Cisco Expressway Administrator Guide (X14.3)

First Published: 2023-06-01

Last Modified: 2023-05-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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 of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **What's New in This Version?** 1

What's New in This Version? 1

CHAPTER 2 **Introduction** 3

About the Expressway 3

Expressway Types 4

Standard Features 5

Do Not Install Other Cisco or Third-Party Software onto Expressway 6

Hardware Appliance and Virtual Machine Options 6

Limitation 7

About This Guide 7

Change History 8

Training 11

Glossary 11

Accessibility Notice 12

Related Documentation 12

About the Service Setup Wizard (Service Selection Page) 13

Services That Can Be Hosted Together 14

CHAPTER 3 **Expressway Interfaces** 17

About the Web Interface 17

Web Page Features and Layout 18

Missing Application Menu in Web User Interface 20

About the Command Line Interface 20

To Use the CLI 20

Command Types 21

Useful Controls 21
About the API 21
Software Versions Supported by Hardware Platforms 22

CHAPTER 4 Expressway Capacity and Sizing 23
Overview 23
Important Caveats 23
Dependencies 24
Capacity Guidelines for Standalone Systems 24
Capacity Guidelines for Clustered Systems 25
Fast Path Registration for MRA (Caching Optimization for Registrations) 25
Intracluster Calls 26

CHAPTER 5 Call Types and Licensing 29
Call Types 29
Limitation 30
Room and Desktop Registrations on Expressway 31
Limitation 33
License Usage for Device Registrations 33
RMS License Consumption Table 33
License Bypass for Calls to Collaboration Meeting Rooms (CMRs) 34
License Usage for Cisco Video Integration (CVI) Calls 35
Intracluster Calls 35
Usage Limits 35
Limitations 36

CHAPTER 6 Smart Licensing 37
About Smart Licensing 37
Factory Reset 39
How Smart Licensing Works 41
Creating a Smart Account 42
Requesting License Reservation for Your Smart Account 42
Before You Enable Smart Licensing 43
Smart Licensing Settings 43

Configure Smart Licensing 47
Before You Start 47
Process Summary 48
Obtain the Product Instance Registration Token 48
Configure Transport Settings on Expressway 49
Register with Cisco Smart Software Manager 49
Important Configuration Information for Smart Licensing 50
Manage Smart Licensing Registrations and Authorizations 50
Renew Authorization 51
Renew Registration 51
Deregister 52
Reregister with Cisco Smart Software Manager 52
How to Register a Change to the Expressway Hostname 52
Deregister First if Expressway is Permanently Shutdown 53
About Cisco Smart License Reservation and Its Types 53
CLI Commands for PLR and SLR 55
Permanent License Reservation 56
How does PLR Licenses Work? 56
How to Apply PLR Licenses? 56
Task Flow 57
Specific License Reservation 67
Task Flow 67
Additional Information 80
Limitation 81
Smart Licensing Export Compliance 82
Export Control Alarms 82
Additional Information 82
Limitations 83

CHAPTER 7 **Managing Security** 85
Security Basics 85
Data at Rest 85
TLS and Certificates 85
Configuring Certificate-Based Authentication 86

Enabling Certificate-Based Authentication 87
Authentication Versus Authorization 87
Obtaining the Username from the Certificate 88
Emergency Account and Certificate-Based Authentication 88
Managing the Trusted CA Certificate List 88
Managing the Expressway Server Certificate 89
Using the ACME Service 89
Server Certificates and Clustered Systems 89
Server Certificates and Unified Communications 90
Managing Certificate Revocation Lists (CRLs) 90
Certificate Revocation Sources 90
Limitations and Usage Guidelines 90
Automatic CRL Updates 91
Manual CRL Updates 91
Online Certificate Status Protocol (OCSP) 92
Configuring Revocation Checking for SIP TLS Connections 92
Managing mTLS Client Certificate Verification for MRA Onboarding 93
Testing Client Certificates 93
To test if a certificate is valid 94
To retrieve authorization credentials (username) from the certificate 94
Testing Secure Traversal 95
Managing the Expressway Server Certificate with HSM 96
Install the HSM private key and certificate 96
Download the HSM key handle across a cluster 97
Restart Expressway 97
Configuring Hardware Security Module Functionality 97
Configuring Minimum TLS Version and Cipher Suites 97
Minimum TLS Version 98
Cipher Suites 98
Configuring SSH 100
Advanced Security 101
Configuring Advanced Account Security Mode 101
Prerequisites 102
Enabling Advanced Account Security 103

Expressway Functionality: Changes and Limitations 103
Disabling Advanced Account Security 104
Configuring FIPS140-2 Cryptographic Mode 104
Prerequisites 104
Enable FIPS 140-2 Cryptographic Mode 105

CHAPTER 8 **Serviceability, Logging, Monitoring, and Metrics** 109
Configure Logging 109
Change the Event Log Verbosity 109
Certificate-Compliant Logging 111
How to Configure Certification-compliant Logging 111
Publishing Logs to Remote Syslog Servers 111
Configuring Remote Syslog Servers 111
Typical Values Used 112
Media Statistics Logging for Calls 113
How to Enable Media Statistics 113
Capture Call Detail Records 114
How to Configure CDRs 114
CDR Properties 114
APIs to Access CDRs 115
CDR Examples 117
Configure Alarm-Based Email Notifications 118
Before You Begin 119
Process to Configure Alarm-Based Email Notifications 119
How to Customize Notifications - Disable or Send to an Email Address 120
Reducing Email Notifications 121
System Metrics Collection 121
How to Configure System Metrics Collection (collected) 122
Configure on Expressway 122
Configure a Remote Server 123
Troubleshooting 123
Metrics Collected from Expressway 123

CHAPTER 9 **Network and System Settings** 133

Network Settings 133
Ethernet Settings 133
Configuring IP Settings 133
IP Protocol Configuration 134
IPv4 to IPv6 Interworking 134
IP Gateways 134
LAN Configuration 134
Dedicated Management Interface 135
About Advanced Networking and Dual Network Interfaces 136
Configuring Dual Network Interfaces 136
Configuring Static NAT 137
IPv6 Mode Features and Limitations 137
Explicit IPv6 Supported Features 137
Supported RFCs 138
Known Limitations in IPv6 Mode 138
Configuring DNS Settings 138
Configuring the System Host Name and Domain Name 138
Configuring DNS Server Addresses 139
Caching DNS Records 140
Configuring DSCP / Quality of Service Settings 140
About DSCP Marking 140
Configuring DSCP Values 141
Static Routes 142
To add a static route: 142
Intrusion Protection 142
Configuring Firewall Rules 142
Setting Up and Activating Firewall Rules 143
Rule settings 144
Current Active Firewall Rules 146
Configuring Automated Intrusion Protection 146
Enabling Automated Protection 147
Configuring Protection Categories 147
Configuring Exemptions 148
Managing Blocked Addresses 149

Investigating Access Failures and Intrusions 149
Automated Protection Service and Clustered Systems 149
Automated Protection in MRA Deployments 149
Additional Information 150
Configuring Rate Limits 150
Network Services 151
Configuring System Name and Access Settings 151
HTTP Strict Transport Security 158
Configuring SNMP Settings 159
Configuring Time Settings 161
Configuring the NTP Servers 161
Expressway Time Display and Time Zone 163
Configuring the Login Page 164
Configuring External Manager Settings 164
Configuring the Dedicated Management Interface (DMI) 165
Introduction to the DMI 165
How to Configure the DMI 166
(Optional) Make DMI Sole Interface 167
Configuring TMS Provisioning Extension Services 168
Before You Start 168
Configuration Settings 169

CHAPTER 10 **Firewall Traversal** 171
About Firewall Traversal 171
The Expressway Solution 171
Recommendations and Prerequisites 172
How Does it Work? 172
Endpoint Traversal Technology Requirements 173
H.323 Firewall Traversal Protocols 173
SIP Firewall Traversal Protocols 173
Media Demultiplexing 174
Firewall Traversal Configuration Overview 175
Expressway as a Firewall Traversal Client 175
Expressway as a Firewall Traversal Server 175

Configuring Traversal Server Zones 175
Configuring Other Traversal Server Features 176
Firewall Traversal and Advanced Networking 176
Configuring a Traversal Client and Server 176
Configuring Ports for Firewall Traversal 177
Configuring the Firewall 178
Configuring Traversal Server Ports 178
RTP and RTCP Media Demultiplexing Ports 178
Configuring Ports for Connections From Traversal Clients 179
Configuring TURN Ports 179
Configuring Ports for Connections Out to the Public Internet 179
Firewall Traversal and Authentication 180
Authentication and NTP 180
Configuring Expressway-E and Traversal Endpoint Communications 181
About ICE and TURN Services 182
About ICE 182
ICE Passthrough for MRA Deployments 182
About TURN 182
Configuring TURN Services 185

CHAPTER 11 **Unified Communications** 189
Unified Communication Prerequisites 189
Configuring a Secure Traversal Zone Connection for Unified Communications 189
Installing Expressway Security Certificates 189
Configuring Encrypted Expressway Traversal Zones 190
Server Certificate Requirements for Unified Communications 192
Cisco Unified Communications Manager Certificates 192
IM and Presence Service Certificates 192
Expressway Certificates 193
Managing Domain Certificates and Sever Name Indication 196
SNI Call Flow 197
Managing the Expressway's Domain Certificates 198
Automated Certificate Management Environment Service 200
Domain Certificates and Clustered Systems 201

Mobile and Remote Access Overview 201
Deployment Scope 202
Mobile and Remote Access Ports 203
Jabber Client Connectivity Without VPN 203
Where to Get Detailed Configuration Information 203
XMPP Federation Through Expressway 203
Supported Systems 204
Limitations 204
Prerequisites 205
Detailed Configuration Information 206
Delayed Cisco XCP Router Restart 206
Jabber Guest Services Overview 207
Information Scope 207
Meeting Server Web Proxy on Expressway 208

CHAPTER 12 **Protocols** 209
About H.323 209
Using the Expressway as an H.323 Gatekeeper 209
H.323 Endpoint Registration 209
Preventing Automatic H.323 Registrations 210
Registration Refresh 210
Configuring H.323 210
About SIP 212
Expressway as a SIP Registrar 212
Expressway as a SIP Proxy Server 214
Proxying Registration Requests 215
Expressway as a SIP Presence Server 215
Configuring SIP 215
SIP Functionality and SIP-Specific Transport Modes and Ports 216
Certificate Revocation Checking Modes 216
Registration Controls 217
Authentication Controls 219
Advanced SIP Settings 220
Retain Connection for Corrupt/Malformed SIP Message (CLI) 220

Configuring Domains 220
Configuring the Supported Services for Unified Communications (Expressway-C Only) 221
Configuring Delegated Credential Checking (Expressway-E Only) 221
Testing the credential checking service 222
Configuring SIP and H.323 Interworking 222

CHAPTER 13 Registration Control 225
About Registrations 225
Finding an Expressway with Which to Register 226
MCU, Gateway, and Content Server Registration 226
Configuring Registration Restriction Policy 226
Registering Aliases 227
About Allow and Deny Lists 228
Configuring the Registration Allow List 229
Configuring the Registration Deny List 229
Configuring Registration Policy to Use an External Service 230

CHAPTER 14 Device Authentication 233
About Device Authentication 233
Authentication Policy 234
Authentication Policy Configuration Options 234
Controlling System Behavior for Authenticated and Non-Authenticated Devices 236
SIP Authentication Trust 237
Device Provisioning and Authentication Policy 238
Authentication Methods 238
Configuring Authentication to Use the Local Database 238
Authenticating with External Systems 239

CHAPTER 15 Zones and Neighbors 241
Video Network Fundamentals 241
Structuring the Dial Plan 242
Flat Dial Plan 242
Structured Dial Plan 243
Hierarchical Dial Plan 243

About Zones 243
Configuring ICE Messaging Support 244
Configuring Media Encryption Policy 246
Configuring the B2BUA for Media Encryption 247
About the Local Zone and Subzones 247
Configuring the Default Zone 248
Default Zone Settings 248
Using Links and Pipes to Manage Access and Bandwidth 249
Configuring Default Zone Access Rules 249
Configuring Zones (Non-Default Zones) 250
Configuring Neighbor Zones 251
Configuring Traversal Client Zones 256
Configuring Traversal Server Zones 261
Configuring ENUM Zones 266
Configuring DNS Zones 266
Configuring the Webex Zone 270
Limitation 270
Zone Configuration: Advanced Settings 271
Zone Configuration: Pre-Configured Profile Settings 275
TLS Certificate Verification of Neighbor Systems 276
Configuring a Zone for Incoming Calls Only 277

CHAPTER 16 **Clustering and Peers** 279
About Clusters 279
Cluster License Usage and Capacity Guidelines 281
Important Caveats 281
Dependencies 281
Capacity Guidelines for Standalone Systems 282
Capacity Guidelines for Clustered Systems 282
Intracluster Calls 282
Managing Clusters and Peers 282
Setting Up a Cluster 282
Before you Start 282
Process 282

Maintaining a Cluster 283
Basics of Cluster Configuration 283
Other Configuration for the Cluster 283
Adding and Removing Peers From a Cluster 284
Changing the Primary Peer 284
Monitoring Cluster Status 284
Troubleshooting Cluster Problems 284
Peer-Specific Items in Clustered Systems 284
Sharing Registrations Across Peers 287
Sharing Bandwidth Across Peers 288
Cluster Upgrades, Backup, and Restore 288
Clustering and Cisco TMS 289
About the Cluster Subzone 289
Neighboring Between Expressway Clusters 290
Process to Neighbor Clusters 290
Troubleshooting Cluster Replication Problems 291
Troubleshooting System Key Related Issues 292

CHAPTER 17 **Dial Plan and Call Processing** 295
Call Routing Process 295
About Cisco VCS's Directory Service 297
Configuring Hop Counts 297
Configuring hop counts for a zone 298
Configuring Dial Plan Settings 298
About the Fallback Alias 299
About Transforms and Search Rules 300
About Pre-Search Transforms 301
Configuring Pre-Search Transforms 302
Search and Zone Transformation Process 303
Configuring Search Rules 304
Example Searches and Transforms 307
Filter Queries to a Zone Without Transforming 308
Always Query a Zone with Original Alias (No Transforms) 308
Query a Zone for a Transformed Alias 309

Query a Zone for Original and Transformed Aliases 310
Query a Zone for Two or More Transformed Aliases 311
Stripping @domain for Dialing to H.323 Numbers 312
Pre-Search Transform 313
Local Zone Search Rules 313
Transforms for Alphanumeric H.323 ID Dial Strings 315
Pre-Search Transform 315
Local Zone Search Rules 315
Allowing Calls to IP Addresses only if They Come From Known Zones 317
Forward Microsoft SIP Calls to Cisco Meeting Server 317
Direct 9-1-1 Calls for Kari's Law (with Expressway as Call Control and a PSTN Gateway) 318
When Does Kari's Law Apply to Expressway? 318
Before You Begin 318
Configuring the Search Rules 319
Example 1: Search Rules for a Standalone Gateway 319
Example 2: Search Rules for Multiple Gateways 320
Configuring Search Rules to Use an External Service 323
Configuring a Policy Service to be Used by Search Rules 324
Configuring a Search Rule to Direct a Search to the Policy Service 325
About Call Policy 326
Configuring Call Policy 326
Call Policy Mode 327
Configuring Call Policy Rules Using the Web Interface 327
Configuring Call Policy Using a CPL Script 329
Viewing existing CPL script 329
About CPL XSD files 330
Uploading a CPL script 330
Deleting an existing CPL script 330
Configuring Call Policy to Use an External Service 330
Supported Address Formats 333
Dialing by IP Address 333
Dialing by H.323 ID or E.164 Alias 333
Dialing by H.323 or SIP URI 333
Dialing by ENUM 334

Dialing by IP Address 334
About URI Dialing 336
URI Dialing Without DNS 336
URI Dialing With DNS 337
URI Resolution Process Using DNS 337
URI Dialing via DNS for Outgoing Calls 339
Adding and configuring DNS zones 339
Configuring search rules for DNS zones 340
URI Dialing via DNS for Incoming Calls 341
Configuring H.323 SRV Records 342
Configuring SIP SRV Records 342
Example DNS Record Configuration 343
URI Dialing and Firewall Traversal 344
About ENUM Dialing 344
ENUM Dialing Process 344
Enabling ENUM Dialing 345
ENUM Dialing for Outgoing Calls 345
Configuring Zones and Search Rules for ENUM Dialing 347
Adding and configuring ENUM zones 347
Configuring search rules for ENUM zones 348
Configuring transforms for ENUM zones 348
ENUM dialing for Incoming Calls 349
Configuring DNS Servers for ENUM and URI Dialing 350
Configuring Call Routing and Signaling 351
Call Signaling Optimization 351
Call Loop Detection Mode 351
Identifying Calls 352
Identifying Calls in the CLI 353
Disconnecting Calls 353
Disconnecting a call using the web interface 353
Disconnecting a call using the CLI 353
Limitations when disconnecting SIP calls 354

CHAPTER 18 **Bandwidth Control** 355

About Bandwidth Control 355
Configuring Bandwidth Controls 356
About Downspeeding 357
About Subzones 357
About the Traversal Subzone 358
Configuring Bandwidth Limitations 358
Configuring the Traversal Subzone Ports 358
Configuring the Default Subzone 360
Configuring Subzones 360
Configuring Subzone Membership Rules 362
Applying Bandwidth Limitations to Subzones 363
Links and Pipes 365
Configuring Links 365
Default Links 365
Configuring Pipes 366
Applying Pipes to Links 367
Bandwidth Control Examples 368
Without a Firewall 368

CHAPTER 19 **Applications** 371
Configuring Conference Factory 371
About Presence 373
Presence Server 373
Presence User Agent 374
Configuring Presence 375
Presence User Agent 376
Presence Server 376
Recommendations 377
B2BUA (Back-to-Back User Agent) Overview 377
Configuring B2BUA TURN Servers 378
About Microsoft Interoperability 378
Capabilities 379
Configuration Summary 379
Why do I need the Microsoft Interoperability Option Key? 379

Features and Limitations 380
Configuring Microsoft Interoperability 381
Configuring the B2BUA's Trusted Hosts 384
Restarting the Microsoft Interoperability Service 385
About FindMe 385
End-User FindMe Account Configuration 386
How are Devices Specified? 386
FindMe Process Overview 386
Recommendations when Deploying FindMe 387
Configuring FindMe 387
Management and Storage of FindMe Data 388
Cisco TMS Provisioning (Including FindMe) 388
Expressway Provisioning Server 390
Hybrid Services and Connector Management 391
Connector Proxy 392
Cisco Webex CA Root Certificates on Expressway-E 392
Related Reading 393
Cisco Webex Edge 393
Using Webex Edge Connect - and no Expressway-C 393

CHAPTER 20 **User Accounts** 395
About User Accounts 395
Account Authentication 395
Password complexity 396
Account Types 396
More Information 397
Configuring Password Security 397
Password Encryption 399
Forbidden Password Dictionary 400
Downloading Forbidden Password Dictionary 400
Uploading Forbidden Password Dictionary 401
Updating Forbidden Password Dictionary 401
Generating Passphrase 401
Configuring Administrator Accounts 402

Editing Administrator Account Details 402
Changing the Password 402
About the Administrator Account and Field References 403
Viewing Active Administrator Sessions 405
Configuring Remote Account Authentication Using LDAP 406
Checking the LDAP Server Connection Status 409
Configuring Administrator Groups 410
Resetting Forgotten Passwords 412
Changing an Administrator Account Password Through the Web Interface 412
Resetting the Root or Admin Password Through a Serial Connection 413
Resetting Root or Admin Password via vSphere 413
Using the Root Account 414
Changing the Root Account Password 414
Accessing the Root Account Over SSH 414
Setting the Pwrec Account Password 415
Managing SSO tokens 415
Managing the tokens of a particular user 415

CHAPTER 21 **Status and System Information** 417
Status Overview 417
System Information 419
Ethernet Status 420
IP Status 420
Resource Usage 422
Registration Status 422
Call Status 424
Disconnecting Calls 426
B2BUA Calls 426
Known Limitation 427
Viewing B2BUA Call Media Details 427
Search History 427
Search Details 428
Local Zone Status 429
Zone Status 430

Bandwidth 431
Link Status 431
Pipe Status 431
Policy Server Status and Resiliency 431
Viewing Policy Server Status via the Expressway 432
TURN Relay Usage 433
TURN Relay Summary 433
Unified Communications Status 434
Checking MRA Authentication Statistics 434
SSH Tunnels Status 434
Microsoft Interoperability 435
Microsoft-registered FindMe User Status 435
Microsoft Interoperability Status 436
TMS Provisioning Extension Service Status 436
Provisioning Server Device Requests Status (Cisco TMSPE) 436
User Records Provided by Cisco TMSPE Services 437
FindMe Records Provided by Cisco TMSPE Services 438
Phone Book Records Provided by Cisco TMSPE Services 439
Provisioned Devices 439
Checking Provisioned Data 440
Managing Alarms 440
Logs 442
Event Log 442
Configuration Log 444
Network Log 445
Filtering the Network Log 445
Results Section 445
Hardware Status 446

CHAPTER 22 **Maintenance** 447
Enable Maintenance Mode 447
Impact on Active Calls and Registrations 447
Process to Enable Maintenance Mode 448
Enabling SSH Access to Expressway 448

Upgrading Expressway Software 449
Upgrading Using Web Interface 449
Upgrading Expressway 449
Prerequisites and Software Dependencies 450
Upgrade Instructions 453
Process to Upgrade a Standalone System 454
Process to Upgrade a Clustered System 455
Upgrading Using Secure Copy (SCP/PSCP) 457
Upgrading Using APIs 458
Upgrading Firmware (Physical Appliances Only) 458
Known Issues and Workarounds 458
Configuring Language Settings 459
Changing the Language 459
Installing Language Packs 459
Removing Language Packs 460
Backing Up and Restoring Expressway Data 460
When to Create a Backup 460
What Gets Backed Up 461
Clustered Systems 461
Creating a System Backup 461
Before you Begin 461
Passwords 462
Process 462
Restoring a Previous Backup 463
Before you Begin 463
Passwords 463
Process 464
Checking the Effect of Pattern 464
Locating an Alias 465
Port Usage 466
Local Inbound Ports 466
Local Outbound Ports 467
Remote Listening Ports 467
Restarting, Rebooting, and Shutting Down 467

CHAPTER 23 **Diagnostics and Troubleshooting** 471

Network Utilities 471

Ping 471

Traceroute 472

Tracepath 472

DNS Lookup 473

SRV Connectivity Tester 475

Diagnostics Tools 478

Configuring Diagnostic Logging 478

Creating a System Snapshot 481

Configuring Network Log Levels 482

Configuring Support Log Levels 482

XCP Routing Information 482

Incident Reporting 484

Incident Reporting Caution: Privacy-Protected Personal Data 484

Enabling Automatic Incident Reporting 485

Sending Incident Reports Manually 485

Viewing Incident Reports 486

Incident Report Details 486

Developer Resources 487

Debugging and System Administration Tools 488

Experimental Menu 488

Enabling or Disabling CDB API Access 489

CHAPTER 24 **Reference Material** 491

About Event Log Levels 491

Event Log Format 492

Administrator Events 493

Message Details Field 493

Events and Levels 496

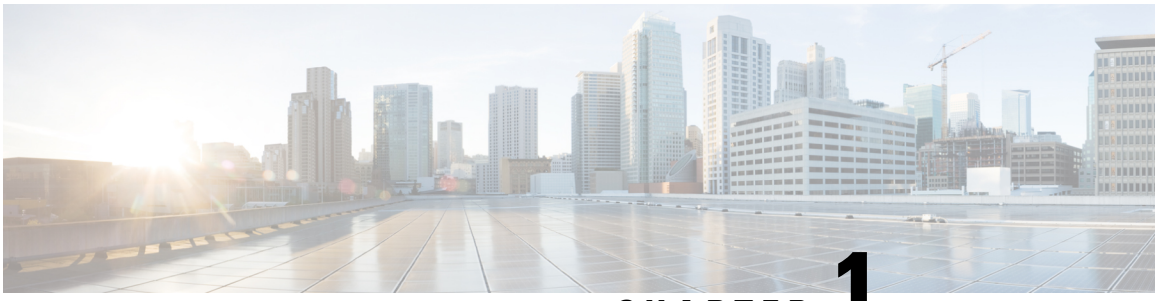
CPL Reference 502

CPL Address-Switch Node 503

Otherwise 505

Not-Present 505
Location 505
Rule-Switch 506
Proxy 507
Reject 507
Unsupported CPL Elements 507
CPL Examples 508
LDAP Server Configuration for Device Authentication 512
Downloading the H.350 Schemas 512
Configuring a Microsoft Active Directory LDAP Server 513
Configuring an OpenLDAP Server 515
Using the Collaboration Solutions Analyzer Tool 517
Changing the Default SSH Key 518
Restoring the Default Configuration (Factory Reset) 518
Before You Begin 518
Prerequisites 519
Process to Reset to the Default Configuration 519
Resetting via USB Stick - CE Hardware Appliances 520
Pattern Matching Variables 520
Port Reference 522
Regular Expressions 522
Supported Characters 524
Product Identifiers and Corresponding Keys 525
Allow List Rules File Reference 530
Allow List Tests File Reference 532
Expressway Multitenancy Overview 533
Multitenant Expressway Restrictions 534
More Information 534
Multitenant Expressway Sizing 534
Alarms Reference 536
Command Reference — xConfiguration 602
xConfiguration Commands 603
Command Reference — xCommand 685
xCommand Commands 686

Command Reference — xStatus 722
xStatus elements 722
External Policy Overview 724
Using an External Policy Server 725
External Policy Request Parameters 725
Default CPL for Policy Services 727
Flash Status Word Reference Table 727
Supported RFCs 728
Software Version History 731
X12.6 Features 731
X12.5 Features 732
X8.11 Features 733
X8.10 Features 736
X8.9 Features 738
X8.8 Features 739
X8.7 Features 739
Legal Notices 740
Intellectual Property Rights 740
Copyright Notice 740
Patent Information 741



CHAPTER 1

What's New in This Version?

- What's New in This Version?, on page 1

What's New in This Version?

New features from software version X12.5 and later are not supported for the Cisco VCS product, and apply only to the Cisco Expressway product. For VCS systems, this version is provided for maintenance and bug fixing purposes only.

Table 1: Features by Release Number

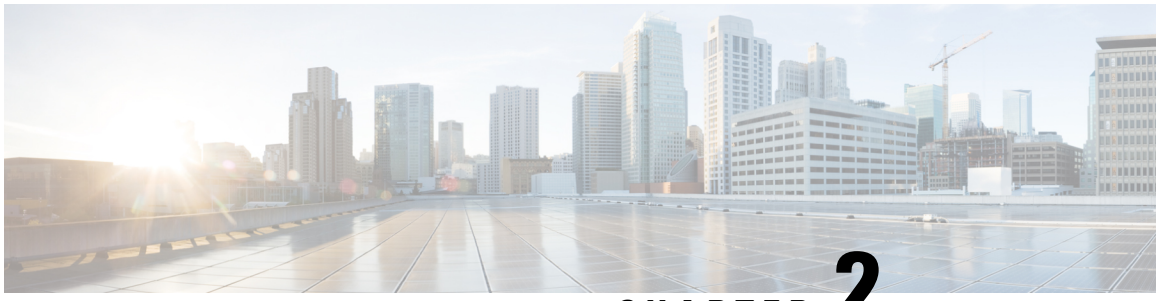
Feature / change	Status
Set the Default Value of SIP TLS DH key size to 2048 for Fresh Install and Upgrade	Supported from X14.3
Route calls to US Suicide Prevention Hotline (988) without RMS licenses	Supported from X14.3
Support for Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate, Update to the Command Line Interface	Supported from X14.3
Smart Licensing	Supported from X14.2 Capped at 2500 encrypted signaling sessions to endpoints
SIP Registration Failover for Cisco Jabber - MRA Deployments	Supported from X14.0
XCP Support for Jabber Zero Downtime	Supported from X14.0
Expressway Cluster Load Balancing Not Applicable to SIP Federation	Supported from X14.0
Escalation from P2P to Meeting	Supported from X14.0
AV1 Support	Supported from X14.0

What's New in This Version?

Feature / change	Status
Webex Client Embedded Browser Support	Supported from X14.0
Dedicated Management Interface	Supported from X12.7
Fast Path Registration for MRA (Caching Optimization for Registrations)	Supported from X12.7
Webex VDI for MRA	Supported from X12.7
Virtualized Systems - ESXi 7.0 Qualification	Supported from X12.7
Hardware Security Module (HSM) Support	Preview
MRA SIP Registration Failover (Phone HA Support)	Preview
MRA Mobile Application Management clients	Preview
MRA Android Push Notifications for IM&P	Preview (disabled by default from X12.6.2)
MRA Headset Capabilities for Cisco Contact Center	Preview

More information

For information about a particular feature, please see the Release Notes for the relevant software version.



CHAPTER 2

Introduction

- About the Expressway, on page 3
- About This Guide, on page 7
- About the Service Setup Wizard (Service Selection Page), on page 13

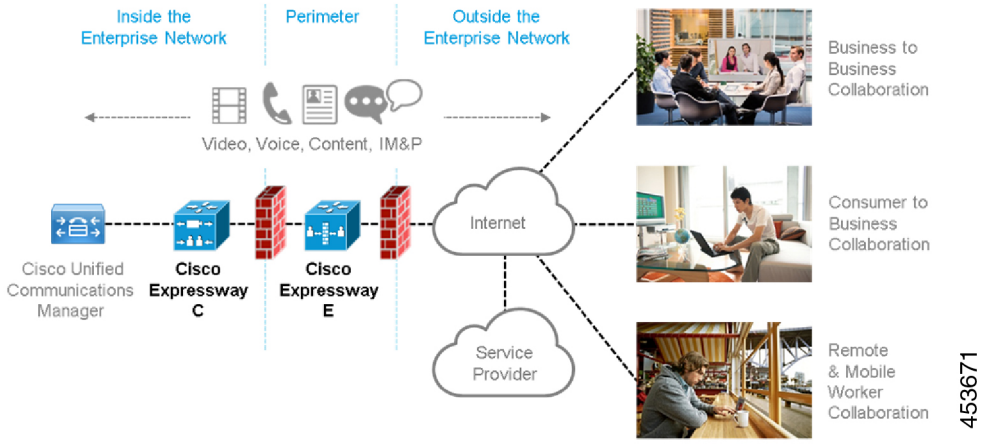
About the Expressway

Cisco Expressway Series (Expressway) is designed specifically for comprehensive collaboration services. It features established firewall-traversal technology and helps to redefine traditional enterprise collaboration boundaries, to support our Cisco vision of any-to-any collaboration.

Expressway offers the following primary features and benefits:

- Provides proven, highly secure, firewall-traversal technology.
- Facilitates connections for business-to-business, business-to-consumer, and business-to-cloud-service-provider.
- Facilitates session-based access to collaboration services for remote workers, with no need for a separate VPN client.
- Supports a wide range of devices, including Cisco Jabber for smartphones, tablets, and desktops.
- Complements bring-your-own-device strategies and policies for remote and mobile workers.

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



Expressway is available on a dedicated physical appliance such as a CE12100, or as a virtual machine (VM) on a Cisco UCS server.

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.

Standard Features

Standard features on Expressway include the following:

- Secure firewall traversal and session-based access to Cisco Unified Communications Manager for remote workers, without the need for a separate VPN client
- Endpoint registration support.
- SIP Registrar (requires Room or Desktop SIP Proxy. Note that SIP and H.323 protocols are disabled by default on new installs, and can be enabled from **Configuration** > **Protocols** Registration licenses.)
- SIP and H.323 support, including SIP / H.323 interworking
- IPv4 and IPv6 support, including IPv4 / IPv6 interworking
- TURN relay licenses
- Advanced networking
- Device provisioning and FindMe services
- 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
- Rich media session (RMS) support
- 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.
- Can be clustered with up to 6 Expressways to provide n+2 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 13.2 or later
- Active Directory authentication

- Pre-configured neighbor zone defaults for Cisco Unified Communications Manager and for Nortel Communication Server
- Embedded setup wizard using a serial port for initial configuration
- System administration using a web interface or SSH, or via the CIMC port for a CE*nnnn* physical appliance
- Intrusion protection

Do Not Install Other Cisco or Third-Party Software onto Expressway

Cisco does not support the installation of any additional Cisco or third-party software, applications, or agents on Expressway (VMs or physical appliances), unless we state explicitly otherwise. Non-Expressway products may corrupt the Expressway code and must not be installed.

Hardware Appliance and Virtual Machine Options

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

Expressway has these virtualized application deployment types:

- Small (for Cisco Business Edition 6000 or supported VMware ESXi platforms, subject to the required minimum hardware specification)
- Medium (standard installation)
- Large (extra performance and scalability capabilities)

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

Hardware CE Series Appliances

The Expressway is also available as a dedicated CE Series appliance based on UCS hardware. For example, the CE1200 appliance based on a UCS C220 M5L, operates as a medium capacity or large capacity Expressway.

Note The Cisco VCS series is not supported on CE1200 appliances.

Changing the default system size

For appliances deployed as Expressway-E you can manually change the default system size of appliances from Large to Medium, or the other way round. This capability was introduced to mitigate an issue with demultiplexing ports for media traversal on appliances with a 1 Gbps NIC (SFP module) that are configured as Medium systems.

To change the size of the appliance, go to **System** > **Administration** settings page and select the required size from the **Deployment Configuration** list.

Installation information

See *Cisco Expressway CE1200 Appliance Installation Guide* on the Expressway Installation Guides page.

Limitation

Medium Appliances with 1 Gbps NIC - Demultiplexing Ports

If you upgrade a Medium appliance with a 1 Gbps NIC to X8.10 or later, Expressway/Cisco VCS automatically converts the system to a Large system. This means that Expressway-E/Cisco VCS Expressway listens for multiplexed RTP/RTCP traffic on the default demultiplexing ports for Large systems (36000 to 36011) and not on the demultiplexing ports configured for Medium systems. In this case, the Expressway-E/ Cisco VCS Expressway drops the calls because ports 36000 to 36011 are not open on the firewall.

Workaround

From X8.11.4 you can manually change the system size back to Medium, through the **System** > **Administration settings** page (select *Medium* from the **Deployment Configuration** list).

Before X8.11.4, the workaround is to open the default demultiplexing ports for Large systems on the firewall.

About This Guide

This guide describes the various features, services, and capabilities of Expressway. It assumes a fully equipped version of Expressway, so your deployment may not support all of the items described.

The guide only applies to the Cisco Expressway Series product. For information about Cisco VCS, please refer to the *X12.5.x Cisco VCS Administrator Guide* on the Cisco TelePresence Video Communication Server Maintain and Operate Guides page.

Most configuration tasks on Expressway can be done through the web user interface or the command line interface (CLI). The guide mainly describes how to use the web user interface. Some features are only available through the CLI, and these are described where relevant.

Web user interface directions are shown in the format **Menu** > **Submenu** followed by the **Name** of the page that you will be taken to.

CLI commands where provided, are shown in the format:

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

Change History

Table 2: Change History

Date	Change	Reason
June 2023	First published for X14.3. • Updated the following tables "Capacity Guidelines for Standalone Systems, Capacity Guidelines for Clustered Systems, and Fast Path Registration for MRA (Caching Optimization for Registrations)" in chapter "Expressway Capacity and Sizing". • Removed the tables, Standalone Systems, Capacity Guidelines for Clustered Systems, and Fast Path Registration for MRA (Caching Optimization for Registrations) from the chapter "Clustering and Peers." Provided a link to the chapter "Expressway Capacity and Sizing" for details. • Support for Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate, Update to the Command Line Interface • Route calls to US Suicide Prevention Hotline (988) without RMS licenses • Set the Default Value of SIP TLS DH key size to 2048 for Fresh Install and Upgrade	X14.3 release
August 2022	Republished X14.2. Replaced Bug ID	X14.2 release
August 2022	First published for X14.2. • Smart Licensing Export Compliance - Capped at 2500 encrypted signaling sessions to endpoints • New REST API - CDB Rest API Access - Enable/Disable CDB REST API Access • TLS Verification Mode - Enabled server certificate verification by default • TLS 1.3 Support • ECDSA Cipher Preference Over RSA • Alternate Method of Using xCommand FIPS • Reducing Email Notifications • XCP Routing Table • Support for 4+1 and 5+1 Redundancy Models	X14.2 release

Date	Change	Reason
July 2021	Updates for X14.0.2. • Updated the section "Certificate Requirements". Traffic Server Enforces Certificate Verification • New REST API - Status - fail2banbannedaddress • Auto Created CE Zone Status	X14.0.2 release
June 2021	Updates for X14.0.1. • Updated a few security related enhancements, MRA Registration issues using a wrong Traversal Zone are fixed • New REST API - Alarms - view and acknowledge, SNMP Configuration	X14.0.1 release
May 2021	Changed the MRA Registrations (proxied) value for CE1200 in the Table - Standalone Capacity Guidelines - Single Expressway.	Document correction
April 2021	First published for X14.0.	X14.0 release
December 2020	Updates for X12.7.	X12.7 release
October 2020	• Update missing and out of date settings in pre-configured zones. • Remove duplicated content about HSM. • Clarify external/third party gatekeeper meaning in RMS license usage.	Document corrections
October 2020	Update missing and out of date settings in pre-configured zones.	Document correction
October 2020	Updates for X12.6.4 maintenance release (fix for software bug ID CSCvv92477 - configurable DH key length for H.323-SIP interworking). Changes to *Configuring Password Security* topic to reflect that **Enforce strict passwords** applies to all locally-managed accounts since X12.6, not just to local admin accounts.	X12.6.4 maintenance release / document correction
August 2020	Updates for X12.6.2 maintenance release.	X12.6.2 maintenance release
July 2020	Restructure content related to logging and serviceability and integrate content that was formerly in the Expressway Serviceability Guide and is now merged into this guide. Also restructure troubleshooting and diagnostics information into its own chapter.	Document reorganization
July 2020	Updates for X12.6.1 maintenance release including MRA registrations count; and Expressway-E TURN server no longer functions as a generic STUN server.	X12.6.1 maintenance release

Date	Change	Reason
June 2020	Update *Firewall Traversal* section to explain cases of IP address mismatch in STUN packets.	Document clarification
June 2020	Updates for X12.6, add process to restore “Applications” menu if not visible in web UI.	X12.6 release
February 2020	Updates for X12.5.7 maintenance release including “Kari's Law”. **Note** X12.5.7 now withdrawn and replaced with X12.5.9. Clarify option keys for CE1200 appliances.	X12.5.7 maintenance release
January 2020	Update *Cluster License Usage and Capacity Guidelines* section to clarify no capacity gain from clustering Small VMs.	Document correction
December 2019	Clarify not to install other software onto the product. Correct location of VM Size field.	Document clarification Document correction
November 2019	Updates for X12.5.6 maintenance release.	X12.5.6 maintenance release
July 2019	Updated for X12.5.4. Removed references to release key as it is not required to upgrade a system on X8.6.x or later software to 12.5.4 or later. Fix incorrect default value for “Redirect HTTP requests to HTTPS” in the *Network Services* section. CSCvq39362 refers.	X12.5.4 release
June 2019	RMS license consumption table updated, now includes only those scenarios which consume RMS licenses.	Document correction
May 2019	Fix incorrect reference to 488 response code in the description of Meeting Server load balancing setting.	Document correction
April 2019	Updates for X12.5.2 maintenance release (includes support for virtualized Small VMs on VMware ESXi platform).	X12.5.2 maintenance release
March 2019	Updates for X12.5.1 maintenance release.	X12.5.1 maintenance release
February 2019	Reinstate “Services That Can be Hosted Together” table in the Introduction.	Documentation correction
January 2019	Updates for X12.5.	X12.5 release

Date	Change	Reason
December 2018	Retitle for X8.11.4 (no substantive updates). Adjust B2BUA calls status section for CSCvn73111.	X8.11.4 maintenance release
October 2018	Updates for X8.11.3 maintenance release.	X8.11.3 maintenance release (withdrawn)
September 2018	Updated for Webex and Spark platform rebranding, CE1200 appliance, and X8.11.1 release.	X8.11.1 release (withdrawn)
July 2018	Updates for X8.11.	X8.11 release (withdrawn)
July 2017	Updates for 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 corrections
June 2016	Updates for X8.8.	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

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:

http://www.cisco.com/web/about/responsibility/accessibility/index.html

Related Documentation

Table 3: Links to Related Documents and Videos

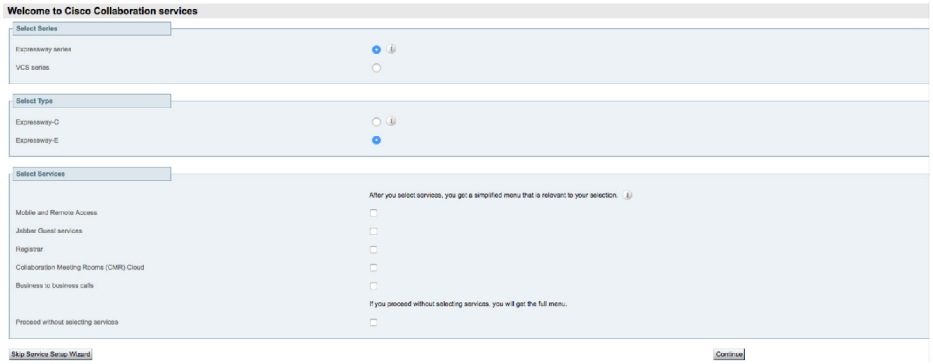
Support videos	Videos provided by Cisco TAC engineers about certain common Expressway configuration procedures are available on the Expressway/VCS Screencast Video List page (search for "Expressway videos")
Installation - virtual machines	*Cisco Expressway Virtual Machine Installation Guide* on the Expressway Installation Guides page
Installation - physical appliances	*Cisco Expressway CE1200 Appliance Installation Guide* on the Expressway Installation Guides page.
Basic configuration for single-box systems	*Cisco Expressway Registrar Deployment Guide* on the Expressway Configuration Guides page
Basic configuration for paired-box systems (firewall traversal)	*Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide* on the Expressway Configuration Guides page
Administration and maintenance	*Cisco Expressway Administrator Guide* on the Expressway Maintain and Operate Guides page (includes Serviceability information)
Clustering	*Cisco Expressway Cluster Creation and Maintenance Deployment Guide* on the Expressway Configuration Guides page
Certificates	*Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway Configuration Guides page
Ports	*Cisco Expressway IP Port Usage Configuration Guide* on the Expressway Configuration Guides page
Unified Communications	*Mobile and Remote Access Through Cisco Expressway* on the Expressway Configuration Guides page

Cisco Meeting Server	*Cisco Meeting Server with Cisco Expressway Deployment Guide* on the Expressway Configuration Guides page *Cisco Meeting Server API Reference Guide* on the Cisco Meeting Server Programming Guides page Other Cisco Meeting Server guides are available on the Cisco Meeting Server Configuration Guides page
Cisco Webex Hybrid Services	Hybrid Services Knowledge Base
Cisco Hosted Collaboration Solution (HCS)	HCS Customer Documentation
Microsoft infrastructure	*Cisco Expressway with Microsoft Infrastructure Deployment Guide* on the Expressway Configuration Guides page *Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet* on the Expressway Configuration Guides page
Rest API	*Cisco Expressway REST API Summary Guide* on the Expressway Configuration Guides page (high-level information only as the API is self-documented)
Multiway Conferencing	*Cisco TelePresence Multiway Deployment Guide* on the Expressway Configuration Guides page

About the Service Setup Wizard (Service Selection Page)

The Service Setup Wizard makes it easier to configure Expressway for its chosen purpose in your environment, and simplifies the web user interface. As well as running the wizard for initial configuration you can subsequently access its service selection page at any time (**Status** > **Overview**). For more details about using the wizard, see the *Cisco Expressway-E and Expressway-C - Basic Configuration guide* on the Expressway Configuration Guides page.

Figure 1: Service Setup Wizard - Example Service Selection Page



453645

Note If you use Smart Licensing, you cannot change the **Series** setting from the Service Selection page/wizard (to convert an Expressway to a VCS product). Instead this process must start with a factory reset (to disable Smart Licensing because it's not supported on VCS). Some of the other settings shown in this example are unnecessary with Smart Licensing and do not appear in the wizard on Expressways that use Smart Licensing.

Services That Can Be Hosted Together

Some services are incompatible and cannot be selected together. The following table provides a matrix of compatible services. The matrix specifies which services you can use together on the same system or cluster.

Table 4: Services That Can be Hosted Together

	Cisco Webex Hybrid Services (Connectors	Mobile and Remote Access	Jabber	Microsoft gateway server	Registration	CMR Cloud	Business to Business calling (includes Hybrid Call Service)
Cisco Webex 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 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

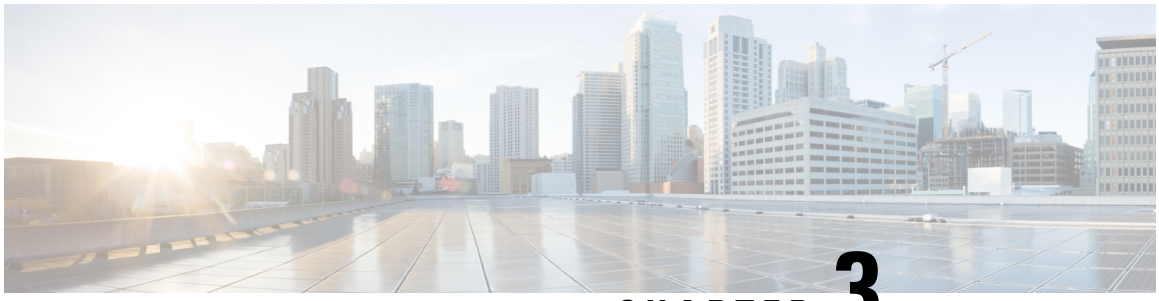
N: No, these services may not be hosted on the same system or cluster

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.



CHAPTER 3

Expressway Interfaces

- About the Web Interface, on page 17
- Web Page Features and Layout, on page 18
- About the Command Line Interface, on page 20
- About the API, on page 21
- Software Versions Supported by Hardware Platforms, on page 22

About the Web Interface

This section summarizes the Expressway web user interface, and the CLI and API.

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 the IP address or 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). The **Overview** page is displayed.

If you receive a warning message regarding Expressway's security certificate, you can ignore this until you are ready to secure the system.

Field Markers

- A red star * indicates a mandatory field
- An orange symbol § 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.

Web Page Features and Layout

This section describes the available features on Expressway web interface pages.

Figure 2: Example list page

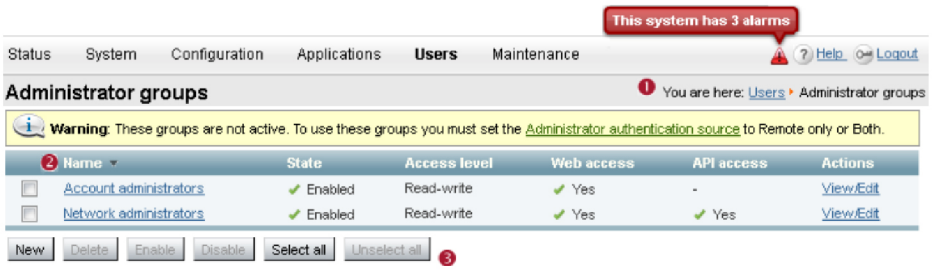
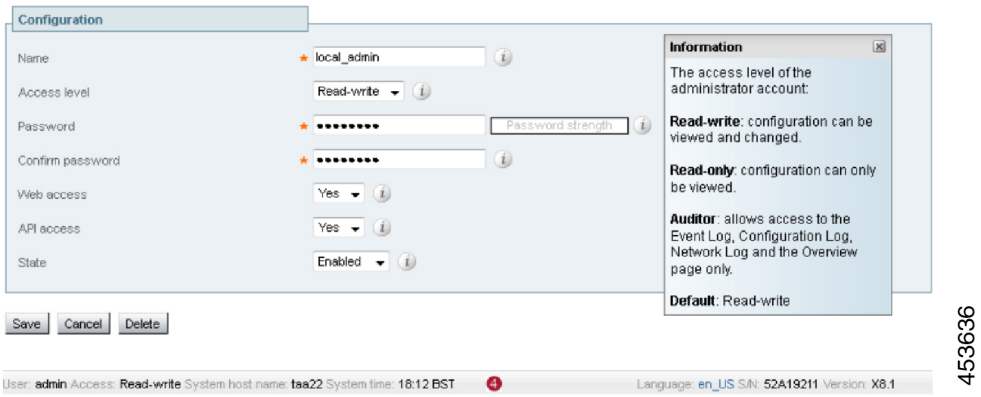


Figure 3: Example configuration page



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

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

Page element		Description
Select All and Unselect All	3	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	4	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 You cannot change configuration settings if your administrator account has read-only privileges.

Missing Application Menu in Web User Interface

When Expressway is installed, the menus that appear in the web user interface are tailored to match the service selections chosen in the Service Setup Wizard. In some cases, depending on the combination of services selected, the **Applications** menu may be missing from the interface. If this happens and you want to restore the menu, do the following:

1. Go to **Status** > **Overview** and click **Run service setup**, to go back to the service setup options.
2. Check the option *Proceed without selecting services* and click **Continue**.

About the Command Line Interface

The Command Line Interface (CLI) is available by default over SSH, and through the serial port on appliance-based systems. 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 as *Admin* (Enter username and password as *Admin*).

   See Enabling SSH Access to Expressway if you prefer to use your private key to authenticate.

4. You can now start using the CLI by typing the appropriate commands.

Note Use the *admin* and *root* accounts for SSH access. Other local or remote accounts are restricted from CLI access through SSH.

Command Types

Commands are categorized into the following groups:

- **xStatus** 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 for a full list of **xStatus** commands.
- **xConfiguration** allow you to add and edit single items of data such as IP address and zones. See Command Reference — xConfiguration for a full list of **xConfiguration** commands.
- **xCommand** these commands allow you to add and configure items and obtain information. See Command Reference — xCommand for a full list of **xCommand** commands.
- **xHistory** provide historical information about calls and registrations.
- **xFeedback** provide information about events as they happen, such as calls and registrations.

Useful Controls

- 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.

About the API

Administrators have access to the Expressway REST API by default, unless the Expressway is in advanced account security mode or if individual access is disabled through the administrator's user configuration options.

The API is self documented using RESTful API Modeling Language (RAML). We provide a *REST API Summary Guide* on the "Expressway Configuration Guides" page, which summarizes how to access the base URL and the RAML definitions, and gives some example requests and responses.

From the X14.2 release, if you are using any of these RAML APIs, you must add a custom header called X-CSRF-Header when making the POST Request. The Header value is not important.

/api/provisioning/restart

/api/provisioning/common/defaultlinks

/api/provisioning/controller/b2bua/microsoftinterop/restartservice

/api/provisioning/domaincerts/domain/<domain>

/api/provisioning/certs/acme/pendingcert

/api/provisioning/certs/acme/pendingcert/deploy

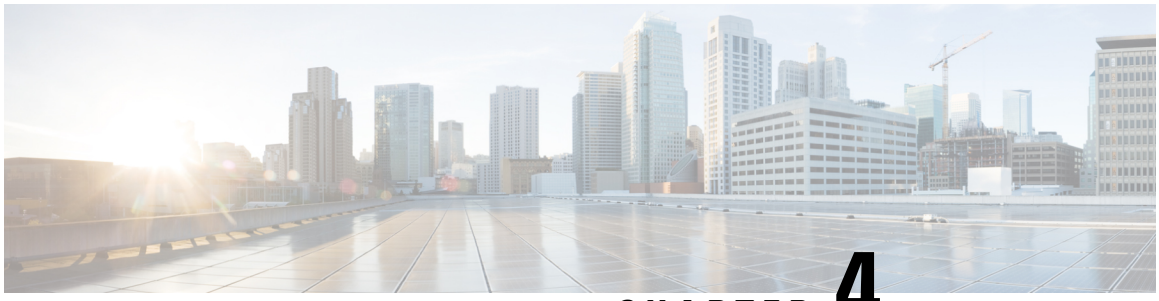
/api/provisioning/domaincerts/domain/<domain>/acme/pendingcert/deploy

Note You need not add any changes to the scripts while using any RAML API other than the above.

Software Versions Supported by Hardware Platforms

Table 5: Expressway Platforms Supported in this Release

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
CE1200 Hardware Revision 2 (preinstalled on UCS C220 M5L)	52E1####	X12.5.5 onwards
CE1200 Hardware Revision 1 (preinstalled on UCS C220 M5L)	52E0####	X8.11.1 onwards
CE1100 (Expressway pre-installed on UCS C220 M4L)	52D#####	Not supported (after X12.5.x) except limited support with X12.6.x versions for maintenance and bug fixing purposes only
CE1000 (Expressway pre-installed on UCS C220 M3L)	52B#####	Not supported (after X8.10.x)
CE500 (Expressway pre-installed on UCS C220 M3L)	52C#####	Not supported (after X8.10.x)



CHAPTER 4

Expressway Capacity and Sizing

- Overview, on page 23
- Important Caveats, on page 23
- Dependencies, on page 24
- Capacity Guidelines for Standalone Systems, on page 24
- Capacity Guidelines for Clustered Systems, on page 25
- Fast Path Registration for MRA (Caching Optimization for Registrations), on page 25
- Intracluster Calls, on page 26

Overview

The maximum supported capacities / sizing for Cisco Expressway Series (not Cisco VCS) are listed in the tables below. These figures/values are guidelines only and are NOT guaranteed, because many factors affect performance in real-life deployments. Expressway supports so many different use cases that it is not possible to provide capacity limits for individual, specific deployments.

Expressway sizing / capacity information is categorized on the basis of the number of supported concurrent registrations and/or calls.

Important Caveats

- The figures/values provided here assume all necessary software licenses are applied.
- The figures/values are tested for specific, dedicated Expressway scenarios. Based on an Expressway or cluster being used for a single service or scenario, such as just for MRA or just for B2B calling. It is not possible to provide tested capacity guidelines for multi-service deployments.
- **N+1 Model**
  - Prior to the X14.2 release, up to 6 Expressway systems can be clustered to yield a total cluster capacity of **four times** that of a single system (except for Small VMs, which have no gain).
  - From the X14.2 release, in the 4+1 redundancy model, up to 5 Expressway systems can be clustered to yield a total cluster capacity of **four times** that of a single system (with 1 redundancy server) (except for Small VMs, which have no gain).

- From the X14.2 release, in the 5+1 redundancy model, up to 6 Expressway systems can be clustered to yield a total cluster capacity of **five times** that of a single system (with 1 redundancy server) (except for Small VMs, which have no gain).
- For Small VMs, clustering is only for redundancy and not for scale and **there is no capacity gain from clustering**.

- The figures/values provided for video calls and audio-only calls are alternatives - the stated capacity is available either for video or for audio, not for both.

Dependencies

The figures/values for calls refer to concurrent calls.

Concurrent calls and Rich Media Session (RMS) licenses do not have a one-to-one relationship. Various factors determine RMS license usage, which means that some calls may be "free" and others may use multiple licenses.

To support 6000 TURN relays on a large system (Large VM or CE1200) you need to enable "TURN Port Multiplexing on Large Expressway" (**Configuration** > **Traversal** > **TURN**).

