



Cisco Expressway

Administrator Guide

Last Updated: December 2018

X8.10.3

Preface

Change History

Table 1 Administrator Guide Change History

| Date | Change | Reason |
|----------------|---|-----------------------------|
| November 2017 | General corrections and updates. | X8.10.3 Maintenance release |
| July 2017 | Updates for software version X8.10. | X8.10 Release |
| January 2017 | General corrections and updates. New feature added. | X8.9.1 Maintenance release |
| December 2016 | New features and general corrections. | X8.9 Release |
| September 2016 | Help and admin guide updates including new call policy rule configuration. | X8.8.2 Maintenance release |
| July 2016 | Correction in MRA overview and Xconfig SIP Advanced CLI commands added. | X8.8 document errata |
| June 2016 | General corrections and updates. New features added. | X8.8 release |
| April 2016 | General corrections and updates. New features added. | X8.7.2 Maintenance release |
| February 2016 | General corrections and updates. Document change history (this table) added. DNS zone parameters and alarm reference updated. | X8.7.1 Maintenance release |

Contents

| | |
|--|-----|
| Preface | 2 |
| Change History | 2 |
| Contents | 3 |
| Introduction | 7 |
| About the Cisco Expressway | 7 |
| About This Guide | 15 |
| What's New in This Version? | 20 |
| Service Setup Wizard: Choose Services | 20 |
| Service Setup Wizard: Apply Options and Licenses | 21 |
| Service Setup Wizard: Review Networking Configuration | 22 |
| Network and System Settings | 25 |
| Network Settings | 25 |
| Intrusion Protection | 31 |
| Network Services | 36 |
| Configuring External Manager Settings | 44 |
| Configuring TMS Provisioning Extension services | 45 |
| Firewall Traversal | 49 |
| About Firewall Traversal | 49 |
| Firewall Traversal Configuration Overview | 51 |
| Configuring a Traversal Client and Server | 52 |
| Configuring Ports for Firewall Traversal | 53 |
| Firewall Traversal and Authentication | 56 |
| About ICE and TURN Services | 57 |
| Configuring TURN Services | 58 |
| Unified Communications | 62 |
| Unified Communications Prerequisites | 62 |
| Mobile and Remote Access | 71 |
| External XMPP Federation | 101 |
| Delayed Cisco XCP Router Restart | 112 |
| Jabber Guest Services Overview | 115 |
| Meeting Server Web Proxy on Expressway | 116 |
| Protocols | 117 |
| About H.323 | 117 |
| Configuring H.323 | 118 |
| About SIP | 119 |
| Configuring SIP | 121 |
| Configuring Domains | 126 |
| Configuring SIP and H.323 Interworking | 127 |
| Registration Control | 129 |
| About Registrations | 129 |
| About Allow and Deny Lists | 131 |
| Configuring Registration Policy to Use an External Service | 133 |
| Device Authentication | 135 |
| About Device Authentication | 135 |
| Authenticating with External Systems | 140 |

Contents

| | |
|--|-----|
| Zones and Neighbors | 141 |
| About your Video Communications Network | 141 |
| Structuring your Dial Plan | 142 |
| About Zones | 143 |
| Configuring Media Encryption Policy | 144 |
| Configuring ICE Messaging Support | 145 |
| About the Local Zone and Subzones | 146 |
| The Default Zone | 146 |
| Configuring Default Zone access rules | 147 |
| Zone List | 148 |
| Clustering and Peers | 169 |
| About Clusters | 169 |
| License Usage Within a Cluster | 171 |
| Managing Clusters and Peers | 173 |
| Troubleshooting Cluster Replication Problems | 179 |
| Dial Plan and Call Processing | 181 |
| Call Routing Process | 181 |
| Configuring Hop Counts | 184 |
| Configuring Dial Plan Settings | 184 |
| About Transforms and Search Rules | 185 |
| Example Searches and Transforms | 192 |
| Configuring Search Rules to Use an External Service | 201 |
| About Call Policy | 203 |
| Supported Address Formats | 208 |
| Dialing by IP Address | 209 |
| About URI Dialing | 210 |
| About ENUM Dialing | 216 |
| Configuring DNS Servers for ENUM and URI Dialing | 221 |
| Configuring Call Routing and Signaling | 221 |
| Identifying Calls | 222 |
| Disconnecting Calls | 223 |
| Bandwidth Control | 225 |
| About Bandwidth Control | 225 |
| Configuring Bandwidth Controls | 226 |
| About Subzones | 227 |
| Links and Pipes | 233 |
| Bandwidth Control Examples | 236 |
| Applications | 237 |
| B2BUA (Back-to-Back User Agent) Overview | 238 |
| FindMe™ | 247 |
| Cisco TMS Provisioning | 250 |
| Hybrid Services and Connector Management | 252 |
| User Accounts | 255 |
| About User Accounts | 255 |
| Configuring Password Security | 257 |
| Configuring Administrator Accounts | 258 |
| Configuring Remote Account Authentication Using LDAP | 260 |
| Resetting Forgotten Passwords | 265 |
| Using the Root Account | 266 |

Contents

| | |
|---|-----|
| Managing SSO tokens | 266 |
| Maintenance | 269 |
| Enabling SSH access | 269 |
| Enabling Maintenance Mode | 270 |
| About Upgrading Software Components | 270 |
| Configuring Logging | 273 |
| Managing Option Keys | 277 |
| About Security | 278 |
| About Domain Certificates and Server Name Indication for Multitenancy | 289 |
| Domain Certificates and Clustered Systems | 293 |
| Advanced Security | 293 |
| Configuring Language Settings | 298 |
| Backing Up and Restoring Expressway Data | 299 |
| Diagnostics Tools | 302 |
| Incident Reporting | 304 |
| Checking the Effect of a Pattern | 307 |
| Locating an Alias | 307 |
| Port Usage | 308 |
| Network Utilities | 309 |
| Restarting, Rebooting and Shutting Down | 312 |
| Developer Resources | 313 |
| Overview and Status Information | 315 |
| Status Overview | 315 |
| System Information | 316 |
| Ethernet Status | 317 |
| IP Status | 317 |
| Resource Usage | 318 |
| Registration Status | 320 |
| Call Status | 321 |
| B2BUA Calls | 322 |
| Search History | 323 |
| Search Details | 324 |
| Local Zone Status | 324 |
| Zone Status | 324 |
| Bandwidth | 325 |
| Policy Server Status and Resiliency | 326 |
| TURN Relay Usage | 327 |
| Unified Communications Status | 327 |
| Microsoft interoperability | 328 |
| TMS Provisioning Extension Service Status | 329 |
| Managing Alarms | 332 |
| Logs | 333 |
| Hardware Status | 336 |
| Reference Material | 337 |
| About Event Log Levels | 338 |
| CPL Reference | 347 |
| LDAP Server Configuration for Device Authentication | 356 |
| Changing the Default SSH Key | 360 |
| Restoring the Default Configuration (Factory Reset) | 360 |

Contents

| | |
|--|-----|
| Password Encryption | 362 |
| Pattern Matching Variables | 363 |
| Port Reference | 364 |
| Mobile and Remote Access Port Reference | 369 |
| Microsoft Interoperability Port Reference | 371 |
| Regular expressions | 374 |
| Supported Characters | 376 |
| Call Types and Licensing | 377 |
| Product Identifiers and Corresponding Keys | 380 |
| Allow List Rules File Reference | 382 |
| Allow List Tests File Reference | 383 |
| Expressway Multitenancy Overview | 384 |
| Multitenant Expressway Sizing | 386 |
| Alarms | 389 |
| Command Reference – xConfiguration | 423 |
| Command Reference – xCommand | 491 |
| Command Reference – xStatus | 518 |
| External Policy Overview | 519 |
| Flash Status Word Reference Table | 523 |
| Supported RFCs | 524 |
| Software Version History | 526 |
| Related Documentation | 558 |
| Legal Notices | 559 |
| Cisco Legal Information | 560 |
| Cisco Trademark | 560 |



Introduction

| | |
|-----------------------------------|----|
| About the Cisco Expressway | 7 |
| About This Guide | 15 |
| What's New in This Version? | 20 |

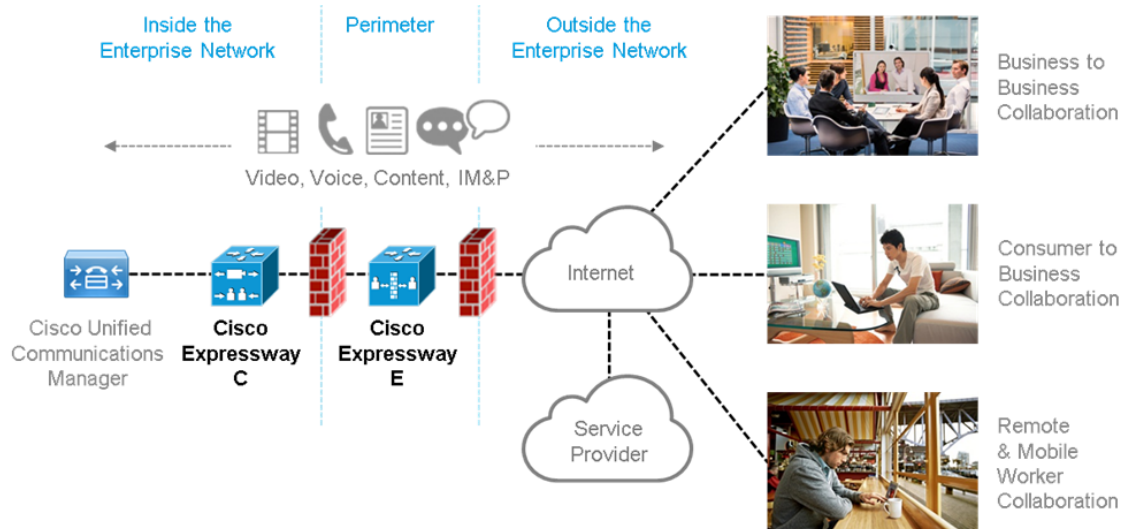
About the Cisco Expressway

Cisco Expressway is designed specifically for comprehensive collaboration services. 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 often 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.



Optional packages that you can deploy include Registrations for TelePresence Rooms or Desktop systems (includes FindMe and Device Provisioning), Microsoft Interoperability, and Advanced Networking (Expressway-E only).

Introduction

The Expressway is available on a dedicated appliance (CE1100) and also runs on VMware on a range of Cisco UCS servers. See *Expressway on Virtual Machine Installation Guide* on the [Expressway Install Guides page](#) for more information.

Expressway Types

Each Expressway can be configured as one of two types, which offer different capabilities.

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.

Cisco Expressway Base

In version X8.7, the system is called "Cisco Expressway Base" if you register it for Hybrid Services but do not apply a release key. The release key is not required for a system that is being used for Hybrid Services.

In X8.8, this behavior changed with the introduction of the Service Setup Wizard. You still do not need to apply a release key, but you must select Expressway-C when you run the service setup wizard.

About the Service Setup Wizard

The Service Setup Wizard, (introduced in X8.8) improves the user experience of configuring the Expressway for its chosen purpose in your environment.

When you first launch the user interface, you see the Service Setup Wizard instead of going straight into the menu. You can select the system series (VCS or Expressway) and type (*VCS Expressway/VCS Control* or *Expressway-E/Expressway-C*). These choices affect the list of services available.

Then you select from a number of popular Expressway services:

- Cisco Spark Hybrid Services (renamed to Cisco Webex Hybrid Services)
- Mobile and Remote Access including Meeting Server Web Proxy
- Jabber Guest Services
- Microsoft gateway service - this service is only for when you want *this system* to adapt between Microsoft SIP and standards-based SIP variants. If a different system (such as Cisco Meeting Server) is doing that adaptation in your deployment, you don't need this service.
- Registrar/ Proxy registrations - previously only possible on VCS, now also possible on Expressway.
- Collaboration Meeting Rooms (CMR) Cloud

Introduction

- Business to Business Calling - from X8.9, this service includes B2B calling with organizations using Microsoft collaboration infrastructure, if you use Meeting Server to adapt between Microsoft and standards-based SIP variants.

When you select from the list, the wizard helps you to apply appropriate licenses for your selection, verify your basic configuration (network settings should have been configured previously), and then restart the system. After the restart, you only see the configuration pages and fields that are relevant for your selection.

If you don't want to use the wizard you can skip through it. And you can go back to the start at any time.

Table 2 Services That Can Be Hosted Together

| | Cisco Spark Hybrid Services (Connectors) | Mobile and Remote Access | Jabber Guest Services | Microsoft gateway service | Registrar | CMR Cloud | Business to Business calling (incl. Hybrid Call Service) |
|--|--|--------------------------|-----------------------|---------------------------|-----------|-----------|--|
| Cisco Spark Hybrid Services (Connectors) | Y | N | N | N | N | Y | Y |
| Mobile and Remote Access and/or (from X8.9) Meeting Server Web Proxy | N | Y | N | N | Y | Y | Y* |
| Jabber Guest Services | N | N | Y | N | Y | Y | Y |
| Microsoft gateway service | N | N | N | Y | N | N | N |
| Registrar | N | Y | Y | N | Y | Y | Y |
| CMR Cloud | Y | Y | Y | N | Y | Y | Y |
| Business to Business calling (includes Cisco Webex Hybrid Call Service) | Y | Y* | Y | N | Y | Y | Y |

Key to Table

Y: Yes, these services can be hosted on the same system or cluster

N: No, these services may not be hosted on the same system or cluster

Rules

- Hybrid Services connectors may co-reside with the Expressway-C of a traversal pair used for Call Service, subject to user number limitations.
 - * If your Hybrid Call Service (or B2B) traversal pair is also used for MRA, then the Hybrid Services connectors must be on a separate Expressway-C. This is because we do not support the connectors being hosted on the Expressway-C that is used for MRA.
- Microsoft gateway service requires a dedicated VCS Control or Expressway-C (called "Gateway VCS" or "Gateway Expressway" in the help and documentation)
- Jabber Guest cannot work with MRA (technical limitation)
- MRA is currently not supported in IPv6 only mode. If you want IPv6 B2B calling to co-reside with IPv4 MRA on the same Expressway traversal pair, the Expressway-E and Expressway-C must both be in dual stack mode.

Standard Features

The Expressway has the following standard features:

- Provides secure firewall traversal and session-based access to Cisco Unified Communications Manager for remote workers, without the need for a separate VPN client

Introduction

- 2500 endpoint registrations on a standard [Small/Medium](#) system. 5000 registrations on a Large system - for Mobile and Remote Access registrations the limit is 2500
- SIP Proxy

Note: The SIP and H.323 protocols are disabled by default on new installs of X8.9.2 or later versions. You must enable them on the **Configuration > Protocols** menu.
- SIP Registrar (requires Room or Desktop Registration licenses)
- SIP and H.323 support, including SIP / H.323 interworking
- IPv4 and IPv6 support, including IPv4 / IPv6 interworking
- H.323 gatekeeper
- QoS tagging
- Bandwidth management on both a per-call and a total usage basis, configurable separately for calls within the local subzones and to external systems and zones
- 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
- 1000 subzones and supporting up to 3000 membership rules
- Flexible zone configuration with prefix, suffix and regex support
- Can function as a standalone Expressway, or be neighbored with other systems such as other Expressways, gatekeepers and SIP proxies
- Can be clustered with up to 6 Expressways to provide n+1 redundancy, and up to 4 x individual capacity.
- Intelligent Route Director for single number dialing and network failover facilities
- Optional endpoint authentication
- Control over which endpoints are allowed to register
- Call Policy (also known as Administrator Policy) including support for CPL
- Support for external policy servers
- Can be managed with Cisco TelePresence Management Suite (Cisco TMS) 13.2 or later
- AD authentication for administrators of the Expressway
- Pre-configured defaults for:
 - Cisco Unified Communications Manager neighbor zones
 - Cisco TelePresence Advanced Media Gateway
 - Nortel Communication Server neighbor zones
- Embedded setup wizard using a serial port for initial configuration
- System administration using a web interface or SSH, or via CIMC port (CE1100 appliance)
- Intrusion protection

Optional Features

Some Expressway features are unlocked when you buy and install the appropriate option key. The option keys are described in [Product Identifiers and Corresponding Keys, page 380](#).

FindMe™

FindMe gives individual video users a single alias on which they can be contacted regardless of location. Users can log into a web-based Cisco TMS interface to control where and how they are contacted. The FindMe feature can also

Introduction

be used to enhance interoperability with Microsoft infrastructure (requires Microsoft Interoperability key).

Note: On Expressway, the FindMe feature is included in the Room/Desktop registration license keys.



Device Provisioning

The Device Provisioning option key allows Expressway to provision endpoints with configuration information on request and to supply endpoints with phone book information. All configuration and phone book information is managed in Cisco TMS. Cisco TMS transfers the data to the Expressway, which has a Provisioning Server to distribute the information to endpoint clients.

Note: On Expressway, the Device Provisioning feature is included in the Room/Desktop registration license keys.

See [TMS provisioning](#) and [Cisco TMS Provisioning Extension Deployment Guide](#) for more information about how to configure provisioning.

SIP to Microsoft Interoperability

The Microsoft interoperability service on the Expressway can be used to route SIP calls between the Expressway and a Microsoft server. It provides interworking between Microsoft ICE (used by Microsoft clients) and media for communications with standard video endpoints.

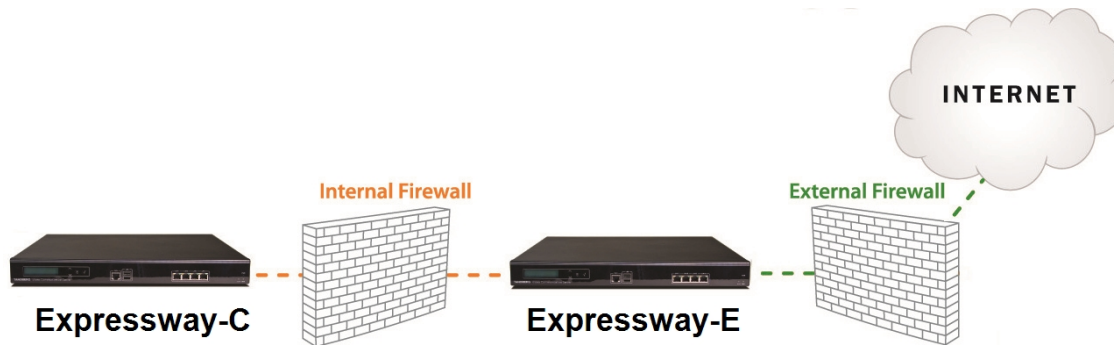
If you use a Gateway Expressway, the **Microsoft Interoperability** option key is needed for all types of communication with Microsoft infrastructure. The option key is not needed if Cisco Meeting Server does the interworking.

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.

Introduction



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.

Virtual Machine Options

The Expressway has 3 virtualized application deployment types:

- Small (only for Cisco Business Edition 6000)
- Medium (standard installation, can also be on BE6000)
- Large (extra performance and scalability capabilities)

See *Cisco Expressway Virtual Machine Installation Guide* on the [Expressway installation guides page](#).

CE Series Appliances

The Expressway is available as a dedicated CE Series appliance based on UCS hardware, as follows:

CE1100 appliance: introduced to fit the UCS M4 chassis. Based on a UCS C220 M4L, replaces the CE500 and CE1000. The CE1100 appliance operates as a medium capacity or large capacity Expressway.

From X8.10 onwards, the requirement to have a 10 Gbps NIC in order to achieve the scalability of a large system is removed. It is now possible to have the capacity of a large system with a 1 Gbps NIC subject to your bandwidth constraints.

Note: The CE500 and CE1000 platforms are no longer available to order. See [End-of-Sale and End-of-Life Announcement for the Cisco TelePresence Video Communication Server \(VCS\) Second-Generation Platform \(Cisco UCS C220 M3 Bundle\)](#).

See *Cisco Expressway CE1100 Appliance Installation Guide* on the [Expressway installation guides page](#).

Software Versions Supported by Hardware Platforms

Table 3 Expressway Software Versions Supported by Platform

| Platform name | Serial Numbers | Scope of software version support |
|-----------------|------------------|-----------------------------------|
| Small VM (OVA) | (Auto-generated) | X8.1 onwards |
| Medium VM (OVA) | (Auto-generated) | X8.1 onwards |
| Large VM (OVA) | (Auto-generated) | X8.1 onwards |

Table 3 Expressway Software Versions Supported by Platform (continued)

| Platform name | Serial Numbers | Scope of software version support |
|--|----------------|-----------------------------------|
| CE500* (Expressway pre-installed on UCS C220 M3L) | 52C##### | X8.1.1 onwards |
| CE1000* (Expressway pre-installed on UCS C220 M3L) | 52B##### | X8.1.1 onwards |
| CE1100 (Expressway pre-installed on UCS C220 M4L) | 52D##### | X8.6.1 onwards |

* As of 26th February 2016, you cannot order the CE500 and CE1000 appliances from Cisco. See the [End-of-sale announcement](#) for other important dates in the lifecycle of these platforms.

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, page 558](#) 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.

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

You can find more information about accessibility here:

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. You can ignore this until you are ready to secure the system.

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

Field Markers

- A red star ★ indicates a mandatory field
- An orange dagger † indicates a field that must be configured on each peer in the cluster

Supported Browsers

The Expressway web interface is designed for and tested with Internet Explorer 8 and 9 (not in compatibility mode), Internet Explorer 10 and 11, Firefox, and Chrome. We do not officially support using other browsers for accessing the UI.

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

HTTP Methods

The Expressway web server allows the following HTTP methods:

| Method | Used by Web UI? | Used by API? | Used to... |
|---------|-----------------|--------------|--|
| GET | Yes | Yes | Retrieve data from a specified resource. For example, to return a specific page in the Expressway web interface. |
| POST | Yes | Yes | Apply data to a web resource. For example, when an administrator saves changes to a setting using the Expressway web interface. |
| OPTIONS | No | Yes | For a specified URL, returns the HTTP methods supported by the server. For example, the Expressway can use OPTIONS to test a proxy server for HTTP/1.1 compliance. |
| PUT | No | Yes | Send a resource to be stored at a specified URI. Our REST API commands use this method to change the Expressway configuration. |
| DELETE | No | Yes | Delete a specified resource. For example, the REST API uses DELETE for record deletion. |

How to disable user access to the API

Administrators have API access by default. This can be disabled in two ways:

- If the Expressway is running in advanced account security mode, then API access is automatically disabled for all users.
- API access for individual administrators can be disabled through their user configuration options.

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 (on the appliance). 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 your administrator username and password.
See [Enabling SSH access, page 269](#) if you prefer to use your private key to authenticate.
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 and registrations is available through this command group. See [Command Reference – xStatus, page 518](#) 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, page 423](#) for a full list of **xConfiguration** commands.
- **xCommand**: these commands allow you to add and configure items and obtain information. See [Command Reference – xCommand, page 491](#) for a full list of **xCommand** commands.
- **xHistory**: these commands provide historical information about calls and registrations.
- **xFeedback**: these commands provide information about events as they happen, such as calls and registrations.

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

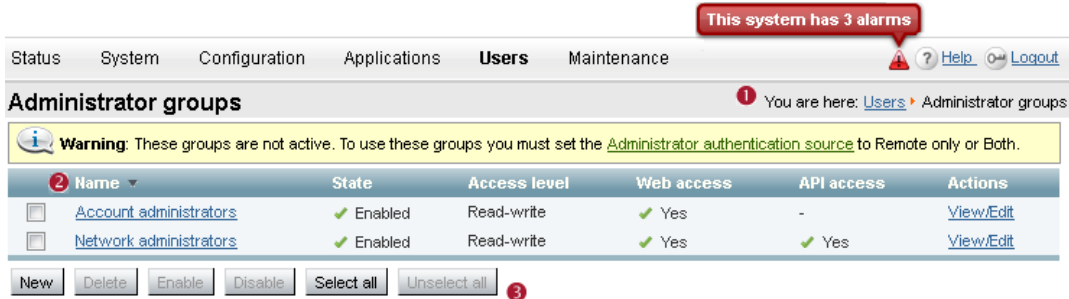
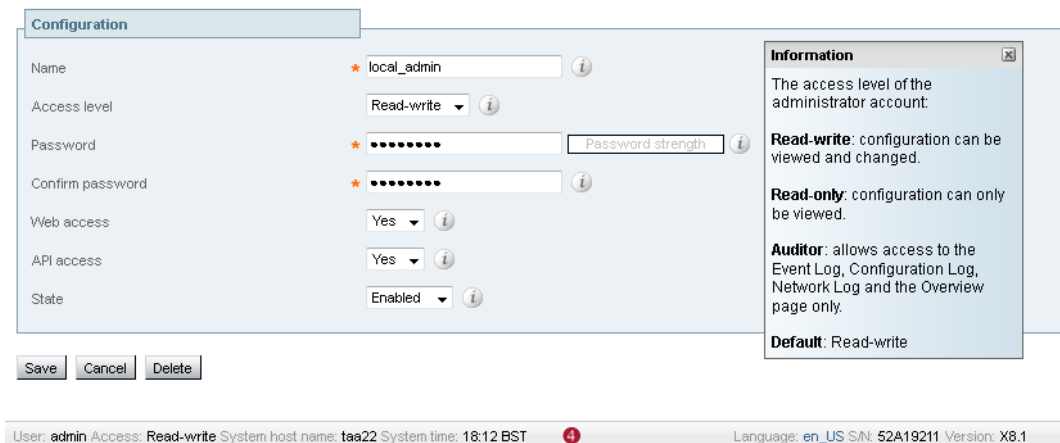









Figure 2 Example configuration page



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

| Page element | | Description |
|------------------------|--|--|
| Page name and location | | 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 | | This icon appears on the top right corner of every page. Clicking on this icon ends your administrator session. |

Introduction

| 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?

Table 4 Feature History by Release Number

| Feature / change | X8.10 | X8.10.1 | X8.10.2 | X8.10.3 (no change) |
|---|---------------|---------------|-----------|------------------------|
| Built-in-Bridge Recording over MRA | Not supported | Not supported | Preview | Preview |
| Improved Push Notification Support for MRA | Preview | Supported | Supported | Supported |
| Self-Describing Tokens Support for MRA (OAuth tokens with refresh) | Preview | Supported | Supported | Supported |
| Access Control Configuration Changes for MRA | Supported | Supported | Supported | Supported |
| Access Policy Support for MRA | Preview | Preview | Preview | Preview |
| Changes to TLS and Cipher Suite Defaults | Supported | Supported | Supported | Supported |
| AES-GCM Cipher Mode for Media Encryption | Supported | Supported | Supported | Supported |
| Delayed Cisco XCP Router Restart for Multitenancy | Supported | Supported | Supported | Supported |
| Server Name Indication for Multitenancy | Supported | Supported | Supported | Supported |
| Session Identifier Support | Supported | Supported | Supported | Supported |
| REST API Expansion | Supported | Supported | Supported | Supported |
| Smart Call Home (Not new in X8.10. Included for information due to its preview status) | Preview | Preview | Preview | Preview |
| Other X8.10 Changes and Enhancements | Supported | Supported | Supported | Supported |

More Information

For information about a particular feature, please see the [Release Notes](#) for the relevant software version.

Service Setup Wizard: Choose Services

Navigating the Wizard

- As of X8.8, you'll see the service setup wizard when you first log in to the Expressway user interface. If you previously logged in or have upgraded, you'll see the **Status > Overview** page (as usual). Click **Run service setup** from that page to launch the wizard. You can run or rerun the wizard at any time.
- While you're in the wizard, click **Skip Service Setup Wizard** if you want to back out completely, or **Back** to the previous page.
- Click **Continue** to save and move to the next wizard page.
- At the end you must restart the Expressway. When you go back into the user interface, you'll only see menus and pages that apply to the services you chose with the wizard.

Choose Series, Type, and Services

1. Choose *Cisco TelePresence Video Communication Server (VCS)* or *Cisco Expressway Series*.
2.
 - If you chose VCS: Choose *VCS Control* or *VCS Expressway*
 - If you chose Expressway: Choose *Expressway-C* or *Expressway-E*The list of services changes to match what is available on your chosen Series and Type.
3. Check the boxes next to the services you want to host on this system.
If you want to keep all the menu options, or if you want to use the wizard for applying licenses but don't want to choose services yet, check *Proceed without selecting services*.
4. Click **Continue**.

Example 1: Hybrid Services

1. Click *Expressway Series*.
2. Click *Expressway-C*.
3. Check *Spark Hybrid Services*.
4. Click **Continue**.
The wizard asks you to review your network configuration. It skipped the licensing page because you don't need a release key, or licenses, or option keys, to register for Hybrid Services.
5. Review the network configuration and modify the settings if necessary (save your changes before you continue the wizard).
6. Click **Finish**.
The wizard opens the **Connector Management** page where you can register the Expressway for Hybrid Services.

Example 2: Expressway Registrar

1. Click *Expressway Series*.
2. Click *Expressway-C*.
3. Check *Registrar*.
4. Check any other compatible services that you have bought for this system. For this example, let's assume *Business to business calls*.
(See [About the Service Setup Wizard, page 9](#), for a matrix of compatible services)
5. Click **Continue**.
The wizard takes you to the licensing and options page.

Service Setup Wizard: Apply Options and Licenses

How do I get Option Keys and Release Keys?

When you order Expressway systems, your Cisco sales representative creates a PAK (Product Authorization Key) for you. The PAK contains one or many Product Identifiers (PIDs) that translate into keys or licenses when you apply them to a particular system. If you are a Cisco partner / reseller, you may prefer to order PIDs for multiple systems in one PAK.

1. Access your PAK at the [Product License Registration Portal](#).
Inside the PAK, you'll see the list of PIDs that you ordered. They are not yet specific to any Expressway. The names and purposes of the PIDs are tabulated in [Product Identifiers and Corresponding Keys, page 380](#).
2. Choose what you want the system to do, and select the PIDs required for that set of features.
3. Click **Assign to device** and then enter the system's serial number.

Service Setup Wizard: Choose Services

4. Click **Finish**.

The system sends you an email containing the option keys you need to unlock your system's features. They are unique to the system with the serial number you used.

5. You can repeat this process, so you may get several emails relevant to one system.

Apply Keys

On the second page of the Service Setup Wizard:

1. Paste the text from your release key email into the first text area.

The system reads the release key out of the pasted text and displays it next to the text area.

2. Paste the text from your option keys email into the second text area.

The system reads the option keys out of the pasted text and displays them next to the text area.

3. Add new text areas if you have more email text to paste in.

4. Click **Add Keys**.

The **License status** table groups the keys that are possible on this system, and whether they are loaded or not loaded. The keys are grouped as follows:

- **Required:** If any keys in this section are not yet loaded, you'll see status **Required** and will not be able to continue through the wizard.
- **Optional:** Shows keys that you may or may not be useful, but that are not strictly required for the services you chose.
- **Unrelated:** These keys won't harm the system if they are loaded, but will not provide any benefit for the services you chose.
- **Incompatible:** These keys cannot work with the selected services. You need to remove them or choose different services before you can continue.

5. Click **Continue**.

The wizard moves on to the next page so you can review the networking configuration.

Example: Expressway Registrar (continued)

1. Paste text containing your release key into the first text area.

2. Paste text containing an Expressway Series key into the second text area (eg. 116341E00-1-AAAAAAA).

3. Click **Continue**.4. Review the networking configuration and click **Continue**.

5. Restart the system when prompted.

This completes the service setup and licensing for the Expressway-C part of your desired outcome. However, since we chose *Business to business calls*, we would have to run the wizard to setup and license an Expressway-E, because the business to business calling deployment requires firewall traversal.

Service Setup Wizard: Review Networking Configuration

Why do I need to see this page?

The purpose of this page is to gather the information you already configured, so you can review it before you commit to the services you've chosen. These parameters are normally found on different pages of the user interface, so this is an opportunity to edit or copy the details.

Before you could log in to the Expressway user interface, you (or another person at your organization) had to configure the basic networking parameters in one of these ways:

- Using a virtual machine deployment template
- Accessing the VM console

Service Setup Wizard: Choose Services

- Accessing the appliance console

You can read about these options in documents that are listed on the [Expressway Install Guides page](#).



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 | 25 |
| Intrusion Protection | 31 |
| Network Services | 36 |
| Configuring External Manager Settings | 44 |
| Configuring TMS Provisioning Extension services | 45 |

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. However, in virtual machine-based Expressway systems, you cannot set the speed 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.

Note: In virtual machine-based Expressway systems, the speed of the connections between the Expressway and Ethernet networks always show as 10000 Mb/s, regardless of the underlying physical NIC(s) actual speed. This is due to a limitation in virtual machines, which cannot retrieve the actual speed from the physical NIC(s).

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 versions of the IP protocol suite. The default is *Both*.

- *IPv4 only*: it only accepts registrations from endpoints using an IPv4 address, and only takes calls between two endpoints communicating via IPv4. It communicates with other systems via IPv4 only.
- *IPv6 only*: it only accepts registrations from endpoints using an IPv6 address, and only takes calls between two endpoints communicating via IPv6. It communicates with other systems via IPv6 only.
- *Both*: it accepts registrations from endpoints using either an IPv4 or IPv6 address, and 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.

Network and System Settings

Some endpoints support both IPv4 and IPv6, however an endpoint can use only one protocol when registering with the Expressway. Which protocol it uses is determined by the format used to specify the IP address of the Expressway on the endpoint. After the endpoint has registered using either IPv4 or IPv6, the Expressway only sends calls to it using this addressing scheme. Calls made to that endpoint from another device using the other addressing scheme are converted (gatewayed) by the Expressway.

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

IPv4 to IPv6 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*. Calls for which the Expressway is acting as an IPv4 to IPv6 gateway are traversal calls and require a Rich Media Session license.

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 the Expressway, which allows you to have a second IP address for your Expressway. On the Expressway-E, the option key also enables static NAT functionality on the external facing LAN port.

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. Select which interface will be the **External LAN interface**, for example *LAN2*.

You can now choose to enable static NAT on the external interface. This setting also determines which port allocates TURN server relays.

Note that:

Network and System Settings

- 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 should switch **Use dual network interfaces** to *No*.
- 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 IP 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 port's private IP address.
 - b. Set **IPv4 static NAT mode** to *On*.
 - c. In the **IPv4 static NAT address** field, enter the port's public IP address - this is the IP address as it appears after translation (outside the NAT element).

IPv6 Mode Features and Limitations

When you set the IP interfaces of the Expressway to *IPv6 Only* mode, those interfaces only use IPv6. They do not use IPv4 to communicate with other systems, and they do not interwork between IPv4 and IPv6 (Dual stack).

Explicit IPv6 Supported Features

- Calls between Expressway-registered IPv6 endpoints.
- DiffServ traffic class (TC) tagging.
- TURN server (on Expressway-E).
- Automated intrusion protection.
- DNS lookups.
- Port usage and status pages.

Supported RFCs

- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification (partially implemented: static global addresses only).
- RFC 2464: Transmission of IPv6 Packets over Ethernet Networks.
- RFC 3596: DNS Extensions to Support IP Version 6.

Network and System Settings

- RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers.
- RFC 4291: IP Version 6 Addressing Architecture.
- RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.
- RFC 4861: Neighbor Discovery for IP version 6 (IPv6).
- RFC 5095: Deprecation of Type 0 Routing Headers in IPv6.
- RFC 6156: Traversal Using Relays around NAT (TURN) Extension for IPv6.

Known Limitations in IPv6 Mode

- IPv6 addresses must be static; they cannot be link-local or SLAAC addresses.
- You must restart the Expressway when you change its IP address or its gateway's IP address.
- Mobile and Remote Access (MRA) is not tested or supported in IPv6 mode. For MRA, the primary call control agent is Unified CM which does not support IPv6.
- Getting revocation status from distributed Certificate Revocation Lists is not supported in IPv6 mode.

Configuring DNS Settings

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

Configuring the System Host Name 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 `ldapserver`). 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 `ldapserver.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.

Network and System Settings

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 DSCP / Quality of Service Settings

About DSCP Marking

From X8.9, the Expressway supports improved DSCP (Differentiated Service Code Point) packet marking for traffic passing through the firewall, including Mobile and Remote Access. DSCP is a measure of the Quality of Service level of the packet. To provide more granular control of traffic prioritization, DSCP values are set (marked) for these individual traffic types:

| Traffic type | Supplied default value | Web UI field |
|--------------|------------------------|---------------|
| Video | 34 | QoS Video |
| Audio | 46 | QoS Audio |
| XMPP | 24 | QoS XMPP |
| Signaling | 24 | QoS Signaling |

Network and System Settings

Before X8.9 you had to apply DSCP values to all signaling and media traffic collectively.

You can optionally change the default DSCP values from the **System > Quality of Service** web UI page (or the CLI).

Notes:

- DSCP value "0" specifies standard best-effort service.
- DSCP marking is applied to SIP and H.323 traffic.
- DSCP marking is applied to TURN media, providing the TURN traffic is actually handled by the Expressway.
- Traffic type "Video" is assigned by default if the media type cannot be identified. (For example, if different media types are multiplexed on the same port.)

Existing QoS/DSCP Commands and API are Discontinued

From X8.9 we no longer support the previous methods to specify QoS/DSCP values. The former Web UI settings **QoS Mode** and **QoS Value**, CLI commands `xConfiguration IP QoS Mode` and `xConfiguration IP QoS Value` and corresponding API are now discontinued. Do not use these commands.

What if I currently use these commands?

When you upgrade the Expressway, any existing QoS value you have defined is automatically applied to the new fields and replaces the supplied defaults. For example, if you had a value of 20 defined, all four DSCP settings (QoS Audio, QoS Video, QoS XMPP, QoS Signaling) are set to 20 also.

We don't support downgrades. If you need to revert to your pre-upgrade software version, the QoS settings are reset to their original supplied defaults. So QoS Mode is set to *None* and QoS Value is set to 0. You will need to manually redefine the values you want to use.

Configuring DSCP Values

To optionally change the supplied DSCP default values, go to the **Quality of Service** page (**System > Quality of Service**) and specify the new values you want to use.

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

Network and System Settings

- 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

Use the **Firewall rules configuration** page to set up and activate a new set of firewall rules.

The set of rules shown is initially a copy of the current active rules. (On a system where no firewall rules have been defined, the list is 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 change the set of firewall rules by adding new rules, or by modifying or deleting existing ones. Changes to the current active rules are held in a pending state. When you finish making changes, you activate the new rules to replace the previous set. For UDP-related rules, note that new rules only take effect at the next system reboot (although if you delete UDP rules, they become inactive as soon as you activate the rule set).

To configure and activate rules:

1. Go to **System > Protection > Firewall rules > Configuration**.
2. Make your changes by adding, modifying, or deleting rules as required.
To change the order of the rules, use 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 finish 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.
6. This step only applies if you add UDP rules. That is, one or more custom rules with **Transport=UDP**. New UDP rules do not take effect until the next system reboot. In this special case, activating the firewall rules is not sufficient by itself. Deleted UDP rules do not have this requirement, and become inactive as soon as you activate the rule set.

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 |
|-------------------------------------|--|---|
| Priority | 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. Firewall rules must have unique priorities. Rule activation will fail if there are multiple rules with the same priority. |
| Interface | The LAN interface on which you want to control access. | This only applies if the Advanced Networking option key is installed. |
| IP address and Prefix length | These two fields together determine the range of IP addresses to which the rule applies. | The Address range field shows the range of IP addresses to which the rule applies, based on the combination of the IP address and Prefix length . The prefix length range is 0-32 for an IPv4 address, and 0-128 for an IPv6 address. |

Network and System Settings

| Field | Description | Usage tips |
|---------------------------|--|---|
| Service | 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. |
| Transport | The transport protocol to which the rule applies. | Only applies if specifying a <i>Custom</i> service. |
| Start and end port | The port range to which the rule applies. | Only applies if specifying a UDP or TCP <i>Custom</i> service. |
| Action | The action to take against any IP traffic that matches the rule. <i>Allow</i> : Accept the traffic. <i>Drop</i> : Drop the traffic without any response to the sender. <i>Reject</i> : Reject the traffic with an 'unreachable' response. | Dropping the traffic means that potential attackers are not provided with information as to which device is filtering the packets or why. 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. |
| Description | An optional free-form description of the firewall rule. | If you have a lot of rules you can use the Filter 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

You can use the automated protection service 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, page 35](#) below).

You should use automated protection in combination with [firewall rules](#); automated protection to dynamically detect and temporarily block specific threats, and 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 new categories.

Network and System Settings

The rules which associate specific log file messages with each category are also pre-configured and you cannot change them. 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

From X8.9 onwards, automated intrusion protection is enabled, by default, for the following categories:

- http-ce-auth
- http-ce-intrusion
- sshpfd-auth
- sshpfd-intrusion
- xmpp-intrusion

This change affects new systems. Upgraded systems keep their existing protection configuration.

To enable intrusion protection on your Expressway:

1. Go to **System > Administration**.
2. Set **Automated protection service** to *On*.
3. Click **Save**.

The service is running now, but you must configure the protection categories and any exemptions necessary for your environment.

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.

Network and System Settings

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 IP 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.

Automated Protection in MRA Deployments

The Expressway-C receives a lot of inbound traffic from Unified CM and from the Expressway-E when it is used for Mobile and Remote Access.

If you want to use automated protection on the Expressway-C, you should add exemptions for all hosts that use the automatically created neighbor zones and the Unified Communications secure traversal zone. The Expressway does not automatically create exemptions for discovered Unified CM or related nodes.

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.

Network and System Settings

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.

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 |
|-------------------------------------|--|--|
| Services | | |
| Serial port / console | 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. |
| SSH service | Whether the Expressway can be accessed via SSH and SCP. Default is <i>On</i> . | |
| Web interface (over HTTPS) | 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. |
| Session limits | | |
| Session time out | 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. | |
| Per-account session limit | 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. |
| System session limit | 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. |
| System protection | | |
| Automated protection service | Whether the automated protection service is active. Default is <i>On</i> . | After enabling the service you must go and configure the specific protection categories . |

Network and System Settings

| Field | Description | Usage tips |
|--|---|--|
| Automatic discovery protection | <p>Controls how management systems such as Cisco TMS can discover this Expressway.</p> <p><i>Off:</i> automatic discovery is allowed.</p> <p><i>On:</i> Cisco TMS has to be manually configured to discover this Expressway and must provide administrator account credentials.</p> <p>Default is <i>Off</i>.</p> | You must restart the system for any changes to take effect. |
| Web server configuration | | |
| Redirect HTTP requests to HTTPS | Determines whether HTTP requests are redirected to the HTTPS port. Default is <i>On</i> . | <p>HTTPS must also be enabled for access via HTTP to function.</p> <p>When you enter the address without prepending the protocol, your browser assumes HTTP (on port 80). If this setting is <i>On</i>, the Expressway redirects your browser to the Web administrator port.</p> |
| HTTP Strict Transport Security (HSTS) | <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. |
| Web administrator port | <p>Sets the https listening port for administrators to access the Expressway web interface. Default is 443.</p> <p>We strongly recommend using a non-default port for web administration on the Expressway-E if you enable any features that need 443, eg. Meeting Server Web Proxy.</p> <p>Restart the Expressway to make this change effective.</p> | <p>If you use a non-default port, and you prepend the <code>https://</code> protocol to the address, you must append the port. For example, you would put the address <code>https://vcse.example.com:445</code> into your browser; if you try <code>https://vcse.example.com</code>, the browser assumes port 443 and the Expressway denies access.</p> <p>Note: You could lose web access to the Expressway if a network element blocks traffic to the web admin port; you can use SSH or the console to change the port if necessary.</p> |

Network and System Settings

| Field | Description | Usage tips |
|---|--|---|
| Client certificate-based security | <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>Important:</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 Managing the Trusted CA Certificate List, page 279 page, and test client certificates on the Testing Client Certificates, page 287 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 Certificate-based authentication configuration page.</p> <p>This setting does not affect client verification of the Expressway's server certificate.</p> |
| Certificate revocation list (CRL) checking | <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> | <p>Only applies if Client certificate-based security is enabled.</p> |

| Field | Description | Usage tips |
|--|---|--|
| CRL inaccessibility fallback behavior | <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 Client certificate-based security 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

Network and System Settings

- 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 |
|---|---|--|
| SNMP mode | Controls the level of SNMP support. <i>Disabled</i> : no SNMP support. <i>v3 secure SNMP</i> : supports authentication and encryption. <i>v3 plus TMS support</i> : secure SNMPv3 plus non-secure access to OID 1.3.6.1.2.1.1.2.0 only. <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> . |
| Description | 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. |
| Community name | 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> . |
| System contact | The name of the person who can be contacted regarding issues with the Expressway. The default is <i>Administrator</i> . | The System contact and Location are used for reference purposes by administrators when following up on queries. |
| Location | Specifies the physical location of the Expressway. | |
| Username | 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) | | |
| Authentication mode | Enables or disables SNMPv3 authentication. | |
| Type | The algorithm used to hash authentication credentials. <i>SHA</i> : Secure Hash Algorithm. <i>MD5</i> : Message-Digest algorithm 5. The default is <i>SHA</i> . | |
| Password | The password used to encrypt authentication credentials. | Must be at least 8 characters. |
| v3 Privacy settings (only applicable to SNMPv3) | | |
| Privacy mode | Enables or disables SNMPv3 encryption. | |

Network and System Settings

| Field | Description | Usage tips |
|-----------------|--|--------------------------------|
| Type | <p>The security model used to encrypt messages.</p> <p><i>DES</i>: Data Encryption Standard 56-bit encryption.</p> <p><i>AES</i>: Advanced Encryption Standard 128-bit encryption.</p> <p>If available, the default and recommended setting is <i>AES</i>.</p> | |
| Password | 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 Key ID , Hash method and Pass phrase 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. 00 ok means there are no issues. See the Flash Status Word Reference Table, page 523 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 Authentication method is <i>Disabled</i> . |
| Event | Shows the last event as determined by NTP (for example <i>reachable</i> or <i>sys.peer</i>) |
| 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. Each time the NTP configuration is changed, the NTP client is restarted and the Reachability 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.

Network and System Settings

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

Use the **Login page configuration** page (**System > Login page**) to specify a message and image to appear on the login page. The **Welcome message title** and **text** appears to administrators when they log in using the CLI or the web interface.

You can upload an image to appear above the welcome message on the login page, in the web interface.

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

Optionally you can specify that the welcome message must be acknowledged before the person logging in is allowed to continue. In this case the system displays an acceptance button, which the user must click to continue.

If the Expressway is using the [TMS Provisioning Extension services](#) to provide FindMe account data, then users log into their FindMe accounts through Cisco TMS, not through Expressway.

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 |
|--------------------------------------|---|--|
| Address and path | 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 tms/public/external/management/SystemManagementService.asmx . |
| Protocol | Determines whether communications with the external manager are over <i>HTTP</i> or <i>HTTPS</i> . The default is <i>HTTPS</i> . | |
| Certificate verification mode | 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 Managing the Trusted CA Certificate List, page 279 page (Maintenance > Security > Trusted CA certificate). |

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".

Configuring TMS Provisioning Extension services

Cisco TMSPE services are hosted on Cisco TMS. They provide the user, device and phone book data that is used by the Expressway's [Provisioning Server](#) to service provisioning requests from endpoint devices. They also provide the Expressway with the FindMe account configuration data that it uses to provide FindMe services.

The **TMS Provisioning Extension services** page (**System > TMS Provisioning Extension services**) is used to configure how the Expressway connects to the Cisco TMSPE services. We recommend that you use Cisco TMS to make any changes to the Cisco TMSPE services' configuration settings. Any changes made to the settings via this page will not be applied within Cisco TMS.

The **FindMe**, **Users**, **Phone books** and **Devices** services are only available if you have installed registration licenses.

The configurable options are:

| Field | Description | Usage tips |
|---|--|---|
| Default connection configuration | | |
| This section specifies default connection settings for accessing the Cisco TMSPE services. Each specific service can choose to use these default settings or, alternatively, specify its own connection settings, for example if a different Cisco TMSPE server is being used for each service. | | |
| Server address | The IP address or Fully Qualified Domain Name (FQDN) of the service. | |
| Destination port | The listening port on the Cisco TMSPE service. Default is 443. | |
| Encryption | The encryption to use for the connection to the Cisco TMSPE service. <i>Off</i> : no encryption is used. <i>TLS</i> : TLS encryption is used. Default is <i>TLS</i> . | A TLS connection is recommended. |
| Verify certificate | Controls whether the certificate presented by the Cisco TMSPE service is verified against the Expressway's current trusted CA list and, if loaded, the revocation list. Default is Yes. | If you enable verification: <ul style="list-style-type: none"> ■ IIS (on the Cisco TMSPE server) must be installed with a signed certificate and be set to enforce SSL connections. ■ You must add the certificate of the issuer of the Cisco TMSPE server's certificate to the file containing the Expressway's trusted CA certificates. This is done from the Managing the Trusted CA Certificate List, page 279 page (Maintenance > Security > Trusted CA certificate). |

Network and System Settings

| Field | Description | Usage tips |
|---|---|---|
| Check certificate hostname | Controls whether the hostname contained within the certificate presented by the Cisco TMSPE service is verified by the Expressway. Default is <i>Yes</i> . | If enabled, the certificate hostname (also known as the Common Name) must match the specified Server address . If the server address is an IP address, the required hostname is obtained via a DNS lookup. This only applies if Verify certificate is <i>Yes</i> . |
| Base group | The ID used to identify this Expressway (or Expressway cluster) with the Cisco TMSPE service. | The TMS administrator will supply this value. The Base group ID used by the Devices service must be explicitly specified as it is normally different from that used by the other services. |
| Authentication username and password | The username and corresponding password used by the Expressway to authenticate itself with the Cisco TMSPE service. | If TLS encryption is not enabled, the authentication password is sent in the clear. |
| Service-specific configuration | | |
| You can specify the connection details for each of the Cisco TMSPE services: Users , FindMe , Phone books and Devices . | | |
| Connect to this service | Controls whether the Expressway connects to the Cisco TMSPE service. Default is <i>No</i> . | If enabled, the status of the connection is shown to the right of the field; this can be either <i>Checking</i> , <i>Active</i> or <i>Failed</i> . Click details to view full status information. |
| Polling interval | The frequency with which the Expressway checks the Cisco TMSPE service for updates. Defaults are: FindMe: <i>2 minutes</i> Users: <i>2 minutes</i> Phone books: <i>1 day</i> The Device service polling interval is set to 30 seconds and cannot be modified. | You can request an immediate update of all services by clicking Check for updates at the bottom of the page. |
| Use the default connection configuration | Controls whether the service uses the default connection configuration for Cisco TMSPE services. Default is <i>Yes</i> . | If <i>No</i> is selected, an additional set of connection configuration parameters will appear. You can then specify alternative connection details for the service that will override those specified in the Default connection configuration section. |

A full and immediate resynchronization of all data between the Expressway and Cisco TMS can be triggered at any time by clicking **Perform full synchronization** (at the bottom of the of the **TMS Provisioning Extension services** page). Note that this will result in a temporary (a few seconds) lack of service on the Expressway while the data is deleted and fully refreshed. If you only need to ensure that all of the latest updates within Cisco TMS have been supplied to the Expressway then click **Check for updates** instead.

Further status information

The menu options under **Status > Applications > TMS Provisioning Extension services** provide full status information about the Cisco TMSPE services, including:

Network and System Settings

- the status of the connection between the Expressway and the Cisco TMSPE services
- views of the user, FindMe and phone book data supplied by the Cisco TMSPE services
- a summary of the requests received from endpoint devices and the number of provisioning licenses being consumed
- the status of the devices that are making provisioning requests to the Expressway's Provisioning Server



Firewall Traversal

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

| | |
|---|----|
| About Firewall Traversal | 49 |
| Firewall Traversal Configuration Overview | 51 |
| Configuring a Traversal Client and Server | 52 |
| Configuring Ports for Firewall Traversal | 53 |
| Firewall Traversal and Authentication | 56 |
| About ICE and TURN Services | 57 |
| Configuring TURN Services | 58 |

About Firewall Traversal

The purpose of a firewall is to control IP traffic entering your network. Firewalls 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:

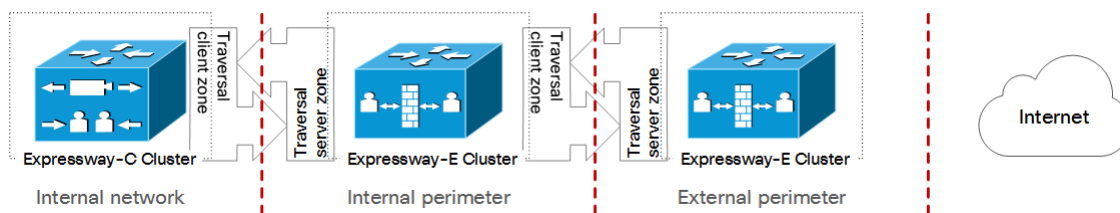
- An Expressway-E located outside the firewall on the public network or in the DMZ, which acts as the firewall traversal server.
- An Expressway-C or other traversal-enabled endpoint located in a private network, which acts as the firewall traversal client.

The two systems work together to create an environment where all connections between the two are outbound. That is, established from the client to the server. And so able to successfully traverse the firewall.

Chained firewall traversal

For business-to-business Expressway deployments, you can configure firewall traversal chaining. As well as acting as a traversal server, Expressway-E can act as a traversal client to another Expressway-E.

Figure 3 Example of Two Chained Expressway-Es



If you chain two Expressway-Es for example (pictured), the first Expressway-E is a traversal server for the Expressway-C. That first Expressway-E is also a traversal client of the second Expressway-E. The second Expressway-E is a traversal server for the first Expressway-E.

Firewall Traversal

Note:

- Traversal chaining is not supported for Mobile and Remote Access deployments.
- This capability was formally introduced to the Cisco Expressway Series in version X8.10. It has been possible with the Cisco TelePresence VCS since firewall traversal was introduced.

Recommendations and Prerequisites

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

Do not use a shared address for the Expressway-E and the Expressway-C, as the firewall cannot distinguish between them. If you use static NAT for IP addressing on the Expressway-E, make sure that any NAT operation on the Expressway-C does not resolve to the same traffic IP address. We do not support shared NAT addresses between Expressway-E and Expressway-C.

How Does it Work?

The traversal client constantly maintains a connection through 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, page 52](#) 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:

Firewall Traversal

- 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 > Local Zones > 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: Changes to the **Use configured demultiplexing ports** setting need a system restart to take effect.

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:

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

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.

Firewall Traversal

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, page 153](#) 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, page 156](#) 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, page 57](#).
- To reconfigure the default ports used by the Expressway-E, see [Configuring Ports for Firewall Traversal, page 53](#).

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 Username 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 Username and Password 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 Peer 1 address field. |

Firewall Traversal

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

Create credential 2

Configuration

Name: client_username

Password: *****

VCS Control (client)

Create zone 3

Configuration

Name: to Traversal Server

Type: Traversal client

Hop count: 15

Connection credentials 4

Username: client_username

Password: *****

H.323 5

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 6: traversalserver@example.com

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, page 308](#) 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:

Firewall Traversal

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 is 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. They are not needed 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

Firewall Traversal

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 5 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 Note). 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 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 Note). 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. RTP and RTCP media non-demultiplexing ports are allocated from the remainder of the traversal media ports range: UDP/36002-59999 Note . |
| 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. |

Note:

The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at **Configuration > Local Zones > 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: Changes to the **Use configured demultiplexing ports** setting need a system restart to take effect.

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.

Firewall Traversal

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 6 Port connections out to the public internet

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

* The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at **Configuration > Local Zones > 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:** Changes to the **Use configured demultiplexing ports** setting need a system restart to take effect.

** 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 |
|---|--|
| Expressway-C The Expressway client provides its Username and Password . These are set on the traversal client zone by using Configuration > Zones > Zones > Edit zone , in the Connection credentials section. | The traversal server zone for the Expressway client must be configured with the client's authentication Username . This is set on the Expressway-E by using Configuration > Zones > Zones > Edit zone , in the Connection credentials section. There must also be an entry in the Expressway-E's authentication database with the corresponding client username and password. |

Firewall Traversal

| Traversal client | Expressway-E traversal server |
|---|---|
| Endpoint The endpoint client provides its Authentication ID and Authentication Password . | There must be an entry in the Expressway-E's authentication database with the corresponding client username and password. |

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 (and is therefore a non-traversal call). 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 and thus requires a RMS license.

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 clients that are registered through a Microsoft Edge Server you need to use the [Microsoft interoperability service](#).
- 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.
- Some limitations apply if you want to use TURN on port 443:
 - You must first change the web administrator port to a different port (**System > Administration**).
 - The option to use port 443 does not apply to large systems - Expressway-E Large OVAs or large scale appliances.
 - Not currently supported with Cisco Meeting Server.

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 |
|----------------------|--|------------|
| TURN services | Determines whether the Expressway offers TURN services to traversal clients. | |

Firewall Traversal

| Field | Description | Usage tips |
|-------------------------------------|--|--|
| TURN requests port | <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 Turn requests port (or range, for Large systems) while the Turn services are already <i>On</i>:</p> <ol style="list-style-type: none"> 1. Change Turn services to <i>Off</i> and Save 2. Edit the port number/range 3. Change Turn services to <i>On</i> and Save <p>This is because changes to the port numbers do not come into effect until the TURN services are restarted.</p> |
| Authentication realm | 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. |
| Media port range start / end | <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 | 62 |
| Mobile and Remote Access | 71 |
| External XMPP Federation | 101 |
| Delayed Cisco XCP Router Restart | 112 |
| Jabber Guest Services Overview | 115 |
| Meeting Server Web Proxy on Expressway | 116 |

Unified Communications Prerequisites

Configuring a Secure Traversal Zone Connection for Unified Communications

Unified Communications features such as Mobile and Remote Access or Jabber Guest, require 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: Configure only one *Unified Communications traversal* zone per Expressway traversal pair. That is, one *Unified Communications traversal* zone on the Expressway-C cluster, and one corresponding *Unified Communications traversal* zone on the Expressway-E cluster.

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 let you upload a server certificate without this extension when Unified Communications features are 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, page 64](#)).
 - To generate a CSR and /or to upload a server certificate to the Expressway, go to **Maintenance > Security > Server certificate**. You must restart the Expressway for the new server certificate to take effect.

Unified Communications

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 > Trusted CA certificate**. You must restart the Expressway for the new trusted CA certificate to take effect.

See *Cisco Expressway Certificate Creation and Use Deployment Guide* on the [Expressway configuration guides page](#).

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 Expressway-C or a traversal server zone when selected on 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> |
| Connection credentials section | | |
| Username | "exampleauth" for example | "exampleauth" for example |
| Password | "ex4mpl3.c0m" for example | Click Add/Edit local authentication database , then in the popup dialog click New and enter the Name ("exampleauth") and Password ("ex4mpl3.c0m") and click Create credential . |
| SIP 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. |
| Authentication section | | |
| Authentication policy | <i>Do not check credentials</i> | <i>Do not check credentials</i> |
| Location section | | |
| Peer 1 address | Enter the FQDN of the Expressway-E. 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 |

4. 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 CA-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.

Unified Communications

This means that either secure HTTP or secure SIP, between Expressway-C and Cisco Unified Communications Manager, will fail.

Also, when generating *tomcat* certificate signing requests for any products within the Cisco Collaboration Systems Release 10.5.2, you need to be aware of [CSCus47235](#). You need to work around this issue to ensure that the FQDNs of the nodes are in the certificates as Subject Alternative Names. The *Expressway X8.5.3 Release Notes* have the details of the workarounds.

Expressway Certificates

The Expressway certificate signing request (CSR) tool prompts for and incorporates the relevant subject alternative 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:

| Add these items ↓ as subject alternative names | ← When generating a CSR for these purposes → | | | |
|---|--|-------------------------------|-------------------------------|----------------------------|
| | Mobile and Remote Access | Jabber Guest | XMPP Federation | Business to Business Calls |
| Unified CM registrations domains (despite their name, these have more in common with service discovery domains than with Unified CM SIP registration domains) | Required on Expressway-E only | – | – | – |
| XMPP federation domains | – | – | Required on Expressway-E only | – |
| IM and Presence chat node aliases (federated group chat) | – | – | Required | – |
| Unified CM phone security profile names | Required on Expressway-C only | – | – | – |
| (Clustered systems only) Expressway cluster name | Required on Expressway-C only | Required on Expressway-C only | Required on Expressway-C only | |

Note:

- You may need to produce a new server certificate for the Expressway-C if chat node aliases are added or renamed. Or when IM and Presence nodes are added or renamed, or new TLS phone security profiles are added.
- You must produce a new Expressway-E certificate 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 4 Entering subject alternative names for security profiles and chat node aliases on the Expressway-C's CSR generator

Expressway-E server certificate requirements

The Expressway-E server certificate needs to include the following elements in its list of subject alternative names (SAN):

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

The Unified CM registration domains used in the Expressway configuration and Expressway-E certificate, are used by Mobile and Remote Access clients to lookup the `_co11ab-edge` DNS SRV record during service discovery. They enable MRA registrations on Unified CM, and are primarily for service discovery.

These service discovery domains may or may not match the SIP registration domains. It depends on the deployment, and they don't have to match. One example is a deployment that uses a .local or similar private domain with Unified CM on the internal network, and public domain names for the Expressway-E FQDN and service discovery. In this case, you need to include the public domain names in the Expressway-E certificate as SANs. There is no need to include the private domain names used on Unified CM. You only need to list the edge domain as a SAN.

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 `co11ab-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.

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

Figure 5 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 | |
|--|---|
| Subject alternative names | FQDN of Expressway cluster plus FQDN of this peer i |
| Additional alternative names (comma separated) | <input type="text"/> i |
| Unified CM registrations domains | <input type="text" value="example.com"/> Format <input type="text" value="CollabEdgeDNS"/> i |
| XMPP federation domains | <input type="text" value="example.com"/> Format <input type="text" value="DNS"/> i |
| IM and Presence chat node aliases (federated group chat) | <input type="text" value="chatnode1.example.com,chatnode2.example.com"/> Format <input type="text" value="DNS"/> i |
| Alternative name as it will appear | DNS:vcse.example.com DNS:vcs-e-cluster.example.com DNS:collab-edge.example.com DNS:example.com DNS:chatnode1.example.com DNS:chatnode2.example.com |

See *Cisco Expressway Certificate Creation and Use Deployment Guide* on the [Expressway configuration guides page](#).

About Domain Certificates and Server Name Indication for Multitenancy

Multitenancy is part of Cisco Hosted Collaboration Solution (HCS), and allows a service provider to share a Expressway-E cluster among multiple tenants.

Using the Server Name Indication (SNI) protocol extension within TLS, the Expressway can now store and use domain-specific certificates that can be offered to a client during the TLS handshake. This capability allows seamless integration of endpoints registering through MRA in a multitenant environment, and ensures the certificate domain name matches the client's domain. During a TLS handshake, the client includes an SNI field in the *ClientHello* request. The Expressway looks up its certificate store and tries to find a match for the SNI hostname. If a match is found the domain-specific certificate is returned to the client.

Note: In multitenant mode, you must configure the system hostname on the **System > DNS** page of the Cisco Expressway-E to match the hostname configured in DNS (case-specific before X8.10.1, case insensitive from X8.10.1). Otherwise Cisco Jabber clients will be unable to register successfully for MRA.

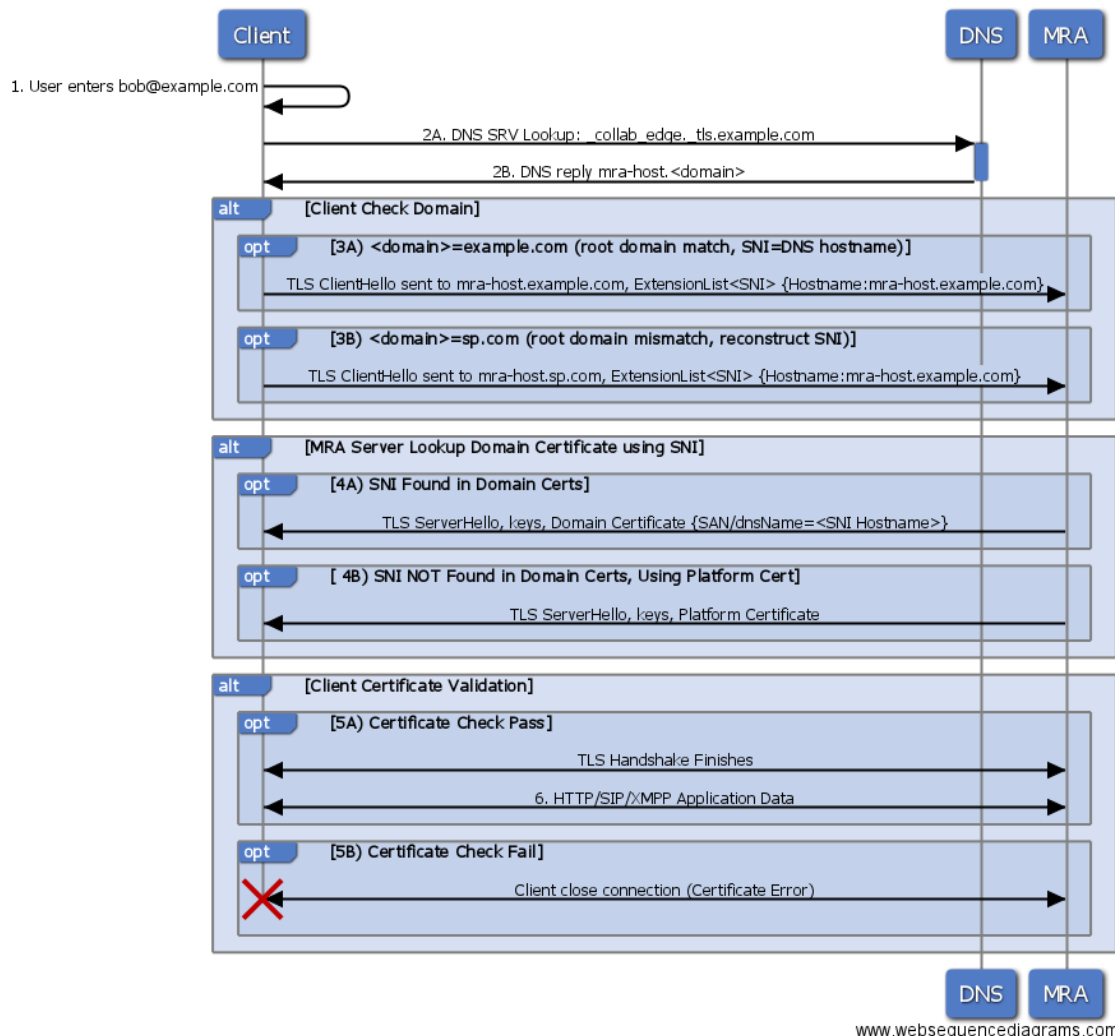
See *Multitenancy with Cisco Expressway* on the [Cisco Hosted Collaboration Solution page](#).

SNI Call Flow

1. On the MRA client being registered, the user enters `bob@example.com` where `example.com` is the user's service domain (customer domain).
2. The client does a DNS resolution.
 - a. It sends a DNS SRV request for `_collab-edge._tls.example.com`.
 - b. The DNS replies to the request:
 - In a single tenant setup: the DNS reply usually includes the hostname within the service domain (for example, `mra-host.example.com`).
 - In a multitenant setup: DNS may instead return the service provider's MRA hostname in the service provider's domain, which is different from the user's service domain (for example, `mra-host.sp.com`).

3. The client sets up SSL connection.
 - a. The client sends SSL ClientHello request with an SNI extension:
 - If the DNS-returned hostname has the same domain as the user's service domain, the DNS hostname is used in SNI server_name (unchanged).
 - Otherwise, in the case of a domain mismatch, the client sets the SNI server_name to the DNS hostname plus the service domain (for example instead of the DNS-returned `mra-host.sp.com` it changes to `mra-host.example.com`).
 - b. The Expressway-E searches its certificate store to find a certificate matching the SNI hostname.
 - If a match is found, the Expressway-E will send back the certificate (SAN/dnsName=SNI hostname)
 - Otherwise, MRA will return it's platform certificate.
 - c. The client validates the server certificate.
 - If the certificate is verified, SSL setup continues and SSL setup finishes successfully.
 - Otherwise, a certificate error occurs.
4. Application data starts. Note, for SIP and HTTPS, the application starts SSL negotiation immediately. For XMPP, the SSL connection starts once the client receives XMPP StartTLS.

SNI Certificate Workflow on Expressway



Managing the Expressway's Domain Certificates

You manage the Expressway's domain certificates through the **Domain certificates** page (**Maintenance > Security > Domain certificates**). These certificates are used to identify domains when multiple customers – in a multitenant environment – are sharing a Expressway-E cluster to communicate with client systems using TLS encryption and with web browsers over HTTPS. You can use the domain certificate page to:

- View details about the currently loaded certificate.
- Generate a Certificate Signing Request (CSR).
- Upload a new domain certificate.

Note: We highly recommend using certificates based on RSA keys. Other types of certificate, such as those based on DSA keys, are not tested and may not work with the Expressway in all scenarios. Use the **Trusted CA certificate** page to manage the list of certificates for the Certificate Authorities (CAs) trusted by this Expressway.

Viewing a Currently Uploaded Domain Certificate

When you click on a domain, the domain certificate data section shows information about the specific domain certificate currently loaded on the Expressway.

To view the currently uploaded domain 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. To delete the currently uploaded domain click **Delete**.

Note: Do not allow your domain 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.

Adding a New Domain

1. Go to **Maintenance > Security > Domain certificates**.
2. Click **New**.
3. Under **New local domain**, enter the name of the domain you wish to add. An example valid domain name is `100.example-name.com`.
4. Click **Create domain**.
5. The new domain will be added on the **Domain certificates** page and you can proceed to upload a certificate for the domain.

Generating a Certificate Signing Request

The Expressway can generate domain CSRs. This removes the need to use an external mechanism to generate and obtain certificate requests.

To generate a CSR:

1. Go to **Maintenance > Security > Domain certificates**.
2. Click on the domain for which you wish to generate a CSR.
3. Click **Generate CSR** to go to the **Generate CSR** page.
4. Enter the required properties for the certificate.
 - See [Domain Certificates and Clustered Systems, page 70](#) if your Expressway is part of a cluster.
5. 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.

6. You are returned to the **Domain 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**.
- The user interface provides an option to set the Digest Algorithm. The default is set to SHA-256, with options to change it to SHA-384 or SHA-512.
- The user interface provides an option to set the key length. Expressway support a key length of 1024, 2048 and 4096.

Uploading a New Domain Certificate

When the signed domain certificate is received back from the certificate authority, it must be uploaded to the Expressway. Use the **Upload new certificate** section to replace the current domain certificate with a new certificate.

To upload a domain certificate:

1. Go to **Maintenance > Security > Domain certificates**.
2. Use the **Browse** button in the **Upload new certificate** section to select and upload the domain certificate PEM file.
3. If you used an external system to generate the CSR you must also upload the server private key PEM file that was used to encrypt the domain certificate. (The private key file will have been automatically generated and stored earlier if the Expressway was used to produce the CSR for this domain 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 domain certificate data**.

Domain 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 domain certificates uploaded to each relevant peer.

You must ensure that the correct domain certificate is uploaded to the appropriate peer, otherwise the stored private key on each peer will not correspond to the uploaded certificate.

Mobile and Remote Access

This section describes how to configure your Expressway to support Unified Communications Mobile and Remote Access (MRA).

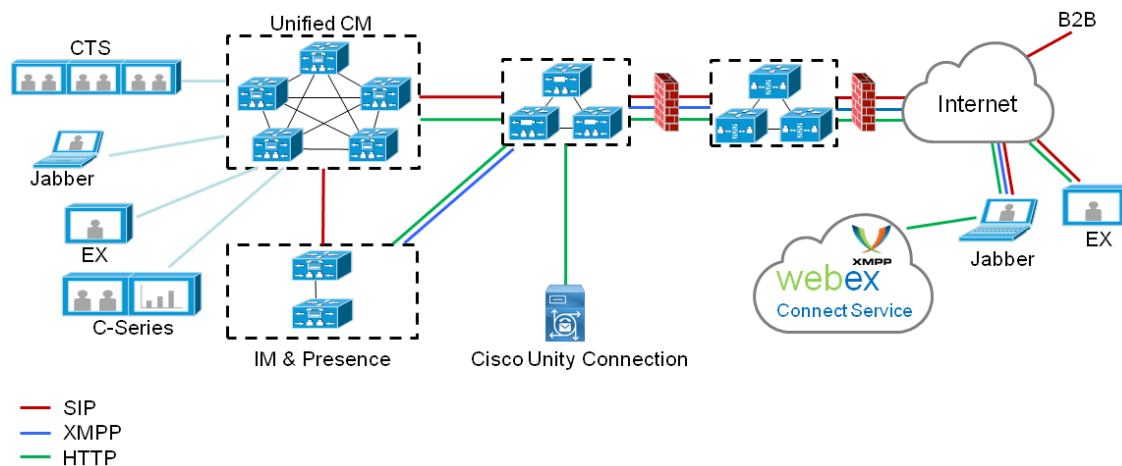
Mobile and Remote Access Overview

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:

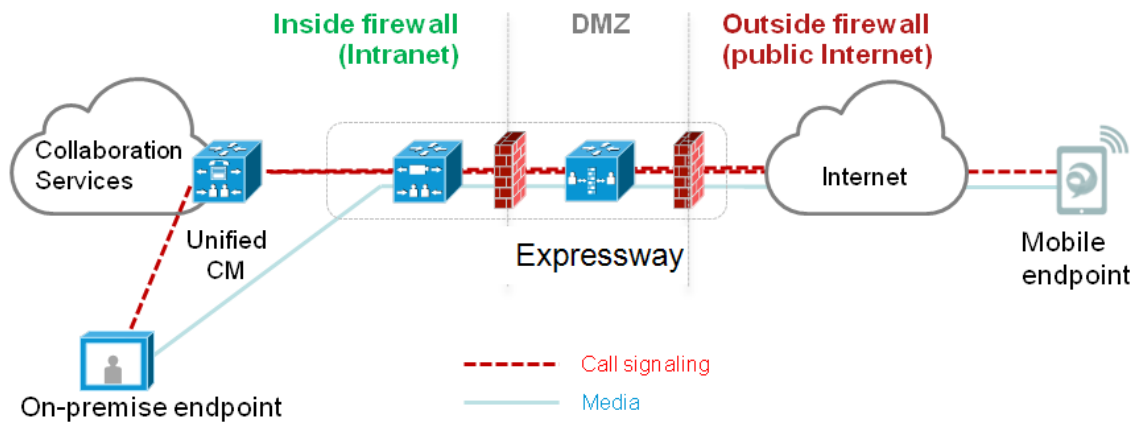
- **Off-premises access:** a consistent experience outside the network for Jabber and EX/MX/SX Series clients
- **Security:** secure business-to-business communications
- **Cloud services:** enterprise grade flexibility and scalable solutions providing rich WebEx integration and Service Provider offerings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

Figure 6 Unified Communications: Mobile and Remote Access



Note that third-party SIP or H.323 devices can register to the Expressway-C and, if necessary, interoperate with Unified CM-registered devices over a SIP trunk.

Figure 7 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.

Deployment Scope

The following major Expressway-based deployments do not work together. They cannot be implemented together on the same Expressway (or traversal pair):

- Mobile and Remote Access
- Microsoft interoperability, using the Expressway-C-based B2BUA
- Jabber Guest services

Jabber Client Connectivity Without VPN

The Mobile and Remote Access solution (MRA) supports a hybrid on-premises and cloud-based service model. This provides a consistent experience inside and outside the enterprise. MRA 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.

MRA allows Jabber clients that are outside the enterprise to do the following:

- 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: Cisco Jabber Video for TelePresence (Jabber Video) does not work with MRA. (It is supported as a general client registered to Expressway.)

Setting Up the Expressway-E for Mobile and Remote Access

This section describes the configuration steps required on the Expressway-E for Mobile and Remote Access.

Configuring DNS and NTP Settings

Make sure that the following basic system settings are configured on Expressway:

1. **System host name** and **Domain name** are specified (**System > DNS**).
2. Public DNS servers are specified (**System > DNS**).
3. 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, make sure 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**.

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. It also describes the access control settings for MRA, and how to configure them.

Installing Expressway Security Certificates and Setting Up a Secure Traversal Zone

Unified Communications features such as Mobile and Remote Access or Jabber Guest, require 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:

- [Unified Communications Prerequisites, page 62](#) (if your system does not already have a secure traversal zone in place)
- [Server Certificate Requirements for Unified Communications, page 64](#)

If you want to use XMPP federation, the IM&P servers must be discovered on the Expressway-C. So that all relevant information is available when generating certificate signing requests.

Unified Communications

Setting Up the Expressway-C for Mobile and Remote Access

This section describes the configuration steps required on the Expressway-C for Mobile and Remote Access.

Configuring DNS and NTP Settings

Make sure that the following basic system settings are configured on Expressway:

1. **System host name** and **Domain name** are specified (**System > DNS**).
2. Local DNS servers are specified (**System > DNS**).
3. 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.

[Recommended] Disabling Automated Intrusion Protection on Expressway-C

If your Expressway-C is newly installed from X8.9 onwards, the automated intrusion protection service is running by default. This could prevent your deployment working properly, so we recommend you disable it on the Expressway-C as follows:

1. Go to **System > Administration**.
2. Switch **Automated protection service** to *Off*.
3. Click **Save**.

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**.

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.

Unified Communications

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 Expressway:** the Expressway is authoritative for this SIP domain. The Expressway acts as a SIP registrar for the domain, and accepts registration requests for any SIP endpoints attempting to register with an alias that includes this domain. The default is *On*.
 - **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 *Off*.
 - **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 *Off*.
 - **XMPP federation:** Enables XMPP federation between this domain and partner domains. The default is *Off*.
 - **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. For example, the same domain may be used by endpoints such as Jabber or EX Series devices that require line-side Unified Communications support, and by other endpoints such as third-party SIP or H.323 devices that require Expressway support. (In this scenario, the signaling messages sent from the endpoint indicate whether line-side unified communications or Expressway support is required.)

Note that these settings are not entirely independent. You cannot disable **SIP registration and provisioning on Unified CM** 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 on Unified CM is ignored and the Expressway-C behaves as though it was *On*.

Enabling Shared Line / Multiple Lines for MRA Endpoints

Requires Unified CM 11.5(1)SU3 or later.

If you want MRA endpoints to be able to register multiple lines, or to share lines with other endpoints, then you must enable SIP Path headers on the Expressway-C. Due to a known issue in Unified CM 11.5(1)SU2, only enable SIP Path headers if you are running Unified CM version 11.5(1)SU3 or later (CDETS [CSCvd84831](#) refers).

The default behavior is for the Expressway-C to rewrite the Contact header in REGISTER messages. When you turn SIP Path headers on, the Expressway-C does not rewrite the Contact header, but adds its address into the Path header instead.

1. On the Expressway-C, go to **Configuration > Unified Communications > Configuration**.
2. Change **SIP Path headers** to *On*.
3. Click **Save**.
The Expressway-C puts its address in the Path headers of registrations from now on, and preserves the Contact header.
4. Refresh your Unified CM servers (**Configuration > Unified Communications > Unified CM servers**, click **Refresh servers**).

Note: This feature is disabled by default, because it impacts some features on earlier versions of Unified CM.

If you are using a Unified CM version before 11.5(1)SU3, and you enable SIP Path headers on Expressway-C, the following Unified CM features will *report the MRA devices' IP addresses instead of the Expressway's IP address*:

- Device Mobility
- Real-Time Monitoring Tool (RTMT)
- Cisco Emergency Responder (CER)

Other features may also be affected by this change. The devices' IP addresses are not useful for determining their location, as they are typically from reserved private ranges and could overlap with your organization's internal range.

Unified Communications

Discover 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?](#), page 80

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

Trust 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 > Trusted CA certificate**).
3. Restart the Expressway-C (**Maintenance > Restart options**).

Discover 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.

Unified Communications

2. Add the details of a Unified CM publisher node:**a.** Click **New**.**b.** Enter the **Unified CM publisher address**.You must enter an 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.

Discover 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.

Unified Communications

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 must enter an 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.

Discover 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 must enter an 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.

Unified Communications

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 MRA Access Control

To define how clients must authenticate for Mobile and Remote Access (MRA) requests, on the Expressway-C go to **Configuration > Unified Communications > Configuration > MRA Access Control**.

Caution: If you are upgrading from X8.9 or earlier, the settings applied after the upgrade are not the same as listed here. Please refer instead to the upgrade instructions in the Expressway Release Notes.

Authorization and authentication compared

We use the concepts "authorization" and "authentication" in documentation and the user interface. At a high level, these terms can be explained using a hotel analogy:

Authentication. Equates to hotel registration by a visitor. Defines the initial check-in process to allow you access into the hotel, where you prove who you are by presenting credentials like a passport or driving license.

Authorization. Equates to a hotel key card given to a visitor. Controls the specific hotel room and other services that you are allowed to use during your stay.

The fields you actually see in the Web UI depend on whether MRA is enabled (**Unified Communications mode** set to *Mobile and remote access*) and on the selected authentication path. Not all the fields in the table are necessarily displayed.

Table 7 Settings for MRA access control

| Field | Description | Default |
|--|--|--|
| Authentication path | <p>Hidden field until MRA is enabled. Defines how MRA authentication is controlled.</p> <p><i>SAML SSO authentication:</i> Clients are authenticated by an external IdP.</p> <p><i>UCM/LDAP basic authentication:</i> Clients are authenticated locally by the Unified CM against their LDAP credentials.</p> <p><i>SAML SSO and UCM/LDAP:</i> Allows either method.</p> <p><i>None:</i> No authentication is applied. The default until MRA is first enabled. The "None" option is required (rather than just leaving MRA turned off) because some deployments must turn on MRA to allow functions which are not actually MRA. (Such as the Web Proxy for Meeting Server, or XMPP Federation.) Only these customers should use "None". It is not recommended in other cases.</p> | <p>None before MRA turned on</p> <p>UCM/LDAP after MRA turned on</p> |
| Authorize by OAuth token with refresh | <p>This option requires self-describing tokens for authorization. It's our recommended authorization option for all deployments that have the infrastructure to support them.</p> <p>Only Jabber clients are currently capable of using this authorization method. Other MRA endpoints do not currently support it. The clients must also be in OAuth token with refresh authorization mode.</p> <p>Important: From X8.10.1, the Expressway fully supports the benefits of self-describing tokens (including token refresh, fast authorization, and access policy support). However, not all of the benefits are actually available throughout the wider solution. Depending on what other products you use (Unified CM, IM and Presence Service, Cisco Unity Connection) and what versions they are on, not all products fully support all benefits of self-describing tokens.</p> | On |
| Authorize by OAuth token (previously SSO Mode) | <p>Available if Authentication path is <i>SAML SSO</i> or <i>SAML SSO and UCM/LDAP</i>.</p> <p>This option requires authentication through the IdP. Currently, only Jabber clients are capable of using this authorization method, which is not supported by other MRA endpoints.</p> | Off |
| Authorize by user credentials | <p>Available if Authentication path is <i>UCM/LDAP</i> or <i>SAML SSO and UCM/LDAP</i>.</p> <p>Clients attempting to perform authentication by user credentials are allowed through MRA. This includes Jabber, and supported IP phone and TelePresence devices.</p> | Off |

Table 7 Settings for MRA access control (continued)

| Field | Description | Default |
|--|--|---------|
| Check for internal authentication availability | <p>Available if Authorize by OAuth token with refresh or Authorize by OAuth token is enabled.</p> <p>The default is No, for optimal security and to reduce network traffic.</p> <p>Controls how the Expressway-E reacts to remote client authentication requests by selecting whether or not the Expressway-C should check the home nodes.</p> <p>The request asks whether the client may try to authenticate the user by OAuth token, and includes a user identity with which the Expressway-C can find the user's home cluster:</p> <p><i>Yes:</i> The <code>get_edge_sso</code> request will ask the user's home Unified CM if OAuth tokens are supported. The home Unified CM is determined from the identity sent by the Jabber client's <code>get_edge_sso</code> request.</p> <p><i>No:</i> If the Expressway is configured not to look internally, the same response will be sent to all clients, depending on the Edge authentication settings.</p> <p>The option to choose depends on your implementation and security policy. If all Unified CM nodes support OAuth tokens, you can reduce response time and overall network traffic by selecting <i>No</i>. Or select <i>Yes</i> if you want clients to use either mode of getting the edge configuration - during rollout or because you can't guarantee OAuth on all nodes.</p> <p>Caution: Setting this to Yes has the potential to allow rogue inbound requests from unauthenticated remote clients. If you specify No for this setting, the Expressway prevents rogue requests.</p> | No |

Table 7 Settings for MRA access control (continued)

| Field | Description | Default |
|--|--|---------|
| Identity providers: Create or modify IdPs | <p>Available if Authentication path is <i>SAML SSO</i> or <i>SAML SSO and UCM/LDAP</i>.</p> <p>Selecting an Identity Provider</p> <p>Cisco Collaboration solutions use SAML 2.0 (Security Assertion Markup Language) to enable SSO (single sign-on) for clients consuming Unified Communications services.</p> <p>If you choose SAML-based SSO for your environment, note the following:</p> <ul style="list-style-type: none"> ■ 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. <p>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:</p> <ul style="list-style-type: none"> ■ OpenAM 10.0.1 ■ Active Directory Federation Services 2.0 (AD FS 2.0) ■ PingFederate® 6.10.0.4 | – |
| Identity providers: Export SAML data | <p>Available if Authentication path is <i>SAML SSO</i> or <i>SAML SSO and UCM/LDAP</i>.</p> <p>For details about working with SAML data, see SAML SSO Authentication Over the Edge, page 91.</p> | – |

Table 7 Settings for MRA access control (continued)

| Field | Description | Default |
|---|---|-----------|
| Allow Jabber iOS clients to use embedded Safari | <p>By default the IdP or Unified CM authentication page is displayed in an embedded web browser (not the Safari browser) on iOS devices. That default browser is unable to access the iOS trust store, and so cannot use any certificates deployed to the devices.</p> <p>This setting optionally allows Jabber on iOS devices to use the native Safari browser. Because the Safari browser <i>is</i> able to access the device trust store, you can now enable password-less authentication or two-factor authentication in your OAuth deployment.</p> <p>A potential security issue exists for this option. The mechanism to return browser control from Safari to Jabber after the authentication completes, uses a custom URL scheme that invokes a custom protocol handler. It's possible that another application other than Jabber could intercept the scheme and gain control from iOS. In that case, the application would have access to the OAuth token in the URL.</p> <p>If you are confident that your iOS devices will not have other applications that register the Jabber custom URL scheme, for example because all mobile devices are managed, then it's safe to enable the option. If you are concerned about the possibility of another app intercepting the custom Jabber URL, then do not enable the embedded Safari browser.</p> | No |
| SIP token extra time to live | <p>Available if Authorize by OAuth token is <i>On</i>.</p> <p>Optionally extends the time-to-live for simple OAuth tokens (in seconds). Gives users a short window to accept calls after their credentials expire. However, it increases the potential security exposure.</p> | 0 seconds |

Refresh Unified CMs if you use self-describing tokens (Authorize by OAuth token with refresh)

If you configure authorization by self-describing tokens (**Authorize by OAuth token with refresh**) you must refresh the Unified CM nodes defined on the Expressway. This fetches keys from the Unified CM that the Expressway needs to decrypt the tokens.

