Recommended configuration for firewall traversal

When an Expressway-E is neighbored with an Expressway-C for firewall traversal, you should typically set **Calls to unknown IP addresses** to *Indirect* on the Expressway-C and *Direct* on the Expressway-E.

## About ENUM dialing

ENUM dialing allows an endpoint to be contacted by a caller dialing an E.164 number - a telephone number - even if that endpoint has registered using a different format of alias.

Using ENUM dialing, when an E.164 number is dialed it is converted into a URI using information stored in DNS. The Expressway then attempts to find the endpoint based on the URI that has been returned.

The ENUM dialing facility allows you to retain the flexibility of URI dialing while having the simplicity of being called using just a number - particularly important if any of your callers are restricted to dialing using a numeric keypad.

The Expressway supports outward ENUM dialing by allowing you to configure ENUM zones on the Expressway. When an ENUM zone is queried, this triggers the Expressway to transform the E.164 number that was dialed into an ENUM domain which is then queried for using DNS.

---

**Note:** ENUM dialing relies on the presence of relevant DNS NAPTR records for the ENUM domain being queried. These are the responsibility of the administrator of that domain.

---

## ENUM dialing process

When the Expressway attempts to locate a destination endpoint using ENUM, the general process is as follows:

1. The user dials the E.164 number from their endpoint.
2. The Expressway converts the E.164 number into an ENUM domain as follows:
  - a. The digits are reversed and separated by a dot.
  - b. The name of the domain that is hosting the NAPTR records for that E.164 number is added as a suffix.
3. DNS is then queried for the resulting ENUM domain.
4. If a NAPTR record exists for that ENUM domain, this will advise how the number should be converted into one (or possibly more) H.323/SIP URIs.
5. The Expressway begins the search again, this time for the converted URI as per the URI dialing process. Note that this is considered to be a completely new search, and so pre-search transforms and Call Policy will therefore apply.

## Enabling ENUM dialing

ENUM dialing is enabled separately for incoming and outgoing calls.

### Outgoing calls

To allow outgoing calls to other endpoints using ENUM, you must:

- configure at least one ENUM zone, and
- configure at least one DNS Server

This is described in the [ENUM dialing for outgoing calls \[p.171\]](#) section.

### Incoming calls

To enable endpoints in your enterprise to receive incoming calls from other endpoints via ENUM dialing, you must configure a DNS NAPTR record mapping your endpoints' E.164 numbers to their SIP/H.323 URIs. See

the [ENUM dialing for incoming calls \[p. 174\]](#) section for instructions on how to do this.

---

**Note:** if an ENUM zone and a DNS server have not been configured on the local Expressway, calls made using ENUM dialing could still be placed if the local Expressway is neighbored with another Expressway that has been appropriately configured for ENUM dialing. Any ENUM dialed calls will go via the neighbor. This configuration is useful if you want all ENUM dialing from your enterprise to be configured on one particular system.

---

## ENUM dialing for outgoing calls

For a local endpoint to be able to dial another endpoint using ENUM via your Expressway, the following conditions must be met:

- There must be a NAPTR record available in DNS that maps the called endpoint's E.164 number to its URI. It is the responsibility of the administrator of the enterprise to which the called endpoint belongs to provide this record, and they will only make it available if they want the endpoints in their enterprise to be contactable via ENUM dialing.
- You must [configure an ENUM zone](#) on your local Expressway. This ENUM zone must have a DNS Suffix that is the same as the domain where the NAPTR record for the called endpoint is held.
- You must configure your local Expressway with the address of at least one [DNS server](#) that it can query for the NAPTR record (and if necessary any resulting URI).

After the ENUM process has returned one or more URIs, a new search will begin for each of these URIs in accordance with the URI dialing process. You also need to configure a DNS zone if they are to be located using a DNS lookup.

### Calling process

The process below is followed when searching for an ENUM (E.164) number:

1. The Expressway initiates a search for the E.164 number as dialed. It follows the usual [call routing process](#).
2. After applying any pre-search transforms, the Expressway checks its [search rules](#) to see if any of them are configured with a **Mode** of either:
  - *Any alias*, or
  - *Alias pattern match* with a pattern that matches the E.164 number
3. The target zones associated with any matching search rules are queried in rule priority order.
  - If a target zone is a neighbor zone, the neighbor is queried for the E.164 number. If the neighbor supports ENUM dialing, it may route the call itself.
  - If a target zone is an ENUM zone, the Expressway attempts to locate the endpoint through ENUM. As and when each ENUM zone configured on the Expressway is queried, the E.164 number is transformed into an ENUM domain as follows:
    - i. The digits are reversed and separated by a dot.
    - ii. The **DNS suffix** configured for that ENUM zone is appended.
4. DNS is then queried for the resulting ENUM domain.
5. If the DNS server finds at that ENUM domain a NAPTR record that matches the transformed E.164 number (that is, after it has been reversed and separated by a dot), it returns the associated URI to the Expressway.
6. The Expressway then initiates a new search for that URI (maintaining the existing hop count). The Expressway starts at the beginning of the search process (applying any pre-search transforms, then

searching local and external zones in priority order). From this point, as it is now searching for a SIP/H.323 URI, the process for URI dialing is followed.

In this example, we want to call Fred at Example Corp. Fred's endpoint is actually registered with the URI `fred@example.com`, but to make it easier to contact him his system administrator has configured a DNS NAPTR record mapping this alias to his E.164 number: `+44123456789`.

We know that the NAPTR record for `example.com` uses the DNS domain of `e164.arpa`.

1. We create an ENUM zone on our local Expressway with a **DNS suffix** of `e164.arpa`.
2. We configure a search rule with a **Pattern match mode** of *Any alias*, and set the **Target** to the ENUM zone. This means that ENUM will always be queried regardless of the format of the alias being searched for.
3. We dial `44123456789` from our endpoint.
4. The Expressway initiates a search for a registration of `44123456789` and the search rule of *Any alias* means the ENUM zone is queried. (Note that other higher priority searches could potentially match the number first.)
5. Because the zone being queried is an ENUM zone, the Expressway is automatically triggered to transform the number into an ENUM domain as follows:
  - a. The digits are reversed and separated by a dot: `9.8.7.6.5.4.3.2.1.4.4`.
  - b. The **DNS suffix** configured for this ENUM zone, `e164.arpa`, is appended. This results in a transformed domain of `9.8.7.6.5.4.3.2.1.4.4.e164.arpa`.
6. DNS is then queried for that ENUM domain.
7. The DNS server finds the domain and returns the information in the associated NAPTR record. This tells the Expressway that the E.164 number we have dialed is mapped to the SIP URI of `fred@example.com`.
8. The Expressway then starts another search, this time for `fred@example.com`. From this point the process for URI dialing is followed, and results in the call being forwarded to Fred's endpoint.

## Configuring zones and search rules for ENUM dialing

To support ENUM dialing, you must configure an ENUM zone and related search rules for each ENUM service used by remote endpoints.

### Adding and configuring ENUM zones

To set up an ENUM zone:

1. Go to **Configuration > Zones > Zones**.
2. Click **New**. You are taken to the **Create zone** page.
3. Enter a **Name** for the zone and select a **Type** of *ENUM*.
4. Configure the ENUM zone settings as follows:

| Field            | Guidelines   |
|------------------|--|
| <b>Hop count</b> | The <a href="#">hop count</a> specified for an ENUM zone is applied in the same manner as hop counts for other zone types. The currently applicable hop count is maintained when the Expressway initiates a new search process for the alias returned by the DNS lookup. |

| Field             | Guidelines  |
|-------------------|---|
| <b>DNS suffix</b> | The suffix to append to a transformed E.164 number to create an ENUM host name. It represents the DNS zone (in the domain name space) to be queried for a NAPTR record. |
| <b>H.323 mode</b> | Controls if H.323 records are looked up for this zone.  |
| <b>SIP mode</b>   | Controls if SIP records are looked up for this zone.  |

5. Click **Create zone**.

Note that:

- Any number of ENUM zones may be configured on the Expressway. You should configure at least one ENUM zone for each DNS suffix that your endpoints may use.
- Normal search rule pattern matching and prioritization rules apply to ENUM zones.
- You must also [configure the Expressway with details of DNS servers](#) to be used when searching for NAPTR records.

### Configuring search rules for ENUM zones

If you want to be able to make ENUM calls via the Expressway, then at a minimum you should configure an ENUM zone and a related search rule with:

- a **DNS suffix** of **e164 . arpa** (the domain specified by the ENUM standard)
- a related search rule with a **Mode** of *Any alias*

This results in DNS always being queried for all types of aliases, not just ENUMs. It also means that ENUM dialing will only be successful if the enterprise being dialed uses the **e164 . arpa** domain. To ensure successful ENUM dialing, you must configure an ENUM zone for each domain that holds NAPTR records for endpoints that callers in your enterprise might want to dial.

You can then set up search rules that filter the queries sent to each ENUM zone as follows:

- use a **Mode** of *Alias pattern match*
- use the **Pattern string** and **Pattern type** fields to define the aliases for each domain that will trigger an ENUM lookup

For example, you want to enable ENUM dialing from your network to a remote office in the UK where the endpoints' E.164 numbers start with **44**. You would configure an ENUM zone on your Expressway, and then an associated search rule with:

- **Mode** of *Alias pattern match*
- **Pattern string** of **44**
- **Pattern type** of *Prefix*

This results in an ENUM query being sent to that zone only when someone dials a number starting with **44**.

### Configuring transforms for ENUM zones

You can configure transforms for ENUM zones in the same way as any other zones (see the [Search and zone transform process \[p.150\]](#) section for full information).

Any ENUM zone transforms are applied before the number is converted to an ENUM domain.

For example, you want to enable ENUM dialing from your network to endpoints at a remote site using a prefix of 8 followed by the last 4 digits of the remote endpoints' E.164 number. You would configure an ENUM zone on your Expressway and then an associated search rule with:

- **Mode** of *Alias pattern match*
- **Pattern string** of `8(\d{4})`
- **Pattern type** of *Regex*
- **Pattern behavior** of *Replace*
- **Replace string** of `44123123(\1)`

With this configuration, it is the resulting string (`44123123xxxx`) that is converted into an ENUM domain and queried for via DNS.

To verify you have configured your outward ENUM dialing correctly, use the [Locate tool](#) (**Maintenance > Tools > Locate**) to try to resolve an E.164 alias.

## ENUM dialing for incoming calls

For endpoints to be reached using ENUM dialing, you must configure a DNS NAPTR record that maps your endpoints' E.164 numbers to their SIP/H.323 URIs. This record must be located at an appropriate DNS domain where it can be found by any systems attempting to reach you by using ENUM dialing.

### About DNS domains for ENUM

ENUM relies on the presence of NAPTR records to provide the mapping between E.164 numbers and their SIP/H.323 URIs.

[RFC 3761](#), which is part of a suite of documents that define the ENUM standard, specifies that the domain for ENUM - where the NAPTR records should be located for public ENUM deployments - is `e164.arpa`. However, use of this domain requires that your E.164 numbers are assigned by an appropriate national regulatory body. Not all countries are yet participating in ENUM, so you may want to use an alternative domain for your NAPTR records. This domain could reside within your corporate network (for internal use of ENUM) or it could use a public ENUM database such as `http://www.e164.org`.

### Configuring DNS NAPTR records

ENUM relies on the presence of NAPTR records, as defined by [RFC 2915](#). These are used to obtain an H.323 or SIP URI from an E.164 number.

The record format that the Expressway supports is:

```
order flag preference service regex replacement
```

where:

- **order** and **preference** determine the order in which NAPTR records are processed. The record with the lowest order is processed first, with those with the lowest preference being processed first in the case of matching order.
- **flag** determines the interpretation of the other fields in this record. Only the value `u` (indicating that this is a terminal rule) is currently supported, and this is mandatory.
- **service** states whether this record is intended to describe E.164 to URI conversion for H.323 or for SIP. Its value must be either `E2U+h323` or `E2U+SIP`.
- **regex** is a regular expression that describes the conversion from the given E.164 number to an H.323 or

## SIP URI.

- **replacement** is not currently used by the Expressway and should be set to . (the full stop character).

Non-terminal rules in ENUM are not currently supported by the Expressway. For more information on these, see section 2.4.1 of [RFC 3761](#).

For example, the record:

```
IN NAPTR 10 100 "u" "E2U+h323" "!^(.*)$!h323:\1@example.com!" .
```

would be interpreted as follows:

- 10 is the **order**
- 100 is the **preference**
- **u** is the **flag**
- **E2U+h323** states that this record is for an H.323 URI
- **!^(.\*)\$!h323:\1@example.com!** describes the conversion:
  - **!** is a field separator
  - the first field represents the string to be converted. In this example, **^(.\*)\$** represents the entire E.164 number
  - the second field represents the H.323 URI that will be generated. In this example, **h323:\1@example.com** states that the E.164 number will be concatenated with **@example.com**. For example, **1234** will be mapped to **1234@example.com**.
- **.** shows that the replacement field has not been used.

# Configuring DNS servers for ENUM and URI dialing

DNS servers are required to support ENUM and URI dialing:

- **ENUM dialing:** to query for NAPTR records that map E.164 numbers to URIs
- **URI dialing:** to look up endpoints that cannot be accessed via neighbor systems

To configure the DNS servers used by the Expressway for DNS queries:

1. Go to the **DNS** page (**System > DNS**).
2. Enter in the **Address 1** to **Address 5** fields the IP addresses of up to 5 DNS servers that the Expressway will query when attempting to locate a domain. These fields must use an IP address, not a FQDN.



# Configuring call routing and signaling

The **Call routing** page (**Configuration > Call routing**) is used to configure the Expressway's call routing and signaling functionality.

## Call signaling optimization

Calls are made up of two components - signaling and media. For [traversal calls](#), the Expressway always handles both the media and the signaling. For non-traversal calls, the Expressway does not handle the media, and may or may not need to handle the signaling.

The **Call signaling optimization** setting specifies whether the Expressway removes itself, where it can, from the call signaling path after the call has been set up. The options for this setting are:

- *Off*: the Expressway always handles the call signaling.
- *On*: the Expressway handles the call signaling when the call is one of:
  - a traversal call
  - an H.323 call that has been modified by Call Policy such that the call resolves to more than one alias
  - a SIP call where the incoming transport protocol (UDP, TCP, TLS) is different from the outgoing protocol

In all other cases the Expressway removes itself from the call signaling path after the call has been set up. The Expressway does not consume a call license for any such calls, and the call signaling path is simplified.

## Call loop detection mode

Your dial plan or that of networks to which you are neighbored may be configured in such a way that there are potential signaling loops. An example of this is a structured dial plan, where all systems are neighbored together in a mesh. In such a configuration, if the [hop counts](#) are set too high, a single search request may be sent repeatedly around the network until the hop count reaches 0, consuming resources unnecessarily.

The Expressway can be configured to detect search loops within your network and terminate such searches through the **Call loop detection mode** setting, thus saving network resources. The options for this setting are:

- *On*: the Expressway will fail any branch of a search that contains a loop, recording it as a level 2 "loop detected" event. Two searches are considered to be a loop if they meet all of the following criteria:
  - have same call tag
  - are for the same destination alias
  - use the same protocol
  - originate from the same zone
- *Off*: the Expressway will not detect and fail search loops. You are recommended to use this setting only in advanced deployments.

# Identifying calls

Each call that passes through the Expressway is assigned a Call ID and a Call Serial Number. Calls also have a Call Tag assigned if one does not already exist.

## Call ID

The Expressway assigns each call currently in progress a different Call ID. The Call ID numbers start at 1 and go up to the maximum number of calls allowed on that system.

Each time a call is made, the Expressway will assign that call the lowest available Call ID number. For example, if there is already a call in progress with a Call ID of 1, the next call will be assigned a Call ID of 2. If Call 1 is then disconnected, the third call to be made will be assigned a Call ID of 1.

The Call ID is not therefore a unique identifier: while no two calls in progress at the same time will have the same Call ID, the same Call ID will be assigned to more than one call over time.

Note that the Expressway web interface does not show the Call ID.

## Call Serial Number

The Expressway assigns a unique Call Serial Number to every call passing through it. No two calls on an Expressway will ever have the same Call Serial Number. A single call passing between two or more Expressways will be identified by a different Call Serial Number on each system.

## Call Tag

Call Tags are used to track calls passing through a number of Expressways. When the Expressway receives a call, it checks to see if there is a Call Tag already assigned to it. If so, the Expressway will use the existing Call Tag; if not, it will assign a new Call Tag to the call. This Call Tag is then included in the call's details when the call is forwarded on. A single call passing between two or more Expressways will be assigned a different Call Serial Number each time it arrives at an Expressway (including one it has already passed through) but can be identified as the same call by use of the Call Tag. This is particularly useful if you are using a [remote syslog server](#) to collate events across a number of Expressways in your network.

The Call Tag also helps identify loops in your network - it is used as part of the automatic [call loop detection](#) feature, and you can also search the Event Log for all events relating to a single call tag. Loops occur when a query is sent to a neighbor zone and passes through one or more systems before being routed back to the original Expressway. In this situation the outgoing and incoming query will have different Call Serial Numbers and may even be for different destination aliases (depending on whether any transforms were applied). However, the call will still have the same Call Tag.

---

**Note:** If a call passes through a system that is not an Expressway or TelePresence Conductor then the Call Tag information will be lost.

---

## Identifying calls in the CLI

To control a call using the CLI, you must reference the call using either its Call ID or Call Serial Number. These can be obtained using the command:

### **xStatus Calls**

This returns details of each call currently in progress in order of their Call ID. The second line of each entry lists the Call Serial Number, and the third lists the Call Tag.

# Disconnecting calls

## Disconnecting a call using the web interface

To disconnect one or more existing calls using the web interface:

1. Go to the **Calls** page (**Status > Calls**).
2. If you want to confirm the details of the call, including the Call Serial Number and Call Tag, click **View**. Click the back button on your browser to return to the **Calls** page.
3. Select the box next to the calls you want to terminate and click **Disconnect**.

Note that if your Expressway is part of a cluster you have to be logged into the peer through which the call is associated to be able to disconnect the call.

## Disconnecting a call using the CLI

To disconnect an existing call using the CLI, you must first obtain either the call ID number or the call serial number (see [Identifying calls \[p. 178\]](#)). Then use either one of the following commands as appropriate:

- **xCommand DisconnectCall Call: <ID number>**
- **xCommand DisconnectCall CallSerialNumber: <serial number>**

While it is quicker to use the call ID number to reference the call to be disconnected, there is a risk that in the meantime the call has already been disconnected and the call ID assigned to a new call. For this reason, the Expressway also allows you to reference the call using the longer but unique call serial number.

Note that when disconnecting a call, only the call with that Call Serial Number is disconnected. Other calls with the same Call Tag but a different Call Serial Number may not be affected.

## Limitations when disconnecting SIP calls

Call disconnection works differently for H.323 and SIP calls due to differences in the way the protocols work.

For H.323 calls, and interworked calls, the **Disconnect** command actually disconnects the call.

For SIP calls, the **Disconnect** command causes the Expressway to release all resources used for the call; the call will appear as disconnected on the Expressway. However, endpoints will still consider themselves to be in the call. SIP calls are peer-to-peer, and as the Expressway is a SIP proxy it has no authority over the endpoints. Releasing the resources on the Expressway means that the next time there is any signaling from the endpoint to the Expressway, the Expressway will respond with a '481 Call/Transaction Does Not Exist' causing the endpoint to clear the call.

Note that endpoints that support SIP session timers (see [RFC 4028](#)) have a call refresh timer which allows them to detect a hung call (signaling lost between endpoints). The endpoints will release their resources after the next session-timer message exchange.

# Bandwidth control

---

This section describes how to control the bandwidth that is used for calls within your Local Zone, as well as calls out to other zones ([Configuration > Traversal Subzone](#) and [Configuration > Bandwidth](#)).

|                               |     |
|-------------------------------|-----|
| About bandwidth control ..... | 181 |
| About subzones .....          | 183 |
| Links and pipes .....         | 186 |

## About bandwidth control

The Expressway allows you to control the amount of bandwidth used by calls passing through the system's Traversal Subzone. This is done by using [links](#) and [pipes](#) to apply limits to the bandwidth that can be used.

Bandwidth limits may be set on a call-by-call basis and/or on a total concurrent usage basis. This flexibility allows you to set appropriate bandwidth controls on individual components of your network.

Calls will fail if links are not configured correctly. You can check whether a call will succeed, and what bandwidth will be allocated to it, using the command `xCommand CheckBandwidth`.

For specific information about how bandwidth is managed across peers in a cluster, see [Sharing bandwidth across peers \[p. 140\]](#).

## Configuring bandwidth controls

The [Bandwidth configuration](#) page ([Configuration > Bandwidth > Configuration](#)) is used to specify how the Expressway behaves in situations when it receives a call with no bandwidth specified, and when it receives a call that requests more bandwidth than is currently available.

The configurable options are:

| Field                                | Description  | Usage tips  |
|--------------------------------------|--|---|
| <b>Default call bandwidth (kbps)</b> | <p>The bandwidth to use for calls for which no bandwidth value has been specified by the system that initiated the call.</p> <p>It also defines the minimum bandwidth to use on SIP to H.323 interworked calls.</p> <p>This value cannot be blank. The default value is 384kbps.</p>         | Usually, when a call is initiated the endpoint will include in the request the amount of bandwidth it wants to use. |
| <b>Downspeed per call mode</b>       | <p>Determines what happens if the <b>per-call</b> bandwidth restrictions on a subzone or pipe mean that there is insufficient bandwidth available to place a call at the requested rate.</p> <p><i>On</i>: the call will be downspeeded.</p> <p><i>Off</i>: the call will not be placed.</p> |   |
| <b>Downspeed total mode</b>          | <p>Determines what happens if the <b>total</b> bandwidth restrictions on a subzone or pipe mean that there is insufficient bandwidth available to place a call at the requested rate.</p> <p><i>On</i>: the call will be downspeeded.</p> <p><i>Off</i>: the call will not be placed.</p>    |   |

## About downspeeding

If bandwidth control is in use, there may be situations when there is insufficient bandwidth available to place a call at the requested rate. By default (and assuming that there is some bandwidth still available) the Expressway will still attempt to connect the call, but at a reduced bandwidth – this is known as **downspeeding**.

Downspeeding can be configured so that it is applied in either or both of the following scenarios:

- when the requested bandwidth for the call exceeds the lowest per-call limit for the subzone or pipes
- when placing the call at the requested bandwidth would mean that the total bandwidth limits for that subzone or pipes would be exceeded

You can turn off downspeeding, in which case if there is insufficient bandwidth to place the call at the originally requested rate, the call will not be placed at all. This could be used if, when your network is nearing capacity, you would rather a call failed to connect at all than be connected at a lower than requested speed. In this situation endpoint users will get one of the following messages, depending on the system that initiated the search:

- "Exceeds Call Capacity"
- "Gatekeeper Resources Unavailable"

# About subzones

The Local Zone is made up of subzones. Subzones are used to control the bandwidth used by various parts of your network.

Three special subzones — the Default Subzone, the Traversal Subzone and the Cluster Subzone (only applies if the Expressway is in a cluster) — are automatically created and cannot be deleted.

Note that the Traversal Subzone is the only configurable subzone.

## Default links between subzones

The Expressway is shipped with the Default Subzone and Traversal Subzone (and Default Zone) already created, and with links between them. If the Expressway is added to a cluster then default links to the Cluster Subzone are also established automatically. You can delete or amend these [default links](#) if you need to model restrictions of your network.

## About the Traversal Subzone

The Traversal Subzone is a conceptual subzone. Its sole purpose is to control the bandwidth used by [traversal calls](#).

The [Traversal Subzone](#) page ([Configuration > Traversal Subzone](#)) allows you to place bandwidth restrictions on calls being handled by the Traversal Subzone and to configure the range of ports used for the media in traversal calls.

## Configuring bandwidth limitations

All traversal calls pass through the Traversal Subzone, so by applying bandwidth limitations to the Traversal Subzone you can control how much processing of media the Expressway will perform at any one time. These limitations can be applied on a total concurrent usage basis, and on a per-call basis.

See [Applying bandwidth limitations to the Traversal Subzone \[p. 185\]](#) for more details.

## Configuring the Traversal Subzone ports

On [Configuration > Traversal Subzone](#) you can configure the range of ports used for media in traversal calls.

### What is a valid range to use?

You can define the media port range anywhere within the range 1024 to 65533. **Traversal media port start** must be an even number and **Traversal media port end** must be an odd number, because ports are allocated in pairs and the first port allocated in each pair is even.

### How big should the range be?

Up to 48 ports could be required for a single traversal call, and you can have up to 100 concurrent traversal calls on a small/medium system, or 500 concurrent traversal calls on a large system. The default range is thus  $48 \times 500 = 24000$  ports.

If you want to reduce the range, be aware that the Expressway will raise an alarm if the range is not big enough to meet the nominal maximum of 48 ports per call for the licensed number of rich media sessions. You may need to increase the range again if you add new licenses.

## Why are 48 ports required for each call?

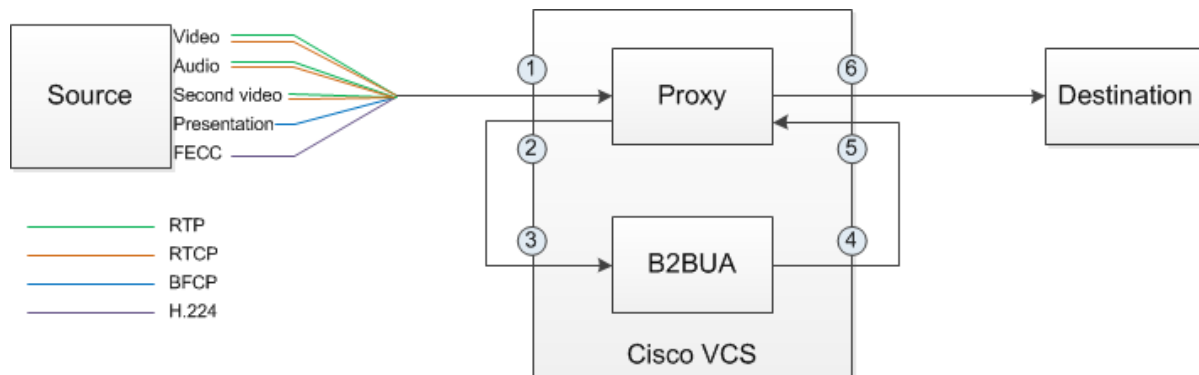
The nominal maximum number of ports allocated per call = max number of ports per allocation \* max number of allocation instances. This is  $8 * 6 = 48$ , and those numbers are derived as follows:

Each call can have up to 5 types of media; video (RTP/RTCP), audio (RTP/RTCP), second/duo video (RTP/RTCP), presentation (BFCP), and far end camera control (H.224). If all these media types are in the call, then the call requires **8** ports; 3 RTP/RTCP pairs, 1 for BFCP, and 1 for H.224.

Each call has at least two legs (inbound to Expressway and outbound from Expressway), requiring two instances of port allocation. A further four instances of allocation are required if the call is routed via the B2BUA. In this case, ports are allocated at the following points:

1. Inbound to the local proxy from the source
2. Outbound from the local proxy to the local B2BUA
3. Inbound to the local B2BUA from the local proxy
4. Outbound from the local B2BUA to the local proxy
5. Inbound to the local proxy from the local B2BUA
6. Outbound from the local proxy to the destination

Figure 9: Maximum port allocation for a media traversal call



In practice, you probably won't reach the maximum number of concurrent traversal calls, have them all routed through the B2BUA, and have all the possible types of media in every call. However, we defined the default range to accommodate this extreme case, and the Expressway raises an alarm if the total port requirement *could* exceed the port range you specify.

## What is the default 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).

## Applying bandwidth limitations to the Traversal Subzone

You can apply bandwidth limits to the Traversal Subzone as follows:

| Limitation          | Description  |
|---------------------|--|
| Total               | Limits the maximum bandwidth available for all concurrent traversal calls. |
| Calls handled by... | The maximum bandwidth available to any individual traversal call.          |

For all the above limitations, the **Bandwidth restriction** setting has the following effect:

- *No bandwidth*: no bandwidth is allocated and therefore no calls can be made.
- *Limited*: limits are applied. You must also enter a value in the corresponding bandwidth (kbps) field.
- *Unlimited*: no restrictions are applied to the amount of bandwidth being used.

If your bandwidth configuration is such that multiple types of bandwidth restrictions are placed on a call (for example, if there are subzone bandwidth limits and pipe limits), the lowest limit will always apply to that call.

# Links and pipes

## Configuring links

Links are configured between zones and the Traversal Subzone.

The **Links** page (**Configuration > Bandwidth > Links**) lists all existing links and allows you to create, edit and delete links.

The following information is displayed:

| Field                    | Description  |
|--------------------------|--|
| <b>Name</b>              | The name of the link. Automatically created links have names based on the nodes that the link is between.  |
| <b>Node 1 and Node 2</b> | The Traversal Subzone and the zone that the link is between.   |
| <b>Pipe 1 and Pipe 2</b> | Any pipes that have been used to apply bandwidth limitations to the link. See <a href="#">Applying pipes to links [p.187]</a> for more information. Note that in order to apply a pipe, you must first have created it via the <a href="#">Pipes</a> page. |
| <b>Calls</b>             | Shows the total number of calls currently traversing the link.   |
| <b>Bandwidth used</b>    | Shows the total amount of bandwidth currently being consumed by all calls traversing the link.   |

You can configure up to 3000 links. Some links are created automatically when a zone is created.

## Default links

The Expressway is shipped with the Default Subzone, Traversal Subzone and Default Zone already created, and with default links pre-configured between them as follows: *DefaultSZtoTraversalSZ*, *DefaultSZtoDefaultZ* and *TraversalSZtoDefaultZ*. If the Expressway is in a cluster, an additional link, *DefaultSZtoClusterSZ*, between the Default Subzone and the Cluster Subzone is also established.

You can edit any of these default links in the same way you would edit manually configured links. If any of these links have been deleted you can re-create them, either:

- manually through the web interface
- automatically by using the CLI command `xCommand DefaultLinksAdd`

### Automatically created links

Whenever a new zone is created, links are automatically created as follows:

| New zone type         | Default links are created to...       |
|-----------------------|---------------------------------------|
| Neighbor zone         | Default Subzone and Traversal Subzone |
| DNS zone              | Default Subzone and Traversal Subzone |
| ENUM zone             | Default Subzone and Traversal Subzone |
| Traversal client zone | Traversal Subzone                     |
| Traversal server zone | Traversal Subzone                     |

Along with the pre-configured default links this ensures that, by default, any zone has connectivity to all other subzones and zones. You may rename, delete and amend any of these default links.

---

**Note:** calls will fail if links are not configured correctly. You can check whether a call will succeed, and what bandwidth will be allocated to it, using the CLI command `xCommand CheckBandwidth`.

---

## Configuring pipes

Pipes are used to control the amount of bandwidth used on calls between specific subzones and zones. The limits can be applied to the total concurrent bandwidth used at any one time, or to the bandwidth used by any individual call.

To apply these limits, you must first create a pipe and configure it with the required bandwidth limitations. Then when configuring [links](#) you assign the pipe to one or more links. Calls using the link will then have the pipe's bandwidth limitations applied to them. See [Applying pipes to links \[p.187\]](#) for more information.

The [Pipes](#) page ([Configuration > Bandwidth > Pipes](#)) lists all the pipes that have been configured on the Expressway and allows you to create, edit and delete pipes.

The following information is displayed:

| Field                     | Description  |
|---------------------------|--|
| <b>Name</b>               | The name of the pipe.  |
| <b>Total bandwidth</b>    | The upper limit on the total bandwidth used at any one time by all calls on all links to which this pipe is applied.         |
| <b>Per call bandwidth</b> | The maximum bandwidth of any one call on the links to which this pipe is applied.  |
| <b>Calls</b>              | Shows the total number of calls currently traversing all links to which the pipe is applied.                                 |
| <b>Bandwidth used</b>     | Shows the total amount of bandwidth currently being consumed by all calls traversing all links to which the pipe is applied. |

You can configure up to 1000 pipes.

See [Applying bandwidth limitations to the Traversal Subzone \[p.185\]](#) for more information about how the bandwidth limits are set and managed.

## Applying pipes to links

Pipes are used to restrict the bandwidth of a link. When a pipe is applied to a link, it restricts the bandwidth of calls made between the two nodes of the link - the restrictions apply to calls in either direction. Normally a single pipe would be applied to a single link. However, one or more pipes may be applied to one or more links, depending on how you want to model your network.

# Applications

---

This section provides information about each of the additional services that are available under the **Applications** menu of the Expressway.

B2BUA (back-to-back user agent) overview .....189

## B2BUA (back-to-back user agent) overview

A B2BUA operates between both endpoints of a SIP call and divides the communication channel into two independent call legs. Unlike a proxy server, the B2BUA maintains complete state for the calls it handles. Both legs of the call are shown as separate calls on the [Call status](#) and [Call history](#) pages.

B2BUA instances are hosted on the Expressway. They are used in the following scenarios:

- to apply [media encryption policy](#); this usage does not require any explicit B2BUA configuration
- to support [ICE messaging](#); the only B2BUA-related configuration required is to define the set of [TURN servers](#) required to support ICE calls
- to route SIP calls between the Expressway and a Microsoft Edge Server; this requires the manual configuration of the [Microsoft Lync B2BUA](#) and the set of [TURN servers](#) available for use by the B2BUA

### Configuring B2BUA TURN servers

The [B2BUA TURN servers](#) page ([Applications > B2BUA > B2BUA TURN servers](#)) is used to configure the set of TURN servers available for use by a B2BUA instance. The page lists all the currently configured TURN servers and lets you create, edit and delete TURN servers.

The B2BUA chooses which TURN server to offer via random load-balancing between all of the available servers. There is no limit to the number of servers that can be configured for the B2BUA to choose from.

To use these TURN servers with the Microsoft Lync B2BUA, you must enable **Offer TURN services** on the [Lync B2BUA configuration](#) page. They are used automatically by the B2BUA instance used when [ICE messaging](#) is enabled for a zone.

The configurable options are:

| Field                                      | Description  | Usage tips   |
|--|--|--|
| <b>TURN server address</b>                 | The IP address of a TURN server to offer when establishing ICE calls (for example, with a Microsoft Lync Edge server). | The TURN server must be RFC 5245 compliant, for example an Expressway-E TURN server. |
| <b>TURN server port</b>                    | The listening port on the TURN server. Default is 3478.  |  |
| <b>Description</b>                         | A free-form description of the TURN server.  |  |
| <b>TURN services username and password</b> | The username and password that are required to access the TURN server.   |  |

If the TURN server is running on a Large Expressway-E, you can make use of its scaling capabilities by specifying additional address/port combinations.

## Microsoft Lync B2BUA

The Microsoft Lync back-to-back user agent (Lync B2BUA) on the Expressway is used to route SIP calls between the Expressway and a Microsoft Lync Server.

It provides interworking between Microsoft ICE (used by Lync clients) and media for communications with standard video endpoints. It also provides call hold and call transfer support for calls with Lync clients.

The setting up of the Lync B2BUA includes the following tasks:

- Configuring and enabling the [B2BUA for Microsoft Lync communications](#).
- Configuring the [transcoders](#) that may be used by the B2BUA and any [policy rules](#) used to control routing through them (this is optional and are typically only used with Lync 2010).
- Defining the B2BUA's [trusted hosts](#) — the devices that may send signaling messages to the B2BUA.
- Defining the set of [TURN servers](#) available for use by the B2BUA when establishing ICE calls.
- Setting up search rules to route calls to the Lync domain via the B2BUA — when the B2BUA is enabled a non-configurable neighbor zone (named "**To Microsoft Lync server via B2BUA**") is automatically created; this zone must be selected as the target zone of the search rules.

A service restart is sometimes required to enable certain configuration changes to the Lync B2BUA to take effect. A system alarm is raised if a service restart is necessary.

## Microsoft Lync 2010

The **Microsoft Interoperability** option key must be installed to enable encrypted calls to and from Microsoft Lync 2010 Server (for both native SIP calls and calls interworked from H.323). It is also required by the B2BUA when establishing ICE calls to Lync 2010 clients.

The B2BUA can use the Cisco AM GW to transcode between standard codecs (such as H.264) and Microsoft RT Video and RT Audio to allow high definition calls between Microsoft Lync 2010 clients and Cisco endpoints.

## Microsoft Lync 2013

The B2BUA provides interworking between standard H.264 AVC and Lync 2013's H.264UC SVC codec. You can still configure the B2BUA to use Cisco AM GW transcoders with Lync 2013, but it is not necessary and we recommend that they are not deployed with Lync 2013.

Lync 2013 no longer supports H.263, so X8.1 or later software is required to interoperate successfully with Lync 2013.

The **Microsoft Interoperability** option key is required for all types of communication with Lync 2013.

## Usage features and limitations

- The Lync B2BUA has a maximum simultaneous call capability of 100 calls (for all system sizes, including Large systems); however, calls that use transcoder resources count as 2 calls.
- If a call is routed through the Lync B2BUA, the B2BUA always takes the media and always remains in the signaling path. The call component that is routed through the B2BUA can be identified in the call history details as having a component type of *Microsoft Lync B2BUA*.

- The Lync B2BUA does not consume any call licenses in addition to the license required by the leg of the call between the endpoint and the Expressway.
- If all configured transcoders reach their capacity limits, any calls that would normally route via a transcoder will not fail; the call will still connect as usual but will not be transcoded.
- The Lync B2BUA supports multiple TURN servers. TURN servers are recommended for calls traversing a Microsoft Lync Edge server.
- Bandwidth controls can be applied to the leg of the call between the endpoint and the B2BUA, but cannot be applied to the B2BUA to Microsoft Lync leg of the call. However, as the B2BUA forwards the media it receives without any manipulation, any bandwidth controls applied to the Expressway to B2BUA leg in effect also controls the B2BUA to Lync leg implicitly.
- The non-configurable neighbor zone (named "**To Microsoft Lync server via B2BUA**") that connects the Expressway to the Lync B2BUA uses a special zone profile of *Microsoft Lync* — this profile is only used by the Lync B2BUA and cannot be selected against any manually configured zones.

For more information about configuring Expressway and Microsoft Lync see:

- [Microsoft Lync B2BUA port reference \[p.310\]](#)
- [Microsoft Lync and Expressway Deployment Guide](#)

## Configuring the Microsoft Lync B2BUA

The [Microsoft Lync B2BUA configuration](#) page ([Applications > B2BUA > Microsoft Lync > Configuration](#)) is used to enable and configure the B2BUA's connection to Microsoft Lync devices.

The configurable options are:

| Field                                     | Description   | Usage tips  |
|---|---|---|
| <b>Configuration</b> section:             |   |   |
| <b>Microsoft Lync B2BUA</b>               | Enables or disables the Microsoft Lync B2BUA.   |   |
| <b>Lync signaling destination address</b> | The IP address or Fully Qualified Domain Name (FQDN) of the Hardware Load Balancer, Director or Front End Processor to which the Expressway sends the signaling messages. | You must also configure the IP addresses of the <a href="#">trusted hosts</a> . These are the Lync devices that may send signaling messages to the Expressway.  |
| <b>Lync signaling destination port</b>    | The IP port on the Hardware Load Balancer, Director or Front End Processor to which the Expressway sends the signaling messages. Default port is 5061.                    |   |
| <b>Lync signaling transport</b>           | The transport type used for connection to the Microsoft Lync server. The default is <i>TLS</i> .  |   |
| <b>Transcoders</b> section:               |   |   |
| <b>Enable transcoders for this B2BUA</b>  | Controls whether calls may be routed through a transcoder.  | You should enable this option if you need to use a transcoder such as the Cisco TelePresence Advanced Media Gateway to transcode between standard codecs (such as H.264) and Microsoft RT Video and RT Audio. |

| Field   | Description  | Usage tips  |
|---|--|---|
| <b>Port on B2BUA for transcoder communications</b>  | The IP port used on the B2BUA for communicating with the transcoders. Default is 65080.  | All transcoder communications are carried out over TLS.   |
| <b>Use transcoder policy rules</b>  | Specifies whether the transcoder policy rules are used to control access to the transcoders. Default is No.  | <p>If <b>Enable transcoders for this B2BUA</b> is Yes, then all calls are routed via the transcoders by default.</p> <p>If transcoder resources need to be reserved for specific types of calls, you can use this option to limit the types of calls that are routed via the transcoders. Set this option to Yes and then define the required <a href="#">policy rules</a>.</p>   |
| <b>TURN</b> section:  |  |   |
| <b>Offer TURN services</b>  | Controls whether the B2BUA offers TURN services. Default is No.  | <p>This is recommended for calls traversing a Microsoft Lync Edge server.</p> <p>To configure the associated TURN servers, click <a href="#">Configure B2BUA TURN servers</a>.</p>  |
| <b>Advanced settings:</b> you should only modify the advanced settings on the advice of Cisco customer support. |  |   |
| <b>Encryption</b>   | <p>Controls how the B2BUA handles encrypted and unencrypted call legs.</p> <p><i>Required:</i> both legs of the call must be encrypted.</p> <p><i>Auto:</i> encrypted and unencrypted combinations are supported.</p> <p>The default is <i>Auto</i>.</p> | <p>A call via the B2BUA comprises two legs: one leg from the B2BUA to a standard video endpoint, and one leg from the B2BUA to the Lync client. Either leg of the call could be encrypted or unencrypted.</p> <p>A setting of <i>Auto</i> means that the call can be established for any of the encrypted and unencrypted call leg combinations. Thus, one leg of the call could be encrypted while the other leg could be unencrypted.</p> |
| <b>B2BUA media port range start/end</b>   | The port range used by the B2BUA for handling media. Default range is 56000–57000.   | Ensure that the port range does not overlap with other port ranges used by this Expressway or this Expressway's TURN server.  |
| <b>Hop count</b>  | Specifies the Max-Forwards value to use in SIP messages. Default is 70.  |   |
| <b>Session refresh interval</b>   | The maximum time allowed between session refresh requests for SIP calls. Default is 1800 seconds.  | For further information see the definition of <i>Session-Expires</i> in <a href="#">RFC 4028</a> .  |
| <b>Minimum session refresh interval</b>   | The minimum value the B2BUA will negotiate for the session refresh interval for SIP calls. Default is 500 seconds.   | For further information see the definition of <i>Min-SE header</i> in <a href="#">RFC 4028</a> .  |
| <b>Port on B2BUA for Expressway communications</b>  | The port used on the B2BUA for communicating with the Expressway. Default is 65070.  |   |
| <b>Port on B2BUA for Lync call communications</b>   | The port used on the B2BUA for call communications with the Microsoft Lync server. Default is 65072.   |   |



## Configuring the B2BUA's trusted hosts

The **B2BUA trusted hosts** page ([Applications > B2BUA > Microsoft Lync > B2BUA trusted hosts](#)) is used to specify the devices that may send signaling messages to the Lync B2BUA.

The B2BUA only accepts messages from devices whose IP address is included in the list of trusted hosts.

Note that trusted host verification only applies to calls initiated by Lync that are inbound to the Expressway video network. It is not necessary to configure trusted hosts if calls are only ever to be initiated from the Expressway video network.

The Expressway has a limit of 25 trusted hosts. If there are more than 25 trusted hosts, the Expressway raises an alarm. You can work around this limit by adding another "Lync gateway" Expressway, or by pointing some of the Lync servers to a Lync proxy and then trusting the proxy instead.

The configurable options are:

| Field             | Description  | Usage tips  |
|-------------------|--|---|
| <b>Name</b>       | An optional free-form description of the trusted host device.  | The name is not used as part of the "trusted" criteria. It is provided only to help distinguish between multiple devices, rather than having to rely on their IP addresses. |
| <b>IP address</b> | The IP address of the trusted host device.   |   |
| <b>Type</b>       | The type of device that may send signaling messages to the B2BUA.<br><br><i>Lync device:</i> this includes Hardware Load Balancers, Directors and Front End Processors<br><br><i>Transcoder:</i> a transcoder device such as a Cisco TelePresence Advanced Media Gateway |   |

## Configuring transcoder policy rules

The **Microsoft Lync B2BUA transcoder policy rules** page ([Applications > B2BUA > Microsoft Lync > Transcoder policy rules](#)) is used to define the rules that control which Lync B2BUA calls are routed via a [transcoder](#).

If **Enable transcoders for this B2BUA** (configured on the [Microsoft Lync B2BUA configuration](#) page) is Yes, then all calls are routed via the transcoders by default. If transcoder resources need to be reserved for specific types of calls then you can specify rules to limit the types of calls that are routed via the transcoders.

- The rules on this page are only applied if **Use transcoder policy rules** (also configured on the [Microsoft Lync B2BUA configuration](#) page) is set to Yes.
- A rule is applied if it matches either the source or destination alias of a call.
- If the aliases associated with a call do not match any of the policy rules, the call will be routed via the transcoder. Therefore you may want to consider having a general low priority rule with a regex pattern match for all aliases that denies transcoder resources, and then have more specific rules with a higher priority that define the participants that are allowed to use the transcoder resources.

The page lists all the currently configured rules and lets you create, edit, delete, enable and disable rules. Note that you can click on a column heading to sort the list, for example by **Rule name** or **Priority**.

The configurable options are:

| Field                 | Description   | Usage tips  |
|-----------------------|---|---|
| <b>Name</b>           | The name assigned to the rule.  |   |
| <b>Description</b>    | An optional free-form description of the rule.  | The description appears as a tooltip if you hover your mouse pointer over a rule in the list.   |
| <b>Priority</b>       | Sets the order in which the rules are applied. The rules with the highest priority (1, then 2, then 3 and so on) are applied first.   | Multiple rules with the same priority are applied in configuration order. For clarity you are recommended to use unique priority settings for each rule.  |
| <b>Pattern type</b>   | The way in which the <b>Pattern string</b> must match either the source or destination alias of the call.<br><i>Exact:</i> the entire string must exactly match the alias character for character.<br><i>Prefix:</i> the string must appear at the beginning of the alias.<br><i>Suffix:</i> the string must appear at the end of the alias.<br><i>Regex:</i> treats the string as a <a href="#">regular expression</a> . | You can test whether a pattern matches a particular alias and is transformed in the expected way by using the <a href="#">Check pattern</a> tool ( <a href="#">Maintenance &gt; Tools &gt; Check pattern</a> ). |
| <b>Pattern string</b> | The pattern against which the alias is compared.  |   |
| <b>Action</b>         | The action to take if the source or destination alias of the call matches this policy rule.<br><i>Allow:</i> the call can connect via the transcoder.<br><i>Deny:</i> the call can connect but it will not use transcoder resources.  |   |
| <b>State</b>          | Indicates if the rule is enabled or not.  | Use this setting to test configuration changes, or to temporarily disable certain rules. Any disabled rules still appear in the rules list but are ignored.   |

## Configuring B2BUA transcoders

Transcoders are used to convert digital media from one format to another. The only transcoder currently supported by the Lync B2BUA is the Cisco TelePresence Advanced Media Gateway (Cisco AM GW).

The B2BUA can use the Cisco AM GW to transcode between standard codecs (such as H.264) and Microsoft RT Video and RT Audio to allow high definition calls between Microsoft Lync clients and Cisco endpoints.

The [Transcoders](#) page ([Applications > B2BUA > Microsoft Lync > Transcoders](#)) is used to manage the set of transcoders available to the B2BUA.

- Multiple transcoders can be configured for load balancing purposes; the B2BUA automatically manages which transcoder to use.
- The status of each transcoder is shown, this includes:
  - whether the transcoder is accessible or not
  - the number of available connections; note that Cisco AM GW calls require 2 connections per call
- You can use the [B2BUA configuration page](#) to control whether the B2BUA uses transcoder resources and whether specific [policy rules](#) are used to filter which calls are allowed to be routed through the transcoders.

Note that the B2BUA can operate without any associated transcoders (calls will still connect but will not be transcoded).

The configurable options are:

| Field          | Description   | Usage tips   |
|----------------|---|--|
| <b>Name</b>    | An optional free-form description of the transcoder.                    |  |
| <b>Address</b> | The IP address or Fully Qualified Domain Name (FQDN) of the transcoder. | <p>If you have several transcoders you are recommended to either use their IP addresses or to give each device a different FQDN.</p> <p>You may encounter problems if you use an FQDN that resolves to multiple transcoders (via DNS-based load balancing). This is because the B2BUA will first use DNS to discover the number of available ports on a transcoder, and then use DNS again to route a call to the transcoder. If the DNS lookup can resolve to different transcoders there is no guarantee that the call will be directed to the same transcoder that provided the resource information.</p> |
| <b>Port</b>    | The listening port on the transcoder.                                   |  |

## Restarting the B2BUA service

The **B2BUA service restart** page ([Applications > B2BUA > Microsoft Lync > B2BUA service restart](#)) is used to restart the Lync B2BUA service.

A restart is sometimes required to enable certain configuration changes to the B2BUA to take effect. A system alarm will be raised if a service restart is necessary.

Note that this function only restarts the B2BUA service; it does not restart the Expressway. However, restarting the service will cause any active calls being managed by the B2BUA to be lost.

To restart the B2BUA service:

1. Go to [Applications > B2BUA > Microsoft Lync > B2BUA service restart](#).
2. Check the number of active calls currently in place.
3. Click **Restart service**.

The service should restart after a few seconds. The status of the B2BUA service is displayed on the [B2BUA configuration page](#).

### Clustered Expressway systems

On a clustered Expressway you have to restart the Lync B2BUA service on every peer. You are recommended to ensure the service is configured and running correctly on the master peer before restarting the B2BUA service on the other peers.

# User accounts

---

This section provides information about how to configure administrator accounts, and how to display the details of all active administrator sessions.

|  |     |
|--|-----|
| About user accounts .....                                  | 197 |
| Configuring password security .....                        | 199 |
| Configuring administrator accounts .....                   | 201 |
| Configuring remote account authentication using LDAP ..... | 204 |
| Resetting forgotten passwords .....                        | 209 |
| Using the root account .....                               | 211 |
| Managing SSO tokens .....                                  | 212 |

# About user accounts

**Administrator accounts** are used to configure the Expressway.

## Account authentication

Administrator accounts must be authenticated before access is allowed to the Expressway.

Expressway can authenticate accounts either locally or against a remote directory service using LDAP (currently, only Windows Active Directory is supported), or it can use a combination of local and remotely managed accounts. The remote option allows administration groups to be set up in the directory service for all Expressways in an enterprise, removing the need to have separate accounts on each Expressway.

See [Configuring remote account authentication using LDAP \[p.204\]](#) and [Authenticating Expressway Accounts using LDAP Deployment Guide](#) for more information about setting up remote authentication.

If a remote source is used for administrator account authentication, you also need to configure the Expressway with:

- appropriate LDAP server connection settings
- administrator groups that match the corresponding group names already set up in the remote directory service to manage administrator access to this Expressway (see [Configuring administrator groups \[p.207\]](#))

The Expressway can also be configured to use [certificate-based authentication](#). This would typically be required if the Expressway was deployed in a highly-secure environment.

## Account types

### Administrator accounts

Administrator accounts are used to configure the Expressway.

- The Expressway has a default **admin** local administrator account with full read-write access. It can be used to access the Expressway using the web interface, the API interface or the CLI. Note that you cannot access the Expressway via the default **admin** account if a *Remote only* authentication source is in use.
- You can add additional local administrator accounts which can be used to access the Expressway using the web and API interfaces only.
- Remotely managed administrator accounts can be used to access the Expressway using the web and API interfaces only.

You can configure the complexity requirements for local administrator passwords on the [Password security](#) page (**Users > Password security**). All passwords and usernames are case sensitive.

Note that:

- The [Configuration Log](#) records all login attempts and configuration changes made using the web interface, and can be used as an audit trail. This is particularly useful when you have multiple administrator accounts.
- More than one administrator session can be running at the same time. These sessions could be using the web interface, command line interface, or a mixture of both. This may cause confusion if each administrator session attempts to modify the same configuration settings - changes made in one session will overwrite changes made in another session.

- You can configure account session limits and inactivity timeouts (see [Configuring system name and access settings \[p.35\]](#)).

See the [Configuring administrator accounts \[p.201\]](#) section for more information.

### Root account

The Expressway provides a root account which can be used to log in to the Expressway operating system. The **root** account should not be used in normal operation, and in particular system configuration should not be conducted using this account. Use the **admin** account instead.

See the [Using the root account \[p.211\]](#) section for more information.

---

**Note:** remember to change the passwords for the **admin** and **root** accounts from their default values.

---

# Configuring password security

The **Password security** page (**Users > Password security**) controls whether or not local [administrator account](#) passwords must meet a minimum level of complexity before they are accepted.

If **Enforce strict passwords** is set to *On*, all subsequently configured local administrator account passwords must conform to the following rules for what constitutes a strict password.

If **Enforce strict passwords** is set to *Off*, no extra checks are made on local administrator account passwords.

---

## Notes:

- You can never set a blank password for any administrator account, regardless of this setting.
- This setting affects only local administrator account passwords. It does not affect any other passwords used on the Expressway, such as in the local authentication database, LDAP server, external registration credentials, user account passwords, or administrator account passwords stored on remote credential directories.
- All passwords and usernames are case sensitive.

---

## Non-configurable rules for strict passwords

The following password rules always apply when **Enforce strict passwords** is set to *On*. There is no way to configure them:

- Avoid multiple instances of the same characters (non-consecutive instances are checked)
- Avoid three or more consecutive characters such as "abc" or "123"
- Avoid dictionary words, or reversed dictionary words
- Avoid palindromes, such as "risetovotesir"

## Configurable rules for strict passwords

The following properties of the password policy can be configured:

- Length must be at least 6 ASCII characters, but can be up to 255 (default 15)
- Number of numeric digits [0-9] may be between 0 and 255 (default 2)
- Number of uppercase letters [A-Z] may be between 0 and 255 (default 2)
- Number of lowercase letters [a-z] may be between 0 and 255 (default 2)
- Number of special characters [printable characters from 7-bit ASCII, eg. (space), @, \$ etc.)] may be between 0 and 255 (default 2)
- Number of consecutive repeated characters allowed may be between 1 and 255 (the default 0 disables the check, so consecutive repeated characters are allowed by default; set it to 1 to prevent a password from containing any consecutive repeats)
- The minimum number of character classes may be between 0 and 4 (the default 0 disables the check). Character classes are digits, lowercase letters, uppercase letters, and special characters.

**Note:** You may experience precedence effects between the required number of character classes and the number of characters per class.

For example, if you leave the default requirements of 2 characters of each class, there is an *implied* rule that 4 character classes are required. In this case, any setting of **Minimum number of character classes** is irrelevant.

For another example, if you set the minimum number of character classes to 2, and set the minimum number of characters required from each class to 0, then a password that contains characters from any two of the classes will suffice (presuming it meets all the other criteria as well).