Small VMs are supported on the Cisco Business Edition 6000 platform, or on general purpose hardware / ESXi which matches the Cisco Business Edition 6000 specification. The figures/values for Small VMs are for M5-based BE6000 appliances.

Capacity Guidelines for Standalone Systems

The table lists the base capacity for a standalone Expressway.

Note

- Expressway Select can exceed 2500 encrypted signaling sessions. There is no encrypted session limit/capping on the number of registrations/calls/sessions (hardware limit still applies).
- Values with PRRH = OFF.

Table 6: Standalone Capacity Guidelines

X14.x					
Platform	**Native Registrations (room/desktop)**	**Calls (Video or Audio-only)**	**RMS Licenses**	**MRA Registrations (proxied)**	**TURN Relays**
CE1200	5000	500 video or 1000 audio	500	7000	6000
Large VM	5000	500 video or 1000 audio	500	3500	6000

X14.x					
Platform	**Native Registrations (room/desktop)**	**Calls (Video or Audio-only)**	**RMS Licenses**	**MRA Registrations (proxied)**	**TURN Relays**
Medium VM	2500	150 video or 300 audio	150	2500	1800
Small VM	2000	20 video or 40 audio (40 non-MRA video)	75	200	1800

Capacity Guidelines for Clustered Systems

To determine the capacity for cluster of size *n+1*, 1 node will be counted towards redundancy and the cluster capacity will be a factor of n x single node capacity in table Table 6: Standalone Capacity Guidelines.

The maximum cluster size supported is 6.

Note For Small VMs, where the figures/values for clustered systems and for standalone systems are always the same (because there's no capacity gain from clustering Small VMs).

Fast Path Registration for MRA (Caching Optimization for Registrations)

From X12.7, Expressway supports Fast Path Registration for MRA-based devices. This optimizes routing processes, reducing the server workload, so leading to increased capacities. Expressway caches the initial routing calculation and then uses a Pre-Routed Route Header to forward subsequent packets to the destination using the cached routing result. This has the following benefits:

- Reduces the routing workload.
- Increases registration capacity.
- Ensures that each media packet follows the same route path.

Important This feature only applies to MRA deployments. The increased capacity and other benefits do not apply to non-MRA Expressway deployments.

Fast Path Registration is supported for the following SIP methods: REGISTER. Configuration is through the command line interface, and detailed instructions are provided in the latest *Expressway MRA Deployment Guide*.

Remember Make sure you restart Expressway.

The tested results for a standalone Expressway MRA deployment (Expressway-C + Expressway-E) when this feature is configured are:

Note

- Expressway Select can exceed 2500 encrypted signaling sessions. There is no encrypted session limit/capping on the number of registrations/calls/sessions (hardware limit still applies).
- Values with PRRH = ON.

Table 7: Standalone Capacity Guidelines

X14.x			
Platform	**Calls (Video or Audio-only)**	**RMS Licenses**	**MRA Registrations (proxied)**
CE1200	500 video or 1000 audio	500	7500
Large VM	500 video or 1000 audio	500	4000
Medium VM	150 video or 300 audio	150	3000
Small VM	20 video or 40 audio (40 non-MRA video)	75	200

To determine the capacity for cluster of size *n+1*, 1 node will be counted towards redundancy and the cluster capacity will be a factor of n x single node capacity in table Table 7: Standalone Capacity Guidelines..

The maximum cluster size supported is 6.

Note For Small VMs, where the figures/values for clustered systems and for standalone systems are always the same (because there's no capacity gain from clustering Small VMs).

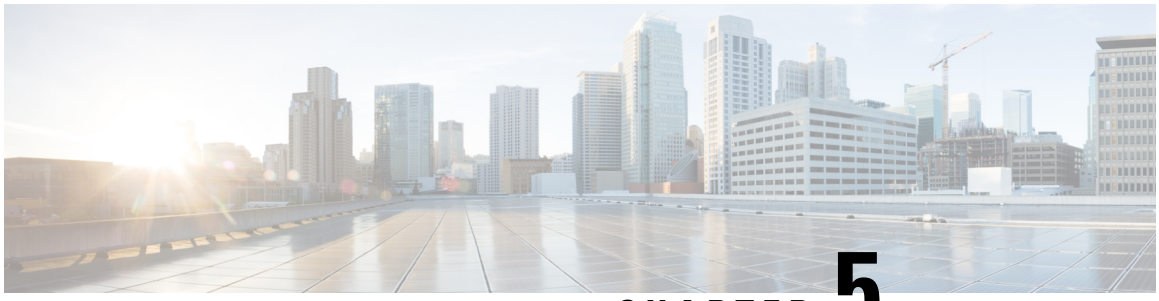
Intracluster Calls

License usage when endpoints are registered to different peers in the same cluster, depends on call media traversal across the cluster:

- If call media does not traverse the cluster peers, a call between the endpoints does not use any RMS licenses (it's a “Registered” call).
  - If any of the endpoint is not registered to Cisco infrastructure then calls will use RMS license.

- If call media does traverse the cluster peers, a call between the endpoints uses an RMS license on the Expressway where the B2BUA is engaged.
    - If both the endpoints are registered to Cisco infrastructure then call will not use RMS license.

More information about how licenses are used in clustered systems is provided in the licensing section of this guide.



CHAPTER 5

Call Types and Licensing

- Call Types, on page 29
- Room and Desktop Registrations on Expressway, on page 31
- License Usage for Device Registrations, on page 33
- RMS License Consumption Table, on page 33
- License Bypass for Calls to Collaboration Meeting Rooms (CMRs), on page 34
- License Usage for Cisco Video Integration (CVI) Calls, on page 35
- Intracluster Calls, on page 35
- Limitations, on page 36

Call Types

Expressway distinguishes between the following types of call:

- Registered. That is, room and desktop registrations
- Rich Media Sessions (RMS)

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 – video or audio calls from devices located outside the enterprise that are routed via the Expressway firewall traversal solution to endpoints registered to Unified CM.
- 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.
- Expressway does not support ICE candidates in the SDP of a 1xx Provisional Message

RMS

These calls consume RMS licenses and consist of every other type of video or audio call that is routed through the Expressway. RMS licenses are consumed on the exit node of the Expressway in the following scenarios:

- B2B
- Jabber Guest
- Interworked or gatewayed calls to third-party solutions (If the third-party endpoint is not registered to Cisco infrastructure)

Expressway may take the media or just the signaling.

Audio-only SIP calls are treated distinctly from video SIP calls. Each RMS license allows either 1 video call or 2 audio only SIP calls. So for example, a 100 RMS license would allow 90 video and 20 SIP audio-only simultaneous calls. Any other type of audio-only call uses an RMS license.

Note

- Expressway defines an “audio-only” SIP call as one that was negotiated with a single “m=” line in the SDP. For example, if a person makes a “telephone” call but the SIP UA includes an additional m= line in the SDP, the call will use a video call license.
- While an “audio-only” SIP call is being established, it is treated (licensed) as a video call. It only becomes licensed as “audio-only” when the call setup has completed. This means that if your system approaches its maximum licensed limit, you may be unable to connect some “audio-only” calls if they are made simultaneously.
- The Expressway does not support midcall license optimization.
- For deployments with TelePresence Conductor, license consumption is only applicable when TelePresence Conductor is deployed with a B2BUA base configuration and not in a policy server base deployment.
- SIP to H.323 interworking uses an RMS license (if any of the endpoints are not registered to cisco infrastructure) on the node where interworking takes place.
- WebRTC, MRA, and Cisco Webex sessions do not consume RMS licenses.

Limitation

Resource Usage Call Counters Increment Incorrectly for “audio-only” Calls

Condition: Expressway should ideally keep the video counters at zero if a video call is never made.

Explanation: The call counters in the Expressway Web User Interface under **Status** > **Overview** page can increment non-intuitively under certain scenarios. Before a call connects, the counters are incremented as

video calls. After the call connects, if no video is negotiated, the video counter decrements, and “audio-only” call counter increments. It is observed on early-offer calls as well when the Expressway never sees video capabilities.

The following **behaviors** are observed:

1. If an endpoint makes an “audio-only” call through an Expressway and the far-end does not answer, the call is counted as a “Current video” call while it is ringing. Subsequently, the call is counted towards the “Peak video” calls as well.
2. If multiple “audio-only” calls occur simultaneously: For example, 4 endpoints joining a meeting at once, the “Current video” counter increments 4 times before the calls connect. The “Peak video” counter will permanently increase to 4 . After the calls connect, the “Current video” counter is decremented to 0 and the audio call counters are incremented correctly.

These counters increasing can lead to confusion about video calls unexpectedly traversing an Expressway pair that is only supposed to handle audio calls. The Expressway should ideally keep the video counters at zero if a video call is never made.

Room and Desktop Registrations on Expressway

If Expressway is configured as a SIP registrar or H.323 Gatekeeper, it needs to be licensed for concurrent systems (the Unified CM model) and not for concurrent calls.

For SIP deployments, you do this by adding either or both of the following license types to the Cisco Expressway-C or Cisco Expressway-E:

- TelePresence Room System License
- Desktop System License

The following SIP devices register as desktop systems; all other devices are considered room systems:

- Cisco TelePresence EX60
- Cisco TelePresence EX90
- Cisco Webex DX70
- Cisco Webex DX80
- If you use Cisco Jabber Video for TelePresence (Movi) soft clients (now end-of-sale), they also register to Expressway as desktop systems.

Note To register as desktop systems (for SIP), DX systems must be running version CE8.2 or later, and EX systems must be running TC7.3.6 or later. DX and EX systems running earlier versions still register for SIP, but will consume a room system license.

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, although H.323 is available as a fall back for endpoints that do not support SIP.

Licensing considerations when Expressway is the SIP registrar / H.323 Gatekeeper

- Option keys containing licenses for local registrations are installed on the Cisco Expressway-C and/or the Cisco Expressway-E depending on where the endpoints are registered. These licenses are pooled in a cluster, which means that Expressway 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 same domain cannot also be used for direct Expressway-E registrations.
- If you have existing licenses on the Expressway-C and want to register some or all of your existing licensed endpoints to the Expressway-E, manually delete the relevant licenses from the Expressway-C and reload them on the Expressway-E.
- The Large VM and the CE1200 and CE1100 appliances can support up to 5000 registrations, subject to the appropriate licensing. For MRA registrations (proxied to CUCM) the limits are 5000 for the CE1200, and 2500 for the Large VM and the CE1100. Local registrations, proxy registrations (via Expressway-E) and MRA registrations all count towards the registration limit.
- Proxy registration is possible with SIP endpoints only and does not apply to H.323 endpoints.
- FindMe device provisioning is supported with Cisco TMSPE (although this support is deprecated from Expressway version X12.5).

Licensing considerations if device registers as both SIP and H.323

Be aware that multiple licenses are consumed if the same device registers to Expressway both as SIP and as H.323. For example, say a DX80 is registered on Expressway-C as a SIP user agent, and also as an H.323 endpoint (with the same or different URL/DN). A Desktop System License will be consumed for the SIP registration, and a TelePresence Room System License will be consumed for the H.323 endpoint registration. The same dual license usage would apply, for example, if a Cisco Webex Room similarly registers for both SIP and H.323.

RMS license usage

The 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 are not used for the following call types:
  - Calls between registered systems. Here, “registered systems” means systems registered directly to the Expressway, 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. 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 use RMS licenses.
  - Calls from registered systems (as above) to Cisco Collaboration Cloud.
- Calls from registered systems to all other systems use one RMS license. Including, but not limited to, the following call types:
  - Business to business calls. Require one RMS license on Expressway-E.
  - Business to consumer calls (Jabber Guest). Require one RMS license 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.

Limitation

Proxy Registration Resulting in Incorrect Registration License Consumption On Expressway C Cluster

Proxy registrations may consume duplicate registration licenses on a cluster Expressway C deployment. This results in proxy registering on more than one Expressway C at the same time (refresh register proxy to different Expressway C than active registered Expressway C).

This is due to the Expressway C cluster nodes not sharing awareness of existing registrations for the same Call-ID.

Duplicate registration status (and consumption of duplicate registration license) will clear out once registration TTL expires.

License Usage for Device Registrations

Devices that are directly registered on Expressway (Cisco Expressway-C or Cisco Expressway-E) consume licenses as follows:

- SIP. Cisco TelePresence EX60, Cisco TelePresence EX90, Cisco DX70, and Cisco DX80 endpoints consume a desktop license. Other SIP endpoints consume a room system license.
- H.323. Each registered H.323 endpoint consumes a room system license.

SIP proxy registrations on the Cisco Expressway-C consume the same licenses as for direct SIP registrations. SIP proxy registrations on the Cisco Expressway-E do not consume licenses.

Note Registrations are counted per *alias*, not per device (IP address). So a registration request with multiple aliases, like an MCU, consumes multiple room licenses even if only a single device is registered on Expressway.

RMS License Consumption Table

This table lists the scenarios in which Expressway consumes RMS licenses. References to "Third-party Gatekeeper" mean the gatekeeper is connected to Expressway-C; references to "External" mean the gatekeeper is connected to Expressway-E.

Calling endpoint registered to ...	Called endpoint registered to...	Expressway-C	Expressway-E
Unified CM	Expressway-C (Lync)	1 Expressway-C (Lync Gateway)	0
Unified CM	External	0	1

Calling endpoint registered to ...	Called endpoint registered to...	Expressway-C	Expressway-E
Unified CM	Third-party Gatekeeper	1	0
Expressway-C	External	0	1
Expressway-C (Remote [SIP] - proxy)	External	0	1
Expressway-C (SIP)	Third-party Gatekeeper	1	0
Expressway-C (H323)	Third-party Gatekeeper	1	0
Expressway-C (Remote [SIP]) - proxy	Third-party Gatekeeper	1	0
Expressway-C	Expressway-C (Lync)	0	1 Expressway-C (Lync Gateway)
Expressway-C (Remote)	Expressway-C (Lync)	0	1 Expressway-C (Lync Gateway)
Expressway-C (SIP)	Third-party SIP server	1	0
Expressway-C (H323)	Third-party SIP server	1	0
Expressway-E (SIP)	External	-	1
Expressway-E (H.323)	External	-	1

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/ H.323 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 use licenses, they do use 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 consume CMR licenses but not RMS licenses.

License Usage for Cisco Video Integration (CVI) Calls

Cisco Video Integration (CVI) on Expressway does not require any licenses. It will raise an alarm that licenses have expired, but functionality will remain intact.

Intracluster Calls

License usage when endpoints are registered to different peers in the same cluster, depends on call media traversal across the cluster:

- If call media does not traverse the cluster peers, a call between the endpoints does not use any RMS licenses (it's a “Registered” call).
    - If any of the endpoint is not registered to Cisco infrastructure then calls will use RMS license.
- If call media does traverse the cluster peers, a call between the endpoints uses an RMS license on the Expressway where the B2BUA is engaged.
    - If both the endpoints are registered to Cisco infrastructure then call will not use RMS license.

Usage Limits

Usage limits have two aspects: physical capacity and licensing. The physical constraints of the Expressway cluster determine the ultimate limits, and within that the capacity available to the system is determined by its licensing.

Physical capacity limits

The maximum number of licenses that each Expressway peer can actually use depends on the physical capacity of the appliance or VM. For example, the maximum capacity supported by a large Expressway VM is 500 concurrent video calls.

Capacity alarms are raised if either of the following usage thresholds are reached:

- Number of concurrent calls reaches 90% of the capacity of the cluster.
- Number of concurrent calls on any one unit reaches 90% of the physical capacity of the unit.

License limits

The licensed capacity of a cluster will depend on whether the system uses classic PAK-based licensing, or smart licensing. For PAK-based, for example, if two large VMs are clustered and each has 300 RMS licenses installed, the effective capacity of the cluster is 600 concurrent video calls. If one peer is removed from the cluster, the remaining peer retains all 600 RMS licenses for 14 days, but only supports up to 500 concurrent video calls.

For smart licensed systems, the licensed capacity depends on the license pool that's assigned to your organization's registered account with the Cisco Smart Software Manager.

Limitations

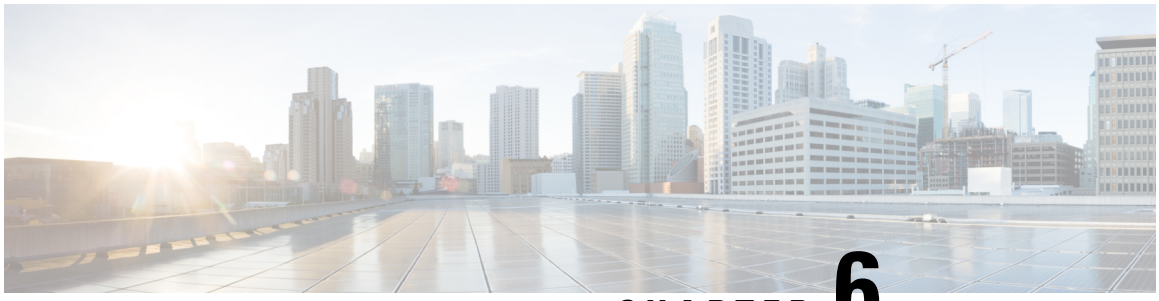
Licensing Behavior with Chained Expressway-Es

If you chain Expressway-Es to traverse firewalls (from X8.10), be aware of this licensing behavior:

- If you connect through the firewall to the Cisco Webex cloud, each of the *additional* Expressway-Es which configure a traversal zone with the traversal client role, will consume a Rich Media Session license (per call). As before, the original Expressway-C and Expressway-E pair do not consume a license.
- If you connect through the firewall to a third-party organization (Business to Business call), *all* of the Expressway-Es in the chain, including the original one in the traversal pair, will consume a Rich Media Session license (per call). As before, the original Expressway-C does not consume a license.

Option Keys Only Take Effect for 65 Keys or Fewer

If you try to add more than 65 option keys (licenses), they appear as normal in the web interface (**Maintenance** > **Option keys**). However, only the first 65 keys take effect. Additional keys from 66 onwards appear to be added, but actually the does not process them. Bug ID CSCvf78728 refers.



CHAPTER 6

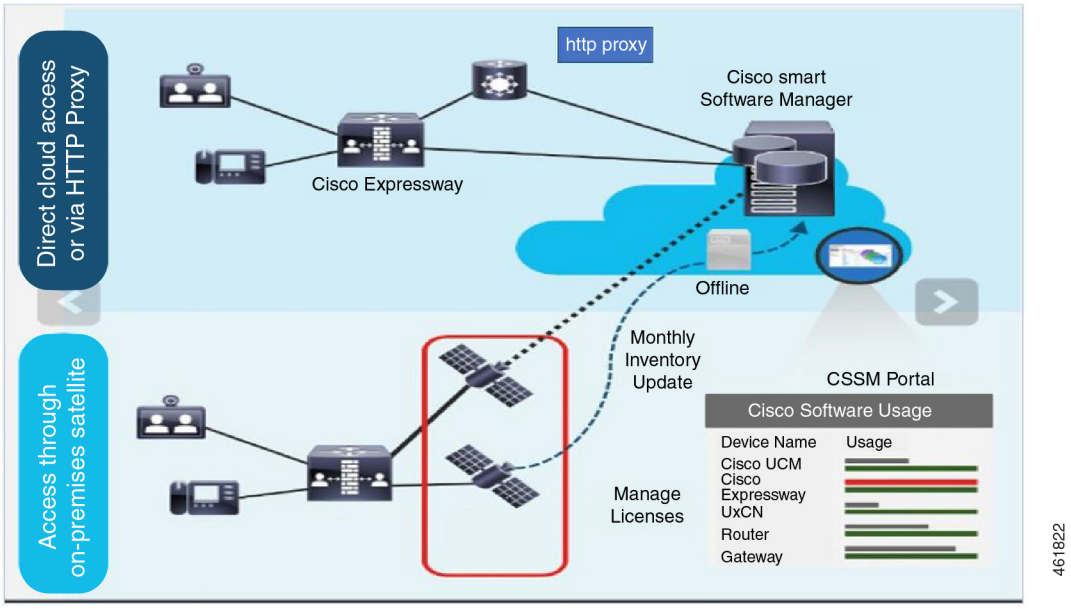
Smart Licensing

- About Smart Licensing, on page 37
- Before You Enable Smart Licensing, on page 43
- Smart Licensing Settings, on page 43
- Configure Smart Licensing, on page 47
- Manage Smart Licensing Registrations and Authorizations, on page 50
- About Cisco Smart License Reservation and Its Types, on page 53
- Smart Licensing Export Compliance, on page 82
- Limitations, on page 83

About Smart Licensing

Note Cisco Expressway X14.2 **only** supports Smart Licensing and is capped at 2500 encrypted signaling sessions to endpoints. It also includes changes in the trafficserver behavior (bug ID CSCwc69661 refers) that can lead to MRA failures - see here. For detailed information, see the *Cisco Expressway and Cisco TelePresence Video Communication Server Release Note (x14.2)* and *Cisco Expressway Administrator Guide (X14.2) before upgrading to X14.2*.

Cisco Smart Software Licensing is a new way to think about licensing. From X14.2 release, Smart Licensing is typically managed with the cloud-based Cisco Smart Software Manager (CSSM). Alternatively, deployments that need an on premises approach can use the Smart Software Manager On-Prem product (formerly known as “Smart Software Manager satellite”). Basically it is a cloud-based, software license management solution. It simplifies the licensing experience across the enterprise and makes it easier to purchase, deploy, enables you to automate time-consuming, manual licensing tasks. The solution allows you to easily track the status of your license and software usage trends. It provides visibility into license ownership and consumption through a single, simple user interface.



You place an order on Cisco Commerce and the order is associated with the smart account, this information is populated on Smart Software Manager, which resides on cisco.com. Now you have a complete view on what you have ordered and purchased.

You can use Smart Licensing to:

- See the license usage and count.
- See the status of each license type.
- See the product licenses available on Cisco Smart Software Manager or Smart Software Manager On-Prem.
- Renew License Authorization with Cisco Smart Software Manager or Smart Software Manager On-Prem.
- Renew Registration
- Deregister with Cisco Smart Software Manager or Smart Software Manager On-Prem.
- Reregister License with Cisco Smart Software Manager

Important

- Product Activation Keys (PAK) Licensing (Option Keys) are removed from version X14.2.
- Smart License is default and the only licensing mode for Expressway-C and Expressway-E.
- We recommend you to enable Smart License before upgrading Expressway to version X14.2. This will help while reverting to a previous image.
- You are not allowed to add the Microsoft Interoperability (MS Interop) key from version X14.2. This functionality is available only in cases where you have the MS Interop options before upgrade. But once on X14.2, you cannot add MS Interop key.
- Once Smart Licensing is turned ON, you do not have an option for reverting to Cisco VCS through **Service Select**.
- Once Smart Licensing is turned ON, you cannot disable it and revert to legacy licensing. There is no option available to revert it to Cisco VCS (except for a Factory Reset), either.
- For Cisco VCS, legacy/option key license mode remains the only licensing mode.
- When Cisco VCS is converted to Expressway Series X14.2, Smart License mode is turned *ON* automatically.
- Smart Licensing is FIPS compliant. For more information, see Prerequisites for Configuring FIPS140-2 Cryptographic Mode.
- In Smart License mode, the functionality is enabled by default and hence they are not needed or supported and may not be converted in the License Registration Portal.

This product has Smart Licensing *enabled* (through CLI and GUI), is registered to CSSM, and reports license consumption to CSSM. Two models exist to report the usage:

- **Direct Model**- Use this model in networks where devices can communicate directly to the Internet or can connect to the Internet via a HTTPS proxy. Communication to Cisco.com is through HTTPS, therefore all traffic is encrypted during transport. If the traffic is sent through a HTTPS proxy, all communications between devices and Cisco.com are channeled through a centralized location if additional inspection or security policies have to be applied.
- **Mediated Deployment Model**- Use this model in networks where devices cannot connect to the Internet and therefore cannot reach Cisco.com. This deployment model requires installing a CSSM satellite virtual machine on your premises which all internal hosts can reach. The on-premise satellite can be deployed in a connected mode that synchronizes with CSSM. The synchronization with cisco.com can be either monthly, weekly, or can be deployed in a totally disconnected configuration requiring manual file uploads and downloads to keep the satellite in sync. It is recommended to sync at least every 30 days.

Factory Reset

The following are a few changes to the way Factory Reset works for Expressway Devices.

- Cisco VCS Factory Reset is **unchanged**.
- **Flag Removed**: Flag `**-o**` (saving of the option keys) is removed from the Expressway factory reset.
- To reset the unit to factory default settings, at the command prompt, execute the following command.

Note Use the chosen flags (if you have any) when you perform a factory reset or you will be prompted with the following list if you do not give any flags in the command.

factory-reset [list of flags]

```
************************************************************
Warning! This operation resets the unit to factory default settings!
************************************************************

To cancel operation before final confirmation press Ctrl+C
Keep brand and type of the device [YES/NO]? yes
Keep smart licensing settings [YES/NO]? no
Keep FIPS 140 configuration [YES/NO]? no
Keep IP configuration [YES/NO]? yes
Keep dedicated management interface configuration [YES/NO]? yes
Keep ssh keys [YES/NO]? yes
Keep server certificate, associated key and CA trust store [YES/NO]? yes
Keep root and admin passwords [YES/NO]? yes
Save log files [YES/NO]? yes

Are you sure you want to continue [YES/NO]? yes
```

- **New Flags Added**: Two new flags `**-v**` (device brand and type) and `**-t**` (Smart License configuration settings) are added.
  - '**-v**' flag: When the factory reset is triggered and the `**-v**` flag is chosen, the device prompts you to save the brand and box type of their device (where brand is Expressway Series or Cisco VCS and type is Expressway-E or Expressway-C).

    Condition:

    Choice is "No": The default values are Expressway-C and Cisco VCS.
  - '**-t**' flag: When the factory reset is triggered and the `**-t**` flag is chosen, the device prompts you to save the Smart Licensing configuration.

    Conditions:

    - **Choice is "No"**: The Smart Licensing is reverted to *'Direct'* if the device is still an Expressway.
    - **Choice is "Yes"**: The Smart Licensing configuration and registration (if it exists) is preserved.

      In this case, after factory reset the device will go offline until the DNS settings are configured. This means, you will see two different alarms indicating the Smart License registration and authentication are not working. These alarms will clear when the device goes back online.

      For more information on alarms (Alarm IDs - 30042 and 30044), see Alarms Reference.

- The new factory reset is FIPS compliant.
- At the command prompt, execute the following command:

  `# factory-reset --help` - Lists all the available options.

Restrictions for Smart Licensing

You are not allowed to add the Microsoft Interoperability (MS Interop) Option Key from version X14.2. This functionality is available only in cases where you have the MS Interop Option Key before upgrade from Cisco VCS to Expressway Series. But once on X14.2, you cannot add MS Interop Option Key.

Note After Factory Reset, if the MS Interop option key is on the device, it will be preserved.

How Smart Licensing Works

Cisco Smart Software Licensing (Smart Licensing) is a new approach to licensing which is enabled across multiple Cisco products. It simplifies licensing and makes license ownership and consumption clearer. Devices self-register and report license consumption, which removes the need to use option keys (Product Activation Keys). License entitlements are pooled in a single account that can be used across Expressways or across different clusters of Expressways. You can use a license on any compatible device owned by your company and move them around to meet the needs of your organization.

You use Smart Licensing to register/deregister Expressway with the Cisco Smart Software Manager (CSSM) or the Cisco Smart Software Manager On-Prem to view/monitor smart license usage, count/manage licenses, know the status per license type, and renew license authorizations. CSSM is hosted on the Cisco Software Manager and allows product instances to register and report license consumption to it.

There are two main deployment options for Smart Licensing:

- Cisco Smart Software Manager
- Cisco Smart Software Manager On-premises

Cisco Smart Software Manager

The Cisco Smart Software Manager is a cloud-based service that handles your system licensing. It enables you to manage all of your Cisco Smart software licenses from one centralized website. With Cisco Smart Software Manager, you can organize and view your licenses in groups called virtual accounts (collections of licenses and product instances). The Cisco Smart Software Manager allows you to:

- Create, manage, track, or view virtual accounts
- Create and manage Product Instance Registration Tokens
- Transfer licenses across virtual account or view licenses
- Transfer, remove, or view product instances
- Remove registered product instance
- Run reports against your virtual accounts
- View overall account information

To access or for additional information about Cisco Smart Software Manager, go to https://software.cisco.com.

On-premises option - using Smart Software Manager On-Prem

If you do not want to manage Cisco products directly using Cisco Smart Software Manager, either for policy or network availability reasons, you can instead use Smart Software Manager On-Prem. This is an on-premises component of Cisco Smart Licensing and products register and report license consumption to it in the same way as with Cisco Smart Software Manager.

Smart Software Manager On-Prem can be deployed in either Connected or Disconnected mode, depending on whether the satellite can connect directly to cisco.com.

- **Connected**. Used when there is direct connectivity to cisco.com. Smart account synchronization occurs automatically.
- **Disconnected**. Used when there is no direct connectivity to cisco.com. Smart Account synchronization must be manually uploaded and downloaded.

More information

For detailed product information about the Cisco Smart Software Manager, see Cisco Smart Software Manager. Or for information about the on-prem manager, see Smart Software Manager On-Prem.

Creating a Smart Account

Smart Account provides the repository for Smart enabled products and enables you to manage Cisco Licenses. Once they are deposited, you can activate licenses, monitor license usage and track them. You can manage your Smart Account directly. A Smart Account is needed to fully utilize the license management features of the smart enabled products. The creation of Smart Account is a one-time setup activity.

Navigate to the Cisco Software Central web page:

https://software.cisco.com/

The **Cisco Software Central** page is displayed.

Note You need a Smart Account to use Smart Licensing.

Requesting License Reservation for Your Smart Account

Complete the following steps to request license reservation to your Smart Account in Cisco Smart Software Manager:

1. Go to Support Case Manager.
2. Click **OPEN NEW CASE**.
3. Select **Software Licensing**.

The licensing team will contact you to start the process or for any additional information.

Before You Enable Smart Licensing

This section has some caveats to be aware of before you implement Smart Licensing on Expressway.

Caution After Smart Licensing is enabled, the only way to revert to PAK-based licensing (or to convert an Expressway system to a Cisco VCS system) is with a factory reset. Because a factory reset reinstalls the software image and resets the Expressway configuration to the default, we strongly advise you to backup the Expressway data before you enable Smart Licensing.

Product Instance Evaluation Mode

After enabling Smart Licensing on Expressway allows only a 90-day Evaluation period. During the evaluation period, Expressway does allow cluster-related configuration. After the evaluation period, if Expressway is not registered with either CSSM or Smart Software Manager On-Prem, the product moves to Unauthorized state. In the Unauthorized state, it does not allow new device registrations until the product is registered.

After Smart Licensing is enabled, you cannot use option keys on the Expressway. So, if you want to use any Expressway functions that still require option keys, use PAK-based licensing.

We recommend you to set up Smart and Virtual accounts before you review the general Expressway licensing information in Call Types. For details, see Cisco Smart Accounts.

Smart Licensing Settings

This section describes how to use the Smart Licensing settings in the Expressway web interface to do the following:

- Enable Smart Licensing.
- Register and deregister the Expressway with CSSM or Smart Software Manager On-Prem.
- Manually renew the registration and license authorization.
- View system license usage information as it is reported to CSSM or Smart Software Manager On-Prem. (Licenses are assigned to your organization's Smart Account and are not locked to a device.)

Note This section describes the web interface. For information about CLI commands for Smart Licensing, see the *Command Reference* section of this guide.

Table 8: Smart Licensing settings on Expressway

Field	Description
Smart licensing mode	Enables Smart Licensing on this Expressway product instance. Before you select this option, review the Smart Licensing Settings section. **Note** It is always recommended to take a configuration backup in order to avoid any partial or complete configuration lost scenario.
Transport settings	Determines how this Expressway product instance communicates with CSSM to send and receive usage information. **Caution** If the Expressway product instance is already registered, you must first deregister it if you want to change transport settings from Direct (CSSM) to On-Prem, or the other way round. Choose Transport settings under licensing page, as per your smart licensing deployment model.
Transport settings	*Direct*: Expressway sends usage information directly over the internet and no additional components are needed. This is the default setting. To use the Direct option, you must configure DNS settings on Expressway so that it can resolve cisco.com. If you choose not to configure the domain and DNS on Expressway, you can instead select Smart Software Manager On-Prem or proxy server. If you choose not to use the DNS server in your deployment and not to connect to the internet, you can select the Smart Software Manager On-Prem with manual synchronization in disconnected mode. *Smart Software Manager On-Prem*: Expressway sends usage information to an on-premise CSSM. Periodic information exchange keeps the databases in sync between Smart Software Manager On-Prem and CSSM. In the **URL** field, be sure to enter the **exact Smart Transport URL of Smart Software Manager On-Prem**. Enter the protocol and FQDN of the satellite server prefixed to "*SmartTransport*". This is an example of a valid transport URL: *https://example.com/SmartTransport* For more information about installing or configuring Smart Software Manager On-Prem, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html. *Proxy Server*: Optionally you can use this setting to have Expressway send usage information over the internet through a proxy server. Enter the following details: • **Proxy address** IPv4 address or FQDN of the proxy server. • **Port** Port on which the proxy server is listening for requests. • **Username** Username for authorizing requests at the proxy server. • **Password** Password for authenticating the authorized user.

Field	Description
Do not share my hostname or IP address with Cisco	Check this check box if the hostname and IP address of this Expressway product instance must not be exchanged with CSSM or Cisco Smart Software Manager On-Prem
Additional operations	The **Additional operations** drop-down list is activated after a successful registration. • *Renew authorization now*: Perform this operation if automatic authorization status renewal fails due to network connectivity issues with CSSM. • *Renew registration now*: Perform this operation if automatic registration renewal fails due to network connectivity issues with CSSM. • *Deregister*: The product reverts to Unregistered mode. All license entitlements used for the product are released immediately to the virtual account and are available for other product instances to use it. If the evaluation period has not expired, the product reverts to evaluation mode.
Product Instance Registration token	Enter the Product Instance Registration token that you generated from CSSM or Smart Software Manager On-Prem to register the product.
Reregister this product instance if it is already registered	Check this check box to reregister this Expressway product instance to a different virtual account.
Register	Click **Register** to register the Expressway with CSSM or Smart Software Manager On-Prem. (Changes to **Reregister** after successful registration.)
Licensing status	
Registration status	Displays the registration status of this Expressway product instance: • *Registered*: Product is registered. • *Unregistered*: Product is not registered. • *Unregistered*: *Registration Expired*: Registration has expired for this product. • *Unregistered*: *Registration Pending*: Registration is in progress. • *Unregistered*: *Registration Failed*: Product registration failed because the token is invalid or expired.

Field	Description
License authorization status	Displays the license authorization status of this Expressway product instance. • *Authorized*: Product is authorized and in compliance state. • *Authorization Expired*: Authorization has expired. This usually happens if the product has not communicated with Cisco for 90 continuous days. • *Out-of-compliance*: Status for this product is out-of-compliance, due to insufficient licenses. • *No Licenses in Use*: No licenses are being consumed by the product. • *Evaluation Mode*: Product is in evaluation mode and not yet registered with Cisco. • *Evaluation Expired*: Evaluation period has expired. • *Not Applicable*: Product is unable to determine the current registration status.
Smart account	Displays information about the customer's Smart Account with Cisco. The Smart Account is created from the *Request Smart Account* option under the **Administration** section of Cisco Software Central.
Virtual account	A self-defined element to reflect the company organization. Licenses and Product instances can be distributed across virtual accounts. Created and maintained by an administrator on CSSM or Smart Software Manager On-Prem. The administrator needs full visibility to company assets.
Export-Controlled Functionality	Displays one of the following states: • *Allowed*: Export-controlled functionality is enabled in the token with which this product was registered. • *Not Allowed*: Export-controlled functionality is not enabled in the token with which this product was registered. The **Allow export-controlled functionality on the products registered with this token** check box is not displayed for Smart Accounts that are not allowed to use Export-Controlled functionality.
License usage	

Field	Description
Update usage details	License usage provides summary and detailed information on system license usage as it's reported to CSSM or Smart Software Manager On-Prem. The information is auto-updated every 6 hours. Optionally you can manually update the usage details by clicking **Update usage details**. However, this is a resource intensive operation and we don't recommend using it frequently. It may take upwards of a minute depending on the size of the system. Within a cluster if 1 node consumes more than the installed licenses then only the number of installed licenses will be reported. For example, In a 2 node cluster, if each node has 10 licenses then 1 node can consume a maximum of 20 licenses. In that case, it will be reporting only the installed number of licenses that is, 10 licenses instead of 20 licenses. **Note** For more information, see “Resource usage” section of the "Overview" page in the *Cisco Expressway Web User Interface*.
License type	Lists the license types - Rich Media Session or Room/Desktop Registrations.
Current usage	Shows current license usage by license type. If a license type is not in use (being consumed) it is not displayed here.
Status	Displays the status of each license type. • *Authorization Expired*: Authorized period has expired. • *Evaluation Mode*: The agent is using the evaluation period for this entitlement. • *Evaluation Expired*: Evaluation period has expired. • *Authorized*: In compliance (authorized). • *Invalid*: Error condition state. • *Invalid-tag*: The entitlement tag is invalid. • *Not Authorized*: Enforcement mode is not applicable. • *Out of compliance*: Out of compliance. • *Waiting*: The initial state after an entitlement request while waiting for the authorization request response.

Configure Smart Licensing

This section describes the tasks required to configure Smart Licensing.

Before You Start

Review the cautions and other information in Before You Enable Smart Licensing.

The following additional configuration caveats apply:

- The only supported transport protocol is HTTPS between Expressway and CSSM / Smart Software Manager On-Prem.
- If a communication issue occurs with the registration server when you register the Expressway product instance, the registration fails with this message: *The last attempt to renew smart software licensing registration is in progress because of the following reason: HTTP Server Error 200: Operation timed out*.

  The product instance reattempts to register at 15-minute intervals. Refresh the page on your browser after each reattempt, to check current registration status. If the communication issue is resolved during the reattempts, the product will be registered. If the product is not registered after multiple reattempts, verify if there is any communication issue with the registration server and manually reregister the product instance.
- When you restore a system, the Smart Licensing settings that are restored depends on whether you restore the backup onto the same system or on a different system.
  - If you restore on the same system, the registration settings are restored on the restored system.
  - If you restore on a different system, you must register the product again with a registration key.
- If you are configuring Smart Software Manager On-Prem, be sure to enter the exact URL of the Smart Transport component (details and an example are provided in Smart Licensing Settings).

Process Summary

1. Obtain the Product Instance Registration Token
2. Configure Transport Settings on Expressway
3. Register with Cisco Smart Software Manager

Obtain the Product Instance Registration Token

This task gets the product instance registration token from CSSM or Smart Software Manager On-Prem to register the product instance. Tokens can be generated with or without Export-Controlled functionality. Detailed information is available from Cisco Software Central.

Step 1 Log in to your smart account in CSSM or Smart Software Manager On-Prem.

Step 2 Navigate to the virtual account that you want to associate with the Expressway.

Step 3 Generate a Product Instance Registration Token.

Step 4 Select the **Allow export-controlled functionality on the products registered with this token** check box to enable export-controlled functionality on the products registered with this token.

Caution Use this option only if you are compliant with the export-controlled functionality.

By checking this check box and accepting the terms, you enable higher levels of product encryption for products registered with this Registration Token. By default, this check box is selected. You can uncheck this check box to disallow Export-Controlled functionality on a product.

The **Allow export-controlled functionality on the products registered with this token** check box is not displayed for Smart Accounts that are not permitted to use the Export-Controlled functionality.

Step 5 Copy the token or save it to another location.

Configure Transport Settings on Expressway

This task selects the transport settings for Expressway to communicate to CSSM.

Step 1 In the Expressway web interface, go to **Maintenance** > **Smart licensing**.

Step 2 Navigate to **Transport settings** and select one of the following transport options:

- *Direct* Expressway sends usage information directly over the internet and no additional components are needed. This is the default.
- *Smart Software Manager On-Prem* Expressway sends usage information to an on-premise CSSM.
- *Proxy Server* Expressway sends usage information over the internet through a proxy server.

Details about the transport settings are provided in Smart Licensing Settings. Remember that if the Expressway product instance is already registered, you must first deregister it if you want to change transport settings from Direct (CSSM) to On-Prem, or the other way round.

Step 3 If the hostname and IP address of this product instance must not be exchanged with CSSM or Cisco Smart Software Manager On-Prem, check the setting **Do not share my hostname or IP address with Cisco**.

Step 4 Click **Save**.

Register with Cisco Smart Software Manager

This task registers your Expressway with CSSM or Smart Software Manager On-Prem. Until you register, the product runs in Evaluation Mode. You need the Product Instance Registration Token (see Obtain the Product Instance Registration Token) and transport settings must be configured as described in the previous task.

Step 1 In the Expressway web interface, go to **Maintenance** > **Smart licensing**.

Step 2 In the **Registration** section, paste the Product Instance Registration Token that you previously generated using CSSM or Smart Software Manager On-Prem.

Step 3 Click **Register** to complete the registration process. (After successful registration the button changes to **Reregister**.)

Step 4 In the **License usage** section, click **Update usage details** to manually update the system license usage information. This is resource-intensive and may take a few minutes depending on the size of the system.

The configuration for Smart Licensing is now complete.

The following section describes how to manage Smart Licensing registrations and authorizations, including what to do if the Expressway hostname is changed in future, or if you decide to permanently shut it down.

Important Configuration Information for Smart Licensing

Caution After Smart Licensing is set to *On* you cannot reset to *Off* using the web interface. To go back to PAK-based licensing (or to change the system to a VCS) requires a factory reset. For detailed information on *Factory Reset*, see the chapter *Smart Licensing*, section *Factory Reset* in Cisco Expressway Administrator Guide (X14.2). Because the reset will reinstall the software image and reset the Expressway configuration to the default, we strongly advise you to backup the Expressway data before you enable Smart Licensing.

- After Smart Licensing is enabled, you cannot use option keys on the Expressway.
- If a communication issue occurs with the registration server when you register the Expressway product instance, the registration fails with this message:

```
The last attempt to renew smart software licensing registration is in progress
 because of the
following reason: HTTP Server Error 200: Operation timed out.
```

  The product instance reattempts to register at 15-minute intervals. Refresh the page on your browser after each reattempt, to check current registration status. If the communication issue is resolved during the reattempts, the product will be registered. If the product is not registered after multiple reattempts, verify if there is any communication issue with the registration server and manually reregister the product instance.
- When you restore a system, the Smart Licensing settings that are restored depends on whether you restore the backup onto the same system or on a different system.
  - If you restore on the same system, Smart Licensing will be enabled and the registration settings are restored on the restored system.
  - If you restore on a different system, Smart Licensing will be enabled on the restored system but you must register the product again with a registration key.

More details

For detailed product information about the Cisco Smart Software Manager, see Cisco Smart Software Manager. Or for information about the On-Prem Manager, see Smart Software Manager On-Prem.

For more information about how to configure Smart Licensing, see the chapter on *Smart Licensing* in Cisco Expressway Administrator Guide (X14.2).

Manage Smart Licensing Registrations and Authorizations

This section describes Smart Licensing operations, including:

- *Renew Authorization*: Use to manually renew the License authorization status for all the licenses listed under the License type. The license authorization is renewed automatically every 30 days. The authorization status will expire after 90 days if it is not connected to CSSM or Smart Software Manager On-Prem.

- *Renew Registration*: Use to renew the registration information manually. The initial registration is valid for one year. Renewal of registration is automatically done every six months provided the product is connected to CSSM or Smart Software Manager On-Prem.
- *Deregister*: Use to disconnect the Expressway from CSSM or Smart Software Manager On-Prem. The product reverts to evaluation mode as long as the evaluation period is not expired. All license entitlements used for the product are immediately released back to the virtual account and are available for other product instances to use it.
- *Reregister License with Cisco Smart Software Manager*: Use to reregister Expressway with CSSM or Smart Software Manager On-Prem. The product may migrate to a different virtual account by reregistering with a token from a new virtual account.

Important Caveat

Smart Licensing Registration is a per-node operation. This means that a cluster of two or more peers requires every peer to register with Smart Licensing. However, alternate nodes *do not* register since the primary peer is registered.

Renew Authorization

Use this procedure to manually renew the License authorization status for all the licenses listed under the **License type**. This process assumes that the product is registered with CSSM or Smart Software Manager On-Prem.

Step 1 In the Expressway web interface, go to **Maintenance** > **Smart licensing**.

Step 2 In the **Action** section, from the **Additional operations** drop-down list, choose *Renew authorization now*.

Step 3 Click **Save**.

Expressway sends a request to Cisco Smart Software Manager or Smart Software Manager On-Prem to check the "License Authorization Status" and Cisco Smart Software Manager or Smart Software Manager On-Prem reports back the status to Cisco Expressway.

Step 4 In the **License usage** section, click **Update usage details** to manually update the system license usage information. This is resource-intensive and may take a few minutes depending on the size of the system.

Renew Registration

During product registration to Cisco Smart Software Manager or Smart Software Manager On-Prem, a security association is used to identify the product and is anchored by the registration certificate, which has a lifetime of one year (the registration period). This is different from the registration token ID expiration, which has the time limit for the token to be active. This registration period is automatically renewed every 6 months. However, if there is an issue, you can manually renew this registration period.

This process assumes that the product is registered with CSSM or Smart Software Manager On-Prem.

Step 1 In the Expressway web interface, go to **Maintenance** > **Smart licensing**.

Step 2 In the **Action** section, from the **Additional operations** drop-down list, choose *Renew registration now*.

Step 3 Click **Save**.

Expressway sends a request to CSSM or Smart Software Manager On-Prem to check the "Registration Status" and CSSM / Smart Software Manager On-Prem reports the status to Cisco Unified Communications Manager.

Step 4 In the **License usage** section, click **Update usage details** to manually update the system license usage information. This is resource-intensive and may take a few minutes depending on the size of the system.

Deregister

Use this procedure to unregister an Expressway from CSSM or Smart Software Manager On-Prem and release all the licenses from the current virtual account. This procedure also disconnects the Expressway from CSSM / Smart Software Manager On-Prem. All license entitlements used for the product are released back to the virtual account and are available for other product instances to use.

If Expressway is unable to connect with CSSM or Smart Software Manager On-Prem, and the product is still deregistered, a warning message displays. The message notifies you to remove the product manually from CSSM / Smart Software Manager On-Prem to free up licenses.

Step 1 In the Expressway web interface, go to **Maintenance** > **Smart licensing**.

Step 2 In the **Action** section, from the **Additional operations** drop-down list, choose **Deregister**.

Step 3 Click **Save**.

Step 4 In the **License usage** section, click **Update usage details** to manually update the system license usage information. This is resource-intensive and may take a few minutes depending on the size of the system.

Reregister with Cisco Smart Software Manager

Use this procedure to reregister the Expressway with CSSM or Smart Software Manager On-Prem. You need the Product Instance Registration Token (see Manage Smart Licensing Registrations and Authorizations).

Step 1 From the web interface, choose **Maintenance** > **Smart licensing**.
The Smart licensing window appears.

Step 2 In the **Registration** section, paste the "Registration Token Key" that you generated using the CSSM or Smart Software Manager On-Prem.

Step 3 Click **Reregister** to complete the reregistration process.

Step 4 In the **License usage** section, click **Update usage details** to manually update the system license usage information. This is resource-intensive and may take a few minutes depending on the size of the system.

How to Register a Change to the Expressway Hostname

If the Expressway hostname is changed, to reflect the change in CSSM, go to the **Expressway Smart Licensing web page** and click "**Renew Registration Now**".

Deregister First if Expressway is Permanently Shutdown

We recommend that if you plan to shutdown an Expressway machine permanently, you first deregister the product instance from the Expressway Smart Licensing web page. This is to avoid leaving unused product instances in CSSM.

In case you forget to do so, there is an alternate approach to remove the Expressway product instance from the CSSM portal.

This step is not needed for restarts or temporary shutdowns.

About Cisco Smart License Reservation and Its Types

Cisco Smart License Reservation is meant to reserve licenses and install them on the device. This process enables you to generate a unique reservation code from your Cisco device, which is then used to reserve a license type and quantity from your Cisco Smart Account's inventory.

The following are the license reservation types:

- **Permanent License Reservation (PLR):** All licenses are reserved.
- **Specific License Reservation (SLR):** Only specific licenses are reserved.

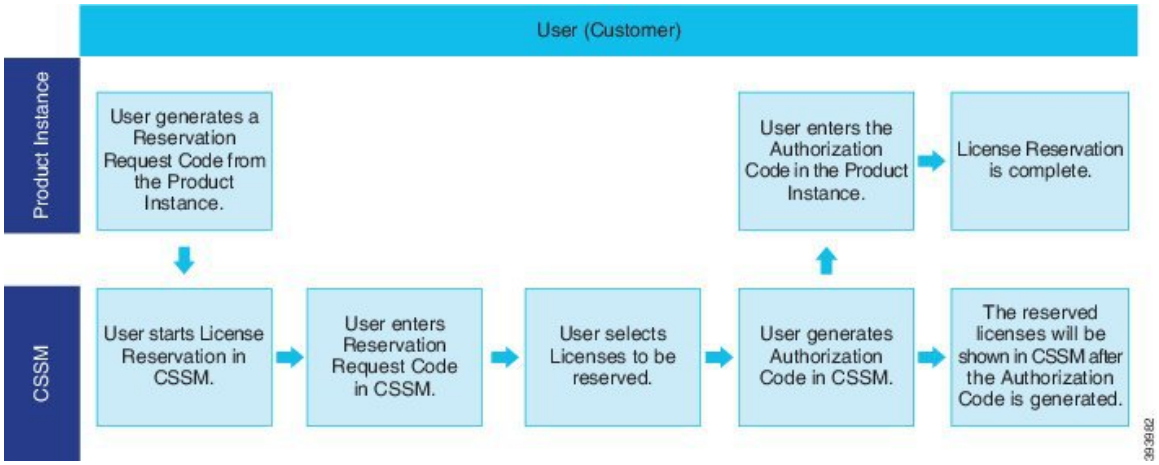
Note The following processes are common for both Permanent License Reservation (PLR) and Specific License Reservation (SLR).

Reserving a New Smart License

Section Purpose: This section outlines the procedure to reserve a new smart license for use.

The user can specify and reserve licenses against the product. For more information, see Requesting License Reservation for Your Smart Account. After the authorization code is exchanged, regular product synchronization is not required until there are changes in the reservation. Reserved licenses remain blocked in the Cisco Smart Software Manager unless released from the product with a return code.

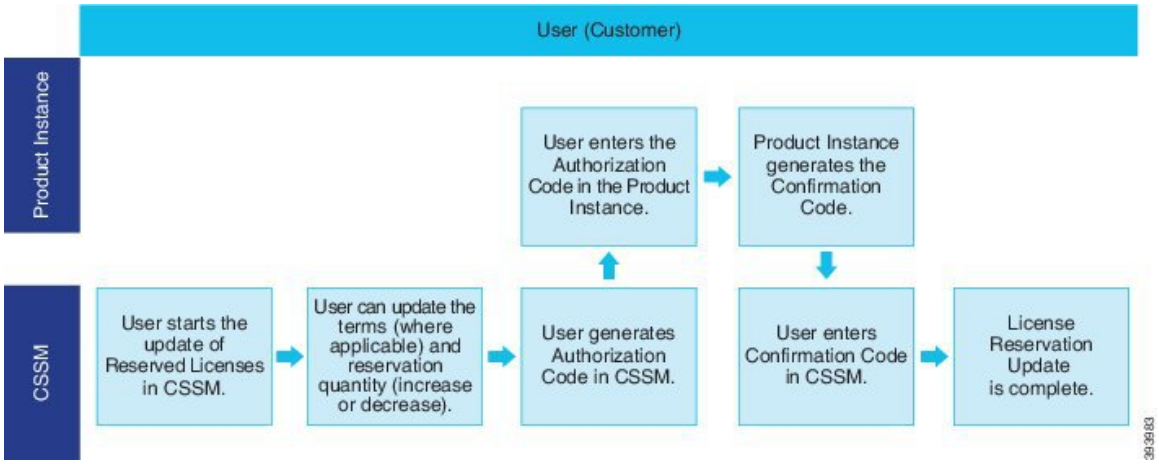
Figure 4: Reserve Licenses



Updating a Smart License Reservation

Use the Cisco Smart Software Manager to update or change reserved licenses (increase or decrease). You can install a new authorization code on the Product and obtain a confirmation code. The new changes remain in transit status unless confirmation code from the product is installed on the Cisco Smart Software Manager.

Figure 5: Update Reserve Licenses

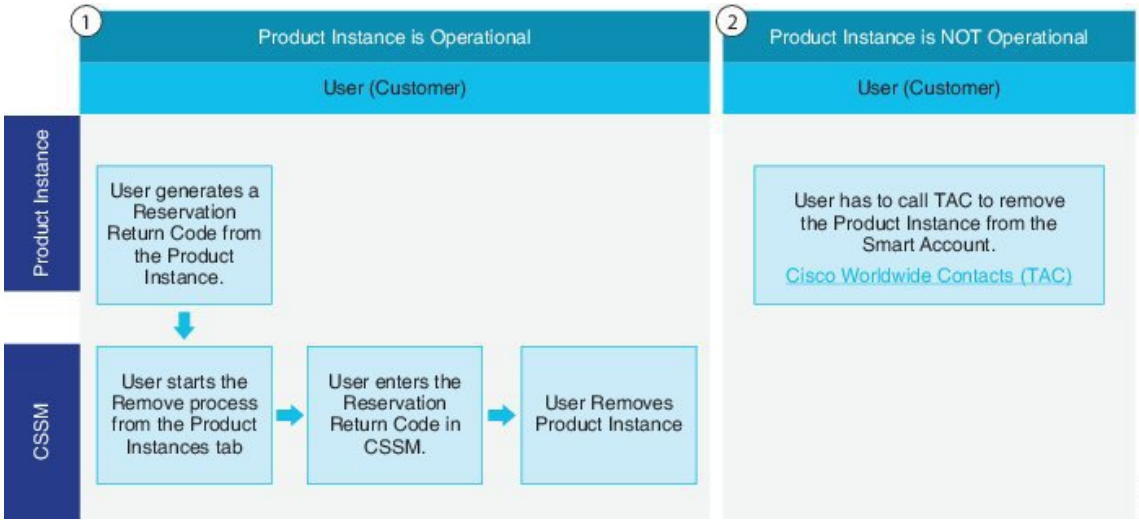


Removing the Product Instance from CSSM

You can remove the product from the smart account and release all the licenses that are reserved for that Product Instance (Expressway) when licenses are reserved on a Product Instance (Expressway).

Product Instance is operational (graceful removal): Users can create a Reservation Return Code on the Product Instance (which removes the Authorization Code) using the Cisco Smart Software Manager and return the Specific License Reservation Authorization.

Figure 6: Remove a Product Instance - Expressway



Note User can use only the CLI configuration to enable Permanent License Reservation and Specific License Reservation.

Functionality

Customers entitled to License reservation feature on their Smart Account can reserve licenses from their virtual account, tie them to a devices Unique Device Identifier (UDI) and use their device with these reserved licenses in a disconnected mode. The customer reserves specific licenses and counts the UDI from their virtual account.