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

How to check Unified CM support

You can check what authorization methods your Unified CM servers support, on the Expressway **Configuration > Unified Communications > Unified CM servers** page. This displays the version numbers in use.

About the HTTP Allow List on Expressway-C

Expressway-C automatically adds rules (inbound and outbound) to the HTTP allow list.

For example, it adds inbound rules to allow external clients to access the Unified Communications nodes discovered during MRA configuration. These include Unified CM nodes (running CallManager and TFTP service), IM and Presence Service nodes, and Cisco Unity Connection nodes.

Inbound rules are viewable at **Configuration > Unified Communications > HTTP allow list > Automatic inbound rules**. Outbound rules are viewable at **Configuration > Unified Communications > HTTP allow list > Automatic outbound rules**.

Can I edit the allow list?

- You can't add outbound rules to the list.
- You can add your own inbound rules, if clients from outside need to access other web services inside the enterprise. For example, these services may require you to configure the allow list.
 - Jabber Update Server
 - Cisco Extension Mobility
 - Directory Photo Host
 - Advanced File Transfer (AFT)
 - Problem Report Tool server
- You can't edit or delete auto-added rules in the list.

AFT feature

For the AFT feature to work across Expressway, make sure that *all* Unified CM IM and Presence Service nodes are on the allow list, whether manually or automatically added.

Automatic Inbound Rules

Expressway automatically edits the HTTP allow list when you discover or refresh Unified Communications nodes. This page shows the discovered nodes, and the rules that apply to those nodes.

The first list is Discovered nodes, and contains all the nodes currently known to this Expressway-C. For each node, the list contains the node's address, its type, and the address of its publisher.

The second list is the rules that have been added for you, to control client access to the different types of Unified Communications nodes. For each type of node in your MRA configuration, you'll see one or more rules in this list. They are shown in the same format as the editable rules, but you cannot modify these rules.

Table 8 Properties of Automatically Added Allow List Rules

| Column | Description |
|-----------------|---|
| Type | This rule affects all nodes of the listed type: <ul style="list-style-type: none"> ■ Unified CM servers: Cisco Unified Communications Manager nodes ■ IM and Presence Service nodes: Cisco Unified Communications Manager IM and Presence Service nodes ■ Unity Connection servers: Cisco Unity Connection nodes ■ TFTP: TFTP nodes |
| Protocol | The protocol on which the rule allows clients to communicate with these types of nodes. |

Table 8 Properties of Automatically Added Allow List Rules (continued)

| Column | Description |
|-------------------|--|
| Ports | The ports on which the rule allows clients to communicate with these types of nodes. |
| Match type | <i>Exact</i> or <i>Prefix</i> . Depends on the nature of the service the clients access with the help of this rule. |
| Path | The path to the resource that clients access with the help of this rule. This may not be present, or may only be a partial match of the actual resource, if the rule allows <i>Prefix</i> match. |
| Methods | The HTTP methods that will be allowed through by this rule (such as <code>GET</code>). |

Edit the HTTP Allow List

1. Go to **Configuration > Unified Communications > HTTP allow list > Editable inbound rules** to view, create, modify, or delete HTTP allow list rules.

The page has two areas; one for controlling the default HTTP methods, and the other showing the editable rules.

2. [Optional] Use the checkboxes to modify the set of default HTTP methods, then click **Save**.

You can override the defaults while you're editing individual rules. If you want to be as secure as possible, clear all methods from the default set and specify methods on a per rule basis.

Note: When you change the default methods, all rules that you previously created with the default methods will use the new defaults.

3. [Recommended] Delete any rules you don't need by checking the boxes in the left column, then clicking **Delete**.
4. Click **New** to create a rule.

5. Configure the rule to your requirements. Here is some advice for each of the fields:

Table 9 Properties of Manually Added Allow List Rules

| Column | Description |
|------------------------|--|
| Description | Enter a meaningful description for this rule, to help you recognize its purpose. |
| Url | Specify a URL that MRA clients are allowed to access. For example, to allow access to <code>https://www.example.com:8080/resource/path</code> just type it in exactly like that. <ol style="list-style-type: none"> a. The protocol the clients are using to access the host must be <code>http://</code> or <code>https://</code> b. Specify a port when using a non-default port eg. <code>:8080</code> (Default ports are 80 (http) and 443 (https)) c. Specify the path to limit the rule scope (more secure), eg. <code>/resource/path</code> If you select <i>Prefix match</i> for this rule, you can use a partial path or omit the path. Be aware that this could be a security risk if the target resources are not resilient to malformed URLs. |
| Allowed methods | Select <i>Use defaults</i> or <i>Choose methods</i> . If you choose specific HTTP methods for this rule, they will override the defaults you chose for all rules. |
| Match type | Select <i>Exact match</i> or <i>Prefix match</i> . Your decision here depends on your environment. It is more secure to use exact matches, but you may need more rules. It is more convenient to use prefix matches, but there is some risk of unintentionally exposing server resources. |
| Deployment | If you are using multiple deployments for your MRA environment, you also need to choose which deployment uses the new rule. You won't see this field unless you have more than one deployment. |

6. Click **Create Entry** to save the rule and return to the editable allow list.
7. [Optional] Click **View/Edit** to change the rule.

Upload Rules to the HTTP Allow List

Note: You cannot upload outbound rules.

1. Go to **Configuration > Unified Communications > HTTP allow list > Upload rules**.
2. Browse to and select the CSV file containing your rule definitions.
See [Allow List Rules File Reference, page 382](#).
3. Click **Upload**.

The Expressway responds with a success message and displays the **Editable inbound rules** page.

Automatic Outbound Rules

The Expressway has a built-in forward proxy service, providing it is supported by your Unified CM software.

Predefined outbound rules in the HTTP allow list permit Push Notifications through the forward proxy to the Collaboration Cloud servers. The Expressway automatically adds the outbound rules if you enable the forward proxy.

You can see these rules on **Configuration > Unified Communications > HTTP allow list > Automatic outbound rules**. The rules can't be edited or deleted. They contain the following entries for each Unified CM node discovered by the Expressway:

Table 10 Properties of Automatic Outbound Rules if Expressway Forward Proxy Enabled

| Column | Description |
|--------------------|---|
| Target host | The Cisco Collaboration cloud URL (WebEx, etc). |
| Protocol | The required protocol for proxy traffic. Always HTTPS in this case. |
| Ports | The port allowed by proxy for the target host. |
| Path | The path to the service for client requests. |
| Methods | The HTTPS methods to allow through. |

When are automatic outbound rules used?

These outbound rules apply if you enable the built-in forward proxy service in the Expressway. For example, to support Apple's Push Notification service if you have Cisco Jabber users with iOS devices (Cisco Jabber for iPhone and iPad) who sign in remotely.

Using Deployments to Partition Unified Communications Services

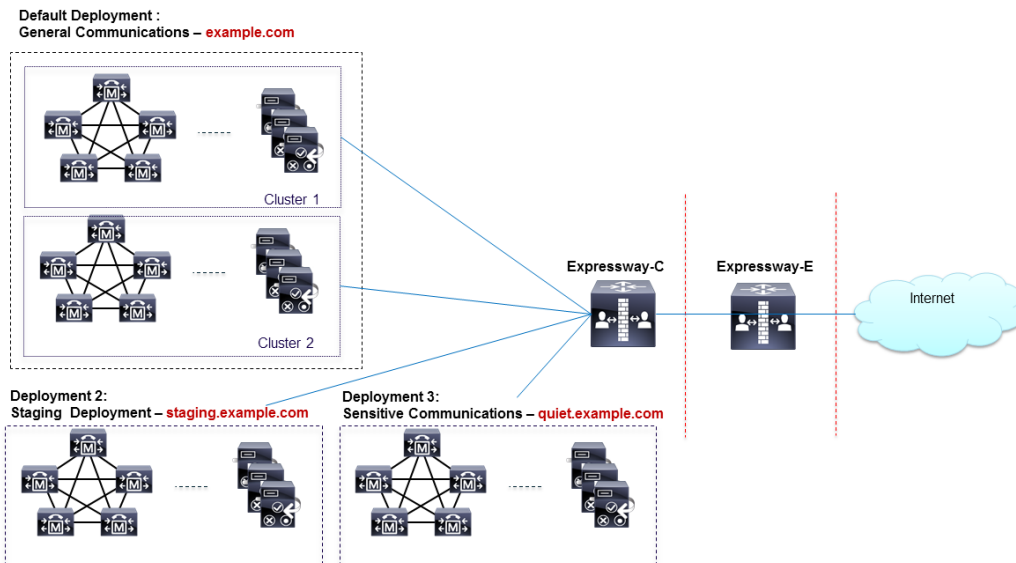
A deployment is an abstract boundary used to enclose a domain and one or more Unified Communications service providers (such as Unified CM, Cisco Unity Connection, and IM and Presence Service nodes). The purpose of multiple deployments is to partition the Unified Communications services available to Mobile and Remote Access (MRA) users. So different subsets of MRA users can access different sets of services over the same Expressway pair.

We recommend that you do not exceed ten deployments.

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, as a third set.

Figure 8 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 through Mobile and Remote Access, create as many deployments as you need. Associate a different domain with each one, 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**.

Unified Communications

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, page 126](#)).
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 [Discover Unified Communications Servers and Services, page 77](#).

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.

SAML SSO Authentication Over the Edge

SAML-based SSO is an option for authenticating Unified Communications service requests. The requests can originate inside the enterprise network, or, as described here, from clients requesting Unified Communications services from outside through MRA.

SAML SSO authentication over the edge requires an external identity provider (IdP). It relies on the secure traversal capabilities of the Expressway pair at the edge, and on trust relationships between the internal service providers and an externally resolvable 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.

The Expressway supports two types of OAuth token authorization with SAML SSO:

- Simple (standard) tokens. These always require SAML SSO authentication.
- Self-describing tokens with refresh. These can also work with Unified CM-based authentication.

About Simple OAuth Token Authorization

Prerequisites

- Cisco Jabber 10.6 or later. Jabber clients are the *only* endpoints supported for OAuth token authorization through Mobile and Remote Access (MRA).
- 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

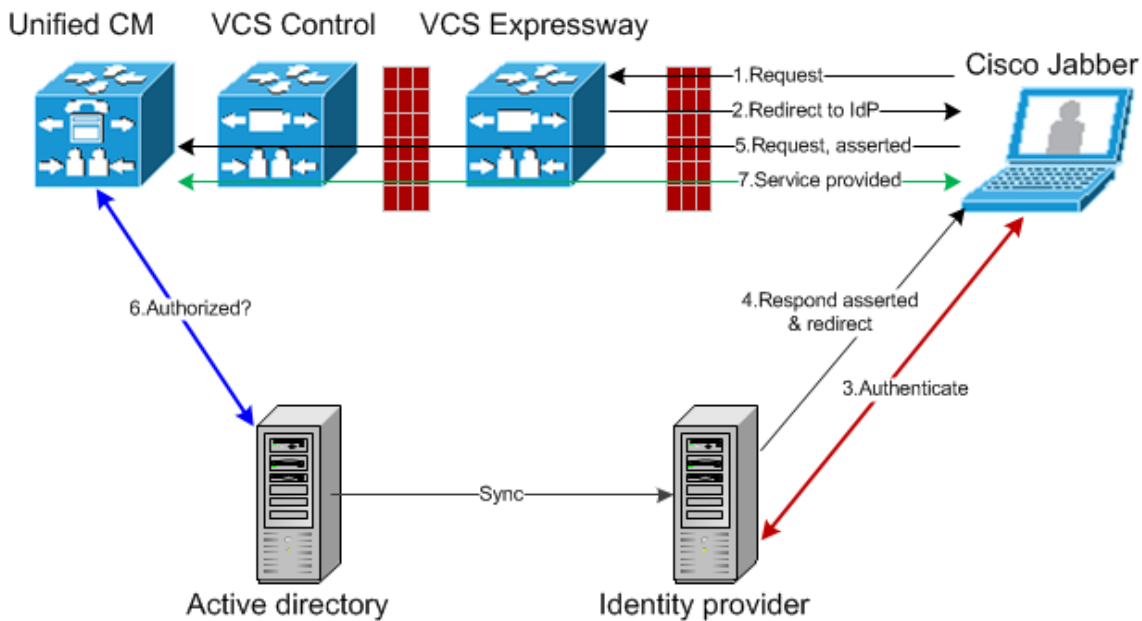
How it works

Cisco Jabber determines whether it is inside the organization's network before requesting a Unified Communications service. If Jabber is outside the network, it requests the service from the Expressway-E on the edge of the network. If SAML SSO authentication 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 9 Simple OAuth token-based authorization for on-premises UC services



About Self-Describing OAuth Token Authorization with Refresh

We introduced this feature in X8.10 in **preview status only**. It's fully supported from **X8.10.1**.

Expressway supports using self-describing tokens as an MRA authorization option. (Set "**Authorize by OAuth token with refresh**" to Yes.) Self-describing tokens offer significant benefits:

- Token refresh capability, so users don't have to repeatedly re-authenticate.
- Fast authorization.
- Access policy support. The Expressway can enforce MRA access policy settings applied to users on the Unified CM.
- Roaming support. Tokens are valid on-premises and remotely, so roaming users don't need to re-authenticate if they move between on-premises and off-premises.

The Expressway uses self-describing tokens in particular to facilitate Cisco Jabber users. Jabber users who are mobile or work remotely, can authenticate while away from the local network (off-premises). If they originally authenticate on the premises, they don't have to re-authenticate if they later move off-premises. Similarly, users don't have to re-authenticate if they move on-premises after authenticating off-premises. Either case is subject to any configured access token or refresh token limits, which may force re-authentication.

For users with Jabber iOS devices, the high speeds supported by self-describing tokens optimize Expressway support for Apple Push Notifications (APNs).

We recommend self-describing token authorization for all deployments, assuming the necessary infrastructure exists to support it. Subject to proper Expressway configuration, if the Jabber client presents a self-describing token then the Expressway simply checks the token. No password or certificate-based authentication is needed. The token is issued by Unified CM (regardless of whether the configured authentication path is by external IdP or by the Unified CM). Self-describing token authorization is used automatically if all devices in the call flow are configured for it.

The Expressway-C performs token authorization. This avoids authentication and authorization settings being exposed on Expressway-E.

Prerequisites

- Expressway is already providing Mobile and Remote Access for Jabber for iPhone and iPad.
- All other devices in the call flow are similarly enabled.
- You have the following product versions installed (or later):
 - Expressway X8.10
 - Cisco Jabber for iPhone and iPad iOS 11.9
 - Cisco Unified Communications Manager 11.5(SU3)
 - Cisco Unified Communications Manager IM and Presence Service 11.5(SU3)
 - Cisco Unity Connection 11.5(SU3)
- Do not enable OAuth tokens until all of the other system components are known to also support it.

If you configure authorization by self-describing tokens (**Authorize by OAuth token with refresh**) you must refresh the Unified CM nodes defined on the Expressway. This fetches keys from the Unified CM that the Expressway needs to decrypt the tokens.

Limitations

Important: From X8.10.1, the Expressway fully supports the benefits of self-describing tokens (including token refresh, fast authorization, and access policy support). However, not all of the benefits are actually available throughout the wider solution. Depending on what other products you use (Unified CM, IM and Presence Service, Cisco Unity Connection) and what versions they are on, not all products fully support all benefits of self-describing tokens.

OAuth Token Authorization 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 OAuth is configured on the Expressway-C.
- The Expressway-C has MRA enabled and has discovered the required Unified CM resources.
- The required Unified CM resources are in the HTTP allow list on the Expressway-C.
- If you are using multiple deployments, the Unified CM resources that will be accessed by OAuth 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 Unified CM:

- Users who are associated with non-OAuth MRA clients or endpoints, have their credentials stored in Unified CM. Or Unified CM is configured for LDAP authentication.

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

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

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

Unified Communications

- 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. If you intend to use self-describing token authorization (**Authorize by OAuth token with refresh**) we recommend getting it working on-premises first, before attempting to enable it for MRA clients.
2. 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 11.x Solution Reference Network Designs \(SRND\)](#) document.
3. 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*.
4. 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.
5. 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*.
6. Create the Identity Provider on the Expressway-C, by importing the SAML metadata file from the IdP.
7. Associate the IdP with SIP domain(s) on the Expressway-C.
8. Export the SAML metadata file(s) from the (primary) Expressway-C; ensure that it includes the externally resolvable address of the (primary) 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).
9. 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*.
10. Similarly, import the SAML metadata file from the Expressway-C to the IdP. See your IdP documentation for details.
11. Turn on SAML SSO at the edge, on the Expressway-C. See [Configuring MRA Access Control, page 80](#)

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 primary 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.

Unified Communications

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. If you have multiple deployments configured, 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 OAuth token-based authorization 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.

You also need to add a claim rule, for each relying party trust, that sets the uid attribute of the SAML response to the AD attribute value that users are authenticating with.

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)
- Add a claim rule to send identity as uid attribute

To sign the whole response:

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

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

To add a claim rule for each Relying Party Trust:

1. Open the Edit Claims Rule dialog, and create a new claim rule that sends AD attributes as claims
2. Select the AD attribute to match the one that identify the OAuth users to the internal systems, typically email or SAMAccountName
3. Enter uid as the Outgoing Claim Type

Enabling Support for Apple Push Notifications

We introduced this feature in X8.10 **in preview status only**. It's fully supported from **X8.10.1**.

This feature applies if you have Cisco Jabber users with iOS devices (Cisco Jabber for iPhone and iPad) who sign in remotely. Expressway deployments that are configured for MRA can support Apple's cloud-based Push Notification service. From X8.9.1, we supported Push Notifications for IM and Presence Service instant messages. From X8.10, we support them for voice and video calls too. Push Notifications are only used for Jabber for iPhone and iPad clients. Android, Windows, and Mac users are unaffected.

Note: If Unified CM detects a remote or mobile Jabber for iPhone and iPad connection, it always sends a Push Notification as well as a SIP Invite.

Prerequisites and recommendations

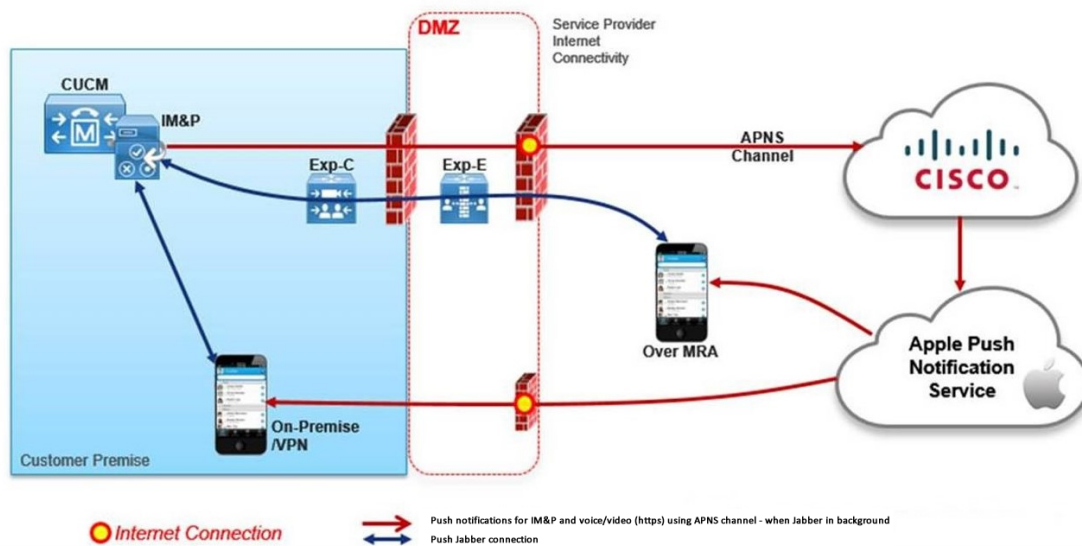
No specific configuration is needed on the Expressway for Push Notifications, assuming Expressway-E is already providing Mobile and Remote Access (MRA) for Jabber iOS devices. However, these prerequisites and recommendations apply:

- Push Notifications in the Expressway require a network connection between Expressway and the Cisco WebEx cloud, and between Cisco Jabber and the Push Notification servers in the Apple cloud. **They cannot work in a private network, with no internet connection.**
- Expressway is already providing Mobile and Remote Access for Jabber for iPhone and iPad. MRA must be fully configured (domain, zone, server settings).
- Depending on your Unified CM configuration, the Unified CM may need a forward proxy to send Push Notifications to the Cisco Collaboration Cloud.
- We recommend using self-describing token authorization.
- Expressway-E **restart required for Push Notifications with instant messages**. After you enable Push Notifications on the IM and Presence Service you need to restart the Expressway-E. Until the restart, Expressway-E can't recognize the push capability on IM and Presence Service, and does not send PUSH messages to the Jabber clients.
- You need the following Push Notification-enabled releases (or higher) on Cisco Unified Communications Manager, IM and Presence Service, and the Jabber devices:
 - – Expressway X8.10
 - – Cisco Jabber for iPhone and iPad iOS 11.9
 - – Cisco Unified Communications Manager 11.5(SU3)
 - – Cisco Unified Communications Manager IM and Presence Service 11.5(SU3)
 - – Cisco Unity Connection 11.5(SU3)

Why have we implemented support for Push Notifications?

Apple now deprecates the VoIP Background Mode that allows Jabber iOS to keep a SIP session open even when the app is running in the background. Push Notifications allow Unified CM to tell Jabber about incoming calls and messages. Then Jabber can reconnect to Unified CM to retrieve the message or answer the call. Jabber uses the new self-describing token feature in this release to help it to do this quickly.

Figure 10 Push Notifications architecture



Information about Push Notifications in Unified Communications products

For information about Push Notifications in Unified CM and IM and Presence Service, see *Deploying Push Notifications for Cisco Jabber on iPhone and iPad* available from the [Cisco Unified Communications Manager documentation pages](#) on Cisco.com.

Prerequisites

- Expressway is already providing Mobile and Remote Access for Jabber for iPhone and iPad.
- A forward proxy service is configured on the Expressway (if it is supported by your Unified CM software) or on the Unified CM using a 3rd party proxy.
- You have the following product versions installed (or later):
 - Expressway X8.10
 - Cisco Jabber for iPhone and iPad iOS 11.9
 - Cisco Unified Communications Manager 11.5(SU3)
 - Cisco Unified Communications Manager IM and Presence Service 11.5(SU3)
 - Cisco Unity Connection 11.5(SU3)

Process to use APNs

1. Configure OAuth token validation on the Expressway. See [Configuring MRA Access Control, page 80](#).
2. Unified CM must be able to make HTTPS connections to Cisco's cloud services. To allow that you may have to configure Unified CM to use a forward proxy server (depending on your requirements for external requests from iOS devices). If required, the forward proxy can be a third party server or, **if supported by your Unified CM software**, the built-in forward proxy service on the Expressway.

To enable the Expressway forward proxy (only if the Unified CM supports it):

- a. On the Expressway-C, go to **Configuration > Unified Communications > Forward proxy**.
- b. Locate **Forward proxy enabled** and select *On*.
- c. Do the same for the Expressway-E.

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 (for small/medium systems on X8.1 or later) | UDP | 36000 to 59999* | 36000 (RTP), 36001 (RTCP) (defaults) |
| Traversal zone SIP media (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 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 36012 to 59999* |

| Purpose | Protocol | Internet endpoint (source) | Expressway-E (listening) |
|---|----------|----------------------------|--------------------------|
| SIP signaling | TLS | >= 1024 | 5061 |
| HTTPS (only required for external administrative access, which is strongly discouraged) | TCP | >= 1024 | 443 |

From Expressway-C to Internal Infrastructure and Endpoints

| Purpose | Protocol | Expressway-C (source) | Internal Device Port/Range |
|---|----------|-----------------------|--|
| 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/HTTPS (configuration file retrieval) | TCP | Ephemeral port | (Unified CM) HTTP 6970 Or HTTPS 6972 if you have Cisco Jabber 11.x or later with Unified CM 11.x or later |
| 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 (Media recipient eg. endpoint) |
| SIP signaling | TCP | 25000 to 29999 | 5060 (Unified CM) |
| Secure SIP signaling | TLS | 25000 to 29999 | 5061 (Unified CM) |

* The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at **Configuration > Local Zones > 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:** Changes to the **Use configured demultiplexing ports** setting need a system restart to take effect.

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)

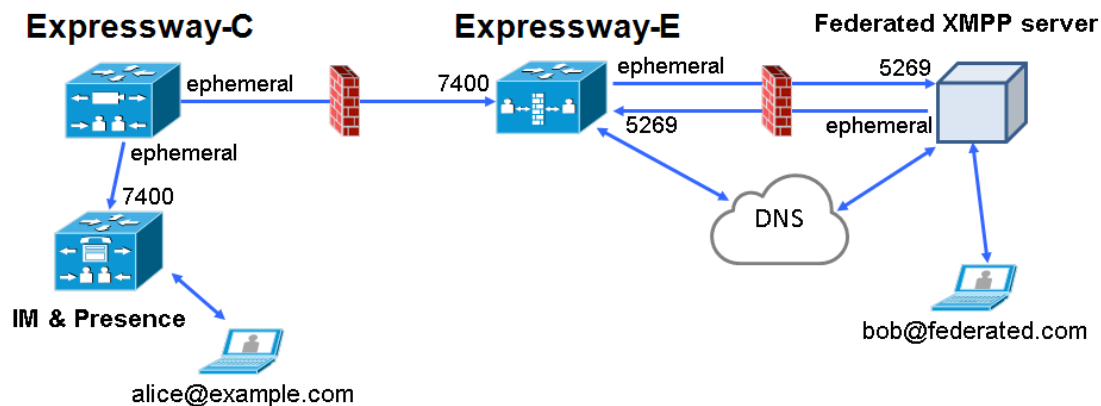
External XMPP Federation

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.



Please note the following:

- SIP and XMPP federations are separate and do not impact on each other. For example, it is possible to deploy SIP federation on `[[[Undefined variable call_control.IM&PLong]]]` and external XMPP federation on Expressway.
- If you deploy external XMPP federation through Expressway, do not activate the Cisco XCP XMPP federation Connection Manager feature service on `[[[Undefined variable call_control.IM&PLong]]]`.

See *Cisco Unified Communications XMPP Federation using IM and Presence Service or Expressway* on the [Expressway configuration guides page](#).

Supported Systems

- Expressway-E supports XMPP federation with:
 - Expressway X8.2 or later.
 - Cisco Unified Communications Manager `[[[Undefined variable call_control.IM&PLong]]]` 9.1.1 or later.
 - Cisco Jabber 9.7 or later.
 - Cisco Webex Connect Release 6.x.
 - Other XMPP standards-compliant servers.

Prerequisites

Before configuring your Expressway system for external XMPP federation:

- Ensure that you are running the following software versions:
 - Expressway X8.2 or later.
 - Unified CM 9.1.1 or later.

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

- Ensure that Interdomain XMPP federation has been **disabled** on Unified CM:
Go to **Cisco Unified CM Administration > Presence > Inter Domain Federation > XMPP Federation > Settings** and ensure that **XMPP Federation Node Status** is set to *Off*.
- When using Expressway for XMPP federation, the Expressway-E handles the connection to the remote federation server and can only use Jabber IDs to manage XMPP messages. Expressway-E does not support XMPP address translation (of email addresses, for example).

If you, as an external user, attempt to chat with a user in an enterprise through federation, you must use the enterprise user's Jabber ID to contact them through XMPP. If the enterprise user's Jabber ID does not match their email address, especially if their Jabber ID uses an internal user ID or domain, you will be unable to have federation, as you will not know the enterprise user's email address. For this reason, we recommend that enterprises configure their Unified CM nodes to use the same address for a user's Jabber ID and email when using Expressway for XMPP federation.

Note: This limitation does not apply to users contacting each other within the enterprise (not using federation) even when federation is handled by Expressway-E. You can configure Unified CM to use either the Jabber ID or the Directory URI (typically email) for such non-federated use cases.

You can make a user's Jabber ID resemble a user's email address, so that the federated partner can approximate email addresses for federation, by:

- Setting the Unified CM Lightweight Directory Access Protocol (LDAP) attribute for User ID to be the user's sAMAccountName
 - Setting the Unified CM presence domain to be the same as the email domain.
 - Setting your email address so that it is the same as samaccountname@presencedomain.
- Simultaneous internal federation managed by Unified CM and external federation managed by Expressway is not supported. If only internal federation is required then you must use interdomain federation on Unified CM. The available federation deployment configuration options are:
 - External federation only (managed by Expressway).
 - Internal federation only (managed by Cisco Unified CM).
 - Internal and external federation managed by Cisco Unified CM, but requires you to configure your firewall to allow inbound connections.

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

- If you intend to use both Transport Layer Security (TLS) and group chat, the Expressway-C and Expressway-E server certificates must include in their list of subject alternate names the **Chat Node Aliases** that are configured on the Unified CM servers. Use either the XMPPAddress or DNS formats. Note that the Expressway-C automatically includes the chat node aliases in its certificate signing requests (CSRs), providing it has discovered a set of Unified CM 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, page 64](#) for more information.

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

- [Configuring Expressway for External XMPP Federation, page 103](#)
- [DNS SRV Records for XMPP Federation, page 107](#)
- [Port Usage for XMPP Federation, page 108](#)
- [Checking XMPP Federation Status, page 109](#)
- [Troubleshooting External XMPP Federation, page 109](#)

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. This document assumes X8.10.3
- Unified CM IM & Presence 10.x 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, page 64](#) 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*.

Unified Communications

5. Click **Save**.
6. Repeat for any other local domains requiring federation.

Note:

- A single Expressway cluster can support multiple IM and Presence Service clusters using the same presence domain.
- XMPP federation of multiple IM and Presence Service clusters with multiple Expressway clusters is not supported.
- Each IM and Presence Service cluster needs to be discovered by Expressway-C.

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](#), page 111 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 do not require a restart.

3. Configure the remaining fields as described in the table below.

Unified Communications You are here: [Configuration](#) > [Unified Communications](#) > Configuration

Configuration

Unified Communications mode: Mobile and remote access ⓘ

Single Sign-On

Single Sign-On support: On ⓘ

When clients ask if they can try SSO: Query users' home nodes to check SSO support before responding ⓘ

XMPP federation

XMPP federation support: On ⓘ

Use static routes: Off ⓘ [Configure static routes for federated XMPP domains](#)

Dialback secret: *..... ⓘ

Security mode: TLS required ⓘ

Require client-side security certificates: On ⓘ

Privacy mode: Allow List ⓘ [Configure federation allow list](#)

Save

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.

Table 11 Settings for XMPP Federation

| | |
|--|---|
| Use static routes | 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 Configuring How XMPP Servers for Federated Domains and Chat Node Aliases Are Located , page 106 below. |
| Dialback secret | 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. For more information about server dialback, see http://xmpp.org/extensions/xep-0220.html . |
| Security mode | Indicates if a TLS connection to federated XMPP servers is required, preferred or not required. <i>TLS required:</i> the system guarantees a secure (encrypted) connection with the foreign domain. <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. <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. 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. The default, and recommended setting, is <i>TLS required</i> . |
| Require client-side security certificates | 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. This setting does not apply if Security mode is <i>No TLS</i> . 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. |

Table 11 Settings for XMPP Federation (continued)

| | |
|---------------------|--|
| Privacy mode | <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 Configuring the Allow and Deny Lists for Federated Domains and Chat Node Aliases, page 107 below.</p> |
|---------------------|--|

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: All XMPP federated partners must publish in DNS the addresses of their XMPP servers as described in [DNS SRV Records for XMPP Federation](#), page 107.

To use static routes:

1. 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:

| | |
|----------------|--|
| Domain | The federated XMPP domain or chat node alias. |
| Address | 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:

- 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:

Unified Communications

| 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.
- If you are using group chat over TLS, ensure that the Expressway-C and Expressway-E server certificate 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 Service 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**).

Unified Communications

- 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.
- If the address of an IM and Presence Service node has changed, or a new peer has been added to an IM and Presence Service cluster, go to **Configuration > Unified Communications > IM and Presence Service** nodes and click **Refresh Servers**. You must then save the updated configuration.

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, page 64](#) 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 choose whether to enable Interdomain XMPP Federation on IM and Presence Service or on Expressway.

To disable Interdomain Federation on IM and Presence Service, 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.

Unified Communications

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.

Temporary or Partial Loss of IM and Presence Service Federation

XMPP federation for IM and Presence Service via Expressway relies on a persistent TCP connection to the federated server. If a federated server becomes unavailable due to a graceful shutdown, Expressway will immediately seek to reestablish a connection with the federated server or with another server advertised by the federated partner.

If, however, the federated server fails abruptly, it can take up to 15 minutes for Expressway to discover the TCP connection outage and attempt reconnection. During this time, a partial or full loss of IM and Presence Service connectivity with the federated partner may occur.

Delayed Cisco XCP Router Restart

Part of Cisco Hosted Collaboration Solution (HCS), the delayed Cisco XCP Router restart feature is only available when the Expressway-E is in multitenant mode.

The Expressway-E enters multitenant mode when you add a second Unified CM traversal zone with a new SIP domain. See [Expressway Multitenancy Overview](#), page 384.

Note: In multitenant mode, you must configure the system hostname on the **System > DNS** page of the Cisco Expressway-E to match the hostname configured in DNS (case-specific before X8.10.1, case insensitive from X8.10.1). Otherwise Cisco Jabber clients will be unable to register successfully for MRA.

Multitenancy allows a service provider to share an Expressway-E cluster among multiple tenants. Each tenant has a dedicated Expressway-C cluster that connects to the shared Expressway-E cluster.

Certain configuration changes on the Expressway-E cluster, or a customer's Expressway-C cluster, require a restart of the Cisco XCP Router on each Expressway-E in the shared cluster.

The restart is required for Cisco XCP Router configuration changes to take effect across all nodes in a multitenant Expressway-E cluster. The restart affects all users across all customers.

To reduce the frequency of this restart, and the impact it has on users, you can use the delayed Cisco XCP Router restart feature.

Note: Without the delayed restart feature enabled, the restart happens automatically and occurs each time you save any configuration change that affects the Cisco XCP Router. If multiple configuration changes are required, resulting in several restarts of the Cisco XCP Router, it can adversely affect users. We strongly recommend that multitenant customers enable the delayed Cisco XCP Router restart feature.

See *Multitenancy with Cisco Expressway* on the [Cisco Hosted Collaboration Solution](#) page.

The delayed restart feature lets you control when the restart takes place. You can make a batch of configuration changes – followed by a single Cisco XCP Router restart – and apply all the changes at once.

A delayed restart generates the latest configuration and performs a Cisco XCP Router restart on each node in the multitenant Cisco Expressway-E cluster.

When a restart of the Cisco XCP Router occurs, all XMPP clients (such as Cisco Jabber) across all customers go offline for a few minutes and then reconnect. Because of this impact, Cisco recommends that you take advantage of the delayed restart capability.

Once enabled, you can carry out the restart manually or set it to be schedule-based. In either mode, you can initiate the restart at any time and the system determines which Cisco XCP Router instances require a restart, performing the restart only as needed.

When you set the restart to be scheduled, the restart happens at the scheduled time, but again only as needed. Cisco recommends performing the Cisco XCP Router restart during off-peak hours whenever possible.

Note:

- Nodes on the latest configuration are not impacted. This action disconnects all external XCP-based users connected through the delayed nodes during the restart.
- All nodes will be on the latest configuration after the restart.

To configure the delayed Cisco XCP Router restart:

1. Go to **Configuration > Unified Communications > Delayed Cisco XCP Router restart**.
2. Under **Configuration**, turn **Delayed Cisco XCP Router restart** *On*.
3. If you do not enable **Scheduled Restart**, initiate the restart manually using the **Restart** button as configuration changes do not happen automatically.

To schedule the restart:

1. Under **Configuration**, turn **Scheduled Restart** *On* and set the time that all nodes in the multi-tenant Expressway-E cluster are updated each day. Only nodes that are not running on the latest configuration are impacted.
2. Set the time that the restart takes place each day using the **Scheduled restart time (UTC)** option.

Configuration Changes That Require a Restart of the Cisco XCP Router

If you make any system configuration changes in the following areas a restart of the Cisco XCP Router takes place:

- XMPP federation
- Internal/external Ethernet
- Hostname or IP address
- DNS
- NTP
- Option keys
- QoS
- Clustering
- Zones
- MRA
- Domains
- Maintenance mode
- Cisco XCP Router delayed restart
- Cisco XCP Router / XMPP changes through networking
- Server-to-server communication to IM and Presence Service
- Changes to the logging flags for any of the above

Refer to the *Impact of Configuration Changes on a Live System* section of the [Cisco Unified Communications XMPP Federation](#) guide.

See *Multitenancy with Cisco Expressway* on the [Cisco Hosted Collaboration Solution](#) page.

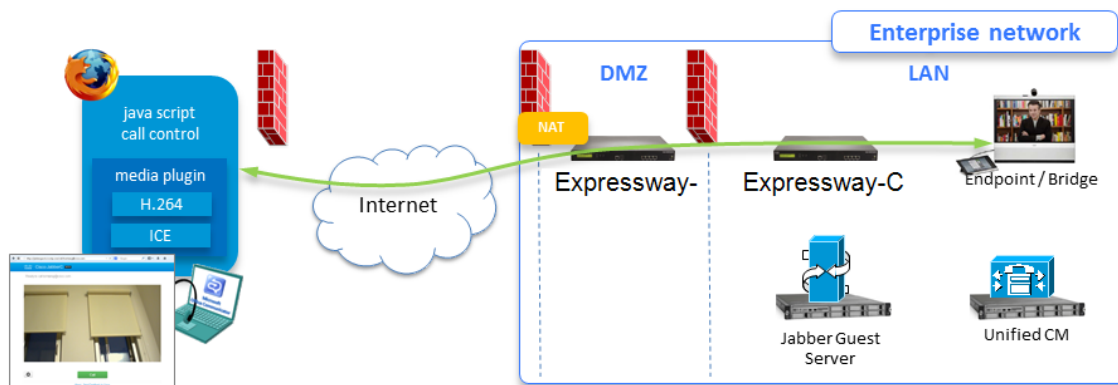
Jabber Guest Services Overview

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) an 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).

Figure 11 Jabber Guest Components



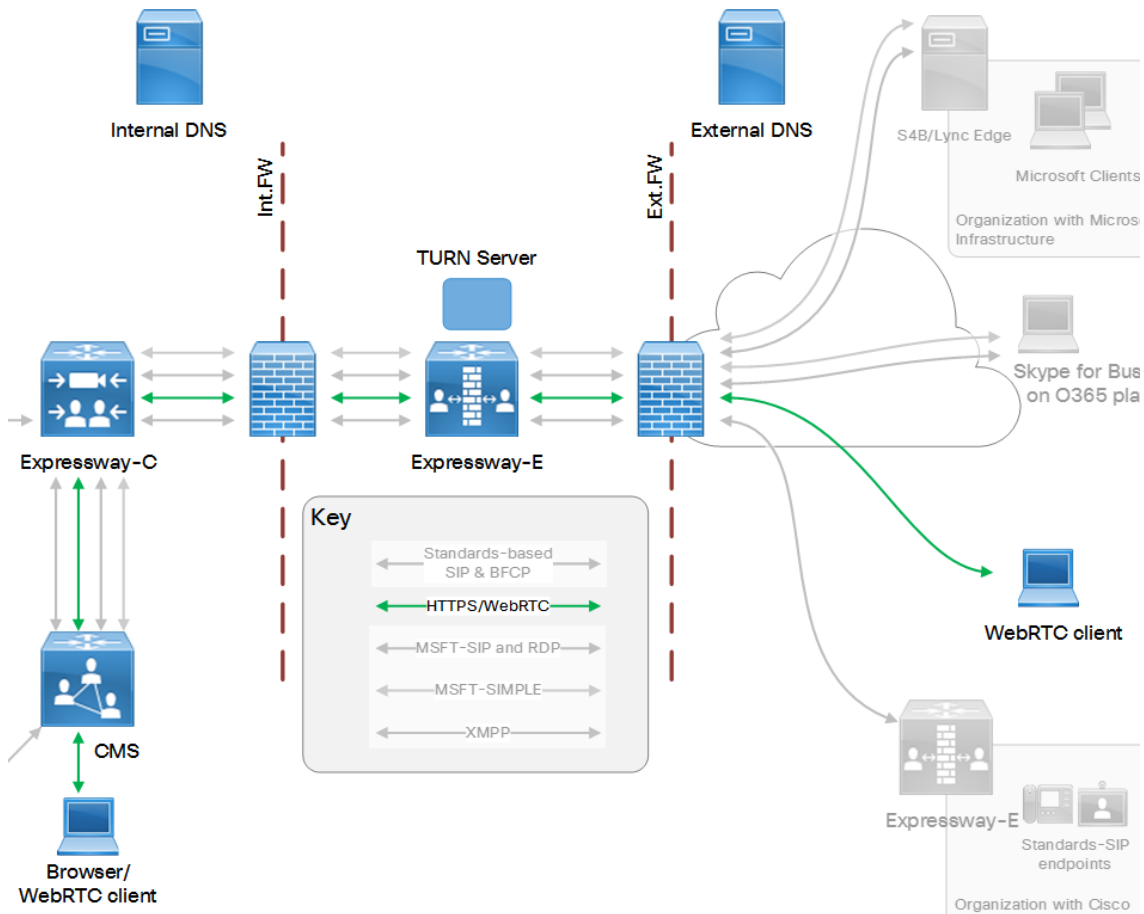
Information Scope

In versions X8.7 and earlier, all Expressway configuration required for deployment with Jabber Guest was contained in the Administrator Guide. From X8.8 onwards, that information is kept in a separate deployment guide. You can read more detailed information about Jabber Guest in the following documents:

- *Cisco Expressway with Jabber Guest Deployment Guide*, at the [Expressway Configuration Guides page](#).
- *Cisco Jabber Guest Server Installation and Configuration Guide*, for your version, at the [Jabber Guest Installation and Upgrade Guides page](#).
- *Cisco Jabber Guest Administration Guide*, for your version, at the [Jabber Guest Maintain and Operate Guides page](#).
- *Cisco Jabber Guest Release Notes*, for your version, at the [Jabber Guest Release Notes page](#).

Meeting Server Web Proxy on Expressway

This option enables external users to join or administer Meeting Server spaces using their browser. All the external user needs is the URL to the space and their credentials for accessing the Meeting Server.



Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure on the [Expressway configuration guides page](#).



Protocols

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

Note: The SIP and H.323 protocols are disabled by default on new installs of X8.9.2 or later versions. You must enable them on the **Configuration > Protocols** menu.

| | |
|--|-----|
| About H.323 | 117 |
| Configuring H.323 | 118 |
| About SIP | 119 |
| Configuring SIP | 121 |
| Configuring Domains | 126 |
| Configuring SIP and H.323 Interworking | 127 |

About H.323

The Expressway supports the H.323 protocol. It's an H.323 gatekeeper.

The Expressway can also provide [interworking](#) between H.323 and SIP. It translates between the two protocols to enable endpoints that only support one of these protocols to call each other. To support H.323, the **H.323 mode** must be enabled.

Using the Expressway as an H.323 Gatekeeper

As an H.323 gatekeeper, the Expressway accepts registrations from H.323 endpoints and provides call control functions such as address translation and admission control.

To enable the Expressway as an H.323 gatekeeper, ensure that **H.323 mode** is set to *On* (**Configuration > Protocols > H.323**).

H.323 Endpoint Registration

H.323 endpoints in your network must register with the Expressway in order to use it as their gatekeeper.

There are two ways an H.323 endpoint can locate an Expressway with which to register: manually or automatically. The option is configured on the endpoint itself under the Gatekeeper Discovery setting (consult your endpoint manual for how to access this setting).

- If the mode is set to automatic, the endpoint will try to register with any Expressway it can find. It does this by sending out a Gatekeeper Discovery Request, to which eligible Expressways will respond.
- If the mode is set to manual, you must specify the IP address of the Expressway with which you want your endpoint to register, and the endpoint will attempt to register with that Expressway only.

Preventing Automatic H.323 Registrations

You can prevent H.323 endpoints being able to register automatically with the Expressway by disabling **Auto Discovery** on the Expressway (**Configuration > Protocols > H.323**).

Protocols

Registration Refresh

The H.323 Time to live setting controls the frequency of H.323 endpoint registration refresh. The refresh frequency increases when the time to live is decreased. When you have many H.323 endpoints, be careful not to set the TTL too low, because a flood of registration requests will unnecessarily impact the Expressway performance.

Configuring H.323

Go to **Configuration > Protocols > H.323** to configure the [H.323](#) settings on the Expressway.

The configurable options are:

| Field | Description | Usage tips |
|--|--|---|
| H.323 mode | Enables or disables H.323 on the Expressway. H.323 support is <i>Off</i> by default. | You must enable H.323 mode if you are clustering the Expressway, even if there are no H.323 endpoints in your deployment. |
| Registration UDP port | The listening port for H.323 UDP registrations. Default is 1719. | The default Expressway configuration uses standard port numbers so you can use H.323 services out of the box without having to first set these up. |
| Registration conflict mode | Determines how the system behaves if an endpoint attempts to register an alias currently registered from another IP address. <i>Reject</i> : denies the new registration. This is the default. <i>Overwrite</i> : deletes the original registration and replaces it with the new registration. | An H.323 endpoint may attempt to register with the Expressway using an alias that has already been registered on the Expressway from another IP address. The reasons for this could include: <ul style="list-style-type: none"> Two endpoints at different IP addresses are attempting to register using the same alias. A single endpoint has previously registered using a particular alias. The IP address allocated to the endpoint then changes, and the endpoint attempts to re-register using the same alias. <i>Reject</i> is useful if your priority is to prevent two users registering with the same alias. <i>Overwrite</i> is useful if your network is such that endpoints are often allocated new IP addresses, because it will prevent unwanted registration rejections. Note that in a cluster a registration conflict is only detected if the registration requests are received by the same peer. |
| Call signaling TCP port | The listening port for H.323 call signaling. Default is 1720. | |
| Call signaling port range start and end | 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. |

Protocols

| Field | Description | Usage tips |
|--------------------------|--|--|
| Time to live | The interval (in seconds) at which an H.323 endpoint must re-register with the Expressway in order to confirm that it is still functioning. Default is 1800. | Some older endpoints do not support the ability to periodically re-register with the system. In this case, and in any other situation where the system has not had a confirmation from the endpoint within the specified period, it will send an IRQ to the endpoint to verify that it is still functioning. Note: By reducing the registration time to live too much, you risk flooding the Expressway with registration requests, which will severely impact performance. This impact is proportional to the number of endpoints, so you should balance the need for occasional quick failover against the need for continuous good performance. |
| Call time to live | 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 is disconnected. The system polls endpoints in a call, whether the call type is traversal or non-traversal. |
| Auto discover | Determines whether it will respond to Gatekeeper Discovery Requests sent out by endpoints. The default is <i>On</i> . | To prevent H.323 endpoints being able to register automatically with the Expressway, set Auto discover to <i>Off</i> . This means that endpoints can only register with the Expressway if their Gatekeeper Discovery setting is <i>Manual</i> and they have been configured with the Expressway's IP address. |
| Caller ID | 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. |

About SIP

The Expressway supports the SIP protocol. It can act as a SIP registrar and proxy.

The Expressway can provide interworking between SIP and H.323, translating between the two protocols to enable endpoints that only support one of these protocols to call each other.

To support SIP:

- **SIP mode** must be enabled.
- At least one of the SIP transport protocols (UDP, TCP or TLS) must be active. Note that the use of UDP is not recommended for video as SIP message sizes are frequently larger than a single UDP packet.

Any dialog-forming requests, such as INVITE and SUBSCRIBE, that contain Route Sets are rejected. Requests that do not have Route Sets are proxied as normal in accordance with existing call processing rules.

Expressway as a SIP Registrar

For a SIP endpoint to be contactable via its alias, it must register its Address of Record (AOR) and its location with a SIP registrar. The SIP registrar maintains a record of the endpoint's details against the endpoint's AOR. The AOR is the alias through which the endpoint can be contacted; it is a SIP URI and always takes the form `username@domain`.

When a call is received for that AOR, the SIP registrar refers to the record to find its corresponding endpoint. (Note that the same AOR can be used by more than one SIP endpoint at the same time, although to ensure that all endpoints are found they must all register with the same Expressway or Expressway cluster.)

A SIP registrar only accepts registrations for domains for which it is authoritative. The Expressway can act as a SIP registrar for up to 200 domains. To make the Expressway act as a SIP registrar, you must configure it with the [SIP domains](#) for which it will be authoritative. It will then handle registration requests for any endpoints attempting to

Protocols

register against that domain. Note that the Expressway will also accept registration requests where the domain portion of the AOR is either the FQDN or the IP address of the Expressway. Whether or not the Expressway accepts a registration request depends on its [registration control](#) settings.

In a [Unified Communications](#) deployment, endpoint registration for SIP devices may be provided by Unified CM. In this scenario, the Expressway provides secure firewall traversal and line-side support for Unified CM registrations. When configuring a domain, you can select whether Cisco Unified Communications Manager or Expressway provides registration and provisioning services for the domain.

SIP endpoint registration

There are two ways a SIP endpoint can locate a registrar with which to register: manually or automatically. The option is configured on the endpoint itself under the SIP **Server Discovery** option (consult your endpoint user guide for how to access this setting; it may also be referred to as **Proxy Discovery**).

- If the **Server Discovery** mode is set to automatic, the endpoint will send a REGISTER message to the SIP server that is authoritative for the domain with which the endpoint is attempting to register. For example, if an endpoint is attempting to register with a URI of `john.smith@example.com`, the request will be sent to the registrar authoritative for the domain `example.com`. The endpoint can discover the appropriate server through a variety of methods including DHCP, DNS or provisioning, depending upon how the video communications network has been implemented.
- If the **Server Discovery** mode is set to manual, the user must specify the IP address or FQDN of the registrar (Expressway or Expressway cluster) with which they want to register, and the endpoint will attempt to register with that registrar only.

The Expressway is a SIP server and a SIP registrar.

- If an endpoint is registered to the Expressway, the Expressway will be able to forward inbound calls to that endpoint.
- If the Expressway is not configured with any SIP domains, the Expressway will act as a SIP server. It may proxy registration requests to another registrar, depending upon the **SIP registration proxy mode** setting.

Registration refresh intervals

Depending on the typical level of active registrations on your system, you may want to configure the **Standard registration refresh strategy** to *Variable* and set the refresh intervals as follows:

| Active registrations | Minimum refresh interval | Maximum refresh interval |
|----------------------|--------------------------|--------------------------|
| 1-100 | 45 | 60 |
| 101-500 | 150 | 200 |
| 501-1000 | 300 | 400 |
| 1000-1500 | 450 | 800 |
| 1500+ | 750 | 1000 |

Note: If you have a mix of H.323 and SIP endpoints, be aware that H.323 registration requests and SIP registration requests can both impair performance of the Expressway if it receives too many.

If you want to ensure registration resiliency, use SIP outbound registrations as described below.

SIP registration resiliency

The Expressway supports multiple client-initiated connections (also referred to as "SIP Outbound") as outlined in [RFC 5626](#).

This allows SIP endpoints that support *RFC 5626* to be simultaneously registered to multiple Expressway cluster peers. This provides extra resiliency: if the endpoint loses its connection to one cluster peer it will still be able to receive calls via one of its other registration connections.

Expressway as a SIP Proxy Server

The Expressway acts as a SIP proxy server when **SIP mode** is enabled. The role of a proxy server is to forward requests (such as REGISTER and INVITE) from endpoints or other proxy servers on to further proxy servers or to the destination endpoint.

The Expressway's behavior as a SIP proxy server is determined by:

- the SIP registration proxy mode setting
- the presence of Route Set information in the request header
- whether the proxy server from which the request was received is a neighbor of the Expressway

A Route Set specifies the path to take when requests are proxied between an endpoint and its registrar. For example, when a REGISTER request is proxied by the Expressway, it adds a path header component to the request. This signals that calls to that endpoint should be routed through the Expressway. This is usually required in situations where firewalls exist and the signaling must follow a specified path to successfully traverse the firewall. For more information about path headers, see [RFC 3327](#).

When the Expressway proxies a request that contains Route Set information, it forwards it directly to the URI specified in the path. Any call processing rules configured on the Expressway are bypassed. This may present a security risk if the information in the Route Set cannot be trusted. For this reason, you can configure how the Expressway proxies requests that contain Route Sets by setting the **SIP registration proxy mode** as follows:

- *Off*: requests containing Route Sets are rejected. This setting provides the highest level of security.
- *Proxy to known only*: requests containing Route Sets are proxied only if the request was received from a known zone.
- *Proxy to any*: requests containing Route Sets are always proxied.

In all cases, requests that do not have Route Sets are proxied as normal in accordance with existing call processing rules. This setting only applies to dialog-forming requests, such as INVITE and SUBSCRIBE. Other requests, such as NOTIFY, are always proxied regardless of this setting.

Proxying Registration Requests

If the Expressway receives a registration request for a domain for which it is not acting as a Registrar (the Expressway does not have that SIP domain configured), then the Expressway may proxy the registration request onwards. This depends on the **SIP registration proxy mode** setting, as follows:

- *Off*: the Expressway does not proxy any registration requests. They are rejected with a “403 Forbidden” message.
- *Proxy to known only*: the Expressway proxies the request in accordance with existing call processing rules, but only to known neighbor, traversal client and traversal server zones.
- *Proxy to any*: this is the same as *Proxy to known only* but for all zone types i.e. it also includes ENUM and DNS zones.

Accepting proxied registration requests

If the Expressway receives a proxied registration request, in addition to the Expressway's standard [registration controls](#), you can also control whether the Expressway accepts the registration depending upon the zone through which the request was received. You do this through the **Accept proxied registrations** setting when [configuring a zone](#).

Proxied registrations are classified as belonging to the zone they were last proxied from. This is different from non-proxied registration requests which are assigned to a subzone within the Expressway.

Configuring SIP

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

Protocols

- SIP functionality and SIP-specific transport modes and ports.
- Certificate revocation checking modes for TLS connections.
- Registration controls for standard and outbound registrations.

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 |
|---|---|---|
| SIP mode | Enables and disables SIP functionality (SIP registrar and SIP proxy services) on the Expressway. Default is <i>Off</i> . | This mode must be enabled to use either the Presence Server or the Presence User Agent. |
| SIP protocols and ports | <p>The Expressway supports SIP over UDP, TCP, and TLS transport protocols. Use the Mode and Port 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>The default modes and ports are:</p> <ul style="list-style-type: none"> ■ UDP mode <i>Off</i>, port 5060 ■ TCP mode <i>Off</i>, port 5060 ■ TLS mode <i>On</i>, port 5061 ■ Mutual TLS mode <i>Off</i>, port 5062 | <p>At least one of the transport protocol modes must be <i>On</i> to enable SIP functionality.</p> <p>If you use both TLS and MTLT, we recommend that you enable them on different ports. If you must use port 5061 for MTLT, you should avoid engaging the B2BUA - by switching Media encryption mode to <i>Auto</i> on all zones in the call path.</p> |
| TCP outbound port start / end | 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. |
| Session refresh interval | 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 RFC 4028 . |
| Minimum session refresh interval | The minimum value the Expressway 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 RFC 4028 . |
| TLS handshake timeout | 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:

Protocols

| Field | Description | Usage tips |
|---|--|--|
| Certificate revocation checking mode | Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment. | We recommend that revocation checking is enabled. |
| Use OCSP | 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. |
| Use CRLs | Controls whether Certificate Revocation Lists (CRLs) are used to perform certificate revocation checking. | CRLs can be used if the certificate does not support OCSP. CRLs can be loaded manually onto the Expressway, downloaded automatically from preconfigured URIs (see Managing Certificate Revocation Lists (CRLs), page 282), or downloaded automatically from a CRL distribution point (CDP) URI contained in the X.509 certificate. |
| Allow CRL downloads from CDPs | Controls whether the download of CRLs from the CDP URIs contained in X.509 certificates is allowed. | |
| Fallback behavior | Controls the revocation checking behavior if the revocation status cannot be established, for example if the revocation source cannot be contacted. <i>Treat as revoked:</i> treat the certificate as revoked (and thus do not allow the TLS connection). <i>Treat as not revoked:</i> treat the certificate as not revoked. Default: <i>Treat as not revoked</i> | <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. |

Registration Controls

This section contains the registration controls for standard and outbound SIP registrations. The configurable options are:

| Field | Description | Usage tips |
|---|---|---|
| Standard registration refresh strategy | <p>The method used to generate the SIP registration expiry period (the period within which a SIP endpoint must re-register to prevent its registration expiring) for standard registrations.</p> <p><i>Maximum</i>: uses the lesser of the configured Maximum refresh value and the value requested in the registration.</p> <p><i>Variable</i>: generates a random value between the configured Minimum refresh value and the lesser of the configured Maximum refresh value and the value requested in the registration.</p> <p>The default is <i>Maximum</i>.</p> | <p>The <i>Maximum</i> setting uses the requested value providing it is within the specified maximum and minimum ranges.</p> <p>The <i>Variable</i> setting calculates a random refresh period for each registration (and re-registration) request in an attempt to continually spread the load. The Expressway never returns a value higher than what was requested.</p> <p>This applies only to endpoints registered with the Expressway. It does not apply to endpoints whose registrations are proxied through the Expressway.</p> |
| Standard registration refresh minimum | <p>The minimum allowed value for a SIP registration refresh period for standard registrations. Requests for a value lower than this will result in the registration being rejected with a 423 Interval Too Brief response. The default is 45 seconds.</p> | <p>See Registration refresh intervals, page 120</p> |
| Standard registration refresh maximum | <p>The maximum allowed value for a SIP registration refresh period for standard registrations. Requests for a value greater than this will result in a lower value being returned (calculated according to the Standard registration refresh strategy). The default is 60 seconds.</p> | |
| Outbound registration refresh strategy | <p>The method used to generate the SIP registration expiry period for outbound registrations.</p> <p><i>Maximum</i>: uses the lesser of the configured Maximum refresh value and the value requested in the registration.</p> <p><i>Variable</i>: generates a random value between the configured Minimum refresh value and the lesser of the configured Maximum refresh value and the value requested in the registration.</p> <p>The default is <i>Variable</i>.</p> | <p>These options work in the same manner as for the Standard registration refresh strategy.</p> <p>However, outbound registrations allow a much higher maximum value than standard registrations. This is because standard registrations use the re-registration mechanism to keep their connection to the server alive. With outbound registrations the keep-alive process is handled by a separate, less resource-intensive process, meaning that re-registrations (which are more resource-intensive) can be less frequent.</p> |
| Outbound registration refresh minimum | <p>The minimum allowed value for a SIP registration refresh period for outbound registrations. Requests for a value lower than this will result in the registration being rejected with a 423 Interval Too Brief response. The default is 300 seconds.</p> | |

Protocols

| Field | Description | Usage tips |
|--|--|--|
| Outbound registration refresh maximum | The maximum allowed value for a SIP registration refresh period for an outbound registration. Requests for a value greater than this will result in a lower value being returned (calculated according to the Outbound registration refresh strategy). The default is 3600 seconds. | |
| SIP registration proxy mode | <p>Specifies how proxied registrations and requests containing Route Sets are handled when the Expressway receives a registration request for a domain for which it is not acting as a Registrar.</p> <p><i>Off:</i> registration requests are not proxied (but are still permitted locally if the Expressway is authoritative as a Registrar for that domain). Requests with existing Route Sets are rejected.</p> <p><i>Proxy to known only:</i> registration requests are proxied in accordance with existing call processing rules, but only to known neighbor, traversal client and traversal server zones. Requests containing Route Sets are proxied only if they were received from a known zone.</p> <p><i>Proxy to any:</i> registration requests are proxied in accordance with existing call processing rules to all known zones. Requests containing Route Sets are always proxied.</p> <p>The default is <i>Off</i>.</p> | See Proxying Registration Requests, page 121 for more information. |

Authentication Controls

This section contains the device authentication controls for enabling delegated credential checking. The configurable options are:

| Field | Description | Usage tips |
|--------------------------------------|---|--|
| Delegated credential checking | <p>Controls whether the credential checking of SIP messages is delegated, via a traversal zone, to another Expressway.</p> <p><i>Off:</i> use the relevant credential checking mechanisms (local database, Active Directory Service or H.350 directory via LDAP) on the Expressway performing the authentication challenge.</p> <p><i>On:</i> delegate the credential checking to a traversal client.</p> <p>The default is <i>Off</i>.</p> | <p>Note that delegated credential checking must be enabled on both the traversal server and the traversal client.</p> <p>See delegated credential checking for more information.</p> |

Advanced SIP Settings

| Field | Description | Usage tips |
|--------------------------------|---|--|
| SIP max size | Specifies the maximum SIP message size that can be handled by the Expressway (in bytes). Default is 32768 bytes. | If you use Microsoft interop with dual-homed conferencing through Expressway and Meeting Server with an AVMCU invoked on the Microsoft side, we recommend 32768 or greater. |
| SIP TCP connect timeout | Specifies the maximum number of seconds to wait for an outgoing SIP TCP connection to be established. Default is 10 seconds. | You can reduce this to speed up the time between attempting a broken route (such as an unavailable onward SIP proxy peer) and failing over to a good one. In high latency networks, take care to leave enough time for the connection to establish. |

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 (Expressway-C Only)

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 Expressway:** the Expressway is authoritative for this SIP domain. The Expressway acts as a SIP registrar for the domain, and accepts registration requests for any SIP endpoints attempting to register with an alias that includes this domain. The default is *On*.
- **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 *Off*.
- **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 *Off*.
- **XMPP federation:** Enables XMPP federation between this domain and partner domains. The default is *Off*.
- **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 Delegated Credential Checking (Expressway-E Only)

If you have enabled delegated credential checking (**Configuration > Protocols > SIP**), you need to specify the traversal zone to use when delegating credential checks for SIP messages for this domain. This only applies to the SIP domains for which Expressway is acting as the service provider and SIP registrar.

You can specify a different zone for each SIP domain, if required.

Choose *Do not delegate* if you want to continue to use this Expressway-E to perform the credential checking.

Testing the credential checking service

To verify whether the Expressway to which credential checking has been delegated is able to receive messages and perform the relevant authentication checks:

1. Go to **Configuration > Domains**.
2. Select the relevant domains.
3. Click **Test credential checking service**.

The system displays a **Results** section and reports whether the receiving Expressway can be reached over the traversal zone and, additionally, if it is able to perform credential checking for both NTLM and SIP digest type challenges.

If you are not using NTLM authentication in your video network, and thus the receiving Expressway is not configured with a connection to an Active Directory Service, then the NTLM check will be expected to fail.

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”.

By default, the Expressway acts as a SIP–H.323 and H.323–SIP gateway but only if one of the endpoints that are involved in the call is locally registered. You can change this setting so that the Expressway acts as a SIP–H.323 gateway regardless of whether the endpoints involved are locally registered. You also have the option to disable interworking completely.

The options for the **H.323 <-> SIP interworking mode** are:

- *Off*: the Expressway does not act as a SIP–H.323 gateway.
- *Registered only*: the Expressway acts as a SIP–H.323 gateway but only if one of the endpoints is locally registered.
- *On*: the Expressway acts as a SIP–H.323 gateway regardless of whether the endpoints are locally registered.

We recommend that you leave this setting as *Registered only*. Unless your network is correctly configured, setting it to *On* (where all calls can be interworked) may result in unnecessary interworking, for example where a call between two H.323 endpoints is made over SIP, or vice versa.

Calls for which the Expressway acts as a SIP to H.323 gateway are RMS calls. 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

Protocols

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).

- If the request has come from a neighboring system and **Interworking mode** is set to *Registered only*, the Expressway searches the Local Zone using both protocols, and all other zones using the native protocol only (because it will interwork the call only if one of the endpoints is locally registered).
- If **Interworking mode** is set to *On*, or the request has come from a locally registered endpoint, the Expressway searches the Local Zone and all external zones using both protocols.

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.

Interworking DTMF signals

For SIP calls, the Expressway implements RFC 2833 for DTMF signaling in RTP payloads.

For H.323 calls, the Expressway implements H.245 UserInputIndication for DTMF signaling. `dtmf` is the only supported `UserInputCapability`. Expressway does not support any other H.245 user input capabilities (eg. `basicString`, `generalString`)

When the Expressway is interworking a call between SIP and H.323, it also interworks the DTMF signaling, but only between RFC 2833 DTMF and H.245 `dtmf` user input.



Registration Control

This section provides information about the pages that appear under the **Configuration > Registration** menu.

| | |
|--|-----|
| About Registrations | 129 |
| About Allow and Deny Lists | 131 |
| Configuring Registration Policy to Use an External Service | 133 |

About Registrations

For an endpoint to use the Expressway as its H.323 gatekeeper or SIP registrar, the endpoint must first register with the Expressway. The Expressway can be configured to control which devices are allowed to register with it by using the following mechanisms:

- a [device authentication](#) process based on the username and password supplied by the endpoint
- a [registration restriction policy](#) that uses either [Allow Lists or Deny Lists](#) or an external policy service to specify which aliases can and cannot register with the Expressway
- restrictions based on IP addresses and subnet ranges through the specification of subzone membership rules and [subzone registration policies](#)

You can use these mechanisms together. For example, you can use authentication to verify an endpoint's identity from a corporate directory, and registration restriction to control which of those authenticated endpoints may register with a particular Expressway.

You can also control some protocol-specific behavior, including:

- the **Registration conflict mode** and **Auto discover** settings for [H.323](#) registrations
- the **SIP registration proxy mode** for [SIP](#) registrations

For specific information about how registrations are managed across peers in a cluster, see the [Sharing Registrations Across Peers, page 176](#) section.

In a [Unified Communications](#) deployment, endpoint registration for SIP devices may be provided by Unified CM. In this scenario, the Expressway provides secure firewall traversal and line-side support for Unified CM registrations. When configuring a domain, you can select whether Cisco Unified Communications Manager or Expressway provides registration and provisioning services for the domain.

Finding a Expressway With Which to Register

Before an endpoint can register with a Expressway, it must determine which Expressway it can or should be registering with. This setting is configured on the endpoint, and the process is different for [SIP](#) and [H.323](#).

MCU, Gateway and Content Server Registration

H.323 systems such as gateways, MCUs and Content Servers can also register with a Expressway. They are known as locally registered services. These systems are configured with their own prefix, which they provide to the Expressway when registering. The Expressway will then know to route all calls that begin with that prefix to the gateway, MCU or Content Server as appropriate. These prefixes can also be used to control registrations.

Registration Control

SIP devices cannot register prefixes. If your dial plan dictates that a SIP device should be reached via a particular prefix, then you should add the device as a neighbor zone with an associated search rule using a pattern match equal to the prefix to be used.

Configuring Registration Restriction Policy

The **Registration configuration** page (**Configuration > Registration > Configuration**) is used to control how the Expressway manages its registrations.

The **Restriction policy** option specifies the policy to use when determining which endpoints may register with the Expressway. The options are:

- *None*: any endpoint may register.
- *Allow List*: only those endpoints with an alias that matches an entry in the Allow List may register.
- *Deny List*: all endpoints may register, unless they match an entry on the Deny List.
- *Policy service*: only endpoints that register with details allowed by the external policy service may register.

The default is *None*.

If you use an *Allow List* or *Deny List*, you must also go to the appropriate [Registration Allow List](#) or [Registration Deny List](#) configuration page to create the list.

The *Policy service* option is used if you want to refer all registration restriction 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 Registration Policy to Use an External Service](#), page 133.

Registering Aliases

After the [device authentication](#) process (if required) has been completed, the endpoint will then attempt to register its aliases with the Expressway.

H.323

When registering, the H.323 endpoint presents the Expressway with one or more of the following:

- one or more H.323 IDs
- one or more E.164 aliases
- one or more URIs

Users of other registered endpoints can then call the endpoint by dialing any of these aliases.

- You are recommended to register your H.323 endpoints using a URI. This facilitates interworking between SIP and H.323, as SIP endpoints register using a URI as standard.
- You are recommended to not use aliases that reveal sensitive information. Due to the nature of H.323, call setup information is exchanged in an unencrypted form.

SIP

When registering, the SIP endpoint presents the Expressway with its contact address (IP address) and logical address (Address of Record). The logical address is considered to be its alias, and will generally be in the form of a URI.

H.350 directory authentication and registrations

If the Expressway is using an H.350 directory service to authenticate registration requests, the **Source of aliases for registration** setting is used to determine which aliases the endpoint is allowed to attempt to register with. See [Using an H.350 directory service lookup via LDAP](#) for more information.

Attempts to register using an existing alias

An endpoint may attempt to register with the Expressway using an alias that is already registered to the system. How this is managed depends on how the Expressway is configured and whether the endpoint is SIP or H.323.

Registration Control

- **H.323:** an H.323 endpoint may attempt to register with the Expressway using an alias that has already been registered on the Expressway from another IP address. You can control how the Expressway behaves in this situation by configuring the **Registration conflict mode**, on the [H.323](#) page (**Configuration > Protocols > H.323**).
- **SIP:** a SIP endpoint will always be allowed to register using an alias that is already in use from another IP address. When a call is received for this alias, all endpoints registered using that alias will be called simultaneously. This SIP feature is known as “forking”.

Blocking registrations

If you have configured the Expressway to use a [Deny List](#), you will have an option to block the registration. This will add all the aliases used by that endpoint to the Deny List.

Removing existing registrations

After a restriction policy has been activated, it controls all registration requests from that point forward. However, any existing registrations may remain in place, even if the new list would otherwise block them. Therefore, you are recommended to manually remove all existing unwanted registrations after you have implemented a restriction policy.

To manually remove a registration, go to **Status > Registrations > By device**, select the registrations you want to remove, and click **Unregister**.

If the registered device is in an active call and its registration is removed (or expires), the effect on the call is dependent on the protocol:

- **H.323:** the call is taken down.
- **SIP:** the call stays up by default. This SIP behavior can be changed but only via the CLI by using the command `xConfiguration SIP Registration Call Remove`.

Re-registrations

All endpoints must periodically re-register with the Expressway in order to keep their registration active. If you do not manually delete the registration, the registration could be removed when the endpoint attempts to re-register, but this depends on the protocol being used by the endpoint:

- H.323 endpoints may use "light" re-registrations which do not contain all the aliases presented in the initial registration, so the re-registration may not get filtered by the restriction policy. If this is the case, the registration will not expire at the end of the registration timeout period and must be removed manually.
- SIP re-registrations contain the same information as the initial registrations so will be filtered by the restriction policy. This means that, after the list has been activated, all SIP registrations will disappear at the end of their registration timeout period.

The frequency of re-registrations is determined by the **Registration controls** setting for [SIP](#) (**Configuration > Protocols > SIP**) and the **Time to live** setting for [H.323](#) (**Configuration > Protocols > H.323**).

Note: By reducing the registration time to live too much, you risk flooding the Expressway with registration requests, which will severely impact performance. This impact is proportional to the number of endpoints, so you should balance the need for occasional quick failover against the need for continuous good performance.

About Allow and Deny Lists

When an endpoint attempts to register with the Expressway it presents a list of aliases. One of the methods provided by the Expressway to control which endpoints are allowed to register is to set the **Restriction policy** (on the [Configuring Registration Restriction Policy, page 130](#) page) to *Allow List* or *Deny List* and then to include any one of the endpoint’s aliases on the Allow List or the Deny List as appropriate. Each list can contain up to 2,500 entries.

When an endpoint attempts to register, each of its aliases is compared with the patterns in the relevant list to see if it matches. Only one of the aliases needs to appear in the Allow List or the Deny List for the registration to be allowed or denied.

For example, if the **Restriction policy** is set to *Deny List* and an endpoint attempts to register using three aliases, one of which matches a pattern on the Deny List, that endpoint’s registration will be denied. Likewise, if the **Restriction**

Registration Control

policy is set to *Allow List*, only one of the endpoint's aliases needs to match a pattern on the Allow List for it to be allowed to register using all its aliases.

Allow Lists and Deny Lists are mutually exclusive: only one may be in use at any given time. You can also control registrations at the [subzone](#) level. Each subzone's registration policy can be configured to allow or deny registrations assigned to it via the subzone membership rules.

Configuring the Registration Allow List

The **Registration Allow List** page (**Configuration > Registration > Allow List**) shows the endpoint aliases and alias patterns that are allowed to register with the Expressway. Only one of an endpoint's aliases needs to match an entry in the Allow List for the registration to be allowed.

To use the Allow List, you must select a **Restriction policy** of *Allow List* on the [Registration configuration](#) page.

The configurable options are:

| Field | Description | Usage tips |
|-----------------------|--|---|
| Description | An optional free-form description of the entry. | |
| Pattern type | The way in which the Pattern string must match the alias. Options are: <i>Exact</i> : the alias must match the pattern string exactly. <i>Prefix</i> : the alias must begin with the pattern string. <i>Suffix</i> : the alias must end with the pattern string. <i>Regex</i> : the pattern string is a regular expression . | You can test whether a pattern matches a particular alias by using the Check pattern tool (Maintenance > Tools > Check pattern). |
| Pattern string | The pattern against which an alias is compared. | |

Configuring the Registration Deny List

The **Registration Deny List** page (**Configuration > Registration > Deny List**) shows the endpoint aliases and alias patterns that are **not** allowed to register with the Expressway. Only one of an endpoint's aliases needs to match an entry in the Deny List for the registration to be denied.

To use the Deny List, you must select a **Restriction policy** of *Deny List* on the [Registration configuration](#) page.

The configurable options are:

| Field | Description | Usage tips |
|--------------------|---|------------|
| Description | An optional free-form description of the entry. | |

Registration Control

| Field | Description | Usage tips |
|-----------------------|---|---|
| Pattern type | The way in which the Pattern string must match the alias. Options are: <i>Exact</i> : the alias must match the pattern string exactly. <i>Prefix</i> : the alias must begin with the pattern string. <i>Suffix</i> : the alias must end with the pattern string. <i>Regex</i> : the pattern string is a regular expression . | You can test whether a pattern matches a particular alias by using the Check pattern tool (Maintenance > Tools > Check pattern). |
| Pattern string | The pattern against which an alias is compared. | |

Configuring Registration Policy to Use an External Service

To configure Registration Policy to refer all registration restriction policy decisions out to an external service:

1. Go to **Configuration > Registration > Configuration**.
2. Select a **Restriction policy** of *Policy service*.
3. Configure the fields as follows:

| Field | Description | Usage tips |
|---|---|--|
| Protocol | The protocol used to connect to the policy service. The default is <i>HTTPS</i> . | The Expressway automatically supports HTTP to HTTPS redirection when communicating with the policy service server. |
| Certificate verification mode | When connecting over HTTPS, this setting controls whether the certificate presented by the policy server is verified. 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 Server address fields below. | The Expressway's root CA certificates are loaded via (Maintenance > Security > Trusted CA certificate). |
| HTTPS certificate revocation list (CRL) checking | 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 Maintenance > Security > CRL management to configure how the Expressway uploads CRL files. |

Registration Control

| Field | Description | Usage tips |
|-----------------------------|---|--|
| Server address 1 - 3 | Enter the IP address or Fully Qualified Domain Name (FQDN) of the server hosting the service. You can specify a port by appending :<port> to the address. | If an FQDN is specified, ensure that the Expressway has an appropriate DNS configuration that allows the FQDN to be resolved. For resiliency, up to three server addresses can be supplied. |
| Path | Enter the URL of the service on the server. | |
| Status path | The Status path identifies the path from where the Expressway can obtain the status of the remote service. The default is <i>status</i> . | The policy server must supply return status information, see Policy Server Status and Resiliency, page 326 . |
| Username | The username used by the Expressway to log in and query the service. | |
| Password | The password used by the Expressway to log in and query the service. | The maximum plaintext length is 30 characters (which is subsequently encrypted). |
| Default CPL | 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. For more information, see Default CPL for Policy Services, page 521 . |

4. Click **Save**.

The Expressway should connect to the policy service server and start using the service for Registration 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.



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 | 135 |
| Authenticating with External Systems | 140 |

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.

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. If the Expressway is the authenticating agent for these devices (compared to an external IdP), then it automatically handles the authentication of these devices against their home Unified CM clusters.

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:

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

Device Authentication

When the Expressway uses a policy service it sends information about the call or registration 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.

See *Cisco Expressway External Policy Deployment Guide* at the [Cisco Expressway Series Configuration Guides page](#).

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 messages, SIP messages received from local domains and SIP messages from non-local domains.

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. 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. |

Device Authentication

| 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) and whether the message was received from a local domain (a domain for which the Expressway is authoritative) or a non-local domain.

| Policy | Trust | In local domain | Outside local domain |
|--------------------------|-------|--|--|
| Check credentials | Off | <p>Messages are challenged for authentication.</p> <p>Messages that fail authentication are rejected.</p> <p>Messages that pass authentication are classified as authenticated and a P-Asserted-Identity header is inserted into the message.</p> | <p>Messages are not challenged for authentication.</p> <p>All messages are classified as unauthenticated.</p> <p>Any existing P-Asserted-Identity headers are removed.</p> |
| | On | <p>Messages with an existing P-Asserted-Identity header are classified as authenticated, without further challenge. The P-Asserted-Identity header is passed on unchanged (keeping the originator's asserted ID).</p> <p>Messages without an existing P-Asserted-Identity header are challenged. If authentication passes, the message is classified as authenticated and a P-Asserted-Identity header is inserted into the message. If authentication fails, the message is rejected.</p> | <p>Messages are not challenged for authentication.</p> <p>Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged.</p> <p>Messages without an existing P-Asserted-Identity header are classified as unauthenticated.</p> |
| Do not check credentials | Off | <p>Messages are not challenged for authentication.</p> <p>All messages are classified as unauthenticated.</p> <p>Any existing P-Asserted-Identity headers are removed.</p> | <p>Messages are not challenged for authentication.</p> <p>All messages are classified as unauthenticated.</p> <p>Any existing P-Asserted-Identity headers are removed.</p> |
| | On | <p>Messages are not challenged for authentication.</p> <p>Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged.</p> <p>Messages without an existing P-Asserted-Identity header are classified as unauthenticated.</p> | <p>Messages are not challenged for authentication.</p> <p>Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged.</p> <p>Messages without an existing P-Asserted-Identity header are classified as unauthenticated.</p> |

Device Authentication

| Policy | Trust | In local domain | Outside local domain |
|------------------------|-------|---|--|
| Treat as authenticated | Off | <p>Messages are not challenged for authentication.</p> <p>All messages are classified as authenticated.</p> <p>Any existing P-Asserted-Identity header is removed and a new one containing the Expressway's originator ID is inserted into the message.</p> | <p>Messages are not challenged for authentication.</p> <p>All messages are classified as unauthenticated.</p> <p>Any existing P-Asserted-Identity headers are removed.</p> |
| | On | <p>Messages are not challenged for authentication.</p> <p>All messages are classified as authenticated.</p> <p>Messages with an existing P-Asserted-Identity header are passed on unchanged. Messages without an existing P-Asserted-Identity header have one inserted.</p> | <p>Messages are not challenged for authentication.</p> <p>Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged.</p> <p>Messages without an existing P-Asserted-Identity header are classified as unauthenticated.</p> |

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.

Device Provisioning and Authentication Policy

The Provisioning Server requires that any provisioning or phone book requests it receives have already been authenticated at the zone or subzone point of entry into the Expressway. The Provisioning Server does not do its own authentication challenge and will reject any unauthenticated messages.

The Expressway must be configured with appropriate device authentication settings, otherwise provisioning-related messages will be rejected:

- Initial provisioning authentication (of a subscribe message) is controlled by the authentication policy setting on the Default Zone. (The Default Zone is used as the device is not yet registered.)

The Default Zone and any traversal client zone's authentication policy must be set to either *Check credentials* or *Treat as authenticated*, otherwise provisioning requests will fail.

In each case, the Expressway performs its authentication checking against the local database. This includes all credentials supplied by Cisco TMS.

For more information about provisioning configuration in general, see [Cisco TMS Provisioning Extension Deployment Guide](#).

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), traversal client, and TURN client authentication.

Adding credentials to the local database

To enter a set of device credentials:

1. Go to **Configuration > Authentication > Devices > 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.

Credentials managed within Cisco TMS (for device provisioning)

When the Expressway is using TMS Provisioning Extension services, the credentials supplied by the Users service are stored in the local authentication database, along with any manually configured entries. The **Source** column identifies whether the user account name is provided by **TMS**, or is a **Local** entry. Only **Local** entries can be edited.

Incorporating Cisco TMS credentials within the local database means that Expressway can authenticate all messages (i.e. not just provisioning requests) against the same set of credentials used within Cisco TMS.

Local database authentication in combination with H.350 directory authentication

You can configure the Expressway to use both the local database and an H.350 directory.

If an H.350 directory is configured, the Expressway will always attempt to verify any Digest credentials presented to it by first checking against the local database before checking against the H.350 directory.

Local database authentication in combination with Active Directory (direct) authentication

If Active Directory (direct) authentication has been configured and NTLM protocol challenges is set to Auto, then NTLM authentication challenges are offered to those devices that support NTLM.

- NTLM challenges are offered in addition to the standard Digest challenge.
- Endpoints that support NTLM will respond to the NTLM challenge in preference to the Digest challenge, and the Expressway will attempt to authenticate that NTLM response.

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 your Video Communications Network | 141 |
| Structuring your Dial Plan | 142 |
| About Zones | 143 |
| Configuring Media Encryption Policy | 144 |
| Configuring ICE Messaging Support | 145 |
| About the Local Zone and Subzones | 146 |
| The Default Zone | 146 |
| Configuring Default Zone access rules | 147 |
| Zone List | 148 |

About your Video Communications Network

The most basic implementation of a video communications network is a single Expressway connected to the internet with one or more endpoints registered to it. However, depending on the size and complexity of your enterprise the Expressway may be part of a network of endpoints, other Expressways and other network infrastructure devices, with one or more firewalls between it and the internet. In such situations you may want to apply restrictions to the amount of bandwidth used by and between different parts of your network.

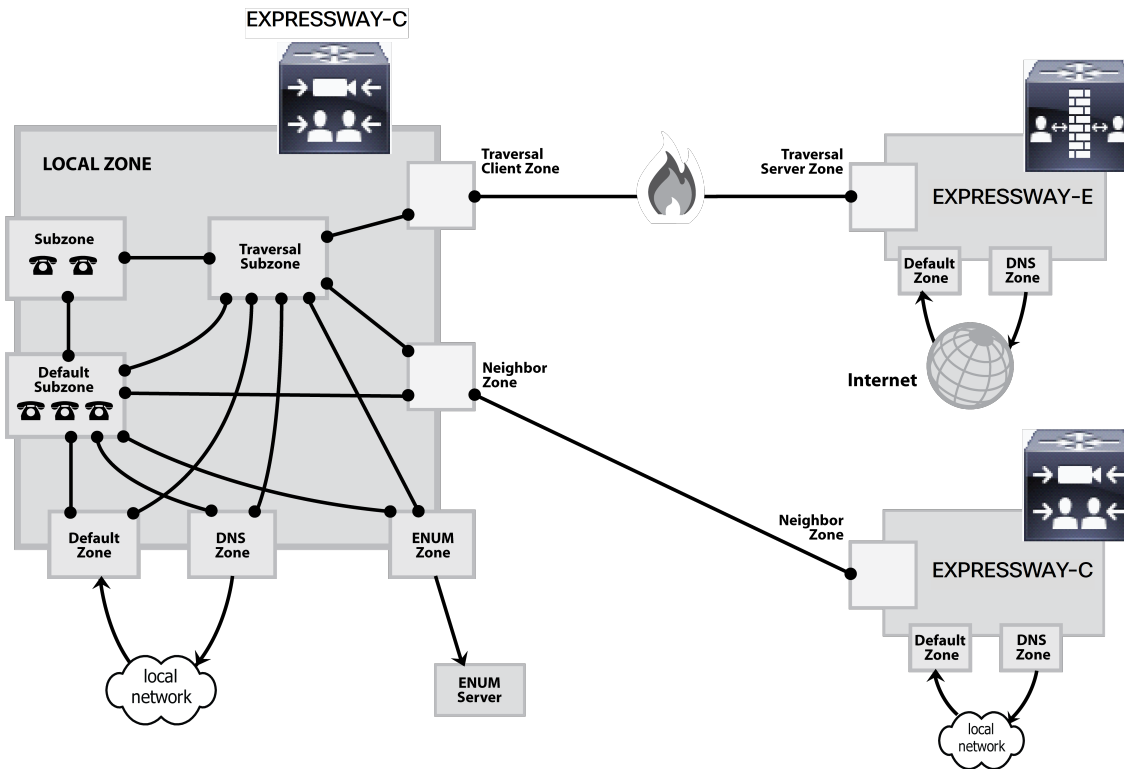
This section provides an overview of the different parts of the video communications network and the ways in which they can be connected. This information should allow you to configure your Expressway to best suit your own infrastructure.

Example network diagram

The diagram below shows the different components of an Expressway (i.e. subzones and zones) and how they interrelate. Using an Expressway-C as the example Local Zone, it shows that it is made up of a number of subzones which are all connected by links. The Local Zone is also connected to external Expressways and to the internet via different types of zones.

All these components are described in more detail in the sections that follow.

Zones and Neighbors



Structuring your Dial Plan

As you start deploying more than one Expressway, it is useful to neighbor the systems together so that they can query each other about their registered endpoints. Before you start, you should consider how you will structure your dial plan. This will determine the aliases assigned to the endpoints, and the way in which the Expressways are neighbored together. The solution you choose will depend on the complexity of your system. Some possible options are described in the following sections.

Flat Dial Plan

The simplest approach is to assign each endpoint a unique alias and divide the endpoint registrations between the Expressways. Each Expressway is then configured with all the other Expressway as neighbor zones. When one Expressway receives a call for an endpoint which is not registered with it, it will send out a Location Request to all the other neighbor Expressways.

While conceptually simple, this sort of flat dial plan does not scale very well. Adding or moving an Expressway requires changing the configuration of every Expressway, and one call attempt can result in a large number of location requests. This option is therefore most suitable for a deployment with just one or two Expressways plus its peers.

Structured Dial Plan

An alternative deployment would use a structured dial plan where endpoints are assigned an alias based on the system they are registering with.

If you are using E.164 aliases, each Expressway would be assigned an area code. When the Expressways are neighbored together, each neighbor zone would have an associated search rule configured with its corresponding area code as a prefix (a **Mode** of *Alias pattern match* and a **Pattern type** of *Prefix*). That neighbor would then only be queried for calls to numbers which begin with its prefix.

In a URI based dial plan, similar behavior may be obtained by configuring search rules for each neighbor with a suffix to match the desired domain name.

Zones and Neighbors

It may be desirable to have endpoints register with just the subscriber number – the last part of the E.164 number. In that case, the search rule could be configured to strip prefixes before sending the query to that zone.

A structured dial plan minimizes the number of queries issued when a call is attempted. However, it still requires a fully connected mesh of all Expressways in your deployment. A hierarchical dial plan can simplify this.