---



# Configuring administrator accounts

The **Administrator accounts** page ([Users > Administrator accounts](#)) lists all the local administrator accounts on the Expressway.

In general, local administrator accounts are used to access the Expressway on its web interface or API interface, but are not permitted to access the CLI.

On this page you can:

- Create a new administrator account
- Change an administrator password
- Change the access level of an account: *Read-write*, *Read-only*, or *Auditor*
- Change the access scope of an account: *Web access*, *API access*, or both
- Delete, enable, or disable individual or multiple administrator accounts

## Editing administrator account details

You can edit the details for the default administrator account and for additional local administrator accounts.

Go to [Users > Administrator accounts](#). Under **Actions** for the relevant administrator account, click **Edit user**.

A new page is displayed, where you can edit all fields for the selected administrator account except for the password. To change the password, see below.

## About the "admin" account

This default local administrator account has full *Read-write* access and can access the Expressway using the web UI, the API interface, or the CLI. You can access the Expressway via the **admin** account even if a *Remote* authentication source is in use.

The username for this account is **admin** (all lower case) and the default password is **TANDBERG** (all upper case).

You cannot delete, rename, or disable **admin** and you cannot change its access level from *Read-write*, but you can disable its web and API access.

You should change the password as soon as possible. Choose a strong password, particularly if administration over IP is enabled.

If you forget the password for the **admin** account, you can log in as another administrator account with read-write access and change the password for the **admin** account. If there are no other administrator accounts, or you have forgotten those passwords as well, you can still reset the password for the **admin** account providing you have physical access to the Expressway. See [Resetting forgotten passwords \[p.209\]](#) for details.

## Administrator account fields reference

| Field                        | Description  | Usage tips  |
|------------------------------|--|---|
| <b>Name</b>                  | The username for the administrator account.  | Some names such as "root" are reserved. Local administrator account user names are case sensitive.  |
| <b>Access level</b>          | <p>The access level of the administrator account:</p> <p><i>Read-write</i>: allows all configuration information to be viewed and changed. This provides the same rights as the default <b>admin</b> account.</p> <p><i>Read-only</i>: allows status and configuration information to be viewed only and not changed. Some pages, such as the <a href="#">Upgrade</a> page, are blocked to read-only accounts.</p> <p><i>Auditor</i>: allows access to the <a href="#">Event Log</a>, <a href="#">Configuration Log</a>, <a href="#">Network Log</a>, <a href="#">Alarms</a> and <a href="#">Overview</a> pages only .</p> <p>Default: <i>Read-write</i></p> | <p>The access permissions of the currently logged in user are shown in the system information bar at the bottom of each web page.</p> <p>The access level of the default <b>admin</b> account cannot be changed from <i>Read-write</i>.</p>   |
| <b>Password</b>              | The password that this administrator will use to log in to the Expressway.   | <p>All passwords on the Expressway are encrypted, so you only see placeholder characters here.</p> <p>When entering passwords, the bar next to the <b>Password</b> field changes color to indicate the complexity of the password. You can configure the complexity requirements for local administrator passwords on the <a href="#">Password security</a> page (<a href="#">Users &gt; Password security</a>).</p> <p>You cannot set blank passwords.</p> |
| <b>New password</b>          | Enter a new password for the account.  | This field only appears when you are changing a password.   |
| <b>Confirm password</b>      | Re-enter the password for the account.   | This field only appears when you create an account or when you change its password.   |
| <b>Web access</b>            | <p>Select whether this account is allowed to log in to the system using the web interface.</p> <p>Default: Yes</p>   |   |
| <b>API access</b>            | <p>Select whether this account is allowed to access the system's status and configuration using the Application Programming Interface (API).</p> <p>Default: Yes</p>   | This controls access to the XML and REST APIs by systems such as Cisco TMS.   |
| <b>State</b>                 | Select whether the account is <i>Enabled</i> or <i>Disabled</i> . Disabled accounts are not allowed to access the system.  |   |
| <b>Your current password</b> | Enter your own, current password here if the system requires you to authorize a change.  | To improve security, the system requires that administrators enter their own passwords when creating an account or changing a password.   |

## Viewing active administrator sessions

The **Active administrator sessions** page ([Users > Active administrator sessions](#)) lists all administrator accounts that are currently logged in to this Expressway.

It displays details of their session including their login time, session type, IP address and port, and when they last accessed this Expressway.

You can terminate active web sessions by selecting the required sessions and clicking **Terminate session**.

You may see many sessions listed on this page if a zero **Session time out** value is configured. This typically occurs if an administrator ends their session by closing down their browser without first logging out of the Expressway.

# Configuring remote account authentication using LDAP

The **LDAP configuration** page (**Users > LDAP configuration**) is used to configure an LDAP connection to a remote directory service for administrator account authentication.

The configurable options are:

| Field  | Description   | Usage tips  |
|--|---|---|
| <p><b>Remote account authentication:</b> this section allows you to enable or disable the use of LDAP for remote account authentication.</p> |   |   |
| <p><b>Administrator authentication source</b></p>  | <p>Defines where administrator login credentials are authenticated.</p> <p><i>Local only:</i> credentials are verified against a local database stored on the system.</p> <p><i>Remote only:</i> credentials are verified against an external credentials directory.</p> <p><i>Both:</i> credentials are verified first against a local database stored on the system, and then if no matching account is found the external credentials directory is used instead.</p> <p>The default is <i>Local only</i>.</p>  | <p><i>Both</i> allows you to continue to use locally-defined accounts. This is useful while troubleshooting any connection or authorization issues with the LDAP server.</p> <p>You cannot log in using a locally-configured administrator account, including the default <b>admin</b> account, if <i>Remote only</i> authentication is in use.</p> <p>Note: do not use <i>Remote only</i> if Expressway is managed by Cisco TMS.</p> |
| <p><b>LDAP server configuration:</b> this section specifies the connection details to the LDAP server.</p>                                   |   |   |
| <p><b>FQDN address resolution</b></p>  | <p>Defines how the LDAP server address is resolved.</p> <p><i>SRV record:</i> DNS SRV record lookup.</p> <p><i>Address record:</i> DNS A or AAAA record lookup.</p> <p><i>IP address:</i> entered directly as an IP address.</p> <p>The default is <i>Address record</i>.</p> <hr/> <p><b>Note:</b> if you use SRV records, ensure that the records use the standard ports for LDAP. <code>_ldap._tcp.&lt;domain&gt;</code> must use 389 and <code>_ldaps._tcp.&lt;domain&gt;</code> must use 636. The Expressway does not support other port numbers for LDAP.</p> | <p>The SRV lookup is for either <code>_ldap._tcp</code> or <code>_ldaps._tcp</code> records, depending on whether <b>Encryption</b> is enabled. If multiple servers are returned, the priority and weight of each SRV record determines the order in which the servers are used.</p>  |
| <p><b>Host name and Domain</b><br/>or<br/><b>Server address</b></p>  | <p>The way in which the server address is specified depends on the <b>FQDN address resolution</b> setting:</p> <p><i>SRV record:</i> only the <b>Domain</b> portion of the server address is required.</p> <p><i>Address record:</i> enter the <b>Host name</b> and <b>Domain</b>. These are then combined to provide the full server address for the DNS address record lookup.</p> <p><i>IP address:</i> the <b>Server address</b> is entered directly as an IP address.</p>  | <p>If using TLS, the address entered here must match the CN (common name) contained within the certificate presented by the LDAP server.</p>  |
| <p><b>Port</b></p>   | <p>The IP port to use on the LDAP server.</p>   | <p>Non-secure connections use 389 and secure connections use 636.</p>   |

| Field  | Description   | Usage tips  |
|--|---|---|
| <b>Encryption</b>  | <p>Determines whether the connection to the LDAP server is encrypted using Transport Layer Security (TLS).</p> <p><i>TLS</i>: uses TLS encryption for the connection to the LDAP server.</p> <p><i>Off</i>: no encryption is used.</p> <p>The default is <i>TLS</i>.</p>  | <p>When TLS is enabled, the LDAP server's certificate must be signed by an authority within the Expressway's trusted CA certificates file.</p> <p>Click <a href="#">Upload a CA certificate file for TLS</a> (in the <a href="#">Related tasks</a> section) to go to the <a href="#">Managing the trusted CA certificate list [p.223]</a> page.</p> |
| <b>Certificate revocation list (CRL) checking</b>  | <p>Specifies whether certificate revocation lists (CRLs) are checked when forming a TLS connection with the LDAP server.</p> <p><i>None</i>: no CRL checking is performed.</p> <p><i>Peer</i>: only the CRL associated with the CA that issued the LDAP server's certificate is checked.</p> <p><i>All</i>: all CRLs in the trusted certificate chain of the CA that issued the LDAP server's certificate are checked.</p> <p>The default is <i>None</i>.</p> | <p>If you are using revocation lists, any required CRL data must also be included within the CA certificate file.</p>   |
| <p><b>Authentication configuration:</b> this section specifies the Expressway's authentication credentials to use when binding to the LDAP server.</p> |   |   |
| <b>Bind DN</b>   | <p>The distinguished name (case insensitive) used by the Expressway when binding to the LDAP server.</p> <p>It is important to specify the DN in the order cn=, then ou=, then dc=</p>  | <p>Any special characters within a name must be escaped with a backslash as per the LDAP standard (<i>RFC 4514</i>). Do not escape the separator character between names.</p> <p>The bind account is usually a read-only account with no special privileges.</p>  |
| <b>Bind password</b>   | <p>The password (case sensitive) used by the Expressway when binding to the LDAP server.</p>  | <p>The maximum plaintext length is 60 characters, which is then encrypted.</p>  |
| <b>SASL</b>  | <p>The SASL (Simple Authentication and Security Layer) mechanism to use when binding to the LDAP server.</p> <p><i>None</i>: no mechanism is used.</p> <p><i>DIGEST-MD5</i>: the DIGEST-MD5 mechanism is used.</p> <p>The default is <i>DIGEST-MD5</i>.</p>   | <p>Enable Simple Authentication and Security Layer if it is company policy to do so.</p>  |
| <b>Bind username</b>   | <p>Username of the account that the Expressway will use to log in to the LDAP server (case sensitive).</p> <p>Only required if SASL is enabled.</p>   | <p>Configure this to be the sAMAccountName; Security Access Manager Account Name (in AD this is the account's user logon name).</p>   |
| <p><b>Directory configuration:</b> this section specifies the base distinguished names to use when searching for account and group names.</p>          |   |   |

| Field                       | Description  | Usage tips  |
|-----------------------------|--|---|
| <b>Base DN for accounts</b> | The ou= and dc= definition of the Distinguished Name where a search for user accounts should start in the database structure (case insensitive).<br>It is important to specify the DN in the order ou=, then dc= | The Base DN for accounts and groups must be at or below the dc level (include all dc= values and ou= values if necessary). LDAP authentication does not look into sub dc accounts, only lower ou= and cn= levels. |
| <b>Base DN for groups</b>   | The ou= and dc= definition of the Distinguished Name where a search for groups should start in the database structure (case insensitive).<br>It is important to specify the DN in the order ou=, then dc=        | If no <b>Base DN for groups</b> is specified, then the Base DN for accounts will be used for both groups and accounts.  |

## Checking the LDAP server connection status

The status of the connection to LDAP server is displayed at the bottom of the page.

### State = Active

No error messages are displayed.

### State = Failed

The following error messages may be displayed:

| Error message   | Reason / resolution   |
|---|---|
| DNS unable to do reverse lookup                                 | Reverse DNS lookup is required for SASL authentication.   |
| DNS unable to resolve LDAP server address                       | Check that a valid DNS server is configured, and check the spelling of the LDAP server address.   |
| Failed to connect to LDAP server. Check server address and port | Check that the LDAP server details are correct.   |
| Failed to setup TLS connection. Check your CA certificate       | CA certificate, private key and server certificate are required for TLS.  |
| Failure connecting to server. Returned code<return code>        | Other non-specific problem.   |
| Invalid Base DN for accounts                                    | Check <b>Base DN for accounts</b> ; the current value does not describe a valid part of the LDAP directory.   |
| Invalid server name or DNS failure                              | DNS resolution of the LDAP server name is failing.  |
| Invalid bind credentials  | Check <b>Bind DN</b> and <b>Bind password</b> , this error can also be displayed if SASL is set to <i>DIGEST-MD5</i> when it should be set to <i>None</i> . |

| Error message                        | Reason / resolution   |
|--------------------------------------|---|
| Invalid bind DN                      | <p>Check <b>Bind DN</b>; the current value does not describe a valid account in the LDAP director.</p> <p>This failed state may be wrongly reported if the <b>Bind DN</b> is 74 or more characters in length. To check whether there is a real failure or not, set up an administrator group on the Expressway using a valid group name. If Expressway reports "saved" then there is not a problem (the Expressway checks that it can find the group specified). If it reports that the group cannot be found then either the <b>Bind DN</b> is wrong, the group is wrong or one of the other configuration items may be wrong.</p> |
| There is no CA certificate installed | CA certificate, private key and server certificate are required for TLS.  |
| Unable to get configuration          | LDAP server information may be missing or incorrect.  |

## Configuring administrator groups

The **Administrator groups** page ([Users > Administrator groups](#)) lists all the administrator groups that have been configured on the Expressway, and lets you add, edit and delete groups.

Administrator groups only apply if [remote account authentication](#) is enabled.

When you log in to the Expressway web interface, your credentials are authenticated against the remote directory service and you are assigned the access rights associated with the group to which you belong. If the administrator account belongs to more than one group, the highest level permission is assigned.

The configurable options are:

| Field               | Description  | Usage tips   |
|---------------------|--|--|
| <b>Name</b>         | <p>The name of the administrator group.</p> <p>It cannot contain any of the following characters:<br/> <code>\/[]:; =,+*?&gt;&lt;@"</code></p>   | <p>The group names defined in the Expressway must match the group names that have been set up in the remote directory service to manage administrator access to this Expressway.</p>   |
| <b>Access level</b> | <p>The access level given to members of the administrator group:</p> <p><i>Read-write</i>: allows all configuration information to be viewed and changed. This provides the same rights as the default <b>admin</b> account.</p> <p><i>Read-only</i>: allows status and configuration information to be viewed only and not changed. Some pages, such as the <b>Upgrade</b> page, are blocked to read-only accounts.</p> <p><i>Auditor</i>: allows access to the <b>Event Log, Configuration Log, Network Log, Alarms</b> and <b>Overview</b> pages only .</p> <p><i>None</i>: no access is allowed.</p> <p>Default: <i>Read-write</i></p> | <p>If an administrator belongs to more than one group, it is assigned the highest level permission for each of the access settings across all of the groups to which it belongs (any groups in a disabled state are ignored). See <a href="#">Determining the access level for accounts that belong in multiple groups [p.208]</a> below for more information.</p> |
| <b>Web access</b>   | <p>Determines whether members of this group are allowed to log in to the system using the web interface.</p> <p>Default: Yes</p>   |  |

| Field             | Description   | Usage tips   |
|-------------------|---|--|
| <b>API access</b> | Determines whether members of this group are allowed to access the system's status and configuration using the Application Programming Interface (API).<br>Default: Yes | This controls access to the XML and REST APIs by systems such as Cisco TMS.  |
| <b>State</b>      | Indicates if the group is enabled or disabled. Access will be denied to members of disabled groups.   | If an administrator account belongs to more than one administrator group with a combination of both <i>Enabled</i> and <i>Disabled</i> states, their access will be <i>Enabled</i> . |

### Determining the access level for accounts that belong in multiple groups

If an administrator belongs to groups with different levels of access, the highest level of access is granted. Any groups in a disabled state are ignored.

For example, if the following groups were configured:

| Group name            | Access level | Web access | API access |
|-----------------------|--------------|------------|------------|
| <b>Administrators</b> | Read-write   | -          | -          |
| <b>Region A</b>       | Read-only    | Yes        | -          |
| <b>Region B</b>       | Read-only    | -          | Yes        |
| <b>Region C</b>       | Read-only    | Yes        | Yes        |

The following table shows examples of the access permissions that would be granted for accounts that belong in one or more of those groups:

| Groups belonged to                        | Access permissions granted  |
|---|---|
| <b>Administrators</b> and <b>Region A</b> | read-write access to the web interface but no API access            |
| <b>Administrators</b> and <b>Region B</b> | read-write access to the API interface, but no web interface access |
| <b>Administrators</b> and <b>Region C</b> | read-write access to the web and API interfaces                     |
| <b>Region A</b> only                      | read-only access to the web interface and no API access             |



## Resetting forgotten passwords

You can reset any account password by logging in to the Expressway as the default **admin** account or as any other administrator account that has read-write access. If this is not possible you can reset the **admin** or **root** password via the console.

### Changing an administrator account password via GUI

You can change the password for the default administrator account and for additional local administrator accounts.

Go to **Users > Administrator accounts**. Under **Actions** for the relevant administrator account, click **Change password**.

A new page is displayed, where you can change the password for the selected administrator. Enter the new password and confirm it. You must also enter the password for the administrator account with which you are currently logged in to authorize the password change.

### Resetting root or admin password via serial connection

On a hardware Expressway, reset the **admin** or **root** password as follows:

1. Connect a PC to the Expressway using the serial cable. Serial port / console access is always enabled for one minute following a restart, even if it is normally disabled.
2. Restart the Expressway.
3. Log in from the PC with the username **pwrec**. No password is required.
4. If the administrator account authentication source is set to *Remote*, you are given the option to change the setting to *Both*; this will allow local administrator accounts to access the system.
5. Select the account (**root** or **admin**) whose password you want to change.
6. You will be prompted for a new password.

The **pwrec** account is only active for one minute following a restart. After that time you will have to restart the system again to change the password.

### Resetting root or admin password via vSphere

If you have forgotten the password for either an administrator account or the **root** account and you are using a VM (Virtual Machine) Expressway, you can reset it using the following procedure:

1. Open the vSphere client.
2. Click on the link **Launch Console**.
2. Reboot the Expressway.
3. In the vSphere console log in with the username **pwrec**. No password is required.
4. When prompted, select the account (*root* or the username of the administrator account) whose password you want to change.
5. You will be prompted for a new password.

The **pwrec** account is only active for one minute following a reboot. After that time you will have to reboot the system again to reset the password.

## Using the root account

The Expressway provides a root account which can be used to log in to the Expressway operating system. This account has a username of **root** (all lower case) and a default password of **TANDBERG** (all upper case). For security reasons you must change the password as soon as possible. An alarm is displayed on the web interface and the CLI if the **root** account has the default password set.

---

**Note:** the **root** account may allow access to sensitive information and it should not be used in normal operation, and in particular system configuration should not be conducted using this account. Use the **admin** account instead.

---

## Changing the root account password

To change the password for the **root** account:

1. Log in to the Expressway as **root** using the existing password. By default you can only do this using a serial connection or SSH.
2. Type the command **passwd**.  
You will be asked for the new password.
3. Enter the new password and when prompted, retype the password.
4. Type **exit** to log out of the root account.

## Accessing the root account over SSH

The root account can be accessed over a serial connection or SSH only.

To enable and disable access to the root account using SSH:

1. Log in to the Expressway as **root**.
2. Type one of the following commands:
  - **rootaccess --ssh on** to enable access using SSH
  - **rootaccess --ssh off** to disable access using SSH
3. Type **exit** to log out of the root account.

If you have disabled SSH access while logged in using SSH, your current session will remain active until you log out, but all future SSH access will be denied.

# Managing SSO tokens

Go to **Users > SSO token holders** to view the list of users who currently hold SSO tokens. This page can help you troubleshoot issues related to single sign-on for a particular user.

You can also use this page to **Purge tokens from all holders**. This option is probably disruptive for your users so make sure you need it before you proceed. You may need it, for example, if you know your security is compromised, or if you are upgrading internal or edge infrastructure.

## To manage the tokens of a particular user:

1. [Optional] Filter by a substring of the username to return a smaller list.  
You may need this if there are many usernames in the list, because a long list spans multiple pages of up to 200 usernames each.
2. Click a username to see the detail of the tokens held by that user.  
The **SSO tokens for user <Username>** page appears, listing details of the tokens issued to that user. The details include the token issuer and expiry.
3. [Optional] Click **Delete these tokens** if you want the user's identity to be confirmed before they continue to access the UC services.  
The next time the user's client attempts to access UC services via this Expressway-C, the client will be redirected to the IdP with a new, signed request. The user may need to reauthenticate at the IdP, so that it can assert their identity to the Expressway-C. The user can then be issued with new tokens where authorized.

# Maintenance

---

This section describes the pages that appear under the **Configuration > Maintenance** menu of the Expressway web interface.

- Enabling SSH access ..... 214
- Enabling maintenance mode ..... 215
- About upgrading software components ..... 216
- Configuring logging ..... 219
- Managing option keys ..... 222
- About security certificates ..... 223
- Configuring language settings ..... 234
- Backing up and restoring Expressway data ..... 236
- Diagnostics tools ..... 238
- Incident reporting ..... 241
- Checking the effect of a pattern ..... 244
- Locating an alias ..... 245
- Port usage ..... 246
- Network utilities ..... 248
- Restarting, rebooting and shutting down ..... 252
- Developer resources ..... 254

## Enabling SSH access

You may want to enable SSH access to the Expressway so that you can access it securely without requiring password-based login. One common reason for this is to improve the efficiency of monitoring and logging. You will need to repeat this procedure on each Expressway that you want to access in this way.

---

**CAUTION:** You will use root access to authorize your public key. Take care not to increase your security exposure or cause any unsupported configuration. We strongly discourage using `root`.

---

1. Use SSH to log in as `root`
2. Enter `mkdir /tandberg/.ssh` to create `.ssh` directory if it is not already present
3. Copy your public key to `/tandberg/.ssh`
4. Append your public key to the `authorized_keys` file with `cat /tandberg/.ssh/id_rsa.pub >> /tandberg/.ssh/authorized_keys`  
where `id_rsa.pub` is substituted with the name of your public key. Do not place your key anywhere else because the key could be lost on upgrade (`authorized_keys` file does persist)
5. Log off and test SSH access using your own key  
If you cannot access the Expressway with your key, you may need to connect as `root` and restart the SSH daemon with `/etc/init.d/sshd restart`

## Enabling maintenance mode

Maintenance mode is typically used when you need to upgrade or take out of service an Expressway peer that is part of a cluster. It allows the other cluster peers to continue to operate normally while the peer that is in maintenance mode is upgraded or serviced.

Putting a peer into maintenance mode provides a controlled method of stopping any further calls from being managed by that peer:

- Standard Expressway sessions:
  - New calls will be handled by another peer in the cluster.
  - Existing calls will continue until the call is terminated. If necessary, you can manually remove any calls on this peer that do not clear automatically by going to **Status > Calls**, selecting the check box next to the calls you want to terminate and clicking **Disconnect** (note that SIP calls may not disconnect immediately).
- Unified CM mobile and remote access sessions:
  - Any existing calls passing through that Expressway will be dropped.
  - Jabber clients will failover automatically and re-register through another peer in the cluster.
  - Clients running TC software will not failover automatically will have to be restarted.

To maintain capacity, we recommend that you only enable maintenance mode on one peer at a time.

To enable maintenance mode:

1. Log in the relevant peer.
2. Go to the **Maintenance mode** page (**Maintenance > Maintenance mode**).
3. Set **Maintenance mode** to *On*.
4. Click **Save** and click **OK** on the confirmation dialog.

Note that:

- An alarm is raised while the peer is in maintenance mode.
- You can monitor the **Resource usage** page (**Status > System > Resource usage**) to check how many calls are currently being handled by that peer.
- Maintenance mode is automatically disabled if the peer is restarted.

# About upgrading software components

You can install new releases of the Expressway software components on your existing hardware.

Component upgrades can be performed in one of two ways:

- [Using the web interface](#) - this is the recommended process.
- [Using secure copy](#) (SCP/PSCP).

This guide describes how both of these methods are used to perform upgrades.

- We recommended that you upgrade Expressway components while the system is inactive.
- If you are upgrading a cluster, you must follow the directions in [Expressway Cluster Creation and Maintenance Deployment Guide](#)

## Expressway software components

All existing installed components are listed on the **Upgrade** page (**Maintenance > Upgrade**), showing their current version and associated release key where appropriate.

The main component is the **System platform**, and when upgraded this will typically include automatic upgrades of some or all of the other components. However, you can independently upgrade the other components if required to do so. The upgrade process ensures that compatibility is maintained across all components.

## Upgrade prerequisites

The upgrade requires you to have:

- a valid **Release key**, if you are upgrading to the next major release of the **System platform**, for example from X8.1 to X9.0; it is not required for dot releases, for example X8.1 to X8.2
- a software image file for the component you want to upgrade, and it is stored in a network location that is locally accessible from your client computer; use the standard .tar.gz software image file when upgrading a virtual machine (the .ova file is only required for the initial install of the Expressway software on VMware)
- release notes for the software version you are upgrading to — additional manual steps may be required

Contact your Cisco representative for more information on how to obtain these.

## Backing up before upgrading

You should backup your system configuration before upgrading. Click **System backup** to go to the [Backup and restore](#) page.

## Upgrading and option keys

All existing option keys are retained through the upgrade from one version of the **System platform** to the next, including upgrades to the next major release. However, you are recommended to take note of your existing option keys before performing the upgrade.

New features may also become available with each major release of the **System platform** component, and you may need to install new option keys to take advantage of these new features. Contact your Cisco representative for more information on all the options available for the latest release of Expressway software.

## Installing and rebooting

Upgrading the **System platform** component is a two-stage process. First, the new software image is uploaded onto the Expressway. At the same time, the current configuration of the system is recorded, so that



this can be restored after the upgrade. During this initial stage the system will continue running on its existing software version, and all normal system processes will continue.

The second part of the upgrade involves rebooting the system. It is only during the reboot that the Expressway installs the new software version and restores the previous configuration. Rebooting causes all current calls to terminate.

This means that you can upload the new software at any time, and then wait until a convenient moment (for example, when no calls are taking place) to switch to the new version by rebooting the system.

---

**Note:** any configuration changes made between the software upload and the reboot will be lost when the system restarts using the new software version.

---

The upgrade of components other than the **System platform** does not involve a system reboot, however the services provided by that component will be temporarily stopped while the upgrade process completes.

## Upgrading Expressway software

The **Upgrade** page (**Maintenance > Upgrade**) is used to install new (or to downgrade) versions of Expressway software components.

To upgrade a component using the web interface:

1. Review the relevant release notes to see if any special steps are required either before or after installing the software image file.
2. Go to the **Upgrade** page (**Maintenance > Upgrade**).
3. Click **Browse** and select the software image file for the component you want to upgrade.  
The Expressway automatically detects which component you are upgrading based upon the selected software image file.
4. Enter the **Release key** if required.
5. Click **Upgrade**.  
The Expressway will start loading the file. This may take a few minutes.
6. For upgrades to the **System platform** component, the **Upgrade confirmation** page is displayed:
  - a. Check that:
    - o the expected **New software version** number is displayed
    - o the **MD5 hash** and **SHA1 hash** values match the values displayed on the cisco.com page, where you have downloaded the software image file
  - b. Click **Continue with upgrade**.  
The **System upgrade** page opens and displays a progress bar while the software installs.  
When the software has installed, a summary of active calls is displayed. These will be lost when you reboot the system.
  - c. Click **Reboot system**.  
Note that if you make any configuration changes between uploading the software and rebooting, those changes will be lost when the system restarts.  
After the reboot is complete you are taken to the **Login** page.
7. For upgrades to other components, the software is automatically installed. No reboot is required.

The upgrade is now complete. The **Overview** and **Upgrade** pages now show the upgraded software component version numbers.

Note that some components may require [option keys](#) to enable them; this is done through the Option keys page (**Maintenance > Option keys**).

## Downgrading

If you need to downgrade to an earlier release of the **System platform**, configuration changes will be lost. When the downgrade has completed you will have to restore a backup of the system configuration that was made against the release you have just reinstalled. Other manual steps may be required — you must review the release notes for the version you are downgrading from.

- To downgrade a component to an older release you should follow the same instructions as above for upgrading, but select the appropriate software image file for the software version you want to downgrade to.
- As with upgrading, you are recommended to backup your system configuration before downgrading.

## Upgrading using secure copy (SCP/PSCP)

To upgrade using a secure copy program such as SCP or PSCP (part of the PuTTY free package) you need to transfer two files to the Expressway:

- A text file containing just the 16-character Release Key (required for the **System platform** component only). Ensure there is no extraneous white space in this file.
- The file containing the software image.

To transfer these files:

1. If you are upgrading the **System platform** component, upload the Release Key file using SCP/PSCP to the `/tmp/` folder on the system. The target name must be **release-key**, for example:  

```
scp release-key root@10.0.0.1:/tmp/release-key
```

  - Enter the root password when prompted.
  - The Release Key file must be uploaded before the image file.
2. Upload the software image using SCP/PSCP.
  - For the **System platform** component:  
Upload to the `/tmp` folder on the system. The target name must be `/tmp/tandberg-image.tar.gz`, for example: 

```
scp s42700x8_1_0.tar.gz root@10.0.0.1:/tmp/tandberg-image.tar.gz
```
  - For other components:  
Upload to the `/tmp/pkgs/new/` folder on the system, preserving the file name and extension, for example: 

```
scp root@10.0.0.1:/tmp/pkgs/new/vcs-lang-es-es_8.1_amd64.tlp
```
3. Enter the root password when prompted.  
The software installation begins automatically. Wait until the software has installed completely. This should not take more than five minutes.
4. If you have upgraded the **System platform** component, log in to the Expressway, either using the web interface or CLI, and reboot the Expressway. After about five minutes the system will be ready to use.

---

**Note:** if you make any further configuration changes before rebooting, those changes will be lost when the system restarts, so you are recommended to reboot your system immediately.

---

# Configuring logging

The Expressway provides syslogging features for troubleshooting and auditing purposes.

The Event Log is a rotating local log that records information about such things as calls and messages sent and received.

The Expressway's logging options are configured on the **Logging** page (**Maintenance > Logging**) where you can:

- specify the [Local event log verbosity](#) to change the depth of event information recorded locally
- toggle [Media statistics logging](#)
- define one or more [remote syslog server](#) addresses
- filter the events sent to each remote syslog server by severity

## Changing Event log verbosity

Control the local log verbosity by setting the **Local event log verbosity** between 1 and 4.

All events have an associated level in the range 1-4, with Level 1 Events considered the most important. The table below gives an overview of the levels assigned to different events.

| Level | Assigned events   |
|-------|---|
| 1     | <p>High-level events such as registration requests and call attempts. Easily human readable. For example:</p> <ul style="list-style-type: none"> <li>■ call attempt/connected/disconnected</li> <li>■ registration attempt/rejected</li> </ul> <p>Note that endpoints or other devices cannot register to the Expressway. Registration requests will be rejected and will be logged with 'License limit exceeded' messages.</p> |
| 2     | <p>All Level 1 events, plus:</p> <ul style="list-style-type: none"> <li>■ logs of protocol messages sent and received (SIP, H.323, LDAP and so on) excluding noisy messages such as H.460.18 keepalives and H.245 video fast-updates</li> </ul>   |
| 3     | <p>All Level 1 and Level 2 events, plus:</p> <ul style="list-style-type: none"> <li>■ protocol keepalives</li> <li>■ call-related SIP signaling messages</li> </ul>   |
| 4     | <p>The most verbose level: all Level 1, Level 2 and Level 3 events, plus:</p> <ul style="list-style-type: none"> <li>■ network level SIP messages</li> </ul>  |

See the [Events and levels](#) section for a complete list of all events that are logged by the Expressway, and the level at which they are logged.

---

**Notes:**

- Events are always logged locally (to the Event Log) regardless of whether or not remote logging is enabled.
  - Logging at level 3 or level 4 is not recommended for normal operation, because such detailed logging may cause the 2GB log to rotate too quickly. You may need to record this level of detail while troubleshooting.
  - Changes to the log level affect both the Event Log that you can view via the web interface, and the information that is copied to any remote log server.
  - Changes to the log level are not retrospective — they only affect what is logged after you change the level.
  - The Expressway uses the following facilities for local logging. The software components / logs that map to the (local) facilities are emphasised:
    - 0 (kern)
    - 3 (daemon)
    - 16 (local0) *Administrator*
    - 17 (local1) *Config*
    - 18 (local2) *Mediastats*
    - 19 (local3) *Apache error*
    - 20 (local4) *etc/opt/apache2*
    - 21 (local5) *Developer*
    - 22 (local6) *Network*
- 

## Logging media statistics

When you switch **Media statistics** to *On*, the Expressway starts logging media statistics to the local hard disk, in `/mnt/harddisk/log`. Up to 200 files of 10MB each are stored, with the oldest being deleted when the 200<sup>th</sup> is full.

Media statistics messages are also published as syslog messages. While the Media statistics logging option is on, the Expressway publishes statistics using facility 18 (local2) to all remote syslog servers you have configured.

Some examples of the media statistics are packets forwarded, packets lost, jitter, media type, codec, and actual bitrate.

---

**Note:** The message severity is *Informational* but media statistics messages are always published, irrespective of the severity filters.

---

## Publishing logs to remote syslog servers

Syslog is a convenient way to aggregate log messages from multiple systems to a single location. This is particularly recommended for peers in a cluster.

- You can configure the Expressway to publish log messages to up to 4 remote syslog servers.
- The syslog servers must support one of the following standard protocols:
  - BSD (as defined in [RFC 3164](#))
  - IETF (as defined in [RFC 5424](#))

### Configuring remote syslog servers

1. Go to **Maintenance > Logging**, and enter the IP addresses or Fully Qualified Domain Names (FQDNs) of the **Remote syslog servers** to which this system will send log messages.

2. For each server address, specify the syslog protocol in the **Mode** field.  
If you select *Custom*, you can specify the **Transport**, **Port**, and **Format**.
3. For each server, use the **Log level** control to select how much detail to send.  
The Expressway sends messages of the selected severity and all of the more severe messages.
4. Click **Save**.

### Which Mode should I use?

The **Mode** option of the Expressway's syslog feature configures several parameters of the outgoing syslog messages. The following table should help you select the mode that best matches your logging server(s) and network configuration. *Custom* allows you the most control over the transport, port, and message format used, and you must use *Custom* if you want revocation checking for the syslog server certificate.

Table 7: Syslog Mode options

| Option in the user interface            | Transport protocol                             | Port number  | Message format   |
|---|--|--|--|
| <i>Legacy BSD format</i>                | UDP  | 514  | BSD format. See <a href="#">RFC 3164</a>                     |
| <i>IETF syslog format</i>               | UDP  | 514  | IETF format. See <a href="#">RFC 5424</a>                    |
| <i>IETF syslog using TLS connection</i> | TLS  | 6514   | IETF format. See <a href="#">RFC 5424</a>                    |
| <i>Custom</i>                           | Select <i>UDP</i> , <i>TCP</i> , or <i>TLS</i> | Configurable. We recommend (UDP) 514 or (TCP) 6514 | Select <i>Legacy BSD format</i> or <i>IETF syslog format</i> |

### Notes:

- The UDP protocol is stateless. If reliability of syslog messages is very important in your environment, you should use a different transport protocol.
- If there is a firewall between the Expressway and the syslog server, you must open the appropriate port to allow the messages through.
- If you select TLS transport, the Expressway must trust the syslog server's certificate. Upload the syslog server's CA certificate to the local trust store if necessary.
- CRL checking is disabled by default; to enable CRL checking you must use *Custom* mode, set **CRL check** to *On*, and ensure that relevant certificate revocation lists (CRLs) are loaded. See [About security certificates \[p.223\]](#) for more information.
- The remote server cannot be another Expressway.
- An Expressway cannot act as a remote log server for other systems.
- The Expressway uses the following facilities for remote logging. The software components / logs that map to the (local) facilities are emphasised:
  - 0 (kern)
  - 3 (daemon)
  - 16 (local0) *Administrator*
  - 17 (local1) *Config*
  - 18 (local2) *Mediastats*
  - 19 (local3) *Apache error*
  - 20 (local4) *etc/opt/apache2*
  - 21 (local5) *Developer*
  - 22 (local6) *Network*

# Managing option keys

Options are used to add additional features to the Expressway. Option keys can either be valid for a fixed time period or have an unlimited duration. Your Expressway may have been shipped with one or more optional features pre-installed. To purchase further options, contact your Cisco representative.

The **Option keys** page ([Maintenance > Option keys](#)) lists all the existing options currently installed on the Expressway, and allows you to add new options.

The **System information** section summarizes the existing features installed on the Expressway and displays the **Validity period** of each installed key. The options that you may see here include:

- **Traversal Server:** enables the Expressway to work as a firewall traversal server.
- **H.323 to SIP Interworking gateway:** enables H.323 calls to be translated to SIP and vice versa.
- **Advanced Networking:** enables static NAT functionality and the LAN 2 port on an Expressway-E.
- **Rich media sessions:** determines the number of non-Unified Communications calls allowed on the Expressway (or Expressway cluster) at any one time. See the [Call types and licensing \[p.315\]](#) section for more information.
- **TURN Relays:** the number of concurrent TURN relays that can be allocated by this Expressway (or Expressway cluster). See [About ICE and TURN services \[p.55\]](#) for more information.
- **Encryption:** indicates that AES (and DES) encryption is supported by this software build.
- **Microsoft Interoperability:** enables encrypted calls to and from Microsoft Lync 2010 Server (for both native SIP calls and calls interworked from H.323). It is also required by the Lync B2BUA when establishing [ICE](#) calls to Lync 2010 clients. It is required for all types of communication with Lync 2013.
- **Expressway Series:** identifies and configures the product for Expressway Series system functionality.

See [License usage within a cluster \[p.136\]](#) for more information about how rich media session and TURN relay option key licenses are shared across all peers in the cluster.

## Adding option keys using the web interface

To add an option key:

1. In the **Add option key** field, enter the key that has been provided to you for the option you want to add.
2. Click **Add option**.

Some option keys require that the Expressway is restarted before the option key will take effect. In such cases you will receive an alarm on the web interface, which will remain in place as a reminder until the system has been restarted. However, you can continue to use and configure the Expressway in the meantime.

## Adding option keys using the CLI

To return the indexes of all the option keys that are already installed on your system:

```
xStatus Options
```

To add a new option key to your system:

```
xConfiguration Option [1..64] Key
```

---

**Note:** when using the CLI to add an extra option key, you can use any unused option index. If you chose an existing option index, that option will be overwritten and the extra functionality provided by that option key will no longer exist. To see which indexes are currently in use, type `xConfiguration option`.

---

## About security certificates

For extra security, you may want to have the Expressway communicate with other systems (such as LDAP servers, neighbor Expressways, or clients such as SIP endpoints and web browsers) using TLS encryption.

For this to work successfully in a connection between a client and server:

- The server must have a certificate installed that verifies its identity. This certificate must be signed by a Certificate Authority (CA).
- The client must trust the CA that signed the certificate used by the server.

The Expressway allows you to install appropriate files so that it can act as either a client or a server in connections using TLS. The Expressway can also authenticate client connections (typically from a web browser) over HTTPS. You can also upload certificate revocation lists (CRLs) for the CAs used to verify LDAP server and HTTPS client certificates.

The Expressway can generate server certificate signing requests (CSRs). This removes the need to use an external mechanism to generate and obtain certificate requests.

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.

Note that in connections:

- to an endpoint, the Expressway acts as the TLS server
- to an LDAP server, the Expressway is a client
- between two Expressway systems, either Expressway may be the client with the other Expressway being the TLS server
- via HTTPS, the web browser is the client and the Expressway is the server

TLS can be difficult to configure. For example, when using it with an LDAP server we recommend that you confirm that your system is working correctly before you attempt to secure the connection with TLS. You are also recommended to use a third party LDAP browser to verify that your LDAP server is correctly configured to use TLS.

---

**Note:** be careful not to allow your CA certificates or CRLs to expire as this may cause certificates signed by those CAs to be rejected.

---

Certificate and CRL files can only be managed via the web interface. They cannot be installed using the CLI.

See [Managing the trusted CA certificate list \[p.223\]](#) and [Managing the Expressway's server certificate \[p.224\]](#) for instructions about how to install certificates. For further information, see [Certificate Creation and Use with Expressway Deployment Guide](#).

## Managing the trusted CA certificate list

The **Trusted CA certificate** page ([Maintenance > Security certificates > Trusted CA certificate](#)) allows you to manage the list of certificates for the Certificate Authorities (CAs) trusted by this Expressway. When a TLS connection to Expressway mandates certificate verification, the certificate presented to the Expressway must be signed by a trusted CA in this list and there must be a full chain of trust (intermediate CAs) to the root CA.

- To upload a new file containing one or more CA certificates, **Browse** to the required PEM file and click **Append CA certificate**. This will append any new certificates to the existing list of CA certificates. If you are replacing existing certificates for a particular issuer and subject, you have to manually delete the previous certificates.
- To replace all of the currently uploaded CA certificates with the system's original list of trusted CA certificates, click **Reset to default CA certificate**.
- To view the entire list of currently uploaded trusted CA certificates, click **Show all (decoded)** to view it in a human-readable form, or click **Show all (PEM file)** to view the file in its raw format.
- To view an individual trusted CA certificate, click on **View (decoded)** in the row for the specific CA certificate.
- To delete one or more CA certificates, tick the box(es) next to the relevant CA certificate(s) and click **Delete**.

---

**Note:** if you have enabled certificate revocation list (CRL) checking for TLS encrypted [connections to an LDAP server](#) (for account authentication), you must add the PEM encoded CRL data to your trusted CA certificate file.

---

## Managing the Expressway's server certificate

The **Server certificate** page (**Maintenance > Security certificates > Server certificate**) is used to manage the Expressway's server certificate. This certificate is used to identify the Expressway when it communicates with client systems using TLS encryption, and with web browsers over HTTPS. You can:

- view details about the currently loaded certificate
- generate a certificate signing request
- upload a new server certificate

### Viewing the currently uploaded certificate

The **Server certificate data** section shows information about the server certificate currently loaded on the Expressway.

- To view the currently uploaded server certificate file, click **Show (decoded)** to view it in a human-readable form, or click **Show (PEM file)** to view the file in its raw format.  
Note that if a certificate contains SRV-ID or XMPP-ID formatted entries, when that certificate is viewed those entries will show as '<unsupported>'. That does not mean the certificate is invalid, but that the openssl code does not know how to display those identifiers.
- To replace the currently uploaded server certificate with the Expressway's original certificate, click **Reset to default server certificate**.

---

**Note:** Do not allow your server certificate to expire as this may cause other external systems to reject your certificate and prevent the Expressway from being able to connect to those systems.

---

### Generating a certificate signing request (CSR)

The Expressway can generate server certificate signing requests. This removes the need to use an external mechanism to generate and obtain certificate requests.



To generate a CSR:

1. Go to **Maintenance > Security certificates > Server certificate**.
2. Click **Generate CSR** to go to the **Generate CSR** page.
3. Enter the required properties for the certificate.
  - See [Server certificates and clustered systems \[p.226\]](#) if your Expressway is part of a cluster.
  - See [Server certificate requirements for Unified Communications \[p.61\]](#) if this Expressway is part of a Unified Communications solution.
  - The certificate request includes automatically the public key that will be used in the certificate, and the client and server authentication Enhanced Key Usage (EKU) extension.
4. Click **Generate CSR**. The system will produce a signing request and an associated private key. The private key is stored securely on the Expressway and cannot be viewed or downloaded. You must never disclose your private key, not even to the certificate authority.
5. You are returned to the **Server certificate** page. From here you can:
  - **Download** the request to your local file system so that it can be sent to a certificate authority. You are prompted to save the file (the exact wording depends on your browser).
  - View the current request (click **Show (decoded)** to view it in a human-readable form, or click **Show (PEM file)** to view the file in its raw format).

---

**Note:**

- Only one signing request can be in progress at any one time. This is because the Expressway has to keep track of the private key file associated with the current request. To discard the current request and start a new request, click **Discard CSR**.
- From version X8.5.1 the user interface provides an option to set the Digest algorithm. The default is set to SHA-256, with options to change to SHA-1, SHA-384, or SHA-512.
- The certificate signing request storage location changed in X8.  
When you generate a CSR in X7, the application puts **csr.pem** and **privkey\_csr.pem** into **/tandberg/persistent/certs**.  
When you generate a CSR in X8, the application puts **csr.pem** and **privkey.pem** into **/tandberg/persistent/certs/generated\_csr**.  
If you want to upgrade from X7 and have an unsubmitted CSR, then we recommend discarding the CSR before upgrade, and then regenerating the CSR after upgrade.

---

**Uploading a new server certificate**

When the signed server certificate is received back from the certificate authority it must be uploaded to the Expressway.

The **Upload new certificate** section is used to replace the Expressway's current server certificate with a new certificate.

To upload a server certificate:

1. Go to **Maintenance > Security certificates > Server certificate**.
2. Use the **Browse** button in the **Upload new certificate** section to select and upload the **server certificate** PEM file.
3. If you used an external system to generate the Certificate Signing Request (CSR) you must also upload the **server private key** PEM file that was used to encrypt the server certificate. (The private key file will have been automatically generated and stored earlier if the Expressway was used to produce the CSR for this server certificate.)

- The **server private key** PEM file must not be password protected.
  - You cannot upload a server private key if a certificate signing request is in progress.
4. Click **Upload server certificate data**.

## Server certificates and clustered systems

When a CSR is generated, a single request and private key combination is generated for that peer only.

If you have a cluster of Expressways, you must generate a separate signing request on each peer. Those requests must then be sent to the certificate authority and the returned server certificates uploaded to each relevant peer.

You must ensure that the correct server certificate is uploaded to the appropriate peer, otherwise the stored private key on each peer will not correspond to the uploaded certificate.

## Server certificates and Unified Communications

### Expressway-C server certificate requirements

The Expressway-C server certificate needs to include the following elements in its list of subject alternate names:

- **Unified CM phone security profile names:** the names of the **Phone Security Profiles** in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. Use the FQDN format and separate multiple entries with commas.  
Having the secure phone profiles as alternative names means that Unified CM can communicate via TLS with the Expressway-C when it is forwarding messages from devices that use those profiles.
- **IM and Presence chat node aliases (federated group chat):** the **Chat Node Aliases** (e.g. chatroom1.example.com) that are configured on the IM and Presence servers. These are required only for Unified Communications XMPP federation deployments that intend to support group chat over TLS with federated contacts.  
The Expressway-C automatically includes the chat node aliases in the CSR, providing it has discovered a set of IM&P servers.  
We recommend that you use DNS format for the chat node aliases when generating the CSR. You must include the same chat node aliases in the Expressway-E server certificate's alternative names.

Figure 10: Entering subject alternative names for security profiles and chat node aliases on the Expressway-C's CSR generator

The screenshot shows a web form titled "Alternative name" for generating a CSR. It has three main input sections:

- Additional alternative names (comma separated):** An empty text input field with an information icon.
- IM and Presence chat node aliases (federated group chat):** A text input field containing "chatnode1.xmpp.example.com,chatnode2.xmpp.example.com" and a "Format" dropdown menu set to "DNS".
- Unified CM phone security profile names:** A text input field containing "DX80TLSprofile.example.com" with an information icon.

Below these inputs, the "Alternative name as it will appear" section displays the following list of entries:

- DNS:vcsc.example.com
- DNS:chatnode1.xmpp.example.com
- DNS:chatnode2.xmpp.example.com
- DNS:DX80TLSprofile.example.com

### Expressway-E server certificate requirements

The Expressway-E server certificate needs to include the following elements in its list of subject alternate names:

- Unified CM registrations domains:** all of the domains which are configured on the Expressway-C for Unified CM registrations. They are required for secure communications between endpoint devices and Expressway-E.  
 Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. You may select *CollabEdgeDNS* format instead, which simply adds the prefix `collab-edge.` to the domain that you enter. This format is recommended if you do not want to include your top level domain as a SAN (see example in following screenshot).
- XMPP federation domains:** the domains used for point-to-point XMPP federation. These are configured on the IM&P servers and should also be configured on the Expressway-C as domains for XMPP federation.  
 Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. Do not use the *XMPPAddress* format as it may not be supported by your CA, and may be discontinued in future versions of the Expressway software.
- IM and Presence chat node aliases (federated group chat):** the same set of **Chat Node Aliases** as entered on the Expressway-C's certificate. They are only required for voice and presence deployments which will support group chat over TLS with federated contacts.  
 Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. Do not use the *XMPPAddress* format as it may not be supported by your CA, and may be discontinued in future versions of the Expressway software.  
 Note that you can copy the list of chat node aliases from the equivalent [Generate CSR](#) page on the Expressway-C.

Figure 11: Entering subject alternative names for Unified CM registration domains, XMPP federation domains, and chat node aliases, on the Expressway-E's CSR generator

| Alternative name   |   |
|--|---|
| Additional alternative names (comma separated)           | <input type="text"/>  |
| Unified CM registrations domains                         | <input type="text" value="example.com"/> Format: <span>CollabEdgeDNS</span>   |
| XMPP federation domains                                  | <input type="text" value="xmpp.example.com"/> Format: <span>DNS</span>  |
| IM and Presence chat node aliases (federated group chat) | <input type="text" value="chatnode1.xmpp.example.com,chatnode2.xmpp.example.com"/> Format: <span>DNS</span>                                     |
| Alternative name as it will appear                       | DNS:vcse.example.com<br>DNS:collab-edge.example.com<br>DNS:xmpp.example.com<br>DNS:chatnode1.xmpp.example.com<br>DNS:chatnode2.xmpp.example.com |

## Managing certificate revocation lists (CRLs)

Certificate revocation list (CRL) files are used by the Expressway to validate certificates presented by client browsers and external systems that communicate with the Expressway over TLS/HTTPS. A CRL identifies those certificates that have been revoked and can no longer be used to communicate with the Expressway.

We recommend that you upload CRL data for the CAs that sign TLS/HTTPS client and server certificates. When enabled, CRL checking is applied for every CA in the chain of trust.

### Certificate revocation sources

The Expressway can obtain certificate revocation information from multiple sources:

- automatic downloads of CRL data from CRL distribution points
- through OCSP (Online Certificate Status Protocol) responder URIs in the certificate to be checked (SIP TLS only)
- manual upload of CRL data
- CRL data embedded within the Expressway's **Trusted CA certificate** file

The following limitations and usage guidelines apply:

- when establishing SIP TLS connections, the CRL data sources are subject to the **Certificate revocation checking** settings on the **SIP** configuration page
- automatically downloaded CRL files override any manually loaded CRL files (except for when verifying SIP TLS connections, when both manually uploaded or automatically downloaded CRL data may be used)
- when validating certificates presented by external policy servers, the Expressway uses manually loaded CRLs only
- when validating TLS connections with an LDAP server for remote login account authentication, the Expressway uses CRL data within the **Trusted CA certificate** only

### Automatic CRL updates

We recommend that you configure the Expressway to perform automatic CRL updates. This ensures that the latest CRLs are available for certificate validation.

To configure the Expressway to use automatic CRL updates:

1. Go to **Maintenance > Security certificates > CRL management**.
2. Set **Automatic CRL updates** to *Enabled*.
3. Enter the set of **HTTP(S) distribution points** from where the Expressway can obtain CRL files.  
**Note:**
  - you must specify each distribution point on a new line
  - only HTTP(S) distribution points are supported; if HTTPS is used, the distribution point server itself must have a valid certificate
  - PEM and DER encoded CRL files are supported
  - the distribution point may point directly to a CRL file or to ZIP and GZIP archives containing multiple CRL files
  - the file extensions in the URL or on any files unpacked from a downloaded archive do not matter as the Expressway will determine the underlying file type for itself; however, typical URLs could be in the format:
    - <http://example.com/crl.pem>
    - <http://example.com/crl.der>
    - <http://example.com/ca.crl>
    - <https://example.com/allcrls.zip>
    - <https://example.com/allcrls.gz>
4. Enter the **Daily update time** (in UTC). This is the approximate time of day when the Expressway will attempt to update its CRLs from the distribution points.
5. Click **Save**.

### Manual CRL updates

You can upload CRL files manually to the Expressway. Certificates presented by external policy servers can only be validated against manually loaded CRLs.

To upload a CRL file:

1. Go to **Maintenance > Security certificates > CRL management**.
2. Click **Browse** and select the required file from your file system. It must be in PEM encoded format.
3. Click **Upload CRL file**.  
This uploads the selected file and replaces any previously uploaded CRL file.

Click **Remove revocation list** if you want to remove the manually uploaded file from the Expressway.

If a certificate authority's CRL expires, all certificates issued by that CA will be treated as revoked.

### Online Certificate Status Protocol (OCSP)

The Expressway can establish a connection with an OCSP responder to query the status of a particular certificate. The Expressway determines the OCSP responder to use from the responder URI listed in the certificate being verified. The OCSP responder sends a status of 'good', 'revoked' or 'unknown' for the certificate.

The benefit of OCSP is that there is no need to download an entire revocation list. OCSP is supported for SIP TLS connections only. See below for information on how to enable OCSP.

Outbound communication from the Expressway-E is required for the connection to the OCSP responder. Check the port number of the OCSP responder you are using (typically this is port 80 or 443) and ensure that outbound communication is allowed to that port from the Expressway-E.

## Configuring revocation checking for SIP TLS connections

You must also configure how certificate revocation checking is managed for SIP TLS connections.

1. Go to **Configuration > SIP**.
2. Scroll down to the **Certificate revocation checking** section and configure the settings accordingly:

| Field                                       | Description  | Usage tips   |
|---|--|--|
| <b>Certificate revocation checking mode</b> | Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment.  | We recommend that revocation checking is enabled.  |
| <b>Use OCSP</b>                             | Controls whether the Online Certificate Status Protocol (OCSP) may be used to perform certificate revocation checking. | To use OCSP, the X.509 certificate to be checked must contain an OCSP responder URI.   |
| <b>Use CRLs</b>                             | Controls whether Certificate Revocation Lists (CRLs) are used to perform certificate revocation checking.              | CRLs can be used if the certificate does not support OCSP.<br><br>CRLs can be loaded manually onto the Expressway, downloaded automatically from preconfigured URIs (see <a href="#">Managing certificate revocation lists (CRLs) [p.227]</a> ), or downloaded automatically from a CRL distribution point (CDP) URI contained in the X.509 certificate. |

| Field                                | Description   | Usage tips   |
|--------------------------------------|---|--|
| <b>Allow CRL downloads from CDPs</b> | Controls whether the download of CRLs from the CDP URIs contained in X.509 certificates is allowed.   |  |
| <b>Fallback behavior</b>             | <p>Controls the revocation checking behavior if the revocation status cannot be established, for example if the revocation source cannot be contacted.</p> <p><i>Treat as revoked</i>: treat the certificate as revoked (and thus do not allow the TLS connection).</p> <p><i>Treat as not revoked</i>: treat the certificate as not revoked.</p> <p>Default: <i>Treat as not revoked</i></p> | <p><i>Treat as not revoked</i> ensures that your system continues to operate in a normal manner if the revocation source cannot be contacted, however it does potentially mean that revoked certificates will be accepted.</p> |

## Configuring certificate-based authentication

The [Certificate-based authentication configuration](#) page ([Maintenance > Security certificates > Certificate-based authentication configuration](#)) is used to configure how the Expressway retrieves authorization credentials (the username) from a client browser's certificate.