CLI Commands for PLR and SLR

The table lists a set of CLI commands applicable for PLR and SLR.

Prerequisites

- Enable smart licensing before executing the reservation commands.
- Select the appropriate PLR or SLR licenses using the CLI commands before running the smart licensing commands.

Table 9: CLI Commands for PLR/SLR

CLI Command	Description
`xconfiguration License Smart ReservationEnable: On`	Enables license reservation feature.
`xcommand License Smart Reservation Request`	Prints the “Reservation Request Code”. Paste this into the portal to start the reservation process.

CLI Command	Description
`xcommand License Smart Reservation Install <authorization code>`	Enters the “Reservation Authorization Code” into the device to complete the process.
`xcommand License Smart Reservation Return`	Prints the “Reservation Return Code”. Paste this into the portal to return licenses and delete the product instance. This uses the previously installed authorization code.
`xcommand License Smart Reservation ReturnAuthorization <auth code>`	Prints the “Reservation Return Code”. Paste this into the portal to return licenses and delete the product instance. Uses the authorization code from the command line. **Note:** An extra authorization is not necessary for smart license reservation return authorization code.
`xcommand License Smart Reservation Cancel`	Cancels a reservation that is in progress and allows entitlement changes.

Permanent License Reservation

Permanent License Reservation (PLR) is a part of Cisco smart licensing solution. Smart Licensing needs a smart account. The product must connect to the Cisco Smart Software Management (CSSM) or Smart Software Manage (SSM On-Prem) in order to reactivate and report the most recent license status. You will use Cisco Permanent License Reservation or PLR license if you have extremely secured inner networks with restricted internet access.

You can apply Permanent licenses over evaluation licenses, and also apply it incrementally (that is, you can have multiple permanent licenses, and so on). Its capabilities are designed for highly secure environments, where communication with outside environment is impossible.

How does PLR Licenses Work?

Permanent License Reservation is a permanent solution for highly secure network architecture where all outbound connections are limited. PLR license allows you to register all product instances along with unlimited features (along with all entitlements on Expressway till the physical capacity of the Expressway box) and permanently (no renewal needed) using a reservation code. This solution is similar to traditional PAK licenses and is mostly available for Cisco Secure product lines. Furthermore, PLR licenses counts as an easy-to-use and intuitive solution which can be applied easily on different devices. In addition, you can provide a single authorization code to permanently enable all features or eliminate various features and expiration dates.

How to Apply PLR Licenses?

There are a few Command Line Interface (CLI) commands. These commands can generate a reservation code. You can use the reservation code to receive a unique authorization code. Entering this Authorization Code in CLI will permanently activate all features.

Task Flow

You can use a set of commands through the Command Line Interface (CLI) to call the Smart Agent and obtain the required information. You can paste this information on the Cisco Smart Software Manager (CSSM) portal.

This reservation is also called Online-Offline mode. You must be online to register and use the reservation. First, deregister yourself if you have already registered to enable reservation and start the process.

Complete these tasks to reserve permanent licenses for Expressway.

Enable Reservation

Use this procedure to enable Permanent License Reservation.

Note Reservation is disabled by default. You must enable it.

Before you begin

Expressway is unregistered with Cisco Smart Software Manager or On-Prem.

From Expressway Admin Console, execute the command.

```
xconfiguration License Smart ReservationEnable: On
```

```
OK
```

Now you can start the process.

What to do next

For information on the procedure to generate reservation request code from the Expressway product, see the steps on Reservation Request Code.

Reservation Request Code

Use this procedure to generate reservation request code from the Expressway product.

Before you begin

Execute this command.

```
xconfiguration License Smart ReservationEnable: On
```

Step 1 Execute the following command from the Expressway Admin Console.

```
xcommand License Smart Reservation Request
<code is generated>
```

Invoke this command to obtain the code from Smart Agent Reservation Request. After the code is generated, copy the code and paste it into the CSSM portal (**Smart Software Licensing** page).

```
xcommand License Smart Reservation Request

Enter the following reservation request code into the CSSM:
CB-PExpressway,S08F8FF3C,V1.0,H320aa69d-A7C3vjcjf-AE
```

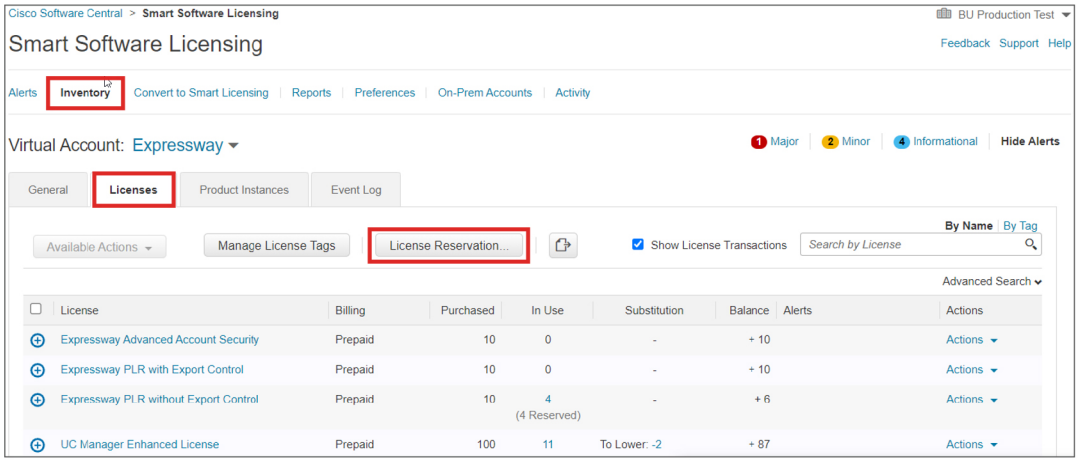
464228

This will start the process and generate the authorization code in CSSM.

Step 2 Log into Cisco Smart Software Manager (CSSM) from https://software.cisco.com/#..

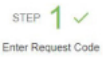
Use the Cisco provided username and password to Log in to the Cisco SSM portal.

a) Click **Inventory** > **Licenses tab** > **License Reservation...**.



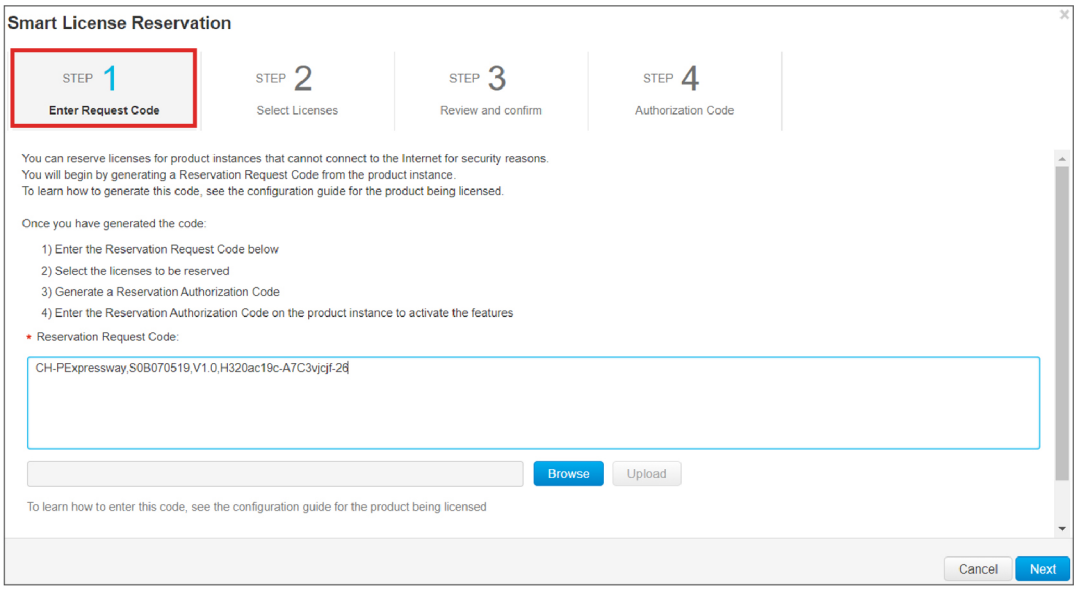
461922

This displays the **Smart License Reservation** window.



The is the default tab.

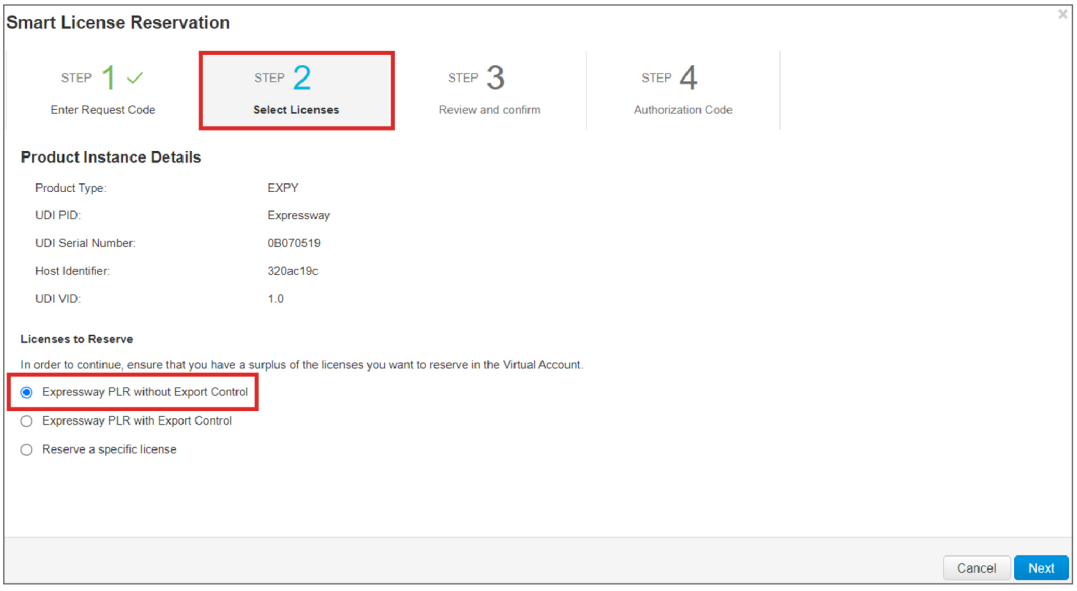
In the **Reservation Request Code** field, paste the reservation request code that is generated from Expressway.



Click **Next**.

This displays the tab.

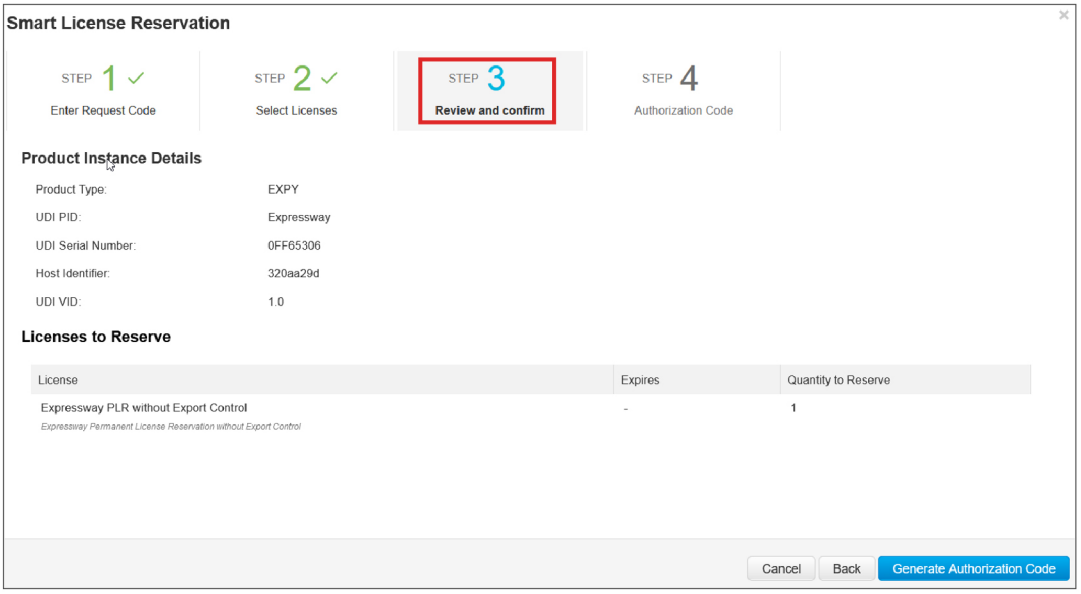
b) Choose **Expressway PLR without Export Control** from **Licenses to Reserve**.



Click **Next**.

This displays the tab.

c) Click **Generate Authorization Code**.



The code is generated in the **Authorization Code** field.

Copy the code and navigate to the Expressway Admin Console.

What to do next

For information on the procedure to install license reservation authorization code generated from Cisco Smart Software Manager, see the steps on Install License Reservation Authorization Code from CSSM.

Install License Reservation Authorization Code from CSSM

Use this procedure to install license reservation authorization code generated from Cisco Smart Software Manager.

Before you begin

Execute these commands in sequence:

- **xconfiguration License Smart ReservationEnable**
- **xcommand License Smart Reservation Request**

Step 1 Execute the command from the Expressway Admin Console:

```
xcommand License Smart Reservation Install <authorization code>
```

Remember In the command, paste the <authorization code> copied from the CSSM portal.

Execute this command to install the code and all licenses. In the Permanent Reservation License, you do not choose anything but will install the entire package. This completes the process of Reservation.

```
xcommand License Smart Reservation Install CAvfS8-tqmsHn-ntioqo-Z8Q4wK-jsddDU-3YkM

Authorization code installed.
```

464226

Result: A message appears that the installation is successful after all the steps are completed.

Step 2 Navigate to Cisco Smart Software Manager (CSSM) portal.

From the tab, click **Close**.

What to do next

For information on the procedure to generate a return code, see the steps on Return Reservation Code.

Return Reservation Code

Use this procedure to generate a return code. You must enter this code into the Cisco Smart Software Manager (CSSM) to return the licenses to the virtual account pool and remove the product instance from CSSM.

Before you begin

Execute the following commands in sequence:

- **xconfiguration License Smart ReservationEnable**
- **xcommand License Smart Reservation Request**
- **xcommand License Smart Reservation Install <authorization code>**

Step 1 From Expressway Admin Console, execute the command.

```
xcommand License Smart Reservation Return
```

This generates a return code. Copy the code and paste it in the CSSM portal in order to return the previously installed permanent licenses.

```
xcommand License Smart Reservation Return

Enter the following return code into the CSSM:
CvfS8d-Fx1Yev-qmViq3-1KhkSR-iJfCzN-biB
```

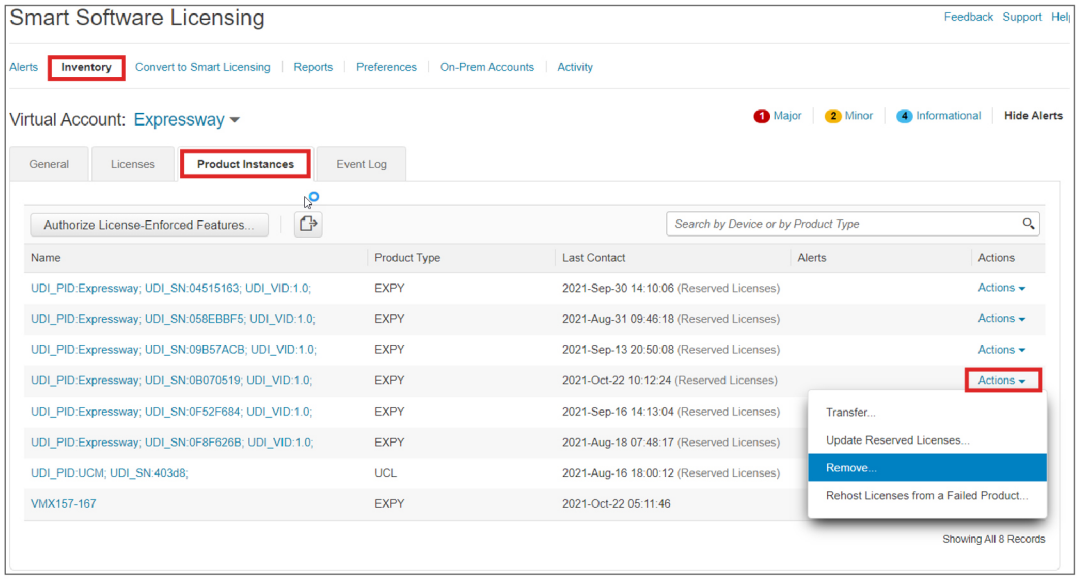
464229

Step 2 Navigate to the Cisco Smart Software Manager (CSSM) portal, **Smart Software Licensing** page, follow the path: Click **Inventory** > **Product Instances** tab.

This displays the available list of product instances.

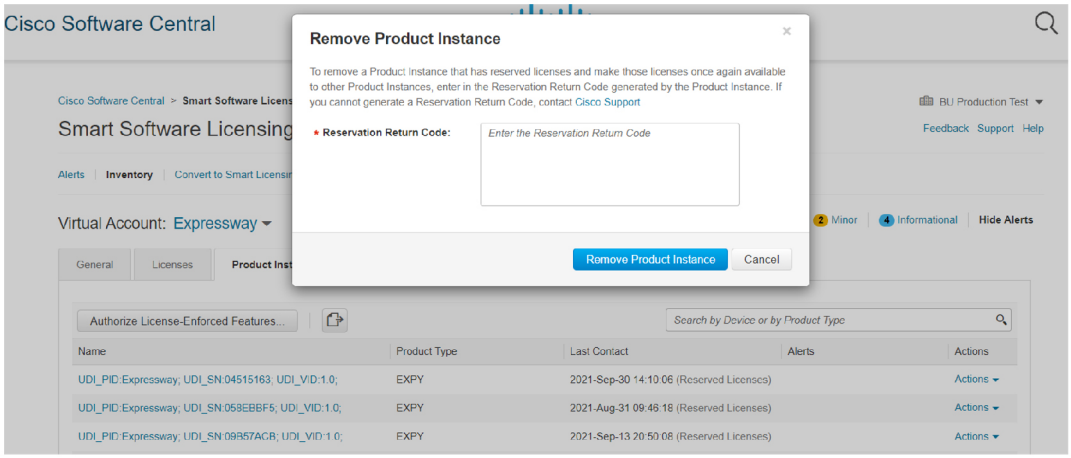
Step 3 Locate an appropriate product instance where the licenses are installed. Optionally, you can enter a name or product type string in the search tab to locate the product instance or Time and Date stamp or Serial Number of the machine.

Step 4 Click the **Actions** drop-down list from the **Actions** column. and choose **Remove**



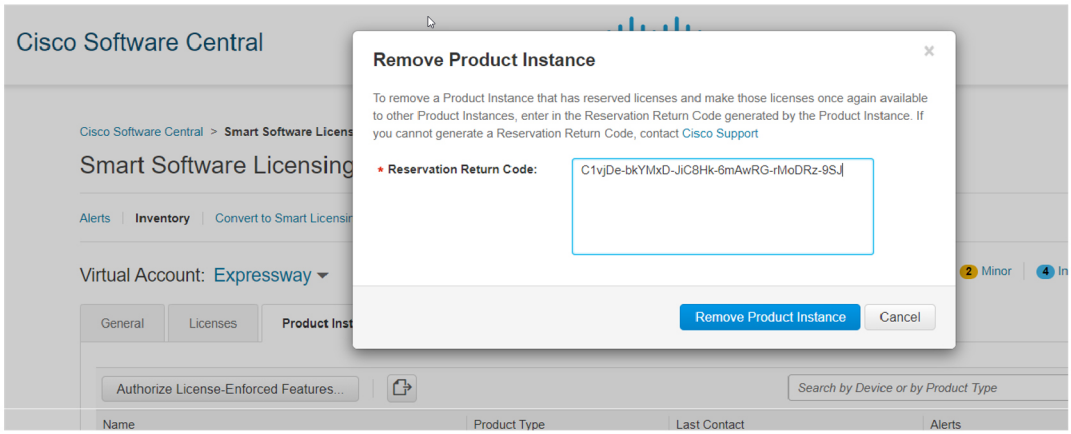
461921

Result: This displays the **Remove Product Instance** popup window.



Step 5 Paste the reservation return code in the **Reservation Return Code** field.

Step 6 Click **Remove Product Instance**.



Result: A message that the Product Instance was successfully removed appears.

This removes the reservation information and makes the license available in the virtual account.

What to do next

For information on the procedure to cancel the reservation process, see the steps on Cancel the Reservation Process.

Cancel the Reservation Process

Use this procedure to cancel the reservation process before the authorization code from Cisco Smart Software Manager (CSSM) against Expressway request code is installed.

Before you begin

Execute the following commands in sequence:

- **xconfiguration License Smart ReservationEnable**
- **xcommand License Smart Reservation Request**

Step 1 Execute the command from Expressway Admin Console:

```
xcommand License Smart Reservation Request
```

Result: <Reservation Request Code> is generated.

Step 2 Copy the request code.

Step 3 Navigate to Cisco Smart Software Manager (CSSM) portal.

Step 4 Click **Inventory** > **Licenses** > **License Reservation...**.

This displays the **Smart License Reservation** window.

The is the default tab.

Step 5 In the **Reservation Request Code** field, paste the request code that is generated from Product Instance - Expressway.

Step 6 Click **Next** to generate the Authorization Code.

This displays the tab.

Step 7 Choose **Expressway PLR without Export Control** from **Licenses to Reserve**.

Step 8 Click **Next**.

This displays the tab.

Step 9 Click **Generate Authorization Code**.

This generates code in the **Authorization Code** field.

Remember Now, do not install the authorization code since you are canceling the reservation.

Step 10 Navigate to the Expressway Admin Console and execute this command:

```
xcommand License Smart Reservation Cancel
```

```
OK
```

Step 11 Navigate to Cisco Smart Software Manager (CSSM) portal, copy the <authorization code> that is generated.

What to do next

For information on the procedure to generate a return code for the authorization code you have not yet installed, see the steps on Generate a Return Code for the Authorization Code to complete the process.

Generate a Return Code for the Authorization Code

Use this procedure to generate a return code for the authorization code you have not yet installed. Enter the return code into the Cisco Smart Software Manager to return the licenses to the virtual account pool and remove the product instance from CSSM.

Before you begin

Execute the following commands in sequence:

- **xconfiguration License Smart ReservationEnable**
- **xcommand License Smart Reservation Request**

Step 1 Navigate to the Expressway Admin Console and execute the command:

```
xcommand License Smart Reservation ReturnAuthorization <auth code>
                            (paste the authorization code from CSSM)
```

<Reservation Return Code> is generated.

In order to complete the process, copy the <generated reservation return code> from the Expressway Admin Console.

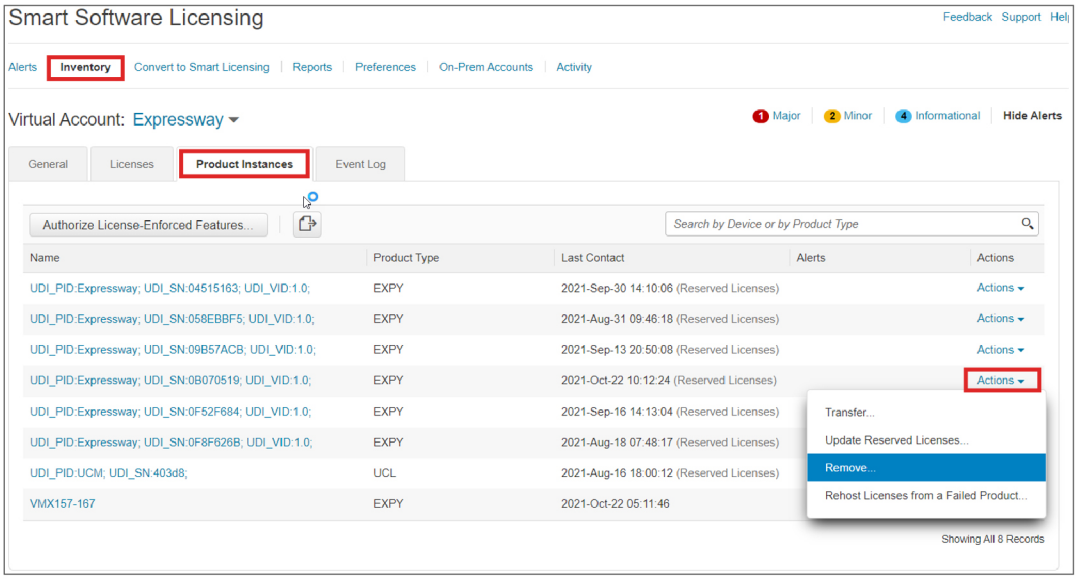
Step 2 Navigate to the Cisco Smart Software Manager (CSSM) portal.

Step 3 Click **Inventory** > **Product Instances** tab from the **Smart Software Licensing** page.

The displays the list of available product instances.

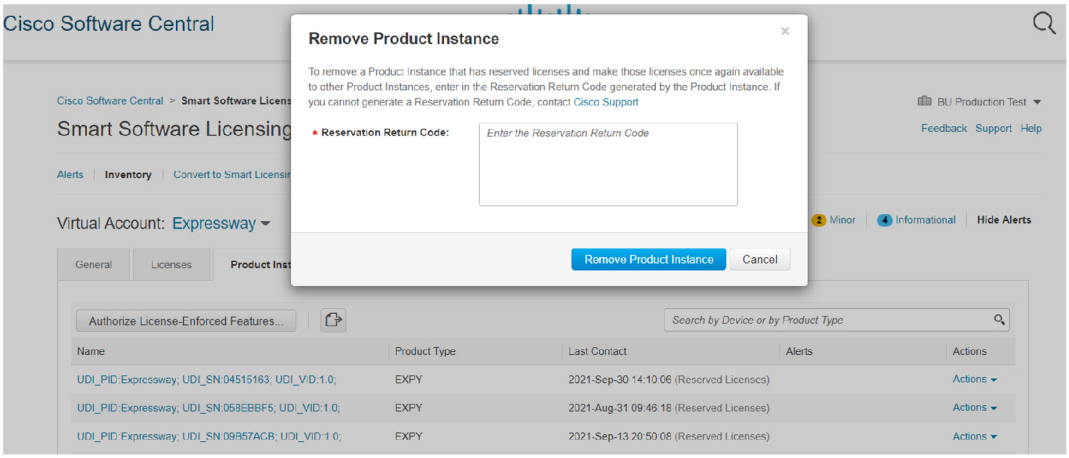
Step 4 Locate an appropriate product instance where the licenses are installed. Optionally, you can enter a name or product type string in the search tab to locate the product instance or Time and Date stamp or Serial Number of the machine.

Step 5 Click **Actions** drop-down list from the **Actions** column and choose **Remove**.



461921

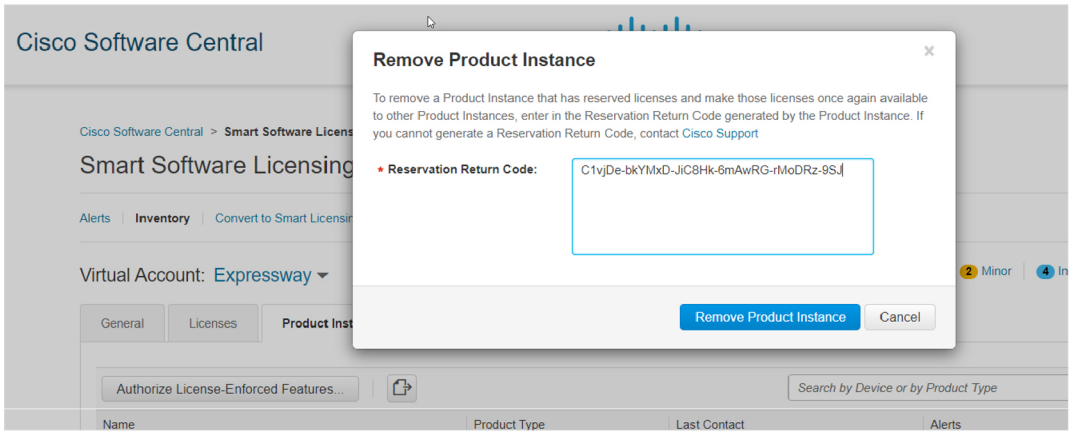
Result: This displays the **Remove Product Instance** popup window.



461924

Step 6 Paste the reservation return code in the **Reservation Return Code** field.

Step 7 Click **Remove Product Instance**.



Result: A message that the Product Instance was successfully removed appears.

STEP 4
Authorization Code

Step 8 From the tab, click **Close**.
Result: This completes the process.

Specific License Reservation

Specific License Reservation is a feature that is used in highly secure networks. It provides a method for customers to deploy a software license on a device (Product Instance - Expressway) without communicating usage information.

Task Flow

Enable Reservation

Use this procedure to enable Specific License Reservation.

Note Reservation is disabled by default. You must enable it.

Before you begin

Expressway is unregistered with Cisco Smart Software Manager or On-Prem.

Execute this command from the Expressway Admin Console.

```
xconfiguration License Smart ReservationEnable: On

OK
```

Now you can start the process.

What to do next

For information on the procedure to generate reservation request code from the Expressway product, see the steps on Reservation Request Code.

Reservation Request Code

Use this procedure to generate reservation request code from the Expressway product.

Before you begin

Execute the following command:

```
xconfiguration License Smart ReservationEnable: On
```

Step 1 Execute the following command from the Expressway Admin Console.

```
xcommand License Smart Reservation Request
<request code is generated>
```

Invoke this command to obtain the code from the Smart Agent Reservation Request. After the code is generated, copy the code and paste it into the CSSM portal (**Smart Software Licensing** page).

```
xcommand License Smart Reservation Request

Enter the following reservation request code into the CSSM:
CB-PExpressway,S08F8FF3C,V1.0,H320aa69d-A7C3vjcjf-AE
```

464228

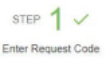
This will start the process and generate the authorization code in CSSM.

Step 2 Log into Cisco Smart Software Manager (CSSM) from https://software.cisco.com/#..

Use the Cisco provided username and password to log in to the Cisco SSM portal.

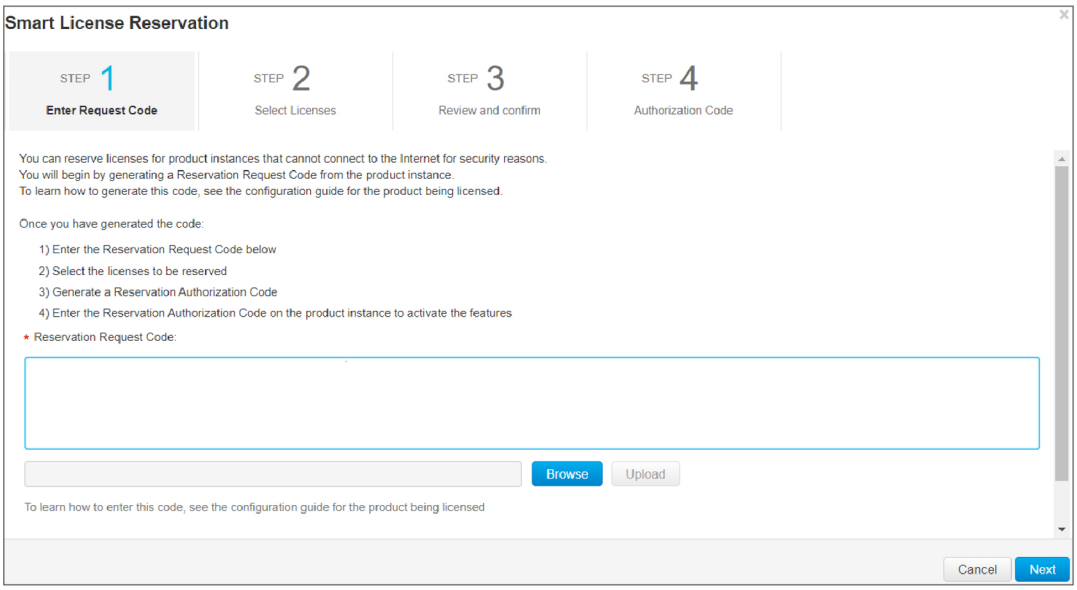
a) Click **Inventory** > **Licenses tab** > **License Reservation...**.

This displays the **Smart License Reservation** window.



The is the default tab.

In the **Reservation Request Code** field, paste the reservation request code that is generated from Expressway.



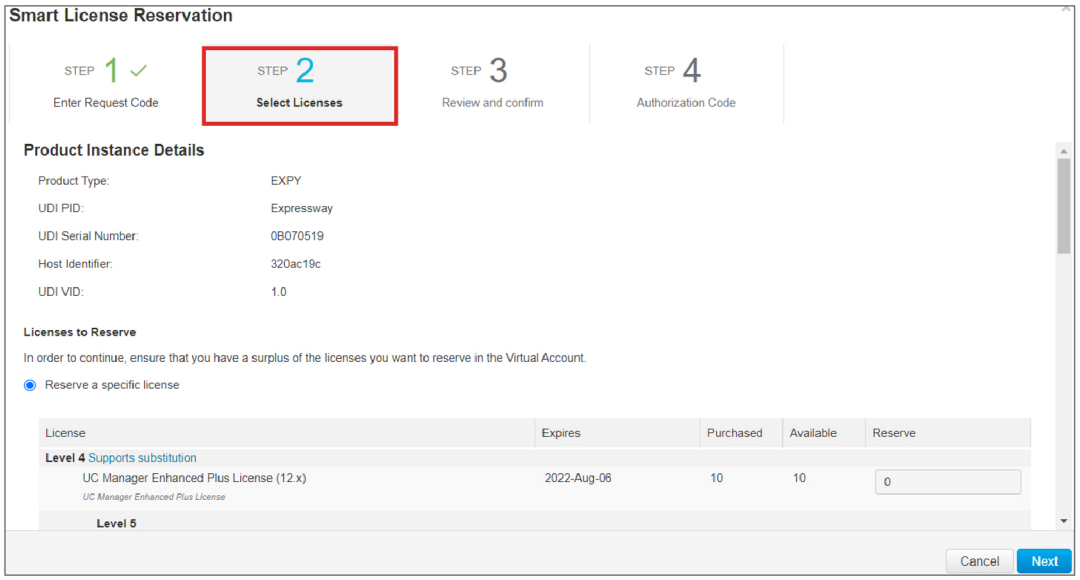
b) Click **Next**.

This displays the tab.

c) Choose **Reserve a specific license** from **Licenses to Reserve**.
d) In the **Quantity to Reserve** field, enter the numeral adjacent to the required license.

Information Here you can choose the number of licenses and the type of license to reserve. You can choose between version 12 and version 14 that Expressway uses to communicate with both the versions of UCM. The Expressway Advanced Account Security Entitlement is linked with Export Control. Make sure that you do not choose 0 in the quality to reserve field. Choosing 0 will not allow enabling Export Control.

e) Click **Next**.

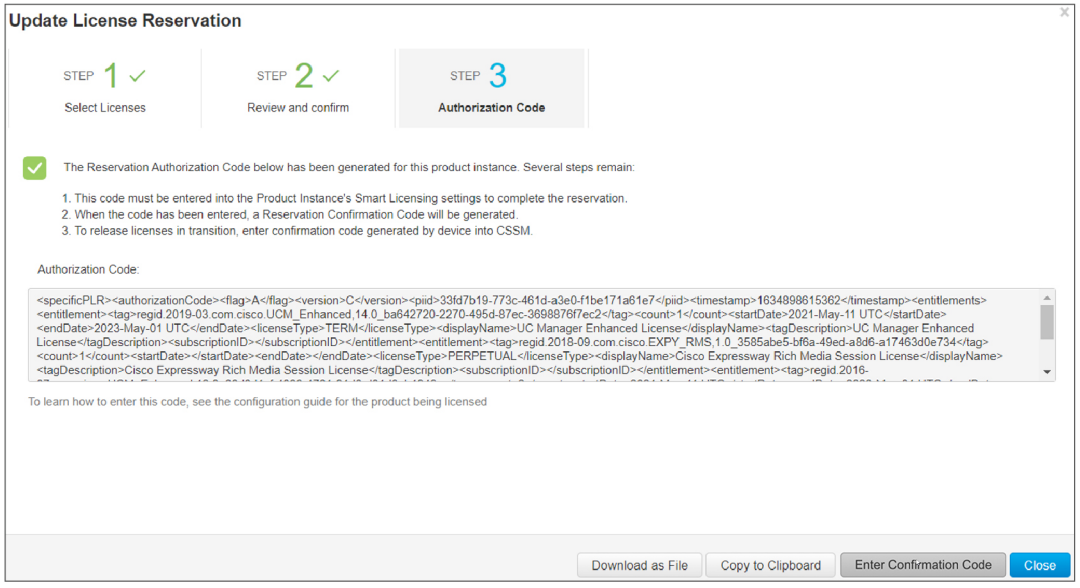


461917

This displays the tab.

f) Click **Generate Authorization Code**.

The code is generated in the **Authorization Code** field.



461930

Note This authorization code is slightly different from the code generated in Permanent License Reservation.

Copy the code and navigate to the Expressway Admin Console.

Step 3 Navigate to the Expressway Admin Console.

What to do next

For information on the procedure to install license reservation authorization code generated from Cisco Smart Software Manager, see the steps on Install License Reservation Authorization Code from CSSM.

Install License Reservation Authorization Code from CSSM

Use this procedure to install license reservation authorization code generated from Cisco Smart Software Manager.

Before you begin

Execute the following commands in sequence:

- **xconfiguration License Smart ReservationEnable**
- **xcommand License Smart Reservation Request**

Step 1 Execute the command from the Expressway Admin Console.

```
xcommand License Smart Reservation Install "<authorization code>"
```

Information This is an XML file. Make sure you insert the code within double quotes.

Remember In the Expressway Admin Console, paste the "<authorization code>" that is copied from the CSSM portal.

464227

Result: This displays the message that the installation is successful. Along with this message, a confirmation code is also generated on the product after the authorization code is successfully installed.

Note This is different from Permanent License Reservation (PLR). This confirmation code is used whenever you must update the licenses.

Step 2 Navigate to the Cisco Smart Software Manager (CSSM) portal.

What to do next

For information on the procedure to update the license reservation for your product instance and get a new authorization code, see the steps on Update License Reservation.

Update License Reservation

Use this procedure to update the license reservation for your product instance and get a new authorization code.

Before you begin

Execute the following command:

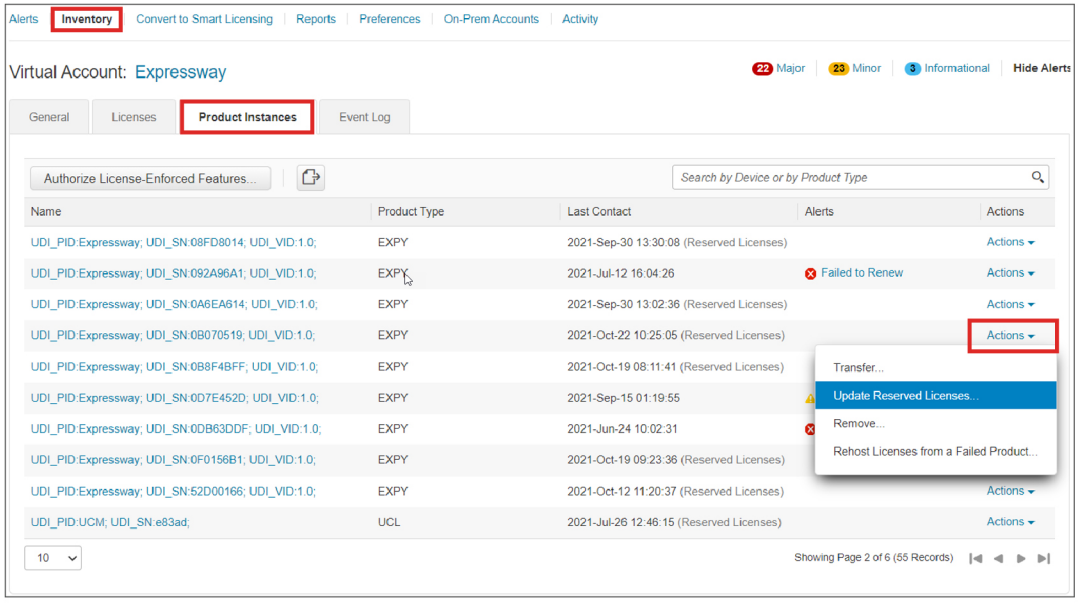
- **xconfiguration License Smart ReservationEnable**
- **xcommand License Smart Reservation Request**
- **xcommand License Smart Reservation Install "<authorization code>"**

Step 1 Follow the path, click **Inventory** > **Product Instances** tab from the Cisco Smart Software Manager (CSSM) portal.

The displays the list of available product instances.

Step 2 Locate an appropriate product instance where the licenses are installed. Optionally, you can enter a name or product type string in the search tab to locate the product instance or Time and Date stamp or Serial Number of the machine.

Step 3 Click the **Actions** drop-down list from the **Actions** column and choose **Update Reserved Licenses**.



This displays the **Update License Reservation** window.

STEP 2
Select Licenses

The tab and is selected by default.

Step 4 Select **Reserve a specific license** from **Licenses to Reserve**..

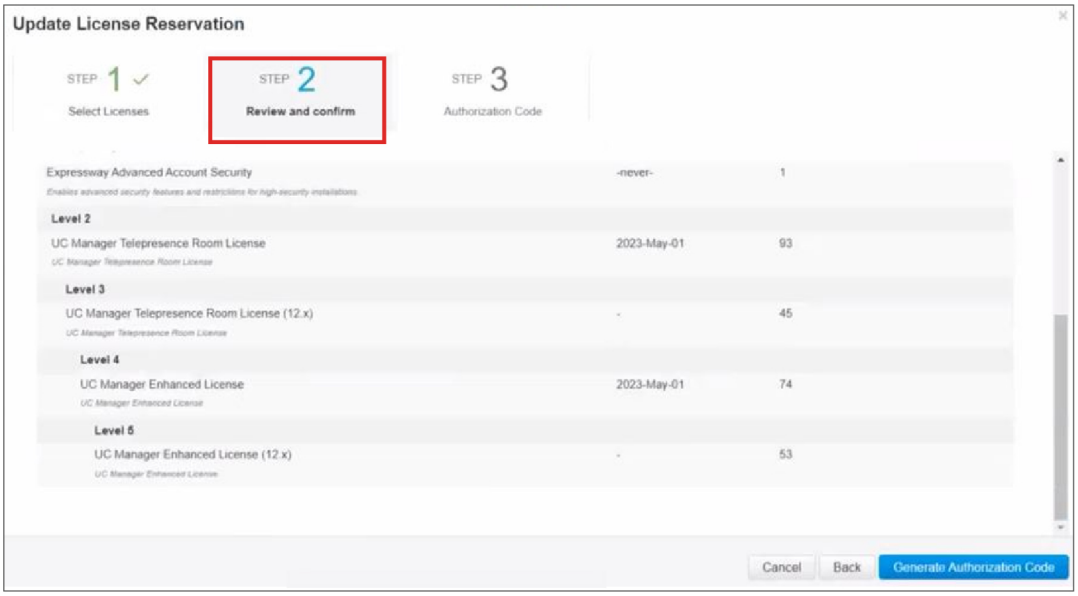
You can view the previously reserved licenses and modify them.

Step 5 In the **Quantity to Reserve** field adjacent the corresponding license, enter/modify the number of licenses you want to reserve.

Step 6 Click **Next**.

This displays the tab. You can review the license reservation information.

Step 7 Click **Generate Authorization Code**.



The code is generated in the **Authorization Code** field.

Step 8 After generating the authorization code, click **Copy to Clipboard** to copy the authorization, or **Download as File** to download the file and save it to the Flash drive or the TFTP server.

Step 9 Navigate to the Expressway Admin Console and paste the code in the command:

```
xcommand License Smart Reservation Install "<authorization code>"
```

Information This is an XML file. Make sure you insert the code within double quotes.

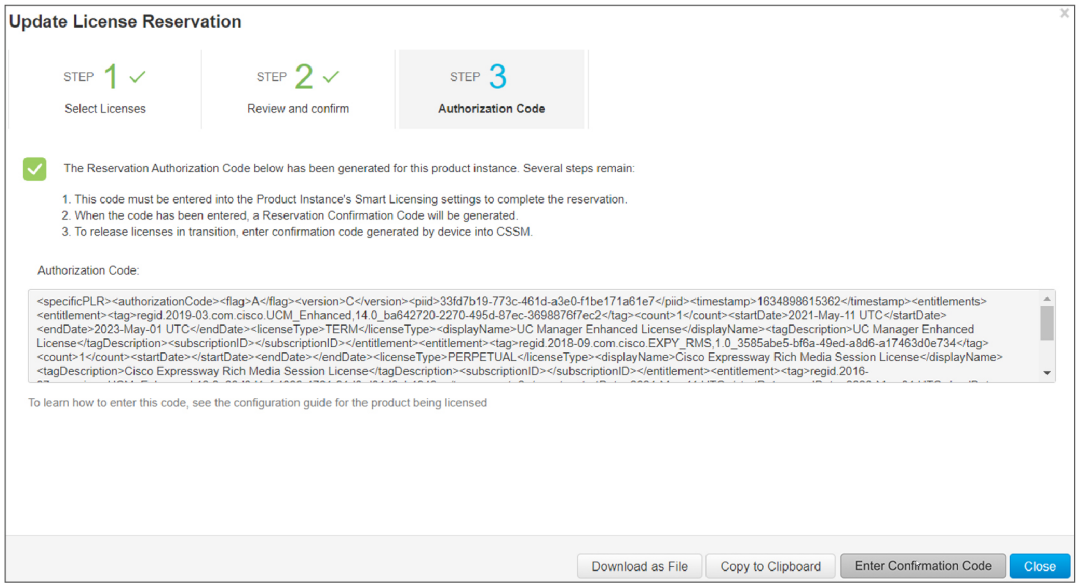
Remember In the Expressway Admin Console, paste the "<authorization code>" that is copied from the CSSM portal.

Result: The installation is successful message appears. Along with the message, a confirmation code is also generated on the product after the authorization code is successfully installed.

Step 10 Copy the <Confirmation Code>.

Step 11 Navigate to the Cisco Smart Software Manager (CSSM) portal to complete the process of updating the licenses.

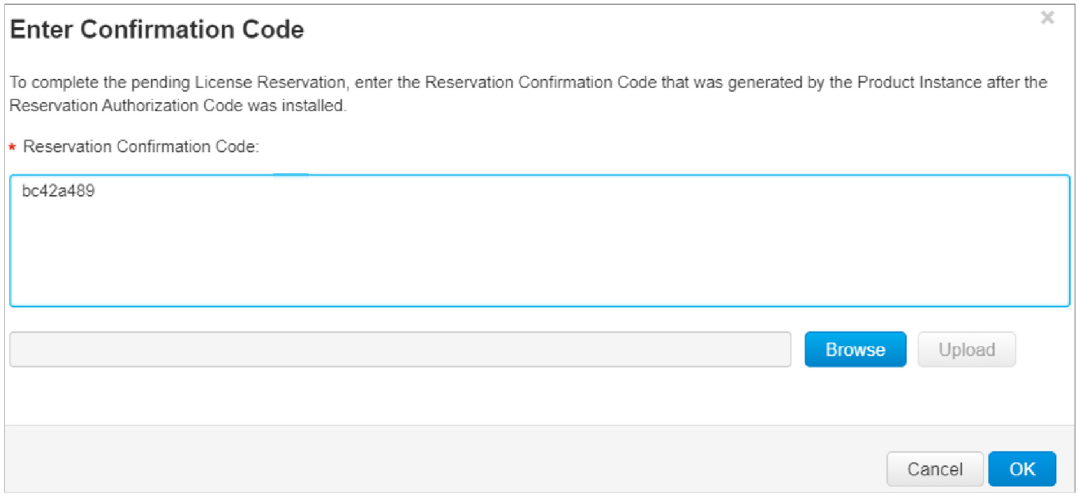
Step 12 Click **Enter Confirmation Code**.



This displays the **Enter Confirmation Code** window.

Step 13 Paste the confirmation code in the **Reservation Confirmation Code** field.

Step 14 Click **OK**.



A message that the licenses are successfully reserved appears. Thus the licenses are updated.

What to do next

For information on the procedure to generate a return code, see the steps on Return Reservation Code.

Return Reservation Code

Use this procedure to generate a return code that must be entered into the Cisco Smart Software Manager to return the licenses to the virtual account pool and remove the product instance from CSSM.

Before you begin

Execute the following command:

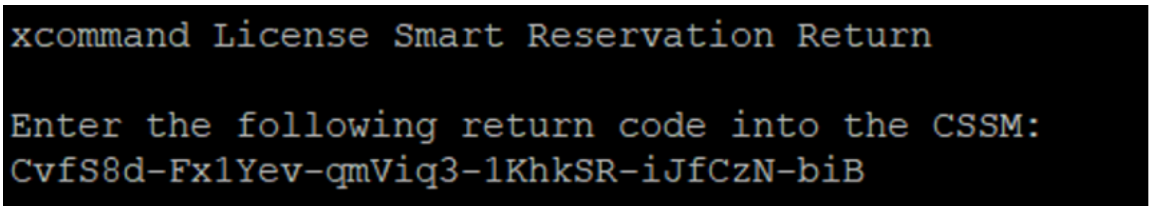
- **xconfiguration License Smart ReservationEnable**
- **xcommand License Smart Reservation Request**
- **xcommand License Smart Reservation Install "<authorization code>"**

Step 1 Execute this command from the Expressway Admin Console.

```
xcommand License Smart Reservation Return
```

This command is executed after successful installation.

This generates a <Return Code>. Copy the return code and paste it in the CSSM portal.

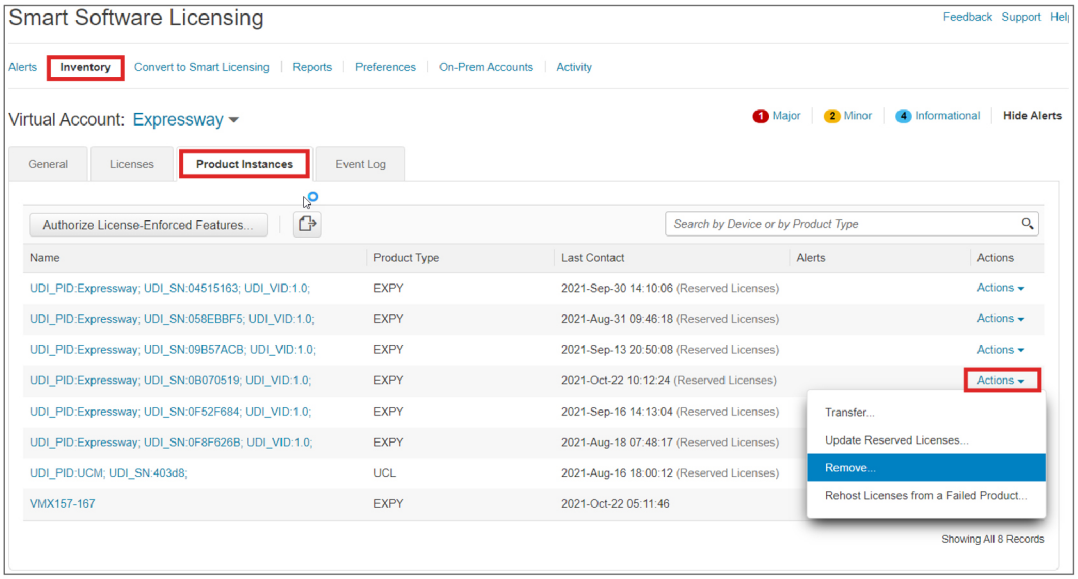


Step 2 Navigate to the Cisco Smart Software Manager (CSSM) portal, **Smart Software Licensing** page, follow the path, click **Inventory** > **Product Instances** tab.

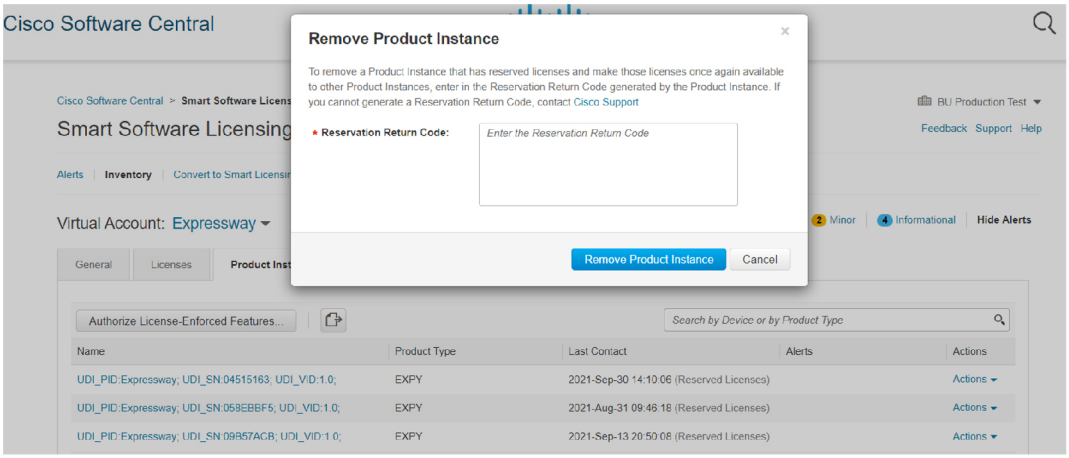
The displays the list of available product instances.

Step 3 Locate an appropriate product instance where the licenses are installed. Optionally, you can enter a name or product type string in the search tab to locate the product instance or Time and Date stamp or Serial Number of the machine.

Step 4 Click the **Actions** drop-down list from the **Actions** column and choose **Remove**.

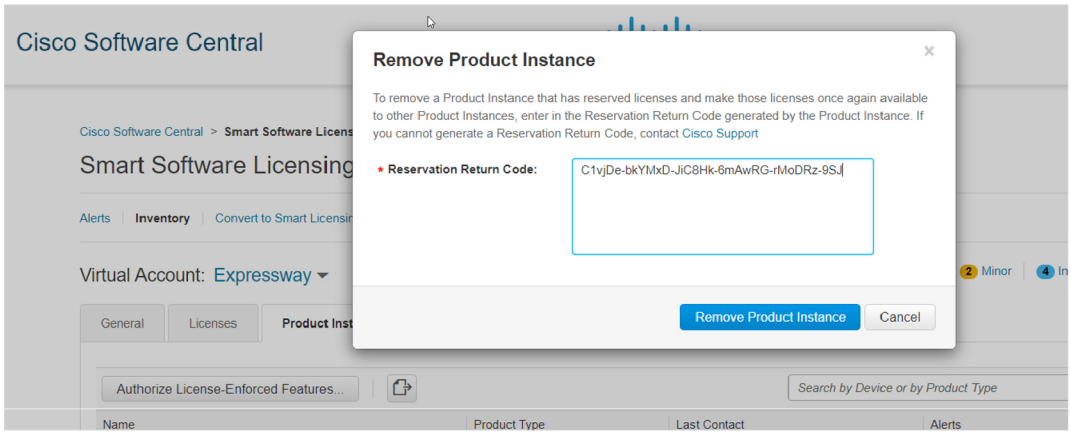


Result: This displays the **Remove Product Instance** popup window.