Hierarchical dial plan

In this type of structure one Expressway is nominated as the central directory Expressway for the deployment, and all other Expressways are neighbored with it alone.

The directory Expressway is configured with:

- each Expressway as a neighbor zone
- search rules for each zone that have a **Mode** of *Alias pattern match* and the target Expressway's prefix (as with the structured dial plan) as the **Pattern string**

Each Expressway is configured with:

- the directory Expressway as a neighbor zone
- a search rule with a **Mode** of *Any alias* and a **Target** of the directory Expressway

There is no need to neighbor every Expressway with each other. Adding a new Expressway now only requires changing configuration on the new Expressway and the directory Expressway. However, note that it may be necessary to neighbor your Expressways to each other if you are using device authentication – see below for more information.

Also, failure of the directory Expressway in this situation could cause significant disruption to communications. Consideration should be given to the use of [clustering](#) for increased resilience.

Hierarchical dial plan (directory Expressway) deployments and device authentication

See Hierarchical dial plans and authentication policy for important information about how to configure your authentication policy within a hierarchical dial plan.

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 between your local subzones and endpoints in other zones
- search for aliases that are not registered locally
- 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.

Zones and Neighbors

- **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 destination via B2BUA" when the **Microsoft interoperability service** 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/subzone basis and applies only to that leg of the call in/out of that zone/subzone.
- 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 and subzone, 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/subzone 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*.
- As the B2BUA must take the media, each call is classified as a traversal call and thus consumes a Rich Media Session (RMS) license.

Zones and Neighbors

- 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 interoperability. The Microsoft interoperability service 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. B2BUA is not normally invoked (however, see the note below regarding media encryption policy). | B2BUA is invoked. B2BUA includes ICE candidates in messages to hosts in Zone A. |
| | On | B2BUA is invoked. B2BUA includes ICE candidates in messages to hosts in Zone B. | Standard Expressway proxying behavior. 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 not Auto | Yes | The B2BUA will not perform any ICE negotiation with either host. |
| Both zones = <i>On</i> | At least one zone is not Auto | 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:

Zones and Neighbors

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

About the Local Zone and Subzones

The collection of all devices registered with the Expressway makes up its **Local Zone**.

The Local Zone is divided into **subzones**. These include an automatically created **Default Subzone** and up to 1000 manually configurable subzones.

When an endpoint registers with the Expressway, it is allocated to an appropriate subzone based on subzone membership rules. These rules specify the range of IP addresses or alias pattern matches for each subzone. If an endpoint's IP address or alias does not match any of the membership rules, it is assigned to the Default Subzone.

The Local Zone may be independent of network topology, and may comprise multiple network segments. The Expressway also has two special types of subzones:

- the **Traversal Subzone**, which is always present
- the **Cluster Subzone**, which is always present but only used when your Expressway is part of a cluster

Bandwidth management

The Local Zone's subzones are used for bandwidth management. After you have set up your subzones you can apply bandwidth limits to:

- individual calls between two endpoints within the subzone
- individual calls between an endpoint within the subzone and another endpoint outside of the subzone
- the total of calls to or from endpoints within the subzone

For full details of how to create and configure subzones, and apply bandwidth limitations to subzones including the Default Subzone and Traversal Subzone, see the [Bandwidth control](#) section.

Registration, authentication and media encryption policies

In addition to bandwidth management, subzones are also used to control the Expressway's registration, authentication and media encryption policies.

See [Configuring Subzones, page 229](#) for more information about how to configure these settings.

Local Zone searches

One of the functions of the Expressway is to route a call received from a locally registered endpoint or external zone to its appropriate destination. Calls are routed based on the address or alias of the destination endpoint.

The Expressway searches for a destination endpoint in its Local Zone and its configured external zones. You can prioritize the order in which these zones are searched, and filter the search requests sent to each zone, based on the address or alias being searched for. This allows you to reduce the potential number of search requests sent to the Local Zone and out to external zones, and speed up the search process.

For further information about how to configure search rules for the Local Zone, see the [Configuring search and zone transform rules](#) section.

The Default Zone

The Default Zone represents any incoming calls from endpoints or other devices that are unregistered or not recognized as belonging to the Local Zone or 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.

Zones and Neighbors

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 |
|--|---|--|
| Authentication policy | The Authentication policy setting controls how the Expressway challenges incoming messages to the Default Zone. | See Authentication Policy Configuration Options, page 136 for more information. |
| Media encryption mode | The Media encryption mode setting controls the media encryption capabilities for SIP calls flowing through the Default Zone. | See Configuring Media Encryption Policy, page 144 for more information. |
| ICE support | Controls whether ICE messages are supported by the devices in this zone. | See Configuring ICE Messaging Support, page 145 for more information. |
| Enable Mutual TLS on Default Zone | <p><i>On</i> enforces MTLS (Mutual Transport Layer Security) on incoming connections through the Default Zone.</p> <p><i>Off</i> means that MTLS is not enforced on connections to the TLS port. MTLS will still be enforced if the connections are made to the dedicated MTLS port - if that port is enabled on Configuration > Protocols > SIP.</p> <p>Default: <i>Off</i></p> | <p>This setting does not affect other connections to the Default Zone (H.323, SIP UDP, or SIP TCP).</p> <p>Note: The B2BUA is not capable of client certificate checks. Calls will fail if you engage the B2BUA when MTLS is configured on TLS port 5061. We recommend that you enable TLS and MTLS on different ports (on Protocols > SIP page).</p> <p>If you must use port 5061 for MTLS, then you should avoid engaging the B2BUA - by switching Media encryption mode to <i>Auto</i> on all zones in the call path.</p> |

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

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

For each rule, you specify a pattern to compare against the CN (and any SANs) in the certificates received from external systems. You can then choose whether to allow or deny access to systems that present matching certificates. Up to 10,000 rules can be configured.

Table 12 Default Zone Access Rule Parameters

| Field | Description | Usage tips |
|--------------------|--|------------|
| Name | The name assigned to the rule. | |
| Description | An optional free-form description of the rule. | |

Table 12 Default Zone Access Rule Parameters (continued)

| Field | Description | Usage tips |
|-----------------------|--|--|
| Priority | 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. | |
| Pattern type | The way in which the Pattern string must match the Subject Common Name or any Subject Alternative Names contained within the certificate. <i>Exact:</i> the entire string must exactly match the name, character for character. <i>Prefix:</i> the string must appear at the beginning of the name. <i>Suffix:</i> the string must appear at the end of the name. <i>Regex:</i> treats the string as a regular expression . | You can test whether a pattern matches a particular name by using the Check pattern tool (Maintenance > Tools > Check pattern). |
| Pattern string | The pattern against which the name is compared. | |
| Action | The action to take if the certificate matches this access rule. <i>Allow:</i> allows the external system to connect via the Default Zone. <i>Deny:</i> rejects any connection requests received from the external system. | |
| State | 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. |

Zone List

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.

For each zone in the list, the columns show information about the number of calls, bandwidth used, number of proxied registrations, protocol status, and search rule status.

The H.323 or SIP status options are:

- *Off:* the protocol is disabled at either the zone or system level
- *Active:* the protocol is enabled for the 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:* indicates that the protocol is enabled for the zone (for zone types that do not have active connections, eg. DNS and ENUM zones)
- *Failed:* the protocol is enabled for the zone but its connection has failed
- *Checking:* the protocol is enabled for the zone and the system is currently trying to establish a connection

Zones and Neighbors

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 unregistered or not recognized as belonging to the Local Zone or 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 VCS or Expressway), 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 |
|-------------------------------|---|------------|
| Configuration section: | | |
| Name | The name acts as a unique identifier, allowing you to distinguish between zones of the same type. | |

Zones and Neighbors

| Field | Description | Usage tips |
|-------------------------------------|--|--|
| Type | The nature of the specified zone, in relation to the local Expressway. Select <i>Neighbor</i> . | After a zone has been created, the Type cannot be changed. |
| Hop count | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the Hop counts 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. |
| H.323 section: | | |
| Mode | Determines whether H.323 calls are allowed to and from the neighbor system. | |
| Port | 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. |
| SIP section: | | |
| Mode | Determines whether SIP calls are allowed to and from the neighbor system. | |
| Port | 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 Transport mode is in use). |
| Transport | Determines which transport type is used for SIP calls to and from the neighbor system. The default is <i>TLS</i> . | |
| TLS verify mode | 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 TLS Certificate Verification of Neighbor Systems, page 168 for more information. |
| Accept proxied registrations | Controls whether proxied SIP registrations routed through this zone are accepted. | This setting only applies to registration requests for a domain for which the Expressway is acting as a Registrar. For requests for other domains the SIP registration proxy mode setting applies. See Proxying registration requests for more information. |
| Media encryption mode | Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. | See Configuring Media Encryption Policy, page 144 for more information. |
| ICE support | Controls whether ICE messages are supported by the devices in this zone. | See Configuring ICE Messaging Support, page 145 for more information. |

Zones and Neighbors

| Field | Description | Usage tips |
|--------------------------------------|--|---|
| Multistream mode | <p>Controls whether the Expressway B2BUA allows multistream calls to be negotiated between calling parties.</p> <p><i>On:</i> Expressway allows the calling parties to negotiate and set up a multistream call through this zone</p> <p><i>Off:</i> Expressway rejects multistream negotiation through this zone. The calling parties should fall back on negotiating a standard call.</p> | <p>This toggle has no effect on the call when the call does not traverse the B2BUA.</p> <p>The default is <i>On</i> because we expect calling parties to respond correctly to each other if they do not both have multistream capability. However, if you are having trouble with configuring multistream between the calling parties, you may wish to disable multistream mode to check if the calling parties can negotiate a standard call.</p> <p>In the case of a TelePresence Server, a standard call means that the TelePresence Server composes the streams from multiple participants into one 'conference stream' to send to the endpoint, instead of sending multiple streams to the endpoint to process in its own way.</p> |
| Preloaded SIP routes support | Switch Preloaded SIP routes support <i>On</i> to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support <i>Off</i> if you want the zone to reject SIP INVITE requests containing this header. | |
| AES GCM support | Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. | This is disabled by default. You should enable it if the calling parties are trying to negotiate AES GCM. |
| Authentication section: | | |
| Authentication policy | 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 Authentication Policy Configuration Options, page 136 for more information. |
| SIP authentication trust mode | Controls whether authenticated SIP messages (ones containing a P-Asserted-Identity header) from this zone are trusted without further challenge. | See SIP Authentication Trust, page 138 for more information. |
| Location section: | | |

Zones and Neighbors

| Field | Description | Usage tips |
|---------------------------------|---|---|
| Look up peers by | <p>Determines whether you look up peers by:</p> <ul style="list-style-type: none"> ■ <i>Address</i> (default) allows you to add up to six peers. When you click Save, the Expressway does the lookup for the addresses. ■ <i>Service record</i> produces a field to enter the Service Domain. When you click Save, the Expressway queries its DNS server for service records based on the domain you entered and the protocols and transports that are enabled on the zone. | <p>When using <i>Service record</i>, there are four possible service lookups, given as example.com, they are:</p> <ul style="list-style-type: none"> ■ <code>_sip._udp.example.com</code>. SIP over UDP (this is disabled on Expressway and its zones by default) ■ <code>_sip._tcp.example.com</code>. SIP over TCP ■ <code>_sips._tcp.example.com</code>. SIP over TLS (secure SIP) ■ <code>_h323._udp.example.com</code>. H.323 over UDP (other transports have never been supported for H.323) <p>When you next visit the zone page, the status is reported where the peer addresses are shown. It shows the protocol (SIP, SIPS, H323), whether the peer is reachable and the peer address followed by the port.</p> <p>Note: If you use look up by DNS server be aware that your zones will communicate over the SRV record specified port and not the zone port—you will therefore need to keep the DNS specified port open on your firewall.</p> |
| Peer 1 to Peer 6 address | <p>The IP address or FQDN of the neighbor system.</p> <p>Enter the addresses of additional peers if:</p> <ul style="list-style-type: none"> ■ the neighbor is an Expressway cluster, in which case you must specify all of the peers in the cluster ■ 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 | <p>Calls to an Expressway cluster are routed to whichever peer in that neighboring cluster has the lowest resource usage. See Neighboring Between Expressway Clusters, page 178 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> |
| Advanced section: | | |

Zones and Neighbors

| Field | Description | Usage tips |
|---------------------|---|---|
| Zone profile | <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"> ■ <i>Cisco Unified Communications Manager</i> ■ <i>Cisco Unified Communications Manager (8.6.1 or 8.6.2)</i> ■ <i>Cisco Unified Communications Manager (9.x or later)</i> ■ <i>Nortel Communication Server 1000</i> ■ <i>Infrastructure device</i> (typically used for non-gatekeeper devices such as an MCU) | <p>See Zone Configuration: Advanced Settings, page 163 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 Cisco Unified Communications Manager with Expressway Deployment Guide 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, page 49](#).

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

The configurable options for a traversal client zone are:

| Field | Description | Usage tips |
|-------------------------------|---|------------|
| Configuration section: | | |
| Name | The name acts as a unique identifier, allowing you to distinguish between zones of the same type. | |

Zones and Neighbors

| Field | Description | Usage tips |
|--|--|--|
| Type | The nature of the specified zone, in relation to the local Expressway. Select <i>Traversal client</i> . | After a zone has been created, the Type cannot be changed. |
| Hop count | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the Hop counts 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. |
| Connection credentials section: | | |
| Username and Password | Traversal clients must always authenticate with traversal servers by providing their authentication credentials. Each traversal client zone must specify a Username and Password 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. |
| H.323 section: | | |
| Mode | Determines whether H.323 calls are allowed to and from the traversal server. | |
| Protocol | 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 Configuring Ports for Firewall Traversal , page 53 for more information. |
| Port | 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. |
| SIP section: | | |
| Mode | Determines whether SIP calls are allowed to and from the traversal server. | |
| Port | The port on the traversal server to use for SIP calls to and from the Expressway. 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. |
| Transport | Determines which transport type is used for SIP calls to and from the traversal server. The default is <i>TLS</i> . | |
| TLS verify mode | Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal server when communicating over TLS. | See TLS Certificate Verification of Neighbor Systems , page 168 for more information. |
| Accept proxied registrations | Controls whether proxied SIP registrations routed through this zone are accepted. | This setting only applies to registration requests for a domain for which the Expressway is acting as a Registrar. For requests for other domains the SIP registration proxy mode setting applies. See Proxying registration requests for more information. |

Zones and Neighbors

| Field | Description | Usage tips |
|-------------------------------------|---|--|
| Media encryption mode | Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. | See Configuring Media Encryption Policy, page 144 for more information. |
| ICE support | Controls whether ICE messages are supported by the devices in this zone. | See Configuring ICE Messaging Support, page 145 for more information. |
| Multistream mode | Controls whether the Expressway B2BUA allows multistream calls to be negotiated between calling parties. <i>On:</i> Expressway allows the calling parties to negotiate and set up a multistream call through this zone <i>Off:</i> Expressway rejects multistream negotiation through this zone. The calling parties should fall back on negotiating a standard call. | This toggle has no effect on the call when the call does not traverse the B2BUA. The default is <i>On</i> because we expect calling parties to respond correctly to each other if they do not both have multistream capability. However, if you are having trouble with configuring multistream between the calling parties, you may wish to disable multistream mode to check if the calling parties can negotiate a standard call. In the case of a TelePresence Server, a standard call means that the TelePresence Server composes the streams from multiple participants into one 'conference stream' to send to the endpoint, instead of sending multiple streams to the endpoint to process in its own way. |
| SIP poison mode | 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. | |
| Preloaded SIP routes support | Switch Preloaded SIP routes support <i>On</i> to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support <i>Off</i> if you want the zone to reject SIP INVITE requests containing this header. | |
| SIP parameter preservation | Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. | <i>On</i> preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. <i>Off</i> allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: <i>Off</i> |
| AES GCM support | Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. | This is disabled by default. You should enable it if the calling parties are trying to negotiate AES GCM. |
| Authentication section: | | |

Zones and Neighbors

| Field | Description | Usage tips |
|---------------------------------|--|--|
| Authentication policy | 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 Authentication Policy Configuration Options , page 136 for more information. |
| Client settings section: | | |
| Retry interval | The interval in seconds with which a failed attempt to establish a connection to the traversal server should be retried. | |
| Location section: | | |
| Peer 1 to Peer 6 address | The IP address or FQDN of the traversal server. If the traversal server is an Expressway-E cluster, this should include all of its peers. | See Neighboring Between Expressway Clusters , page 178 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](#), page 52. For full details on how traversal client zones and traversal server zones work together to achieve firewall traversal, see [About Firewall Traversal](#), page 49.

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 13 Traversal server zone configuration reference

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

Table 13 Traversal server zone configuration reference (continued)

| Field | Description | Usage tips |
|--|--|---|
| Hop count | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the Hop counts 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. |
| Connection credentials section: | | |
| Username | Traversal clients must always authenticate with traversal servers by providing their authentication credentials. The authentication username is the name that the traversal client must provide to the Expressway-E. (It is configured as the connection credentials Username in its traversal client zone.) | 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 Local authentication database page. Either: <ul style="list-style-type: none"> ■ click on the Add/Edit local authentication database link ■ go to Configuration > Authentication > Local database |
| H.323 section: | | |
| Mode | Determines whether H.323 calls are allowed to and from the traversal client. | |
| Protocol | Determines the protocol (<i>Assent</i> or <i>H.460.18</i>) to use to traverse the firewall/NAT. | See Configuring Ports for Firewall Traversal , page 53 for more information. |
| Port | The port on the local Expressway-E to use for H.323 calls to and from the traversal client. | |
| H.460.19 demultiplexing mode | Determines whether or not the same two ports are used for media by two or more calls. <i>On</i> : all calls from the traversal client use the same two ports for media. <i>Off</i> : each call from the traversal client uses a separate pair of ports for media. | |
| SIP section: | | |
| Mode | Determines whether SIP calls are allowed to and from the traversal client. | |
| Port | 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). |
| Transport | Determines which transport type is used for SIP calls to and from the traversal client. The default is <i>TLS</i> . | |

Table 13 Traversal server zone configuration reference (continued)

| Field | Description | Usage tips |
|---|---|--|
| Unified Communications services | 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 TLS verify mode enabled. This setting only applies when Unified Communications mode is set to <i>Mobile and remote access</i> . |
| TLS verify mode and subject name | Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If TLS verify mode is enabled, a TLS verify subject name 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 TLS verify subject name must be the FQDN of the cluster. See TLS Certificate Verification of Neighbor Systems, page 168 for more information. |
| Media encryption mode | Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. | See Configuring Media Encryption Policy, page 144 for more information. |
| ICE support | Controls whether ICE messages are supported by the devices in this zone. | See Configuring ICE Messaging Support, page 145 for more information. |
| Multistream mode | Controls whether the Expressway B2BUA allows multistream calls to be negotiated between calling parties. <i>On</i> : Expressway allows the calling parties to negotiate and set up a multistream call through this zone <i>Off</i> : Expressway rejects multistream negotiation through this zone. The calling parties should fall back on negotiating a standard call. | This toggle has no effect on the call when the call does not traverse the B2BUA. The default is <i>On</i> because we expect calling parties to respond correctly to each other if they do not both have multistream capability. However, if you are having trouble with configuring multistream between the calling parties, you may wish to disable multistream mode to check if the calling parties can negotiate a standard call. In the case of a TelePresence Server, a standard call means that the TelePresence Server composes the streams from multiple participants into one 'conference stream' to send to the endpoint, instead of sending multiple streams to the endpoint to process in its own way. |
| Poison mode | 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. | |
| Preloaded SIP routes support | Switch Preloaded SIP routes support <i>On</i> to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support <i>Off</i> if you want the zone to reject SIP INVITE requests containing this header. | |

Table 13 Traversal server zone configuration reference (continued)

| Field | Description | Usage tips |
|-----------------------------------|--|---|
| SIP parameter preservation | Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. | <p><i>On</i> preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA.</p> <p><i>Off</i> allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary.</p> <p>Default: <i>Off</i></p> |
| AES GCM support | Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. | This is disabled by default. You should enable it if the calling parties are trying to negotiate AES GCM. |
| Authentication section: | | |
| Authentication policy | 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 Authentication Policy Configuration Options, page 136 for more information. |
| UDP / TCP probes section: | | |
| UDP retry interval | 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. |
| UDP retry count | The number of times the client attempts to send a UDP probe to the Expressway-E during call setup. | |
| UDP keep alive interval | 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. | |
| TCP retry interval | 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. | |
| TCP retry count | The number of times the client attempts to send a TCP probe to the Expressway-E during call setup. | |
| TCP keep alive interval | 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. | |

Zones and Neighbors

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, page 216](#) section.

The configurable options for an ENUM zone are:

| Field | Description | Usage tips |
|-------------------|--|---|
| Name | The name acts as a unique identifier, allowing you to distinguish between zones of the same type. | |
| Type | The nature of the specified zone, in relation to the local Expressway. Select <i>ENUM</i> . | After a zone has been created, the Type cannot be changed. |
| Hop count | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the Hop counts 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. |
| DNS suffix | The domain to be appended to the transformed E.164 number to create an ENUM domain for which this zone is queried. | |
| H.323 mode | Determines whether H.323 records are looked up for this zone. | |
| SIP mode | 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

See [About URI Dialing, page 210](#) for more information on configuring and using DNS zones.

The configurable options for a DNS zone are:

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

Zones and Neighbors

| Field | Description | Usage tips |
|---|--|--|
| Hop count | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the Hop counts 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. |
| H.323 Section | | |
| H.323 mode | Determines whether H.323 calls are allowed to systems and endpoints located using DNS lookups via this zone. | |
| SIP Section | | |
| SIP mode | Determines whether SIP calls are allowed to systems and endpoints located using DNS lookups via this zone. | |
| TLS verify mode and subject name | Controls whether the Expressway performs X.509 certificate checking against the destination system server returned by the DNS lookup. If TLS verify mode is enabled, a TLS verify subject name 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. See TLS Certificate Verification of Neighbor Systems, page 168 for more information. |
| TLS verify subject name | 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). | |
| TLS verify inbound mapping | Switch Inbound TLS mapping <i>On</i> to map inbound TLS connections to this zone if the peer certificate contains the TLS verify subject name. If the received certificate does not contain the TLS verify subject name (as Common Name or Subject Alternative Name) then the connection is not mapped to this zone. | Switch Inbound TLS mapping <i>Off</i> to prevent the Expressway from attempting to map inbound TLS connections to this zone. |
| Fallback transport protocol | 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. The default is <i>UDP</i> (if enabled). | |
| Media encryption mode | Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to the internet. | See Configuring Media Encryption Policy, page 144 for more information. |
| ICE support | Controls whether ICE messages are supported by the devices in this zone. | See Configuring ICE Messaging Support, page 145 for more information. |
| Preloaded SIP routes support | Switch Preloaded SIP routes support <i>On</i> to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support <i>Off</i> if you want the zone to reject SIP INVITE requests containing this header. | |

Zones and Neighbors

| Field | Description | Usage tips |
|--------------------------------------|---|---|
| Modify DNS request | Routes outbound SIP calls from this zone to a manually specified SIP domain instead of the domain in the dialed destination. | This option is primarily intended for use with Call Service Connect. See www.cisco.com/go/hybrid-services . |
| Domain to search for | Enter a fully qualified domain name to find in DNS instead of searching for the domain on the outbound SIP URI. The original SIP URI is not affected. | |
| AES GCM support | Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. | This is disabled by default. You should enable it if the calling parties are trying to negotiate AES GCM. |
| Authentication Section | | |
| SIP authentication trust mode | <p>Used in conjunction with the Authentication Policy to control whether pre-authenticated SIP messages (ones containing a P-Asserted-Identity header) received from this zone are trusted and are subsequently treated as authenticated or unauthenticated within the Expressway.</p> <p><i>On:</i> 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 <i>Check credentials</i>.</p> <p><i>Off:</i> 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 <i>Check credentials</i>.</p> | For a DNS zone, you should always set Authentication policy to treated as authenticated. |
| Advanced Section | | |
| Include address record | <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> (default) the Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.</p> | |

Zones and Neighbors

| Field | Description | Usage tips |
|---------------------|--|---|
| Zone profile | <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>See Zone Configuration: Advanced Settings, page 163 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> |

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 |
|-----------------------------------|--|---------|------------|
| Include address record | <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 |
| Monitor peer status | <p>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.</p> | Yes | Neighbor |
| Call signaling routed mode | <p>Specifies how the Expressway handles the signaling for calls to and from this neighbor.</p> <p><i>Auto:</i> signaling is taken as determined by the Call signaling optimization (Configuration > Call routing) configuration.</p> <p><i>Always:</i> signaling is always taken for calls to or from this neighbor, regardless of the Call signaling optimization configuration.</p> <p>Calls via traversal zones or the B2BUA always take the signaling.</p> | Auto | Neighbor |

Zones and Neighbors

| Setting | Description | Default | Zone types |
|--|--|---------|-----------------|
| Automatically respond to H.323 searches | <p>Determines what happens when the Expressway receives an H.323 search, destined for this zone.</p> <p><i>Off:</i> an LRQ message is sent to the zone.</p> <p><i>On:</i> searches are responded to automatically, without being forwarded to the zone.</p> | Off | Neighbor |
| Automatically respond to SIP searches | <p>Determines what happens when the Expressway receives a SIP search that originated as an H.323 search.</p> <p><i>Off:</i> a SIP OPTIONS or SIP INFO message is sent.</p> <p><i>On:</i> searches are responded to automatically, without being forwarded.</p> <p>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.</p> | Off | Neighbor DNS |
| Send empty INVITE for interworked calls | <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 DNS |

Zones and Neighbors

| Setting | Description | Default | Zone types |
|--------------------------------------|---|---------|---|
| SIP parameter preservation | <p>Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone.</p> <p><i>On</i> preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA.</p> <p><i>Off</i> allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary.</p> <p>Default: <i>Off</i></p> | Off | Neighbor DNS UC Traversal Traversal Server Traversal Client |
| SIP poison mode | <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 Traversal client Traversal server DNS |
| SIP encryption mode | <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 |
| SIP REFER mode | <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 |
| SIP multipart MIME strip mode | <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 |
| SIP UPDATE strip mode | <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 |

Zones and Neighbors

| Setting | Description | Default | Zone types |
|--|--|---|-----------------|
| Interworking SIP search strategy | <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 |
| SIP UDP/BFCP filter mode | <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 DNS |
| SIP UDP/IX filter mode | <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 SIP UDP/IX filter mode is set to <i>On</i> for:</p> <ul style="list-style-type: none"> ■ business-to-business calls routed through neighbor zones that connect to external networks / non-Cisco infrastructure ■ calls that connect internally to Unified CM 8.x or earlier (use <i>Off</i> for 9.x or later) | <p>Off in Cisco Unified Communications Manager preconfigured zone profile.</p> <p>On otherwise.</p> | Neighbor DNS |
| SIP record route address type | <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 System host name (if it is blank the IP address is used instead).</p> | IP | Neighbor DNS |
| SIP Proxy-Require header strip list | <p>A comma-separated list of option tags to search for and remove from Proxy-Require headers in SIP requests received from this zone.</p> | None | Neighbor |

Zones and Neighbors

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 |
| 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 multipart MIME strip mode | Off | Off | Off | Off | Off |
| 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 | Off | On | On | On | On |
| SIP record route address type | IP | IP | IP | IP | IP |

Zones and Neighbors

| Setting | Cisco Unified Communications Manager | Cisco Unified Communications Manager (8.6.1 or later) | Nortel Communication Server 1000 | Infrastructure device | Default |
|-------------------------------------|--------------------------------------|---|----------------------------------|-----------------------|---------|
| 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, page 278](#) 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.

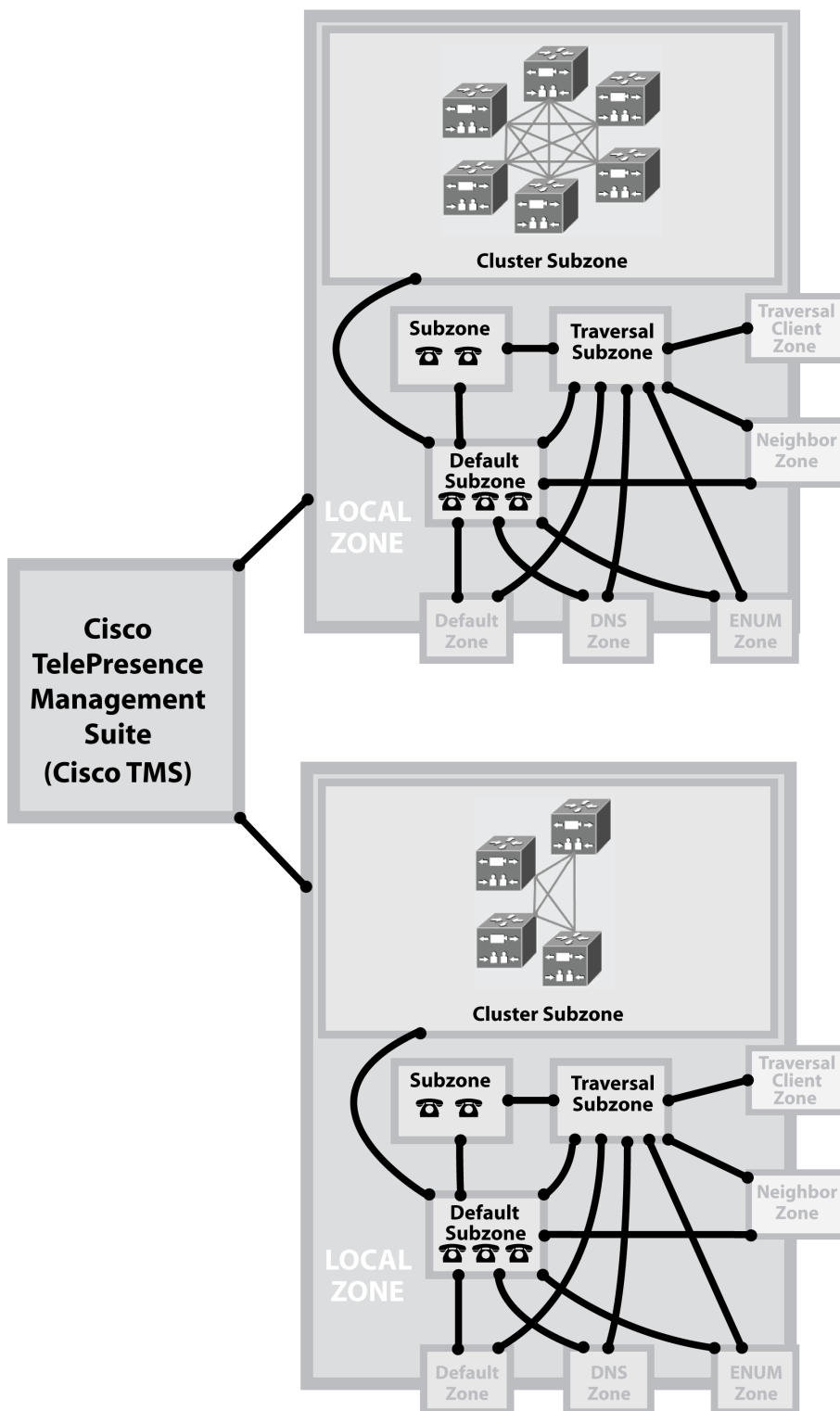
| | |
|--|-----|
| About Clusters | 169 |
| License Usage Within a Cluster | 171 |
| Managing Clusters and Peers | 173 |
| Troubleshooting Cluster Replication Problems | 179 |

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 primary 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).

Peers share information with each other about their use of bandwidth, registrations, and user accounts. This allows the cluster to act as one large Expressway Local Zone as shown in the example below.



About the configuration primary

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

Clustering and Peers

primary. Any configuration changes made to the primary peer are then automatically replicated across all the other peers in the cluster.

You should only make configuration changes on the primary Expressway.

Caution: Do not adjust any cluster-wide configuration until the cluster is stable with all peers running. Cluster database replication will be negatively impacted if any peers are upgrading, restarting, or out of service when you change the cluster's configuration.

Any changes made on other peers are not reflected across the cluster, and will be overwritten the next time the primary'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 TLS (Transport Layer Security) to secure the communications between cluster peers. Peers identify each other using certificates; if you wish to enforce TLS verification, a Expressway must have a certificate that is trusted by all other peers, or it will be unable to join the cluster.

DNS resolution of peers

If you want to enforce TLS verification between peers, the peers must be able to resolve each others' FQDNs, as read from their certificates.

Prior to X8.9.2, this required that peers resolve each others' IP addresses using DNS. However, this causes an issue when creating a cluster of Cisco Expressway-E peers in an isolated network like a DMZ. In this case, typically, the peers can't reach your internal DNS servers, and it's undesirable to put (private) clustering IP addresses into the public DNS. Not being able to use IP addresses as common names or subject alternate names on server certificates compounds the issue.

From X8.9.2 onwards, you can do FQDN clustering with enforced TLS verification using the internal cluster address mapping table. Public FQDNs are still used to define the cluster peers and are still found in their certificates. However, the internal mapping table is consulted - prior to the regular DNS - to resolve these into each cluster peers' (private) clustering IP addresses.

We recommend you form a cluster using FQDN and TLS authentication. To configure this: build up your cluster; firstly using IP addresses, then add the address mappings before changing to FQDNs. You can then enable TLS authentication.

For detailed steps, see the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide* for your version on the [Cisco Expressway Series configuration guides page](#).

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

You can cluster up to 6 Expressway systems to increase capacity by a maximum factor of 4.

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.

The maximum number of licenses that each Expressway system can use depends on the [type of appliance or VM](#):

Table 14 Maximum licenses that a peer can use

| | Small / Medium systems | Large [‡] / CE500/ CE1000 / CE1100 systems |
|-------------------------------------|------------------------|---|
| Rich media sessions | 150 [†] | 500 |
| Room / Desktop system registrations | 2500 | 5000 (2500 for MRA registrations) |
| TURN relays * | 1800 | 6000 |

[‡] From X8.10 onwards, the requirement to have a 10 Gbps NIC in order to achieve the scalability of a large system is removed. It is now possible to have the capacity of a large system with a 1 Gbps NIC subject to your bandwidth constraints.

[†] This is the maximum number of licenses the system can *use*. This limit specifically applies to the case where a peer becomes unavailable and the other peers must use that peer's licenses to honor the cluster's overall capacity. This is not intended as a production capacity limit, only as a temporary measure to allow the affected peer to be returned to normal service. **We strongly discourage installing more than 100 licenses on any platform that has small or medium capacity.**

* 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 see a summary of all of the call, registration, and TURN relay licenses installed on each cluster peer by going to the **Option keys** page and scrolling down to the **Current licenses** section.

Licenses Used in Intracluster Calls

This section describes the licenses used when endpoints are registered to different peers in the same cluster.

If the call media does not traverse the cluster peers:

- A call between the endpoints does not consume any RMS licenses; this is a "Registered" call.

If the call media traverses the cluster peers:

- A call between the endpoints consumes an RMS license on the Expressway where the B2BUA is engaged.

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

Example deployment

If, for example, you want to deploy a resilient cluster that can handle up to 750 concurrent desktop registrations and 250 Rich Media Sessions, you could configure 4 peers as follows:

| | Peer 1 | Peer 2 | Peer 3 | Peer 4 | Total cluster capacity |
|-------------------------------|--------|--------|--------|--------|------------------------|
| Desktop registration licenses | 250 | 250 | 250 | 0 | 750 |
| Rich Media Sessions | 100 | 100 | 50 | 0 | 250 |

It would not matter to which peer an endpoint registers as the licenses are shared across all of the peers. If any one of the peers is temporarily taken out of service the full set of call licenses will remain available to the entire cluster.

We recommend that, where possible, you distribute the licenses evenly across all peers in the cluster.

Managing Clusters and Peers

Setting Up a Cluster

Before you Start

1. Make sure that all prerequisites listed in the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide* for your version are complete (on the [Cisco Expressway Series configuration guides page](#)).
2. We recommend that you backup your Expressway data before setting up a cluster. Instructions are in the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide*.

Process

To create the cluster you must first configure a primary peer and then add the other peers into the cluster one at a time.

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 configuration primary peer.

Cluster configuration

- 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.
A cluster name is required if FindMe is enabled.
- All peers must agree on which is the **Configuration primary**. Use the same number on each peer, and keep the **Peer N address** list in the same order on all peers.
- All peers must use the same IP version. Set the **Cluster IP version** to the same value on all peers.
- All peers must use the same **TLS verification mode**. Choose *Enforce* for better security, but be aware that the peers must be able to verify each others' certificates against their trusted CAs.
- The **Cluster Address Mapping** option allows you to map Cisco Expressway-E peers' FQDNs to their private IP addresses. Cluster address mapping allows you to enforce TLS clustering of peers in an isolated network, because it does not require the use of the public DNS and the peers' public IP addresses.

Other configuration for the cluster

You should only make configuration changes on the primary Expressway.

Caution: Do not adjust any cluster-wide configuration until the cluster is stable with all peers running. Cluster database replication will be negatively impacted if any peers are upgrading, restarting, or out of service when you change the cluster's configuration.

Any changes made on other peers are not reflected across the cluster, and will be overwritten the next time the primary'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.

Clustering and Peers

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.
- 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 Primary Peer

You should only need to change the **Configuration primary** when:

- the original primary peer fails
- you want to take the primary Expressway unit out of service

Note that if the primary fails, the remaining peers will continue to function normally, except they are no longer able to copy their configuration from the primary so they may become out of sync with each other.

To change the primary peer you must log in to every other Expressway in the cluster and change the configuration primary on each peer:

1. Log in to the Expressway and go to **System > Clustering**.
2. Change the **Configuration primary** to the peer you want to set as the new primary (the numbers match against the **Peer N address** fields on the same page).
3. Click **Save**.
4. Repeat this for every peer in the cluster, ensuring that you select the same new primary on each peer.

Note: During this process you may see alarms raised on some peers about inconsistent primary peer configuration. These alarms will be lowered when every peer in the cluster is configured with the new primary.

Note: No additional steps are required if you are using FQDN's and have a valid cluster address mapping configured.

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.

Peer-Specific Items in Clustered Systems

Most items of configuration are applied via the primary 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 primary peer. At best it will result in the changes being overwritten from the primary; at worst it will cause cluster replication to fail.

Cluster configuration (System > Clustering)

The list of **Peer N addresses** (including the peer's own address) that make up the cluster has to be specified on each peer and they must be identical on each peer.

The **Cluster name**, **Configuration primary**, and **Cluster IP version** must be specified on each peer and must be identical for all peers.

Note: If you need to enable cluster address mapping, we recommend forming the cluster on IP addresses first. Then you will only need to add the mappings on one peer.

Clustering and 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)

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 that control features are specific to the peer where they are applied. Option keys that control licenses are pooled for use by the whole cluster.

Clustering and Peers

Each peer must have an identical set of feature option keys installed, which means you must purchase a key for each peer in the cluster.

License option keys can be applied to one or more peers in the cluster, and the sum of the installed licenses is available across the cluster. This license pooling behavior includes the following option keys:

- Expressway: Rich media sessions
- Expressway: Telepresence room systems
- Expressway: Desktop systems
- VCS: Traversal calls
- VCS: Non-traversal calls
- TURN relays

Note: In some cases a peer will raise an alarm that it has no key to enable licenses the peer needs, even though there are licenses available in the cluster. You can acknowledge and ignore this category of alarm, unless the only peer that has the required licenses is out of service.

Active Directory Service (Configuration > Authentication > Devices > Active Directory Service)

When configuring the connection to an Active Directory Service for device authentication, the **NetBIOS machine name (override)**, and domain administrator **Username** and **Password** are specific to each peer.

For VCS: Conference Factory template (Applications > Conference Factory)

The template used by the Conference Factory application to route calls to the MCU is peer-specific, as it must be unique for each peer in the cluster.

For VCS: Expressway front panel display mode (configurable through CLI only)

The `xConfiguration Administration LCDPanel Mode` CLI setting is specific to each peer.

Sharing Registrations Across Peers

When a cluster peer receives a search request (such as an INVITE), it checks its own and its peers' registration lists before responding. This allows all endpoints in the cluster to be treated as if they were registered with a single Expressway.

Peers are periodically queried to ensure they are still functioning.

H.323 registrations

All the peers in a cluster share responsibility for their H.323 endpoint community. When an H.323 endpoint registers with one peer, it receives a registration response which contains a list of alternate gatekeepers, populated with a randomly ordered list of the IP addresses of all the other peers in that cluster.

If the endpoint loses contact with the initial peer, it will seek to register with one of the other peers. The random ordering of the list of alternate peers ensures that endpoints that can only store a single alternate peer will failover evenly across the cluster.

When using a cluster, you may want to reduce the registration **Time to live** on all peers in the cluster from the default 30 minutes. This setting determines how often endpoints are *required* to re-register with their Expressway, and reducing it means that if a cluster peer is unavailable, the endpoint will failover more quickly to an available peer.

Note: By reducing the registration time to live too much, you risk flooding the Expressway with registration requests, which will severely impact performance. This impact is proportional to the number of endpoints, so you should balance the need for occasional quick failover against the need for continuous good performance.

To change this setting, go to **Configuration > Protocols > H.323 > Gatekeeper > Time to live**.

SIP registrations

The Expressway supports multiple client-initiated connections (also referred to as "SIP Outbound") as outlined in [RFC 5626](#).

Clustering and Peers

This allows SIP endpoints that support *RFC 5626* to be simultaneously registered to multiple Expressway cluster peers. This provides extra resiliency: if the endpoint loses its connection to one cluster peer it will still be able to receive calls via one of its other registration connections.

You can also use DNS round-robin techniques to implement a registration failover strategy. Some SIP UAs, such as Jabber Video, can be configured with a SIP server address that is an FQDN. If the FQDN resolves to a round-robin DNS record populated with the IP addresses of all the peers in the cluster, then this could allow the endpoint to re-register with another peer if its connection to the original peer is lost.

Sharing Bandwidth Across Peers

When clustering has been configured, all peers share the bandwidth available to the cluster.

- Peers must be configured identically for all aspects of bandwidth control including subzones, links and pipes.
- Peers share their bandwidth usage information with all other peers in the cluster, so when one peer is consuming part or all of the bandwidth available within or from a particular subzone, or on a particular pipe, this bandwidth will not be available for other peers.

For general information on how the Expressway manages bandwidth, see the [bandwidth control](#) section.

Cluster Upgrades, Backup and Restore

Upgrading a cluster

See the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide*, for your version, on the [Cisco Expressway Series configuration guides page](#).

Note: If you are upgrading to X8.8 or later from an earlier version, clustering communications changed in X8.8 to use TLS connections between peers instead of IPSec. TLS verification is not enforced (by default) after you upgrade, and you'll see an alarm reminding you to enforce TLS verification.

Backing up a cluster

Use the [backup and restore](#) process to save cluster configuration information. The backup process saves *all* configuration information for the cluster, regardless of the Expressway used to make the backup.

Caution: Do not take VMware snapshots of Cisco Expressway systems. The process interferes with database timing and negatively impacts performance.

Restoring a cluster

To restore previously backed up cluster configuration data, follow this process.

Important! You can't restore data to an Expressway that is part of a cluster. As described here, first remove the Expressway peer from the cluster. Then do the restore. (After the restore you need to build a new cluster.)

1. Remove the Expressway peer from the cluster so that it becomes a standalone Expressway.
2. Restore the configuration data to the standalone Expressway. See [Restoring a Previous Backup, page 300](#) for details.
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, page 173](#) for details.

Note: No additional steps are required if you are using FQDN's and have a valid cluster address mapping configured. Mappings will be configured on a restore action.

Clustering and Cisco TMS

Cisco TMS version 13.2 or later is mandatory if your cluster is configured to use FindMe or Device Provisioning.

Clustering and Peers

Size limitations for clusters and provisioning

An Expressway cluster of any size supports up to:

- 10,000 FindMe accounts
- 10,000 users for provisioning
- 200,000 phonebook entries

Note that:

- **Small/Medium** systems can support up to 2,500 device registrations per peer, subject to a maximum of 10,000 registrations per cluster. Typically this means one device per FindMe account.
- **Large** systems can support up to 5,000 device registrations per peer (with a maximum of 20,000 registrations per cluster). However, you are still limited to 10,000 FindMe accounts/users and 10,000 provisioned devices per cluster.

If you need to provision more than 10,000 devices, your network will require additional Expressway clusters with an appropriately designed and configured dial plan.

See the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide*, for your version, on the [Cisco Expressway Series configuration guides page](#).

About the Cluster Subzone

When two or more Expressways are clustered together, a new subzone is created within the cluster's Local Zone. This is the Cluster Subzone (see the diagram in the [About Clusters, page 169](#) section). Any calls between two peers in the cluster will briefly pass via this subzone during call setup.

The Cluster Subzone is (like the Traversal Subzone) a virtual subzone used for call routing only, and endpoints cannot register to this subzone. After a call has been established between two peers, the Cluster Subzone will no longer appear in the call route and the call will appear as having come from (or being routed to) the Default Subzone.

The two situations in which a call will pass via the Cluster Subzone are:

- Calls between two endpoints registered to different peers in the cluster.
For example, Endpoint A is registered in the Default Subzone to Peer 1. Endpoint B is also registered in the Default Subzone, but to Peer 2. When A calls B, the call route is shown on Peer 1 as **Default Subzone -> Cluster Subzone**, and on Peer 2 as **Cluster Subzone -> Default Subzone**.
- Calls received from outside the cluster by one peer, for an endpoint registered to another peer.
For example, we have a single Expressway for the Branch Office, which is neighbored to a cluster of 4 Expressways at the Head Office. A user in the Branch Office calls Endpoint A in the Head Office. Endpoint A is registered in the Default Subzone to Peer 1. The call is received by Peer 2, as it has the lowest resource usage at that moment. Peer 2 then searches for Endpoint A within the cluster's Local Zone, and finds that it is registered to Peer 1. Peer 2 then forwards the call to Peer 1, which forwards it to Endpoint A. In this case, on Peer 2 the call route will be shown as **Branch Office -> Default Subzone -> Cluster Subzone**, and on Peer 1 as **Cluster Subzone -> Default Subzone**.

Note that if **Call signaling optimization** is set to *On* and the call is H.323, the call will not appear on Peer 2, and on Peer 1 the route will be **Branch Office > Default Subzone**.

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:

- locally registered endpoints (if the endpoint is registered to that peer)
- peers (if the endpoint is registered to another peer in that cluster)

Clustering and Peers

- external zones (if the endpoint has been located elsewhere)

For Expressway: 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.

For VCS: Lowest resource usage is determined by comparing the number of available traversal calls (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 primary 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 FQDNs in these fields. Each FQDN must be different and must resolve to a single IP address for each peer. With IP addresses, you may not be able to use TLS verification, because many CAs will not supply certificates to authenticate an IP address.
- 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. For more detailed information:

See the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide*, for your version, on the [Cisco Expressway Series configuration guides page](#).

Some peers have a different primary peer defined

1. For each peer in the cluster, go to the **System > Clustering** page.
2. Ensure each peer identifies the same **Configuration primary**.

Unable to reach the cluster configuration primary peer

The Expressway operating as the primary peer could be unreachable for many reasons, including:

- Network access problems
- Expressway unit is powered down
- Incorrectly configured addresses

Clustering and Peers

- TLS verification mode is set to Enforce but some peers have invalid or revoked certificates
- Different software versions on peers
- DNS settings not correct in cluster

"Manual synchronization of configuration is required" alarms are raised on subordinate peer Expressways

1. Log in to the peer as **admin** through the CLI (available by default over SSH and through the serial port on hardware versions).
2. Type `xCommand ForceConfigUpdate`.

This will delete the subordinate Expressway peer's configuration and force it to update its configuration from the primary Expressway.

Caution: Never issue this command on the primary Expressway because you will lose all configuration for the cluster.

Incorrect IP to FQDN mappings

1. Go to the **System > Clustering** page on any peer.
2. Check that all FQDN and IP addresses have been entered correctly.

Firewall preventing the cluster communicating

- If you intended to cluster using public IP addresses, make sure your firewall isn't preventing cluster communication by blocking the clustering communications ports. If it is, consider whether you can change your firewall rules.
- If you intended to cluster with private addresses, ensure you have configured your cluster as per our recommendations, i.e. form a cluster using FQDN with IP address mappings, and TLS authentication.



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 | 181 |
| Configuring Hop Counts | 184 |
| Configuring Dial Plan Settings | 184 |
| About Transforms and Search Rules | 185 |
| Example Searches and Transforms | 192 |
| Configuring Search Rules to Use an External Service | 201 |
| About Call Policy | 203 |
| Supported Address Formats | 208 |
| Dialing by IP Address | 209 |
| About URI Dialing | 210 |
| About ENUM Dialing | 216 |
| Configuring DNS Servers for ENUM and URI Dialing | 221 |
| Configuring Call Routing and Signaling | 221 |
| Identifying Calls | 222 |
| Disconnecting Calls | 223 |

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:

- locally registered endpoints
- 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.

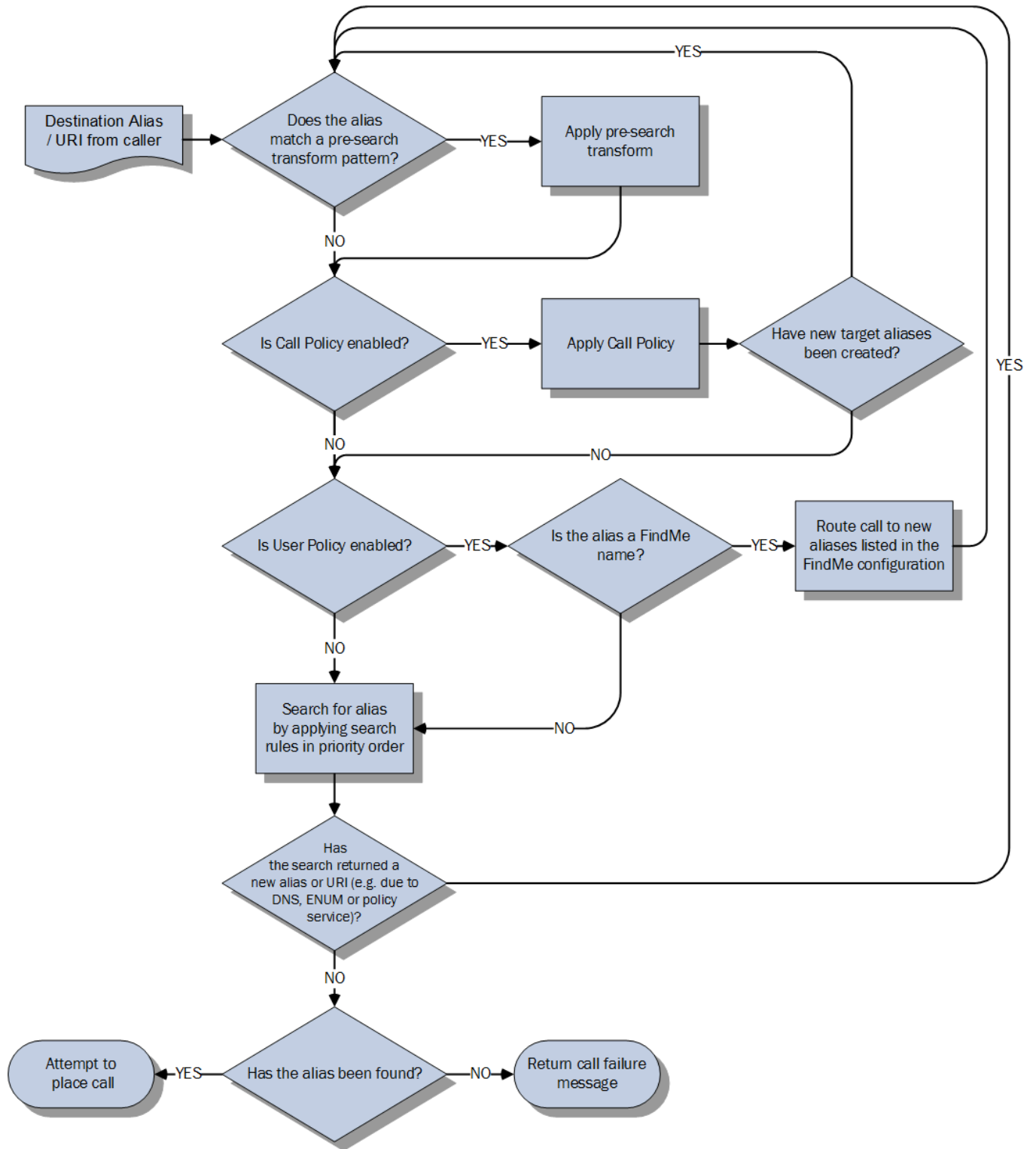
1. The caller enters into their endpoint the alias or address of the destination endpoint. This alias or address can be in a number of [different address formats](#).

Dial Plan and Call Processing

2. The destination address is received by the Expressway.
(The address comes to Expressway directly from a registered endpoint, or it may come indirectly as a result of other call processing infrastructure in your deployment)
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. Any User Policy (if **FindMe** is enabled) is applied to the alias. If the alias is a FindMe ID that resolves to one or more new target aliases, the process starts again with all the resulting aliases checked against pre-search transforms and Call Policy.
6. The Expressway then searches for the alias according to its search rules:

Note: The Expressway deliberately only searches for the first destination alias it reads from an H.323 Location Request. In very rare cases, this can lead to calls not being routed as expected.
 - 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:
 - **Local Zone:** the endpoints and devices registered to the Expressway.
 - **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.
7. 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 and User Policy are applied and a new Expressway search is performed.
8. If the alias is found within the Local Zone, in one of the external zones, or a routing destination is returned by the policy service, the Expressway attempts to place the call.
9. If the alias is not found, it responds with a message to say that the call has failed.

Figure 12 Call Routing Flowchart



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 [Zone List, page 148](#) 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 |
|--------------------------------------|--|---|
| Calls to unknown IP addresses | <p>Determines the way in which the Expressway attempts to call systems which are not registered with it or 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. The call setup would occur just as it would if the far end were registered directly to the local system.</p> <p><i>Indirect:</i> 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.</p> <p><i>Off:</i> endpoints registered directly to the Expressway may only call an IP address of a system also registered directly to that Expressway.</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, Call Policy or User Policy rules have been applied.</p> <p>In addition to controlling calls, this setting also determines the behavior of provisioning messages to SIP devices, as these messages are routed to IP addresses.</p> <p>See Dialing by IP Address, page 209 for more information.</p> |
| Fallback alias | <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.

Dial Plan and Call Processing

- **Pre-search transforms** are applied before any Call Policy or User Policy are applied and before the search process is performed (see [About Pre-Search Transforms, page 186](#) 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, page 188](#) for more details).

Search rules

Search rules are used to route incoming search requests to the appropriate target zones (including the Local Zone) 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 (such as the Local Zone, or a specific zone or subzone)
- set up rules that only match specific traffic types, for example standards-based SIP or Microsoft SIP
- 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](#)):

- If the request has come from a neighboring system and **Interworking mode** is set to *Registered only*, the Expressway searches the Local Zone using both protocols, and all other zones using the native protocol only (because it will interwork the call only if one of the endpoints is locally registered).
- If **Interworking mode** is set to *On*, or the request has come from a locally registered endpoint, the Expressway searches the Local Zone and all external zones using both protocols.

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 or User Policy is applied, and before any searches take place.

- It applies to all incoming search requests received from locally registered endpoints, 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 transforms are not applied to GRQ or RRQ messages received from endpoints registering with the Expressway; endpoints will be registered with the aliases as presented in these messages.
- All peers in a cluster should be configured identically, including any pre-search transforms. Each Expressway treats search requests from any of its peers as having come from its own Local Zone, and does not re-apply any pre-search transforms on receipt of the request.

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. This may be as a result of [Call Policy](#) (also known as Administrator Policy) or User Policy (if [FindMe](#) is enabled). 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 |
|-----------------------|---|---|
| Priority | 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. | |
| Description | 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. |
| Pattern type | How the Pattern string must match the alias for the rule to be applied. Options are: <i>Exact</i> : the entire string must exactly match the alias character for character. <i>Prefix</i> : the string must appear at the beginning of the alias. <i>Suffix</i> : the string must appear at the end of the alias. <i>Regex</i> : treats the string as a regular expression . | 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). |
| Pattern string | Specifies the pattern against which the alias is compared. | The Expressway has a set of predefined pattern matching variables that can be used to match against certain configuration elements. |

Dial Plan and Call Processing

| Field | Description | Usage tips |
|-------------------------|---|---|
| Pattern behavior | Specifies how the matched part of the alias is modified. Options are: <i>Strip</i> : the matching prefix or suffix is removed. <i>Replace</i> : the matching part of the alias is substituted with the text in the Replace string. <i>Add Prefix</i> : prepends the Additional text to the alias. <i>Add Suffix</i> : appends the Additional text to the alias. | |
| Replace string | The string to substitute for the part of the alias that matches the pattern. | Only applies if the Pattern behavior is <i>Replace</i> . You can use regular expressions. |
| Additional text | The string to add as a prefix or suffix. | Only applies if the Pattern behavior is <i>Add Prefix</i> or <i>Add Suffix</i> . |
| State | Indicates if the transform 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 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](#), [Call Policy](#) and [User 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, page 181](#) starts again

Dial Plan and Call Processing

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 |
|--------------------|--|--|
| Rule name | A descriptive name for the search rule. | |
| Description | 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. |
| Priority | 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. |
| Protocol | The source protocol for which the rule applies. The options are <i>Any</i> , <i>H.323</i> or <i>SIP</i> . | |

Dial Plan and Call Processing

| Field | Description | Usage tips |
|--------------------------------------|--|---|
| Traffic type | <p>The source traffic type for which this rule applies. Options are:</p> <p><i>Any</i>: The rule does not inspect the traffic type</p> <p><i>Standard</i>: The rule applies if the traffic is standards-based SIP</p> <p><i>Any Microsoft</i>: The rule applies if the traffic is Microsoft SIP or Microsoft SIP-SIMPLE</p> <p><i>Microsoft SIP</i>: The rule applies if the traffic is Microsoft SIP</p> <p><i>Microsoft IM and Presence</i>: The rule applies if the traffic is Microsoft SIP-SIMPLE</p> | <p>This option helps you route different types of calls to the infrastructure most suited to processing them.</p> <p>For example, you could use two search rules to route Standard SIP towards a Unified CM neighbor zone and route Any Microsoft towards a Cisco Meeting Server neighbor zone.</p> |
| Source | <p>The sources of the requests for which this rule applies.</p> <p><i>Any</i>: locally registered devices, neighbor or traversal zones, and any non-registered devices.</p> <p><i>All zones</i>: locally registered devices plus neighbor or traversal zones.</p> <p><i>Local Zone</i>: locally registered devices only.</p> <p><i>Named</i>: a specific source zone or subzone for which the rule applies.</p> | <p>Named sources creates the ability for search rules to be applied as dial plan policy for specific subzones and zones.</p> |
| Source name | <p>The specific source zone or subzone for which the rule applies. Choose from the Default Zone, Default Subzone or any other configured zone or subzone.</p> | <p>Only applies if the Source is set to <i>Named</i>.</p> |
| Request must be authenticated | <p>Specifies whether the search rule applies only to authenticated search requests.</p> | <p>This can be used in conjunction with the Expressway's Authentication Policy to limit the set of services available to unauthenticated devices.</p> |
| Mode | <p>The method used to test if the alias applies to the search rule.</p> <p><i>Alias pattern match</i>: the alias must match the specified Pattern type and Pattern string.</p> <p><i>Any alias</i>: any alias (providing it is not an IP address) is allowed.</p> <p><i>Any IP Address</i>: the alias must be an IP address.</p> | |

| Field | Description | Usage tips |
|----------------------------|---|--|
| Pattern type | How the Pattern string must match the alias for the rule to be applied. Options are: <i>Exact</i> : the entire string must exactly match the alias character for character. <i>Prefix</i> : the string must appear at the beginning of the alias. <i>Suffix</i> : the string must appear at the end of the alias. <i>Regex</i> : treats the string as a regular expression . | Applies only if the Mode is <i>Alias Pattern Match</i> . 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). |
| Pattern string | The pattern against which the alias is compared. | Applies only if the Mode is <i>Alias Pattern Match</i> . The Expressway has a set of predefined pattern matching variables that can be used to match against certain configuration elements. |
| Pattern behavior | Determines whether the matched part of the alias is modified before being sent to the target zone or policy service <i>Leave</i> : the alias is not modified. <i>Strip</i> : the matching prefix or suffix is removed from the alias. <i>Replace</i> : the matching part of the alias is substituted with the text in the Replace string . | Applies only if the Mode is <i>Alias Pattern Match</i> . If you want to transform the alias before applying search rules you must use pre-search transforms . |
| Replace string | The string to substitute for the part of the alias that matches the pattern. | Only applies if the Pattern behavior is <i>Replace</i> . You can use regular expressions. |
| On successful match | Controls the ongoing search behavior if the alias matches the search rule. <i>Continue</i> : continue applying the remaining search rules (in priority order) until the endpoint identified by the alias is found. <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. |
| Target | The zone or policy service to query if the alias matches the search rule. | You can configure external policy services 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. |
| State | 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](#)
- [Stripping the domain from an alias to allow dialing from SIP to H.323 numbers](#)
- [Stripping the domain from an alias to allow dialing from SIP to H.323 IDs](#)
- [Allow calls to IP addresses only if they come from known zones](#)
- [Forward Microsoft SIP Calls to Cisco Meeting Server](#)

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 |

Dial Plan and Call Processing

| Field | Value |
|---------------------|---------------------|
| Mode | Alias pattern match |
| Pattern type | Suffix |
| Pattern string | @sales.example.com |
| Pattern behavior | Leave |
| On successful match | Stop |
| 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 |

Dial Plan and Call Processing

| Field | Value |
|-------------------------------|---------------------|
| Request must be authenticated | No |
| Mode | Alias pattern match |
| 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 |

Dial Plan and Call Processing

| Field | Value |
|-------------------------------|---------------------|
| Source | Any |
| 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 |

Dial Plan and Call Processing

| 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 |

Stripping @domain for Dialing to H.323 Numbers

SIP endpoints can only make calls in the form of URIs - for example `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 registered as 123, the Expressway will be unable to locate the alias `123@domain` and the call will fail.

If you have a deployment that includes both SIP and H.323 endpoints that register using a number, you will need to set up the following [pre-search transform](#) and [local zone search rules](#). Together these will let users place calls from both SIP and H.323 endpoints to H.323 endpoints registered using their H.323 E.164 number only.

Pre-Search Transform

On the **Create transforms** page (**Configuration > Dial plan > Transforms > New**):

| Field | Value |
|----------------|---|
| Priority | 1 |
| Description | Take any number-only dial string and append @domain |
| Pattern type | Regex |
| Pattern string | (\d+) |

Dial Plan and Call Processing

| Field | Value |
|------------------|-----------|
| Pattern behavior | Replace |
| Replace string | \1@domain |
| State | Enabled |

This pre-search transform takes any number-only dial string (such as 123) and appends the domain used in endpoint AORs and URIs in your deployment. This ensures that calls made by SIP and H.323 endpoints result in the same URI.

Local Zone Search Rules

On the **Create search rule** page (**Configuration > Dial plan > Search rules > New**), create two new search rules as follows:

Rule #1

| Field | Value |
|-------------------------------|---|
| Rule name | Dialing H.323 numbers |
| Description | Transform aliases in format number@domain to number |
| Priority | 50 |
| Source | Any |
| Request must be authenticated | No |
| Mode | Alias pattern match |
| Pattern type | Regex |
| Pattern string | (\d+)@domain |
| Pattern behavior | Replace |
| Replace string | \1 |
| On successful match | Continue |
| Target zone | Local Zone |
| State | Enabled |

Rule #2

| Field | Value |
|-------------------------------|--|
| Rule name | Dialing H.323 numbers |
| Description | Place calls to number@domain with no alias transform |
| Priority | 60 |
| Source | Any |
| Request must be authenticated | No |
| Mode | Alias pattern match |

Dial Plan and Call Processing

| Field | Value |
|---------------------|--------------|
| Pattern type | Regex |
| Pattern string | (\d+)@domain |
| Pattern behavior | Leave |
| On successful match | Continue |
| Target zone | Local Zone |
| State | Enabled |

These search rules ensure that both the E.164 number and full URI are searched for, so that endpoints can still be reached whether they have registered with an H.323 number (123) or a full URI (123@domain).

- The first search rule takes any aliases in the format `number@domain` and transforms them into the format `number`.
- To ensure that any endpoints that have actually registered with an alias in the format `number@domain` can also still be reached, the lower-priority second search rule places calls to `number@domain` without transforming the alias.

Transforms for Alphanumeric H.323 ID Dial Strings

This example builds on the [Stripping @domain for dialing to H.323 numbers](#) example. That example caters for number-only dial strings, however H.323 IDs do not have to be purely numeric; they can contain alphanumeric (letters and digits) characters.

This example follows the same model as the example mentioned above – a [pre-search transform](#) and two [local zone search rules](#) to ensure that endpoints can be reached whether they have registered with an H.323 ID or a full URI – but uses a different regex (regular expression) that supports alphanumeric characters.

Pre-Search Transform

On the **Create transforms** page (**Configuration > Dial plan > Transforms > New**):

| Field | Value |
|------------------|--|
| Priority | 1 |
| Description | Append @domain to any alphanumeric dial string |
| Pattern type | Regex |
| Pattern string | ([^\@]*) |
| Pattern behavior | Replace |
| Replace string | \1@domain |
| State | Enabled |

This pre-search transform takes any alphanumeric dial string (such as 123abc) and appends the domain used in your deployment to ensure that calls made by SIP and H.323 endpoints result in the same URI.

Local Zone Search Rules

On the **Create search rule** page (**Configuration > Dial plan > Search rules > New**), create two new search rules as follows:

Rule #1

Dial Plan and Call Processing

| Field | Value |
|-------------------------------|---|
| Rule name | Dialing H.323 strings |
| Description | Transform aliases in format string@domain to string |
| Priority | 40 |
| Source | Any |
| Request must be authenticated | No |
| Mode | Alias pattern match |
| Pattern type | Regex |
| Pattern string | (.+@domain |
| Pattern behavior | Replace |
| Replace string | \1 |
| On successful match | Continue |
| Target zone | Local Zone |
| State | Enabled |

Rule #2

| Field | Value |
|-------------------------------|--|
| Rule name | Dialing H.323 strings with domain |
| Description | Place calls to string@domain with no alias transform |
| Priority | 50 |
| Source | Any |
| Request must be authenticated | No |
| Mode | Alias pattern match |
| Pattern type | Regex |
| Pattern string | (.+@domain |
| Pattern behavior | Leave |
| On successful match | Continue |
| Target zone | Local Zone |
| State | Enabled |

These search rules ensure that both the E.164 number and full URI are searched for, so that endpoints can still be reached whether they have registered with an H.323 ID (123abc) or a full URI (123abc@domain).

- The first search rule takes any aliases in the format `string@domain` and transforms them into the format `string`.
- To ensure that any endpoints that have actually registered with an alias in the format `string@domain` can also still be reached, the lower-priority second search rule places calls to `string@domain` without transforming the alias.

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 |
| Request must be authenticated | No |
| Mode | Any IP address |
| On successful match | Continue |
| Target zone | Overseas office |
| State | Enabled |

Forward Microsoft SIP Calls to Cisco Meeting Server

If you are using Cisco Meeting Server to enable Microsoft users to meet in spaces, you could forward any incoming calls of this type towards your Meeting Server neighbor zone with a search rule like this:

| Field | Value |
|-------------------------------|---|
| Rule name | Route all to Meeting Server |
| Description | Send all inbound MS traffic to Meeting Server |
| Priority | 100 |
| Protocol | SIP |
| Traffic type | Any Microsoft |
| Source | Any |
| Request must be authenticated | No |
| Mode | Any alias |
| On successful match | Stop |
| Target | Cisco Meeting Server |
| 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 |
|---|---|--|
| Name | The name of the policy service. | |
| Description | 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. |
| Protocol | The protocol used to connect to the policy service. The default is <i>HTTPS</i> . | The Expressway automatically supports HTTP to HTTPS redirection when communicating with the policy service server. |
| Certificate verification mode | When connecting over HTTPS, this setting controls whether the certificate presented by the policy server is verified. 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 Server address fields below. | The Expressway's root CA certificates are loaded via (Maintenance > Security > Trusted CA certificate). |
| HTTPS certificate revocation list (CRL) checking | 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 Maintenance > Security > CRL management to configure how the Expressway uploads CRL files. |
| Server address 1 - 3 | Enter the IP address or Fully Qualified Domain Name (FQDN) of the server hosting the service. You can specify a port by appending <code>:<port></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. For resiliency, up to three server addresses can be supplied. |
| Path | Enter the URL of the service on the server. | |

| Field | Description | Usage tips |
|--------------------|---|--|
| Status path | The Status path identifies the path from where the Expressway can obtain the status of the remote service. The default is <i>status</i> . | The policy server must supply return status information, see Policy Server Status and Resiliency, page 326 . |
| Username | The username used by the Expressway to log in and query the service. | |
| Password | The password used by the Expressway to log in and query the service. | The maximum plaintext length is 30 characters (which is subsequently encrypted). |
| Default CPL | 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. For more information, see Default CPL for Policy Services, page 521 . |

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**.

- 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:

| | |
|--------------------------------------|--|
| Rule name | A short name that describes the rule. |
| Description | A free-form description of the rule. |
| Priority | As required, for example 10. |
| Protocol | As required, for example <i>Any</i> . |
| Source | As required, for example <i>Any</i> . |
| Request must be authenticated | Configure this setting according to your authentication policy. |
| Mode | As required, for example <i>Alias pattern match</i> . |
| Pattern type | As required, for example <i>Regex</i> . |
| Pattern string | As required, for example <code>*\meet@example.com</code> |
| Pattern behavior | As required, for example <i>Leave</i> . |
| On successful match | As required. 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. |
| Target | Select the policy service that was created in the previous step. |
| State | <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*.

- 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:

Dial Plan and Call Processing

- use Call Policy to determine which callers can make or receive calls via the Expressway
- use [Registration restriction policy](#) to determine which aliases can or cannot register with 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, page 207](#) .

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 calls from a particular **Source** 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 you have not configured any call policy rules, the default policy is to allow all calls, regardless of source or destination.

Click on the rule you want to configure (or click **New** to create a new rule, or click **Delete** to remove a selected rule).

The configurable options for each rule are:

Dial Plan and Call Processing

| Field | Description | Usage tips |
|----------------------------|---|---|
| Source type | This field lets you choose from two types of call source: <i>Zone</i> or <i>From address</i> . Your choice affects the other fields that you use to configure the rule. | You can have a mixture of rules using different source types. Define and order them to implement your call policy or protect your conferencing resources from toll fraud. |
| Originating Zone | Visible for rules with Source type set to <i>Zone</i> . The dropdown shows all the zones configured on this Expressway, so you can choose the source for calls inspected by this rule. The rule inspects all calls originating from the zone that you choose. | |
| Rule applies to | Visible for rules with Source type set to <i>From address</i> . The field lets you choose whether the rule inspects calls from <i>Authenticated callers</i> or <i>Unauthenticated callers</i> . Authenticated callers are devices that are: <ul style="list-style-type: none"> ■ locally registered and authenticated with the Expressway, or ■ registered and authenticated to a neighbor which in turn has authenticated with the local Expressway | See About Device Authentication, page 135 for more information. |
| Source pattern | Visible for rules with Source type set to <i>From address</i> . The rule tries to match what you enter in this field to the source address that the calling endpoint uses to identify itself. If this field is blank, the policy rule applies to all incoming calls from the selected type of caller (Authenticated or Unauthenticated). | You can use a pattern for a more general rule or a single alias if you need to explicitly allow or reject a particular caller. This field supports regular expressions . |
| Destination pattern | Required for all rules. The rule tries to match what you enter in this field to the destination address from the incoming call. | You can use a pattern for a more general rule or a single alias if you need to explicitly allow or reject calls to a particular destination. This field supports regular expressions . |
| Action | Defines what the rule does when a call it has inspected matches what you specified for the source and destination. You can choose <i>Allow</i> or <i>Reject</i> . <i>Allow</i> : if the from address or originating zone matches the rule's source parameters, and if the call destination matches the rule's destination pattern, then the Expressway continues processing the call. <i>Reject</i> : if the from address or originating zone matches the rule's source parameters, and if the call destination matches the rule's destination pattern, then the Expressway rejects the call. | |

| Field | Description | Usage tips |
|------------------|--|---|
| Rearrange | <p>This field is only visible in the list of call policy rules (on the Call Policy rules page).</p> <p>You can click the  and  icons to change the order of the rules, which changes their relative priority.</p> | <p>Each rule is compared with the details of the incoming call in top-down order until a rule matches the call.</p> <p>When a rule matches, the rule's action is applied to the call.</p> |

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, page 347](#) 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 |
|---|---|--|
| Protocol | The protocol used to connect to the policy service. The default is <i>HTTPS</i> . | The Expressway automatically supports HTTP to HTTPS redirection when communicating with the policy service server. |
| Certificate verification mode | When connecting over HTTPS, this setting controls whether the certificate presented by the policy server is verified. 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 Server address fields below. | The Expressway's root CA certificates are loaded via (Maintenance > Security > Trusted CA certificate). |
| HTTPS certificate revocation list (CRL) checking | 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 Maintenance > Security > CRL management to configure how the Expressway uploads CRL files. |
| Server address 1 - 3 | Enter the IP address or Fully Qualified Domain Name (FQDN) of the server hosting the service. You can specify a port by appending <code>:<port></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. For resiliency, up to three server addresses can be supplied. |
| Path | Enter the URL of the service on the server. | |
| Status path | The Status path identifies the path from where the Expressway can obtain the status of the remote service. The default is <i>status</i> . | The policy server must supply return status information, see Policy Server Status and Resiliency, page 326 . |
| Username | The username used by the Expressway to log in and query the service. | |
| Password | The password used by the Expressway to log in and query the service. | The maximum plaintext length is 30 characters (which is subsequently encrypted). |

| Field | Description | Usage tips |
|--------------------|--|--|
| Default CPL | 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. For more information, see Default CPL for Policy Services, page 521 . |

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 endpoint is not registered with any system. See the [Dialing by IP Address, page 209](#) 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 Local Zone and 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 locally registered or 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 Local Zone and external zones for the alias, according to the search rules.

If the destination endpoint is not locally registered, 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.

Dial Plan and Call Processing

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.

If the destination endpoint is registered, it may be possible to call it using its IP address but the call may not succeed if the endpoint is on a private network or behind a firewall. For this reason you are recommended to place calls to registered endpoints via other address formats, such as its AOR or H.323 ID. Similarly, callers outside of your network should not try to contact endpoints within your network using their IP addresses.

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 it or one of its neighbors.

The Expressway considers an IP address to be "known" if it either:

- is the IP address of a locally registered endpoint, or
- falls within the IP address range of one of the subzone membership rules configured on the Expressway

The Expressway will always attempt to place calls to known IP addresses (providing there is a search rule for *Any IP Address* against the Local Zone).

All other IP addresses are considered to be "unknown" and are handled by the Expressway according to the **Calls to Unknown IP addresses** setting:

- *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, Call Policy or User Policy rules have been applied.

Note that in addition to controlling calls, this setting also determines the behavior of provisioning messages to SIP devices, as these messages are routed to IP addresses.

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. When a caller inside the firewall attempts to place a call to an IP address outside the firewall, it will be routed as follows:

1. The call will go from the endpoint to the Expressway-C with which it is registered.
2. As the IP address being called is not registered to that Expressway, and its **Calls to unknown IP addresses** setting is *Indirect*, the Expressway will not place the call directly. Instead, it will query its neighbor Expressway-E to see if that system is able to place the call on the Expressway-C's behalf. Note that you need to configure a search rule for *Any IP Address* against the traversal server zone.
3. The Expressway-E receives the call and because its **Calls to unknown IP addresses** setting is *Direct*, it will make the call directly to the called IP address.

About URI Dialing

A URI address typically takes the form `name@example.com`, where `name` is the alias and `example.com` is the domain.

URI dialing can make use of DNS to enable endpoints registered with different systems to locate and call each other. Without DNS, the endpoints would need to be registered to the same or neighbored systems in order to locate each other.

URI Dialing Without DNS

Without the use of DNS, calls made by a locally registered endpoint using URI dialing will be placed only if the destination endpoint is also locally registered, or is accessible via a neighbor system. This is because these endpoints would be located using the [search and zone transform process](#), rather than a DNS query.

If you want to use URI dialing from your network without the use of DNS, you would need to ensure that all the systems in your network were connected to each other by neighbor relationships - either directly or indirectly. This would ensure that any one system could locate an endpoint registered to itself or any another system, by searching for the endpoint's URI.

This does not scale well as the number of systems grows. It is also not particularly practical, as it means that endpoints within your network will not be able to dial endpoints registered to systems outside your network (for example when placing calls to another company) if there is not already a neighbor relationship between the two systems.

If a DNS zone and a DNS server have not been configured on the local Expressway, calls to endpoints that are not registered locally or to a neighbor system could still be placed if the local Expressway is neighbored (either directly or indirectly) with another Expressway that has been configured for URI dialing via DNS. In this case, any URI-dialed calls that are picked up by search rules that refer to that neighbor zone will go via that neighbor, which will perform the DNS lookup.

This configuration is useful if you want all URI dialing to be made via one particular system, such as an Expressway-E.

If you do not want to use DNS as part of URI dialing within your network, then no special configuration is required. Endpoints will register with an alias in the form of a URI, and when calls are placed to that URI the Expressway will query its local zone and neighbors for that URI.

Dial Plan and Call Processing

If the Expressway does not have DNS configured and your network includes H.323 endpoints, then in order for these endpoints to be reachable using URI dialing:

- an appropriate transform should be written to convert URIs into the format used by the H.323 registrations. An example would be a deployment where H.323 endpoints register with an `alias`, and incoming calls are made to `alias@domain.com`. A local transform is then configured to strip the `@domain`, and the search is made locally for `alias`. See [Stripping @domain for Dialing to H.323 Numbers, page 196](#) for an example of how to do this.

SIP endpoints always register with an AOR in the form of a URI, so no special configuration is required.

URI Dialing With DNS

By using DNS as part of URI dialing, it is possible to find an endpoint even though it may be registered to an unknown system. The Expressway uses a DNS lookup to locate the domain in the URI address and then queries that domain for the alias. See the [URI Resolution Process Using DNS, page 211](#) section for more information.

URI dialing via DNS is enabled separately for outgoing and incoming calls.

Outgoing calls

To enable your Expressway to locate endpoints using URI dialing via DNS, you must:

- configure at least one DNS zone and an associated search rule
- configure at least one DNS server

This is described in the [URI Dialing via DNS for Outgoing Calls, page 212](#) section.

Incoming calls

To enable endpoints registered to your Expressway to receive calls from non-locally registered endpoints using URI dialing via DNS, you must:

- ensure all endpoints are registered with an AOR (SIP) or H.323 ID in the form of a URI
- configure appropriate DNS records, depending on the protocols and transport types you want to use

This is described in the [URI Dialing via DNS for Incoming Calls, page 214](#) section.

Firewall traversal calls

To configure your system so that you can place and receive calls using URI dialing through a firewall, see the [URI Dialing and Firewall Traversal, page 216](#) section.

URI Resolution Process Using DNS

When the Expressway attempts to locate a destination URI address using the DNS system, the general process is as follows:

H.323

1. The Expressway sends a query to its DNS server for an SRV record for the domain in the URI. (If more than one DNS server has been configured on the Expressway, the query will be sent to all servers at the same time, and all responses will be prioritized by the Expressway with only the most relevant SRV record being used.) If available, this SRV record returns information (such as the FQDN and listening port) about either the device itself or the authoritative H.323 gatekeeper for that domain.
 - If the domain part of the URI address was resolved successfully using an H.323 Location SRV record (that is, for `_h323ls`) then the Expressway will send an A/AAAA record query for each name record returned. These will resolve to one or more IP addresses, and the Expressway then sends, in priority order, an LRQ for the full URI to those IP addresses.

Dial Plan and Call Processing

- If the domain part of the URI address was resolved using an H.323 Call Signaling SRV record (that is, for `_h323cs`) then the Expressway will send an A/AAAA record query for each name record returned. These will resolve to one or more IP addresses, and the Expressway then routes the call, in priority order to the IP addresses returned in those records. (An exception to this is where the original dial string has a port specified - for example, `user@example.com:1719` - in which case the address returned is queried via an LREQ for the full URI address.)
2. If a relevant SRV record cannot be located:
 - If the **Include address record** setting for the DNS zone being queried is set to *On*, the system will fall back to looking for an A or AAAA record for the domain in the URI. If such a record is found, the call will be routed to that IP address and the search will terminate. Note that if the A and AAAA records that are found at this domain are for systems other than those that support SIP or H.323, the Expressway will still forward the call to this zone, and the call will therefore fail. For this reason, you are recommended to use the default setting of *Off*.
 - If the **Include address record** setting for the DNS zone being queried is set to *Off*, the Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.

SIP

The Expressway supports the SIP resolution process as outlined in [RFC 3263](#). An example of how the Expressway implements this process is as follows:

1. The Expressway sends a NAPTR query for the domain in the URI. If available, the result set of this query describes a prioritized list of SRV records and transport protocols that should be used to contact that domain. If no NAPTR records are present in DNS for this domain name then the Expressway will use a default list of `_sips._tcp.<domain>`, `_sip._tcp.<domain>` and `_sip._udp.<domain>` for that domain as if they had been returned from the NAPTR query.
 - The Expressway sends SRV queries for each result returned from the NAPTR record lookup. A prioritized list of A/AAAA records returned is built.
 - The Expressway sends an A/AAAA record query for each name record returned by the SRV record lookup.

The above steps will result in a tree of IP addresses, port and transport protocols to be used to contact the target domain. The tree is sub-divided by NAPTR record priority and then by SRV record priority. When the tree of locations is used, the searching process will stop on the first location to return a response that indicates that the target destination has been contacted.

2. If the search process does not return a relevant SRV record:
 - If the **Include address record** setting for the DNS zone being queried is set to *On*, the system will fall back to looking for an A or AAAA record for the domain in the URI. If such a record is found, the call will be routed to that IP address and the search will terminate. Note that if the A and AAAA records that are found at this domain are for systems other than those that support SIP or H.323, the Expressway will still forward the call to this zone, and the call will therefore fail. For this reason, you are recommended to use the default setting of *Off*.
 - If the **Include address record** setting for the DNS zone being queried is set to *Off*, the Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.

URI Dialing via DNS for Outgoing Calls

When a user places a call using URI dialing, they will typically dial an address in the form `name@example.com` from their endpoint. Below is the process that is followed when a URI address is dialed from an endpoint registered with your Expressway, or received as a query from a neighbor system:

1. 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 URI address

Dial Plan and Call Processing

2. The associated target zones are queried, in rule priority order, for the URI.
 - If one of the target zones is a DNS zone, the Expressway attempts to locate the endpoint through a DNS lookup. It does this by querying the DNS server configured on the Expressway for the location of the domain as per the [URI resolution process via DNS](#). If the domain part of the URI address is resolved successfully the request is forwarded to those addresses.
 - If one of the target zones is a neighbor, traversal client or traversal server zones, those zones are queried for the URI. If that system supports URI dialing via DNS, it may route the call itself.

Adding and configuring DNS zones

To enable URI dialing via DNS, you must configure at least one DNS zone. To do this:

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 *DNS*.
4. Configure the DNS zone settings as follows:

| Field | Guidelines |
|-------------------------------|--|
| Hop count | <p>When dialing by URI via DNS, the hop count used is that configured for the DNS zone associated with the search rule that matches the URI address (if this is lower than the hop count currently assigned to the call).</p> <p>If URI address isn't matched to a DNS zone, the query may be forwarded to a neighbor. In this case, the hop count used will be that configured for the neighbor zone (if this is lower than the hop count currently assigned to the call).</p> |
| H.323 and SIP modes | The H.323 and SIP sections allow you to filter calls to systems and endpoints located via this zone, based on whether the call is located using SIP or H.323 SRV lookups. |
| Include address record | <p>This setting 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.</p> <p>You are recommended to use the default setting of <i>Off</i>, meaning that the Expressway will not query for A and AAAA records, and instead will continue with the search, querying the remaining lower priority zones. This is because, unlike for NAPTR and SRV records, there is no guarantee that the A/AAAA records will point to a system capable of processing the relevant SIP or H.323 messages (LRQs, Setups, etc.) - the system may instead be a web server that processes http messages, or a mail server that processes mail messages. If this setting is <i>On</i>, when a system is found using A/AAAA lookup, the Expressway will send the signaling to that destination and will not continue the search process. If the system does not support SIP or H.323, the call will fail.</p> |
| Zone profile | For most deployments, this option should be left as <i>Default</i> . |

5. Click **Create zone**.

Configuring search rules for DNS zones

If you want your local Expressway to use DNS to locate endpoints outside your network, you must:

- [configure the DNS servers](#) used by the Expressway for DNS queries
- create a DNS zone and set up associated search rules that use the **Pattern string** and **Pattern type** fields to define the aliases that will trigger a DNS query

For example, rules with:

Dial Plan and Call Processing

- a **Pattern string** of `*@.*` and a **Pattern type** of *Regex* will query DNS for all aliases in the form of typical URI addresses
- a **Pattern string** of `(?!.*@example.com$).*` and a **Pattern type** of *Regex* will query DNS for all aliases in the form of typical URI addresses except those for the domain `example.com`

To set up further filters, configure extra search rules that target the same DNS zone. You do not need to create new DNS zones for each rule unless you want to filter based on the protocol (SIP or H.323) or use different hop counts.

Note: you are not recommended to configure search rules with a **Mode** of *Any alias* for DNS zones. This will result in DNS always being queried for all aliases, including those that may be locally registered and those that are not in the form of URI addresses.

URI Dialing via DNS for Incoming Calls

DNS record types

The ability of the Expressway to receive incoming calls (and other messages, such as registrations) made using URI dialing via DNS relies on the presence of DNS records for each domain the Expressway is hosting.

These records can be of various types including:

- A records, which provide the IPv4 address of the Expressway
- AAAA records, which provide the IPv6 address of the Expressway
- Service (SRV) records, which specify the FQDN of the Expressway and the port on it to be queried for a particular protocol and transport type.
- NAPTR records, which specify SRV record and transport preferences for a SIP domain.

You must provide an SRV or NAPTR record for each combination of domain hosted and protocol and transport type enabled on the Expressway.

Incoming call process

When an incoming call has been placed using URI dialing via DNS, the Expressway will have been located by the calling system using one of the DNS record lookups described above. The Expressway will receive the request containing the dialed URI in the form `user@example.com`. This will appear as coming from the Default Zone. The Expressway will then search for the URI in accordance with its normal [call routing process](#), applying any pre-search transforms, Call Policy and FindMe policy, then searching its Local Zone and other configured zones, in order of search rule priority.

SRV record format

The format of SRV records is defined by [RFC 2782](#) as:

```
_Service._Proto.Name TTL Class SRV Priority Weight Port Target
```

For the Expressway, these are as follows:

- `_Service` and `_Proto` will be different for H.323 and SIP, and will depend on the protocol and transport type being used
- `Name` is the domain in the URI that the Expressway is hosting (such as `example.com`)
- `Port` is the IP port on the Expressway that has been configured to listen for that particular service and protocol combination
- `Target` is the FQDN of the Expressway.