This configuration is required if **Client certificate-based security** (as defined on the [System](#) page) has been set to *Certificate-based authentication*. This setting means that the standard login mechanism is no longer available and that administrators can log in only if they present a valid browser certificate — typically provided via a smart card (also referred to as a Common Access Card or CAC) — and the certificate contains appropriate credentials that have a suitable authorization level.

### Enabling certificate-based authentication

The recommended procedure for enabling certificate-based authentication is described below:

1. Add the Expressway's trusted CA and server certificate files (on the [Trusted CA certificate](#) and [Server certificate](#) pages, respectively).
2. Configure certificate revocation lists (on the [CRL management](#) page).
3. Use the [Client certificate testing](#) page to verify that the client certificate you intend to use is valid.
4. Set **Client certificate-based security** to *Certificate validation* (on the [System administration](#) page).
5. Restart the Expressway.
6. Use the [Client certificate testing](#) page again to set up the required regex and format patterns to extract the username credentials from the certificate.
7. Only when you are sure that the correct username is being extracted from the certificate, set **Client certificate-based security** to *Certificate-based authentication*.

### Authentication versus authorization

When the Expressway is operating in certificate-based authentication mode, user authentication is managed by a process external to the Expressway.

When a user attempts to log in to the Expressway, the Expressway will request a certificate from the client browser. The browser may then interact with a card reader to obtain the certificate from the smart card (or alternatively the certificate may already be loaded into the browser). To release the certificate from the

card/browser, the user will typically be requested to authenticate themselves by entering a PIN. If the client certificate received by the Expressway is valid (signed by a trusted certificate authority, in date and not revoked by a CRL) then the user is deemed to be authenticated.

To determine the user's authorization level (read-write, read-only and so on) the Expressway must extract the user's authorization username from the certificate and present it to the relevant local or remote authorization mechanism.

Note that if the client certificate is not protected (by a PIN or some other mechanism) then unauthenticated access to the Expressway may be possible. This lack of protection may also apply if the certificates are stored in the browser, although some browsers do allow you to password protect their certificate store.

## Obtaining the username from the certificate

The username is extracted from the client browser's certificate according to the patterns defined in the **Regex** and **Username format** fields on the [Certificate-based authentication configuration](#) page:

- In the **Regex** field, use the `(?<name>regex)` syntax to supply names for capture groups so that matching sub-patterns can be substituted in the associated **Username format** field, for example, `/(Subject:.* , CN=(?<Group1>.*))/m`.  
The regex defined here must conform to [PHP regex guidelines](#).
- The **Username format** field can contain a mixture of fixed text and the capture group names used in the **Regex**. Delimit each capture group name with #, for example, `prefix#Group1#suffix`. Each capture group name will be replaced with the text obtained from the regular expression processing.

You can use the [Client certificate testing](#) page to test the outcome of applying different **Regex** and **Username format** combinations to a certificate.

## Testing client certificates

The [Client certificate testing](#) page ([Maintenance > Security certificates > Client certificate testing](#)) is used to check client certificates before enabling [client certificate validation](#). You can:

- Test whether a client certificate is valid when checked against the Expressway's current trusted CA list and, if loaded, the revocation list (see [Managing certificate revocation lists \(CRLs\) \[p.227\]](#)).
- Test the outcome of applying the regex and template patterns that retrieve a certificate's authorization credentials (the username).

You can test against:

- a certificate on your local file system
- the browser's currently loaded certificate

### To test if a certificate is valid:

1. Select the **Certificate source**. You can choose to:
  - upload a test file from your file system in either PEM or plain text format; if so click **Browse** to select the certificate file you want to test
  - test against the certificate currently loaded into your browser (only available if the system is already configured to use *Certificate validation* and a certificate is currently loaded)
2. Ignore the **Certificate-based authentication pattern** section - this is only relevant if you are extracting authorization credentials from the certificate.

3. Click **Check certificate**.
4. The results of the test are shown in the **Certificate test results** section.

#### To retrieve authorization credentials (username) from the certificate:

1. Select the **Certificate source** as described above.
2. Configure the **Regex** and **Username format** fields as required. Their purpose is to extract a username from the nominated certificate by supplying a regular expression that will look for an appropriate string pattern within the certificate. The fields default to the currently configured settings on the **Certificate-based authentication configuration** page but you can change them as required.
  - In the **Regex** field, use the `(?<name>regex)` syntax to supply names for capture groups so that matching sub-patterns can be substituted in the associated **Username format** field, for example, `/(Subject:.*, CN=(?<Group1>.*) )/m`.  
The regex defined here must conform to [PHP regex guidelines](#).
  - The **Username format** field can contain a mixture of fixed text and the capture group names used in the **Regex**. Delimit each capture group name with #, for example, `prefix#Group1#suffix`. Each capture group name will be replaced with the text obtained from the regular expression processing.
3. Click **Check certificate**.  
The results of the test are shown in the **Certificate test results** section. The **Resulting string** item is the username credential that would be checked against the relevant authorization mechanism to determine that user's authorization (account access) level.
4. If necessary, you can modify the **Regex** and **Username format** fields and repeat the test until the correct results are produced.  
Note that if the **Certificate source** is an uploaded PEM or plain text file, the selected file is temporarily uploaded to the Expressway when the test is first performed:
  - if you want to keep testing different **Regex** and **Username format** combinations against the same file, you do not have to reselect the file for every test
  - if you change the contents of your test file on your file system, or you want to choose a different file, you must click **Browse** again and select the new or modified file to upload
5. If you have changed the **Regex** and **Username format** fields from their default values and want to use these values in the Expressway's actual configuration (as specified on the **Certificate-based authentication configuration** page) then click **Make these settings permanent**.

Note:

- Any uploaded test file is automatically deleted from the Expressway at the end of your login session.
- The regex is applied to a plain text version of an encoded certificate. The system uses the command `openssl x509 -text -nameopt RFC2253 -noout` to extract the plain text certificate from its encoded format.

## Testing secure traversal

This utility tests whether a secure connection can be made from the Expressway-C to the Expressway-E. A secure connection is required for a Unified Communications traversal zone, and is optional (recommended) for a normal traversal zone.

If the secure traversal test fails, the utility raises a warning with appropriate resolution where possible.

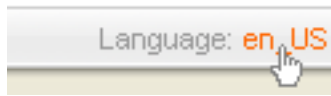
1. On the Expressway-C, go to **Maintenance > Security certificates > Secure traversal test**.
2. Enter the FQDN of the Expressway-E that is paired with this Expressway-C.



3. Enter the TLS verify name of this Expressway-C, as it appears on the paired Expressway-E. This setting is in the SIP section of the Expressway-E's traversal zone configuration page.
4. Click **Test connection**.  
The secure traversal test utility checks whether the hosts on either side of the traversal zone recognize each other and trust each others' certificate chains.

# Configuring language settings

The **Language** page (**Maintenance > Language**) controls which language is used for text displayed in the web user interface.



You can also get to the **Language** page by clicking on the **Language** link at the bottom of every page.

## Changing the language

You can configure both the default language and the language to use on an individual browser:

| Field                          | Description  | Usage tips  |
|--------------------------------|--|---|
| <b>System default language</b> | The default language used on the web interface.  | You can select from the set of installed language packs.  |
| <b>This browser</b>            | The language used by the current browser on the current client computer. It can be set to use either the system default language or a specific alternative language. | This setting applies to the browser currently in use on the client computer. If you access the Expressway user interface using a different browser or a different computer, a different language setting may be in place. |

## 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.

For the list of available languages, see the relevant release notes for your software version.

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.
- If you upgrade to a later version of Expressway software you will see a "Language pack mismatch" alarm. You may need to install a later version of the associated language pack to ensure that all text is available in the chosen language.

## Removing language packs

To remove a language pack:

1. Go to the **Language** page (**Maintenance > Language**).
2. From the list of installed language packs, select the language packs you want to remove.
3. Click **Remove**.
4. Click **Yes** when asked to confirm their removal.  
The selected language packs are then removed. This may take several seconds.

# Backing up and restoring Expressway data

The **Backup and restore** page (**Maintenance > Backup and restore**) is used to create and restore backup files of your Expressway data.

## When to create a backup

You are recommended to create a backup in the following situations:

- before performing an upgrade
- before performing a system restore
- in demonstration and test environments if you want to be able to restore the Expressway to a known configuration

## Content of the backup file

The data in the backup includes:

- system configuration settings
- clustering configuration
- security certificates
- administrator account details
- call detail records (if the CDR service on Expressway is enabled)

Log files are not included in the backup files.

## Limitations

The following limitations apply:

- Backups can only be restored to a system running the same version of software from which the backup was made.
- You can create a backup on one Expressway and restore it to a different Expressway, for example if the original system has failed. However, before performing the restore you must install on the new system the same set of option keys that were installed on the old system. If you attempt to restore a backup made on a different Expressway, you will receive a warning message, but you will be allowed to continue.
- Do not use backups to copy data between Expressways, because system specific information, such as IP addresses, will be duplicated.

---

**Note:** We recommend that you take the Expressway unit out of service before performing a restore.

---

For extra information about backing up and restoring peers in a cluster, see the [Cluster upgrades, backup and restore \[p.141\]](#) section.

## Creating a system backup

To create a backup of Expressway system data:

1. Go to **Maintenance > Backup and restore**.
2. Optionally, enter an **Encryption password** with which to encrypt the backup file. If a password is specified, the same password will be required to restore the file.
3. Click **Create system backup file**.
4. After the backup file has been prepared, a pop-up window appears and prompts you to save the file (the exact wording depends on your browser). The default name is in the format:  
**<software version>\_<hardware serial number>\_<date>\_<time>\_backup.tar.gz**.  
(The file extension is normally **.tar.gz.enc** if an encryption password is specified. However, if you use Internet Explorer to create an encrypted backup file, the filename extension will be **.tar.gz.gz** by default. These different filename extensions have no operational impact; you can create and restore encrypted backup files using any supported browser.)  
The preparation of the system backup file may take several minutes. Do not navigate away from this page while the file is being prepared.
5. Save the file to a designated location.

Log files are not included in the system backup file.

## Restoring a previous backup

To restore the Expressway to a previous configuration of system data:

1. Go to **Maintenance > Backup and restore**.
2. In the **Restore** section, **Browse** to the backup file containing the configuration you want to restore.
3. In the **Decryption password** field, enter the password that was used to create the backup file, or leave it blank if the backup file was created without a password.
4. Click **Upload system backup file**.
5. The Expressway checks the file and takes you to the **Restore confirmation** page.
  - If the backup file is not valid or an incorrect decryption password is entered, you will receive an error message at the top of the **Backup and restore** page.
  - You are shown the current software version and the number of calls.
6. Read all the warning messages that appear before proceeding with the restore.
7. Click **Continue with system restore** to continue with the restore process.  
This will restart your system, so ensure that there are no active calls.

After the system restarts, you are taken to the **Login** page.

# Diagnostics tools

This section provides information about how to use the diagnostics tools:

- [diagnostic logging](#)
- [system snapshot](#)
- [Network Log](#) and [Support Log](#) advanced logging configuration tools
- [incident reporting](#)

## Configuring diagnostic logging

The **Diagnostic logging** tool (**Maintenance > Diagnostics > Diagnostic logging**) can be used to assist in troubleshooting system issues.

It allows you to generate a diagnostic log of system activity over a period of time, and then to download the log so that it can be sent to your Cisco customer support representative. You can also take and subsequently download a tcpdump while logging is in progress.

To use this tool:

1. Go to **Maintenance > Diagnostics > Diagnostic logging**.
2. Optionally, select **Take tcpdump while logging**.
3. Click **Start new log**.
4. (Optional) Enter some **Marker** text and click **Add marker**.
  - The marker facility can be used to add comment text to the log file before certain activities are performed. This helps to subsequently identify the relevant sections in the downloaded diagnostic log file.
  - You can add as many markers as required, at any time while the diagnostic logging is in progress.
  - Marker text is added to the log with a "**DEBUG\_MARKER**" tag.
5. Reproduce the system issue you want to trace in the diagnostic log.
6. Click **Stop logging**.
7. Click **Download log** to save the diagnostic log archive to your local file system. You are prompted to save the archive (the exact wording depends on your browser).

The downloaded diagnostic log archive contains the following files:

- `loggingsnapshot.txt` - containing log messages in response to the activities performed during the logging period
- `xconf_dump.txt` - containing information about the configuration of the system at the time the logging was started
- `xstat_dump.txt` - containing information about the status of the system at the time the logging was started
- (if relevant) `diagnostic_logging_tcpdump.pcap` - containing the packets captured during the logging period

These files can be sent to your Cisco support representative, if you have been requested to do so.

---

**CAUTION:** tcpdump files may contain sensitive information. Only send tcpdump files to trusted recipients. Consider encrypting the file before sending it, and also send the decrypt password out-of-band.

---

Note that:

- Only one diagnostic log can be produced at a time; creating a new diagnostic log will replace any previously produced log.
- The Expressway continually logs all system activity to a unified log file. The diagnostic logging facility works by extracting a portion of this unified log. On busy systems the unified log file may become full over time and will discard historic log data so that it can continue logging current activity. This means that all or part of your diagnostic log could be overwritten. The system will warn you if you attempt to download a partial diagnostic log file.
- The diagnostic log will continue logging all system activity until it is stopped, including over multiple login sessions and system restarts.
- When starting a diagnostic log, the relevant system modules have their log levels automatically set to "debug". You can ignore any "Verbose log levels configured" alarms; the log levels are reset to their original values when you stop logging.
- Diagnostic logging can only be controlled through the web interface; there is no CLI option.
- The tcpdump has a maximum file size limit of 50 MB.

## Clustered systems

Diagnostic logging can also be used if your Expressway is a part of a cluster, however some activities only apply to the "current" peer (the peer to which you are currently logged in to as an administrator):

- The start and stop logging operations are applied to every peer in the cluster, regardless of the current peer.
- The taking a tcpdump operation is applied to every peer in the cluster, regardless of the current peer.
- Each cluster peer maintains its own unified log, and logs activity that occurs only on that peer.
- Marker text is only applied to log of the current peer.
- You can only download the diagnostic log from the current peer.
- To add markers to other peers' logs, or to download diagnostic logs from other peers, you must log in as an administrator to that other peer.

To collect comprehensive information for debugging purposes, we recommend that you extract the diagnostic log for each peer in a cluster.

## Creating a system snapshot

The **System snapshot** page ([Maintenance > Diagnostics > System snapshot](#)) lets you create files that can be used for diagnostic purposes. The files should be sent to your support representative at their request to assist them in troubleshooting issues you may be experiencing.

You can create several types of snapshot file:

- **Status snapshot:** contains the system's current configuration and status settings.
- **Logs snapshot:** contains log file information (including the Event Log, Configuration Log and Network Log).
- **Full snapshot:** contains a complete download of all system information. The preparation of this snapshot file may take several minutes to complete and may lead to a drop in system performance while the snapshot is in progress.

### To create a system snapshot file:

1. Click one of the snapshot buttons to start the download of the snapshot file. Typically your support representative will tell you which type of snapshot file is required.
  - The snapshot creation process will start. This process runs in the background. If required, you can navigate away from the snapshot page and return to it later to download the generated snapshot file.
  - When the snapshot file has been created, a **Download snapshot** button will appear.
2. Click **Download snapshot**. A pop-up window appears and prompts you to save the file (the exact wording depends on your browser). Select a location from where you can easily send the file to your support representative.

## Configuring Network Log levels

The **Network Log configuration** page ([Maintenance > Diagnostics > Advanced > Network Log configuration](#)) is used to configure the log levels for the range of Network Log message modules.

---

**CAUTION:** changing the logging levels can affect the performance of your system. You should only change a log level on the advice of Cisco customer support.

---

To change a logging level:

1. Click on the **Name** of the module whose log level you want to modify.
2. Choose the required **Level** from the drop-down list.
  - A log level of *Fatal* is the least verbose; *Trace* is the most verbose.
  - Each message category has a log level of *Info* by default.
3. Click **Save**.

## Configuring Support Log levels

The **Support Log configuration** page ([Maintenance > Diagnostics > Advanced > Support Log configuration](#)) is used to configure the log levels for the range of Support Log message modules.

---

**CAUTION:** changing the logging levels can affect the performance of your system. You should only change a log level on the advice of Cisco customer support.

---

To change a logging level:

1. Click on the **Name** of the module whose log level you want to modify.
2. Choose the required **Level** from the drop-down list.
  - A log level of *Fatal* is the least verbose; *Trace* is the most verbose.
  - Each message category has a log level of *Info* by default.
3. Click **Save**.



# Incident reporting

The incident reporting feature of the Expressway automatically saves information about critical system issues such as application failures. You can:

- Configure the Expressway to [send the reports automatically](#) to Cisco customer support
- [View the reports](#) from the Expressway web interface
- [Download and send the reports manually](#) to Cisco (usually at the request of Cisco customer support)

The information contained in these reports can then be used by Cisco customer support to diagnose the cause of the failures. All information gathered during this process will be held in confidence and used by Cisco personnel for the sole purpose of issue diagnosis and problem resolution.

## Incident reporting caution: privacy-protected personal data

IN NO EVENT SHOULD PRIVACY-PROTECTED PERSONAL DATA BE INCLUDED IN ANY REPORTS TO CISCO.

Privacy-Protected Personal Data means any information about persons or entities that the Customer receives or derives in any manner from any source that contains any personal information about prospective, former, and existing customers, employees or any other person or entity. Privacy-Protected Personal Data includes, without limitation, names, addresses, telephone numbers, electronic addresses, social security numbers, credit card numbers, customer proprietary network information (as defined under 47 U.S.C. § 222 and its implementing regulations), IP addresses or other handset identifiers, account information, credit information, demographic information, and any other information that, either alone or in combination with other data, could provide information specific to a particular person.

PLEASE BE SURE THAT PRIVACY-PROTECTED PERSONAL DATA IS NOT SENT TO CISCO WHEN THE EXPRESSWAY IS CONFIGURED TO AUTOMATICALLY SEND REPORTS.

IF DISCLOSURE OF SUCH INFORMATION CANNOT BE PREVENTED, PLEASE DO NOT USE THE AUTOMATIC CONFIGURATION FEATURE. Instead, copy the data from the [Incident detail](#) page and paste it into a text file. You can then edit out any sensitive information before forwarding the file on to Cisco customer support.

Incident reports are always saved locally, and can be viewed via the [Incident view](#) page.

## Enabling automatic incident reporting

Read the [privacy-protected personal data caution](#) before you decide whether to enable automatic incident reporting.

To configure the Expressway to send incident reports automatically to Cisco customer support:

1. Go to **Maintenance > Diagnostics > Incident reporting > Configuration**.
2. Set the **Incident reports sending mode** to *On*.
3. Specify the **Incident reports URL** of the web service to which any error reports are to be sent. The default is `https://cc-reports.cisco.com/submitapplicationerror/`.
4. Optional. Specify a **Contact email address** that can be used by Cisco customer support to follow up any error reports.
5. Optional. Specify a **Proxy server** to use for the connection to the incident reporting server.

Use the format (http|https)://address:port/ such as `http://www.example.com:3128/`

6. Ensure that **Create core dumps** is *On*; this is the recommended setting as it provides useful diagnostic information.

**Note:** If the **Incident reports sending mode** is *Off*, incidents will not be sent to any URL but they will still be saved locally and can be [viewed and downloaded](#) from the **Incident detail** page.

## Sending incident reports manually

Read the [privacy-protected personal data caution](#) before you decide whether to send an incident report manually to Cisco.

To send an incident report manually to Cisco customer support:

1. Go to **Maintenance > Diagnostics > Incident reporting > View**.
2. Click on the incident you want to send. You will be taken to the **Incident detail** page.
3. Scroll down to the bottom of the page and click **Download incident report**. You will be given the option to save the file.
4. Save the file in a location from where it can be forwarded to Cisco customer support.

## Removing sensitive information from a report

The details in the downloaded incident report are Base64-encoded, so you will not be able to meaningfully view or edit the information within the file.

If you need to edit the report before sending it to Cisco (for example, if you need to remove any potentially sensitive information) you must copy and paste the information from the **Incident detail** page into a text file, and edit the information in that file before sending it to Cisco.

## Viewing incident reports

The **Incident view** page (**Maintenance > Diagnostics > Incident reporting > View**) shows a list of all incident reports that have occurred since the Expressway was last upgraded. A report is generated for each incident, and the information contained in these reports can then be used by Cisco customer support to diagnose the cause of the failures.

For each report the following information is shown:

| Field          | Description   |
|----------------|---|
| <b>Time</b>    | The date and time when the incident occurred.   |
| <b>Version</b> | The Expressway software version running when the incident occurred.   |
| <b>Build</b>   | The internal build number of the Expressway software version running when the incident occurred.  |
| <b>State</b>   | The current state of the incident:<br><i>Pending</i> : indicates that the incident has been saved locally but not sent.<br><i>Sent</i> : indicates that details of the incident have been sent to the URL specified in the <a href="#">Incident reporting configuration</a> page. |

To view the information contained in a particular incident report, click on the report's **Time**. You will be taken to the [Incident detail](#) page, from where you can view the report on screen, or download it as an XML file for forwarding manually to Cisco customer support.

## Incident report details

The **Incident detail** page (**Maintenance > Diagnostics > Incident reporting > View**, then click on a report's **Time**) shows the information contained in a particular incident report.

This is the information that is sent to the external web service if you have enabled **Incident reports sending mode** (via **Maintenance > Diagnostics > Incident reporting > Configuration**). It is also the same information that is downloaded as a Base64-encoded XML file if you click **Download incident report**.

The information contained in the report is:

| Field                    | Description  |
|--------------------------|--|
| <b>Time</b>              | The date and time when the incident occurred.  |
| <b>Version</b>           | The Expressway software version running when the incident occurred.                              |
| <b>Build</b>             | The internal build number of the Expressway software version running when the incident occurred. |
| <b>Name</b>              | The name of the software.  |
| <b>System</b>            | The system name (if configured), otherwise the IP address.                                       |
| <b>Serial number</b>     | The hardware serial number.  |
| <b>Process ID</b>        | The process ID the Expressway application had when the incident occurred.                        |
| <b>Release</b>           | A true/false flag indicating if this is a release build (rather than a development build).       |
| <b>User name</b>         | The name of the person that built this software. This is blank for release builds.               |
| <b>Stack</b>             | The trace of the thread of execution that caused the incident.                                   |
| <b>Debug information</b> | A full trace of the application call stack for all threads and the values of the registers.      |

**CAUTION:** for each call stack, the Debug information includes the contents of variables which may contain some sensitive information, for example alias values and IP addresses. If your deployment is such that this information could contain information specific to a particular person, read the [caution](#) regarding privacy-protected personal data before you decide whether to enable automatic incident reporting.

## Checking the effect of a pattern

The **Check pattern** tool (**Maintenance > Tools > Check pattern**) lets you test whether a pattern or transform you intend to configure on the Expressway will have the expected result.

Patterns can be used when configuring:

- [Transforms](#) to specify aliases to be transformed before any searches take place
- [Search rules](#) to filter searches based on the alias being searched for, and to transform an alias before the search is sent to a zone

To use this tool:

1. Enter an **Alias** against which you want to test the transform.
2. In the **Pattern** section, enter the combination of **Pattern type** and **Pattern behavior** for the **Pattern string** being tested.
  - If you select a **Pattern behavior** of *Replace*, you also need to enter a **Replace string**.
  - If you select a **Pattern behavior** of *Add prefix* or *Add suffix*, you also need to enter an **Additional text** string to append/prepend to the **Pattern string**.
  - The Expressway has a set of predefined [pattern matching variables](#) that can be used to match against certain configuration elements.
3. Click **Check pattern** to test whether the alias matches the pattern.  
The **Result** section shows whether the alias matched the pattern, and displays the resulting alias (including the effect of any transform if appropriate).

## Locating an alias

The **Locate** tool (**Maintenance > Tools > Locate**) lets you test whether the Expressway can find an endpoint identified by the given alias, within the specified number of "hops", without actually placing a call to that endpoint.

This tool is useful when diagnosing dial plan and network deployment issues.

### To use this tool:

1. Enter the **Alias** you want to locate.
2. Enter the **Hop count** for the search.
3. Select the **Protocol** used to initiate the search, either *H.323* or *SIP*. The search may be interworked during the search process, but the Expressway always uses the native protocol first to search those target zones and policy services associated with search rules at the same priority, before searching those zones again using the alternative protocol.
4. Select the **Source** from which to simulate the search request.
5. Select whether the request should be treated as **Authenticated** or not (search rules can be restricted so that they only apply to authenticated messages).
6. Optionally, you can enter a **Source alias**. Typically, this is only relevant if the routing process uses CPL that has rules dependent on the source alias. (If no value is specified a default alias of `xcom-locate` is used.)
7. Click **Locate** to start the search.  
The status bar shows **Searching...** followed by **Search completed**. The results include the list of zones that were searched, any transforms and Call Policy that were applied, and if found, the zone in which the alias was located.

The locate process performs the search as though the Expressway received a call request from the selected **Source zone**. For more information, see the [Call routing process \[p.145\]](#) section.

# Port usage

The pages under the **Maintenance > Tools > Port usage** menu show, in table format, all the IP ports that have been configured on the Expressway.

The information shown on these pages is specific to that particular Expressway and varies depending on the Expressway's configuration, the option keys that have been installed and the features that have been enabled.

The information can be sorted according to any of the columns on the page, so for example you can sort the list by IP port, or by IP address.

Each page contains an **Export to CSV** option. This lets you save the information in a CSV (comma separated values) format file suitable for opening in a spreadsheet application.

Note that IP ports cannot be configured separately for IPv4 and IPv6 addresses, nor for each of the two LAN interfaces. In other words, after an IP port has been configured for a particular service, for example SIP UDP, this will apply to all IP addresses of that service on the Expressway. Because the tables on these pages list all IP ports and all IP addresses, a single IP port may appear on the list up to 4 times, depending on your Expressway configuration.

The port information is split into the following pages:

- [Local inbound ports \[p.246\]](#)
- [Local outbound ports \[p.246\]](#)
- [Remote listening ports \[p.247\]](#)

On an Expressway-E you can also configure the specific listening ports used for firewall traversal via **Configuration > Traversal > Ports**.

See [Port reference \[p.303\]](#) for more information about the specific ports used by the Expressway.

## Local inbound ports

The **Local inbound ports** page (**Maintenance > Tools > Port usage > Local inbound ports**) shows the listening IP ports on the Expressway that are used to receive inbound communications from other systems.

For each port listed on this page, if there is a firewall between the Expressway and the source of the inbound communications, your firewall must allow:

- inbound traffic to the IP port on the Expressway from the source of the inbound communications, and
- return traffic from that same Expressway IP port back out to the source of the inbound communication.

## Local outbound ports

The **Local outbound ports** page (**Maintenance > Tools > Port usage > Local outbound ports**) shows the source IP ports on the Expressway that are used to send outbound communications to other systems.

For each port listed on this page, if there is a firewall between the Expressway and the destination of the outbound communications, your firewall must allow:

- outbound traffic out from the IP port on the Expressway to the destination of the outbound communications, and

- return traffic from that destination back to the same Expressway IP port.

## Remote listening ports

The **Remote listening ports** page ([Maintenance > Tools > Port usage > Remote listening ports](#)) shows the destination IP addresses and IP ports of remote systems with which the Expressway communicates.

Your firewall must be configured to allow traffic originating from the local Expressway to the remote devices identified by the IP addresses and IP ports listed on this page.

---

**Note:** there are other remote devices not listed here to which the Expressway will be sending media and signaling, but the ports on which these devices receive traffic from the Expressway is determined by the configuration of the destination device, so they cannot be listed here. If you have opened all the ports listed in the [Local outbound ports](#) page, the Expressway will be able to communicate with all remote devices. You only need to use the information on this page if you want to limit the IP ports opened on your firewall to these remote systems and ports.

---

# Network utilities

This section provides information about how to use the network utility tools:

- [Ping](#): allows you to check that a particular host system is contactable from the Expressway and that your network is correctly configured to reach it.
- [Traceroute](#): allows you to discover the details of the route taken by a network packet sent from the Expressway to a particular destination host system.
- [Tracepath](#): allows you to discover the path taken by a network packet sent from the Expressway to a particular destination host system.
- [DNS lookup](#): allows you to check which domain name server (DNS server) is responding to a request for a particular hostname.

## Ping

The **Ping** tool ([Maintenance > Tools > Network utilities > Ping](#)) can be used to assist in troubleshooting system issues.

It allows you to check that a particular host system is contactable and that your network is correctly configured to reach it. It reports details of the time taken for a message to be sent from the Expressway to the destination host system.

To use this tool:

1. In the **Host** field, enter the IP address or hostname of the host system you want to try to contact.
2. Click **Ping**.

A new section will appear showing the results of the contact attempt. If successful, it will display the following information:

---

|                    |  |
|--------------------|--|
| Host               | The hostname and IP address returned by the host system that was queried.                                |
| Response time (ms) | The time taken (in ms) for the request to be sent from the Expressway to the host system and back again. |

---

## Traceroute

The **Traceroute** tool ([Maintenance > Tools > Network utilities > Traceroute](#)) can be used to assist in troubleshooting system issues.

It allows you to discover the route taken by a network packet sent from the Expressway to a particular destination host system. It reports the details of each node along the path, and the time taken for each node to respond to the request.

To use this tool:

1. In the **Host** field, enter the IP address or hostname of the host system to which you want to trace the path.
2. Click **Traceroute**.



A new section will appear with a banner stating the results of the trace, and showing the following information for each node in the path:

|          |  |
|----------|--|
| TTL      | (Time to Live). This is the hop count of the request, showing the sequential number of the node.   |
| Response | This shows the IP address of the node, and the time taken (in ms) to respond to each packet received from the Expressway.<br>*** indicates that the node did not respond to the request. |

The route taken between the Expressway and a particular host may vary for each traceroute request.

## Tracepath

The **Tracepath** tool (**Maintenance > Tools > Network utilities > Tracepath**) can be used to assist in troubleshooting system issues.

It allows you to discover the route taken by a network packet sent from the Expressway to a particular destination host system.

To use this tool:

1. In the **Host** field, enter the IP address or hostname of the host system to which you want to trace the route.
2. Click **Tracepath**.

A new section will appear with a banner stating the results of the trace, and showing the details of each node along the path, the time taken for each node to respond to the request, and the maximum transmission units (MTU).

The route taken between the Expressway and a particular host may vary for each tracepath request.

## DNS lookup

The **DNS lookup** tool (**Maintenance > Tools > Network utilities > DNS lookup**) can be used to assist in troubleshooting system issues.

It allows you to query DNS for a supplied hostname and display the results of the query if the lookup was successful.

To use this tool:

1. In the **Host** field, enter either:
  - the name of the host you want to query, or
  - an IPv4 or IPv6 address if you want to perform a reverse DNS lookup
2. In the **Query type** field, select the type of record you want to search for:  
(for reverse lookups the **Query type** is ignored - the search automatically looks for PTR records)

| Option           | Searches for...  |
|------------------|--|
| All              | any type of record   |
| A (IPv4 address) | a record that maps the hostname to the host's IPv4 address |

| Option                         | Searches for...  |
|--------------------------------|--|
| AAAA (IPv6 address)            | a record that maps the hostname to the host's IPv6 address   |
| SRV (services)                 | SRV records (which includes those specific to H.323, SIP, Unified Communications and TURN services, see below) |
| NAPTR (Name authority pointer) | a record that rewrites a domain name (into a URI or other domain name for example)                             |

- By default the system will submit the query to all of the system's default DNS servers (**System > DNS**). To query specific servers only, set **Check against the following DNS servers** to *Custom* and then select the DNS servers you want to use.
- Click **Lookup**.

A separate DNS query is performed for each selected **Query type**. The domain that is included within the query sent to DNS depends upon whether the supplied **Host** is fully qualified or not (a fully qualified host name contains at least one "dot"):

- If the supplied **Host** is fully qualified:
  - DNS is queried first for **Host**
  - If the lookup for **Host** fails, then an additional query for **Host.<system\_domain>** is performed (where **<system\_domain>** is the **Domain name** as configured on the **DNS** page)
- If the supplied **Host** is not fully qualified:
  - DNS is queried first for **Host.<system\_domain>**
  - If the lookup for **Host.<system\_domain>** fails, then an additional query for **Host** is performed

For SRV record type lookups, multiple DNS queries are performed. An SRV query is made for each of the following `_service._protocol` combinations:

- `_h323ls._udp.<domain>`
- `_h323rs._udp.<domain>`
- `_h323cs._tcp.<domain>`
- `_sips._tcp.<domain>`
- `_sip._tcp.<domain>`
- `_sip._udp.<domain>`
- `_collab-edge._tls`
- `_cuplogin._tcp`
- `_cisco-uds._tcp`
- `_turn._udp.<domain>`
- `_turn._tcp.<domain>`

In each case, as for all other query types, either one or two queries may be performed for a `<domain>` of either **Host** and/or **Host.<system\_domain>**.

## Results

A new section will appear showing the results of all of the queries. If successful, it will display the following information:

---

|            |   |
|------------|---|
| Query type | The type of query that was sent by the Expressway.  |
| Name       | The hostname contained in the response to the query.  |
| TTL        | The length of time (in seconds) that the results of this query will be cached by the Expressway.                        |
| Class      | <b>IN</b> (internet) indicates that the response was a DNS record involving an internet hostname, server or IP address. |
| Type       | The record type contained in the response to the query.   |
| Response   | The content of the record received in response to the query for this <b>Name</b> and <b>Type</b> .                      |

---

# Restarting, rebooting and shutting down

The **Restart options** page (**Maintenance > Restart options**) allows you to restart, reboot or shut down the Expressway without having physical access to the hardware.

---

**CAUTION:** do not restart, reboot or shut down the Expressway while the red ALM LED on the front of the unit is on. This indicates a hardware fault. Contact your Cisco customer support representative.

---

## Restarting

The restart function shuts down and restarts the Expressway application software, but not the operating system or hardware. A restart takes approximately 3 minutes.

A restart is typically required in order for some configuration changes to take effect, or when the system is being added to, or removed from, a cluster. In these cases a system alarm is raised and will remain in place until the system is restarted.

If the Expressway is part of a cluster and other peers in the cluster also require a restart, we recommend that you wait until each peer has restarted before restarting the next peer.

## Rebooting

The reboot function shuts down and restarts the Expressway application software, operating system and hardware. A reboot takes approximately 5 minutes.

Reboots are normally only required after software upgrades and are performed as part of the upgrade process. A reboot may also be required when you are trying to resolve unexpected system errors.

## Shutting down

A shutdown is typically required if you want to unplug your unit, prior to maintenance or relocation for example. The system must be shut down before it is unplugged. Avoid uncontrolled shutdowns, in particular the removal of power to the system during normal operation.

## Effect on active calls

Any of these restart options will cause all active calls to be terminated. (If the Expressway is part of a cluster, only those calls for which the Expressway is taking the signaling will be terminated.)

For this reason, the **System status** section displays the number of current calls so you can check these before you restart the system. If you do not restart the system immediately, you should refresh this page before restarting to check the current status of calls.

If **Mobile and remote access** is enabled, the number of currently provisioned sessions is displayed (Expressway-C only).

## Restarting, rebooting or shutting down using the web interface

To restart the Expressway using the web interface:

1. Go to **Maintenance > Restart options**.
2. Check the number of calls currently in place.
3. Click **Restart**, **Reboot** or **Shutdown** as appropriate and confirm the action.  
Sometimes only one of these options, such as **Restart** for example, may be available. This typically occurs when you access the **Restart options** page after following a link in an alarm or a banner message.

- Restart/reboot: the **Restarting/Rebooting** page appears, with an orange bar indicating progress. After the system has successfully restarted or rebooted, you are automatically taken to the **Login** page.
- Shutdown: the **Shutting down** page appears. This page remains in place after the system has successfully shut down but any attempts to refresh the page or access the Expressway will be unsuccessful.

## Developer resources

The Expressway includes some features that are intended for the use of Cisco support and development teams only. Do not access these pages unless it is under the advice and supervision of your Cisco support representative.

---

**CAUTION:** incorrect usage of the features on these pages could cause the system operation to become unstable, cause performance problems and cause persistent corruption of system configuration.

---

These features are:

- [Debugging and system administration tools \[p.254\]](#)
- [Experimental menu \[p.254\]](#)

## Debugging and system administration tools

---

**CAUTION:** these features are not intended for customer use unless on the advice of a Cisco support representative. Incorrect usage of these features could cause the system operation to become unstable, cause performance problems and cause persistent corruption of system configuration.

---

The Expressway includes a number of debugging and system admin tools that allow administrators to inspect what is happening at a detailed level on a live system, including accessing and modifying configuration data and accessing network traffic.

To access these tools:

1. Open an SSH session.
2. Log in as admin or root as required.
3. Follow the instructions provided by your Cisco support representative.

## Experimental menu

The Expressway web interface contains a number of pages that are not intended for use by customers. These pages exist for the use of Cisco support and development teams only. Do not access these pages unless it is under the advice and supervision of your Cisco support representative.

---

**CAUTION:** incorrect usage of the features on these pages could cause the system operation to become unstable, cause performance problems and cause persistent corruption of system configuration.

---

To access these pages:

1. Go to `https://<Expressway host name or IP address>/setaccess`.  
The **Set access** page appears.
2. In the **Access password** field, enter `qwertsys`.
3. Click **Enable access**.

A new top-level **Experimental** menu will appear to the right of the existing menu items.

# Overview and status information

---

You can view information about the current status, current calls and call history, and configuration of the Expressway by using the **Status** menu options.

|   |     |
|---|-----|
| Status overview .....                     | 256 |
| System information .....                  | 257 |
| Ethernet status .....                     | 258 |
| IP status .....                           | 259 |
| Resource usage .....                      | 260 |
| Call status .....                         | 262 |
| B2BUA calls .....                         | 264 |
| Search history .....                      | 265 |
| Search details .....                      | 266 |
| Local Zone status .....                   | 267 |
| Zone status .....                         | 268 |
| Bandwidth .....                           | 269 |
| Policy server status and resiliency ..... | 270 |
| TURN relay usage .....                    | 271 |
| Unified Communications status .....       | 272 |
| Lync B2BUA .....                          | 273 |
| Managing alarms .....                     | 274 |
| Logs .....                                | 275 |
| Hardware status .....                     | 279 |

# Status overview

The **Overview** page (**Status > Overview**) provides an overview of the current status of the Expressway (or Expressway cluster, if applicable). This page is displayed by default after logging in to the Expressway as an administrator.

The following information is displayed:

| Field  | Description  |
|--|--|
| <b>System information:</b> many of the items in this section are configurable; click on the item name to go to its configuration page. |  |
| <b>System name</b>   | The name that has been assigned to the Expressway.   |
| <b>Up time</b>   | The amount of time that has elapsed since the system last restarted.   |
| <b>Software version</b>  | The version of software that is currently installed on the Expressway.   |
| <b>IPv4 address</b>  | The Expressway's IPv4 addresses.   |
| <b>IPv6 address</b>  | The Expressway's IPv6 addresses.   |
| <b>Options</b>   | The maximum number of calls and the availability of additional Expressway features such as TURN Relays and Advanced Networking, are controlled through the use of <a href="#">option keys</a> . This section shows all the options that are currently installed on the Expressway. |

## Resource usage

This section provides statistics about the current and cumulative license usage for calls.

It shows current and peak (highest concurrent) usage broken down by:

- Unified CM remote session calls
- Rich media sessions
- TURN relays (Expressway-E only)

It also displays resource and license usage information:

- Monitored resource usage, expressed as a percentage of the system capacity.
- Current and peak license usage, expressed as a percentage of the available licenses for each license type. Each rich media session license allows either 1 video call or 2 audio-only SIP traversal calls. Hence, a 100 rich media session license would allow, for example, 90 video and 20 SIP audio-only simultaneous calls. Any other audio-only call (non-traversal, H.323 or interworked) will consume a rich media session license.

You can view details of current calls by clicking on the relevant item in the section.

All statistics are based on data since the system was last restarted. The information on this page refreshes automatically every 5 seconds.

You can go to the **Resource usage** page to see more details, including total usage statistics.

## Clustered Expressway systems

If the Expressway is part of a cluster, then details for each peer are shown as well as totals for the entire cluster.

See [About clusters \[p. 135\]](#) for more information.



# System information

The **System information** page ([Status > System > Information](#)) provides details of the software, hardware, and time settings of the Expressway.

Many of the items in the **System information** and **Time information** sections are configurable; click on the item name to be taken to its configuration page.

The following information is displayed:

| Field                              | Description  |
|------------------------------------|--|
| <b>System information</b> section: |  |
| <b>System name</b>                 | The name that has been assigned to the Expressway.   |
| <b>Product</b>                     | This identifies the Expressway.  |
| <b>Software version</b>            | The version of software that is currently installed on the Expressway.   |
| <b>Software build</b>              | The build number of this software version.   |
| <b>Software release date</b>       | The date on which this version of the software was released.   |
| <b>Software name</b>               | The internal reference number for this software release.   |
| <b>Software options</b>            | The maximum number of calls, and the availability of additional Expressway features such as Advanced Networking, are controlled through the use of <a href="#">option keys</a> . This section shows all the optional features currently installed on the Expressway. |
| <b>Hardware version</b>            | The version number of the hardware on which the Expressway software is installed.  |
| <b>Serial number</b>               | The serial number of the hardware or virtual machine on which the Expressway software is installed.  |
| <b>Time information</b> section:   |  |
| <b>Up time</b>                     | The amount of time that has elapsed since the system last restarted.   |
| <b>System time (UTC)</b>           | The time as determined by the NTP server.<br>If no NTP server is configured, this shows <i>Time Not Set</i> .  |
| <b>Time zone</b>                   | The time zone that has been configured on the <a href="#">Time</a> page.   |
| <b>Local time</b>                  | If an NTP server is configured, the system time is shown in local time (UTC adjusted according to the local time zone).<br>If no NTP server is configured, the time according to the Expressway's operating system is shown.   |
| <b>Active sessions</b> section:    |  |
| <b>Administrator sessions</b>      | The number of current active administrator sessions. Click on the link to see the list of active sessions.   |

## Ethernet status

The **Ethernet** page (**Status > System > Ethernet**) shows the MAC address and Ethernet speed of the Expressway.

The page displays the following information for the LAN 1 port and, if the Advanced Networking option key has been installed, the LAN 2 port:

| Field              | Description   |
|--------------------|---|
| <b>MAC address</b> | The MAC address of the Expressway's Ethernet device for that LAN port.                      |
| <b>Speed</b>       | The speed of the connection between the LAN port on the Expressway and the Ethernet switch. |

The Ethernet speed can be configured via the [Ethernet](#) page.

# IP status

The **IP status** page (**Status > System > IP**) shows the current IP settings of the Expressway.

The following information is displayed:

| Field                      | Description  |
|----------------------------|--|
| <b>IP section:</b>         |  |
| <b>Protocol</b>            | Indicates the IP protocol supported by the Expressway: <ul style="list-style-type: none"> <li>■ <i>IPv4</i>: it only takes calls between two endpoints communicating via IPv4. It communicates with other systems via IPv4 only.</li> <li>■ <i>IPv6</i>: it only takes calls between two endpoints communicating via IPv6. It communicates with other systems via IPv6 only.</li> <li>■ <i>Both</i>: it takes calls using either protocol. If a call is between an IPv4-only and an IPv6-only endpoint, the Expressway acts as an IPv4 to IPv6 gateway. It communicates with other systems via either protocol.</li> </ul> |
| <b>IPv4 gateway</b>        | The IPv4 gateway used by Expressway.   |
| <b>IPv6 gateway</b>        | The IPv6 gateway used by Expressway.   |
| <b>Advanced Networking</b> | Indicates whether the second LAN port has been enabled. This is done by installing the <b>Advanced Networking</b> option key.  |
| <b>LAN 1</b>               | Shows the IPv4 address and subnet mask, and IPv6 address of the LAN 1 port.  |
| <b>LAN 2</b>               | If the <b>Advanced Networking</b> option key has been installed, this shows the IPv4 address and subnet mask, and IPv6 address of the LAN 2 port.  |
| <b>DNS section:</b>        |  |
| <b>Server 1..5 address</b> | The IP addresses of each of the DNS servers that are queried when resolving domain names. Up to 5 DNS servers may be configured.   |
| <b>Domain</b>              | Specifies the name to be appended to the host name before a query to the DNS server is executed.   |

The IP settings can be configured via the [IP](#) page.

## Resource usage

The **Resource usage** page (**Status > System > Resource usage**) provides statistics about the current and cumulative license usage for calls.

It shows current and peak (highest concurrent) usage broken down by:

- Unified CM remote session calls
- Rich media sessions
- TURN relays (Expressway-E only)

It also displays resource and license usage information:

- Monitored resource usage, expressed as a percentage of the system capacity.
- Current and peak license usage, expressed as a percentage of the available licenses for each license type. Each rich media session license allows either 1 video call or 2 audio-only SIP traversal calls. Hence, a 100 rich media session license would allow, for example, 90 video and 20 SIP audio-only simultaneous calls. Any other audio-only call (non-traversal, H.323 or interworked) will consume a rich media session license.

You can view details of current calls by clicking on the relevant item in the section.

All statistics are based on data since the system was last restarted. The information on this page refreshes automatically every 5 seconds.

### Clustered Expressway systems

If the Expressway is part of a cluster, details for each peer are shown as well as totals for the entire cluster.

The following types of licenses are pooled for use by any peer in a cluster, irrespective of which peer the licenses are installed on:

- Rich media session licenses
- TURN relay licenses

The maximum number of licenses that each Expressway system can use depends on the [type of appliance or VM](#):

Table 8: Maximum licenses that a peer can use

|                     | Small / Medium / CE500 systems | Large / CE1000 systems |
|---------------------|--------------------------------|------------------------|
| Rich media sessions | 150                            | 500                    |
| TURN relays *       | 1800                           | 6000                   |

\* On a Large system, the total TURN capacity of 6000 relays is spread evenly across 6 ports; each port is limited to handling 1000 relays. On a Small/Medium system, there is a single TURN port that handles up to 1800 relays.

You can cluster up to 6 Expressway systems to increase capacity by a maximum factor of 4 (see [Performance capabilities \[p.281\]](#) for more information).

If a cluster peer becomes unavailable, the shareable licenses installed on that peer remain available to the rest of the cluster peers for two weeks from the time the cluster lost contact with the peer. This will maintain the overall license capacity of the cluster — however, note that each peer is limited by its physical capacity. After this two week period, the licenses associated with the unavailable peer are removed from the cluster.

To maintain the same capacity for your cluster, you should ensure that either the problem with the peer is resolved or new option keys are installed on another peer in the cluster.

You can see a summary of all of the call and TURN relay licenses installed on each cluster peer by going to the **Option keys** page and scrolling down to the **Current licenses** section.

See [About clusters \[p.135\]](#) for more information.

# Call status

Call status information can be displayed for both current and completed calls:

- **Current calls:** the [Call status](#) page ([Status > Calls > Calls](#)) lists all the calls currently passing through the Expressway.
- **Completed calls:** the [Call history](#) page ([Status > Calls > History](#)) lists all the calls that are no longer active. The list is limited to the most recent 500 calls, and only includes calls that have taken place since the Expressway was last restarted.

If the Expressway is part of a cluster, all calls that apply to any peer in the cluster are shown, although the list is limited to the most recent 500 calls per peer.

## Call summary information

The following summary information is displayed initially:

| Field       | Description   |
|-------------|---|
| Start time  | The date and time when the call was placed.   |
| End time    | The date and time when the call ended (completed calls only).   |
| Duration    | The length of time of the call.   |
| Source      | The alias of the device that placed the call.   |
| Destination | The alias dialed from the device. This may be different from the alias to which the call was placed, which may have been transformed (due to pre-search or zone transforms).  |
| Type        | Indicates either a traversal or non-traversal call.   |
| Protocol    | Shows whether the call used H.323, SIP, or both protocols. For calls passing through the B2BUA, this may show "Multiple components"; you can view the call component summary section to see the protocol of each individual call component. |
| Status      | The reason the call ended (completed calls only).   |
| Peer        | Identifies the cluster peer through which the call is being made.   |
| Actions     | Click <b>View</b> to see further information about the call, including a list of all of the call components that comprise that call.  |

## Call components summary information

After selecting a call from the primary list (as described above) you are shown further details of that call, including a list of all of the call components that comprise that call.

Each call component may be one of the following types:

- *Expressway:* a standard Expressway call
- *B2BUA:* a call component that is routed through the B2BUA to apply a media encryption policy or ICE messaging support
- *Microsoft Lync B2BUA:* a call component that is routed through the Microsoft Lync B2BUA

You can view full details of each call component by clicking on the **Local call serial number** associated with each component. This will open the [Call details](#) page which lists full information about that component, including all call legs and sessions. It also provides further links to the [Call media](#) page which lists the individual media channels (audio, video, data and so on) for the most relevant session for a traversal call.

If the Expressway is part of a cluster and the call passes through two cluster peers, you can click **View associated call on other cluster peer** to see the details of the other leg of the call.

Mobile and remote access calls have different component characteristics depending on whether the call is being viewed on the Expressway-C or Expressway-E:

- On an Expressway-C, a Unified CM remote session will have 3 components (as it uses the B2BUA to enforce media encryption). One of the Expressway components will route the call through one of the automatically generated neighbor zones (with a name prefixed by either **CEtcp** or **CEtls**) between Expressway and Unified CM.
- On an Expressway-E, there will be one component and that will route the call through the **CollaborationEdgeZone**.

Note that if both endpoints are outside of the enterprise (i.e. off premises), you will see this treated as 2 separate calls.

### Rich media sessions

If your system has a rich media session key installed and thus has been extended to support business-to-business calls, and interworked or gatewayed calls to third-party solutions and so on, those calls are also listed on the call status and call history pages.

## Disconnecting calls

Click **Disconnect** to disconnect the selected calls. Note that if your Expressway is part of a cluster you have to be logged into the peer through which the call is associated to be able to disconnect the call.

Call disconnection works differently for H.323 and SIP calls due to differences in the way the protocols work:

- H.323 calls, and interworked H.323 to SIP calls: the **Disconnect** command will actually disconnect the call.
- SIP to SIP calls: the **Disconnect** command will cause the Expressway to release all resources used for the call and the call will appear on the system as disconnected. However, SIP calls are peer-to-peer and as a SIP proxy the Expressway has no authority over the endpoints. Although releasing the resources may have the side-effect of disconnecting the SIP call, it is also possible that the call signaling, media or both may stay up (depending on the type of call being made). The call will not actually disconnect until the SIP endpoints involved have also cleared their resources.
- SIP calls via the B2BUA: as the B2BUA can control the state of a call, if you disconnect the leg of the call that is passing through the B2BUA (where the **Type** is *B2BUA*), the call will fully disconnect. Note that the call may take a few seconds to disappear from the **Call status** page — you may have to refresh the page on your browser.

## B2BUA calls

The **B2BUA calls** page (**Status > Calls > Calls** or **Status > Calls > History**, then click **View** for a particular B2BUA call) provides overview information about a call routed through the B2BUA.

Calls are routed through the B2BUA if:

- a [media encryption policy](#) (any encryption setting other than *Auto*) has been applied to the call
- [ICE messaging](#) support has been triggered
- the [Microsoft Lync B2BUA service](#) is enabled and the call has been routed through the **To Microsoft Lync server via B2BUA** neighbor zone

Note that for Microsoft Lync B2BUA calls, you can click the **Corresponding Expressway call** link to see details of the leg passing through the Expressway.

## Viewing B2BUA call media details

The **B2BUA call media** page (accessed from the [B2BUA calls](#) page by clicking **View media statistics for this call**) shows information about the media channels (audio and video) that made up the call passing through the B2BUA. For calls using the Microsoft Lync B2BUA, this comprises legs between the Expressway, the Lync server and, if applicable, the transcoder.



# Search history

The **Search history** page (**Status > Search history**) lists the most recent 255 searches that have taken place since the Expressway was last restarted.

## About searches

Before a call can be placed, the endpoint being called must be located. The Expressway sends and receives a series of messages during its attempt to locate the endpoint being called; these messages are each known as searches. An individual call can have one or more searches associated with it, and these searches can be of different types.

The type of search message that is sent depends on whether the call is for SIP or H.323, and whether the call request was received locally or from an external zone, as follows:

- H.323 calls that are placed locally: two messages are sent - the first is an **ARQ** which locates the device being called, and the second is the call **Setup** which sends a request to the device asking it to accept the call. Each message shows up as a separate search in the **Search history** page, but only the **Setup** message is associated with a particular call.
- H.323 searches originating from external zones: an **LRQ** will appear in the **Search history** page.
- SIP: a single message is sent in order to place a call: this is either a SIP **INVITE** or a SIP **OPTIONS**.

Note that an individual call can have one or more searches associated with it, and these searches can be of different types. Each search has an individual *Search ID*; each call has an individual *Call Tag* (see [Identifying calls \[p.178\]](#)).

The Expressway supports up to 500 concurrent searches.

## Search history list

The search history summary list shows the following information:

| Field              | Description   |
|--------------------|---|
| <b>Start time</b>  | The date and time at which the search was initiated.  |
| <b>Search type</b> | The type of message being sent.   |
| <b>Source</b>      | The alias of the endpoint that initiated the call.  |
| <b>Destination</b> | The alias that was dialed from the endpoint. This may be different from the alias to which the call was actually placed, as the original alias may have been transformed either locally or before the neighbor was queried. |
| <b>Status</b>      | Indicates whether or not the search was successful.   |
| <b>Actions</b>     | Allows you to click <b>View</b> to go to the <a href="#">Search details</a> page, which lists full details of this search.  |

## Filtering the list

To limit the list of searches, enter one or more characters in the **Filter** field and click **Filter**. Only those searches that contain (in any of the displayed fields) the characters you entered are shown.

To return to the full list of searches, click **Reset**.

## Search details

The **Search details** page lists full information about either an individual search, or all searches associated with a single call (depending on how you reached the page). The information shown includes:

- the subzones and zones that were searched
- the call path and hops
- any transforms that were applied to the alias being searched for
- use of policies such as Admin Policy
- any policy services that were used

Other information associated with the search and (if it was successful) the resulting call can be viewed via the links in the **Related tasks** section at the bottom of the page:

- **View all events associated with this call tag** takes you to the [Event Log](#) page, filtered to show only those events associated with the Call Tag relating to this search.
- **View call information associated with this call tag** takes you to the **Call details** page, where you can view overview information about the call.
- **View all searches associated with this call tag** is shown if you are viewing details of an individual search and there are other searches associated with the same call. It takes you to a new **Search details** page which lists full information about all the searches associated with the call's Call Tag.