Step 5 Paste the reservation return code in the **Reservation Return Code** field.

Step 6 Click **Remove Product Instance**.



A message that the Product Instance was successfully removed appears.

STEP 4
Authorization Code

Step 7 From the tab, click **Close**.

What to do next

For information on the procedure to cancel the reservation process, see the steps on Cancel the Reservation Process.

Cancel the Reservation Process

Use this procedure to cancel the reservation process before the authorization code from Cisco Smart Software Manager (CSSM) against Expressway request code is installed.

Before you begin

Execute the following commands in sequence:

- **xconfiguration License Smart ReservationEnable**
- **xcommand License Smart Reservation Request**

Step 1 Execute the command from Expressway Admin Console.

```
xcommand License Smart Reservation Request
```

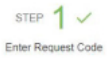
Result: <Reservation Request Code> is generated>

Step 2 Copy the request code.

Step 3 Navigate to Cisco Smart Software Manager (CSSM) portal.

Step 4 Click **Inventory** > **Licenses** > **License Reservation...**.

This displays the **Smart License Reservation** window.



The is the default tab.

Step 5 In the **Reservation Request Code** field, paste the request code that is generated from Product Instance - Expressway.

Step 6 Click **Next** to generate the Authorization Code.

This displays the tab.

Step 7 Choose **Reserve a specific license** from **Licenses to Reserve**.

Step 8 Click **Next**.

This displays the tab.

Step 9 Click **Generate Authorization Code**.

This generates code in the **Authorization Code** field.

Remember Now, do not install the authorization code since you are canceling the reservation.

Step 10 Navigate to the Expressway Admin Console and execute this command:

```
xcommand License Smart Reservation Cancel

OK
```

Step 11 Navigate to Cisco Smart Software Manager (CSSM) portal, copy the <authorization code> that is generated.

What to do next

For information on the procedure to generate a return code for the authorization code you have not yet installed, see the steps on Generate a Return Code for the Authorization Code to complete the process.

Generate a Return Code for the Authorization Code

Use this procedure to generate a return code for the authorization code you have not yet installed. Enter the return code into the Cisco Smart Software Manager to return the licenses to the virtual account pool and remove the product instance from CSSM.

Before you begin

Execute the following commands in sequence:

- **xconfiguration License Smart ReservationEnable**

- **xcommand License Smart Reservation Request**

Step 1 Navigate to the Expressway Admin Console and execute the command:

```
xcommand License Smart Reservation ReturnAuthorization "<auth code>"
                            (paste the authorization code from CSSM)
```

<Reservation Return Code> is generated.

Information This is an XML file. Make sure you insert the code within double quotes.

In order to complete the process, copy the <generated reservation return code> from the Expressway Admin Console.

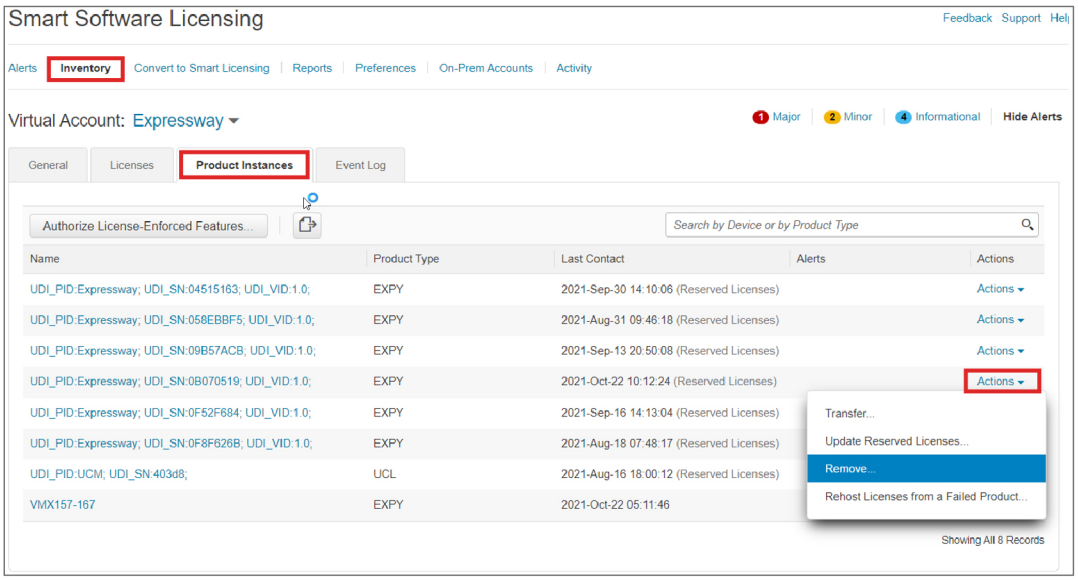
Step 2 Navigate to the Cisco Smart Software Manager (CSSM) portal.

Step 3 Click **Inventory** > **Product Instances** tab from the **Smart Software Licensing** page.

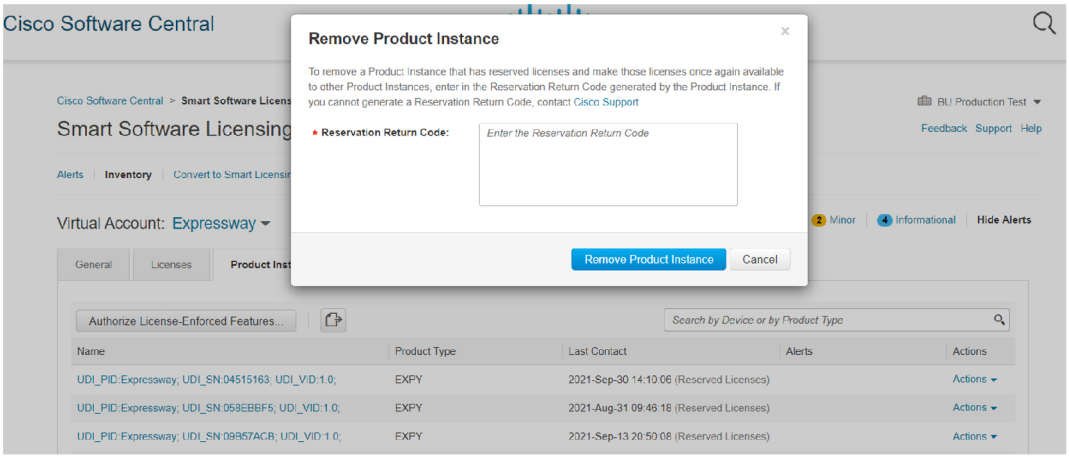
The displays the list of available product instances.

Step 4 Locate an appropriate product instance where the licenses are installed. Optionally, you can enter a name or product type string in the search tab to locate the product instance or Time and Date stamp or Serial Number of the machine.

Step 5 Click **Actions** drop-down list from the **Actions** column and choose **Remove**.

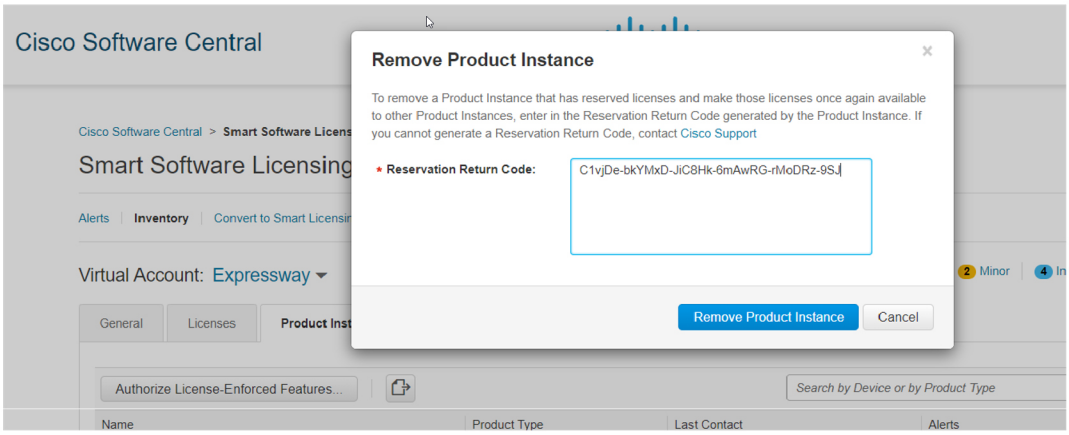


Result: This displays the **Remove Product Instance** popup window.



Step 6 Paste the reservation return code in the **Reservation Return Code** field.

Step 7 Click **Remove Product Instance**.



Result: A message that the Product Instance was successfully removed appears.

STEP 4
Authorization Code

Step 8 From the tab, click **Close**.
Result: This completes the process.

Additional Information

Note Make sure that Smart Licensing is *enabled* and Expressway is in *Specific License Reservation (SLR)* mode.

Sharing of Licenses Across Nodes in a Cluster

Consider Node 1 and Node 2 where,

Node 1 : 10 Desk Registrations + 10 Rich Media Session (RMS)

Node 2 : 10 Desk Registrations + 10 RMS

Explanation: 10 RMS licenses are consumed when there are 10 Business to Business (B2B) calls made from Node 1.

A cluster license is shared among all the nodes. For example, Node 1 has 10 licenses, if 11th endpoint tries to register then the Node automatically borrows 1 license from other nodes.

Information: The license is borrowed only if there are no available RMS licenses in Node 1.

Note This behavior is similar to PAK-based licenses.

Reporting of the License Consumption to Smart Agent

The license consumption is reported to the Smart Agent over pre-configured intervals.

Within a cluster if 1 node consumes more than the installed licenses then only the number of installed licenses will be reported.

For example, In a 2 node cluster, if each node has 10 licenses then 1 node can consume a maximum of 20 licenses. In that case, it will be reporting only the installed number of licenses that is, 10 licenses instead of 20 licenses.

Limitation

Note Make sure that Smart Licensing is *enabled* and Expressway is in *Specific License Reservation (SLR)* mode.

Hard Enforce Entitlement for SLR/Expiry of Smart License Reservation Licenses

After the license expires, there is no impact on the registration of calling functionalities of the Expressway device until it is restarted.

After the Expressway device is restarted, if the license has expired, the respective functionality will stop and an alarm is triggered.

The functionality associated with license expiry does stop immediately since the device triggers a notification only upon restart.

Smart Licensing Export Compliance

Note

- The Export Limit of 2500 registrations/calls/sessions is *On* by default for all customers. This means that now every customer will **not** be able to create more than 2500 encrypted connections.
- Advanced Account Security is not available.
- FIPS140-2 Cryptographic Mode is not available.
- Encrypted signaling sessions to endpoints' is capped at 2500.

Export Control Alarms

The Export Control approaching alarm and approached alarm are raised once calls and registration capacity have reached 90% and 100% of the export control limit, respectively.

Export Control limit is ideally set to a count of 2500 (Calls+Registrations). This applies to both Smart Licensing *Connected* and *Reservation* mode(s).

For more information, see "Alarms Reference".

Additional Information

The following are the values used for Export Control.

Lower Watermark for Export Control

In Export Control, a lower watermark is introduced to update if the export control limit is reached or not. The lower watermark is a 1% value of the current export control limit (~2500).

This is to avoid call(s) to change notification when there is a frequent change in the resource usage value.

For example, if the export control limit is reached (~2500). Consequently, a few calls and registrations are dropped. In the current scenario, it is considered that the export limit is reached only when calls or registrations drop until 25 (1% of 2500). New Registrations or Calls are allowed only when the resource usage value is below 2475. This is to avoid call(s) to change notification between 100% to 99% range.

Export Control Limit When WebRTC is Enabled

When WebRTC is enabled on either Cisco Expressway-C or Cisco Expressway-E, the Export Control limit value is set to 2244, since the maximum WebRTC connections allowed on the Expressway C or E is 256.

When the WebRTC value is disabled, the Export Control limit is set back to 2500.

VCS Behavior

The 2500 Limit is applicable to VCS also. But the requirement to go over the limit with crypto key is not available. From X14.2, VCS always will be within the limit and there is no crypto key to go above the 2500 limit.

Limitations

Product License Registration - Issue with Converting to Smart Licensing

This item applies if you want to convert existing Expressway licenses (RMS, Desktop, or Room) to Smart Licensing entitlements. In this case do not use the option in the Cisco Product License Registration portal to partially convert just some of the licenses. Due to a known issue, if you opt to convert only some licenses, the system automatically forfeits/removes the remaining licenses as well. So the licenses that are not converted are also removed, and a licensing case will be required to retrieve them.

To avoid this happening, please ensure that the **Quantity to Convert** field is the same value as the **Quantity Available** field; this is the default when you open the page.

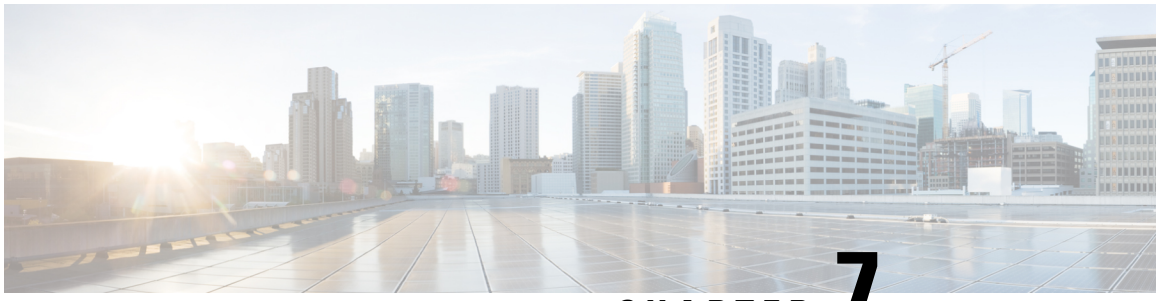
Smart Licensing not Available With Features that Use Option Keys (including HSM)

The following Expressway features are enabled by option keys. Because option keys are incompatible with Smart Licensing, if you need these features, you must use PAK-based licensing and not Smart Licensing:

- Advanced account security
- HSM (Hardware Security Module)
- Microsoft Interoperability

Expressway Reporting "Unknown CA" for Smart Licensing Through Proxy Server with Intercept Mode

The Expressway does not initiate connections with a proxy or a smart licensing server. A smart licensing agent component initiates these connections. The smart licensing agent validates certificates using its *trust store* list. Users cannot change this list. Therefore, the device rejects connections to any proxy server presenting a CA signed certificate other than the "QuoVadis Root CA 2" with an "Unknown CA" error.



CHAPTER 7

Managing Security

- Security Basics, on page 85
- Configuring Certificate-Based Authentication, on page 86
- Managing the Trusted CA Certificate List, on page 88
- Managing the Expressway Server Certificate, on page 89
- Managing Certificate Revocation Lists (CRLs), on page 90
- Managing mTLS Client Certificate Verification for MRA Onboarding, on page 93
- Testing Client Certificates, on page 93
- Testing Secure Traversal, on page 95
- Managing the Expressway Server Certificate with HSM, on page 96
- Configuring Hardware Security Module Functionality, on page 97
- Configuring Minimum TLS Version and Cipher Suites, on page 97
- Configuring SSH, on page 100
- Advanced Security, on page 101

Security Basics

Data at Rest

Every software installation (from X8.11) has a unique root of trust. Each Expressway system has a unique key that is used to encrypt data local to that system. This improves the security of data at rest in the following ways:

- The new key is created when you upgrade a pre-X8.11 version to X8.11 or later, and is used to encrypt all data on the first restart.
- Only this key can be used to decrypt data from this system. No other Expressway key can decrypt this system's data.
- The key is never exposed on the UI, and it is never logged--locally or remotely.

TLS and Certificates

For TLS encryption to work successfully in a connection between a client and server:

- The server must have a certificate installed that verifies its identity, which is signed by a Certificate Authority (CA).
- The client must trust the CA that signed the certificate used by the server.

Expressway lets you install a certificate that can represent the Expressway as either a client or a server in TLS connections. Expressway can also authenticate client connections (typically from a web browser) over HTTPS. You can upload certificate revocation lists (CRLs) for the CAs used to verify LDAP server and HTTPS client certificates. Expressway can generate server certificate signing requests (CSRs), so there is no need to use an external mechanism to do this.

Note For all secure communications (HTTPS and SIP/TLS), we recommend that you replace the Expressway default certificate with a certificate generated by a trusted CA.

Table 10: 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.

Note We also recommend using a third-party LDAP browser to verify that your LDAP server is correctly configured for TLS.

TLS can be difficult to configure. So if using it with an LDAP server, for example, we recommend verifying that the system works correctly over TCP, before you attempt to secure the connection with TLS.

Caution Certificates must be RFC-compliant. Do not allow CA certificates or CRLs to expire, as this may cause certificates signed by those CAs to be rejected.

Certificate and CRL files are managed via the web interface, and cannot be installed using the CLI.

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** (defined on the Network Services page) is 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:

Step 1 Add the Expressway's trusted CA and server certificate files (on the **Trusted CA certificate** and **Server certificate** pages, respectively).

Step 2 Configure certificate revocation lists (on the **CRL management** page).

Step 3 Use the **Client certificate testing** page to verify that the client certificate you intend to use is valid.

Step 4 Set **Client certificate-based security** to *Certificate validation* (on the **System administration** page).

Step 5 Restart the Expressway.

Step 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.

Step 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 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 Testing Client Certificates 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.

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.

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 Configuring Remote Account Authentication Using LDAP (for account authentication), you must add the PEM encoded CRL data to your trusted CA certificate file.

Note this Recommendation

The maximum number of Certificate Authority (CAs) that can be uploaded/supported to the Expressway *trust store* is 1000.

Root CAs included by default

Expressway X12.6 and later includes these trusted root CAs, which are installed as part of the *Cisco Intersection CA Bundle*:

- O=Internet Security Research Group, CN=ISRG Root X1
- O=Digital Signature Trust Co., CN=DST Root CA X3

Managing the Expressway Server Certificate

Use the **Server certificate** page (**Maintenance** > **Security** > **Server certificate**) to manage the Expressway server certificate, which identifies Expressway when it communicates with client systems using TLS encryption and with web browsers over HTTPS.

You can view details of the currently loaded certificate, generate a CSR, upload a new certificate, and configure the ACME service. These tasks are described in the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway Configuration Guides page.

Note We strongly 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 Expressway in all scenarios.

Using the ACME Service

From X12.5 the Cisco Expressway Series supports the ACME protocol (Automated Certificate Management Environment) which enables automatic certificate signing and deployment to the Expressway-E from a certificate authority such as Let's Encrypt.

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.

Make sure 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

If you deploy Mobile and Remote Access, details about the Unified Communication and Expressway certificate requirements are in the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway Configuration Guides page.

Managing Certificate Revocation Lists (CRLs)

Certificate revocation list files (CRLs) are used by the Expressway to validate certificates presented by client browsers and external systems that communicate with the Expressway over TLS/HTTPS. A CRL identifies those certificates that have been revoked and can no longer be used to communicate with the Expressway.

We recommend that you upload CRL data for the CAs that sign TLS/HTTPS client and server certificates. When enabled, CRL checking is applied for every CA in the chain of trust.

Certificate Revocation Sources

The Expressway can obtain certificate revocation information from multiple sources:

- Automatic downloads of CRL data from CRL distribution points.
- Through OCSP (Online Certificate Status Protocol) responder URIs in the certificate to be checked (SIP TLS only).
- Manual upload of CRL data.
- CRL data embedded within the Expressway's **Trusted CA certificate** file.

Limitations and Usage Guidelines

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. Also, it does not use the manual or automatic update settings on the **CRL management** page.

Automatic CRL Updates

Note We recommend that you configure the Expressway to perform automatic CRL updates. This ensures that the latest CRLs are available for certificate validation.

Step 1 Go to **Maintenance** > **Security** > **CRL management**.

Step 2 Set **Automatic CRL updates** to *Enabled*.

Step 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

Step 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.

Step 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.

Step 1 Go to **Maintenance** > **Security** > **CRL management**.

Step 2 Click **Browse** and select the required file from your file system. It must be in PEM encoded format.

Step 3 Click **Upload CRL file**.

This uploads the selected file and replaces any previously uploaded CRL file.

Click **Remove revocation** list if you want to remove the manually uploaded file from the Expressway.

If a certificate authority's CRL expires, all certificates issued by that CA will be treated as revoked.

Online Certificate Status Protocol (OCSP)

The Expressway can establish a connection with an OCSP responder to query the status of a particular certificate. The Expressway determines the OCSP responder to use from the responder URI listed in the certificate being verified. The OCSP responder sends a status of “good”, “revoked” or “unknown” for the certificate.

The benefit of OCSP is that there is no need to download an entire revocation list. OCSP is supported for SIP TLS connections only. See below for information on how to enable OCSP.

Outbound communication from the Expressway-E is required for the connection to the OCSP responder. Check the port number of the OCSP responder you are using (typically this is port 80 or 443) and ensure that outbound communication is allowed to that port from the Expressway-E.

Configuring Revocation Checking for SIP TLS Connections

You must also configure how certificate revocation checking is managed for SIP TLS connections.

1. Go to **Configuration** > **SIP**.
2. Scroll down to the **Certificate revocation checking** section and configure the settings accordingly:

Field	Description	Usage Tips
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. • The OCSP responder must support the SHA-256 hash algorithm. If it is not supported, the OCSP revocation check and the certificate validation will fail.

Field	Description	Usage Tips
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)), 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. *Treat as revoked*: Treat the certificate as revoked (and thus do not allow the TLS connection). *Treat as not revoked*: Treat the certificate as not revoked. Default: *Treat as not revoked*	*Treat as not revoked* 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.

Managing mTLS Client Certificate Verification for MRA Onboarding

The **CA certificate page for mTLS** is accessed from the **Trusted CA certificate** page (**Maintenance** > **Security** > **Trusted CA certificate**). This page only applies if you use Expressway for Mobile and Remote Access (MRA) with Cisco Unified Communications products, and onboarding with activation codes is enabled for MRA.

Testing Client Certificates

The **Client certificate testing** page (**Maintenance** > **Security** > **Client certificate testing**) is used to check client certificates before enabling Network Services. 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)).
- 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 or the browser's currently loaded certificate.

To test if a certificate is valid

Step 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)

Step 2 Ignore the **Certificate-based authentication pattern** section - this is only relevant if you are extracting authorization credentials from the certificate.

Step 3 Click **Check certificate**.
The results of the test are shown in the **Certificate test results** section.

To retrieve authorization credentials (username) from the certificate

Step 1 Select the **Certificate source** as described above.

Step 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.

Step 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.

Step 4 If necessary, you can modify the **Regex** and **Username format** fields and repeat the test until the correct results are produced.

Note 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.

Step 5 If you have changed the **Regex** and **Username format** fields from their default values and want to use these values in the Expressway's actual configuration (as specified on the **Certificate-based authentication configuration** page) then click **Make these settings permanent**.

Note
- Any uploaded test file is automatically deleted from the Expressway at the end of your login session.
- The regex is applied to a plain text version of an encoded certificate. The system uses the command **openssl x509 -text -nameopt RFC2253 -noout** to extract the plain text certificate from its encoded format.

Testing Secure Traversal

This utility tests whether a secure connection can be made from the Expressway-C to the Expressway-E. A secure connection is required for a Unified Communications traversal zone, and is optional (recommended) for a normal traversal zone.

If the secure traversal test fails, the utility raises a warning with appropriate resolution where possible.

Step 1 On the Expressway-C, go to **Maintenance** > **Security** > **Secure traversal test**.

Step 2 Enter the FQDN of the Expressway-E that is paired with this Expressway-C.

Step 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.

Step 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.

Note You must select the version of **HTTPS minimum TLS version** to test the applicability of a secure connection that enables the minimum supported TLS version by Expressway. Also, select the **HTTPS ciphers** for the same. This selection of *HTTPTLSversion* is required for connection establishment towards Unified Communication servers like VCSE, CUCM, CUP, and UCXN. These settings are configured on the **Ciphers** page (**Maintenance** > **Security** > **Ciphers**).

Managing the Expressway Server Certificate with HSM

Important HSM functionality support on Expressway may be a **Preview feature only**, depending on the Expressway software version. For example, it is a Preview feature in version X12.6. Please check the release notes for your Expressway version before you use HSM and if its status is Preview for your software version, **only enable HSM if you are willing to implement it as a Preview feature and subject to the Preview disclaimer contained in the Expressway Release Notes**. Instructions for how to configure and enable HSM are currently provided only in the Expressway Release Notes.

These instructions assume that HSM is already enabled on Expressway (**Maintenance** > **Security** > **HSM configuration**).

Step 1 Go to **Maintenance** > **Security** > **Server certificate**.

Step 2 Click **Generate CSR**. You are navigated to the **Generate CSR** page.

The **Server certificate type** section displays at the top of the **Generate CSR** page. If HSM usage is not configured, the section does not display.

If you have an Expressway cluster, issues may arise if the CSR fields are incorrectly completed. For details on how to fill these fields, see the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide* on the Cisco Expressway Series Configuration Guides page.

Step 3 After generating as HSM private key and CSR, you are returned to the **Server certificate** page.

Step 4 You can view and download the generated HSM CSR from the **Certificate signing request (CSR)** section.

Step 5 Click **Download** to download the certificate.

Step 6 Sign the certificate using certificate signing authority.

Install the HSM private key and certificate

Note Only use these instructions if you use Hardware Security Module (HSM) functionality.

Step 1 To upload a signed certificate, click **Choose File** to navigate to the location and choose the certificate.

Step 2 Select a certificate file and corresponding certificate type, and click **Upload server certificate** data to upload the certificate.

For more information, see the section about managing the Expressway's server certificate.

Download the HSM key handle across a cluster

After deploying an HSM certificate and private key to an Expressway, the HSM certificate and private key can be deployed to other Expressways in a cluster. To do this:

Step 1 On the primary peer. Download the HSM private key from the first Expressway. After deploying an HSM certificate and private key, a **Download HSM key handle** button displays on the **Server certificate data** section.

Step 2 On the cluster peers. Upload the HSM private key with HSM certificate to other peers in the cluster from the **Upload new certificate** section. Browse to and select the signed HSM certificate and private key.

Restart Expressway

After an HSM certificate is installed on Expressway, a banner on the **Server certificate** page prompts you to restart Expressway. An alarm is also raised to restart. Although the certificate is now installed, the restart is required for the Expressway to begin using it.

After the restart, the alarm disappears and all services on the Expressway use the new HSM certificate.

Configuring Hardware Security Module Functionality

The **HSM configuration** page (**Maintenance** > **Security** > **HSM configuration**) is used to manage HSM devices with Expressway.

Important HSM functionality may be a **Preview feature only**, depending on the Expressway software version. For example, it is a Preview feature in version X12.6. Please check the release notes for your Expressway version before you use HSM and if its status is Preview for your software version, only enable HSM if you are willing to implement it as a Preview feature. Instructions for how to configure HSM are currently provided only in the Expressway release notes and not in this section.

Configuring Minimum TLS Version and Cipher Suites

The **Maintenance** > **Security** > **Ciphers** page is used to manage the minimum TLS version for services on Expressway, and their associated cipher suites.

Note

- For improved security, TLS version 1.2 or later is recommended for all encrypted sessions.
- From X14.2 release, Expressway does not support Anonymous Diffie-Hellman (ADH) ciphers, any longer.

Expressway defaults to TLS 1.2 when establishing secure connections for the following:

- HTTPS

- Certificate checker
- Cisco Meeting Server discovery
- SIP
- XMPP
- UC server discovery
- Reverse proxy
- LDAP
- SMTP mail server
- TMS Provisioning Service

Restart required in some cases

A restart is required after changing the cipher suite configuration or TLS protocol version for the following:

- SIP
- XCP

Minimum TLS Version

On upgrade of an existing system, the previous behavior and defaults persist so you won't be defaulted to TLS 1.2.

For new installations, check that all browsers and other equipment that must connect to Expressway support TLS 1.2.

If required--typically for compatibility reasons with legacy equipment--the minimum TLS versions can be configured per service to use versions 1.0 or 1.1.

Cipher Suites

You can configure the cipher suite and minimum supported TLS version for services on the Expressway. The cipher suites are shown in the table (cipher strings are in OpenSSL format).

For services where the Expressway can act as a client, such as HTTPS, the same minimum TLS version and cipher suites will be negotiated.

Services	Cipher Suite Values (Defaults)
HTTPS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH
LDAP TLS Ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH

Services	Cipher Suite Values (Defaults)
Reverse proxy TLS ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH
SIP TLS ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH
SMTP TLS Ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH
TMS Provisioning Ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH
UC server discovery TLS ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH
XMPP TLS ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH

Note these Recommendations

1. From X14.2 release, Expressway does not support Anonymous Diffie-Hellman (ADH) ciphers, any longer.
2. Endpoints, for example, the E20 supports only Anonymous Diffie Hellmen (ADH) ciphers whereas Expressway does not support ADH ciphers for endpoints. This results in an issue with the TLS connection.

   Solution: Service Certificate On TC/CE Endpoints

   a. To enable certificate for SIP on TC/CE endpoints, login to **TC/CE endpoint** and follow the path -

      - **For TC endpoints** - Go to **Configuration** > **Security**.
      - **For CE endpoints** - Go to **Security** > **Service Certificate**.

   b. On the **Service Certificates** page, by default, SIP option is set to *Off*. In order to use the certificate, enable certificate for SIP, that is, must be *On*. Not enabling this option, will result in a TLS Handshake error.

Note Expressway does not support any Anonymous Diffie Hellmen (ADH) cipher for SIP services.

Configuring SSH

Tunnel Configuration

The Expressway pair uses SSH tunnels to securely transfer data from the Expressway-E to the Expressway-C without requiring Expressway-E to open the connection. The Expressway-C opens a TCP session with the Expressway-E which is listening on a fixed TCP port. The pair then use the selected cipher and algorithms to establish an encrypted tunnel for securely sharing data.

The cipher and algorithms that the pair use to encrypt SSH tunnels are configured as follows:

1. Go to **Maintenance** > **Security** > **SSH configuration**.
2. Modify the following settings, if necessary:

Note This is based on the type of certificate used. Enter the X.509 public key algorithm used to authenticate SSH tunnel. You must enter at least one peer public key algorithm.

Setting	Description
Ciphers	*aes256-ctr*: Advanced Encryption Standard using the CTR (counter) mode to encipher 256-bit blocks. (Default)
Public Key Algorithms	*x509v3-rsa2048-sha256,x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521*
Key Exchange Algorithms	*ecdh-sha2-nistp256* *ecdh-sha2-nistp384*(Default)

3. Click **Save**.

Remote Access Configuration

The cipher and algorithms that the pair use to encrypt remote access between a SSH client and server are configured as follows:

1. Go to **Maintenance** > **Security** > **SSH configuration**.
2. Modify the following settings, if necessary:

Setting	Description
Ciphers	*"aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr, aes128-ctr"*

Setting	Description
Key Exchange Algorithms	*"ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group14-sha1"*
MAC Algorithms	*"hmac-sha2-512,hmac-sha2-256, hmac-sha1"*

3. Click **Save**.

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:

- Configuring Advanced Account Security Mode
- Configuring FIPS140-2 Cryptographic Mode

Configuring Advanced Account Security Mode

Important Advanced Account Security option is **not available** for Expressway Series devices. The entire section described is applicable **only** for Cisco TelePresence Video Communication Server (VCS) Series.

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.
POST	Yes	Yes	Apply data to a web resource. For example, when an administrator saves changes to a setting using the Expressway web interface.

Method	Used by Web UI?	Used by API?	Used to...
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 Configuring Remote Account Authentication Using LDAP 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:

- Configuring SNMP Settings is disabled.
- The Network Services is set to a non-zero value.
- Network Services is enabled.
- Configuring Remote Account Authentication Using LDAP configuration uses TLS encryption and has certificate revocation list (CRL) checking set to *All*.
- Configure Logging is disabled.
- Incident Reporting is disabled.

- Any connection to an Configuring External Manager Settings 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:

Step 1 Go to **Maintenance** > **Advanced security**.

Step 2 Enter a `Classification banner`.

The text entered here is displayed on every web page.

Step 3 Set **Advanced account security mode** to *On*.

Step 4 Click **Save**.

Step 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.
- 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 If Configuring Automated 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.

Step 1 Sign in with the emergency account.

Step 2 Disable Advanced Account Security mode (**Maintenance** > **Advanced security**).

Step 3 Enable SSH service (**System** > **Administration settings**) and restart.

Step 4 After the restart is complete, connect to the console.

Step 5 Sign in as **root** and run **factory-reset**.

See Restoring the Default Configuration (Factory Reset) for details.

Configuring FIPS140-2 Cryptographic Mode

Important FIPS option is **not available** for Expressway Series devices. The entire section described is applicable **only** for Cisco TelePresence Video Communication Server (VCS) Series.

FIPS, or Federal Information Processing Standard 140 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 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.

Alternate Method of Using xcommand FIPS

Remember **Cisco VCS**: You must add J00 Option Key in **Maintenance** > **Option keys** in **Add option key** field (or using CLI command). The options available for FIPS (<*leave/enter/status*>) are only visible before adding the JOO Option Key. You can use the JOO Option Key only after it is added.

For more information, see the chapter *Reference Material*, section *Command Reference - xCommand*, section *xCommand Commands*, xCommand Fips.

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, perform a system upgrade before you continue. 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 FIPS 140-2 Cryptographic Mode

Caution The transition to FIPS 140-2 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 FIPS 140-2 cryptographic system:

Step 1 Enable FIPS 140-2 cryptographic mode:

a. Go to **Maintenance** > **Advanced security**.

b. Set **FIPS 140-2 cryptographic mode** to *On*.

c. Click **Save**.

Step 2 Fix any alarms that have been raised that report non-compliant configuration.

Note When you enable FIPS in a Mobile and Remote Access scenario, if alarm #40042 (some SIP configuration is not using TLS transport; FIPS 140-2 compliance requires TLS) is raised you can disable and enable this feature to clear the alarm.

Step 3 Take a Creating a System Backup if you want to preserve your current configuration data.

Note Ensure that all backups require password protection.

Step 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.

Step 5 Follow the prompts to complete the Install Wizard.

Step 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.

Step 7 Restoring a Previous Backup your previous data, if required.

Note While in FIPS 140-2 mode, you can only restore backup files that were taken when **FIPS 140-2 cryptographic mode** is set to *On*. Any previous administrator account information and passwords will be restored however, the previous **root** account password is not 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.

Step 8 From X12.6 you must manually change the SIP TLS Diffie-Hellman key size from the default 1024 bits, to at least 2048. To do this type the following command in the Expressway command line interface (change the value in the final element if you want a key size higher than 2048): *xconfiguration SIP Advanced SipTlsDhKeySize: "2048"*

FIPS140-2 Compliant Features

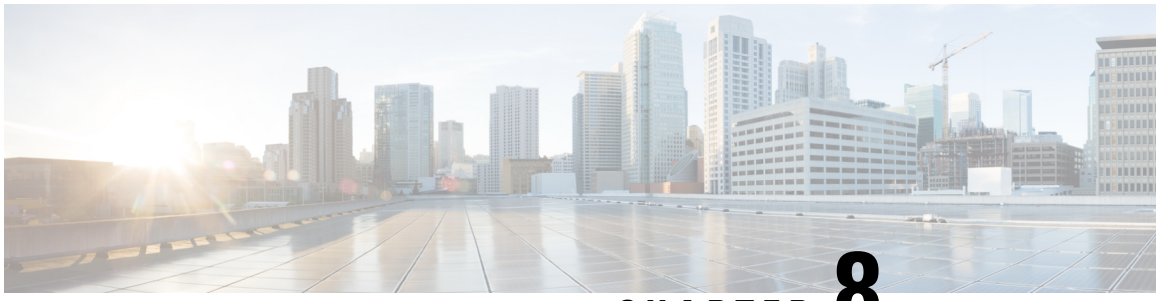
The following Expressway features are FIPS140-2 compliant / use FIPS140-2 compliant algorithms:

- 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
- 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:

- SIP authentication over NTLM / Active Directory
- SIP/H.323 device authentication against an H.350 directory service
- Microsoft Interoperability service
- Use of Cisco TMSPE



CHAPTER 8

Serviceability, Logging, Monitoring, and Metrics

- Configure Logging, on page 109
- Capture Call Detail Records, on page 114
- Configure Alarm-Based Email Notifications, on page 118
- System Metrics Collection, on page 121

Configure Logging

Expressway provides syslogging features for troubleshooting and auditing purposes. The Event Log is a rotating local log that records information about things like calls, registrations, and messages sent and received.

To configure Expressway logging options, go to **Maintenance** > **Logging**. From the **Logging** page you can do the following tasks:

- Specify the Change the Event Log Verbosity to change the depth of event information recorded locally
- Toggle Media Statistics Logging for Calls
- Toggle Capture Call Detail Records
- Toggle Certificate-Compliant Logging
- Define one or more Publishing Logs to Remote Syslog Servers addresses
- Filter by severity the events sent to each remote syslog server
- Toggle How to Configure System Metrics Collection (collected)

Change the Event Log Verbosity

You can optionally 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.

Note 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. However, you may need to record this level of detail for troubleshooting.

Events are always logged locally - to the Event Log - regardless of whether or not remote logging is enabled.

The table 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: • 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: • protocol keepalives • call-related SIP signaling messages
4	The most verbose level: all Level 1, Level 2 and Level 3 events, plus: • network level SIP messages

Changes to the log level affect both the Event Log that you view through the web interface, and the information that is copied to any remote log server. Changes are not retrospective and only affect what is logged after the change.

Expressway uses the following facilities for local logging. The software components / logs that map to the (local) facilities are emphasized:

- 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*

The Events and Levels section has a complete list of all events that are logged by the Expressway, and the level at which they are logged.

Certificate-Compliant Logging

In some environments you may want to ensure that the Expressway logs are compliant with the requirements of your security certification. There is a trade-off between security and the purpose of the logs for diagnostics, and in the certification-compliant modes it may be impossible to establish the exact cause of a problem call.

How to Configure Certification-compliant Logging

Step 1 Go to **Maintenance** > **Logging**.

Step 2 In the **Logging options** section, set the **Certification logging** mode to one of the following:

Certification logging mode	Description
Diagnostic	This mode is not certification-compliant, but is most useful for diagnosing call issues.
Secretive	This mode is certification-compliant.
Secretive and Verbose	This mode is also certification-compliant, but enables you to collect some log information using a secure connection to a syslog server. These logs are not particularly useful in the diagnostic sense.

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

Note

- 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.
- 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.

Step 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.

Step 2 Click on the **Options** button for each server.

Step 3 Specify the **Transport** protocol and **Port** you wish to use. If you choose to use TLS, you will see the option to enable Certificate Revocation List (CRL) checking for the syslog server.

Step 4 In the **Message Format** field, select the writing format for remote syslog messages. The default is *Legacy BSD*.

Step 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.

Step 6 Use the **Filter by Keywords** option if you only want to send messages with certain keywords.

Step 7 Click **Save**.

Typical Values Used

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 11: Syslog message formats

Message format	Transport protocol	Suggested port	RFC
Legacy BSD format	UDP	514	BSD format. See RFC 3164
IETF syslog format	UDP	514	IETF format. See RFC 5424
IETF syslog using TLS connection	TLS	6514	IETF format. See RFC 5424

Note

- 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 Security Basics 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 emphasized:
  - 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*

Media Statistics Logging for Calls

How to Enable Media Statistics

To optionally enable media statistics collection on the Expressway, go to **Maintenance** > **Logging** and set **Media statistics** to *On*. The system starts logging media statistics for each call, to the local hard disk in **/mnt/harddisk/log**. Up to 200 files of 10MB each are stored, and the oldest is deleted when file 200 is full.

The media statistics collected include packets forwarded, packets lost, jitter, media type, codec, and actual bitrate.

Media statistics are also published as syslog messages. While Media statistics logging is on, the Expressway publishes statistics using facility 18 (local2) to all remote syslog servers you have configured. The message severity is *Informational* but the media statistics messages are published irrespective of severity filter settings.

Capture Call Detail Records

Subject to enabling the service (which is off by default) Expressway can optionally capture CDRs. The CDRs are stored locally for seven days, and, if you use remote logging, can also be published as syslog messages.

How to Configure CDRs

To configure CDRs on Expressway:

Step 1 Go to **Maintenance** > **Logging**.

Step 2 In the **Logging Options** section, set the **Call Detail Records** field to the required option:

- *Services and Logging* - The CDRs are stored locally for 7 days and then deleted. The records are accessible from the local Event Log, and are also sent as INFO messages to your syslog host if external logging is enabled.
- *Service Only* - The CDRs are stored locally for 7 days and then deleted. The records are not accessible through the web user interface. The CDRs can only be read via the REST API.
- *Off* - CDRs are not logged locally. This is the default setting.

CDR Properties

This table defines the properties that are visible in CDRs:

Field	Definition
uuid	ID of the CDR entry.
service_uuid	ID used to identify whether a record is from a proxy, Lync B2BUA or Encryption B2BUA.
active	Whether a call is a live or a historical one.
initial_call	Used internally to tie to a B2BUA call when it is a multiple-component one (involves a B2BUA hop).
licensed	Shows if a call used a license.
licensed_as_traversal	Shows if a call used a traversal license.
status	200 OK message indicates a call was successful. Contains an error message if the call was unsuccessful.
tag	Call ID.
box_call_serial_number	Extra ID added to tie multiple calls together (for example, through the B2BUA).

Field	Definition
start_time	Date and time of the call. Time zone can be set in **System** > **Times** > **Time Zone** and the date format is YYYY-MM-DD.
end_time	End time of the call.
source_alias	Alias of the caller.
destination_alias	Alias of the callee.
aside_destination_alias	Alias of the caller (or MS Lync client if Lync Interop).
bside_destination_alias	Alias of the callee (or non-Lync client).
aside_request_uri	Request uri of the caller (or MS Lync client if Lync Interop).
bside_request_uri	Request uri of the callee (or non-Lync client).
protocol	Shows if the call was SIP <-> SIP, SIP <-> H323, H323 <-> SIP, or H323 <-> H323.
protocol_summary	As above but can have extra info like if a call was multi-component, DVO, etc.
media_routed	Shows if media was sent during the call (e.g. NAT/IWF/B2BUA).
audio	Shows if the call was an audio-only one.
traversal_license_tokens	Indicates if a call fork/branch took media (audio equates to 1 token and video 2).*
non_traversal_license_tokens	Indicates if a call fork/branch did not need to take media (audio equates to 1 token and video 2).*
disconnect_reason	Gives reasons for a call drop such as normal call teardown or other errors (that is, the last status).
details	Gives more details of the call, including media statistics.
last_updated_timestamp	Last time that any of the above fields were updated.

* Once a call is set up only one of these entries will have a non-zero value (i.e. only for the answered fork/branch).

APIs to Access CDRs

You can use the following secure REST APIs to gather CDRs:

- get_all_records (returns all records up to seven days old).
- get_records_for_interval (returns records from during the time specified).
- get_records_for_filter (filters results using any combination).
- get_all_csv_records (returns all records up to seven days old in csv format).

Important The call history is stored locally for seven days only, and is deleted automatically.

To access the desired API use the following URL:

https://%3CExpressway_IP%3E/api/external/callusage/%3CAPI%3E

API examples

- http://%3CExpressway_IP%3E/api/external/callusage/get_all_records
- `http://<Expressway_IP>/api/external/callusage/get_records_for_interval?fromtime=<fromtime>&totime=<to_time>`

  for example,

  ```
  https://203.0.113.17/api/external/callusage/
  get_records_for_interval?fromtime=2014-05-09 2000:00:00&totime=
  2014-05-10 2000:00:00
  ```

Input Parameters

Parameter	Description
fromtime	Mandatory. The start time from which the CDR records are required. **Format**: *YYYY-MM-DD HH:MI:SS*
totime	Mandatory. The end time from which the CDR records are required. **Format**: *YYYY-MM-DD HH:MI:SS*

- `http://<Expressway_IP>/api/external/callusage/get_records_for_interval?fromtime=<fromtime>&totime=<to_time>`

  for example,

  ```
  https://203.0.113.17/api/external/callusage/
  get_records_for_interval?fromtime=2014-05-09 2000:00:00&totime=
  2014-05-10 2000:00:00
  ```

- `http://<Expressway_IP>/api/external/callusage/get_records_for_filter?uuid=<uuid>&src_alias=<src_alias>&dest_alias=<dest_alias>&protocol=<protocol>`

  for example,

  ```
  https://203.0.113.17/api/external/callusage/
  get_records_for_filter?uuid=6e3b5a8a-346c-421b-aa2e-f4409c43a81a
  &src_alias=TC149-057-h323@domain.com&dest_alias=
  TC149-065-h323@domain.com&protocol=H323 <-> H323
  ```

Input Parameters

Parameter	Description
uuid	Unique identifier of the record.
src_alias	Origin point of the call.

Parameter	Description
dest_ alias	Destination point of the call.
protocol	Protocol that was used for the call (SIP, H323 etc).

- http://%3CExpressway_IP%3E/api/external/callusage/get_all_csv_records

CDR Examples

Sample CDR

This sample CDR applies to all APIs except csv:

[{"initial_call": "false", "protocol": "SIP <-> SIP", "protocol_summary": "", "disconnect_reason": "200 OK", "licensed": "false", "tag": "b8d52a60-16a1-4bdb-be93-f5a675408811", "aside_request_uri": "", "box_call_serial_number": "22cd0e7d-c498-4068-9239-624038fe5130", "source_alias": "sip:10000005@10.196.4.82", "uuid": "800fe013-83f4-4094-a5e6-e2f9489912e2", "last_updated_timestamp": 1444725389, "details": "{\"Call\":{\"SerialNumber\":
\"800fe013-83f4-4094-a5e6-e2f9489912e2\",\"BoxSerialNumber\":
\"22cd0e7d-c498-4068-9239-624038fe5130\",\"Tag\": \"b8d52a60-16a1-4bdb-be93-f5a675408811\",\"State\":
\"Disconnected\",\"StartTime\": \"2015-10-13 01:36:26.485636\",\"InitialCall\": \"False\",\"Licensed\":
\"False\",\"LicensedAsTraversal\": \"False\",\"SourceAlias\":
\"sip:10000005@10.196.4.82\",\"DestinationAlias\": \"sip:10000010@cucm-82\",\"ToLocalB2BUA\":
\"False\",\"Audio\": \"False\",\"License\":{\"Traversal\": \"0\",\"NonTraversal\": \"0\",\"DemotedTraversal\":
\"0\",\"CollaborationEdge\": \"0\",\"Cloud\": \"0\"},\"Duration\": \"3\",\"Legs\":[{\"Leg\":{\"Protocol\":
\"SIP\",\"SIP\":{\"Address\": \"10.196.4.61:5073\",\"Transport\": \"TLS\",\"Aliases\":[{\"Alias\":{\"Type\":
\"Url\",\"Origin\": \"Unknown\",\"Value\":
\"sip:10000005@10.196.4.82\"}}]},\"Targets\":[{\"Target\":{\"Type\": \"Url\",\"Origin\":
\"Unknown\",\"Value\": \"sip:10000010@10.196.4.116\"}}],\"BandwidthNode\":
\"DefaultZone\",\"EncryptionType\": \"AES\",\"Cause\": \"200\",\"Reason\": \"OK\"}},{\"Leg\":{\"Protocol\":
\"SIP\",\"SIP\":{\"Address\": \"10.196.4.71:7001\",\"Transport\": \"TLS\",\"Aliases\":[{\"Alias\":{\"Type\":
\"Url\",\"Origin\": \"Unknown\",\"Value\":
\"sip:10000010@cucm-82\"}}]},\"Source\":{\"Aliases\":[{\"Alias\":{\"Type\": \"Url\",\"Origin\":
\"Unknown\",\"Value\": \"10000005@10.196.4.82\"}}]},\"BandwidthNode\":
\"Traversal-zone\",\"EncryptionType\": \"AES\",\"Cause\": \"200\",\"Reason\":
\"OK\"}}],\"Sessions\":[{\"Session\":{\"Status\": \"Completed\",\"MediaRouted\": \"False\",\"CallRouted\":
\"True\",\"Participants\":{\"Leg\": \"1\",\"Leg\": \"2\",\"Incoming\":{\"Leg\": \"1\"},\"Outgoing\":{\"Leg\":
\"2\"}}}}],\"EndTime\": \"2015-10-13 01:36:29.745651\"}}", "status": "Disconnected", "destination_alias":
"sip:10000010@cucm-82", "licensed_as_traversal": "false", "service_uuid":
"e6723fd0-5ca2-11e1-b86c-0800200c9a66", "start_time": "2015-10-13 01:36:26.485636",
"traversal_license_tokens": 0, "bside_destination_alias": "", "active": "false", "media_routed": "false",
"aside_destination_alias": "", "non_traversal_license_tokens": 0, "bside_request_uri": "", "end_time":
"2015-10-13 01:36:29.745651", "audio": "false”}]

Sample csv CDR

```
uuid,service_uuid,active,initial_call,licensed,licensed_as_traversal,
status,tag,box_call_serial_number,start_time,end_time,source_alias,
destination_alias,aside_destination_alias,bside_destination_alias,
aside_request_uri,bside_request_uri,protocol_summary,protocol,
```

```
media_routed,audio,traversal_license_tokens,non_traversal_license_tokens,
disconnect_reason,details,last_updated_timestamp

800fe013-83f4-4094-a5e6-e2f9489912e2,e6723fd0-5ca2-11e1-
b86c-0800200c9a66,false,false,false,false,Disconnected,b8d52a60-16a1-
4bdb-be93-f5a675408811,22cd0e7d-c498-4068-9239-624038fe5130,2015-10-
13 01:36:26.485636,2015-10-13
```

01:36:26.485636,2015-10-13 01:36:29.745651,sip:10000005@10.196.4.82,sip:10000010@cucm-82,,,,,,SIP <-> SIP,false,false,0,0,200 OK,"{""Call"":{""SerialNumber"": ""800fe013-83f4-4094-a5e6-e2f9489912e2"",""BoxSerialNumber"": ""22cd0e7d-c498-4068-9239-624038fe5130"",""Tag"": ""b8d52a60-16a1-4bdb-be93-f5a675408811"",""State"": ""Disconnected"",""StartTime"": ""2015-10-13 01:36:26.485636"",""InitialCall"": ""False"",""Licensed"": ""False"",""LicensedAsTraversal"": ""False"",""SourceAlias"": ""sip:10000005@10.196.4.82"",""DestinationAlias"": ""sip:10000010@cucm-82"",""ToLocalB2BUA"": ""False"",""Audio"": ""False"",""License"":{""Traversal"": ""0"",""NonTraversal"": ""0"",""DemotedTraversal"": ""0"",""CollaborationEdge"": ""0"",""Cloud"": ""0""},""Duration"": ""3"",""Legs"":[{""Leg"":{""Protocol"": ""SIP"",""SIP"":{""Address"": ""10.196.4.61:5073"",""Transport"": ""TLS"",""Aliases"":[{""Alias"":{""Type"": ""Url"",""Origin"": ""Unknown"",""Value"": ""sip:10000005@10.196.4.82""}}]},""Targets"":[{""Target"":{""Type"": ""Url"",""Origin"": ""Unknown"",""Value"": ""sip:10000010@10.196.4.116""}}],""BandwidthNode"": ""DefaultZone"",""EncryptionType"": ""AES"",""Cause"": ""200"",""Reason"": ""OK""}},{""Leg"":{""Protocol"": ""SIP"",""SIP"":{""Address"": ""10.196.4.71:7001"",""Transport"": ""TLS"",""Aliases"":[{""Alias"":{""Type"": ""Url"",""Origin"": ""Unknown"",""Value"": ""sip:10000010@cucm-82""}}]},""Source"":{""Aliases"":[{""Alias"":{""Type"": ""Url"",""Origin"": ""Unknown"",""Value"": ""10000005@10.196.4.82""}}]},""BandwidthNode"": ""Traversal-zone"",""EncryptionType"": ""AES"",""Cause"": ""200"",""Reason"": ""OK""}}],""Sessions"":[{""Session"":{""Status"": ""Completed"",""MediaRouted"": ""False"",""CallRouted"": ""True"",""Participants"":{""Leg"": ""1"",""Leg"": ""2"",""Incoming"":{""Leg"": ""1""},""Outgoing"":{""Leg"": ""2""}}}}],""EndTime"": ""2015-10-13 01:36:29.745651""}}",1444725389

Configure Alarm-Based Email Notifications

Expressway supports email-based notifications based on alarm severity and optionally by alarm ID. If configured, when an alarm is generated in the system an email notification is sent to the configured destination address. For each alarm severity classification you can define a different email ID, to differentiate the urgency of the notification. Multiple email IDs can be configured for alarms of the same severity.

From X12.6.2 you can also direct notifications for a specific alarm ID to a particular email ID, or disable notifications for a specific alarm ID.

Important The maximum permitted length for email IDs is 256 characters.

This functionality is also available to U.S.-based customers who want to implement Kari's Law. When a 9-1-1 call is made which meets the criteria for direct 9-1-1 dialing through Expressway, an alarm of severity *Emergency* is generated, and (if configured) a notification will be sent to the email ID configured for the alarm severity *Emergency*.

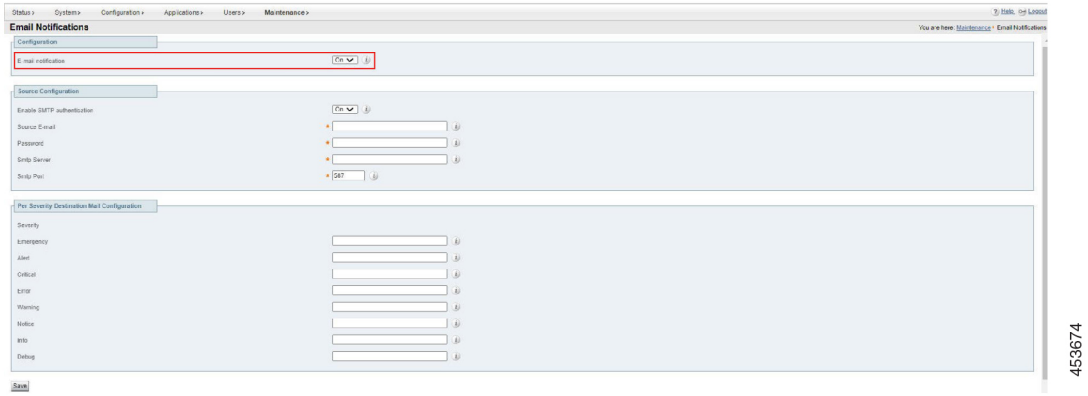
Before You Begin

- You will need to provide SMTP server details to establish the connection for sending the email.
- Expressway only supports the TLS connection with the SMTP server.
- The SMTP server must be reachable from Expressway either directly or using an SMTP proxy. Using an HTTP proxy for SMTP is not supported.
- The source email and password are validated in the SMTP server before sending the mail.
- From X12.7, Expressway requires SMTP services to use TLS 1.2 certificate-based verification.
  - As the client validates the SMTP server certificate, its IP address and/or Fully Qualified Domain Name (FQDN) must be in the certificate's Common Names (CN)/ Subject Alternative Names (SAN).
  - The SMTP server certificate issuer needs to be imported into the Expressway trusted Certificate Authority (CA) certificate list (**Maintenance** > **Security** > **Trusted CA Certificate**).