Configuring H.323 SRV Records

Annex O of [ITU Specification: H.323](#) defines the procedures for using DNS to locate gatekeepers and endpoints and for resolving H.323 URL aliases. It also defines parameters for use with the H.323 URL.

The Expressway supports the location, call and registration service types of SRV record as defined by this Annex.

Location service SRV records

Location records are required for gatekeepers that route calls to the Expressway. For each domain hosted by the Expressway, you should configure a location service SRV record as follows:

- `_Service is_h323ls`
- `_Proto is_udp`
- Port is the port number that has been configured from **Configuration > Protocols > H.323** as the **Registration UDP port**

Call signaling SRV records

Call signaling SRV records (and A/AAAA records) are intended primarily for use by non-registered endpoints which cannot participate in a location transaction, exchanging LRQ and LCF. For each domain hosted by the Expressway, you should configure a call signaling SRV record as follows:

- `_Service is_h323cs`
- `_Proto is_tcp`
- Port is the port number that has been configured from **Configuration > Protocols > H.323** as the **Call signaling TCP port**.

Registration service SRV records

Registration records are used by devices attempting to register to the Expressway. For each domain hosted by the Expressway, you should configure a registration service SRV record as follows:

- `_Service is_h323rs`
- `_Proto is_udp`
- Port is the port number that has been configured from **Configuration > Protocols > H.323** as the **Registration UDP port**

Configuring SIP SRV Records

[RFC 3263](#) describes the DNS procedures used to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact.

If you want the Expressway to be contactable using SIP URI dialing, you should configure an SRV record for each SIP transport protocol enabled on the Expressway (that is, UDP, TCP or TLS) as follows:

- Valid combinations of `_Service` and `_Proto` are:
 - `_sips._tcp`
 - `_sip._tcp`
 - `_sip._udp` (although not recommended)
- Port is the IP port number that has been configured from **Configuration > Protocols > SIP** as the port for that particular transport protocol.

`_sip._udp` is not recommended because SIP messages for video systems are too large to be carried on a packet based (rather than stream based) transport. UDP is often used for audio only devices. Also, UDP tends to be spammed more than TCP or TLS.

Example DNS Record Configuration

A company with the domain name `example.com` wants to enable incoming H.323 and SIP calls using URI addresses in the format `user@example.com`. The Expressway hosting the domain has the FQDN `expressway.example.com`.

Their DNS records would typically be as follows:

Dial Plan and Call Processing

- SRV record for `_h3231s._udp.example.com` returns `expressway.example.com`
- SRV record for `_h323cs._tcp.example.com` returns `expressway.example.com`
- SRV record for `_h323rs._tcp.example.com` returns `expressway.example.com`
- NAPTR record for `example.com` returns
 - `_sip._tcp.example.com` and
 - `_sips._tcp.example.com`
- SRV record for `_sip._tcp.example.com` returns `expressway.example.com`
- SRV record for `_sips._tcp.example.com` returns `expressway.example.com`
- A record for `expressway.example.com` returns the IPv4 address of the Expressway
- AAAA record for `expressway.example.com` returns the IPv6 address of the Expressway

How you add the DNS records depends on the type of DNS server you are using. Instructions for setting up two common DNS servers are given in the DNS configuration section.

For locally registered H.323 endpoints to be reached using URI dialing, either:

- the H.323 endpoints should register with the Expressway using an address in the format of a URI
- an appropriate transform should be written to convert URIs into the format used by the H.323 registrations. An example would be a deployment where H.323 endpoints register with an alias, and incoming calls are made to `alias@domain.com`. A local transform is then configured to strip the `@domain`, and the search is made locally for `alias`. See [Stripping @domain for Dialing to H.323 Numbers, page 196](#) for an example of how to do this.

SIP endpoints always register with an AOR in the form of a URI, so no special configuration is required.

Several mechanisms could have been used to locate the Expressway. You may want to enable calls placed to `user@<IP_address>` to be routed to an existing registration for `user@example.com`. In this case you would configure a [pre-search transform](#) that would strip the `IP_address` suffix from the incoming URI and replace it with the suffix of `example.com`.

URI Dialing and Firewall Traversal

If URI dialing via DNS is being used in conjunction with firewall traversal, DNS zones should be configured on the Expressway-E and any Expressways on the public network only. Expressways behind the firewall should not have any DNS zones configured. This will ensure that any outgoing URI calls made by endpoints registered with the Expressway will be routed through the Expressway-E.

In addition, the DNS records for incoming calls should be configured with the address of the Expressway-E as the authoritative proxy for the enterprise (the DNS configuration section for more information). This ensures that incoming calls placed using URI dialing enter the enterprise through the Expressway-E, allowing successful traversal of the firewall.

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 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, page 217](#) 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, page 220](#) 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](#). If the URIs belong to locally registered endpoints, no further configuration is required. However, if one or more of the URIs are not locally registered, you may also need to configure a DNS zone if they are to be located using a DNS lookup.

Calling process

The Expressway follows this process when searching for an ENUM (E.164) number:

1. The Expressway initiates a search for the received E.164 number as it was 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:
 1. The digits are reversed and separated by a dot.
 2. 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 |
|-------------------|---|
| Hop count | The hop count 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. |
| DNS suffix | 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. |
| H.323 mode | Controls if H.323 records are looked up for this zone. |
| SIP mode | 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 locally registered endpoints 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, page 188](#) 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 your locally registered endpoints to be reached using ENUM dialing, you must configure a DNS NAPTR record that maps your endpoints' E.164 numbers to their 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 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 preference flag 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

Dial Plan and Call Processing

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 are not locally registered or 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.
 - The call consumes either an RMS Call license or a Registered Call license on the Expressway.

Dial Plan and Call Processing

- *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 or FindMe such that:
 - the call resolves to more than one alias
 - the source alias of the call has been modified to display the associated FindMe ID
 - the FindMe has a "no answer" or "busy" device configured
 - one of the endpoints in the call is locally registered
 - 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. This setting is useful in a [hierarchical dial plan](#), when used on the directory Expressway. In such deployments the directory Expressway is used to look up and locate endpoints and it does not have any endpoints registered directly to it.

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, page 222](#)). 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.

Dial Plan and Call Processing

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 > Local Zone** and **Configuration > Bandwidth**).

| | |
|--------------------------------------|-----|
| About Bandwidth Control | 225 |
| Configuring Bandwidth Controls | 226 |
| About Subzones | 227 |
| Links and Pipes | 233 |
| Bandwidth Control Examples | 236 |

About Bandwidth Control

The Expressway allows you to control the amount of bandwidth used by endpoints on your network. This is done by grouping endpoints into subzones, and then using [links](#) and [pipes](#) to apply limits to the bandwidth that can be used:

- within each subzone
- between a subzone and another subzone
- between a subzone and a zone

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`.

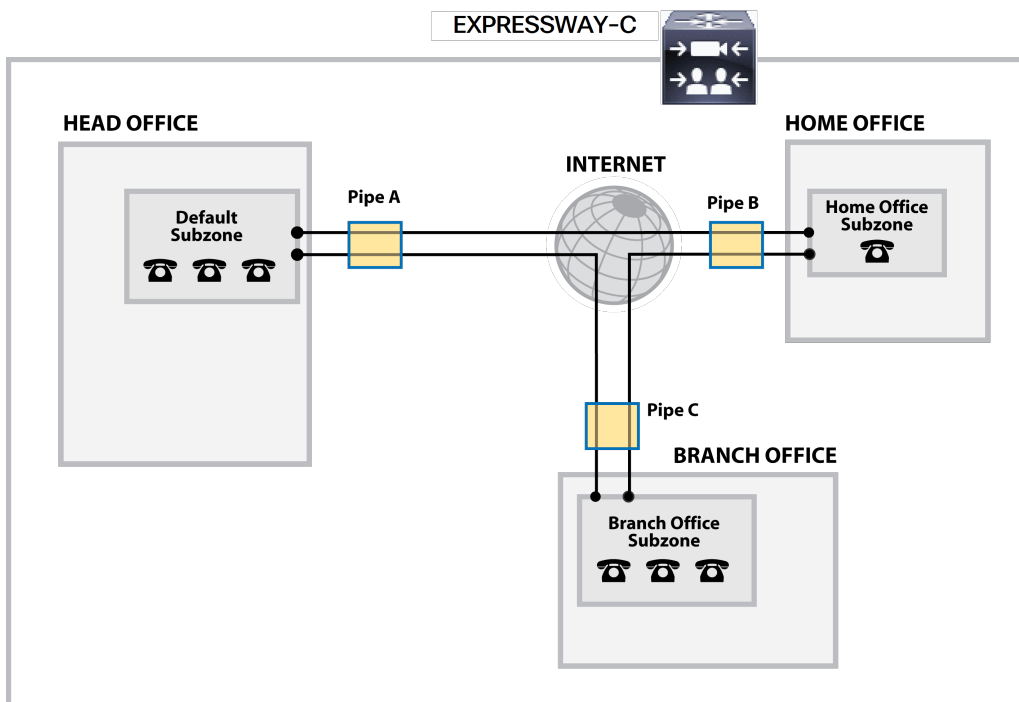
For specific information about how bandwidth is managed across peers in a cluster, see [Sharing Bandwidth Across Peers, page 177](#).

Example network deployment

The following diagram shows a typical network deployment:

- a broadband LAN between the Enterprise and the internet, where high bandwidth calls are acceptable
- a pipe to the internet (Pipe A) with restricted bandwidth
- two satellite offices, Branch and Home, each with their own internet connections and restricted pipes

In this example each pool of endpoints has been assigned to a different subzone, so that suitable limitations can be applied to the bandwidth used within and between each subzone based on the amount of bandwidth they have available via their internet connections.



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 |
|--------------------------------------|--|---|
| Default call bandwidth (kbps) | <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. |
| Downspeed per call mode | <p>Determines what happens if the per-call 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> | |
| Downspeed total mode | <p>Determines what happens if the total 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, and to control the Expressway's registration, authentication and media encryption policies.

When an endpoint registers with the Expressway it is allocated to an appropriate subzone, determined by [subzone membership rules](#) based on endpoint IP address ranges or alias pattern matches.

You can create and configure subzones through the [Subzones](#) page (**Configuration > Local Zone > Subzones**).

The Expressway automatically creates the following special subzones, which you cannot delete:

- the Default Subzone
- the Traversal Subzone
- the Cluster Subzone (only applies if the Expressway is in a cluster)

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. No endpoints can be registered to the Traversal Subzone; its sole purpose is to control the bandwidth used by traversal calls.

The **Traversal Subzone** page (**Configuration > Local Zone > 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 Subzones, page 232](#) for more details.

Configuring the Traversal Subzone Ports

On **Configuration > Local Zone > 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 $48 * 500 = 24000$ 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?

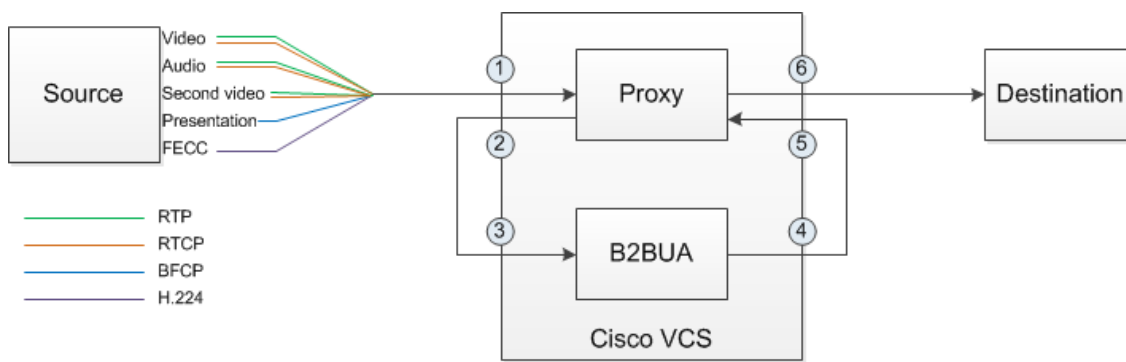
The nominal maximum number of ports allocated per call = max number of ports per allocation * max number of allocation instances. This is $8 * 6 = 48$, and those numbers are derived as follows:

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 13 Maximum port allocation for a media traversal call



Bandwidth Control

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 > Local Zones > 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: Changes to the **Use configured demultiplexing ports** setting need a system restart to take effect.

Configuring the Default Subzone

The **Default Subzone** page (**Configuration > Local Zone > Default Subzone**) is used to place bandwidth restrictions on calls involving endpoints in the Default Subzone, and to specify the Default Subzone's registration, authentication and media encryption policies.

When an endpoint registers with the Expressway, its IP address and alias is checked against the subzone membership rules and it is assigned to the appropriate subzone. If no subzones have been created, or the endpoint's IP address or alias does not match any of the subzone membership rules, it is assigned to the Default Subzone (subject to the Default Subzone's **Registration policy** and **Authentication policy**).

The use of a Default Subzone on its own (without any other manually created subzones) is suitable only if you have uniform bandwidth available between all your endpoints. Note that if your Local Zone contains two or more different networks with different bandwidth limitations, you should configure separate subzones for each different part of the network.

Default Subzone configuration options

The Default Subzone can be configured in the same manner as any other [manually created subzone](#).

Configuring Subzones

The **Subzones** page (**Configuration > Local Zone > Subzones**) lists all the subzones that have been configured on the Expressway, and allows you to create, edit and delete subzones. For each subzone, it shows how many membership rules it has, how many devices are currently registered to it, and the current number of calls and bandwidth in use. Up to 1000 subzones can be configured.

After configuring a subzone you should set up the [Subzone membership rules](#) which control which subzone an endpoint device is assigned to when it registers with the Expressway as opposed to defaulting to the [Default Subzone](#).

The configurable options are:

Bandwidth Control

| Field / section | Description |
|------------------------------|--|
| Registration policy | <p>When an endpoint registers with the Expressway, its IP address and alias is checked against the subzone membership rules and it is assigned to the appropriate subzone. If no subzones have been created, or the endpoint's IP address or alias does not match any of the subzone membership rules, it is assigned to the Default Subzone.</p> <p>In addition to using a registration restriction policy to control whether an endpoint can register with the Expressway, you can also configure a subzone's Registration policy as to whether it will accept registrations assigned to it via the subzone membership rules.</p> <p>This provides additional flexibility when defining your registration policy. For example you can:</p> <ul style="list-style-type: none"> Deny registrations based on IP address subnet. You can do this by creating a subzone with associated membership rules based on an IP address subnet range, and then setting that subzone to deny registrations. Configure the Default Subzone to deny registrations. This would cause any registration requests that do not match any of the subzone membership rules, and hence fall into the Default Subzone, to be denied. <p>Note that registration requests have to fulfill any registration restriction policy rules before any subzone membership and subzone registration policy rules are applied.</p> |
| Authentication policy | <p>The Authentication policy setting controls how the Expressway challenges incoming messages to the Default Subzone. See Authentication Policy Configuration Options, page 136 for more information.</p> |
| Media encryption mode | <p>The Media encryption mode setting controls the media encryption capabilities for SIP calls flowing through the subzone. See Configuring Media Encryption Policy, page 144 for more information.</p> <p>Note that if H.323 is enabled and the subzone has a media encryption mode of <i>Force encrypted</i> or <i>Force unencrypted</i>, any H.323 and SIP to H.323 interworked calls through this subzone will ignore this mode.</p> |
| ICE support for media | <p>Controls whether ICE messages are supported by the devices in this subzone.</p> |
| Bandwidth controls | <p>When configuring your subzones you can apply bandwidth limits to:</p> <ul style="list-style-type: none"> individual calls between two endpoints within the subzone individual calls between an endpoint within the subzone and another endpoint outside of the subzone the total of calls to or from endpoints within the subzone <p>See Applying Bandwidth Limitations to Subzones, page 232 for information about how bandwidth limits are set and managed.</p> |

Configuring Subzone Membership Rules

The **Subzone membership rules** page ([Configuration > Local Zone > Subzone membership rules](#)) is used to configure the rules that determine, based on the address of the device, to which [subzone](#) an endpoint is assigned when it registers with the Expressway.

The page lists all the subzone membership rules that have been configured on the Expressway, and lets you create, edit, delete, enable and disable rules. Rule properties include:

- rule name and description
- priority

Bandwidth Control

- the subnet or alias pattern matching configuration
- the subzone to which endpoints whose addresses satisfy this rule are assigned

Note that if an endpoint's IP address or registration alias does not match any of the membership rules, it is assigned to the [Default Subzone](#).

Up to 3000 subzone membership rules can be configured.

The configurable options are:

| Field | Description | Usage tips |
|---|---|---|
| Rule name | A descriptive name for the membership rule. | |
| Description | 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. |
| Priority | The order in which the rules are applied (and thus to which subzone the endpoint is assigned) if an endpoint's address satisfies multiple rules. | The rules with the highest priority (1, then 2, then 3 and so on) are applied first. If multiple <i>Subnet</i> rules have the same priority, the rule with the largest prefix length is applied first. <i>Alias pattern match</i> rules at the same priority are searched in configuration order. |
| Type | Determines how a device's address is checked: <i>Subnet</i> : assigns the device if its IP address falls within the configured IP address subnet. <i>Alias pattern match</i> : assigns the device if its alias matches the configured pattern. | Pattern matching is useful, for example, for home workers on dynamic IP addresses; rather than having to continually update the subnet to match what has been allocated, you can match against their alias instead. |
| Subnet address and Prefix length | These two fields together determine the range of IP addresses that will belong to this subzone. The Address range field shows the range of IP addresses to be allocated to this subzone, based on the combination of the Subnet address and Prefix length . | Applies only if the Type is <i>Subnet</i> . |
| Pattern type | How the Pattern string must match the alias for the rule to be applied. Options are: <i>Exact</i> : the entire string must exactly match the alias character for character. <i>Prefix</i> : the string must appear at the beginning of the alias. <i>Suffix</i> : the string must appear at the end of the alias. <i>Regex</i> : treats the string as a regular expression . | Applies only if the Type is <i>Alias pattern match</i> . |
| Pattern string | The pattern against which the alias is compared. | Applies only if the Type is <i>Alias pattern match</i> . |
| Target subzone | The subzone to which an endpoint is assigned if its address satisfies this rule. | |

Bandwidth Control

| Field | Description | Usage tips |
|--------------|--|---|
| State | 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. |

Applying Bandwidth Limitations to Subzones

You can apply bandwidth limits to the Default Subzone, Traversal Subzone and all manually configured subzones. The limits you can apply vary depending on the type of subzone, as follows:

| Limitation | Description | Can be applied to |
|--------------------------|---|--|
| Total | Limits the total concurrent bandwidth being used by all endpoints in the subzone at any one time. In the case of the Traversal Subzone, this is the maximum bandwidth available for all concurrent traversal calls. | Default Subzone Traversal Subzone Manually configured subzones |
| Calls entirely within... | Limits the bandwidth of any individual call between two endpoints within the subzone. | Default Subzone Manually configured subzones |
| Calls into or out of... | Limits the bandwidth of any individual call between an endpoint in the subzone, and an endpoint in another subzone or zone. | Default Subzone Manually configured subzones |
| Calls handled by... | The maximum bandwidth available to any individual traversal call. | Traversal Subzone |

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.

Use subzone bandwidth limits if you want to configure the bandwidth available between one specific subzone and **all other** subzones or zones.

Use pipes if you want to configure the bandwidth available between one specific subzone and **another specific** subzone or zone.

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.

How different bandwidth limitations are managed

In situations where there are differing bandwidth limitations applied to the same link, the lower limit will always be the one used when routing the call and taking bandwidth limitations into account.

For example, Subzone A may have a per call inter bandwidth of 128. This means that any calls between Subzone A and any other subzone or zone will be limited to 128kbps. However, Subzone A also has a link configured between it and Subzone B. This link uses a pipe with a limit of 512kbps. In this situation, the lower limit of 128kbps will apply to calls between the two, regardless of the larger capacity of the pipe.

In the reverse situation, where Subzone A has a per call inter bandwidth limit of 512kbps and a link to Subzone B with a pipe of 128kbps, any calls between the two subzones will still be limited to 128kbps.

Bandwidth Control

Bandwidth consumption of traversal calls

A non-traversal call between two endpoints within the same subzone would consume from that subzone the amount of bandwidth of that call.

A traversal call between two endpoints within the same subzone must, like all traversal calls, pass through the Traversal Subzone. This means that such calls consume an amount of bandwidth from the originating subzone's total concurrent allocation that is equal to twice the bandwidth of the call – once for the call from the subzone to the Traversal Subzone, and again for the call from the Traversal Subzone back to the originating subzone. In addition, as this call passes through the Traversal Subzone, it will consume an amount of bandwidth from the Traversal Subzone equal to that of the call.

Links and Pipes

Configuring Links

Links connect local subzones with other subzones and zones. For a call to take place, the endpoints involved must each reside in subzones or zones that have a link between them. The link does not need to be direct; the two endpoints may be linked via one or more intermediary subzones.

Links are used to calculate how a call is routed over the network and therefore which zones and subzones are involved and how much bandwidth is available. If multiple routes are possible, your Expressway will perform the bandwidth calculations using the one with the fewest links.

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 |
|--------------------------|--|
| Name | The name of the link. Automatically created links have names based on the nodes that the link is between. |
| Node 1 and Node 2 | The Traversal Subzone and the zone that the link is between. The two subzones, or one subzone and one zone, that the link is between. |
| Pipe 1 and Pipe 2 | Any pipes that have been used to apply bandwidth limitations to the link. See Applying Pipes to Links, page 235 for more information. Note that in order to apply a pipe, you must first have created it via the Pipes page. |
| Calls | Shows the total number of calls currently traversing the link. |
| Bandwidth used | 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 subzone or zone is created.

Default Links

If a subzone has no links configured, then endpoints within the subzone are only able to call other endpoints within the same subzone. For this reason, the Expressway comes shipped with a set of pre-configured links and will also automatically create new links each time you create a new subzone.

Pre-configured 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.

Bandwidth Control

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 subzone or zone is created, links are automatically created as follows:

| New zone/subzone type | Default links are created to... |
|-----------------------|---------------------------------------|
| Subzone | Default Subzone and Traversal Subzone |
| 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 new subzone or 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, page 235](#) 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 |
|---------------------------|--|
| Name | The name of the pipe. |
| Total bandwidth | The upper limit on the total bandwidth used at any one time by all calls on all links to which this pipe is applied. |
| Per call bandwidth | The maximum bandwidth of any one call on the links to which this pipe is applied. |
| Calls | Shows the total number of calls currently traversing all links to which the pipe is applied. |
| Bandwidth used | 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 Subzones, page 232](#) 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.

One pipe, one link

Applying a single pipe to a single link is useful when you want to apply specific limits to calls between a subzone and another specific subzone or zone.

One pipe, two or more links

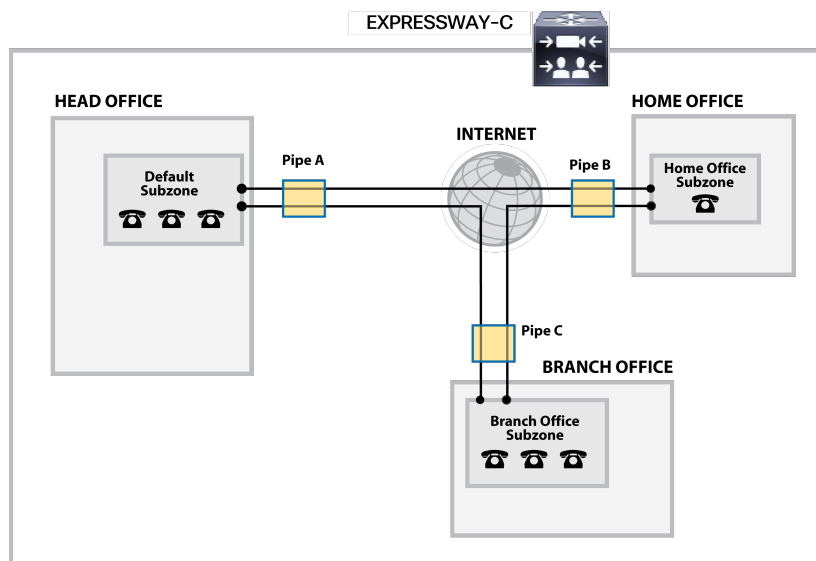
Each pipe may be applied to multiple links. This is used to model the situation where one site communicates with several other sites over the same broadband connection to the Internet. A pipe should be configured to represent the broadband connection, and then applied to all the links. This allows you to configure the bandwidth options for calls in and out of that site.

In the diagram below, Pipe A has been applied to two links: the link between the Default Subzone and the Home Office subzone, and the link between the Default Subzone and the Branch Office subzone. In this case, Pipe A represents the Head Office's broadband connection to the internet, and would have total and per-call restrictions placed on it.

Two pipes, one link

Each link may have up to two pipes associated with it. This is used to model the situation where the two nodes of a link are not directly connected, for example two sites that each have their own broadband connection to the Internet. Each connection should have its own pipe, meaning that a link between the two nodes should be subject to the bandwidth restrictions of both pipes.

In the diagram below, the link between the Default Subzone and the Home Office Subzone has two pipes associated with it: Pipe A, which represents the Head Office's broadband connection to the internet, and Pipe B, which represents the Home Office's dial-up connection to the internet. Each pipe would have bandwidth restrictions placed on it to represent its maximum capacity, and a call placed via this link would have the lower of the two bandwidth restrictions applied.



Bandwidth Control Examples

Without a Firewall

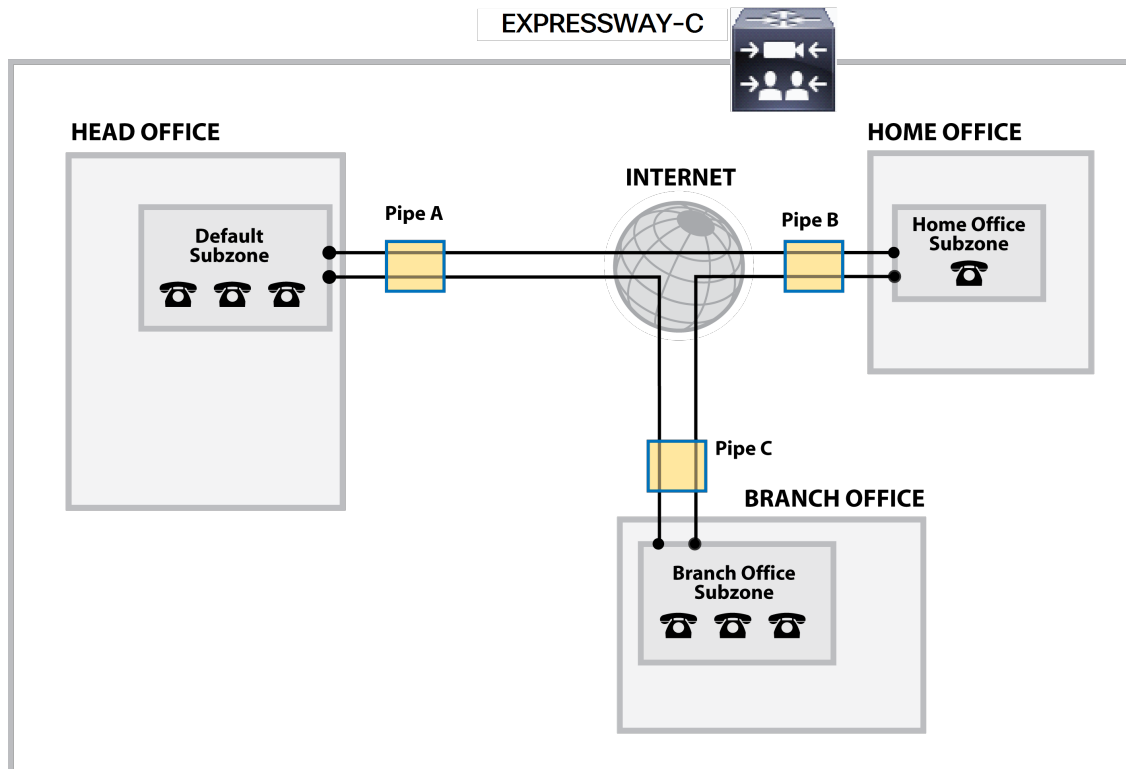
In the example below, there are three geographically separate offices: Head, Branch and Home. All endpoints in the Head Office register with the Expressway-C, as do those in the Branch and Home offices.

Each of the three offices is represented as a separate subzone on the Expressway, with bandwidth configured according to local policy.

The enterprise's leased line connection to the Internet, and the DSL connections to the remote offices are modeled as separate pipes.

There are no firewalls involved in this scenario, so direct links can be configured between each of the offices. Each link is then assigned two pipes, representing the Internet connections of the offices at each end of the link.

In this scenario, a call placed between the Home Office and Branch Office will consume bandwidth from the Home and Branch subzones and on the Home and Branch pipes (Pipe B and Pipe C). The Head Office's bandwidth budget will be unaffected by the call.





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 | 238 |
| FindMe™ | 247 |
| Cisco TMS Provisioning | 250 |
| Hybrid Services and Connector Management | 252 |

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 SIP domain. This requires manual configuration of [Microsoft Interoperability](#) and the set of [TURN servers](#) available for use by the B2BUA.

Configuring B2BUA TURN Servers

Go to **Applications > B2BUA > B2BUA TURN servers** to enter details of the TURN servers that are needed by the Expressway B2BUA instances. The page lists the currently configured TURN servers and lets you create, edit and delete them.

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.

The TURN servers are automatically used by B2BUA instances for [ICE messaging](#) when it is enabled on a zone or subzone.

If you want to use the TURN servers for Microsoft interoperability, you must enable **Offer TURN services** (See [Configuring Microsoft Interoperability, page 240](#)).

Table 15 TURN Server Configuration Details

| Field | Description |
|--|---|
| TURN server address | The IP address of a TURN server to offer when establishing ICE calls (for example, with a Microsoft Edge server). The TURN server must be RFC 5245 compliant, for example an Expressway-E TURN server. |
| TURN server port | The listening port on the TURN server. Default is 3478. |
| Description | A free-form description of the TURN server. |
| TURN services username and password | The username and password that are required to access the TURN server. |

If you are using the TURN server on a Large Expressway-E, it listens on all ports in the range 3478-3483 by default. You can enter the same TURN server address up to six times if you supply a different port each time, to make the best use of the Large Expressway-E's capacity.

Applications

Microsoft Interoperability

Expressway interoperability with Microsoft is based on a back-to-back user agent (B2BUA) which handles SIP calls between the Expressway and the Microsoft Skype for Business infrastructure.

Note: In version X8.9, you can interoperate with Microsoft infrastructure without using the B2BUA on the Expressway. You can now use enhanced search rules to route calls to Cisco Meeting Server which does the transcoding instead. See *Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure* on the [Expressway configuration guides page](#).

Capabilities

- Interwork between Microsoft ICE and standards-based media for Cisco collaboration endpoints and bridges.
- Call hold and call transfer support for calls with Microsoft clients.
- Transcoding of Microsoft client screen sharing (RDP) to H.264
- Filter the messaging and presence traffic from Microsoft SIP, and redirect it towards appropriate servers, eg. IM and Presence Service nodes, while handling the voice/video traffic on the Expressway.

Configuration Summary

- Selecting the Microsoft interoperability service on a dedicated Expressway.
- Adding the *Microsoft Interoperability* key.
- [Configuring Microsoft Interoperability, page 240](#).
- [Configuring the B2BUA's Trusted Hosts, page 243](#) – the devices that may send signaling messages to the B2BUA.
- [Configuring B2BUA TURN Servers, page 238](#) – TURN servers available for use by the B2BUA when establishing ICE calls.
- Setting up search rules to route calls to the Microsoft domain, through the automatically configured zone, to the B2BUA.
When you enable the B2BUA, the Expressway automatically creates a non-configurable neighbor zone called **To Microsoft destination via B2BUA**; this zone must be the target of your search rules.
The zone is not automatically deleted when you disable the B2BUA; Also, the old zone name (To Microsoft Lync Server via B2BUA) persists if you already had this zone when you upgraded to X8.8.
- [Configuring External B2BUA Transcoders, page 245](#), that may be used by the B2BUA, and any [policy rules](#) used to control routing through them (this is optional; External transcoders are typically only used with Lync 2010 Server).
- [Restarting the Microsoft Interoperability Service, page 246](#), if required. The system notifies you if you must restart the service.

Why do I need Microsoft Interoperability Option Key?

You need this key on the Expressway-C (on each peer if the Expressway-C is clustered) if you are using the Expressway to modify traffic between Microsoft collaboration infrastructure and standards-based infrastructure. This includes:

- Microsoft SIP to standard SIP call interworking
- Screen share transcoding (RDP to H.264 in BFCP)
- Microsoft SIP message and presence forwarding (SIP Broker)

You do not need this key if you are using the Expressway to route Microsoft traffic without modifying it. For example, if you are using the Expressway search rules to send Microsoft variant SIP traffic to be interworked by a Cisco Meeting Server.

Applications

Features and Limitations

- Maximum simultaneous call capability is 100 calls (for all system sizes, including Large systems)
- A call routed through an external transcoder counts as 2 calls.
- If a call is routed through the Microsoft interoperability 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 interoperability*.
- The Microsoft interoperability service does not consume additional call licenses beyond what is required by the call leg between the endpoint and the Expressway.
- If all configured external 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.
- You can use multiple TURN servers with the Microsoft interoperability service. TURN servers are required for calls traversing a Microsoft Edge server.
- You can apply bandwidth controls to the call leg between the endpoint and the B2BUA, but not to the call leg between the B2BUA and the Microsoft infrastructure. However, because the B2BUA forwards the media it receives without any manipulation, any bandwidth controls you apply to the Expressway to B2BUA leg will implicitly apply to the B2BUA to Microsoft leg.
- The non-configurable neighbor zone (named "**To Microsoft destination via B2BUA**") uses a special zone profile of *Microsoft interoperability*. You cannot select this profile for any manually configured zones.

For more information about configuring Expressway for Microsoft interoperability:

- See [Microsoft Interoperability Port Reference, page 371](#)
- See *Cisco Expressway with Microsoft Infrastructure Deployment Guide* on the [Expressway configuration guides page](#).

Configuring Microsoft Interoperability

Go **Applications > B2BUA > Microsoft interoperability > Configuration** configure and enable and the B2BUA's connection to the Microsoft environment.

The configurable options are:

| Field | Description | Usage tips |
|------------------------------------|---|--|
| Configuration section: | | |
| Microsoft interoperability | Enables or disables the Microsoft interoperability service. | |
| Destination address | 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 trusted hosts . These are the Microsoft systems that may send signaling messages to the Expressway. |
| Listening port | 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. | |
| Signaling transport | The transport type used for connection to the Microsoft infrastructure. The default is <i>TLS</i> . | |
| FindMe integration section: | | |

Applications

| Field | Description | Usage tips |
|---|--|---|
| Register FindMe users as clients to Microsoft server | Controls whether to register FindMe users to the Microsoft registrar so that it can forward calls to FindMe aliases. Default is Yes. | This feature only applies if FindMe is enabled. Note that FindMe users can only register to Microsoft infrastructure if the FindMe ID is a valid user in the Active Directory (in the same way that Microsoft clients can only register if they have a valid account enabled in AD). |
| Microsoft domain | The SIP domain in use on the Microsoft server. This must be selected from one of the SIP domains already configured on the Expressway. | Only FindMe names with this domain will be registered to the Microsoft server. |
| Remote Desktop Protocol section: | | |
| Enable RDP transcoding for this B2BUA | Controls whether the B2BUA offers Remote Desktop Protocol transcoding. This feature requires the Microsoft Interoperability option key. Default is <i>No</i> . | You should enable this option if you want Microsoft client users to be able to share their screens with Cisco Collaboration endpoints / conference participants. |
| External transcoders section: | | |
| Enable external transcoders for this B2BUA | Controls whether calls may be routed through an external 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. |
| Port on B2BUA for transcoder communications | The IP port used on the B2BUA for communicating with the transcoders. Default is 65080. | All transcoder communications are carried out over TLS. |
| Use transcoder policy rules | Specifies whether the transcoder policy rules are used to control access to the transcoders. Default is No. | If Enable transcoders for this B2BUA is Yes, then all calls are routed via the transcoders by default. 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 policy rules . |
| SIP broker section: | | |
| Enable broker for inbound SIP | Toggles the SIP broker, and opens a list of destination presence servers. The broker inspects Microsoft SIP, and routes the SIP SIMPLE to IM and Presence Service nodes that you enter. | If the broker is not enabled, then the B2BUA attempts to process all inbound SIP from Microsoft. If it receives SIP SIMPLE, it tries to route it as if it were SIP audio/video traffic. The SIP SIMPLE will probably be rejected by the call control infrastructure in this case. |

Applications

| Field | Description | Usage tips |
|---|--|---|
| Listening port on presence destination servers | This is the port configured on the IM and Presence Service nodes. | |
| Destination presence server 1..6 | IP address, hostname, or FQDN of the IM and Presence Service node. | Enter up to 6. The Expressway polls them regularly to determine liveness state, and routes traffic to them using a round-robin algorithm. |
| TURN section: | | |
| Offer TURN services | Controls whether the B2BUA offers TURN services. Default is <i>No</i> . | This is recommended for calls traversing a Microsoft Edge server. To configure the associated TURN servers, click Configure B2BUA TURN servers . |
| Advanced settings: you should only modify the advanced settings on the advice of Cisco customer support. | | |
| Encryption | Controls how the B2BUA handles encrypted and unencrypted call legs. <i>Required:</i> both legs of the call must be encrypted. <i>Auto:</i> encrypted and unencrypted combinations are supported. The default is <i>Auto</i> . | 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 Microsoft client. Either leg of the call could be encrypted or unencrypted. 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. |
| B2BUA media port range start/end | 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. You may need to increase this range if you Enable RDP Transcoding for this B2BUA , because desktop sharing increases the number of media ports required per call. |
| Hop count | Specifies the Max-Forwards value to use in SIP messages. Default is 70. | |
| Session refresh interval | 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 RFC 4028 . |
| Minimum session refresh interval | 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 RFC 4028 . |
| Port on B2BUA for Expressway communications | The port used on the B2BUA for communicating with the Expressway. Default is 65070. | |
| Port on B2BUA for Microsoft call communications | The port used on the B2BUA for call communications with the Microsoft server. Default is 65072. | |

Applications

| Field | Description | Usage tips | | | | | | | | |
|---------------------------------------|---|--|---|------------|----|---------------------------------------|----|----------|--|---|
| RDP TCP port range start / end | <p>Defines the range of TCP ports on which the transcoder instances listen for RDP media. Default is 6000 - 6099.</p> <p>Note: Save the page and restart the Microsoft interoperability service to apply your changes.</p> | Each simultaneous RDP transcoding session created on the B2BUA requires a receiving port. The range is limited to 100 as this is the maximum possible number of simultaneous transcode sessions. | | | | | | | | |
| RDP UDP port range start / end | <p>Defines the range of UDP ports from which the transcoder instances transmit H.264 media. Default is 6100 - 6199.</p> <p>Note: Save the page and restart the Microsoft interoperability service to apply your changes.</p> | Each simultaneous RDP transcoding session created on the B2BUA requires a port to send out the resulting H.264 media. The range is limited to 100 as this is the maximum possible number of simultaneous transcode sessions. | | | | | | | | |
| Maximum RDP transcode sessions | <p>Limits the number of simultaneous RDP transcoding sessions on this Expressway. Default is 10.</p> <p>Note: Save the page and restart the Microsoft interoperability service to apply your changes.</p> <p>Table 16 Recommended Number of Desktop Transcode Sessions by Platform</p> <table border="1"> <thead> <tr> <th>On this platform:</th> <th>Set Maximum RDP transcode sessions to:</th> </tr> </thead> <tbody> <tr> <td>Medium OVA</td> <td>10</td> </tr> <tr> <td>‡ CE500/ CE1000/ CE1100, or Large OVA</td> <td>20</td> </tr> <tr> <td>Clusters</td> <td>Same as the individual platform setting. The Maximum RDP transcode sessions you enter on the primary applies to each peer in the cluster.</td> </tr> </tbody> </table> <p>‡ From X8.10 onwards, the requirement to have a 10 Gbps NIC in order to achieve the scalability of a large system is removed. It is now possible to have the capacity of a large system with a 1 Gbps NIC subject to your bandwidth constraints.</p> | On this platform: | Set Maximum RDP transcode sessions to: | Medium OVA | 10 | ‡ CE500/ CE1000/ CE1100, or Large OVA | 20 | Clusters | Same as the individual platform setting. The Maximum RDP transcode sessions you enter on the primary applies to each peer in the cluster. | Higher values will mean that more system resources can be consumed by RDP transcoding, which could impact other services. Maximum is 100. |
| On this platform: | Set Maximum RDP transcode sessions to: | | | | | | | | | |
| Medium OVA | 10 | | | | | | | | | |
| ‡ CE500/ CE1000/ CE1100, or Large OVA | 20 | | | | | | | | | |
| Clusters | Same as the individual platform setting. The Maximum RDP transcode sessions you enter on the primary applies to each peer in the cluster. | | | | | | | | | |

Configuring the B2BUA's Trusted Hosts

Go to **Applications > B2BUA > Microsoft Interoperability > Trusted hosts**) to specify the Microsoft hosts from which the Expressway will trust SIP signaling.

The interoperability service does not accept messages from any addresses that are not on the trusted hosts list.

Applications

Note that trusted host verification only applies to calls initiated by Microsoft clients 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 currently has a nominal limit of 25 trusted hosts. If there are more than 25 trusted hosts, the Expressway raises an alarm.

In practice, you can have more than 25 trusted hosts if you need them in your deployment. We recommend that you keep the number below 50, and you can safely ignore the alarm. If you need to go beyond 50, we recommend adding another Gateway Expressway.

The configurable options are:

| Field | Description | Usage tips |
|-------------------|--|--|
| Name | An optional free-form description of the trusted host. | The name is not used as part of the "trusted" criteria. It is only to help you distinguish between multiple hosts without relying on the IP addresses. |
| IP address | The IP address of the trusted host. | |
| Type | The type of device that may send signaling messages to the B2BUA. <i>Microsoft infrastructure:</i> this includes Hardware Load Balancers, Directors and Front End Processors <i>External transcoder:</i> a transcoder device such as a Cisco TelePresence Advanced Media Gateway | |

Configuring External Transcoder Policy Rules

Go to **Applications > B2BUA > Microsoft Interoperability > Transcoder policy rules**) to define rules that control which Microsoft interoperability calls are routed via a [transcoder](#).

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**.

If **Enable external transcoders for this B2BUA** is *Yes* (configured on the **Microsoft interoperability configuration** page), then all calls are routed via the external transcoders by default. If you want to reserve transcoder resources for specific types of calls, then you can specify rules to control which calls are routed to the external transcoders.

- The rules on this page only apply if **Use transcoder policy rules** is set to *Yes* (on the **Microsoft interoperability configuration** page).
- A rule is applied if it matches either the source or destination alias of a call.
- If call aliases do not match any policy rules, the call will be routed via the external transcoder.

You should set a general, low priority rule to match all aliases and deny transcoder resources - and then have more specific, higher priority rules to allow specific aliases to use the transcoder resources.

The configurable options are:

| Field | Description | Usage tips |
|--------------------|--|---|
| Name | The name assigned to the rule. | |
| Description | 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. |

Applications

| Field | Description | Usage tips |
|-----------------------|---|--|
| Priority | 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. |
| Pattern type | The way in which the Pattern string must match either the source or destination alias of the call. <i>Exact</i> : the entire string must exactly match the alias character for character. <i>Prefix</i> : the string must appear at the beginning of the alias. <i>Suffix</i> : the string must appear at the end of the alias. <i>Regex</i> : treats the string as a regular expression . | 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). |
| Pattern string | The pattern against which the alias is compared. | |
| Action | The action to take if the source or destination alias of the call matches this policy rule. <i>Allow</i> : the call can connect via the transcoder. <i>Deny</i> : the call can connect but it will not use transcoder resources. | |
| State | 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 External B2BUA Transcoders

Transcoders are used to convert digital media from one format to another. The only transcoder currently supported by the Microsoft interoperability service 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 clients and Cisco endpoints.

Go to **Applications > B2BUA > Microsoft Interoperability > External transcoders** 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
- Go to [Configuring Microsoft Interoperability, page 240](#) 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:

Applications

| Field | Description | Usage tips |
|----------------|---|--|
| Name | An optional free-form description of the transcoder. | |
| Address | 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> |
| Port | The listening port on the transcoder. | |

Restarting the Microsoft Interoperability Service

Sometimes you need a restart to apply changes to the Microsoft interoperability service. The system raises an alarm if you need a restart.

When you restart this service, the Expressway does not restart, but it does drop any calls that are being managed by the B2BUA.

1. Go to **Applications > B2BUA > Microsoft interoperability > Restart service...**
2. Check the number of active calls currently in place.
3. Click **Restart**.

The service restarts after a few seconds. You can check the service status on the [Microsoft Interoperability page](#).

Clustered Expressway systems

You must restart the Microsoft interoperability service on every peer. Configure, restart and verify the service on the primary before restarting the service on other peers.

FindMe™

FindMe is a form of User Policy, which is the set of rules that determines what happens to a call for a particular user or group when it is received by the Expressway.

The FindMe feature lets you assign a single FindMe ID to individuals or teams in your enterprise. By logging into their FindMe account, users can set up a list of locations such as "at home" or "in the office" and associate their devices with those locations. They can then specify which devices are called when their FindMe ID is dialed, and what happens if those devices are busy or go unanswered. Each user can specify up to 15 devices and 10 locations.

This means that potential callers can be given a single FindMe alias on which they can contact an individual or group in your enterprise – callers won't have to know details of all the devices on which that person or group might be available.

To enable this feature you must purchase and install Desktop System or TelePresence Room System registration licenses.

End-User FindMe Account Configuration

From version X8.8, users can configure their FindMe settings using Cisco TMS provisioning:

- If Cisco TMS provisioning is enabled:
 - Users manage their FindMe settings by logging in to Cisco TMS using their FindMe account.
 - User account and FindMe data is provided from Cisco TMS to Expressway by the [TMS Provisioning Extension services](#).

See [FindMe Deployment Guide](#) for more details about setting up FindMe accounts.

How are Devices Specified?

When configuring their FindMe account, users are asked to specify the devices to which calls to their FindMe ID are routed.

It is possible to specify aliases and even other FindMe IDs as one or more of the devices. However, care must be taken in these situations to avoid circular configurations.

For this reason, we recommend that users specify the physical devices they want to ring when their FindMe ID is called by entering the alias with which that device has registered.

Principal devices

A FindMe user's account should be configured with one or more principal devices. These are the main devices associated with that account.

Users are not allowed to delete or change the address of their principal devices. This is to stop users from unintentionally changing their basic FindMe configuration.

Principal devices are also used by the Expressway to decide which FindMe ID to display as a **Caller ID** if the same device address is associated with more than one FindMe ID. Only an administrator (and not FindMe users themselves) can configure which of a FindMe user's devices are their principal devices.

FindMe Process Overview

When the Expressway receives a call for a particular alias it applies its User Policy as follows:

- It first checks to see if FindMe is enabled. If so, it checks if the alias is a FindMe ID, and, if it is, the call is forwarded to the aliases associated with the active location for that user's FindMe configuration.
- If FindMe is not enabled, or the alias is not a FindMe ID, the Expressway continues to search for the alias in the usual manner.

Applications

Note that User Policy is invoked after any Call Policy configured on the Expressway has been applied. See [Call Routing Process, page 181](#) for more information.

Recommendations when Deploying FindMe

- The FindMe ID should be in the form of a URI, and should be the individual's primary URI.
- Endpoints should not register with an alias that is the same as an existing FindMe ID. You can prevent this by including all FindMe IDs on the Deny List.

Example

Users at Example Corp. have a FindMe ID in the format `john.smith@example.com`. Each of the user's endpoints are registered with a slightly different alias that identifies its physical location. For example their office endpoint is registered with an alias in the format `john.smith.office@example.com` and their home endpoint as `john.smith.home@example.com`.

Both of these endpoints are included in the list of devices to ring when the FindMe ID is dialed. The alias `john.smith@example.com` is added to the Deny List, to prevent an individual endpoint registering with that alias.

Configuring FindMe

The **FindMe configuration** page (**Applications > FindMe**) is used to enable and configure [FindMe User Policy](#).

Note that you can only access the **FindMe configuration** page if you are entitled to use FindMe. You need to install Desktop or Room registration licenses.

The configurable options are:

| Field | Description | Usage tips |
|--------------------|---|---|
| FindMe mode | Determines whether or not FindMe is enabled, and if a third-party manager is to be used. <i>Off:</i> disables FindMe. <i>Remote service:</i> enables FindMe and uses a FindMe manager located on an off-box system (eg.TMS). | Call Policy is always applied regardless of the FindMe mode. If you enable FindMe, you must ensure a Cluster name is specified (you do this on the Clustering page). |
| Caller ID | Determines how the source of an incoming call is presented to the callee. <i>Incoming ID:</i> displays the address of the endpoint from which the call was placed. <i>FindMe ID:</i> displays the FindMe ID associated with the originating endpoint's address. | Using <i>FindMe ID</i> means that if the recipient subsequently returns that call, all the devices associated with that FindMe account will be called. The FindMe ID is only displayed if the source endpoint has been authenticated (or treated as authenticated). If it is not authenticated the Incoming ID is displayed. See About Device Authentication, page 135 for more details. |

The following options apply when **FindMe mode** is *Remote service*:

| Field | Description |
|-----------------|---|
| Protocol | The protocol used to connect to the remote service. |
| Address | The IP address or domain name of the remote service. |
| Path | The URL of the remote service. |
| Username | The username used by the Expressway to log in and query the remote service. |

Applications

| Field | Description |
|-----------------|---|
| Password | The password used by the Expressway to log in and query the remote service. |

Management and Storage of FindMe Data

If you use FindMe and want to use Cisco TMS to manage your FindMe data, you must configure Cisco TMSPE services to provide the Expressway with FindMe data.

Cisco TMS Provisioning

Cisco TMS provisioning is the mechanism through which the Expressway and Cisco TMS share FindMe and device provisioning data. The shared data includes:

- user account, device and phone book data that is used by the Expressway to service [provisioning requests](#) from endpoint devices
- FindMe account configuration data that is used by the Expressway to provide [FindMe services](#)

The **FindMe** and **Device Provisioning** option keys must be installed on the Expressway for it to provide FindMe and provisioning services.

As from version X8.8, the Expressway supports only the Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) services to provide the Expressway with provisioning and FindMe data. In this mode all provisioning and FindMe data is managed and maintained exclusively within Cisco TMS.

Size limitations for clusters and provisioning

An Expressway cluster of any size supports up to:

- 10,000 FindMe accounts
- 10,000 users for provisioning
- 200,000 phonebook entries

Note that:

- **Small/Medium** systems can support up to 2,500 device registrations per peer, subject to a maximum of 10,000 registrations per cluster. Typically this means one device per FindMe account.
- **Large** systems can support up to 5,000 device registrations per peer (with a maximum of 20,000 registrations per cluster). However, you are still limited to 10,000 FindMe accounts/users and 10,000 provisioned devices per cluster.

If you need to provision more than 10,000 devices, your network will require additional Expressway clusters with an appropriately designed and configured dial plan.

See [Cisco TMS Provisioning Extension Deployment Guide](#) for full information about how to configure provisioning in Cisco TMS and Expressway.

Cisco TMSPE services

When TMS provisioning is enabled, the Expressway uses the following Cisco TMSPE services (which are hosted on Cisco TMS) to provide the Expressway (or Expressway cluster) with provisioning and FindMe data:

| Service | Description |
|------------------------|--|
| User Preference | The data provided by the User Preference service enables the Expressway to configure a device with settings that pertain to a specific user (a user is essentially a SIP URI). Devices such as Jabber Video are configured entirely using this service. This service also provides connection details to a TURN server (typically the Expressway-E). |
| FindMe | The FindMe service provides the details of users' FindMe accounts, in particular the locations and devices associated with each FindMe ID. This allows the Expressway to apply its User Policy, and to be able to change a caller's source alias to its corresponding FindMe ID. |
| Phone books | The Phone books service provides the data that allows users to search for contacts within phone books. Access to phone books is controlled on a per user basis according to any access control lists that have been defined (within Cisco TMS). |

Applications

| Service | Description |
|----------------|---|
| Devices | <p>The Devices service exchanges provisioning licensing information between the Expressway and Cisco TMS. Information is exchanged every 30 seconds – the Expressway is provided with the current number of free licenses available across the range of Expressway clusters being managed by Cisco TMS, and the Expressway updates Cisco TMS with the status of provisioning licenses being used by this Expressway (or Expressway cluster).</p> <p>If the Devices service is not active, the Expressway's Provisioning Server will not be able to provision any devices.</p> |

The current status of the services is displayed on the [TMS Provisioning Extension service status](#) page.

- The Expressway periodically polls the Cisco TMSPE services to ensure the data held on Expressway is kept up to date. The polling interval can be defined for each service. In typical deployments you are recommended to use the default settings which provide frequent (every 2 minutes) updates to FindMe and user provisioning data, and daily updates to phone book data.

If you have a cluster of Expressways, only one of the cluster peers maintains the physical connection to Cisco TMS. The data obtained from Cisco TMS is then shared between other peers in the cluster through the Expressway's cluster replication mechanism.

- A full and immediate resynchronization of all data between the Expressway and Cisco TMS can be triggered at any time by clicking **Perform full synchronization** (at the bottom of the of the **TMS Provisioning Extension services** page). Note that this will result in a temporary (a few seconds) lack of service on the Expressway while the data is deleted and fully refreshed. If you only need to ensure that all of the latest updates within Cisco TMS have been supplied to the Expressway then click **Check for updates** instead.

You are recommended to use Cisco TMS to make any changes to the Cisco TMSPE services' configuration settings. You can configure the services on the Expressway through the **TMS Provisioning Extension services** page, but any changes made to the settings via this page will not be applied within Cisco TMS.

Expressway Provisioning Server

The Expressway Provisioning Server provides provisioning-related services to provisioned devices, using data supplied by Cisco TMS through the [Cisco TMS provisioning](#) mechanism. The server only operates if the **Device Provisioning** option key is installed.

As from version X8.8, the Expressway supports only the Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) services to provide the Expressway with provisioning and FindMe data. In this mode all provisioning and FindMe data is managed and maintained exclusively within Cisco TMS.

Provisioning Server Status

Comprehensive status information can be found under the Expressway's (**Status > Applications > TMS Provisioning Extension services**) menu options.

Provisioning Licenses

There is a limit to the number of devices that can be provisioned concurrently by the Provisioning Server. Expressway and Cisco TMS manage the number of available provisioning licenses by exchanging information through the Cisco TMSPE Devices service. If the Devices service is not active, the Expressway's Provisioning Server will not be able to provision any devices.

The Expressway is provided with the current number of free licenses available across the range of Expressway clusters being managed by Cisco TMS, and the Expressway updates Cisco TMS with the status of provisioning licenses being used by this Expressway (or Expressway cluster). License limits can be managed at a per device type basis.

- Go to **Status > Applications > TMS Provisioning Extension services > Device requests** to see a summary status of the provisioning licenses that are available within your system.

Applications

- Go to **Status > Applications > TMS Provisioning Extension services > Provisioned device status** to see a list of all of the devices that have submitted provisioning requests to the Provisioning Server.

Note that some devices, including Jabber Video 4.x, do not inform the Expressway when they sign out (unsubscribe) from being provisioned. The Expressway manages these devices by applying a 1 hour timeout interval before releasing the license.

Provisioning and Device Authentication

The Provisioning Server requires that any provisioning or phone book requests it receives have already been authenticated at the zone or subzone point of entry into the Expressway. The Provisioning Server does not do its own authentication challenge and will reject any unauthenticated messages.

See [Device Provisioning and Authentication Policy, page 139](#) for more information.

Hybrid Services and Connector Management

If you are already registered for Hybrid Services, visit the [Hybrid Services help site](#) to get more detailed and recent information.

[What are Spark Hybrid Services and what do they do?](#)

Cisco Spark Hybrid Services empower cloud-based and premises-based solutions to deliver a more capable, better integrated collaboration user experience.

[Which services am I entitled to use?](#)

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

[What software do I need?](#)

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

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

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

[How do I install, upgrade, or downgrade?](#)

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

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

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

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

[Where can I read more about Spark Hybrid Services?](#)

Hybrid Services are continuously developed and may be published more frequently than Expressway. This means that

Applications

information about Hybrid Services is maintained on the [Hybrid Services help site](#), and several Expressway interface pages link out to that site.

Connector Proxy

If you are already registered for Hybrid Services, visit the [Hybrid Services help site](#) to get more detailed and recent information.

[What is this proxy for?](#)

Use the **Applications > Hybrid Services > Connector Proxy** page if this Expressway needs a proxy to connect to the Cisco Collaboration Cloud. This proxy is not used by the Expressway for other purposes.

[What kind of traffic goes through this proxy?](#)

The proxy must be capable of handling outbound HTTPS and secure web socket connections. It must also allow those connections to be initiated by the Expressway using either basic authentication or no authentication.

[What details do I need to configure the proxy?](#)

You'll need the address of the proxy, the port it's listening on, and the basic authentication username and password (if your proxy requires authentication).

Collaboration Cloud CA Root Certificates on Expressway-E

The Cisco Collaboration Cloud CA root certificates are packaged in the Expressway software and you can click **Get certificates** to load them into the trusted CA list. You can click **Remove certificates** to reverse this decision if necessary.

The Expressway-E needs to trust these CAs so that it can authenticate the server certificates from Collaboration Cloud, to make the encrypted connections needed by some Expressway-based hybrid services.

Note: The Expressway-E cannot register for hybrid services. It must be connected by a secure traversal zone to the Expressway (or cluster) that is registered to the Collaboration Cloud.

Root certificates from the following CAs will be installed when you click **Get certificates**:

- O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority
- O=QuoVadis Limited, CN=QuoVadis Root CA 2
- O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority

You can verify that the certificates are installed, and manually maintain the trusted CA list, on the **Maintenance > Security > Trusted CA certificate** page. See [Managing the Trusted CA Certificate List, page 279](#) for more help.



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 | 255 |
| Configuring Password Security | 257 |
| Configuring Administrator Accounts | 258 |
| Configuring Remote Account Authentication Using LDAP | 260 |
| Resetting Forgotten Passwords | 265 |
| Using the Root Account | 266 |
| Managing SSO tokens | 266 |

About User Accounts

The Expressway has two types of user account for normal operation:

- **Administrator accounts:** used to configure the Expressway.
- **FindMe accounts:** used by individuals in an enterprise to configure their FindMe profile.

Account Authentication

Administrator and FindMe 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, page 260](#) and [Authenticating Expressway Accounts using LDAP Deployment Guide](#) for more information about setting up remote authentication.

If a remote source is used for either administrator or FindMe account authentication, you also need to configure the Expressway with:

- appropriate LDAP server connection settings
- administrator groups and/or FindMe groups that match the corresponding group names already set up in the remote directory service to manage administrator and FindMe access to this Expressway (see [Configuring Administrator Groups, page 263](#) and [Configuring user groups](#))

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.

User Accounts

- 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 one administrator account to be the emergency account. This special account gives access to the Expressway even when it disallows local authentication, in case remote authentication is not possible.

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 [Network Services, page 36](#)).
- If the system is in [advanced account security mode](#), a **Login history** page is displayed immediately after logging in. It shows the recent activity of the currently logged in account.

See the [Configuring Administrator Accounts, page 258](#) section for more information.

FindMe accounts

FindMe accounts are used by individuals in an enterprise to configure the devices and locations on which they can be contacted through their FindMe ID.

Each FindMe account is accessed using a username and password.

- If remote FindMe account authentication is selected, the Expressway administrator must set up FindMe groups to match the corresponding group names in the remote directory service. Note that only the username and password details are managed remotely. All other properties of the FindMe account, such as the FindMe ID, devices and locations are stored in the local Expressway database.

See the [Configuring FindMe accounts](#) section for more information about defining FindMe account details and their associated FindMe devices and locations.

We recommend that you use Cisco TMS if you need to provision a large number of FindMe accounts. See [Cisco TMS Provisioning Extension Deployment Guide](#) for more details on configuring FindMe and user accounts.

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 an administrator account instead.

See the [Using the Root Account, page 266](#) section for more information.

SECURITY CAUTION: The pre-X8.9 default passwords of the **admin** and **root** accounts are well known. You must use strong passwords for these accounts. If your new system is on X8.9 or later, you must supply non-default passwords on startup.

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
- Nominate an emergency account

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.

The username for this account is **admin** (all lower case).

Before X8.9, the default password was **TANDBERG** (all upper case). From X8.9 onwards, new systems run a secure install wizard on startup, so that you can provide new passwords before the system is connected to the network.

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.

If your system was upgraded from a pre-X8.9 version, you may need to change the password. 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, page 265](#) for details.

Administrator account fields reference

| Field | Description | Usage tips |
|-------------|---|--|
| Name | The username for the administrator account. | Some names such as "root" are reserved. Local administrator account user names are case sensitive. |

User Accounts

| Field | Description | Usage tips |
|--------------------------|---|--|
| Access level | <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 admin account.</p> <p><i>Read-only</i>: allows status and configuration information to be viewed only and not changed. Some pages, such as the Upgrade page, are blocked to read-only accounts.</p> <p><i>Auditor</i>: allows access to the Event Log, Configuration Log, Network Log, Alarms and Overview 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 admin account cannot be changed from <i>Read-write</i>.</p> |
| Password | <p>The password that this administrator will use to log in to the Expressway.</p> | <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 Password field changes color to indicate the complexity of the password. You can configure the complexity requirements for local administrator passwords on the Password security page (Users > Password security).</p> <p>You cannot set blank passwords.</p> |
| New password | <p>Enter a new password for the account.</p> | <p>This field only appears when you are changing a password.</p> |
| Confirm password | <p>Re-enter the password for the account.</p> | <p>This field only appears when you create an account or when you change its password.</p> |
| Emergency account | <p>Select <i>Yes</i> to use this account as the emergency account.</p> <p>You must use an enabled local administrator account that has read-write access and web access.</p> | <p>You may only have one emergency account, and you can use this account to gain access to the Expressway even if it does not allow local authentication.</p> <p>The purpose of this account is to help you work around being locked out of the system when remote authentication is not available.</p> |
| Web access | <p>Select whether this account is allowed to log in to the system using the web interface.</p> <p>Default: <i>Yes</i></p> | |
| API access | <p>Select whether this account is allowed to access the system's status and configuration using the Application Programming Interface (API).</p> <p>Default: <i>Yes</i></p> | <p>This controls access to the XML and REST APIs by systems such as Cisco TMS.</p> |

User Accounts

| Field | Description | Usage tips |
|------------------------------|---|---|
| State | Select whether the account is <i>Enabled</i> or <i>Disabled</i> . Disabled accounts are not allowed to access the system. | |
| Your current password | 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 |
|---|--|---|
| Remote account authentication: this section allows you to enable or disable the use of LDAP for remote account authentication. | | |
| Administrator authentication source | <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 admin 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> |
| LDAP server configuration: this section specifies the connection details to the LDAP server. | | |

| Field | Description | Usage tips |
|--|---|---|
| FQDN address resolution | <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> <p>Note: if you use SRV records, ensure that the records use the standard ports for LDAP. <code>_ldap._tcp.<domain></code> must use 389 and <code>_ldaps._tcp.<domain></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 Encryption 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> |
| Host name and Domain or Server address | <p>The way in which the server address is specified depends on the FQDN address resolution setting:</p> <p><i>SRV record:</i> only the Domain portion of the server address is required.</p> <p><i>Address record:</i> enter the Host name and Domain. These are then combined to provide the full server address for the DNS address record lookup.</p> <p><i>IP address:</i> the Server address 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> |
| Port | <p>The IP port to use on the LDAP server.</p> | <p>Non-secure connections use <i>389</i> and secure connections use <i>636</i>.</p> |
| Encryption | <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 Upload a CA certificate file for TLS (in the Related tasks section) to go to the Managing the Trusted CA Certificate List, page 279 page.</p> |
| Certificate revocation list (CRL) checking | <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>Authentication configuration: this section specifies the Expressway's authentication credentials to use when binding to the LDAP server.</p> | | |

| Field | Description | Usage tips |
|--|---|---|
| Bind DN | The distinguished name (case insensitive) used by the Expressway when binding to the LDAP server. It is important to specify the DN in the order cn=, then ou=, then dc= | 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. The bind account is usually a read-only account with no special privileges. |
| Bind password | The password (case sensitive) used by the Expressway when binding to the LDAP server. | The maximum plaintext length is 60 characters, which is then encrypted. |
| SASL | The SASL (Simple Authentication and Security Layer) mechanism to use when binding to the LDAP server. <i>None</i> : no mechanism is used. <i>DIGEST-MD5</i> : the DIGEST-MD5 mechanism is used. The default is <i>DIGEST-MD5</i> . | Enable Simple Authentication and Security Layer if it is company policy to do so. |
| Bind username | Username of the account that the Expressway will use to log in to the LDAP server (case sensitive). Only required if SASL is enabled. | Configure this to be the sAMAccountName; Security Access Manager Account Name (in AD this is the account's user logon name). |
| Directory configuration: this section specifies the base distinguished names to use when searching for account and group names. | | |
| Base DN for accounts | The ou= and dc= definition of the Distinguished Name where a search for user accounts should start in the database structure (case insensitive). 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. |
| Base DN for groups | The ou= and dc= definition of the Distinguished Name where a search for groups should start in the database structure (case insensitive). It is important to specify the DN in the order ou=, then dc= | If no Base DN for groups 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. |

User Accounts

| Error message | Reason / resolution |
|---|---|
| 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 Base DN for accounts ; 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 Bind DN and Bind password , this error can also be displayed if SASL is set to <i>DIGEST-MD5</i> when it should be set to <i>None</i> . |
| Invalid bind DN | Check Bind DN ; the current value does not describe a valid account in the LDAP director. This failed state may be wrongly reported if the Bind DN 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 Bind DN is wrong, the group is wrong or one of the other configuration items may be wrong. |
| 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 |
|-------------|---|---|
| Name | The name of the administrator group. It cannot contain any of the following characters: / \ [] : ; = , + * ? > < @ " | 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. |

User Accounts

| Field | Description | Usage tips |
|---------------------|--|--|
| Access level | <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 admin account.</p> <p><i>Read-only</i>: allows status and configuration information to be viewed only and not changed. Some pages, such as the Upgrade page, are blocked to read-only accounts.</p> <p><i>Auditor</i>: allows access to the Event Log, Configuration Log, Network Log, Alarms and Overview 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 Determining the access level for accounts that belong in multiple groups, page 264 below for more information.</p> |
| Web access | <p>Determines whether members of this group are allowed to log in to the system using the web interface.</p> <p>Default: <i>Yes</i></p> | |
| API access | <p>Determines whether members of this group are allowed to access the system's status and configuration using the Application Programming Interface (API).</p> <p>Default: <i>Yes</i></p> | <p>This controls access to the XML and REST APIs by systems such as Cisco TMS.</p> |
| State | <p>Indicates if the group is enabled or disabled. Access will be denied to members of disabled groups.</p> | <p>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>.</p> |

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 |
|-----------------------|--------------|------------|------------|
| Administrators | Read-write | - | - |
| Region A | Read-only | Yes | - |
| Region B | Read-only | - | Yes |
| Region C | 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 |
|---|--|
| Administrators and Region A | read-write access to the web interface but no API access |

| Groups belonged to | Access permissions granted |
|------------------------------------|---|
| Administrators and Region B | read-write access to the API interface, but no web interface access |
| Administrators and Region C | read-write access to the web and API interfaces |
| Region A 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.

Note: Stored configuration and data will not be affected when you reset your password.

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**.
3. Reboot the Expressway.
4. In the vSphere console log in with the username **pwrec**. No password is required.
5. When prompted, select the account (*root* or the username of the administrator account) 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 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

Note: This page applies to standard OAuth tokens configured by the **Authorize by OAuth token** setting. It does not apply to self-describing OAuth tokens (configured by **Authorize by OAuth token with refresh**).

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.

User Accounts

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 | 269 |
| Enabling Maintenance Mode | 270 |
| About Upgrading Software Components | 270 |
| Configuring Logging | 273 |
| Managing Option Keys | 277 |
| About Security | 278 |
| About Domain Certificates and Server Name Indication for Multitenancy | 289 |
| Domain Certificates and Clustered Systems | 293 |
| Advanced Security | 293 |
| Configuring Language Settings | 298 |
| Backing Up and Restoring Expressway Data | 299 |
| Diagnostics Tools | 302 |
| Incident Reporting | 304 |
| Checking the Effect of a Pattern | 307 |
| Locating an Alias | 307 |
| Port Usage | 308 |
| Network Utilities | 309 |
| Restarting, Rebooting and Shutting Down | 312 |
| Developer Resources | 313 |

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 registrations or calls from being managed by that peer:

- Standard Expressway sessions:
 - New calls and registrations will be handled by another peer in the cluster.
 - Existing registrations are allowed to expire and they then should re-register to another peer (see *Expressway Cluster Creation and Maintenance Deployment Guide* for more information about endpoint configuration and setting up DNS SRV records).
 - 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 registrations and calls are currently being handled by that peer.
- Maintenance mode is automatically disabled if the peer is restarted.
- Maintenance mode is not supported over MRA for endpoints running CE software. The Expressway drops MRA calls from these endpoints when you enable maintenance mode.

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.
- From X8.8 onwards, the Expressway release packages are signed to give you confidence in their integrity.

Maintenance

- If your Expressway is registered for Hybrid Services: **Important! Your Management Connector must be up to date before you upgrade your Expressway. You must authorize and accept any Management Connector upgrades advertised by the Cisco Collaboration Cloud before attempting to upgrade your Expressway. Failure to do so may cause issues with the connector once you have upgraded your Expressway.**
- If you are upgrading a cluster:
See *Expressway Cluster Creation and Maintenance Deployment Guide* on the [Expressway Configuration Guides page](#).

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, and all current registrations to be ended.

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 you make 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 versions of Expressway software components. (Downgrading to an older version is not supported.)

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:
 - the expected **New software version** number is displayed
 - 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 and registrations 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**).

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.

Maintenance

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](#)
- toggle [Call Detail Records](#)
- define one or more [remote syslog server](#) addresses
- filter the events sent to each remote syslog server by severity
- toggle [System Metrics Collection](#)

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 | High-level events such as registration requests and call attempts. Easily human readable. For example: <ul style="list-style-type: none"> ■ call attempt/connected/disconnected ■ registration attempt accepted/rejected |
| 2 | All Level 1 events, plus: 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 |

Maintenance

| Level | Assigned events |
|-------|--|
| 3 | All Level 1 and Level 2 events, plus: <ul style="list-style-type: none"> ■ protocol keepalives ■ call-related SIP signaling messages |
| 4 | The most verbose level: all Level 1, Level 2 and Level 3 events, plus: <ul style="list-style-type: none"> ■ network level SIP messages |

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 200th 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.

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.

Maintenance

If you select *Service only* the system keeps the CDRs for 7 days, and these CDRs can only be read via the Representational State Transfer (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.

How to Configure CDRs

To configure CDRs on Expressway:

1. Go to **Maintenance > Logging**.
2. In the **Logging Options** section, set the **Call Detail Records** field following the below guide.

| CDR Mode | Description |
|-----------------------------|---|
| <i>Off</i> | CDRs are not logged locally (default). |
| <i>Service Only</i> | CDRs are stored locally for 7 days and then deleted. The records are not accessible via the web GUI. |
| <i>Services and Logging</i> | CDRs are stored locally for 7 days and then deleted. The records are accessible from the local event log and the external syslog server if external logging has been enabled. |

For more information:

See the *Cisco Expressway Serviceability Guide* on the [Expressway Maintain and Operate Guides](#) page.

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. Click on the **Options** button for each server.
3. Specify the **Transport** protocol and **Port** you wish to use. The default is *UDP* over port *514*. If you choose to use TLS, you will see the option to enable Certificate Revocation List (CRL) checking for the syslog server.
4. In the **Message Format** field, select the writing format for remote syslog messages. The default is *Legacy BSD*.
5. Use the **Filter by Severity** option to select how much detail to send. The Expressway sends messages of the selected severity and all of the more severe messages.
6. Use the **Filter by Keywords** option if you only want to send messages with certain keywords.
7. Click **Save**.

Notes:

- The **Filter by Keywords** option is applied to messages already filtered by severity.
- You can use up to five keywords, which includes groups of words (for example 'login successful'), separated by commas.
- You can use a maximum of 256 characters in the keyword search.

Maintenance

- We recommend that you search for the most relevant keywords first to avoid any impact on system performance. This ensures the system pushes the relevant log messages to the syslog server at the earliest opportunity.

What are the Typical Values used for my Syslog Server?

The following table should help you select the format that best matches your logging server(s) and network configuration and shows the typical values used.

Table 17 Syslog message formats

| Message format | Transport protocol | Suggested port | RFC |
|---|--------------------|----------------|---|
| <i>Legacy BSD format</i> | UDP | 514 | BSD format. See RFC 3164 |
| <i>IETF syslog format</i> | UDP | 514 | IETF format. See RFC 5424 |
| <i>IETF syslog using TLS connection</i> | TLS | 6514 | IETF format. See RFC 5424 |

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 when using TLS is disabled by default. To enable CRL, set **CRL checking** to *On* and ensure that relevant certificate revocation lists (CRLs) are loaded.
See [About Security, page 278](#) 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*

Configure System Metrics Collection on Expressway

In the following procedure you'll use the web interface to configure the Expressway to collect statistics and publish them to a specified server.

1. Log on to the Expressway and go to **Maintenance > Logging**.
2. Toggle **System Metrics Collection** to *On*.

Maintenance

3. Enter the Collection server address.

You can use IP address, hostname or FQDN to identify the remote server.

4. Change the Collection Interval and Collection server port if necessary.

You may need to change the port if the collection server is listening on a different port to the default (25826). You may need to change the collection interval if your policy requires finer metrics than the default interval (60s).

5. Click Save.

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.

Note: When installing an option key on your system you must ensure you remove any demo option key in relation to the feature or it may stop working when the demo key expires.

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.
- **FindMe™:** enables [FindMe](#) functionality.
- **Advanced Networking:** enables the LAN 2 port on an Expressway, and enables static NAT functionality on an Expressway-E.
- **Device Provisioning:** enables the Expressway's [Provisioning Server](#). This allows Expressway to provision endpoints with configuration information on request and to supply endpoints with phone book information. (Endpoints including Jabber Video, E20, and the EX and MX Series can request to be provisioned.) Note that the Expressway must use Cisco TMS to obtain configuration and phone book information for distribution.
- **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, page 377](#) 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, page 57](#) for more information.
- **Encryption:** indicates that AES (and DES) encryption is supported by this software build.
- **Advanced account security:** enables [advanced security](#) features and restrictions for high-security installations.
- **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.
- **TelePresence Room Systems:** adds to the number of room systems that may register to the Expressway.
- **TelePresence Desktop Systems:** adds to the number of desktop systems that may register to the Expressway.

See [License Usage Within a Cluster, page 171](#) for more information about how rich media session and TURN relay option key licenses are shared across all peers in the cluster.

See [Product Identifiers and Corresponding Keys, page 380](#), for all option keys and associated PIDs.

Maintenance

Removing demo option keys

When installing an option key for a feature permanently on your system, you must first ensure you remove any demo option key in relation to the feature and restart your system.

Otherwise, the feature may become locked and stop working when the demo option key, which is time-limited, expires.

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**.

The following option keys require that you restart the Expressway before the option key takes effect:

- Traversal Server
- Expressway Series
- Advanced Account Security (if moved into FIPS mode)

When a restart is required, you receive an alarm on the web interface, which remains in place as a notification until you restart the system. 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

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. The 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 lets you install a certificate that can represent the Expressway 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 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.

Table 18 Expressway Role in Different Connection Types

| In connections... | The Expressway acts as... |
|---------------------------------|--|
| To an endpoint. | TLS server. |
| To an LDAP server. | Client. |
| Between two Expressway systems. | Either Expressway may be the client. The other Expressway is the TLS server. |
| Over HTTPS. | Web browser is the client. Expressway is the server. |

TLS can be difficult to configure. For example, when using it with an LDAP server we recommend verifying that the system works correctly over TCP, before you attempt to secure the connection with TLS. We also recommend using a third-party LDAP browser to verify that your LDAP server is correctly configured for TLS.

Note: Be careful not to allow your CA certificates or CRLs to expire. 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, page 279](#) and [Managing the Expressway's Server Certificate, page 279](#) 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 > 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

You manage the Expressway's server certificate through the **Server certificate** page (**Maintenance > Security > 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 use the **Server certificate** page to:

- View details about the currently loaded certificate.
- Generate a certificate signing request.
- Upload a new server certificate.

Note: We highly recommend using certificates based on RSA keys. Other types of certificate, such as those based on DSA keys, are not tested and may not work with the Expressway in all scenarios.

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 > 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, page 281](#) if your Expressway is part of a cluster.
 - See [Server Certificate Requirements for Unified Communications, page 64](#) 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.
- From version X8.10, you cannot select SHA-1.

Uploading a new server certificate

When the signed server certificate is received back from the certificate authority it must be uploaded to the Expressway. Use the **Upload new certificate** section to replace the Expressway's current server certificate with a new certificate.

Maintenance

To upload a server certificate:

1. Go to **Maintenance > Security > 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 14 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" with the following fields and values:

- 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". To its right is a "Format" 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 four 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 alternative names (SAN):

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

The Unified CM registration domains used in the Expressway configuration and Expressway-E certificate, are used by Mobile and Remote Access clients to lookup the `_co11ab-edge` DNS SRV record during service discovery. They enable MRA registrations on Unified CM, and are primarily for service discovery.

These service discovery domains may or may not match the SIP registration domains. It depends on the deployment, and they don't have to match. One example is a deployment that uses a `.local` or similar private domain with Unified CM on the internal network, and public domain names for the Expressway-E FQDN and service discovery. In this case, you need to include the public domain names in the Expressway-E certificate as SANs. There is no need to include the private domain names used on Unified CM. You only need to list the edge domain as a SAN.

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 `co11ab-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.

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

Figure 15 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 the 'Alternative name' configuration page in the Expressway-E CSR generator. It includes the following fields and options:

- Subject alternative names:** A dropdown menu with the value 'FQDN of Expressway cluster plus FQDN of this peer' and an information icon.
- 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 for 'Format' set to 'CollabEdgeDNS' with an information icon.
- XMPP federation domains:** A text input field containing 'example.com' and a dropdown menu for 'Format' set to 'DNS' with an information icon.
- IM and Presence chat node aliases (federated group chat):** A text input field containing 'chatnode1.example.com,chatnode2.example.com' and a dropdown menu for 'Format' set to 'DNS' with an information icon.
- Alternative name as it will appear:** A list of generated SANs:
 - DNS:vcse.example.com
 - DNS:vcs-e-cluster.example.com
 - DNS:collab-edge.example.com
 - DNS:example.com
 - DNS:chatnode1.example.com
 - DNS:chatnode2.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.

Maintenance

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 only uses CRL data that has been embedded into the **Trusted CA certificate (Tools > Security > Trusted CA certificate)**.

For LDAP connections, Expressway does not download the CRL from Certificate Distribution Point URLs in the server or issuing CA certificates; it also does not use the manual or automatic update settings on the **CRL management** page.

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 > CRL management**.
2. Set **Automatic CRL updates** to *Enabled*.

Maintenance

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 > 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.

Maintenance

1. Go to **Configuration > SIP**.
2. Scroll down to the **Certificate revocation checking** section and configure the settings accordingly:

| Field | Description | Usage tips |
|---|--|--|
| Certificate revocation checking mode | Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment. | We recommend that revocation checking is enabled. |
| Use OCSP | 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. |
| Use CRLs | Controls whether Certificate Revocation Lists (CRLs) are used to perform certificate revocation checking. | CRLs can be used if the certificate does not support OCSP. CRLs can be loaded manually onto the Expressway, downloaded automatically from preconfigured URIs (see Managing Certificate Revocation Lists (CRLs) , page 282), or downloaded automatically from a CRL distribution point (CDP) URI contained in the X.509 certificate. |
| Allow CRL downloads from CDPs | Controls whether the download of CRLs from the CDP URIs contained in X.509 certificates is allowed. | |
| Fallback behavior | Controls the revocation checking behavior if the revocation status cannot be established, for example if the revocation source cannot be contacted. <i>Treat as revoked</i> : treat the certificate as revoked (and thus do not allow the TLS connection). <i>Treat as not revoked</i> : treat the certificate as not revoked. Default: <i>Treat as not revoked</i> | <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. |

Configuring Certificate-Based Authentication

The **Certificate-based authentication configuration** page (**Maintenance > Security > 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 (and FindMe accounts, if accessed via the Expressway) 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:

Maintenance

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.

Emergency Account and Certificate-based Authentication

Advanced account security mode requires that you use only remote authentication, but also mandates that you have an emergency account in case the authentication server is unavailable. See [Configuring Advanced Account Security Mode, page 293](#).

If you are using certificate-based authentication, the emergency account must be able to authenticate by presenting a valid certificate with matching credentials.

You should create a client certificate for the emergency account, make sure that the CN matches the **Username format**, and load the certificate into the emergency administrator's certificate store.

Testing Client Certificates

The **Client certificate testing** page (**Maintenance > Security > 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 \(CRLs\)](#), page 282).
- 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

Maintenance

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 `openssl1 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 > 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 Minimum TLS version and Cipher Suites

For improved security, TLS 1.2 or later is recommended for all encrypted sessions. If required (typically for compatibility reasons with legacy equipment), the minimum TLS versions can be configured to use versions 1.0 or 1.1.

The **Maintenance > Security > Ciphers** page allows you to configure the minimum supported TLS version for each service.

From X8.10, Expressway defaults to TLS version 1.2 when establishing secure connections for the following services:

- HTTPS
- SIP
- XMPP
- UC server discovery
- Forward proxy (over port 8445)
- Reverse proxy (over port 8443)

On upgrade, previous behavior and defaults persist so you won't be defaulted to TLS version 1.2. However, new installations will use the new defaults. So for new installations you should check that all browsers and other equipment that must connect to Expressway supports TLS version 1.2.

Cipher Suites

You can configure the cipher suite and minimum supported TLS version for each service on the Expressway. These services and cipher suites are shown in the table below. (The cipher strings are in OpenSSL format.)

Maintenance

| Services | Cipher Suite Values (Defaults) |
|---------------------------------|---|
| Forward proxy TLS ciphers | EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL |
| HTTPS ciphers | EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL |
| Reverse proxy TLS ciphers | EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL |
| SIP TLS ciphers | EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH |
| UC server discovery TLS ciphers | EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL |
| XMPP TLS ciphers | EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL |

For services where the Expressway can act as a client for example, HTTPS, the same minimum TLS version and cipher suites will be negotiated.

SIP Behavior – Disable ADH Recommendation

Some endpoints, for example E20, only support ADH when you connect to them, so ADH is enabled in the default cipher suites. However, if it's an inbound connection, for security reasons you should always add `!ADH` to disable it. If you remove the `ADH` from SIP then the outbound connections to some legacy endpoints will fail.

Known Issues

See the Release Notes for this release for the latest information on TLS version 1.2 support on other products.

Restarts Required

- SIP currently requires a restart after changing the cipher suite configuration. TLS protocol version continues to require a restart.
- XCP requires a restart after changing the cipher suite configuration or TLS protocol version.

About Domain Certificates and Server Name Indication for Multitenancy

Multitenancy is part of Cisco Hosted Collaboration Solution (HCS), and allows a service provider to share a Expressway-E cluster among multiple tenants.

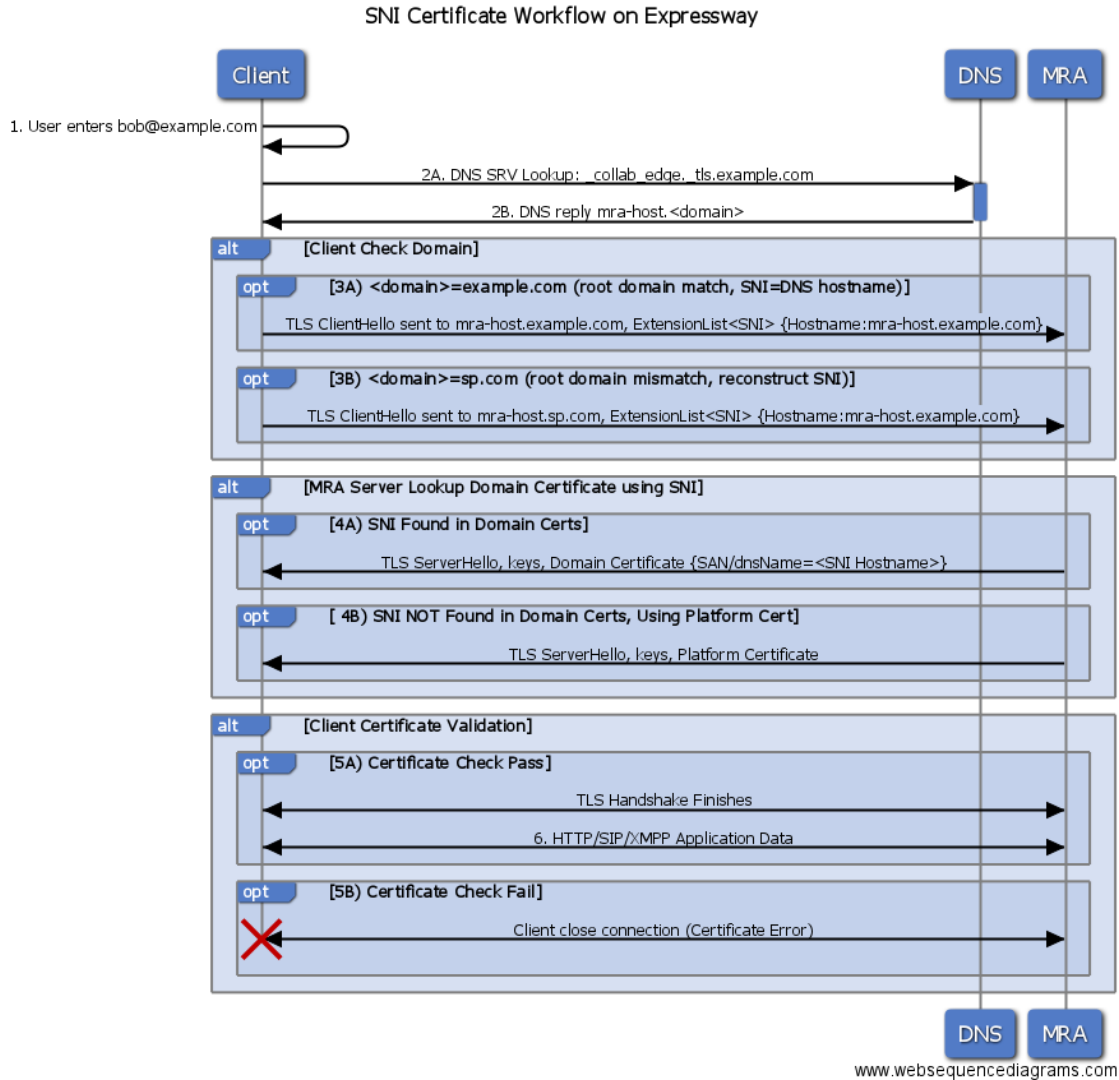
Using the Server Name Indication (SNI) protocol extension within TLS, the Expressway can now store and use domain-specific certificates that can be offered to a client during the TLS handshake. This capability allows seamless integration of endpoints registering through MRA in a multitenant environment, and ensures the certificate domain name matches the client's domain. During a TLS handshake, the client includes an SNI field in the *ClientHello* request. The Expressway looks up its certificate store and tries to find a match for the SNI hostname. If a match is found the domain-specific certificate is returned to the client.