## Local Zone status

The **Local Zone status** page (**Status > Local Zone**) lists the subzones (the Default Subzone and the Traversal Subzone) that make up the Expressway's Local Zone .

The following information is displayed:

| Field                 | Description   |
|-----------------------|---|
| <b>Subzone name</b>   | The names of each subzone currently configured on this Expressway.<br>Clicking on a <b>Subzone name</b> takes you to the configuration page for that subzone. |
| <b>Calls</b>          | The number of calls currently passing through the subzone.  |
| <b>Bandwidth used</b> | The total amount of bandwidth used by all calls passing through the subzone.  |

## Zone status

The **Zone status** page (**Status > Zones**) lists all of the external zones on the Expressway. It shows the number of calls and amount of bandwidth being used by each zone.

The list of zones always includes the Default Zone, plus any other zones that have been created.

The following information is displayed:

| Field                     | Description  |
|---------------------------|--|
| <b>Name</b>               | The names of each zone currently configured on this Expressway.<br>Clicking on a zone <b>Name</b> takes you to the configuration page for that zone.   |
| <b>Type</b>               | The type of zone.  |
| <b>Calls</b>              | The number of calls currently passing out to or received in from each zone.  |
| <b>Bandwidth used</b>     | The total amount of bandwidth used by all calls passing out to or received in from each zone.  |
| <b>H.323 / SIP status</b> | Indicates the zone's H.323 or SIP connection status: <ul style="list-style-type: none"> <li>■ <i>Off</i>: the protocol is disabled at either the zone or system level</li> <li>■ <i>Active</i>: the protocol is enabled for that zone and it has at least one active connection; if multiple connections are configured and some of those connections have failed, the display indicates how many of the connections are <i>Active</i></li> <li>■ <i>On</i>: applies to DNS and ENUM zones only and indicates that the protocol is enabled for that zone</li> <li>■ <i>Failed</i>: the protocol is enabled for that zone but its connection has failed</li> <li>■ <i>Checking</i>: the protocol is enabled for that zone and the system is currently trying to establish a connection</li> </ul> |
| <b>Search rule status</b> | This area is used to indicate if that zone is not a target of any search rules.  |

# Bandwidth

## Link status

The **Link status** page (**Status > Bandwidth > Links**) lists all of the links currently configured on the Expressway, along with the number of calls and the bandwidth being used by each link.

The following information is displayed:

| Field                 | Description   |
|-----------------------|---|
| <b>Name</b>           | The name of each link. Clicking on a link <b>Name</b> takes you to the configuration page for that link.  |
| <b>Calls</b>          | The total number of calls currently traversing the link. Note that a single call may traverse more than one link, depending on how your system is configured. |
| <b>Bandwidth used</b> | The total bandwidth of all the calls currently traversing the link.   |

## Pipe status

The **Pipe status** page (**Status > Bandwidth > Pipes**) lists all of the pipes currently configured on the Expressway, along with the number of calls and the bandwidth being used by each pipe.

The following information is displayed:

| Field                 | Description   |
|-----------------------|---|
| <b>Name</b>           | The name of each pipe. Clicking on a pipe <b>Name</b> takes you to the configuration page for that pipe.  |
| <b>Calls</b>          | The total number of calls currently traversing the pipe. Note that a single call may traverse more than one pipe, depending on how your system is configured. |
| <b>Bandwidth used</b> | The total bandwidth of all the calls currently traversing the pipe.   |

## Policy server status and resiliency

You must specify a **Status path** when configuring the Expressway's connection to a policy server. It identifies the path from where the status of the remote service can be obtained. By default this is *status*.

Up to 3 different policy server addresses may be specified. The Expressway polls each address on the specified path every 60 seconds to test the reachability of that address. The Expressway accepts standard HTTP(S) response status codes. (Note that the developers of the policy service must ensure that this provides the appropriate status of the service.)

If a server does not respond to status requests, Expressway will deem that server's status to be in a failed state and it will not be queried for policy service requests until it returns to an active state. Its availability will not be checked again until after the 60 second polling interval has elapsed.

When the Expressway needs to make a policy service request, it attempts to contact the service via one of the configured server addresses. It will try each address in turn, starting with **Server 1 address**, and then if necessary - and if configured - via the **Server 2 address** and then the **Server 3 address**. The Expressway only tries to use a server address if it is in an active state, based on its most recent status query.

The Expressway has a non-configurable 30 seconds timeout value for each attempt it makes to contact a policy server. However, if the server is not reachable, the connection failure will occur almost instantaneously. (Note that the TCP connection timeout is usually 75 seconds. Therefore, in practice, a TCP connection timeout is unlikely to occur as either the connection will be instantly unreachable or the 30 second request timeout will occur first.)

The Expressway uses the configured **Default CPL** if it fails to contact the policy service via any of the configured addresses.

Note that this method provides resiliency but not load balancing i.e. all requests will be sent to **Server 1 address**, providing that server address is functioning correctly.

## Viewing policy server status via the Expressway

A summarized view of the status of the connection to each policy service can be viewed by going to the **Policy service status** page (**Status > Policy services**).

The set of policy services includes all of the services defined on the **Policy services** page (**Configuration > Dial plan > Policy services**), plus a **Call Policy** service if appropriate.

The following information is displayed:

| Field            | Description   |
|------------------|---|
| <b>Name</b>      | The name of the policy service.<br>Clicking on a <b>Name</b> takes you to the configuration page for that service where you can change any of the settings or see the details of any connection problems. |
| <b>URL</b>       | The address of the service. Note that each service can be configured with multiple server addresses for resiliency. This field displays the server address currently selected for use by the Expressway.  |
| <b>Status</b>    | The current status of the service based on the last attempt to poll that server.  |
| <b>Last used</b> | Indicates when the service was last requested by the Expressway.  |

## TURN relay usage

The **TURN relay usage** page ([Status > TURN relay usage](#)) provides a summary list of all the clients that are connected to the TURN server.

Note that TURN services are available on Expressway-E systems only; they are configured via [Configuration > Traversal > TURN](#).

The following information is displayed:

| Field                      | Description  |
|----------------------------|--|
| <b>Client</b>              | The IP address of the client that requested the relay.           |
| <b>Media destinations</b>  | The address of destination system the media is being relayed to. |
| <b>Connection protocol</b> | Indicates if the client is connected over TCP or UDP.            |
| <b>Relays</b>              | Number of current relays being used by the client.               |

### Viewing TURN relay details for a client connection

You can click on a specific client to see all of the relays and ports that it is using.

For each relay, its associated relay peer address/port is displayed. It also displays each relay's associated peer address/port (the TURN server relay port from which the media is being sent to the destination system). To see specific statistics about a relay, click **View** to go to the [TURN relay summary](#) page.

## TURN relay summary

The **TURN relay summary** page provides overview information about a particular relay, including a summary count of the permissions, channels and requests associated with that relay.

To access this page, go to [Status > TURN relay usage](#), then click **View** for a TURN client, and then **View** again for the required relay.

Further detailed information about the relay can be viewed by using the links in the **Related tasks** section at the bottom of the page. These let you:

- **View permissions for this relay:** information about the permissions that have been defined on this relay.
- **View channels for this relay:** information about the channel bindings that have been defined on this relay.
- **View counters for this relay:** information about the number of TURN requests received, and the number of TURN success or error responses sent. It also shows counts of the number of packets forwarded to and from the client that allocated this relay.

# Unified Communications status

The **Unified Communications status** page (**Status > Unified Communications**) shows the current status of the [Unified Communications](#) services including:

- the number of configured Unified CM and IM&P servers (Expressway-C only)
- the current number of active provisioning sessions (Expressway-C only)
- the number of current calls
- all the domains and zones that have been configured for Unified Communications services
- statistics about SSO access requests and responses

If any configuration or connectivity problems are detected, appropriate messages are displayed with either links or guidelines as to how to resolve the issue.

You can also view some advanced status information, including:

- a list of all current and recent (shown in red) provisioning sessions (Expressway-C only)
- a list of the automatically-generated SSH tunnels servicing requests through the traversal zone

## Checking SSO statistics

The **SSO Statistics** page (**Status > Unified Communications > View detailed SSO statistics**) shows a summary of the requests and responses issued, as well as more detailed statistics about successful and unsuccessful attempts to sign on.

If there are no instances of a particular type of request or response, there is no counter shown for that type.



# Lync B2BUA

## Lync B2BUA status

The **Lync B2BUA status** page (**Status > Applications > Lync B2BUA**) displays the status of the [Microsoft Lync B2BUA service](#).


The Microsoft Lync back-to-back user agent (B2BUA) on the Expressway is used to route SIP calls between the Expressway and a Microsoft Lync Server.

The information shown includes:

- the number of current calls passing through the Lync B2BUA
- resource usage as a percentage of the number of allowed Lync B2BUA calls

## Managing alarms

Alarms occur when an event or configuration change has taken place on the Expressway that requires some manual administrator intervention, such as a restart. Alarms may also be raised for hardware and environmental issues such as faulty disks and fans or high temperatures.

The **Alarms** page (**Status > Alarms**) provides a list of all the alarms currently in place on your system (and, where applicable, their proposed resolution). When there are unacknowledged alarms in place on the Expressway, an alarm icon  appears at the top right of all pages. You can also access the **Alarms** page by clicking on the alarm icon.

Each alarm is identified by a 5-digit **Alarm ID**, shown in the rightmost column in the alarms list. The alarms are grouped into categories as follows:

| Alarm ID prefix | Category  |
|-----------------|---|
| 10nnn           | Hardware issues   |
| 15nnn           | Software issues   |
| 20nnn           | Cluster-related issues  |
| 25nnn           | Network and network services settings   |
| 30nnn           | Licensing / resources / option keys   |
| 35nnn           | External applications and services (such as policy services or LDAP/AD configuration) |
| 40nnn           | Security issues (such as certificates, passwords or insecure configuration)           |
| 45nnn           | General Expressway configuration issues   |
| 55nnn           | B2BUA issues  |
| 6nnnn           | Fusion issues   |

All alarms raised on the Expressway are also raised as Cisco TMS tickets. All the attributes of an alarm (its ID, severity and so on) are included in the information sent to Cisco TMS.

Alarms are dealt with by clicking each **Action** hyperlink and making the necessary configuration changes to resolve the problem.

Acknowledging an alarm (by selecting an alarm and clicking on the **Acknowledge** button) removes the alarm icon from the web UI, but the alarm will still be listed on the **Alarms** page with a status of *Acknowledged*. If a new alarm occurs, the alarm icon will reappear.

- You cannot delete alarms from the **Alarms** page. Alarms are removed by the Expressway only after the required action or configuration change has been made.
- After a restart of the Expressway, any *Acknowledged* alarms that are still in place on the Expressway will reappear with a status of *New*, and must be re-acknowledged.
- The display indicates when the alarm was first and last raised since the Expressway was last restarted.
- If your Expressway is a part of a cluster, the **Alarms** page shows all of the alarms raised by any of the cluster peers. However, you can acknowledge only those alarms that have been raised by the "current" peer (the peer to which you are currently logged in to as an administrator).
- You can click the Alarm ID to generate a filtered view of the Event Log, showing all occurrences of when that alarm has been raised and lowered.

See the [alarms list](#) for further information about the specific alarms that can be raised.

# Logs

## Event Log

The **Event Log** page (**Status > Logs > Event Log**) lets you view and search the Event Log, which is a list of the events that have occurred on your system since the last upgrade.

The Event Log holds a maximum of 2GB of data; when this size is reached, the oldest entries are overwritten. However, only the first 50MB of Event Log data can be displayed through the web interface.

### Filtering the Event Log

The **Filter** section lets you filter the Event Log. It is displayed only if there is more than one page of information to display. Log pages show 1000 records per page.

Enter the words you want to search for and click **Filter**. Only those events that contain all the words you entered are shown.

To do more advanced filtering, click **more options**. This gives you additional filtering methods:

- **Contains the string**: only includes events containing the exact phrase entered here.
- **Contains any of the words**: includes any events that contain at least one of the words entered here.
- **Not containing any of the words**: filters out any events containing any of the words entered here.

Note: use spaces to separate each word you want to filter by.

Click **Filter** to reapply any modified filter conditions. To return to the complete log listing, click **Reset**.

### Reconfiguring the log settings

Clicking **Configure the log settings** takes you to the [Logging configuration](#) page. From this page, you can set the level of events that are recorded in the Event Log, and also set up a remote server to which the Event Log can be copied.

### Saving the results to a local disk

Click **Download this page** if you want to download the contents of the results section to a text file on your local PC or server.

### Results section

The **Results** section shows all the events matching the current filter conditions, with the most recent being shown first.

Most **tvcs** events contain hyperlinks in one or more of the fields (such fields change color when you hover over them). You can click on the hyperlink to show only those events that contain the same text string. For example, clicking on the text that appears after **Event=** filters the list to show all the events of that particular type. Likewise, clicking on a particular **Call-Id** shows just those events that contain a reference to that particular call.

### Event Log color coding

Certain events in the Event Log are color-coded so that you can identify them more easily. These events are as follows:

Green events:

- System Start
- Admin Session Start/Finish
- Installation of <item> succeeded
- Call Connected
- Request Successful
- Beginning System Restore
- Completed System Restore

Orange events:

- System Shutdown
- Intrusion Protection Unblocking

Purple events:

- Diagnostic Logging

Red events:

- Registration Rejected
- Registration Refresh Rejected
- Call Rejected
- Security Alert
- License Limit Reached
- Decode Error
- TLS Negotiation Error
- External Server Communications Failure
- Application Failed
- Request Failed
- System Backup Error
- System Restore Error
- Authorization Failure
- Intrusion Protection Blocking

For more information about the format and content of the Event Log see [Event Log format \[p.282\]](#) and [Events and levels \[p.285\]](#).

## Configuration Log

The **Configuration Log** page (**Status > Logs > Configuration Log**) provides a list of all changes to the Expressway configuration.

The Configuration Log holds a maximum of 30MB of data; when this size is reached, the oldest entries are overwritten. The entire Configuration Log can be displayed through the web interface.

### Filtering the Configuration Log

The **Filter** section lets you filter the Configuration Log. It is displayed only if there is more than one page of information to display. Log pages show 1000 records per page.

Enter the words you want to search for and click **Filter**. Only those events that contain all the words you entered are shown.

To do more advanced filtering, click **more options**. This gives you additional filtering methods:

- **Contains the string**: only includes events containing the exact phrase entered here.
- **Contains any of the words**: includes any events that contain at least one of the words entered here.
- **Not containing any of the words**: filters out any events containing any of the words entered here.

Note: use spaces to separate each word you want to filter by.

Click **Filter** to reapply any modified filter conditions. To return to the complete log listing, click **Reset**.

### Results section

The **Results** section shows all the web-based events, with the most recent being shown first.

Most events contain hyperlinks in one or more of the fields (such fields change color when you hover over them). You can click on the hyperlink to show only those events that contain the same text string. For example, clicking on the text that appears after **Event=** filters the list to show all the events of that particular type. Likewise, clicking on a particular **user** shows just those events relating to that particular administrator account.

All events that appear in the Configuration Log are recorded as Level 1 Events, so any changes to the [logging levels](#) will not affect their presence in the Configuration Log.

### Configuration Log events

Changes to the Expressway configuration made by administrators using the web interface have an Event field of *System Configuration Changed*.

The **Detail** field of each of these events shows:

- the configuration item that was affected
- what it was changed from and to
- the name of the administrator user who made the change, and their IP address
- the date and time that the change was made

## Network Log

The **Network Log** page (**Status > Logs > Network Log**) provides a list of the call signaling messages that have been logged on this Expressway.

The Network Log holds a maximum of 2GB of data; when this size is reached, the oldest entries are overwritten. However, only the first 50MB of Network Log data can be displayed through the web interface.

### Filtering the Network Log

The **Filter** section lets you filter the Network Log. It is displayed only if there is more than one page of information to display. Log pages show 1000 records per page.

Enter the words you want to search for and click **Filter**. Only those events that contain all the words you entered are shown.

To do more advanced filtering, click **more options**. This gives you additional filtering methods:

- **Contains the string:** only includes events containing the exact phrase entered here.
- **Contains any of the words:** includes any events that contain at least one of the words entered here.
- **Not containing any of the words:** filters out any events containing any of the words entered here.

Note: use spaces to separate each word you want to filter by.

Click **Filter** to reapply any modified filter conditions. To return to the complete log listing, click **Reset**.

### Reconfiguring the log settings

Clicking **Configure the log settings** takes you to the [Network Log configuration](#) page. From this page, you can set the level of events that are recorded in the Network Log.

### Saving the results to a local disk

Click **Download this page** if you want to download the contents of the results section to a text file on your local PC or server.

### Results section

The **Results** section shows the events logged by each of the Network Log modules.

Most events contain hyperlinks in one or more of the fields (such fields change color when you hover over them). You can click on the hyperlink to show only those events that contain the same text string. For example, clicking on the text that appears after **Module=** filters the list to show all the events of that particular type.

The events that appear in the Network Log are dependent on the log levels configured on the [Network Log configuration](#) page.

# Hardware status

The **Hardware** page (**Status > Hardware**) provides information about the physical status of your Expressway appliance.

Information displayed includes:

- fan speeds
- component temperatures
- component voltages

Any appropriate minimum or maximum levels are shown to help identify any components operating outside of their standard limits.

---

**WARNING:** do not attempt to service the apparatus yourself as opening or removing covers may expose you to dangerous voltages or other hazards, and will void the warranty. Refer all servicing to qualified service personnel.

---

Note that hardware status information is not displayed if the Expressway is running on VMware.

# Reference material

---

This section provides supplementary information about the features and administration of the Expressway.

|   |     |
|---|-----|
| Performance capabilities .....                        | 281 |
| About Event Log levels .....                          | 282 |
| CPL reference .....                                   | 291 |
| Changing the default SSH key .....                    | 297 |
| Restoring default configuration (factory reset) ..... | 298 |
| Password encryption .....                             | 300 |
| Pattern matching variables .....                      | 301 |
| Port reference .....                                  | 303 |
| Mobile and remote access port reference .....         | 308 |
| Microsoft Lync B2BUA port reference .....             | 310 |
| Regular expressions .....                             | 312 |
| Supported characters .....                            | 314 |
| Call types and licensing .....                        | 315 |
| Alarms .....  | 317 |
| Command reference — xConfiguration .....              | 332 |
| Command reference — xCommand .....                    | 370 |
| Command reference — xStatus .....                     | 383 |
| External policy overview .....                        | 385 |
| Flash status word reference table .....               | 388 |
| Supported RFCs .....                                  | 389 |
| Software version history .....                        | 391 |
| Related documentation .....                           | 399 |
| Legal notices .....                                   | 401 |



# Performance capabilities

The performance capabilities of Expressway X8.5.2 software are summarized below. In all cases, note that:

- You can cluster up to 6 Expressways to increase capacity. This offers N+1 redundancy, because the maximum capacity of a cluster is 4 times the physical limit of a single Expressway.
- Logging is at default levels.
- Performance capacity will be reduced by features such as TURN relay services, and by configuring large numbers of zones and search rules.
- VM hardware requires a minimum of 6GB RAM.
- The Expressway supports up to 500 concurrent searches.

## **CE1000 appliances or Large VM servers (minimum 8 cores with 2 x 10Gb NIC)**

Supports 500 encrypted traversal calls @ 768kbps or 1000 encrypted SIP audio-only traversal calls @ 64kbps, and 500 non-traversal calls.

This assumes a maximum sustained call rate of 10 calls per second.

## **CE500 appliances or Small/Medium VM servers (2 cores and 1Gb NIC)**

Supports 100 encrypted traversal calls @ 768kbps and 500 non-traversal calls.

This assumes a maximum sustained call rate of 5 calls per second.

## About Event Log levels

All events have an associated level in the range 1-4, with Level 1 Events considered the most important. The table below gives an overview of the levels assigned to different events.

| Level | Assigned events   |
|-------|---|
| 1     | <p>High-level events such as registration requests and call attempts. Easily human readable. For example:</p> <ul style="list-style-type: none"> <li>■ call attempt/connected/disconnected</li> <li>■ registration attempt/rejected</li> </ul> <p>Note that endpoints or other devices cannot register to the Expressway. Registration requests will be rejected and will be logged with 'License limit exceeded' messages.</p> |
| 2     | <p>All Level 1 events, plus:</p> <ul style="list-style-type: none"> <li>■ logs of protocol messages sent and received (SIP, H.323, LDAP and so on) excluding noisy messages such as H.460.18 keepalives and H.245 video fast-updates</li> </ul>   |
| 3     | <p>All Level 1 and Level 2 events, plus:</p> <ul style="list-style-type: none"> <li>■ protocol keepalives</li> <li>■ call-related SIP signaling messages</li> </ul>   |
| 4     | <p>The most verbose level: all Level 1, Level 2 and Level 3 events, plus:</p> <ul style="list-style-type: none"> <li>■ network level SIP messages</li> </ul>  |

See the [Events and levels](#) section for a complete list of all events that are logged by the Expressway, and the level at which they are logged.

## Event Log format

The Event Log is displayed in an extension of the UNIX syslog format:

```
date time process_name: message_details
```

where:

| Field           | Description   |
|-----------------|---|
| date            | The local date on which the message was logged.   |
| time            | The local time at which the message was logged.   |
| process_name    | <p>The name of the program generating the log message. This could include:</p> <ul style="list-style-type: none"> <li>■ <b>tvcs</b> for all messages originating from Expressway processes</li> <li>■ <b>web</b> for all web login and configuration events</li> <li>■ <b>licensemanager</b> for messages originating from the call license manager</li> <li>■ <b>b2bua</b> for B2BUA events</li> <li>■ <b>portforwarding</b> for internal communications between the Expressway-C and the Expressway-E</li> <li>■ <b>ssh</b> for ssh tunnels between the Expressway-C and the Expressway-E</li> </ul> <p>but will differ for messages from other applications running on the Expressway.</p> |
| message_details | The body of the message (see the <a href="#">Message details field</a> section for further information).  |

## Administrator events

Administrator session related events are:

- Admin Session Start
- Admin Session Finish
- Admin Session Login Failure

The [Detail](#) field includes:

- the name of the administrator user to whom the session relates, and their IP address
- the date and time that the login was attempted, started, or ended

## Message details field

For all messages logged from the `tvcs` process, the `message_details` field, which contains the body of the message, consists of a number of human-readable `name=value` pairs, separated by a space.

The first name element within the `message_details` field is always `Event` and the last name element is always `Level`.

The table below shows all the possible name elements within the `message_details` field, in the order that they would normally appear, along with a description of each.

Note: in addition to the events described below, a `syslog.info` event containing the string `MARK` is logged after each hour of inactivity to provide confirmation that logging is still active.

| Name     | Description   |
|----------|---|
| Event    | The event which caused the log message to be generated. See <a href="#">Events and levels</a> for a list of all events that are logged by the Expressway, and the level at which they are logged. |
| User     | The username that was entered when a login attempt was made.  |
| ipaddr   | The source IP address of the user who has logged in.  |
| Protocol | Specifies which protocol was used for the communication. Valid values are: <ul style="list-style-type: none"> <li>■ TCP</li> <li>■ UDP</li> <li>■ TLS</li> </ul>                                  |
| Reason   | Textual string containing any reason information associated with the event.   |

| Name               | Description   |
|--------------------|---|
| Service            | Specifies which protocol was used for the communication. Will be one of: <ul style="list-style-type: none"> <li>■ H323</li> <li>■ SIP</li> <li>■ H.225</li> <li>■ H.245</li> <li>■ LDAP</li> <li>■ Q.931</li> <li>■ NeighbourGatekeeper</li> <li>■ Clustering</li> <li>■ ConferenceFactory</li> </ul> |
| Message Type       | Specifies the type of the message.  |
| Response-code      | SIP response code or, for H.323 and interworked calls, a SIP equivalent response code.  |
| Src-ip             | Source IP address (the IP address of the device attempting to establish communications). This can be an IPv4 address or an IPv6 address.  |
| Dst-ip             | Destination IP address (the IP address of the destination for a communication attempt). The destination IP is recorded in the same format as Src-ip.  |
| Src-port           | Source port: the IP port of the device attempting to establish communications.  |
| Dst-port           | Destination port: the IP port of the destination for a communication attempt.   |
| Src-alias          | If present, the first H.323 alias associated with the originator of the message.<br>If present, the first E.164 alias associated with the originator of the message.  |
| Dst-alias          | If present, the first H.323 alias associated with the recipient of the message.<br>If present, the first E.164 alias associated with the recipient of the message.  |
| Detail             | Descriptive detail of the Event.  |
| Auth               | Whether the call attempt has been authenticated successfully.   |
| Method             | SIP method (INVITE, BYE, UPDATE, REGISTER, SUBSCRIBE, etc).   |
| Contact            | Contact: header from REGISTER.  |
| AOR                | Address of record.  |
| Call-id            | The Call-ID header field uniquely identifies a particular invitation or all registrations of a particular client.   |
| Call-serial-number | The local Call Serial Number that is common to all protocol messages for a particular call.   |
| Tag                | The Tag is common to all searches and protocol messages across an Expressway network for all forks of a call.   |
| Call-routed        | Indicates if the Expressway took the signaling for the call.  |

| Name            | Description   |
|-----------------|---|
| To              | <ul style="list-style-type: none"> <li>■ for REGISTER requests: the AOR for the REGISTER request</li> <li>■ for INVITEs: the original alias that was dialed</li> <li>■ for all other SIP messages: the AOR of the destination.</li> </ul> |
| Request-URI     | The SIP or SIPS URI indicating the user or service to which this request is being addressed.  |
| Num-bytes       | The number of bytes sent/received in the message.   |
| Protocol-buffer | Shows the data contained in the buffer when a message could not be decoded.   |
| Duration        | Request/granted registration expiry duration.   |
| Time            | A full UTC timestamp in YYYY/MM/DD-HH:MM:SS format. Using this format permits simple ASCII text sorting/ordering to naturally sort by time. This is included due to the limitations of standard syslog timestamps.                        |
| Level           | The level of the event as defined in the <a href="#">About Event Log levels</a> section.  |
| UTCTime         | Time the event occurred, shown in UTC format.   |

## Events and levels

The following table lists the events that can appear in the Event Log.

| Event                                   | Description  | Level |
|---|--|-------|
| Alarm acknowledged                      | An administrator has acknowledged an alarm. The <b>Detail</b> event parameter provides information about the nature of the issue.                    | 1     |
| Alarm lowered                           | The issue that caused an alarm to be raised has been resolved. The <b>Detail</b> event parameter provides information about the nature of the issue. | 1     |
| Alarm raised                            | The Expressway has detected an issue and raised an alarm. The <b>Detail</b> event parameter provides information about the nature of the issue.      | 1     |
| Admin Session CBA Authorization Failure | An unsuccessful attempt has been made to log in when the Expressway is configured to use certificate-based authentication.                           | 1     |
| Admin Session Finish                    | An administrator has logged off the system.  | 1     |
| Admin Session Login Failure             | An unsuccessful attempt has been made to log in as an administrator. This could be because an incorrect username or password (or both) was entered.  | 1     |
| Admin Session Start                     | An administrator has logged onto the system.   | 1     |
| Application Exit                        | The Expressway application has been exited. Further information may be provided in the <b>Detail</b> event parameter.                                | 1     |
| Application Failed                      | The Expressway application is out of service due to an unexpected failure.   | 1     |
| Application Start                       | The Expressway has started. Further detail may be provided in the <b>Detail</b> event parameter.   | 1     |

| Event                     | Description   | Level |
|---------------------------|---|-------|
| Application Warning       | The Expressway application is still running but has experienced a recoverable problem. Further detail may be provided in the <b>Detail</b> event parameter.                                   | 1     |
| Authorization Failure     | The user has either entered invalid credentials, does not belong to an access group, or belongs to a group that has an access level of "None". Applies when remote authentication is enabled. | 1     |
| Beginning System Backup   | A system backup has started.  | 1     |
| Beginning System Restore  | A system restore has started.   | 1     |
| Call Answer Attempted     | An attempt to answer a call has been made.  | 1     |
| Call Attempted            | A call has been attempted.  | 1     |
| Call Bandwidth Changed    | The endpoints in a call have renegotiated call bandwidth.   | 1     |
| Call Connected            | A call has been connected.  | 1     |
| Call Diverted             | A call has been diverted.   | 1     |
| Call Disconnected         | A call has been disconnected.   | 1     |
| Call Inactivity Timer     | A call has been disconnected due to inactivity.   | 1     |
| Call Rejected             | A call has been rejected. The <b>Reason</b> event parameter contains a textual representation of the H.225 additional cause code.   | 1     |
| Call Rerouted             | The Expressway has <b>Call signaling optimization</b> set to <i>On</i> and has removed itself from the call signaling path.   | 1     |
| CBA Authorization Failure | An attempt to log in using certificate-based authentication has been rejected due to authorization failure.   | 1     |
| Certificate Management    | Indicates that security certificates have been uploaded. See the <b>Detail</b> event parameter for more information.  | 1     |
| Completed System Backup   | A system backup has completed.  | 1     |
| Completed System restore  | A system restore has completed.   | 1     |
| Configlog Cleared         | An operator cleared the Configuration Log.  | 1     |
| Decode Error              | A syntax error was encountered when decoding a SIP or H.323 message.  | 1     |
| Diagnostic Logging        | Indicates that diagnostic logging is in progress. The <b>Detail</b> event parameter provides additional details.  | 1     |
| Error Response Sent       | The TURN server has sent an error message to a client (using STUN protocol).  | 3     |
| Eventlog Cleared          | An operator cleared the Event Log.  | 1     |

| Event                                 | Description  | Level |
|---------------------------------------|--|-------|
| External Server Communication Failure | Communication with an external server failed unexpectedly. The <b>Detail</b> event parameter should differentiate between "no response" and "request rejected". Servers concerned are: <ul style="list-style-type: none"> <li>■ DNS</li> <li>■ LDAP servers</li> <li>■ Neighbor Gatekeeper</li> <li>■ NTP servers</li> <li>■ Peers</li> </ul>  | 1     |
| Hardware Failure                      | There is an issue with the Expressway hardware. If the problem persists, contact your Cisco support representative.  | 1     |
| License Limit Reached                 | Licensing limits for a given feature have been reached. The <b>Detail</b> event parameter specifies the facility/limits concerned.<br>If this occurs frequently, you may want to contact your Cisco representative to purchase more licenses.  | 1     |
| Message Received                      | An incoming RAS message has been received.   | 2     |
| Message Received                      | An incoming RAS NSM Keepalive, H.225, H.245 or a RAS message between peers has been received.  | 3     |
| Message Received                      | (SIP) An incoming message has been received.   | 4     |
| Message Rejected                      | This could be for one of two reasons: <ul style="list-style-type: none"> <li>■ If authentication is enabled and an endpoint has unsuccessfully attempted to send a message to the Expressway. This could be either because the endpoint has not supplied any authentication credentials, or because its credentials do not match those expected by the Expressway.</li> <li>■ Clustering is enabled but bandwidth across the cluster has not been configured identically, and the Expressway has received a message relating to an unknown peer, link, pipe, subzone or zone.</li> </ul> | 1     |
| Message Sent                          | An outgoing RAS message has been sent.   | 2     |
| Message Sent                          | An outgoing RAS NSM Keepalive, H.225, H.245 or a RAS message between peers has been sent.  | 3     |
| Message Sent                          | (SIP) An outgoing message has been sent.   | 4     |
| Operator Call Disconnect              | An administrator has disconnected a call.  | 1     |
| Outbound TLS Negotiation Error        | The Expressway is unable to communicate with another system over TLS. The event parameters provide more information.   | 1     |
| Package Install                       | A package, for example a language pack, has been installed or removed.   | 2     |
| Policy Change                         | A policy file has been updated.  | 1     |
| POST request failed                   | A HTTP POST request was submitted from an unauthorized session.  | 1     |

| Event                          | Description  | Level |
|--------------------------------|--|-------|
| Provisioning                   | Diagnostic messages from the provisioning server. The <b>Detail</b> event parameter provides additional information.                                       | 1     |
| Reboot Requested               | A system reboot has been requested. The <b>Reason</b> event parameter provides specific information.   | 1     |
| Registration Refresh Rejected  | A request to refresh a registration has been rejected.   | 1     |
| Registration Refresh Requested | A request to refresh or keep a registration alive has been received.   | 3     |
| Registration Rejected          | A registration request has been rejected. The <b>Reason</b> and <b>Detail</b> event parameters provide more information about the nature of the rejection. | 1     |
| Registration Requested         | A registration has been requested.   | 1     |
| Relay Allocated                | A TURN server relay has been allocated.  | 2     |
| Relay Deleted                  | A TURN server relay has been deleted.  | 2     |
| Relay Expired                  | A TURN server relay has expired.   | 2     |
| Request Failed                 | A request sent to the Conference Factory has failed.   | 1     |
| Request Received               | A call-related SIP request has been received.  | 2     |
| Request Received               | A non-call-related SIP request has been received.  | 3     |
| Request Sent                   | A call-related SIP request has been sent.  | 2     |
| Request Sent                   | A non-call-related SIP request has been sent.  | 3     |
| Request Successful             | A successful request was sent to the Conference Factory.   | 1     |
| Response Received              | A call-related SIP response has been received.   | 2     |
| Response Received              | A non-call-related SIP response has been received.   | 3     |
| Response Sent                  | A call-related SIP response has been sent.   | 2     |
| Response Sent                  | A non-call-related SIP response has been sent.   | 3     |
| Restart Requested              | A system restart has been requested. The <b>Reason</b> event parameter provides specific information.  | 1     |
| Search Attempted               | A search has been attempted.   | 1     |
| Search Cancelled               | A search has been cancelled.   | 1     |
| Search Completed               | A search has been completed.   | 1     |



| Event   | Description  | Level |
|---|--|-------|
| Search Loop detected                              | The Expressway is in <b>Call loop detection</b> mode and has identified and terminated a looped branch of a search.  | 2     |
| Secure mode disabled                              | The Expressway has successfully exited <b>Advanced account security</b> mode.  | 1     |
| Secure mode enabled                               | The Expressway has successfully entered <b>Advanced account security</b> mode.   | 1     |
| Security Alert                                    | A potential security-related attack on the Expressway has been detected.   | 1     |
| Success Response Sent                             | The TURN server has sent a success message to a client (using STUN protocol).  | 3     |
| System backup completed                           | The system backup process has completed.   | 1     |
| System Backup error                               | An error occurred while attempting a system backup.  | 1     |
| System backup started                             | The system backup process has started.   | 1     |
| System Configuration Changed                      | An item of configuration on the system has changed. The <b>Detail</b> event parameter contains the name of the changed configuration item and its new value. | 1     |
| System restore completed                          | The system restore process has completed.  | 1     |
| System restore backing up current config          | System restore process has started backing up the current configuration  | 1     |
| System restore backup of current config completed | System restore process has completed backing up the current configuration  | 1     |
| System restore error                              | An error occurred while attempting a system restore.   | 1     |
| System restore started                            | The system restore process has started.  | 1     |
| System Shutdown                                   | The operating system was shutdown.   | 1     |
| System snapshot started                           | A system snapshot has been initiated.  | 1     |
| System snapshot completed                         | A system snapshot has completed.   | 1     |
| System Start                                      | The operating system has started. The <b>Detail</b> event parameter may contain additional information if there are startup problems.                        | 1     |
| TLS Negotiation Error                             | Transport Layer Security (TLS) connection failed to negotiate.   | 1     |

| <b>Event</b>             | <b>Description</b>   | <b>Level</b> |
|--------------------------|--|--------------|
| Unregistration Rejected  | An unregistration request has been rejected.   | 1            |
| Unregistration Requested | An unregistration request has been received.   | 1            |
| Upgrade                  | Messages related to the software upgrade process. The <b>Detail</b> event parameter provides specific information. | 1            |

# CPL reference

Call Processing Language (CPL) is an XML-based language for defining call handling. This section gives details of the Expressway's implementation of the CPL language and should be read in conjunction with the CPL standard [RFC 3880](#).

The Expressway has many powerful inbuilt transform features so CPL should be required only if advanced call handling rules are required.

The Expressway supports most of the CPL standard along with some TANDBERG-defined extensions. It does not support the top level actions `<incoming>` and `<outgoing>` as described in *RFC 3880*. Instead it supports a single section of CPL within a `<taa:routed>` section.

When Call Policy is implemented by uploading a CPL script to the Expressway, the script is checked against an XML schema to verify the syntax. There are two schemas - one for the basic CPL specification and one for the TANDBERG extensions. Both of these schemas can be [downloaded from the web interface](#) and used to validate your script before uploading to the Expressway.

The following example shows the correct use of namespaces to make the syntax acceptable:

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
  xmlns:taa="http://www.tandberg.net/cpl-extensions"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
  <taa:routed>
    <address-switch field="destination">
      <address is="reception@example.com">
        <proxy/>
      </address>
    </address-switch>
  </taa:routed>
</cpl>
```

## Source and destination address formats

When the descriptions in this section refer to the source or destination aliases of a call, this means all supported address formats (URIs, IP addresses, E.164 aliases and so on).

## CPL address-switch node

The **address-switch** node allows the script to run different actions based on the source or destination aliases of the call. It specifies which fields to match, and then a list of address nodes contains the possible matches and their associated actions.

The address-switch has two node parameters: **field** and **subfield**.

### address

The **address** construct is used within an **address-switch** to specify addresses to match. It supports the use of [regular expressions](#).

Valid values are:

|                                   |   |
|-----------------------------------|---|
| <b>is=string</b>                  | Selected field and subfield exactly match the given string.   |
| <b>contains=string</b>            | Selected field and subfield contain the given string. Note that the CPL standard only allows for this matching on the display subfield; however the Expressway allows it on any type of field.  |
| <b>subdomain-of=string</b>        | If the selected field is numeric (for example, the tel subfield) then this matches as a prefix; so <code>address subdomain-of="555"</code> matches 5556734 and so on. If the field is not numeric then normal domain name matching is applied; so <code>address subdomain-of="company.com"</code> matches <code>nodeA.company.com</code> and so on. |
| <b>regex="regular expression"</b> | Selected field and subfield match the given regular expression.   |

All address comparisons ignore upper/lower case differences so `address is="Fred"` will also match `fred`, `freD` and so on.

## field

Within the `address-switch` node, the mandatory `field` parameter specifies which address is to be considered. The supported attributes and their interpretation are shown below:

| Field parameter attributes                          | SIP   | H.323   |
|---|---|---|
| <b>unauthenticated-origin</b>                       | The "From" and "ReplyTo" fields of the incoming message.  | The source aliases from the original LRQ or ARQ that started the call. If a SETUP is received without a preceding RAS message then the origin is taken from the SETUP.  |
| <b>authenticated-origin</b><br>and<br><b>origin</b> | The "From" and "ReplyTo" fields of the message if it authenticated correctly (or where the relevant <b>Authentication Policy</b> is <i>Treat as authenticated</i> ), otherwise <b>not-present</b> .   | The source aliases from the original LRQ or ARQ that started the call if it authenticated correctly (or where the relevant <b>Authentication Policy</b> is <i>Treat as authenticated</i> ) otherwise <b>not-present</b> . Because SETUP messages are not authenticated, if the Expressway receives a SETUP without a preceding RAS message the origin will always be <b>not-present</b> . |
| <b>originating-zone</b>                             | The name of the zone or subzone for the originating leg of the call. If the call originates from a neighbor, traversal server or traversal client zone then this will equate to the zone name. In all other cases this will be "DefaultZone". |   |
| <b>originating-user</b>                             | If the relevant <b>Authentication Policy</b> is <i>Check credentials</i> or <i>Treat as authenticated</i> this is the username used for authentication, otherwise <b>not-present</b> .  |   |
| <b>registered-origin</b>                            | If the call originates from a registered endpoint this is the list of all aliases it has registered, otherwise <b>not-present</b> .   |   |
| <b>destination</b>                                  | The destination aliases.  |   |
| <b>original-destination</b>                         | The destination aliases.  |   |

Note that any Authentication Policy settings that apply are those configured for the relevant zone according to the source of the incoming message.

If the selected field contains multiple aliases then the Expressway will attempt to match each address node with all of the aliases before proceeding to the next address node, that is, an address node matches if it matches any alias.

## subfield

Within the `address-switch` node, the optional `subfield` parameter specifies which part of the address is to be considered. The following table gives the definition of subfields for each alias type.

If a subfield is not specified for the alias type being matched then the `not-present` action is taken.

|                     |  |
|---------------------|--|
| <b>address-type</b> | Either <code>h323</code> or <code>sip</code> , based on the type of endpoint that originated the call.   |
| <b>user</b>         | For URI aliases this selects the username part. For H.323 IDs it is the entire ID and for E.164 numbers it is the entire number.   |
| <b>host</b>         | For URI aliases this selects the domain name part. If the alias is an IP address then this subfield is the complete address in dotted decimal form.  |
| <b>tel</b>          | For E.164 numbers this selects the entire string of digits.  |
| <b>alias-type</b>   | Gives a string representation of the type of alias. The type is inferred from the format of the alias. Possible types are: <ul style="list-style-type: none"> <li>■ Address Type</li> <li>■ Result</li> <li>■ URI</li> <li>■ url-ID</li> <li>■ H.323 ID</li> <li>■ h323-ID</li> <li>■ Dialed Digits</li> <li>■ dialedDigits</li> </ul> |

## otherwise

The `otherwise` node is executed if the address specified in the `address-switch` was found but none of the preceding address nodes matched.

## not-present

The `not-present` node is executed when the address specified in the `address-switch` was not present in the call setup message. This form is most useful when authentication is being used. With authentication enabled the Expressway will only use authenticated aliases when running policy so the `not-present` action can be used to take appropriate action when a call is received from an unauthenticated user (see the example Call screening of authenticated users).

## location

As the CPL script is evaluated it maintains a list of addresses (H.323 IDs, URLs and E.164 numbers) which are used as the destination of the call if a `proxy` node is executed. The `taa:location` node allows the location set to be modified so that calls can be redirected to different destinations.

At the start of script execution the location set is initialized to the original destination.

The following attributes are supported on `taa:location` nodes. It supports the use of [regular expressions](#).

|   |  |
|---|--|
| <b>Clear = "yes"   "no"</b>   | Specifies whether to clear the current location set before adding the new location. The default is to append this location to the end of the set.  |
| <b>url=string</b>   | The new location to be added to the location set. The given string can specify a URL (for example, <code>user@domain.com</code> ), H.323 ID or an E.164 number.  |
| <b>priority=&lt;0.0..1.0&gt;   "random"</b>   | Specified either as a floating point number in the range 0.0 to 1.0, or <code>random</code> , which assigns a random number within the same range. 1.0 is the highest priority. Locations with the same priority are searched in parallel. |
| <b>regex="&lt;regular expression&gt;"<br/>replace="&lt;string&gt;"</b>  | Specifies the way in which a location matching the regular expression is to be changed.  |
| <b>source-url-for-message="&lt;string&gt;"</b>  | Replaces the From header (source alias) with the specified string.   |
| <b>source-url-for-message-regex="&lt;regular expression&gt;"</b><br>together with<br><b>source-url-for-message-replace="&lt;string&gt;"</b> | Replaces any From header (source alias) that matches the regular expression with the specified replacement string. If there are multiple From headers (applies to H.323 only) then any From headers that do not match are left unchanged.  |

If the source URL of a From header is modified, any corresponding display name is also modified to match the username part of the modified source URL.

## rule-switch

This extension to CPL is provided to simplify Call Policy scripts that need to make decisions based on both the source and destination of the call. A `taa:rule-switch` can contain any number of rules that are tested in sequence; as soon as a match is found the CPL within that rule element is executed.

Each rule must take one of the following forms:

```
<taa:rule-switch>
  <taa:rule origin="<regular expression>" destination="<regular expression>" message-
  regex="<regular expression>">
    <taa:rule authenticated-origin="<regular expression>" destination="<regular
  expression>" message-regex="<regular expression>">
      <taa:rule unauthenticated-origin="<regular expression>" destination="<regular
  expression>" message-regex="<regular expression>">
          <taa:rule registered-origin="<regular expression>" destination="<regular expression>"
  message-regex="<regular expression>">
              <taa:rule originating-user="<regular expression>" destination="<regular expression>"
  message-regex="<regular expression>">
                  <taa:rule originating-zone="<regular expression>" destination="<regular expression>"
  message-regex="<regular expression>">
                      </taa:rule-switch>
```

The meaning of the various `origin` selectors is as described in the [field](#) section.

The `message-regex` parameter allows a regular expression to be matched against the entire incoming SIP message.

Note that any rule containing a `message-regex` parameter will never match an H.323 call.

## proxy

On executing a proxy node the Expressway attempts to forward the call to the locations specified in the current location set. If multiple entries are in the location set then this results in a forked call. If the current location set is empty the call is forwarded to its original destination.

The proxy node supports the following optional parameters:

|  |  |
|--|--|
| <code>timeout=&lt;1..86400&gt;</code>    | Timeout duration, specified in seconds                   |
| <code>stop-on-busy = "yes"   "no"</code> | Whether to stop searching if a busy response is received |

The proxy action can lead to the results shown in the table below.

|                          |  |
|--------------------------|--|
| <code>failure</code>     | The proxy failed to route the call           |
| <code>busy</code>        | Destination is found but is busy             |
| <code>noanswer</code>    | Destination is found but does not answer     |
| <code>redirection</code> | Expressway is asked to redirect the call     |
| <code>default</code>     | CPL to run if the other results do not apply |

The CPL can perform further actions based on these results. Any results nodes must be contained within the **proxy** node. For example:

```
<proxy timeout="10">
  <busy>
    <!--If busy route to recording service-->
    <location clear="yes" url="recorder">
      <proxy/>
    </location>
  </busy>
</proxy>
```

## reject

If a **reject** node is executed the Expressway stops any further script processing and rejects the current call.

The custom reject strings `status=string` and `reason=string` options are supported here and should be used together to ensure consistency of the strings.

## Unsupported CPL elements

The Expressway does not currently support some elements that are described in the CPL RFC. If an attempt is made to upload a script containing any of the following elements an error message will be generated and the Expressway will continue to use its existing policy.

The following elements are not currently supported:

- time-switch
- string-switch

- language-switch
- priority-switch
- redirect
- mail
- log
- subaction
- lookup
- remove-location



## Changing the default SSH key

Using the default key means that SSH sessions established to the Expressway may be vulnerable to "man-in-the-middle" attacks, so you are recommended to generate new SSH keys which are unique to your Expressway.

An alarm message "Security alert: the SSH service is using the default key" is displayed if your Expressway is still configured with its factory default SSH key.

To generate a new SSH key for the Expressway:

1. Log into the CLI as *root*.
2. Type `regeneratesshkey`.
3. Type `exit` to log out of the root account.
4. Log in to the web interface.
5. Go to **Maintenance > Restart**. You are taken to the **Restart** page.
6. Check the number of calls currently in place.
7. Click **Restart system** and then confirm the restart when asked.

If you have a clustered Expressway system you must generate new SSH keys for every cluster peer. Log into each peer in turn and follow the instructions above. You do not have to decluster or disable replication.

**When you next log in to the Expressway over SSH you may receive a warning that the key identity of the Expressway has changed. Please follow the appropriate process for your SSH client to suppress this warning.**

**If your Expressway is subsequently downgraded to an earlier version of Expressway firmware, the default SSH keys will be restored.**

# Restoring default configuration (factory reset)

Very rarely, it may become necessary to run the “factory-reset” script on your system. This reinstalls the software image and resets the configuration to the functional minimum.

**Note:** Restoring default configuration causes the system to use its current default values, which may be different from the previously configured values, particularly if the system has been upgraded from an older version. In particular this may affect port settings, such as multiplexed media ports. After restoring default configuration you may want to reset those port settings to match the expected behavior of your firewall.

## Prerequisite files

The **factory-reset** procedure described below rebuilds the system based on the most recent successfully-installed software image. The files that are used for this reinstallation are stored in the **/mnt/harddisk/factory-reset/** folder on the system. These files are:

- A text file containing just the 16-character Release Key, named **rk**
- A file containing the software image in tar.gz format, named **tandberg-image.tar.gz**

In some cases (most commonly a fresh VM installation that has not been upgraded), these files will not be present on the system. If so, these files must first be put in place using SCP as root.

## Performing a reset to default configuration

The following procedure must be performed from the serial console (or via a direct connection to the appliance with a keyboard and monitor). This is because the network settings will be rewritten, so any SSH session used to initiate the reset would be dropped and the output of the procedure would not be seen.

The process takes approximately 20 minutes.

1. Log in to the system as **root**.
2. Type **factory-reset**
3. Answer the questions as required:

The recommended responses will reset the system completely to a factory default state.

| Prompt                                   | Recommended response |
|--|----------------------|
| Keep option keys [YES/NO]?               | YES                  |
| Keep IP configuration [YES/NO]?          | YES                  |
| Keep ssh keys [YES/NO]?                  | YES                  |
| Keep ssl certificates and keys [YES/NO]? | YES                  |
| Keep root and admin passwords [YES/NO]?  | YES                  |
| Save log files [YES/NO]?                 | YES                  |

4. Finally, confirm that you want to proceed.

## Resetting via USB stick

Cisco TAC may also suggest an alternative reset method. This involves downloading the software image onto a USB stick and then rebooting the system with the USB stick plugged in.

If you use this method you must clear down and rebuild the USB stick after use. Do not reset one system and then take the USB stick and re-use it on another system.

# Password encryption

All passwords configured on the Expressway are stored securely in either an encrypted or hashed form. This applies to the following items, which all have usernames and passwords associated with them:

- the default admin administrator account
- any additional administrator accounts
- local authentication database credentials (a list of valid usernames and passwords that are used when other devices are required to authenticate with the Expressway)
- outbound connection credentials (used by the Expressway when required to authenticate with another system)
- LDAP server (used by the Expressway when binding to an LDAP server)

## Web interface

When entering or viewing passwords using the web interface, you will see placeholder characters (e.g. dots or stars, depending on your browser) instead of the characters you are typing.

## Command line interface (CLI)

When entering passwords using the command line interface (CLI), you type the password in plain text. However, after the command has been executed, the password is displayed in its encrypted form with a `{cipher}` prefix, for example:

```
xConfiguration Authentication Password: "{cipher}xcy6k+4NgB025vYEgoEXXw=="
```

## Maximum length of passwords

For each type of password, the maximum number of plain text characters that can be entered is shown in the table below.

| Password type                             | Maximum length |
|---|----------------|
| Admin account                             | 1024           |
| Other local administrator accounts        | 1024           |
| Local database authentication credentials | 128            |
| Outbound connection credentials           | 128            |
| LDAP server                               | 60             |

Note that:

- local administrator account passwords are hashed using SHA512; other passwords are stored in an encrypted format
- when a password is encrypted and stored, it uses more characters than the original plain text version of the password

## Pattern matching variables

The Expressway makes use of pattern matching in a number of its features, namely [pre-search transforms](#) and when configuring [search rules and zone transforms](#).

For each of these pattern matches, the Expressway allows you to use a variable that it will replace with the current configuration values before the pattern is checked.

These variables can be used as either or both of:

- all or part of the pattern that is being searched for
- all or part of the string that is replacing the pattern that was found

The variables can be used in all types of patterns (*Prefix*, *Suffix*, *Regex* and *Exact*).

The table below shows the strings that are valid as variables, and the values they represent.

| String   | Represents value returned by...  | When used in a Pattern field  | When used in a Replace field  |
|----------|--|---|---|
| %ip%     | xConfiguration Ethernet 1 IP V4 Address<br>xConfiguration Ethernet 1 IP V6 Address<br>xConfiguration Ethernet 2 IP V4 Address<br>xConfiguration Ethernet 2 IP V6 Address | Matches all IPv4 and IPv6 addresses.<br><br>Applies to all peer addresses if the Expressway is part of a cluster.                                 | not applicable  |
| %ipv4%   | xConfiguration Ethernet 1 IP V4 Address<br>xConfiguration Ethernet 2 IP V4 Address   | Matches the IPv4 addresses currently configured for LAN 1 and LAN 2.<br><br>Applies to all peer addresses if the Expressway is part of a cluster. | not applicable  |
| %ipv4_1% | xConfiguration Ethernet 1 IP V4 Address  | Matches the IPv4 address currently configured for LAN 1.<br><br>Applies to all peer addresses if the Expressway is part of a cluster.             | Replaces the string with the LAN 1 IPv4 address.<br><br>If the Expressway is part of a cluster, the address of the local peer is always used. |
| %ipv4_2% | xConfiguration Ethernet 2 IP V4 Address  | Matches the IPv4 address currently configured for LAN 2.<br><br>Applies to all peer addresses if the Expressway is part of a cluster.             | Replaces the string with the LAN 2 IPv4 address.<br><br>If the Expressway is part of a cluster, the address of the local peer is always used. |

| String                                    | Represents value returned by...   | When used in a Pattern field   | When used in a Replace field  |
|---|---|--|---|
| %ipv6%                                    | xConfiguration Ethernet 1 IP V6 Address<br>xConfiguration Ethernet 2 IP V6 Address            | Matches the IPv6 addresses currently configured for LAN 1 and LAN 2.<br><br>Applies to all peer addresses if the Expressway is part of a cluster.          | not applicable  |
| %ipv6_1%                                  | xConfiguration Ethernet 1 IP V6 Address   | Matches the IPv6 address currently configured for LAN 1.<br><br>Applies to all peer addresses if the Expressway is part of a cluster.                      | Replaces the string with the LAN 1 IPv6 address.<br><br>If the Expressway is part of a cluster, the address of the local peer is always used. |
| %ipv6_2%                                  | xConfiguration Ethernet 2 IP V6 Address   | Matches the IPv6 address currently configured for LAN 2.<br><br>Applies to all peer addresses if the Expressway is part of a cluster.                      | Replaces the string with the LAN 2 IPv6 address.<br><br>If the Expressway is part of a cluster, the address of the local peer is always used. |
| %localdomains%                            | xConfiguration SIP Domains Domain 1 Name<br>...<br>xConfiguration SIP Domains Domain 200 Name | Matches all the SIP domains currently configured on the Expressway.  | not applicable  |
| %localdomain1%<br>...<br>%localdomain200% | xConfiguration SIP Domains Domain 1 Name<br>...<br>xConfiguration SIP Domains Domain 200 Name | Matches the specified SIP domain. Up to 200 SIP domains can be configured on the Expressway, and they are identified by an index number between 1 and 200. | Replaces the string with the specified SIP domain.  |
| %systemname%                              | xConfiguration SystemUnit Name  | Matches the Expressway's System Name.  | Replaces the string with the Expressway's System Name.  |

You can test whether a pattern matches a particular alias and is transformed in the expected way by using the [Check pattern](#) tool ([Maintenance > Tools > Check pattern](#)).

## Port reference

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

- [Microsoft Lync B2BUA port reference \[p.310\]](#)
- [Mobile and remote access port reference \[p.308\]](#)

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 9: 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<br>outbound | not configurable                |
| Clustering           | IPsec secure communication between cluster peers.   | IP protocol 51 (IPSec AH) | inbound<br>outbound | not configurable                |
| Reserved             |   | 636                       | inbound             | not configurable                |
| DNS                  | Sending requests to DNS servers.  | 1024 - 65535 UDP          | outbound            | <a href="#">System &gt; DNS</a> |
| Gatekeeper discovery | Multicast gatekeeper discovery. The Expressway does not listen on this port when <b>H.323 Gatekeeper Auto discover mode</b> is set to <i>Off</i> (this disables IGMP messages). | 1718 UDP                  | inbound             | not configurable                |

Table 9: 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<br>outbound | <a href="#">Configuration &gt; Protocols &gt; H.323</a> |
| H.323 call signaling                           | Listens for H.323 call signaling.  | 1720 TCP                                    | inbound             | <a href="#">Configuration &gt; Protocols &gt; H.323</a> |
| Assent call signaling                          | Assent signaling on the Expressway-E.  | 2776 TCP                                    | inbound             | <a href="#">Configuration &gt; Traversal &gt; Ports</a> |
| H.460.18 call signaling                        | H.460.18 signaling on the Expressway-E.  | 2777 TCP                                    | inbound             | <a href="#">Configuration &gt; Traversal &gt; Ports</a> |
| 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<br>outbound | <a href="#">Configuration &gt; Traversal &gt; Ports</a> |
| TURN services                                  | Listening port for TURN relay requests on Expressway-E.  | 3478 UDP *                                  | inbound             | <a href="#">Configuration &gt; Traversal &gt; TURN</a>  |
| 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<br>outbound | <a href="#">Configuration &gt; Protocols &gt; SIP</a>   |
| SIP TCP  | Listens for incoming SIP TCP calls.  | 5060 TCP                                    | inbound             | <a href="#">Configuration &gt; Protocols &gt; SIP</a>   |
| SIP TLS  | Listens for incoming SIP TLS calls.  | 5061 TCP                                    | inbound             | <a href="#">Configuration &gt; Protocols &gt; SIP</a>   |
| 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             | <a href="#">Configuration &gt; Zones</a>                |
| 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             | <a href="#">Configuration &gt; Zones</a>                |
| 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<br>outbound | <a href="#">Configuration &gt; Protocols &gt; H.323</a> |
| SIP TCP outbound port range                    | Range of ports used by outbound TCP/TLS SIP connections to a remote SIP device.  | 25000 - 29999 TCP                           | outbound            | <a href="#">Configuration &gt; Protocols &gt; SIP</a>   |



Table 9: Local inbound/outbound ports (continued)

| Service/function   | Purpose  | Expressway port (default)  | Direction           | Configurable via                                     |
|--|--|--|---------------------|--|
| Ephemeral ports  | Various purposes.  | 30000 – 35999  | outbound            | <a href="#">System &gt; Administration</a>           |
| Multiplexed traversal media (Assent, H.460.19 multiplexed media) | <p>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.</p> <p>The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at <a href="#">Configuration &gt; Traversal Subzone</a>. 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 (<a href="#">Configuration &gt; Traversal &gt; Ports</a>). If you choose not to configure a particular pair of ports (<b>Use configured demultiplexing ports = No</b>), then the Expressway-E will listen on the first pair of ports in the media traversal port range (36000 and 36001 by default).</p> | <p>36000 – 36001<br/>UDP (Small / Medium systems)<br/>or<br/>36000 – 36011<br/>UDP (Large systems)</p> | inbound<br>outbound | <a href="#">Configuration &gt; Traversal Subzone</a> |

Table 9: Local inbound/outbound ports (continued)

| Service/function                 | Purpose   | Expressway port (default)  | Direction           | Configurable via                                       |
|----------------------------------|---|--|---------------------|--|
| Non-multiplexed media port range | <p>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.</p> <p>The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at <a href="#">Configuration &gt; Traversal Subzone</a>. 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 (<a href="#">Configuration &gt; Traversal &gt; Ports</a>). If you choose not to configure a particular pair of ports (<b>Use configured demultiplexing ports = No</b>), then the Expressway-E will listen on the first pair of ports in the media traversal port range (36000 and 36001 by default).</p> | <p>36002 – 59999<br/>UDP (Small / Medium systems)<br/>or<br/>36012 – 59999<br/>UDP (Large systems)</p> | inbound<br>outbound | <a href="#">Configuration &gt; Traversal Subzone</a>   |
| TURN relay media port range      | Range of ports available for TURN media relay.  | 24000 – 29999 UDP  | inbound<br>outbound | <a href="#">Configuration &gt; Traversal &gt; TURN</a> |

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 10: Remote listening ports

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

## Mobile and remote access port reference

This section summarizes the ports that could potentially be used between your internal network (where the Expressway-C is located) and the DMZ (where the Expressway-E is located) and between the DMZ and the public internet.

### Outbound from Expressway-C (private) to Expressway-E (DMZ)

| Purpose   | Protocol | Expressway-C (source) | Expressway-E (listening)   |
|---|----------|-----------------------|--|
| XMPP (IM and Presence)  | TCP      | Ephemeral port        | 7400   |
| SSH (HTTP/S tunnels)  | TCP      | Ephemeral port        | 2222   |
| Traversal zone SIP signaling  | TLS      | 25000 to 29999        | 7001   |
| Traversal zone SIP media<br>(for small/medium systems on X8.1 or later) | UDP      | 36000 to 59999*       | 36000 (RTP), 36001 (RTCP) (defaults)   |
| Traversal zone SIP media<br>(for large systems)                         | UDP      | 36000 to 59999*       | 36000 to 36011 (6 pairs of RTP and RTCP ports for multiplexed media traversal) |

### Outbound from Expressway-E (DMZ) to public internet

| Purpose       | Protocol | Expressway-E (source)               | Internet endpoint (listening) |
|---------------|----------|-------------------------------------|-------------------------------|
| SIP media     | UDP      | 36002 to 59999 or<br>36012 to 59999 | >= 1024                       |
| SIP signaling | TLS      | 25000 to 29999                      | >= 1024                       |

### Inbound from public internet to Expressway-E (DMZ)

| Purpose   | Protocol | Internet endpoint (source) | Expressway-E (listening)             |
|---|----------|----------------------------|--------------------------------------|
| XMPP (IM and Presence)  | TCP      | >= 1024                    | 5222                                 |
| HTTP proxy (UDS)  | TCP      | >= 1024                    | 8443                                 |
| Media   | UDP      | >= 1024                    | 36002 to 59999 or<br>36012 to 59999* |
| SIP signaling   | TLS      | >= 1024                    | 5061                                 |
| HTTPS (only required for external administrative access, which is strongly discouraged) | TCP      | >= 1024                    | 443                                  |

## From Expressway-C to Unified CM / Cisco Unity Connection

| Purpose   | Protocol | Expressway-C (source) | Unified CM (listening)         |
|---|----------|-----------------------|--------------------------------|
| XMPP (IM and Presence)                                | TCP      | Ephemeral port        | 7400 (IM and Presence)         |
| HTTP proxy (UDS)                                      | TCP      | Ephemeral port        | 8443 (Unified CM)              |
| HTTP proxy (SOAP)                                     | TCP      | Ephemeral port        | 8443 (IM and Presence Service) |
| HTTP (configuration file retrieval)                   | TCP      | Ephemeral port        | 6970                           |
| CUC (voicemail)                                       | TCP      | Ephemeral port        | 443 (Unity Connection)         |
| Message Waiting Indicator (MWI) from Unity Connection | TCP      | Ephemeral port        | 7080 (Unity Connection)        |
| Media   | UDP      | 36000 to 59999*       | >= 1024                        |
| SIP signaling   | TCP      | 25000 to 29999        | 5060                           |
| Secure SIP signaling                                  | TLS      | 25000 to 29999        | 5061                           |

\* 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).

Note that:

- Ports 8191/8192 TCP and 8883/8884 TCP are used internally within the Expressway-C and the Expressway-E applications. Therefore these ports must not be allocated for any other purpose. The Expressway-E listens externally on port 8883; therefore we recommend that you create custom firewall rules on the external LAN interface to drop TCP traffic on that port.
- The Expressway-E listens on port 2222 for SSH tunnel traffic. The only legitimate sender of such traffic is the Expressway-C (cluster). Therefore we recommend that you create the following firewall rules for the SSH tunnels service:
  - one or more rules to allow all of the Expressway-C peer addresses (via the internal LAN interface, if appropriate)
  - followed by a lower priority (higher number) rule that drops all traffic for the SSH tunnels service (on the internal LAN interface if appropriate, and if so, another rule to drop all traffic on the external interface)

## Microsoft Lync B2BUA port reference

The port numbers listed below are the default port values. The values used in a real deployment may vary if they have been modified, for example, by changes of registry settings or through group policy, on Lync and Lync client, or configuration on Expressway ([Applications > B2BUA](#)).

### Between B2BUA and Lync

| Purpose   | Protocol | B2BUA IP port  | Lync IP port                           |
|---|----------|----------------|--|
| Signaling to Lync Server  | TLS      | 65072          | 5061 (Lync signaling destination port) |
| Signaling from Lync Server  | TLS      | 65072          | Lync ephemeral port                    |
| Media (the Lync B2BUA should be deployed on a separate "Lync Gateway" Expressway and thus there should be no conflict with the standard traversal media port range) | UDP      | 56000 to 57000 | Lync client media ports                |

**Note:** The Expressway does not forward DSCP information that it receives in media streams.

### Between B2BUA and Expressway (internal communications)

| Purpose   | Protocol | B2BUA IP port | Expressway IP port    |
|---|----------|---------------|-----------------------|
| Internal communications with Expressway application | TLS      | 65070         | SIP TCP outbound port |

### Between B2BUA and Expressway-E hosting the TURN server

| Purpose            | Protocol | B2BUA IP port  | Expressway-E IP port     |
|--------------------|----------|----------------|--------------------------|
| All communications | UDP      | 56000 to 57000 | 3478 (media/signaling) * |

Ensure that the firewall is opened to allow the data traffic through from B2BUA to Expressway-E.

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

### External Lync client and Edge server

| Purpose  | Protocol | Edge server | Lync client |
|--|----------|-------------|-------------|
| SIP/MTLS used between Lync Client and Edge server for signaling (including any ICE messaging to the Edge Server) | TCP      | 5061        | 5061        |
| SIP/TLS  | TCP      | 443         | 443         |

| Purpose   | Protocol | Edge server | Lync client |
|-----------|----------|-------------|-------------|
| STUN      | UDP      | 3478        | 3478        |
| UDP Media | UDP      | 50000-59999 | 1024-65535  |
| TCP Media | TCP      | 50000-59999 | 1024-65535  |

### External Lync client / Edge server and Expressway-E

| Purpose   | Protocol | Lync client / Edge server | Expressway-E |
|---|----------|---------------------------|--------------|
| ICE messaging (STUN/TURN) if media is sent via the Expressway-E | UDP      | 3478                      | 3478         |
| UDP media if it is sent via the Expressway-E                    | UDP      | 1024-65535                | 24000-29999  |

### Between B2BUA and transcoder

| Purpose  | Protocol | B2BUA IP port | Transcoder |
|--|----------|---------------|------------|
| B2BUA communications with transcoder (Cisco AM GW) | TLS      | 65080         | 5061       |

# Regular expressions

Regular expressions can be used in conjunction with a number of Expressway features such as alias transformations, zone transformations, CPL policy and ENUM. The Expressway uses POSIX format regular expression syntax. The table below provides a list of commonly used special characters in regular expression syntax. This is only a subset of the full range of expressions available. For a detailed description of regular expression syntax see the publication *Regular Expression Pocket Reference*.

| Character | Description   | Example   |
|-----------|---|---|
| .         | Matches any single character.   |   |
| \d        | Matches any decimal digit, i.e. 0-9.  |   |
| *         | Matches 0 or more repetitions of the previous character or expression.  | . * matches against any sequence of characters  |
| +         | Matches 1 or more repetitions of the previous character or expression.  |   |
| ?         | Matches 0 or 1 repetitions of the previous character or expression.   | 9?123 matches against 9123 and 123  |
| {n}       | Matches n repetitions of the previous character or expression   | \d{3} matches 3 digits  |
| {n,m}     | Matches n to m repetitions of the previous character or expression  | \d{3,5} matches 3, 4 or 5 digits  |
| [...]     | Matches a set of specified characters. Each character in the set can be specified individually, or a range can be specified by giving the first character in the range followed by the - character and then the last character in the range.<br><br>You cannot use special characters within the [] - they will be taken literally.                   | [a-z] matches any alphabetical character<br>[0-9#*] matches against any single E.164 character - the E.164 character set is made up of the digits 0-9 plus the hash key (#) and the asterisk key (*)  |
| [^...]    | Matches anything except the set of specified characters. Each character in the set can be specified individually, or a range can be specified by giving the first character in the range followed by the - character and then the last character in the range.<br><br>You cannot use special characters within the [] - they will be taken literally. | [^a-z] matches any non-alphabetical character<br>[^0-9#*] matches anything other than the digits 0-9, the hash key (#) and the asterisk key (*)   |
| (...)     | Groups a set of matching characters together. Groups can then be referenced in order using the characters \1, \2, etc. as part of a replace string.   | A regular expression can be constructed to transform a URI containing a user's full name to a URI based on their initials. The regular expression (.) .*_(.) .* (@example.com) would match against the user john_smith@example.com and with a replace string of \1\2\3 would transform it to js@example.com |
|           | Matches against one expression or an alternate expression.  | .*@example.(net com) matches against any URI for the domain example.com or the domain example.net   |



|         |   |  |
|---------|---|--|
| \       | Escapes a regular expression special character.   |  |
| ^       | Signifies the start of a line.<br>When used immediately after an opening brace, negates the character set inside the brace. | [ <b>^abc</b> ] matches any single character that is NOT one of a, b or c  |
| \$      | Signifies the end of a line.  | <b>^\d\d\d\$</b> matches any string that is exactly 3 digits long  |
| (?!...) | Negative lookahead. Defines a subexpression that must not be present.   | <b>(?!.*@example.com\$) .*</b> matches any string that does not end with <b>@example.com</b><br><b>(?!alice) .*</b> matches any string that does not start with <b>alice</b> |
| (?!...) | Negative lookbehind. Defines a subexpression that must not be present.  | <b>.*(?!net)</b> matches any string that does not end with <b>net</b>  |

Note that regex comparisons are not case sensitive.

For an example of regular expression usage, see the CPL examples section.

# Supported characters

The Expressway supports the following characters when entering text in the CLI and web interface:

- the letters A-Z and a-z
- decimal digits ( 0-9 )
- underscore ( \_ )
- minus sign / hyphen ( - )
- equals sign ( = )
- plus sign ( + )
- at sign ( @ )
- comma ( , )
- period/full stop ( . )
- exclamation mark ( ! )
- spaces

The following characters are specifically not allowed:

- tabs
- angle brackets ( < and > )
- ampersand ( & )
- caret ( ^ )

Note that some specific text fields (including [Administrator](#) groups) have different restrictions and these are noted in the relevant sections of this guide.

## Case sensitivity

Text items entered through the CLI and web interface are case insensitive. The only exceptions are passwords and local administrator account names which are case sensitive.

# Call types and licensing

This section describes the different call types recognized by the Expressway and how they are licensed.

## Call types

The Expressway distinguishes between the following 2 types of call:

- **Unified CM remote sessions:** these are "mobile and remote access" calls i.e. video or audio calls from devices located outside the enterprise that are routed via the Expressway firewall traversal solution to endpoints registered to Unified CM. These calls do not require rich media session licenses, although they do contribute to overall load.
- **Rich media sessions:** these calls consume rich media session licenses and consist of every other type of video or audio call that is routed through the Expressway. This includes business-to-business calls, B2BUA calls, and interworked or gatewayed calls to third-party solutions. The Expressway may take the media (traversal) or just the signaling (non-traversal).  
Audio-only SIP traversal calls are treated distinctly from video SIP traversal calls. Each rich media session license allows either 1 video call or 2 audio-only SIP traversal calls. Hence, a 100 rich media session license would allow, for example, 90 video and 20 SIP audio-only simultaneous calls. Any other audio-only call (non-traversal, H.323 or interworked) will consume a rich media session license.

Both types of call contribute to the overall load on the system.

Note that:

- Expressway defines an "audio-only" SIP call as one that was negotiated with a single "m=" line in the SDP. Thus, for example, if a person makes a "telephone" call but the SIP UA includes an additional m= line in the SDP, the call will consume a video call license.
- While an "audio-only" SIP call is being established, it is treated (licensed) as a video call. It only becomes licensed as "audio-only" when the call setup has completed. This means that if your system approaches its maximum licensed limit, you may be unable to connect some "audio-only" calls if they are made simultaneously.

## What are traversal calls?

A traversal call is any call passing through the Expressway that includes both the signaling (information about the call) and media (voice and video). The only other type of call is a non-traversal call, where the signaling passes through the Expressway but the media goes directly between the endpoints (or between one endpoint and another system in the call route).

A call is "traversal" or "non-traversal" from the point of view of the Expressway through which it is being routed at the time. Traversal calls use more resource than non-traversal calls.


The following types of calls require the Expressway to take the media. They are classified as traversal calls and always pass through the Traversal Subzone:

- Unified CM remote sessions (these do not require a rich media session license)
- all other firewall traversal calls that are not Unified CM remote sessions, where the local Expressway is either the traversal client or traversal server
- calls that are gatewayed (interworked) between H.323 and SIP on the local Expressway
- calls that are gatewayed (interworked) between IPv4 and IPv6 on the local Expressway

- for an Expressway-E with Advanced Networking enabled, calls that are inbound from one LAN port and outbound on the other
- a SIP to SIP call when one of the participants is behind a NAT (unless both endpoints are using ICE for NAT traversal)
- calls that invoke the B2BUA to apply a media encryption policy or for ICE messaging support

# Alarms

Alarms occur when an event or configuration change has taken place on the Expressway that requires some manual administrator intervention, such as a restart. Alarms may also be raised for hardware and environmental issues such as faulty disks and fans or high temperatures.

The **Alarms** page (**Status > Alarms**) provides a list of all the alarms currently in place on your system (and, where applicable, their proposed resolution). When there are unacknowledged alarms in place on the Expressway, an alarm icon  appears at the top right of all pages. You can also access the **Alarms** page by clicking on the alarm icon.

Each alarm is identified by a 5-digit **Alarm ID**, shown in the rightmost column in the alarms list. The alarms are grouped into categories as follows:

| Alarm ID prefix | Category  |
|-----------------|---|
| 10nnn           | Hardware issues   |
| 15nnn           | Software issues   |
| 20nnn           | Cluster-related issues  |
| 25nnn           | Network and network services settings   |
| 30nnn           | Licensing / resources / option keys   |
| 35nnn           | External applications and services (such as policy services or LDAP/AD configuration) |
| 40nnn           | Security issues (such as certificates, passwords or insecure configuration)           |
| 45nnn           | General Expressway configuration issues   |
| 55nnn           | B2BUA issues  |
| 6nnnn           | Fusion issues   |

All alarms raised on the Expressway are also raised as Cisco TMS tickets. All the attributes of an alarm (its ID, severity and so on) are included in the information sent to Cisco TMS.

## List of alarms

The following table lists the alarms that can be raised on the Expressway.

| ID    | Title            | Description           | Solution   | Severity |
|-------|------------------|-----------------------|--|----------|
| 10001 | Hardware failure | <problem description> |  | Critical |
| 10002 | RAID degraded    | <problem description> | Follow your Cisco RMA process to obtain replacement parts, and then see 'Cisco UCS C220 Server Installation and Service Guide' for information about how to replace server components. | Critical |

| ID    | Title                              | Description  | Solution   | Severity |
|-------|------------------------------------|--|--|----------|
| 10003 | PSU redundancy lost                | <problem description>  | Follow your Cisco RMA process to obtain replacement parts, and then see 'Cisco UCS C220 Server Installation and Service Guide' for information about how to replace server components. | Critical |
| 10004 | RAID rebuilding                    | <problem description>  | Wait for the rebuild to complete. On successful completion, all RAID-related alarms will be automatically lowered.   | Critical |
| 15004 | Application failed                 | An unexpected software error was detected in <module>  | View the <a href="#">incident reporting</a> page   | Error    |
| 15005 | Database failure                   | Please remove database and restore from backup, then reboot the system   | <a href="#">Reboot the system</a>  | Warning  |
| 15007 | The system is busy                 | The system is shutting down, or starting   |  | Alert    |
| 15008 | Failed to load database            | The database failed to load; some configuration data has been lost   | <a href="#">Restore</a> system data from backup  | Warning  |
| 15009 | Factory reset started              | Factory reset started  |  | Alert    |
| 15010 | Application failed                 | An unexpected software error was detected in <module>  | View the <a href="#">incident reporting</a> page   | Error    |
| 15011 | Application failed                 | An unexpected software error was detected in <module>  | View the <a href="#">incident reporting</a> page   | Error    |
| 15012 | Language pack mismatch             | Some text labels may not be translated   | Contact your Cisco representative to see if an up-to-date language pack is available   | Warning  |
| 15013 | Factory reset failed               | Factory reset failed   |  | Alert    |
| 15014 | Restart required                   | Core dump mode has been changed, however a restart is required for this to take effect   | <a href="#">Restart the system</a>   | Warning  |
| 15015 | Maintenance mode                   | The Expressway is in Maintenance mode and will no longer accept calls  |  | Warning  |
| 15016 | Directory service database failure | The directory service database is not running  | <a href="#">Restart the system</a>   | Warning  |
| 15017 | Application failed                 | The OpenDS service has stopped unexpectedly and has been restarted   | If the problem persists, contact your Cisco representative   | Warning  |
| 15018 | Boot selection mismatch            | Booted system does not match expected configuration; this may be caused by user input or spurious characters on the serial console during the boot | <a href="#">Reboot the system</a>  | Critical |
| 15019 | Application failed                 | An unexpected software error was detected in <details>   | Restart the system; if the problem persists, contact your Cisco support representative   | Critical |

| ID    | Title                                  | Description  | Solution   | Severity |
|-------|--|--|--|----------|
| 20003 | Invalid cluster configuration          | The cluster configuration is invalid   | Check the <a href="#">Clustering</a> page and ensure that this system's IP address is included and there are no duplicate IP addresses | Warning  |
| 20004 | Cluster communication failure          | The system is unable to communicate with one or more of the cluster peers  | Check the <a href="#">clustering</a> configuration   | Warning  |
| 20005 | Invalid peer address                   | One or more peer addresses are invalid   | Check the <a href="#">Clustering</a> page and ensure that all Peer fields use a valid IP address                                       | Warning  |
| 20006 | Cluster database communication failure | The database is unable to replicate with one or more of the cluster peers  | Check the <a href="#">clustering</a> configuration and restart   | Warning  |
| 20007 | Restart required                       | Cluster configuration has been changed, however a restart is required for this to take effect                            | <a href="#">Restart the system</a>   | Warning  |
| 20008 | Cluster replication error              | Automatic replication of configuration has been temporarily disabled because an upgrade is in progress                   | Please wait until the upgrade has completed  | Warning  |
| 20009 | Cluster replication error              | There was an error during automatic replication of configuration   | View <a href="#">cluster replication instructions</a>  | Warning  |
| 20010 | Cluster replication error              | The NTP server is not configured   | Configure an NTP server  | Warning  |
| 20011 | Cluster replication error              | This peer's configuration conflicts with the master's configuration, manual synchronization of configuration is required | View <a href="#">cluster replication instructions</a>  | Warning  |
| 20012 | Cluster replication error              | This peer's cluster configuration settings do not match the configuration master peer's settings                         | Configure this peer's <a href="#">cluster settings</a>   | Warning  |
| 20014 | Cluster replication error              | Cannot find master or this peer's configuration file, manual synchronization of configuration is required                | View <a href="#">cluster replication instructions</a>  | Warning  |
| 20015 | Cluster replication error              | The local Expressway does not appear in the list of peers  | Check the <a href="#">list of peers</a> for this cluster   | Warning  |
| 20016 | Cluster replication error              | The master peer is unreachable   | Check the <a href="#">list of peers</a> for this cluster   | Warning  |
| 20017 | Cluster replication error              | Configuration master ID is inconsistent, manual synchronization of configuration is required                             | View <a href="#">cluster replication instructions</a>  | Warning  |
| 20018 | Invalid clustering configuration       | H.323 mode must be turned On - clustering uses H.323 communications between peers  | Configure <a href="#">H.323 mode</a>   | Warning  |

| ID    | Title                          | Description   | Solution   | Severity |
|-------|--------------------------------|---|--|----------|
| 20019 | Cluster name not configured    | If clustering is in use a cluster name must be defined.   | Configure the <a href="#">cluster name</a>   | Warning  |
| 25001 | Restart required               | Network configuration has been changed, however a restart is required for this to take effect   | <a href="#">Restart the system</a>   | Warning  |
| 25002 | Date and time not validated    | The system is unable to obtain the correct time and date from an NTP server   | Check the <a href="#">time configuration</a>   | Warning  |
| 25003 | IP configuration mismatch      | IP protocol is set to both IPv4 and IPv6, but the system does not have any IPv4 addresses defined   | Configure <a href="#">IP settings</a>  | Warning  |
| 25004 | IP configuration mismatch      | IP protocol is set to both IPv4 and IPv6, but the system does not have an IPv4 gateway defined  | Configure <a href="#">IP settings</a>  | Warning  |
| 25006 | Restart required               | Advanced Networking option key has been changed, however a restart is required for this to take effect  | Configure your required LAN and static NAT settings on the <a href="#">IP</a> page and then <a href="#">restart the system</a> . | Warning  |
| 25007 | Restart required               | QoS settings have been changed, however a restart is required for this to take effect   | <a href="#">Restart the system</a>   | Warning  |
| 25008 | Restart required               | Port configuration has been changed, however a restart is required for this to take effect  | <a href="#">Restart the system</a>   | Warning  |
| 25009 | Restart required               | Ethernet configuration has been changed, however a restart is required for this to take effect  | <a href="#">Restart the system</a>   | Warning  |
| 25010 | Restart required               | IP configuration has been changed, however a restart is required for this to take effect  | <a href="#">Restart the system</a>   | Warning  |
| 25011 | Restart required               | HTTPS service has been changed, however a restart is required for this to take effect   | <a href="#">Restart the system</a>   | Warning  |
| 25013 | IP configuration mismatch      | IP protocol is set to both IPv4 and IPv6, but the system does not have an IPv6 gateway defined  | Configure <a href="#">IP settings</a>  | Warning  |
| 25014 | Configuration warning          | IP protocol is set to both IPv4 and IPv6, but the Expressway does not have any IPv6 addresses defined   | Configure <a href="#">IP settings</a>  | Warning  |
| 25015 | Restart required               | SSH service has been changed, however a restart is required for this to take effect   | <a href="#">Restart the system</a>   | Warning  |
| 25016 | Ethernet speed not recommended | An Ethernet interface speed setting has been negotiated to a value other than 1000Mb/s full duplex or 100Mb/s full duplex; this may result in packet loss over your network | Configure <a href="#">Ethernet</a> parameters  | Warning  |



| ID    | Title                                     | Description   | Solution  | Severity |
|-------|---|---|---|----------|
| 25017 | Restart required                          | HTTP service has been changed, however a restart is required for this to take effect                        | <a href="#">Restart the system</a>  | Warning  |
| 25018 | Port conflict                             | There is a port conflict between <function> <port> and <function> <port>                                    | Review the port configuration on the <a href="#">Local inbound ports</a> and <a href="#">Local outbound ports</a> pages   | Warning  |
| 25019 | Verbose log levels configured             | One or more modules of the Network Log or Support Log are set to a level of Debug or Trace                  | <a href="#">Network Log</a> and <a href="#">Support Log</a> modules should be set to a level of Info, unless advised otherwise by your Cisco support representative. If diagnostic logging is in progress they will be reset automatically when diagnostic logging is stopped | Warning  |
| 25020 | NTP client failure                        | The system is unable to run the NTP client  | Check <a href="#">NTP status</a> information, including any key configuration and expiry dates  | Warning  |
| 25021 | NTP server not available                  | The system is unable to contact an NTP server   | Check <a href="#">Time</a> configuration and status; check <a href="#">DNS</a> configuration  | Warning  |
| 25022 | Time not synchronized over traversal zone | The system time of this server is different from that on a server on the other side of a SIP traversal zone | Ensure that your systems have consistent Time configuration; note that any changes may take some time to become effective   | Warning  |
| 30001 | Capacity warning                          | The number of concurrent traversal calls has approached the licensed limit                                  | Contact your Cisco representative   | Warning  |
| 30002 | Capacity warning                          | The number of concurrent traversal calls has approached the unit's physical limit                           | Contact your Cisco representative   | Warning  |
| 30003 | Capacity warning                          | The number of concurrent non-traversal calls has approached the unit's physical limit                       | Contact your Cisco representative   | Warning  |
| 30005 | Capacity warning                          | TURN relays usage has approached the unit's physical limit  | Contact your Cisco representative   | Warning  |
| 30006 | Restart required                          | The release key has been changed, however a restart is required for this to take effect                     | <a href="#">Restart the system</a>  | Warning  |
| 30007 | Capacity warning                          | TURN relays usage has approached the licensed limit   | Contact your Cisco representative   | Warning  |
| 30008 | Invalid release key                       | The release key is not valid; if you do not have a valid key, contact your Cisco support representative     | Add/Remove <a href="#">option keys</a>  | Warning  |
| 30009 | TURN relays installed                     | TURN services are only available on Expressway-E; TURN option key ignored                                   | Add/Remove <a href="#">option keys</a>  | Warning  |
| 30011 | TURN relay licenses required              | TURN services are enabled but no TURN relay license option keys are installed                               | Add <a href="#">option key</a> or disable <a href="#">TURN services</a>   | Warning  |

| ID    | Title  | Description   | Solution   | Severity |
|-------|--|---|--|----------|
| 30012 | License usage of lost cluster peer                                 | Cluster peer <n> has been unavailable for more than <n> hours. Its licenses will be removed from the total available for use across the cluster on <date>.                      | Resolve the issue with this peer, or remove it from the cluster configuration                            | Warning  |
| 30013 | License usage of lost cluster peer                                 | Several cluster peers have been unavailable for more than <n> hours. Their licenses will be removed from the total available for use across the cluster as follows: <details>.  | Resolve the issue with this peer, or remove it from the cluster configuration                            | Warning  |
| 30014 | License usage of lost cluster peer                                 | Cluster peer <n> has been unavailable for more than <n> days. Its licenses will be removed from the total available for use across the cluster on <date>.                       | Resolve the issue with this peer, or remove it from the cluster configuration                            | Warning  |
| 30015 | License usage of lost cluster peer                                 | Several cluster peers have been unavailable for more than <n> days. Their licenses will be removed from the total available for use across the cluster as follows: <details>.   | Resolve the issue with this peer, or remove it from the cluster configuration                            | Warning  |
| 30016 | Licenses of lost cluster peer have been taken off the license pool | Cluster peer <n> has been unavailable for more than <n> days. Its licenses have been removed from the total available for use across the cluster on <date>.                     | Resolve the issue with this peer, or remove it from the cluster configuration                            | Warning  |
| 30017 | Licenses of lost cluster peer have been taken off the license pool | Several cluster peers have been unavailable for more than <n> days. Their licenses have been removed from the total available for use across the cluster as follows: <details>. | Resolve the issue with this peer, or remove it from the cluster configuration                            | Warning  |
| 30018 | Provisioning licenses limit reached                                | The number of concurrently provisioned devices has reached the licensed limit   | Provisioning limits are set by Cisco TMS; contact your Cisco representative if you require more licenses | Warning  |
| 30020 | Call license limit reached   | You have reached your license limit of <n> concurrent traversal call licenses   | If the problem persists, contact your Cisco representative to buy more call licenses                     | Warning  |
| 30021 | TURN relay license limit reached                                   | You have reached your license limit of <n> concurrent TURN relay licenses   | If the problem persists, contact your Cisco representative to buy more TURN relay licenses               | Warning  |
| 30022 | Call capacity limit reached  | The number of concurrent non-traversal calls has reached the unit's physical limit  | Add more capacity to your system; contact your Cisco representative                                      | Warning  |
| 30023 | Call capacity limit reached  | The number of concurrent traversal calls has reached the unit's physical limit  | Add more capacity to your system; contact your Cisco representative                                      | Warning  |
| 30024 | TURN relay capacity limit reached                                  | The number of concurrent TURN relay calls has reached the unit's physical limit   | Add more capacity to your system; contact your Cisco representative                                      | Warning  |

| ID    | Title   | Description   | Solution   | Severity |
|-------|---|---|--|----------|
| 30025 | Restart required  | An option key has been changed, however a restart is required for this to take effect   | <a href="#">Restart the system</a>   | Warning  |
| 35001 | Configuration warning                                     | Active Directory mode has been enabled but the DNS hostname has not been configured   | Configure <a href="#">DNS hostname</a>   | Warning  |
| 35002 | Configuration warning                                     | Active Directory mode has been enabled but the NTP server has not been configured   | Configure <a href="#">NTP server</a>   | Warning  |
| 35003 | Configuration warning                                     | Active Directory mode has been enabled but no DNS servers have been configured  | Configure a <a href="#">DNS server</a>   | Warning  |
| 35004 | LDAP configuration required                               | Remote login authentication is in use for administrator accounts but a valid LDAP Server address, Port, Bind_DN and Base_DN have not been configured  | Configure <a href="#">LDAP parameters</a>  | Warning  |
| 35005 | Configuration warning                                     | Active Directory mode has been enabled but a domain has not been configured   | Configure domain on Active Directory Service page  | Warning  |
| 35007 | Configuration warning                                     | Active Directory SPNEGO disabled; you are recommended to enable the SPNEGO setting  | Enable SPNEGO  | Warning  |
| 35008 | Configuration warning                                     | Active Directory mode has been enabled but a workgroup has not been configured  | Configure workgroup on Active Directory Service page   | Warning  |
| 35009 | TMS Provisioning Extension services communication failure | The Expressway is unable to communicate with the TMS Provisioning Extension services. Phone book service failures can also occur if TMS does not have any users provisioned against this cluster. | Go to the TMS Provisioning Extension service status page and select the failed service to view details about the problem   | Warning  |
| 35010 | TMS Provisioning Extension services data import failure   | An import from the TMS Provisioning Extension services has been canceled as it would cause the Expressway to exceed internal table limits   | See the Expressway Event Log for details, then check the corresponding data within TMS; you must perform a full synchronization after the data has been corrected in TMS | Warning  |
| 35011 | TMS Provisioning Extension services data import failure   | One or more records imported from the TMS Provisioning Extension services have been dropped due to unrecognized data format   | See the Expressway Event Log for details, then check the corresponding data within TMS; you must perform a full synchronization after the data has been corrected in TMS | Warning  |
| 35012 | Failed to connect to LDAP server                          | Failed to connect to the LDAP server for H.350 device authentication  | Ensure that your H.350 directory service is correctly configured   | Warning  |

| ID    | Title  | Description   | Solution   | Severity |
|-------|--|---|--|----------|
| 35013 | Unified Communications SSH tunnel failure              | This system cannot communicate with one or more remote hosts  | Review the Event Log and check that the traversal zone between the Expressway-C and the Expressway-E is active   | Warning  |
| 35014 | Unified Communications SSH tunnel notification failure | This system cannot communicate with one or more remote hosts  | Ensure that your firewall allows traffic from the Expressway-C ephemeral ports to 2222 TCP on the Expressway-E   | Warning  |
| 35015 | Unified CM port conflict                               | There is a port conflict on Unified CM <name> between neighbor zone <name> and Unified Communications (both are using port <number>)  | The same port on Unified CM cannot be used for line side (Unified Communications) and SIP trunk traffic. Review the port configuration on Unified CM and reconfigure the <zone> if necessary | Warning  |
| 35016 | SAML metadata has been modified                        | Configuration changes have modified the local SAML metadata, which is now different to any copies on Identity Provider(s). This metadata may have been modified by changing the server certificate or the SSO-enabled domains, or by changing the number of traversal server peers or their addresses | Export the SAML metadata so you can import it on the Identity Provider   | Warning  |
| 40001 | Security alert   | No CRL distribution points have been defined for automatic updates  | Check <a href="#">CRL configuration</a>  | Warning  |
| 40002 | Security alert   | Automatic updating of CRL files has failed  | If the problem persists, contact your Cisco representative   | Warning  |
| 40003 | Insecure password in use                               | The root user has the default password set  | View instructions on <a href="#">changing the root password</a>  | Warning  |
| 40004 | Certificate-based authentication required              | Your system is recommended to have client certificate-based security set to <i>Certificate-based authentication</i> when in advanced account security mode  | Configure <a href="#">client certificate-based security</a>  | Warning  |
| 40005 | Insecure password in use                               | The admin user has the default password set   | Change the <a href="#">admin password</a>  | Error    |
| 40006 | Security alert   | Unable to download CRL update   | Check <a href="#">CRL distribution points</a> and the <a href="#">Event Log</a>  | Warning  |
| 40007 | Security alert   | Failed to find configuration file for CRL automatic updates   | If the problem persists, contact your Cisco representative   | Warning  |
| 40008 | Security alert   | The SSH service is using the default key  | View instructions on <a href="#">replacing the default SSH key</a>   | Warning  |
| 40009 | Restart required                                       | HTTPS client certificates validation mode has changed, however a restart is required for this to take effect  | <a href="#">Restart the system</a>   | Warning  |

| ID    | Title  | Description   | Solution  | Severity |
|-------|--|---|---|----------|
| 40011 | Per-account session limit required           | A non-zero per-account session limit is required when in advanced account security mode   | Configure <a href="#">per-account session limit</a>               | Warning  |
| 40013 | HTTPS client certificate validation disabled | You are recommended to enable client side certificate validation for HTTPS connections when in advanced account security mode   | Configure <a href="#">HTTPS client certificate validation</a>     | Warning  |
| 40014 | Time out period required                     | A non-zero system session time out period is required when in advanced account security mode  | Configure <a href="#">session time out period</a>                 | Warning  |
| 40015 | System session limit required                | A non-zero system session limit is required when in advanced account security mode  | Configure <a href="#">system session limit</a>                    | Warning  |
| 40016 | Encryption required                          | Your login account LDAP server configuration is recommended to have encryption set to <i>TLS</i> when in advanced account security mode                                 | Configure <a href="#">login account LDAP server</a>               | Warning  |
| 40017 | Incident reporting enabled                   | You are recommended to disable incident reporting when in advanced account security mode  | Configure <a href="#">incident reporting</a>                      | Warning  |
| 40018 | Insecure password in use                     | One or more users has a non-strict password   |   | Warning  |
| 40020 | Security alert                               | The connection to the Active Directory Service is not using TLS encryption  | Configure Active Directory Service connection settings            | Warning  |
| 40021 | Remote logging enabled                       | You are recommended to disable the remote syslog server when in advanced account security mode  | Configure <a href="#">remote logging</a>                          | Warning  |
| 40022 | Security alert                               | Active Directory secure channel disabled; you are recommended to enable the secure channel setting  | Enable secure channel   | Warning  |
| 40024 | CRL checking required                        | Your login account LDAP server configuration is recommended to have certificate revocation list (CRL) checking set to <i>All</i> when in advanced account security mode | Configure <a href="#">login account LDAP server</a>               | Warning  |
| 40025 | SNMP enabled                                 | You are recommended to disable SNMP when in advanced account security mode  | Configure <a href="#">SNMP mode</a>                               | Warning  |
| 40026 | Reboot required                              | The advanced account security mode has changed, however a reboot is required for this to take effect  | <a href="#">Reboot the Expressway</a>                             | Warning  |
| 40027 | Security alert                               | The connection to the TMS Provisioning Extension services is not using TLS encryption   | Configure TMS Provisioning Extension services connection settings | Warning  |
| 40028 | Insecure password in use                     | The root user's password is hashed using MD5, which is not secure enough  | View instructions on <a href="#">changing the root password</a>   | Warning  |

| ID    | Title                                      | Description  | Solution  | Severity |
|-------|--|--|---|----------|
| 40029 | LDAP server CA certificate is missing      | A valid CA certificate for the LDAP database has not been uploaded; this is required for connections via TLS                                 | Upload a valid CA certificate   | Warning  |
| 40030 | Security alert                             | Firewall rules activation failed; the firewall configuration contains at least one rejected rule   | Check your <a href="#">firewall rules configuration</a> , fix any rejected rules and re-try the activation  | Warning  |
| 40031 | Security alert                             | Unable to restore previous firewall configuration  | Check your <a href="#">firewall rules configuration</a> , fix any rejected rules, activate and accept the rules; if the problem persists, contact your Cisco representative       | Warning  |
| 40032 | Security alert                             | Unable to initialize firewall  | <a href="#">Restart the system</a> ; if the problem persists, contact your Cisco representative   | Warning  |
| 40033 | Configuration warning                      | The Default Zone access rules are enabled, but leaving SIP over UDP or SIP over TCP enabled offers a way to circumvent this security feature | Either disable UDP and TCP on the <a href="#">SIP page</a> to enforce certificate identity checking using TLS, or disable the access rules for the <a href="#">Default Zone</a> . | Warning  |
| 40034 | Security alert                             | Firewall rules activation failed; the firewall configuration contains rules with duplicated priorities                                       | Check your <a href="#">firewall rules configuration</a> , ensure all rules have a unique priority and re-try the activation   | Warning  |
| 40040 | Unified Communications configuration error | TLS verify mode is not enabled on a traversal zone configured for Unified Communications services  | Ensure that TLS verify mode is enabled on the traversal zone; you may also need to check the remote traversal system  | Warning  |
| 40041 | Security alert                             | Automated intrusion protection rules are not available   | Disable and then re-enable the failed services  | Warning  |
| 40043 | Unified Communications configuration error | Media encryption is not enforced on a traversal zone configured for Unified Communications services  | Ensure that media encryption is set to 'Force encrypted' on the traversal zone  | Warning  |
| 40048 | Unified Communications configuration error | Unified Communications services are enabled but SIP TLS is disabled  | Ensure that SIP TLS mode is set to 'On' on SIP configuration page   | Warning  |
| 40100 | Security alert                             | Firewall rules are not synchronized with network interfaces  | <a href="#">Restart the system</a> ; if the problem persists, contact your Cisco representative   | Warning  |
| 45001 | Failed to load Call Policy file            | <failure details>  | Configure <a href="#">Call Policy</a>   | Warning  |
| 45002 | Configuration warning                      | Expected default link between the Default Subzone and the Default Zone is missing  | Configure <a href="#">default links</a>   | Warning  |

| ID    | Title                          | Description  | Solution   | Severity |
|-------|--------------------------------|--|--|----------|
| 45003 | Configuration warning          | H.323 and SIP modes are set to Off; one or both of them should be enabled  | Configure <a href="#">H.323</a> and/or <a href="#">SIP</a> modes   | Warning  |
| 45005 | Configuration conflict         | H323-SIP Protocol Interworking mode is enabled but the H323-SIP Interworking Gateway option key has been deleted                           | Reconfigure <a href="#">Interworking mode</a> or <a href="#">reinstall the option key</a>                                | Warning  |
| 45006 | Configuration warning          | Expected default link between the Default Subzone and the Cluster Subzone is missing   | Configure <a href="#">default links</a>  | Warning  |
| 45007 | Configuration warning          | Expected default link between the Default Subzone and the Traversal Subzone is missing   | Configure <a href="#">default links</a>  | Warning  |
| 45008 | Configuration warning          | Expected default link between the Traversal Subzone and the Default Zone is missing  | Configure <a href="#">default links</a>  | Warning  |
| 45014 | Configuration warning          | H.323 is enabled in a zone with a SIP media encryption mode of "Force encrypted" or "Force unencrypted"                                    | On the relevant zone, either disable H.323 or select a different SIP media encryption mode                               | Warning  |
| 45016 | Configuration warning          | A zone has a SIP media encryption mode of "Best effort" or "Force encrypted" but the transport is not TLS. TLS is required for encryption. | On the relevant zone, either set the SIP transport to TLS or select a different SIP media encryption mode                | Warning  |
| 45018 | Configuration warning          | DNS zones (including <zone_name>) have their SIP default transport protocol set to <protocol>, but that protocol is disabled system-wide.  | Check that the SIP default transport protocol for the DNS zone and the system-wide SIP transport settings are consistent | Warning  |
| 45019 | Insufficient media ports       | There is an insufficient number of media ports to support the number of licensed calls   | Increase the media port range  | Warning  |
| 55001 | B2BUA service restart required | Some B2BUA service specific configuration has changed, however a restart is required for this to take effect                               | <a href="#">Restart the B2BUA service</a>  | Warning  |
| 55002 | B2BUA misconfiguration         | The port on B2BUA for Expressway communications is misconfigured   | Check <a href="#">B2BUA configuration</a> (advanced settings)  | Warning  |
| 55003 | B2BUA misconfiguration         | Invalid trusted host IP address of Lync device   | Check configured <a href="#">addresses of trusted hosts</a>  | Warning  |
| 55004 | B2BUA misconfiguration         | The port on B2BUA for Lync communications is misconfigured   | Check <a href="#">B2BUA configuration</a> (advanced settings)  | Warning  |
| 55005 | B2BUA misconfiguration         | The Lync signaling destination address is misconfigured  | Check <a href="#">B2BUA configuration</a>  | Warning  |
| 55005 | B2BUA misconfiguration         | The Lync signaling destination address is misconfigured  | Check <a href="#">B2BUA configuration</a>  | Warning  |
| 55006 | B2BUA misconfiguration         | The Lync signaling destination port is misconfigured   | Check <a href="#">B2BUA configuration</a>  | Warning  |
| 55007 | B2BUA misconfiguration         | The Lync transport type is misconfigured   | Check <a href="#">B2BUA configuration</a>  | Warning  |

| ID    | Title                  | Description   | Solution  | Severity |
|-------|------------------------|---|---|----------|
| 55008 | B2BUA misconfiguration | Missing or invalid FQDN of service  | Check the Expressway's <a href="#">system host name and domain name</a>   | Warning  |
| 55009 | B2BUA misconfiguration | Invalid IP address of service   | Check the Expressway's <a href="#">LAN 1 IPv4 address</a>   | Warning  |
| 55010 | B2BUA misconfiguration | The B2BUA media port range end value is misconfigured                                       | Check <a href="#">B2BUA configuration</a> (advanced settings)   | Warning  |
| 55011 | B2BUA misconfiguration | The B2BUA media port range start value is misconfigured                                     | Check <a href="#">B2BUA configuration</a> (advanced settings)   | Warning  |
| 55012 | B2BUA misconfiguration | Invalid Microsoft Lync B2BUA mode   | Check <a href="#">B2BUA configuration</a>   | Warning  |
| 55013 | B2BUA misconfiguration | Invalid option key  | Check <a href="#">option keys</a>   | Warning  |
| 55014 | B2BUA misconfiguration | Invalid hop count   | Check <a href="#">B2BUA configuration</a> (advanced settings)   | Warning  |
| 55015 | B2BUA misconfiguration | Invalid trusted host IP address of transcoder   | Check configured <a href="#">addresses of trusted hosts</a>   | Warning  |
| 55016 | B2BUA misconfiguration | The setting to enable transcoders for this B2BUA is misconfigured                           | Check <a href="#">B2BUA configuration</a> (transcoder settings)   | Warning  |
| 55017 | B2BUA misconfiguration | The port on B2BUA for transcoder communications is misconfigured                            | Check <a href="#">B2BUA configuration</a> (transcoder settings)   | Warning  |
| 55018 | B2BUA misconfiguration | Transcoder address and/or port details are misconfigured                                    | Check <a href="#">B2BUA configuration</a> (transcoder settings) and the configured <a href="#">addresses of trusted hosts</a> | Warning  |
| 55019 | B2BUA misconfiguration | Invalid TURN server address   | Check <a href="#">B2BUA configuration</a> (TURN settings)   | Warning  |
| 55021 | B2BUA misconfiguration | The setting to offer TURN services for this B2BUA is misconfigured                          | Check <a href="#">B2BUA configuration</a> (TURN settings)   | Warning  |
| 55023 | B2BUA misconfiguration | The transcoder policy rules are misconfigured   | Check <a href="#">transcoder policy rules</a> configuration   | Warning  |
| 55024 | B2BUA misconfiguration | The setting to use transcoder policy rules is misconfigured                                 | Check <a href="#">B2BUA configuration</a> (transcoder settings)   | Warning  |
| 55025 | B2BUA misconfiguration | The B2BUA has been enabled to use transcoders, but there are no transcoders configured      | Configure one or more <a href="#">transcoders</a>   | Warning  |
| 55026 | B2BUA misconfiguration | TURN services are enabled, but there are no valid TURN servers configured                   | Configure the <a href="#">TURN server address</a>   | Warning  |
| 55028 | B2BUA misconfiguration | The start and end media port ranges are misconfigured                                       | Check the <a href="#">B2BUA media port range</a> settings   | Warning  |
| 55029 | B2BUA misconfiguration | The media port ranges used by the B2BUA overlap with the media port ranges used by <module> | Check the port configuration for both services  | Warning  |



| ID    | Title                      | Description   | Solution  | Severity |
|-------|----------------------------|---|---|----------|
| 55030 | B2BUA misconfiguration     | The port used by the B2BUA for Expressway communications is also used by <module> | Check the port configuration for both services  | Warning  |
| 55031 | B2BUA misconfiguration     | The port used by the B2BUA for Lync communications is also used by <module>       | Check the port configuration for both services  | Warning  |
| 55032 | B2BUA misconfiguration     | The port used by the B2BUA for transcoder communications is also used by <module> | Check the port configuration for both services  | Warning  |
| 55033 | B2BUA misconfiguration     | No valid Lync trusted host devices have been configured                           | Configure at least one <a href="#">Lync trusted host device</a>   | Warning  |
| 55034 | B2BUA misconfiguration     | No valid transcoder trusted hosts have been configured                            | Configure at least one <a href="#">transcoder trusted host</a>  | Warning  |
| 55035 | B2BUA connectivity problem | The B2BUA cannot connect to the transcoders                                       | <a href="#">Restart the B2BUA service</a>   | Warning  |
| 55036 | B2BUA connectivity problem | The B2BUA cannot connect to the Expressway  | <a href="#">Restart the B2BUA service</a>   | Warning  |
| 55037 | B2BUA connectivity problem | The B2BUA cannot connect to Lync  | Check the <a href="#">Lync B2BUA status</a> page for more information about the problem; you will then need to <a href="#">restart the B2BUA service</a> after making any configuration changes | Warning  |
| 55101 | B2BUA misconfiguration     | Invalid Expressway authorized host IP address                                     | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists   | Warning  |
| 55102 | B2BUA misconfiguration     | Invalid URI format of Expressway contact address                                  | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists   | Warning  |
| 55103 | B2BUA misconfiguration     | Invalid Expressway encryption mode  | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists   | Warning  |
| 55104 | B2BUA misconfiguration     | Invalid Expressway ICE mode   | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists   | Warning  |
| 55105 | B2BUA misconfiguration     | Invalid Expressway next hop host configuration                                    | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists   | Warning  |
| 55106 | B2BUA misconfiguration     | Invalid Expressway next hop liveness mode   | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists   | Warning  |
| 55107 | B2BUA misconfiguration     | Invalid Expressway next hop mode  | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists   | Warning  |

| ID    | Title                  | Description   | Solution  | Severity |
|-------|------------------------|---|---|----------|
| 55108 | B2BUA misconfiguration | Invalid Expressway next hop port                          | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55109 | B2BUA misconfiguration | Invalid Expressway transport type                         | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55110 | B2BUA misconfiguration | Invalid URI format of B side contact address              | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55111 | B2BUA misconfiguration | Invalid B side encryption mode                            | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55112 | B2BUA misconfiguration | Invalid B side ICE mode                                   | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55113 | B2BUA misconfiguration | Invalid B side next hop liveness mode                     | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55114 | B2BUA misconfiguration | Invalid B side next hop mode                              | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55115 | B2BUA misconfiguration | Invalid command listening port                            | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55116 | B2BUA misconfiguration | Invalid debug status path                                 | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55117 | B2BUA misconfiguration | Invalid service   | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55118 | B2BUA misconfiguration | Invalid software string                                   | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55119 | B2BUA misconfiguration | Invalid URI format of transcoding service contact address | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55120 | B2BUA misconfiguration | Invalid transcoding service encryption mode               | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55121 | B2BUA misconfiguration | Invalid transcoding service ICE mode                      | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |
| 55122 | B2BUA misconfiguration | Invalid transcoding service next hop liveness mode        | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists | Warning  |

| ID    | Title                       | Description  | Solution   | Severity |
|-------|-----------------------------|--|--|----------|
| 55123 | B2BUA misconfiguration      | The transcoding service transport type is misconfigured  | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists  | Warning  |
| 55124 | B2BUA misconfiguration      | The mandatory TURN server setting is misconfigured   | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists  | Warning  |
| 55125 | B2BUA misconfiguration      | Invalid Expressway next hop host configuration   | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists  | Warning  |
| 55126 | B2BUA misconfiguration      | Invalid Expressway authorized host IP address  | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists  | Warning  |
| 55127 | B2BUA misconfiguration      | Cannot start B2BUA application because FQDN configuration is missing   | Configure the <b>System host name</b> and <b>Domain name</b> on the <a href="#">DNS</a> page, and then <a href="#">restart the B2BUA service</a> | Warning  |
| 55128 | B2BUA misconfiguration      | Cannot start B2BUA application because IPv4 interface address configuration is missing   | Configure the LAN 1 IPv4 address on the <a href="#">IP</a> page, and then <a href="#">restart the B2BUA service</a>                              | Warning  |
| 55129 | B2BUA misconfiguration      | Cannot start B2BUA application because cluster name configuration is missing   | Configure the cluster name on the <a href="#">Clustering</a> page  | Warning  |
| 55130 | B2BUA misconfiguration      | Invalid cluster name   | Check the cluster name and then <a href="#">restart the B2BUA service</a>  | Warning  |
| 55131 | B2BUA misconfiguration      | Invalid session refresh interval   | Check <a href="#">B2BUA configuration</a> (advanced settings), then <a href="#">restart the B2BUA service</a>                                    | Warning  |
| 55132 | B2BUA misconfiguration      | Invalid call resource limit  | <a href="#">Restart the service</a> ; contact your Cisco representative if the problem persists  | Warning  |
| 55133 | B2BUA misconfiguration      | The B2BUA session refresh interval is smaller than the minimum session refresh interval  | Check both settings on the <a href="#">B2BUA configuration</a> (advanced settings) and then <a href="#">restart the B2BUA service</a>            | Warning  |
| 55134 | B2BUA misconfiguration      | Invalid minimum session refresh interval   | Check <a href="#">B2BUA configuration</a> (advanced settings), then <a href="#">restart the B2BUA service</a>                                    | Warning  |
| 55135 | B2BUA configuration warning | A large number of Lync trusted host devices have been configured; this may impact performance, or in extreme cases it may prevent calls from accessing enough network resources to connect | Review your network topology and try lowering the number of trusted host devices on the <a href="#">B2BUA trusted hosts</a> page.                | Warning  |

## Command reference — xConfiguration

The **xConfiguration** group of commands are used to set and change individual items of configuration. Each command is made up of a main element followed by one or more sub-elements.

To obtain information about existing configuration, type:

- **xConfiguration** to return all current configuration settings