Process to Configure Alarm-Based Email Notifications

Step 1 Go to **Maintenance** > **Email Notifications**.

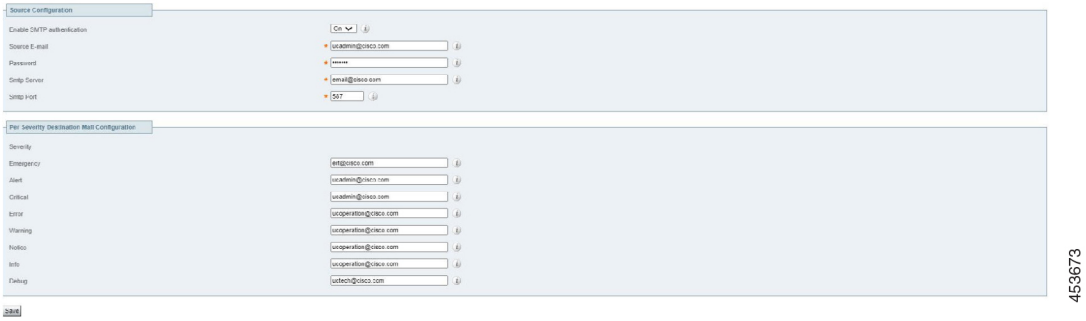
Step 2 In the **Email notification** drop-down list, select *On*.



Step 3 In the **Source Configuration** section, enter the following information:

- **Enable SMTP authentication** - The SMTP server authentication is enabled (in *On* state) by default. The drop-down list allows you to toggle between *On* and *Off* state. It should be turned *Off* only if the User's SMTP server doesn't require authentication. Most of the Users require it.
- Source email address from which notifications are sent to the configured destination address.
- IP address or FQDN of the SMTP server to be used to send the notifications.
- In the **Per Severity Destination Mail Configuration** section, enter the email address that you want to receive notifications for alarms of a given severity.
- Click **Save**.

Figure 7: Example configuration for email notifications



How to Customize Notifications - Disable or Send to an Email Address

Optionally use this process to send notifications for a given alarm ID to a specific email address, or to disable notifications for a given alarm ID altogether. For example to send threshold warning alarms to a designated individual, or to stop notifications from an unwanted alarm.

Step 1 Go to the **Custom notifications** section of the **Email notifications** page. Here you can view, edit, and delete existing custom notifications, and add new ones.

Step 2 To create a customized notification:

a. Click **Add**.

b. Select the alarm ID you want to work with.

c. In the **Notification** drop-down select *Custom* to define an email destination for the selected alarm, or select *Disable* if you don't want emails to be sent for this alarm.

d. If you selected Custom, in the **Email** field type the destination email address to which the selected alarm notifications are to be sent.

e. Click **Save**.

f. To test that the alarm notifications work as you intended:

1. Select the alarm to test from the **Select Alarm** dropdown.
2. Click the **Test Now** button.
3. Check that the email notification(s) received from the test are as expected.

Reducing Email Notifications

The purpose of this improvement is to stop spamming the administrator with emails if, for some reason, multiple alarms are raised over a short period.

From X14.2, if the same alarm is raised two or more times within an hour, emails will be sent only once. If the same alarm gets lowered, and raised again, email will be sent, regardless of the time passed. Obviously, this only applies when the administrator has configured to receive email notifications on a device.

Note If an email is already sent for a specific alarm within the last one hour, the system must not send repeated email notifications.

Here are a few examples.

1. **Example 1**
   a. Alarm with ID 15000 gets raised at 14:00.
   b. Email notification is configured and email is sent for the alarm with ID 15000.
   c. The same alarm (with ID 15000) gets raised at 14:55, an email notification will not be sent as an hour has not passed. However, if the same alarm is raised at 15:01, an email notification is sent.

2. **Example 2**
   a. Alarm with ID 15000 gets raised at 14:00.
   b. Email notification is configured and email is sent for the alarm with ID 15000.
   c. The same alarm is lowered at 14:05.
   d. Alarm with ID 15000 gets raised again at 14:10.
   e. Email notification for alarm with ID 15000 is sent again.

System Metrics Collection

System Metrics Collection is a feature on Expressway that publishes system performance statistics, to allow remote monitoring of performance. 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. You can configure this feature on Expressway through the web interface or the command line.

Note Configuration from one peer applies throughout the cluster, so if you are monitoring a cluster we recommend configuring System Metrics Collection on the primary peer.

Configuration is also required on the remote server. The collectd daemon must be running on the server, with the collectd network plugin configured to listen on an address that can be seen by the clients. The configuration details depend on your monitoring environment and are beyond the scope of this guide.

How to use the collected data

You can use tools such as Circonus and Graphite to generate graphs and aggregate statistics, and to analyze performance, based on the data collected from Expressway. You can also use it to visualize trends and even to predict potential issues. Metrics that you can visualize include:

- Active calls per zone and by system
- Key process metrics: System CPU, user CPU, and memory usage of key processes
- Alarms

How to Configure System Metrics Collection (collected)

Configure on Expressway

Use this procedure to optionally configure Expressway from the web user interface, to collect statistics and publish them to a specified server.

Note You need System Metrics Server IP Address to turn *ON* collectd from CLI (similar behavior as for Web User Interface).

Step 1 Log on to the Expressway and go to **Maintenance** > **Logging**.

Step 2 Toggle **System Metrics Collection** to *On*.

Step 3 Enter the `Collection server address`.

You can use IP address, hostname, or FQDN to identify the remote server.

Step 4 Change the default **Collection server port** (the listening port) if necessary - if the collection server is listening on a non-default port.

Step 5 Change the default **Collection Interval** if necessary - if your policy requires finer-grained metrics than the default interval of 60 seconds.

Step 6 Click **Save**.

Examples of the CLI Commands to Configure Collectd

If you prefer to use the CLI, these are examples of the relevant commands:

Table 12: CLI commands to configure collectd

What the command does	Example command
Toggle Metrics Collection on/off	**xconfig log SystemMetrics mode: on**
Specify the server address	**xconfig log SystemMetrics network address: address**
Specify the listening port	**xconfig log SystemMetrics network port: 25826**

What the command does	Example command
Specify the collection interval	**xconfig log SystemMetrics interval: 60**
Read System Metrics configuration	**xstatus SystemMetrics**

Configure a Remote Server

Selection and configuration of the server you use for data analytics in your environment is beyond the scope of this document. Circonus and Graphite are examples of applications that can handle collectd information. Your analytics tool must support receiving data from the collectd daemon. This daemon is running on the Expressway and pushes the metrics to your analytics server, using the collectd network plugin.

The network plugin implements the collectd binary protocol for data encapsulation. The analytics server must be able to parse and present this data. Your analytics server will probably have its own UI for configuring how it collects and shows the data, which could be based on collectd or an alternative software.

If you are using collectd on the analytics server, modify *collectd.conf* file so that the server:

- Listens for data from the collectd clients (such as Expressway). You need to enable the network plugin and configure the listen block with the server's IP address. For example:

```
<Plugin "network">
                Listen "198.51.100.15"
        </Plugin>
```

- Stores the data it receives in a human readable form (such as CSV files). You need to enable the csv plugin to tell it where to write the files. For example:

```
<Plugin "csv">
                 DataDir "/var/lib/collectd/csv"
                 StoreRates true
        </Plugin>
```

More information

- https://collectd.org/wiki/index.php/Networking_introduction
- https://collectd.org/documentation/manpages/collectd.conf.5.shtml#plugin_network
- https://collectd.org/wiki/index.php/Binary_protocol
- https://collectd.org/wiki/index.php/Plugin:CSV
- https://collectd.org/documentation/manpages/collectd.conf.5.shtml#plugin_csv

Troubleshooting

To check whether Expressway is sending data, configure a TCP dump from the Expressway and check for packets sent to the address of the data analytics server. Go to **Maintenance** > **Diagnostics** > **Diagnostics logging**, check **Take tcpdump while logging** and start logging.

Metrics Collected from Expressway

The following hardware statistics are monitored:

- aggregation-cpu-sum
- aggregation-cpu-average
- Per-core CPU usage for each core in the system
- df
- disk
- load
- protocols-Tcp
- protocols-Udp
- swap
- Users
- memory
- Uptime
- Process

The following application data is monitored by the custom exec-app plugin for collectd:

- `gauge-active_alarms` is the count of active alarms on this Expressway
- `gauge-active_calls` is the count of calls being handled by this Expressway
- `gauge-<service name>` is the status of each system service.
- `gauge-<zone name>_ActiveCalls` counts the active calls in the named zone
- `gauge-<zone name>_BandwidthAllocated` measures the total bandwidth allocated to the named zone
- `gauge-<zone name>_BandwidthLimit`

Each of these metrics uses the collectd GAUGE data source type, which allows free-form data. On the collection server, the full collectd value name will be shown, for example *collectdHostnamecollectd.exec-app.gauge-active_calls*.

Note Zone names are user-configurable and may thus be in conflict with the naming schema for collectd metrics. If your collection server is enforcing the schema, there is a chance that metrics from some zones will not be accepted.

Data that's sent to the collection server

The network plugin uses the collectd binary protocol to encapsulate numeric, string, and value data representing the monitored hardware resources and software processes. The plugin pushes the metrics data packets to the analytics server once every interval, using UDP 25826 by default. The analytics server parses and presents the data in human readable form.

If the analytics server is using the collectd network plugin and csv plugin, then the metrics are stored as small CSV files, using the metric name and timestamp to create the filename. For example, *gauge-H323-2015-05-21*

collectd plugins

These collectd plugins are implemented in Expressway:

Plugin name	Description
Aggregation	Aggregates CPU values into the counters `aggregation_cpu_sum and aggregation_cpu_average`.
CPU	Processor information. The raw information is `aggregated into aggregation_cpu_average and aggregation_cpu_sum`.
DF	File system information; see DF description on collectd Wiki.
Disk	Hard disk performance; see Disk description on collectd Wiki.

Plugin name	Description
Exec-app	Customized version of **exec** that returns specific Expressway information on calls, alarms, zones, and services. • gauge-active_alarms → Count of Active Alarms on Expressway • gauge-active_calls → Count of Active Calls Handled by Expressway • gauge-B2BUA → Status of B2BUA Service • gauge-callusagemanager → Status of service used for CDR's • gauge-<zone>_ActiveCalls → Count the active calls in the named zone • gauge-<zone>_BandwidthAllocated → Measures the total bandwidth allocated to the named zone • gauge-c_mgmt → ManagementConnector service • gauge-collectd → Status of Collectd service • gauge-edgeconfigprovisioning → Status of provisioning service used with MRA • gauge-fail2ban → Status of fail2ban service used with Automated Protection Feature • gauge-findmed → Status of FindMe service, used with TMS provisioning

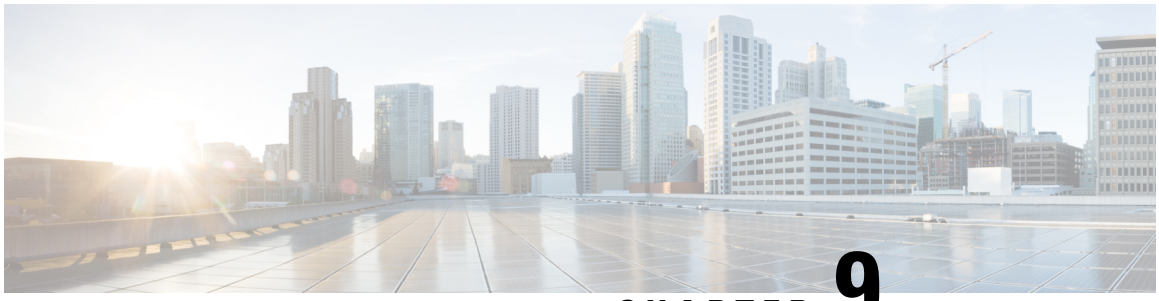
Plugin name	Description
Exec-app	• gauge-H323 → Status of H.323 Service handler • gauge-http → Status of Redirect of http request to https • gauge-https → Enabled/Disabled the web Interface • gauge-importcontrol → Status of service used with TMS provisioning • gauge-jabberd → Status of service used with XMPP • gauge-phonebookserver → Status of Phonebook service • gauge-portforwarding → Status of service used with Traffic Sever (ATS) • gauge-provisioningd → Status of service used with TMS provisioning • gauge-provisioningserver → Service status of provisioning server • gauge-proxy-registrationd → Counter for Proxy registrations on Exp-E • gauge-restmanager → Status of RESTAPI service • gauge-samlverifier → Status for service used with SAML SSO • gauge-SIP → Status of SIP Service handler • gauge-snmpd → Status of SNMP service • gauge-sshd → Status of SSH service

Plugin name	Description
Exec-app	• gauge-sshdpfwd → Status of SSH PortForwarding Service used with MRA/WebRTC etc. • gauge-sslh → Status of service used with WebRTC and TURN • gauge-trafficserver → Status of ATS service used for MRA/WebRTC etc. • gauge-winbindd → Internal Expressway service, Status of the service
Load	System load based on task queue.
Memory	Memory statistics.
Network	Enables publishing to a remote address. The plugin implements the collectd binary protocol for data encapsulation. The remote server must have the appropriate parsing tool.
Protocols	Configurable subset of the protocols used by the Expressway.
Process	Counts the system processes and groups them by state (such as running, sleeping, zombies). Also collects detailed statistics about specific processes. The plugin monitors the following processes in detail: • app → Status of Main APP process • bramble → Deprecated, used for presence notifications • credentialmanagerservermain → Status for process used for Authentication Purposes • cvs_main → Status for Certificate verifier process • erlang-beam → Internal CDB process status • erlang-epmd → Internal CDB Process status • httpd → HTTP daemon process status

Plugin name	Description
Process	• httpserver → HTTP server process status • ivy → Internal B2BUA process status • licensemanagerservermain → Status for Licensing process • managementconnectormain → Status for Management Connector Process • managementframework → Internal Process Status • openssl2nss → Status for SSL process. • policyservermain → Status for Policy Service used for call routing etc. • sshdpfwd → SSH port-forwarding process status, used with MRA, WebRTC • syslog-ng → Status for Syslog process • traffic_server → Status for ATS process, used with MRA, WebRTC • XCP → Status of Internal process with JabberD

Plugin name	Description
Statsd	Customized version that returns specific Expressway information. For example, ICE usage. • gauge-ICEPassthroughMetrics.b2buacalls → B2BUA Call is connected • gauge-ICEPassthroughMetrics.candidatesofferedmissingiceconfig → B2BUA Call is connected but ingress/egress zones are not properly configured for ICE Passthrough. If one or both endpoints offer ICE, peg a metric to indicate that there may be a configuration issue to investigate. • gauge-ICEPassthroughMetrics.failedicenegotiationcalls → Expressway is configured for ICE Passthrough and endpoints signaled they were going to attempt to negotiated ICE, but one or both failed to send remote candidates Passthrough ICE Failed to be negotiated. • gauge-ICEPassthroughMetrics.hosthostcalls → Both sides have remote candidates and both sides have a selected local candidate type. This is an ICE Passthrough call. host candidate and host candidate. • gauge-ICEPassthroughMetrics.hostrelaycalls → Both sides have remote candidates and both sides have a selected local candidate type. This is an ICE Passthrough call. host candidate and relay candidate. • gauge-ICEPassthroughMetrics.hostsrvrflxcalls → Both sides have remote candidates and both sides have a selected local candidate type. This is an ICE Passthrough call. host candidate and server reflexive candidate. • gauge-ICEPassthroughMetrics.icecalls → Both sides have remote candidates and both sides have a selected local candidate type. This is an ICE Passthrough call. • gauge-ICEPassthroughMetrics.icecandidatecalls → One or both sides offered ICE candidates. • gauge-ICEPassthroughMetrics.iceconfiguredcalls → B2BUA Call is connected and both sides were properly configured for ICE Passthrough. • gauge-ICEPassthroughMetrics.noicecandidatesoffered → Neither side offered ICE candidates.

Plugin name	Description
Statsd	• gauge-ICEPassthroughMetrics.onepartyicecandidatecalls → One or both sides offered ICE candidates. • gauge-ICEPassthroughMetrics.relayrelaycalls → Both sides have remote candidates and both sides have a selected local candidate type. This is an ICE Passthrough call. relay candidate and relay candidate. • gauge-ICEPassthroughMetrics.srvrflxrelaycalls → Both sides have remote candidates and both sides have a selected local candidate type. This is an ICE Passthrough call. server reflexive candidate and relay candidate. • gauge-ICEPassthroughMetrics.srvrflxsrvrflxcalls → Both sides have remote candidates and both sides have a selected local candidate type. This is an ICE Passthrough call. server reflexive candidate and server reflexive candidate.
Swap	Amount of system memory written to disk.
Uptime	Tracks system uptime, providing counters like average running time or maximum uptime for a particular period; see Uptime description on collectd Wiki.
Users	Count of currently logged in users.



CHAPTER 9

Network and System Settings

- Network Settings, on page 133
- Intrusion Protection, on page 142
- Network Services, on page 151
- Configuring External Manager Settings, on page 164
- Configuring the Dedicated Management Interface (DMI), on page 165
- Configuring TMS Provisioning Extension Services, on page 168

Network 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).

Ethernet Settings

Note The speed settings on this page are for systems running on Cisco Expressway physical appliances only. They do not apply to virtual machine (VM)-based systems. The connection speed shown for VM systems is invalid, and always appears as 10000 Mb/s regardless of the actual speed of the underlying physical NIC(s). This is because VMs cannot retrieve the actual speed from the physical NIC.

The **Ethernet** page (**System** > **Network interfaces** > **Ethernet**) displays the connection speeds between Expressway and the Ethernet networks to which it is connected. As the Expressway only supports auto-negotiation, the **Speed** is always *Auto*. The Expressway and the connected switch automatically negotiate the speed and the duplex mode for the connection.

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.

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 stateless auto-configuration (SLAAC) address.

The **Maximum transmission unit (MTU)** defaults to 1500 bytes.

If you have **Advanced Networking** enabled, you can also configure these options for the LAN 2 port.

Detecting a Duplicate IPv4 Address on Your Network

Duplicate IPv4 address detection in the network is performed every 300 seconds (5 minutes) on all enabled LAN interfaces. An alarm is raised if a duplicate IPv4 address is detected. The alarm raised for a specific interface is lowered within the next 5 minutes after the conflict is resolved. You can see or check this duplicate address on the User Interface and CLI command. This Command only detects duplicate IPv4 addresses. It does not detect an IPv6 address.

Dedicated Management Interface

If you want to enable the Expressway's DMI:

Step 1 Set **Use Dedicated Management Interface** to *Yes*.

Step 2 In the **LAN3 - DMI** section:

a. Specify the IPv4 and/or IPv6 address of the LAN3 port.

b. For IPv4 also specify the subnet mask.

c. For IPv6 use a static, global address. It cannot be link-local or stateless SLAAC.

d. Optionally change the maximum Ethernet packet size that can be sent over the DMI by setting the **Maximum transmission unit (MTU)** for the port. The default is 1500 bytes.

Step 3 Restart the system. These changes require a restart to take effect.

The DMI is now activated on LAN3 as an interface for management traffic. If you want the DMI to be the *sole* interface for management, go on to the next tasks.

What to do next

Make DMI Sole Interface

Make DMI Sole Interface

(Optional) Make DMI Sole Interface - Server Management Traffic

Use this task to make management traffic use the DMI, where Expressway is the server.

1. You can do this for administration services (web user interface, REST API, and CLI) and/or for SNMP. Do either or both the following steps, depending on which services you want to configure for DMI only:
   - Go to the **System** > **SNMP** page and in the **Configuration** section set **Use Dedicated Management Interface** only to *Yes*.
   - Go to the **System** > **Administration settings** page and in the **Services** section set **Use Dedicated Management Interface only (for administration)** to *Yes*.
2. You need to restart the system for the changes to take effect for the web user interface and the API, which remain accessible from LAN1 / LAN2 until you restart. Changes take immediate effect for the command line interface (SSH) and SNMP service, regardless of restart.

The specified management services can now be accessed only from the DMI / LAN3 port.

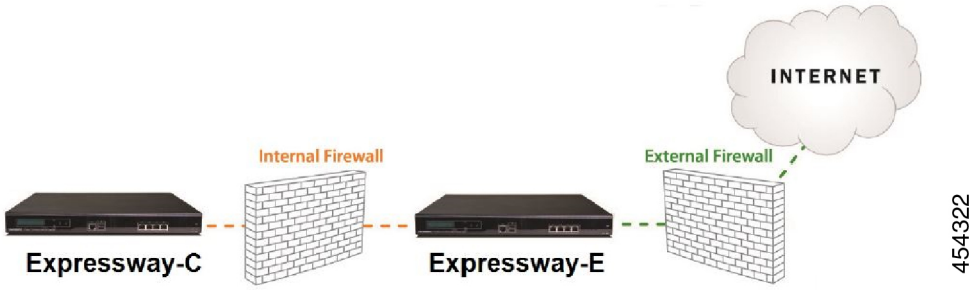
Note Expressway will not let you disable the DMI while a management service is configured to use it as the only interface.

(Optional) Make DMI Sole Interface - Client Management Traffic Outside Subnet

Depending on the Expressway software version, for management traffic where Expressway acts as the client, the traffic may only be directed to the DMI if the target server is in the same subnet as the DMI / LAN3 port. Check your release notes to see if this issue applies. If it does, and if it's not possible to deploy the server in the same subnet as LAN3, you can optionally force Expressway management traffic to use the DMI, by configuring static IP routes for LAN3 per service.

About Advanced Networking and Dual Network Interfaces

The Advanced Networking feature enables the LAN 2 Ethernet port on the Expressway-E, to allow a secondary IP address for the Expressway. It 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.



Configuring Dual Network Interfaces

Dual network interfaces are **only supported on Expressway-E** systems; you cannot deploy them on an Expressway-C.

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 dual network interfaces

Before you begin

- Configure the LAN 1 port and restart the Expressway before you configure the LAN 2 port.
- The LAN 1 and LAN 2 interfaces must be on different, non-overlapping subnets.
- 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.

Step 1 Set **Use dual network interfaces** to *Yes*.

Step 2 Select *LAN2* as the interface in the **External LAN interface** setting.

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

Troubleshooting Tips

If you have Advanced Networking enabled but only want to configure one of the Ethernet ports, switch **Use dual network interfaces** to *No*

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 static NAT

For the externally-facing LAN port, specify the following settings:

Step 1 In the **IPv4 address** field, enter the private IP address of the port.

Step 2 Set **IPv4 static NAT mode** to *On*.

Step 3 In the **IPv4 static NAT address** field, enter the public IP address of the port - 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.
- Mobile and Remote Access (MRA)

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.
- 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.
- 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 DNS servers and DNS settings on the Expressway.

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).
- It must contain only letters, digits, hyphens, and underscore. The first character must be a letter, and the last character must be a letter or a digit.

The **Domain name** is used when attempting to resolve unqualified server addresses (for example, ldapserver). It's 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. The domain name applies to the following Expressway configuration settings:

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

We recommend using an IP address or FQDN (Fully Qualified Domain Name) for all server addresses (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 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.

Custom domain searches

The **Search domains** setting is relevant for Edge deployments where the external hosts are in a different DNS domain from Expressway-C, and are configured with non-qualified hostnames. You can optionally use this setting to specify one or more DNS domains. The Expressway appends these domains one by one, to the unqualified hostname and queries DNS for the resultant FQDN. It repeats this process until DNS returns an IP address. This means that there's no need to enter FQDNs when configuring connections between hosts.

Use a space to separate multiple addresses.

DNS requests

By default, DNS requests use a random port from within the system's ephemeral port range. If required, you can specify a custom port range instead by setting **DNS requests port range** to *Use a custom port range* and then defining the **DNS requests port range start** and **DNS requests port range end** fields.

Note 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 the following:

- FQDNs instead of IP addresses when specifying external addresses (for example, for LDAP and NTP servers, neighbor zones, and peers).
- Features like About URI Dialing or About ENUM Dialing.

Default DNS servers

You can specify up to five default DNS servers. The Expressway only queries one server at a time. If that server is unavailable the Expressway tries another server from the list.

The order that the servers are specified is not significant. The Expressway favors servers that were last known to be available.

Per-domain DNS servers

As well as the five default DNS servers, you can specify up to five 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 two **Domain names**. Any DNS queries under those domains are forwarded to the specified DNS server instead of the default DNS servers.

To specify redundant per-domain servers, add an additional per-domain DNS server address and associate it with the same **Domain names**. DNS requests for those domains are sent in parallel to both DNS servers.

You can 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.

Transport protocols

The Expressway uses UDP and TCP to do DNS resolution, and DNS servers usually send both UDP and TCP responses. If the UDP response exceeds the UDP message size limit of 512 bytes, then the Expressway cannot process the UDP response. This is not usually a problem, because the Expressway can process the TCP response instead.

However, if you block TCP inbound on port 53, and if the UDP response is greater than 512 bytes, then the Expressway cannot process the response from the DNS. In this case you won't see the results using the DNS lookup tool, and any operations that need the requested addresses will fail.

Caching DNS Records

DNS lookups may be cached to improve performance. The cache is flushed automatically whenever the DNS configuration is changed, and you can optionally force a flush 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

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

Note 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:

Step 1 Enter the base destination address of the new static route from this Expressway.

For example, enter **`203.0.113.0 or 2001:db8::`**

Step 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.

Step 3 Enter the IP address of the gateway for your new route.

Step 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.

Step 5 Click **Create route**.

The new static route is listed in the table. You can delete routes from this table if necessary.

Note
- 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 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.

  For certain scenarios, even if there is a firewall rule to drop or reject certain inbound traffic, the Expressway still proxies the traffic. This is because firewall rules apply only to new inbound traffic. If the device on the internal network initiates the outbound connection, the device on the external network uses the same ports to response. It takes high priority than the firewall rules since the IP table contains the existing media path information.
- 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 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:

Step 1 Go to **System** > **Protection** > **Firewall rules** > **Configuration**.

Step 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**.

Step 3 When you finish configuring the new set of firewall rules, click **Activate firewall rules**.

Step 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.

Step 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.

Step 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.
Service	Choose the service to which the rule applies, or choose *Custom* to specify your own transport type and port ranges.	**Note** 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 *Custom* service.
Start and end port	The port range to which the rule applies.	Only applies if specifying a UDP or TCP *Custom* service.

Field	Description	Usage tips
Action	The action to take against any IP traffic that matches the rule. *Allow*: Accept the traffic. *Drop:* Drop the traffic without any response to the sender. *Reject:* 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).

You should use automated protection in combination with Configuring 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.

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, automated intrusion protection is enabled by default for various categories, including the following:

- HTTP proxy authentication failure
- HTTP proxy protocol violation
- SSH authorization failure
- SSH protocol violation
- XMPP protocol violation

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

Step 1 Go to **System** > **Administration**.

Step 2 Set **Automated protection service** to *On*.

Step 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

- 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 or Disabling Categories

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

Configuring a Category's Blocking Rules

Step 1 Go to **System** > **Protection** > **Automated detection** > **Configuration**.
Step 2 Click on the name of the category you want to configure. You are taken to the configuration page for that category.
Step 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.

Step 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.

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

Note 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 Configuring 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:

Step 1 Go to **System** > **Protection** > **Automated detection** > **Configuration**.

Step 2 Click on the name of the category you want to investigate.

Step 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.
- From X14.0 release:
  - SIP registration failure is enabled by default for new installations and factory reset cases. In case of upgrade scenario, the previous value is retained.
  - SIP authentication failure is enabled by default for new installations and factory reset cases. In case of upgrade scenario, the pervious value is retained.
  - Disable the SIP authentication failure jail rule on Expressway-C if it is impacting the service.

Configuring Rate Limits

The **Rate limits overview** page (**System** > **Protection** > **Rate limits** > **Configuration**) limits categories of traffic to rates under which Expressway can perform without any issues like crash, high CPU usage, high memory usage etc.

From X14.2 release, there is a default rate limit set for new connections on SIP and EDGE traffic categories. **Management** category is also included in a monitoring capacity allowing visibility and logging of connection events above the configured level.

- By default, 100 connections per second are allowed with a category specific burst limit. Affected ports are listed on the individual category edit pages.
  - The default restricted ports for SIP are 5060, 5061, and 5062. These ports can be changed in the sip configuration.
  - The default restricted ports for EDGE are 8443 and 9443 and are fixed.
- You can enable/disable or change number of connections per second and burst limit.
  - Connections per second range value is 1 to 250 and default value is 100.
  - Burst limit range value is 15 to 30 and default value is 20.

- Mode is one of:
  - **Enforce** - Log and Drop packets above threshold.
  - **Monitor** - Log and Drop packets above threshold.
  - **Disable** - Disable functionality for this category.

- The bar graph shows number of connections established over the time and number of connections dropped, or flood values for monitor mode.
- Logging links filtered on category are provided in the **Related tasks** section.

Important

- In case of TCP protocol only “NEW” state is considered as new connection. All the related and established connections are treated as same connection, so that the packets are not dropped from the existing connection.
- In case of UDP protocol all the related and established connections as “NEW” connections.

Configuring rate limits rules

To configure rate limits rules:

1. Go to **System** > **Protection** > **Rate limits** > **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:
   a. **Status** – whether rate limit mode is enabled or disabled.
   b. **Connections (per second)** – Change the number of connections per second.
   c. **Burst limit** – Maximum initial number of connections/packets to match, this number gets recharged by one every time the limit specified above is not reached, up to this number.
4. Click **Save**.

Network Services

Configuring System Name and Access Settings

The **System administration** page (**System** > **Administration**) is used to configure the following settings:

- Name of the Cisco Expressway system.
- Methods by which the system may be accessed by administrators. Although you can administer the Expressway through a PC connected directly to the unit with a serial cable, you may want to access the

system remotely over IP. You can do this using the web interface via HTTPS, or through a command line interface via SSH.

- Whether to use FindMe or other provisioning services from the Cisco TelePresence Management Suite Provisioning Extension.
- Optionally direct management traffic for administration services - web user interface, REST API and CLI - to use Expressway's Dedicated Management Interface (DMI) on LAN3.

Table 13: Settings for the System Administration page

Field	Description	Usage Tips
System name	Used to identify the Expressway. 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).	We recommend using a name which allows you to easily and uniquely identify the system.
Ephemeral port range	The **start** and **end** values define the port range to use for ephemeral outbound connections that are not otherwise constrained by Expressway call processing.	
Services		
Serial port / console	Whether the system can be accessed locally via the VMware console. Default is *On*.	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 *On*.	
Web interface (over HTTPS)	Whether the Expressway can be accessed via the web interface. Default is *On*.	
Provisioning services	Whether the **System** > **TMS Provisioning Extension services** page is accessible in the Expressway web user interface. From there you can connect to the Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) and its provisioning services for users, devices, FindMe and phone books. Default is *Off*.	FindMe is deprecated in Expressway from X12.5 and support will be withdrawn in a subsequent release.

Field	Description	Usage Tips
Use Dedicated Management Interface only	Optionally requires management traffic for administration services - web user interface, REST API and CLI - to use Expressway's Dedicated Management Interface (DMI) on LAN3. Default is *No*.	The same function is available for SNMP management traffic, from the **System** > **SNMP** page.
Session limits		
Session time out	The number of minutes that an administration session (serial port, HTTPS or SSH) or a FindMe session 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 Configuring Automated Intrusion Protection is active. Default is *On*.	After enabling the service you need to configure the specific About Protection Categories.
Automatic discovery protection	Controls how management systems such as Cisco TMS can discover this Expressway. *Off*: Automatic discovery is allowed. *On*: Cisco TMS must be manually configured to discover this Expressway and must provide administrator account credentials. Default is *Off*.	Restart the system for any changes to take effect.
Web server configuration		

Field	Description	Usage Tips
Redirect HTTP requests to HTTPS	Determines whether HTTP requests are redirected to the HTTPS port. Default is *Off*.	HTTPS must also be enabled for access via HTTP to function. When you enter the address without prepending the protocol, your browser assumes HTTP (on port 80). If this setting is *On*, Expressway redirects the browser to the **Web administrator port**.
HTTP Strict Transport Security (HSTS)	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. *On*: The Strict-Transport-Security header is sent with all responses from the web server, with a 1 year expiry time. *Off*: The Strict-Transport-Security header is not sent, and browsers work as normal. Default is *On*.	See below for more information about HSTS.
Web administrator port	Sets the https listening port for administrators to access the Expressway web interface. We strongly recommend using a non-default port for web administration on the Expressway-E if you enable any features that need TCP 443, for example, Meeting Server Web Proxy. Restart the Expressway to make this change effective.	If you use a non-default port, and you prepend the `https://` protocol to the address, you must append the port. For example, you would put the address *https://vcse.example.com:7443* into your browser; if you try *https://vcse.example.com*, the browser assumes port 443 and the Expressway denies access. Web access to the Expressway could be lost if a network element blocks traffic to the web admin port - you can use SSH or the console to change the port if necessary.

Field	Description	Usage Tips
Client certificate-based security	Controls the level of security required to allow client systems (typically web browsers) to communicate with the Expressway over HTTPS. *Not required*: The client system does not have to present any form of certificate. *Certificate validation*: The client system must present a valid certificate that has been signed by a trusted certificate authority (CA). **Note** Restart is required if you are changing from *Not required* to *Certificate validation*. *Certificate-based authentication*: The client system must present a valid certificate that has been signed by a trusted CA and contains the client's authentication credentials. Default: *Not required*	

Field	Description	Usage Tips
		Important • *Enabling Certificate validation* 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. • 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. • You can upload CA certificates on the Managing the Trusted CA Certificate List page, and test client certificates on the Testing Client Certificates page. • *Enabling Certificate-based authentication* 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 Configuring Certificate-Based Authentication page.

Field	Description	Usage Tips
		• This setting does not affect client verification of the Expressway's server certificate.
Certificate revocation list (CRL) checking	Specifies whether HTTPS client certificates are checked against certificate revocation lists (CRLs). *None*: No CRL checking is performed. *Peer*: Only the CRL associated with the CA that issued the client's certificate is checked. *All*: All CRLs in the trusted certificate chain of the CA that issued the client's certificate are checked. Default: *All*	Only applies if **Client certificate-based security** is enabled.
CRL inaccessibility fallback behavior	Controls the revocation checking behavior if the revocation status cannot be established, for example if the revocation source cannot be contacted. • *Treat as revoked*: Treat the certificate as revoked (and thus do not allow the TLS connection). • *Treat as not revoked*: Treat the certificate as not revoked. • Default: *Treat as not revoked*	Only applies if **Client certificate-based security** is enabled.
Deployment Configuration		

Field	Description	Usage Tips
Configuration	Determines the size of the system. The possible options are: *Large*: 8 CPU cores , 6 GB memory, and 1 Gbps or 10 Gbps NIC. *Medium*: 2 CPU cores: 4 GB memory, and 1 Gbps NIC.	If you upgrade a *Medium system* with a 1 Gbps NIC, Expressway **automatically converts the appliance to a Large system**. As a result, Expressway-E listens for multiplexed RTP/RTCP traffic on default demultiplexing ports for Large systems (36000 to 36011). In this case, Expressway drops the calls because these ports are not open on the firewall. If this problem occurs, do either of the following: • To change the system default size to Medium and use the ports that you have configured for multiplexed RTP/RTCP traffic, select **Medium**. • If you prefer to use it as Large system, open the default demultiplexing ports for Large systems on the firewall. This option is available only for CE1200 and later appliances that are deployed as Expressway-Es, and with the following minimum specification: • Supported Expressway software version (detailed in the *Cisco Expressway CExxxx Installation Guide* for your appliance) • CPU: 8 cores • Memory: 6 GB • NIC: 1 Gbps

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

HTTP Strict Transport Security (HSTS) is a mechanism for a web server to force a web browser to communicate with it using secure connections only. Depending on the version, it may not be supported by all browsers. When HSTS is enabled, a browser that supports HSTS will:

- Automatically turn any insecure links to the website into secure links before accessing the server(for example, `http://example.com/page/` is modified to `https://example.com/page/`).
- 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 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 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:

- System uptime
- System name
- Location
- Contact
- Interfaces
- Disk space, memory, and other machine-specific statistics

SNMP is disabled by default. So to allow the Expressway to be monitored by an SNMP NMS (including Cisco TMS) you need to select an alternative **SNMP mode**. The configurable options are:

Field	Description	Usage Tips
SNMP mode	Controls the level of SNMP support. *Disabled*: no SNMP support. *v3 secure SNMP*: supports authentication and encryption. *v3 plus TMS support*: secure SNMPv3 plus non-secure access to OID 1.3.6.1.2.1.1.2.0 only. *v2c*: 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 *v3 plus TMS support*.
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 *public*.	Only applies when using *v2c* or *v3 plus TMS support*.

Field	Description	Usage Tips
System contact	The name of the person who can be contacted regarding issues with the Expressway. The default is *Administrator*.	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 *v3 secure SNMP* or *v3 plus TMS support*.
Use Dedicated Management Interface only	Optionally requires management traffic for SNMP to use Expressway's Dedicated Management Interface (DMI) on LAN3. Default is *No*.	The same function is available for management traffic related to administration services - web user interface, REST API, and CLI - from the **System** > **Administration settings** page.
v3 Authentication settings (only applicable to SNMPv3)		
Authentication mode	Enables or disables SNMPv3 authentication.	
Type	The algorithm used to hash authentication credentials. From X12.5.7, SHA (Secure Hash Algorithm) is the only supported option. MD5 (Message-Digest algorithm 5) passwords are not supported. From X14.2, SHA (Secure Hash Algorithm) is the default and only supported option. MD5 (Message-Digest algorithm 5) passwords are completely removed.	
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.	

Field	Description	Usage Tips
Type	The security model used to encrypt messages. *AES*: Advanced Encryption Standard 128-bit encryption. The default and recommended setting is *AES*.	
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
Disabled	No authentication is used.

Authentication method	Description
Symmetric key	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.
Private key	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 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 *Candidate*; of those, the server that the Expressway considers to be providing the most accurate time and is therefore using shows a status of *sys.peer*.
Flash	A code giving information about the server's status. `00 ok` means there are no issues. See the Flash Status Word Reference Table for a complete list of codes.
Authentication	Indicates the status of the current authentication method. One of *ok*, *bad* or *none*. *none* is specified when the **Authentication** method is *Disabled*.

Field	Description
Event	Shows the last event as determined by NTP (for example *reachable* or *sys.peer*)
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.

Recommendation(s)

An accurate and reliable Network Time Protocol (NTP) reference is important for Transport Layer Security (TLS) connections.

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

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

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

Configuring the Login Page

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 Service Status to provide FindMe account data, then users log into their FindMe accounts through Cisco TMS, not through Expressway.

Note 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 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.

Note Cisco TMS identifies the Expressway as a "TANDBERG VCS".

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.

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`

Field	Description	Usage Tips
Protocol	Determines whether communications with the external manager are over *HTTP* or *HTTPS*. The default is *HTTPS*.	
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 (**Maintenance** > **Security** > **Trusted CA certificate**).

Configuring the Dedicated Management Interface (DMI)

From X12.7, Expressway supports the Dedicated Management Interface (DMI). This is a new network interface that uses the third LAN port (LAN3) to access Expressway for management-related activities. Instead of sharing a routing interface with other traffic, management traffic is sent and received through LAN3 and no other traffic uses that port.

The DMI is disabled by default.

Note If you are using a physical CE1200 appliance, connect **port 3a** (See "Figure 2: Rear view of the Cisco Expressway") provided on your physical appliance and configure the DMI address on it as explained in the chapter "Rear Panel Layout". For specific instructions, see "*Cisco Expressway CE1200 Appliance Installation Guide*".

Introduction to the DMI

Enabling the DMI has two aspects:

1. Enabling the DMI function - this switches on the LAN3 port for management traffic. However, it is not exclusive and LAN1 (and LAN2 if configured) can also be used - Expressway continues to listen for management traffic on LAN1/LAN2 as well, not just on the LAN3 port.
2. If you want LAN3 to be the only interface for management traffic, you need to configure the individual management services in Expressway for DMI only.

Note If you have management servers outside the LAN3 subnet, currently you also need to configure static IP routes in order for their traffic to be directed to LAN3.

Expressway management traffic can be classified as server-based or client-based.

Management traffic where Expressway is the server:

- HTTP(S) - for web UI administration and REST API
- ssh - for CLI (not for MRA tunnels)
- SNMP

Management traffic where Expressway is the client, for example:

- HTTP(S) for feedback events to external managers like Cisco TMS
- NTP
- directory (LDAP, Active Directory)
- remote syslog
- system metrics (collectd)

How to Configure the DMI

Enable DMI

Before you begin

The new DNS name for the DMI interface must be entered as a Subject Alternative Name (SAN) on the Expressway server certificate. If an IP address is used to access the interface (or a DNS that is not a SAN entry in the certificate) a certificate validation warning will be issued and access may be blocked.

Caution It is essential to properly secure the DMI, as it provides access into the Expressway configuration.

Step 1 Go to **System** > **Network Interfaces** > **IP** and set **Use Dedicated Management Interface** to *Yes*.

Step 2 In the **LAN3 - DMI** section:

a. Specify the IPv4 and/or IPv6 address of the LAN3 port.

b. For IPv4 also specify the subnet mask.

c. For IPv6 use a static, global address. It cannot be link-local or stateless SLAAC.

d. Optionally change the maximum Ethernet packet size that can be sent over the DMI by setting the **Maximum transmission unit (MTU)** for the port. The default is 1500 bytes.

Step 3 Restart the system. These changes require a restart to take effect.

The DMI is now activated on LAN3 as an interface for management traffic. If you want the DMI to be the *sole* interface for management, go on to the next tasks.

Note For Expressway VMs, the OVF template includes a customization option to define the DMI IP address.

(Optional) Make DMI Sole Interface

(Optional) Make DMI sole interface - server management traffic

Use this task to make management traffic use the DMI, where Expressway is the server.

Caution Before you do this, make sure that the required services are accessible on LAN3, else they won't have access after the change to DMI only. This is especially important for administration services, as the only way to recover them would be to turn off DMI using the console (serial/VMWare).

1. You can do this for administration services (web user interface, REST API, and CLI) and/or for SNMP. Do either or both the following steps, depending on which services you want to configure for DMI only:
   - Go to **System** > **SNMP** and in the **Configuration** section set **Use Dedicated Management Interface only** to *Yes*.
   - Go to **System** > **Administration settings** and in the **Services** section set **Use Dedicated Management Interface only (for administration)** to *Yes*.
2. You need to restart the system for the changes to take effect for the web user interface and the API, which remain accessible from LAN1 / LAN2 until you restart. Changes take immediate effect for the command line interface (SSH) and SNMP service, regardless of restart.

The specified management services can now be accessed only from the DMI / LAN3 port.

Note Expressway will not let you disable the DMI while a management service is configured to use it as the only interface.

(Optional) Make DMI sole interface - client management traffic outside subnet

For management traffic where Expressway acts as the client, depending on your Expressway version the traffic will only be directed to the DMI if the target server is in the same subnet as the DMI / LAN3 port. If it's not possible to deploy the server in the same subnet as LAN3, you can optionally force Expressway management traffic to use the DMI, by configuring static IP routes for LAN3 per service.

Example

This example assumes an Expressway with these subnets:

- LAN3 subnet range: a.b.128.0 - a.b.191.255
- LAN1 subnet range: x.y.156.0 - x.y.159.255

Say you want to configure NTP with Expressway. The NTP server is in the LAN1 subnet. You want outgoing NTP traffic from Expressway and incoming responses from NTP to use the DMI / LAN3. This can be achieved by creating a static route for LAN3 (**System** > **Network interfaces** > **Static routes** select Add) with the following settings:

- IP address: *x.y.151.0*
- Prefix length: *24*

- Gateway: *172.22.128.1* (gateway of LAN3 subnet)
- Interface: *LAN3*

For more details, see Static Routes.

Configuring TMS Provisioning Extension Services

Cisco TMSPE services are hosted on Cisco TMS. They provide the user, device, and phone book data used by the Expressway's Expressway Provisioning Server to service provisioning requests from endpoint devices. They also provide the Expressway with FindMe account configuration data for FindMe services.

From X8.11, the Cisco TMS-hosted provisioning services are enabled through the **System** > **Administration settings** page in the web user interface or the device provisioning CLI command (*xconfiguration Administration DeviceProvisoning*). You do not need special option keys or licenses to enable these services. The following device provisioning services are available:

- Users
- FindMe
- Phone Books
- Devices

For new installations all services are *off* by default. For existing systems your current service settings are preserved and remain unchanged after upgrading.

Note Cisco Expressway X14.0.1 and later releases include more secure parsing of HTTP headers. Hence, Cisco TMS Provisioning Extension (TMSPE) Service will not work with Expressway, if you enable more than one authentication method. Enable only the “Basic Authentication” method for the *tmsagent* virtual directory in Internet Information Services (IIS) Manager.

Before You Start

If you have not already done so, go to **System** > **Administration** and set **Provisioning services** to *On*. Then you can use the **System** > **TMS Provisioning Extension services** page to configure how Expressway connects to Cisco TMSPE services, and which services you want. (To configure the services themselves, we recommend using the TMS. Changes to Cisco TMSPE service configuration settings made through Expressway **are not applied in TMS**.)

FindMe is a special case. If you enable provisioning services you may see the following configuration warning alarms. If you plan to use FindMe only, and no other provisioning services, you can ignore these alarms:

- *For phone book requests to work correctly, authentication policy must be enabled on the Default Subzone and any other relevant subzone; authentication must also be enabled on the Default Zone if the endpoints are not registered.*
- *For provisioning to work correctly, authentication policy must be enabled on the Default Zone and any other relevant zone that receives provisioning requests.*

Configuration Settings

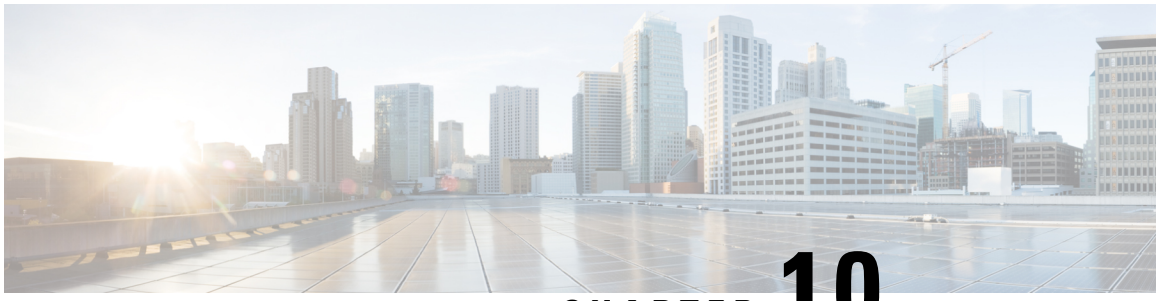
The configurable options for provisioning services are described in the table:

Table 14: Configurable Options for Provisioning Services

Field	Description	Usage Tips
Default connection configuration This section specifies default connection settings for accessing Cisco TMSPE services. Each service can choose to use these settings, or specify its own connection settings (for example, if a different Cisco TMSPE server is in use per 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.	
Encryption	The encryption to connect the Cisco TMSPE service. For more information see Configuring Minimum TLS Version and Cipher Suites *Off*: No encryption. *TLS*: Provides TLS encryption. Default is *TLS*.	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 any) revocation list. Default is *Yes*.	If verification is enabled: • 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. Do this from the Managing the Trusted CA Certificate List page (**Maintenance** > **Security** > **Trusted CA certificate**).
Check certificate hostname	Controls whether the hostname contained within the certificate presented by the Cisco TMSPE service is verified by the Expressway. Default is *Yes*.	Applies if **Verify certificate** is *Yes*. If enabled, the certificate hostname (the Common Name) must match the specified **Server address**. If the server address is an IP address, the required hostname is obtained through a DNS lookup.

Field	Description	Usage Tips
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 *No*.	If *Yes*, the status of an enabled connection is shown next to the field: *Checking*, *Active* or *Failed*. (Click TMS Provisioning Extension Service Status to view full status information.)
Polling interval	The frequency with which the Expressway checks the Cisco TMSPE service for updates. Defaults are: **FindMe**: *2 minutes* **Users**: *2 minutes* **Phone books**: *1 day* 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 *Yes*.	If *No*, an additional set of connection configuration parameters appears. There you can specify alternative connection details, to override the default connection settings for the service.

You can do an immediate resynchronization of data between Expressway and Cisco TMS at any time by clicking **Perform full synchronization** on the **TMS Provisioning Extension services** page. This will result in a few seconds lack of service on the Expressway while data is deleted and refreshed. If you only need to apply recent updates in Cisco TMS to the Expressway, click **Check for updates** instead.



CHAPTER 10

Firewall Traversal

- About Firewall Traversal, on page 171
- Firewall Traversal Configuration Overview, on page 175
- Configuring a Traversal Client and Server, on page 176
- Configuring Ports for Firewall Traversal, on page 177
- Firewall Traversal and Authentication, on page 180
- Configuring Expressway-E and Traversal Endpoint Communications, on page 181
- About ICE and TURN Services, on page 182
- Configuring TURN Services, on page 185

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:

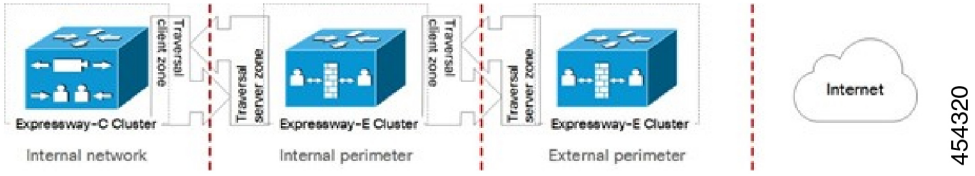
- An Expressway-E located outside the firewall on the public network or in the DMZ, which acts as the firewall traversal server.
- An Expressway-C or other traversal-enabled endpoint located in a private network, which acts as the firewall traversal client.

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 8: 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.

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

Note 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 (this does not include traversal-enabled endpoints which register directly with the Expressway-E; the settings for these connections are configured in a different way). 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 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.

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

Endpoint Traversal Technology Requirements

The “far end” (at home or at a hotel, for example) endpoint requirements to support firewall traversal are summarized below:

- For H.323, the endpoint needs to support Assent or H460.18 and H460.19.
- For SIP, the endpoint just needs to support standard SIP.
  - Registration messages will keep the “far end” firewall ports open for Expressway to send messages to that endpoint. The Expressway waits for media from the endpoint behind the firewall, before returning media to it on that same port – the endpoint does have to support media transmission and reception on the same port.
  - The Expressway also supports SIP outbound, which is an alternative method of keeping firewalls open without the overhead of using the full registration message.
- SIP and H.323 endpoints can register to the Expressway-E or they can just send calls to the Expressway-E as the local “DMZ” firewall has relevant ports open to allow communication to the Expressway-E over SIP and H.323 ports.

Endpoints can also use About ICE to find the optimal (in their view of what optimal is) path for media communications between themselves. Media can be sent directly from endpoint to endpoint, from endpoint via the outside IP address of the destination firewall to the destination endpoint, or from the endpoint via a TURN server to destination endpoint.

- The Expressway supports ICE for calls where the Expressway does not have to traverse media (for example if there is no IPv4/IPv6 conversion or SIP / H.323 conversion required); typically this means 2 endpoints which are able to support ICE, directly communicating to an Expressway-E cluster.
- The Expressway-E has its own built-in Configuring TURN Services to support ICE-enabled endpoints.

H.323 Firewall Traversal Protocols

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

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

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

SIP Firewall Traversal Protocols

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

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

Media Demultiplexing

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

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

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

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

The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at **Configuration** > **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 SIP and H.323 endpoints registered to it, and any systems that are neighbored with it. To act as a firewall traversal client, the Expressway must be configured with information about the systems that will act as its firewall traversal server.

You do this by adding a traversal client zone on the Expressway client (**Configuration** > **Zones** > **Zones**) and configuring it with the details of the traversal server. See Configuring Traversal Client Zones for more information. You can create more than one traversal client zone if you want to connect to multiple traversal servers.

Expressway-C or Expressway-E?

- Typically you use an Expressway-C as a firewall traversal client. However, an Expressway-E can also do this role.
- The firewall traversal server used by the Expressway client must be an Expressway-E.

Expressway as a Firewall Traversal Server

The Expressway-E has all the functionality of an Expressway-C (including being able to act as a firewall traversal client). However, its main feature is that it can act as a firewall traversal server for other Cisco systems and any traversal-enabled endpoints that are registered directly to it. 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 for more information.

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

Configuring Other Traversal Server Features

- For the Expressway-E to act as a firewall traversal server for traversal-enabled endpoints (such as Cisco MXP endpoints and any other endpoints that support the ITU H.460.18 and H.460.19 standards), no additional configuration is required. See Configuring Expressway-E and Traversal Endpoint Communications for more information.
- To enable TURN relay services and find out more about ICE, see About ICE and TURN Services.
- To reconfigure the default ports used by the Expressway-E, see Configuring Ports for Firewall Traversal.

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.

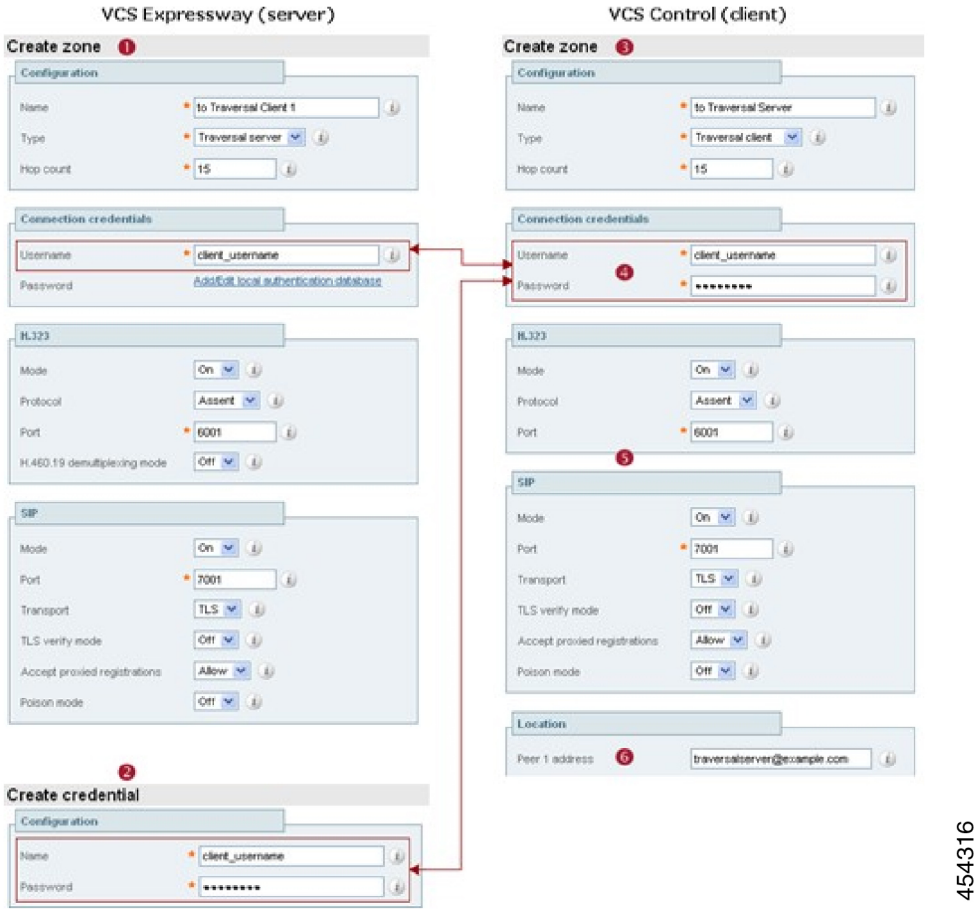
With the LAN 2 interface enabled, you can configure the Expressway with two separate IP addresses, one for each network in the DMZ. Your Expressway then acts as a proxy server between the two networks, allowing calls to pass between the internal and outer firewalls that make up your DMZ.