Note: In multitenant mode, you must configure the system hostname on the **System > DNS** page of the Cisco Expressway-E to match the hostname configured in DNS (case-specific before X8.10.1, case insensitive from X8.10.1). Otherwise Cisco Jabber clients will be unable to register successfully for MRA.

See *Multitenancy with Cisco Expressway* on the [Cisco Hosted Collaboration Solution page](#).

SNI Call Flow

1. On the MRA client being registered, the user enters `bob@example.com` where `example.com` is the user's service domain (customer domain).
2. The client does a DNS resolution.
 - a. It sends a DNS SRV request for `_collab-edge._tls.example.com`.
 - b. The DNS replies to the request:
 - In a single tenant setup: the DNS reply usually includes the hostname within the service domain (for example, `mra-host.example.com`).
 - In a multitenant setup: DNS may instead return the service provider's MRA hostname in the service provider's domain, which is different from the user's service domain (for example, `mra-host.sp.com`).
3. The client sets up SSL connection.
 - a. The client sends SSL ClientHello request with an SNI extension:
 - If the DNS-returned hostname has the same domain as the user's service domain, the DNS hostname is used in SNI `server_name` (unchanged).
 - Otherwise, in the case of a domain mismatch, the client sets the SNI `server_name` to the DNS hostname plus the service domain (for example instead of the DNS-returned `mra-host.sp.com` it changes to `mra-host.example.com`).
 - b. The Expressway-E searches its certificate store to find a certificate matching the SNI hostname.
 - If a match is found, the Expressway-E will send back the certificate (SAN/dnsName=SNI hostname)
 - Otherwise, MRA will return its platform certificate.
 - c. The client validates the server certificate.
 - If the certificate is verified, SSL setup continues and SSL setup finishes successfully.
 - Otherwise, a certificate error occurs.
4. Application data starts. Note, for SIP and HTTPS, the application starts SSL negotiation immediately. For XMPP, the SSL connection starts once the client receives XMPP StartTLS.



Managing the Expressway's Domain Certificates

You manage the Expressway's domain certificates through the **Domain certificates** page (**Maintenance > Security > Domain certificates**). These certificates are used to identify domains when multiple customers – in a multitenant environment – are sharing a Expressway-E cluster to communicate with client systems using TLS encryption and with web browsers over HTTPS. You can use the domain certificate page to:

- View details about the currently loaded certificate.
- Generate a Certificate Signing Request (CSR).
- Upload a new domain certificate.

Note: We highly recommend using certificates based on RSA keys. Other types of certificate, such as those based on DSA keys, are not tested and may not work with the Expressway in all scenarios. Use the **Trusted CA certificate** page to manage the list of certificates for the Certificate Authorities (CAs) trusted by this Expressway.

Maintenance

Viewing a Currently Uploaded Domain Certificate

When you click on a domain, the domain certificate data section shows information about the specific domain certificate currently loaded on the Expressway.

To view the currently uploaded domain 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. To delete the currently uploaded domain click **Delete**.

Note: Do not allow your domain 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.

Adding a New Domain

1. Go to **Maintenance > Security > Domain certificates**.
2. Click **New**.
3. Under **New local domain**, enter the name of the domain you wish to add. An example valid domain name is `100.example-name.com`.
4. Click **Create domain**.
5. The new domain will be added on the **Domain certificates** page and you can proceed to upload a certificate for the domain.

Generating a Certificate Signing Request

The Expressway can generate domain CSRs. This removes the need to use an external mechanism to generate and obtain certificate requests.

To generate a CSR:

1. Go to **Maintenance > Security > Domain certificates**.
2. Click on the domain for which you wish to generate a CSR.
3. Click **Generate CSR** to go to the **Generate CSR** page.
4. Enter the required properties for the certificate.
 - See [Domain Certificates and Clustered Systems, page 293](#) if your Expressway is part of a cluster.
5. 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.
6. You are returned to the **Domain 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**.
- The user interface provides an option to set the Digest Algorithm. The default is set to SHA-256, with options to change it to SHA-384 or SHA-512.
- The user interface provides an option to set the key length. Expressway support a key length of 1024, 2048 and 4096.

Maintenance

Uploading a New Domain Certificate

When the signed domain certificate is received back from the certificate authority, it must be uploaded to the Expressway. Use the **Upload new certificate** section to replace the current domain certificate with a new certificate.

To upload a domain certificate:

1. Go to **Maintenance > Security > Domain certificates**.
2. Use the **Browse** button in the **Upload new certificate** section to select and upload the domain certificate PEM file.
3. If you used an external system to generate the CSR you must also upload the server private key PEM file that was used to encrypt the domain certificate. (The private key file will have been automatically generated and stored earlier if the Expressway was used to produce the CSR for this domain 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 domain certificate data**.

Domain 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 domain certificates uploaded to each relevant peer.

You must ensure that the correct domain certificate is uploaded to the appropriate peer, otherwise the stored private key on each peer will not correspond to the uploaded certificate.

Advanced Security

The **Advanced security** page (**Maintenance > Advanced security**) is used to configure the Expressway for use in highly secure environments. You need to install the **Advanced Account Security** option key to see this page.

You can configure the system for:

- [Advanced account security mode](#)
- [FIPS140-2 cryptographic mode](#)

Configuring Advanced Account Security Mode

Enabling advanced account security limits login access to remotely authenticated users using the web interface only, and also restricts access to some system features. To indicate that the Expressway is in advanced account security mode, any text specified as the **Classification banner** message is displayed on every web page.

A system reboot is required for changes to the advanced account security mode to take effect.

HTTP methods

The Expressway web server allows the following HTTP methods:

| Method | Used by Web UI? | Used by API? | Used to... |
|--------|-----------------|--------------|--|
| GET | Yes | Yes | Retrieve data from a specified resource. For example, to return a specific page in the Expressway web interface. |

Maintenance

| Method | Used by Web UI? | Used by API? | Used to... |
|---------|-----------------|--------------|--|
| POST | Yes | Yes | Apply data to a web resource. For example, when an administrator saves changes to a setting using the Expressway web interface. |
| OPTIONS | No | Yes | For a specified URL, returns the HTTP methods supported by the server. For example, the Expressway can use OPTIONS to test a proxy server for HTTP/1.1 compliance. |
| PUT | No | Yes | Send a resource to be stored at a specified URI. Our REST API commands use this method to change the Expressway configuration. |
| DELETE | No | Yes | Delete a specified resource. For example, the REST API uses DELETE for record deletion. |

How to disable user access to the API

Administrators have API access by default. This can be disabled in two ways:

- If the Expressway is running in advanced account security mode, then API access is automatically disabled for all users.
- API access for individual administrators can be disabled through their user configuration options.

Prerequisites

Before you can enable advanced account security mode, the following items are required:

- The system must be configured to use [remote account authentication](#) for administrator accounts.
- The **Advanced Account Security** option key must be installed.
- You must create a local administrator account and nominate it as the emergency account, so that you can get in if remote authentication is unavailable. You cannot use a remote account for this purpose.

Do not use the built in *admin* account.

Caution: The Expressway will disallow local authentication by all accounts except the emergency account. Ensure that the remote directory service is working properly before you enable the mode.

You are also recommended to configure your system so that:

- [SNMP](#) is disabled.
- The [session time out period](#) is set to a non-zero value.
- [HTTPS client certificate validation](#) is enabled.
- [User account LDAP server](#) configuration uses TLS encryption and has certificate revocation list (CRL) checking set to *All*.
- [Remote logging](#) is disabled.
- [Incident reporting](#) is disabled.
- Any connection to an [external manager](#) uses HTTPS and has certificate checking enabled.

Alarms are raised for any non-recommended configuration settings.

Enabling Advanced Account Security

To enable advanced account security:

Maintenance

1. Go to **Maintenance > Advanced security**.
2. Enter a **Classification banner**.
The text entered here is displayed on every web page.
3. Set **Advanced account security mode** to *On*.
4. Click **Save**.
5. Reboot the Expressway (**Maintenance > Restart options**).

Expressway Functionality: Changes and Limitations

When in secure mode, the following changes and limitations to standard Expressway functionality apply:

- Access over SSH and through the serial port is disabled and cannot be turned on (the pwrec password recovery function is also unavailable).
- Access over HTTPS is enabled and cannot be turned off.
- The command line interface (CLI) and API access are unavailable.
- Administrator account authentication source is set to *Remote only* and cannot be changed.
- Local authentication is disabled. There is no access using the root account or any local administrator account except the emergency account.
- Only the emergency account may change the emergency account.
- If you are using certificate-based authentication, the emergency account must be authenticated by credentials in the client's certificate. See [Emergency Account and Certificate-based Authentication, page 286](#)
- If there are three consecutive failed attempts to log in (by the same or different users), login access to the Expressway is blocked for 60 seconds.
- Immediately after logging in, the current user is shown statistics of when they previously logged in and details of any failed attempts to log in using that account
- Administrator accounts with read-only or read-write access levels cannot view the Event Log, Configuration Log and Network Log pages. These pages can be viewed only by accounts with *Auditor* access level.
- The **Upgrade** page only displays the **System platform** component.

The Event Log, Configuration Log, Network Log, call history, search history and registration history are cleared whenever the Expressway is taken out of advanced account security mode. Note that if [intrusion protection](#) is enabled, this will cause any existing blocked addresses to become unblocked.

Disabling Advanced Account Security

Note: This operation wipes all configuration. You cannot maintain any configuration or history when exiting this mode. The system returns to factory state.

1. Sign in with the emergency account.
2. Disable Advanced Account Security mode (**Maintenance > Advanced security**).
3. Sign out.
4. Connect to the console.
5. Sign in as **root** and run `factory-reset`.
See [Restoring the Default Configuration \(Factory Reset\), page 360](#) for details.

Configuring FIPS140-2 Cryptographic Mode

FIPS140 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. FIPS140-1 became a mandatory standard for the protection of sensitive data in 1994 and was superseded by

Maintenance

FIPS140-2 in 2001.

Expressway X8.8 or later implements FIPS140-2 compliant features.

When in FIPS140-2 cryptographic mode, system performance may be affected due to the increased cryptographic workload.

You can cluster Expressways that have FIPS140-2 mode enabled.

Prerequisites

Before you enable FIPS140-2 mode:

- Ensure that the system is not using NTLM protocol challenges with a direct Active Directory Service connection for device authentication; NTLM cannot be used while in FIPS140-2 mode.
- If login authentication via a remote LDAP server is configured, ensure that it uses TLS encryption if it is using SASL binding.
- The **Advanced Account Security** option key must be installed.

FIPS140-2 compliance also requires the following restrictions:

- System-wide SIP transport mode settings must be TLS: *On*, TCP: *Off* and UDP: *Off*.
- All SIP zones must use TLS.
- SNMP and NTP server connections should use strong hashing and encryption. Use these settings:

System > SNMP > v3 Authentication > Type = SHA

System > SNMP > v3 Privacy > Type = AES

System > Time > NTP server *n* > Authentication = Symmetric key

System > Time > NTP server *n* > Hash = SHA-1

If your system is running as a virtualized application and has never been through an upgrade process:

1. Ensure it has a valid release key (check this via **Maintenance > Option keys**).
2. Perform a system upgrade. You can upgrade the system to the same software release version that it is currently running.

If you do not complete this step, the activation process described below will fail.

Enable FIPS140-2 Cryptographic Mode

Caution: The transition to FIPS140-2 cryptographic mode requires a system reset to be performed. This will remove all existing configuration data. To preserve your data you should take a backup immediately prior to performing the reset, and then restore the backup file when the reset has completed.

The reset removes all administrator account information and reinstates the default security certificates. To log in after the reset has completed you will have to first complete the Install Wizard.

To turn your system into a compliant FIPS140-2 cryptographic system:

1. Enable FIPS140-2 cryptographic mode:
 - a. Go to **Maintenance > Advanced security**.
 - b. Set **FIPS140-2 cryptographic mode** to *On*.
 - c. Click **Save**.
2. Fix any alarms that have been raised that report non-compliant configuration.
3. Take a [system backup](#) if you want to preserve your current configuration data.
Note that backups taken while in FIPS140-2 mode require password protection.

Maintenance

4. Reset the system and complete the activation of FIPS140-2 mode:

- a. Log in to Expressway as **root**.
- b. Type `fips-activate`

The reset takes up to 30 minutes to complete.

5. Follow the prompts to complete the Install Wizard.

6. When the system has applied the configuration and restarted, log in as `admin` using the password you set.

You may see alarms related to non-compliance with FIPS 140-2. Ignore these alarms if you intend to restore the backup taken prior to the reset. You must take action if they persist after restoring the backup.

7. **Restore** your previous data, if required.

Note that while in FIPS140-2 mode, you can only restore backup files that were taken when **FIPS140-2 cryptographic mode** was set *On*. Any previous administrator account information and passwords will be restored, however the previous **root** account password will not be restored. If the data you are restoring contains untrusted security certificates, the restart that occurs as part of the restore process may take up to 6 minutes to complete.

FIPS140-2 Compliant Features

The following Expressway features are FIPS140-2 compliant / use FIPS140-2 compliant algorithms:

- Administration over the web interface
- Clustering
- XML and REST APIs
- SSH access (restricted to only use AES or 3DES ciphers)
- Login authentication via a remote LDAP server (must use TLS if using SASL binding)
- Client certificate verification
- SIP certificate revocation features
- SNMP (SNMPv3 authentication is restricted to SHA1, and SNMPv3 privacy is restricted to AES)
- NTP (NTP server authentication using symmetric key is restricted to SHA1)
- Device authentication against the local database
- SIP connections to/from the Expressway providing they use TLS
- H.323 connections to/from the Expressway
- Delegated credential checking
- SRTP media encryption
- SIP/H.323 interworking
- Unified Communications Mobile and Remote Access (MRA)
- TURN server authentication
- Encrypted backup/restore operations
- Connections to an external manager
- Connections to external policy services
- Remote logging
- Incident reporting
- CSR generation

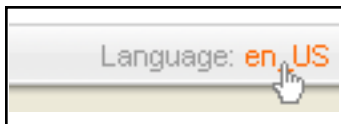
Other Expressway features are not FIPS140-2 compliant, including:

Maintenance

- SIP authentication over NTLM / Active Directory
- SIP/H.323 device authentication against an H.350 directory service
- Microsoft Interoperability service
- Use of Cisco TMSPE

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 |
|--------------------------------|--|---|
| System default language | The default language used on the web interface. | This applies to administrator and user (FindMe) sessions. You can select from the set of installed language packs. |
| This browser | 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

Use the **Backup and restore** page (**Maintenance > Backup and restore**) to create backup files of Expressway data, and to restore the Expressway to a previous, saved configuration.

When to Create a Backup

We recommend creating regular backups, and always 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.

What Gets Backed Up

The data saved to a backup file includes:

- System configuration settings
- Clustering configuration
- Local authentication data (but **not** Active Directory credentials for remotely managed accounts)
 - User account and password details
 - Server security certificate **and** private key
- Call detail records (if the CDR service on Expressway is enabled)

Note: Log files are not included in backup files.

Clustered Systems

For extra information about backing up and restoring peers in a cluster, see [Cluster Upgrades, Backup and Restore, page 177](#)

Creating a System Backup

Before You Begin

- We recommend that you encrypt backup files, in particular because they include sensitive information such as authentication data.
- Backups can only be restored to a system that is running the **same version of software from which the backup was made**.

Maintenance

- You can create a backup on one Expressway and restore it to a different Expressway. For example if the original system has failed. Before the restore, you must install the same option keys on the new system that were present on the old one.

If you try to restore a backup made on a different Expressway, you receive a warning message, but you will be allowed to continue.

(If you use FIPS140-2 cryptographic mode) You can't restore a backup made on a non-FIPS system, onto a system that's running in FIPS mode. You can restore a backup from a FIPS-enabled system onto a non-FIPS system.

- Do not use backups to copy data between Expressways. If you do so, system-specific information will be duplicated (like IP addresses).
- Because backup files contain sensitive information, you should not send them to Cisco in relation to technical support cases. Use snapshot and diagnostic files instead.

Passwords

- If you restore to a previous backup, and the administrator account password has changed since the backup was done, you must provide the old password when you first log in after the restore.
- Active Directory credentials are **not** included in system backup files. If you use NTLM device authentication, you must provide the Active Directory password to rejoin the Active Directory domain after any restore.
- For backup and restore purposes, emergency account passwords are handled the same as standard administrator account passwords.

Process

To create a backup of Expressway system data:

1. Go to **Maintenance > Backup and restore**.
2. (Optional, but recommended.) Enter an **Encryption password** to encrypt the backup file.
If you specify a password, it will be required in future if you ever want to restore the backup file.
3. Click **Create system backup file**.
4. Wait for the backup file to be created. This may take several minutes. Do not navigate away from this page while the file is being prepared.
5. When the backup file is ready, you are prompted to save it. The default filename uses format: **<software version>_<hardware serial number>_<date>_<time>_backup.tar.gz**.
The file extension is normally **.tar.gz.enc** if you specify an encryption password. 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
6. Save the backup file to a secure location.

Restoring a Previous Backup

Before You Begin

- We recommend that you take the Expressway unit out of service before doing a restore.
- The restore process involves **doing a factory reset** back to the original software version. Then upgrading to the **same software version that was running when you took the backup**.

Maintenance

- If the backup is out of date (made on an earlier version than the version you want) these extra steps are needed after the restore:
 - a. Upgrade the software version to the required later version.
 - b. Manually redo any configuration changes made since the backup was taken.
- (If you use FIPS140–2 cryptographic mode) You can't restore a backup made on a non-FIPS system, onto a system that's running in FIPS mode. You can restore a backup from a FIPS-enabled system onto a non-FIPS system.
- You can't restore data to a Expressway while it's part of a cluster. You must first remove it from the cluster. For details, see [Cluster Upgrades, Backup and Restore, page 177](#).

Passwords

- If you restore to a previous backup, and the administrator account password has changed since the backup was done, you must provide the old password when you first log in after the restore.
- Active Directory credentials are **not** included in system backup files. If you use NTLM device authentication, you must provide the Active Directory password to rejoin the Active Directory domain after any restore.
- For backup and restore purposes, emergency account passwords are handled the same as standard administrator account passwords.

Process

To restore the Expressway to a previous configuration of system data:

1. First do a factory reset, as described in [Restoring the Default Configuration \(Factory Reset\), page 360](#). This removes your configuration data, and reverts the system back to its original state. The reset maintains your current software version if you've upgraded since the system was first set up.
2. Upgrade the system to the software version that was running when you made the backup.
 - For standalone systems, see [Upgrade Instructions, page 1](#).
 - For clustered systems, see the *Expressway Cluster Creation and Maintenance Deployment Guide*.
3. Now you can restore the system from the backup, as follows:
 - a. Go to **Maintenance > Backup and restore**.
 - b. In the **Restore** section, click **Browse** and navigate to the backup file that you want to restore.
 - c. In the **Decryption password** field, enter the password used to create the backup file. Or leave blank if the file was created without a password.
 - d. Click **Upload system backup file**.
 - e. The Expressway checks the file and takes you to the **Restore confirmation** page.
 - If the backup file is invalid or the decryption password was entered incorrectly, an error message is displayed at the top of the **Backup and restore** page.
 - The current software version and the number of calls is displayed.
 - f. Read the warning messages that appear, before you continue.
 - g. Click **Continue with system restore** to proceed with the restore.

This will restart the system, so make sure that no active calls exist.
 - h. When the system restarts, the **Login** page is displayed.
4. This step only applies if the backup file is out of date. That is, the software version was upgraded, or system configuration changes were made after the backup was done. In this case:
 - a. Upgrade the system again, this time to the required software version for the system.
 - b. Redo any configuration changes made after the backup (assuming you still need them on the restored system).

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](#)

From X8.10 the Expressway can support SIP "session identifiers". Assuming all devices in the call use session identifiers, the mechanism uses the *Session-ID* field in SIP headers to maintain a unique code through the entire transit of a call. Session identifiers are useful for investigating issues with calls that involve multiple components, as they can be used to find and track a specific call on the Expressway server. Support for session identifiers includes the SIP side of interworked SIP/H.323 calls, and calls to and from Microsoft systems. Session identifiers are defined in [RFC 7989](#).

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_<system host name>_<timestamp>.txt` - containing log messages in response to the activities performed during the logging period
- `xconf_dump_<system host name>_<timestamp>.txt` - containing information about the configuration of the system at the time the logging was started
- `xconf_dump_<system host name>_<timestamp>.xml` - more complete version of xconfig, in XML format
- `xstat_dump_<system host name>_<timestamp>.txt` - containing information about the status of the system at the time the logging was started
- `xstat_dump_<system host name>_<timestamp>.xml` - more complete version of xstatus, in XML format
- (if relevant) `ethn_diagnostic_logging_tcpdump_<system host name>_<timestamp>.pcap` - containing the packets captured during the logging period

Maintenance

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.

Maintenance

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 |
|----------------|---|
| Time | The date and time when the incident occurred. |
| Version | The Expressway software version running when the incident occurred. |
| Build | The internal build number of the Expressway software version running when the incident occurred. |
| State | The current state of the incident: <i>Pending</i> : indicates that the incident has been saved locally but not sent. <i>Sent</i> : indicates that details of the incident have been sent to the URL specified in the Incident reporting configuration 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 |
|----------------------|--|
| Time | The date and time when the incident occurred. |
| Version | The Expressway software version running when the incident occurred. |
| Build | The internal build number of the Expressway software version running when the incident occurred. |
| Name | The name of the software. |
| System | The system name (if configured), otherwise the IP address. |
| Serial number | The hardware serial number. |

Maintenance

| Field | Description |
|--------------------------|---|
| Process ID | The process ID the Expressway application had when the incident occurred. |
| Release | A true/false flag indicating if this is a release build (rather than a development build). |
| User name | The name of the person that built this software. This is blank for release builds. |
| Stack | The trace of the thread of execution that caused the incident. |
| Debug information | 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.

Maintenance

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. Choose from the *Default Zone* (an unknown remote system), the *Default Subzone* (a locally registered endpoint) or any other configured zone or subzone.
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, page 181](#) 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, page 308](#)
- [Local Outbound Ports, page 309](#)
- [Remote Listening Ports, page 309](#)

On an Expressway-E you can also configure the specific listening ports used for firewall traversal via **Configuration > Traversal > Ports**.

See [Port Reference, page 364](#) 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. |
|------|---|

Maintenance

| | |
|--------------------|--|
| 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. *** 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 |
| 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) |

3. 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.
4. 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**
- **_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>**.

Maintenance

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 | <code>IN</code> (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 Name and Type . |

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).

Maintenance

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, page 313](#)
- [Experimental Menu, page 313](#)

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:

Maintenance

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, registrations, current calls and call history, and configuration of the Expressway by using the **Status** menu options.

| | |
|---|-----|
| Status Overview | 315 |
| System Information | 316 |
| Ethernet Status | 317 |
| IP Status | 317 |
| Resource Usage | 318 |
| Registration Status | 320 |
| Call Status | 321 |
| B2BUA Calls | 322 |
| Search History | 323 |
| Search Details | 324 |
| Local Zone Status | 324 |
| Zone Status | 324 |
| Bandwidth | 325 |
| Policy Server Status and Resiliency | 326 |
| TURN Relay Usage | 327 |
| Unified Communications Status | 327 |
| Microsoft interoperability | 328 |
| TMS Provisioning Extension Service Status | 329 |
| Managing Alarms | 332 |
| Logs | 333 |
| Hardware Status | 336 |

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 |
|---|---|
| System information: many of the items in this section are configurable. Click on an item name to go to its configuration page. | |
| System name | Name assigned to the Expressway. |
| Up time | Time elapsed since the system last restarted. |
| Software version | Software version currently installed on the Expressway. |
| IPv4 address | Expressway's IPv4 addresses. |

Overview and Status Information

| Field | Description |
|---------------------|--|
| IPv6 address | Expressway's IPv6 addresses. |
| VM size | (Virtual machine-based systems only) Size of the VM hardware platform - small, medium or large. |
| Options | Maximum limits for calls and registrations, and availability of additional Expressway features like TURN Relays, FindMe™, Device Provisioning and Advanced Networking, are controlled by option keys . |

Resource usage

This section provides statistics about current and cumulative license usage for calls and registrations.

It shows current and peak (highest concurrent) usage broken down by:

- Rich media sessions
- Registrations (including Unified CM remote 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 or registrations 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, page 169](#) 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 |
|------------------------------------|--|
| System information section: | |
| System name | The name that has been assigned to the Expressway. |
| Product | This identifies the Expressway. |
| Software version | The version of software that is currently installed on the Expressway. |

Overview and Status Information

| Field | Description |
|----------------------------------|--|
| Software build | The build number of this software version. |
| Software release date | The date on which this version of the software was released. |
| Software name | The internal reference number for this software release. |
| Software options | The maximum number of calls, and the availability of additional Expressway features such as Advanced Networking, are controlled through the use of option keys . This section shows all the optional features currently installed on the Expressway. |
| Hardware version | The version number of the hardware on which the Expressway software is installed. |
| Serial number | The serial number of the hardware or virtual machine on which the Expressway software is installed. |
| Time information section: | |
| Up time | The amount of time that has elapsed since the system last restarted. |
| System time (UTC) | The time as determined by the NTP server. If no NTP server is configured, this shows <i>Time Not Set</i> . |
| Time zone | The time zone that has been configured on the Time page. |
| Local time | If an NTP server is configured, the system time is shown in local time (UTC adjusted according to the local time zone). If no NTP server is configured, the time according to the Expressway's operating system is shown. |
| Active sessions section: | |
| Administrator sessions | The number of current active administrator sessions. Click on the link to see the list of active sessions. |
| User sessions | The number of current user sessions. Click on the link to see the list of active sections. |

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 |
|--------------------|---|
| MAC address | The MAC address of the Expressway's Ethernet device for that LAN port. |
| Speed | 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 |
|----------------------------|---|
| IP section: | |
| Protocol | Indicates the IP protocol supported by the Expressway: <ul style="list-style-type: none"> ■ <i>IPv4 only</i>: it only accepts registrations from endpoints using an IPv4 address, and only takes calls between two endpoints communicating via IPv4. It communicates with other systems via IPv4 only. ■ <i>IPv6 only</i>: it only accepts registrations from endpoints using an IPv6 address, and only takes calls between two endpoints communicating via IPv6. It communicates with other systems via IPv6 only. ■ <i>Both</i>: it accepts registrations from endpoints using either an IPv4 or IPv6 address, and 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. |
| IPv4 gateway | The IPv4 gateway used by Expressway. |
| IPv6 gateway | The IPv6 gateway used by Expressway. |
| Advanced Networking | Indicates whether the second LAN port has been enabled. This is done by installing the Advanced Networking option key. |
| LAN 1 | Shows the IPv4 address and subnet mask, and IPv6 address of the LAN 1 port. |
| LAN 2 | If the Advanced Networking option key has been installed, this shows the IPv4 address and subnet mask, and IPv6 address of the LAN 2 port. |
| DNS section: | |
| Server 1..5 address | The IP addresses of each of the DNS servers that are queried when resolving domain names. Up to 5 DNS servers may be configured. |
| Domain | 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 and registrations.

It shows current and peak (highest concurrent) usage broken down by:

- Rich media sessions
- Registrations (including Unified CM remote 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 or registrations by clicking on the relevant item in the section.

Overview and Status Information

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

You can cluster up to 6 Expressway systems to increase capacity by a maximum factor of 4.

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.

The maximum number of licenses that each Expressway system can use depends on the [type of appliance or VM](#):

Table 19 Maximum licenses that a peer can use

| | Small / Medium systems | Large [‡] / CE500/ CE1000 / CE1100 systems |
|-------------------------------------|------------------------|---|
| Rich media sessions | 150 [†] | 500 |
| Room / Desktop system registrations | 2500 | 5000 (2500 for MRA registrations) |
| TURN relays * | 1800 | 6000 |

[‡] From X8.10 onwards, the requirement to have a 10 Gbps NIC in order to achieve the scalability of a large system is removed. It is now possible to have the capacity of a large system with a 1 Gbps NIC subject to your bandwidth constraints.

[†] This is the maximum number of licenses the system can use. This limit specifically applies to the case where a peer becomes unavailable and the other peers must use that peer's licenses to honor the cluster's overall capacity. This is not intended as a production capacity limit, only as a temporary measure to allow the affected peer to be returned to normal service. **We strongly discourage installing more than 100 licenses on any platform that has small or medium capacity.**

* 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 see a summary of all of the call, registration, and TURN relay licenses installed on each cluster peer by going to the [Option keys](#) page and scrolling down to the **Current licenses** section.

Licenses Used in Intracluster Calls

This section describes the licenses used when endpoints are registered to different peers in the same cluster.

If the call media does not traverse the cluster peers:

- A call between the endpoints does not consume any RMS licenses; this is a "Registered" call.

If the call media traverses the cluster peers:

- A call between the endpoints consumes an RMS license on the Expressway where the B2BUA is engaged.

See [About Clusters, page 169](#) for more information.

Registration Status

Registration status information can be displayed for both current and historic registrations. If the Expressway is part of a cluster, all registrations that apply to any peer in the cluster are shown.

- The **Registrations by device** page (**Status > Registrations > By device**) lists each device currently registered with the Expressway, and allows you to remove a device's registration. If the Expressway is part of a cluster, all registrations across the cluster are shown.
- The **Registrations by alias** page (**Status > Registrations > By alias**) lists all the aliases, E.164 numbers and prefixes used by all endpoints and systems currently registered with the Expressway.
- The **Registration history** page (**Status > Registrations > History**) lists all the registrations that are no longer current. It contains all historical registrations since the Expressway was last restarted.

The following information is displayed:

| Field | Description |
|----------------------|---|
| Name | For SIP devices, this is its SIP AOR. |
| Number | For SIP devices this will always be blank because they cannot register E.164 numbers. (This is shown in the Alias column in the registration by alias view.) |
| Alias | The SIP AOR registered by a device. (Registration by alias view only.) |
| Type | Indicates the nature of the registration. This will most commonly be Endpoint, MCU, Gateway, or SIP UA. |
| Protocol | Indicates whether the registration is for a SIP device. |
| Creation time | The date and time at which the registration was accepted. If an NTP server has not been configured, this will say <i>Time not set</i> . |
| Address | For SIP UAs this is the Contact address presented in the REGISTER request. |
| End time | The date and time at which the registration was terminated. (Registration history view only.) |
| Duration | The length of time that the registration was in place. (Registration history view only.) |
| Reason | The reason why the registration was terminated. (Registration history view only.) |
| Peer | Identifies the cluster peer to which the device is registered. |
| Actions | Click View to go to the Registration details page to see further detailed information about the registration. |

Registration details

The information shown on the **Registration details** page depends on the device's protocol, and whether the registration is still current. For example, SIP registrations include the AOR, contact and, if applicable, public GRUU details. It also provides related tasks that let you **View active calls involving this registration** and **View previous calls involving this registration**; these options take you to the **Calls by registration** page, showing the relevant current or historic [call status](#) information filtered for that particular registration.

Unregistering and blocking devices

The registration status pages provide options to manually unregister and block devices.

- Click **Unregister** to unregister the device. Note that the device may automatically re-register after a period of time, depending on its configuration. To prevent this, you must also use a [registration restriction policy](#) such as an Allow List or Deny List.
- Click **Unregister and block** to unregister the device and add the alias to the [Deny List](#) page, thus preventing the device from automatically re-registering. (This option is only available if the **Restriction policy** is set to *Deny List*.)

Overview and Status Information

Note that if your Expressway is part of a cluster you have to be logged into the peer to which the device is registered to be able to unregister it.

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 taking place to or from devices registered with the Expressway, or that are 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.

The same set of call status information is also shown on the **Calls by registration** page (accessed via the **Registration details** page).

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. (If the call passes through more than one Expressway and User Policy is enabled, the caller's FindMe ID may be displayed instead.) |
| 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 transforms, zone transforms or User Policy). |
| Type | Indicates the type of call. |
| SIP variant | <i>Standards-based</i> , <i>Microsoft AV</i> , <i>Microsoft SIP IM&P</i> , or <i>Microsoft Share</i> to distinguish between the different implementations of SIP and SDP that can be routed by the Expressway. Does not display for H.323 calls. |
| 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 View 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:

Overview and Status Information

- *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 the Expressway-C, a Unified CM remote session has three components (as it uses the B2BUA to enforce media encryption). One of the Expressway components routes 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 the Expressway-E, there is one component and that routes the call through the **CollaborationEdgeZone**.

If both endpoints are outside of the enterprise (that is, off premises), you will see this treated as two separate calls.

Rich media sessions

If your system has a rich media session key installed and thus supports 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

Overview and Status Information

- the [Microsoft interoperability service](#) is enabled and the call has been routed through the **To Microsoft destination via B2BUA** neighbor zone

Note that for Microsoft interoperability 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 interoperability service, this comprises legs between the Expressway, the Microsoft server and, if applicable, the external 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, page 222](#)).

The Expressway supports up to 500 concurrent searches.

Search history list

The search history summary list shows the following information:

| Field | Description |
|--------------------|---|
| Start time | The date and time at which the search was initiated. |
| Search type | The type of message being sent. |
| Source | The alias of the endpoint that initiated the call. |
| Destination | 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. |
| Status | Indicates whether or not the search was successful. |
| Actions | Allows you to click View to go to the Search details page, which lists full details of this search. |

Overview and Status Information

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
- the SIP variant used by the call
- use of policies such as Admin Policy or User Policy (FindMe)
- 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 |
|-----------------------|--|
| Subzone name | The names of each subzone currently configured on this Expressway. Clicking on a Subzone name takes you to the configuration page for that subzone. |
| Calls | The number of calls currently passing through the subzone. . Note that a single call may pass through more than one subzone, depending on the route it takes. For example, calls from a locally registered endpoint will always pass through the Traversal Subzone, so they will show up twice; once in the originating subzone and once in the Traversal Subzone. |
| Bandwidth used | 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:

Overview and Status Information

| Field | Description |
|---------------------------|--|
| Name | The names of each zone currently configured on this Expressway. Clicking on a zone Name takes you to the configuration page for that zone. |
| Type | The type of zone. |
| Calls | The number of calls currently passing out to or received in from each zone. |
| Bandwidth used | The total amount of bandwidth used by all calls passing out to or received in from each zone. |
| H.323 / SIP status | Indicates the zone's H.323 or SIP connection status: <ul style="list-style-type: none"> ■ <i>Off</i>: the protocol is disabled at either the zone or system level ■ <i>Active</i>: the protocol is enabled for the 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> ■ <i>On</i>: indicates that the protocol is enabled for the zone (for zone types that do not have active connections, eg. DNS and ENUM zones) ■ <i>Failed</i>: the protocol is enabled for the zone but its connection has failed ■ <i>Checking</i>: the protocol is enabled for the zone and the system is currently trying to establish a connection |
| Search rule status | 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 |
|-----------------------|---|
| Name | The name of each link. Clicking on a link Name takes you to the configuration page for that link. |
| Calls | 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. |
| Bandwidth used | 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 |
|-------------|--|
| Name | The name of each pipe. Clicking on a pipe Name takes you to the configuration page for that pipe. |

Overview and Status Information

| Field | Description |
|-----------------------|---|
| Calls | 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. |
| Bandwidth used | 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 |
|------------------|---|
| Name | The name of the policy service. Clicking on a Name 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. |
| URL | 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. |
| Status | The current status of the service based on the last attempt to poll that server. |
| Last used | 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 |
|----------------------------|--|
| Client | The IP address of the client that requested the relay. |
| Media destinations | The address of destination system the media is being relayed to. |
| Connection protocol | Indicates if the client is connected over TCP or UDP. |
| Relays | 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:

Overview and Status Information

- 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 MRA Authentication Statistics

Go to **Status > Unified Communications > View detailed MRA authentication statistics** to view a summary of requests and responses issued, and more detailed statistics about successful and unsuccessful attempts to authenticate.

If no instances of a particular request or response type exist, then no counter is shown for that type.

SSH Tunnels Status

This page shows the status of the SSH tunnels between this Expressway and its "traversal partner". You can view this status from either side of the tunnel, that is, on the Expressway-C or the Expressway-E.

Here are some reasons why SSH tunnels could fail:

- The Expressway-C cannot find the Expressway-E:
 - Is there a firewall between them? Is TCP 2222 open from the Expressway-C to the Expressway-E?
 - Are there forward and reverse DNS entries for the Expressway-C and Expressway-E?

Use traceroute and ping to establish if there is a connectivity problem.

- The servers do not trust each other:
 - Are the partners synchronized using NTP servers? A large time difference between the partners could prevent them from trusting each other.
 - Are the server certificates valid and current? Are their issuing CAs trusted by the other side?
 - Is the authentication account added to the local database in the Expressway-E?
 - Is the same authentication account entered on the Expressway-C?

Try a secure traversal test from the Expressway-C (**Maintenance > Security > Secure traversal test** and enter the FQDN of the Expressway-E).

Microsoft interoperability

Microsoft-registered FindMe User Status

The **Status > Applications > Microsoft-registered FindMe users** page lists the current status of all FindMe IDs being handled by the [Microsoft Interoperability service](#).

It applies to deployments that use both Microsoft clients and FindMe, if they both use the same SIP domain. To enable this feature, **Register FindMe users as clients to Microsoft server** must be set to **Yes** on the [Microsoft Interoperability configuration](#) page.

The following information is displayed:

| Field | Description |
|---------------------------|--|
| URI | The FindMe ID. |
| Registration state | Indicates whether the FindMe ID has registered successfully with a Microsoft Front End server. Doing so allows Microsoft infrastructure to forward calls to the FindMe ID. Note that FindMe users can only register to Microsoft infrastructure if the FindMe ID is a valid user in the Active Directory (in the same way that Microsoft clients can only register if they have a valid account enabled in AD). |
| Peer | The cluster peer that is registering the URI. |

Overview and Status Information

You can view further status information for each FindMe ID by clicking **Edit** in the **Action** column. This can help diagnose registration or subscription failures.

Microsoft Interoperability Status

Go to **Status > Applications > Microsoft interoperability** to see the status of the [Microsoft interoperability service](#).

This service routes SIP calls between the Expressway and a Microsoft server.

The information shown includes:

- the number of current calls passing through the Microsoft interoperability B2BUA
- resource usage as a percentage of the number of allowed Microsoft interoperability calls

TMS Provisioning Extension Service Status

The **TMS Provisioning Extension service status** page (**Status > Applications > TMS Provisioning Extension services > TMS Provisioning Extension service status**) shows the status of each of the Cisco TMSPE services to which the Expressway is connected (or to which it is attempting to connect).

Summary details of each service are shown including:

- the current status of the connection
- when the most recent update of new data occurred
- when the service was last polled for updates
- the scheduled time of the next poll

Click **View** to display further details about a service, including:

- additional connection status and configuration information, including troubleshooting information about any connection failures
- which Expressway in the cluster has the actual connection to the Cisco TMSPE services (only displayed if the Expressway is part of a cluster)
- details of each of the data tables provided by the service, including the revision number of the most recent update, and the ability to **View** the records in those tables

You are recommended to use Cisco TMS to make any changes to the services' configuration settings, however you can modify the current configuration for this Expressway from the [TMS Provisioning Extension services](#) page (**System > TMS Provisioning Extension services**).

See the [Provisioning Server](#) section for more information.

Provisioning Server Device Requests Status (Cisco TMSPE)

The **Device requests status** page (**Status > Applications > TMS Provisioning Extension services > Device requests**) shows the status of the Expressway [Provisioning Server](#) when using Cisco TMSPE.

The Expressway Provisioning Server provides provisioning-related services to provisioned devices, using data supplied by Cisco TMS through the [Cisco TMS provisioning](#) mechanism. The server only operates if the **Device Provisioning** option key is installed.

As from version X8.8, the Expressway supports only the Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) services to provide the Expressway with provisioning and FindMe data. In this mode all provisioning and FindMe data is managed and maintained exclusively within Cisco TMS.

Provisioning server

This section displays the server's status and summarizes the subscription requests received by the server since the Expressway was last restarted. It shows counts of:

Overview and Status Information

- the total number of subscription requests received
- how many requests were sent a successful provisioning response
- failed requests because the account requesting provisioning could not be found
- failed requests because the account requesting provisioning had no provisioned devices associated with it

Model licenses

This section shows the status of the provisioning licenses that are available within your system. Information displayed includes:

- the total license limit and the number of licenses still available (free) for use
- the number of licenses currently being used by devices that are registered to this Expressway (or Expressway cluster); this information is broken down by the device types that can be provisioned by this Expressway

License information is exchanged between Cisco TMS and Expressway by the Cisco TMSPE Devices service. If the Devices service is not active, the Expressway's Provisioning Server will not be able to provision any devices.

The license limit and the number of free licenses indicate the overall number of licenses that are available to all of the Expressways or Expressway clusters that are being managed by Cisco TMS, hence the difference between the license limit and free counts may not equal the sum of the number of used licenses shown for this particular Expressway or Expressway cluster

Phone book server

The phone book server provides phone book directory and lookup facilities to provisioned users.

This section displays the server's status and summarizes the number of phone book search requests received by the server from provisioned users since the Expressway was last restarted.

User Records Provided by Cisco TMSPE Services

You can view the data records provided by the Cisco TMSPE **Users** service by going to **Status > Applications > TMS Provisioning Extension services > Users > ...** and then the relevant table:

- **Accounts**
- **Groups**
- **Templates**

All the records in the chosen table are listed. Note that some tables can contain several thousand records and you may experience a delay before the data is displayed.

Filtering the view

The **Filter** section lets you filter the set of records that are shown. It is displayed only if there is more than one page of information to display. Status pages show 200 records per page.

Enter a text string or select a value with which to filter each relevant field, and then click **Filter**.

Only those records that match all of the selected filter options are shown. Note that text string filtering is case insensitive.

Viewing more details and related records

You can click **View** to display further details about the selected record. Many views also allow you to click on related information to see the data records associated with that item. For example, when viewing user groups, you can also access the related user templates. When viewing user accounts you can check the data that would be provisioned to that user by clicking [Check provisioned data](#).

FindMe Records Provided by Cisco TMSPE Services

You can view the data records provided by the Cisco TMSPE **FindMe** service by going to **Status > Applications > TMS Provisioning Extension services > FindMe > ...** and then the relevant table:

Overview and Status Information

- **Accounts**
- **Locations**
- **Devices**

All the records in the chosen table are listed. Note that some tables can contain several thousand records and you may experience a delay before the data is displayed.

Filtering the view

The **Filter** section lets you filter the set of records that are shown. It is displayed only if there is more than one page of information to display. Status pages show 200 records per page.

Enter a text string or select a value with which to filter each relevant field, and then click **Filter**.

Only those records that match all of the selected filter options are shown. Note that text string filtering is case insensitive.

Viewing more details and related records

You can click **View** to display further details about the selected record. Many views also allow you to click on related information to see the data records associated with that item. For example, when viewing a FindMe user, you can also access the related location and device records.

Phone Book Records Provided by Cisco TMSPE Services

You can view the data records provided by the Cisco TMSPE **Phone books** service by going to **Status > Applications > TMS Provisioning Extension services > Phone book > ...** and then the relevant table:

- **Folders**
- **Entries**
- **Contact methods**
- **User access**

All the records in the chosen table are listed. Note that some tables can contain several thousand records and you may experience a delay before the data is displayed.

Filtering the view

The **Filter** section lets you filter the set of records that are shown. It is displayed only if there is more than one page of information to display. Status pages show 200 records per page.

Enter a text string or select a value with which to filter each relevant field, and then click **Filter**.

Only those records that match all of the selected filter options are shown. Note that text string filtering is case insensitive.

Viewing more details and related records

You can click **View** to display further details about the selected record. Many views also allow you to click on related information to see the data records associated with that item. For example, when viewing a phone book entry, you can also access the related contact method or folder.

Provisioned Devices

The **Provisioned device status** page (**Status > Applications > TMS Provisioning Extension services > Provisioned device status**) displays a list of all of the devices that have submitted provisioning requests to the Expressway's Provisioning Server.

Filtering the view

The **Filter** section lets you filter the set of records that are shown. It is displayed only if there is more than one page of information to display. Status pages show 200 records per page.

Enter a text string or select a value with which to filter each relevant field, and then click **Filter**.

Overview and Status Information

Only those records that match all of the selected filter options are shown. Note that text string filtering is case insensitive.

The list shows all current and historically provisioned devices. A device appears in the list after it has made its first provisioning request. The **Active** column indicates if the device is currently being provisioned (and is thus consuming a provisioning license).

Checking Provisioned Data

The **Check provisioned data** page is used to check the configuration data that the Expressway's [Provisioning Server](#) will provision to a specific user and device combination.

You can get to this page only through the **User accounts** status page (**Status > Applications > TMS Provisioning Extension services > Users > Accounts**, locate the user you want to check and then click **Check provisioned data**).


To check provisioned data:

1. Verify that the **User account name** is displaying the name of the user account you want to check.
2. Select the **Model** and **Version** of the user's endpoint device.
If the actual **Version** used by the endpoint is not listed, select the nearest earlier version.
3. Click **Check provisioned data**.

The **Results** section will show the data that would be provisioned out to that user and device combination.

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 | Hybrid Services alarms |
| 60000–60099 | Management Connector alarms |
| 60100–60199 | Calendar Connector alarms |
| 60300–60399 | Call Connector alarms |

Overview and Status Information

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, page 338](#) and [Events and Levels, page 341](#).

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.

Overview and Status Information

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.

| | |
|---|-----|
| About Event Log Levels | 338 |
| CPL Reference | 347 |
| LDAP Server Configuration for Device Authentication | 356 |
| Changing the Default SSH Key | 360 |
| Restoring the Default Configuration (Factory Reset) | 360 |
| Password Encryption | 362 |
| Pattern Matching Variables | 363 |
| Port Reference | 364 |
| Mobile and Remote Access Port Reference | 369 |
| Microsoft Interoperability Port Reference | 371 |
| Regular expressions | 374 |
| Supported Characters | 376 |
| Call Types and Licensing | 377 |
| Product Identifiers and Corresponding Keys | 380 |
| Allow List Rules File Reference | 382 |
| Allow List Tests File Reference | 383 |
| Expressway Multitenancy Overview | 384 |
| Multitenant Expressway Sizing | 386 |
| Alarms | 389 |
| Command Reference – xConfiguration | 423 |
| Command Reference – xCommand | 491 |
| Command Reference – xStatus | 518 |
| External Policy Overview | 519 |
| Flash Status Word Reference Table | 523 |
| Supported RFCs | 524 |
| Software Version History | 526 |
| Related Documentation | 558 |
| Legal Notices | 559 |

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 | High-level events such as registration requests and call attempts. Easily human readable. For example: <ul style="list-style-type: none"> ■ call attempt/connected/disconnected ■ registration attempt accepted/rejected |
| 2 | All Level 1 events, plus: 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 |
| 3 | All Level 1 and Level 2 events, plus: <ul style="list-style-type: none"> ■ protocol keepalives ■ call-related SIP signaling messages |
| 4 | The most verbose level: all Level 1, Level 2 and Level 3 events, plus: <ul style="list-style-type: none"> ■ network level SIP messages |

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 | The name of the program generating the log message. This could include: <ul style="list-style-type: none"> ■ tvcs for all messages originating from Expressway processes ■ web for all web login and configuration events ■ licensemanager for messages originating from the call license manager ■ b2bua for B2BUA events ■ portforwarding for internal communications between the Expressway-C and the Expressway-E ■ ssh for ssh tunnels between the Expressway-C and the Expressway-E but will differ for messages from other applications running on the Expressway. |
| message_details | The body of the message (see the Message details field 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 Events and levels 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"> ■ TCP ■ UDP ■ TLS |
| Reason | Textual string containing any reason information associated with the event. |
| Service | Specifies which protocol was used for the communication. Will be one of: <ul style="list-style-type: none"> ■ H323 ■ SIP ■ H.225 ■ H.245 ■ LDAP ■ Q.931 ■ NeighbourGatekeeper ■ Clustering ■ ConferenceFactory |

Reference Material

| Name | Description |
|--------------------|---|
| 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. 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. 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. |
| To | <ul style="list-style-type: none"> ■ for REGISTER requests: the AOR for the REGISTER request ■ for INVITEs: the original alias that was dialed ■ for all other SIP messages: the AOR of the destination. |
| 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. |

Reference Material

| Name | Description |
|---------|--|
| 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 About Event Log levels 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 Detail 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 Detail event parameter provides information about the nature of the issue. | 1 |
| Alarm raised | The Expressway has detected an issue and raised an alarm. The Detail 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 Detail 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 Detail event parameter. | 1 |
| Application Warning | The Expressway application is still running but has experienced a recoverable problem. Further detail may be provided in the Detail 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 |

Reference Material

| Event | Description | Level |
|---------------------------|---|-------|
| 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 Reason event parameter contains a textual representation of the H.225 additional cause code. | 1 |
| Call Rerouted | The Expressway has Call signaling optimization 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 Detail 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 Detail 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 |

Reference Material

| Event | Description | Level |
|---------------------------------------|--|-------|
| External Server Communication Failure | <p>Communication with an external server failed unexpectedly. The Detail event parameter should differentiate between "no response" and "request rejected". Servers concerned are:</p> <ul style="list-style-type: none"> ■ DNS ■ LDAP servers ■ Neighbor Gatekeeper ■ NTP servers ■ Peers | 1 |
| Hardware Failure | There is an issue with the Expressway hardware. If the problem persists, contact your Cisco support representative. | 1 |
| License Limit Reached | <p>Licensing limits for a given feature have been reached. The Detail event parameter specifies the facility/limits concerned.</p> <p>If this occurs frequently, you may want to contact your Cisco representative to purchase more licenses.</p> | 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 | <p>This could be for one of two reasons:</p> <ul style="list-style-type: none"> ■ If authentication is enabled and an endpoint has unsuccessfully attempted to send a message (such as a registration request) 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. ■ 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. | 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 |

Reference Material

| Event | Description | Level |
|--------------------------------|--|-------|
| Provisioning | Diagnostic messages from the provisioning server. The Detail event parameter provides additional information. | 1 |
| Reboot Requested | A system reboot has been requested. The Reason event parameter provides specific information. | 1 |
| Registration Accepted | A registration request has been accepted. | 1 |
| Registration Refresh Accepted | A request to refresh or keep a registration alive has been accepted. | 3 |
| 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 Reason and Detail event parameters provide more information about the nature of the rejection. | 1 |
| Registration Removed | A registration has been removed by the Expressway. The Reason event parameter specifies the reason why the registration was removed. This is one of: <ul style="list-style-type: none"> ■ Authentication change ■ Conflicting zones ■ Operator forced removal ■ Operator forced removal (all registrations removed) ■ Registration superseded. | 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 |

Reference Material

| Event | Description | Level |
|---|--|-------|
| 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 Reason 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 |
| Search Loop detected | The Expressway is in Call loop detection mode and has identified and terminated a looped branch of a search. | 2 |
| Secure mode disabled | The Expressway has successfully exited Advanced account security mode. | 1 |
| Secure mode enabled | The Expressway has successfully entered Advanced account security 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 Detail 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 |

Reference Material

| Event | Description | Level |
|---------------------------|---|-------|
| 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 Detail event parameter may contain additional information if there are startup problems. | 1 |
| TLS Negotiation Error | Transport Layer Security (TLS) connection failed to negotiate. | 1 |
| Unregistration Accepted | An unregistration request has been accepted. | 1 |
| 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 Detail 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 (URLs, 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:

| | |
|------------------------------|--|
| <code>is=string</code> | Selected field and subfield exactly match the given string. |
| <code>contains=string</code> | 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. |

Reference Material

| | |
|---|---|
| <code>subdomain-of=string</code> | 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. |
| <code>regex="regular expression"</code> | 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 |
|---|--|---|
| <code>unauthenticated-origin</code> | 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. |
| <code>authenticated-origin</code> and <code>origin</code> | The "From" and "ReplyTo" fields of the message if it authenticated correctly (or where the relevant Authentication Policy is <i>Treat as authenticated</i>), otherwise <i>not-present</i> . | The source aliases from the original LRQ or ARQ that started the call if it authenticated correctly (or where the relevant Authentication Policy is <i>Treat as authenticated</i>) otherwise <i>not-present</i> . Because SETUP messages are not authenticated, if the Expressway receives a SETUP without a preceding RAS message the origin will always be <i>not-present</i> . |
| <code>originating-zone</code> | 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. If it comes from an endpoint within one of the local subzones this will be the name of the subzone. If the call originates from any other locally registered endpoint this will be "DefaultSubZone". In all other cases this will be "DefaultZone". | |
| <code>originating-user</code> | If the relevant Authentication Policy is <i>Check credentials</i> or <i>Treat as authenticated</i> this is the username used for authentication, otherwise <i>not-present</i> . | |
| <code>registered-origin</code> | If the call originates from a registered endpoint this is the list of all aliases it has registered, otherwise <i>not-present</i> . | |
| <code>destination</code> | The destination aliases. | |
| <code>original-destination</code> | 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.

Reference Material

If a subfield is not specified for the alias type being matched then the `not-present` action is taken.

| | |
|---------------------------|---|
| <code>address-type</code> | Either <code>h323</code> or <code>sip</code> , based on the type of endpoint that originated the call. |
| <code>user</code> | 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. |
| <code>host</code> | 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. |
| <code>tel</code> | For E.164 numbers this selects the entire string of digits. |
| <code>alias-type</code> | <p>Gives a string representation of the type of alias. The type is inferred from the format of the alias. Possible types are:</p> <ul style="list-style-type: none"> ■ Address Type ■ Result ■ URI ■ url-ID ■ H.323 ID ■ h323-ID ■ Dialed Digits ■ dialedDigits |

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](#).

| | |
|-----------------------------------|---|
| <code>Clear = "yes" "no"</code> | 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. |
| <code>url=string</code> | 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. |

Reference Material

| | |
|---|--|
| <code>priority=<0.0..1.0></code> <code>"random"</code> | 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. |
| <code>regex="<regular expression>"</code> <code>replace="<string>"</code> | Specifies the way in which a location matching the regular expression is to be changed. |
| <code>source-url-for-message="<string>"</code> | Replaces the From header (source alias) with the specified string. |
| <code>source-url-for-message-regex="<regular expression>"</code> together with <code>source-url-for-message-replace="<string>"</code> | 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.

Reference Material

The proxy node supports the following optional parameters:

| | |
|--|--|
| <code>timeout=<1..86400></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`

CPL Examples

This section provides a selection of CPL examples:

- [Call screening of authenticated users](#)
- [Call screening based on domain](#)
- [Allow calls from locally registered endpoints only](#)
- [Block calls from Default Zone and Default Subzone](#)
- [Restricting access to a local gateway](#)

CPL Example: Call Screening of Authenticated Users

Note: You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See [About Call Policy, page 203](#).

In this example, only calls from users with authenticated source addresses are allowed. See [About Device Authentication, page 135](#) for details on how to enable authentication.

If calls are coming in through Expressway-E, then we recommend screening on the Expressway-E to prevent unwelcome calls from progressing into the network.

```
<?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="authenticated-origin">
      <not-present>
        <!-- Reject call with a status code of 403 (Forbidden) -->
        <reject status="403" reason="Denied by policy"/>
      </not-present>
    </address-switch>
  </taa:routed>
</cpl>
```

CPL Example: Call Screening Based on Alias

Note: You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See [About Call Policy, page 203](#).

In this example, user ceo will only accept calls from users vpsales, vpmarketing Or vpengeering.

If calls are coming in through Expressway-E, then we recommend screening on the Expressway-E to prevent unwelcome calls from progressing into the network.

```
<?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="ceo">
        <address-switch field="authenticated-origin">
          <address regex="vpsales|vpmarketing|vpengeering">
            <!-- Allow the call -->
          </address-switch>
        </address-switch>
      </address>
    </address-switch>
  </taa:routed>
</cpl>
```

Reference Material

```

    <proxy/>
  </address>
</not-present>
  <!-- Unauthenticated user -->
  <!-- Reject call with a status code of 403 (Forbidden) -->
  <reject status="403" reason="Denied by policy"/>
</not-present>
</otherwise>
  <!-- Reject call with a status code of 403 (Forbidden) -->
  <reject status="403" reason="Denied by policy"/>
</otherwise>
</address-switch>
</address>
</address-switch>
</taa:routed>
</cpl>

```

CPL Example: Call Screening Based on Domain

Note: You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See [About Call Policy, page 203](#).

In this example, user fred will not accept calls from anyone at `annoying.com`, or from any unauthenticated users. All other users will allow any calls.

If calls are coming in through Expressway-E, then we recommend screening on the Expressway-E to prevent unwelcome calls from progressing into the network.

```

<?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="fred">
        <address-switch field="authenticated-origin" subfield="host">
          <address subdomain-of="annoying.com">
            <!-- Don't accept calls from this source -->
            <!-- Reject call with a status code of 403 (Forbidden) -->
            <reject status="403" reason="Denied by policy"/>
          </address>
        </address-switch>
      </address>
    </address-switch>
  </not-present>
  <!-- Don't accept calls from unauthenticated sources -->
  <!-- Reject call with a status code of 403 (Forbidden) -->
  <reject status="403" reason="Denied by policy"/>
</not-present>
</otherwise>
  <!-- All other calls allowed -->
  <proxy/>
</otherwise>
</address-switch>
</address>
</address-switch>
</taa:routed>
</cpl>

```

CPL Example: Allow Calls From Locally Registered Endpoints Only

In this example, the administrator only wants to allow calls that originate from locally registered endpoints.

Reference Material

```
<?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="registered-origin">
      <not-present>
        <reject status="403" reason="Only local endpoints can use this Expressway"/>
      </not-present>
    </address-switch>
  </taa:routed>
</cpl>
```

CPL Example: Block Calls From Default Zone and Default Subzone

Note: You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See [About Call Policy, page 203](#).

The script to [allow calls from locally registered endpoints only](#) can be extended to also allow calls from configured zones but not from the Default Zone or Default Subzone.

```
<?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="registered-origin">
      <not-present>
        <address-switch field="originating-zone">
          <address is="DefaultZone">
            <!-- Reject call with a status code of 403 (Forbidden) -->
            <reject status="403" reason="Denied by policy"/>
          </address>
          <address is="DefaultSubZone">
            <!-- Reject call with a status code of 403 (Forbidden) -->
            <reject status="403" reason="Denied by policy"/>
          </address>
          <otherwise>
            <proxy/>
          </otherwise>
        </address-switch>
      </not-present>
    </address-switch>
  </taa:routed>
</cpl>
```

CPL Example: Restricting Access to a Local Gateway

Note: You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See [About Call Policy, page 203](#).

In these examples, a gateway is registered to the Expressway with a prefix of 9 and the administrator wants to stop calls from outside the organization being routed through it.

This can be done in two ways: using the `address-switch` node or the `taa:rule-switch` node. Examples of each are shown below.

Reference Material

Note: You can achieve the same result with Call Routing on Cisco Unified Communications Manager. This example is here because you may want to prevent these types of calls from getting any deeper into the network.

Using the Address-Switch Node

```
<?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 regex="9(.*)">
        <address-switch field="originating-zone">
          <!-- Calls coming from the traversal zone are not allowed to use this gateway -->
          <address is="TraversalZone">
            <!-- Reject call with a status code of 403 (Forbidden) -->
            <reject status="403" reason="Denied by policy"/>
          </address>
        </address-switch>
      </address>
    </address-switch>
  </taa:routed>
</cpl>
```

Using the Taa:Rule-Switch Node

```
<?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>
    <taa:rule-switch>
      <taa:rule originating-zone="TraversalZone" destination="9(.*)">
        <!-- Calls coming from the traversal zone are not allowed to use this gateway -->
        <!-- Reject call with a status code of 403 (Forbidden) -->
        <reject status="403" reason="Denied by policy"/>
      </taa:rule>
      <taa:rule origin="(.*)" destination="(.*)">
        <!-- All other calls allowed -->
        <proxy/>
      </taa:rule>
    </taa:rule-switch>
  </taa:routed>
</cpl>
```

LDAP Server Configuration for Device Authentication

The Expressway can be configured to authenticate devices against an H.350 directory service on an LDAP server.

This section describes how to:

- [download the schemas](#) that must be installed on the LDAP server
- install and configure two common types of LDAP servers for use with the Expressway:
 - [Microsoft Active Directory](#)
 - [OpenLDAP](#)

Downloading the H.350 Schemas

The following ITU specifications describe the schemas which are required to be installed on the LDAP server:

| | |
|---------|---|
| H.350 | Directory services architecture for multimedia conferencing - an LDAP schema to represent endpoints on the network. |
| H.350.1 | Directory services architecture for H.323 - an LDAP schema to represent H.323 endpoints. |
| H.350.2 | Directory services architecture for H.235 - an LDAP schema to represent H.235 elements. |
| H.350.4 | Directory services architecture for SIP - an LDAP schema to represent SIP endpoints. |

The schemas can be downloaded from the web interface on the Expressway. To do this:

1. Go to **Configuration > Authentication > Devices > H.350 directory schemas**. You are presented with a list of downloadable schemas.
2. Click on the **Download** button next to each file to open it.
3. Use your browser's **Save As** command to store it on your file system.

Configuring a Microsoft Active Directory LDAP Server

Prerequisites

These instructions assume that Active Directory has already been installed. For details on installing Active Directory please consult your Windows documentation.

The following instructions are for Windows Server 2003 Enterprise Edition. If you are not using this version of Windows, your instructions may vary.

Installing the H.350 Schemas

After you have [downloaded the H.350 schemas](#), install them as follows:

Open an elevated command prompt by right-clicking Command Prompt and selecting 'Run as administrator'. For each file execute the following command:

```
ldifde -i -c DC=X <ldap_base> -f filename.ldf
```

where:

<ldap_base> is the base DN for your Active Directory server.

Adding H.350 Objects

Create the organizational hierarchy:

Reference Material

1. Open up the Active Directory **Users and Computers** MMC snap-in.
2. Under your BaseDN right-click and select **New Organizational Unit**.
3. Create an Organizational unit called *h350*.

It is good practice to keep the H.350 directory in its own organizational unit to separate out H.350 objects from other types of objects. This allows access controls to be setup which only allow the Expressway read access to the BaseDN and therefore limit access to other sections of the directory.

Add the H.350 objects:

1. Create an Ldif file with the following contents:

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,DC=X
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
objectClass: SIPIdentity
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
SIPIdentityUserName: meetingroom1
SIPIdentityPassword: mypassword
SIPIdentitySIPURI: sip:MeetingRoom@X
```

2. Add the Ldif file to the server using the command:

```
ldifde -i -c DC=X <ldap_base> -f filename.ldf
where:
```

<ldap_base> is the base DN of your Active Directory Server.

The example above will add a single endpoint with an H.323 ID alias of `MeetingRoom1`, an E.164 alias of `626262` and a SIP URI of `MeetingRoom@X`. The entry also has H.235 and SIP credentials of ID `meetingroom1` and password `mypassword` which are used during authentication.

H.323 registrations will look for the H.323 and H.235 attributes; SIP will look for the SIP attributes. Therefore if your endpoint is registering with just one protocol you do not need to include elements relating to the other.

Note: the SIP URI in the `ldif` file must be prefixed by `sip:`.

For information about what happens when an alias is not in the LDAP database see **Source of aliases for registration** in the Device authentication using LDAP section.

Securing with TLS

To enable Active Directory to use TLS, you must request and install a certificate on the Active Directory server. The certificate must meet the following requirements:

- Be located in the Local Computer's Personal certificate store. This can be seen using the **Certificates MMC** snap-in.
- Have the private details on how to obtain a key associated for use with it stored locally. When viewing the certificate you should see a message saying "You have a private key that corresponds to this certificate".
- Have a private key that does not have strong private key protection enabled. This is an attribute that can be added to a key request.
- The Enhanced Key Usage extension includes the Server Authentication object identifier, again this forms part of the key request.
- Issued by a CA that both the domain controller and the client trust.

Reference Material

- Include the Active Directory fully qualified domain name of the domain controller in the common name in the subject field and/or the DNS entry in the subject alternative name extension.

To configure the Expressway to use TLS on the connection to the LDAP server you must upload the CA's certificate as a trusted CA certificate. This can be done on the Expressway by going to: **Maintenance > Security > Trusted CA certificate**.

Configuring an OpenLDAP Server

Prerequisites

These instructions assume that an OpenLDAP server has already been installed. For details on installing OpenLDAP see the documentation at <http://www.openldap.org>.

The following examples use a standard OpenLDAP installation on the Linux platform. For installations on other platforms the location of the OpenLDAP configuration files may be different. See the OpenLDAP installation documentation for details.

Installing the H.350 Schemas

1. Download all the schema files from the Expressway (**Configuration > Authentication > Devices > LDAP schemas**). Ensure that all characters in the filename are in lowercase and name each file with a .schema extension. Hence:

```
commobject.schema
h323identity.schema
h235identity.schema
sipidentity.schema
```

2. Determine the index of each schema file via `slapcat`. For example, for **commobject.schema**:

```
sudo slapcat -f schema_convert.conf -F ldif_output -n 0 | grep commobject,cn=schema
```

will return something similar to: `dn: cn={14}commobject,cn=schema,cn=config`

The index value inside the curly brackets `{}` will vary.

3. Convert each schema file into ldif format via `slapcat`. Use the index value returned by the previous command. For example, for **commobject.schema**:

```
slapcat -f schema_convert.conf -F ldif_output -n0 -H ldap:///cn={14}commobject,cn=schema,cn=config -l cn=commobject.ldif
```

4. Use a text editor to edit the newly created file (**cn=commobject.ldif** in the case of the commobject file) and remove the following lines:

```
structuralObjectClass:
entryUUID:
creatorsName:
createTimestamp:
entryCSN:
modifiersName:
modifyTimestamp:
```

5. Add each schema to the ldap database via `ldapadd`. For example, for **cn=commobject.ldif**:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn\=commobject.ldif
```

(the backslash after `cn` is an escape character)

6. Repeat these steps for every schema file.

More information is available at <https://help.ubuntu.com/13.04/serverguide/openldap-server.html>.

Adding H.350 Objects

Create the organizational hierarchy:

Reference Material

1. Create an `ldif` file with the following contents:

```
# This example creates a single organizational unit to contain the H.350 objects
dn: ou=h350,dc=my-domain,dc=com
objectClass: organizationalUnit
ou: h350
```

2. Add the `ldif` file to the server via `slapadd` using the format:

```
slapadd -l <ldif_file>
```

This organizational unit will form the BaseDN to which the Expressway will issue searches. In this example the BaseDN will be: `ou=h350,dc=my-domain,dc=com`.

It is good practice to keep the H.350 directory in its own organizational unit to separate out H.350 objects from other types of objects. This allows access controls to be setup which only allow the Expressway read access to the BaseDN and therefore limit access to other sections of the directory.

Note: the SIP URI in the `ldif` file must be prefixed by `sip`:

Add the H.350 objects:

1. Create an `ldif` file with the following contents:

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,dc=mydomain,dc=com
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
objectClass: SIPIdentity
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
SIPIdentityUserName: meetingroom1
SIPIdentityPassword: mypassword
SIPIdentitySIPURI: sip:MeetingRoom@domain.com
```

2. Add the `ldif` file to the server via `slapadd` using the format:

```
slapadd -l <ldif_file>
```

The example above will add a single endpoint with an H.323 ID alias of `MeetingRoom1`, an E.164 alias of `626262` and a SIP URI of `MeetingRoom@domain.com`. The entry also has H.235 and SIP credentials of ID `meetingroom1` and password `mypassword` which are used during authentication.

H.323 registrations will look for the H.323 and H.235 attributes; SIP will look for the SIP attributes. Therefore if your endpoint is registering with just one protocol you do not need to include elements relating to the other.

For information about what happens when an alias is not in the LDAP database see **Source of aliases for registration** in the Device authentication using LDAP section.

Securing with TLS

The connection to the LDAP server can be encrypted by enabling Transport Level Security (TLS) on the connection. To do this you must create an X.509 certificate for the LDAP server to allow the Expressway to verify the server's identity. After the certificate has been created you will need to install the following three files associated with the certificate onto the LDAP server:

- the certificate for the LDAP server
- the private key for the LDAP server
- the certificate of the Certificate Authority (CA) that was used to sign the LDAP server's certificate

All three files should be in PEM file format.

Reference Material

The LDAP server must be configured to use the certificate. To do this:

- Edit `/etc/openldap/slapd.conf` and add the following three lines:

```
TLSCACertificateFile <path to CA certificate>
TLSCertificateFile <path to LDAP server certificate>
TLSCertificateKeyFile <path to LDAP private key>
```

The OpenLDAP daemon (`slapd`) must be restarted for the TLS settings to take effect.

To configure the Expressway to use TLS on the connection to the LDAP server you must upload the CA's certificate as a trusted CA certificate. This can be done on the Expressway by going to: **Maintenance > Security > Trusted CA certificate**.

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 we recommend that you generate new SSH keys that 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 and registrations 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 the Default Configuration (Factory Reset)

Rarely, it may be necessary to run the "factory-reset" script on your system. This reinstalls the software image and resets the configuration to the default, functional minimum.

Notes:

- If you've upgraded since the system was first set up, the reset reinstalls your latest software version.
- The system uses the default configuration values that currently apply in the software version installed by the reset. These may differ from your previously configured values, especially if the system has been upgraded from an older version. In particular this may affect port settings, such as multiplexed media ports. After restoring the default configuration you may want to reset those port settings to match the expected behavior of your firewall. (As described below, optionally it's possible to retain a few configuration values like option keys, SSH keys, and FIPS140 mode, but we recommend that you reset all these values.)

Reference Material

Prerequisite Files

The factory reset procedure described below rebuilds the system based on the most recent successfully installed software image. The following two files stored in the `/mnt/harddisk/factory-reset/` system folder, are used for the reinstallation:

- 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 these files are not present on the system (most commonly with a fresh VM installation that has not been upgraded). If so, you must first put the files in place using SCP as root.

Process to Reset to Default Configuration

You must do this procedure from the serial console (or via a direct connection to the appliance with a keyboard and monitor). Because the network settings are rewritten, all calls and any SSH session used to initiate the reset will be dropped and you won't be able to see the procedure output.

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]? | NO |
| Keep FIPS140 configuration [YES/NO]? | NO |
| Keep IP configuration [YES/NO]? | NO |
| Keep ssh keys [YES/NO]? | NO |
| Keep server certificate, associated key and CA trust store [YES/NO]? | NO |
| Keep root and admin passwords [YES/NO]? | NO |
| Save log files [YES/NO]? | NO |

4. Confirm that you want to proceed.
5. After the serial boots, you will be taken to the Install Wizard. Some of the questions in the wizard may be skipped depending on your responses in step 3.

Note: If you were using FIPS140 and you want to enable it again, see the relevant section in the *Cisco Expressway Administration Guide* on the [Maintain and Operate Guides](#) page.

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 xConfiguration Ethernet 1 IP V6 Address xConfiguration Ethernet 2 IP V4 Address xConfiguration Ethernet 2 IP V6 Address | Matches all IPv4 and IPv6 addresses. Applies to all peer addresses if the Expressway is part of a cluster. | not applicable |
| %ipv4% | xConfiguration Ethernet 1 IP V4 Address xConfiguration Ethernet 2 IP V4 Address | Matches the IPv4 addresses currently configured for LAN 1 and LAN 2. 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. Applies to all peer addresses if the Expressway is part of a cluster. | Replaces the string with the LAN 1 IPv4 address. 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. Applies to all peer addresses if the Expressway is part of a cluster. | Replaces the string with the LAN 2 IPv4 address. If the Expressway is part of a cluster, the address of the local peer is always used. |

Reference Material

| String | Represents value returned by... | When used in a Pattern field | When used in a Replace field |
|--------------|--|---|---|
| %ipv6% | xConfiguration Ethernet 1 IP V6 Address xConfiguration Ethernet 2 IP V6 Address | Matches the IPv6 addresses currently configured for LAN 1 and LAN 2. 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. Applies to all peer addresses if the Expressway is part of a cluster. | Replaces the string with the LAN 1 IPv6 address. 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. Applies to all peer addresses if the Expressway is part of a cluster. | Replaces the string with the LAN 2 IPv6 address. If the Expressway is part of a cluster, the address of the local peer is always used. |
| %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 Interoperability Port Reference, page 371](#)
- [Mobile and Remote Access Port Reference, page 369](#)

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.

Reference Material

Table 20 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 | System > Administration |
| Clustering | TLS between cluster peers for database synchronization. | 4371-4372 TCP | inbound outbound | not configurable |
| Reserved | | 636 | inbound | not configurable |
| Clustering | If the Expressway is part of a cluster, this port is used for inbound and outbound communication with peers, even if H.323 is disabled. | 1719 UDP | inbound outbound | Configuration > Protocols > H.323 |
| DNS | Sending requests to DNS servers. | 1024 - 65535 UDP | outbound | System > DNS |
| Gatekeeper discovery | Multicast gatekeeper discovery. The Expressway does not listen on this port when H.323 Gatekeeper Auto discover mode is set to <i>Off</i> (this disables IGMP messages). | 1718 UDP | inbound | not configurable |
| H.323 call signaling | Listens for H.323 call signaling. | 1720 TCP | inbound | Configuration > Protocols > H.323 |
| Assent call signaling | Assent signaling on the Expressway-E. | 2776 TCP | inbound | Configuration > Traversal > Ports |
| H.460.18 call signaling | H.460.18 signaling on the Expressway-E. | 2777 TCP | inbound | Configuration > Traversal > Ports |
| Traversal server media demultiplexing RTP/RTCP | Optionally used on the Expressway-E for demultiplexing RTP/RTCP media on Small/Medium systems only. | 2776/2777 UDP | inbound outbound | Configuration > Traversal > Ports |
| TURN services | Listening port for TURN relay requests on Expressway-E. | 3478 UDP/TCP * | inbound | Configuration > Traversal > TURN |
| System database | Encrypted administration connector to the Expressway system database. | 4444 TCP | inbound | not configurable |
| SIP UDP | Listens for incoming SIP UDP calls. | 5060 UDP | inbound outbound | Configuration > Protocols > SIP |
| SIP TCP | Listens for incoming SIP TCP calls. | 5060 TCP | inbound | Configuration > Protocols > SIP |
| SIP TLS | Listens for incoming SIP TLS calls. | 5061 TCP | inbound | Configuration > Protocols > SIP |

Table 20 Local inbound/outbound ports (continued)

| Service/function | Purpose | Expressway port (default) | Direction | Configurable via |
|---|---|---|---------------------|--|
| SIP MTLs | Listens for incoming SIP Mutual TLS calls. | 5062 TCP | inbound | Configuration > Protocols > SIP |
| B2BUA | Internal ports used by the B2BUA. Other traffic sent to these ports is blocked automatically by the Expressway's non-configurable firewall rules. | 5071, 5073 TCP | inbound | not configurable |
| Traversal server zone H.323 Port | Port on the Expressway-E used for H.323 firewall traversal from a particular traversal client. | 6001 UDP, increments by 1 for each new zone | inbound | Configuration > Zones |
| Traversal server zone SIP Port | Port on the Expressway-E used for SIP firewall traversal from a particular traversal client. | 7001 TCP, increments by 1 for each new zone | inbound | Configuration > Zones |
| H.225 and H.245 call signaling port range | Range of ports used for call signaling after a call is established. | 15000 - 19999 TCP | inbound outbound | Configuration > Protocols > H.323 |
| SIP TCP outbound port range | Range of ports used by outbound TCP/TLS SIP connections to a remote SIP device. | 25000 - 29999 TCP | outbound | Configuration > Protocols > SIP |
| Ephemeral ports | Various purposes. | 30000 - 35999 | outbound | System > Administration |

Table 20 Local inbound/outbound ports (continued)

| Service/function | Purpose | Expressway port (default) | Direction | Configurable via |
|--|---|---|---------------------|---|
| 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 Configuration > Local Zones > 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).</p> <p>Note: Changes to the Use configured demultiplexing ports setting need a system restart to take effect.</p> | <p>2776-2777 OR 36000 - 36001 UDP (Small / Medium systems)</p> <p>or</p> <p>36000 - 36011 UDP (Large systems)</p> | inbound outbound | Configuration > Local Zone > Traversal Subzone |

Table 20 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 Configuration > Local Zones > 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).</p> <p>Note: Changes to the Use configured demultiplexing ports setting need a system restart to take effect.</p> | <p>36002 – 59999 UDP (Small / Medium systems)</p> <p>or</p> <p>36012 – 59999 UDP (Large systems)</p> | inbound outbound | Configuration > Local Zone > Traversal Subzone |
| TURN relay media port range | Range of ports available for TURN media relay. | 24000 – 29999 UDP | inbound outbound | Configuration > Traversal > TURN |

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

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

Remote Listening Ports

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

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

Reference Material

Table 21 Remote listening ports

| Service/function | Purpose | Destination port (default) | Configurable via |
|---|--|----------------------------|--|
| DNS | Requests to a DNS server. | 53 UDP | System > DNS |
| External manager | Outbound connection to an external manager, for example Cisco TMS. | 80 TCP | System > External manager |
| NTP | System time updates. | 123 UDP | System > Time |
| LDAP account authentication | LDAP queries for login account authentication. | 389 / 636 TCP | Users > LDAP configuration |
| TMS Provisioning Extension | Connection to Cisco TMSPE services. | 443 TCP | System > TMS Provisioning Extension services |
| Incident reporting | Sending application failure details. | 443 TCP | Maintenance > Diagnostics > Incident reporting > Configuration |
| Third-party FindMe / User Policy server | Outbound connection to a third-party FindMe / User Policy server. | 443 TCP | Applications > FindMe |
| Remote logging | Sending messages to the remote syslog server. | 514 UDP 6514 TCP | Maintenance > Logging |
| Neighbors (H.323) | H.323 connection to a neighbor zone. | 1710 UDP | Configuration > Zones |
| Neighbors (SIP) | SIP connection to a neighbor zone. | 5060 / 5061 TCP | Configuration > Zones |
| Traversal zone (H.323) | H.323 connection to a traversal server. | 6001 UDP | Configuration > Zones |
| Traversal zone (SIP) | SIP connection to a traversal server. | 7001 TCP | Configuration > Zones |
| Endpoint (H.323) | Endpoint listening port | 1720 TCP | Defined by endpoint's registration |
| Endpoint (SIP) | Endpoint listening port | 5060 / 5061 TCP / UDP | Defined by endpoint's registration |
| System Metrics Collection | Publishing metrics to a remote analytics server | 25826 UDP | Maintenance > Logging |
| TURN media relay | Range of ports available for TURN media relay. | 24000 - 29999 UDP | Configuration > Traversal > TURN (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 |

Reference Material

| Purpose | Protocol | Expressway-C (source) | Expressway-E (listening) |
|---|----------|-----------------------|--|
| Traversal zone SIP media (for small/medium systems on X8.1 or later) | UDP | 36000 to 59999* | 36000 (RTP), 36001 (RTCP) (defaults) |
| Traversal zone SIP media (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 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 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 Internal Infrastructure and Endpoints

| Purpose | Protocol | Expressway-C (source) | Internal Device Port/Range |
|---|----------|-----------------------|--|
| 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/HTTPS (configuration file retrieval) | TCP | Ephemeral port | (Unified CM) HTTP 6970 Or HTTPS 6972 if you have Cisco Jabber 11.x or later with Unified CM 11.x or later |
| CUC (voicemail) | TCP | Ephemeral port | 443 (Unity Connection) |

Reference Material

| Purpose | Protocol | Expressway-C (source) | Internal Device Port/Range |
|---|----------|-----------------------|--|
| Message Waiting Indicator (MWI) from Unity Connection | TCP | Ephemeral port | 7080 (Unity Connection) |
| Media | UDP | 36000 to 59999* | >= 1024 (Media recipient eg. endpoint) |
| SIP signaling | TCP | 25000 to 29999 | 5060 (Unified CM) |
| Secure SIP signaling | TLS | 25000 to 29999 | 5061 (Unified CM) |

* The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at **Configuration > Local Zones > 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:** Changes to the **Use configured demultiplexing ports** setting need a system restart to take effect.

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 Interoperability 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 Microsoft infrastructure or clients, or configuration on Expressway (**Applications > B2BUA**).

Table 22 Between B2BUA and Microsoft Environment

| Purpose | Protocol | Expressway port | Microsoft port |
|---------------------------------|----------|-----------------|----------------------------------|
| Signaling to Microsoft server | TLS | 65072 | 5061 (Server SIP listening port) |
| Signaling from Microsoft server | TLS | 65072 | Ephemeral port |

Reference Material

Table 22 Between B2BUA and Microsoft Environment (continued)

| Purpose | Protocol | Expressway port | Microsoft port |
|---|-----------|--|------------------------------|
| <p>Media</p> <p>(The Microsoft interoperability service should run on a separate "Gateway" Expressway and so this range should not conflict with the standard traversal media port range)</p> <p>Note: The Expressway does not forward DSCP information that it receives in media streams.</p> | UDP & TCP | <p>56000 to 57000</p> <p>Each call can use up to 18 ports if you Enable RDP Transcoding for this B2BUA.</p> <p>Increase this range if you see "Media port pool exhausted" warnings.</p> | Microsoft client media ports |
| Screen share from Microsoft clients to B2BUA | TCP | 56000 to 57000 | Microsoft client RDP ports |

Table 23 Between B2BUA and Internal Video Network

| Purpose | Protocol | Expressway port | Expressway IP port |
|--|----------|-----------------|---|
| Internal communications with Expressway application | TLS | 65070 | SIP TCP outbound port on Expressway |
| Transcoded screen shares (H.264) from B2BUA to BFCP capable recipients | UDP | 56000 to 57000 | Recipient of media is dependent on deployment and called alias; eg. endpoint, TelePresence Server, Expressway-C |

Table 24 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.

Table 25 External Microsoft Client and Edge Server

| Purpose | Protocol | Edge server | Microsoft client |
|---|----------|-------------|------------------|
| SIP/MTLS used between Microsoft Client and Edge server for signaling (including any ICE messaging to the Edge Server) | TCP | 5061 | 5061 |
| SIP/TLS | TCP | 443 | 443 |
| STUN | UDP | 3478 | 3478 |
| UDP Media | UDP | 50000-59999 | 1024-65535 |
| TCP Media | TCP | 50000-59999 | 1024-65535 |

Reference Material

Table 26 External Microsoft Client / Edge Server and Expressway-E

| Purpose | Protocol | Microsoft client / Edge server | Expressway-E |
|--|-----------|--------------------------------|--------------|
| ICE messaging (STUN/TURN) (Expressway-E must listen on TCP 3478 for screen sharing relay requests from Microsoft clients, and on UDP 3478 for A/V media relay requests) | UDP & TCP | 3478 | 3478 |
| UDP media | UDP | 1024-65535 | 24000-29999 |

Table 27 Between B2BUA and External 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. | . <code>*</code> 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? <code>?</code> 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. You cannot use special characters within the [] - they will be taken literally. | [a-z] matches any alphabetical character [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. You cannot use special characters within the [] - they will be taken literally. | [^a-z] matches any non-alphabetical character [^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 (.) <code>*</code> _(.) <code>*</code> (@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. | . <code>*</code> @example.(net com) matches against any URI for the domain example.com or the domain example.net |

Reference Material

| | | |
|----------|---|--|
| \ | Escapes a regular expression special character. | |
| ^ | Signifies the start of a line. When used immediately after an opening brace, negates the character set inside the brace. | [^abc] matches any single character that is NOT one of a, b or c |
| \$ | Signifies the end of a line. | ^\d\d\d\$ matches any string that is exactly 3 digits long |
| (?!...) | Negative lookahead. Defines a subexpression that must not be present. | (?!.*@example.com\$) .* matches any string that does not end with @example.com (?!alice) .* matches any string that does not start with alice |
| (?<!...) | Negative lookbehind. Defines a subexpression that must not be present. | .*(?<!net) matches any string that does not end with net |

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

Room and Desktop Registrations on Expressway

X8.8 introduced the ability to use the Expressway-C as a SIP registrar, for TelePresence room and desktop systems. And a new licensing model with that feature.

X8.9 extends the feature to enable H.323 Gatekeeper functionality on the Expressway-C.

When you configure the Expressway as a SIP registrar or H.323 Gatekeeper, you must license it for concurrent systems (the Unified CM model), not for concurrent calls (the VCS model).

For SIP deployments, you can do this by adding either or both of the following license types to the Expressway-C:

- TelePresence Room System License
- Desktop System License

The following SIP devices register as desktop systems with all other devices considered room systems:

- Cisco TelePresence EX60
- Cisco TelePresence EX90
- Cisco DX70
- Cisco DX80

For H.323 deployments, all endpoints consume a TelePresence Room System License. This is due to a limitation in H.323, which does not determine the difference between desktop and room type endpoints.

We therefore recommend SIP as the preferred signaling protocol. H.323 is available as a fall back for endpoints that do not support SIP.

Note: DX systems must be running version CE8.2 or later and EX systems TC7.3.6 or later in order to register as desktop systems (for SIP only). DX and EX systems running earlier versions will still register for SIP but will consume a room system license.

Scope of the registrar feature:

- Option keys containing licenses for local registrations are installed on the Expressway-C. These licenses are pooled in a cluster, which means that Expressway-C peers can use each others' licenses. However, rooms cannot use desktop licenses, and desktop systems cannot use room licenses.
- Registrations from outside the network are proxied to Expressway-C by the Expressway-E. The Expressway-E cannot accept direct registrations.
- Proxy registration is possible with SIP endpoints only and does not apply to H.323 endpoints.
- Device provisioning and FindMe are supported with Cisco TelePresence Management Suite.
- The Large VM or CE1100 can support up to 5000 registrations, or 2500 MRA registrations (proxied to CUCM). Local registrations, proxy registrations (via Expressway-E), and MRA registrations, all count towards this number.

Implications of the new licensing model reduces the usage of Rich Media Session (RMS) licenses in the following scenarios:

- If you have already paid for a registration license, RMS licenses will not be consumed for the following call types; provided that the Expressway is not required for encryption interworking (invoking the B2BUA):
 - Calls between registered systems do not use RMS licenses. Here, 'registered systems' means systems registered directly to the Expressway-C, by proxy to the Expressway-C through the Expressway-E, or by proxy through the Expressway pair (MRA) to neighbored Unified CMs.

Reference Material

- Calls from registered systems (as above) to Cisco infrastructure do not use RMS licenses. Currently, this extends only to Cisco Meeting Server, and to CiscoTelePresence Server and TelePresence MCUs that are managed by TelePresence Conductor. However, calls from MCUs that are not managed by Conductor do consume RMS licenses.
- Calls from registered systems (as above) to Cisco Collaboration Cloud do not use RMS licenses.
- However, calls from registered systems to all other systems use one RMS license. This includes, but is not limited to, the following call types:
 - Business to business calls. Previously required two RMS licenses, now require one on Expressway-E.
 - Business to consumer calls (Jabber Guest). Previously required two RMS licenses, now require one on the Expressway-E.
 - Interoperability gateway calls, including Microsoft Lync / Skype for Business and third-party call control servers require one RMS license on the Expressway-C.

See [Call Types and Licensing, page 377](#) for more information about the calls that consume RMS licenses.

Call Types

The Expressway distinguishes between the following types of call:

Registered: calls between locally registered endpoints (registered to Unified CM or Expressway) do not consume licenses, as that entitlement is included within the registration.

The call entitlement within the registration license includes the following scenarios:

- Calls to other endpoints registered to Unified CM or Expressway within the same network when the call is routed through a neighbor or traversal zone.
- Unified CM remote sessions: these are Mobile and Remote Access (MRA) calls i.e. video or audio calls from devices located outside the enterprise that are routed via the Cisco Expressway firewall traversal solution to endpoints registered to Unified CM.
- Calls to Cisco conferencing resources (CMR, TelePresence Server/ TelePresence Conductor, or Acano servers).

Note: These calls are still counted against the physical limit of the box.

Rich Media Sessions: these calls consume rich media session (RMS) licenses and consist of every other type of video or audio call that is routed through the Expressway. RMS licenses are consumed in the following scenarios:

- B2B
- B2BUA
- Jabber Guest
- Interworked or gatewayed calls to third-party solutions
- Interworked SIP to H.323 calls (RMS license is consumed on the node where interworking takes place)
- Interworked IPV4 to IPV6 calls

The Expressway may take the media or just the signaling.

Audio-only SIP calls are treated distinctly from video SIP calls. Each rich media session license allows either 1 video call or 2 audio-only SIP calls. Hence, a 100 rich media session license would allow, for example, 90 video and 20 SIP audio-only simultaneous calls. Any other type of audio-only call will consume a rich media session license.

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.

Reference Material

- 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.
- The Expressway does not support midcall license optimization.

RMS License Consumption

The below table details RMS license consumption in different call scenarios.

| Calling from | Calling to | Expressway-C | Expressway-E |
|-----------------------------|------------------------|-------------------------------|-------------------------------|
| Unified CM | Unified CM (MRA) | 0 | 0 |
| Unified CM (MRA) | Unified CM (MRA) | 0 | 0 |
| Unified CM | CMR | 0 | 0 |
| Unified CM | Expressway-C (Lync) | 1 Expressway-C (Lync Gateway) | 0 |
| Unified CM | External | 0 | 1 |
| Unified CM | Third-party Gatekeeper | 1 | 0 |
| Unified CM | Expressway-C | 0 | 0 |
| Expressway-C | Expressway-C | 0 | 0 |
| Expressway-C | Expressway-C (Remote) | 0 | 0 |
| Expressway-C (Remote) | Expressway-C (Remote) | 0 | 0 |
| Expressway-C | External | 0 | 1 |
| Expressway-C (Remote) | External | 0 | 1 |
| Expressway-C | CMR | 0 | 0 |
| Expressway-C (Remote) | CMR | 0 | 0 |
| Expressway-C (SIP) | Third-party Gatekeeper | 1 | 0 |
| Expressway-C (H323) | Third-party Gatekeeper | 0 | 0 |
| Expressway-C (Remote [SIP]) | Third-party Gatekeeper | 1 | 0 |
| Expressway-C | TelePresence Conductor | 0 | 0 |
| Expressway-C (Remote) | TelePresence Conductor | 0 | 0 |
| Expressway-C | Expressway-C (Lync) | 0 | 1 Expressway-C (Lync Gateway) |

Reference Material

| | | | |
|-----------------------|------------------------|---|-------------------------------|
| Expressway-C (Remote) | Expressway-C (Lync) | 0 | 1 Expressway-C (Lync Gateway) |
| Expressway-C (SIP) | Third-party SIP server | 0 | 0 |
| Expressway-C (H323) | Third-party SIP server | 1 | 0 |

License Bypass for Calls to Collaboration Meeting Rooms (CMRs)

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

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

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

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

Product Identifiers and Corresponding Keys

| Feature or License Option | PID (Product Identifier) | Key Pattern | Valid On | Required For |
|-----------------------------|--------------------------|---------------------------|-------------------------------|--|
| Release Key | LIC-SW- VMVCS-K9 | 16 digit number | VCS Control VCS Expressway | Enabling the system. The key is unique to a serial number and a particular base version of software. Most features will not work permanently without this key. |
| Release Key | LIC-SW- EXP-K9 | 16 digit number | Expressway-C Expressway-E | Enabling the system. The key is unique to a serial number and a particular base version of software. Most features will not work permanently without this key. |
| Expressway Series | LIC-EXP- SERIES | 116341E00- m- ##### | Expressway-C Expressway-E | Enabling an Expressway Series system (for anything except Spark Hybrid Services) |
| Rich Media Session licenses | LIC-EXP- RMS | 116341Yn- m- ##### | Expressway-C Expressway-E | <p>Calls enabled by Expressway where the Expressway must process the media streams (also known as 'traverse' or 'handle' the media).</p> <p>RMS licenses are used by calls that require:</p> <ul style="list-style-type: none"> ■ IPv4-IPv6 interworking ■ H.323-SIP interworking ■ Media encryption on behalf of another entity ■ Microsoft SIP to standards-based SIP interworking <p>RMS licenses are not used by CMR Cloud calls</p> |

Reference Material

| Feature or License Option | PID (Product Identifier) | Key Pattern | Valid On | Required For |
|--------------------------------------|--------------------------|-------------------|--------------------------------|--|
| Traversal call licenses | LIC-VCSE-n | 116341Wn-m-##### | VCS Control VCS Expressway | <p>Calls enabled by VCS where the VCS must process the media streams (also known as 'traverse' or 'handle' the media).</p> <p>Traversal call licenses are used by calls that require:</p> <ul style="list-style-type: none"> ■ IPv4-IPv6 interworking ■ H.323-SIP interworking ■ Media encryption on behalf of another entity ■ Microsoft SIP to standards-based SIP interworking <p>Traversal call licenses are not used by CMR Cloud calls</p> |
| Non-traversal call licenses | LIC-VCS-n | 116341Vn-m-##### | VCS Control VCS Expressway | Calls enabled by VCS that don't require media traversal (signaling only) |
| Registration licenses | LIC-VCS-nREG | 116341Rn-m-##### | VCS Control VCS Expressway | Registering callers to VCS |
| Room system registration licenses | LIC-EXP-ROOM | 116341An-m-##### | Expressway-C | Registering TelePresence rooms to Expressway-C. Includes the FindMe and Device Provisioning features. |
| Desktop system registration licenses | LIC-EXP-DSK | 116341Bn-m-##### | Expressway-C | Registering desktop endpoints to Expressway-C. Includes the FindMe and Device Provisioning features. |
| TURN relay licenses | LIC-EXP-TURN | 116341In-m-##### | VCS Expressway Expressway-E | Jabber Guest, Microsoft Interoperability (offsite MS clients) |
| Traversal Server feature | LIC-EXP-E | 116341T00-m-##### | VCS Expressway Expressway-E | Firewall traversal: MRA, B2B, CMR Cloud, CMR Hybrid, Proxy registrations, Jabber Guest, MS interop (offsite MS clients) |
| FindMe feature | LIC-VCS-FINDME | 116341U00-m-##### | VCS Control | <p>Multiple aliases managed by Cisco TMS.</p> <p>This key is not required on Expressway-C. The feature is automatically enabled when Expressway-C has Room/Desktop registration licenses installed.</p> |
| Interworking H.323 to SIP feature | LIC-EXP-GW | 116341G00-m-##### | VCS Control Expressway-C | This key is not explicitly required on Expressway, but does not interfere with operation if loaded. |

Reference Material

| Feature or License Option | PID (Product Identifier) | Key Pattern | Valid On | Required For |
|-----------------------------------|--------------------------|-------------------|--------------------------------|--|
| Device Provisioning feature | LIC-VCS-DEVPROV | 116341P00-m-##### | VCS Control | Provisioning endpoints with configuration and phonebook data from Cisco TMS. This key is not required on Expressway-C. The feature is automatically enabled when Expressway-C has Room/Desktop registration licenses installed. |
| Advanced Networking feature | LIC-EXP-AN | 116341L00-m-##### | VCS Expressway Expressway-E | Enabling second NIC and static NAT. |
| Advanced Account Security feature | LIC-VCS-JITC | 116341J00-m-##### | VCS Control VCS Expressway | Enabling FIPS140-2 cryptographic mode (in highly secure environments) Enabling Advanced Account Security mode |
| Advanced Account Security feature | LIC-EXP-JITC= | 116341J00-m-##### | Expressway-C Expressway-E | Enabling FIPS140-2 cryptographic mode (in highly secure environments) Enabling Advanced Account Security mode |
| Microsoft Interoperability | LIC-EXP-MSFT | 116341C00-m-##### | VCS Control Expressway-C | All integration between Expressway and Microsoft infrastructure, including: A/V call interworking, desktop sharing from Microsoft clients, chat and presence federation with IM&P. |

n - the number of licenses supplied with this key. If this position contains 00, it means the key is for a feature, rather than a number of licenses.

m - the index of the key, usually 1.

- a hex digit.

Allow List Rules File Reference

You can define rules using a CSV file. This topic provides a reference to acceptable data for each rule argument, and demonstrates the format of the CSV rules.

Table 28 Allow List Rule Arguments

| Argument index | Parameter name | Required/Optional | Sample value |
|----------------|----------------|-------------------|---|
| 0 | Url | Required | <p><code>protocol://host[:port] [/path]</code></p> <p>Where:</p> <ul style="list-style-type: none"> ■ protocol is <code>http</code> or <code>https</code> ■ host may be a DNS name or IP address ■ :port is optional, and may only be <code>:</code> followed by one number in the range 0-65535, eg. <code>:8443</code> <p>If the port is not specified, then the Expressway uses the default port for the supplied protocol (80 or 443)</p> <ul style="list-style-type: none"> ■ /path is optional and must conform to HTTP specification |
| 1 | Deployment | Optional | Name of the deployment that uses this rule. Required when you have more than one deployment, otherwise supply an empty argument. |
| 2 | HttpMethods | Optional | Comma-delimited list of HTTP methods, optionally in double-quotes, eg. <code>"GET,PUT"</code> |
| 3 | MatchType | Optional | <code>exact</code> or <code>prefix</code> . Default is <code>prefix</code> |
| 4 | Description | Optional | Text description of the rule. Enclose with double quotes if there are spaces. |

Example CSV file