- **xConfiguration <element>** to return configuration for that element and all its sub-elements
- **xConfiguration <element> <subelement>** to return configuration for that sub-element

To obtain information about using each of the **xConfiguration** commands, type:

- **xConfiguration ?** to return a list of all elements available under the **xConfiguration** command
- **xConfiguration ??** to return a list of all elements available under the **xConfiguration** command, along with the valuespace, description and default values for each element
- **xConfiguration <element> ?** to return all available sub-elements and their valuespace, description and default values
- **xConfiguration <element> <sub-element> ?** to return all available sub-elements and their valuespace, description and default values

To set a configuration item, type the command as shown. The valid values for each command are indicated in the angle brackets following each command, using the following notation:

Table 11: Data conventions used in the CLI reference

| Format                | Meaning  |
|-----------------------|--|
| <0..63>               | Indicates an integer value is required. The numbers indicate the minimum and maximum value. In this example the value must be in the range 0 to 63.  |
| <S: 7,15>             | An <b>S</b> indicates a string value, to be enclosed in quotation marks, is required. The numbers indicate the minimum and maximum number of characters for the string. In this example the string must be between 7 and 15 characters long.   |
| <Off/Direct/Indirect> | Lists the set of valid values. Do not enclose the value in quotation marks.  |
| [1..50]               | Square brackets indicate that you can configure more than one of this particular item. Each item is assigned an index within the range shown.<br><br>For example <b>IP Route [1..50] Address &lt;S: 0,39&gt;</b> means that up to 50 IP routes can be specified with each route requiring an address of up to 39 characters in length. |

### xConfiguration commands

All of the available **xConfiguration** commands are listed in the table below:

Table 12: xConfiguration CLI reference

|  |
|--|
| <p><b>Administration HTTP Mode: &lt;On/Off&gt;</b></p> <p>Determines whether HTTP calls will be redirected to the HTTPS port. You must restart the system for any changes to take effect. Default: On.</p> <p><i>On</i>: calls will be redirected to HTTPS.</p> <p><i>Off</i>: no HTTP access will be available.</p> <p>Example: <code>xConfiguration Administration HTTP Mode: On</code></p>  |
| <p><b>Administration HTTPS Mode: &lt;On/Off&gt;</b></p> <p>Determines whether the Expressway can be accessed via the web interface. This must be On to enable both web interface and TMS access. You must restart the system for any changes to take effect. Default: On.</p> <p>Example: <code>xConfiguration Administration HTTPS Mode: On</code></p>  |
| <p><b>Administration LCDPanel Mode: &lt;On/Off&gt;</b></p> <p>Controls whether the LCD panel on the front of the Expressway identifies the system. Default: On.</p> <p><i>On</i>: the system name and first active IP address are shown.</p> <p><i>Off</i>: the LCD panel reveals no identifying information about the system.</p> <p>Example: <code>xConfiguration Administration LCDPanel Mode: On</code></p>  |
| <p><b>Administration SSH Mode: &lt;On/Off&gt;</b></p> <p>Determines whether the Expressway can be accessed via SSH and SCP. You must restart the system for any changes to take effect. Default: On.</p> <p>Example: <code>xConfiguration Administration SSH Mode: On</code></p>   |
| <p><b>Alternates Cluster Name: &lt;S: 0,128&gt;</b></p> <p>The fully qualified domain name used in SRV records that address this Expressway cluster, for example "cluster1.example.com". The name can only contain letters, digits, hyphens and underscores.</p> <p>Warning: if you change the cluster name after any user accounts have been configured on this Expressway, you may need to reconfigure your user accounts to use the new cluster name.</p> <p>Example: <code>xConfiguration Alternates Cluster Name: "Regional"</code></p> |
| <p><b>Alternates ConfigurationMaster: &lt;1..6&gt;</b></p> <p>Specifies which peer in this cluster is the master, from which configuration will be replicated to all other peers. A cluster consists of up to 6 peers, including the local Expressway.</p> <p>Example: <code>xConfiguration Alternates ConfigurationMaster: 1</code></p>   |
| <p><b>Alternates Peer [1..6] Address: &lt;S: 0, 128&gt;</b></p> <p>Specifies the IP address of one of the peers in the cluster to which this Expressway belongs. A cluster consists of up to 6 peers, including the local Expressway. This must be a valid IPv4 or IPv6 address.</p> <p>Example: <code>xConfiguration Alternates 1 Peer Address: "10.13.0.2"</code></p>  |
| <p><b>ApacheModReqTimeOut</b></p> <p>You can set all available properties for the request timeout using a single shorthand command.</p> <p>Example: <code>xConfiguration ApacheModReqTimeout Apachehead:20 Apachebody:20 Status:On</code></p>  |
| <p><b>ApacheModReqTimeOut Apachebody: &lt;0..120&gt;</b></p> <p>Modifies the number of seconds that the Apache web server waits for the request body. If the full request body is not received before the timeout expires, Apache returns a timeout error. Default: 20.</p> <p>Example: <code>xConfiguration ApacheModReqTimeout Apachebody:20</code></p>  |

Table 12: xConfiguration CLI reference (continued)

|  |
|--|
| <p><b>ApacheModReqTimeOut Apacheheader: &lt;0..120&gt;</b></p> <p>Modifies the number of seconds that the Apache web server waits for the request header. If the full request header is not received before the timeout expires, Apache returns a timeout error. Default: 20.</p> <p>Example: <code>xConfiguration ApacheModReqTimeout Apacheheader: 20</code></p>   |
| <p><b>ApacheModReqTimeOut Status: &lt;On/Off&gt;</b></p> <p>Toggles the custom Apache request timeout. Displays the status of the timeout if you omit the switch.</p> <p><i>On:</i> The default Apache request timeout is superseded with your settings (or the defaults) for <code>Apachebody</code> and <code>Apacheheader</code>.</p> <p><i>Off:</i> <code>Apachebody</code> and <code>Apacheheader</code> have no effect. The Apache request timeout defaults to 300 seconds.</p> <p>Example: <code>xConfiguration ApacheModReqTimeout Status: On</code></p> |
| <p><b>Applications ConferenceFactory Alias: &lt;S:0,60&gt;</b></p> <p>The alias that will be dialed by the endpoints when the Multiway feature is activated. This must be pre-configured on all endpoints that may be used to initiate the Multiway feature.</p> <p>Example: <code>xConfiguration Applications ConferenceFactory Alias: "multiway@example.com"</code></p>  |
| <p><b>Applications ConferenceFactory Mode: &lt;On/Off&gt;</b></p> <p>The Mode option allows you to enable or disable the Conference Factory application. Default: Off.</p> <p>Example: <code>xConfiguration Applications ConferenceFactory Mode: Off</code></p>  |
| <p><b>Applications ConferenceFactory Range End: &lt;1..65535&gt;</b></p> <p>The last number of the range that replaces %% in the template used to generate a conference alias. Default: 65535.</p> <p>Example: <code>xConfiguration Applications ConferenceFactory Range End: 30000</code></p>   |
| <p><b>Applications ConferenceFactory Range Start: &lt;1..65535&gt;</b></p> <p>The first number of the range that replaces %% in the template used to generate a conference alias. Default: 65535.</p> <p>Example: <code>xConfiguration Applications ConferenceFactory Range Start: 10000</code></p>  |
| <p><b>Applications ConferenceFactory Template: &lt;S:0,60&gt;</b></p> <p>The alias that the Expressway will tell the endpoint to dial in order to create a Multiway conference on the MCU. This alias must route to the MCU as a fully-qualified SIP alias</p> <p>Example: <code>Applications ConferenceFactory Template: "563%%@example.com"</code></p>   |
| <p><b>Applications External Status [1..10] Filename: &lt;S:0,255&gt;</b></p> <p>XML file containing status that is to be attached for an external application.</p> <p>Example: <code>xConfiguration Applications External Status 1 Filename: "foo.xml"</code></p>  |
| <p><b>Applications External Status [1..10] Name: &lt;S:0,64&gt;</b></p> <p>Descriptive name for the external application whose status is being referenced.</p> <p>Example: <code>xConfiguration Applications External Status 1 Name: "foo"</code></p>  |
| <p><b>Authentication Account Admin Account [1..n] AccessAPI: &lt;On/Off&gt;</b></p> <p>Determines whether this account is allowed to access the system's status and configuration via the Application Programming Interface (API). Default: On.</p> <p>Example: <code>xConfiguration Authentication Account Admin Account 1 AccessAPI: On</code></p>   |
| <p><b>Authentication Account Admin Account [1..n] AccessWeb: &lt;On/Off&gt;</b></p> <p>Determines whether this account is allowed to log in to the system using the web interface. Default: On.</p> <p>Example: <code>xConfiguration Authentication Account Admin Account 1 AccessWeb: On</code></p>   |

Table 12: xConfiguration CLI reference (continued)

|   |
|---|
| <p><b>Authentication Account Admin Account [1..n] Enabled: &lt;On/Off&gt;</b></p> <p>Indicates if the account is enabled or disabled. Access will be denied to disabled accounts. Default: On.</p> <p>Example: <code>xConfiguration Authentication Account Admin Account 1 Enabled: On</code></p>   |
| <p><b>Authentication Account Admin Account [1..n] Name: &lt;S: 0, 128&gt;</b></p> <p>The username for the administrator account.</p> <p>Example: <code>xConfiguration Authentication Account Admin Account 1 Name: "bob_smith"</code></p>   |
| <p><b>Authentication Account Admin Account [1..n] Password: &lt;Password&gt;</b></p> <p>The password that this administrator will use to log in to the Expressway.</p> <p>Example: <code>xConfiguration Authentication Account Admin Account 1 Password: "abcXYZ_123"</code></p>  |
| <p><b>Authentication Account Admin Group [1..n] AccessAPI: &lt;On/Off&gt;</b></p> <p>Determines whether members of this group are allowed to access the system's status and configuration using the Application Programming Interface (API). Default: On.</p> <p>Example: <code>xConfiguration Authentication Account Admin Group 1 AccessAPI: On</code></p>  |
| <p><b>Authentication Account Admin Group [1..n] AccessWeb: &lt;On/Off&gt;</b></p> <p>Determines whether members of this group are allowed to log in to the system using the web interface. Default: On.</p> <p>Example: <code>xConfiguration Authentication Account Admin Group 1 AccessWeb: On</code></p>  |
| <p><b>Authentication Account Admin Group [1..n] Enabled: &lt;On/Off&gt;</b></p> <p>Indicates if the group is enabled or disabled. Access will be denied to members of disabled groups. Default: On.</p> <p>Example: <code>xConfiguration Authentication Account Admin Group 1 Enabled: On</code></p>  |
| <p><b>Authentication Account Admin Group [1..n] Name: &lt;S: 0, 128&gt;</b></p> <p>The name of the administrator group.</p> <p>Example: <code>xConfiguration Authentication Account Admin Group 1 Name: "administrators"</code></p>   |
| <p><b>Authentication Certificate Crlcheck: &lt;None/Peer/All&gt;</b></p> <p>Specifies whether HTTPS client certificates are checked against certificate revocation lists (CRLs). CRL data is uploaded to the Expressway via the CRL management page. Default: All.</p> <p><i>None</i>: no CRL checking is performed.</p> <p><i>Peer</i>: only the CRL associated with the CA that issued the client's certificate is checked.</p> <p><i>All</i>: all CRLs in the trusted certificate chain of the CA that issued the client's certificate are checked.</p> <p>Example: <code>xConfiguration Authentication Certificate Crlcheck: All</code></p> |
| <p><b>Authentication Certificate Crlinaccessible: &lt;Ignore/Fail&gt;</b></p> <p>Controls the revocation list checking behavior if the revocation status cannot be established, for example if the revocation source cannot be contacted or no appropriate revocation list is present. Default: Ignore.</p> <p><i>Ignore</i>: treat the certificate as not revoked.</p> <p><i>Fail</i>: treat the certificate as revoked (and thus do not allow the TLS connection).</p> <p>Example: <code>xConfiguration Authentication Certificate Crlinaccessible: Ignore</code></p>   |

Table 12: xConfiguration CLI reference (continued)

---

|  |
|--|
| <p><b>Authentication Certificate Mode: &lt;NotRequired/Validation/Authentication&gt;</b></p> <p>Controls the level of security required to allow client systems (typically web browsers) to communicate with the Expressway over HTTPS. Default: NotRequired.</p> <p><i>NotRequired</i> : the client system does not have to present any form of certificate.</p> <p><i>Validation</i> : the client system must present a valid certificate that has been signed by a trusted certificate authority (CA). Note that a restart is required if you are changing from Not required to Certificate validation.</p> <p><i>Authentication</i> : the client system must present a valid certificate that has been signed by a trusted CA and contains the client's authentication credentials. When this mode is enabled, the standard login mechanism is no longer available.</p> <p>Example: <code>xConfiguration Authentication Certificate Mode: NotRequired</code></p> |
| <p><b>Authentication Certificate UsernameRegex: &lt;String&gt;</b></p> <p>The regular expression to apply to the client certificate presented to the Expressway. Use the (? regex) syntax to supply names for capture groups so that matching sub-patterns can be substituted in the associated template. Default: <code>/Subject.*CN=(? ([^,] (\\,))*)/m</code></p> <p>Example: <code>xConfiguration Authentication Certificate UsernameRegex: "/Subject:.*CN= (? ([^,] (\\,))*)/m"</code></p>  |
| <p><b>Authentication Certificate UsernameTemplate: &lt;String&gt;</b></p> <p>A template containing a mixture of fixed text and the capture group names used in the Regex. Delimit each capture group name with #, for example, prefix#Group1#suffix. Each capture group name will be replaced with the text obtained from the regular expression processing. The resulting string is used as the user's authentication credentials (username). Default: <code>#captureCommonName#</code></p> <p>Example: <code>xConfiguration Authentication Certificate UsernameTemplate: "#captureCommonName#"</code></p>  |
| <p><b>Authentication Password: &lt;S: 0, 215&gt;</b></p> <p>The password used by the Expressway when authenticating with another system. The maximum plaintext length is 128 characters, which is then encrypted. Note: this does not apply to traversal client zones.</p> <p>Example: <code>xConfiguration Authentication Password: "password123"</code></p>  |
| <p><b>Authentication Remote Digest Cache ExpireCheckInterval: &lt;0..65535&gt;</b></p> <p>The interval between digest authentication cache expiration checks in seconds. Default: 600</p> <p>Example: <code>xConfiguration Authentication Remote Digest Cache ExpireCheckInterval: 600</code></p>  |
| <p><b>Authentication Remote Digest Cache Lifetime: &lt;0..43200&gt;</b></p> <p>The lifetime of digest authentication interim hashes in seconds. Default: 600</p> <p>Example: <code>xConfiguration Authentication Remote Digest Cache Lifetime: 600</code></p>  |
| <p><b>Authentication Remote Digest Cache Limit: &lt;0..65535&gt;</b></p> <p>The interval between digest authentication cache expiration checks in seconds. Default: 10000</p> <p>Example: <code>xConfiguration Authentication Remote Digest Cache Limit: 10000</code></p>  |
| <p><b>Authentication Remote Digest Cache Mode: &lt;On/Off&gt;</b></p> <p>Controls whether the digest authentication cache is enabled. Default: On</p> <p>Example: <code>xConfiguration Authentication Remote Digest Cache Mode: On</code></p>  |
| <p><b>Authentication StrictPassword Enabled: &lt;On/Off&gt;</b></p> <p>Determines whether local administrator account passwords must meet a minimum level of complexity before they are accepted. In addition, passwords must not: be based on a dictionary word contain too many consecutive characters such as "abc" or "123", contain too few different characters or be palindromes. Default: Off.</p> <p><i>On</i> : local administrator account passwords must meet the complexity requirements.</p> <p><i>Off</i> : passwords are not checked for complexity.</p> <p>Example: <code>xConfiguration Authentication StrictPassword Enabled: Off</code></p>  |

---



Table 12: xConfiguration CLI reference (continued)

**Authentication StrictPassword MaximumConsecutiveRepeated: <0..255>**

The maximum number of times the same character can be repeated consecutively. A value of 0 disables this check. Default: 0

Example: `xConfiguration Authentication StrictPassword MaximumConsecutiveRepeated: 0`

**Authentication StrictPassword MinimumClasses: <0..4>**

The minimum number of character classes that must be present. There are four character classes: digit, upper case, lower case and special. Use this setting if you want to mandate the use of 2-3 different character classes without requiring all of them to be present. A value of 0 disables this check. Default: 0.

Example: `xConfiguration Authentication StrictPassword MinimumClasses: 0`

**Authentication StrictPassword MinimumDigits: <0..255>**

The minimum number of digits that must be present. A value of 0 disables this check. Default: 2.

Example: `xConfiguration Authentication StrictPassword MinimumDigits: 2`

**Authentication StrictPassword MinimumLength: <6..255>**

The minimum length of the password. Default: 15.

Example: `xConfiguration Authentication StrictPassword MinimumLength: 15`

**Authentication StrictPassword MinimumLowerCase: <0..255>**

The minimum number of lower case characters that must be present. A value of 0 disables this check. Default: 2.

Example: `xConfiguration Authentication StrictPassword MinimumLowerCase: 2`

**Authentication StrictPassword MinimumOther: <0..255>**

The minimum number of special characters that must be present. A special character is anything that is not a letter or a digit. A value of 0 disables this check. Default: 2

Example: `xConfiguration Authentication StrictPassword MinimumOther: 2`

**Authentication StrictPassword MinimumUpperCase: <0..255>**

The minimum number of upper case characters that must be present. A value of 0 disables this check. Default : 2

Example: `xConfiguration Authentication StrictPassword MinimumUpperCase: 2`

**Authentication UserName: <S: 0, 128>**

The username used by the Expressway when authenticating with another system. Note: this does not apply to traversal client zones.

Example: `xConfiguration Authentication UserName: "user123"`

**Bandwidth Default: <64..65535>**

The bandwidth (in kbps) to use on calls managed by the Expressway where no bandwidth has been specified by the endpoint. Default: 384.

Example: `xConfiguration Bandwidth Default: 384`

**Bandwidth Downspeed PerCall Mode: <On/Off>**

Determines whether the Expressway attempts to downspeed a call if there is insufficient per-call bandwidth available to fulfill the request. Default: On.

*On*: the Expressway will attempt to place the call at a lower bandwidth.

*Off*: the call will be rejected.

Example: `xConfiguration Bandwidth Downspeed PerCall Mode: On`

Table 12: xConfiguration CLI reference (continued)

**Bandwidth Downspeed Total Mode: <On/Off>**

Determines whether the Expressway attempts to downspeed a call if there is insufficient total bandwidth available to fulfill the request.  
Default: On.

*On*: the Expressway will attempt to place the call at a lower bandwidth.

*Off*: the call will be rejected.

Example: `xConfiguration Bandwidth Downspeed Total Mode: On`

**Bandwidth Link [1..3000] Name: <S: 1, 50>**

Assigns a name to this link.

Example: `xConfiguration Bandwidth Link 1 Name: "HQ to BranchOffice"`

**Bandwidth Link [1..3000] Node1 Name: <S: 0, 50>**

Specifies the first zone or subzone to which this link will be applied.

Example: `xConfiguration Bandwidth Link 1 Node1 Name: "HQ"`

**Bandwidth Link [1..3000] Node2 Name: <S: 0, 50>**

Specifies the second zone or subzone to which this link will be applied.

Example: `xConfiguration Bandwidth Link 1 Node2 Name: "BranchOffice"`

**Bandwidth Link [1..3000] Pipe1 Name: <S: 0, 50>**

Specifies the first pipe to be associated with this link.

Example: `xConfiguration Bandwidth Link 1 Pipe1 Name: "512Kb ASDL"`

**Bandwidth Link [1..3000] Pipe2 Name: <S: 0, 50>**

Specifies the second pipe to be associated with this link.

Example: `xConfiguration Bandwidth Link 1 Pipe2 Name: "2Gb Broadband"`

**Bandwidth Pipe [1..1000] Bandwidth PerCall Limit: <1..100000000>**

If this pipe has limited per-call bandwidth, sets the maximum amount of bandwidth (in kbps) available for any one call. Default: 1920.

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Limit: 256`

**Bandwidth Pipe [1..1000] Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth>**

Determines whether or not this pipe is limiting the bandwidth of individual calls. Default: Unlimited.

*NoBandwidth*: no bandwidth available. No calls can be made on this pipe.

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Mode: Limited`

**Bandwidth Pipe [1..1000] Bandwidth Total Limit: <1..100000000>**

If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe. Default: 500000.

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth Total Limit: 1024`

**Bandwidth Pipe [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>**

Determines whether or not this pipe is enforcing total bandwidth restrictions. Default: Unlimited.

*NoBandwidth*: no bandwidth available. No calls can be made on this pipe.

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth Total Mode: Limited`

**Bandwidth Pipe [1..1000] Name: <S: 1, 50>**

Assigns a name to this pipe.

Example: `xConfiguration Bandwidth Pipe 1 Name: "512Kb ASDL"`

Table 12: xConfiguration CLI reference (continued)

**Call Loop Detection Mode: <On/Off>**

Specifies whether the Expressway will check for call loops. Default: On.

Example: `xConfiguration Call Loop Detection Mode: On`

**Call Routed Mode: <Always/Optimal>**

Specifies whether the Expressway routes the signaling for calls. Default: Always.

*Always*: the Expressway will always route the call signaling.

*Optimal*: if possible, the Expressway will remove itself from the call signaling path, which may mean the call does not consume a call license.

Example: `xConfiguration Call Routed Mode: Always`

**Call Services CallsToUnknownIPAddresses: <Off/Direct/Indirect>**

The way in which the Expressway attempts to call systems that are not registered with it or one of its neighbors. Default: Indirect.

*Direct*: allows an endpoint to make a call to an unknown IP address without the Expressway querying any neighbors. The call setup would occur just as it would if the far end were registered directly to the local system.

*Indirect*: upon receiving a call to an unknown IP address, the Expressway will query its neighbors for the remote address and if permitted will route the call through the neighbor.

*Off*: endpoints registered directly to the Expressway may only call an IP address of a system also registered directly to that Expressway.

Example: `xConfiguration Call Services CallsToUnknownIPAddresses: Indirect`

**Call Services Fallback Alias: <S: 0, 60>**

Specifies the alias to which incoming calls are placed for calls where the IP address or domain name of the Expressway has been given but no callee alias has been specified.

Example: `xConfiguration Call Services Fallback Alias: "reception@example.com"`

**CDR Service: <off/serviceonly/serviceandlogging>**

Controls whether the Call Detail Records service is running, and whether the CDRs are published to syslog hosts. Default: off.

*off*: The CDR service is disabled, and no call detail records are kept.

*serviceonly*: The CDR service is enabled. The system keeps the most recent 7 days worth of CDRs, but these are only accessible via the API.

*serviceandlogging*: CDRs are also written to disk (in messages.log) and sent to any syslog hosts that are configured for INFO or DEBUG messages.

Example: `xConfiguration CDR Service: serviceonly`

**CollaborationEdge SsoAlwaysAvailable: <On/Off>**

Determines whether the Expressway-C will check if the user's home node has SSO available.

*On*: The Expressway-E always tells the client that SSO is available, without actually checking the home node.

*Off*: Allow the Expressway-C to check if SSO is available on the user's home node before the Expressway-E responds to the client.

Example: `xConfiguration CollaborationEdge SsoAlwaysAvailable: Off`

**Note:** The default value *Off* corresponds to the following default on the web UI: **Check for internal SSO availability: Yes**

**CollaborationEdge SsoEnabled: <On/Off>**

Toggles Single Sign-On for mobile and remote access to UC services.

Example: `xConfiguration CollaborationEdge SsoEnabled: Off`

**CollaborationEdge SsoSipTokenExtraTtl: <0..172800>**

Extends the lifetime of the SIP authorization token by the supplied number of seconds.

Example: `xConfiguration CollaborationEdge SsoSipTokenExtraTtl: 0`

Table 12: xConfiguration CLI reference (continued)

|  |
|--|
| <p><b>DNS PerDomainServer [1..5] Address: &lt;S: 0, 39&gt;</b></p> <p>The IP address of the DNS server to use only when resolving hostnames for the associated domain names.</p> <p>Example: <code>xConfiguration DNS PerDomainServer 1 Address: "192.168.12.1"</code></p>   |
| <p><b>DNS PerDomainServer [1..5] Domain1: &lt;S: 0, 39&gt;</b></p> <p>The first domain name to be resolved by this particular DNS server.</p> <p>Example: <code>xConfiguration DNS PerDomainServer 1 Domain1: "dept.example.com"</code></p>  |
| <p><b>DNS PerDomainServer [1..5] Domain2: &lt;S: 0, 39&gt;</b></p> <p>The second domain name to be resolved by this particular DNS server.</p> <p>Example: <code>xConfiguration DNS PerDomainServer 1 Domain2: "other.example.com"</code></p>  |
| <p><b>DNS Server [1..5] Address: &lt;S: 0, 39&gt;</b></p> <p>The IP address of a default DNS server to use when resolving domain names. You can specify up to 5 servers. These default DNS servers are used if there is no per-domain DNS server defined for the domain being looked up.</p> <p>Example: <code>xConfiguration DNS Server 1 Address: "192.168.12.0"</code></p>  |
| <p><b>EdgeConfigServer RateLimitLogins: &lt;0..100&gt;</b></p> <p>Limits the number of times that any user's credentials can authorize via VCS per rate control period. Any device using the same user credentials contributes to the number.</p> <p>After the limit is reached, any further attempts to use these credentials are rejected until the current rate control period expires.</p> <p>Enter 0 to disable the rate control feature.</p> <p>Example: <code>xConfiguration EdgeConfigServer RateLimitLogins: 3</code></p> |
| <p><b>EdgeConfigServer RateLimitPeriod: &lt;0..86400&gt;</b></p> <p>Defines the period (in seconds) over which authorizations are counted. If rate control is enabled, then a user's first authorization starts the counter and the timer. When the rate control period expires, the counter is reset and a new period will start with the user's next authorization.</p> <p>Enter 0 to disable the rate control feature.</p> <p>Example: <code>xConfiguration EdgeConfigServer RateLimitPeriod: 300</code></p>                    |
| <p><b>ErrorReport Contact: &lt;S: 0, 128&gt;</b></p> <p>An optional contact email address for follow up on incident reports if required.</p> <p>Example: <code>xConfiguration ErrorReport Contact: "bob smith"</code></p>  |
| <p><b>ErrorReport CoreDump: &lt;On/Off&gt;</b></p> <p>Determines whether diagnostic core dump files are created. Default: On.</p> <p>Example: <code>xConfiguration ErrorReport CoreDump: On</code></p>   |
| <p><b>ErrorReport Mode: &lt;On/Off&gt;</b></p> <p>Determines whether details of application failures are automatically sent to a web service. Default: Off.</p> <p>Example: <code>xConfiguration ErrorReport Mode: Off</code></p>  |
| <p><b>ErrorReport Proxy: &lt;S: 0, 128&gt;</b></p> <p>An optional proxy server to use for the HTTP/HTTPS connections to the incident reporting server.</p> <p>Example: <code>xConfiguration ErrorReport Proxy: https://proxy_address/submiterror/</code></p>   |
| <p><b>ErrorReport Url: &lt;S: 0, 128&gt;</b></p> <p>The URL of the web service to which details of application failures are sent. Default: <code>https://cc-reports.cisco.com/submitapplicationerror/</code></p> <p>Example: <code>xConfiguration ErrorReport Url: https://cc-reports.cisco.com/submitapplicationerror/</code></p>   |

Table 12: xConfiguration CLI reference (continued)

|   |
|---|
| <p><b>Ethernet [1..2] IP V4 Address: &lt;S: 7,15&gt;</b></p> <p>Specifies the IPv4 address of the specified LAN port. Note: you must restart the system for any changes to take effect.</p> <p>Example: <code>xConfiguration Ethernet 1 IP V4 Address: "192.168.10.10"</code></p>   |
| <p><b>Ethernet [1..2] IP V4 StaticNAT Address: &lt;S:7,15&gt;</b></p> <p>If the Expressway is operating in static NAT mode, this specifies the external public IPv4 address of that static NAT. You must restart the system for any changes to take effect.</p> <p>Example: <code>xConfiguration Ethernet 1 IP V4 StaticNAT Address: "64.22.64.85"</code></p> |
| <p><b>Ethernet [1..2] IP V4 StaticNAT Mode: &lt;On/Off&gt;</b></p> <p>Specifies whether the Expressway is located behind a static NAT. You must restart the system for any changes to take effect. Default: Off.</p> <p>Example: <code>xConfiguration Ethernet 1 IP V4 StaticNAT Mode: On</code></p>  |
| <p><b>Ethernet [1..2] IP V4 SubnetMask: &lt;S: 7,15&gt;</b></p> <p>Specifies the IPv4 subnet mask of the specified LAN port. You must restart the system for any changes to take effect.</p> <p>Example: <code>xConfiguration Ethernet 1 IP V4 SubnetMask: "255.255.255.0"</code></p>   |
| <p><b>Ethernet [1..2] IP V6 Address: &lt;S: 0, 39&gt;</b></p> <p>Specifies the IPv6 address of the specified LAN port. You must restart the system for any changes to take effect.</p> <p>Example: <code>xConfiguration Ethernet 1 IP V6 Address: "2001:db8::1428:57ab"</code></p>  |
| <p><b>Ethernet [1..2] Speed: &lt;Auto/10half/10full/100half/100full/1000full&gt;</b></p> <p>Sets the speed of the Ethernet link from the specified LAN port. Use Auto to automatically configure the speed. You must restart the system for any changes to take effect. Default: Auto.</p> <p>Example: <code>xConfiguration Ethernet 1 Speed: Auto</code></p> |
| <p><b>ExternalManager Address: &lt;S: 0, 128&gt;</b></p> <p>Sets the IP address or Fully Qualified Domain Name (FQDN) of the external manager.</p> <p>Example: <code>xConfiguration ExternalManager Address: "192.168.0.0"</code></p>   |
| <p><b>ExternalManager Path: &lt;S: 0, 255&gt;</b></p> <p>Sets the URL of the external manager. Default: <code>tms/public/external/management/SystemManagementService.asmx</code></p> <p>Example: <code>xConfiguration ExternalManager Path: "tms/public/external/management/SystemManagementService.asmx"</code></p>  |
| <p><b>ExternalManager Protocol: &lt;HTTP/HTTPS&gt;</b></p> <p>The protocol used to connect to the external manager. Default: HTTPS.</p> <p>Example: <code>xConfiguration ExternalManager Protocol: HTTPS</code></p>   |
| <p><b>ExternalManager Server Certificate Verification Mode: &lt;On/Off&gt;</b></p> <p>Controls whether the certificate presented by the external manager is verified. Default: On.</p> <p>Example: <code>xConfiguration ExternalManager Server Certificate Verification Mode: On</code></p>   |
| <p><b>H323 Gatekeeper AutoDiscovery Mode: &lt;On/Off&gt;</b></p> <p>Determines whether or not the Expressway responds to gatekeeper discovery requests from endpoints. Default: On.</p> <p>Example: <code>xConfiguration H323 Gatekeeper AutoDiscovery Mode: On</code></p>  |
| <p><b>H323 Gatekeeper CallSignaling PortRange End: &lt;1024..65534&gt;</b></p> <p>Specifies the upper port in the range to be used by calls once they are established. Default: 19999.</p> <p>Example: <code>xConfiguration H323 Gatekeeper CallSignaling PortRange End: 19999</code></p>   |

Table 12: xConfiguration CLI reference (continued)

|   |
|---|
| <p><b>H323 Gatekeeper CallSignaling PortRange Start: &lt;1024..65534&gt;</b></p> <p>Specifies the lower port in the range to be used by calls once they are established. Default: 15000.</p> <p>Example: <code>xConfiguration H323 Gatekeeper CallSignaling PortRange Start: 15000</code></p>   |
| <p><b>H323 Gatekeeper CallSignaling TCP Port: &lt;1024..65534&gt;</b></p> <p>Specifies the port that listens for H.323 call signaling. Default: 1720.</p> <p>Example: <code>xConfiguration H323 Gatekeeper CallSignaling TCP Port: 1720</code></p>  |
| <p><b>H323 Gatekeeper CallTimeToLive: &lt;60..65534&gt;</b></p> <p>Specifies the interval (in seconds) at which the Expressway polls the endpoints in a call to verify that they are still in the call. Default: 120.</p> <p>Example: <code>xConfiguration H323 Gatekeeper CallTimeToLive: 120</code></p>   |
| <p><b>H323 Gateway CallerId: &lt;IncludePrefix/ExcludePrefix&gt;</b></p> <p>Specifies whether the prefix of the ISDN gateway is inserted into the caller's E.164 number presented on the destination endpoint. Including the prefix allows the recipient to directly return the call. Default: ExcludePrefix.</p> <p><i>IncludePrefix</i>: inserts the ISDN gateway's prefix into the source E.164 number.</p> <p><i>ExcludePrefix</i>: only displays the source E.164 number.</p> <p>Example: <code>xConfiguration H323 Gateway CallerId: ExcludePrefix</code></p> |
| <p><b>H323 Mode: &lt;On/Off&gt;</b></p> <p>Determines whether or not the Expressway will provide H.323 gatekeeper functionality. Default: On.</p> <p>Example: <code>xConfiguration H323 Mode: On</code></p>   |
| <p><b>Interworking BFCP Compatibility Mode: &lt;Auto/TAA/Draft&gt;</b></p> <p>Controls the compatibility settings of the SIP to H.323 interworking BFCP component. Default: Auto.</p> <p>Example: <code>xConfiguration Interworking BFCP Compatibility Mode: Auto</code></p>  |
| <p><b>Interworking Encryption Mode: &lt;Auto/Off&gt;</b></p> <p>Determines whether or not the Expressway will allow encrypted calls between SIP and H.323 endpoints. Default: Auto.</p> <p><i>Off</i>: interworked calls will never be encrypted.</p> <p><i>Auto</i>: interworked calls will be encrypted if the endpoints request it.</p> <p>Example: <code>xConfiguration Interworking Encryption Mode: Auto</code></p>   |
| <p><b>Interworking Encryption Replay Protection Mode: &lt;On/Off&gt;</b></p> <p>Controls whether the Expressway will perform replay protection for incoming SRTP packets when interworking a call. Default: Off.</p> <p><i>On</i>: replayed SRTP packets will be dropped by the Expressway.</p> <p><i>Off</i>: the Expressway will not check for replayed SRTP packets.</p> <p>Example: <code>xConfiguration Interworking Encryption Replay Protection Mode: Off</code></p>   |
| <p><b>Interworking Mode: &lt;On/Off/RegisteredOnly&gt;</b></p> <p>Determines whether or not the Expressway will act as a gateway between SIP and H.323 calls. Default: RegisteredOnly.</p> <p><i>Off</i>: the Expressway will not act as a SIP-H.323 gateway.</p> <p><i>On</i>: the Expressway will act as SIP-H.323 gateway.</p> <p>Example: <code>xConfiguration Interworking Mode: On</code></p>   |

Table 12: xConfiguration CLI reference (continued)

---

|   |
|---|
| <b>Interworking Require Invite Header Mode: &lt;On/Off&gt;</b>  |
| Controls whether the SIP to H.323 interworking function sends com.tandberg.sdp.duo.enable and com.tandberg.sdp.bfcp.udp in the require header for dialog forming INVITEs. Default: Off. |
| Example: <code>xConfiguration Interworking Require Invite Header Mode: Off</code>   |

---

|   |
|---|
| <b>IP DNS Domain Name: &lt;S: 0, 128&gt;</b>  |
| The name to be appended to an unqualified host name before querying the DNS server. Used when attempting to resolve unqualified domain names for NTP, LDAP, external manager and remote syslog servers. May also be used along with the <b>System host name</b> to identify references to this Expressway in SIP messaging. |
| Example: <code>xConfiguration IP DNS Domain Name: "example.com"</code>  |

---

|  |
|--|
| <b>IP DNS Hostname : &lt;S: 0, 63&gt;</b>  |
| The DNS host name that this system is known by. This is not the fully-qualified domain name, just the host label portion. The name can only contain letters, digits, hyphens and underscores. The first character must be a letter and the last character must be a letter or a digit. |
| Example: <code>xConfiguration IP DNS Hostname: "localsystem"</code>  |

---

|  |
|--|
| <b>IP DNS MaxPort: &lt;1024..65535&gt;</b>   |
| The upper source port in the range used for sending DNS queries. Requests choose a random port from this range. Warning: setting a small source port range increases your vulnerability to DNS spoofing attacks. Default: 65535. |
| Example: <code>xConfiguration IP DNS MaxPort: 65535</code>   |

---

|   |
|---|
| <b>IP DNS MinPort: &lt;1024..65535&gt;</b>  |
| The lower source port in the range used for sending DNS queries. Requests choose a random port from this range. Warning: setting a small source port range increases your vulnerability to DNS spoofing attacks. Default: 1024. |
| Example: <code>xConfiguration IP DNS MinPort: 1024</code>   |

---

|   |
|---|
| <b>IP DNS UseEphemeralPortRange: &lt;On/Off&gt;</b>   |
| Determines whether outgoing DNS queries use the system's normal ephemeral port range, or a custom port range that you can configure. Default: On. |
| Example: <code>xConfiguration IP DNS UseEphemeralPortRange: On</code>   |

---

|  |
|--|
| <b>IP Ephemeral PortRange End: &lt;1024..65534&gt;</b>   |
| The highest port in the range used for ephemeral outbound connections not otherwise constrained by Expressway call processing. Default: 35999. |
| Example: <code>xConfiguration IP Ephemeral PortRange End: 35999</code>   |

---

|   |
|---|
| <b>IP Ephemeral PortRange Start: &lt;1024..65534&gt;</b>  |
| The lowest port in the range used for ephemeral outbound connections not otherwise constrained by Expressway call processing. Default: 30000. |
| Example: <code>xConfiguration IP Ephemeral PortRange Start: 30000</code>  |

---

|  |
|--|
| <b>IP External Interface: &lt;LAN1/LAN2&gt;</b>                  |
| Defines which LAN interface is externally facing. Default: LAN1. |
| Example: <code>xConfiguration IP External Interface: LAN1</code> |

---

|  |
|--|
| <b>IP Gateway: &lt;S: 7,15&gt;</b>   |
| Specifies the IPv4 gateway of the Expressway. Note: you must restart the system for any changes to take effect. Default: 127.0.0.1 |
| Example: <code>xConfiguration IP Gateway: "192.168.127.0"</code>   |

---

Table 12: xConfiguration CLI reference (continued)

|  |
|--|
| <p><b>IP QoS Mode: &lt;None/DiffServ&gt;</b></p> <p>The type of QoS (Quality of Service) tags to apply to all signaling and media packets. You must restart the system for any changes to take effect. Default: None.</p> <p><i>None:</i> no specific QoS tagging is applied.</p> <p><i>DiffServ:</i> puts the specified Tag value in the TOS (Type Of Service) field of the IPv4 header or TC (Traffic Class) field of the IPv6 header.</p> <p>Example: <code>xConfiguration IP QoS Mode: DiffServ</code></p>       |
| <p><b>IP QoS Value: &lt;0..63&gt;</b></p> <p>The value to stamp onto all signaling and media traffic routed through the system. You must restart the system for any changes to take effect. Default: 0.</p> <p>Example: <code>xConfiguration IP QoS Value: 16</code></p>   |
| <p><b>IP RFC4821 Mode: &lt;Auto/Enabled/Disabled&gt;</b></p> <p>Determines when RFC4821 Packetization Layer Path MTU Discovery is used by the Expressway network interface. Default: Disabled.</p> <p><i>Enabled:</i> Packetization layer MTU probing is always performed.</p> <p><i>Auto:</i> Disabled by default, enabled when an ICMP black hole is detected.</p> <p><i>Disabled:</i> Packetization layer MTU probing is not performed.</p> <p>Example: <code>xConfiguration IP RFC4821 Mode: Disabled</code></p> |
| <p><b>IP Route [1..50] Address: &lt;S: 0, 39&gt;</b></p> <p>Specifies an IP address used in conjunction with the Prefix Length to determine the network to which this route applies.</p> <p>Example: <code>xConfiguration IP Route 1 Address: "128.168.0.0"</code></p>   |
| <p><b>IP Route [1..50] Gateway: &lt;S: 0, 39&gt;</b></p> <p>Specifies the IP address of the Gateway for this route.</p> <p>Example: <code>xConfiguration IP Route 1 Gateway: "192.168.0.0"</code></p>  |
| <p><b>IP Route [1..50] Interface: &lt;Auto/LAN1/LAN2&gt;</b></p> <p>Specifies the LAN interface to use for this route. Auto: The Expressway will select the most appropriate interface to use. Default: Auto.</p> <p>Example: <code>xConfiguration IP Route 1 Interface: Auto</code></p>   |
| <p><b>IP Route [1..50] PrefixLength: &lt;0..128&gt;</b></p> <p>The number of bits of the IP address which must match when determining the network to which this route applies. Default: 32.</p> <p>Example: <code>xConfiguration IP Route 1 PrefixLength: 16</code></p>  |
| <p><b>IP V6 Gateway: &lt;S: 0, 39&gt;</b></p> <p>Specifies the IPv6 gateway of the Expressway. You must restart the system for any changes to take effect.</p> <p>Example: <code>xConfiguration IP V6 Gateway: "3dda:80bb:6::9:144"</code></p>   |
| <p><b>IPProtocol: &lt;Both/IPv4/IPv6&gt;</b></p> <p>Selects whether the Expressway is operating in IPv4, IPv6 or dual stack mode. You must restart the system for any changes to take effect. Default: IPv4.</p> <p>Example: <code>xConfiguration IPProtocol: IPv4</code></p>  |
| <p><b>Language Default: &lt;S: 0, 128&gt;</b></p> <p>The default language used on the web interface. Default: "en_US".</p> <p>Example: <code>xConfiguration Language Default: "en_US"</code></p>   |



Table 12: xConfiguration CLI reference (continued)

|  |
|--|
| <p><b>Log Level: &lt;1..4&gt;</b></p> <p>Controls the granularity of Event Logging. 1 is the least verbose, 4 the most. Note: this setting is not retrospective; it determines which events are written to the Event Log from now onwards. Default: 1</p> <p>Example: <code>xConfiguration Log Level: 1</code></p>   |
| <p><b>Log MediaStats Logging: &lt;On/Off&gt;</b></p> <p>Toggles media statistics logging. Default: Off</p> <p>Example: <code>xConfiguration Log MediaStats Logging: On</code></p>  |
| <p><b>Logger Network [1..n] Level: &lt;FATAL/ERROR/WARN/INFO/DEBUG/TRACE&gt;</b></p> <p>The logging level for the nominated module. Default : INFO.</p> <p>Example: <code>xConfiguration Logger Developer 1 Level: INFO</code></p>   |
| <p><b>Login Remote LDAP BaseDN Accounts: &lt;S: 0,255&gt;</b></p> <p>Sets the Distinguished Name to use as the base when searching for administrator and user accounts.</p> <p>Example: <code>xConfiguration Login Remote LDAP BaseDN Accounts: "ou=useraccounts,dc=corporation,dc=int"</code></p>   |
| <p><b>Login Remote LDAP BaseDN Groups: &lt;S: 0,255&gt;</b></p> <p>Sets the Distinguished Name to use as the base when searching for administrator and user groups.</p> <p>Example: <code>xConfiguration Login Remote LDAP BaseDN Groups: "ou=groups,dc=corporation,dc=int"</code></p>   |
| <p><b>Login Remote LDAP CRLCheck: &lt;None/Peer/All&gt;</b></p> <p>Specifies whether certificate revocation lists (CRLs) are checked when forming a TLS connection with the LDAP server. CRL data is uploaded to the Expressway via the trusted CA certificate PEM file. Default: None.</p> <p><i>None</i>: no CRL checking is performed.</p> <p><i>Peer</i>: only the CRL associated with the CA that issued the LDAP server's certificate is checked.</p> <p><i>All</i>: all CRLs in the trusted certificate chain of the CA that issued the LDAP server's certificate are checked.</p> <p>Example: <code>xConfiguration Login Remote LDAP CRLCheck: Peer</code></p> |
| <p><b>Login Remote LDAP DirectoryType: &lt;ActiveDirectory&gt;</b></p> <p>Defines the type of LDAP directory that is being accessed. Default: ActiveDirectory.</p> <p><i>ActiveDirectory</i>: directory is Windows Active Directory.</p> <p>Example: <code>xConfiguration Login Remote LDAP DirectoryType: ActiveDirectory</code></p>  |
| <p><b>Login Remote LDAP Encryption: &lt;Off/TLS&gt;</b></p> <p>Sets the encryption to use for the connection to the LDAP server. Default: TLS.</p> <p><i>Off</i>: no encryption is used.</p> <p><i>TLS</i>: TLS encryption is used.</p> <p>Example: <code>xConfiguration Login Remote LDAP Encryption: Off</code></p>  |
| <p><b>Login Remote LDAP SASL: &lt;None/DIGEST-MD5&gt;</b></p> <p>The SASL (Simple Authentication and Security Layer) mechanism to use when binding to the LDAP server. Default: DIGEST-MD5.</p> <p><i>None</i>: no mechanism is used.</p> <p><i>DIGEST-MD5</i>: The DIGEST-MD5 mechanism is used.</p> <p>Example: <code>xConfiguration Login Remote LDAP SASL: DIGEST-MD5</code></p>   |
| <p><b>Login Remote LDAP Server Address: &lt;S: 0,128&gt;</b></p> <p>Sets the IP address or Fully Qualified Domain Name (FQDN) of the LDAP server to use when making LDAP queries.</p> <p>Example: <code>xConfiguration Login Remote LDAP Server Address: "server.example.com"</code></p>   |

Table 12: xConfiguration CLI reference (continued)

---

|  |
|--|
| <p><b>Login Remote LDAP Server FQDNResolution: &lt;AddressRecord/SRVRecord&gt;</b></p> <p>Sets how the LDAP server address is resolved if specified as an FQDN. Default: AddressRecord.</p> <p><i>AddressRecord:</i> DNS A or AAAA record lookup.</p> <p><i>SRVRecord:</i> DNS SRV record lookup.</p> <p>Example: <code>xConfiguration Login Remote LDAP Server FQDNResolution: AddressRecord</code></p>   |
| <p><b>Login Remote LDAP Server Port: &lt;1..65534&gt;</b></p> <p>Sets the IP port of the LDAP server to use when making LDAP queries. Non-secure connections use 389 and secure connections use 636. Other ports are not supported. Default: 389.</p> <p>Example: <code>xConfiguration Login Remote LDAP Server Port: 389</code></p>   |
| <p><b>Login Remote LDAP VCS BindDN: &lt;S: 0,255&gt;</b></p> <p>Sets the user distinguished name to use when binding to the LDAP server.</p> <p>Example: <code>xConfiguration Login Remote LDAP VCS BindDN: "systemmanager"</code></p>   |
| <p><b>Login Remote LDAP VCS BindPassword: &lt;S: 0,122&gt;</b></p> <p>Sets the password to use when binding to the LDAP server. The maximum plaintext length is 60 characters, which is then encrypted.</p> <p>Example: <code>xConfiguration Login Remote LDAP VCS BindPassword: "password123"</code></p>  |
| <p><b>Login Remote LDAP VCS BindUsername: &lt;S: 0,255&gt;</b></p> <p>Sets the username to use when binding to the LDAP server. Only applies if using SASL.</p> <p>Example: <code>xConfiguration Login Remote LDAP VCS BindUsername: "systemmanager"</code></p>  |
| <p><b>Login Remote Protocol: &lt;LDAP&gt;</b></p> <p>The protocol used to connect to the external directory. Default: LDAP.</p> <p>Example: <code>xConfiguration Login Remote Protocol: LDAP</code></p>  |
| <p><b>Login Source Admin: &lt;LocalOnly/RemoteOnly/Both&gt;</b></p> <p>Defines where administrator login credentials are authenticated before access is allowed. Default: LocalOnly.</p> <p><i>LocalOnly:</i> credentials are verified against a local database stored on the Expressway.</p> <p><i>RemoteOnly:</i> credentials are verified against an external credentials directory, for example Windows Active Directory. Note that this disables login access via the default admin account.</p> <p><i>Both:</i> credentials are verified first against a local database stored on the Expressway, and then if no matching account is found the external credentials directory is used instead.</p> <p>Example: <code>xConfiguration Login Source Admin: LocalOnly</code></p> |
| <p><b>Login User [1..n] Name: &lt;S: 0,60&gt;</b></p> <p>Defines the name for this entry in the local authentication database.</p> <p>Example: <code>xConfiguration Login User 1 Name: "alice"</code></p>  |
| <p><b>Login User [1..n] Password: &lt;S: 0,128&gt;</b></p> <p>Defines the password for this entry in the local authentication database.</p> <p>Example: <code>xConfiguration Login User 1 Password: "abcXYZ_123"</code></p>  |

---

Table 12: xConfiguration CLI reference (continued)

**Management Interface HstsMode: <On/Off>**

Determines whether web browsers are instructed to only ever use a secure connection to access this server. Enabling this feature gives added protection against man-in-the-middle (MITM) attacks. Default: On.

*On*: the Strict-Transport-Security header is sent with all responses from the web server, with a 1 year expiry time.

*Off*: the Strict-Transport-Security header is not sent, and browsers work as normal. Note: you must restart the system for any changes to take effect.

Example: `xConfiguration Management Interface HstsMode: On`

**Management Session InactivityTimeout: <0..65535>**

Sets the number of minutes that an administration session (serial port, HTTPS or SSH) may be inactive before the session is timed out. A value of 0 turns session time outs off. Default: 30.

Example: `xConfiguration Management Session InactivityTimeout: 30`

**Management Session MaxConcurrentSessionsTotal: <0..65535>**

The maximum number of concurrent administrator sessions allowed on the system. This includes web, SSH and serial sessions. A value of 0 turns session limits off. Default: 0.

Example: `xConfiguration Management Session MaxConcurrentSessionsTotal: 0`

**Management Session MaxConcurrentSessionsUser: <0..65535>**

The number of concurrent sessions that each individual administrator account is allowed on the system. This includes web, SSH and serial sessions. A value of 0 turns session limits off. Default: 0.

Example: `xConfiguration Management Session MaxConcurrentSessionsUser: 0`

**NTP Server [1..5] Address: <S: 0, 128>**

Sets the IP address or Fully Qualified Domain Name (FQDN) of up to 5 NTP servers to be used when synchronizing system time.

Example: `xConfiguration NTP Server 1 Address: "ntp.server.example.com"`

**Option [1..64] Key: <S: 0, 90>**

Specifies the option key of your software option. These are added to the system in order to add extra functionality, such as increasing the system's capacity. Contact your Cisco support representative for further information.

Example: `xConfiguration Option 1 Key: "1X4757T5-1-60BAD5CD"`

**Policy AdministratorPolicy Mode: <Off/LocalCPL/LocalService/PolicyService>**

Enables and disables use of Call Policy. Default: Off.

*Off*: Disables call policy.

*LocalCPL*: uses policy from an uploaded CPL file.

*LocalService*: uses group policy information and a local file.

*PolicyService*: uses an external policy server.

Example: `xConfiguration Policy AdministratorPolicy Mode: Off`

**Policy AdministratorPolicy Service DefaultCPL: <S: 0,255>**

The CPL used by the Expressway when the remote service is unavailable. Default: `<reject status='403' reason='Service Unavailable'/>`

Example: `xConfiguration Policy AdministratorPolicy Service DefaultCPL: "<reject status='403' reason='Service Unavailable' />"`

**Policy AdministratorPolicy Service Password: <S: 0,82>**

Specifies the password used by the Expressway to log in and query the remote service. The maximum plaintext length is 30 characters, which will then be encrypted.

Example: `xConfiguration Policy AdministratorPolicy Service Password: "password123"`

Table 12: xConfiguration CLI reference (continued)

|   |
|---|
| <p><b>Policy AdministratorPolicy Service Path: &lt;S: 0,255&gt;</b></p> <p>Specifies the URL of the remote service.</p> <p>Example: <code>xConfiguration Policy AdministratorPolicy Service Path: "service"</code></p>  |
| <p><b>Policy AdministratorPolicy Service Protocol: &lt;HTTP/HTTPS&gt;</b></p> <p>Specifies the protocol used to connect to the remote service. Default: HTTPS.</p> <p>Example: <code>xConfiguration Policy AdministratorPolicy Service Protocol: HTTPS</code></p>   |
| <p><b>Policy AdministratorPolicy Service Server [1..3] Address: &lt;S: 0,128&gt;</b></p> <p>Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.</p> <p>Example: <code>xConfiguration Policy AdministratorPolicy Service Server 1 Address: "service.server.example.com"</code></p>   |
| <p><b>Policy AdministratorPolicy Service Status Path: &lt;S: 0..255&gt;</b></p> <p>Specifies the path for obtaining the remote service status. Default: status</p> <p>Example: <code>xConfiguration Policy AdministratorPolicy Service Status Path: status</code></p>   |
| <p><b>Policy AdministratorPolicy Service TLS CRLCheck Mode: &lt;On/Off&gt;</b></p> <p>Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate will be checked against the revocation list of the certificate authority of the certificate. Default: Off.</p> <p>Example: <code>xConfiguration Policy AdministratorPolicy Service TLS CRLCheck Mode: Off</code></p>  |
| <p><b>Policy AdministratorPolicy Service TLS Verify Mode: &lt;On/Off&gt;</b></p> <p>Controls X.509 certificate checking and mutual authentication between this Expressway and the policy service. When enabled, the server's FQDN or IP address, as specified in the address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: On.</p> <p>Example: <code>xConfiguration Policy AdministratorPolicy Service TLS Verify Mode: On</code></p> |
| <p><b>Policy AdministratorPolicy Service UserName: &lt;S: 0,30&gt;</b></p> <p>Specifies the user name used by the Expressway to log in and query the remote policy service.</p> <p>Example: <code>xConfiguration Policy AdministratorPolicy Service UserName: "user123"</code></p>  |
| <p><b>Policy Services Service [1..20] DefaultCPL: &lt;S: 0,255&gt;</b></p> <p>The CPL used by the Expressway when the remote service is unavailable. Default: <code>&lt;reject status='504' reason='Policy Service Unavailable'/&gt;</code></p> <p>Example: <code>xConfiguration Policy Services Service 1 DefaultCPL: "&lt;reject status='403' reason='Service Unavailable' /&gt;"</code></p>  |
| <p><b>Policy Services Service [1..20] Description: &lt;S: 0,64&gt;</b></p> <p>A free-form description of the Policy Service.</p> <p>Example: <code>xConfiguration Policy Services Service 1 Description: "Conference management service"</code></p>   |
| <p><b>Policy Services Service [1..20] HTTPMethod: &lt;POST/GET&gt;</b></p> <p>Specifies the HTTP method type to use for the remote service. Default: POST.</p> <p>Example: <code>xConfiguration Policy Services Service 1 HTTPMethod: POST</code></p>   |
| <p><b>Policy Services Service [1..20] Name: &lt;S: 0,50&gt;</b></p> <p>Assigns a name to this Policy Service.</p> <p>Example: <code>xConfiguration Policy Services Service 1 Name: "Conference handler"</code></p>  |

Table 12: xConfiguration CLI reference (continued)

|   |
|---|
| <p><b>Policy Services Service [1..20] Password: &lt;S: 0,82&gt;</b></p> <p>Specifies the password used by the Expressway to log in and query the remote service. The maximum plaintext length is 30 characters, which will then be encrypted.</p> <p>Example: <code>xConfiguration Policy Services Service 1 Password: "password123"</code></p>   |
| <p><b>Policy Services Service [1..20] Path: &lt;S: 0,255&gt;</b></p> <p>Specifies the URL of the remote service.</p> <p>Example: <code>xConfiguration Policy Services Service 1 Path: "service"</code></p>  |
| <p><b>Policy Services Service [1..20] Protocol: &lt;HTTP/HTTPS&gt;</b></p> <p>Specifies the protocol used to connect to the remote service. Default: HTTPS.</p> <p>Example: <code>xConfiguration Policy Services Service 1 Protocol: HTTPS</code></p>   |
| <p><b>Policy Services Service [1..20] Server [1..3] Address: &lt;S: 0,128&gt;</b></p> <p>Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.</p> <p>Example: <code>xConfiguration Policy Services Service 1 Server 1 Address: "192.168.0.0"</code></p>  |
| <p><b>Policy Services Service [1..20] Status Path: &lt;S: 0..255&gt;</b></p> <p>Specifies the path for obtaining the remote service status. Default: status</p> <p>Example: <code>xConfiguration Policy Services Service 1 Status Path: status</code></p>   |
| <p><b>Policy Services Service [1..20] TLS CRLCheck Mode: &lt;On/Off&gt;</b></p> <p>Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate will be checked against the revocation list of the certificate authority of the certificate. Default: Off.</p> <p>Example: <code>xConfiguration Policy Services Service 1 TLS CRLCheck Mode: Off</code></p>  |
| <p><b>Policy Services Service [1..20] TLS Verify Mode: &lt;On/Off&gt;</b></p> <p>Controls X.509 certificate checking and mutual authentication between this Expressway and the policy service. When enabled, the server's FQDN or IP address, as specified in the address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: On.</p> <p>Example: <code>xConfiguration Policy Services Service 1 TLS Verify Mode: On</code></p> |
| <p><b>Policy Services Service [1..20] UserName: &lt;S: 0,30&gt;</b></p> <p>Specifies the user name used by the Expressway to log in and query the remote service.</p> <p>Example: <code>xConfiguration Policy Services Service 1 UserName: "user123"</code></p>   |
| <p><b>Remote Syslog [1..4] Address: &lt;S: 0..128&gt;</b></p> <p>The IP address or Fully Qualified Domain Name (FQDN) of up to 4 remote syslog servers to which the log is written. These servers must support the BSD or IETF syslog protocols.</p> <p>Example: <code>xConfiguration Remote Syslog 1 Address: "remote_server.example.com"</code></p>   |
| <p><b>Remote Syslog [1..4] Crlcheck: &lt;On/Off&gt;</b></p> <p>Controls whether the certificate supplied by the syslog server is checked against the certificate revocation list (CRL). Default: Off.</p> <p>Example: <code>xConfiguration Remote Syslog 1 Crlcheck: Off</code></p>   |
| <p><b>Remote Syslog [1..4] Format: &lt;bsd/ietf&gt;</b></p> <p>The format in which remote syslog messages are written. Default: bsd.</p> <p>Example: <code>xConfiguration Remote Syslog 1 Format: bsd</code></p>  |

Table 12: xConfiguration CLI reference (continued)

|  |
|--|
| <p><b>Remote Syslog [1..4] Loglevel: &lt;emergency/alert/critical/error/warning/notice/informational/debug&gt;</b></p> <p>Select the minimum severity of log messages to send to this syslog server. Default: informational.</p> <p>Example: <code>xConfiguration Remote Syslog 1 Loglevel: informational</code></p>   |
| <p><b>Remote Syslog [1..4] Mode: &lt;bsd/ietf/ietf_secure/user_defined&gt;</b></p> <p>Select the syslog protocol to use when sending messages to the syslog server, or choose user_defined to configure individually the transport type, port and format. Default: bsd.</p> <p>Example: <code>xConfiguration Remote Syslog 1 Mode: bsd</code></p>  |
| <p><b>Remote Syslog [1..4] Port: &lt;1..65535&gt;</b></p> <p>The UDP/TCP destination port to use. Suggested ports: UDP=514 TCP/TLS=6514. Default: 514.</p> <p>Example: <code>xConfiguration Remote Syslog 1 Port: 514</code></p>   |
| <p><b>Remote Syslog [1..4] Transport: &lt;udp/tcp/tls&gt;</b></p> <p>The transport protocol to use when communicating with the syslog server. If you use TLS encryption, you must upload a suitable CA certificate file. Default: UDP.</p> <p>Example: <code>xConfiguration Remote Syslog 1 Transport: udp</code></p>  |
| <p><b>ResourceUsage Warning Activation Level: &lt;0..100&gt;</b></p> <p>Controls if and when the Expressway will warn that it is approaching its maximum licensed capacity for calls. The number represents the percentage of the maximum that, when reached, will trigger a warning. 0: Warnings will never appear. Default: 90.</p> <p>Example: <code>xConfiguration ResourceUsage Warning Activation Level: 90</code></p> |
| <p><b>SIP Authentication Digest Nonce ExpireDelta: &lt;30..3600&gt;</b></p> <p>Specifies the maximum time (in seconds) that a nonce may be re-used for. Default: 300.</p> <p>Example: <code>xConfiguration SIP Authentication Digest Nonce ExpireDelta: 300</code></p>   |
| <p><b>SIP Authentication Digest Nonce Length: &lt;32..512&gt;</b></p> <p>Length of nonce or cnonce to generate for use in SIP Digest authentication. Default: 60.</p> <p>Example: <code>xConfiguration SIP Authentication Digest Nonce Length: 60</code></p>   |
| <p><b>SIP Authentication Digest Nonce Limit: &lt;1..65535&gt;</b></p> <p>Maximum limit on the number of nonces to store. Default: 10000.</p> <p>Example: <code>xConfiguration SIP Authentication Digest Nonce Limit: 10000</code></p>  |
| <p><b>SIP Authentication Digest Nonce Maximum Use Count: &lt;1..1024&gt;</b></p> <p>Maximum number of times that a nonce generated by the Expressway may be used by a client. Default: 128.</p> <p>Example: <code>xConfiguration SIP Authentication Digest Nonce Maximum Use Count: 128</code></p>   |
| <p><b>SIP Authentication Retry Limit: &lt;1..16&gt;</b></p> <p>The number of times a SIP UA will be challenged due to authentication failure before receiving a 403 Forbidden response. Default: 3.</p> <p>Example: <code>xConfiguration SIP Authentication Retry Limit: 3</code></p>  |
| <p><b>SIP Domain [1..200] Authzone: &lt;S: 0,128&gt;</b></p> <p>The traversal zone to use when delegating credential checks for SIP messages for this domain.</p> <p>Example: <code>xConfiguration SIP Domain 1 Authzone: "traversalzone"</code></p>   |
| <p><b>SIP Domain [1..200] Edge: &lt;On/Off&gt;</b></p> <p>Whether remote and mobile collaboration features are enabled. Default Off.</p> <p>Example: <code>xConfiguration SIP Domain 1 Edge: On</code></p>   |

Table 12: xConfiguration CLI reference (continued)

---

**SIP Domain [1..200] Name: <S: 0,128>**

Specifies a domain for which this Expressway is authoritative. The domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is "100.example-name.com".

Example: `xConfiguration SIP Domain 1 Name: "100.example-name.com"`

---

**SIP GRUU Mode: <On/Off>**

Controls whether GRUU (RFC5627) support is active. Default: On.

Example: `xConfiguration SIP GRUU Mode: On`

---

**SIP MediaRouting ICE Mode: <On/Off>**

Controls whether the Expressway takes the media for an ICE to non-ICE call where the ICE participant is thought to be behind a NAT device. Default: Off.

Example: `xConfiguration SIP MediaRouting ICE Mode: Off`

---

**SIP Mode: <On/Off>**

Determines whether or not the Expressway will provide SIP proxy functionality. Default: On.

Example: `xConfiguration SIP Mode: On`

---

**SIP Require Duo Video Mode: <On/Off>**

Controls whether the Expressway requires the use of the com.tandberg.sdp.duo.enable extension for endpoints that support it. Default: On.

Example: `xConfiguration SIP Require Duo Video Mode: On`

---

**SIP Require UDP BFCP Mode: <On/Off>**

Controls whether the Expressway will require the use of the com.tandberg.udp.bfcp extension for endpoints that support it. Default: On.

Example: `xConfiguration SIP Require UDP BFCP Mode: On`

---

**SIP Routes Route [1..20] Address: <S:0,39>**

Specifies the IP address of the next hop for this route, where matching SIP requests will be forwarded. Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Address: "127.0.0.1"`

---

**SIP Routes Route [1..20] Authenticated: <On/Off>**

Whether to forward authenticated requests. Default: Off. Note: this command is intended for developer use only.

*On*: only forward requests along route if incoming message has been authenticated.

*Off*: always forward messages that match this route.

Example: `xConfiguration SIP Routes Route 1 Authenticated: On`

---

**SIP Session Refresh Minimum: <90..7200>**

The minimum value the Expressway will negotiate for the session refresh interval for SIP calls. For more information see the definition of Min-SE header in RFC 4028. Default: 500.

Example: `xConfiguration SIP Session Refresh Minimum: 500`

---

**SIP Session Refresh Value: <90..7200>**

The maximum time allowed between session refresh requests for SIP calls. For more information see the definition of Session-Expires in RFC 4028. Default: 1800.

Example: `xConfiguration SIP Session Refresh Value: 1800`

---

Table 12: xConfiguration CLI reference (continued)

|   |
|---|
| <p><b>SIP TCP Mode: &lt;On/Off&gt;</b></p> <p>Determines whether incoming and outgoing SIP calls using the TCP protocol will be allowed. Default: On.</p> <p>Example: <code>xConfiguration SIP TCP Mode: On</code></p>  |
| <p><b>SIP TCP Outbound Port End: &lt;1024..65534&gt;</b></p> <p>Specifies the upper port in the range to be used by outbound TCP/TLS SIP connections. Default: 29999.</p> <p>Example: <code>xConfiguration SIP TCP Outbound Port End: 29999</code></p>  |
| <p><b>SIP TCP Outbound Port Start: &lt;1024..65534&gt;</b></p> <p>Specifies the lower port in the range to be used by outbound TCP/TLS SIP connections. Default: 25000.</p> <p>Example: <code>xConfiguration SIP TCP Outbound Port Start: 25000</code></p>  |
| <p><b>SIP TCP Port: &lt;1024..65534&gt;</b></p> <p>Specifies the listening port for incoming SIP TCP calls. Default: 5060.</p> <p>Example: <code>xConfiguration SIP TCP Port: 5060</code></p>   |
| <p><b>SIP TLS Certificate Revocation Checking CRL Mode: &lt;On/Off&gt;</b></p> <p>Controls whether Certificate Revocation Lists (CRLs) are used to perform certificate revocation checking. CRLs can be loaded manually onto the Expressway, downloaded automatically from pre-configured URIs, or downloaded automatically from a CRL distribution point (CDP) URI contained in the X.509 certificate. Default: On.</p> <p>Example: <code>xConfiguration SIP TLS Certificate Revocation Checking CRL Mode: On</code></p> |
| <p><b>SIP TLS Certificate Revocation Checking CRL Network Fetch Mode: &lt;On/Off&gt;</b></p> <p>Controls whether the download of CRLs from the CDP URIs contained in X.509 certificates is allowed. Default: On.</p> <p>Example: <code>xConfiguration SIP TLS Certificate Revocation Checking CRL Network Fetch Mode: On</code></p>   |
| <p><b>SIP TLS Certificate Revocation Checking Mode: &lt;On/Off&gt;</b></p> <p>Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment. Default: Off.</p> <p>Example: <code>xConfiguration SIP TLS Certificate Revocation Checking Mode: Off</code></p>   |
| <p><b>SIP TLS Certificate Revocation Checking OCSP Mode: &lt;On/Off&gt;</b></p> <p>Controls whether the Online Certificate Status Protocol (OCSP) may be used to perform certificate revocation checking. To use OCSP, the X.509 certificate to be checked must contain an OCSP responder URI. Default: On.</p> <p>Example: <code>xConfiguration SIP TLS Certificate Revocation Checking OCSP Mode: On</code></p>   |
| <p><b>SIP TLS Certificate Revocation Checking Source Inaccessibility Behavior: &lt;Ignore/Fail&gt;</b></p> <p>Controls the revocation checking behavior if the revocation source cannot be contacted. Default: Fail.</p> <p><i>Fail</i>: treat the certificate as revoked (and thus do not allow the TLS connection).</p> <p><i>Ignore</i>: treat the certificate as not revoked.</p> <p>Example: <code>xConfiguration SIP TLS Certificate Revocation Checking Source Inaccessibility Behavior: Fail</code></p>           |
| <p><b>SIP TLS Mode: &lt;On/Off&gt;</b></p> <p>Determines whether incoming and outgoing SIP calls using the TLS protocol will be allowed. Default: On.</p> <p>Example: <code>xConfiguration SIP TLS Mode: On</code></p>  |
| <p><b>SIP TLS Port: &lt;1024..65534&gt;</b></p> <p>Specifies the listening port for incoming SIP TLS calls. Default: 5061.</p> <p>Example: <code>xConfiguration SIP TLS Port: 5061</code></p>   |



Table 12: xConfiguration CLI reference (continued)

|   |
|---|
| <p><b>SIP UDP Mode: &lt;On/Off&gt;</b></p> <p>Determines whether incoming and outgoing SIP calls using the UDP protocol will be allowed. Default: Off.</p> <p>Example: <code>xConfiguration SIP UDP Mode: On</code></p>                           |
| <p><b>SIP UDP Port: &lt;1024..65534&gt;</b></p> <p>Specifies the listening port for incoming SIP UDP calls. Default: 5060.</p> <p>Example: <code>xConfiguration SIP UDP Port: 5060</code></p>   |
| <p><b>SNMP CommunityName: &lt;S: 0, 16&gt;</b></p> <p>The Expressway's SNMP community name. Default: public</p> <p>Example: <code>xConfiguration SNMP CommunityName: "public"</code></p>  |
| <p><b>SNMP SystemContact: &lt;S: 0, 70&gt;</b></p> <p>The name of the person who can be contacted regarding issues with the Expressway. Default: Administrator.</p> <p>Example: <code>xConfiguration SNMP SystemContact: Administrator</code></p> |
| <p><b>SNMP SystemLocation: &lt;S: 0, 70&gt;</b></p> <p>The physical location of the system.</p> <p>Example: <code>xConfiguration SNMP SystemLocation: "Server Room 128"</code></p>  |
| <p><b>SNMP V1Mode: &lt;On/Off&gt;</b></p> <p>Enables or disables SNMP Version 1 support. Default: Off.</p> <p>Example: <code>Configuration SNMP V1Mode: Off</code></p>  |
| <p><b>SNMP V2cMode: &lt;On/Off&gt;</b></p> <p>Enables or disables SNMP Version 2c support. Default: On.</p> <p>Example: <code>xConfiguration SNMP V2cMode: On</code></p>  |
| <p><b>SNMP V3AuthenticationMode: &lt;On/Off&gt;</b></p> <p>Enables or disables SNMP Version 3 authentication. Default: On.</p> <p>Example: <code>xConfiguration SNMP V3AuthenticationMode: On</code></p>  |
| <p><b>SNMP V3AuthenticationPassword: &lt;S: 0,215&gt;</b></p> <p>Sets SNMP Version 3 authentication password. It must be at least 8 characters.</p> <p>Example: <code>xConfiguration SNMP V3AuthenticationPassword: "password123"</code></p>      |
| <p><b>SNMP V3AuthenticationType: &lt;MD5/SHA&gt;</b></p> <p>Sets SNMP Version 3 authentication type. Default: SHA.</p> <p>Example: <code>xConfiguration SNMP V3AuthenticationType: SHA</code></p>   |
| <p><b>SNMP V3Mode: &lt;On/Off&gt;</b></p> <p>Enables or disables SNMP Version 3 support. Default: On.</p> <p>Example: <code>xConfiguration SNMPV3 Mode: On</code></p>   |
| <p><b>SNMP V3PrivacyMode: &lt;On/Off&gt;</b></p> <p>Enables or disables SNMP Version 3 privacy. Default: On.</p> <p>Example: <code>xConfiguration SNMP V3PrivacyMode: On</code></p>   |
| <p><b>SNMP V3PrivacyPassword: &lt;S: 0,215&gt;</b></p> <p>Sets SNMP Version 3 privacy password. It must be at least 8 characters.</p> <p>Example: <code>xConfiguration SNMP V3PrivacyPassword: "password123"</code></p>                           |

Table 12: xConfiguration CLI reference (continued)

|   |
|---|
| <p><b>SNMP V3PrivacyType: &lt;DES/AES&gt;</b></p> <p>Sets SNMP Version 3 privacy type. Default: AES.</p> <p>Example: <code>xConfiguration SNMP V3PrivacyType: AES</code></p>  |
| <p><b>SNMP V3UserName: &lt;S: 0,70&gt;</b></p> <p>Sets the username to use when using SNMP V3.</p> <p>Example: <code>xConfiguration SNMP V3UserName: "user123"</code></p>   |
| <p><b>SystemUnit Maintenance Mode: &lt;On/Off&gt;</b></p> <p>Sets the Expressway into maintenance mode. New calls are disallowed. Default: Off.</p> <p>Example: <code>xConfiguration SystemUnit Maintenance Mode: Off</code></p>  |
| <p><b>SystemUnit Name: &lt;S:, 0, 50&gt;</b></p> <p>Defines the name of the Expressway. The system name appears in various places in the web interface and on the front panel of the unit. Choose a name that uniquely identifies the system.</p> <p>Example: <code>xConfiguration SystemUnit Name: "MainHQ"</code></p>   |
| <p><b>TimeZone Name: &lt;S: 0, 64&gt;</b></p> <p>Sets the local time zone of the Expressway. Time zone names follow the POSIX naming convention e.g. Europe/London or America/New_York. Default: GMT.</p> <p>Example: <code>xConfiguration TimeZone Name: "GMT"</code></p>  |
| <p><b>Transform [1..100] Description: &lt;S: 0,64&gt;</b></p> <p>A free-form description of the transform.</p> <p>Example: <code>xConfiguration Transform [1..100] Description: "Change example.net to example.com"</code></p>  |
| <p><b>Transform [1..100] Pattern Behavior: &lt;Strip/Replace&gt;</b></p> <p>How the alias is modified. Default: Strip.</p> <p><i>Strip</i>: removes the matching prefix or suffix from the alias.</p> <p><i>Replace</i>: substitutes the matching part of the alias with the text in replace string.</p> <p><i>AddPrefix</i>: prepends the replace string to the alias.</p> <p><i>AddSuffix</i>: appends the replace string to the alias.</p> <p>Example: <code>xConfiguration Transform 1 Pattern Behavior: Replace</code></p>   |
| <p><b>Transform [1..100] Pattern Replace: &lt;S: 0, 60&gt;</b></p> <p>The text string to use in conjunction with the selected Pattern behavior.</p> <p>Example: <code>xConfiguration Transform 1 Pattern Replace: "example.com"</code></p>  |
| <p><b>Transform [1..100] Pattern String: &lt;S: 0, 60&gt;</b></p> <p>The pattern against which the alias is compared.</p> <p>Example: <code>xConfiguration Transform 1 Pattern String: "example.net"</code></p>   |
| <p><b>Transform [1..100] Pattern Type: &lt;Exact/Prefix/Suffix/Regex&gt;</b></p> <p>How the pattern string must match the alias for the transform to be applied. Default: Prefix.</p> <p><i>Exact</i>: the entire string must exactly match the alias character for character.</p> <p><i>Prefix</i>: the string must appear at the beginning of the alias.</p> <p><i>Suffix</i>: the string must appear at the end of the alias.</p> <p><i>Regex</i>: the string is treated as a regular expression.</p> <p>Example: <code>xConfiguration Transform 1 Pattern Type: Suffix</code></p> |

Table 12: xConfiguration CLI reference (continued)

|   |
|---|
| <p><b>Transform [1..100] Priority: &lt;1..65534&gt;</b></p> <p>Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform. Default: 1 .</p> <p>Example: <code>xConfiguration Transform 1 Priority: 10</code></p>   |
| <p><b>Transform [1..100] State: &lt;Enabled/Disabled&gt;</b></p> <p>Indicates if the transform is enabled or disabled. Disabled transforms are ignored.</p> <p>Example: <code>xConfiguration Transform 1 State: Enabled</code></p>  |
| <p><b>Traversal Media Port End: &lt;1025..65533&gt;</b></p> <p>For traversal calls (where the Expressway takes the media as well as the signaling), specifies the upper port in the range to use for the media. Ports are allocated from this range in pairs, the first of each being even. Thus the range must end with an odd number. Default: 59999 .</p> <p>Example: <code>xConfiguration Traversal Media Port End: 59999</code></p>        |
| <p><b>Traversal Media Port Start: &lt;1024..65532&gt;</b></p> <p>For traversal calls (where the Expressway takes the media as well as the signaling), specifies the lower port in the range to use for the media. Ports are allocated from this range in pairs, the first of each being even. Thus the range must start with an even number. Default: 36000 .</p> <p>Example: <code>xConfiguration Traversal Media Port Start: 36000</code></p> |
| <p><b>Traversal Server H323 Assent CallSignaling Port: &lt;1024..65534&gt;</b></p> <p>The port on the Expressway to use for Assent signaling. Default: 2776 .</p> <p>Example: <code>xConfiguration Traversal Server H323 Assent CallSignaling Port: 2777</code></p>   |
| <p><b>Traversal Server H323 H46018 CallSignaling Port: &lt;1024..65534&gt;</b></p> <p>The port on the Expressway to use for H460.18 signaling. Default: 2777 .</p> <p>Example: <code>xConfiguration Traversal Server H323 H46018 CallSignaling Port: 2777</code></p>  |