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.



Configuring Ports for Firewall Traversal

Note Specific port information is collected in a separate document. See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series Configuration Guides page.

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

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

The Expressway solution works as follows:

1. Each traversal client connects via the firewall to a unique port on the Expressway-E.
2. The server identifies each client by the port on which it receives the connection, and the authentication credentials provided by the client.
3. After the connection 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**
- **H.323 H.460.18 call signaling port**

RTP and RTCP Media Demultiplexing Ports

The port configuration options depend upon the Hardware Appliance and Virtual Machine Options:

- **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 traversal 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

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

The call signaling ports are configured via **Configuration** > **Traversal** > **Ports**. The traversal media port range is configured via **Configuration** > **Local Zone** > **Traversal Subzone**.

If your Expressway-E does not have any endpoints registering directly with it, and it is not part of a cluster, then UDP/1719 is not required. You therefore do not need to allow outbound connections to this port through the firewall between the Expressway-C and Expressway-E.

Configuring TURN Ports

The Expressway-E can be enabled to provide About ICE and TURN Services (Traversal Using Relays around NAT) which can be used by ICE-enabled SIP endpoints.

The ports used by these services are configurable via **Configuration** > **Traversal** > **TURN**.

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

Configuring Ports for Connections Out to the Public Internet

In situations where the Expressway-E is attempting to connect to an endpoint on the public internet, you will not know the exact ports on the endpoint to which the connection will be made. This is because the ports to be used are determined by the endpoint and advised to the Expressway-E only after the server has located the

endpoint on the public internet. This may cause problems if your Expressway-E is located within a DMZ (where there is a firewall between the Expressway-E and the public internet) as you will not be able to specify in advance any rules that will allow you to connect out to the endpoint's ports.

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

See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series Configuration Guides page.

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 (or Expressway-E) 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.
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 All Expressway traversal clients must authenticate with the Expressway-E, even if the Expressway-E is not using device authentication for endpoint clients.

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 Configuring the NTP Servers.

Configuring Expressway-E and Traversal Endpoint Communications

Traversal-enabled H.323 endpoints can register directly with the Expressway-E and use it for firewall traversal.

The **Locally registered endpoints** page (**Configuration** > **Traversal** > **Locally registered endpoints**) allows you to configure the way in which the Expressway-E and traversal-enabled endpoints communicate.

The options available are:

Field	Description
H.323 Assent mode	Determines whether or not H.323 calls using Assent mode for firewall traversal are allowed.
H.460.18 mode	Determines whether or not H.323 calls using H.460.18/19 mode for firewall traversal are allowed.
H.460.19 demux mode	Determines whether the Expressway-E operates in demultiplexing mode for calls from locally registered endpoints. *On*: Uses the media demultiplexing ports for all calls. *Off*: Each call uses a separate pair of ports for media.
H.323 preference	Determines which protocol the Expressway-E uses if an endpoint supports both Assent and H.460.18.
UDP probe retry interval	The frequency (in seconds) with which locally registered endpoints send a UDP probe to the Expressway-E.
UDP probe retry count	The number of times locally registered endpoints attempt to send a UDP probe to the Expressway-E.
UDP probe keep alive interval	The interval (in seconds) with which locally registered endpoints send a UDP probe to the Expressway-E after a call is established, in order to keep the firewall's NAT bindings open.
TCP probe retry interval	The frequency (in seconds) with which locally registered endpoints send a TCP probe to the Expressway-E.
TCP probe retry count	The number of times locally registered endpoints attempt to send a TCP probe to the Expressway-E.
TCP probe keep alive interval	The interval (in seconds) with which locally registered endpoints send a TCP probe to the Expressway-E after a call is established, in order to keep the firewall's NAT bindings open.

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 (Traversal Using Relays around NAT) and STUN (Session Traversal Utilities for NAT).

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.

For more information about ICE, see RFC 5245.

ICE Passthrough for MRA Deployments

From X12.5, we support Interactive Connectivity Establishment (ICE) passthrough to allow MRA-registered endpoints to pass media directly between endpoints by bypassing the WAN and the Cisco Expressway Series.

Configuration details and required versions for ICE passthrough are in the *Mobile and Remote Access Through Cisco Expressway guide* on the Expressway Configuration Guides page.

About TURN

TURN services are relay extensions to the STUN network protocol that enable a SIP client to communicate via UDP or TCP from behind a NAT device.

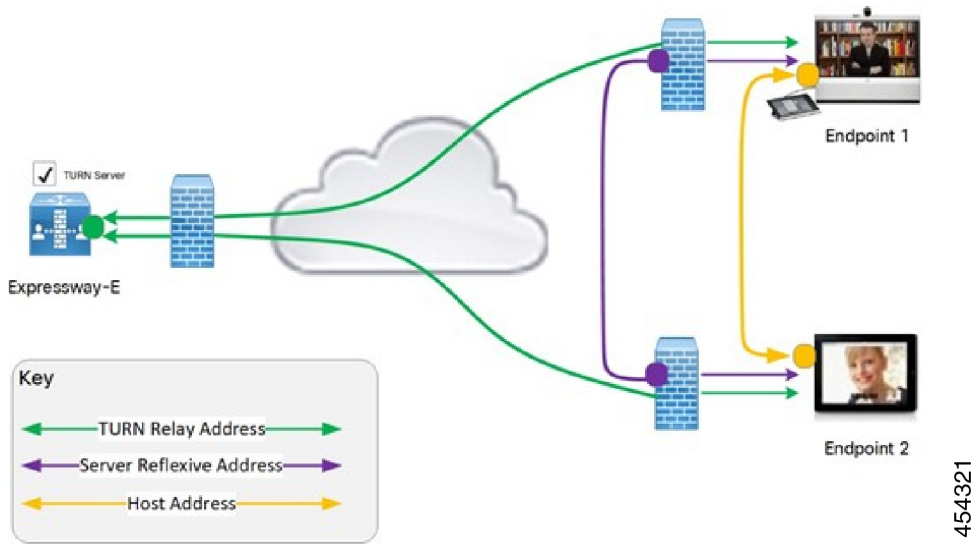
For more information about TURN see RFC 5766, and for detailed information about the base STUN protocol, see RFC 5389.

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.

Figure 9: ICE Media connection paths



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 is selected, the TURN relay allocations are released if the chosen connection paths do not involve routing via the TURN server.

Note

- The signaling always goes via the Expressway, regardless of the final media communication path chosen by the endpoints.

  The TURN server can relay media between any two ICE clients, even if one or both are inside the enterprise internal firewall.
- We recommend that the TURN password to be different from the Administrator password.

Capabilities and Limitations

- From X12.6.1, due to security enhancements, the Expressway-E TURN server no longer functions as a generic STUN server and will not accept unauthenticated STUN binding requests. This leads to the following scenarios:
  - **Scenario A**: If you use the B2BUA as a TURN client for Microsoft interoperability (as described in the *Cisco Expressway with Microsoft Infrastructure Deployment Guide*), the B2BUA will not send any STUN binding requests to the TURN server to check if it is alive or not. This means that from Expressway X12.6.1, the B2BUA may try to use a TURN server that is not reachable and hence that **calls may fail**.

  - **Scenario B**: Depending on the CMS version deployed, the CMS WebRTC solution may use STUN bind requests towards TURN server on Expressway-E, which will cause failures. So if you use Meeting Server WebRTC, check that your CMS version is compatible before you install Expressway version X12.6.1 or later software. Bug ID CSCvv01243 refers. (For more information about Expressway-E TURN server configuration, see the *Cisco Expressway Web Proxy for Cisco Meeting Server Deployment Guide*.)

- Hardware Appliance and Virtual Machine Options or Hardware Appliance and Virtual Machine Options systems support up to 1800 relay allocations. This is typically enough to support their maximum concurrent call limits, but does depend on the network topology and the number of media stream components used for the call. For example, some calls use Duo Video, or other calls use only audio.
- A Hardware Appliance and Virtual Machine Options system supports up to 6000 relays. The full relay capacity is available on one external port when port multiplexing is enabled or spread across six external ports when port range is configured. When it is spread across the ports, each port is limited to handling 1000 relays.

  This limit is not strictly enforced. Therefore we recommend creating DNS SRV record with six A/AAAA entries, with the same address, for each port address in the range. After creating the record, configure the clients with the SRV record of the Expressway-E TURN server. If TURN multiplexing is enabled, we recommend creating an SRV record only for the external port that listens to TURN requests.
- On a Hardware Appliance and Virtual Machine Options system, you can configure the TURN server to listen for TURN requests on a range of ports, from 3478 to 3483 by default. From X8.11, if TURN multiplexing is enabled, the Expressway-E accepts all TURN requests on the first port in the range (typically UDP 3478). The Expressway internally demultiplexes those requests onto the port range. The TURN clients must send requests on the configured single port, but the full capacity of the large Expressway-E TURN server is available.
- From X8.11, Expressway-E can listen to both TURN and Cisco Meeting Server requests on the TCP port 443. When Expressway-E receives a connection request through port 443, it forwards the request either to the TURN server or to the Meeting Server Web Proxy depending on the request type. As a result, it allows external users to use TURN services and join Meeting Server spaces from an environment with restricted firewall policies.

  If the web administrator port is configured to listen on port 443 (**System** > **Administration Settings**), for Expressway versions before X12.7 it must be changed from 443 to any other valid port. From X12.7, you do not need to do this if the Expressway is configured to use its Dedicated Management Interface as the only administration interface. That is, on the **System** > **Administration settings** page, **Use Dedicated Management Interface only (for administration)** is set to *Yes*.
- On a Hardware Appliance and Virtual Machine Options system, if TCP 443 TURN service is enabled, and the TURN multiplexing feature is also enabled, then 6000 TCP TURN relays are supported.
- 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.
- Expressway-E's TURN server does not support Microsoft ICE (which is not standards-based). To enable communications between the Expressway and Microsoft clients that are registered through a Microsoft Edge Server you need to use the About Microsoft Interoperability.

- 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.

STUN Packets Sometimes Sent Over the Internal Interface

Expressway always sends STUN packets that it receives through its external LAN interface, using the external LAN IP address as the packet source address. Typically the packets are sent from the external interface, and so the IP addresses usually match up. However, in the following cases, note that Expressway sends the STUN packets out from the *internal* LAN interface:

- If the TURN client is using a relay session to send a message to a device in the same subnet as the internal IP of the Expressway-E, or
- If the TURN client is using a relay session to send a message to a device in a subnet which matches a static route that uses the internal gateway IP of the Expressway-E.

This behavior may create the impression that there is a mismatch in the IP address, but in fact the system is working as designed.

Configuring TURN Services

TURN relay services are only available on the Expressway-E. (From X8.11, the TURN Relay option key is not required to use TURN services.)

The **TURN** page (**Configuration** > **Traversal** > **TURN**) is used to configure the Expressway-E's TURN settings. If you are configuring your Expressway-E for delegated credential checking you can also determine, via the **Authentication realm**, the traversal zone through which credential checking of TURN server requests is delegated.

The configurable options are:

Field	Description	Usage Tips
TURN services	Determines whether the Expressway offers TURN services to traversal clients.	If you need to modify other TURN settings while the **TURN services** is already set to *On*: 1. Change **TURN services** to *Off* and **Save**. 2. Modify the required TURN settings. 3. Change **TURN services** to *On* and **Save**. This is because changes to other TURN settings do not come into effect until the **TURN services** is restarted

Field	Description	Usage Tips
TCP 443 TURN service	Determines if the TURN server must listen to TCP request from TURN clients on TCP port 443. The options are: • *On*: The TURN server listens to the TCP requests from TURN clients on the TCP port 443 and the UDP requests on the configured port. • *Off*: TURN server does not listen to TURN clients on TCP port 443. However this setting does not affect the ports configured to listen to TURN requests.	Before enabling this feature, make sure the following: • **TURN services** is set to *On*. • Before X12.7, if the web administrator port is configured to listen on port 443 (**System** > **Administration Settings**), it must be changed from 443 to any other valid port. From X12.7, you do not need to do this if the Expressway is configured to use its Dedicated Management Interface as the only administration interface. That is, on the **System** > **Administration settings** page, **Use Dedicated Management Interface only (for administration)** is set to *Yes*.

Field	Description	Usage Tips

TURN port multiplexing	On Large systems, enables the full capacity of the Expressway TURN server on a single listening port and internally demultiplexes those requests onto the range of ports.
	Note This option is only available on Large systems.
	The possible options are:
	• *On:*
	  • The Expressway listens on a single configurable external port instead of a range.
	  • If **TCP 443 TURN services** is *On*, the configurable external port only multiplexes UDP TURN requests.
	  Note If **TCP 443 TURN services** is *On*, the external port does not multiplexes the TCP TURN requests due to technical limitation.
	• *Off*: The TURN server listens to the TCP and UDP requests on the range of ports.
		Before enabling this feature, make sure that the **TURN services** is set to *On*.

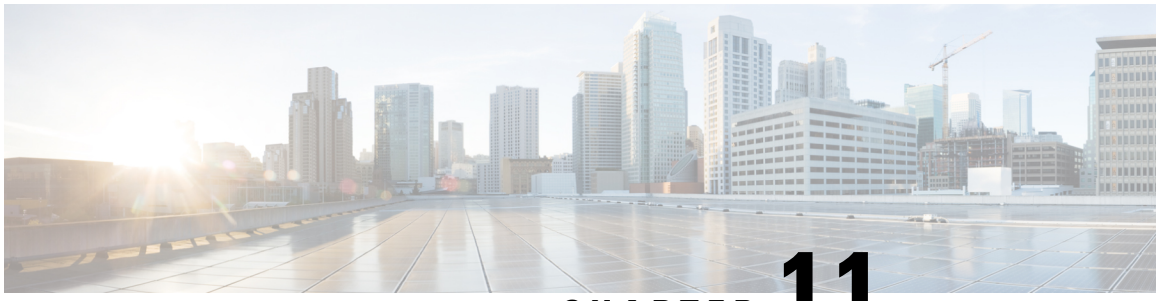
TURN requests port	The listening port for TURN requests. The default port is 3478.	On a Large system, this option is available only if **TURN port multiplexing** is set to *On*. To allow endpoints to discover TURN services, create DNS SRV records for **_turn._udp.** and **_turn._tcp** (either for the single port, or range of ports as appropriate).
TURN requests port range start	If **TURN port multiplexing** is *Off*, this port represents the first port in the configurable range on Large systems. The default port range start is 3478.	This option is available only on Large systems and if **TURN port multiplexing** is set to *Off*.

Field	Description	Usage Tips
TURN requests port range end	If **TURN port multiplexing** is *Off*, this port represents the upper port in the configurable range on Large systems. The default port range end is 3483.	This option is available only on Large systems and if **TURN port multiplexing** is set to *Off*.
Delegated credential checking	Controls whether the credential checking of TURN server requests is delegated, via a traversal zone, to another Expressway. The associated **Authentication realm** determines which traversal zone is used. *Off*: Use the relevant credential checking mechanisms (local database or H.350 directory via LDAP) on the Expressway performing the authentication challenge. *On*: Delegate the credential checking to a traversal client. The default is *Off*.	See delegated credential checking for more information.
Authentication realm	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	The lower port in the range used for the allocation of TURN relays. The default TURN relay media port range is 24000 to 29999.	
Media port range end	The upper port in the range used for the allocation of TURN.	

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.



CHAPTER 11

Unified Communications

- Unified Communication Prerequisites, on page 189
- Mobile and Remote Access Overview, on page 201
- XMPP Federation Through Expressway, on page 203
- Delayed Cisco XCP Router Restart, on page 206
- Jabber Guest Services Overview, on page 207
- Meeting Server Web Proxy on Expressway, on page 208

Unified Communication 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).

- 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.

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:

- Configure the Expressway-C and Expressway-E 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 client and server, you must ensure that each Expressway's certificate is valid both as client and server.
- Be aware that Expressway uses the SAN attribute (Subject Alternative Name) to validate the received certificate, not the CN (Common Name).
- If you require a H.323 or a nonencrypted connection, configure a separate pair of traversal zones.

Note If ICMP is blocked between Expressway-C and Expressway-E then secure test fails with "<Exp-E FQDN> cannot be reached" error. (simulated in TAC lab by creating a firewall rule in Expressway-E to drop the ICMP queries from Expressway-C).

To set up a secure traversal zone

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

Step 1 Go to **Configuration** > **Zones** > **Zones**.

Step 2 Click **New**.

Step 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	*Unified Communications traversal*	*Unified Communications traversal*
Connection credentials section		
Username	"exampleauth" for example	"exampleauth" for example **Note:** When creating users for a local authentication database, do not include a space in this field.
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	Must match the Expressway-E setting.	**7001** (default. See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series Configuration Guides page.)
TLS verify subject name	Not applicable	Enter the name to look for in the traversal client's certificate (must be in the SAN - Subject Alternative Name - attribute). 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		

	Expressway-C	Expressway-E
Authentication policy	*Do not check credentials*	*Do not check credentials*
Location section		
Peer 1 address	Enter the FQDN of the Expressway-E. **Note** 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**

Step 4 Click **Create zone**.

Server Certificate Requirements for Unified Communications

Cisco Unified Communications Manager Certificates

Two Cisco Unified Communications Manager certificates are significant for Mobile and Remote Access:

- *CallManager* certificate
- *tomcat* certificate

These certificates 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. However, if you do use self-signed certificates, the two certificates must have different common names. The Expressway does not allow two self-signed certificates with the same CN. So if the *CallManager* and *tomcat* self-signed certificates have the same CN in the Expressway's trusted CA list, the Expressway can only trust one of them. This means that either secure HTTP or secure SIP, between Expressway-C and Cisco Unified Communications Manager, will fail.

Also, when generating *tomcat* certificate signing requests for any products in 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 Name (SAN) entries. The *Expressway X8.5.3 Release Note* on the Release Notes page has details of the workarounds.

IM and Presence Service Certificates

Two IM and Presence Service certificates are significant if you use XMPP:

- *cup-xmpp* certificate
- *tomcat* certificate

We recommend using CA-signed certificates. However, if you do use self-signed certificates, the two certificates must have different common names. The Expressway does not allow two self-signed certificates with the same CN. If the *cup-xmpp* and *tomcat* (self-signed) certificates have the same CN, Expressway only trusts one of them, and some TLS attempts between Cisco Expressway-E and IM and Presence Service servers will fail. For more details, see CSCve56019.

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 must include the elements listed below in its list of subject alternative names (SAN).

- **Unified CM phone security profile names:** The names of the **Phone Security Profiles** in Unified CM are configured for encrypted Transport Line Signaling (TLS) and are used for devices requiring remote access. Use the Fully Qualified Domain Name (FQDN) format and separate multiple entries with commas.

  It is essential to generate Certificate Signing Request (CSR) for the new node while adding a new Expressway-C node to an existing cluster of Expressway-C. It is mandated to put secure profile names as they are on CUCM, if secure registration of Mobile and Remote Access (MRA) client is needed over MRA. CSR creation on the new node will fail if "Unified CM phone security profile names" are just names or hostnames on CUCM device security profiles. This will force Administrators to change the value of "Unified CM phone security profile names" on CUCM under the **Secure Phone Profile** page.

  From X12.6, it is mandated that the Unified CM phone security profile name must be a Fully Qualified Domain Name (FQDN). It cannot be just any name or hostname or a value.

  For example, `jabbersecureprofile.domain.com`, `DX80SecureProfile.domain.com`

  Note 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.

  The Endpoint supports OAuth Authentication functionality. The Phone Security Profile configuration is detailed as follows:

  1. The Endpoint is linked to Phone Security Profile with Device Security Mode set as *Encrypted* and **with** OAuth Authentication enabled, then the Phone does not require its Security Profile Name to be part of the Subject Alternate Name (SAN) list of Expressway-C certificate.
  2. The Endpoint is linked to Phone Security Profile with Device Security Mode set as *Encrypted* but **without** OAuth Authentication enabled, then the Phone requires its Security Profile Name to be part of the Subject Alternate Name (SAN) list of Expressway-C certificate.

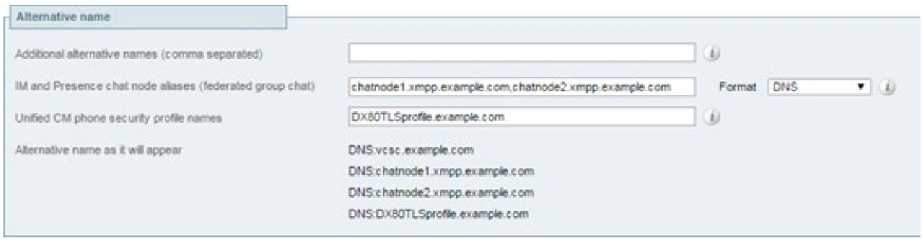
  Having the secure phone profiles as alternative names means that Unified CM can communicate via Transport Line Signaling (TLS) with the Expressway-C when it is forwarding messages from devices that use those profiles.

- **IM and Presence chat node aliases (federated group chat):** The **Chat Node Aliases** (e.g. **`chatroom1.example.com`**) that are configured on the IM and Presence servers. These are required only for Unified Communications XMPP federation deployments that intend to support group chat over TLS with federated contacts.

  The Expressway-C automatically includes the chat node aliases in the CSR, providing it has discovered a set of IM&P servers.

  We recommend that you use DNS format for the chat node aliases when generating the CSR. You must include the same chat node aliases in the Expressway-E server certificate's alternative names.

Figure 10: Entering subject alternative names for security profiles and chat node aliases on the Expressway-C's CSR generator



Expressway-E server certificate requirements

The Expressway-E server certificate must include the elements listed below in its list of subject alternative names (SAN). If the Expressway-E is also known by other FQDNs, **all of the aliases** must be included in the server certificate 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 **_collab-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 **collab-edge.** to the domain that you enter. This format is recommended if you do not want to include your top level domain as a SAN (see example in following screenshot).

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

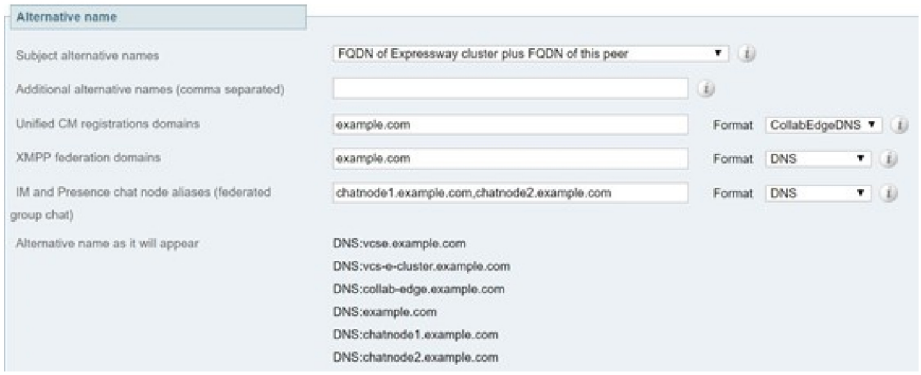
  Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains.

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

Figure 11: Entering subject alternative names for Unified CM registration domains, XMPP federation domains, and chat node aliases, on the Expressway-E's CSR generator



For detailed information, see *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway Configuration Guides page.

Certificates for mTLS if you use MRA onboarding

If you enable activation code onboarding over MRA, the necessary CA certificates for mutual TLS are automatically generated (mutual TLS is a requirement for activation code onboarding). The certificates are available on the CA certificate page for mTLS, which you access from the Trusted CA certificate page (**Maintenance** > **Security** > **Trusted CA certificate)**.

Managing Domain Certificates and Sever Name Indication

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.

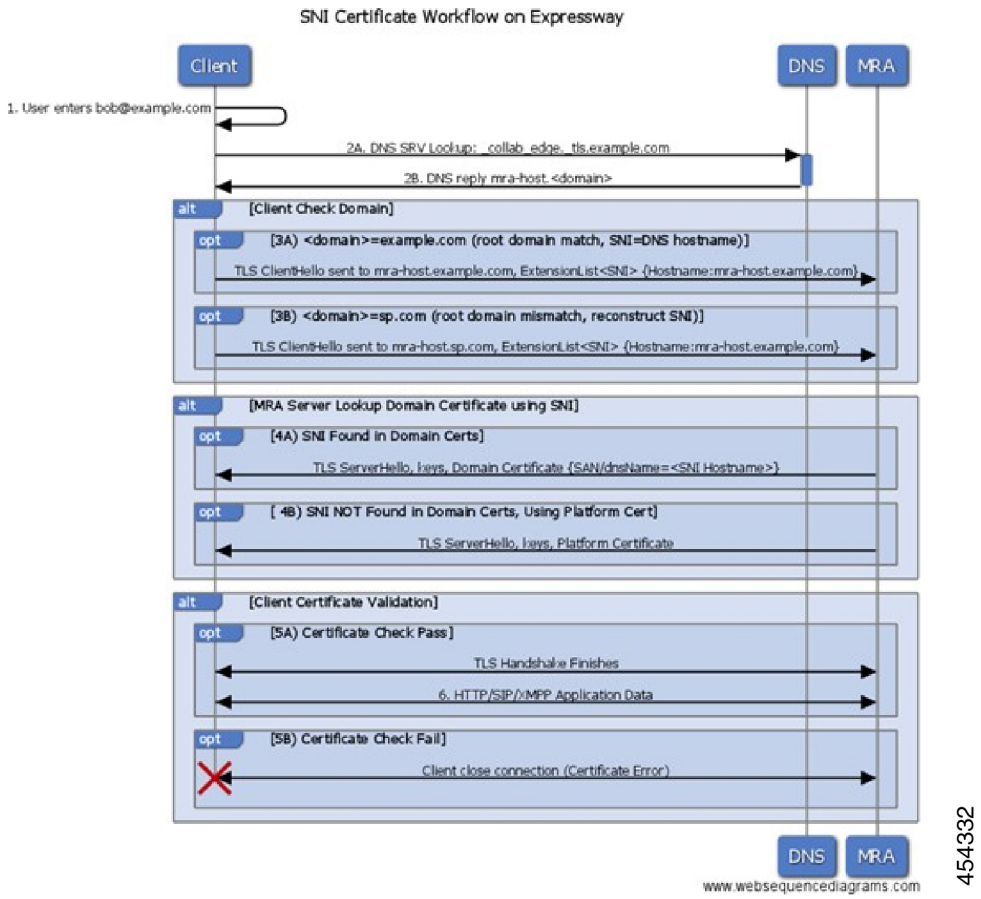
Note In multitenant mode, you must configure the system hostname on the **System** > **DNS** page of the Cisco Expressway-E to match the hostname configured in DNS (case specific before X8.10.1, case insensitive from X8.10.1). Otherwise Cisco Jabber clients will be unable to register successfully for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



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 an 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.
- Configure the Automated Certificate Management Environment (ACME) service to automatically submit a CSR to an ACME provider, and automatically deploy the resulting 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. 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

Step 1 Go to **Maintenance** > **Security** > **Domain certificates**.

Step 2 Click **New**.

Step 3 Under **New local domain**, enter the name of the domain you wish to add.

Example:

An example valid domain name is `100.example-name.com`.

Step 4 Click **Create domain**.

Step 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, which removes the need to use an external mechanism to generate and obtain certificate requests.

Note

- Only one signing request can be in progress at any one time. This is because the Expressway must 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 supports a key length of 1024, 2048 and 4096.

Step 1 Go to **Maintenance** > **Security** > **Domain certificates**.

Step 2 Click on the domain for which you wish to generate a CSR.

Step 3 Click **Generate CSR** to go to the **Generate CSR** page.

Step 4 Enter the required properties for the certificate.

See Domain Certificates and Clustered Systems, page 145 if your Expressway is part of a cluster.

Step 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.

Note Never disclose your private key, not even to the certificate authority.

Step 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).

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.

Step 1 Go to **Maintenance** > **Security** > **Domain certificates**.

Step 2 Use the **Browse** button in the **Upload new certificate** section to select and upload the domain certificate PEM file.

Step 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.

Step 4 Click **Upload domain certificate data**.

Automated Certificate Management Environment Service

The Automated Certificate Management Environment (ACME) service on the Expressway-E, from version X12.5, can request and deploy domain certificates (used with SNI).

When you go to **Maintenance** > **Security** > **Domain certificates**, the list of domains has an ACME column that shows the status of the **ACME** service for each domain.

Click **View/Edit** next to the domain name to enable the ACME service.

The process of configuring ACME service for domain certificates is the same as it is for the server certificate, only from a different place in the Expressway-E interface.

See *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway Configuration Guides page.

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.

Note Make sure 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.

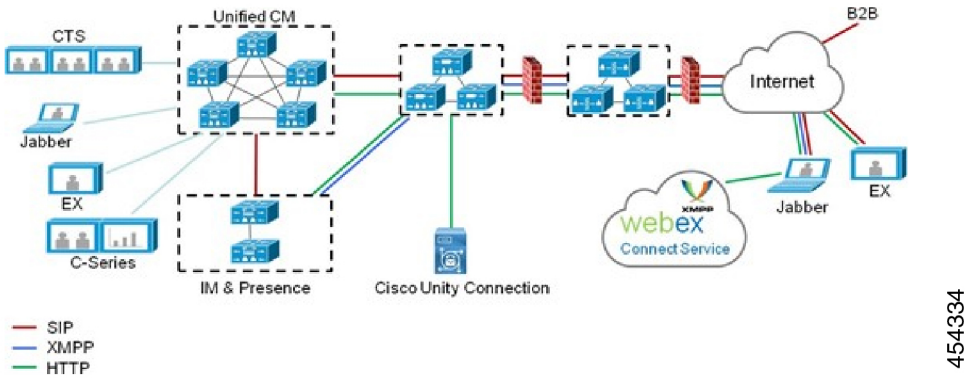
Mobile and Remote Access Overview

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 the following functions:

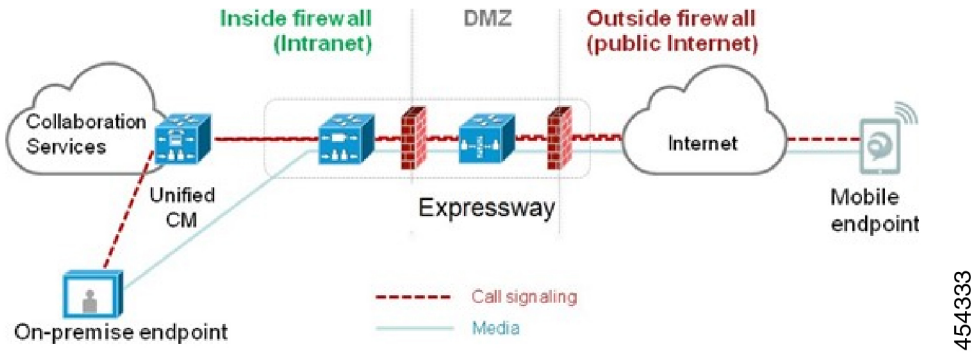
- **Off-premises access:** A consistent experience outside the network for Jabber and EX/MX/SX Series clients.
- **Security:** Secure business-to-business communications.
- **Cloud services:** Enterprise grade flexibility and scalable solutions providing rich Cisco Webex integration and service provider offerings.
- **Gateway and interoperability services:** Media and signaling normalization, and support for non-standard endpoints.

Figure 12: Unified Communications: Mobile and Remote Access



Note 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 13: 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

Mobile and Remote Access Ports

Information about MRA ports is available in the *Cisco Expressway IP Port Usage Configuration Guide* at the Cisco Expressway Series Configuration Guides page. This includes ports that can potentially be used between the 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.

Jabber Client Connectivity Without VPN

The MRA solution 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

Where to Get Detailed Configuration Information

For details about using Expressway for MRA, see the *Mobile and Remote Access Deployment Guide* on the Expressway Configuration Guides page. The guide describes:

- How to enable and configure MRA features on Expressway-C and Expressway-E?
- How to discover the Unified CM servers and IM&P servers used by the MRA service?
- MRA access control, including authentication settings, SAML SSO, and allow lists.
- How to enable support for push notifications?

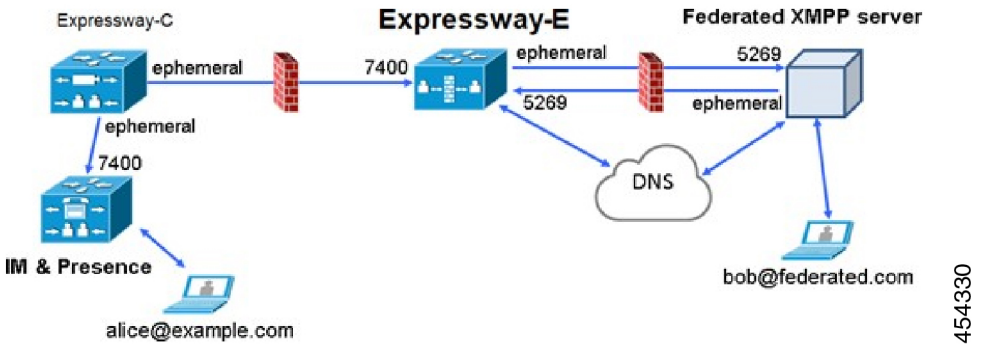
XMPP Federation Through Expressway

External XMPP federation enables users registered to Cisco Unified Communications Manager IM and Presence Service, to communicate via the Expressway-E with users from a different XMPP deployment.

Note This section describes XMPP federation as managed through Expressway, but it can also be managed through the IM and Presence Service, as described later in this guide.

The diagram shows XMPP message routing from the on-premises IM & Presence server, through the Expressway-C and Expressway-E Collaboration Edge solution, to the federated XMPP server. It also shows the ports and connections as the messages traverse DMZ firewalls. The “example.com” organization is using an Expressway federation model (left of picture), while the “federated.com” organization (right of picture) is using an IM and Presence Service in DMZ federation model.

Figure 14: Message routing for XMPP federation



Supported Systems

Expressway-E supports XMPP federation with the following products:

- Expressway X8.2 or later
- Cisco Unified Communications Manager IM and Presence Service 9.1.1 or later
- Cisco Webex Connect Release 6.x
- Cisco Jabber 9.7 or later
- Other XMPP standards-compliant servers

Limitations

- 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, try 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 their Jabber ID does not match their email address (especially if their Jabber ID uses an internal user ID or domain) you are unable to have federation, as you won't know the enterprise user’s email address. We therefore 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. 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 IM and Presence Service to use either the Jabber ID or the Directory URI (typically email) for non-federated use cases.

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

a. Unified CM Lightweight Directory Access Protocol (LDAP) attribute for User ID to be the user's sAMAccountName

b. IM and Presence Service presence domain to be the same as the email domain.

c. Your email address to the same as samaccountname@presencedomain.

- Simultaneous internal federation managed by IM and Presence Service and external federation managed by Expressway is not supported. If only internal federation is required then you must use interdomain federation on IM and Presence Service. The available federation deployment configuration options are:
  - External federation only (managed by Expressway).
  - Internal federation only (managed by IM and Presence Service).
  - Internal and external federation managed by IM and Presence Service, but requires you to configure your firewall to allow inbound connections.

Prerequisites

- Interdomain XMPP Federation must be **disabled** on the IM and Presence Service before you enable XMPP federation on Expressway:

  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*.
- XMPP federation is only supported on a single Expressway cluster.
- An Expressway-C (cluster) and Expressway-E (cluster) must be configured for Mobile and Remote Access (MRA) to Unified Communications services, as described in the *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), these 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 The federated communications are available to both on-premises clients (connected directly to IM and Presence Service) and off-premises clients (connected to IM and Presence Service through MRA).

- SIP and XMPP federations are separate and do not impact on each other. For example, it's possible to deploy SIP federation on IM and Presence Service 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 the IM and Presence Service.
- 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 IM and Presence Service servers. Use either the XMPPAddress or DNS formats.

Note The Expressway-C automatically includes the chat node aliases in its certificate signing requests (CSRs), providing it has discovered a set of IM and Presence Service 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.

Detailed Configuration Information

For information about configuring XMPP federation managed by IM and Presence Service, see Interdomain Federation on IM and Presence Service for Cisco Unified Communications Manager.

For information about configuring XMPP federation managed by Expressway, see *XMPP Federation using Expressway or IM and Presence Service* on the Expressway Configuration Guides page.

Delayed Cisco XCP Router Restart

The delayed Cisco XCP Router restart feature is part of Cisco Hosted Collaboration Solution (HCS), and 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.

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 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.

For more information, please see *Cisco Unified Communications XMPP Federation using IM and Presence Service or Expressway* on the Expressway Configuration Guides page.

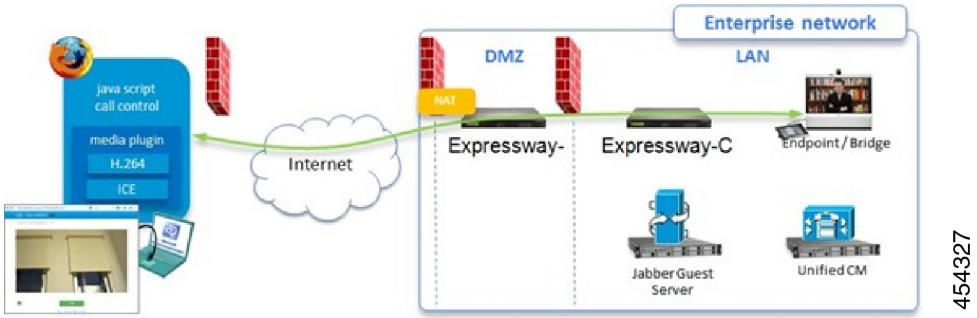
Jabber Guest Services Overview

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 15: 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:

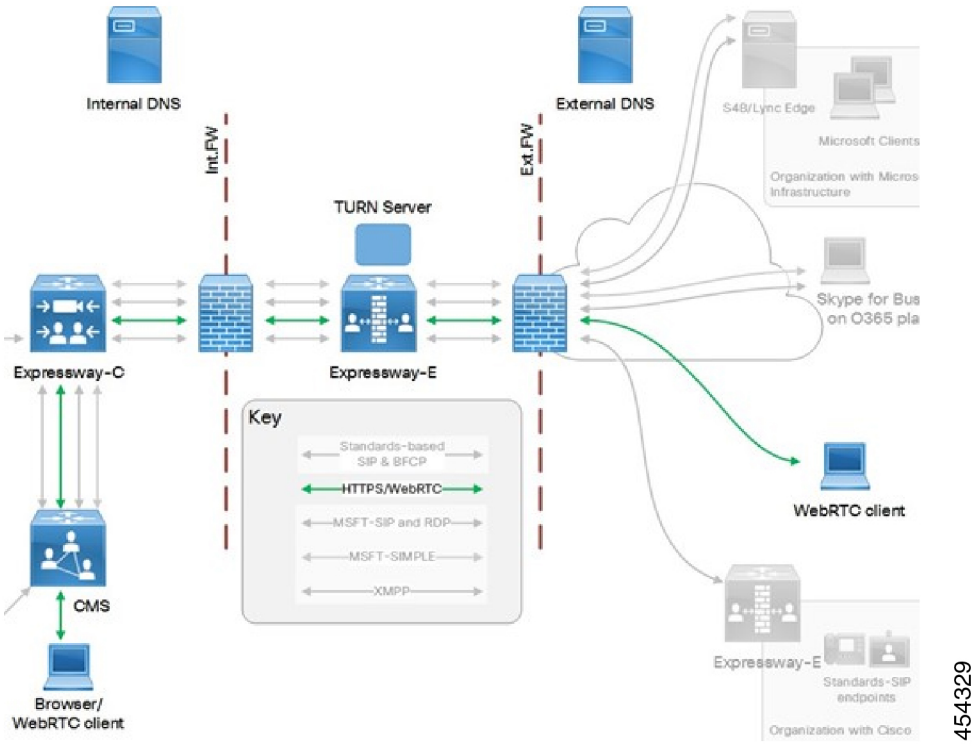
- *Cisco Expressway with Jabber Guest Deployment Guide*, at the Expressway Configuration Guides page.
- *Cisco Jabber Guest Server Installation and Configuration Guide*, for your version, at the Jabber Guest Installation and Upgrade Guides page.

- *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.

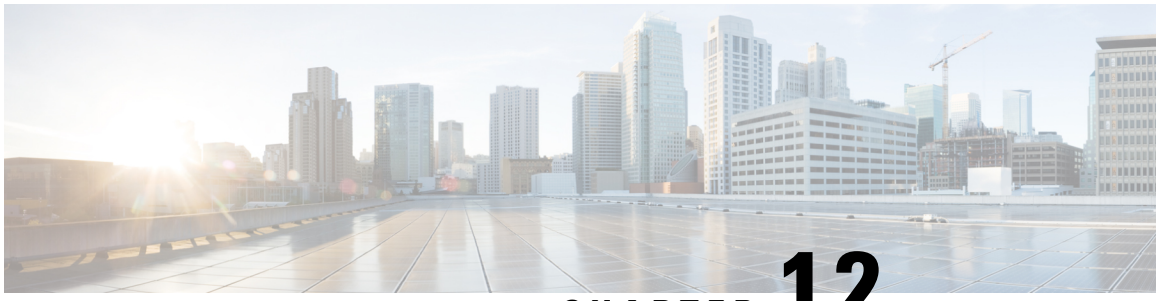
Meeting Server Web Proxy on Expressway

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.

Figure 16: Meeting Server web proxy on Expressway



Cisco Meeting Server with Cisco Expressway Deployment Guide on the Expressway Configuration Guides page (previously called the *Cisco Expressway Traffic Classification Deployment Guide*).



CHAPTER 12

Protocols

- About H.323, on page 209
- Configuring H.323, on page 210
- About SIP, on page 212
- Configuring SIP, on page 215
- Configuring Domains, on page 220
- Configuring SIP and H.323 Interworking, on page 222

About H.323

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

The Expressway can also provide Configuring SIP and H.323 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:

- Manual
- 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**).

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 About 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 *Off* 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.	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.

Field	Description	Usage tips
Registration conflict mode	Determines how the system behaves if an endpoint attempts to register an alias currently registered from another IP address. *Reject*: Denies the new registration. This is the default. *Overwrite*: 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: • 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. *Reject* is useful if your priority is to prevent two users registering with the same alias. *Overwrite* is useful if your network is such that endpoints are often allocated new IP addresses, because it will prevent unwanted registration rejections. **Note** 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.	
Call signaling port range start and end	Specifies the port range used by H.323 calls after they are established.	The call signaling port range must be great enough to support all the required concurrent calls.
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.

Field	Description	Usage tips
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 About H.323 sent out by endpoints. The default is *On*.	To prevent H.323 endpoints being able to register automatically with the Expressway, set **Auto discover** to *Off*. This means that endpoints can only register with the Expressway if their **Gatekeeper Discovery** setting is *Manual* 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, SIP proxy and as a SIP Presence Server. Expressway can provide interworking between SIP and H.323, translating between the two protocols to enable endpoints that only support one of the protocols to call each other.

To support SIP:

- Configuring SIP must be enabled.
- At least one of the SIP transport protocols (UDP, TCP or TLS) must be active.

Note 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 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 Configuring Domains for which it will be authoritative . It will then handle registration requests for any endpoints attempting to register against that domain.

Note 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 About Registrations settings.

In a Mobile and Remote Access Overview 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	Minimum 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. See Configuring H.323.

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.

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

- SIP registration proxy mode setting
- 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 About Registrations, 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 Zones (Non-Default Zones).

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.

Expressway as a SIP Presence Server

The Expressway supports the SIP-based SIMPLE protocol. It can act as a Presence Server and Presence User Agent for any of the SIP domains for which it is authoritative. For details on how to enable and use Expressway as a SIP Presence server, see the About Presence section.

Configuring SIP

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

- 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 *Off*.	This mode must be enabled to use either the Presence Server or the Presence User Agent.
SIP protocols and ports	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. The default modes are: • UDP mode *Off* • TCP mode *Off* • TLS mode *On* • Mutual TLS mode *Off*	At least one of the transport protocol modes must be *On* to enable SIP functionality. If you use both TLS and MTLS, we recommend that you enable them on different ports. If you must use port 5061 for MTLS, you should avoid engaging the B2BUA - by switching **Media encryption mode** to *Auto* on all zones in the call path.
TCP outbound port start / end	The range of ports the Expressway uses when TCP and TLS connections are established.	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 *Session-Expires* 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 *Min-SE header* 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:

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. • The OCSP responder must support the SHA-256 hash algorithm. If it is not supported, the OCSP revocation check and the certificate validation will fail.
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)), 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. *Treat as revoked*: Treat the certificate as revoked (and thus do not allow the TLS connection). *Treat as not revoked*: Treat the certificate as not revoked. Default: *Treat as not revoked*.	*Treat as not revoked* 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	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. *Maximum*: Uses the lesser of the configured **Maximum** refresh value and the value requested in the registration. *Variable*: 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. The default is *Maximum*.	The *Maximum* setting uses the requested value providing it is within the specified maximum and minimum ranges. The *Variable* 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. This applies only to endpoints registered with the Expressway. It does not apply to endpoints whose registrations are proxied through the Expressway.
Standard registration refresh minimum	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.	See Registration refresh intervals.
Standard registration refresh maximum	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.	
Outbound registration refresh strategy	The method used to generate the SIP registration expiry period for outbound registrations. *Maximum*: Uses the lesser of the configured **Maximum** refresh value and the value requested in the registration. *Variable*: 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. The default is *Variable*.	These options work in the same manner as for the **Standard registration refresh strategy**. 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.

Field	Description	Usage tips
Outbound registration refresh minimum	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.	
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	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. *Off*: 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. *Proxy to known only*: 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. *Proxy to any*: Registration requests are proxied in accordance with existing call processing rules to all known zones. Requests containing Route Sets are always proxied. The default is *Off*.	See Proxying Registration Requests 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	Controls whether the credential checking of SIP messages is delegated, via a traversal zone, to another Expressway. *Off:* Use the relevant credential checking mechanisms (local database, Active Directory Service or H.350 directory via LDAP) on the Expressway performing the authentication challenge. *On:* Delegate the credential checking to a traversal client. The default is *Off*.	**Note** Delegated credential checking must be enabled on both the traversal server and the traversal client. See delegated credential checking for more information.

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 (like an unavailable onward SIP proxy peer) and failing over to a good one. Be careful in high latency networks that you leave enough time for the connection to establish.

Retain Connection for Corrupt/Malformed SIP Message (CLI)

From X8.11, a CLI command (not the web user interface) is available to optionally configure the Expressway to keep a connection open even if it receives malformed or corrupt SIP messages. You can specify this for non-mandatory headers only, or for mandatory headers too. See Zones Zone [1..1000] Neighbor RetainConnectionOnParseErrorMode: <mode>.

Configuring Domains

The **Domains** page (**Configuration** > **Domains**) lists the SIP domains managed by this Expressway.

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 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 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 Mobile and Remote Access Overview 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 Presence Server in the case of VCS systems), 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:

Step 1 Go to **Configuration** > **Domains**.

Step 2 Select the relevant domains.

Step 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 at least 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 at least 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.

Note 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 except when both the endpoints are registered to the Cisco infrastructure. 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.

Configuring DH key length

X12.6 introduced support for 2048-bit Diffie-Hellman keys for H.323 call encryption, as part of the ongoing security enhancements for Expressway, so Expressway offers both 1024-bit and 2048-bit encryption key length as default behavior.

This may cause unexpected H.323 call failures if the deployed firewall's ALG function or endpoints are unable to handle both 1024-bit and 2048-bit for the Diffie-Hellman key exchange. In this case, from X12.6.4 administrators can optionally revert to 1024-bit encryption by using the CLI command `xConfiguration Interworking Encryption KeySize2048: <On/Off>`.

Changes to the interworking encryption key size do not need a restart to take effect. Changes to the primary node in a cluster are automatically replicated to its subsidiary nodes.

Searching by protocol

When searching a zone, the Expressway first performs the search using the protocol of the incoming call. If the search is unsuccessful the Expressway may then search the zone again using the alternative protocol, depending on where the search came from and the **Interworking mode**.

Note 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**.

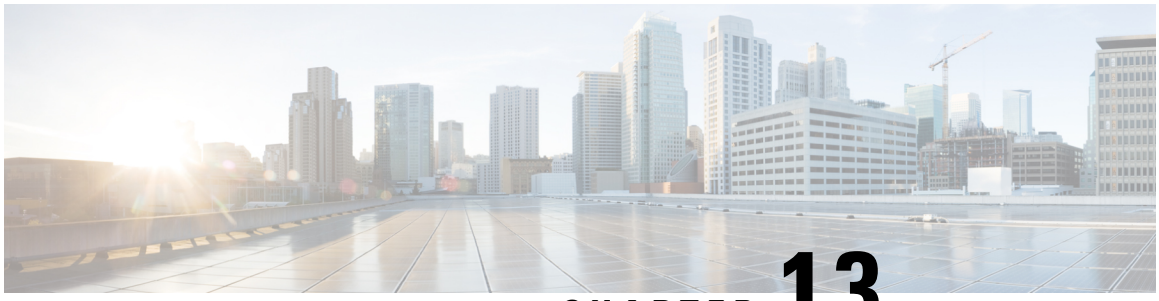
  See the About Pre-Search Transforms section for information about how to configure pre-search transforms, and the Stripping @domain for Dialing to H.323 Numbers section for an example of how to do this.

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 (for example, **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 the H.245 user input indicators “dtmf” and “basicString”.



CHAPTER 13

Registration Control

- About Registrations, on page 225
- About Allow and Deny Lists, on page 228
- Configuring Registration Policy to Use an External Service, on page 230

About Registrations

For an endpoint to use the Expressway as its SIP registrar or H.323 gatekeeper, 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 About Device Authentication process based on the username and password supplied by the endpoint.
- A Configuring Registration Restriction Policy that uses either About Allow and 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 About Subzones.

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 Configuring H.323 registrations
- The **SIP registration proxy mode** for Configuring SIP registrations

For specific information about how registrations are managed across peers in a cluster, see the Sharing Registrations Across Peers section.

In a Mobile and Remote Access Overview 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 an 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 Configuring SIP and Configuring H.323.

Note If you select MRA (for example), Expressway E will register devices even upon disabling the **Registration** tab.

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.

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 Configuring the Registration Allow List or Configuring the 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.

Registering Aliases

After the About 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.

- **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 Configuring 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 Configuring the Registration 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 Configuring 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) 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 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 Configuring Subzones 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 Configuring Registration Restriction Policy 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: *Exact*: The alias must match the pattern string exactly. *Prefix*: The alias must begin with the pattern string. *Suffix*: The alias must end with the pattern string. *Regex*: The pattern string is a Regular Expressions.	You can test whether a pattern matches a particular alias by using the Checking the Effect of 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 Configuring Registration Restriction Policy page.

The configurable options are:

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

Field	Description	Usage tips
Pattern type	The way in which the **Pattern string** must match the alias. Options are: *Exact*: The alias must match the pattern string exactly. *Prefix*: The alias must begin with the pattern string. *Suffix*: The alias must end with the pattern string. *Regex*: The pattern string is a Regular Expressions.	You can test whether a pattern matches a particular alias by using the Checking the Effect of 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:

Step 1 Go to **Configuration** > **Registration** > **Configuration**.

Step 2 Select a **Restriction policy** of *Policy service*.

Step 3 Configure the fields as follows:

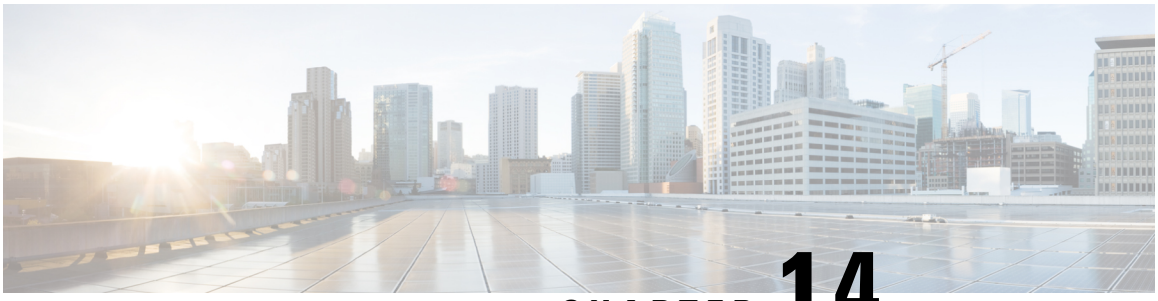
Field	Description	Usage tips
Protocol	The protocol used to connect to the policy service. The default is *HTTPS*.	The Expressway automatically supports HTTP to HTTPS redirection when communicating with the policy service server.
Certificate verification mode	When connecting over HTTPS, this setting controls whether the certificate presented by the policy server is verified. If *On*, 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.

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 *status*.	The policy server must supply return status information, see Policy Server Status and Resiliency.
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.

Step 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.



CHAPTER 14

Device Authentication

- About Device Authentication, on page 233
- Authentication Policy, on page 234
- Authentication Methods, on page 238
- Authenticating with External Systems, on page 239

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 Configuring Authentication to Use the Local 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.

Authentication Policy

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 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 is 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 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.

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	Messages are challenged for authentication. Messages that fail authentication are rejected. Messages that pass authentication are classified as authenticated and a P-Asserted-Identity header is inserted into the message.	Messages are not challenged for authentication. All messages are classified as unauthenticated. Any existing P-Asserted-Identity headers are removed.
	On	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). 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.	Messages are not challenged for authentication. Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged. Messages without an existing P-Asserted-Identity header are classified as unauthenticated.
Do not check credentials	Off	Messages are not challenged for authentication. All messages are classified as unauthenticated. Any existing P-Asserted-Identity headers are removed.	Messages are not challenged for authentication. All messages are classified as unauthenticated. Any existing P-Asserted-Identity headers are removed.

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

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:

- Configuring Registration Restriction Policy

- Configuring Search Rules
- Configuring Call Policy
- Configuring FindMe

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

SIP Authentication Trust

If the Expressway is configured to use About 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 3326.

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.

Authentication Methods

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 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.