```
Url,Deployment,HttpMethods,MatchType,Description
https://myServer1:8443/myPath1,myDomain1,GET,, "First Rule"
http://myServer2:8000/myPath2,myDomain200,"GET,PUT",exact,
https://myServer3:8080/myPath3,myDomain1,,prefix,"Third Rule"
https://myServer4/myPath4,myDomain1,,prefix,"Fourth Rule"
http://myServer5/myPath5,myDomain1,,prefix,"Fifth Rule"
```

- List the parameter names (as shown) in the first line of the file
- One rule per line, one line per rule
- Separate arguments with commas
- Correctly order the rule values as shown in the table above
- Enclose values that have spaces in them with double quotes

Allow List Tests File Reference

You can define tests using a CSV file. This topic provides a reference to acceptable data for each test argument, and demonstrates the format of the CSV tests.

Table 29 Allow List Test Arguments

| Argument index | Parameter name | Required/Optional | Sample value |
|----------------|----------------|-------------------|--|
| 0 | Url | Required | <code>protocol://host[:port] [/path]</code> Where: <ul style="list-style-type: none"> ■ protocol is <code>http</code> or <code>https</code> ■ host may be a DNS name or IP address ■ :port is optional, and may only be <code>:</code> followed by one number in the range 0-65535 ■ /path is optional and must conform to HTTP specification |
| 1 | ExpectedResult | Required | <code>allow</code> or <code>block</code> . Specifies whether the test expects that the rules should allow or block the specified URL. |
| 2 | Deployment | Optional | Name of the deployment to test with this URL. If you omit this argument, the test will use the default deployment. |
| 3 | Description | Optional | Text description of the rule. Enclose with double quotes if there are spaces. |
| 4 | HttpMethod | Optional | Specify one HTTP method to test eg. <code>PUT</code> . Defaults to <code>GET</code> if not supplied. |

Example CSV file