| <p><b>Traversal Server TURN Authentication Realm: &lt;S: 1,128&gt;</b></p> <p>The realm sent by the server in its authentication challenges. Default: TANDBERG .</p> <p>Example: <code>xConfiguration Traversal Server TURN Authentication Realm: "TANDBERG"</code></p>   |
| <p><b>Traversal Server TURN Authentication Remote Mode: &lt;On/Off&gt;</b></p> <p>Determines whether the server requires requests to be authenticated. When enabled the server will also authenticate its responses. Default: On.</p> <p>Example: <code>xConfiguration Traversal Server TURN Authentication Remote Mode: On</code></p>  |
| <p><b>Traversal Server TURN Media Port End: &lt;1024..65534&gt;</b></p> <p>The upper port in the range used for TURN relays. Default: 61799.</p> <p>Example: <code>xConfiguration Traversal Server TURN Media Port End: 61799</code></p>  |
| <p><b>Traversal Server TURN Media Port Start: &lt;1024..65534&gt;</b></p> <p>The lower port in the range used for TURN relays. Default: 60000.</p> <p>Example: <code>xConfiguration Traversal Server TURN Media Port Start: 60000</code></p>  |
| <p><b>Traversal Server TURN Mode: &lt;On/Off&gt;</b></p> <p>Determines whether the Expressway offers TURN services to traversal clients. Default: Off .</p> <p>Example: <code>xConfiguration Traversal Server TURN Mode: Off</code></p>   |

Table 12: xConfiguration CLI reference (continued)

|   |
|---|
| <p><b>Traversal Server TURN Port: &lt;1024..65534&gt;</b></p> <p>The listening port for TURN requests. Default: 3478.</p> <p>Example: <code>xConfiguration Traversal Server TURN Port: 3478</code></p>  |
| <p><b>Traversal Server TURN PortRangeEnd: &lt;1024..65534&gt;</b></p> <p>The upper port in the range used for TURN requests. Default: 3483</p> <p>Example: <code>xConfiguration Traversal Server TURN PortRangeEnd: 3483</code></p>   |
| <p><b>Traversal Server TURN PortRangeStart: &lt;1024..65534&gt;</b></p> <p>The lower port in the range used for TURN requests. Default: 3478.</p> <p>Example: <code>xConfiguration Traversal Server TURN PortRangeStart: 3478</code></p>  |
| <p><b>Traversal Server TURN ProtocolMode: &lt;TCP/UDP/Both&gt;</b></p> <p>The permitted protocols for TURN requests. Default: Both.</p> <p>Example: <code>xConfiguration Traversal Server TURN ProtocolMode: Both</code></p>  |
| <p><b>Zones DefaultZone Authentication Mode: &lt;DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials&gt;</b></p> <p>Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials.</p> <p>Example: <code>xConfiguration Zones DefaultZone Authentication Mode: DoNotCheckCredentials</code></p> |
| <p><b>Zones DefaultZone SIP Media Encryption Mode: &lt;Off/On/BestEffort/Auto&gt;</b></p> <p>The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto.</p> <p><i>On:</i> All media must be encrypted.</p> <p><i>Off:</i> All media must be unencrypted.</p> <p><i>BestEffort:</i> Use encryption if available otherwise fallback to unencrypted media.</p> <p><i>Auto:</i> No media encryption policy is applied.</p> <p>Example: <code>xConfiguration Zones DefaultZone SIP Media Encryption Mode: Auto</code></p> |
| <p><b>Zones DefaultZone SIP Record Route Address Type: &lt;IP/Hostname&gt;</b></p> <p>Controls whether the Expressway uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.</p> <p>Example: <code>xConfiguration Zones DefaultZone SIP Record Route Address Type: IP</code></p>  |
| <p><b>Zones DefaultZone SIP TLS Verify Mode: &lt;On/Off&gt;</b></p> <p>Controls whether the hostname contained within the certificate presented by the external system is verified by the Expressway. If enabled, the certificate hostname (also known as the Common Name) is checked against the patterns specified in the Default Zone access rules. Default: Off.</p> <p>Example: <code>xConfiguration Zones DefaultZone SIP TLS Verify Mode: Off</code></p>   |
| <p><b>Zones LocalZone SIP Record Route Address Type: &lt;IP/Hostname&gt;</b></p> <p>Controls whether the Expressway uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.</p> <p>Example: <code>xConfiguration Zones LocalZone SIP Record Route Address Type: IP</code></p>  |
| <p><b>Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: &lt;1..100000000&gt;</b></p> <p>The bandwidth limit (in kbps) applied to any one traversal call being handled by the Expressway (applies only if the mode is set to Limited). Default: 1920.</p> <p>Example: <code>xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: 1920</code></p>   |

Table 12: xConfiguration CLI reference (continued)

|   |
|---|
| <p><b>Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: &lt;Limited/Unlimited/NoBandwidth&gt;</b></p> <p>Determines whether there is a limit on the bandwidth of any one traversal call being handled by the Expressway. Default: Unlimited.</p> <p><i>NoBandwidth</i>: no bandwidth available. No traversal calls can be made.</p> <p>Example: <code>xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: Limited</code></p>   |
| <p><b>Zones LocalZone TraversalSubZone Bandwidth Total Limit: &lt;1..100000000&gt;</b></p> <p>The total bandwidth (in kbps) allowed for all traversal calls being handled by the Expressway (applies only if the mode is set to Limited). Default: 500000 .</p> <p>Example: <code>xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Limit: 500000</code></p>  |
| <p><b>Zones LocalZone TraversalSubZone Bandwidth Total Mode: &lt;Limited/Unlimited/NoBandwidth&gt;</b></p> <p>Determines whether or not there is a limit to the total bandwidth of all traversal calls being handled by the Expressway. Default: Unlimited.</p> <p><i>NoBandwidth</i>: no bandwidth available. No traversal calls can be made.</p> <p>Example: <code>xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: Limited</code></p>   |
| <p><b>Zones Policy Mode: &lt;SearchRules/Directory&gt;</b></p> <p>The mode used when attempting to locate a destination. Default: SearchRules.</p> <p><i>SearchRules</i>: use the configured search rules to determine which zones are queried and in what order.</p> <p><i>Directory</i>: use the facilities of a directory service to direct the request to the correct zones.</p> <p>Example: <code>xConfiguration Zones Policy Mode: SearchRules</code></p>   |
| <p><b>Zones Policy SearchRules Rule [1..2000] Authentication: &lt;Yes/No&gt;</b></p> <p>Specifies whether this search rule applies only to authenticated search requests. Default: No.</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Authentication: No</code></p>   |
| <p><b>Zones Policy SearchRules Rule [1..2000] Description: &lt;S: 0,64&gt;</b></p> <p>A free-form description of the search rule.</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Description: "Send query to the DNS zone"</code></p>   |
| <p><b>Zones Policy SearchRules Rule [1..2000] Mode: &lt;AliasPatternMatch/AnyAlias/AnyIPAddress&gt;</b></p> <p>Determines whether a query is sent to the target zone. Default: AnyAlias.</p> <p><i>AliasPatternMatch</i>: queries the zone only if the alias matches the corresponding pattern type and string.</p> <p><i>AnyAlias</i>: queries the zone for any alias (but not IP address).</p> <p><i>AnyIPAddress</i>: queries the zone for any given IP address (but not alias).</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Mode: AnyAlias</code></p>                                    |
| <p><b>Zones Policy SearchRules Rule [1..2000] Name: &lt;S: 0,50&gt;</b></p> <p>Descriptive name for the search rule.</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Name: "DNS lookup"</code></p>   |
| <p><b>Zones Policy SearchRules Rule [1..2000] Pattern Behavior: &lt;Strip/Leave/Replace&gt;</b></p> <p>Determines whether the matched part of the alias is modified before being sent to the target zone. (Applies to Alias Pattern Match mode only.) Default: Strip.</p> <p><i>Leave</i>: the alias is not modified.</p> <p><i>Strip</i>: the matching prefix or suffix is removed from the alias.</p> <p><i>Replace</i>: the matching part of the alias is substituted with the text in the replace string.</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Pattern Behavior: Strip</code></p> |

Table 12: xConfiguration CLI reference (continued)

|   |
|---|
| <p><b>Zones Policy SearchRules Rule [1..2000] Pattern Replace: &lt;S: 0,60&gt;</b></p> <p>The string to substitute for the part of the alias that matches the pattern. (Applies to Replace pattern behavior only.)</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Pattern Replace: "@example.net"</code></p>  |
| <p><b>Zones Policy SearchRules Rule [1..2000] Pattern String: &lt;S: 0,60&gt;</b></p> <p>The pattern against which the alias is compared. (Applies to Alias Pattern Match mode only.)</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Pattern String: "@example.com"</code></p>  |
| <p><b>Zones Policy SearchRules Rule [1..2000] Pattern Type: &lt;Exact/Prefix/Suffix/Regex&gt;</b></p> <p>How the pattern string must match the alias for the rule to be applied. (Applies to Alias Pattern Match mode only.) Default: Prefix.</p> <p><i>Exact</i>: the entire string must exactly match the alias character for character.</p> <p><i>Prefix</i>: the string must appear at the beginning of the alias.</p> <p><i>Suffix</i>: the string must appear at the end of the alias.</p> <p><i>Regex</i>: the string is treated as a regular expression.</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Pattern Type: Suffix</code></p>         |
| <p><b>Zones Policy SearchRules Rule [1..2000] Priority: &lt;1..65534&gt;</b></p> <p>The order in the search process that this rule is applied, when compared to the priority of the other search rules. All Priority 1 search rules are applied first, followed by all Priority 2 search rules, and so on. Default: 100 .</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Priority: 100</code></p>   |
| <p><b>Zones Policy SearchRules Rule [1..2000] Progress: &lt;Continue/Stop&gt;</b></p> <p>Specifies the ongoing search behavior if the alias matches this search rule. If 'stop' is selected, any rules with the same priority level as this rule are still applied. Default: Continue.</p> <p><i>Continue</i>: continue applying the remaining search rules (in priority order) until the endpoint identified by the alias is found.</p> <p><i>Stop</i>: do not apply any more search rules, even if the endpoint identified by the alias is not found in the target zone.</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Progress: Continue</code></p> |
| <p><b>Zones Policy SearchRules Rule [1..2000] Protocol: &lt;Any/H323/SIP&gt;</b></p> <p>The source protocol required for the rule to match.</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Protocol: Any</code></p>   |
| <p><b>Zones Policy SearchRules Rule [1..2000] Source Mode: &lt;Any/AllZones/LocalZone/Named&gt;</b></p> <p>The sources of the requests for which this rule applies. Default: Any.</p> <p><i>Any</i>: neighbor or traversal zones, and any non-registered devices.</p> <p><i>All zones</i>: neighbor or traversal zones.</p> <p><i>Named</i>: A specific Zone or SubZone.</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Source Mode: Any</code></p>   |
| <p><b>Zones Policy SearchRules Rule [1..2000] Source Name: &lt;S: 0..50&gt;</b></p> <p>The name of the source (Sub)Zone for which this rule applies.</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Source Name: "Local Office"</code></p>  |
| <p><b>Zones Policy SearchRules Rule [1..2000] State: &lt;Enabled/Disabled&gt;</b></p> <p>Indicates if the search rule is enabled or disabled. Disabled search rules are ignored. Default: Enabled .</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 State: Enabled</code></p>  |

Table 12: xConfiguration CLI reference (continued)

|  |
|--|
| <p><b>Zones Policy SearchRules Rule [1..2000] Target Name: &lt;S: 0,50&gt;</b></p> <p>The zone or policy service to query if the alias matches the search rule.</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Target Name: "Sales Office"</code></p>  |
| <p><b>Zones Policy SearchRules Rule [1..2000] Target Type: &lt;Zone/PolicyService&gt;</b></p> <p>The type of target this search rule applies to.</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Target Type: Zone</code></p>   |
| <p><b>Zones Zone [1..1000] DNS IncludeAddressRecord: &lt;On/Off&gt;</b></p> <p>Determines whether, if no NAPTR (SIP) or SRV (SIP and H.323) records have been found for the dialed alias via this zone, the Expressway will then query for A and AAAA DNS Records. Default: Off .</p> <p>Example: <code>xConfiguration Zones Zone 1 DNS IncludeAddressRecord: Off</code></p>   |
| <p><b>Zones Zone [1..1000] DNS Interworking SIP Audio DefaultCodec: &lt;G711u/G711a/G722_48/G722_56/G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48/G723_1/G728/G729/AACLD_48/AACLD_56/AACLD_64/AMR&gt;</b></p> <p>Specifies which audio codec to use when empty INVITEs are not allowed. Default: G711u .</p> <p>Example: <code>xConfiguration Zones Zone 1 DNS Interworking SIP Audio DefaultCodec: G711u</code></p>   |
| <p><b>Zones Zone [1..1000] DNS Interworking SIP EmptyInviteAllowed: &lt;On/Off&gt;</b></p> <p>Controls if the Expressway will generate a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. Default: On.</p> <p><i>On:</i> SIP INVITEs with no SDP will be generated and sent to this neighbor.</p> <p><i>Off:</i> SIP INVITEs will be generated and a pre-configured SDP will be inserted before the INVITEs are sent to this neighbor.</p> <p>Example: <code>xConfiguration Zones Zone 1 DNS Interworking SIP EmptyInviteAllowed: On</code></p> |
| <p><b>Zones Zone [1..1000] DNS Interworking SIP Video DefaultBitrate: &lt;64..65535&gt;</b></p> <p>Specifies which video bit rate to use when empty INVITEs are not allowed. Default: 384 .</p> <p>Example: <code>xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultBitrate: 384</code></p>  |
| <p><b>Zones Zone [1..1000] DNS Interworking SIP Video DefaultCodec: &lt;None/H261/H263/H263p/H263pp/H264&gt;</b></p> <p>Specifies which video codec to use when empty INVITEs are not allowed. Default: H263 .</p> <p>Example: <code>xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultCodec: H263</code></p>  |
| <p><b>Zones Zone [1..1000] DNS Interworking SIP Video DefaultResolution: &lt;None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA&gt;</b></p> <p>Specifies which video resolution to use when empty INVITEs are not allowed. Default: CIF .</p> <p>Example: <code>xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultResolution: CIF</code></p>   |
| <p><b>Zones Zone [1..1000] DNS SIP Default Transport: &lt;UDP/TCP/TLS&gt;</b></p> <p>Determines which transport type is used for SIP calls from the DNS zone, when DNS NAPTR records and SIP URI parameters do not provide the preferred transport information. RFC 3263 suggests that UDP should be used. Default: UDP.</p> <p>Example: <code>xConfiguration Zones Zone [1..1000] DNS SIP Default Transport: UDP</code></p>   |
| <p><b>Zones Zone [1..1000] DNS SIP Duo Video Filter Mode: &lt;On/Off&gt;</b></p> <p>Determines whether INVITE requests sent to this zone filter out Duo Video. This option may be required to enable interoperability with SIP devices that do not support Duo Video. Default: Off .</p> <p><i>On:</i> the second video line in any outgoing INVITE request is removed.</p> <p><i>Off:</i> INVITE requests are not modified.</p> <p>Example: <code>xConfiguration Zones Zone 1 DNS SIP Duo Video Filter Mode: Off</code></p>   |

Table 12: xConfiguration CLI reference (continued)

**Zones Zone [1..1000] DNS SIP Media Encryption Mode: <Off/On/BestEffort/Auto>**

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto.

*On*: All media must be encrypted.

*Off*: All media must be unencrypted.

*BestEffort*: Use encryption if available otherwise fallback to unencrypted media.

*Auto*: No media encryption policy is applied.

Example: `xConfiguration Zones Zone 1 DNS SIP Media Encryption Mode: Auto`

**Zones Zone [1..1000] DNS SIP Poison Mode: <On/Off>**

Determines whether SIP requests sent out to this zone will be "poisoned" such that if they are received by the local Expressway again they will be rejected. Default: Off .

*On*: SIP requests sent out via this zone that are received again by this Expressway will be rejected.

*Off*: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.

Example: `xConfiguration Zones Zone 1 DNS SIP Poison Mode: Off`

**Zones Zone [1..1000] DNS SIP Record Route Address Type: <IP/Hostname>**

Controls whether the Expressway uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.

Example: `xConfiguration Zones Zone 1 DNS SIP Record Route Address Type: IP`

**Zones Zone [1..1000] DNS SIP SDP Attribute Line Limit Length: <80..65535>**

If SIP SDP attribute line limit mode is set to On, sets the maximum line length of a=fmtp SDP lines. Default: 130 .

Example: `xConfiguration Zones Zone 1 DNS SIP SDP Attribute Line Limit Length: 130`

**Zones Zone [1..1000] DNS SIP SDP Attribute Line Limit Mode: <On/Off>**

Determines whether requests containing SDP sent out to this zone will have the length of a=fmtp lines restricted.

*On*: the length will be truncated to the maximum length specified by the SIP SDP attribute line limit length setting.

*Off*: the length will not be truncated.

Example: `xConfiguration Zones Zone 1 DNS SIP SDP Attribute Line Limit Mode: Off`

**Zones Zone [1..1000] DNS SIP SearchAutoResponse: <On/Off>**

Controls what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. Default: Off .

*Off*: a SIP OPTION message will be sent to the zone.

*On*: searches will be responded to automatically, without being forwarded to the zone.

Example: `xConfiguration Zones Zone 1 DNS SIP SearchAutoResponse: Off`

**Zones Zone [1..1000] DNS SIP TLS Verify Mode: <On/Off>**

Controls X.509 certificate checking between this Expressway and the destination system server returned by the DNS lookup. When enabled, the domain name submitted to the DNS lookup must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: Off .

Example: `xConfiguration Zones Zone 1 DNS SIP TLS Verify Mode: On`

**Zones Zone [1..1000] DNS SIP TLS Verify Subject Name: <S: 0..128>**

The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). If empty then the domain portion of the resolved URI is used.

Example: `xConfiguration Zones Zone 1 DNS SIP TLS Verify Subject Name: "example.com"`



Table 12: xConfiguration CLI reference (continued)

---

**Zones Zone [1..1000] DNS SIP UDP BFCP Filter Mode: <On/Off>**

Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. Default: Off .

*On:* any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled.

*Off:* INVITE requests are not modified.

Example: `xConfiguration Zones Zone 1 DNS SIP UDP BFCP Filter Mode: Off`

---

**Zones Zone [1..1000] DNS ZoneProfile: <Default/Custom/CiscoUnifiedCommunicationsManager/CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDevice/LocalB2BUAService>**

Determines how the zone's advanced settings are configured.

*Default:* uses the factory defaults.

*Custom:* allows you to configure each setting individually.

*Preconfigured profiles:* alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.

Example: `xConfiguration Zones Zone 1 DNS ZoneProfile: Default`

---

**Zones Zone [1..1000] ENUM DNSSuffix: <S: 0, 128>**

The DNS zone to append to the transformed E.164 number to create an ENUM host name which this zone is then queried for.

Example: `xConfiguration Zones Zone 2 ENUM DNSSuffix: "e164.arpa"`

---

**Zones Zone [1..1000] H323 Mode: <On/Off>**

Determines whether H.323 calls will be allowed to and from this zone. Default: On .

Example: `xConfiguration Zones Zone 2 H323 Mode: On`

---

**Zones Zone [1..1000] HopCount: <1..255>**

Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used. Default: 15 .

Example: `xConfiguration Zones Zone 2 HopCount: 15`

---

**Zones Zone [1..1000] Name: <S: 1, 50>**

Assigns a name to this zone.

Example: `xConfiguration Zones Zone 3 Name: "UK Sales Office"`

---

**Zones Zone [1..1000] Neighbor Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>**

Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials.

Example: `xConfiguration Zones Zone 3 Neighbor Authentication Mode: DoNotCheckCredentials`

---

**Zones Zone [1..1000] Neighbor H323 CallSignaling Port: <1024..65534>**

The port on the neighbor to use for H.323 calls to and from this Expressway. Default: 1720 .

Example: `xConfiguration Zones Zone 3 Neighbor H323 CallSignaling Port: 1720`

---

**Zones Zone [1..1000] Neighbor H323 Port: <1024..65534>**

The port on the neighbor to use for H.323 searches to and from this Expressway. Default: 1719 .

Example: `xConfiguration Zones Zone 3 Neighbor H323 Port: 1719`

---

Table 12: xConfiguration CLI reference (continued)

**Zones Zone [1..1000] Neighbor H323 SearchAutoResponse: <On/Off>**

Determines what happens when the Expressway receives a H323 search, destined for this zone. Default: Off.

*Off:* an LRQ message will be sent to the zone.

*On:* searches will be responded to automatically, without being forwarded to the zone.

Example: `xConfiguration Zones Zone 3 Neighbor H323 SearchAutoResponse: Off`

**Zones Zone [1..1000] Neighbor Interworking SIP Audio DefaultCodec: <G711u/G711a/G722\_48/G722\_56/G722\_64/G722\_1\_16/G722\_1\_24/G722\_1\_32/G722\_1\_48/G723\_1/G728/G729/AACLD\_48/AACLD\_56/AACLD\_64/AMR>**

Specifies which audio codec to use when empty INVITEs are not allowed. Default: G711u .

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Audio DefaultCodec: G711u`

**Zones Zone [1..1000] Neighbor Interworking SIP EmptyInviteAllowed: <On/Off>**

Determines whether the Expressway will generate a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. Default: On .

*On:* SIP INVITEs with no SDP will be generated and sent to this neighbor.

*Off:* SIP INVITEs will be generated and a pre-configured SDP will be inserted before the INVITEs are sent to this neighbor.

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP EmptyInviteAllowed: On`

**Zones Zone [1..1000] Neighbor Interworking SIP Encryption EncryptSRTCP: <Yes/No>**

Controls if the Expressway offers encrypted SRTCP in calls to this zone. The Expressway will send an INFO request. Default: No.

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Encryption EncryptSRTCP: No`

**Zones Zone [1..1000] Neighbor Interworking SIP Search Strategy: <Options/Info>**

Determines how the Expressway will search for SIP endpoints when interworking an H.323 call. Default: Options .

*Options:* the Expressway will send an OPTIONS request.

*Info:* the Expressway will send an INFO request.

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Search Strategy: Options`

**Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultBitrate: <64..65535>**

Specifies which video bit rate to use when empty INVITEs are not allowed. Default: 384 .

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultBitrate: 384`

**Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264>**

Specifies which video codec to use when empty INVITEs are not allowed. Default: H263 .

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultCodec: H263`

**Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>**

Specifies which video resolution to use when empty INVITEs are not allowed. Default: CIF .

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultResolution: CIF`

**Zones Zone [1..1000] Neighbor Monitor: <Yes/No>**

Specifies whether the zone monitors the aliveness of its neighbor peers. H323 LRQs and/or SIP OPTIONS will be periodically sent to the peers. If any peer fails to respond, that peer will be marked as inactive. If no peer manages to respond the zone will be marked as inactive. Default: Yes.

Example: `xConfiguration Zones Zone 3 Neighbor Monitor: Yes`

Table 12: xConfiguration CLI reference (continued)

**Zones Zone [1..1000] Neighbor Peer [1..6] Address: <S:0,128>**

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the neighbor. If the neighbor zone is an Expressway cluster, this will be one of the peers in that cluster.

Example: `xConfiguration Zones Zone 3 Neighbor Peer 1 Address: "192.44.0.18"`

**Zones Zone [1..1000] Neighbor SIP Authentication Trust Mode: <On/Off>**

Controls if authenticated SIP messages (ones containing a P-Asserted-Identity header) from this zone are trusted. Default: Off .

*On*: messages are trusted without further challenge.

*Off*: messages are challenged for authentication.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Authentication Trust Mode: On`

**Zones Zone [1..1000] Neighbor SIP B2BUA Service Identifier: <0..64>**

The identifier that represents an instance of a local SIP Back-to-Back User Agent service.

Example: `xConfiguration Zones Zone 3 Neighbor SIP B2BUA Service Identifier: 1`

**Zones Zone [1..1000] Neighbor SIP ClassFiveResponseLiveness: <Yes/No>**

Specifies whether Class 5 SIP responses from neighbor peers result in the zone being considered alive for use. Default: Yes.

Example: `xConfiguration Zones Zone 3 Neighbor SIP ClassFiveResponseLiveness: Yes`

**Zones Zone [1..1000] Neighbor SIP Duo Video Filter Mode: <On/Off>**

Determines whether INVITE requests sent to this zone filter out Duo Video. This option may be required to enable interoperability with SIP devices that do not support Duo Video. Default: Off.

*On*: the second video line in any outgoing INVITE request is removed.

*Off*: INVITE requests are not modified.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Duo Video Filter Mode: Off`

**Zones Zone [1..1000] Neighbor SIP Encryption Mode: <Auto/Microsoft/Off>**

Determines how the Expressway handles encrypted SIP calls on this zone. Default: Auto.

*Auto*: SIP calls are encrypted if a secure SIP transport (TLS) is used.

*Microsoft*: SIP calls are encrypted using MS-SRTP.

*Off*: SIP calls are never encrypted.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Encryption Mode: Auto`

**Zones Zone [1..1000] Neighbor SIP MIME Strip Mode: <On/Off>**

Controls whether multipart MIME stripping is performed on requests from this zone. This must be set to On for connections to a Microsoft Office Communications Server 2007. Default: Off .

Example: `xConfiguration Zones Zone 3 Neighbor SIP MIME Strip Mode: Off`

**Zones Zone [1..1000] Neighbor SIP Media Encryption Mode: <Off/On/BestEffort/Auto>**

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto

*On*: All media must be encrypted.

*Off*: All media must be unencrypted.

*BestEffort*: Use encryption if available otherwise fallback to unencrypted media.

*Auto*: No media encryption policy is applied.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Media Encryption Mode: Auto`

Table 12: xConfiguration CLI reference (continued)

|   |
|---|
| <p><b>Zones Zone [1..1000] Neighbor SIP MediaRouting Mode: &lt;Auto/Signaled/Latching&gt;</b></p> <p>How the Expressway handles media for calls to and from this neighbor, and where it will forward the media destined for this neighbor. Default: Auto.</p> <p><i>Signaled:</i> media is always taken for calls to and from this neighbor. It will be forwarded as signaled in the SDP received from this neighbor.</p> <p><i>Latching:</i> media is always taken for calls to and from this neighbor. It will be forwarded to the IP address and port from which media from this neighbor is received.</p> <p><i>Auto:</i> media is only taken if the call is a traversal call. If this neighbor is behind a NAT the Expressway will forward the media to the IP address and port from which media from this zone is received (latching). Otherwise it will forward the media to the IP address and port signaled in the SDP (signaled).</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP MediaRouting Mode: Auto</code></p> |
| <p><b>Zones Zone [1..1000] Neighbor SIP Poison Mode: &lt;On/Off&gt;</b></p> <p>Controls whether SIP requests sent out to this zone will be "poisoned" such that if they are received by the local Expressway again they will be rejected. Default: Off.</p> <p><i>On:</i> SIP requests sent out via this zone that are received again by this Expressway will be rejected.</p> <p><i>Off:</i> SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP Poison Mode: Off</code></p>  |
| <p><b>Zones Zone [1..1000] Neighbor SIP Port: &lt;1024..65534&gt;</b></p> <p>Specifies the port on the neighbor to be used for SIP calls to and from this Expressway. Default: 5061.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP Port: 5061</code></p>   |
| <p><b>Zones Zone [1..1000] Neighbor SIP ProxyRequire Strip List: &lt;S: 0,255&gt;</b></p> <p>A comma separated list of option tags to search for and remove from Proxy-Require headers in SIP requests received from this zone. By default, no option tags are specified.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP ProxyRequire Strip List: "com.example.something,com.example.somethingelse"</code></p>  |
| <p><b>Zones Zone [1..1000] Neighbor SIP RFC3327 Enabled: &lt;Yes/No&gt;</b></p> <p>Controls whether the Expressway will insert RFC3327 Path headers when proxying REGISTER messages toward this zone. If disabled the Expressway will instead rewrite the contact header to allow interworking with SIP registrars that do not support RFC3327. Default: Yes.</p> <p>Example: <code>xConfiguration Zones Zone [1..1000] Neighbor SIP RFC3327 Enabled: Yes</code></p>  |
| <p><b>Zones Zone [1..1000] Neighbor SIP Record Route Address Type: &lt;IP/Hostname&gt;</b></p> <p>Controls whether the Expressway uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP Record Route Address Type: IP</code></p>  |
| <p><b>Zones Zone [1..1000] Neighbor SIP SDP Attribute Line Limit Length: &lt;80..65535&gt;</b></p> <p>If SIP SDP attribute line limit mode is set to On, sets the maximum line length of a=fmtp SDP lines. Default: 130.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP SDP Attribute Line Limit Length: 130</code></p>   |
| <p><b>Zones Zone [1..1000] Neighbor SIP SDP Attribute Line Limit Mode: &lt;On/Off&gt;</b></p> <p>Determines whether requests containing SDP sent out to this zone will have the length of a=fmtp lines restricted. Default: Off.</p> <p><i>On:</i> the length will be truncated to the maximum length specified by the SIP SDP attribute line limit length setting.</p> <p><i>Off:</i> the length will not be truncated.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP SDP Attribute Line Limit Mode: Off</code></p>   |

Table 12: xConfiguration CLI reference (continued)

**Zones Zone [1..1000] Neighbor SIP SearchAutoResponse: <On/Off>**

Controls what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone.  
Default: Off.

*Off:* a SIP OPTION message will be sent to the zone.

*On:* searches will be responded to automatically, without being forwarded to the zone.

Example: `xConfiguration Zones Zone 3 Neighbor SIP SearchAutoResponse: Off`

**Zones Zone [1..1000] Neighbor SIP TLS Verify Mode: <On/Off>**

Controls X.509 certificate checking and mutual authentication for inbound and outbound connections between this Expressway and the neighbor system. When enabled, the neighbor system's FQDN or IP address, as specified in the Peer address field, must be contained within the neighbor's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes).  
Default: Off.

Example: `xConfiguration Zones Zone 3 Neighbor SIP TLS Verify Mode: On`

**Zones Zone [1..1000] Neighbor SIP Transport: <UDP/TCP/TLS>**

Determines which transport type will be used for SIP calls to and from this neighbor. Default: TLS.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Transport: TLS`

**Zones Zone [1..1000] Neighbor SIP UDP BFCP Filter Mode: <On/Off>**

Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. Default: Off.

*On:* any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled.

*Off:* INVITE requests are not modified.

Example: `xConfiguration Zones Zone 3 Neighbor SIP UDP BFCP Filter Mode: Off`

**Zones Zone [1..1000] Neighbor SIP UPDATE Strip Mode: <On/Off>**

Determines whether the Expressway strips the UPDATE method from the Allow header of all requests and responses going to and from this zone. Default: Off.

Example: `xConfiguration Zones Zone 3 Neighbor SIP UPDATE Strip Mode: Off`

**Zones Zone [1..1000] Neighbor SignalingRouting Mode: <Auto/Always>**

Specifies how the Expressway handles the signaling for calls to and from this neighbor. Default: Auto.

*Auto:* Signaling will be taken as determined by the Call Routed Mode configuration.

*Always:* Signaling will always be taken for calls to or from this neighbor, regardless of the Call Routed Mode configuration.

Example: `xConfiguration Zones Zone 3 Neighbor SignalingRouting Mode: Auto`

**Zones Zone [1..1000] Neighbor ZoneProfile: <Default/Custom/CiscoUnifiedCommunicationsManager/CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDevice/LocalB2BUAService>**

Determines how the zone's advanced settings are configured.

*Default:* uses the factory defaults.

*Custom:* allows you to configure each setting individually.

*Preconfigured profiles:* alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.

Example: `xConfiguration Zones Zone 3 Neighbor ZoneProfile: Default`

**Zones Zone [1..1000] SIP Mode: <On/Off>**

Determines whether SIP calls will be allowed to and from this zone. Default: On.

Example: `xConfiguration Zones Zone 3 SIP Mode: On`

Table 12: xConfiguration CLI reference (continued)

**Zones Zone [1..1000] TraversalClient Authentication Mode:****<DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>**

Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials.

Example: `xConfiguration Zones Zone 4 TraversalClient Authentication Mode: DoNotCheckCredentials`

**Zones Zone [1..1000] TraversalClient Authentication Password: <S: 0,215>**

The password used by the Expressway when connecting to the traversal server. The maximum plaintext length is 128 characters, which is then encrypted.

Example: `xConfiguration Zones Zone 4 TraversalClient Authentication Password: "password123"`

**Zones Zone [1..1000] TraversalClient Authentication UserName: <S: 0,128>**

The user name used by the Expressway when connecting to the traversal server.

Example: `xConfiguration Zones Zone 4 TraversalClient Authentication UserName: "clientname"`

**Zones Zone [1..1000] TraversalClient H323 Port: <1024..65534>**

The port on the traversal server to use for H.323 firewall traversal calls from this Expressway. If the traversal server is an Expressway-E, this must be the port number that is configured on the Expressway-E's traversal server zone associated with this Expressway.

Example: `xConfiguration Zones Zone 4 TraversalClient H323 Port: 2777`

**Zones Zone [1..1000] TraversalClient H323 Protocol: <Assent/H46018>**

Determines which of the two firewall traversal protocols will be used for calls to and from the traversal server. Note: the same protocol must be set on the server for calls to and from this traversal client. Default: Assent.

Example: `xConfiguration Zones Zone 4 TraversalClient H323 Protocol: Assent`

**Zones Zone [1..1000] TraversalClient Peer [1..6] Address: <S:0,128>**

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the traversal server. If the traversal server is an Expressway-E cluster, this will be one of the peers in that cluster.

Example: `xConfiguration Zones Zone 4 TraversalClient Peer 1 Address: "10.192.168.1"`

**Zones Zone [1..1000] TraversalClient RetryInterval: <1..65534>**

The interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. Default: 120.

Example: `xConfiguration Zones Zone 4 TraversalClient RetryInterval: 120`

**Zones Zone [1..1000] TraversalClient SIP Media Encryption Mode: <Off/On/BestEffort/Auto>**

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto.

*On:* All media must be encrypted.

*Off:* All media must be unencrypted.

*BestEffort:* Use encryption if available otherwise fallback to unencrypted media.

*Auto:* No media encryption policy is applied.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Media Encryption Mode: Auto`

**Zones Zone [1..1000] TraversalClient SIP Poison Mode: <On/Off>**

Controls whether SIP requests sent out to this zone are "poisoned" such that if they are received by the local Expressway again they will be rejected. Default: Off.

*On:* SIP requests sent out via this zone that are received again by this Expressway will be rejected.

*Off:* SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Poison Mode: Off`

Table 12: xConfiguration CLI reference (continued)

**Zones Zone [1..1000] TraversalClient SIP Port: <1024..65534>**

Specifies the port on the traversal server to be used for SIP calls from this Expressway. If your traversal server is an Expressway-E, this must be the port number that has been configured in the traversal server zone for this Expressway.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Port: 5061`

**Zones Zone [1..1000] TraversalClient SIP Protocol: <Assent/TURN/ICE>**

Determines which firewall traversal protocol will be used for SIP calls to and from the traversal server. Note: the same protocol must be set on the server for calls to and from this traversal client. Default: Assent.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Protocol: Assent`

**Zones Zone [1..1000] TraversalClient SIP TLS Verify Mode: <On/Off>**

Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal server. When enabled, the server's FQDN or IP address, as specified in the Peer address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: Off.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP TLS Verify Mode: On`

**Zones Zone [1..1000] TraversalClient SIP Transport: <TCP/TLS>**

Determines which transport type will be used for SIP calls to and from the traversal server. Default: TLS.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Transport: TLS`

**Zones Zone [1..1000] TraversalServer Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>**

Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials.

Example: `xConfiguration Zones Zone 5 TraversalServer Authentication Mode: DoNotCheckCredentials`

**Zones Zone [1..1000] TraversalServer Authentication UserName: <S: 0,128>**

The name used by the traversal client when authenticating with the traversal server. If the traversal client is an Expressway, this must be the Expressway's authentication user name. If the traversal client is a gatekeeper, this must be the gatekeeper's System Name.

Example: `xConfiguration Zones Zone 5 TraversalServer Authentication UserName: "User123"`

**Zones Zone [1..1000] TraversalServer H323 H46019 Demultiplexing Mode: <On/Off>**

Determines whether the Expressway will operate in demultiplexing mode for calls from the traversal client. Default: Off.

*On*: allows use of the same two ports for all calls.

*Off*: each call will use a separate pair of ports for media.

Example: `xConfiguration Zones Zone 5 TraversalServer H323 H46019 Demultiplexing Mode: Off`

**Zones Zone [1..1000] TraversalServer H323 Port: <1024..65534>**

Specifies the port on the Expressway being used for H.323 firewall traversal from this traversal client. Default: 6001, incrementing by 1 for each new zone.

Example: `xConfiguration Zones Zone 5 TraversalServer H323 Port: 2777`

**Zones Zone [1..1000] TraversalServer H323 Protocol: <Assent/H46018>**

Determines which of the two firewall traversal protocols will be used for calls to and from the traversal client. Note: the same protocol must be set on the client for calls to and from this traversal server. Default: Assent.

Example: `xConfiguration Zones Zone 5 TraversalServer H323 Protocol: Assent`

Table 12: xConfiguration CLI reference (continued)

**Zones Zone [1..1000] TraversalServer SIP Media Encryption Mode: <Off/On/BestEffort/Auto>**

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto

*On*: All media must be encrypted.

*Off*: All media must be unencrypted.

*BestEffort*: Use encryption if available otherwise fallback to unencrypted media.

*Auto*: No media encryption policy is applied.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Media Encryption Mode: Auto`

**Zones Zone [1..1000] TraversalServer SIP Poison Mode: <On/Off>**

Controls whether SIP requests sent out to this zone are "poisoned" such that if they are received by the local Expressway again they will be rejected. Default: Off.

*On*: SIP requests sent out via this zone that are received again by this Expressway will be rejected.

*Off*: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Poison Mode: Off`

**Zones Zone [1..1000] TraversalServer SIP Port: <1024..65534>**

The port on the Expressway being used for SIP firewall traversal from this traversal client. Default: 7001, incrementing by 1 for each new zone.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Port: 5061`

**Zones Zone [1..1000] TraversalServer SIP Protocol: <Assent/TURN/ICE>**

Determines which firewall traversal protocol will be used for SIP calls to and from the traversal client. Note: the same protocol must be set on the client for calls to and from this traversal server. Default: Assent.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Protocol: Assent`

**Zones Zone [1..1000] TraversalServer SIP TLS Verify Mode: <On/Off>**

Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified. Default: Off.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Mode: On`

**Zones Zone [1..1000] TraversalServer SIP TLS Verify Subject Name: <S: 0,128>**

The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes).

Example: `xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Subject Name: "myclientname"`

**Zones Zone [1..1000] TraversalServer SIP Transport: <TCP/TLS>**

Determines which of the two transport types will be used for SIP calls between the traversal client and Expressway. Default: TLS.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Transport: TLS`

**Zones Zone [1..1000] TraversalServer TCPProbe KeepAliveInterval: <1..65534>**

Sets the interval (in seconds) with which the traversal client will send a TCP probe to the Expressway once a call is established, in order to keep the firewall's NAT bindings open. Default: 20.

Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe KeepAliveInterval: 20`

**Zones Zone [1..1000] TraversalServer TCPProbe RetryCount: <1..65534>**

Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway. Default: 5.

Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryCount: 5`



Table 12: xConfiguration CLI reference (continued)

**Zones Zone [1..1000] TraversalServer TCPProbe RetryInterval: <1..65534>**

Sets the frequency (in seconds ) with which the traversal client will send a TCP probe to the Expressway. Default: 2 .

Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryInterval: 2`

**Zones Zone [1..1000] TraversalServer UDPProbe KeepAliveInterval: <1..65534>**

Sets the interval (in seconds) with which the traversal client will send a UDP probe to the Expressway once a call is established, in order to keep the firewall's NAT bindings open. Default: 20.

Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe KeepAliveInterval: 20`

**Zones Zone [1..1000] TraversalServer UDPProbe RetryCount: <1..65534>**

Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway. Default: 5.

Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryCount: 5`

**Zones Zone [1..1000] TraversalServer UDPProbe RetryInterval: <1..65534>**

Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway. Default: 2.

Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryInterval: 2`

**Zones Zone [1..1000] Type: <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>**

Determines the nature of the specified zone, in relation to the local Expressway.

*Neighbor*: the new zone will be a neighbor of the local Expressway.

*TraversalClient*: there is a firewall between the zones, and the local Expressway is a traversal client of the new zone.

*TraversalServer*: there is a firewall between the zones and the local Expressway is a traversal server for the new zone.

*ENUM*: the new zone contains endpoints discoverable by ENUM lookup.

*DNS*: the new zone contains endpoints discoverable by DNS lookup.

Example: `xConfiguration Zones Zone 3 Type: Neighbor`

## Command reference — xCommand

The **xCommand** group of commands are used to add and delete items and issue system commands.

The following section lists all the currently available **xCommand** commands.

To issue a command, type the command as shown, followed by one or more of the given parameters and values. The valid values for each parameter are indicated in the angle brackets following each parameter, using the following notation:

| Format                | Meaning   |
|-----------------------|---|
| <0..63>               | Indicates an integer value is required. The numbers indicate the minimum and maximum value.<br>In this example the value must be in the range 0 to 63.  |
| <S: 7,15>             | An <b>S</b> indicates a string value, to be enclosed in quotation marks, is required. The numbers indicate the minimum and maximum number of characters for the string.<br>In this example the string must be between 7 and 15 characters long. |
| <Off/Direct/Indirect> | Lists the set of valid values for the command. Do not enclose the value in quotation marks  |
| (r)                   | (r) indicates that this is a required parameter. Note that the (r) is not part of the command itself.   |

To obtain information about using each of the **xCommand** commands from within the CLI, type:

- **xCommand** or **xCommand ?** to return a list of all available **xCommand** commands.
- **xCommand ??** to return all current **xCommand** commands, along with a description of each command, a list of its parameters, and for each parameter its valuespaces and description.
- **xCommand <command> ?** to return a description of the command, a list of its parameters, and for each parameter its valuespaces and description.

### xCommand commands

All of the available **xCommand** commands are listed in the table below:

|   |
|---|
| <p><b>AdminAccountAdd</b><br/>Adds a local administrator account.<br/>Name(r): &lt;S: 0, 128&gt;<br/>    The username for this account.<br/>Password(r): &lt;Password&gt;<br/>    The password for this account.<br/>AccessAPI: &lt;On/Off&gt;<br/>    Whether this account is allowed to access the system's status and configuration via the API. Default: On.<br/>AccessWeb: &lt;On/Off&gt;<br/>    Whether this account is allowed to log in to the system using the web interface. Default: On.<br/>Enabled: &lt;On/Off&gt;<br/>    Indicates if the account is enabled or disabled. Access is denied to disabled accounts. Default: On.<br/>Example: <b>xCommand AdminAccountAdd Name: "bob_smith" Password: "abcXYZ_123" AccessAPI: On AccessWeb: On Enabled: On</b></p> |
|---|

---

**AdminAccountDelete**

Deletes a local administrator account.

Name(r): <S: 0, 128>

The username of the account to delete.

Example: **xCommand AdminAccountDelete: "bob\_smith"**

---

**AdminGroupAdd**

Name(r): <S: 0, 128>

The name of the administrator group.

AccessAPI: <On/Off>

Whether members of this group are allowed to access the system's status and configuration using the API. Default: On.

AccessWeb: <On/Off>

Whether members of this group are allowed to log in to the system using the web interface. Default: On.

Enabled: <On/Off>

Indicates if the group is enabled or disabled. Access is denied to members of disabled groups. Default: On.

Example: **xCommand AdminGroupAdd Name: "administrators" AccessAPI: On AccessWeb: On Enabled: On**

---

**AdminGroupDelete**

Deletes an administrator group.

Name(r): <S: 0, 128>

The name of the group to delete.

Example: **xCommand AdminGroupDelete: "administrators"**

---

**Boot**

Reboots the Expressway.

This command has no parameters.

Example: **xCommand boot**

---

**CheckBandwidth**

A diagnostic tool that returns the status and route (as a list of nodes and links) that a call of the specified type and bandwidth would take between two nodes. Note that this command does not change any existing system configuration.

Node1(r): <S: 1, 50>

The subzone or zone from which the call originates.

Node2(r): <S: 1, 50>

The subzone or zone at which the call terminates.

Bandwidth(r): <1..100000000>

The requested bandwidth of the call (in kbps).

CallType(r): <Traversal/NonTraversal>

Whether the call type is Traversal or Non-traversal.

Example: **xCommand CheckBandwidth Node1: "DefaultSubzone" Node2: "UK Sales Office" Bandwidth: 512 CallType: nontraversal**

---

---

**CheckPattern**

A diagnostic tool that allows you to check the result of an alias transform (local or zone) before you configure it on the system.

Target(r): <S: 1, 60>

The alias you want to use to test the pattern match or transform.

Pattern(r): <S: 1, 60>

The pattern against which the alias is compared.

Type(r): <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the pattern behavior to be applied.

Behavior(r): <Strip/Leave/Replace/AddPrefix/AddSuffix>

How the alias is modified.

Replace: <S: 0, 60>

The text string to use in conjunction with the selected Pattern behavior.

Example: **xCommand CheckPattern Target: "bob@a.net" Pattern: "@a.net" Type: "suffix" Behavior: replace Replace: "@a.com"**

---

**ClearAllStatus**

Clears all status and history on the system.

Example: **xCommand ClearAllStatus**

---

**Cucmconfigadd**

Performs a lookup on a Unified CM publisher.

Address(r): <Value>

The FQDN or IP address of the Unified CM publisher.

Axpassword(r): <Value>

The password used by the Expressway to access the Unified CM publisher.

Axusername(r): <Value>

The user name used by the Expressway to access the Unified CM publisher.

CertValidationDisabled: <On/Off>

Controls X.509 certificate checking against the certificate presented by the Unified CM publisher. Default: On

Example: **xCommand Cucmconfigadd Address: "cucm.example.com" Axpassword: "xyz" Axusername: "abc"**

---

**Cucmconfigdelete**

Deletes the details of a Unified CM publisher.

Address(r): <Value>

The FQDN or IP address of the Unified CM publisher.

Example: **xCommand Cucmconfigdelete Address: "cucm.example.com"**

---

**DefaultLinksAdd**

Restores links between the Default Subzone, Traversal Subzone and the Default Zone.

This command has no parameters.

Example: **xCommand DefaultLinksAdd**

---

---

**DisconnectCall**

Disconnects a call.

Call: <1..1000>

The index of the call to be disconnected.

CallSerialNumber: <S: 1, 255>

The serial number of the call to be disconnected. You must specify either a call index or a call serial number.

Example: **xCommand DisconnectCall CallSerialNumber: "6d843434-211c-11b2-b35d-0010f30f521c"**

---

**Dnslookup**

Queries DNS for a supplied hostname.

Hostname: <Value>

The name of the host you want to query.

RecordType: <all/a/aaaa/srv/naptr>

The type of record you want to search for. If not specified, all record types are returned.

Example: **xCommand Dnslookup Hostname: "example.com" RecordType: all**

---

**DNSPerDomainServerAdd**

Adds a DNS server to use only for resolving hostnames for specific domains.

Address(r): <Value>

The IP address of the DNS server to use when resolving hostnames for the associated domain names.

Domain1(r): <Value>

The domain to associate with the specific DNS server.

Domain2(r): <Value>

An optional second domain to associate with the specific DNS server.

Index: <0..5>

The index of the server to add.

Example: **xCommand DNSServerAdd Address: "192.168.12.0" Index: 1**

---

**DNSPerDomainServerDelete**

Deletes a DNS server used for resolving hostnames for a specific domain.

Address: <Value>

The IP address of the DNS server to delete.

Example: **xCommand DNSPerDomainServerDelete Address: "192.168.12.0"**

---

**DNSServerAdd**

Adds a default DNS server. Default servers are used if there is no per-domain DNS server defined for the domain being looked up.

Address(r): <Value>

The IP address of a default DNS server to use when resolving domain names.

Index: <0..5>

The index of the server to add.

Example: **xCommand DNSServerAdd Address: "192.168.12.0" Index: 1**

---

**DNSServerDelete**

Deletes a DNS server

Address: <Value>

The IP address of the DNS server to delete.

Example: **xCommand DNSServerDelete Address: "192.168.12.0"**

---

**DomainAdd**

Adds a domain for which this Expressway is authoritative.

Name(r): <S: 1, 128>

The domain name. It can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter.

Edgesip: <On/Off>

Endpoint registration, call control and provisioning services are provided by Unified CM. Default: Off.

Edgexmpp: <On/Off>

Instant messaging and presence services for this SIP domain are provided by the Unified CM IM&P service. Default: Off.

Xmppfederation: <On/Off>

Controls whether the domain is available for XMPP federation. Default: Off.

Example: **xCommand DomainAdd Name: "100.example-name.com" Authzone: "Traversal zone" Edge: Off**

---

**DomainDelete**

Deletes a domain.

DomainId(r): <1..200>

The index of the domain to be deleted.

Example: **xCommand DomainDelete DomainId: 2**

---

**Edgessodeletetokens**

Deletes all tokens issued to a particular user.

Username(r): <String>

Specifies which user's tokens will be deleted.

Example: **xCommand Edgessodeletetokens Username: "APerson"**

---

**Edgessopurgetokens**

Deletes all tokens issued to all users.

Example: **xCommand Edgessopurgetokens**

---

**Edgessostatusclear**

Resets the SSO request/response counters to 0.

Example: **xCommand Edgessostatusclear**

---

**FeedbackDeregister**

Deactivates a particular feedback request.

ID: <1..3>

The index of the feedback request to be deactivated.

Example: **xCommand FeedbackDeregister ID: 1**

---

---

**FeedbackRegister**

Activates notifications on the event or status changes described by the expressions. Notifications are sent in XML format to the specified URL. Up to 15 expressions may be registered for each of 3 feedback IDs.

ID: <1..3>

The ID of this particular feedback request.

URL(r): <S: 1, 256>

The URL to which notifications are to be sent.

Expression.1..15: <S: 1, 256>

The events or status change to be notified. Valid Expressions are:

|                     |                           |                             |
|---------------------|---------------------------|-----------------------------|
| Status/Ethernet     | Event/RegistrationFailure | Event/AuthenticationFailure |
| Event/              | Status/Calls              | Event/CallDisconnected      |
| Event/CallFailure   | Status/NTP                | Status/LDAP                 |
| Status/Zones        | Event/Bandwidth           | Event/Locate                |
| Status/Feedback     | Event/CallAttempt         | Event/CallConnected         |
| Event/ResourceUsage | Status/ExternalManager    |                             |

Example: **xCommand FeedbackRegister ID: 1 URL: "http://192.168.0.1/feedback/" Expression.1: "Status/Calls" Expression.2: "Event/CallAttempt"**

---

**ForceConfigUpdate**

Forces the relevant configuration on this peer to be updated to match that of the cluster master.

This command has no parameters.

Example: **xCommand ForceConfigUpdate**

---

**LinkAdd**

Adds and configures a new link.

LinkName(r): <S: 1, 50>

Assigns a name to this link.

Node1: <S: 1, 50>

Specifies the first zone or subzone to which this link will be applied.

Node2: <S: 1, 50>

Specifies the second zone or subzone to which this link will be applied.

Pipe1: <S: 1, 50>

Specifies the first pipe to be associated with this link.

Pipe2: <S: 1, 50>

Specifies the second pipe to be associated with this link.

Example: **xCommand LinkAdd LinkName: "Subzone1 to UK" Node1: "Subzone1" Node2: "UK Sales Office" Pipe1: "512Kb ASDL"**

---

**LinkDelete**

Deletes a link.

LinkId(r): <1..3000>

The index of the link to be deleted.

Example: **xCommand LinkDelete LinkId: 2**

---

---

**Locate**

Runs the Expressway's location algorithm to locate the endpoint identified by the given alias, searching locally, on neighbors, and on systems discovered through the DNS system, within the specified number of 'hops'. Results are reported back through the xFeedback mechanism, which must therefore be activated before issuing this command (e.g. xFeedback register event/locate).

Alias(r): <S: 1, 60>

The alias associated with the endpoint you wish to locate.

HopCount(r): <0..255>

The hop count to be used in the search.

Protocol(r): <H323/SIP>

The protocol used to initiate the search.

SourceZone: <S: 1, 50>

The zone from which to simulate the search request. Choose from the Default Zone (an unknown remote system), the Local Zone (a locally registered endpoint) or any other configured neighbor, traversal client or traversal server zone.

Authenticated: <Yes/No>

Whether the search request should be treated as authenticated or not.

SourceAlias: <S: 0, 60>

The source alias to be used for the search request. Default: xcom-locate

Example: **xCommand Locate Alias: "john.smith@example.com" HopCount: 15 Protocol: SIP SourceZone: LocalZone Authenticated: Yes SourceAlias: alice@example.com**

---

**LoginUserAdd**

Adds an entry to the local authentication database.

Name(r): <String>

Defines the name for this entry in the local authentication database.

Password(r): <Password>

Defines the password for this entry in the local authentication database.

Example: **xCommand LoginUserAdd Name: "alice" Password: "abcXYZ\_123"**

---

**LoginUserDelete**

Deletes an entry from the local authentication database.

Name(r): <String>

The name of the entry to delete.

Example: **xCommand LoginUserDelete Name: "alice"**

---

**Networkinterface**

Controls whether the LAN 2 port is enabled for management and call signaling.

DualInterfaces(r): <enable/disable/status>

Sets or reports on the current status of the the LAN 2 port.

Example: **xCommand Networkinterface DualInterfaces: enable**

---

**NTPServerAdd**

Adds an NTP server to be used when synchronizing system time.

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the NTP server to add.

Example: **xCommand NTPServerAdd Address: "ntp.server.example.com"**

---



---

**NTPServerDelete**

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the NTP server to delete.

Example: **xCommand NTPServerDelete Address: "ntp.server.example.com"**

---

**OptionKeyAdd**

Adds a new option key to the Expressway. These are added to the Expressway in order to add extra functionality, such as increasing the Expressway's capacity. Contact your Cisco representative for further information.

Key(r): <S: 0, 90>

Specifies the option key of your software option.

Example: **xCommand OptionKeyAdd Key: "1X4757T5-1-60BAD5CD"**

---

**OptionKeyDelete**

Deletes a software option key from the Expressway.

OptionKeyId(r): <1..64>

Specifies the ID of the software option to be deleted.

Example: **xCommand OptionKeyDelete OptionKeyId: 2**

---

**Ping**

Checks that a particular host system is contactable.

Hostname: <Value>

The IP address or hostname of the host system you want to try to contact.

Example: **xCommand Ping Hostname: "example.com"**

---

**PipeAdd**

Adds and configures a new pipe.

PipeName(r): <S: 1, 50>

Assigns a name to this pipe.

TotalMode: <Unlimited/Limited/NoBandwidth>

Controls total bandwidth restrictions for the pipe. *NoBandwidth*: no calls can be made using this pipe. Default: Unlimited.

Total: <1..100000000>

If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe. Default: 500000.

PerCallMode: <Unlimited/Limited/NoBandwidth>

Controls bandwidth restrictions of individual calls. *NoBandwidth*: no calls can be made using this pipe. Default: Unlimited.

PerCall: <1..100000000> For limited per-call mode, sets the maximum bandwidth (in kbps) available per call. Default: 1920.

Example: **xCommand PipeAdd PipeName: "512k ADSL" TotalMode: Limited Total: 512 PerCallMode: Limited PerCall: 128**

---

**PipeDelete**

Deletes a pipe.

PipeId(r): <1..1000>

The index of the pipe to be deleted.

Example: **xCommand PipeDelete PipeId: 2**

---

---

**PolicyServiceAdd**

Adds a policy service.

Name(r): <S: 0, 50>

Assigns a name to this Policy Service.

Description: <S: 0, 64>

A free-form description of the Policy Service.

Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote service. Default: HTTPS

Verify: <On/Off>

Controls X.509 certificate checking and mutual authentication between this Expressway and the policy service. When enabled, the server's FQDN or IP address, as specified in the address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: On

CRLCheck: <On/Off>

Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate will be checked against the revocation list of the certificate authority of the certificate. Default: Off

Address: <S: 0, 128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.

Path: <S: 0, 255>

Specifies the URL of the remote service.

StatusPath: <S: 0..255>

Specifies the path for obtaining the remote service status. Default: status

UserName: <S: 0, 30>

Specifies the user name used by the Expressway to log in and query the remote service.

Password: <S: 0, 82>

The password used by the Expressway to log in and query the remote service. The maximum plaintext length is 30 characters.

DefaultCPL: <S: 0, 255>

The CPL used when the remote service is unavailable. Default: <reject status='403' reason='Service Unavailable'/>

Example: **xCommand PolicyServiceAdd Name: "Conference" Description: "Conference service" Protocol: HTTPS Verify: On CRLCheck: On Address: "service.example.com" Path: "service" StatusPath: "status" UserName: "user123" Password: "password123" DefaultCPL: "<reject status='403' reason='Service Unavailable'/>"**

---

**PolicyServiceDelete**

Deletes a policy service.

PolicyServiceId(r): <1..20>

The index of the policy service to be deleted.

Example: **xCommand PolicyServiceDelete PolicyServiceId: 1**

---

---

**RemoteSyslogAdd**

Adds the address of a remote syslog server.

Address(r): <Value>

The IP address or FQDN of the remote syslog server.

Crlcheck: <On/Off>

Controls whether the certificate supplied by the syslog server is checked against the certificate revocation list (CRL). Default : Off

Format: <bsd/ietf>

The format in which remote syslog messages are written. Default : bsd

LogLevel: <emergency/alert/critical/error/warning/notice/informational/debug>

The minimum severity of log messages to send to this syslog server. Default: informational.

Mode: <bsd/ietf/ietf\_secure/user\_defined>

The syslog protocol to use when sending messages to the syslog server. Default: bsd.

Port: <1..65535>

The UDP/TCP destination port to use. Suggested ports: UDP=514 TCP/TLS=6514 Default : 514

Transport: <udp/tcp/tls>

The transport protocol to use when communicating with the syslog server. Default: udp

Example: **xCommand RemoteSyslogAdd Address: "remote\_server.example.com" Crlcheck: Off Format: bsd LogLevel: warning Mode: bsd Port: 514 Transport: udp**

---

**RemoteSyslogDelete**

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the remote syslog server to delete.

Port(r): <1..65535>

The port used by the remote syslog server to be deleted.

Transport(r): <udp/tcp/tls>

The transport protocol used by the remote syslog server to be deleted.

Example: **xCommand RemoteSyslogDelete Address: "remote\_server.example.com" Port: 514 Transport: udp**

---

**Restart**

Restarts the Expressway without a full system reboot.

This command has no parameters.

Example: **xCommand Restart**

---

**RouteAdd**

Adds and configures a new IP route (also known as a static route).

Address(r): <S: 1, 39>

Specifies an IP address used in conjunction with the prefix length to determine the network to which this route applies. Default: 32

PrefixLength(r): <1..128>

Specifies the number of bits of the IP address which must match when determining the network to which this route applies.

Gateway(r): <S: 1, 39>

Specifies the IP address of the gateway for this route.

Interface: <Auto/LAN1/LAN2>

The LAN interface to use for this route. *Auto*: the Expressway will select the most appropriate interface to use. Default: Auto

Example: **xCommand RouteAdd Address: "10.13.8.0" PrefixLength: 32 Gateway: "192.44.0.1"**

---

**RouteDelete**

Deletes a route.

RouteId(r): <1..50>

The index of the route to be deleted.

Example: **xCommand RouteDelete RouteId: 1**

---

**SearchRuleAdd**

Adds a new search rule to route searches and calls toward a zone or policy service.

Name(r): <S: 0, 50>

Descriptive name for the search rule.

ZoneName: <S: 0, 50>

The zone or policy service to query if the alias matches the search rule.

Description: <S: 0, 64>

A free-form description of the search rule.

Example: **xCommand SearchRuleAdd Name: "DNS lookup" ZoneName: "Sales Office" Description: "Send query to the DNS zone"**

---

**SearchRuleDelete**

Deletes a search rule.

SearchRuleId(r): <1..2000>

The index of the search rule to be deleted.

Example: **xCommand SearchRuleDelete SearchRuleId: 1**

---

**Tracepath**

Discover the path taken by a network packet sent to a particular destination host system.

Hostname: <Value>

The IP address or hostname of the host system to which you want to trace the path.

Example: **xCommand Tracepath Hostname: "example.com"**

---

**Traceroute**

Discover the route taken by a network packet sent to a particular destination host system. It reports the details of each router along the path, and the time taken for each router to respond to the request.

Hostname: <Value>

The IP address or hostname of the host system to which you want to trace the route.

Example: **xCommand Traceroute Hostname: "example.com"**

---

---

**TransformAdd**

Adds and configures a new transform.

Pattern(r): <S: 1, 60>

Specifies the pattern against which the alias is compared.

Type: <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the transform to be applied. *Exact*: the entire string must exactly match the alias character for character. *Prefix*: the string must appear at the beginning of the alias. *Suffix*: the string must appear at the end of the alias. *Regex*: the string is treated as a regular expression. Default: Prefix

Behavior: <Strip/Replace/AddPrefix/AddSuffix>

How the alias is modified. *Strip*: removes the matching prefix or suffix from the alias. *Replace*: substitutes the matching part of the alias with the text in the replace string. *AddPrefix*: prepends the replace string to the alias. *AddSuffix*: appends the replace string to the alias. Default: Strip

Replace: <S: 0, 60>

The text string to use in conjunction with the selected Pattern behavior.

Priority: <1..65534>

Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform. Default: 1

Description: <S: 0, 64>

A free-form description of the transform.

State: <Enabled/Disabled>

Indicates if the transform is enabled or disabled. Disabled transforms are ignored. Default: Enabled

Example: **xCommand TransformAdd Pattern: "example.net" Type: suffix Behavior: replace Replace: "example.com" Priority: 3 Description: "Change example.net to example.com" State: Enabled**

---

**TransformDelete**

Deletes a transform.

TransformId(r): <1..100>

The index of the transform to be deleted.

Example: **xCommand TransformDelete TransformId: 2**

---

**Xmppdelete**

Deletes the details of IM and Presence servers.

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the IM and Presence server to delete.

Example: **xCommand Xmppdelete Address: "imp\_server.example.com"**

---

**Xmppdiscovery**

Discovers the details of IM and Presence servers.

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the IM and Presence server to discover.

Axlpasword(r): <Password>

The password used to access the IM and Presence publisher.

Axlusername(r): <String>

The username used to access the IM and Presence publisher.

CertValidationDisabled: <On/Off>

Controls X.509 certificate checking against the certificate presented by the IM and Presence publisher. Default: On

Example: **xCommand Xmppdiscovery Address: "imp.example.com" Axlpasword: "xyz" Axlusername: "abc"**

---

**ZoneAdd**

Adds and configures a new zone.

ZoneName(r): <S: 1, 50>

Assigns a name to this zone.

Type(r): <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>

Determines the nature of the specified zone, in relation to the local Expressway. *Neighbor*: the new zone will be a neighbor of the local Expressway. *TraversalClient*: there is a firewall between the zones, and the local Expressway is a traversal client of the new zone. *TraversalServer*: there is a firewall between the zones and the local Expressway is a traversal server for the new zone.

*ENUM*: the new zone contains endpoints discoverable by ENUM lookup. *DNS*: the new zone contains endpoints discoverable by DNS lookup.

Example: **xCommand ZoneAdd ZoneName: "UK Sales Office" Type: Neighbor**

---

**ZoneDelete**

Deletes a zone.

ZoneId(r): <1..1000>

The index of the zone to be deleted.

Example: **xCommand ZoneDelete ZoneId: 2**

---

**ZoneList**

A diagnostic tool that returns the list of zones (grouped by priority) that would be queried, and any transforms that would be applied, in a search for a given alias.

Note that this command does not change any existing system configuration.

Alias(r): <S: 1, 60>

The alias to be searched for.

Example: **xCommand ZoneList Alias: "john.smith@example.com"**

---

## Command reference — xStatus

The **xStatus** group of commands are used to return information about the current status of the system. Each **xStatus** element returns information about one or more sub-elements.

The following section lists all the currently available **xStatus** commands, and the information that is returned by each command.

To obtain information about the existing status, type:

- **xStatus** to return the current status of all status elements
- **xStatus <element>** to return the current status for that particular element and all its sub-elements
- **xStatus <element> <sub-element>** to return the current status of that group of sub-elements

To obtain information about the **xStatus** commands, type:

- **xStatus ?** to return a list of all elements available under the **xStatus** command

### xStatus elements

The current xStatus elements are:

- Alarm
- Alternates
- Applications
- B2BUACalls
- B2buapresencereplayservice
- B2buapresencereplayuser
- Calls
- CDR
- Cluster
- CollaborationEdge
- EdgeSSO
- ExternalManager
- Fail2banjailbannedaddress
- Feedback
- Firewall
- H323
- Hardware
- Iptablesacceptedrule
- Iptablesrule
- License
- Links
- Mediastatistics
- NetworkInterface
- Ntpcertificates
- Options

- Phonebookserver
- Pipes
- Policy
- Portusage
- ResourceUsage
- SIP
- SipServiceDomains
- SipServiceZones
- SystemUnit
- TURN
- Time
- Warnings
- Zones



## External policy overview

The Cisco Expressway (Expressway) supports CPL (Call Processing Language) for implementing complex policy decisions. CPL is designed as a machine-generated language and is not immediately intuitive; while the Expressway can be loaded with CPL to implement advanced call policy decisions, complex CPL is difficult to write and maintain.

The Expressway's external policy feature allows policy decisions to be taken by an external system which can then instruct the Expressway on the course of action to take (such as whether to fork a call and so on). Call policy can now be managed independently of the Expressway, and can implement features that are unavailable on the Expressway. The external policy server can make routing decisions based on data available from any source that the policy server has access to, allowing companies to make routing decisions based on their specific requirements.

When the Expressway is configured to use an external policy server the Expressway sends the external policy server a service request (over HTTP or HTTPS), the service will send a response back containing a CPL snippet which the Expressway will then execute.

## Using an external policy server

The main areas where the Expressway can be configured to use an external policy server are:

- Call Policy (also known as Admin Policy) – to control the allowing, rejecting, routing (with fallback if calls fail) and forking of calls.
- Search rules (policy can be applied for specific dial plan search rules).

Each of these areas can be configured independently of each other as to whether or not to use a policy service. If a policy service is used, the decisions made by the policy service replace (rather than supplement) those made by the Expressway.

When configuring policy services:

- Up to 3 external policy servers may be specified to provide resiliency (and not load balancing).
- Default CPL can be configured, to be processed by the Expressway as a fallback, if the service is not available.
- The status and reachability of the service can be queried via a status path.

More information about policy services, including example CPL, can be found in the [External Policy on Expressway Deployment Guide](#).

## External policy request parameters

When the Expressway uses a policy service it sends information about the call request to the service in a POST message using a set of name-value pair parameters. The service can then make decisions based upon these parameters combined with its own policy decision logic and supporting data.

The service response must be a 200 OK message with CPL contained in the body.

The following table lists the possible parameters contained within a request. It also indicates, where relevant, the range of accepted values.

| Parameter name               | Values  |
|------------------------------|---|
| ALLOW_INTERWORKING           | TRUE / FALSE  |
| AUTHENTICATED                | TRUE / FALSE  |
| AUTHENTICATED_SOURCE_ALIAS   |   |
| AUTHENTICATION_USER_NAME     |   |
| CLUSTER_NAME                 |   |
| DESTINATION_ALIAS            |   |
| DESTINATION_ALIAS_PARAMS     |   |
| GLOBAL_CALL-SERIAL_NUMBER    | GUID  |
| LOCAL_CALL_SERIAL_NUMBER     | GUID  |
| METHOD                       | INVITE / ARQ / LRQ / OPTIONS / SETUP  |
| NETWORK_TYPE                 | IPV4 / IPV6   |
| POLICY_TYPE                  | SEARCH / ADMIN  |
| PROTOCOL                     | SIP / H323  |
| REGISTERED_ALIAS             |   |
| SOURCE_ADDRESS               |   |
| SOURCE_IP                    |   |
| SOURCE_PORT                  |   |
| TRAVERSAL_TYPE               | TYPE_[UNDEF / ASSENTSERVER / ASSENTCLIENT / H460SERVER / H460CLIENT / TURNSEVER / TURNCLIENT / ICE] |
| UNAUTHENTICATED_SOURCE_ALIAS |   |
| UTCTIME                      |   |
| ZONE_NAME                    |   |

### Cryptography support

External policy servers should support TLS and AES-256/AES-128/3DES-168.

SHA-1 is required for MAC and Diffie-Hellman / Elliptic Curve Diffie-Hellman key exchange; the Expressway does not support MD5.

## Default CPL for policy services

When configuring a policy service, you can specify the **Default CPL** that is used by the Expressway if the service is not available.

The **Default CPL** for Call Policy defaults to:

```
<reject status='403' reason='Service Unavailable' />
```

and this will reject the request.

The **Default CPL** for policy services used by search rules defaults to:

```
<reject status='504' reason='Policy Service Unavailable' />
```

and this will stop the search via that particular search rule.

This default CPL mean that in the event of a loss of connectivity to the policy server, all call requests will be rejected. If this is not your required behavior then you are recommended to specify alternative default CPL.

We recommend that you use unique reason values for each type of service, so that if calls are rejected it is clear why and which service is rejecting the request.

## Flash status word reference table

The flash status word is used in diagnosing NTP server synchronization issues.

It is displayed by the `ntpq` program `rv` command. It comprises a number of bits, coded in hexadecimal as follows:

| Code | Tag    | Message      | Description                 |
|------|--------|--------------|-----------------------------|
| 0001 | TEST1  | pkt_dup      | duplicate packet            |
| 0002 | TEST2  | pkt_bogus    | bogus packet                |
| 0004 | TEST3  | pkt_unsync   | server not synchronized     |
| 0008 | TEST4  | pkt_denied   | access denied               |
| 0010 | TEST5  | pkt_auth     | authentication failure      |
| 0020 | TEST6  | pkt_stratum  | invalid leap or stratum     |
| 0040 | TEST7  | pkt_header   | header distance exceeded    |
| 0080 | TEST8  | pkt_autokey  | Autokey sequence error      |
| 0100 | TEST9  | pkt_crypto   | Autokey protocol error      |
| 0200 | TEST10 | peer_stratum | invalid header or stratum   |
| 0400 | TEST11 | peer_dist    | distance threshold exceeded |
| 0800 | TEST12 | peer_loop    | synchronization loop        |
| 1000 | TEST13 | peer_unreach | unreachable or nonselect    |

## Supported RFCs

Expressway supports the following RFCs:

Table 13: 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                    |
| 3891 | Replaces header   |
| 3892 | Referred-by header  |
| 3903 | Session Initiation Protocol (SIP) Extension for Event State Publication                                       |
| 3944 | H.350 Directory Services  |

Table 13: Supported RFCs (continued)

| <b>RFC</b> | <b>Description</b>   |
|------------|--|
| 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  |

# Software version history

This section summarizes feature updates that have occurred in earlier software releases.

For information about earlier releases not listed here, see the online help or previous versions of this document.

- [X8.5.1](#)
- [X8.5](#)
- [X8.2](#)
- [X8.1.1](#)

## X8.5.1

### 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.

---

## X8.5

### 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, are not available in this release (e.g. off-hook dialing).

### 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

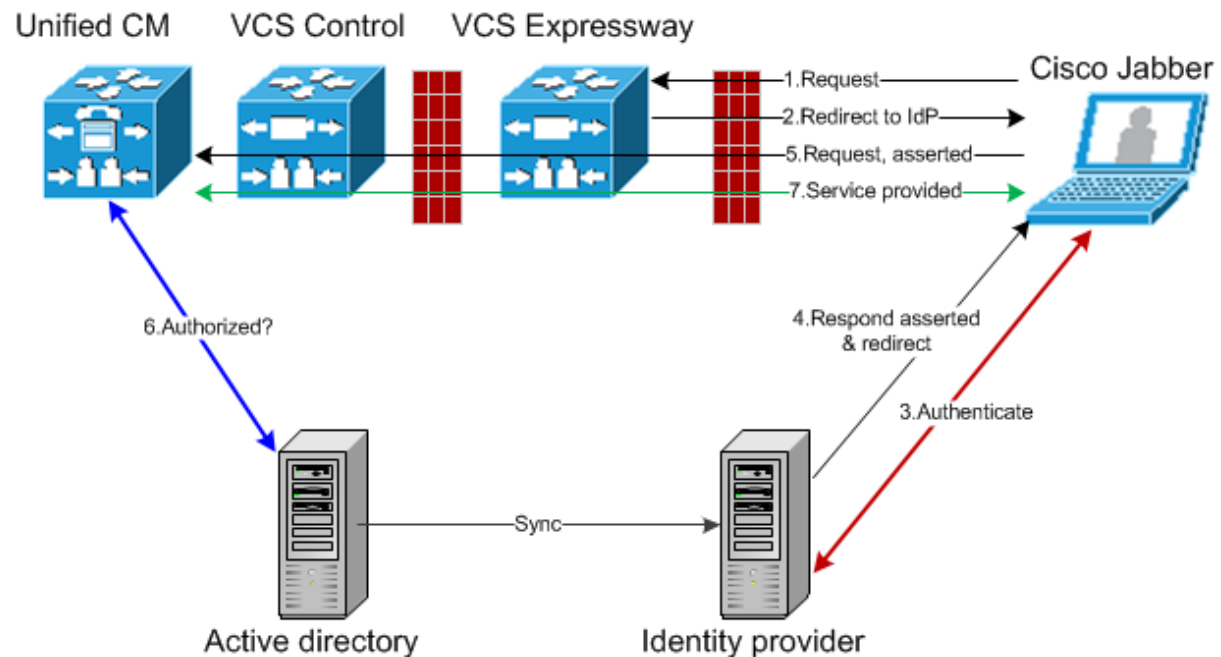
Cisco Jabber determines whether it is inside the organization's network before it requests a Unified Communications service. If it is outside the network, then it requests the service from the Expressway-E on the edge of the network. If single sign-on is enabled at the edge, the Expressway-E redirects 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 12: 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

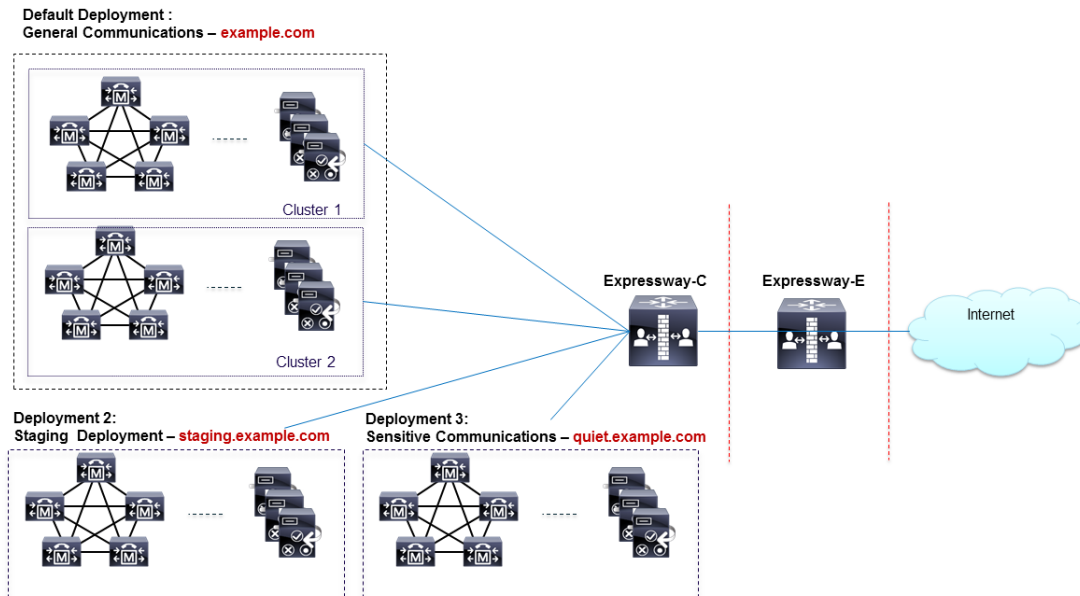
This release introduces the concept of "deployments" to the Expressway.

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 13: 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**).

---

## 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 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.

---

## 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.

## Related documentation

The following table lists documents and web sites referenced in this document, and other supporting documentation. All documentation for the latest version of Expressway can be found at [www.cisco.com](http://www.cisco.com).

| Title   | Link  |
|---|---|
| Expressway Administrator Guide (this document)  | <a href="http://www.cisco.com">www.cisco.com</a>  |
| Authenticating Expressway Accounts Using LDAP Deployment Guide                            | <a href="http://www.cisco.com">www.cisco.com</a>  |
| Expressway Basic Configuration Deployment Guide   | <a href="http://www.cisco.com">www.cisco.com</a>  |
| Expressway Certificate Creation and Use Deployment Guide                                  | <a href="http://www.cisco.com">www.cisco.com</a>  |
| Cisco Unified Communications Manager with Expressway Deployment Guide                     | <a href="http://www.cisco.com">www.cisco.com</a>  |
| Expressway Cluster Creation and Maintenance Deployment Guide                              | <a href="http://www.cisco.com">www.cisco.com</a>  |
| ENUM Dialing on Expressway Deployment Guide   | <a href="http://www.cisco.com">www.cisco.com</a>  |
| External Policy on Expressway Deployment Guide  | <a href="http://www.cisco.com">www.cisco.com</a>  |
| Expressway CE500 Appliance Installation Guide   | <a href="http://www.cisco.com">www.cisco.com</a>  |
| Expressway CE1000 Appliance Installation Guide  | <a href="http://www.cisco.com">www.cisco.com</a>  |
| Expressway IP Port Usage for Firewall Traversal   | <a href="http://www.cisco.com">www.cisco.com</a>  |
| Microsoft Lync and Expressway Deployment Guide  | <a href="http://www.cisco.com">www.cisco.com</a>  |
| Unified Communications: Mobile and Remote Access via Expressway Deployment Guide          | <a href="http://www.cisco.com">www.cisco.com</a>  |
| Expressway on Virtual Machine Installation Guide  | <a href="http://www.cisco.com">www.cisco.com</a>  |
| DNS and BIND Fourth Edition, Albitz and Liu, O'Reilly and Associates, ISBN: 0-596-00158-4 |   |
| ITU Specification: H.235 Security and encryption for H-Series multimedia terminals        | <a href="http://www.itu.int/rec/T-REC-H.235/en">http://www.itu.int/rec/T-REC-H.235/en</a>   |
| ITU Specification: H.323: Packet-based multimedia communications systems                  | <a href="http://www.itu.int/rec/T-REC-H.323/en">http://www.itu.int/rec/T-REC-H.323/en</a>   |
| ITU Specification: H.350 Directory services architecture for multimedia conferencing      | <a href="http://www.itu.int/rec/T-REC-H.350/en">http://www.itu.int/rec/T-REC-H.350/en</a>   |
| Management Information Base for Network Management of TCP/IP-based internets: MIB-II      | <a href="http://tools.ietf.org/html/rfc1213">http://tools.ietf.org/html/rfc1213</a>         |
| Network Time Protocol website   | <a href="http://www.ntp.org/">http://www.ntp.org/</a>                                       |
| PHP regex guidelines  | <a href="http://php.net/manual/en/book.pcre.php">http://php.net/manual/en/book.pcre.php</a> |
| Regular Expression Pocket Reference ISBN-10: 0596514271 ISBN-13: 978-0596514273           |   |
| RFC 791: Internet Protocol  | <a href="http://tools.ietf.org/html/rfc791">http://tools.ietf.org/html/rfc791</a>           |
| RFC 1305: Network Time Protocol   | <a href="http://tools.ietf.org/html/rfc1305">http://tools.ietf.org/html/rfc1305</a>         |
| RFC 2460: Internet Protocol, Version 6 (IPv6) Specification                               | <a href="http://tools.ietf.org/html/rfc2460">http://tools.ietf.org/html/rfc2460</a>         |
| RFC 2782: A DNS RR for specifying the location of services (DNS SRV)                      | <a href="http://tools.ietf.org/html/rfc2782">http://tools.ietf.org/html/rfc2782</a>         |

| Title  | Link  |
|--|---|
| RFC 2915: The Naming Authority Pointer (NAPTR) DNS Resource Record                                       | <a href="http://tools.ietf.org/html/rfc2915">http://tools.ietf.org/html/rfc2915</a> |
| RFC 3164: The BSD syslog Protocol  | <a href="http://tools.ietf.org/html/rfc3164">http://tools.ietf.org/html/rfc3164</a> |
| RFC 3261: SIP: Session Initiation Protocol   | <a href="http://tools.ietf.org/html/rfc3261">http://tools.ietf.org/html/rfc3261</a> |
| RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers  | <a href="http://tools.ietf.org/html/rfc3263">http://tools.ietf.org/html/rfc3263</a> |
| RFC 3326: The Reason Header Field for the Session Initiation Protocol (SIP)                              | <a href="http://tools.ietf.org/html/rfc3326">http://tools.ietf.org/html/rfc3326</a> |
| RFC 3327: Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts | <a href="http://tools.ietf.org/html/rfc3327">http://tools.ietf.org/html/rfc3327</a> |
| RFC 3489: STUN - Simple Traversal of User Datagram Protocol (UDP) Through NATs                           | <a href="http://tools.ietf.org/html/rfc3489">http://tools.ietf.org/html/rfc3489</a> |
| RFC 3550: RTP: A Transport Protocol for Real-Time Applications   | <a href="http://tools.ietf.org/html/rfc3550">http://tools.ietf.org/html/rfc3550</a> |
| RFC 3761: The E.164 to URI Dynamic Delegation Discovery System (DDDS) Application (ENUM)                 | <a href="http://tools.ietf.org/html/rfc3761">http://tools.ietf.org/html/rfc3761</a> |
| RFC 3880: Call Processing Language (CPL): A Language for User Control of Internet Telephony Services     | <a href="http://tools.ietf.org/html/rfc3880">http://tools.ietf.org/html/rfc3880</a> |
| RFC 4028: Session Timers in the Session Initiation Protocol (SIP)  | <a href="http://tools.ietf.org/html/rfc4028">http://tools.ietf.org/html/rfc4028</a> |
| RFC 4787: Network Address Translation (NAT) Behavioral Requirements for Unicast UDP                      | <a href="http://tools.ietf.org/html/rfc4787">http://tools.ietf.org/html/rfc4787</a> |
| RFC 5245: Interactive Connectivity Establishment (ICE)   | <a href="http://tools.ietf.org/html/rfc5245">http://tools.ietf.org/html/rfc5245</a> |
| RFC 5626: Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)                 | <a href="http://tools.ietf.org/html/rfc5626">http://tools.ietf.org/html/rfc5626</a> |
| RFC 5627: Obtaining and Using Globally Routable User Agent URIs (GRUUs) in SIP                           | <a href="http://tools.ietf.org/html/rfc5627">http://tools.ietf.org/html/rfc5627</a> |
| RFC 5806: Diversion Indication in SIP  | <a href="http://tools.ietf.org/html/rfc5806">http://tools.ietf.org/html/rfc5806</a> |
| Session Traversal Utilities for NAT (STUN)   | <a href="http://tools.ietf.org/html/rfc5389">http://tools.ietf.org/html/rfc5389</a> |
| Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN) | <a href="http://tools.ietf.org/html/rfc5766">http://tools.ietf.org/html/rfc5766</a> |



# Legal notices

## Intellectual property rights

This Administrator Guide and the product to which it relates contain information that is proprietary to TANDBERG and its licensors. Information regarding the product is found below in the **Copyright notice** and **Patent information** sections.

TANDBERG® is a registered trademark belonging to Tandberg ASA. Other trademarks used in this document are the property of their respective holders. This Guide may be reproduced in its entirety, including all copyright and intellectual property notices, in limited quantities in connection with the use of this product. Except for the limited exception set forth in the previous sentence, no part of this Guide may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronically, mechanically, by photocopying, or otherwise, without the prior written permission of TANDBERG.

COPYRIGHT © TANDBERG

## Copyright notice

The product that is covered by this Administrator Guide is protected under copyright, patent, and other intellectual property rights of various jurisdictions.

This product is Copyright © 2014, Tandberg Telecom UK Limited. All rights reserved.

TANDBERG is now part of Cisco. Tandberg Telecom UK Limited is a wholly owned subsidiary of Cisco Systems, Inc.

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/ps13435/products\\_licensing\\_information\\_listing.html](http://www.cisco.com/en/US/products/ps13435/products_licensing_information_listing.html).

This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>).

This product includes software developed by the University of California, Berkeley and its contributors.

**IMPORTANT: USE OF THIS PRODUCT IS SUBJECT IN ALL CASES TO THE COPYRIGHT RIGHTS AND THE TERMS AND CONDITIONS OF USE REFERRED TO ABOVE. USE OF THIS PRODUCT CONSTITUTES AGREEMENT TO SUCH TERMS AND CONDITIONS.**

### AVC Video License

With respect to each AVC/H.264 product, we are obligated to provide the following notice:

This product is licensed under the AVC patent portfolio license for the personal use of a consumer or other uses in which it does not receive remuneration to (i) encode video in compliance with the AVC standard (“AVC video”) and/or (ii) decode AVC video that was encoded by a consumer engaged in a personal activity and/or was obtained from a video provider licensed to provide AVC video. No license is granted or shall be implied for any other use. Additional information may be obtained from MPEG LA, L.L.C.

See <http://www.mpegla.com>.

Accordingly, please be advised that service providers, content providers, and broadcasters are required to obtain a separate use license from MPEG LA prior to any use of AVC/H.264 encoders and/or decoders.

## Patent information

This product is covered by one or more of the following patents:

- US7,512,708
- EP1305927
- EP1338127

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

© 2015 Cisco Systems, Inc. All rights reserved.