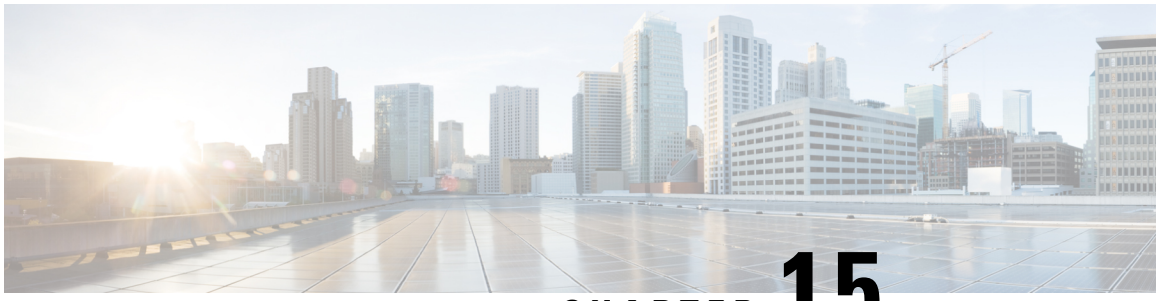
- NTLM challenges are offered in addition to the standard Digest challenge.
- Endpoints that support NTLM will respond to the NTLM challenge in preference to the Digest challenge, and the Expressway will attempt to authenticate that NTLM response.

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 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.



CHAPTER 15

Zones and Neighbors

- Video Network Fundamentals, on page 241
- Structuring the Dial Plan, on page 242
- About Zones, on page 243
- Configuring ICE Messaging Support, on page 244
- About the Local Zone and Subzones, on page 247
- Configuring the Default Zone, on page 248
- Configuring Default Zone Access Rules, on page 249
- Configuring Zones (Non-Default Zones), on page 250

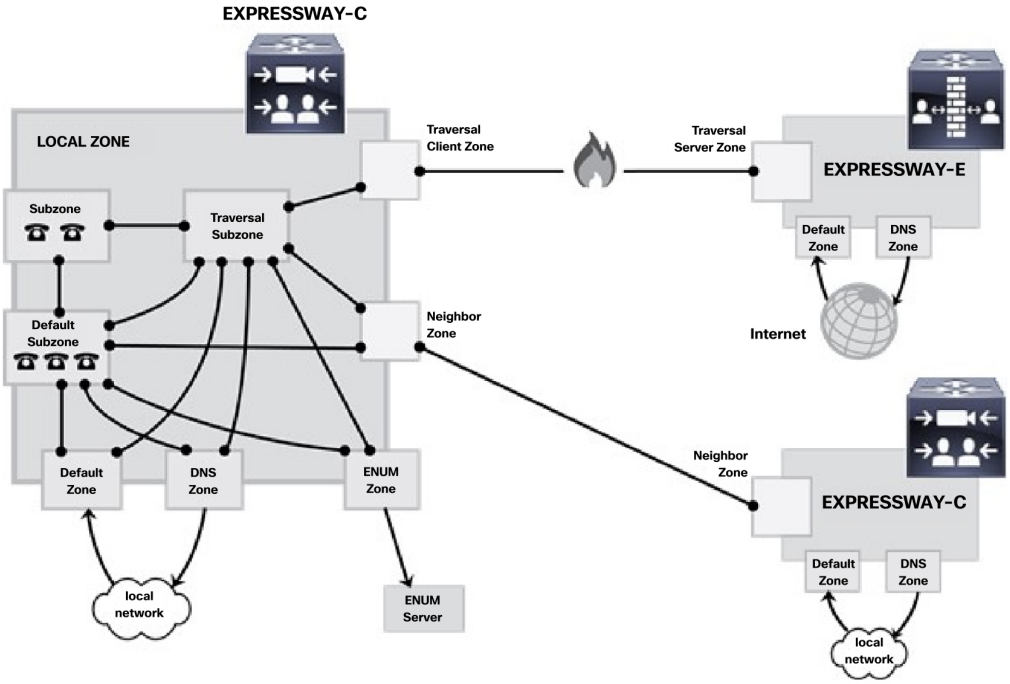
Video Network Fundamentals

This section summarizes the different parts of a video communications network that uses Expressway, and the ways to connect them.

The most basic implementation is a single Expressway connected to the internet with one or more endpoints registered to it. 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, and with one or more firewalls between the Expressway 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.)

The diagram shows the different subzones and zones for an example Expressway deployment. It uses a Expressway-C as the example Local Zone, to show how it's made up of multiple subzones connected by links. The Local Zone is connected to external Expressways and to the internet via particular types of zones.

Figure 17: Example network diagram



Structuring the 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.

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, and 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, and a search rule with a **Mode** of *Any alias* and a **Target** of the directory Expressway.

Unless your deployment uses device authentication, there's 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. It may be necessary to neighbor the Expressways to each other if you use device authentication (see below).

Failure of the directory Expressway in this situation could cause significant disruption to communications. Consideration should be given to the use of About Clusters 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 through an ENUM or DNS lookup. Zones have many functions, including:

- 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 About Device Authentication.
- Control the Configuring Media Encryption Policy and Configuring ICE Messaging Support 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:

- Configuring Neighbor Zones: A connection to a neighbor system of the local Expressway.
- Configuring Traversal Client Zones: The local Expressway is a traversal client of the system being connected to, and there is a firewall between the two.
- Configuring Traversal Server Zones: The local Expressway is a traversal server for the system being connected to, and there is a firewall between the two.
- Configuring ENUM Zones: The zone contains endpoints discoverable by ENUM lookup.
- Configuring DNS Zones: The zone contains endpoints discoverable by DNS lookup.
- Unified Communication Prerequisites: A traversal client or traversal server zone used for Unified Communications features such as mobile and remote access or Jabber Guest.

The Expressway also has a pre-configured Configuring the Default Zone.

- See the Configuring Zones (Non-Default Zones) section for information about the configuration options available for all zone types.
- See the Configuring Search 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 Overview.
- An Expressway automatically generates a neighbor zone named “To Microsoft destination via B2BUA” when the About Microsoft Interoperability service is enabled.
- Expressway automatically generates a neighbor zone named “CEOAuth <Unified CM name>” between itself and each discovered Unified CM node when SIP OAuth Mode is enabled on Unified CM.

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 on the **ICE support** setting configuration on the incoming (ingress) and outgoing (egress) zone. When there is a mismatch of settings (*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 Configuring Media Encryption Policy, on page 246 (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 = *Off*	At least one zone is **not** *Auto*	Yes	The B2BUA will not perform any ICE negotiation with either host.
Both zones = *On*	At least one zone is **not** *Auto*	Yes	The B2BUA will perform ICE negotiation with both hosts.
Both zones = *On*	Both zones = *Auto*	No	The Expressway will not offer any TURN relay candidate addresses to either of the ICE capable hosts. **Note** Each host device may have already been provisioned with TURN relay candidate addresses.

Note

- B2BUA routed calls are identified in the call history by a component type of *B2BUA*.
- An RMS call license is used when a call goes via the encryption B2BUA except when calling to/from a registered endpoint.
- There is a limit of 100 concurrent calls (500 calls on Hardware Appliance and Virtual Machine Options) that can be routed via B2BUA.

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.

Note Remember that when configuring your system to use media encryption:

- 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 uses a Rich Media Session (RMS) license except when both the endpoints are registered to Cisco infrastructure.
- There is a limit per Expressway of 100 simultaneous video calls (500 video calls on Hardware Appliance and Virtual Machine Options) that can have a media encryption policy applied.
- The B2BUA can also be invoked when Configuring 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.

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's 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:

- About the Traversal Subzone, which is always present
- About the Cluster Subzone, which is always present but only used when the 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 About 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 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 Rules section.

Configuring 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 preconfigured with the Default Zone and Default Links between it and the Traversal Subzone. The Default Zone cannot be deleted.

Note All calls through the Default Zone consume RMS licenses. Make sure to create appropriate zone/rules for calls to avoid consumption of RMS licenses.

Default Zone Settings

By configuring the Default Zone you can control how the Expressway handles calls from unrecognized systems and endpoints. Go to **Configuration** > **Zones** > **Zones** and click **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 for more information.

Field	Description	Usage tips
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 for more information.
ICE support	Controls whether ICE messages are supported by the devices in this zone.	See Configuring ICE Messaging Support for more information.
Enable Mutual TLS on Default Zone	*On* enforces MTLS (Mutual Transport Layer Security) on incoming connections through the Default Zone. *Off* 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**. Default: *Off*	This setting does not affect other connections to the Default Zone (H.323, SIP UDP, or SIP TCP). **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). If you must use port 5061 for MTLS, then you should avoid engaging the B2BUA - by switching **Media encryption mode** to *Auto* on all zones in the call path.

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, or 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 15: Default Zone Access Rule Parameters

Field	Description	Usage Tips
Name	The name assigned to the rule.	

Field	Description	Usage Tips
Description	An optional free-form description of the rule.	
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. *Exact*: The entire string must exactly match the name, character for character. *Prefix*: The string must appear at the beginning of the name. *Suffix*: The string must appear at the end of the name. *Regex*: Treats the string as a Regular Expressions.	You can test whether a pattern matches a particular name by using the Checking the Effect of 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. *Allow*: Allows the external system to connect via the Default Zone. *Deny*: 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.

Configuring Zones (Non-Default Zones)

The **Zones** page (**Configuration** > **Zones** > **Zones**) lists all the zones that have been configured on the Expressway, and lets you create, edit and delete zones. Information is displayed for each listed zone 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, for example, 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.

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

- Configuring Neighbor Zones: Connects the local Expressway to a neighbor system.
- Configuring Traversal Client Zones: Connects the local Expressway to a traversal server.
- Configuring Traversal Server Zones: Connects the local Expressway-E to a traversal client.
- Configuring ENUM Zones: Enables ENUM dialing via the local Expressway.
- Configuring DNS Zones: Enables the local Expressway to locate endpoints and other systems by using DNS lookups.
- Unified Communication Prerequisites: A traversal client or traversal server zone used for Unified Communications features such as mobile and remote access or Jabber Guest.
- Configuring the Webex Zone: Enables a specifically configured DNS zone for use with Cisco Collaboration Cloud.

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. See About Zones for more information about zones and the different zone types.

The Expressway also has a preconfigured Configuring 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.

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 Configuring 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. Then you can do the following operations with the neighbor zone:

- 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

- 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 described in the table.

Table 16: Neighbor zone settings

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 *Neighbor*.	Once a zone is created, you cannot change the **Type**.
Hop count	The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the Configuring 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.	Must be the same port number as that configured on the neighbor system as its H.323 UDP port. If the neighbor is a Expressway acting as a gatekeeper, this corresponds to the **Registration UDP Port** on **Configuration** > **Protocols** > **H.323** page.

Field	Description	Usage tips
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.	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 *TLS*.	
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 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 for more information.
ICE support	Controls whether ICE messages are supported by the devices in this zone.	See Configuring ICE Messaging Support for more information.
ICE Passthrough support	Controls how the Expressway supports ICE Passthrough in this zone.	ICE Passthrough support takes precedence over ICE support. Best practice is to turn on ICE Passthrough support and turn off ICE support. Configuration details and required versions for ICE passthrough are in the *Mobile and Remote Access Through Cisco Expressway guide* on the Expressway Configuration Guides page.

Field	Description	Usage tips
Multistream mode	Controls whether the Expressway B2BUA allows multistream calls to be negotiated between calling parties. *On*: Expressway allows the calling parties to negotiate and set up a multistream call through this zone *Off*: 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 *On* 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.
Preloaded SIP routes support	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.	
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.
SIP UPDATE for session refresh	Determines whether this zone supports the SIP UPDATE method to send and receive session refresh requests.	*On*: This zone sends and receives SIP UPDATE for session refresh requests. *Off*: This zone does not allow SIP UPDATE for session refresh requests. Default: *Off*
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 for more information.

Field	Description	Usage tips
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 for more information.
Location section:		
Look up peers by	Determines whether you look up peers by address, or by service (SRV) record lookup. • *Address* (default) allows you to add up to six peers. When you click **Save**, the Expressway does the lookup for the addresses. • *Service record* 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. 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.	**Notes about SRV record lookup:** These four service lookups are possible: • _sip._udp.example.com. SIP over UDP (this is disabled on Expressway and its zones by default) • _sip._tcp.example.com. SIP over TCP • _sips._tcp.example.com. SIP over TLS (secure SIP) • _h323._udp.example.com. H.323 over UDP (other transports have never been supported for H.323) For any given neighbor zone configured with an SRV record lookup, by default the maximum number of peers the Expressway can register against is 15, but a maximum of 30 is allowed through the xConfiguration Command. For more information, see the chapter "Reference Material", section "xConfiguration Command" for the following command xConfiguration Zones Zone [1..1000] Neighbor SRV MaxPeers: <1..30>. If you use look up by DNS server be aware that your zones communicate over the SRV record-specified port and not the zone port. Keep the DNS-specified port open on your firewall.

Field	Description	Usage tips
Peer 1 to Peer 6 address	The IP address or FQDN of the neighbor system. Enter the addresses of additional peers if: • 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	Calls to an Expressway cluster are routed to whichever peer in that neighboring cluster has the lowest resource usage. See Neighboring Between Expressway Clusters for more information. 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.
Advanced section:		
Zone profile	Determines how the zone's advanced settings are configured. *Default*: Uses the factory default profile. *Custom*: Allows you to configure each setting individually. Alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. The options include: • *Default* • *Custom* • *Cisco Unified Communications Manager (8.6 and below)* • *Cisco Unified Communications Manager (8.6.1 or 8.6.2)* • *Cisco Unified Communications Manager (9.x or later)* • *Nortel Communication Server 1000* • *Infrastructure device* (typically used for non-gatekeeper devices such as an MCU)	See Zone Configuration: Advanced Settings for details on the advanced settings. Only use the *Custom* profile to configure the individual advanced settings on the advice of Cisco customer support. See Cisco Unified Communications Manager with Expressway Deployment Guide for more information about *Cisco Unified Communications Manager* profiles.

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 do the following:

- 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.

Note An Configuring the NTP Servers must be configured for traversal zones to work.

More information

Details about how traversal client zones and traversal server zones work together for firewall traversal are in About Firewall Traversal.

Traversal client zone settings

The configurable options for a traversal client zone are described in the table.

Table 17: Traversal client zone settings

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 *Traversal client*.	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 Configuring 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.

Field	Description	Usage tips
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 (*Assent* or *H.460*.18) to use for calls to the traversal server.	See Configuring Ports for Firewall Traversal 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 SIP calls.	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 *TLS*.	
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 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 for more information.
ICE support	Controls whether ICE messages are supported by the devices in this zone.	See Configuring ICE Messaging Support for more information.

Field	Description	Usage tips
ICE Passthrough support	Controls how the Expressway supports ICE Passthrough in this zone.	ICE Passthrough support takes precedence over ICE support. Best practice is to turn on ICE Passthrough support and turn off ICE support. Configuration details and required versions for ICE passthrough are in the *Mobile and Remote Access Through Cisco Expressway Guide* on the Expressway Configuration Guides page.
Multistream mode	Controls whether the Expressway B2BUA allows multistream calls to be negotiated between calling parties. *On*: Expressway allows the calling parties to negotiate and set up a multistream call through this zone *Off*: 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 *On* 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** *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.	

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.	*On* preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. *Off* allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: *Off*
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.
SIP UPDATE for session refresh	Determines whether this zone supports the SIP UPDATE method to send and receive session refresh requests.	*On*: This zone sends and receives SIP UPDATE for session refresh requests. *Off*: This zone does not allow SIP UPDATE for session refresh requests. Default: *Off*
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 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.	
Disconnect on fail interval	When a zone is in failed state, this parameter determines the frequency that the connection for the SIP OPTIONS ping message is disconnected.	
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 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. For full details on how traversal client zones and traversal server zones work together to achieve firewall traversal, see About Firewall Traversal.

Note You must synchronize with an Configuring the NTP Servers 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 18: 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 *Traversal server*.	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 Configuring 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:		

Field	Description	Usage tips
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: • 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 (*Assent* or *H.460.18*) to use to traverse the firewall/NAT.	See Configuring Ports for Firewall Traversal for more information.
Port	The port on the local Expressway-E to use for H.323 calls to and from the traversal client.	**Note** From X14.0.1 versions, if you come across a warning alarm, consider changing the conflicting port number to a new value as you may have created traversal server zone with same port used for H323/SIP in more than one traversal server zone that is disabled.
H.460.19 demultiplexing mode	Determines whether or not the same two ports are used for media by two or more calls. *On*: All calls from the traversal client use the same two ports for media. *Off*: 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 *TLS*.	

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 Mobile and Remote Access Overview is set to *Mobile and remote access*.
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 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 for more information.
ICE support	Controls whether ICE messages are supported by the devices in this zone.	See Configuring ICE Messaging Support for more information.
ICE Passthrough support	Controls how the Expressway supports ICE Passthrough in this zone.	ICE Passthrough support takes precedence over ICE support. Best practice is to turn on ICE Passthrough support and turn off ICE support. Configuration details and required versions for ICE passthrough are in the *Mobile and Remote Access Through Cisco Expressway Guide* on the Expressway Configuration Guides page.

Field	Description	Usage tips
Multistream mode	Controls whether the Expressway B2BUA allows multistream calls to be negotiated between calling parties. *On*: Expressway allows the calling parties to negotiate and set up a multistream call through this zone *Off*: 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 *On* 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** *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.	
SIP parameter preservation	Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone.	*On* preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. *Off* allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: *Off*
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.

Field	Description	Usage tips
SIP UPDATE for session refresh	Determines whether this zone supports the SIP UPDATE method to send and receive session refresh requests.	*On*: This zone sends and receives SIP UPDATE for session refresh requests. *Off*: This zone does not allow SIP UPDATE for session refresh requests. Default: *Off*
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 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.	

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 section.

The configurable options for an ENUM zone are described in the table.

Table 19: ENUM zone settings

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 *ENUM*.	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 Configuring 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 endpoint aliases.

After you configure one or more DNS zones, you can apply transforms to alias search requests directed to that group of endpoints. You can also control the bandwidth used for calls between your local Expressway and each group of DNS endpoints. See About URI Dialing for more information on configuring and using DNS zones.

The configurable options for a DNS zone are described in the table.

Table 20: DNS zone settings

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 *DNS*.	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 Configuring 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 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 the SAN - Subject Alternative Name - attribute).	
TLS verify inbound mapping	Switch Inbound TLS mapping On 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 *Off* to prevent the Expressway from attempting to map inbound TLS connections to this zone.

Field	Description	Usage tips
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 *UDP* (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 for more information.
ICE support	Controls whether ICE messages are supported by the devices in this zone.	See Configuring ICE Messaging Support for more information.
Preloaded SIP routes support	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.	
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.
SIP UPDATE for session refresh	Determines whether this zone supports SIP UPDATE method to send and receive session refresh requests.	*On*: This zone sends and receives SIP UPDATE for session refresh requests. *Off*: This zone does not allow SIP UPDATE for session refresh requests. Default: *Off*
Authentication section		

Field	Description	Usage tips
SIP authentication trust mode	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. *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*.	For a DNS zone, you should always set **Authentication policy** to treated as authenticated.
Advanced section		
Include address record	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. *On*: The Expressway queries for A or AAAA records. If any are found, the Expressway will not then query any lower priority zones. *Off*: (Default) The Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.	
Zone profile	Determines how the zone's advanced settings are configured. *Default*: Uses the factory default profile. *Custom*: Allows you to configure each setting individually.	See Zone Configuration: Advanced Settings for details on the advanced settings. Only use the *Custom* profile to configure the individual advanced settings on the advice of Cisco customer support.

Configuring the Webex Zone

The Webex zone is a pre-configured DNS zone for connecting the Expressway-E to Cisco Webex. You can use this zone to enable Cisco Webex Hybrid Call Service or Webex Meetings, or both.

Expressway-E connects to Cisco Unified Communications Manager without Expressway-C. No traversal or firewall is required for this scenario, and Expressway E connects the Webex Cloud directly to Cisco Unified Communications Manager. The tested configuration uses standard Webex Edge Audio over the internet, with a Neighbor zone between Cisco Unified Communications Manager and Expressway -E.

This scenario requires inbound connections to be opened on the internal firewall. So it is **not** supported for standard Expressway deployments with the usual dual firewall configuration.

To enable the Webex zone:

1. Go to **Configuration** > **Zones** > **Zones**.
2. Click **New**.
3. Select *Webex* from the **Type** dropdown.

   Expressway creates the new zone, with a pre-configured name and pre-configured parameters that ensure the correct connections to Cisco Webex.

Note You cannot create more than one zone of this type, and you cannot modify the single instance of this zone after you have enabled it.

See Hybrid Call Service documentation for detailed configuration information.

How to change the default settings

The media encryption mode for the Webex zone is “Auto”. Because a Webex zone is a pre-configured DNS zone, if some scenarios require it to be “On”, we recommend creating a DNS zone instead. Then change the DNS zone through the Expressway web interface (**Configuration** > **Zones** > **Zones** and set **Media encryption mode** to *On*). The same workaround can be used to change the **SIP authentication trust mode** to *On*.

Limitation

Cisco Webex Calling May Fail with Dual-NIC Expressway

This issue applies if you deploy Expressway/Cisco VCS with a dual-NIC Expressway-E/ Cisco VCS Expressway. Cisco Webex Calling requests may fail if the same (overlapping) static route applies to both the external interface and the interface with the Expressway-C/Cisco VCS Control. This is due to current Expressway-E/Cisco VCS Expressway routing behavior, which treats Webex INVITES as non-NAT and therefore extracts the source address directly from the SIP via header.

Note We recommend that you make static routes as specific as possible, to minimize the risk of the routes overlapping.

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	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. *On*: The Expressway queries for A or AAAA records. If any are found, the Expressway will not then query any lower priority zones. *Off*: The Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.	Off	DNS
Monitor peer status	Specifies whether the Expressway monitors the status of the zone's peers. If enabled, H.323 LRQs and/or SIP OPTIONS are periodically sent to the peers. If a peer fails to respond, that peer is marked as inactive. If all peers fail to respond the zone is marked as inactive.	Yes	Neighbor
Call signaling routed mode	Specifies how the Expressway handles the signaling for calls to and from this neighbor. *Auto*: Signaling is taken as determined by the **Call signaling optimization** (**Configuration** > **Call routing**) configuration. *Always*: Signaling is always taken for calls to or from this neighbor, regardless of the **Call signaling optimization** configuration. Calls via traversal zones or the B2BUA always take the signaling.	Auto	Neighbor
Automatically respond to H.323 searches	Determines what happens when the Expressway receives an H.323 search, destined for this zone. *Off*: An LRQ message is sent to the zone. *On*: Searches are responded to automatically, without being forwarded to the zone.	Off	Neighbor

Setting	Description	Default	Zone types
Automatically respond to SIP searches	Determines what happens when the Expressway receives a SIP search that originated as an H.323 search. *Off*: A SIP OPTIONS or SIP INFO message is sent. *On*: Searches are responded to automatically, without being forwarded. This should normally be left as the default *Off*. However, some systems do not accept SIP OPTIONS messages, so for these zones it must be set to On. If you change this to *On*, you must also configure pattern matches to ensure that only those searches that actually match endpoints in this zone are responded to. If you do not, the search will not continue to other lower-priority zones, and the call will be forwarded to this zone even if it cannot support it.	Off	Neighbor DNS
Send empty INVITE for interworked calls	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. *On*: SIP INVITEs with no SDP are generated. *Off*: SIP INVITEs are generated and a pre-configured SDP is inserted before the INVITEs are sent. In most cases this option should normally be left as the default *On*. However, some devices do not accept invites with no SDP, so for these zones this should be set to *Off*. **Note** The settings for the pre-configured SDP are configurable via the CLI using the `xConfiguration Zones Zone [1..1000] [Neighbor/DNS] Interworking SIP` commands. They should only be changed on the advice of Cisco customer support.		
SIP parameter preservation	Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. *On* preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA. *Off* allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary. Default: *Off*	Off	Neighbor DNS UC Traversal Traversal Server Traversal Client

Setting	Description	Default	Zone types
SIP poison mode	*On*: 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. *Off*: SIP requests sent out via this zone that are received by this Expressway again will not be rejected; they will be processed as normal.	Off	Neighbor Traversal client Traversal server DNS
SIP encryption mode	Determines whether or not the Expressway allows encrypted SIP calls on this zone. *Auto*: SIP calls are encrypted if a secure SIP transport (TLS) is used. *Microsoft*: SIP calls are encrypted using MS-SRTP. *Off*: SIP calls are never encrypted. This option should normally be left as the default *Auto*.	Auto	Neighbor
SIP REFER mode	Determines how SIP REFER requests are handled. *Forward*: SIP REFER requests are forwarded to the target. *Terminate*: SIP REFER requests are terminated by the Expressway.	Forward	Neighbor
Meeting Server load balancing	From X8.11, Cisco Expressway Series supports the mechanism that is used to load balance calls between Meeting Servers that are in call bridge groups. When Cisco Meeting Servers are in a call bridge group, and a participant tries to join a space on a server that has no capacity, the call is rerouted to another server. That other server then sends a SIP INVITE to the call control layer, using the original call details. The participant is now in the correct space, on a different Meeting Server. In cases where there is capacity in the "second" server, but another Meeting Server has more capacity, it asks that Meeting Server in the group to send the SIP INVITE. *On*: Expressway B2BUA processes the INVITEs from the Meeting Server. Required to enable load balancing for endpoints that are registered to Unified CM or this Expressway, or to a neighboring VCS or Expressway. *Off*: Expressway B2BUA does not p	Off	Neighbor
SIP multipart MIME strip mode	Controls whether or not multipart MIME stripping is performed on requests from this zone. This option should normally be left as the default *Off*.	Off	Neighbor

Setting	Description	Default	Zone types
SIP UPDATE strip mode	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. This option should normally be left as the default *Off*. However, some systems do not support the UPDATE method in the Allow header, so for these zones this should be set to *On*.	Off	Neighbor
Interworking SIP search strategy	Determines how the Expressway searches for SIP endpoints when interworking an H.323 call. *Options*: The Expressway sends an OPTIONS request. *Info*: The Expressway sends an INFO request. This option should normally be left as the default *Options*. However, some endpoints cannot respond to OPTIONS requests, so this must be set to *Info* for such endpoints.	Options	Neighbor
SIP UDP/BFCP filter mode	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. *On*: Any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled. *Off*: INVITE requests are not modified.	Off	Neighbor DNS
SIP UDP/IX filter mode	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. *On*: Any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled. *Off*: INVITE requests are not modified. We recommend that **SIP UDP/IX filter mode** is set to *On* for: • 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 *Off* for 9.x or later)	*Off* in Cisco Unified Communications Manager preconfigured zone profile. *On* otherwise.	Neighbor DNS

Setting	Description	Default	Zone types
SIP record route address type	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. *IP*: Uses the Expressway's IP address. *Hostname*: Uses the Expressway's **System host name** (if it is blank the IP address is used instead).	IP	Neighbor DNS
SIP Proxy-Require header strip list	A comma-separated list of option tags to search for and remove from Proxy-Require headers in SIP requests received from this zone.	None	Neighbor

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 CM, (9.x or later)	Cisco Unified CM, (8.6.1 or 8.6.2)	Cisco Unified CM (8.6 and below)	Nortel Communication Server 1000	Infrastructure device	Default
Monitor peer status	Yes	Yes	Yes	Yes	No	Yes
Call signaling routed mode	Always	Always	Always	Auto	Always	Auto
Automatically respond to H.323 searches	Off	Off	Off	Off	On	Off
Automatically respond to SIP searches	Off	Off	Off	Off	On	Off
Send empty INVITE for interworked calls	On	On	On	On	On	On
SIP parameter preservation	Off	Off	Off	Off	Off	Off
SIP poison mode	Off	Off	Off	Off	Off	Off

Setting	Cisco Unified CM, (9.x or later)	Cisco Unified CM, (8.6.1 or 8.6.2)	Cisco Unified CM (8.6 and below)	Nortel Communication Server 1000	Infrastructure device	Default
SIP encryption mode	Auto	Auto	Auto	Auto	Auto	Auto
SIP REFER mode	Forward	Forward	Forward	Forward	Forward	Forward
Meeting Server load balancing	Off	Off	Off	Off	Off	On
SIP multipart MIME strip mode	Off	Off	Off	Off	Off	Off
SIP UPDATE strip mode	Off	Off	Off	On	Off	Off
Interworking SIP search strategy	Options	Options	Options	Options	Options	Options
SIP UDP/BFCP filter mode	Off	Off	On	Off	Off	Off
SIP UDP/IX filter mode	Off	On	On	On	On	Off
SIP record route address type	IP	IP	IP	IP	IP	IP
SIP Proxy-Require header strip list	<blank>	<blank>	<blank>	com.nortel-networks.-firewall	<blank>	<blank>

More information about configuring a SIP trunk between Expressway and Unified CM:

See *Cisco Expressway and CUCM via SIP Trunk Deployment Guide* on the Expressway Configuration Guides page.

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 the Subject Alternative Name attributes of the certificate.) The certificate itself must also be valid and signed by a trusted certificate authority.

Note 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.

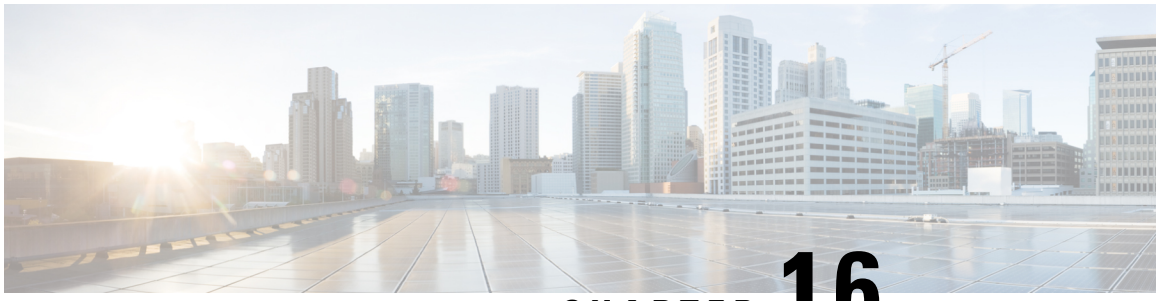
If the neighbor system is another Expressway, or it is a traversal client / traversal server relationship, the two systems can be configured to authenticate each other's certificates. This is known as mutual authentication and in this case each Expressway acts both as a client and as a server and therefore you must ensure that each Expressway's certificate is valid both as a client and as a server.

See Security Basics 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.



CHAPTER 16

Clustering and Peers

- About Clusters, on page 279
- Cluster License Usage and Capacity Guidelines, on page 281
- Managing Clusters and Peers, on page 282
- Troubleshooting Cluster Replication Problems, on page 291
- Troubleshooting System Key Related Issues, on page 292

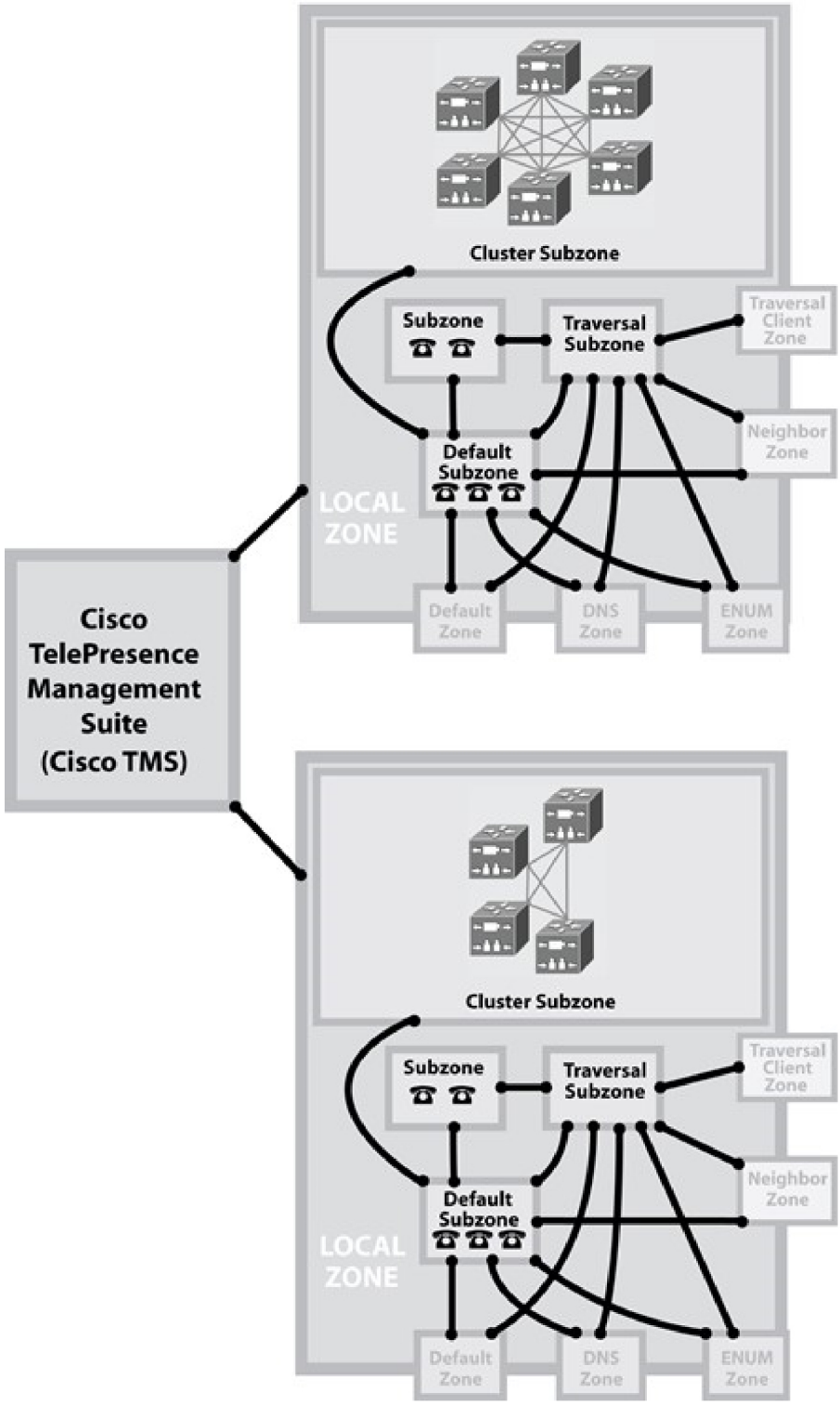
About Clusters

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 that cluster. When creating a cluster you define a cluster name and nominate one peer as the primary from which configuration is replicated to the other peers. Clusters are used for the following reasons:

- **Capacity**. Increase the capacity of your Expressway deployment compared with a single Expressway.
- **Resilience**. Provide redundancy while an Expressway is in Enable Maintenance Mode, or in the rare case that it becomes inaccessible due to a network / power outage, or some other reason.

Note There is no capacity gain after four peers. So in a six-peer cluster for example, the 5th and 6th Expressways do not add extra call capacity to the cluster. Resilience is improved with the extra peers, but not capacity.

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 this example:


Cisco TelePresence Management Suite (Cisco TMS)
Cluster Subzone
Subzone
Traversal Subzone
Traversal Client Zone
Neighbor Zone
Default Subzone
LOCAL ZONE
Default Zone
DNS Zone
ENUM Zone
Cluster Subzone
Subzone
Traversal Subzone
Traversal Client Zone
Neighbor Zone
Default Subzone
LOCAL ZONE
Default Zone
DNS Zone
ENUM Zone
454315

Cluster License Usage and Capacity Guidelines

This section describes how licenses are used across a cluster and provides capacity guidelines. For ease of reference, the capacity guidelines for standalone systems are also included here.

The maximum supported capacities / sizing for Cisco Expressway Series (not Cisco VCS) are listed in the tables below. These figures are guidelines only and are NOT guaranteed, because many factors affect performance in real-life deployments. Expressway supports so many different use cases that it is not possible to provide capacity limits for individual, specific deployments.

Expressway sizing / capacity information is categorized on the basis of the number of supported concurrent registrations and/or calls.

Important Caveats

- The figures/values provided here assume all necessary software licenses are applied.
- The figures/values are tested for specific, dedicated Expressway scenarios. Based on an Expressway or cluster being used for a single service or scenario, such as just for MRA or just for B2B calling. It is not possible to provide tested capacity guidelines for multi-service deployments.
- **N+1 Model**
  - Prior to the X14.2 release, up to 6 Expressway systems can be clustered to yield a total cluster capacity of **four times** that of a single system (except for Small VMs, which have no gain).
  - From the X14.2 release, in the 4+1 redundancy model, up to 5 Expressway systems can be clustered to yield a total cluster capacity of **four times** that of a single system (with 1 redundancy server) (except for Small VMs, which have no gain).
  - From the X14.2 release, in the 5+1 redundancy model, up to 6 Expressway systems can be clustered to yield a total cluster capacity of **five times** that of a single system (with 1 redundancy server) (except for Small VMs, which have no gain).
  - For Small VMs, clustering is only for redundancy and not for scale and **there is no capacity gain from clustering**.
- The figures/values provided for video calls and audio-only calls are alternatives - the stated capacity is available either for video or for audio, not for both.

Dependencies

The figures/values for calls refer to concurrent calls.

Concurrent calls and Rich Media Session (RMS) licenses do not have a one-to-one relationship. Various factors determine RMS license usage, which means that some calls may be “free” and others may use multiple licenses.

To support 6000 TURN relays on a large system (Large VM or CE1200) you need to enable “TURN Port Multiplexing on Large Expressway” (**Configuration** > **Traversal** > **TURN**).

Small VMs are supported on the Cisco Business Edition 6000 platform, or on general purpose hardware / ESXi which matches the Cisco Business Edition 6000 specification. The figures/values for Small VMs are for M5-based BE6000 appliances.

Capacity Guidelines for Standalone Systems

For more information, see the table in chapter "Expressway Capacity and Sizing".

Capacity Guidelines for Clustered Systems

For more information, see the table in chapter "Expressway Capacity and Sizing".

Intracluster Calls

License usage when endpoints are registered to different peers in the same cluster, depends on call media traversal across the cluster:

- If call media does not traverse the cluster peers, a call between the endpoints does not use any RMS licenses (it's a “Registered” call).
  - If any of the endpoint is not registered to Cisco infrastructure then calls will use RMS license.
- If call media does traverse the cluster peers, a call between the endpoints uses an RMS license on the Expressway where the B2BUA is engaged.
  - If both the endpoints are registered to Cisco infrastructure then call will not use RMS license.

More information about how licenses are used in clustered systems is provided in the licensing section of this guide.

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.

Basics of 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.

- You can form an Expressway cluster using an <*hostname*> as the **cluster name** instead of a Fully Qualified Domain Name (FQDN). This formation does not cause any clustering issues (no cluster-related errors). But, when creating a Certificate Signing Request (CSR) (after the cluster is created), either using the cluster name as Common Name (CN) or Subject Alternative Name (SAN), the server will fail to generate a CSR since the cluster name is not in FQDN format. Hence, make sure that you set the cluster name to FQDN format.
- 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.

For details, see the *Expressway Cluster Creation and Maintenance Deployment Guide* on the Expressway Configuration Guides page.

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.

Caution Dbxsh is a python script that connects to a cluster database on the local loopback address over port 4370. The Dbxsh does not need to authenticate the database before executing the commands. The port is open for connection and is strictly for internal use only. This is accessible from root only.

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 Items in Clustered Systems.

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. For details see the *Expressway Cluster Creation and Maintenance Deployment Guide*.

Caution If you clear all the peer address fields from the clustering page and save the configuration, then the Expressway will factory reset itself the next time you do a restart. This means you will lose all existing configuration except basic networking for the LAN1 interface, including all configuration that you do between when you clear the fields and the next restart.

Changing the Primary Peer

Typically you only need to change the **Configuration primary** in the following cases:

- If the original primary peer fails. (If the primary fails, the remaining peers continue to function normally except that, as they are unable to copy their configuration from the primary, they may become out of sync with each other.)
- To take the primary Expressway unit out of service.

For details about how to change the primary peer, see the *Expressway Cluster Creation and Maintenance Deployment Guide*.

Monitoring Cluster Status

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.

Troubleshooting Cluster Problems

See Troubleshooting Cluster Replication Problems.

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 S on the web interface) must be specified separately on each cluster peer.

Configuration data that applies to all peers should only be modified on the primary peer. Otherwise, at best the changes will be overwritten from the primary or at worst the cluster replication will fail.

Service setup wizard

Configuration settings made through the service setup wizard (including Select Type, Select Series, service selection, licensing for those services, and basic network settings) must be configured on each peer in a cluster.

Cluster configuration (System > Clustering)

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

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

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

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 unique IP address, whether that is an **IPv4 address**, an **IPv6 address**, or both.
- **IP gateway** configuration is peer-specific. Each peer can use a different gateway.

Note 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.

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)

This section only applies to systems that use PAK-based licensing (option keys do not apply if your system uses Smart Licensing). Option keys can control licensing or specific features. They are gradually being phased out for Expressway and their use is diminishing.

Option keys that control **licenses** are pooled for use by the whole cluster.

Option keys that control **features** (such as advanced account security or Microsoft Interoperability) are specific to the peer where they are applied. Each peer must have an identical set of feature option keys installed, which means that if you use option keys for features 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:

- Rich media sessions
- Telepresence room systems
- Desktop systems

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.

Conference Factory template (Applications > Conference Factory)

The template used by the Conference Factory application to route calls to a conferencing server must be unique for each peer in the cluster.

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.

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 About 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 Backing Up and Restoring Expressway Data 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 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 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.

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 Even if the Cluster License Usage and Capacity Guidelines of your system is greater, you are 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 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 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. The remote cluster might be a neighbor, traversal client, or traversal server to the local system. When a call is received on the local Expressway and is passed via the relevant zone to the remote cluster, it gets routed to whichever peer in that neighbor cluster has the lowest resource usage (peers in maintenance mode are not considered). That peer then forwards the call to one of the following:

- A locally registered endpoint, if the endpoint is registered to that peer.
- A peer, if the endpoint is registered to another peer in the cluster.
- An external zone, if the endpoint is located elsewhere.

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.

Expressways that are configured as peers **must not also be configured as neighbors** to each other, or the other way round.

Process to Neighbor Clusters

You create a single zone on the local system to represent the connection to the remote cluster, and configure it with the details of all the peers in the remote cluster. Adding this information to the zone ensures that the call is passed to that cluster regardless of the status of the individual peers.

1. On the local Expressway (or on the primary peer for a cluster), create a zone of the appropriate type.
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. You do not do this for **traversal server** zones, as these connections are not configured by specifying the remote system's address.

   Ideally, 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.

Note Whenever you add an extra Expressway to a cluster, you need to modify any Expressways which neighbor to that cluster to let them know about the new 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
- 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.

"Cluster config error" alarms are raised on Expressway peer

You can specify a new configuration primary on the clustering page as per the description of the alarm raised.

Note You can revert to the old configuration primary once all the replication alarms are lowered.

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.

Troubleshooting System Key Related Issues

This section describes the most common problems related to system key and how to resolve them.

Regeneration of system key during upgrade

Below error is commonly seen for upgrades prior to X14.0 whenever there are issues concerning systemkey.

```
Post install script /tandberg/etc/postinstall.current.d/10-verify-syskey failed
```

However, it is a known issue. This is fixed in X14.0 and its subsequent versions.

1. Do not proceed any further with any upgrade operations.
2. SSH as *root*, Execute `/sbin/verify-skey` to establish encrypted entry(ies) that cannot be decrypted.
3. If possible, try to discover when and why it was incorrectly written and/or is incorrectly (re)written.

Workaround

1. Go to the User Interface and Overwrite the existing (bad) entry with a clean encrypted new entry.
2. Execute `/sbin/verify-skey` again to confirm that it is now clean.

Note Users will not encounter these issues post a successful upgrade to versions X14.0 and higher versions.

"Failed to update key file" alarms are raised on Expressways (Single node scenario)

1. Log in as admin through the CLI (available by default over SSH and through the serial port on hardware versions).

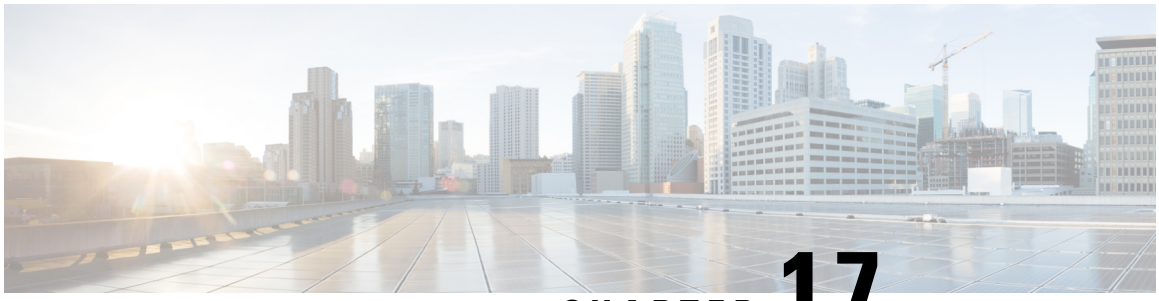
2. Type **xCommand ForceSystemKeyUpdate**.

"Failed to update key file" alarms are raised on Expressways (Cluster scenario)

1. Log in to node as admin through the CLI (available by default over SSH and through the serial port on hardware versions) where this alarm is not raised.
2. Type **xCommand ForceSystemKeyUpdate**.

Note

- Make sure to address "Failed to update key file" alarm before adding the node to a cluster.
- Cluster needs to be recreated if "Failed to update key file" alarm is raised on all the Expressway nodes of a cluster.



CHAPTER 17

Dial Plan and Call Processing

- Call Routing Process, on page 295
- About Cisco VCS's Directory Service, on page 297
- Configuring Hop Counts, on page 297
- Configuring Dial Plan Settings, on page 298
- About Transforms and Search Rules, on page 300
- Example Searches and Transforms, on page 307
- Direct 9-1-1 Calls for Kari's Law (with Expressway as Call Control and a PSTN Gateway), on page 318
- Configuring Search Rules to Use an External Service, on page 323
- About Call Policy, on page 326
- Supported Address Formats, on page 333
- Dialing by IP Address, on page 334
- About URI Dialing, on page 336
- About ENUM Dialing, on page 344
- Configuring DNS Servers for ENUM and URI Dialing, on page 350
- Configuring Call Routing and Signaling, on page 351
- Identifying Calls, on page 352
- Disconnecting Calls, on page 353

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

Several steps are 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's important to understand the process before setting up your Structuring the 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.

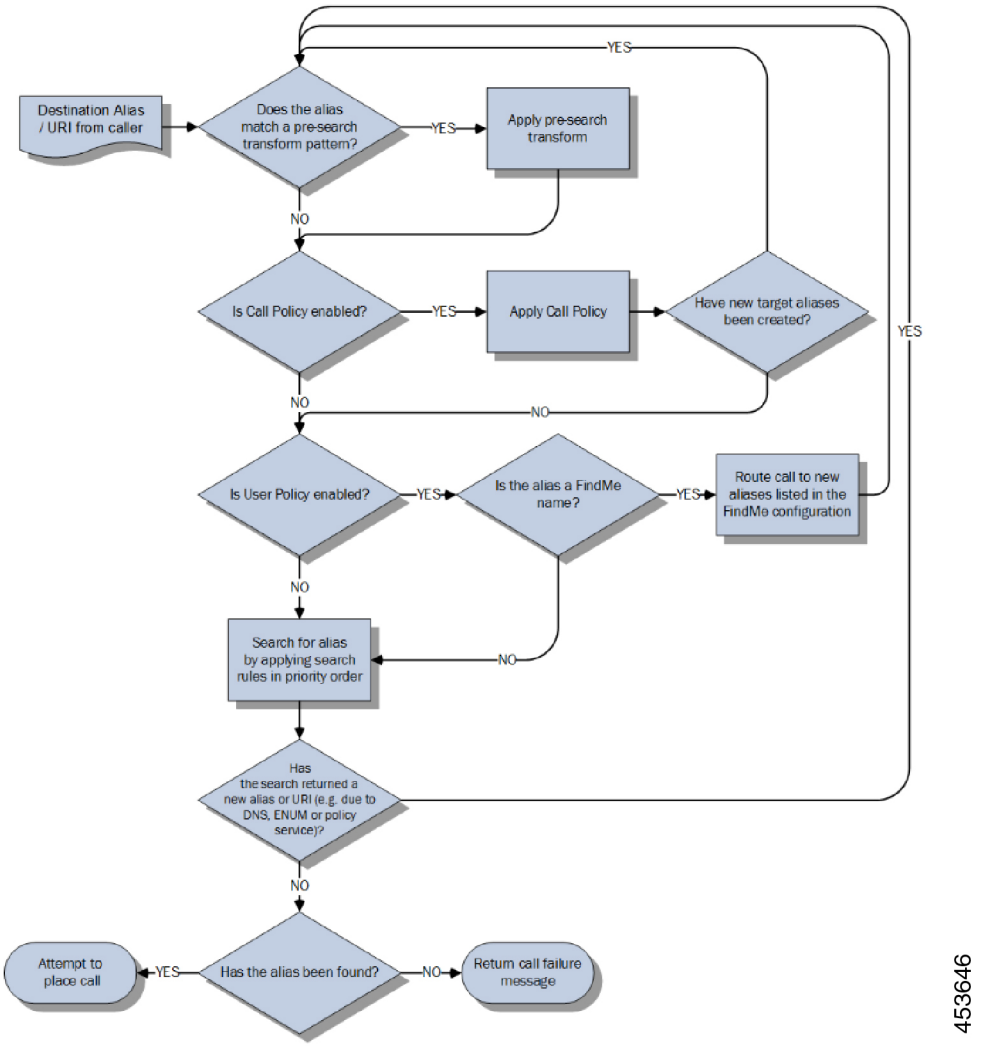
1. The caller enters into their endpoint the alias or address of the destination endpoint. This alias or address can be in a number of Supported Address Formats.
2. The destination address is received by the Expressway.

   (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 About Pre-Search Transforms are applied to the alias.
4. Any Configuring 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 About 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 18: Call Routing Flowchart



About Cisco VCS's Directory Service

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 Configuring Call Routing and Signaling 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.

Important The default hop count may be too low for your environment if you have a complex network. This can cause unexpected call failures in a correctly configured deployment. Consider raising the hop count if you anticipate long call paths.

For full details on other zone options, see the Configuring Zones (Non-Default Zones) section.

Step 1 Go to the **Zones** page (**Configuration** > **Zones** > **Zones**).

Step 2 Click on the name of the zone you want to configure. You are taken to the **Edit zone** page.

Step 3 In the **Configuration** section, in the **Hop count** field, enter the hop count value you want to use for this zone.

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	Determines the way in which the Expressway attempts to call systems which are not registered with it or one of its neighbors. *Direct*: Allows an endpoint to make a call to an unknown IP address without the Expressway querying any neighbors. The call setup would occur just as it would if the far end were registered directly to the local system. *Indirect*: Upon receiving a call to an unknown IP address, the Expressway will query its neighbors for the remote address and if permitted will route the call through the neighbor. *Off*: Endpoints registered directly to the Expressway may only call an IP address of a system also registered directly to that Expressway. The default 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. In addition to controlling calls, this setting also determines the behavior of provisioning and presence messages to SIP devices, as these messages are routed to IP addresses. See Dialing by IP Address for more information.
Fallback alias	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.	If no fallback alias is configured, calls that do not specify an alias will be disconnected. See below for more information.

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 Some endpoints do not allow users to enter an alias and an IP address to which the call should be placed.

Example usage

You may want to configure your fallback alias to be that of your receptionist, so that all calls that do not specify an alias are still answered personally and can then be redirected appropriately.

For example, Example Inc has the domain of **example.com**. The endpoint at reception has the alias **reception@example.com**. They configure their Expressway with a fallback alias of **reception@example.com**.

This means that any calls made directly to **example.com** (that is, without being prefixed by an alias), are forwarded to **reception@example.com**, where the receptionist can answer the call and direct it appropriately.

About Transforms and Search Rules

The Expressway can be configured to use transforms and search rules as a part of its call routing process.

Transforms

Transforms are used to modify the alias in a search request if it matches certain criteria. You can transform an alias by removing or replacing its prefix, suffix, or the entire string, and by the use of regular expressions.

This transformation can be applied to the alias at two points in the routing process: as a pre-search transform, and as a zone transform.

- **Pre-search transforms** are applied before any Call Policy or User Policy are applied and before the search process is performed (see About Pre-Search Transforms 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 Transformation Process 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 Authentication Policy only.
- Use zone transforms to modify an alias before the query is sent to a target zone or policy service.

Note 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.

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.

Note Only one transform can be matched per search.

Clustered systems

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.

When does a transform apply?

- Applied to all incoming search requests received from locally registered endpoints, neighbor, traversal client and traversal server zones, and endpoints on the public internet.
- Not applied to requests received from peers. These are configured identically and therefore will have already applied the same transform.
- Not applied to GRQ or RRQ messages received from endpoints registering with the Expressway. The endpoints will be registered with the aliases as presented in these messages.

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.

1. 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 (only one transform can be matched per search). The new alias is used for the remainder of the **call routing process**.
2. 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 - have their priority incremented by one, and the new transform is added with the specified priority. Or an error message is issued if there are insufficient "slots" to move all the priorities down.

Configuring Pre-Search Transforms

The **Transforms** page (**Configuration** > **Dial plan** > **Transforms**) lists all the About 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 Transforms also apply to any Mobile and Remote Access Overview 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: *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*: Treats the string as a Regular Expressions.	You can test whether a pattern matches a particular alias and is transformed in the expected way by using the Checking the Effect of 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.

Field	Description	Usage tips
Pattern behavior	Specifies how the matched part of the alias is modified. Options are: *Strip*: The matching prefix or suffix is removed. *Replace*: The matching part of the alias is substituted with the text in the Replace string. *Add Prefix*: Prepends the **Additional text** to the alias. *Add Suffix*: 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 *Replace*. You can use regular expressions.
Additional text	The string to add as a prefix or suffix.	Only applies if the **Pattern behavior** is *Add Prefix* or *Add Suffix*.
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 Transformation Process

The search rules and zone transform process is applied after all About Pre-Search Transforms, About Call Policy and About FindMe 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 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 Configuring SIP and H.323 Interworking.
- 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 starts again

4. If the alias is not found, the search rules with the next highest priority are applied (go back to step 1) until:
   - The alias is found, or
   - All target zones and policy services associated with search rules that meet the specified criteria have been queried, or
   - A search rule with a successful match has an **On successful match** setting of *Stop searching*.

Note The difference between a successful match (where the alias matches the search rule criteria) and an alias being found (where a query sent to a target zone is successful). The *Stop searching* option provides better control over the network's signaling infrastructure. For example, if searches for a particular domain should always be routed to a specific zone this option lets you make the search process more efficient and stop the Expressway from searching any other zones unnecessarily.

Configuring Search Rules

The **Search rules** page (**Configuration** > **Dial plan** > **Search rules**) is used to configure how the Expressway routes incoming search requests to the appropriate target zones (including the Local Zone) or policy services.

The page lists all the currently configured search rules and lets you create, edit, delete, enable and disable rules. You can click on a column heading to sort the list, for example by **Target** or **Priority**. If you hover your mouse pointer over a search rule, the rule description (if one has been defined) appears as a tooltip.

You can also copy and then edit any existing search rule by clicking **Clone** in the **Actions** column.

Up to 2000 search rules can be configured. Priority 1 search rules are applied first, followed by all priority 2 search rules, and so on.