```

Url,ExpectedResult,Deployment,Description,HttpMethod
https://myServer1:8443/myPath1,block,"my deployment","a block test",GET
http://myServer2:8000/myPath2,allow,"my deployment","an allow test",PUT
https://myServer4/myPath4,allow,,,GET
http://myServer4/myPath4,block,,,POST

```

- List the parameter names (as shown) in the first line
- One test per line, one line per test
- Separate arguments with commas
- Correctly order the test values as shown in the table above
- Enclose values that have spaces in them with double quotes

Expressway Multitenancy Overview

The Expressway product line is used in Cisco Hosted Collaboration Solution to provide various edge access features including the following:

- Mobile and Remote Access (MRA) allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging, and presence services provided by Cisco Unified Communications Manager for endpoints outside the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations.
- Business to Business (B2B) enables secure connectivity options that allow dialing to and from non-Cisco Hosted Collaboration Solution enterprises reachable through the Internet.
- Spark Hybrid Services that link your on-premises equipment with the Cisco Collaboration Cloud for an integrated Spark experience.

Reference Material

Deploying these services requires a Cisco Expressway-E cluster and Expressway-C cluster to be set up and managed for each customer. For small customers, this can lead to inefficient utilization of resources and an extra management burden.

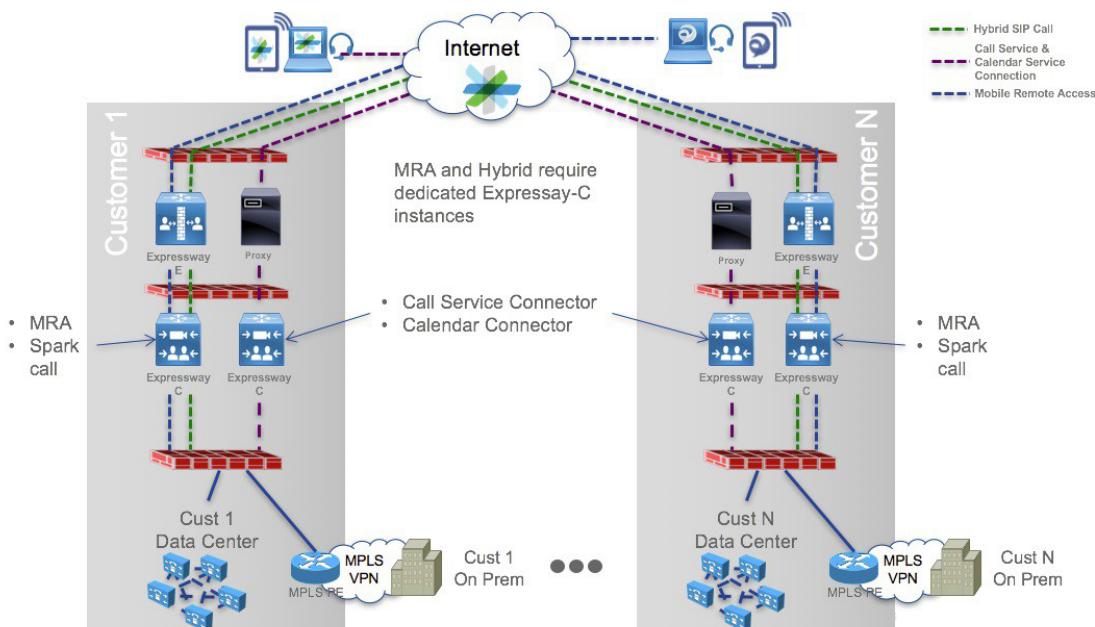
To help alleviate this overhead, a multitenant configuration can be deployed. This allows the partner to share the Expressway-E cluster across up to 50 customers while a dedicated Expressway-C cluster is deployed per customer.

This dedicated Expressway-C cluster can be used for all three services, MRA, B2B, and Hybrid. This configuration is intended to support small customers, up to around 500 users per customer.

For larger customers, we recommend using a single-tenant (dedicated) Expressway-E cluster to meet the customer's scale and performance requirements.

The following diagram shows the single-tenant deployment option. The diagram shows two customers for clarity, but there will typically be many more. In this option, each customer has dedicated and isolated Expressway-E and -C clusters for MRA, B2B, and Hybrid. Also note in this diagram that a separate Expressway-C cluster is used for the Call Service and Calendar connectors.

Figure 16 Single-tenant Expressway deployment

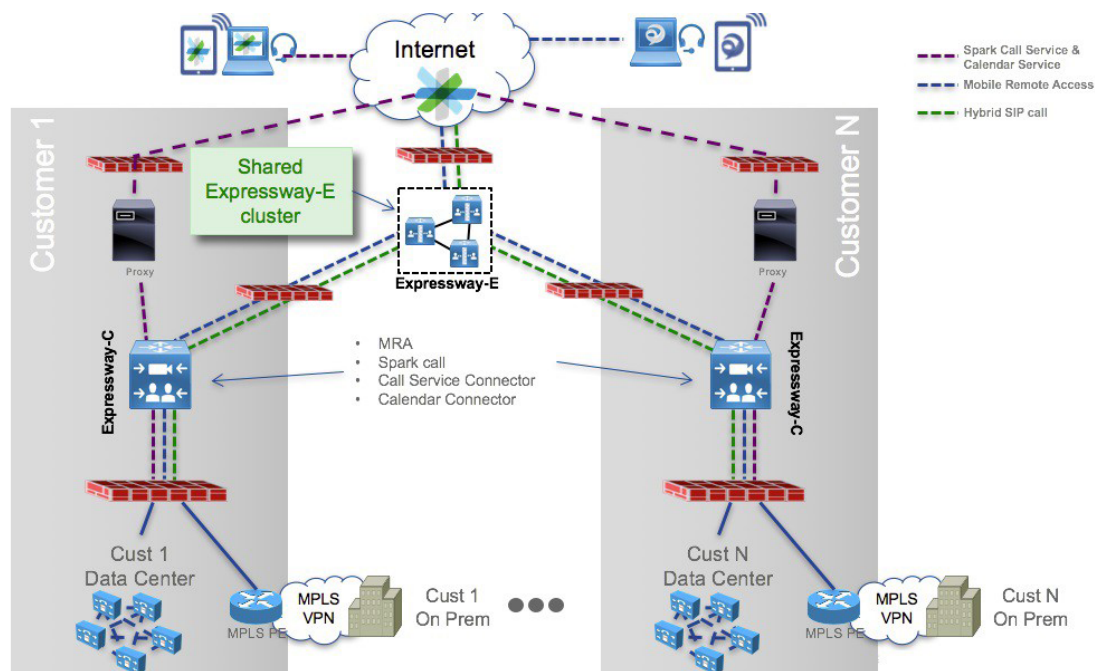


Note that in this diagram, there are two aspects of the Hybrid integration separated out to show the different Expressway-C clusters used:

- Hybrid SIP Call with the green dashed line. This interface is used for the Call Service Connect feature and is a basic SIP call through Expressway. This interface shares the same Expressway-C cluster with the MRA and B2B services.
- Call Service and Calendar Service Connection with the purple dashed line. This interface is used for the Call Service Aware and Calendar services. This interface uses a dedicated Expressway-C cluster.

With the multi-tenant configuration, these two interfaces are combined into a single Expressway-C cluster. The following diagram shows the multitenant deployment option which uses a shared Expressway-E cluster to service multiple customers. It combines the Expressway-C clusters for connectors, MRA, B2B, and Hybrid SIP call (Spark call) into one Expressway-C cluster.

Figure 17 Multitenant Expressway deployment



The shared Expressway-E cluster is deployed in the service provider's DMZ network with six nodes and large-size OVA virtual machines. It is configured for dual-interface deployment with network address translation (NAT) for outside IP addresses of Expressway-Es. A unique traversal zone will be created in the Expressway-E cluster for each per-customer Expressway-C cluster.

Multitenant Expressway Restrictions

Multitenant Expressway has some restrictions relative to the standard Expressway product. The following features are not supported in multi-tenant mode:

- Jabber Guest
- H323 in its various modes, including:
 - H323/SIP Interworking
 - Business-to-Business H323
 - H323 Gatekeeper
- Lync interop
- Skype for Business interop
- IPv6
- Cisco Meeting Server (CMS)

See *Multitenancy with Cisco Expressway* on the [Cisco Hosted Collaboration Solution](#) page.

Multitenant Expressway Sizing

In previous Expressway releases, Expressway-E and Expressway-C cluster deployments are restricted to matching cluster and OVA sizes. The number of nodes in the Expressway-E cluster must match the number of nodes in the Expressway-C cluster. Each node must be the same OVA size in both clusters.

Reference Material

With the multitenant deployment option, that restriction is relaxed. The recommended deployment is a shared 6-node large OVA Expressway-E cluster, and dedicated 2-node medium OVA Expressway-C cluster per customer.

For customers who need more capacity than a 2-node medium OVA cluster affords, we recommend deploying a dedicated Expressway-E cluster to meet their requirements.

For overall sizing recommendations, refer to the [Collaboration Solution Sizing Guidance](#) chapter of the *Cisco Hosted Collaboration Solution Reference Network Design Guide*. In particular, the Expressway section of this chapter discusses the sizing and capacity of Expressway clusters.

In a multitenant deployment, the Expressway-E's capacity is shared across all of the customers, whereas the Expressway-C cluster's capacity is dedicated to the customer. The following tables provide the recommended capacity per customer.

Shared Expressway-E cluster sizing

| Cluster size | Proxied MRA registrations | Video calls | Audio-only calls |
|---|---------------------------|-------------|------------------|
| 6 nodes, large OVA N+2 arrangement so capacity is for 4 nodes, allowing 2 nodes to fail without loss of capacity | 10,000 | 2,000 | 4,000 |
| Per-customer maximum (for 50 customers) | 200 | 40 | 80 |

Dedicated Expressway-C cluster sizing

| Cluster size | Proxied MRA registrations | Video calls | Audio-only calls |
|---|---------------------------|-------------|------------------|
| 2 nodes, medium OVA N+1 arrangement so capacity is a single node, allowing 1 node to fail without loss of capacity | 2,500 | 100 | 200 |

In the above tables, the video calls and audio-only calls account for the total of MRA calls, B2B calls, and Hybrid calls. With the recommended 50-customer maximum per shared Expressway-E cluster, the maximum average concurrent MRA registrations per customer is 200, well below the Expressway-C cluster's capacity.

Likewise, the maximum average concurrent video calls per customer is 40, again below the capacity of the Expressway-C cluster. This spare capacity in the Expressway-C cluster is used by the co-resident Hybrid connectors without impacting the proxied registration or call capacity.

There are two use cases to consider when planning the size of customers that are sharing the Expressway-E. In both of these use cases, the Expressway-E cluster is the limiting factor; there is plenty of capacity in the Expressway-C.

Use Case 1

Most customers are using MPLS for in-office connectivity and only using MRA at home or when mobile. In this case, only a small percentage (10-20%) of users are registered with MRA at any given time. Maximum users per customer should be around 500.

Use Case 2

Most customers are not using MPLS and are using MRA for all connectivity. In this case, 100% of users are registered with MRA. Maximum users per customer must not exceed 200.

The following table summarizes these deployment options.

Deployment scenarios


Reference Material

| Use case | Average maximum users per customer | Percentage of users that can register via MRA at once | Notes |
|----------|------------------------------------|---|---|
| 1 | 500 | 40% | Use this when most customers are using MPLS for in-office connectivity. |
| 2 | 200 | 100% | Use this when most customers are using MRA for in-office connectivity. |

See *Multitenancy with Cisco Expressway* on the [Cisco Hosted Collaboration Solution page](#).

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 | Hybrid Services alarms |
| 60000-60099 | Management Connector alarms |
| 60100-60199 | Calendar Connector alarms |
| 60300-60399 | Call Connector alarms |

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 Reference

The following tables list the alarms that can be raised on the Expressway.

- [Table 30 Hardware Alarms, page 390](#)
- [Table 31 Software Alarms, page 390](#)
- [Table 32 Cluster Alarms, page 391](#)
- [Table 33 Network Alarms, page 393](#)
- [Table 34 License Alarms, page 395](#)
- [Table 35 External Applications / Services Alarms, page 398](#)
- [Table 36 Security Alarms, page 399](#)
- [Table 37 Misconfiguration Alarms, page 404](#)
- [Table 38 Back to Back User Agent Alarms, page 405](#)
- [Table 39 Management Connector Alarms, page 410](#)

Reference Material

- [Table 40 Calendar Connector Alarms, page 413](#)
- [Table 41 Call Connector Alarms, page 417](#)

Table 30 Hardware Alarms

| 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 |
| 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 |

Table 31 Software Alarms

| ID | Title | Description | Solution | Severity |
|-------|-------------------------|--|--|----------|
| 15004 | Application failed | An unexpected software error was detected in <module> | View the incident reporting page | Error |
| 15005 | Database failure | Please remove database and restore from backup, then reboot the system | Reboot the system | 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 | Restore 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 incident reporting page | Error |
| 15011 | Application failed | An unexpected software error was detected in <module> | View the incident reporting 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 |

Reference Material

Table 31 Software Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|------------------------------------|--|---|----------|
| 15014 | Restart required | Core dump mode has been changed, however a restart is required for this to take effect | Restart the system | Warning |
| 15015 | Maintenance mode | The Expressway is in Maintenance mode and will no longer accept calls and registrations | | Warning |
| 15016 | Directory service database failure | The directory service database is not running | Restart the system | 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 | Reboot the system | 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 |
| 15021 | Delayed Cisco XCP Router restart | The Cisco XCP Router service is currently not running on the latest configuration as the delayed Cisco XCP Router restart feature is enabled. | Restart the router on the Delayed Cisco XCP Router restart page or set it to restart at a scheduled time. | Warning |
| 15022 | Restart required | Domain certificate configuration has been changed, however a restart is required for this to take effect. | Restart the system. | Warning |

Table 32 Cluster Alarms

| ID | Title | Description | Solution | Severity |
|-------|-------------------------------|--|--|----------|
| 20020 | Restart required | TLS verification configuration does not match active status. | Restart the system. | Warning |
| 20021 | Cluster communication failure | Unable to establish a TCP connection with <peers> on ports <ports> | Check the port reference guide. | Warning |
| 20003 | Invalid cluster configuration | The cluster configuration is invalid | Check the Clustering page and ensure that this system's IP address is included and there are no duplicate IP addresses | Warning |

Table 32 Cluster Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--|---|--|----------|
| 20004 | Cluster communication failure | The system is unable to communicate with one or more of the cluster peers | Check the clustering configuration | Warning |
| 20005 | Invalid peer address | One or more peer addresses are invalid | Check the Clustering 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 clustering configuration and restart | Warning |
| 20007 | Restart required | Cluster configuration has been changed, however a restart is required for this to take effect | Restart the system | 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 cluster replication instructions | 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 primary's configuration, manual synchronization of configuration is required | View cluster replication instructions | Warning |
| 20012 | Cluster replication error | This peer's cluster configuration settings do not match the configuration primary peer's settings | Configure this peer's cluster settings | Warning |
| 20014 | Cluster replication error | Cannot find primary or this peer's configuration file, manual synchronization of configuration is required | View cluster replication instructions | Warning |
| 20015 | Cluster replication error | The local Expressway does not appear in the list of peers | Check the list of peers for this cluster | Warning |
| 20016 | Cluster replication error | The primary peer is unreachable | Check the list of peers for this cluster | Warning |
| 20017 | Cluster replication error | Configuration primary ID is inconsistent, manual synchronization of configuration is required | View cluster replication instructions | Warning |
| 20018 | Invalid clustering configuration | H.323 mode must be turned On - clustering uses H.323 communications between peers | Configure H.323 mode | Warning |

Reference Material

Table 32 Cluster Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|-----------------------------|--|--|----------|
| 20019 | Cluster name not configured | If FindMe or clustering are in use a cluster name must be defined. | Configure the cluster name | Warning |

Table 33 Network Alarms

| ID | Title | Description | Solution | Severity |
|-------|-----------------------------|--|--|----------|
| 25001 | Restart required | Network configuration has been changed, however a restart is required for this to take effect | Restart the system | Warning |
| 25002 | Date and time not validated | The system is unable to obtain the correct time and date from an NTP server | Check the time configuration | 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 IP settings | 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 IP settings | 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 IP page and then restart the system . | Warning |
| 25007 | Restart required | QoS settings have been changed, however a restart is required for this to take effect | Restart the system | Warning |
| 25008 | Restart required | Port configuration has been changed, however a restart is required for this to take effect | Restart the system | Warning |
| 25009 | Restart required | Ethernet configuration has been changed, however a restart is required for this to take effect | Restart the system | Warning |
| 25010 | Restart required | IP configuration has been changed, however a restart is required for this to take effect | Restart the system | Warning |

Table 33 Network Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--------------------------------|---|---|----------|
| 25011 | Restart required | HTTPS service has been changed, however a restart is required for this to take effect | Restart the system | 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 IP settings | Warning |
| 25014 | Configuration warning | IP protocol is set to both IPv4 and IPv6, but the Expressway does not have any IPv6 addresses defined | Configure IP settings | Warning |
| 25015 | Restart required | SSH service has been changed, however a restart is required for this to take effect | Restart the system | 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 Ethernet parameters | Warning |
| 25017 | Restart required | HTTP service has been changed, however a restart is required for this to take effect | Restart the system | Warning |
| 25018 | Port conflict | There is a port conflict between <function> <port> and <function> <port> | Review the port configuration on the Local inbound ports and Local outbound ports 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 | Network Log and Support Log 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 NTP status information, including any key configuration and expiry dates | Warning |
| 25021 | NTP server not available | The system is unable to contact an NTP server | Check Time configuration and status; check DNS configuration | Warning |

Reference Material

Table 33 Network Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|---|--|--|----------|
| 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 |
| 25023 | XMPP Federation configuration warning | Failed to configure Unified CM IM and Presence Service servers with Expressway address for XMPP federation | Check that the IM and Presence Service servers are running, and that the AXL service is running on them, then refresh the servers. | Warning |
| 25024 | XMPP configuration error | Invalid configuration of XMPP network address | Check that the IPv4 addresses are correct. You may not use 127.0.0.1 (loopback address) | Error |
| 25025 | Smart Call Home connection failed | Expressway could not send information to Smart Call Home. This could be a transient network condition, a misconfiguration, or a certificate mismatch | Check the Smart Call Home and DNS configuration | Critical |
| 25026 | Restart required | Web administration port has been changed, however, a restart is required for this to take effect | Restart the system | Warning |

Table 34 License Alarms

| ID | Title | Description | Solution | Severity |
|-------|------------------|---|------------------------------------|----------|
| 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 | Restart the system | Warning |
| 30007 | Capacity warning | TURN relays usage has approached the licensed limit | Contact your Cisco representative | Warning |

Table 34 License Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--|---|--|----------|
| 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 option keys | Warning |
| 30009 | TURN relays installed | TURN services are only available on Expressway-E; TURN option key ignored | Add/Remove option keys | Warning |
| 30011 | TURN relay licenses required | TURN services are enabled but no TURN relay license option keys are installed | Add option key or disable TURN services | Warning |
| 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 |

Reference Material

Table 34 License Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--|--|---|----------|
| 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 |
| 30025 | Restart required | An option key has been changed, however a restart is required for this to take effect | Restart the system | Warning |
| 30026 | Approaching room system license limit | The number of concurrent registered TelePresence room systems is approaching the license limit | Contact your Cisco representative if you require more licenses | Warning |
| 30027 | Capacity warning | The number of concurrent registered TelePresence room systems and registered desktop systems has reached the physical limit in one or more peer(s) | Ensure that your registrations are distributed evenly across all peers. Add more capacity to your system; contact your Cisco representative | Warning |
| 30028 | Room system registrations limit reached | The number of registered TelePresence room systems has reached the license limit | Contact your Cisco representative to buy more room system licenses | Warning |
| 30029 | Approaching desktop system license limit | The number of concurrent registered desktop systems is approaching the license limit | Contact your Cisco representative if you require more licenses | Warning |
| 30030 | Capacity warning | The number of registered TelePresence room systems and registered desktop systems has reached the unit's physical limit | Add more capacity to your system; contact your Cisco representative | Warning |
| 30031 | Desktop system license limit reached | The number of registered desktop systems has reached the license limit | Contact your Cisco representative to buy more desktop system licenses | Warning |

Table 35 External Applications / Services Alarms

| ID | Title | Description | Solution | Severity |
|-------|---|---|--|----------|
| 35001 | Configuration warning | Active Directory mode has been enabled but the DNS hostname has not been configured | Configure DNS hostname | Warning |
| 35002 | Configuration warning | Active Directory mode has been enabled but the NTP server has not been configured | Configure NTP server | Warning |
| 35003 | Configuration warning | Active Directory mode has been enabled but no DNS servers have been configured | Configure a DNS server | 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 LDAP parameters | 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 |

Table 35 External Applications / Services Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--|---|--|----------|
| 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 |
| 35013 | Unified Communications SSH tunnel failure | This system cannot communicate with one or more remote hosts: <Host 1, Host 2, ...> Note that the list of hosts is truncated to 200 characters. | 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 |

Table 36 Security Alarms

| ID | Title | Description | Solution | Severity |
|-------|--------------------------|--|---|----------|
| 40001 | Security alert | No CRL distribution points have been defined for automatic updates | Check CRL configuration | 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 changing the root password | Warning |

Table 36 Security Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--|--|---|----------|
| 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 client certificate-based security | Warning |
| 40005 | Insecure password in use | The admin user has the default password set | Change the admin password | Error |
| 40006 | Security alert | Unable to download CRL update | Check CRL distribution points and the Event Log | 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 replacing the default SSH key | Warning |
| 40009 | Restart required | HTTPS client certificates validation mode has changed, however a restart is required for this to take effect | Restart the system | Warning |
| 40011 | Per-account session limit required | A non-zero per-account session limit is required when in advanced account security mode | Configure per-account session limit | Warning |
| 40012 | External manager connection is using HTTP | You are recommended to use HTTPS connections to the external manager when in advanced account security mode | Configure external manager | 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 HTTPS client certificate validation | Warning |
| 40014 | Time out period required | A non-zero system session time out period is required when in advanced account security mode | Configure session time out period | Warning |
| 40015 | System session limit required | A non-zero system session limit is required when in advanced account security mode | Configure system session limit | Warning |

Reference Material

Table 36 Security Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--|---|--|----------|
| 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 login account LDAP server | Warning |
| 40017 | Incident reporting enabled | You are recommended to disable incident reporting when in advanced account security mode | Configure incident reporting | Warning |
| 40018 | Insecure password in use | One or more users has a non-strict password | | Warning |
| 40019 | External manager has certificate checking disabled | You are recommended to enable external manager certificate checking when in advanced account security mode | Configure external manager | 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 remote logging | 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 login account LDAP server | Warning |
| 40025 | SNMP enabled | You are recommended to disable SNMP when in advanced account security mode | Configure SNMP mode | Warning |

Table 36 Security Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|---------------------------------------|--|---|----------|
| 40026 | Reboot required | The advanced account security mode has changed, however a reboot is required for this to take effect | Reboot the Expressway | 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 changing the root password | Warning |
| 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 firewall rules configuration , fix any rejected rules and re-try the activation | Warning |
| 40031 | Security alert | Unable to restore previous firewall configuration | Check your firewall rules configuration , 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 | Restart the system ; 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 SIP page to enforce certificate identity checking using TLS, or disable the access rules for the Default Zone . | Warning |
| 40034 | Security alert | Firewall rules activation failed; the firewall configuration contains rules with duplicated priorities | Check your firewall rules configuration , ensure all rules have a unique priority and re-try the activation | Warning |

Reference Material

Table 36 Security Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--|---|--|----------|
| 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 |
| 40042 | FIPS140-2 compliance restriction | Some SIP configuration is not using TLS transport; FIPS140-2 compliance requires TLS | Ensure that TLS is the only enabled system-wide SIP transport mode on the SIP page, and that all zones are using TLS. Alternatively, if you are transitioning into FIPS140-2 you may want to restore a FIPS-compliant backup of your data. | 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 |
| 40044 | System reset required | FIPS140-2 mode has been enabled; a system reset is required to complete this process | Ensure that all alarms are cleared, then take a system backup before performing a system reset | Warning |
| 40045 | Restart required | FIPS140-2 mode has been disabled; a system restart is required to complete this process | Restart the system | Warning |
| 40046 | FIPS140-2 compliance restriction | Clustered systems are not FIPS140-2 compliant | Disband the cluster | 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 |
| 40049 | Cluster TLS permissive | Cluster TLS verification mode permits invalid certificates | Change the cluster's TLS verification mode to Enforcing | Notice |
| 40050 | Security alert | Unable to install new firewall configuration | Check your firewall configuration and rate limits configuration, fix any rejected rules; Do not restart your system; if the problem persists, contact your Cisco representative | |

Table 36 Security Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--|---|--|----------|
| 40051 | CMS not Identified by Server Certificate | CMS address <i><address></i> has been entered on the Expressway-C but is not identified by the Expressway-E server certificate. | Check that the CMS address on the Expressway-C matches the SAN entry on the Expressway-E server. You may need to generate a CSR for a new server certificate that includes the CMS as a SAN, or edit (or remove) the CMS on the Expressway-C | |
| 40052 | Certificate error | Server certificate does not have a Common Name (CN) attribute. Some services do not work without the CN | Update certificate | |
| 40053 | Invalid Cipher config | The following entries have cipher values that are invalid in FIPS140-2 mode: <i><List></i> | Please reconfigure the affected cipher entries at ciphers | |
| 40054 | Token decryption failure | The Expressway-C failed to decrypt or decode an OAuth token issued by Unified CM. This could be caused by changes to the issuer. | Refresh the Cisco Unified Communications Manager configuration. | Warning |
| 40100 | Security alert | Firewall rules are not synchronized with network interfaces | Restart the system ; if the problem persists, contact your Cisco representative | Warning |

Table 37 Misconfiguration Alarms

| ID | Title | Description | Solution | Severity |
|-------|---------------------------------|--|--|----------|
| 45001 | Failed to load Call Policy file | <i><failure details></i> | Configure Call Policy | Warning |
| 45002 | Configuration warning | Expected default link between the Default Subzone and the Default Zone is missing | Configure default links | Warning |
| 45003 | Configuration warning | H.323 and SIP modes are set to Off; one or both of them should be enabled | Configure H.323 and/or SIP modes | Warning |
| 45006 | Configuration warning | Expected default link between the Default Subzone and the Cluster Subzone is missing | Configure default links | Warning |
| 45007 | Configuration warning | Expected default link between the Default Subzone and the Traversal Subzone is missing | Configure default links | Warning |

Table 37 Misconfiguration Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--------------------------|--|--|----------|
| 45008 | Configuration warning | Expected default link between the Traversal Subzone and the Default Zone is missing | Configure default links | 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 |

Table 38 Back to Back User Agent Alarms

| ID | Title | Description | Solution | Severity |
|-------|--------------------------------|--|---|----------|
| 55001 | B2BUA service restart required | Some B2BUA service specific configuration has changed, however a restart is required for this to take effect | Restart the B2BUA service | Warning |
| 55002 | B2BUA misconfiguration | The port on B2BUA for Expressway communications is misconfigured | Check B2BUA configuration (advanced settings) | Warning |
| 55003 | B2BUA misconfiguration | Invalid trusted host IP address of Microsoft device | Check configured addresses of trusted hosts | Warning |
| 55004 | B2BUA misconfiguration | The port on B2BUA for Microsoft call communications is misconfigured | Check B2BUA configuration (advanced settings) | Warning |
| 55005 | B2BUA misconfiguration | The Microsoft destination address is misconfigured | Check B2BUA configuration | Warning |
| 55005 | B2BUA misconfiguration | The Microsoft destination address is misconfigured | Check B2BUA configuration | Warning |
| 55006 | B2BUA misconfiguration | The Microsoft destination port is misconfigured | Check B2BUA configuration | Warning |
| 55007 | B2BUA misconfiguration | The Microsoft transport type is misconfigured | Check B2BUA configuration | Warning |

Table 38 Back to Back User Agent Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|------------------------|--|---|----------|
| 55008 | B2BUA misconfiguration | Missing or invalid FQDN of service | Check the Expressway's system host name and domain name | Warning |
| 55009 | B2BUA misconfiguration | Invalid IP address of service | Check the Expressway's LAN 1 IPv4 address | Warning |
| 55010 | B2BUA misconfiguration | The B2BUA media port range end value is misconfigured | Check B2BUA configuration (advanced settings) | Warning |
| 55011 | B2BUA misconfiguration | The B2BUA media port range start value is misconfigured | Check B2BUA configuration (advanced settings) | Warning |
| 55012 | B2BUA misconfiguration | Invalid Microsoft interoperability mode | Check B2BUA configuration | Warning |
| 55013 | B2BUA misconfiguration | Invalid option key | Check option keys | Warning |
| 55014 | B2BUA misconfiguration | Invalid hop count | Check B2BUA configuration (advanced settings) | Warning |
| 55015 | B2BUA misconfiguration | Invalid trusted host IP address of transcoder | Check configured addresses of trusted hosts | Warning |
| 55016 | B2BUA misconfiguration | The setting to enable transcoders for this B2BUA is misconfigured | Check B2BUA configuration (transcoder settings) | Warning |
| 55017 | B2BUA misconfiguration | The port on B2BUA for transcoder communications is misconfigured | Check B2BUA configuration (transcoder settings) | Warning |
| 55018 | B2BUA misconfiguration | Transcoder address and/or port details are misconfigured | Check B2BUA configuration (transcoder settings) and the configured addresses of trusted hosts | Warning |
| 55019 | B2BUA misconfiguration | Invalid TURN server address | Check B2BUA configuration (TURN settings) | Warning |
| 55021 | B2BUA misconfiguration | The setting to offer TURN services for this B2BUA is misconfigured | Check B2BUA configuration (TURN settings) | Warning |
| 55023 | B2BUA misconfiguration | The transcoder policy rules are misconfigured | Check transcoder policy rules configuration | Warning |
| 55024 | B2BUA misconfiguration | The setting to use transcoder policy rules is misconfigured | Check B2BUA configuration (transcoder settings) | Warning |
| 55025 | B2BUA misconfiguration | The B2BUA has been enabled to use transcoders, but there are no transcoders configured | Configure one or more transcoders | Warning |
| 55026 | B2BUA misconfiguration | TURN services are enabled, but there are no valid TURN servers configured | Configure the TURN server address | Warning |

Table 38 Back to Back User Agent Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|----------------------------|---|---|----------|
| 55028 | B2BUA misconfiguration | The start and end media port ranges are misconfigured | Check the B2BUA media port range 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 |
| 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 Microsoft call 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 Microsoft trusted hosts have been configured | Configure at least one trusted host device | Warning |
| 55034 | B2BUA misconfiguration | No valid transcoder trusted hosts have been configured | Configure at least one transcoder trusted host | Warning |
| 55035 | B2BUA connectivity problem | The B2BUA cannot connect to the transcoders | Restart the B2BUA service | Warning |
| 55036 | B2BUA connectivity problem | The B2BUA cannot connect to the Expressway | Restart the B2BUA service | Warning |
| 55037 | B2BUA connectivity problem | The B2BUA cannot connect to the Microsoft environment | Check the Microsoft interoperability status page for more information about the problem; you will then need to restart the B2BUA service after making any configuration changes | Warning |
| 55101 | B2BUA misconfiguration | Invalid Expressway authorized host IP address | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55102 | B2BUA misconfiguration | Invalid URI format of Expressway contact address | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55103 | B2BUA misconfiguration | Invalid Expressway encryption mode | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55104 | B2BUA misconfiguration | Invalid Expressway ICE mode | Restart the service ; contact your Cisco representative if the problem persists | Warning |

Table 38 Back to Back User Agent Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|------------------------|---|---|----------|
| 55105 | B2BUA misconfiguration | Invalid Expressway next hop host configuration | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55106 | B2BUA misconfiguration | Invalid Expressway next hop liveness mode | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55107 | B2BUA misconfiguration | Invalid Expressway next hop mode | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55108 | B2BUA misconfiguration | Invalid Expressway next hop port | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55109 | B2BUA misconfiguration | Invalid Expressway transport type | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55110 | B2BUA misconfiguration | Invalid URI format of B side contact address | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55111 | B2BUA misconfiguration | Invalid B side encryption mode | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55112 | B2BUA misconfiguration | Invalid B side ICE mode | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55113 | B2BUA misconfiguration | Invalid B side next hop liveness mode | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55114 | B2BUA misconfiguration | Invalid B side next hop mode | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55115 | B2BUA misconfiguration | Invalid command listening port | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55116 | B2BUA misconfiguration | Invalid debug status path | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55117 | B2BUA misconfiguration | Invalid service | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55118 | B2BUA misconfiguration | Invalid software string | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55119 | B2BUA misconfiguration | Invalid URI format of transcoding service contact address | Restart the service ; contact your Cisco representative if the problem persists | Warning |

Reference Material

Table 38 Back to Back User Agent Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|------------------------|---|--|----------|
| 55120 | B2BUA misconfiguration | Invalid transcoding service encryption mode | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55121 | B2BUA misconfiguration | Invalid transcoding service ICE mode | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55122 | B2BUA misconfiguration | Invalid transcoding service next hop liveness mode | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55123 | B2BUA misconfiguration | The transcoding service transport type is misconfigured | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55124 | B2BUA misconfiguration | The mandatory TURN server setting is misconfigured | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55125 | B2BUA misconfiguration | Invalid Expressway next hop host configuration | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55126 | B2BUA misconfiguration | Invalid Expressway authorized host IP address | Restart the service ; contact your Cisco representative if the problem persists | Warning |
| 55127 | B2BUA misconfiguration | Cannot start B2BUA application because FQDN configuration is missing | Configure the System host name and Domain name on the DNS page, and then restart the B2BUA service | Warning |
| 55128 | B2BUA misconfiguration | Cannot start B2BUA application because IPv4 interface address configuration is missing | Configure the LAN 1 IPv4 address on the IP page, and then restart the B2BUA service | Warning |
| 55129 | B2BUA misconfiguration | Cannot start B2BUA application because cluster name configuration is missing | Configure the cluster name on the Clustering page | Warning |
| 55130 | B2BUA misconfiguration | Invalid cluster name | Check the cluster name and then restart the B2BUA service | Warning |
| 55131 | B2BUA misconfiguration | Invalid session refresh interval | Check B2BUA configuration (advanced settings), then restart the B2BUA service | Warning |
| 55132 | B2BUA misconfiguration | Invalid call resource limit | Restart the service ; 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 B2BUA configuration (advanced settings) and then restart the B2BUA service | Warning |

Table 38 Back to Back User Agent Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--------------------------------|--|---|----------|
| 55134 | B2BUA misconfiguration | Invalid minimum session refresh interval | Check B2BUA configuration (advanced settings), then restart the B2BUA service | Warning |
| 55135 | B2BUA configuration warning | A large number of Microsoft trusted host devices have been configured; this may impact performance, or 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 B2BUA trusted hosts page. | Warning |
| 55137 | B2BUA misconfiguration | Invalid VCS multistream mode | Check B2BUA configuration (advanced settings), then restart the B2BUA service | Warning |
| 55139 | B2BUA misconfiguration | Invalid VCS multistream mode | Check B2BUA configuration (advanced settings), then restart the B2BUA service | Warning |
| 55142 | Insufficient RDP TCP/UDP ports | There is an insufficient number of TCP/UDP ports to support the maximum number of RDP calls | Increase the RDP TCP/UDP port ranges on the B2BUA configuration | Warning |

Table 39 Management Connector Alarms

| ID | Title | Description | Solution | Severity |
|-------|---|--|--|----------|
| 60050 | [Hybrid services] Connectivity error | Could not reach Cisco Collaboration Cloud address: <i><string></i> | Check <i><string></i> , or <i><string></i> , or use network utilities <i><string></i> , to verify this address. | error |
| 60051 | [Hybrid services] Communication error | HTTP error code <i><string></i> from Cisco Collaboration Cloud (address: <i><string></i>) | Check Hybrid Services status. Contact your Cisco Collaboration Cloud administrator if the issue persists. | error |
| 60052 | [Hybrid services] Communication error | <i><string></i> | Verify your <i><string></i> , <i><string></i> , <i><string></i> the address. Contact your Cisco Collaboration Cloud administrator if you have ruled these out. | error |
| 60053 | [Hybrid services] Access error | <i><string></i> | Contact your Cisco Collaboration Cloud administrator. | error |
| 60054 | [Hybrid services] Connector install error | <i><string></i> | Contact your Cisco Collaboration Cloud administrator. | error |
| 60055 | [Hybrid services] Download failed because the certificate was not valid | <i><string></i> | Check the Expressway's trusted CA list for the CA that signed the received certificate. | error |

Reference Material

Table 39 Management Connector Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|---|--|--|----------|
| 60056 | [Hybrid services] Upgrade failed because certificate was not valid | <string> | Check the Expressway's trusted CA list for the CA that signed the received certificate. | error |
| 60057 | [Hybrid services] Upgrade failed because certificate name did not match | <string> | Check that the CN or a SAN on the certificate from <string> matches its hostname. | error |
| 60058 | [Hybrid services] Connection failed because the CA certificate was not found | Cannot securely connect to the Cisco Collaboration Cloud because the root CA that signed the certificate from <string> is not in the Expressway's trusted CA list. | Update the Expressway's trusted CA list to include the CA that signed the received certificate. | error |
| 60059 | [Hybrid services] Connection failed because the certificate name did not match | The certificate from <string> did not have a CN or SAN attribute that matches its hostname. | Check that the CN or a SAN on the certificate from the remote server matches its hostname. | error |
| 60060 | [Hybrid services] Connection failed because the certificate was not validated | The Expressway could not validate the certificate from <string>. This can happen because the Expressway does not trust the CA, or because the certificate is not currently valid. | Check that the Expressway <string> list contains the root certificate of the CA that signed the received certificate. Check that the CA certificate is current and was not revoked. Check that the <string> is configured and that the Expressway is synchronized. If you can rule out these potential causes, contact Cisco; the server certificate we sent you might be invalid. | error |
| 60061 | [Hybrid services] Upgrade prevented by user choice | You previously rejected connector upgrades currently advertised by Cisco Collaboration Cloud. Automatic upgrades will continue when the next versions are available. The advertised versions are: <string> | View connector versions | alert |
| 60062 | [Hybrid services] Connector disable error | <string> | Contact your Cisco Collaboration Cloud administrator. | error |

Table 39 Management Connector Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|---|--|--|----------|
| 60063 | [Hybrid services] Connector enable error | <string> | Contact your Cisco Collaboration Cloud administrator | error |
| 60064 | [Hybrid services] Connector unexpectedly not running | <string> | Restart the stopped connector. If that connector upgraded itself recently, roll it back to the previous version. If the error persists, contact your Cisco Collaboration Cloud administrator. | error |
| 60065 | [Hybrid services] Connector version mismatch | <string> | Contact your Cisco Collaboration Cloud administrator. | error |
| 60066 | [Hybrid services] Routine authentication refresh failed | The Expressway periodically renews its authentication through <string>, but did not succeed this time. The Expressway will retry in <string> minutes. | If this issue persists, contact your Cisco Collaboration Cloud administrator. | error |
| 60067 | [Hybrid services] Connectivity Error | Error when trying to access <string>. The Expressway will try again in approximately <string> seconds. | Check <string>, and check for network issues if the error persists. | error |
| 60068 | [Hybrid services] Invalid responses from Cisco Collaboration Cloud | Invalid data was received from <string>. | Check that you have the expected address for Cisco Collaboration Cloud. | error |
| 60069 | [Hybrid services] No service connectors | You registered for Hybrid Services but there are no service connectors installed. The Management Connector is active and is making unnecessary connections to the Cisco Collaboration Cloud. | Go to Cisco Cloud Collaboration Management and check that your organization is entitled to use one or more Hybrid Services. If you are not using any Hybrid Services, we strongly recommend that you <string> this Expressway. | alert |
| 60070 | [Hybrid services] HTTP exception | Received exception: <string>, while processing HTTP response from <string> | If the issue persists, contact your Cisco Collaboration Cloud administrator. | error |

Table 39 Management Connector Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|---|---|--|----------|
| 60071 | [Hybrid services] Key error | This system could not register properly because of a data error in a connector file. The associated services will not work as expected, even if you appear to have registered successfully. | Try to register again (you may need to deregister first). If the issue persists, contact your Cisco Collaboration Cloud administrator. | error |
| 60072 | [Hybrid services] Unsupported Expressway version | Your version of Expressway is no longer supported for Hybrid Services. To continue using Hybrid Services, you must upgrade to a newer version. | Please upgrade to the latest Expressway version, available on cisco.com. | alert |

Table 40 Calendar Connector Alarms

| ID | Title | Description | Solution | Severity |
|-------|---|---|--|----------|
| 60100 | Microsoft Exchange Server unreachable | An error occurred accessing the Microsoft Exchange Server. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <i><string></i> . The last known error is: <i><string></i> | Check network connectivity between Microsoft Exchange Server and Calendar Connector. Check the load on Microsoft Exchange Server | critical |
| 60101 | Microsoft Exchange Server access denied | Access to the Microsoft Exchange Server was denied. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <i><string></i> . The last known error is: <i><string></i> | Verify that the service account has valid credentials and correct permissions, and is not locked out | critical |
| 60102 | Microsoft Exchange Server certificate not validated | The certificate for the Microsoft Exchange Server could not be validated. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <i><string></i> . The last known error is: <i><string></i> | Verify the Microsoft Exchange Server certificate is valid | critical |
| 60103 | Microsoft Exchange Server version unsupported | The version of the configured Microsoft Exchange Server is not supported. Detailed info: <i><string></i> | Microsoft Exchange Server must be upgraded to supported version | critical |

Table 40 Calendar Connector Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|---|--|--|----------|
| 60104 | No Microsoft Exchange Server configured | The Calendar Connector stopped because no Microsoft Exchange Server settings are configured | Configure at least one Microsoft Exchange Server in the Calendar Connector and re-enable it | critical |
| 60110 | Microsoft Exchange Autodiscover unreachable | A timeout occurred accessing the Microsoft Exchange Server during user autodiscover. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <i><string></i> . The last known error is: <i><string></i> | Check network connectivity between Microsoft Exchange Autodiscover Server and Calendar Connector | critical |
| 60111 | Microsoft Exchange Autodiscover access denied | Access to the Microsoft Exchange Server during user autodiscover was denied. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <i><string></i> . The last known error is: <i><string></i> | Verify that the service account has valid credentials and correct permissions, and is not locked out | critical |
| 60112 | Microsoft Exchange Autodiscover certificate not validated | During autodiscover, the certificate for the the Microsoft Exchange Server could not be validated. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <i><string></i> . The last known error is: <i><string></i> | Verify the server certificate is valid | critical |
| 60113 | Redirected Microsoft Exchange Autodiscovery URL not trusted | The redirected Microsoft Exchange Autodiscovery URL is changed and not trusted. Detailed info: <i><string></i> | Open the Exchange Service Record and save the record again. Confirm the new redirection URL is to be trusted | critical |
| 60120 | Microsoft Exchange Autodiscover LDAP unreachable | A timeout occurred during autodiscover, accessing the Microsoft LDAP server. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <i><string></i> . The last known error is: <i><string></i> | Check network connectivity between Microsoft Exchange Autodiscover LDAP Server and Calendar Connector | critical |
| 60121 | Microsoft Exchange Autodiscover LDAP access denied | Access to the Microsoft LDAP Server during autodiscover was denied. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <i><string></i> . The last known error is: <i><string></i> | Verify that the service account has valid credentials and correct permissions, and is not locked out | critical |

Table 40 Calendar Connector Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|---|---|--|----------|
| 60130 | Microsoft Exchange Server user subscription failure | <string> users failed to subscribe to Microsoft Exchange Server(s). Detailed info: the users include <string> | Verify the Microsoft Exchange Server is not busy and the network connectivity between Microsoft Exchange Server and Calendar Connector | error |
| 60131 | SMTP address has no mailbox | Multiple (<string>) SMTP address(es) have been detected with no associated mailbox(es). Detailed info: <string> | Verify the target mailbox is fully enabled and the target server is correct | error |
| 60132 | Subscription not operational | The Calendar Service has not received notifications from the Microsoft Exchange Server for one or more users. Calendar Service requests and notifications for these users will not be processed until this is addressed | Verify that the Microsoft Exchange Server(s) are functioning correctly, and that you have network connectivity. If the condition continues, consider restarting the Calendar Service | error |
| 60140 | Meeting notification incoming rate too high | The incoming meeting notification rate is too high for <string> Calendar Service user(s). Detailed info: the users include <string> | Check Microsoft Exchange Server for the mailbox(es) of the user(s) | error |
| 60142 | Meeting processing time too long | Calendar Service meeting processing time exceeds a threshold of 5 minutes for at least one user | Check Microsoft Exchange Server and Calendar Service for user notification rate | error |
| 60150 | Cisco Collaboration Cloud Monitor Service unreachable | A required cloud service currently cannot be reached. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: <string> | Verify connectivity to Internet | critical |
| 60151 | Cisco Collaboration Cloud Monitor Service access denied | Access to Cisco Collaboration Cloud services was denied. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: <string> | Contact tech support | critical |
| 60152 | Cisco Collaboration Cloud API Service unreachable | A required cloud service currently cannot be reached. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: <string> | Verify connectivity to Internet | critical |
| 60153 | Cisco Collaboration Cloud API Service access denied | Access to Cisco Collaboration Cloud services was denied. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: <string> | Contact tech support | critical |

Table 40 Calendar Connector Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--|---|--|----------|
| 60154 | Retrieving key from encryption service failed | Calendar Connector failed to retrieve an existing key or request to generate a new key from an encryption service. Detailed info: the encryption service is <i><string></i> | Verify the encryption service is on | error |
| 60155 | Cisco Collaboration Cloud Monitor message service not connected | Calendar Connector failed to connect to Cisco Collaboration Cloud Monitor message service. Detailed info: the cloud service route is <i><string></i> | Verify network connectivity to Cisco Collaboration Cloud Monitor message service | critical |
| 60156 | Cisco Collaboration Cloud API message service not connected | Calendar Connector failed to connect to Cisco Collaboration Cloud API message service. Detailed info: the cloud service route is <i><string></i> | Verify network connectivity to Cisco Collaboration Cloud API message service | critical |
| 60160 | Cisco Collaboration Meeting Rooms (CMR) service unreachable or access denied | Cisco Collaboration Meeting Rooms (CMR) service currently cannot be reached or access was denied. @webex meetings will not be processed until this is resolved. Detailed info: the CMR service site name includes <i><string></i> | Verify network connectivity and configured account credentials to CMR service | error |
| 60161 | WebEx user account not available | <i><string></i> WebEx user account(s) are not available. @webex meetings for these users will not be processed until their account problems are resolved. Detailed info: the affected users include <i><string></i> | Verify WebEx service account and user accounts. Make sure the user has a WebEx account, and the account is not locked out, deactivated or Personal Room disabled | warning |
| 60162 | Cisco WebEx administrator password has expired or invalid | Cisco WebEx service cannot be accessed due to expired or invalid administrator password. @webex meetings on affected site will not be processed until this is resolved. Detailed info: the WebEx service site name includes <i><string></i> | Change the expired or invalid administrator password on affected WebEx server | error |
| 60163 | Cisco WebEx administrator password expiring | Cisco WebEx administrator password for <i><string></i> site(s) will expire soon. Detailed info: the WebEx service site with expiring administrator password includes <i><string></i> | Change the expiring administrator password on affected WebEx server | warning |

Reference Material

Table 40 Calendar Connector Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--|--|--|----------|
| 60164 | Cisco WebEx administrator account locked out | Cisco WebEx service cannot be accessed due to locked out administrator account. @webex meetings on affected site will not be processed until this is resolved. Detailed info: the WebEx service site name includes <i><string></i> | Unlock the administrator account on affected WebEx server | error |
| 60170 | Management Connector not running | Calendar Connector is not operational because Management Connector is not running | Go to Applications > Cloud Extensions > Connector Management to start the Management Connector | error |
| 60171 | Management Connector not operational | Calendar Connector is not operational because Management Connector is not operational | Check the status of the Management Connector and restart it if necessary | error |
| 60190 | Calendar Connector not operational | Calendar Connector is not operational since one or more cloud and/or on-premises services are not operational | Check the Calendar Connector status for details | critical |

Table 41 Call Connector Alarms

| ID | Title | Description | Solution | Severity |
|-------|--|---|---|----------|
| 60300 | The user is not configured with any directory numbers. | The user is not configured with any directory numbers - user[<i><string></i>]: <i><string></i> | Add at least one line on a device associated with the user in Unified CM | warning |
| 60301 | The user has no valid devices in the control list. | The user has no valid devices in the control list - user[<i><string></i>]: <i><string></i> | Associate at least one valid device with at least one line with the user in Unified CM | warning |
| 60302 | The user is not configured with a directory URI. | The user is not configured with a directory URI - user [<i><string></i>]: <i><string></i> | Enter a directory URI value under the user's account settings in Unified CM | warning |
| 60303 | Could not find a user with this email address. | Could not find a user with this email address - user [<i><string></i>]: <i><string></i> | Enter an email address for the user in Unified CM | warning |
| 60304 | Email mismatch with directory URI | The user's email does not match the directory URI - user[<i><string></i>]: <i><string></i> | Verify that the user's email and directory URI are identical in Unified CM | warning |
| 60305 | The user's primary directory URI does not match the directory URI configured for the primary line. | The user's primary directory URI does not match the directory URI configured for the primary line - user [<i><string></i>]: <i><string></i> | Verify that the user's directory URI and line URI on an associated device are identical in Unified CM | warning |

Table 41 Call Connector Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--|--|--|----------|
| 60306 | The user is not configured with a valid CTI remote device. | The user is not configured with a valid CTI remote device - user[<string>]: <string> | Configure a CTI remote device and add to the user's control list in Unified CM. | warning |
| 60307 | The user's Spark SIP address cannot be routed to Cisco Spark. | The user's Spark SIP address cannot be routed to Cisco Spark - user[<string>]: <string> | Check the rerouting calling search space on Unified CM and the partition configured for the Spark SIP address pattern. | warning |
| 60308 | The user's Spark SIP address is assigned to another user. | The User's Spark SIP address is assigned to another user - user [<string>]: <string> | Check the user's Unified CM configuration. | warning |
| 60309 | The user's remote destination was not removed. | When the user is deactivated for Call Service Connect, the remote destination was not removed. - user[<string>]: <string> | Remove the Cisco Spark remote destination from the user's CTI remote device in Unified CM. | warning |
| 60310 | Unable to add the user's Spark SIP address in Unified CM. | Unable to add the user's Spark SIP address in Unified CM - user[<string>]: <string> | Call connector will retry. | warning |
| 60311 | The user is not configured with a primary directory number. | The user is not configured with a primary directory number - user[<string>]: <string> | Configure a primary directory number for the user in Unified CM. | warning |
| 60315 | Automatic Spark Remote Device created with truncated name | The Automatic Spark Remote Device name was shortened during Call Service Connect activation. - user[<string>]: <string> has device with name <string> | To avoid this issue, user IDs must not exceed 15 characters. | warning |
| 60316 | Unable to delete Spark Remote Device | Call connector cannot delete the Spark remote device after Call Service Connect was deactivated - user[<string>]: <string> | Check error messages in Unified CM. | warning |
| 60317 | Call connector is unable to create a CTI Remote Device in Unified CM. | Call connector is unable to create a CTI Remote Device in Unified CM - user [<string>]: <string> | Check for any potentially conflicting device names | warning |
| 60318 | Users must have mobility enabled for call connector to create a CTI remote device. | Users must have mobility enabled for call connector to create a Spark Remote Device - user[<string>]: <string> | Check whether the Unified CM user is enabled for mobility. | warning |

Table 41 Call Connector Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--|---|--|----------|
| 60319 | Connectivity to Unified CM AXL Service lost | Connectivity to Unified CM AXL Service lost - for Unified CM [<i><string></i>] | Check whether the AXL service is running on Unified CM and resolve any network issues. | error |
| 60320 | Cannot connect to Unified CM CTIManager Service. | Cannot connect to Unified CM CTIManager Service - for Unified CM [<i><string></i>] | Check whether the CTIManager service is running on Unified CM and resolve any networking issues. | error |
| 60321 | Certificate verification failed | Call Connector stopped and could not verify the certificate from Cisco Spark. | Download the certificate and reregister the Expressway, or update the Cisco Spark certificate in the Expressway trust store. | error |
| 60322 | Fully Qualified Domain Name is not valid | Fully Qualified Domain Name is Empty - user [<i><string></i>]: <i><string></i> | Add a fully qualified domain name in the Unified CM enterprise parameter. See the documentation for guidance. | warning |
| 60323 | Fully Qualified Domain Name is not valid | Fully Qualified Domain Name contains wild card - user [<i><string></i>]: <i><string></i> | Add a new fully qualified domain name without wildcards in the Unified CM enterprise parameter. | warning |
| 60324 | Unable to reach the Unified CM AXL server. | Unable to reach the Unified CM AXL server - server [<i><string></i>] | Check network connectivity between call connector and Unified CM. | error |
| 60325 | Unable to authenticate with Unified CM AXL server | Unable to authenticate with Unified CM AXL server - [<i><string></i>] | Check the Unified CM user credentials that you provided during call connector configuration. | error |
| 60326 | User configured for Unified CM AXL communication is not authorized | User configured for Unified CM AXL communication is not authorized - server [<i><string></i>] | Check the access roles for the user configured in UCM Configuration on the Call Connector. | error |
| 60327 | No Unified CM Configured | No Unified CM is configured for call connector. | Configure a Unified CM for Call Connector. | warning |
| 60328 | The user is configured for more than one Unified CM cluster. | The user is configured for more than one Unified CM cluster - user [<i><string></i>]: <i><string></i> | Check the user's home cluster setting on all Unified CMs configured on this call connector. | warning |
| 60329 | Call connector received an invalid Spark SIP Address. | Invalid Spark SIP Address - for user [<i><string></i>]: <i><string></i> | Check the user and device configuration. Follow the documentation to reconfigure these, if needed, to produce a valid Spark SIP address. | warning |
| 60330 | The user is configured with more than one CTI remote device. | The user is configured with more than one CTI remote device - user [<i><string></i>]: <i><string></i> | Remove extra devices from the user's control list in Unified CM. | warning |

Table 41 Call Connector Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|---|---|---|----------|
| 60331 | The CTI remote device has no configured directory numbers. | The CTI remote device has no configured directory numbers - user[<string>]: <string> | In Unified CM, add at least one line to the CTI remote device associated with the user. | warning |
| 60332 | In Unified CM CTIManager, a request timed out to update the remote destination. | In Unified CM CTIManager, a request timed out to update the remote destination - user[<string>]: <string> | Verify that the Unified CM CTIManager service is up and running. | warning |
| 60333 | Unable to connect to Unified CM CTIManager | Unable to connect to Unified CM CTIManager | Check network connectivity between Call connector and Unified CM. | error |
| 60334 | Unable to authenticate user configured for Unified CM CTIManager | Unable to authenticate user configured for Unified CM CTIManager | Check the user credentials in Unified CM configuration on the call connector. | error |
| 60335 | Conflict in Device Ownership on Unified CM. | Unified CM shows a conflict with the owner of the device - for user[<string>]: <string> | Check the configuration in Unified CM. | warning |
| 60336 | A device exists with the same name as the CTI remote device tried to create for the user. | A device exists with the same name as the CTI remote device tried to create - for user[<string>]: <string> | Check the device names and configuration in Unified CM. | warning |
| 60337 | CTI remote device successfully created for the user, but the device subscription to receive call events failed. | CTI remote device successfully created for the user, but the device subscription to receive call events failed - for user [<string>]: <string> | Check the configuration in Unified CM and retry. | warning |
| 60338 | Invalid remote destination on Unified CM. | Invalid remote destination on Unified CM - for user [<string>]: <string> | Follow the user and remote device configuration in the documentation to create a valid Spark SIP address. | warning |
| 60339 | The user exceeds the remote destination limit at Unified CM. | Unable to create a Spark SIP address; the user exceeds the remote destination limit in Unified CM - for user [<string>]: <string> | Remove any unused remote destination or increase the limit. | warning |
| 60340 | The user is not configured with a home cluster. | The user is not configured with a home cluster - user [<string>]: <string> | Configure a home cluster for this user on Unified CM. | warning |
| 60341 | Call connector invalid configuration | Invalid Configuration reason=[<string>] | Fix the configuration error and then restart the call connector. | error |

Reference Material

Table 41 Call Connector Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|--|--|--|----------|
| 60342 | Call connector version mismatch with Cisco Spark | Invalid message received in state [<i><string></i>], potential version mismatch with Cisco Spark | Upgrade to the latest call connector. | error |
| 60343 | Spark SIP Address exceeds the 48 character limit. | Unable to add spark SIP address for a user. Unified CM does not support remote destinations that are longer than 48 characters - user [<i><string></i>]: <i><string></i> | Change device names so Spark SIP addresses don't exceed the 48 character limit. | warning |
| 60344 | User's directory URI is not in the organization's verified domain list | User's directory URI is not in the organization's verified domain list - user[<i><string></i>]: <i><string></i> has domain list = <i><string></i> | Check the user's directory URI and list of verified domains for this user | warning |
| 60345 | Failed to Build Unified CM Cluster Data-Cache | Failed to Build Unified CM Cluster Data-Cache - server [<i><string></i>] | Check if the AXL service is running on Unified CM cluster nodes and resolve any network issues. | error |
| 60346 | Authentication Failure with Cisco Collaboration Cloud Services. | Authentication credentials available on Expressway are invalid. | Go to the Expressway, and then reregister it to the cloud under Applications > Hybrid Services > Connector Management. | error |
| 60347 | Authorization Failure with Cisco Collaboration Cloud Services. | Invalid role or access scope for this Expressway to access Cisco Collaboration Cloud Services. | Go to the Expressway, and then reregister it to the cloud under Applications > Hybrid Services > Connector Management. | error |
| 60348 | Connection from the Cisco Collaboration Cloud is down. | Connection from the Cisco Collaboration Cloud is down. | Check your network DNS or proxy settings and then try again. | error |
| 60349 | Connection to the Cisco Collaboration Cloud is down. | Connection to the Cisco Collaboration Cloud is down. | Check your network DNS or proxy settings and then try again. | error |
| 60350 | Cannot enable hybrid voicemail for your organization. | Cannot enable hybrid voicemail for your organization. | If this error persists, work with your trials team or contact support by submitting feedback through the Cisco Spark app. | warning |
| 60351 | Call connector detected an invalid hybrid voicemail configuration. | Call connector detected an invalid hybrid voicemail configuration. | Check the Hybrid Voicemail deployment steps. If this error persists, work with your trials team or contact support by submitting feedback through the Cisco Spark app. | error |

Table 41 Call Connector Alarms (continued)

| ID | Title | Description | Solution | Severity |
|-------|---|---|--|----------|
| 60352 | No Directory Number exists in UCM with this directory URI | No Directory Number exists in UCM with this directory URI | Configure a Directory Number in UCM with this directory URI | error |
| 60353 | AXL Change Notification is not started at Unified CM. | AXL Change Notification is not started at Unified CM - server[<string>] | Enable AXL Change Notification in Enterprise Parameters of Unified CM. | error |

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 42 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 S 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. For example <code>IP Route [1..50] Address <S: 0,39></code> 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 43 xConfiguration CLI reference

| |
|--|
| <p>Administration HTTP Mode: <On/Off></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>Administration HTTPS Mode: <On/Off></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>Administration LCDPanel Mode: <On/Off></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>Administration SSH Mode: <On/Off></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>Alternates Cluster Name: <S: 0,128></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>Alternates ConfigurationMaster: <1..6></p> <p>Specifies which peer in this cluster is the primary, 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>Alternates Peer [1..6] Address: <S: 0, 128></p> <p>Specifies the 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. We recommend using FQDNs, but these can be IP addresses.</p> <p>Example: <code>xConfiguration Alternates 1 Peer Address: "cluster1peer3.example.com"</code></p> |
| <p>ApacheModReqTimeOut</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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>ApacheModReqTimeOut Apachebody: <0..120></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> |
| <p>ApacheModReqTimeOut Apacheheader: <0..120></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>ApacheModReqTimeOut Status: <On/Off></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>Applications ConferenceFactory Alias: <S:0,60></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>Applications ConferenceFactory Mode: <On/Off></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>Applications ConferenceFactory Range End: <1..65535></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>Applications ConferenceFactory Range Start: <1..65535></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>Applications ConferenceFactory Template: <S:0,60></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>Applications External Status [1..10] Filename: <S:0,255></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Applications External Status [1..10] Name: <S:0,64></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>Authentication ADS ADDomain: <S: 0,255></p> <p>The Kerberos realm used when the Expressway joins the AD domain. Note: this field is case sensitive.</p> <p>Example: <code>xConfiguration Authentication ADS ADDomain: "CORPORATION.INT"</code></p> |
| <p>Authentication ADS Clockskew: <1..65535></p> <p>Maximum allowed clockskew between the Expressway and the KDC before the Kerberos message is assumed to be invalid (in seconds). Default: 300.</p> <p>Example: <code>xConfiguration Authentication ADS Clockskew: 300</code></p> |
| <p>Authentication ADS CipherSuite: <S:1,2048></p> <p>Specifies the cipher suite to use when the Expressway makes a TLS-encrypted LDAP connection to join the AD domain. The command accepts a string in the 'OpenSSL ciphers' format (See https://www.openssl.org/docs/man1.0.1/apps/ciphers.html#CIPHER-LIST-FORMAT).</p> <p>Example: <code>xConfiguration Authentication ADS CipherSuite: "HIGH:MEDIUM:!ADH:!aNULL:!eNULL:-AES128-SHA256:@STRENGTH"</code></p> |
| <p>Authentication ADS DC [1..5] Address: <S: 0,39></p> <p>The address of a domain controller that can be used when the Expressway joins the AD domain. Not specifying a specific AD will result the use of DNS SRV queries to find an AD.</p> <p>Example: <code>xConfiguration Authentication ADS DC 1 Address: "192.168.0.0"</code></p> |
| <p>Authentication ADS Encryption: <Off/TLS></p> <p>Sets the encryption to use for the LDAP connection to the ADS 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 Authentication ADS Encryption: TLS</code></p> |
| <p>Authentication ADS KDC [1..5] Address: <S: 0,39></p> <p>The address of a Kerberos Distribution Center (KDC) to be used when connected to the AD domain. Not specifying a specific KDC will result in the use of DNS SRV queries to find a KDC.</p> <p>Example: <code>xConfiguration Authentication ADS KDC 1 Address: "192.168.0.0"</code></p> |
| <p>Authentication ADS KDC [1..5] Port: <1..65534></p> <p>Specifies the port of a KDC that can be used when the Expressway joins the AD domain. Default: 88.</p> <p>Example: <code>xConfiguration Authentication ADS KDC 1 Port: 88</code></p> |
| <p>Authentication ADS MachineName: <S: 0..15></p> <p>This overrides the default NETBIOS machine name used when the Expressway joins the AD domain.</p> <p>Example: <code>xConfiguration Authentication ADS MachineName: "short_name"</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Authentication ADS MachinePassword Refresh: <On/Off></p> <p>Determines if this samba client should refresh its machine password every 7 days, when joined to the AD domain. Default: On.</p> <p>Example: <code>xConfiguration Authentication ADS MachinePassword Refresh: On</code></p> |
| <p>Authentication ADS Mode: <On/Off></p> <p>Indicates if the Expressway should attempt to form a relationship with the AD. Default: Off.</p> <p>Example: <code>xConfiguration Authentication ADS Mode: On</code></p> |
| <p>Authentication ADS SPNEGO: <Enabled/Disabled></p> <p>Indicates if SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism) is used when the client (the Expressway) authenticates with the server (the AD domain controller). Default: Enabled.</p> <p>Example: <code>xConfiguration Authentication ADS SPNEGO: Enabled</code></p> |
| <p>Authentication ADS SecureChannel: <Auto/Enabled/Disabled></p> <p>Indicates if data transmitted from the Expressway to an AD domain controller is sent over a secure channel. Default: Auto.</p> <p>Example: <code>xConfiguration Authentication ADS SecureChannel: Auto</code></p> |
| <p>Authentication ADS Workgroup: <S: 0,15></p> <p>The workgroup used when the Expressway joins the AD domain.</p> <p>Example: <code>xConfiguration Authentication ADS Workgroup: "corporation"</code></p> |
| <p>Authentication Account Admin Account [1..n] AccessAPI: <On/Off></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>Authentication Account Admin Account [1..n] AccessWeb: <On/Off></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> |
| <p>Authentication Account Admin Account [1..n] Enabled: <On/Off></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>Authentication Account Admin Account [1..n] Name: <S: 0, 128></p> <p>The username for the administrator account.</p> <p>Example: <code>xConfiguration Authentication Account Admin Account 1 Name: "bob_smith"</code></p> |
| <p>Authentication Account Admin Account [1..n] Password: <Password></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Authentication Account Admin Group [1..n] AccessAPI: <On/Off></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>Authentication Account Admin Group [1..n] AccessWeb: <On/Off></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>Authentication Account Admin Group [1..n] Enabled: <On/Off></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>Authentication Account Admin Group [1..n] Name: <S: 0, 128></p> <p>The name of the administrator group.</p> <p>Example: <code>xConfiguration Authentication Account Admin Group 1 Name: "administrators"</code></p> |
| <p>Authentication Certificate Crlcheck: <None/Peer/All></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>Authentication Certificate Crlinaccessible: <Ignore/Fail></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> |
| <p>Authentication Certificate Mode: <NotRequired/Validation/Authentication></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Authentication Certificate UsernameRegex: <String></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: /Subject.*CN= (? ([^,\\] (\\,))*)/m</p> <p>Example: <code>xConfiguration Authentication Certificate UsernameRegex: "/Subject:.*CN= (? ([^,\\] (\\,))*)/m"</code></p> |
| <p>Authentication Certificate UsernameTemplate: <String></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: #captureCommonName#</p> <p>Example: <code>xConfiguration Authentication Certificate UsernameTemplate: "#captureCommonName#"</code></p> |
| <p>Authentication H350 BindPassword: <S: 0, 60></p> <p>Sets the password to use when binding to the LDAP server.</p> <p>Example: <code>xConfiguration Authentication H350 BindPassword: "abcXYZ_123"</code></p> |
| <p>Authentication H350 BindSaslMode: <None/DIGEST-MD5></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 Authentication H350 BindSaslMode: DIGEST-MD5</code></p> |
| <p>Authentication H350 BindUserDn: <S: 0, 500></p> <p>Sets the user distinguished name to use when binding to the LDAP server.</p> <p>Example: <code>xConfiguration Authentication H350 BindUserDn: "manager"</code></p> |
| <p>Authentication H350 BindUserName: <S: 0, 500></p> <p>Sets the username to use when binding to the LDAP server. Only applies if using SASL.</p> <p>Example: <code>xConfiguration Authentication H350 BindUserName: "manager"</code></p> |
| <p>Authentication H350 DirectoryBaseDn: <S: 0, 500></p> <p>Sets the Distinguished Name to use when connecting to an LDAP server.</p> <p>Example: <code>xConfiguration Authentication H350 DirectoryBaseDn: "dc=example,dc=company,dc=com"</code></p> |
| <p>Authentication H350 LdapEncryption: <Off/TLS></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 Authentication H350 LdapEncryption: TLS</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Authentication H350 LdapServerAddress: <S: 0, 256></p> <p>The IP address or Fully Qualified Domain Name of the LDAP server to use when making LDAP queries for device authentication.</p> <p>Example: <code>xConfiguration Authentication H350 LdapServerAddress: "ldap_server.example.com"</code></p> |
| <p>Authentication H350 LdapServerAddressResolution: <AddressRecord/ServiceRecord></p> <p>Sets how the LDAP server address is resolved if specified as an FQDN. Default: AddressRecord.</p> <p><i>Address record:</i> DNS A or AAAA record lookup.</p> <p><i>SRV record:</i> DNS SRV record lookup.</p> <p>Example: <code>xConfiguration Authentication H350 LdapServerAddressResolution: AddressRecord</code></p> |
| <p>Authentication H350 LdapServerPort: <1..65535></p> <p>Sets the IP port of the LDAP server to use when making LDAP queries for device authentication. Typically, non-secure connections use 389 and secure connections use 636. Default : 389</p> <p>Example: <code>xConfiguration Authentication H350 LdapServerPort: 389</code></p> |
| <p>Authentication H350 Mode: <On/Off></p> <p>Enables or disables the use of an H.350 directory for device authentication. Default: Off.</p> <p>Example: <code>xConfiguration Authentication H350 Mode: Off</code></p> |
| <p>Authentication LDAP AliasOrigin: <LDAP/Endpoint/Combined></p> <p>Determines how aliases are checked and registered. Default: LDAP.</p> <p><i>LDAP:</i> the aliases presented by the endpoint are checked against those listed in the LDAP database.</p> <p><i>Endpoint:</i> the aliases presented by the endpoint are used; any in the LDAP database are ignored.</p> <p><i>Combined:</i> the aliases presented by the endpoint are used in addition to any listed in the LDAP database.</p> <p>Example: <code>xConfiguration Authentication LDAP AliasOrigin: LDAP</code></p> |
| <p>Authentication Password: <S: 0, 215></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>Authentication Remote Digest Cache ExpireCheckInterval: <0..65535></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>Authentication Remote Digest Cache Lifetime: <0..43200></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>Authentication Remote Digest Cache Limit: <0..65535></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Authentication Remote Digest Cache Mode: <On/Off></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>Authentication StrictPassword Enabled: <On/Off></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> |
| <p>Authentication StrictPassword MaximumConsecutiveRepeated: <0..255></p> <p>The maximum number of times the same character can be repeated consecutively. A value of 0 disables this check. Default: 0</p> <p>Example: <code>xConfiguration Authentication StrictPassword MaximumConsecutiveRepeated: 0</code></p> |
| <p>Authentication StrictPassword MinimumClasses: <0..4></p> <p>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.</p> <p>Example: <code>xConfiguration Authentication StrictPassword MinimumClasses: 0</code></p> |
| <p>Authentication StrictPassword MinimumDigits: <0..255></p> <p>The minimum number of digits that must be present. A value of 0 disables this check. Default: 2.</p> <p>Example: <code>xConfiguration Authentication StrictPassword MinimumDigits: 2</code></p> |
| <p>Authentication StrictPassword MinimumLength: <6..255></p> <p>The minimum length of the password. Default: 15.</p> <p>Example: <code>xConfiguration Authentication StrictPassword MinimumLength: 15</code></p> |
| <p>Authentication StrictPassword MinimumLowerCase: <0..255></p> <p>The minimum number of lower case characters that must be present. A value of 0 disables this check. Default: 2.</p> <p>Example: <code>xConfiguration Authentication StrictPassword MinimumLowerCase: 2</code></p> |
| <p>Authentication StrictPassword MinimumOther: <0..255></p> <p>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</p> <p>Example: <code>xConfiguration Authentication StrictPassword MinimumOther: 2</code></p> |
| <p>Authentication StrictPassword MinimumUpperCase: <0..255></p> <p>The minimum number of upper case characters that must be present. A value of 0 disables this check. Default : 2</p> <p>Example: <code>xConfiguration Authentication StrictPassword MinimumUpperCase: 2</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Authentication UserName: <S: 0, 128></p> <p>The username used by the Expressway when authenticating with another system. Note: this does not apply to traversal client zones.</p> <p>Example: <code>xConfiguration Authentication UserName: "user123"</code></p> |
| <p>Bandwidth Default: <64..65535></p> <p>The bandwidth (in kbps) to use on calls managed by the Expressway where no bandwidth has been specified by the endpoint. Default: 384.</p> <p>Example: <code>xConfiguration Bandwidth Default: 384</code></p> |
| <p>Bandwidth Downspeed PerCall Mode: <On/Off></p> <p>Determines whether the Expressway attempts to downspeed a call if there is insufficient per-call bandwidth available to fulfill the request. Default: On.</p> <p><i>On:</i> the Expressway will attempt to place the call at a lower bandwidth.</p> <p><i>Off:</i> the call will be rejected.</p> <p>Example: <code>xConfiguration Bandwidth Downspeed PerCall Mode: On</code></p> |
| <p>Bandwidth Downspeed Total Mode: <On/Off></p> <p>Determines whether the Expressway attempts to downspeed a call if there is insufficient total bandwidth available to fulfill the request. Default: On.</p> <p><i>On:</i> the Expressway will attempt to place the call at a lower bandwidth.</p> <p><i>Off:</i> the call will be rejected.</p> <p>Example: <code>xConfiguration Bandwidth Downspeed Total Mode: On</code></p> |
| <p>Bandwidth Link [1..3000] Name: <S: 1, 50></p> <p>Assigns a name to this link.</p> <p>Example: <code>xConfiguration Bandwidth Link 1 Name: "HQ to BranchOffice"</code></p> |
| <p>Bandwidth Link [1..3000] Node1 Name: <S: 0, 50></p> <p>Specifies the first zone or subzone to which this link will be applied.</p> <p>Example: <code>xConfiguration Bandwidth Link 1 Node1 Name: "HQ"</code></p> |
| <p>Bandwidth Link [1..3000] Node2 Name: <S: 0, 50></p> <p>Specifies the second zone or subzone to which this link will be applied.</p> <p>Example: <code>xConfiguration Bandwidth Link 1 Node2 Name: "BranchOffice"</code></p> |
| <p>Bandwidth Link [1..3000] Pipe1 Name: <S: 0, 50></p> <p>Specifies the first pipe to be associated with this link.</p> <p>Example: <code>xConfiguration Bandwidth Link 1 Pipe1 Name: "512Kb ASDL"</code></p> |
| <p>Bandwidth Link [1..3000] Pipe2 Name: <S: 0, 50></p> <p>Specifies the second pipe to be associated with this link.</p> <p>Example: <code>xConfiguration Bandwidth Link 1 Pipe2 Name: "2Gb Broadband"</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Bandwidth Pipe [1..1000] Bandwidth PerCall Limit: <1..100000000></p> <p>If this pipe has limited per-call bandwidth, sets the maximum amount of bandwidth (in kbps) available for any one call. Default: 1920.</p> <p>Example: <code>xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Limit: 256</code></p> |
| <p>Bandwidth Pipe [1..1000] Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth></p> <p>Determines whether or not this pipe is limiting the bandwidth of individual calls. Default: Unlimited.</p> <p><i>NoBandwidth</i>: no bandwidth available. No calls can be made on this pipe.</p> <p>Example: <code>xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Mode: Limited</code></p> |
| <p>Bandwidth Pipe [1..1000] Bandwidth Total Limit: <1..100000000></p> <p>If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe. Default: 500000.</p> <p>Example: <code>xConfiguration Bandwidth Pipe 1 Bandwidth Total Limit: 1024</code></p> |
| <p>Bandwidth Pipe [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth></p> <p>Determines whether or not this pipe is enforcing total bandwidth restrictions. Default: Unlimited.</p> <p><i>NoBandwidth</i>: no bandwidth available. No calls can be made on this pipe.</p> <p>Example: <code>xConfiguration Bandwidth Pipe 1 Bandwidth Total Mode: Limited</code></p> |
| <p>Bandwidth Pipe [1..1000] Name: <S: 1, 50></p> <p>Assigns a name to this pipe.</p> <p>Example: <code>xConfiguration Bandwidth Pipe 1 Name: "512Kb ASDL"</code></p> |
| <p>Call Loop Detection Mode: <On/Off></p> <p>Specifies whether the Expressway will check for call loops. Default: On.</p> <p>Example: <code>xConfiguration Call Loop Detection Mode: On</code></p> |
| <p>Call Routed Mode: <Always/Optimal></p> <p>Specifies whether the Expressway routes the signaling for calls. Default: Always.</p> <p><i>Always</i>: the Expressway will always route the call signaling.</p> <p><i>Optimal</i>: if possible, the Expressway will remove itself from the call signaling path, which may mean the call does not consume a call license.</p> <p>Example: <code>xConfiguration Call Routed Mode: Always</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Call Services CallsToUnknownIPAddresses: <Off/Direct/Indirect></p> <p>The way in which the Expressway attempts to call systems that are not registered with it or one of its neighbors. Default: Indirect.</p> <p><i>Direct:</i> 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.</p> <p><i>Indirect:</i> 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.</p> <p><i>Off:</i> endpoints registered directly to the Expressway may only call an IP address of a system also registered directly to that Expressway.</p> <p>Example: <code>xConfiguration Call Services CallsToUnknownIPAddresses: Indirect</code></p> |
| <p>Call Services Fallback Alias: <S: 0, 60></p> <p>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.</p> <p>Example: <code>xConfiguration Call Services Fallback Alias: "reception@example.com"</code></p> |
| <p>CollaborationEdge AllowEmbeddedSafari: <Yes/No></p> <p>This only applies to Cisco Jabber 11.8 or later, on iPads or iPhones using iOS 9 or later, when they authorize using OAuth tokens.</p> <p>Select Yes to allow Jabber on iOS devices to display the authentication page in the native Safari browser.</p> <p>Select No to have Jabber on iOS devices display the authentication page in the WebView browser, rather than in the Safari browser.</p> <p>Note: If you toggle this option, also make the corresponding selection for SSO Login Behavior for iOS in Cisco Unified Communications Manager.</p> <p>Example: <code>xConfiguration CollaborationEdge AllowEmbeddedSafari: No</code></p> |
| <p>CollaborationEdge AllowList DefaultMethods: <String></p> <p>Configure one or more default HTTP methods for the HTTP allow list.</p> <p>Configuration Parameters:</p> <p>Methods: <OPTIONS/GET/HEAD/POST/PUT/DELETE> - A comma-delimiting set of one or more http methods</p> <p>Example: <code>xConfiguration CollaborationEdge AllowList DefaultMethods: PUT,GET,POST</code></p> |
| <p>CollaborationEdge Enabled: <On/Off></p> <p>Enables or disables Mobile and Remote Access on this Expressway.</p> <p>Example: <code>xConfiguration CollaborationEdge Enabled: On</code></p> |
| <p>CollaborationEdge InternalCheck: <No/Yes></p> <p>This switch determines whether the Expressway-C will check the user's home node for available authentication modes. If you select No, the Expressway tells the client that the authentication modes enabled on the Expressway-C are available, without actually checking the home node. You should see less traffic on the internal network as a result, but you should only select this option if you know that all nodes have the same authentication modes available.</p> <p>Select Yes to allow the Expressway-C to check on the user's home node before the Expressway-E responds to the client.</p> <p>Example: <code>xConfiguration CollaborationEdge InternalCheck: No</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>CollaborationEdge JabberEnabled: <On/Off></p> <p>Enables or disables Jabber Guest services on this Expressway.</p> <p>Example: <code>xConfiguration JabberEnabled: Off</code></p> |
| <p>CollaborationEdge JabberProxyProtocol: <http/https></p> <p>Selects the protocol used to proxy Jabber Guest services requests through the Expressway.</p> <p>Example: <code>xConfiguration JabberProxyProtocol: https</code></p> |
| <p>CollaborationEdge LegacyCred: <On/Off></p> <p>Select On if Unified Communications services authorize MRA clients based on the username and password they supply to the Expressway.</p> <p>Example: <code>xConfiguration CollaborationEdge LegacyCred: Off</code></p> |
| <p>CollaborationEdge LegacySso: <On/Off/Exclusive></p> <p>Select On if Unified Communications services authorize MRA clients based on the OAuth token they supply to the Expressway. This is not the self-describing OAuth token type.</p> <p>Example: <code>xConfiguration CollaborationEdge LegacySso: Off</code></p> |
| <p>CollaborationEdge OAuthLocal: <On/Off></p> <p>Enables or disables OAuth local authentication for mobile and remote access to Unified Communications services.</p> <p>Example: <code>xConfiguration CollaborationEdge OAuthLocal: Off</code></p> |
| <p>CollaborationEdge OAuthSso: <On/Off></p> <p>Enables or disables OAuth Single Sign-On for mobile and remote access to Unified Communications services.</p> <p>Example: <code>xConfiguration CollaborationEdge OAuthSso: Off</code></p> |
| <p>CollaborationEdge RFC3327Enabled: <On/Off></p> <p>Changes Path header support for registrations going through automatically generated neighbor zones to Unified CM nodes.</p> <p><i>On:</i> The Expressway-C inserts its address into the Path header of the REGISTER message, and into the response to that message.</p> <p><i>Off:</i> The Expressway-C overwrites the address in the Contact header of the REGISTER message.</p> <p>Example: <code>xConfiguration CollaborationEdge rfc3327Enabled: On</code></p> |
| <p>CollaborationEdge SSO IdP <index> Digest: <sha1/sha256></p> <p>Changes the hash algorithm that the Expressway uses when signing SAML authentication requests given to the client.</p> <p><i><index></i> is an integer distinguishing a particular IdP from the list that is configured on the Expressway.</p> <p>Example: <code>xConfiguration CollaborationEdge SSO IdP 1 Digest: sha256</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>CollaborationEdge SsoAlwaysAvailable: <On/Off></p> <p>Determines whether the Expressway-C will check if the user's home node has SSO available.</p> <p><i>On:</i> The Expressway-E always tells the client that SSO is available, without actually checking the home node.</p> <p><i>Off:</i> Allow the Expressway-C to check if SSO is available on the user's home node before the Expressway-E responds to the client.</p> <p>Example: <code>xConfiguration CollaborationEdge SsoAlwaysAvailable: Off</code></p> <p>Note: The default value <i>Off</i> corresponds to the following default on the web UI: Check for internal SSO availability: Yes</p> |
| <p>CollaborationEdge SsoEnabled: <On/Off></p> <p>Toggles Single Sign-On for mobile and remote access to UC services.</p> <p>Example: <code>xConfiguration CollaborationEdge SsoEnabled: Off</code></p> |
| <p>CollaborationEdge SsoSipTokenExtraTtl: <0..172800></p> <p>Extends the lifetime of the SIP authorization token by the supplied number of seconds.</p> <p>Important! The extended time-to-live means that external users can still use SIP over the edge after their on-premises UC credentials have expired. This gives users a short window in which they can still accept calls (if they haven't noticed that they need to re-authenticate), but you should balance this convenience against the increased security exposure.</p> <p>Example: <code>xConfiguration CollaborationEdge SsoSipTokenExtraTtl: 0</code></p> |
| <p>CollaborationEdgeDeployments <index> DeploymentId: <1..65535></p> <p>Changes the deployment ID of a particular deployment.</p> <p><i><index></i> is an integer distinguishing a particular IdP from the list that is configured on the Expressway.</p> <p>Example: <code>xConfiguration CollaborationEdgeDeployments 1 DeploymentId: 5</code></p> |
| <p>CollaborationEdgeDeployments <index> UserReadableName: <String></p> <p>Enter a name for this deployment. You can use multiple deployments to partition the Unified Communications services provided via this Expressway. See Using deployments to partition Unified Communications services.</p> <p><i><index></i> is an integer distinguishing a particular IdP from the list that is configured on the Expressway.</p> <p>Example: <code>xConfiguration CollaborationEdgeDeployments 1 UserReadableName: StagingDeployment</code></p> |
| <p>Ciphers SIPTLSCiphers Value: <S:0,2048></p> <p>Specifies the SIP TLS cipher suite to use in 'OpenSSL ciphers' format (See https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT). Note that a restart is required for this to take effect. Also note that aNULL ciphers are not supported for inbound connections. Default: <code>ECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH</code></p> <p>Example: <code>xConfiguration Ciphers SIPTLSCiphers Value: "ECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH"</code></p> <p>To change SIP TLS protocol value, see: SIP Advanced SipTlsVersions.</p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Ciphers ForwardProxyTLSCiphers Value: <S:0,2048></p> <p>Specifies the Forward Proxy TLS cipher suite to use in 'OpenSSL ciphers' format (See https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT).</p> <p>Default: <code>ECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL</code></p> <p>Example: <code>xConfiguration Ciphers ForwardProxyTLSCiphers Value: "ECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"</code></p> |
| <p>Ciphers ForwardProxyTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2></p> <p>Specifies the Forward Proxy TLS protocol minimum version.</p> <p>Default: <code>minTLSv1.2</code></p> <p>Example: <code>xConfiguration Ciphers ForwardProxyTLSProtocol Value: "minTLSv1.2"</code></p> |
| <p>Ciphers HTTPSCiphers Value: <S:0,2048></p> <p>Specifies the HTTPS cipher suite to use in 'OpenSSL ciphers' format (See https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT).</p> <p>Default: <code>ECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL</code></p> <p>Example: <code>xConfiguration Ciphers HTTPSCiphers Value: "ECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"</code></p> |
| <p>Ciphers HTTPSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2></p> <p>Specifies the HTTPS TLS protocol minimum version.</p> <p>Default: <code>minTLSv1.2</code></p> <p>Example: <code>xConfiguration Ciphers HTTPSProtocol Value: "minTLSv1.2"</code></p> |
| <p>Ciphers ReverseProxyTLSCiphers Value: <S:0,2048></p> <p>Specifies the Reverse Proxy TLS cipher suite to use in 'OpenSSL ciphers' format (See https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT).</p> <p>Default: <code>ECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL</code></p> <p>Example: <code>xConfiguration Ciphers ReverseProxyTLSCiphers Value: "ECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"</code></p> |
| <p>Ciphers ReverseProxyTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2></p> <p>Specifies the Reverse Proxy TLS protocol minimum version.</p> <p>Default: <code>minTLSv1.2</code></p> <p>Example: <code>xConfiguration Ciphers ReverseProxyTLSProtocol Value: "minTLSv1.2"</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Ciphers UClientTLSCiphers Value: <S:0,2048></p> <p>Specifies the UC Client TLS cipher suite to use in 'OpenSSL ciphers' format (See https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT).</p> <p>Default: EEC DH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL</p> <p>Example: xConfiguration Ciphers UClientTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"</p> |
| <p>Ciphers UClientTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2></p> <p>Specifies the UC Client TLS protocol minimum version.</p> <p>Default: minTLSv1.2</p> <p>Example: xConfiguration Ciphers UClientTLSProtocol Value: "minTLSv1.2"</p> |
| <p>Ciphers XCP TLSCiphers Value: <S:0,2048></p> <p>Specifies the XCP TLS cipher suite to use in 'OpenSSL ciphers' format (See https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT). Note that a restart is required for this to take effect.</p> <p>Default: EEC DH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL</p> <p>Example: xConfiguration Ciphers XCP TLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"</p> |
| <p>Ciphers XCP TLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2></p> <p>Specifies the XCP TLS protocol minimum version.</p> <p>Default: minTLSv1.2</p> <p>Example: xConfiguration Ciphers XCP TLSProtocol Value: "minTLSv1.2"</p> |
| <p>Ciphers sshd_ciphers Value: <S:0,2048></p> <p>Configures the available ciphers for admin/root SSH connections (TCP/22) in "openssh" format.</p> <p>Default: aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr,aes256-cbc,aes192-cbc,aes128-cbc</p> <p>Example: xConfiguration Ciphers sshd_ciphers Value: "aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr,aes256-cbc,aes192-cbc,aes128-cbc"</p> |
| <p>Ciphers sshd_kex Value: <S:0,2048></p> <p>Configures key exchange algorithms for admin/root SSH connections (TCP/22) in "openssh" format.</p> <p>Default: ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1</p> <p>Example: xConfiguration Ciphers sshd_kex Value: "ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1"</p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Ciphers sshd_macs Value: <S:0,2048></p> <p>Configures the message authentication code digests for admin/root SSH connections (TCP/22) in "openssh" format.</p> <p>Default: <code>hmac-sha2-512,hmac-sha2-256,hmac-sha1</code></p> <p>Example: <code>xConfiguration Ciphers sshd_macs Value: "hmac-sha2-512,hmac-sha2-256,hmac-sha1"</code></p> |
| <p>Ciphers sshd_pfw_d_ciphers Value: <S:0,2048></p> <p>The ciphers available for the SSH tunnels used for the forward and reverse HTTP proxies (i.e. APNS and MRA HTTP traffic).</p> <p>Default: <code>aes256-ctr</code></p> <p>Example: <code>xConfiguration Ciphers sshd_pfw_d_ciphers Value: "aes256-ctr"</code></p> |
| <p>DNS PerDomainServer [1..5] Address: <S: 0, 39></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>DNS PerDomainServer [1..5] Domain1: <S: 0, 39></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>DNS PerDomainServer [1..5] Domain2: <S: 0, 39></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>DNS Server [1..5] Address: <S: 0, 39></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>EdgeConfigServer CredentialTtl: <0..604800></p> <p>Does not apply to SSO authentications.</p> <p>Specifies the lifetime of the authentication token issued by the Expressway to a successfully authenticated client. A client that successfully authenticates should request a refresh before this token expires, or it will need to re-authenticate.</p> <p>Example: <code>EdgeConfigServer CredentialTtl: 28800</code></p> |
| <p>EdgeConfigServer PurgeInterval: <0..604800></p> <p>Does not apply to SSO authentications.</p> <p>Specifies how long the Expressway waits between cache clearing operations. Only expired tokens are removed when the cache is cleared, so this setting is the longest possible time that an expired token can remain in the cache.</p> <p>Example: <code>EdgeConfigServer PurgeInterval: 43200</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>EdgeConfigServer RateLimitLogins: <0..100></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>EdgeConfigServer RateLimitPeriod: <0..86400></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>ErrorReport Contact: <S: 0, 128></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>ErrorReport CoreDump: <On/Off></p> <p>Determines whether diagnostic core dump files are created. Default: On.</p> <p>Example: <code>xConfiguration ErrorReport CoreDump: On</code></p> |
| <p>ErrorReport Mode: <On/Off></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>ErrorReport Proxy: <S: 0, 128></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>ErrorReport Url: <S: 0, 128></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> |
| <p>Ethernet [1..2] IP V4 Address: <S: 7,15></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>Ethernet [1..2] IP V4 StaticNAT Address: <S:7,15></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Ethernet [1..2] IP V4 StaticNAT Mode: <On/Off></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>Ethernet [1..2] IP V4 SubnetMask: <S: 7,15></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>Ethernet [1..2] IP V6 Address: <S: 0, 39></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>Ethernet [1..2] Speed: <Auto/10half/10full/100half/100full/1000full></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>ExternalManager Address: <S: 0, 128></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>ExternalManager Path: <S: 0, 255></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>ExternalManager Protocol: <HTTP/HTTPS></p> <p>The protocol used to connect to the external manager. Default: HTTPS.</p> <p>Example: <code>xConfiguration ExternalManager Protocol: HTTPS</code></p> |
| <p>ExternalManager Server Certificate Verification Mode: <On/Off></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>H323 Gatekeeper AutoDiscovery Mode: <On/Off></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>H323 Gatekeeper CallSignaling PortRange End: <1024..65534></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 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>H323 Gatekeeper CallSignaling PortRange Start: <1024..65534></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>H323 Gatekeeper CallSignaling TCP Port: <1024..65534></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>H323 Gatekeeper CallTimeToLive: <60..65534></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>H323 Gatekeeper Registration RIPAllRequests: <On/Off></p> <p>Determines whether the Expressway will respond to H.323 registration request with a Request In Progress message.</p> <p>Enable this setting if you are experiencing registration timeouts when authenticating registration requests with a remote LDAP directory service. Default: Off</p> <p>Example: <code>xConfiguration H323 Gatekeeper Registration RIPAllRequests: Off</code></p> |
| <p>H323 Gatekeeper Registration ConflictMode: <Reject/Overwrite></p> <p>How the system behaves if an endpoint attempts to register an alias currently registered from another IP address. Default: Reject.</p> <p><i>Reject</i>: denies the registration.</p> <p><i>Overwrite</i>: deletes the original registration and replaces it with the new registration.</p> <p>Example: <code>xConfiguration H323 Gatekeeper Registration ConflictMode: Reject</code></p> |
| <p>H323 Gatekeeper Registration UDP Port: <1024..65534></p> <p>Specifies the port to be used for H.323 UDP registrations. Default: 1719.</p> <p>Example: <code>xConfiguration H323 Gatekeeper Registration UDP Port: 1719</code></p> |
| <p>H323 Gatekeeper TimeToLive: <60..65534></p> <p>The interval (in seconds) at which an H.323 endpoint must re-register with the Expressway to confirm that it is still functioning. Default: 1800.</p> <p>Example: <code>xConfiguration H323 Gatekeeper TimeToLive: 1800</code></p> |
| <p>H323 Gateway CallerId: <IncludePrefix/ExcludePrefix></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>H323 Mode: <On/Off></p> <p>Determines whether or not the Expressway will provide H.323 gatekeeper functionality. Default: Off.</p> <p>Example: <code>xConfiguration H323 Mode: On</code></p> |
| <p>Interworking BFCP Compatibility Mode: <Auto/TAA/Draft></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>Interworking Encryption Mode: <Auto/Off></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>Interworking Encryption Replay Protection Mode: <On/Off></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>Interworking Mode: <On/Off/RegisteredOnly></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 regardless of whether the endpoints are locally registered.</p> <p><i>RegisteredOnly</i>: the Expressway will act as a SIP-H.323 gateway but only if at least one of the endpoints is locally registered.</p> <p>Example: <code>xConfiguration Interworking Mode: On</code></p> |
| <p>Interworking Require Invite Header Mode: <On/Off></p> <p>Controls whether the SIP to H.323 interworking function sends <code>com.tandberg.sdp.duo.enable</code> and <code>com.tandberg.sdp.bfcf.udp</code> in the require header for dialog forming INVITES. Default: Off.</p> <p>Example: <code>xConfiguration Interworking Require Invite Header Mode: Off"</code></p> |
| <p>IP DNS Domain Name: <S: 0, 128></p> <p>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 System host name to identify references to this Expressway in SIP messaging.</p> <p>Example: <code>xConfiguration IP DNS Domain Name: "example.com"</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>IP DNS Hostname : <S: 0, 63></p> <p>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.</p> <p>Example: <code>xConfiguration IP DNS Hostname: "localsystem"</code></p> |
| <p>IP DNS MaxPort : <1024..65535></p> <p>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.</p> <p>Example: <code>xConfiguration IP DNS MaxPort: 65535</code></p> |
| <p>IP DNS MinPort : <1024..65535></p> <p>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.</p> <p>Example: <code>xConfiguration IP DNS MinPort: 1024</code></p> |
| <p>IP DNS UseEphemeralPortRange : <On/Off></p> <p>Determines whether outgoing DNS queries use the system's normal ephemeral port range, or a custom port range that you can configure. Default: On.</p> <p>Example: <code>xConfiguration IP DNS UseEphemeralPortRange: On</code></p> |
| <p>IP Ephemeral PortRange End : <1024..65534></p> <p>The highest port in the range used for ephemeral outbound connections not otherwise constrained by Expressway call processing. Default: 35999.</p> <p>Example: <code>xConfiguration IP Ephemeral PortRange End: 35999</code></p> |
| <p>IP Ephemeral PortRange Start : <1024..65534></p> <p>The lowest port in the range used for ephemeral outbound connections not otherwise constrained by Expressway call processing. Default: 30000.</p> <p>Example: <code>xConfiguration IP Ephemeral PortRange Start: 30000</code></p> |
| <p>IP External Interface : <LAN1/LAN2></p> <p>Defines which LAN interface is externally facing. Default: LAN1.</p> <p>Example: <code>xConfiguration IP External Interface: LAN1</code></p> |
| <p>IP Gateway : <S: 7,15></p> <p>Specifies the IPv4 gateway of the Expressway. Note: you must restart the system for any changes to take effect. Default: 127.0.0.1</p> <p>Example: <code>xConfiguration IP Gateway: "192.168.127.0"</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>IP QoS Mode: <None/DiffServ></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>Important: This command is discontinued from Version X8.9 and replaced by commands <code>QoS Audio</code>, <code>QoS Video</code>, <code>QoS XMPP</code>, and <code>QoS Signaling</code>.</p> |
| <p>IP QoS Value: <0..63></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>Important: This command is discontinued from Version X8.9 and replaced by commands <code>QoS Audio</code>, <code>QoS Video</code>, <code>QoS XMPP</code>, and <code>QoS Signaling</code>.</p> |
| <p>IP RFC4821 Mode: <Auto/Enabled/Disabled></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>IP Route [1..50] Address: <S: 0, 39></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>IP Route [1..50] Gateway: <S: 0, 39></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>IP Route [1..50] Interface: <Auto/LAN1/LAN2></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>IP Route [1..50] PrefixLength: <0..128></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>IP V6 Gateway: <S: 0, 39></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>IPProtocol: <Both/IPv4/IPv6></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>Language Default: <S: 0, 128></p> <p>The default language used on the web interface. Default: "en_US".</p> <p>Example: <code>xConfiguration Language Default: "en_US"</code></p> |
| <p>Log CDR Service: <off/serviceonly/serviceandlogging></p> <p>Select how to log Call Detail Records produced by this Expressway.</p> <p><i>Off:</i> Call Detail Records are not logged.</p> <p><i>serviceonly:</i> Call Detail Records are stored locally for 7 days and then deleted. The logged records are not accessible via the user interface.</p> <p><i>serviceandlogging:</i> As for <i>serviceonly</i>, except the CDRs are accessible via the local Event log. If you have added syslog server addresses, the records are sent to those as Info messages.</p> <p>Default: <i>off</i></p> <p>Example: <code>xconfig Log CDR Service: serviceonly</code></p> |
| <p>Log Level: <1..4></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>Log MediaStats Logging: <On/Off></p> <p>Toggles media statistics logging. Default: Off</p> <p>Example: <code>xConfiguration Log MediaStats Logging: On</code></p> |
| <p>Log SystemMetrics Interval: <30..600></p> <p>Sets the number of seconds to wait between metrics collection events.</p> <p>Important: A shorter interval has more impact on system performance, while a longer interval yields coarser metrics. We recommend using the longest interval unless you need very fine metrics.</p> <p>Default: 60</p> <p>Example: <code>xconfig Log SystemMetrics Interval: 60</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Log SystemMetrics Mode: <On/Off></p> <p>Toggles the System Metrics Collection service. Enter On to start collecting metrics for this system.</p> <p>Default: Off</p> <p>Example: <code>xconfig Log SystemMetrics Mode: On</code></p> |
| <p>Log SystemMetrics Network Address: <S: 0,1024></p> <p>Enter the address of the listening server. You may use IP address, hostname, or FQDN.</p> <p>Default: Empty</p> <p>Example: <code>xconfig log SystemMetrics Network Address: "192.168.0.5"</code></p> |
| <p>Log SystemMetrics Network Port: <1..65535></p> <p>Enter the port on which the listening server is expecting System Metrics traffic.</p> <p>Default: 25826</p> <p>Example: <code>xconfig log SystemMetrics Network Port: 25826</code></p> |
| <p>Logger Network [1..n] Level: <FATAL/ERROR/WARN/INFO/DEBUG/TRACE></p> <p>The logging level for the nominated module. Default : INFO.</p> <p>Example: <code>xConfiguration Logger Developer 1 Level: INFO</code></p> |
| <p>Login Remote LDAP BaseDN Accounts: <S: 0,255></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>Login Remote LDAP BaseDN Groups: <S: 0,255></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>Login Remote LDAP CRLCheck: <None/Peer/All></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>Login Remote LDAP DirectoryType: <ActiveDirectory></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Login Remote LDAP Encryption: <Off/TLS></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>Login Remote LDAP SASL: <None/DIGEST-MD5></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>Login Remote LDAP Server Address: <S: 0,128></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> |
| <p>Login Remote LDAP Server FQDNResolution: <AddressRecord/SRVRecord></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>Login Remote LDAP Server Port: <1..65534></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>Login Remote LDAP VCS BindDN: <S: 0,255></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>Login Remote LDAP VCS BindPassword: <S: 0,122></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>Login Remote LDAP VCS BindUsername: <S: 0,255></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Login Remote Protocol: <LDAP></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>Login Source Admin: <LocalOnly/RemoteOnly/Both></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>Login User [1..n] Name: <S: 0,60></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>Login User [1..n] Password: <S: 0,128></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> |
| <p>Management Interface HstsMode: <On/Off></p> <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. Default: On.</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. Note: you must restart the system for any changes to take effect.</p> <p>Example: <code>xConfiguration Management Interface HstsMode: On</code></p> |
| <p>Management Interface Port: <1..65535></p> <p>Sets the https listening port for administrators to access the Expressway web interface. Default: 443.</p> <p>Example: <code>xConfiguration Management Interface Port: 445</code></p> |
| <p>Management Session InactivityTimeout: <0..65535></p> <p>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.</p> <p>Example: <code>xConfiguration Management Session InactivityTimeout: 30</code></p> |
| <p>Management Session MaxConcurrentSessionsTotal: <0..65535></p> <p>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.</p> <p>Example: <code>xConfiguration Management Session MaxConcurrentSessionsTotal: 0</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Management Session MaxConcurrentSessionsUser: <0..65535></p> <p>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.</p> <p>Example: <code>xConfiguration Management Session MaxConcurrentSessionsUser: 0</code></p> |
| <p>NetworkLimits</p> <p>Configures the experimental rate limiting feature. Enter <code>xconfig networklimits ?</code> to read the help.</p> <p>Example: <code>xConfiguration NetworkLimits Configuration GarbageCollectSecs: 5</code></p> |
| <p>NTP Server [1..5] Address: <S: 0, 128></p> <p>Sets the IP address or Fully Qualified Domain Name (FQDN) of up to 5 NTP servers to be used when synchronizing system time.</p> <p>Example: <code>xConfiguration NTP Server 1 Address: "ntp.server.example.com"</code></p> |
| <p>Option [1..64] Key: <S: 0, 90></p> <p>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.</p> <p>Example: <code>xConfiguration Option 1 Key: "1X4757T5-1-60BAD5CD"</code></p> |
| <p>Policy AdministratorPolicy Mode: <Off/LocalCPL/LocalService/PolicyService></p> <p>Enables and disables use of Call Policy. Default: Off.</p> <p><i>Off:</i> Disables call policy.</p> <p><i>LocalCPL:</i> uses policy from an uploaded CPL file.</p> <p><i>LocalService:</i> uses group policy information and a local file.</p> <p><i>PolicyService:</i> uses an external policy server.</p> <p>Example: <code>xConfiguration Policy AdministratorPolicy Mode: Off</code></p> |
| <p>Policy AdministratorPolicy Service DefaultCPL: <S: 0,255></p> <p>The CPL used by the Expressway when the remote service is unavailable. Default: <code><reject status='403' reason='Service Unavailable' /></code></p> <p>Example: <code>xConfiguration Policy AdministratorPolicy Service DefaultCPL: "<reject status='403' reason='Service Unavailable' />"</code></p> |
| <p>Policy AdministratorPolicy Service Password: <S: 0,82></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 AdministratorPolicy Service Password: "password123"</code></p> |
| <p>Policy AdministratorPolicy Service Path: <S: 0,255></p> <p>Specifies the URL of the remote service.</p> <p>Example: <code>xConfiguration Policy AdministratorPolicy Service Path: "service"</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Policy AdministratorPolicy Service Protocol: <HTTP/HTTPS></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>Policy AdministratorPolicy Service Server [1..3] Address: <S: 0,128></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>Policy AdministratorPolicy Service Status Path: <S: 0..255></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>Policy AdministratorPolicy Service TLS CRLCheck Mode: <On/Off></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>Policy AdministratorPolicy Service TLS Verify Mode: <On/Off></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>Policy AdministratorPolicy Service UserName: <S: 0,30></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>Policy FindMe CallerID: <FindMeID/IncomingID></p> <p>Determines how the source of an incoming call is presented to the callee. Default: IncomingID.</p> <p><i>IncomingID</i>: displays the address of the endpoint from which the call was placed.</p> <p><i>FindMeID</i>: displays the FindMe ID associated with the originating endpoint's address.</p> <p>Example: <code>xConfiguration Policy FindMe CallerId: FindMeID</code></p> |
| <p>Policy FindMe Mode: <Off/On/ThirdPartyManager></p> <p>Configures how the FindMe application operates. Default: Off.</p> <p><i>Off</i>: disables FindMe.</p> <p><i>On</i>: enables FindMe.</p> <p><i>ThirdPartyManager</i>: uses an off-box, third-party FindMe manager.</p> <p>Example: <code>xConfiguration Policy FindMe Mode: On</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Policy FindMe Server Address: <S: 0, 128></p> <p>Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote FindMe Manager.</p> <p>Example: <code>xConfiguration Policy FindMe Server Address: "userpolicy.server.example.com"</code></p> |
| <p>Policy FindMe Server Password: <S: 0, 82></p> <p>Specifies the password used by the Expressway to log in and query the remote FindMe Manager. The maximum plaintext length is 30 characters, which will then be encrypted.</p> <p>Example: <code>xConfiguration Policy FindMe Server Password: "password123"</code></p> |
| <p>Policy FindMe Server Path: <S: 0, 255></p> <p>Specifies the URL of the remote FindMe Manager.</p> <p>Example: <code>xConfiguration Policy FindMe Server Path: "service"</code></p> |
| <p>Policy Services Service [1..20] DefaultCPL: <S: 0,255></p> <p>The CPL used by the Expressway when the remote service is unavailable. Default: <code><reject status='504' reason='Policy Service Unavailable' /></code></p> <p>Example: <code>xConfiguration Policy Services Service 1 DefaultCPL: "<reject status='403' reason='Service Unavailable' />"</code></p> |
| <p>Policy Services Service [1..20] Description: <S: 0,64></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>Policy Services Service [1..20] HTTPMethod: <POST/GET></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>Policy Services Service [1..20] Name: <S: 0,50></p> <p>Assigns a name to this Policy Service.</p> <p>Example: <code>xConfiguration Policy Services Service 1 Name: "Conference handler"</code></p> |
| <p>Policy Services Service [1..20] Password: <S: 0,82></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>Policy Services Service [1..20] Path: <S: 0,255></p> <p>Specifies the URL of the remote service.</p> <p>Example: <code>xConfiguration Policy Services Service 1 Path: "service"</code></p> |
| <p>Policy Services Service [1..20] Protocol: <HTTP/HTTPS></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Policy Services Service [1..20] Server [1..3] Address: <S: 0,128></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>Policy Services Service [1..20] Status Path: <S: 0..255></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>Policy Services Service [1..20] TLS CRLCheck Mode: <On/Off></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>Policy Services Service [1..20] TLS Verify Mode: <On/Off></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>Policy Services Service [1..20] UserName: <S: 0,30></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>QoS Audio <0..63></p> <p>Defines a DSCP (Differentiated Service Code Point) value for Quality of Service marking of audio traffic. The DSCP value is stamped (marked) onto SIP and H.323 audio media traffic routed through the Expressway, by writing it to the IP packet headers. To the ToS field for IPv4 or to the TC field for IPv6. A value of "0" specifies standard best effort service. Default: 46.</p> <p>You must restart the system for any changes to take effect.</p> <p>Example: <code>xConfiguration QoS Audio: 30</code></p> |
| <p>QoS Video <0..63></p> <p>Defines a DSCP value for Quality of Service marking of video traffic. The DSCP value is stamped (marked) onto SIP and H.323 video media traffic routed through the Expressway, by writing it to the IP packet headers. To the ToS field for IPv4 or to the TC field for IPv6. A value of "0" specifies standard best effort service. Default: 34.</p> <p>You must restart the system for any changes to take effect.</p> <p>Example: <code>xConfiguration QoS Video: 43</code></p> |
| <p>QoS XMPP <0..63></p> <p>Defines a DSCP value for Quality of Service marking of IM & Presence traffic. The DSCP value is stamped (marked) onto XMPP traffic routed through the Expressway, by writing it to the IP packet headers. To the ToS field for IPv4 or to the TC field for IPv6. A value of "0" specifies standard best effort service. Default: 24.</p> <p>You must restart the system for any changes to take effect.</p> <p>Example: <code>xConfiguration QoS XMPP: 34</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>QoS Signaling <0..63></p> <p>Defines a DSCP value for Quality of Service marking of signaling traffic. The DSCP value is stamped (marked) onto SIP and H.323 signaling traffic routed through the Expressway, by writing it to the IP packet headers. To the ToS field for IPv4 or to the TC field for IPv6. A value of "0" specifies standard best effort service. Default: 24.</p> <p>You must restart the system for any changes to take effect.</p> <p>Example: <code>xConfiguration QoS Signaling: 34</code></p> |
| <p>Registration AllowList [1..2500] Description: <S: 0,64></p> <p>A free-form description of the Allow List rule.</p> <p>Example: <code>xConfiguration Registration AllowList 1 Description: "Everybody at @example.com"</code></p> |
| <p>Registration AllowList [1..2500] Pattern String: <S: 0, 60></p> <p>Specifies an entry to be added to the Allow List. If one of an endpoint's aliases matches one of the patterns in the Allow List, the registration will be permitted.</p> <p>Example: <code>xConfiguration Registration AllowList 1 Pattern String: "john.smith@example.com"</code></p> |
| <p>Registration AllowList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex></p> <p>Specifies whether the entry in the Allow List is a prefix, suffix, regular expression, or must be matched exactly. Default: Exact.</p> <p><i>Exact:</i> the string must 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 will be treated as a regular expression.</p> <p>Example: <code>xConfiguration Registration AllowList 1 Pattern Type: Exact</code></p> |
| <p>Registration DenyList [1..2500] Description: <S: 0,64></p> <p>A free-form description of the Deny List rule.</p> <p>Example: <code>xConfiguration Registration DenyList 1 Description: "Anybody at @nuisance.com"</code></p> |
| <p>Registration DenyList [1..2500] Pattern String: <S: 0, 60></p> <p>Specifies an entry to be added to the Deny List. If one of an endpoint's aliases matches one of the patterns in the Deny List, the registration will not be permitted.</p> <p>Example: <code>xConfiguration Registration DenyList 1 Pattern String: "john.jones@example.com"</code></p> |
| <p>Registration DenyList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex></p> <p>Specifies whether the entry in the Deny List is a prefix, suffix, regular expression, or must be matched exactly. Default: Exact.</p> <p><i>Exact:</i> the string must 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 will be treated as a regular expression.</p> <p>Example: <code>xConfiguration Registration DenyList 1 Pattern Type: Exact</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Registration RestrictionPolicy Mode: <None/AllowList/DenyList/Directory/PolicyService></p> <p>Specifies the policy to be used when determining which endpoints may register with the system. Default: None.</p> <p><i>None</i>: no restriction.</p> <p><i>AllowList</i>: only endpoints attempting to register with an alias listed on the Allow List may register.</p> <p><i>DenyList</i>: all endpoints, except those attempting to register with an alias listed on the Deny List, may register.</p> <p><i>Directory</i>: only endpoints who register an alias listed in the local Directory, may register.</p> <p><i>PolicyService</i>: only endpoints who register with details allowed by the Policy Service, may register.</p> <p>Example: <code>xConfiguration Registration RestrictionPolicy Mode: None</code></p> |
| <p>Registration RestrictionPolicy Service DefaultCPL: <S: 0,255></p> <p>The CPL used by the Expressway when the remote service is unavailable. Default: <code><reject status='504' reason='Policy Service Unavailable' /></code></p> <p>Example: <code>xConfiguration Registration RestrictionPolicy Service DefaultCPL: "<reject status='403' reason='Service Unavailable' />"</code></p> |
| <p>Registration RestrictionPolicy Service Password: <S: 0,82></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 Registration RestrictionPolicy Service Password: "password123"</code></p> |
| <p>Registration RestrictionPolicy Service Path: <S: 0,255></p> <p>Specifies the URL of the remote service.</p> <p>Example: <code>xConfiguration Registration RestrictionPolicy Service Path: "service"</code></p> |
| <p>Registration RestrictionPolicy Service Protocol: <HTTP/HTTPS></p> <p>Specifies the protocol used to connect to the remote service. Default: HTTPS.</p> <p>Example: <code>xConfiguration Registration RestrictionPolicy Service Protocol: HTTPS</code></p> |
| <p>Registration RestrictionPolicy Service Server [1..3] Address: <S: 0,128></p> <p>Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.</p> <p>Example: <code>xConfiguration Registration RestrictionPolicy Service Server 1 Address: "192.168.0.0"</code></p> |
| <p>Registration RestrictionPolicy Service Status Path: <S: 0..255></p> <p>Specifies the path for obtaining the remote service status. Default: status</p> <p>Example: <code>xConfiguration Registration RestrictionPolicy Service Status Path: status</code></p> |
| <p>Registration RestrictionPolicy Service TLS CRLCheck Mode: <On/Off></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 Registration RestrictionPolicy Service TLS CRLCheck Mode: Off</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Registration RestrictionPolicy Service TLS Verify Mode: <On/Off></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 Registration RestrictionPolicy Service TLS Verify Mode: On</code></p> |
| <p>Registration RestrictionPolicy Service UserName: <S: 0,30></p> <p>Specifies the user name used by the Expressway to log in and query the remote service.</p> <p>Example: <code>xConfiguration Registration RestrictionPolicy Service UserName: "user123"</code></p> |
| <p>Remote Syslog [1..4] Address: <S: 0..128></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>Remote Syslog [1..4] Crlcheck: <On/Off></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>Remote Syslog [1..4] Format: <bsd/ietf></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> |
| <p>Remote Syslog [1..4] Loglevel: <emergency/alert/critical/error/warning/notice/informational/debug></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>Remote Syslog [1..4] Mode: <bsd/ietf/ietf_secure/user_defined></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>Remote Syslog [1..4] Port: <1..65535></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>Remote Syslog [1..4] Transport: <udp/tcp/tls></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>ResourceUsage Warning Activation Level: <0..100></p> <p>Controls if and when the Expressway will warn that it is approaching its maximum licensed capacity for calls or registrations. 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>SIP Advanced SipMaxSize: <1..1048576></p> <p>Specifies the maximum size of a SIP message that can be handled by the server (in bytes). Default: 32768</p> <p>Example: <code>xConfiguration SIP Advanced SipMaxSize: 32768</code></p> |
| <p>SIP Advanced SipTcpConnectTimeout: <1..150></p> <p>Enter the maximum number of seconds to wait for an outgoing SIP TCP connection to be established. Default: 10.</p> <p>Example: <code>xConfiguration SIP Advanced SipTcpConnectTimeout: 10</code></p> |
| <p>SIP Advanced SipTlsDhKeySize: <1024/2048/3072></p> <p>Specifies the default key size for inbound connections that use Diffie-Hellman key exchange (in bits). Default: 1024. Note: you must restart the system for any changes to take effect.</p> <p>Example: <code>xConfiguration SIP Advanced SipTlsDhKeySize: 1024</code></p> |
| <p>SIP Advanced SipTlsVersions: <TLSv1/TLSv1.1/TLSv1.2/TLSv1:TLSv1.1/TLSv1:TLSv1.2/TLSv1.1:TLSv1.2/TLSv1:TLSv1.1:TLSv1.2></p> <p>Specifies the supported SIP TLS protocol versions. Default: TLSv1:TLSv1.1:TLSv1.2</p> <p>Example: <code>xConfiguration SIP Advanced SipTlsVersions: TLSv1.1:TLSv1.2</code></p> |
| <p>SIP Authentication Digest Nonce ExpireDelta: <30..3600></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>SIP Authentication Digest Nonce Length: <32..512></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>SIP Authentication Digest Nonce Limit: <1..65535></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>SIP Authentication Digest Nonce Maximum Use Count: <1..1024></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>SIP Authentication NTLM Mode: <On/Off/Auto></p> <p>Controls when the Expressway will challenge endpoints using the NTLM protocol. Default: Auto.</p> <p><i>Off</i>: the Expressway will never send a challenge containing the NTLM protocol.</p> <p><i>On</i>: the Expressway will always include NTLM in its challenges.</p> <p><i>Auto</i>: the Expressway will decide based on endpoint type whether to challenge with NTLM.</p> <p>Example: <code>xConfiguration SIP Authentication NTLM Mode: Auto</code></p> |
| <p>SIP Authentication NTLM SA Lifetime: <30..43200></p> <p>Specifies the lifetime of NTLM security associations in seconds. Default: 28800.</p> <p>Example: <code>xConfiguration SIP Authentication NTLM SA Lifetime: 28800</code></p> |
| <p>SIP Authentication NTLM SA Limit: <1..65535></p> <p>Maximum number of NTLM security associations to store. Default: 10000.</p> <p>Example: <code>xConfiguration SIP Authentication NTLM SA Limit: 10000</code></p> |
| <p>SIP Authentication Retry Limit: <1..16></p> <p>The number of times a SIP UA will be challenged due to authentication failure before receiving a 403 Forbidden response. Note that this applies only to SIP Digest challenges (not NTLM challenges). Default: 3.</p> <p>Example: <code>xConfiguration SIP Authentication Retry Limit: 3</code></p> |
| <p>SIP Domain [1..200] Authzone: <S: 0,128></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>SIP Domain [1..200] Edge: <On/Off></p> <p>Whether remote and mobile collaboration features are enabled. Default Off.</p> <p>Example: <code>xConfiguration SIP Domain 1 Edge: On</code></p> |
| <p>SIP Domain [1..200] Name: <S: 0,128></p> <p>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".</p> <p>Example: <code>xConfiguration SIP Domain 1 Name: "100.example-name.com"</code></p> |
| <p>SIP Domain [1..200] Sip: <On/Off></p> <p>Specifies whether the Expressway will act as a SIP registrar for this domain, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes this domain. Default On.</p> <p>Example: <code>xConfiguration SIP Domain 1 Sip: On</code></p> |
| <p>SIP GRUU Mode: <On/Off></p> <p>Controls whether GRUU (RFC5627) support is active. Default: On.</p> <p>Example: <code>xConfiguration SIP GRUU Mode: On</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>SIP MediaRouting ICE Mode: <On/Off></p> <p>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.</p> <p>Example: <code>xConfiguration SIP MediaRouting ICE Mode: Off</code></p> |
| <p>SIP Mode: <On/Off></p> <p>Determines whether or not the Expressway will provide SIP registrar and SIP proxy functionality. Default: Off.</p> <p>Example: <code>xConfiguration SIP Mode: On</code></p> |
| <p>SIP Registration Call Remove: <Yes/No></p> <p>Specifies whether associated calls are dropped when a SIP registration expires or is removed. Default: No.</p> <p>Example: <code>xConfiguration SIP Registration Call Remove: No</code></p> |
| <p>SIP Registration Outbound Flow Timer: <0..600></p> <p>Specifies the value for the Flow-Timer header in Outbound registration responses. It defines the number of seconds after which the server will consider the registration flow to be dead if no keep-alive is sent by the user agent. Default: 0 (no header is added).</p> <p>Example: <code>xConfiguration SIP Registration Outbound Flow Timer: 0</code></p> |
| <p>SIP Registration Outbound Refresh Maximum: <30..7200></p> <p>The maximum allowed value for a SIP registration refresh period for Outbound registrations. Requests for a value greater than this will result in a lower value (calculated according to the Outbound registration refresh strategy) being returned. Default: 3600 seconds.</p> <p>Example: <code>xConfiguration SIP Registration Outbound Refresh Maximum: 3600</code></p> |
| <p>SIP Registration Outbound Refresh Minimum: <30..7200></p> <p>The minimum allowed value for a SIP registration refresh period for Outbound registrations. Requests for a value lower than this value will result in the registration being rejected with a 423 Interval Too Brief response. Default: 300 seconds.</p> <p>Example: <code>xConfiguration SIP Registration Outbound Refresh Minimum: 300</code></p> |
| <p>SIP Registration Outbound Refresh Strategy: <Maximum/Variable></p> <p>The method used to generate the SIP registration expiry period for Outbound registrations. Default: Variable.</p> <p><i>Maximum:</i> uses the lesser of the configured maximum refresh value and the value requested in the registration.</p> <p><i>Variable:</i> generates a random value between the configured minimum refresh value and the lesser of the configured maximum refresh value and the value requested in the registration.</p> <p>Example: <code>xConfiguration SIP Registration Outbound Refresh Strategy: Variable</code></p> |
| <p>SIP Registration Proxy Mode: <Off/ProxyToKnownOnly/ProxyToAny></p> <p>Specifies how proxied registrations should be handled. Default: Off.</p> <p><i>Off:</i> registration requests will not be proxied.</p> <p><i>ProxyToKnownOnly:</i> registration requests will be proxied to neighbors only.</p> <p><i>ProxyToAny:</i> registration requests will be proxied in accordance with the Expressway's existing call processing rules.</p> <p>Example: <code>xConfiguration SIP Registration Proxy Mode: Off</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>SIP Registration Standard Refresh Maximum: <30..7200></p> <p>The maximum allowed value for a SIP registration refresh period for standard registrations. Requests for a value greater than this will result in a lower value being returned. That value is calculated according to the standard registration refresh strategy. Default: 60 seconds.</p> <p>Example: <code>xConfiguration SIP Registration Standard Refresh Maximum: 60</code></p> |
| <p>SIP Registration Standard Refresh Minimum: <30..3600></p> <p>The minimum allowed value for a SIP registration refresh period for standard registrations. Requests for a value lower than this value will result in the registration being rejected with a 423 Interval Too Brief response. Default: 45 seconds.</p> <p>Example: <code>xConfiguration SIP Registration Standard Refresh Minimum: 45</code></p> |
| <p>SIP Registration Standard Refresh Strategy: <Maximum/Variable></p> <p>The method used to generate the SIP registration expiry period for standard registrations. Default: Maximum.</p> <p><i>Maximum:</i> uses the lesser of the configured maximum refresh value and the value requested in the registration.</p> <p><i>Variable:</i> generates a random value between the configured minimum refresh value and the lesser of the configured maximum refresh value and the value requested in the registration.</p> <p>Example: <code>xConfiguration SIP Registration Standard Refresh Strategy: Maximum</code></p> |
| <p>SIP Require Duo Video Mode: <On/Off></p> <p>Controls whether the Expressway requires the use of the com.tandberg.sdp.duo.enable extension for endpoints that support it. Default: On.</p> <p>Example: <code>xConfiguration SIP Require Duo Video Mode: On</code></p> |
| <p>SIP Require UDP BFCP Mode: <On/Off></p> <p>Controls whether the Expressway will require the use of the com.tandberg.udp.bfcp extension for endpoints that support it. Default: On.</p> <p>Example: <code>xConfiguration SIP Require UDP BFCP Mode: On</code></p> |
| <p>SIP Routes Route [1..20] Address: <S:0,39></p> <p>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.</p> <p>Example: <code>xConfiguration SIP Routes Route 1 Address: "127.0.0.1"</code></p> |
| <p>SIP Routes Route [1..20] Authenticated: <On/Off></p> <p>Whether to forward authenticated requests. Default: Off. Note: this command is intended for developer use only.</p> <p><i>On:</i> only forward requests along route if incoming message has been authenticated.</p> <p><i>Off:</i> always forward messages that match this route.</p> <p>Example: <code>xConfiguration SIP Routes Route 1 Authenticated: On</code></p> |
| <p>SIP Routes Route [1..20] Header Name: <S:0,64></p> <p>Name of SIP header field to match (e.g. Event). Note: this command is intended for developer use only.</p> <p>Example: <code>xConfiguration SIP Routes Route 1 Header Name: "Event"</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>SIP Routes Route [1..20] Header Pattern: <S:0,128></p> <p>Regular expression to match against the specified SIP header field. Note: this command is intended for developer use only.</p> <p>Example: <code>xConfiguration SIP Routes Route 1 Header Pattern: "(my-event-package) (.*)"</code></p> |
| <p>SIP Routes Route [1..20] Method: <S:0,64></p> <p>SIP method to match to select this route (e.g. INVITE, SUBSCRIBE). Note: this command is intended for developer use only.</p> <p>Example: <code>xConfiguration SIP Routes Route 1 Method: "SUBSCRIBE"</code></p> |
| <p>SIP Routes Route [1..20] Port: <1..65534></p> <p>Specifies the port on the next hop for this route to which matching SIP requests will be routed. Default: 5060. Note: this command is intended for developer use only.</p> <p>Example: <code>xConfiguration SIP Routes Route 1 Port: 22400</code></p> |
| <p>SIP Routes Route [1..20] Request Line Pattern: <S:0,128></p> <p>Regular expression to match against the SIP request line. Note: this command is intended for developer use only.</p> <p>Example: <code>xConfiguration SIP Routes Route 1 Request Line Pattern: ".*@(%localdomains% %ip%)"</code></p> |
| <p>SIP Routes Route [1..20] Tag: <S:0,64></p> <p>Tag value specified by external applications to identify routes that they create. Note: this command is intended for developer use only.</p> <p>Example: <code>xConfiguration SIP Routes Route 1 Tag: "Tag1"</code></p> |
| <p>SIP Routes Route [1..20] Transport: <UDP/TCP/TLS></p> <p>Determines which transport type will be used for SIP messages forwarded along this route. Default: TCP. Note: this command is intended for developer use only.</p> <p>Example: <code>xConfiguration SIP Routes Route 1 Transport: TCP</code></p> |
| <p>SIP Session Refresh Minimum: <90..7200></p> <p>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.</p> <p>Example: <code>xConfiguration SIP Session Refresh Minimum: 500</code></p> |
| <p>SIP Session Refresh Value: <90..86400></p> <p>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.</p> <p>Example: <code>xConfiguration SIP Session Refresh Value: 1800</code></p> |
| <p>SIP TCP Mode: <On/Off></p> <p>Determines whether incoming and outgoing SIP calls using the TCP protocol will be allowed. Default: Off.</p> <p>Example: <code>xConfiguration SIP TCP Mode: On</code></p> |
| <p>SIP TCP Outbound Port End: <1024..65534></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>SIP TCP Outbound Port Start: <1024..65534></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>SIP TCP Port: <1024..65534></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>SIP TLS Certificate Revocation Checking CRL Mode: <On/Off></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>SIP TLS Certificate Revocation Checking CRL Network Fetch Mode: <On/Off></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>SIP TLS Certificate Revocation Checking Mode: <On/Off></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>SIP TLS Certificate Revocation Checking OCSP Mode: <On/Off></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>SIP TLS Certificate Revocation Checking Source Inaccessibility Behavior: <Ignore/Fail></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>SIP TLS Mode: <On/Off></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>SIP TLS Port: <1024..65534></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 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>SIP UDP Mode: <On/Off></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>SIP UDP Port: <1024..65534></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>SNMP CommunityName: <S: 0, 16></p> <p>The Expressway's SNMP community name. Default: public</p> <p>Example: <code>xConfiguration SNMP CommunityName: "public"</code></p> |
| <p>SNMP SystemContact: <S: 0, 70></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>SNMP SystemLocation: <S: 0, 70></p> <p>The physical location of the system.</p> <p>Example: <code>xConfiguration SNMP SystemLocation: "Server Room 128"</code></p> |
| <p>SNMP V1Mode: <On/Off></p> <p>Enables or disables SNMP Version 1 support. Default: Off.</p> <p>Example: <code>Configuration SNMP V1Mode: Off</code></p> |
| <p>SNMP V2cMode: <On/Off></p> <p>Enables or disables SNMP Version 2c support. Default: On.</p> <p>Example: <code>xConfiguration SNMP V2cMode: On</code></p> |
| <p>SNMP V3AuthenticationMode: <On/Off></p> <p>Enables or disables SNMP Version 3 authentication. Default: On.</p> <p>Example: <code>xConfiguration SNMP V3AuthenticationMode: On</code></p> |
| <p>SNMP V3AuthenticationPassword: <S: 0,215></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>SNMP V3AuthenticationType: <MD5/SHA></p> <p>Sets SNMP Version 3 authentication type. Default: SHA.</p> <p>Example: <code>xConfiguration SNMP V3AuthenticationType: SHA</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>SNMP V3Mode: <On/Off></p> <p>Enables or disables SNMP Version 3 support. Default: On.</p> <p>Example: <code>xConfiguration SNMPV3 Mode: On</code></p> |
| <p>SNMP V3PrivacyMode: <On/Off></p> <p>Enables or disables SNMP Version 3 privacy. Default: On.</p> <p>Example: <code>xConfiguration SNMP V3PrivacyMode: On</code></p> |
| <p>SNMP V3PrivacyPassword: <S: 0,215></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> |
| <p>SNMP V3PrivacyType: <DES/AES></p> <p>Sets SNMP Version 3 privacy type. Default: AES.</p> <p>Example: <code>xConfiguration SNMP V3PrivacyType: AES</code></p> |
| <p>SNMP V3UserName: <S: 0,70></p> <p>Sets the username to use when using SNMP V3.</p> <p>Example: <code>xConfiguration SNMP V3UserName: "user123"</code></p> |
| <p>SystemUnit Maintenance Mode: <On/Off></p> <p>Sets the Expressway into maintenance mode. New calls and registrations are disallowed and existing calls and registrations are allowed to expire. Default: Off.</p> <p>Example: <code>xConfiguration SystemUnit Maintenance Mode: Off</code></p> |
| <p>SystemUnit Name: <S:, 0, 50></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>TimeZone Name: <S: 0, 64></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>Transform [1..100] Description: <S: 0,64></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Transform [1..100] Pattern Behavior: <Strip/Replace></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>Transform [1..100] Pattern Replace: <S: 0, 60></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>Transform [1..100] Pattern String: <S: 0, 60></p> <p>The pattern against which the alias is compared.</p> <p>Example: <code>xConfiguration Transform 1 Pattern String: "example.net"</code></p> |
| <p>Transform [1..100] Pattern Type: <Exact/Prefix/Suffix/Regex></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> |
| <p>Transform [1..100] Priority: <1..65534></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>Transform [1..100] State: <Enabled/Disabled></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>Traversal Media Port End: <1025..65533></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Traversal Media Port Start: <1024..65532></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>Traversal Server H323 Assent CallSignaling Port: <1024..65534></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>Traversal Server H323 H46018 CallSignaling Port: <1024..65534></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>Traversal Server TURN Authentication Realm: <S: 1,128></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>Traversal Server TURN Authentication Remote Mode: <On/Off></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>Traversal Server TURN Media Port End: <1024..65534></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>Traversal Server TURN Media Port Start: <1024..65534></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>Traversal Server TURN Mode: <On/Off></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> |
| <p>Traversal Server TURN Port: <443, 1024..65534></p> <p>The listening port for TURN requests. Default: 3478.</p> <p>Example: <code>xConfiguration Traversal Server TURN Port: 3478</code></p> |
| <p>Traversal Server TURN PortRangeEnd: <1024..65534></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Traversal Server TURN PortRangeStart: <1024..65534></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>Traversal Server TURN ProtocolMode: <TCP/UDP/Both></p> <p>The permitted protocols for TURN requests. Default: Both.</p> <p>Example: <code>xConfiguration Traversal Server TURN ProtocolMode: Both</code></p> |
| <p>XCP DelayedRestart EnableDelayedRestart: <On/Off></p> <p>Controls whether the Delayed Cisco XCP Router restart feature is enabled. Default: Off.</p> <p>Example: <code>xConfiguration DelayedRestart EnableDelayedRestart: On</code></p> |
| <p>XCP DelayedRestart EnableScheduledRestart: <On/Off></p> <p>Controls whether a scheduled restart of the Cisco XCP Router is enabled. Default: Off.</p> <p>Example: <code>xConfiguration XCP DelayedRestart EnableScheduledRestart: On</code></p> |
| <p>XCP DelayedRestart MultitenancyEnabled: <On/Off></p> <p>Turn on multitenancy to configure the delayed Cisco XCP Router restart. Default: Off.</p> <p>Example: <code>xConfiguration XCP DelayedRestart MultitenancyEnabled: On</code></p> |
| <p>XCP DelayedRestart ScheduledTime:</p> <p>The time each day that the scheduled restart takes place.</p> <p>Example: <code>xConfiguration XCP DelayedRestart ScheduledTime: 01.00</code></p> |
| <p>XCP DelayedRestartNotify RestartTime:</p> <p>Set the notification for the restart time.</p> <p>Example: <code>xConfiguration DelayedRestartNotify RestartTime: 01.00</code></p> |
| <p>XCP TLS Certificate CVS CertificateRevocationCheck: <On/Off></p> <p>Controls whether Certificate Revocation Lists (CRLs) are used to perform certificate revocation checking for XCP TLS connection. 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 as well as using OCSP. Default: Off.</p> <p>Example: <code>xConfiguration XCP TLS Certificate CVS CertificateRevocationCheck: Off</code></p> |
| <p>XCP TLS Certificate CVS ConvertIpToHostname: <On/Off></p> <p>Controls whether Expressway automatically converts XCP peer's IP address to FQDN for certificate verification. Default: On.</p> <p>Example: <code>xConfiguration XCP TLS Certificate CVS ConvertIpToHostname: On</code></p> |
| <p>XCP TLS Certificate CVS CrlNetworkFetchEnabled: <On/Off></p> <p>Controls whether the Expressway is allowed to download CRLs from the CDP URIs contained in its X.509 certificate. Default: On.</p> <p>Example: <code>xConfiguration XCP TLS Certificate CVS CrlNetworkFetchEnabled: On</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>XCP TLS Certificate CVS EnableCvs: <On/Off></p> <p>Controls whether or not to verify XCP peers' certificates during XCP TLS connection. When <i>off</i>, all other XCP TLS Certificate CVS configuration options will have no effect. Default: On.</p> <p>Example: <code>xConfiguration XCP TLS Certificate CVS EnableCvs: On</code></p> |
| <p>XCP TLS Certificate CVS FailOnInaccessibleSource: <On/Off></p> <p>Controls the certificate verification behavior if the revocation source cannot be contacted.</p> <p>On: treat the certificate as revoked (and thus do not allow the TLS connection). Off: treat the certificate as not revoked.</p> <p>Default: On.</p> <p>Example: <code>xConfiguration XCP TLS Certificate CVS FailOnInaccessibleSource: On</code></p> |
| <p>XCP TLS Certificate CVS UseCrl: <On/Off></p> <p>Controls whether Expressway checks its own CRL for revocation of certificates exchanged during establishment of XCP TLS connections. Default: On.</p> <p>Example: <code>xConfiguration XCP TLS Certificate CVS UseCrl: On</code></p> |
| <p>XCP TLS Certificate CVS UseOcsp: <On/Off></p> <p>Controls whether the Expressway can use OCSP to check if the certificate is revoked. 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 XCP TLS Certificate CVS UseOcsp: On</code></p> |
| <p>XCP TLS Certificate CVS VerifyHostname: <On/Off></p> <p>Controls whether the Expressway verifies the hostname from the XCP host's certificate against its own peer configuration. Default: On.</p> <p>Example: <code>xConfiguration XCP TLS Certificate CVS VerifyHostname: On</code></p> |
| <p>Zones DefaultZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials></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>Zones DefaultZone SIP Media Encryption Mode: <Off/On/BestEffort/Auto></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones DefaultZone SIP Multistream Mode: <Off/On></p> <p>Controls if the Expressway allows Multistream to and from devices in this zone. Default: On</p> <p><i>On:</i> allow Multistream</p> <p><i>Off:</i> disallow Multistream.</p> <p>Example: <code>xConfiguration Zones DefaultZone SIP Multistream Mode: Off</code></p> |
| <p>Zones DefaultZone SIP Record Route Address Type: <IP/Hostname></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>Zones DefaultZone SIP TLS Verify Mode: <On/Off></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>Zones LocalZone DefaultSubZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials></p> <p>Controls how the Expressway authenticates incoming messages from this subzone 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 LocalZone DefaultSubZone Authentication Mode: DoNotCheckCredentials</code></p> |
| <p>Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: <1..10000000></p> <p>The bandwidth limit (in kbps) for any one call to or from an endpoint in the Default Subzone (applies only if the mode is set to Limited). Default: 1920.</p> <p>Example: <code>xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: 1920</code></p> |
| <p>Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth></p> <p>Controls if there is a limit on the bandwidth for any one call to or from an endpoint in the Default Subzone. Default: Unlimited.</p> <p><i>NoBandwidth:</i> no bandwidth available. No calls can be made to or from the Default Subzone.</p> <p>Example: <code>xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: Limited</code></p> |
| <p>Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: <1..10000000></p> <p>The bandwidth limit (in kbps) for any one call between two endpoints within the Default Subzone (applies only if the mode is set to Limited). Default: 1920.</p> <p>Example: <code>xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: 1920</code></p> |
| <p>Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth></p> <p>Controls if there is a limit on the bandwidth for any one call between two endpoints within the Default Subzone. Default: Unlimited.</p> <p><i>NoBandwidth:</i> no bandwidth available. No calls can be made within the Default Subzone.</p> <p>Example: <code>xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: Limited</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones LocalZone DefaultSubZone Bandwidth Total Limit: <1..100000000></p> <p>Sets the total bandwidth limit (in kbps) of the Default Subzone (applies only if Mode is set to Limited). Default: 500000 .</p> <p>Example: <code>xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Limit: 500000</code></p> |
| <p>Zones LocalZone DefaultSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth></p> <p>Controls if the Default Subzone has a limit on the total bandwidth being used by its endpoints at any one time. Default: Unlimited.</p> <p><i>NoBandwidth</i>: no bandwidth available. No calls can be made to, from, or within the Default Subzone.</p> <p>Example: <code>xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: Limited</code></p> |
| <p>Zones LocalZone DefaultSubZone Registrations: <Allow/Deny></p> <p>Controls whether registrations assigned to the Default Subzone are accepted. Default: Allow.</p> <p>Example: <code>xConfiguration Zones LocalZone DefaultSubZone Registrations: Allow</code></p> |
| <p>Zones LocalZone DefaultSubZone SIP Media Encryption Mode: <Off/On/BestEffort/Auto></p> <p>The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this subzone. 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 LocalZone DefaultSubZone SIP Media Encryption Mode: Auto</code></p> |
| <p>Zones LocalZone DefaultSubZone SIP Multistream Mode: <Off/On></p> <p>Controls if the Expressway allows Multistream to and from devices in this zone. Default: On</p> <p><i>On</i>: allow Multistream</p> <p><i>Off</i>: disallow Multistream.</p> <p>Example: <code>xConfiguration Zones LocalZone DefaultSubZone SIP Multistream Mode: Off</code></p> |
| <p>Zones LocalZone SIP Record Route Address Type: <IP/Hostname></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>Zones LocalZone SubZones MembershipRules Rule [1..3000] Description: <S: 0,64></p> <p>A free-form description of the membership rule.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Description: "Office-based staff"</code></p> |
| <p>Zones LocalZone SubZones MembershipRules Rule [1..3000] Name: <S: 0,50></p> <p>Assigns a name to this membership rule.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Name: "Office Workers"</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Zones LocalZone SubZones MembershipRules Rule [1..3000] Pattern String: <S: 0,60></p> <p>Specifies the pattern against which the alias is compared.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Pattern String: "@example.com"</code></p> |
| <p>Zones LocalZone SubZones MembershipRules Rule [1..3000] Pattern Type: <Exact/Prefix/Suffix/Regex></p> <p>The way in which the pattern must match the alias.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Pattern Type: Suffix</code></p> |
| <p>Zones LocalZone SubZones MembershipRules Rule [1..3000] Priority: <1..65534></p> <p>Determines the order in which the rules are applied (and thus to which subzone the endpoint is assigned) if an endpoint's address satisfies multiple rules. The rules with the highest priority (1, then 2, then 3 and so on) are applied first. If multiple Subnet rules have the same priority the rule with the largest prefix length is applied first. Alias Pattern Match rules at the same priority are searched in configuration order. Default: 100.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Priority: 100</code></p> |
| <p>Zones LocalZone SubZones MembershipRules Rule [1..3000] State: <Enabled/Disabled></p> <p>Indicates if the membership rule is enabled or disabled. Disabled membership rules are ignored. Default: Enabled.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 State: Enabled</code></p> |
| <p>Zones LocalZone SubZones MembershipRules Rule [1..3000] SubZoneName: <S: 0,50></p> <p>The subzone to which an endpoint is assigned if its address satisfies this rule.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 SubZoneName: "Branch Office"</code></p> |
| <p>Zones LocalZone SubZones MembershipRules Rule [1..3000] Subnet Address: <S: 0,39></p> <p>Specifies an IP address used (in conjunction with the prefix length) to identify this subnet.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Subnet Address: "192.168.0.0"</code></p> |
| <p>Zones LocalZone SubZones MembershipRules Rule [1..3000] Subnet PrefixLength: <1..128></p> <p>The number of bits of the subnet address which must match for an IP address to belong in this subnet. Default: 32.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Subnet PrefixLength: 32</code></p> |
| <p>Zones LocalZone SubZones MembershipRules Rule [1..3000] Type: <Subnet/AliasPatternMatch></p> <p>The type of address that applies to this rule.</p> <p><i>Subnet:</i> assigns the device if its IP address falls within the configured IP address subnet.</p> <p><i>AliasPatternMatch:</i> assigns the device if its alias matches the configured pattern.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Type: Subnet</code></p> |
| <p>Zones LocalZone SubZones SubZone [1..1000] Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials></p> <p>Controls how the Expressway authenticates incoming messages from this subzone 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 the Administrator Guide for further information. Default: DoNotCheckCredentials.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones SubZone 1 Authentication Mode: DoNotCheckCredentials</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Inter Limit: <1..100000000></p> <p>The bandwidth limit (in kbps) on any one call to or from an endpoint in this subzone (applies only if Mode is set to Limited). Default: 1920.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Inter Limit: 1920</code></p> |
| <p>Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth></p> <p>Determines whether there is a limit on the bandwidth for any one call to or from an endpoint in this subzone. Default: Unlimited.</p> <p><i>NoBandwidth</i>: no bandwidth available. No calls can be made to or from this subzone.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Inter Mode: Limited</code></p> |
| <p>Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Intra Limit: <1..100000000></p> <p>The bandwidth limit (in kbps) for any one call between two endpoints within this subzone (applies only if the mode is set to Limited). Default: 1920.</p> <p>Example: <code>Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Intra Limit: 1920</code></p> |
| <p>Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth></p> <p>Determines whether there is a limit on the bandwidth for any one call between two endpoints within this subzone. Default: Unlimited.</p> <p><i>NoBandwidth</i>: no bandwidth available. No calls can be made within this subzone.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Intra Mode: Limited</code></p> |
| <p>Zones LocalZone SubZones SubZone [1..1000] Bandwidth Total Limit: <1..100000000></p> <p>Sets the total bandwidth limit (in kbps) of this subzone (applies only if the mode is set to Limited). Default: 500000.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth Total Limit: 500000</code></p> |
| <p>Zones LocalZone SubZones SubZone [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth></p> <p>Controls if this subzone has a limit on the total bandwidth of calls being used by its endpoints at any one time. Default: Unlimited.</p> <p><i>NoBandwidth</i>: no bandwidth available. No calls can be made to, from, or within this subzone.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth Total Mode: Limited</code></p> |
| <p>Zones LocalZone SubZones SubZone [1..1000] Name: <S: 0, 50></p> <p>Assigns a name to this subzone.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones SubZone 1 Name: "BranchOffice"</code></p> |
| <p>Zones LocalZone SubZones SubZone [1..1000] Registrations: <Allow/Deny></p> <p>Controls whether registrations assigned to this subzone are accepted. Default: Allow.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones SubZone 1 Registrations: Allow</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones LocalZone SubZones SubZone [1..1000] SIP Media Encryption Mode: <Off/On/BestEffort/Auto></p> <p>The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this subzone. 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 LocalZone SubZones SubZone 1 SIP Media Encryption Mode: Auto</code></p> |
| <p>Zones LocalZone SubZones SubZone [1..1000] SIP Multistream Mode: <Off/On></p> <p>Controls if the Expressway allows Multistream to and from devices in this zone. Default: On</p> <p><i>On:</i> allow Multistream</p> <p><i>Off:</i> disallow Multistream.</p> <p>Example: <code>xConfiguration Zones LocalZone SubZones Subzone 1 SIP Multistream Mode: Off</code></p> |
| <p>Zones LocalZone Traversal H323 Assent Mode: <On/Off></p> <p>Determines whether or not H.323 calls using Assent mode for firewall traversal will be allowed. Applies to traversal-enabled endpoints registered directly with the Expressway. Default: On .</p> <p>Example: <code>xConfiguration Zones LocalZone Traversal H323 Assent Mode: On</code></p> |
| <p>Zones LocalZone Traversal H323 H46018 Mode: <On/Off></p> <p>Controls whether H.323 calls using H460.18 mode for firewall traversal are allowed. Applies to traversal-enabled endpoints registered directly with the Expressway. Default: On .</p> <p>Example: <code>xConfiguration Zones LocalZone Traversal H323 H46018 Mode: On</code></p> |
| <p>Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: <On/Off></p> <p>Controls whether the Expressway operates in Demultiplexing mode for calls from traversal-enabled endpoints registered directly with it. Default: Off .</p> <p><i>On:</i> allows use of the same two ports for all calls.</p> <p><i>Off:</i> each call will use a separate pair of ports for media.</p> <p>Example: <code>xConfiguration Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: Off</code></p> |
| <p>Zones LocalZone Traversal H323 Preference: <Assent/H46018></p> <p>If an endpoint that is registered directly with the Expressway supports both Assent and H460.18 protocols, this setting determines which the Expressway uses. Default: Assent.</p> <p>Example: <code>xConfiguration Zones LocalZone Traversal H323 Preference: Assent</code></p> |
| <p>Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: <1..65534></p> <p>Sets the interval (in seconds) with which a traversal-enabled endpoint registered directly with the Expressway 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 .</p> <p>Example: <code>xConfiguration Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: 20</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Zones LocalZone Traversal H323 TCPProbe RetryCount: <1..65534></p> <p>Sets the number of times traversal-enabled endpoints registered directly with the Expressway will attempt to send a TCP probe. Default: 5 .</p> <p>Example: <code>xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryCount: 5</code></p> |
| <p>Zones LocalZone Traversal H323 TCPProbe RetryInterval: <1..65534></p> <p>Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the Expressway will send a TCP probe. Default: 2 .</p> <p>Example: <code>xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryInterval: 2</code></p> |
| <p>Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: <1..65534></p> <p>Sets the interval (in seconds) with which a traversal-enabled endpoint registered directly with the Expressway 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 .</p> <p>Example: <code>xConfiguration Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: 20</code></p> |
| <p>Zones LocalZone Traversal H323 UDPProbe RetryCount: <1..65534></p> <p>Sets the number of times traversal-enabled endpoints registered directly with the Expressway will attempt to send a UDP probe. Default: 5 .</p> <p>Example: <code>xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryCount: 5</code></p> |
| <p>Zones LocalZone Traversal H323 UDPProbe RetryInterval: <1..65534></p> <p>Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the Expressway will send a UDP probe. Default: 2 .</p> <p>Example: <code>xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryInterval: 2</code></p> |
| <p>Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: <1..100000000></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> |
| <p>Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth></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>Zones LocalZone TraversalSubZone Bandwidth Total Limit: <1..100000000></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones LocalZone TraversalSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth></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>Zones Policy Mode: <SearchRules/Directory></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>Zones Policy SearchRules Rule [1..2000] Authentication: <Yes/No></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>Zones Policy SearchRules Rule [1..2000] Description: <S: 0,64></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>Zones Policy SearchRules Rule [1..2000] Mode: <AliasPatternMatch/AnyAlias/AnyIPAddress></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>Zones Policy SearchRules Rule [1..2000] Name: <S: 0,50></p> <p>Descriptive name for the search rule.</p> <p>Example: <code>xConfiguration Zones Policy SearchRules Rule 1 Name: "DNS lookup"</code></p> |
| <p>Zones Policy SearchRules Rule [1..2000] Pattern Behavior: <Strip/Leave/Replace></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 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones Policy SearchRules Rule [1..2000] Pattern Replace: <S: 0,60></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>Zones Policy SearchRules Rule [1..2000] Pattern String: <S: 0,60></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>Zones Policy SearchRules Rule [1..2000] Pattern Type: <Exact/Prefix/Suffix/Regex></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>Zones Policy SearchRules Rule [1..2000] Priority: <1..65534></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>Zones Policy SearchRules Rule [1..2000] Progress: <Continue/Stop></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>Zones Policy SearchRules Rule [1..2000] Protocol: <Any/H323/SIP></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>Zones Policy SearchRules Rule [1..2000] Source Mode: <Any/AllZones/LocalZone/Named></p> <p>The sources of the requests for which this rule applies. Default: Any.</p> <p><i>Any:</i> locally registered devices, neighbor or traversal zones, and any non-registered devices.</p> <p><i>All zones:</i> locally registered devices plus neighbor or traversal zones.</p> <p><i>Local Zone:</i> locally registered devices only.</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> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Zones Policy SearchRules Rule [1..2000] Source Name: <S: 0..50></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>Zones Policy SearchRules Rule [1..2000] State: <Enabled/Disabled></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> |
| <p>Zones Policy SearchRules Rule [1..2000] Target Name: <S: 0,50></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>Zones Policy SearchRules Rule [1..2000] Target Type: <Zone/PolicyService></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>Zones Zone [1..1000] DNS IncludeAddressRecord: <On/Off></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>Zones Zone [1..1000] DNS 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></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>Zones Zone [1..1000] DNS Interworking SIP EmptyInviteAllowed: <On/Off></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>Zones Zone [1..1000] DNS Interworking SIP Video DefaultBitrate: <64..65535></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>Zones Zone [1..1000] DNS Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones Zone [1..1000] DNS Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA></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>Zones Zone [1..1000] DNS SIP Default Transport: <UDP/TCP/TLS></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>xConfiguration Zones Zone [1..1000] DNS SIP Media AesGcm Support: <Off/On></p> <p>Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. Default: Off.</p> <p>Example: <code>xConfiguration Zones Zone 1 DNS SIP Media AesGcm Support: On</code></p> |
| <p>Zones Zone [1..1000] DNS SIP Media Encryption Mode: <Off/On/BestEffort/Auto></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 Zone 1 DNS SIP Media Encryption Mode: Auto</code></p> |
| <p>Zones Zone [1..1000] DNS SIP Poison Mode: <On/Off></p> <p>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 .</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 1 DNS SIP Poison Mode: Off</code></p> |
| <p>Zones Zone [1..1000] DNS SIP PreloadedSipRoutes Accept: <Off/On></p> <p>Switch Preloaded SIP routes support On to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support Off if you want the zone to reject SIP INVITE requests containing this header.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On</code></p> |
| <p>Zones Zone [1..1000] DNS SIP Record Route Address Type: <IP/Hostname></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 1 DNS SIP Record Route Address Type: IP</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones Zone [1..1000] DNS SIP SearchAutoResponse: <On/Off></p> <p>Controls what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. Default: Off .</p> <p><i>Off:</i> a SIP OPTION message will be sent to the zone.</p> <p><i>On:</i> searches will be responded to automatically, without being forwarded to the zone.</p> <p>Example: <code>xConfiguration Zones Zone 1 DNS SIP SearchAutoResponse: Off</code></p> |
| <p>Zones Zone [1..1000] DNS SIP TLS Verify Mode: <On/Off></p> <p>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 .</p> <p>Example: <code>xConfiguration Zones Zone 1 DNS SIP TLS Verify Mode: On</code></p> |
| <p>Zones Zone [1..1000] DNS SIP TLS Verify Subject Name: <S: 0..128></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 1 DNS SIP TLS Verify Subject Name: "example.com"</code></p> |
| <p>Zones Zone [1..1000] DNS SIP UDP BFCP Filter Mode: <On/Off></p> <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. Default: Off .</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> <p>Example: <code>xConfiguration Zones Zone 1 DNS SIP UDP BFCP Filter Mode: Off</code></p> |
| <p>Zones Zone [1..1000] DNS ZoneProfile: <Default/Custom/CiscoUnifiedCommunicationsManager/CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDevice/LocalB2BUAService></p> <p>Determines how the zone's advanced settings are configured.</p> <p><i>Default:</i> uses the factory defaults.</p> <p><i>Custom:</i> allows you to configure each setting individually.</p> <p><i>Preconfigured profiles:</i> alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.</p> <p>Example: <code>xConfiguration Zones Zone 1 DNS ZoneProfile: Default</code></p> |
| <p>Zones Zone [1..1000] ENUM DNSSuffix: <S: 0, 128></p> <p>The DNS zone to append to the transformed E.164 number to create an ENUM host name which this zone is then queried for.</p> <p>Example: <code>xConfiguration Zones Zone 2 ENUM DNSSuffix: "e164.arpa"</code></p> |
| <p>Zones Zone [1..1000] H323 Mode: <On/Off></p> <p>Determines whether H.323 calls will be allowed to and from this zone. Default: On .</p> <p>Example: <code>xConfiguration Zones Zone 2 H323 Mode: On</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Zones Zone [1..1000] HopCount: <1..255></p> <p>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 .</p> <p>Example: <code>xConfiguration Zones Zone 2 HopCount: 15</code></p> |
| <p>Zones Zone [1..1000] Name: <S: 1, 50></p> <p>Assigns a name to this zone.</p> <p>Example: <code>xConfiguration Zones Zone 3 Name: "UK Sales Office"</code></p> |
| <p>Zones Zone [1..1000] Neighbor Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials></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 Zone 3 Neighbor Authentication Mode: DoNotCheckCredentials</code></p> |
| <p>Zones Zone [1..1000] Neighbor H323 CallSignaling Port: <1024..65534></p> <p>The port on the neighbor to use for H.323 calls to and from this Expressway. Default: 1720 .</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor H323 CallSignaling Port: 1720</code></p> |
| <p>Zones Zone [1..1000] Neighbor H323 Port: <1024..65534></p> <p>The port on the neighbor to use for H.323 searches to and from this Expressway. Default: 1719 .</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor H323 Port: 1719</code></p> |
| <p>Zones Zone [1..1000] Neighbor H323 SearchAutoResponse: <On/Off></p> <p>Determines what happens when the Expressway receives a H323 search, destined for this zone. Default: Off.</p> <p><i>Off:</i> an LRQ message will be sent to the zone.</p> <p><i>On:</i> searches will be responded to automatically, without being forwarded to the zone.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor H323 SearchAutoResponse: Off</code></p> |
| <p>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></p> <p>Specifies which audio codec to use when empty INVITES are not allowed. Default: G711u .</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor Interworking SIP Audio DefaultCodec: G711u</code></p> |
| <p>Zones Zone [1..1000] Neighbor Interworking SIP EmptyInviteAllowed: <On/Off></p> <p>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 .</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 3 Neighbor Interworking SIP EmptyInviteAllowed: On</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones Zone [1..1000] Neighbor Interworking SIP Encryption EncryptSRTCP: <Yes/No></p> <p>Controls if the Expressway offers encrypted SRTCP in calls to this zone. The Expressway will send an INFO request. Default: No.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor Interworking SIP Encryption EncryptSRTCP: No</code></p> |
| <p>Zones Zone [1..1000] Neighbor Interworking SIP Search Strategy: <Options/Info></p> <p>Determines how the Expressway will search for SIP endpoints when interworking an H.323 call. Default: Options .</p> <p><i>Options:</i> the Expressway will send an OPTIONS request.</p> <p><i>Info:</i> the Expressway will send an INFO request.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor Interworking SIP Search Strategy: Options</code></p> |
| <p>Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultBitrate: <64..65535></p> <p>Specifies which video bit rate to use when empty INVITEs are not allowed. Default: 384 .</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultBitrate: 384</code></p> |
| <p>Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264></p> <p>Specifies which video codec to use when empty INVITEs are not allowed. Default: H263 .</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultCodec: H263</code></p> |
| <p>Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA></p> <p>Specifies which video resolution to use when empty INVITEs are not allowed. Default: CIF .</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultResolution: CIF</code></p> |
| <p>Zones Zone [1..1000] Neighbor Monitor: <Yes/No></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor Monitor: Yes</code></p> |
| <p>Zones Zone [1..1000] Neighbor Peer [1..6] Address: <S:0,128></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor Peer 1 Address: "192.44.0.18"</code></p> |
| <p>Zones Zone [1..1000] Neighbor Registrations: <Allow/Deny></p> <p>Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow .</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor Registrations: Allow</code></p> |
| <p>Zones Zone [1..1000] Neighbor SIP Authentication Trust Mode: <On/Off></p> <p>Controls if authenticated SIP messages (ones containing a P-Asserted-Identity header) from this zone are trusted. Default: Off .</p> <p><i>On:</i> messages are trusted without further challenge.</p> <p><i>Off:</i> messages are challenged for authentication.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP Authentication Trust Mode: On</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Zones Zone [1..1000] Neighbor SIP B2BUA Service Identifier: <0..64></p> <p>The identifier that represents an instance of a local SIP Back-to-Back User Agent service.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP B2BUA Service Identifier: 1</code></p> |
| <p>Zones Zone [1..1000] Neighbor SIP ClassFiveResponseLiveness: <Yes/No></p> <p>Specifies whether Class 5 SIP responses from neighbor peers result in the zone being considered alive for use. Default: Yes.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP ClassFiveResponseLiveness: Yes</code></p> |
| <p>Zones Zone [1..1000] Neighbor SIP Encryption Mode: <Auto/Microsoft/Off></p> <p>Determines how the Expressway handles encrypted SIP calls on this zone. Default: Auto.</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>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP Encryption Mode: Auto</code></p> |
| <p>Zones Zone [1..1000] Neighbor SIP MIME Strip Mode: <On/Off></p> <p>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 .</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP MIME Strip Mode: Off</code></p> |
| <p>xConfiguration Zones Zone [1..1000] Neighbor SIP Media AesGcm Support: <Off/On></p> <p>Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. Default: Off.</p> <p>Example: <code>xConfiguration Zones Zone 1 Neighbor SIP Media AesGcm Support: On</code></p> |
| <p>Zones Zone [1..1000] Neighbor SIP Media Encryption Mode: <Off/On/BestEffort/Auto></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 Zone 3 Neighbor SIP Media Encryption Mode: Auto</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones Zone [1..1000] Neighbor SIP MediaRouting Mode: <Auto/Signaled/Latching></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>Zones Zone [1..1000] Neighbor SIP Multistream Mode: <Off/On></p> <p>Controls if the Expressway allows Multistream to and from devices in this zone. Default: On</p> <p><i>On:</i> allow Multistream</p> <p><i>Off:</i> disallow Multistream.</p> <p>Example: <code>xConfiguration Zones Zone 1 Neighbor SIP Multistream Mode: Off</code></p> |
| <p>Zones Zone [1..1000] Neighbor SIP Poison Mode: <On/Off></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>Zones Zone [1..1000] Neighbor SIP Port: <1024..65534></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>Zones Zone [1..1000] Neighbor SIP PreloadedSipRoutes Accept: <Off/On></p> <p>Switch Preloaded SIP routes support On to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support Off if you want the zone to reject SIP INVITE requests containing this header.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On</code></p> |
| <p>Zones Zone [1..1000] Neighbor SIP ProxyRequire Strip List: <S: 0,255></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> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones Zone [1..1000] Neighbor SIP RFC3327 Enabled: <Yes/No></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>Note: In version X8.9 we introduced a toggle that controls this feature for the automatically created neighbor zones used for MRA. In that version, on those zones, the default is No. See <code>xConfiguration CollaborationEdge RFC3327Enabled</code>.</p> |
| <p>Zones Zone [1..1000] Neighbor SIP Record Route Address Type: <IP/Hostname></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>Zones Zone [1..1000] Neighbor SIP SearchAutoResponse: <On/Off></p> <p>Controls what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. Default: Off .</p> <p><i>Off:</i> a SIP OPTION message will be sent to the zone.</p> <p><i>On:</i> searches will be responded to automatically, without being forwarded to the zone.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP SearchAutoResponse: Off</code></p> |
| <p>Zones Zone [1..1000] Neighbor SIP TLS Verify Mode: <On/Off></p> <p>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 .</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP TLS Verify Mode: On</code></p> |
| <p>Zones Zone [1..1000] Neighbor SIP Transport: <UDP/TCP/TLS></p> <p>Determines which transport type will be used for SIP calls to and from this neighbor. Default: TLS .</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP Transport: TLS</code></p> |
| <p>Zones Zone [1..1000] Neighbor SIP UDP BFCP Filter Mode: <On/Off></p> <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. Default: Off .</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> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP UDP BFCP Filter Mode: Off</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>xConfiguration Zones Zone 1 Neighbor SIP UDP IX Filter Mode: <On/Off></p> <p>Determines whether INVITE requests sent to this zone filter out UDP/UDT/IX or UDP/DTLS/UDT/IX.</p> <p>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. Default: Off.</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>Example: <code>xConfiguration Zones Zone 1 neighbor SIP UDP IX Filter Mode: On</code></p> |
| <p>Zones Zone [1..1000] Neighbor SIP UPDATE Strip Mode: <On/Off></p> <p>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 .</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP UPDATE Strip Mode: Off</code></p> |
| <p>Zones Zone [1..1000] Neighbor SignalingRouting Mode: <Auto/Always></p> <p>Specifies how the Expressway handles the signaling for calls to and from this neighbor. Default: Auto.</p> <p><i>Auto:</i> Signaling will be taken as determined by the Call Routed Mode configuration.</p> <p><i>Always:</i> Signaling will always be taken for calls to or from this neighbor, regardless of the Call Routed Mode configuration.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SignalingRouting Mode: Auto</code></p> |
| <p>Zones Zone [1..1000] Neighbor ZoneProfile: <Default/Custom/CiscoUnifiedCommunicationsManager/CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDevice/LocalB2BUAService></p> <p>Determines how the zone's advanced settings are configured.</p> <p><i>Default:</i> uses the factory defaults.</p> <p><i>Custom:</i> allows you to configure each setting individually.</p> <p><i>Preconfigured profiles:</i> alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor ZoneProfile: Default</code></p> |
| <p>Zones Zone [1..1000] SIP Mode: <On/Off></p> <p>Determines whether SIP calls will be allowed to and from this zone. Default: On.</p> <p>Example: <code>xConfiguration Zones Zone 3 SIP Mode: On</code></p> |
| <p>Zones Zone [1..1000] TraversalClient Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials></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 Zone 4 TraversalClient Authentication Mode: DoNotCheckCredentials</code></p> |
| <p>Zones Zone [1..1000] TraversalClient Authentication Password: <S: 0,215></p> <p>The password used by the Expressway when connecting to the traversal server. The maximum plaintext length is 128 characters, which is then encrypted.</p> <p>Example: <code>xConfiguration Zones Zone 4 TraversalClient Authentication Password: "password123"</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones Zone [1..1000] TraversalClient Authentication UserName: <S: 0,128></p> <p>The user name used by the Expressway when connecting to the traversal server.</p> <p>Example: <code>xConfiguration Zones Zone 4 TraversalClient Authentication UserName: "clientname"</code></p> |
| <p>Zones Zone [1..1000] TraversalClient H323 Port: <1024..65534></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 4 TraversalClient H323 Port: 2777</code></p> |
| <p>Zones Zone [1..1000] TraversalClient H323 Protocol: <Assent/H46018></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 4 TraversalClient H323 Protocol: Assent</code></p> |
| <p>Zones Zone [1..1000] TraversalClient Peer [1..6] Address: <S:0,128></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 4 TraversalClient Peer 1 Address: "10.192.168.1"</code></p> |
| <p>Zones Zone [1..1000] TraversalClient Registrations: <Allow/Deny></p> <p>Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow.</p> <p>Example: <code>xConfiguration Zones Zone 4 TraversalClient Registrations: Allow</code></p> |
| <p>Zones Zone [1..1000] TraversalClient RetryInterval: <1..65534></p> <p>The interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. Default: 120.</p> <p>Example: <code>xConfiguration Zones Zone 4 TraversalClient RetryInterval: 120</code></p> |
| <p>xConfiguration Zones Zone [1..1000] TraversalClient SIP Media AesGcm Support: <Off/On></p> <p>Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. Default: Off.</p> <p>Example: <code>xConfiguration Zones Zone 1 TraversalClient SIP Media AesGcm Support: On</code></p> |
| <p>Zones Zone [1..1000] TraversalClient SIP Media Encryption Mode: <Off/On/BestEffort/Auto></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 Zone 4 TraversalClient SIP Media Encryption Mode: Auto</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones Zone [1..1000] TraversalClient SIP Multistream Mode: <Off/On></p> <p>Controls if the Expressway allows Multistream to and from devices in this zone. Default: On</p> <p><i>On:</i> allow Multistream</p> <p><i>Off:</i> disallow Multistream.</p> <p>Example: <code>xConfiguration Zones Zone 1 TraversalClient SIP Multistream Mode: Off</code></p> |
| <p>Zones Zone [1..1000] TraversalClient SIP Poison Mode: <On/Off></p> <p>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 .</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 4 TraversalClient SIP Poison Mode: Off</code></p> |
| <p>Zones Zone [1..1000] TraversalClient SIP Port: <1024..65534></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 4 TraversalClient SIP Port: 5061</code></p> |
| <p>Zones Zone [1..1000] TraversalClient SIP PreloadedSipRoutes Accept: <Off/On></p> <p>Switch Preloaded SIP routes support On to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support Off if you want the zone to reject SIP INVITE requests containing this header.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On</code></p> |
| <p>Zones Zone [1..1000] TraversalClient SIP Protocol: <Assent/TURN/ICE></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 4 TraversalClient SIP Protocol: Assent</code></p> |
| <p>Zones Zone [1..1000] TraversalClient SIP TLS Verify Mode: <On/Off></p> <p>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 .</p> <p>Example: <code>xConfiguration Zones Zone 4 TraversalClient SIP TLS Verify Mode: On</code></p> |
| <p>Zones Zone [1..1000] TraversalClient SIP Transport: <TCP/TLS></p> <p>Determines which transport type will be used for SIP calls to and from the traversal server. Default: TLS .</p> <p>Example: <code>xConfiguration Zones Zone 4 TraversalClient SIP Transport: TLS</code></p> |
| <p>Zones Zone [1..1000] TraversalServer Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials></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 Zone 5 TraversalServer Authentication Mode: DoNotCheckCredentials</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Zones Zone [1..1000] TraversalServer Authentication UserName: <S: 0,128></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer Authentication UserName: "User123"</code></p> |
| <p>Zones Zone [1..1000] TraversalServer H323 H46019 Demultiplexing Mode: <On/Off></p> <p>Determines whether the Expressway will operate in demultiplexing mode for calls from the traversal client. Default: Off .</p> <p><i>On</i>: allows use of the same two ports for all calls.</p> <p><i>Off</i>: each call will use a separate pair of ports for media.</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer H323 H46019 Demultiplexing Mode: Off</code></p> |
| <p>Zones Zone [1..1000] TraversalServer H323 Port: <1024..65534></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer H323 Port: 2777</code></p> |
| <p>Zones Zone [1..1000] TraversalServer H323 Protocol: <Assent/H46018></p> <p>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 .</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer H323 Protocol: Assent</code></p> |
| <p>Zones Zone [1..1000] TraversalServer Registrations: <Allow/Deny></p> <p>Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow .</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer Registrations: Allow</code></p> |
| <p>xConfiguration Zones Zone [1..1000] TraversalServer SIP Media AesGcm Support: <Off/On></p> <p>Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. Default: Off.</p> <p>Example: <code>xConfiguration Zones Zone 1 TraversalServer SIP Media AesGcm Support: On</code></p> |
| <p>Zones Zone [1..1000] TraversalServer SIP Media Encryption Mode: <Off/On/BestEffort/Auto></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 Zone 5 TraversalServer SIP Media Encryption Mode: Auto</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|---|
| <p>Zones Zone [1..1000] TraversalServer SIP Multistream Mode: <Off/On></p> <p>Controls if the Expressway allows Multistream to and from devices in this zone. Default: On</p> <p><i>On:</i> allow Multistream</p> <p><i>Off:</i> disallow Multistream.</p> <p>Example: <code>xConfiguration Zones Zone 1 TraversalServer SIP Multistream Mode: Off</code></p> |
| <p>Zones Zone [1..1000] TraversalServer SIP Poison Mode: <On/Off></p> <p>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 .</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 5 TraversalServer SIP Poison Mode: Off</code></p> |
| <p>Zones Zone [1..1000] TraversalServer SIP Port: <1024..65534></p> <p>The port on the Expressway being used for SIP firewall traversal from this traversal client. Default: 7001, incrementing by 1 for each new zone.</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer SIP Port: 5061</code></p> |
| <p>Zones Zone [1..1000] TraversalServer SIP PreloadedSipRoutes Accept: <Off/On></p> <p>Switch Preloaded SIP routes support On to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support Off if you want the zone to reject SIP INVITE requests containing this header.</p> <p>Example: <code>xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On</code></p> |
| <p>Zones Zone [1..1000] TraversalServer SIP Protocol: <Assent/TURN/ICE></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer SIP Protocol: Assent</code></p> |
| <p>Zones Zone [1..1000] TraversalServer SIP TLS Verify Mode: <On/Off></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Mode: On</code></p> |
| <p>Zones Zone [1..1000] TraversalServer SIP TLS Verify Subject Name: <S: 0,128></p> <p>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).</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Subject Name: "myclientname"</code></p> |
| <p>Zones Zone [1..1000] TraversalServer SIP Transport: <TCP/TLS></p> <p>Determines which of the two transport types will be used for SIP calls between the traversal client and Expressway. Default: TLS .</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer SIP Transport: TLS</code></p> |

Table 43 xConfiguration CLI reference (continued)

| |
|--|
| <p>Zones Zone [1..1000] TraversalServer TCPProbe KeepAliveInterval: <1..65534></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer TCPProbe KeepAliveInterval: 20</code></p> |
| <p>Zones Zone [1..1000] TraversalServer TCPProbe RetryCount: <1..65534></p> <p>Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway. Default: 5 .</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryCount: 5</code></p> |
| <p>Zones Zone [1..1000] TraversalServer TCPProbe RetryInterval: <1..65534></p> <p>Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway. Default: 2 .</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryInterval: 2</code></p> |
| <p>Zones Zone [1..1000] TraversalServer UDPProbe KeepAliveInterval: <1..65534></p> <p>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.</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer UDPProbe KeepAliveInterval: 20</code></p> |
| <p>Zones Zone [1..1000] TraversalServer UDPProbe RetryCount: <1..65534></p> <p>Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway. Default: 5.</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryCount: 5</code></p> |
| <p>Zones Zone [1..1000] TraversalServer UDPProbe RetryInterval: <1..65534></p> <p>Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway. Default: 2.</p> <p>Example: <code>xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryInterval: 2</code></p> |
| <p>Zones Zone [1..1000] Type: <Neighbor/TraversalClient/TraversalServer/ENUM/DNS></p> <p>Determines the nature of the specified zone, in relation to the local Expressway.</p> <p><i>Neighbor</i>: the new zone will be a neighbor of the local Expressway.</p> <p><i>TraversalClient</i>: there is a firewall between the zones, and the local Expressway is a traversal client of the new zone.</p> <p><i>TraversalServer</i>: there is a firewall between the zones and the local Expressway is a traversal server for the new zone.</p> <p><i>ENUM</i>: the new zone contains endpoints discoverable by ENUM lookup.</p> <p><i>DNS</i>: the new zone contains endpoints discoverable by DNS lookup.</p> <p>Example: <code>xConfiguration Zones Zone 3 Type: Neighbor</code></p> |

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. In this example the value must be in the range 0 to 63. |
| <S: 7,15> | An S 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 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 Of 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:

AdminAccountAdd

Adds a local administrator account.

Name(r): <S: 0, 128>

The username for this account.

Password(r): <Password>

The password for this account.

AccessAPI: <On/Off>

Whether this account is allowed to access the system's status and configuration via the API. Default: On.

AccessWeb: <On/Off>

Whether this account is allowed to log in to the system using the web interface. Default: On.

Enabled: <On/Off>

Indicates if the account is enabled or disabled. Access is denied to disabled accounts. Default: On.

Example: `xCommand AdminAccountAdd Name: "bob_smith" Password: "abcXYZ_123" AccessAPI: On AccessWeb: On Enabled: On`

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"`

AllowListAdd

Adds an entry to the Allow List.

PatternString(r): <S: 1, 60>

Specifies an entry to be added to the Allow List. If one of an endpoint's aliases matches one of the patterns in the Allow List, the registration will be permitted.

PatternType: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Allow List is a prefix, suffix, regular expression, or must be matched exactly. *Exact*: the string must 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 will be treated as a regular expression.
Default: Exact.

Description: <S: 0,64>

A free-form description of the Allow List rule.

Example: `xCommand AllowListAdd PatternString: "John.Smith@example.com" PatternType: Exact Description: "Allow John Smith"`

AllowListDelete

Deletes an entry from the Allow List.

AllowListId(r): <1..2500>

The index of the entry to be deleted.

Example: `xCommand AllowListDelete AllowListId: 2`

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`

ClusterAddressMappingAdd

Fqdn(r): <Value>

IpAddress(r): <Value>

Adds an FQDN/IP mapping entry to the cluster address mapping table.

ClusterAddressMappingDelete

Fqdn(r): <Value>

IpAddress(r): <Value>

Deletes an FQDN/IP mapping entry from the cluster address mapping table.

Cmsadd

Manage Cisco Meeting Server web bridges. Add a Guest account client URI

Name: <Value>

Example: `xCommand Cmsadd name: "join.example.com"`

Cmsdelete

Manage Cisco Meeting Server web bridges. Delete a Guest account client URI

Name: <Value>

Example: `xCommand Cmsdelete name: "join.example.com"`

CredentialAdd

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.

The maximum plaintext length is 128 characters, which will then be encrypted.

Example: `xCommand CredentialAdd Name: "alice" Password: "abcXYZ_123"`

CredentialDelete

Deletes an entry from the local authentication database.

Name(r): <String>

The name of the entry to delete.

Example: `xCommand CredentialDelete Name: "alice"`

Cucmconfigadd

Performs a lookup on a Unified CM publisher.

Address(r): <Value>

The FQDN or IP address of the Unified CM publisher.

Axlpwrd(r): <Value>

The password used by the Expressway to access the Unified CM publisher.

Axlusername(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" Axlpwrd: "xyz" Axlusername: "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"`

Cucmixedmodecheck

Address(r): <Value>

The FQDN or IP address of the Unified CM publisher.

AxIpassword(r): <Value>

The password used by the Expressway to access the Unified CM publisher.

AxIusername(r): <Value>

The user name used by the Expressway to access the Unified CM publisher.

DefaultLinksAdd

Restores links between the Default Subzone, Traversal Subzone and the Default Zone.

This command has no parameters.

Example: `xCommand DefaultLinksAdd`

DefaultValuesSet

Resets system parameters to default values. Level 1 resets most configuration items to their default value, with the exception of the Level 2 and Level 3 items. Level 2 resets configuration items related to remote authentication, plus Level 1 items to their default value. Level 3 resets all critical configuration items, plus Level 1 and Level 2 items to their default value.

Level(r): <1..3>

The level of system parameters to be reset.

Example: `xCommand DefaultValuesSet Level: 1`

DenyListAdd

Adds an entry to the Deny List.

PatternString(r): <S: 1, 60>

Specifies an entry to be added to the Deny List. If one of an endpoint's aliases matches one of the patterns in the Deny List, the registration will not be permitted.

PatternType: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Deny List is a prefix, suffix, regular expression, or must be matched exactly. *Exact*: the string must 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 will be treated as a regular expression.
Default: Exact.

Description: <S: 0, 64>

A free-form description of the Deny List rule.

Example: `xCommand DenyListAdd PatternString: "sally.jones@example.com" PatternType: exact Description: "Deny Sally Jones"`

DenyListDelete

Deletes an entry from the Deny List.

DenyListId(r): <1..2500>

The index of the entry to be deleted.

Example: `xCommand DenyListDelete DenyListId: 2`

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.

Sip: <On/Off>

Controls whether the Expressway is authoritative for this domain. The Expressway acts as a SIP registrar for the domain, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes this domain. Default: On.

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 Sip: On`

DomainDelete

Deletes a domain.

DomainId(r): <1..200>

The index of the domain to be deleted.

Example: `xCommand DomainDelete DomainId: 2`

Domaincerts

Manage multidomain certificates for Server Name Indication (SNI).

Each Domaincerts xCommand requires a 'command' parameter specifying an operation to be performed, followed by any additional parameters required for the specific command.

Domaincerts commands and associated parameters:

domain_list: Lists domains for which certificates are managed for SNI.

parameters: (none)

Example: `xCommand Domaincerts command: domain_list`

domain_create: Creates a new domain for managing certificates for SNI.

parameters: domain

Example: `xCommand domaincerts command: domain_create domain: a.com`

domain_delete: Deletes the specified certificate domain.

parameters: domain

Example: `xCommand domaincerts command: domain_delete domain: a.com`

is_csr_pending: Returns true if a certificate signing request is pending for the domain.

parameters: domain

Example: `xCommand domaincerts command: is_csr_pending domain: a.com`

csr_create: Creates a certificate signing request for a domain.

parameters: domain, subjectfields, sans, digestalgorithm, keysize

Example: `xCommand domaincerts command: csr_create domain: a.com keysize: 4096 digestalgorithm: sha256 sans: 'DNS:host1.a.com, DNS:host2.a.com' subjectfields: '{ "CN": "www.a.com", "C": "US", "ST": "North Carolina", "L": "RTP", "O": "a", "OU": "example org unit", "emailAddress": "admin@a.com" }'`

Notes:

- xCommand parameter values can be contained in single quotes so that space can be included.
- sans is an optional, comma-separated list of hostnames, each hostname prefixed by 'DNS:', see RFC5280.
- subjectfields is a JSON object containing a list of name: value pairs for each Subject Name field, see RFC5280.
- JSON names and values must be contained in double quotes as shown.
- keysize is the length in bits of the private key generated for the CSR.
- digestalgorithm is the name of the message digest algorithm used to sign the CSR, see 'openssl dgst'.

csr_get: Returns a pending certificate signing request in PEM format.

parameters: domain

Example: `xCommand domaincerts command: csr_get domain: a.com`

csr_delete: Deletes a pending certificate signing request.

parameters: domain

Example: `xCommand domaincerts command: csr_delete domain: a.com`

is_cert_set: Returns true if a certificate has been set for the domain.

parameters: domain

Example: `xCommand domaincerts command: is_cert_set domain: a.com`

cert_put: Uploads a certificate and private key.

parameters: domain, certpath, keypath

Example: `xCommand domaincerts command: cert_put domain: a.com certpath: /tmp/cert.pem keypath: /tmp/key.pem`

Notes:

- When a certificate and key have not been uploaded yet, both must be specified.
- When a certificate signing request is in progress, only a certificate can be uploaded.

cert_get: Returns a domain's certificate in PEM format.

parameters: domain

Example: `xCommand domaincerts command: cert_get domain: a.com`

cert_delete: Deletes a domain's certificate and private key.

parameters: domain

Example: `xCommand domaincerts command: cert_delete domain: a.com`

default command help:"

Certpath: <String>

Command: <domain_list/domain_create/domain_delete/csr_create/csr_get/csr_delete/cert_put/cert_get/cert_delete/is_csr_pending/is_cert_set>

Digestalgorithm: </sha256/sha384/sha512>

Domain: <String>

Keypath: <String>

Keysize: <Value>

Sans: <String>

Subjectfields: <String>

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"`

FindRegistration

Returns information about the registration associated with the specified alias. The alias must be registered on the Expressway on which the command is issued.

Alias(r): <S: 1, 60>

The alias that you wish to find out about.

Example: `xCommand FindRegistration Alias: "john.smith@example.com"`

ForceConfigUpdate

Forces the relevant configuration on this peer to be updated to match that of the cluster primary.

This command has no parameters.

Example: `xCommand ForceConfigUpdate`

Reference Material

Httpallowlistexport

Export the HTTP allow list rules in CSV format from the database.

File: <S>

Specifies the path to a file where the rules will get exported in CSV format.

Deployment: <S>

Use with URL to specify which of your deployments uses this rule. Not required unless you have multiple deployments. If you have multiple deployments, the rule will use the default deployment if you don't specify the deployment.

Httpallowlistexporttest

Export the HTTP allow list tests in CSV format from the database.

File: <S>

Specifies the path to a file where the tests will get exported in CSV format.

Deployment: <S>

Use with URL to specify which of your deployments uses this test. Not required unless you have multiple deployments. If you have multiple deployments, the rule will use the default deployment if you don't specify the deployment.

HTTPAllowListRuleAdd

Adds one or more rules to the HTTP allow list. You must specify at least URL or URLFile.

URL(r): <S>

Specifies the URL of a resource that HTTP clients will be allowed to access. IPv6 addresses must use RFC 2732 format.

For example: `https://[2001:DB8::1]:8443/path` or `https://www.example.com:8443/resource`

Do not supply URL if you are supplying URLFile.

URL must contain the protocol, either `http://` or `https://`, and the hostname. It should also contain domain, port, and path to make the URL more specific. If you omit some portions of the URL, Expressway will supply its defaults. eg. `http://hostname` allows clients to access to everything included by `http://hostname.SystemDNSDomain:80`. The default ports are 80 for http and 443 for https.

URLFile(r): <S>

Specifies the path to a CSV file that contains multiple rules. See [Allow List Rules File Reference, page 382](#).

Do not supply URLFile if you are supplying URL.

MatchType: <exact/starts-with/startswith/prefix>

Use with URL to specify whether the rule matches exactly what is in URL, or uses it as a base for a prefix match. Defaults to **exact** if not supplied. The other options are all equivalent.

Deployment: <S: "Your Deployment 1"/"Your Deployment 2">

Use with URL to specify which of your deployments uses this rule. Not required unless you have multiple deployments. If you have multiple deployments, the rule will use the default deployment if you don't specify the deployment.

Description: <S:128>

A text description of the rule.

HttpMethods: <OPTIONS/GET/HEAD/POST/PUT/DELETE>

A comma-delimited set of methods to allow with this rule. If you do not specify the methods, the rule will use the default methods configured on **Configuration > Unified Communications > HTTP allow list > Editable inbound rules**.

Example 1: `xCommand HTTPAllowListRuleAdd URLfile: "/tmp/rules.csv"`

Example 2: `xCommand HTTPAllowListRuleAdd URL: "https://cucm2.example.com:8443/partial/path"`

`MatchType: starts-with Description: "https access to read everything below partial/path/ on cucm2.example.com" HttpMethods: "OPTIONS,GET"`

HTTPAllowListRuleDelete

Deletes one or more rules from the HTTP allow list. You must specify at least URL or URLFile. You may need to specify other parameters if you have multiple rules for a single host.

URL(r): <S>

Specifies the URL of the rule you are deleting.

Do not supply URL if you are supplying URLFile.

URL must contain the protocol, either `http://` or `https://`, and the hostname. It should also contain domain, port, and path to make the URL more specific. If you omit some portions of the URL, Expressway will supply its defaults. eg. `http://hostname` will delete the rule `http://hostname.SystemDNSDomain:80`. The default ports are 80 for http and 443 for https.

URLFile(r): <S>

Specifies the path to a CSV file that contains multiple rules that you want to delete.

Do not supply URLFile if you are supplying URL.

MatchType: <exact/starts-with/startswith/prefix>

Use with URL to specify whether the rule matches exactly what is in URL, or uses it as a base for a prefix match. Defaults to **exact** if not supplied. The other options are all equivalent.

Deployment: <S>

Use with URL to specify which of your deployments uses this rule. Not required unless you have multiple deployments. If you have multiple deployments, the rule will use the default deployment if you don't specify the deployment.

Description: <S:128>

A text description of the rule.

HttpMethods: <OPTIONS/GET/HEAD/POST/PUT/DELETE>

A comma-delimited set of methods to allow with this rule. If you do not specify the methods, the rule will use the default methods configured on **Configuration > Unified Communications > HTTP allow list > Editable inbound rules**.

Example 1: `xCommand HTTPAllowListRuleDelete URLfile: "/tmp/rules.csv"`

Example 2: `xCommand HTTPAllowListRuleDelete URL: "https://cucm2.example.com:8443/partial/path"`

`MatchType: starts-with Description: "https access to read everything below partial/path/ on cucm2.example.com" HttpMethods: "OPTIONS,GET"`

Reference Material

HTTPAllowListRulesTest

(Experimental)

Tests a collection of URLs (defined in a CSV file) against a list of rules (defined in a CSV file). This enables you to test rules before you apply them, or to test that existing rules are working as expected.

You can provide either the tests, or the rules, or both, as CSV files. If you provide both, the tests in the Tests CSV file are run against the rules in the Rules CSV file. If you omit one or both parameters, this command uses the rules or tests (or both) that are already on the Expressway. (Use `xstatus collaborationedge httpallowlist` to see the current rules).

Tests: <S>

Specifies the path to a CSV file that contains multiple tests, eg. `/tmp/tests.csv`. See [Allow List Tests File Reference, page 383](#).

Rules: <S>

Specifies the path to a CSV file that contains multiple rules you want to test, eg. `/tmp/rules.csv`. See [Allow List Rules File Reference, page 382](#).

Example : `xCommand HTTPAllowListRulesTest Tests: "/tmp/tests.csv" Rules: "/tmp/rules.csv"`

HTTPAllowListTestAdd

(Experimental)

Adds one or more URLs to test against the HTTP allow list. You must specify at least URL or URLFile; if you specify URL, you must specify ExpectedResult.

URL(r): <S>

Specifies the test URL. IPv6 addresses must use RFC 2732 format.

For example: `https://[2001:DB8::1]:8443/path` or `https://www.example.com:8443/resource`

Do not supply URL if you are supplying URLFile.

URL must contain the protocol, either `http://` or `https://`, and the hostname. It should also contain domain, port, and path to make the URL more specific. If you omit some portions of the URL, Expressway will supply its defaults. eg. `http://hostname` tests the URL `http://hostname.SystemDNSDomain:80`. The default ports are 80 for http and 443 for https.

URLFile(r): <S>

Specifies the path to a CSV file that contains multiple tests. See [Allow List Tests File Reference, page 383](#).

Do not supply URLFile if you are supplying URL.

ExpectedResult(r): <allow/block>

Required with URL to specify whether the URL should be allowed or blocked by the allow list.

Deployment: <S>

Use with URL to specify which of your deployments uses this test. Not required unless you have multiple deployments. If you have multiple deployments, the test will use the default deployment unless you specify the deployment.

Description: <S:128>

A text description of the test.

HttpMethod: <OPTIONS/GET/HEAD/POST/PUT/DELETE>

Specify one method to test. If you do not specify the method, the test will use GET.

Example 1: `xCommand HTTPAllowListTestAdd URLfile: "/tmp/tests.csv"`

Example 2: `xCommand MRAAllowListTestAdd URL: "https://cucm2.example.com:8443/partial/path"`

`ExpectedResult: block Description: "https access to write to partial/path/ on cucm2.example.com"`

`HttpMethod: "POST"`

HTTPAllowListTestDelete

(Experimental)

Deletes one or more test URLs from the HTTP allow list. You must specify at least URL or URLFile; if you specify URL, you must specify ExpectedResult.

URL(r): <S>

Specifies the test URL you are deleting.

Do not supply URL if you are supplying URLFile.

URLFile(r): <S>

Specifies the path to a CSV file that contains multiple tests you want to delete.

Do not supply URLFile if you are supplying URL.

ExpectedResult(r): <allow/block>

Specify the result expected by the test you are deleting. Required for deleting the test.

Deployment: <S>

Specify which deployment use the test you are deleting. Not required unless you have multiple deployments.

Description: <S:128>

A text description of the test. Not required for deleting the test unless you have multiple tests that cannot otherwise be distinguished from each other.

HttpMethod: <OPTIONS/GET/HEAD/POST/PUT/DELETE>

Specify which method is used in the test you are deleting. If you omit the methods, the Expressway uses the current default methods with this command. This means the delete could fail unless the test was created with the corresponding methods.

Example 1: `xCommand HTTPAllowListTestDelete URLfile: "/tmp/tests.csv"`

Example 2: `xCommand HTTPAllowListTestDelete URL: "https://cucm2.example.com:8443/partial/path"`

`ExpectedResult: allow HttpMethod: "get"`

HTTPProxyJabberCTargetsAdd

Configures a Jabber Guest Server and associates it with a Jabber Guest domain.

DomainIndex(r): <0..200>

Index of the domain with which this Jabber Guest Server is associated

Host(r): <S:1,1024>

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.

Note that you can specify alternative addresses for the same domain, each with different priorities.

Priority: <0..9>

The order in which connections to this hostname are attempted for this domain. All priority 1 hostnames for the domain are attempted first, followed by all priority 2 hostnames, and so on.

Example: `xCommand HTTPProxyJabberCTargetsAdd DomainIndex: 2 Host: jabberguest.example.com`

HTTPProxyJabberCTargetsDelete

Deletes the configured Jabber Guest Server from the Expressway.

Host(r): <S:1,1024> The FQDN of the Jabber Guest Server to delete.

IMPServerAdd

Adds an external messaging server to which to route Microsoft SIP Simple messages.

IMP(r): <Value> configuration/b2bua/imp/imp

IMPServerDelete

Deletes an external messaging server.

IMP(r): <Value> configuration/b2bua/imp/imp

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`

Reference Material

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`

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`

Networklimits

Controls the experimental rate limiting feature. Enter `xcom networklimits ?` to read the help.

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`

Reference Material

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**

RemoveRegistration

Removes a registration from the Expressway.

Registration: <1..3750>

The index of the registration to be removed.

RegistrationSerialNumber: <S: 1, 255>

The serial number of the registration to be removed.

Example: **xCommand RemoveRegistration RegistrationSerialNumber: "a761c4bc-25c9-11b2-a37f-0010f30f521c"**

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`

Securemode

Controls Advanced Account Security options.

Command(r): <on/off/status>

The index of the route to be deleted.

Example: `xCommand Securemode Command: off`

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`

UcxnConfigAdd

Configures a link to a Cisco Unity Connection server, for use with Mobile and Remote Access.

Address(r): <S:0,1024>

The FQDN or IP address of a Unity Connection publisher.

CertValidationDisabled: <On/Off>

If CertValidationDisabled is Off, the Cisco Unity Connection system's FQDN or IP address must be contained within the X.509 certificate presented by that system (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.

DeploymentId: <1..65535>

This Unity Connection publisher is associated with the selected deployment and can only communicate with other members of the selected deployment. It cannot communicate with members of other deployments.

Password(r): <S:1,1024>

The password used by the Expressway-C to access the Cisco Unity Connection publisher.

Username(r): <S:1,1024>

The username used by the VCS to access the Unity Connection publisher.

UcxnConfigDelete

Removes a link to a Cisco Unity Connection server from the VCS.

Address(r): <S:0,1024>

The FQDN or IP address of a Unity Connection publisher.

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.

Axlpassword(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" Axlpassword: "xyz" Axlusername: "abc"`

Reference Material

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*: a firewall exists between the zones, and the local Expressway is a traversal client of the new zone. *TraversalServer*: a firewall exists 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
- Authentication
- Authzkeys
- B2BUACalls
- B2buapresencerelayservice
- B2buapresencereLAYuser
- CDR
- Cafe
- Calls
- Cloud
- Cluster
- CollaborationEdge
- Edgeauth
- Edgecmsserver
- EdgeConfigProvisioning
- Edgeconfigprovisioning
- Edgedomain
- Edgeexternalfqdn
- Edgeauthcodecache
- Edgesso
- ExternalManager
- Fail2ban
- Feedback
- Fips

Reference Material

- Firewall
- Gwtunnels
- H323
- HTTPProxy
- Hardware
- IntrusionProtection
- Iptablesacceptedrule
- Iptablesrule
- License
- Links
- Mediastatistics
- MicrosoftContent
- MicrosoftIMP
- NetworkInterface
- NetworkLimits (experimental)
- Ntpcertificates
- Options
- PhonebookServer
- Pipes
- Policy
- PortUsage
- Registrations
- ResourceUsage
- Resourceusage
- SIP
- SipServiceDomains
- SipServiceZones
- SystemMetrics
- SystemUnit
- TURN
- Teststatus
- Time
- Traversalserverresourceusage
- Tunnels
- Warnings
- XMPP
- Xcps2s
- Zones

External Policy Overview

The Cisco Expressway (Expressway) has built in support for Registration Policy and Call Policy configuration. It also supports CPL (Call Processing Language) for implementing more complex policy decisions. CPL is designed as a

Reference Material

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 accept a registration, 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:

- Registration Policy – to allow or reject registrations.
- 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 or registration 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 (for example lists of aliases that are allowed to register or make and receive calls, via external data lookups such as an LDAP database or other information sources).

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 and indicates with a ✓ in which request types that parameter is included. It also indicates, where relevant, the range of accepted values.

| Parameter name | Values | Registration Policy | Search rules | Call Policy |
|----------------------------|--------------|---------------------|--------------|-------------|
| ALIAS | | ✓ | | |
| ALLOW_INTERWORKING | TRUE / FALSE | | ✓ | ✓ |
| AUTHENTICATED | TRUE / FALSE | ✓ | ✓ | ✓ |
| AUTHENTICATED_SOURCE_ALIAS | | | ✓ | ✓ |

Reference Material

| Parameter name | Values | Registration Policy | Search rules | Call Policy |
|------------------------------|---|---------------------|--------------|-------------|
| 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 / REGISTER | ✓ | ✓ | ✓ |
| NETWORK_TYPE | IPV4 / IPV6 | | ✓ | ✓ |
| POLICY_TYPE | REGISTRATION / 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 registrations and 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.

Reference Material

This default CPL mean that in the event of a loss of connectivity to the policy server, all call and registration 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 or registrations 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 44 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 |

Table 44 Supported RFCs (continued)

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

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.

- [X8.9.2](#)
- [X8.9.1](#)
- [X8.9](#)
- [X8.8.3](#)
- [X8.8.2](#)
- [X8.8.1](#)
- [X8.8](#)
- [X8.7.3](#)
- [X8.7.2](#)
- [X8.7.1](#)
- [X8.7](#)
- [X8.6.1](#)
- [X8.6](#)
- [X8.5.3](#)
- [X8.5.2](#)
- [X8.5.1](#)
- [X8.5](#)
- [X8.2](#)
- [X8.1.1](#)

X8.9.2 Minor Changes

- SIP TCP mode is now Off by default in this release.
- The Web Proxy for Cisco Meeting Server is supported in this release. Off-premises users can browse to a Meeting Server Web Bridge. All they need to manage or join spaces is a supported browser.
- Expressway-E peers can now cluster on their FQDNs with TLS verification, by using the cluster address mapping table. Public FQDNs are still used to identify the cluster peers and are still required in their certificates. The address mapping table is consulted prior to the regular DNS lookups to resolve these FQDNs into the peers' private IP addresses.

To form a cluster using FQDN and TLS verification, we recommend that you form the cluster using IP addresses, then create the address mappings, then change the peer addresses across the cluster. Finally, you can enable TLS verification. See the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide* for a detailed procedure.
- Product Identifier and key for Advanced Account Security added to the *Expressway Administration Guide*.
- Various corrections to the user documentation.

X8.9.1 Minor Changes

- If you have Cisco Jabber users with iOS devices, Expressway with Mobile and Remote Access now supports the Apple Push Notification Service. (Subject to the dependent systems being available.) See feature description below.

Reference Material

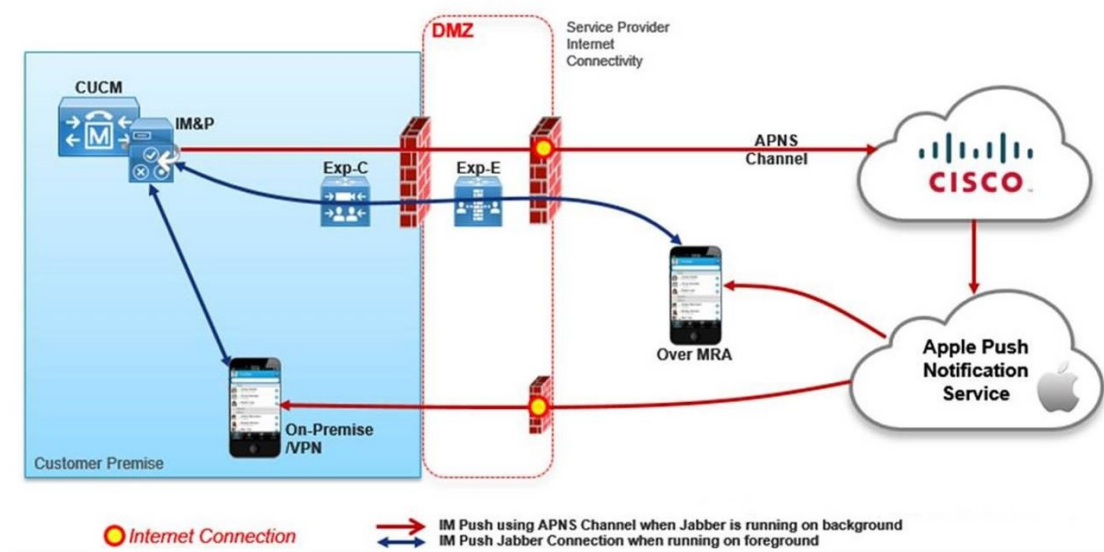
- The Install Wizard has these changes:
 - When deploying an OVA using the Install Wizard, a warning in relation to an RSA key being required has been removed. An RSA public key is only required if you wish to set the root and admin password through SSH – primarily used in automated deployments.
 - The serial number and release key, if available, now appear in the Install Wizard for reference purposes.
- For DCSP marking, traffic type "Video" is now assigned by default if the media type cannot be identified. (For example, if different media types are multiplexed on the same port.) Previously we assigned type "Audio" as the default.
- Miscellaneous security enhancements.
- A new alarm number 20021 exists, to warn about cluster communication failures.

Apple Push Notification Service Pass Through to Cisco Jabber for iPhone and iPad

If you have Cisco Jabber users with iOS devices, Expressway with Mobile and Remote Access is able to support the Apple Push Notification Service (APNs) for the IM&P service.

For detailed information, see *Deploying Apple Push Notifications for the IM and Presence Service* on the [Cisco Unified Communications Manager IM and Presence Service Configuration and TechNotes](#) page on Cisco.com.

Figure 18 Apple Push Notifications for Unified CM IM&P and Jabber iOS



X8.9 Features

Edge Traversal of Microsoft SIP Traffic for Cisco Meeting Server

The Expressway pair at the edge of the network can now traverse Microsoft-variant SIP traffic to and from the Cisco Meeting Server. This allows your users to collaborate with people from external organizations that use Office 365 or Microsoft Skype for Business infrastructure. Users can meet in Meeting Server spaces, or make point-to-point calls between the organizations.

Two Expressway enhancements help you configure these collaboration scenarios:

- The DNS zone can do SRV lookups for the Microsoft federation service (`._sipfederationls._tcp.example.com.`)

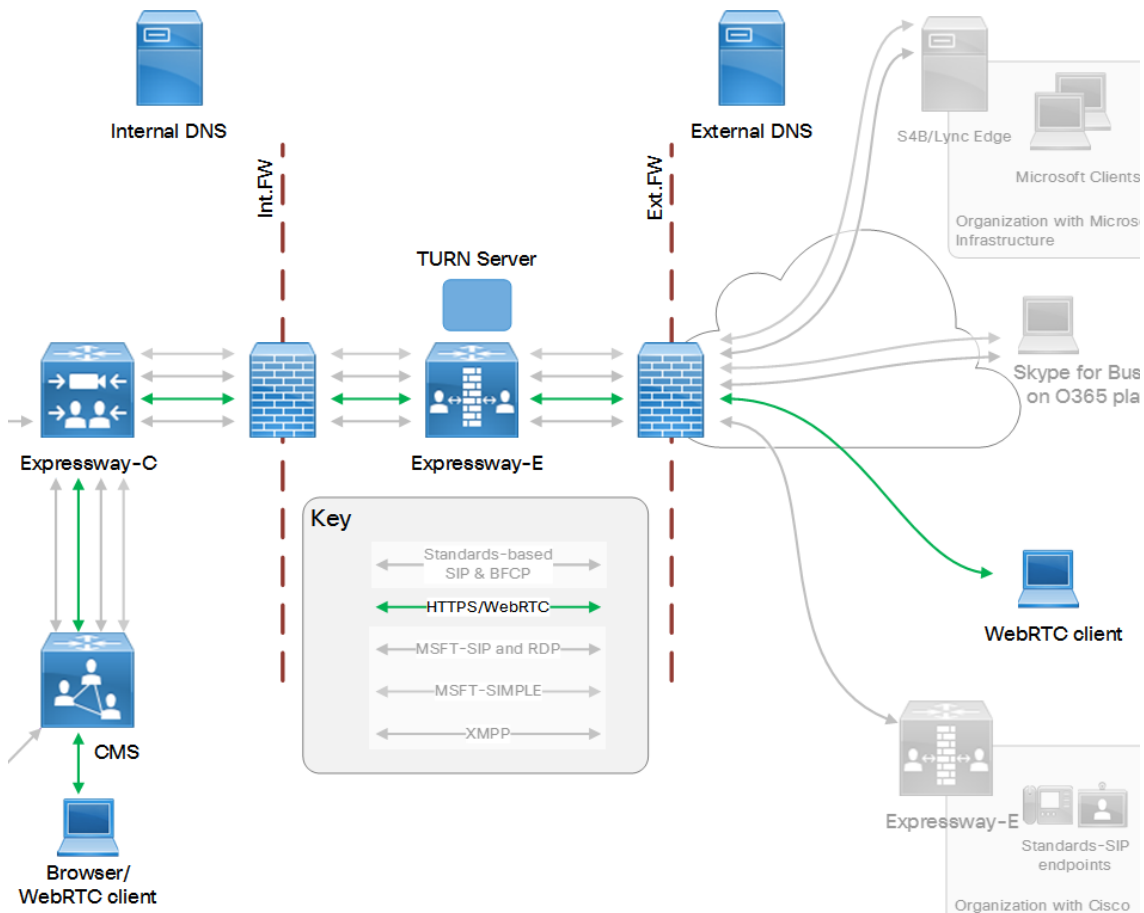
- Search rules now have the ability to route calls based on which variant of SIP is used on the call

| | |
|-------------------------------|------------------|
| Protocol | SIP |
| SIP variant | All SIP Variants |
| Source | |
| Request must be authenticated | |
| Mode | Any alias |

Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure on the [Expressway configuration guides page](#).

Web Proxy for Meeting Server

We've added a reverse https proxy for Cisco Meeting Server, which enables off-premises users to browse to a Meeting Server Web Bridge. Users can manage or join spaces without having any software other than a supported browser.



Assuming that Mobile and Remote Access (MRA) is already enabled, the proxy needs minimal extra configuration on the Expressway pair. Simply enter the Meeting Server listening address on the Expressway-C. Then the pair uses the existing traversal connection to proxy external https requests to that address.

Reference Material

Notes:

- You must have TURN services enabled on the Expressway-E, unless you use TURN services on the Edge server component of the Meeting Server.
- You can enable the Web Proxy for Meeting Server on the same Expressway pair as MRA or other traversal features. However, you can't use it if the pair is configured for Jabber Guest.

More information about the Web Proxy

- [List of supported browsers.](#)
- *Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure* on the [Expressway configuration guides page.](#)

IM and Presence Service Federation With Skype for Business or Office 365 Organizations

The Expressway pair at the edge of the network can now traverse messaging and presence traffic between IM and Presence Service and external organizations using Skype for Business or Office 365. For this feature to work, Cisco Unified Communications Manager IM and Presence Service must be running a compatible software version.

Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure on the [Expressway configuration guides page.](#)

Cisco Expressway as H.323 Gatekeeper

X8.8 introduced the ability to use the Expressway-C as a SIP registrar, for TelePresence room and desktop systems. And a new licensing model with that feature.

X8.9 extends the feature to enable H.323 Gatekeeper functionality on the Expressway-C.

When you configure the Expressway as a SIP registrar or H.323 Gatekeeper, you must license it for concurrent systems (the Unified CM model), not for concurrent calls (the VCS model).

For SIP deployments, you can do this by adding either or both of the following license types to the Expressway-C:

- TelePresence Room System License
- Desktop System License

The following SIP devices register as desktop systems with all other devices considered room systems:

- Cisco TelePresence EX60
- Cisco TelePresence EX90
- Cisco DX70
- Cisco DX80

For H.323 deployments, all endpoints consume a TelePresence Room System License. This is due to a limitation in H.323, which does not determine the difference between desktop and room type endpoints.

We therefore recommend SIP as the preferred signaling protocol. H.323 is available as a fall back for endpoints that do not support SIP.

Note: DX systems must be running version CE8.2 or later and EX systems TC7.3.6 or later in order to register as desktop systems (for SIP only). DX and EX systems running earlier versions will still register for SIP but will consume a room system license.

Scope of the registrar feature:

- Option keys containing licenses for local registrations are installed on the Expressway-C. These licenses are pooled in a cluster, which means that Expressway-C peers can use each others' licenses. However, rooms cannot use desktop licenses, and desktop systems cannot use room licenses.

Reference Material

- Registrations from outside the network are proxied to Expressway-C by the Expressway-E. The Expressway-E cannot accept direct registrations.
- Proxy registration is possible with SIP endpoints only and does not apply to H.323 endpoints.
- Device provisioning and FindMe are supported with Cisco TelePresence Management Suite.
- The Large VM or CE1100 can support up to 5000 registrations, or 2500 MRA registrations (proxied to CUCM). Local registrations, proxy registrations (via Expressway-E), and MRA registrations, all count towards this number.

Implications of the new licensing model reduces the usage of Rich Media Session (RMS) licenses in the following scenarios:

- If you have already paid for a registration license, RMS licenses will not be consumed for the following call types; provided that the Expressway is not required for encryption interworking (invoking the B2BUA):
 - Calls between registered systems do not use RMS licenses. Here, 'registered systems' means systems registered directly to the Expressway-C, by proxy to the Expressway-C through the Expressway-E, or by proxy through the Expressway pair (MRA) to neighbored Unified CMs.
 - Calls from registered systems (as above) to Cisco infrastructure do not use RMS licenses. Currently, this extends only to Cisco Meeting Server, and to CiscoTelePresence Server and TelePresence MCUs that are managed by TelePresence Conductor. However, calls from MCUs that are not managed by Conductor do consume RMS licenses.
 - Calls from registered systems (as above) to Cisco Collaboration Cloud do not use RMS licenses.
- However, calls from registered systems to all other systems use one RMS license. This includes, but is not limited to, the following call types:
 - Business to business calls. Previously required two RMS licenses, now require one on Expressway-E.
 - Business to consumer calls (Jabber Guest). Previously required two RMS licenses, now require one on the Expressway-E.
 - Interoperability gateway calls, including Microsoft Lync / Skype for Business and third-party call control servers require one RMS license on the Expressway-C.

See [Call Types and Licensing, page 377](#) for more information about the calls that consume RMS licenses.

REST API Expansion

In X8.8, we introduced a new API to simplify remote configuration. Third party systems, such as Cisco Prime Collaboration Provisioning, can now use the API to configure the following features / services on the Expressway:

- Mobile and Remote Access (MRA)
- Business to business (B2B) calls

The API is self-documented using REST API Markup Language (RAML).

See *Cisco Expressway REST API Reference Guide* on the [Expressway installation guides page](#).

Allow Jabber on iOS to Use Safari for SSO Over MRA

Available if you use OAuth token authentication, with Cisco Jabber iOS endpoints that access Unified Communications services from outside the network. In this case, by default the identity provider's authentication page is displayed in an embedded web browser (not the Safari browser) on the iOS devices. That default browser is unable to access the iOS trust store, and so cannot use any certificates deployed to the devices. You can optionally configure Expressway-E to allow Jabber on iOS devices to use the native Safari browser. Because the Safari browser is able to access the device trust store, you can now enable password-less authentication or two-factor authentication in your OAuth deployment.

Caveat

A potential security issue exists for this option. The mechanism to return browser control from Safari to Jabber after the authentication completes, uses a custom URL scheme that invokes a custom protocol handler. It's possible that

Reference Material

another application other than Jabber could intercept the scheme and gain control from iOS. In that case, the application would have access to the OAuth token in the URL.

If you are confident that your iOS devices will not have other applications that register the Jabber custom URL scheme, for example because all mobile devices are managed, then it's safe to enable the option. If you are concerned about the possibility of another app intercepting the custom Jabber URL, then do **not** enable the embedded Safari browser.

Note: Make sure that you apply this option consistently in the Expressway and in Unified CM. If you decide to enable or disable it in one application, do the same in the other. The relevant settings are:

- **Allow Jabber iOS clients to use embedded Safari browser** in Expressway-C (Configuration > Unified Communications > Configuration > MRA Access Control section)
- **SSO Login Behavior for iOS > Use Native Browser** in Unified CM (System > Enterprise Parameters > SSO Configuration section)

Supported versions

- Cisco Jabber for iOS 11.8 or later, on devices using iOS 9 or later
- Cisco Unified Communications Manager 11.5(1)SU1 or later
- Cisco Unity Connection 11.5(1) or later

Note: If you use self-describing token authentication (from X8.10) you will be using later versions, as required to support self-described OAuth tokens.

Shared Line / Multiple Line Support for MRA Endpoints

Expressway now supports pass through of Unified CM shared line and multiple line features for endpoints that are connecting by Mobile and Remote Access.

The benefit of this feature is that remote and mobile endpoint users can use features, like barge, conference barge, hold on one device and resume on another, in the same way as they would when they are on the premises.

You need to configure multiple and shared lines for users and their MRA devices on Unified CM.

Required versions:

- Unified CM 11.5(1)SU2 or later
- Expressway X8.9 or later
- Cisco IP Phone 7800 Series / Cisco IP Phone 8811, 8841, 8845, 8861 and 8865 devices, with firmware version 11.5(1) or later

Note: This feature is disabled by default, because it impacts some features on earlier versions of Unified CM.

If you are using a Unified CM version before 11.5(1)SU3, and you enable SIP Path headers on Expressway-C, the following Unified CM features will *report the MRA devices' IP addresses instead of the Expressway's IP address*:

- Device Mobility
- Real-Time Monitoring Tool (RTMT)
- Cisco Emergency Responder (CER)

Other features may also be affected by this change. The devices' IP addresses are not useful for determining their location, as they are typically from reserved private ranges and could overlap with your organization's internal range.

Smart Call Home

This feature is in preview status.

Smart Call Home is a free embedded support capability for Expressway. It offers proactive diagnostics and real-time alerts, enabling higher network availability and increased operational efficiency.

Smart Call Home notifies users of Schedule- and Event-based notifications.

Reference Material

- Schedule-based: inventory, telemetry and configuration messages used to generate a Device Report and improve hardware and software quality by identifying failure trends. You can find these notifications posted on the first day of every month.
- Event-based: asynchronous events already supported by Expressway such as alarms and ACRs. You will find these notifications posted to the Smart Call Home server as and when they occur.

Secure Install Wizard

The Expressway now includes an Install Wizard that helps make the deployment and configuration of your system easier and more secure.

The Install Wizard guides you through the initial configuration required to get your system up and running securely. Any further configuration is then possible using the web interface or CLI.

Only the person authorized to complete the system installation can access and complete the initial setup on the system console (or VM equivalent). All accounts on the Expressway are disabled upon first boot until the installation is complete. The system is also not accessible over the network interface until the installation has been completed and secured.

In a VM deployment, any preconfigured data gets imported when the VM boots for the first time and you are not required to re-enter data.

The Install Wizard does not affect the upgrade procedure for an existing system, as the system maintains any data that you have already configured.

DiffServ Code Point Marking

From X8.9, the Expressway supports improved DSCP (Differentiated Service Code Point) packet marking for traffic passing through the firewall, including Mobile and Remote Access. DSCP is a measure of the Quality of Service level of the packet. To provide more granular control of traffic prioritization, DSCP values are set (marked) for these individual traffic types:

| Traffic type | Supplied default value | Web UI field |
|--------------|------------------------|---------------|
| Video | 34 | QoS Video |
| Audio | 46 | QoS Audio |
| XMPP | 24 | QoS XMPP |
| Signaling | 24 | QoS Signaling |

Before X8.9 you had to apply DSCP values to all signaling and media traffic collectively.

You can optionally change the default DSCP values from the **System > Quality of Service** web UI page (or the CLI).

Notes:

- DSCP value "0" specifies standard best-effort service.
- DSCP marking is applied to SIP and H.323 traffic.
- DSCP marking is applied to TURN media, providing the TURN traffic is actually handled by the Expressway.
- Traffic type "Video" is assigned by default if the media type cannot be identified. (For example, if different media types are multiplexed on the same port.)

Existing QoS/DSCP Commands and API are Discontinued

From X8.9 we no longer support the previous methods to specify QoS/DSCP values. The former Web UI settings **QoS Mode** and **QoS Value**, CLI commands `xConfiguration IP QoS Mode` and `xConfiguration IP QoS Value` and corresponding API are now discontinued. Do not use these commands.

Reference Material

What if I currently use these commands?

When you upgrade the Expressway, any existing QoS value you have defined is automatically applied to the new fields and replaces the supplied defaults. For example, if you had a value of 20 defined, all four DSCP settings (QoS Audio, QoS Video, QoS XMPP, QoS Signaling) are set to 20 also.

We don't support downgrades. If you need to revert to your pre-upgrade software version, the QoS settings are reset to their original supplied defaults. So QoS Mode is set to *None* and QoS Value is set to 0. You will need to manually redefine the values you want to use.

Maintenance Mode For MRA

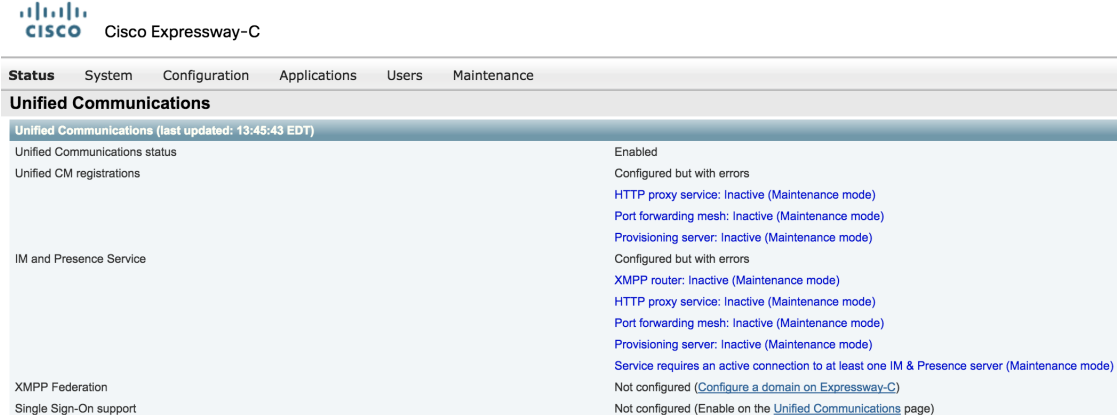
Maintenance mode on the Expressway has been enhanced so that you can bring an MRA system down in a managed way.

When you engage maintenance mode, the Expressway stops accepting new calls or proxy (MRA) traffic. Existing calls and chat sessions are not affected.

As users end their sessions normally, the system comes to a point when it is not processing any traffic of a certain type, and then it shuts that service down.

If users try to make new calls or start new chat sessions while the Expressway is in maintenance mode, the clients will receive a service unavailable response, and they might then choose to use another peer (if they are capable). This fail-over behavior depends on the client, but restarting the client should resolve any connection issues if there are active peers in the cluster.

The Unified Communications status pages also show (Maintenance Mode) in any places where MRA services are affected.



The screenshot shows the Cisco Expressway-C interface with the 'Unified Communications' status page. The page is titled 'Unified Communications (last updated: 13:45:43 EDT)'. It lists several services and their status:

| Service | Status |
|-------------------------------|---|
| Unified Communications status | Enabled |
| Unified CM registrations | Configured but with errors |
| | HTTP proxy service: Inactive (Maintenance mode) |
| | Port forwarding mesh: Inactive (Maintenance mode) |
| | Provisioning server: Inactive (Maintenance mode) |
| IM and Presence Service | Configured but with errors |
| | XMPP router: Inactive (Maintenance mode) |
| | HTTP proxy service: Inactive (Maintenance mode) |
| | Port forwarding mesh: Inactive (Maintenance mode) |
| | Provisioning server: Inactive (Maintenance mode) |
| | Service requires an active connection to at least one IM & Presence server (Maintenance mode) |
| XMPP Federation | Not configured (Configure a domain on Expressway-C) |
| Single Sign-On support | Not configured (Enable on the Unified Communications page) |

Changes and Enhancements

- The Expressway now supports advanced account security mode.
- You can nominate an administrator account as an emergency account. In case the Expressway disallows local authentication but is unable to connect to a remote authentication service.
- We have removed the limitation that TURN services should not be enabled on a system that is being used for MRA. We did this to allow services that require TURN to coexist with MRA. One example is edge traversal for Cisco Meeting Server.

Note: This change does not make Jabber Guest compatible with MRA. It also does not mean that TURN can be used for MRA. The change simply means that MRA is not impacted if you enable TURN services (for other reasons).

- We have discontinued the pre-X8.9 API and CLI commands for defining QoS/DSCP values: `xConfiguration IP QoS Mode` and `xConfiguration IP QoS Value`. They are replaced by new commands / web UI settings.

Reference Material

- The web administration port is now configurable, on the **System > Administration** page. The default port is still 443.
- From X8.9 onwards, automated intrusion protection is enabled, by default, for the following categories:
 - http-ce-auth
 - http-ce-intrusion
 - sshpfd-auth
 - sshpfd-intrusion
 - xmpp-intrusion
 This change affects new systems. Upgraded systems keep their existing protection configuration.
- You can use the following supported Cisco Jabber SDK features over MRA:
 - Sign in/ sign out
 - Register phone services
 - Make or receive audio/ video calls
 - Hold and resume, mute/ unmute, and call transfer

For more information, see the [Getting Started Guide for Cisco Jabber SDK](#).

X8.8.3 Minor Changes

- The Expressway has been updated to match the leap second adjustment to UTC time.
- The Expressway has also been updated to match the recent change to the TRT (Turkey Time) time zone.

X8.8.2 Minor Changes

- The call policy rule editor now has more granular control. You can use the web interface to create policy rules to allow or reject calls from specific zones or callers. You can also choose whether the rule applies to authenticated or unauthenticated callers.
- The clustering page now gives better feedback on DNS resolution and peer certificate status during cluster configuration.
- Zone pages now show how many registrations were proxied by the zones.
- The online help has been updated.

X8.8.1 Minor Changes

- Cisco Expressway Series has been certified FIPS compliant.
- Several important bug fixes and security patches have been applied.
- The online help has been updated for Expressway registrations and MRA allow list features.

X8.8 Features

Table 45 Feature History by Release Number

| | |
|---|-----------|
| Feature / change | X8.8 |
| Registrations On Expressway | Supported |
| Skype for Business 2016 and Skype for Business Mobile Support | Supported |

Table 45 Feature History by Release Number (continued)

| Feature / change | X8.8 |
|-------------------------------------|-----------|
| Broker for Microsoft SIP Traffic | Supported |
| Multistream Support | Supported |
| Service Setup Wizard | Supported |
| MRA Allow List Improvement | Supported |
| API for Remote Configuration of MRA | Supported |
| Large VM CPU Reservation Reduced | Supported |
| High Security Environment | Supported |
| Software Package Signing | Supported |
| SSL/TLS Support Restricted | Supported |
| Changes and Minor Enhancements | Supported |

Registrations On Expressway

Expressway-C can now be used as a SIP registrar for telepresence room and desktop systems. We have also introduced a new licensing model for calls that go through the Expressway, to align more closely with the Unified CM licensing model.

When you configure the Expressway as a registrar, you must license it for concurrent systems (CUCM model), rather than for concurrent calls (VCS model). You can do that by adding either or both of the following license types to the Expressway-C:

- TelePresence Room System License
- Desktop System License

The following devices register as desktop systems with all other devices considered room systems:

- Cisco TelePresence EX60
- Cisco TelePresence EX90
- Cisco DX70
- Cisco DX80

Scope of the registrar feature:

- Option keys containing licenses for local registrations are installed on the Expressway-C. These licenses are pooled in a cluster, that is, Expressway-C peers can use each others' licenses. However, rooms cannot use desktop licenses, nor can desktop systems use room licenses.
- Registrations from outside the network are proxied to the Expressway-C by the Expressway-E. The Expressway-E does not accept direct registrations.
- Device provisioning and FindMe are supported with Cisco TelePresence Management Suite.
- H.323 registrations are not currently supported.
- The Medium VM (or CE1100 with 1 GBps NIC) can support up to 2500 registrations. The Large VM (or CE1100 with 10 GBps NIC) can support up to 5000 registrations. Local registrations, proxy registrations (via Expressway-E), and MRA registrations (proxied to CUCM), all count towards this number.

Implications of the new licensing model:

Reference Material

- Rich Media Session license usage has been reduced, following the principle that if you have already paid for a registration license you should not also pay for the Rich Media Session.
- Calls between registered systems do not use RMS licenses. Here, "registered systems" means systems registered directly to the Expressway-C, by proxy to the Expressway-C through the Expressway-E, or by proxy through the Expressway pair (MRA) to neighbored Unified CMs.
- Calls from registered systems (as above) to Cisco infrastructure do not use RMS licenses. Currently, this extends only to Cisco Meeting Server, or to TelePresence Server when managed by TelePresence Conductor.
- Calls from registered systems (as above) to Cisco Collaboration Cloud do not use RMS licenses.
- Calls from registered systems to all other systems will use one RMS license. This includes, but is not limited to, the following call types:
 - Business to business calls: previously required two RMS licenses, now require one on Expressway-E
 - Business to consumer calls (Jabber Guest): previously required two RMS licenses, now require one on the Expressway-E
 - Interoperability gateway calls (including Microsoft Lync / Skype for Business and third-party call control servers where interworking is required): require one RMS license on the Expressway-C.

Skype for Business 2016 and Skype for Business Mobile Support

We have updated our support for Microsoft client and server combinations. The Gateway Expressway deployment is now interoperable with the following Microsoft collaboration products:

Table 46 Lync and Skype for Business Support Introduced in X8.10.3

| Clients | On Lync Server 2013 | On Skype for Business Server 2015 |
|---|---------------------|--|
| Skype for Business 2016 (Windows desktop) | Supported | Supported |
| Skype for Business 2015 (Windows desktop) | Supported | Supported |
| Skype for Business for iOS | Not supported | Limited support* |
| Skype for Business for Android | Not supported | Limited support*. See CSCva18731 . |

* We do not support these clients in calls to MCU bridges. We do support them in other call scenarios, including calls to TelePresence Server bridges.

Broker for Microsoft SIP Traffic

In some previous versions of our *Cisco Expressway and Microsoft Interoperability Deployment Guide*, we published an appendix describing how to get Lync to Jabber messaging working using CPL on a "directory Expressway".

In X8.8, we have improved that deployment by creating an independent broker to perform the task of filtering and redirecting the messaging and presence traffic coming from the Microsoft infrastructure. This change has the following benefits:

- Maintains the robustness of the SDP parser, by not requiring it to process the non-standard SIP from Microsoft infrastructure
- No requirement for a directory Expressway, because the broker is hosted on the Gateway Expressway.
- The broker is abstracted from the rest of the software so you can disable it if you don't need it.
- If you were using the CPL deployment, you can now upgrade to X8.8 and benefit from the other features and improvements since X8.6.
- There is a new document to help you get Cisco Jabber integrated with Microsoft Skype for Business clients. Note that this integration relies on Lync Server 2013 or 2010; Skype for Business Server 2015 is not yet fully supported across all Cisco infrastructure in this deployment.

See *Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet* on the [Expressway configuration guides page](#).

See *Cisco Expressway with Microsoft Infrastructure Deployment Guide* on the [Expressway configuration guides page](#).

Reference Material

Multistream Support

The Expressway now supports passthrough of encrypted and unencrypted multistream calls. It also supports passthrough of the encrypted iX protocol required for the ActiveControl feature used by endpoints interacting with the TelePresence Server.

There is a new "Multistream mode" on all zone types that can potentially handle media. The mode is enabled by default, but it only applies when the zone passes media to or from the back to back user agent. The signaling of multistream calls is always passed through, irrespective of the zone's multistream mode setting.

Note:

- The Expressway does not encrypt the iX protocol on behalf of other entities; iX must either be encrypted from end to end, with the endpoints and TelePresence Server doing the encryption, or it must be unencrypted from end to end.

Service Setup Wizard

The Service Setup Wizard, (introduced in X8.8) improves the user experience of configuring the Expressway for its chosen purpose in your environment.

When you first launch the user interface, you see the Service Setup Wizard instead of going straight into the menu. You can select the system series (VCS or Expressway) and type (*VCS Expressway/VCS Control* or *Expressway-E/Expressway-C*). These choices affect the list of services available.

Then you select from a number of popular Expressway services:

- Cisco Spark Hybrid Services (renamed to Cisco Webex Hybrid Services)
- Mobile and Remote Access including Meeting Server Web Proxy
- Jabber Guest Services
- Microsoft gateway service - this service is only for when you want *this system* to adapt between Microsoft SIP and standards-based SIP variants. If a different system (such as Cisco Meeting Server) is doing that adaptation in your deployment, you don't need this service.
- Registrar/ Proxy registrations - previously only possible on VCS, now also possible on Expressway.
- Collaboration Meeting Rooms (CMR) Cloud
- Business to Business Calling - from X8.9, this service includes B2B calling with organizations using Microsoft collaboration infrastructure, if you use Meeting Server to adapt between Microsoft and standards-based SIP variants.

When you select from the list, the wizard helps you to apply appropriate licenses for your selection, verify your basic configuration (network settings should have been configured previously), and then restart the system. After the restart, you only see the configuration pages and fields that are relevant for your selection.

If you don't want to use the wizard you can skip through it. And you can go back to the start at any time.

Table 47 Services That Can Be Hosted Together

| | Cisco Spark Hybrid Services (Connectors) | Mobile and Remote Access | Jabber Guest Services | Microsoft gateway service | Registrar | CMR Cloud | Business to Business calling (incl. Hybrid Call Service) |
|--|--|--------------------------|-----------------------|---------------------------|-----------|-----------|--|
| Cisco Spark Hybrid Services (Connectors) | Y | N | N | N | N | Y | Y |
| Mobile and Remote Access and/or (from X8.9) Meeting Server Web Proxy | N | Y | N | N | Y | Y | Y* |
| Jabber Guest Services | N | N | Y | N | Y | Y | Y |
| Microsoft gateway service | N | N | N | Y | N | N | N |
| Registrar | N | Y | Y | N | Y | Y | Y |
| CMR Cloud | Y | Y | Y | N | Y | Y | Y |
| Business to Business calling (includes Cisco Webex Hybrid Call Service) | Y | Y* | Y | N | Y | Y | Y |

Key to Table

Y: Yes, these services can be hosted on the same system or cluster

N: No, these services may not be hosted on the same system or cluster

Rules

- Hybrid Services connectors may co-reside with the Expressway-C of a traversal pair used for Call Service, subject to user number limitations.
 - * If your Hybrid Call Service (or B2B) traversal pair is also used for MRA, then the Hybrid Services connectors must be on a separate Expressway-C. This is because we do not support the connectors being hosted on the Expressway-C that is used for MRA.
- Microsoft gateway service requires a dedicated VCS Control or Expressway-C (called "Gateway VCS" or "Gateway Expressway" in the help and documentation)
- Jabber Guest cannot work with MRA (technical limitation)
- MRA is currently not supported in IPv6 only mode. If you want IPv6 B2B calling to co-reside with IPv4 MRA on the same Expressway traversal pair, the Expressway-E and Expressway-C must both be in dual stack mode.

MRA Allow List Improvements

The MRA allow list feature is more specific in this release. When you add, discover, or refresh the Unified Communications nodes on the Expressway-C, the Expressway automatically adds the nodes to the allow list. We are now being a lot more specific by including the port and request path in the allow list rule.

Reference Material

We also improved the interface for manually adding rules, enabling you to accurately specify the URL and so restrict the scope of access. For example, instead of allowing `something.example.com`, now you can add `https://something.example.com:8443/pathto/resource.htm` instead.

You can also restrict which HTTP methods you allow for each of your rules.

Note: You should review your editable rules after you upgrade the Expressway-Cs in your MRA deployment. We advise this because any servers you previously added to the allow list are upgraded to prefix matching rules. These rules allow any path on that server, using the default ports for the originally entered protocol.

The automatically added entries are automatically upgraded to be more specific than in previous releases.

API for Remote Configuration of MRA

The Expressway has a new API to simplify remote configuration. Third party systems, such as Cisco Prime Collaboration Provisioning, can use the API to configure Mobile and Remote Access on the Expressway.

The API is self-documented using REST API Markup Language (RAML).

See *Cisco Expressway REST API Reference Guide* on the [Expressway installation guides page](#).

Large VM CPU Reservation Reduced

The Large Expressway VM CPU reservation requirement has been reduced from 25600 MHz to 16000 MHz. This means that two Large Expressway VMs can now comfortably co-reside on a UCS server with two eight-core 3.2 GHz processors, when hyperthreading is enabled. This was not previously possible because the higher reservation requirement, added to the CPU requirement for the hypervisor, exceeded the total processing power of the host.

The new reservation does not limit the maximum Expressway CPU speed; the Expressway can use the headroom provided by the higher specification host.

High Security Environments

With this release we have improved security in a number of Expressway components, and have implemented new ways of testing and threat modelling, as part of an ongoing effort to improve security.

If you deploy Expressway into a high security environment, you must apply the *Advanced Account Security* option key, then enable **FIPS140-2 cryptographic mode** and acknowledge that you consent to the associated restrictions.

Software Package Signing

Starting with this release, we are signing Expressway software packages to give you confidence in their integrity and authenticity.

We now do an integrity check before you commit to an upgrade. This means you can't tell that the package is being verified on this particular upgrade, because your pre-upgrade version does not have this feature. During your next upgrade, you'll see package signing information, like this:

Upgrade confirmation

System information

| | |
|--------------------------|------------------|
| Current software version | X8.8Alpha3 |
| New software version | X8.8Alpha6 |
| Serial number | 52A19127 |
| Release key | 3731630340846000 |
| Signing Information | Cisco |

Software package hashes

| | |
|--------------|--------------------------|
| SHA-1 hash | 4c079a4c71a0386440800077 |
| SHA-512 hash | 205a7a0c10706c21e1384 |

TLS Support Restricted

To improve security, the Expressway now only supports specific versions of TLS. The Expressway offers and accepts TLS versions 1.0, 1.1, and 1.2, when establishing secure connections.

Changes and Minor Enhancements

- From version X8.8 onwards, the Expressway does not create DSA host keys. It creates RSA or ECDSA keys instead, for improved security.
If you upgrade a system that already has a DSA host key, the existing key will persist so that SSH client users do not have to verify the fingerprint again.
- From version X8.8 onwards, connections between cluster peers use TLS instead of IPSec. When you upgrade a cluster, the cluster comes up in TLS permissive mode.
- Multiple Device Messaging (a new feature in IM and Presence Service 11.5) is now supported for clients that connect through Expressway to IM and Presence Service in the cloud.
This feature is not supported through any versions of Expressway before X8.8.

X8.7.3 Minor Changes

- The Expressway now accepts SCTP (Stream Control Transmission Protocol).
- The Expressway TURN server has been enhanced to interoperate with the Acano Server (1.9), to enable Microsoft RDP sharing.

X8.7.2 Minor Changes

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

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

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

X8.7.1 Minor Changes

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

This option is primarily intended for use with Cisco Spark Call Service. See www.cisco.com/go/hybrid-services.

- The 2 * 2.4 GHz CPU reservation requirement of the Medium virtual Expressway has been relaxed to allow for slight variance in host clock speeds.

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

See *Cisco Expressway Virtual Machine Installation Guide* on the [Expressway installation guides page](#).

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

X8.7 Features

Table 48 Feature History by Release Number

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

Dial via Office-Reverse Through MRA

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

DVO-R handles call signaling and voice media separately. All call signaling, including the signaling for Mobile and Remote Access on Expressway, traverses the IP connection between the client and Cisco Unified Communications

Reference Material

Manager. Voice media traverses the cellular interface and hairpins at the enterprise Public Switched Telephone Network (PSTN) gateway.

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

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

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

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

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

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

Lync Screen Sharing Through a Gateway Cluster

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

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

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

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

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

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

Mobile and Remote Access with Supported Cisco IP Phones

Mobile and Remote Access is supported with the following Cisco IP Phones, when the phones are running firmware version 11.0(1) or later. We recommend Expressway X8.7 or later for use with these phones.

- Cisco IP Phone 8811, 8841, 8845, 8861 and 8865
- Cisco IP Phone 7800 Series

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

- [Cisco DX650](#)
- [Cisco DX80](#)
- [Cisco DX70](#)

When deploying DX Series or IP Phone 78/8800 Series endpoints to register with Cisco Unified Communications Manager through MRA, 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 through MRA. This is because the MRA solution does not support devices interacting with CAPF (Certificate Authority Proxy Function).

Reference Material

- **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.
- **Off-hook dialling:** The way KPML dialing works between these endpoints and Unified CM means that you need CUCM 10.5(2)SU2 or later to be able to do off-hook dialing via MRA. You can work around this dependency by using on-hook dialing.

Hybrid Services and Expressway/VCS Rebranding

We have changed some terminology in this release:

- **Expressway/VCS base**

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

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

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

- **Hybrid Services**

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

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

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

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

Hosting on VMWare vSphere 6.0

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

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

See the *Cisco Expressway on Virtual Machine Installation Guide* on the [Expressway Install and Upgrade Guides page](#).

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

Keyword Filter for Syslog Output

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

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

Reference Material

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

Changes and Minor Enhancements

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

See *Cisco Expressway Virtual Machine Installation Guide* on the [Expressway installation guides page](#).

There is a delay when you deploy virtual machines with pre-configured network parameters. The deployment will take a few minutes longer than deploying the VM without pre-configured network parameters.

- The Expressway deployment guide now warns against choosing a single NIC, static NAT deployment of the Expressway-E. The preferred option for deploying the Expressway-E in the DMZ is to use both NICs.

See *Cisco Expressway Registrar Deployment Guide* on the [Expressway configuration guides page](#).

X8.6.1 Minor Changes

X8.6.1 is a maintenance release. No new features are introduced.

X8.6 Features

Table 49 Feature history by release number

| Feature / change | X8.6.1 | X8.6 |
|--|---|---|
| Lync Desktop Sharing | Supported | Supported |
| Hybrid Services | Supported | Withdrawn |
| License bypass for calls to cloud-based Collaboration Meeting Rooms (CMRs) | Supported | Supported |
| New codec support: OPUS and H.265 | Supported | Supported |
| System Metrics Collection | Supported | Supported |
| Cisco DX Series endpoints over MRA | Supported with endpoint version 10.2.4(99) or later | Supported with endpoint version 10.2.4(99) or later |
| Cisco IP Phone 7800/8800 Series over MRA | Preview with endpoint version 10.3.1 or later | Preview with endpoint version 10.3.1 or later |
| Multiple Presence Domains via MRA | Preview | Preview |
| Japanese, Korean, Russian localizations | X8.5.1 UI | X8.5.1 UI |
| Changes and minor enhancements | Supported | Supported |

Support for desktop sharing from Lync

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

Reference Material

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

The following deployments support screen sharing from Microsoft clients:

Figure 19 Microsoft environment to conference managed by TelePresence Conductor trunked to Unified CM

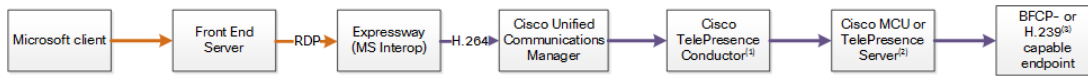


Figure 20 Microsoft environment to SIP endpoint registered to Unified CM



Notes:

1. If you use the Optimize Resources feature with Microsoft client screen sharing, you need the following software versions:
 - TelePresence Conductor XC4.0 or later
 - TelePresence Server 4.2 or later
2. Requires an H.323 registrar, not shown in the diagram.

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

Hybrid Services

What are Spark Hybrid Services and what do they do?

Cisco Spark Hybrid Services empower cloud-based and premises-based solutions to deliver a more capable, better integrated collaboration user experience.

Which services am I entitled to use?

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

What software do I need?

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

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

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

How do I install, upgrade, or downgrade?

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

Reference Material

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

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

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

[Where can I read more about Spark Hybrid Services?](#)

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

License bypass for calls to Collaboration Meeting Rooms (CMRs)

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

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

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

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

New codec support

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

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

System Metrics Collection

[What is System Metrics Collection, and how does it work on Expressway?](#)

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

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

[Where do I configure System Metrics Collection?](#)

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

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

[How can I use this data?](#)

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

Reference Material

Where can I read more about System Metrics Collection?

For more detail, see the *Cisco Expressway Serviceability Guide* on the [Cisco Expressway Series Maintain and Operate Guides](#) page.

MRA support for new endpoints

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

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

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

When deploying DX Series or IP Phone 78/8800 Series endpoints to register with Cisco Unified Communications Manager through MRA, 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 through MRA. This is because the MRA solution does not support devices interacting with CAPF (Certificate Authority Proxy Function).
- **Trust list:** You cannot modify the root CA trust list on these endpoints. Make sure that the Expressway-E's server certificate is signed by one of the CAs that the endpoints trust, and that the CA is trusted by the Expressway-C and the Expressway-E.
- **Bandwidth restrictions:** The **Maximum Session Bit Rate for Video Calls** on the default region on Cisco Unified Communications Manager is 384 kbps by default. The **Default call bandwidth** on Expressway-C is also 384 kbps by default. These settings may be too low to deliver the expected video quality for the DX Series.

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

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

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

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

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

Updated language packs

Language packs are now available for the following languages. The packs include localized web interface and embedded webhelp.

- Japanese
- Russian
- Korean

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

Changes and minor enhancements

- The functionality provided by the Interworking option key is now included in the Expressway option key.
- There is a new option to modify the **SIP TCP connect timeout (Configuration > Protocols > SIP > Advanced)**. The default is 10 seconds.
- Mutual TLS authentication can now be configured for SIP calls (**Configuration > Protocols > SIP**). Two new parameters were added **Mutual TLS mode** (default Off) and **Mutual TLS port** (default 5062).
- A new zone parameter called **SIP parameter preservation** controls whether the SIP URI and Contact parameters are preserved between the zone and the B2BUA.
- A new zone parameter called **Preloaded SIP routes support** controls whether the zone processes SIP INVITE requests that contain the Route header.
- There is a new command line option to change the cipher suites used for SIP TLS connections. The command takes a colon-delimited string of cipher suites (see <https://www.openssl.org/docs/man1.0.1/apps/ciphers.html#CIPHER-LIST-FORMAT>). For example, to set the current Expressway default suite, use:

```
xConfiguration SIP TLS CipherSuite: ALL:!EXP:!LOW:!MD5:@STRENGTH:+ADH
```
- The diagnostic log now includes two new .xml files, to record the xconfig and xstatus of the Expressway at the time the log was taken.
- The **Call Detail Records (CDR)** switch has moved from the **System > Administration** page to the **Maintenance > Logging** page.
- The CLI commands `xCommand LoginUserAdd` and `xCommand LoginUserDelete` have been replaced by `xCommand CredentialAdd` and `xCommand CredentialDelete`.
- The hop count logic has changed so that internal hops between the Expressway application and its B2BUA do not decrement the hop count.
- Several advanced zone parameters have been removed because they are no longer required. These are **SIP SDP attribute line limit mode**, **SIP SDP attribute line limit length**, and **SIP Duo Video filter mode**.
- The **Maximum authorizations per period** default has increased to 8.

X8.5.3

X8.5.3 is a maintenance release. No new features are introduced. X8.5.3 supersedes X8.5.2.

Table 50 Feature history by release number

| Feature / change | X8.5.3 | X8.5.2 (withdrawn) | X8.5.1 | X8.5 |
|--|-------------------------------------|-------------------------------------|--|-------------------|
| KPML | Supported | Supported | Not supported | Not supported |
| Multiple Presence Domains via MRA | Preview | Preview | Preview | Not supported |
| SSO over MRA | Supported | Supported | Supported; SAML signing algorithm changed | Preview |
| CSR UI digest algorithm options | Supported | Supported | Supported | Not supported |
| Cisco DX Series endpoints over MRA | Supported with 10.2.4(99) and later | Supported with 10.2.4(99) and later | Preview (no KPML) | Preview (no KPML) |
| Cisco IP Phone 7800/8800 Series over MRA | Preview (with KPML) | Preview (with KPML) | Preview (no KPML) | Preview (no KPML) |
| Early media | Supported | Supported | Supported | Supported |

Table 50 Feature history by release number (continued)

| Feature / change | X8.5.3 | X8.5.2 (withdrawn) | X8.5.1 | X8.5 |
|--|-----------|--------------------|-----------|-----------|
| Unsolicited NOTIFY pass-through | Supported | Supported | Supported | Supported |
| Multiple deployments | Supported | Supported | Supported | Supported |
| Secure connection checker | Supported | Supported | Supported | Supported |
| Syslog publish filter | Supported | Supported | Supported | Supported |
| Call Detail Records (CDRs) | Supported | Supported | Supported | Supported |
| Media statistics | Supported | Supported | Supported | Supported |
| Password change requires authorization | Supported | Supported | Supported | Supported |
| Static routes | Supported | Supported | Supported | Supported |

X8.5.2

Note: This release has been withdrawn and is no longer available for download.

MRA support for new endpoints

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

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

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

When deploying DX Series or IP Phone 78/8800 Series endpoints to register with Cisco Unified Communications Manager through MRA, 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 through MRA. 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.

Reference Material

- Chinese
- French
- German
- Spanish
- Japanese
- Korean
- Russian

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

Important behavior changes

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

Software enhancements

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

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.

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

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

Reference Material

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

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

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, were not available in X8.5. This limitation was resolved in X8.5.2.

Single sign-on over MRA

Use this feature to enable single sign-on for endpoints that access 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

Note: Jabber clients are the *only* endpoints supported for SSO through Mobile and Remote Access (MRA).

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

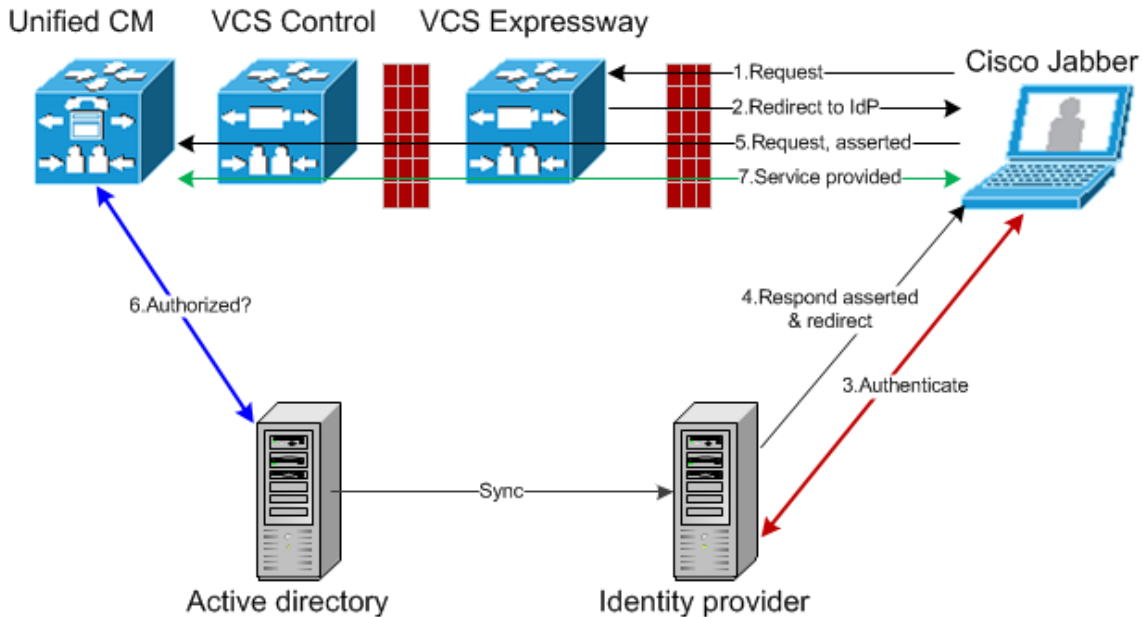
How it works

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 21 Remote single sign-on for on-premises UC services



Understanding the SSO options for MRA

The Expressway options for SSO over the edge (**Configuration > Unified Communications > Configuration** page) are:

- **Exclusive**: This is the most secure option. Requires authentication through the IdP, which is the only permitted authentication agent. Authentication can be certificate-based, two-factor, or username and password. This option only allows Jabber clients through MRA. The clients must be in SSO authentication mode.
- **On**: Allows authentication through the IdP or the Expressway pair. The Expressway supports username and password authentication only. If the IdP is the authentication agent, certificate-based or two-factor authentication is also available. This option allows Jabber clients in SSO authentication mode or basic authentication mode through MRA. And (non-SSO) endpoints, including IP phones and TelePresence devices.
 - Jabber clients in SSO authentication mode first try to authenticate at the IdP. If that fails, they attempt to authenticate through the Expressway.
 - Jabber clients in basic authentication mode use username and password authentication.
 - Other endpoints and IP phones also use username and password authentication.
- **Off**: Requires authentication through the Expressway, which is the only permitted authentication agent. Username and password is the only supported authentication method. Endpoints, IP phones, and Jabber clients in basic authentication mode are allowed through MRA.

Note: When the Expressway is used as the authentication agent, the authentication request is proxied through the Expressway pair, which returns the authorization token.

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:

Reference Material

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.

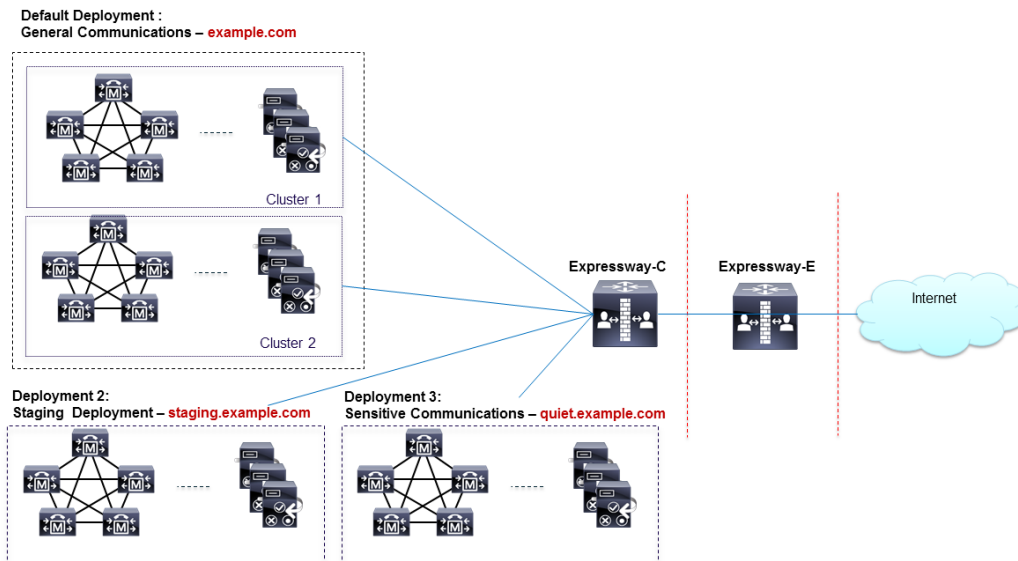
A deployment is an abstract boundary used to enclose a domain and one or more Unified Communications service providers (such as Unified CM, Cisco Unity Connection, and IM and Presence Service nodes). The purpose of multiple deployments is to partition the Unified Communications services available to Mobile and Remote Access (MRA) users. So different subsets of MRA users can access different sets of services over the same Expressway pair.

We recommend that you do not exceed ten deployments.

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, as a third set.

Figure 22 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

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**.

Reference Material

- 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 Expressway-C or a traversal server zone when selected on 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.

Reference Material

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](#).

Reference Material

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

| Title | Link |
|--|--|
| Expressway Administrator Guide (this document) | www.cisco.com |
| Authenticating Expressway Accounts Using LDAP Deployment Guide | www.cisco.com |
| Expressway Registrar Deployment Guide | www.cisco.com |
| Expressway Basic Configuration Deployment Guide | www.cisco.com |
| Expressway Certificate Creation and Use Deployment Guide | www.cisco.com |
| Cisco Unified Communications Manager with Expressway Deployment Guide | www.cisco.com |
| Expressway Cluster Creation and Maintenance Deployment Guide | www.cisco.com |
| Expressway ENUM Dialing Deployment Guide | www.cisco.com |
| Expressway External Policy Deployment Guide | www.cisco.com |
| Expressway on Virtual Machine Installation Guide | www.cisco.com |
| Expressway CE1100 Appliance Installation Guide | www.cisco.com |
| Expressway IP Port Usage for Firewall Traversal | www.cisco.com |
| Expressway and Microsoft Interoperability Deployment Guide | www.cisco.com |
| Unified Communications: Mobile and Remote Access via Expressway Deployment Guide | www.cisco.com |

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/c/en/us/support/unified-communications/expressway-series/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



Cisco Legal Information

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

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

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

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

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

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

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

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

© 2017 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

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