The configurable options are:

Field	Description	Usage tips
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.

Field	Description	Usage tips
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 *Any*, *H.323* or *SIP*.	
Traffic type	The source traffic type for which this rule applies. Options are: *Any*: The rule does not inspect the traffic type. *Standard*: The rule applies if the traffic is standards-based SIP. *Any Microsoft*: The rule applies if the traffic is Microsoft SIP or Microsoft SIP-SIMPLE. *Microsoft SIP*: The rule applies if the traffic is Microsoft SIP. *Microsoft IM and Presence*: The rule applies if the traffic is Microsoft SIP-SIMPLE.	This option helps you route different types of calls to the infrastructure most suited to processing them. 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.
Source	The sources of the requests for which this rule applies. *Any*: Locally registered devices, neighbor or traversal zones, and any non-registered devices. *All zones*: Locally registered devices plus neighbor or traversal zones. *Local Zone*: Locally registered devices only. *Named*: A specific source zone or subzone for which the rule applies.	Named sources creates the ability for search rules to be applied as dial plan policy for specific subzones and zones.
Source name	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.	Only applies if the **Source** is set to *Named*.
Request must be authenticated	Specifies whether the search rule applies only to authenticated search requests.	This can be used in conjunction with the Expressway's Authentication Policy to limit the set of services available to unauthenticated devices.

Field	Description	Usage tips
Mode	The method used to test if the alias applies to the search rule. *Alias pattern match*: The alias must match the specified **Pattern type** and **Pattern string**. *Any alias*: Any alias (providing it is not an IP address) is allowed. *Any IP Address*: The alias must be an IP address.	
Pattern type	How the **Pattern string** must match the alias for the rule to be applied. Options are: *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*: Treats the string as a Regular Expressions.	Applies only if the **Mode** is *Alias Pattern Match*. You can test whether a pattern matches a particular alias and is transformed in the expected way by using the Checking the Effect of Pattern tool (**Maintenance** > **Tools** > **Check pattern**).
Pattern string	The pattern against which the alias is compared.	Applies only if the **Mode** is *Alias Pattern Match*. 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 *Leave*: The alias is not modified. *Strip*: The matching prefix or suffix is removed from the alias. *Replace*: The matching part of the alias is substituted with the text in the **Replace string**.	Applies only if the **Mode** is *Alias Pattern Match*. If you want to transform the alias before applying search rules you must use About 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 *Replace*. You can use regular expressions.

Field	Description	Usage tips
On successful match	Controls the ongoing search behavior if the alias matches the search rule. *Continue*: Continue applying the remaining search rules (in priority order) until the endpoint identified by the alias is found. *Stop*: Do not apply any more search rules, even if the endpoint identified by the alias is not found in the target zone.	If *Stop* 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 Configuring Search Rules to Use an External Service 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 Locating an Alias tool (**Maintenance** > **Tools** > **Locate**).
- You can test whether a pattern matches a particular alias and is transformed in the expected way by using the Checking the Effect of 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 Without Transforming

You can filter the search requests sent to a zone so that it is only queried for aliases that match certain criteria. For example, assume all endpoints in your regional sales office are registered to their local Cisco VCS with a suffix of **@sales.example.com**. In this situation, it makes sense for your Head Office Expressway to query the Sales Office VCS only when it receives a search request for an alias with a suffix of **@sales.example.com**. Sending any other search requests to this particular VCS would take up resources unnecessarily. It would also be wasteful of resources to send search requests for aliases that match this pattern to any other zone (there may be other lower priority search rules defined that would also apply to these aliases). In which case setting **On successful match** to *Stop* means that the Expressway will not apply any further (lower priority) search rules.

To achieve the example described above, on your Head Office Expressway create a zone to represent the Sales Office VCS, and from the **Create search rule** page (**Configuration** > **Dial plan** > **Search rules** > **New**) set up an associated search rule as follows:

Field	Value
Rule name	Regional sales office
Description	Calls to aliases with a suffix of @sales.example.com
Priority	100
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Suffix
Pattern string	@sales.example.com
Pattern behavior	Leave
On successful match	Stop
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

Field	Value
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 *Any alias* mode does not support alias transforms. If you want to always query a zone using a different alias to that received, you need to use a mode of *Alias pattern match* in combination with a regular expression.

You may want to configure your dial plan so that when a user dials an alias in the format **name@example.com** the Expressway queries the zone for **name@example.co.uk** instead.

To achieve this, from the **Create search rule** page (**Configuration** > **Dial plan** > **Search rules** > **New**) set up a search rule as follows:

Field	Value
Rule name	Transform to example.co.uk
Description	Transform example.com to example.co.uk
Priority	100
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Suffix
Pattern string	example.com
Pattern behavior	Replace
Replace string	example.co.uk
On successful match	Continue

Field	Value
Target zone	Head office
State	Enabled

Query a Zone for Original and Transformed Aliases

You may want to query a zone for the original alias at the same time as you query it for a transformed alias. To do this, configure one search rule with a **Mode** of *Any alias*, and a second search rule with a **Mode** of *Alias pattern match* along with details of the transform to be applied. Both searches must be given the same **Priority** level.

For example, you may want to query a neighbor zone for both a full URI and just the name (the URI with the domain removed). To achieve this, on your local Expressway from the **Create search rule** page (**Configuration** > **Dial plan** > **Search rules** > **New**) set up two search rules as follows:

Rule #1

Field	Value
Rule name	Overseas office - original alias
Description	Query overseas office with the original alias
Priority	100
Source	Any
Request must be authenticated	No
Mode	Any alias
On successful match	Continue
Target zone	Overseas office
State	Enabled

Rule #2

Field	Value
Rule name	Overseas office - strip domain
Description	Query overseas office with domain removed
Priority	100
Source	Any

Field	Value
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Suffix
Pattern string	@example.com
Pattern behavior	Strip
On successful match	Continue
Target zone	Overseas office
State	Enabled

Query a Zone for Two or More Transformed Aliases

Zones are queried in order of priority of the search rules configured against them.

It is possible to configure multiple search rules for the same zone each with, for example, the same **Priority** and an identical **Pattern string** to be matched, but with different replacement patterns. In this situation, the Expressway queries that zone for each of the new aliases simultaneously. (Any duplicate aliases produced by the transforms are removed prior to the search requests being sent out.) If any of the new aliases are found by that zone, the call is forwarded to the zone. It is then up to the controlling system to determine the alias to which the call will be forwarded.

For example, you may want to configure your dial plan so that when a user dials an alias in the format **name@example.com**. the Expressway queries the zone simultaneously for both **name@example.co.uk** and **name@example.net**.

To achieve this, from the **Create search rule** page (**Configuration** > **Dial plan** > **Search rules** > **New**) set up two search rules as follows:

Rule #1

Field	Value
Rule name	Transform to example.co.uk
Description	Transform example.com to example.co.uk
Priority	100
Source	Any
Request must be authenticated	No
Mode	Alias pattern match

Field	Value
Pattern type	Suffix
Pattern string	example.com
Pattern behavior	Replace
Replace string	example.co.uk
On successful match	Continue
Target zone	Head office
State	Enabled

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+)
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

Field	Value
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
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 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

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

Field	Value
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

Field	Value
On successful match	Stop
Target	Cisco Meeting Server
State	Enabled

Direct 9-1-1 Calls for Kari's Law (with Expressway as Call Control and a PSTN Gateway)

This section provides recommendations for configuring a dial plan to support direct 9-1-1 emergency calling through Cisco Expressway. “Kari's Law”, mandated by the Federal Communications Commission, requires multi-line telephone systems (MLTS) to support **direct** 911 calls in the United States. That is, so the person making the emergency call does not also need to dial a prefix or other additional digits.

Note Expressway supports 933 and 988 calls without consuming Rich media session (RMS) licenses. This is similar to 911 calls.

- *933 number*: 933 service is used to test E911 call flow. When an end user dials 933, it will play back the phone number and address stored in the E911 database.
- *988 number*: 988 service is used to Route calls to Suicide Prevention Hotline without RMS licenses.

When Does Kari's Law Apply to Expressway?

Kari’s Law deals with audio calls. This law applies to Expressway deployments **in the United States** in cases where all of the following conditions apply:

- Expressway is managing the call control and the endpoint making the emergency call is directly registered to the Expressway-C.
- A gateway is configured with Expressway that enables PSTN calling.
- The PSTN calling capabilities for your deployment include 911 emergency calls.
- The endpoint involved is capable of dialing a PSTN number and making a basic audio call.

Before You Begin

- You need Cisco Expressway version X12.5.7 or later.
- You should have knowledge of the North American Numbering Plan (NANP).
- From X12.5.7, the usual requirement to have at least one RMS license installed before a call can be placed does not apply to direct 911 calls.
- To minimize toll fraud risks, avoid using the “Any” wild card for the Source setting.

- The PSTN gateway also needs to be configured to route 911 calls without a prefix.
- For deployments that are geographically spread with the gateway in a different location from the endpoints, keep in mind the practical routing requirements for 911 calls and the possibility that callers may be connected to an emergency agent in a different place from their own location.

Configuring the Search Rules

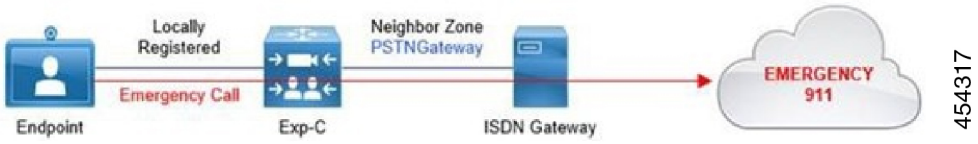
On the **Create search rule** page (**Configuration** > **Dial plan** > **Search rules** > **New**) create the necessary search rules. This section provides examples for these deployment types:

1. Standalone PSTN gateway (no redundancy).
2. Multiple PSTN gateways.

Example 1: Search Rules for a Standalone Gateway

These example rules assume the following:

- An ISDN gateway for PSTN calling is configured on Expressway as a neighbor zone (named "PSTNGateway").
- 911 emergency calls are only allowed from SIP user agents or H.323 endpoints registered locally to the Expressway-C.



Example 1, Rule #1

Field	Value
Rule name	Emergency Call - 911
Description	Route the 911 emergency call via PSTNGateway
Priority	1
Protocol	Any
Source	Local Zone
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex

Field	Value
Pattern string	911|(911@%localdomains%)
Pattern behavior	Leave
On successful match	Stop
Target zone	PSTNGateway
State	Enable

Example 1, Rule #2

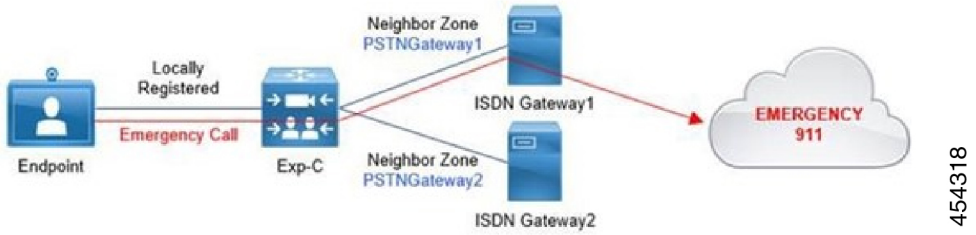
Field	Value
Rule name	Emergency Call - 911 with Prefix 00
Description	Route the 911 emergency call via PSTNGateway
Priority	2
Protocol	Any
Source	Local Zone
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	00(911|911@%localdomains%)
Pattern behavior	Replace
Replace string	\1
On successful match	Stop
Target zone	PSTNGateway
State	Enable

Example 2: Search Rules for Multiple Gateways

These example rules assume the following:

- Two ISDN gateways for PSTN calling, are available in the live network for redundancy.
- Each gateway is configured on Expressway as a neighbor zone (named “PSTNGateway1” and “PSTNGateway2”).

- 911 emergency calls are only allowed from SIP user agents or H.323 endpoints registered locally to the Expressway-C.



Here the rules specify *On successful match* = “Continue” for the primary gateway and *On successful match* = “Stop” for the .backup one.

Example 2, Rule #1

Field	Value
Rule name	Emergency Call - 911 via PSTNGateway1
Description	Route the 911 emergency call via PSTNGateway
Priority	1
Protocol	Any
Source	Local Zone
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	911|(911@%localdomains%)
Pattern behavior	Leave
On successful match	Continue
Target zone	PSTNGateway1
State	Enable

Example 2, Rule #2

Field	Value
Rule name	Emergency Call - 911 via PSTNGateway2

Field	Value
Description	Route the 911 emergency call via PSTNGateway
Priority	2
Protocol	Any
Source	Local Zone
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	911|(911@%localdomains%)
Pattern behavior	Leave
On successful match	Stop
Target zone	PSTNGateway2
State	Enable

Example 2, Rule #3

Field	Value
Rule name	Emergency Call - 911 with Prefix 00 via PSTNGateway1
Description	Route the 911 emergency call via PSTNGateway
Priority	3
Protocol	Any
Source	Local Zone
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	00(911|911@%localdomains%)
Pattern behavior	Replace
Replace string	\1
On successful match	Continue

Field	Value
Target zone	PSTNGateway1
State	Enable

Example 2, Rule #4

Field	Value
Rule name	Emergency Call - 911 with Prefix 00 via PSTNGateway2
Description	Route the 911 emergency call via PSTNGateway
Priority	4
Protocol	Any
Source	Local Zone
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	00(911|911@%localdomains%)
Pattern behavior	Replace
Replace string	\1
On successful match	Stop
Target zone	PSTNGateway2
State	Enable

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

Step 1 Go to **Configuration** > **Dial plan** > **Policy services**.

Step 2 Click **New**.

Step 3 Configure the server address and connection protocols in the same manner as for Call Policy.

Step 4 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 *HTTPS*.	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 *On*, 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 **:<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 *status*.	The policy server must supply return status information, see Policy Server Status and Resiliency.

Field	Description	Usage tips
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.

Step 5 Click **Create policy service**.

Configuring a Search Rule to Direct a Search to the Policy Service

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.

Step 1 Go to **Configuration** > **Dial plan** > **Search rules**.

Step 2 Click **New**.

Step 3 Configure the fields on the **Create search rule** page as appropriate for the searches you want to direct to the external policy server.

This example shows how to divert calls to aliases ending in .meet to the external policy server:

Field	Value
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 *Any*.
Source	As required, for example *Any*.
Request must be authenticated	Configure this setting according to your authentication policy.
Mode	As required, for example *Alias pattern match*.
Pattern type	As required, for example *Regex*.
Pattern string	As required, for example.*\.meet@example.com

Field	Value
Pattern behavior	As required, for example *Leave*.
On successful match	As required. **Note** If Stop 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	*Enabled*

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*.

Step 4 Click **Create search rule**.

About Call Policy

You can set up rules to control which calls are allowed, which calls are rejected, and which calls are to be redirected to a different destination. These rules are known as Call Policy (or Administrator Policy).

If Call Policy is enabled and has been configured, each time a call is made the Expressway will execute the policy in order to decide, based on the source and destination of the call, whether to:

- Proxy the call to its original destination.
- Redirect the call to a different destination or set of destinations.
- Reject the call.

Note When enabled, Call Policy is executed for all calls going through the Expressway.

You should:

- Use Call Policy to determine which callers can make or receive calls via the Expressway
- Use About Allow and Deny Lists 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 About 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:

- Configuring Call Policy Rules Using the Web Interface through the **Call Policy rules** page (**Configuration** > **Call Policy** > **Rules**) or

Note This only lets you allow or reject specified calls.

- Configuring Call Policy Using a CPL Script 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.

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:

Field	Description	Usage tips
Source type	This field lets you choose from two types of call source: *Zone* or *From address*. 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 *Zone*. 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 *From address*. The field lets you choose whether the rule inspects calls from *Authenticated callers* or *Unauthenticated callers*. Authenticated callers are devices that are: • 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 for more information.
Source pattern	Visible for rules with **Source type** set to *From address*. 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.

Field	Description	Usage tips
Action	Defines what the rule does when a call it has inspected matches what you specified for the source and destination. You can choose *Allow* or *Reject*. *Allow*: 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. *Reject*: 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.	
Rearrange	This field is only visible in the list of call policy rules (on the **Call Policy rules** page). You can click the ↑ and ↓ icons to change the order of the rules, which changes their relative priority.	Each rule is compared with the details of the incoming call in top-down order until a rule matches the call. When a rule matches, the rule's action is applied to the call.

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 External Policy Overview instead.

For information on the CPL syntax and commands that are supported by the Expressway, see the CPL Reference section.

Viewing existing CPL script

To view the Call Policy that is currently in place as an XML-based CPL script, go to the Configuring Call Policy 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

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. To upload a new CPL file:

Step 1 Go to **Configuration** > **Call Policy** > **Configuration**.

Step 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.

Step 3 Click **Upload file**.

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:

Step 1 Go to **Configuration** > **Call policy** > **Configuration**.

Step 2 Select a **Call Policy mode** of *Policy service*.

Step 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 *HTTPS*.	The Expressway automatically supports HTTP to HTTPS redirection when communicating with the policy service server.

Field	Description	Usage tips
Certificate verification mode	When connecting over HTTPS, this setting controls whether the certificate presented by the policy server is verified. If *On*, 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 **:<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 *status*.	The policy server must supply return status information, see Policy Server Status and Resiliency.
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.

Step 4 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 *HTTPS*.	The Expressway automatically supports HTTP to HTTPS redirection when communicating with the policy service server.

Field	Description	Usage tips
Certificate verification mode	When connecting over HTTPS, this setting controls whether the certificate presented by the policy server is verified. If *On*, 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 **:<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 *status*.	The policy server must supply return status information, see Policy Server Status and Resiliency.
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.

Step 5 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 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 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 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 Call Routing 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.

Full instructions on how to configure the Expressway to support URI dialing via DNS (both outbound and inbound) are given in the About 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 About 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 known IP addresses

Expressway considers an IP address to be “known” if the IP address is a locally registered endpoint or it falls within the IP address range of one of the subzone membership rules configured on the Expressway.

SIP user agents (and H.323 endpoints) register with either the Default Subzone or a customized Subzone based on membership rules, and interworking timing is different depending on the call flow.

The SIP IP dialing is always treated as UDP and the expected behavior on Expressway. Expressway servers is as follows:

1. Call from Default Subzone to Custom Subzone1 -> Proceed SIP-to-SIP native call ─ if the unit registered on Subzone1 is not registered as SIP UDP, experience delay until server performs interworking as native protocol fails.
2. Call from Subzone1 to Default Subzone -> Fallback SIP-to-H.323 Interworking Call immediately.
3. Call from Subzone1 to Subzone1 -> Proceed SIP-to-SIP native call ─ if the unit registered on Subzone1 is not registered as SIP UDP, experience delay until server performs interworking as native protocol fails.
4. Call from Subzone1 to Subzone2 -> Proceed SIP-to-SIP native call ─ if the unit registered on Subzone2 is not registered as SIP UDP, experience delay until server performs interworking as native protocol fails.
5. Call from Default Subzone to Default Subzone -> Fallback SIP-to-H.323 Interworking Call immediately.

Calls to unknown IP addresses

Although the Expressway supports dialing by IP address, it is sometimes undesirable for the Expressway 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 Configuring Dial Plan Settings page) configures how the Expressway handles calls to IP addresses which are not on its local network, or registered with it or one of its neighbors.

Expressway always attempts to place calls to known IP addresses (provided 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. This is the default setting.
- *Off*: The Expressway will not attempt to place the call, either directly or indirectly to any of its neighbors.

This setting applies to the call's destination address before any zone transforms, but after any pre-search transforms, Call Policy or User Policy rules are applied.

Note As well as controlling calls, this setting also determines the behavior of provisioning and presence 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:

- Dialing its URI. The local Expressway must be configured to support URI dialing, and a DNS record must exist for that URI, which resolves to the unregistered endpoint's IP address.
- 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 goes 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 does not place the call directly. Instead, it queries its neighbor

Expressway-E to see if that system is able to place the call on the Expressway-C's behalf. You must 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 Transformation 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.

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 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 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 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 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 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.

- 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 LRQ 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 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 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 Configuring 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
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 Using 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:

Step 1 Go to **Configuration** > **Zones** > **Zones**.

Step 2 Click **New**. You are taken to the **Create zone** page.

Step 3 Enter a **Name** for the zone and select a **Type** of *DNS*.

Step 4 Configure the DNS zone settings as follows:

Field	Guidelines
Hop count	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). 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).
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	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. You are recommended to use the default setting of *Off*, 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 *On*, 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.
Zone profile	For most deployments, this option should be left as *Default*.

Step 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:

- Configuring DNS Servers for ENUM and URI Dialing 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:

- 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:

- SRV record for **_h323ls._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 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 About Pre-Search Transforms 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 (see the DNS Configuration Examples 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 via DNS for Outgoing Calls.

Note 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 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 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 Configuring Zones and Search Rules for ENUM Dialing 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 Configuring DNS Servers for ENUM and URI Dialing 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 via DNS for Outgoing Calls. 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 Configuring 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:
     a. The digits are reversed and separated by a dot.
     b. 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 About 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 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

Note
- 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 Configuring DNS Servers for ENUM and URI Dialing to be used when searching for NAPTR records.

To set up an ENUM zone:

Step 1 Go to **Configuration** > **Zones** > **Zones**.
Step 2 Click **New**. You are taken to the **Create zone** page.
Step 3 Enter a **Name** for the zone and select a **Type** of *ENUM*.
Step 4 Configure the ENUM zone settings as follows:

Field	Guidelines
Hop count	The Configuring Hop Counts 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.

Step 5 Click **Create zone**.

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 Transformation Process 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 Locating an Alias (**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 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:

Step 1 Go to the **DNS** page (**System** > **DNS**).

Step 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.
- *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 Configuring 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 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 Configure Logging 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 Configuring Call Routing and Signaling 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

Note 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.

To disconnect one or more existing calls using the web interface:

Step 1 Go to the **Calls** page (**Status** > **Calls**).

Step 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.

Step 3 Select the box next to the calls you want to terminate and click **Disconnect**.

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). 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 When disconnecting a call, only the call with that Call Serial Number is disconnected. Other calls with the same Call Tag but a different Call Serial Number may not be affected.

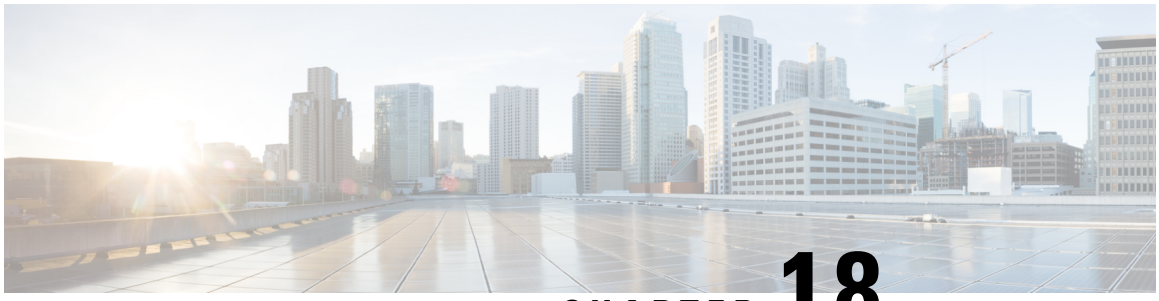
Limitations when disconnecting SIP calls

Call disconnection works differently for H.323 and SIP calls due to differences in the way the protocols work.

For H.323 calls, and interworked calls, the **Disconnect** command actually disconnects the call.

For SIP calls, the **Disconnect** command causes the Expressway to release all resources used for the call; the call will appear as disconnected on the Expressway. However, endpoints will still consider themselves to be in the call. SIP calls are peer-to-peer, and as the Expressway is a SIP proxy it has no authority over the endpoints. Releasing the resources on the Expressway means that the next time there is any signaling from the endpoint to the Expressway, the Expressway will respond with a "481 Call/Transaction Does Not Exist" causing the endpoint to clear the call.

Note 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.



CHAPTER 18

Bandwidth Control

- About Bandwidth Control, on page 355
- Configuring Bandwidth Controls, on page 356
- About Subzones, on page 357
- Links and Pipes, on page 365
- Bandwidth Control Examples, on page 368

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 Configuring Links and Configuring 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**.

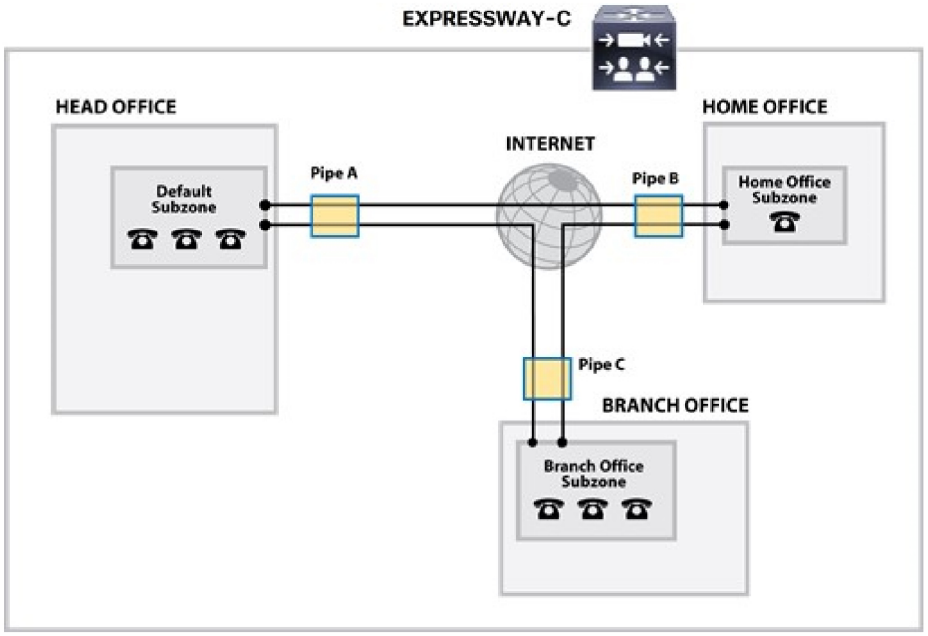
For specific information about how bandwidth is managed across peers in a cluster, see Sharing Bandwidth Across Peers.

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)	The bandwidth to use for calls for which no bandwidth value has been specified by the system that initiated the call. It also defines the minimum bandwidth to use on SIP to H.323 interworked calls. This value cannot be blank. The default value is 384kbps.	Usually, when a call is initiated the endpoint will include in the request the amount of bandwidth it wants to use.

Field	Description	Usage tips
Downspeed per call mode	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. *On*: The call will be downspeeded. *Off*: The call will not be placed.	
Downspeed total mode	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. *On*: The call will be downspeeded. *Off*: The call will not be placed.	

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 Configuring Subzone Membership Rules based on endpoint IP address ranges or alias pattern matches.

You can create and configure subzones through the Configuring 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 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 75 concurrent traversal calls on a small system (M5-based), 100 on a medium system, or 500 on a large system. The default range is thus 48*500 = 24000 ports.

If you want to reduce the range, be aware that Expressway raises 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?

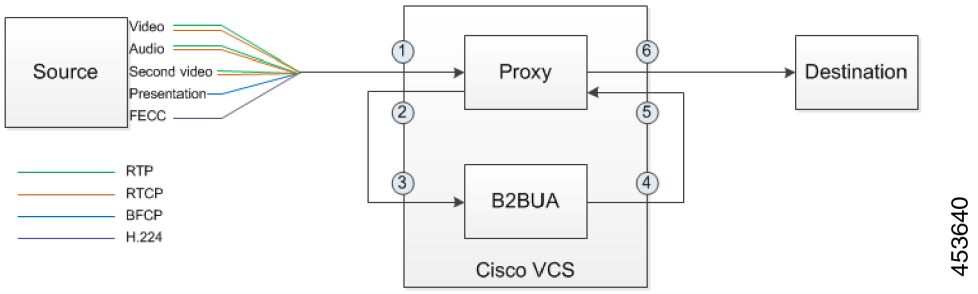
The nominal maximum number of ports allocated per call = max number of ports per allocation * max number of allocation instances. This is 8 * 6 = 48, and those numbers are derived as follows:

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 19: Maximum port allocation for a media traversal call



In practice, you probably won't reach the maximum number of concurrent traversal calls, have them all routed through the B2BUA, and have all the possible types of media in every call. However, we defined the default range to accommodate this extreme case, and the Expressway raises an alarm if the total port requirement *could* exceed the port range you specify.

What is the default range?

The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at **Configuration** > **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 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 Configuring Subzones.

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 Configuring 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 Configuring the Default Subzone.

The configurable options are:

Field / section	Description
Registration policy	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. In addition to using a About Registrations 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. This provides additional flexibility when defining your registration policy. For example you can: • 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. **Note** Registration requests have to fulfill any registration restriction policy rules before any subzone membership and subzone registration policy rules are applied.
Authentication policy	The **Authentication policy** setting controls how the Expressway challenges incoming messages to the Default Subzone. See Authentication Policy for more information.
Media encryption mode	The **Media encryption mode** setting controls the media encryption capabilities for SIP calls flowing through the subzone. See Configuring Media Encryption Policy for more information. **Note** If H.323 is enabled and the subzone has a media encryption mode of *Force encrypted* or *Force unencrypted*, any H.323 and SIP to H.323 interworked calls through this subzone will ignore this mode.
ICE support for media	Controls whether ICE messages are supported by the devices in this subzone.
Bandwidth controls	When configuring 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. See Applying Bandwidth Limitations to Subzones for information about how bandwidth limits are set and managed.

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 Configuring Subzones 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
- The subnet or alias pattern matching configuration
- The subzone to which endpoints whose addresses satisfy this rule are assigned

Note If an endpoint's IP address or registration alias does not match any of the membership rules, it is assigned to the Configuring 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 *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.
Type	Determines how a device's address is checked: *Subnet*: assigns the device if its IP address falls within the configured IP address subnet. *Alias pattern match*: 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.

Field	Description	Usage tips
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 *Subnet*.
Pattern type	How the **Pattern string** must match the alias for the rule to be applied. Options are: *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*: Treats the string as a Regular Expressions.	Applies only if the **Type** is *Alias pattern match.*
Pattern string	The pattern against which the alias is compared.	Applies only if the **Type** is *Alias pattern match*.
Target subzone	The subzone to which an endpoint is assigned if its address satisfies this rule.	
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

Limitation	Description	Can be applied to
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 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 for more information. **Note** In order to apply a pipe, you must first have created it via the Configuring 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.

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 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.

Field	Description
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 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

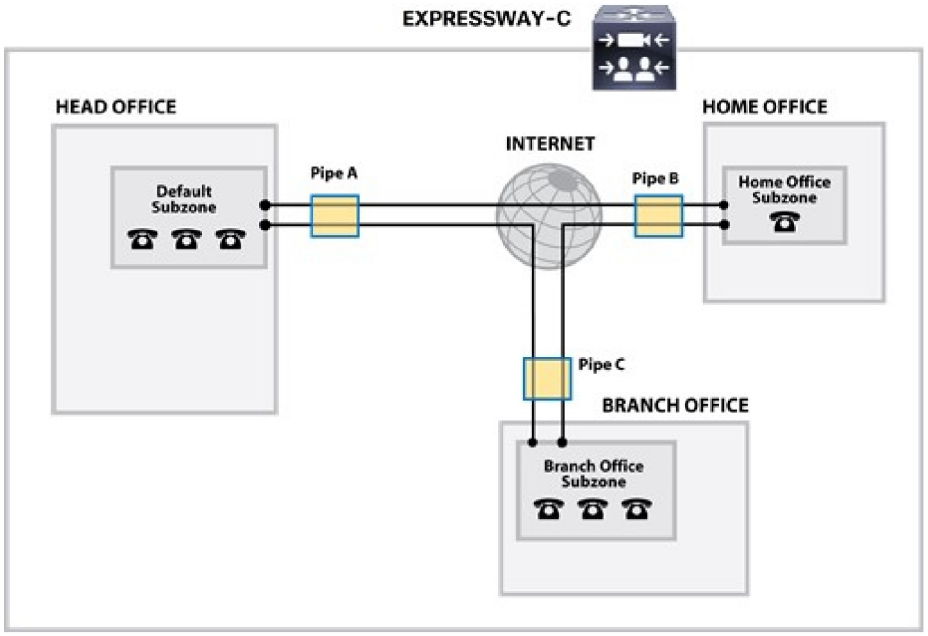
Each pipe may be applied to multiple links. This is used to model the situation where one site communicates with several other sites over the same broadband connection to the Internet. A pipe should be configured to represent the broadband connection, and then applied to all the links. This allows you 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

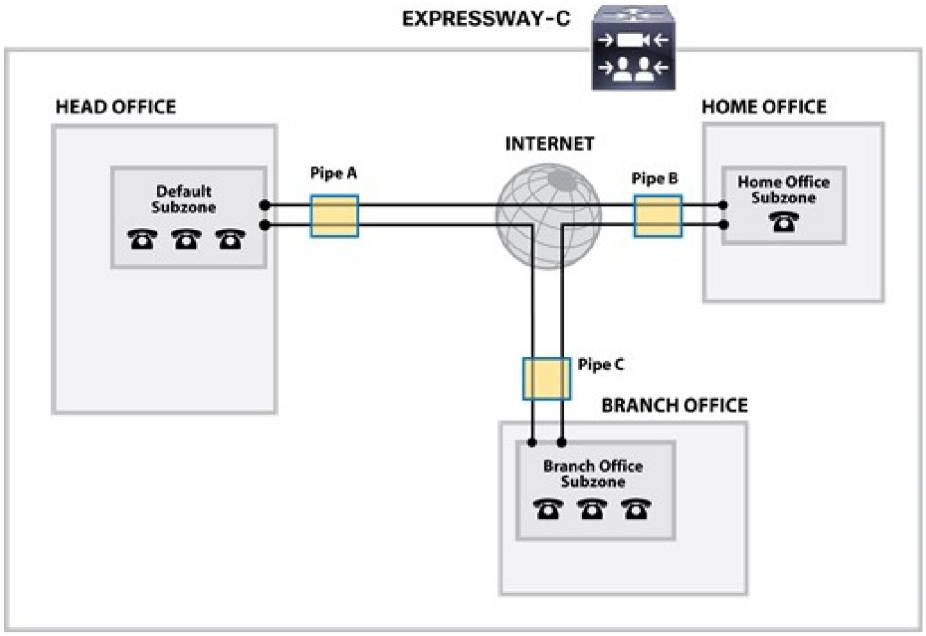
In the example below, there are three geographically separate offices: Head, Branch and Home. All endpoints in the Head Office register with the Expressway-C, as do those in the Branch and Home offices.

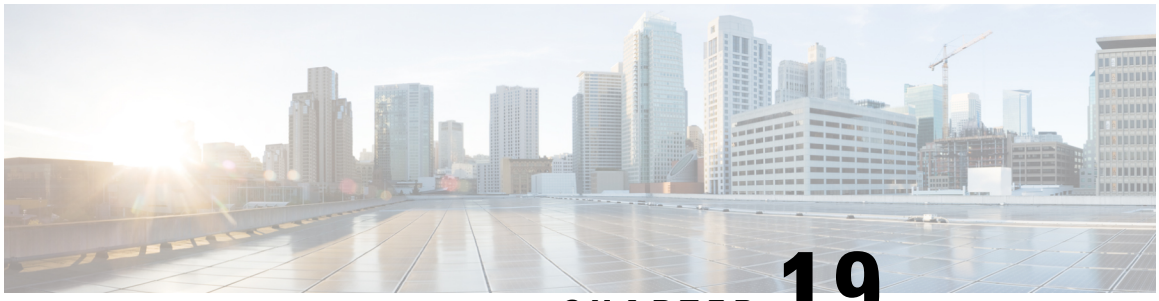
Each of the three offices is represented as a separate subzone on the Expressway, with bandwidth configured according to local policy.

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.


EXPRESSWAY-C
HEAD OFFICE
Default Subzone
Pipe A
INTERNET
Pipe B
HOME OFFICE
Home Office Subzone
Pipe C
BRANCH OFFICE
Branch Office Subzone
454314



CHAPTER 19

Applications

- Configuring Conference Factory, on page 371
- About Presence, on page 373
- B2BUA (Back-to-Back User Agent) Overview, on page 377
- About FindMe, on page 385
- Cisco TMS Provisioning (Including FindMe), on page 388
- Hybrid Services and Connector Management, on page 391
- Cisco Webex Edge, on page 393

Configuring Conference Factory

The **Conference Factory** page (**Applications** > **Conference Factory**) allows you to enable and disable the Conference Factory application, and configure the alias and template it uses.

The Conference Factory application allows the Expressway to support the Multiway feature, subject to Multiway-compliant endpoints and conference bridges (see Cisco TelePresence Multiway Deployment Guide). Multiway enables endpoint users to create a conference while in a call even if their endpoint does not have this functionality built in.

Check with your Cisco representative for an up-to-date list of the Cisco endpoints and infrastructure products that support Multiway.

Conference creation process

When Multiway is activated from the endpoint:

1. The endpoint calls a pre-configured alias which routes to the Conference Factory on the Expressway.
2. The Expressway replies to the endpoint with the alias that the endpoint should use for the Multiway conference. This alias will route to an MCU.
3. The endpoint then places the call to the MCU using the given alias, and informs the other participating endpoints to do the same.

The configurable options are:

Field	Description	Usage tips
Mode	Enables or disables the Conference Factory application.	
Alias	The alias that will be dialed by the endpoints when the Multiway feature is activated. This must also be configured on all endpoints that may be used to initiate the Multiway feature. An example could be **multiway@example.com**.	
Template	The alias that the Expressway tells the endpoint to dial to create a Multiway conference on the MCU.	To ensure that each conference has a different alias, you should use %% as a part of the template. The %% will be replaced by a unique number each time the Expressway receives a new conference request.
Number range start / end	The first and last numbers in the range that replaces %% in the template used to generate a conference alias.	For example, your **Template** could be **563%%@example.com** with a range of 10 - 999. The first conference will use the alias **563010@example.com**, the next conference will use **563011@example.com** and so on up to **563999@example.com**, after which it will loop round and start again at **563010@example.com**. **Note** The %% represents a fixed number of digits – with leading zeroes where required – based upon the length of the upper range limit.

Note

- Use a different **Template** on each Expressway in your network that has the Conference Factory application enabled. If your Expressway is part of a cluster, the template must be different for each cluster peer.
- The alias generated by the template must be a fully-qualified SIP alias, and must route to the MCU. The MCU must be configured to process this alias. No other special configuration is required on the MCU in order to support the Conference Factory application.
- The **SIP mode** setting must be set to *On* (**Configuration** > **Protocols** > **SIP**) for the Conference Factory application to function. If you want to be able to initiate calls to the Conference Factory from H.323 endpoints, you must also set **H.323 mode** to *On* (**Configuration** > **Protocols** > **H.323**), and ensure that **H.323 <-> SIP interworking mode** is set to *Registered only* or *On* (**Configuration** > **Protocols** > **Interworking**).

See Cisco TelePresence Multiway Deployment Guide for full details on how to configure individual components of your network (endpoints, MCUs and Expressways) in order to use Multiway in your deployment.

About Presence

Presence is the ability of endpoints to provide information to other users about their current status - such as whether they are offline, online, or in a call. Any entity which provides presence information, or about whom presence information can be requested, is known as a presentity. Presentities publish information about their own presence status, and also subscribe to the information being published by other presentities and FindMe users.

Endpoints that support presence, such as Jabber Video, can publish their own status information. The Expressway can also provide basic presence information on behalf of endpoints that do not support presence, including H.323 endpoints, as long as they have registered with an alias in the form of a URI.

If FindMe is enabled, the Expressway can also provide presence information about FindMe users by aggregating the information provided by each presentity configured for that FindMe user.

The Presence application on the Expressway supports the SIP-based SIMPLE standard and is made up of two separate services. These are the Presence Server and the Presence User Agent. These services can be Configuring Presence separately.

The Presence status pages provide information about the presentities who are providing presence information and the users who are requesting presence information on others. The status pages are organized into:

- Publishers
- Presentities
- Subscribers

Note Any one presentity can only subscribe to a maximum of 100 other presentities, and can only have a maximum of 100 other presentities subscribed to it.

Presence is supported by clustering.

Presence Server

The Presence Server application on the Expressway is responsible for managing the presence information for all presentities in the Configuring Domains for which the Expressway is authoritative. The Presence Server can manage the presence information for locally registered endpoints and presentities whose information has been received via a SIP proxy (such as another Expressway).

The Presence Server is made up of the following services, all of which are enabled (or disabled) simultaneously when the Presence Server is enabled (or disabled):

- **Publication Manager**: Receives PUBLISH messages, which contain the status information about a presentity, and writes this information to the Presence Database. PUBLISH messages are generated by presence-enabled endpoints and by the Presence User Agent.
- **Subscription Manager**: Handles SUBSCRIBE messages, which request information about the status of a presentity. Upon receipt of a SUBSCRIBE message, the Subscription Manager sends a request to the Presentity Manager for information about that presentity, and forwards the information that is returned

to the subscriber. The Subscription Manager also receives notifications from the Presentity Manager when a presentity's status has changed, and sends this information to all subscribers.

- **Presentity Manager**: An interface to the Presence Database. It is used to support Expressway features such as FindMe and the PUA, where the presence information provided by a number of different devices must be aggregated in order to provide an overall presence status for one particular presentity. When the Presentity Manager receives a request from the subscription manager for information on a presentity, it queries the Presence Database for all information available on all the endpoints associated with that particular presentity. The Presentity Manager then aggregates this information to determine the presentity's current status, and returns this to the Subscription Manager.
- **Presence Database**: Stores current presence information received in the form of PUBLISH messages. Also sends NOTIFY messages to the Presentity Manager to inform it of any changes.

Presence and device authentication

The Presence Server accepts presence PUBLISH messages only if they have already been authenticated:

- The authentication of presence messages by the Expressway is controlled by the authentication policy setting on the Default Subzone (or relevant alternative subzone) if the endpoint is registered (which is the usual case), or by the authentication policy setting on the Default Zone if the endpoint is not registered.
- The relevant **Authentication policy** must be set to either *Check credentials* or *Treat as authenticated*, otherwise PUBLISH messages will fail, meaning that endpoints will not be able to publish their presence status.

See Presence and authentication policy for more information.

Presence User Agent

Endpoints that do not support presence can have status published on their behalf by the Expressway. The service that publishes this information is called the Presence User Agent (PUA).

The PUA takes information from the local registration database and the call manager and determines, for each endpoint that is currently locally registered, whether or not it is currently in a call. The PUA then provides this status information via a PUBLISH message.

For the PUA to successfully provide presence information about a locally registered endpoint:

- The endpoint must be registered with an alias in the form of a URI.
- The domain part of the URI must be able to be routed to a SIP registrar that has a presence server enabled. (This could be either the local Presence Server, if enabled, or another Presence Server on a remote system.)

When enabled, the PUA generates presence information for all endpoints registered to the Expressway, including those which already support presence. The status information provided by the PUA is either:

- *online* (registered but not in a call)
- *in call* (registered and currently in a call)

Aggregation of presence information

When enabled, the PUA generates presence information for all endpoints registered to the Expressway, including those which already support presence. However, endpoints that support presence may provide other,

more detailed status, for example away or do not disturb. For this reason, information provided by the PUA is used by the Presentity Manager as follows:

- Where presence information is provided by the PUA and one other source, the non-PUA presence information will always be used in preference to the PUA presence information. This is because it is assumed that the other source of information is the presentity itself, and this information is more accurate.
- Where presence information is provided by the PUA and two or more other sources, the Presence Server will aggregate the presence information from all presentities to give the "highest interest" information, e.g. *online* rather than *offline*, and *in call* rather than *away*.
- If no information is being published about an endpoint, either by the endpoint itself or by the PUA, the endpoint's status will be *offline*. If the PUA is enabled, the *offline* status indicates that the endpoint is not currently registered.

FindMe presence

When the Presentity Manager receives a request for information about the presences of a FindMe alias, it looks up the presence information for each endpoint that makes up that FindMe alias. It then aggregates this information as follows:

- If the FindMe alias is set to *Individual* mode, if any one of the endpoints making up that FindMe is in a call the FindMe presentity's status will be reported as *in call*.
- If the FindMe alias is set to *Group* mode, if any one of the endpoints is online (i.e. not in call or offline) then the FindMe presentity's status will be reported as *online*.

Registration refresh period

The PUA will update and publish presence information on receipt of:

- A registration request (for new registrations)
- A registration refresh (for existing registrations)
- A deregistration request
- Call setup and cleardown information

For non-traversal H.323 registrations the default registration refresh period is 30 minutes. This means that when the PUA is enabled on an Expressway with existing registrations, it may take up to 30 minutes before an H.323 registration refresh is received and *available* presence information is published for that endpoint.

It also means that if an H.323 endpoint becomes unavailable without sending a deregistration message, it may take up to 30 minutes for its status to change to *offline*. To ensure more timely publication of presence information for H.323 endpoints, you should decrease the H.323 registration refresh period (using **Configuration** > **Protocols** > **H.323** > **Gatekeeper** > **Time to live**).

The default registration refresh period for SIP is 60 seconds, so it will take no more than a minute for the PUA to publish updated presence information on behalf of any SIP endpoints.

Configuring Presence

The **Presence** page (**Applications** > **Presence**) allows you to enable and configure Presence services on the Expressway.

These services can be enabled and disabled separately from each other, depending on the nature of your deployment. Both are disabled by default.

Note **SIP mode** must be enabled for the Presence services to function.

Presence User Agent

The PUA provides presence information on behalf of registered endpoints.

- *Enabled*: If the PUA is enabled, it will publish presence information for all locally registered endpoints, whether or not those endpoints are also publishing their own presence information. Information published by the PUA will be routed to a Presence Server acting for the endpoint's domain. This could be the local Presence Server, or (if this is disabled) a Presence Server on another system that is authoritative for that domain.
- *Disabled*: If the PUA is disabled, only those endpoints that support presence will publish presence information. No information will be available for endpoints that do not support presence.

You can also configure the **Default published status for registered endpoints**. This is the presentity status published by the Presence User Agent for registered endpoints when they are not "In-Call". The options are either *Online* or *Offline*.

Note

- If this is set to *Online*, any permanently registered video endpoints and FindMe entries that include those endpoints will appear as permanently "Online".
- The status of non-registered endpoints always appears as "Offline".
- "Online" status appears as "Available" in Lync clients.

Presence Server

The Presence Server manages the presence information for all presentities in the SIP domains for which the Expressway is authoritative.

- *Enabled*: If the local Presence Server is enabled, it will process any PUBLISH messages intended for the SIP domains for which the local Expressway is authoritative. All other PUBLISH messages will be proxied on in accordance with the Expressway's SIP routing rules.

Note SIP routes are configured using the CLI only.

- The Presence Server requires that any messages it receives have been pre-authenticated (the Presence Server does not do its own authentication challenge).You must ensure that the subzone through which PUBLISH messages are being received has its **Authentication policy** is set to either *Check credentials* or *Treat as authenticated*, otherwise the messages will be rejected.

- *Disabled*: If the local Presence Server is disabled, the Expressway will proxy on all PUBLISH messages to one or more of its neighbor zones in accordance with its locally configured Call Routing Process rules. The local Expressway will do this regardless of whether or not it is authoritative for the presentity's domain. If one of these neighbors is authoritative for the domain, and has a Presence Server enabled, then that neighbor will provide presence information for the presentity.

Regardless of whether or not the Presence Server is enabled, the Expressway will still continue to receive PUBLISH messages if they are sent to it from any of the following sources:

- Locally registered endpoints that support presence
- The local PUA (if enabled)
- Remote SIP Proxies

Note Presence Server is automatically enabled when the **Starter Pack** option key is installed.

Recommendations

- **Expressway-E and Expressway-C**: The recommended configuration for an Expressway-E when acting as a traversal server for an Expressway-C is to enable the PUA and disable the Presence Server on the Expressway-E, and enable the Presence Server on the Expressway-C. This will ensure that all PUBLISH messages generated by the PUA are routed to the Expressway-C.
- **Expressway neighbors**: If you have a deployment with two or more Expressways neighbored together, you are recommended to enable only one presence server per domain. This will ensure a central source of information for all presentities in your network.
- **Expressway clusters**: For information about how Presence works within a cluster.

Note Any defined About Pre-Search Transforms also apply to any Publication, Subscription or Notify URIs handled by the Presence Services.

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 Configuring Media Encryption Policy. This usage does not require any explicit B2BUA configuration.
- To support Configuring ICE Messaging Support. The only B2BUA-related configuration required is to define the set of Configuring B2BUA TURN Servers required to support ICE calls.

- To route SIP calls between the Expressway and a Microsoft SIP domain. This requires manual configuration of Configuring Microsoft Interoperability and the set of Configuring B2BUA 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 Configuring ICE Messaging Support 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).

Table 21: 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.
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.

About 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 From version X8.9, you can interoperate with Microsoft infrastructure without using the B2BUA on the Expressway. You can instead use session classification search rules to route calls to Cisco Meeting Server, which does the transcoding. See *Cisco Meeting Server with Cisco Expressway Deployment Guide* on the Expressway Configuration Guides page (previously called the *Cisco Expressway Traffic Classification Deployment Guide*).

Capabilities

- Interwork between Microsoft ICE and standards-based media for Cisco collaboration endpoints and bridges.
- Call hold, call transfer and Multiway support for calls with Microsoft clients, and can share FindMe presence information with Microsoft infrastructure.
- 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 such as IM and Presence Service nodes, while handling 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.
- Configuring the B2BUA's Trusted Hosts — the devices that may send signaling messages to the B2BUA.
- Configuring B2BUA TURN Servers — 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.
- Restarting the Microsoft Interoperability Service, if required. The system notifies you if you must restart the service.

Why do I need the 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.

Features and Limitations

- Maximum simultaneous call capability is 100 calls *including* Large systems. The exception is M5-based Small systems, which have a limit of 75 calls.
- 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.
- **Intradomain Microsoft Interoperability with Expressway and Cisco Meeting Server**

  If you use Meeting Server for Microsoft Interoperability, a limitation currently applies to the following intradomain/intracompany scenario:

  *You deploy separate Microsoft and standards-based SIP networks in a **single domain** and in a configuration that has an Expressway-E/Cisco VCS Expressway **directly facing** a Microsoft front end server (because you use internal firewalls between subnetworks, or for any other reason). For example, Cisco Unified Call Manager in one (sub)network and Microsoft in a second (sub)network, inside the same domain.*

  In this case we do not generally support Microsoft Interoperability between the two networks, and calls between Meeting Server and Microsoft will be rejected.

  Workaround: If you are not able to deploy the intradomain networks without an intervening Expressway-E/VCS Expressway (you cannot configure Meeting Server <> Expressway-C/VCS Control <> Microsoft), a workaround is to deploy an Expressway-C/VCS-C in each subnet, with an Expressway-E/VCS-E to traverse between them. That is:

  Meeting Server <> Expressway-C/VCS Control <> Firewall <> Expressway-E/VCS Expressway <> Firewall <> Expressway-C/VCS Control <> Microsoft

For more information about configuring Expressway for Microsoft Interoperability:

- See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series Configuration Guides page.
- See Cisco Expressway with *Microsoft Infrastructure Deployment Guide* on the Expressway Configuration Guides page.

Configuring Microsoft Interoperability

Go to **Applications** > **B2BUA** > **Microsoft interoperability** > **Configuration** to configure and enable the B2BUA connection to the Microsoft environment.

The configurable options are described in the table:

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 Configuring the B2BUA's 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.	
Signaling transport	The transport type used for connection to the Microsoft infrastructure. The default is *TLS*.	
FindMe integration section:		
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 and share FindMe presence information. Default is *Yes*.	This feature only applies if FindMe is enabled. **Note** 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 Configuring 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 *No*.	You should enable this option if you want Microsoft client users to be able to share their screens with Cisco Collaboration endpoints / conference participants.

Field	Description	Usage tips
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.
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 *No*.	This is recommended for calls traversing a Microsoft Edge server. To configure the associated TURN servers, click Configuring 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. *Required*: Both legs of the call must be encrypted. *Auto*: Encrypted and unencrypted combinations are supported. The default is *Auto*.	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 *Auto* 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.

Field	Description	Usage tips
B2BUA media port range start/end	The port range used by the B2BUA for handling media.	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 *Session-Expires* 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 *Min-SE header* in RFC 4028.
Port on B2BUA for Expressway communications	The port used on the B2BUA for communicating with the Expressway.	
Port on B2BUA for Microsoft call communications	The port used on the B2BUA for call communications with the Microsoft server. Default is 65072.	
RDP TCP port range start / end	Defines the range of TCP ports on which the transcoder instances listen for RDP media. Default is 6000 - 6099. **Note** Save the page and restart the Microsoft interoperability service to apply your changes.	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	Defines the range of UDP ports from which the transcoder instances transmit H.264 media. Default is 6100 - 6199. **Note** Save the page and restart the Microsoft interoperability service to apply your changes.	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.

Field	Description	Usage tips
Maximum RDP transcode sessions	Limits the number of simultaneous RDP transcoding sessions on this Expressway. Default is 10. **Note** Save the page and restart the Microsoft interoperability service to apply your changes.	Higher values will mean that more system resources can be consumed by RDP transcoding, which could impact other services. Maximum is 100. Recommended maximum RDP transcode sessions: • Medium OVA systems: 10 • Large OVA / CE1200 systems: 20 (From X8.10, it's no longer necessary to have a 10 Gbps NIC for Large system scale. Subject to your bandwidth constraints, the capacity of a Large system is possible with a 1 Gbps NIC.)

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.

Note 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.	

Field	Description	Usage tips
Type	The type of device that may send signaling messages to the B2BUA. *Microsoft infrastructure*: This includes Hardware Load Balancers, Directors and Front End Processors	

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.

Step 1 Go to **Applications** > **B2BUA** > **Microsoft interoperability** > **Restart service....**

Step 2 Check the number of active calls currently in place.

Step 3 Click **Restart**.

The service restarts after a few seconds. You can check the service status on the Configuring 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.

About 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

Users can configure their FindMe settings using Cisco TMS provisioning. If 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 Configuring TMS Provisioning Extension Services.

Expressway looks for an attribute named **distinguishedName** to search the user in the LDAP server.

Note Make sure LDAP server user records have a valid attribute named **distinguishedName**.

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.

Note User Policy is invoked after any Call Policy configured on the Expressway has been applied. See Call Routing Process 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 About FindMe.

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. *Off*: Disables FindMe. *Remote service*: Enables FindMe and uses a FindMe manager located on an off-box system (for example,TMS).	Configuring 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 Maintaining a Cluster page).
Caller ID	Determines how the source of an incoming call is presented to the callee. *Incoming ID*: Displays the address of the endpoint from which the call was placed. *FindMe ID*: Displays the FindMe ID associated with the originating endpoint's address.	Using *FindMe ID* 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, on page 233 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.

Field	Description
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.
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 (Including FindMe)

Cisco TMS provisioning is the mechanism through which the Expressway uses provisioning data for the following services:

- User account, device, and phone book data used by Expressway to service Expressway Provisioning Server from endpoint devices
- FindMe account configuration data used by Expressway to provide About FindMe

How to enable TMS provisioning services

From X8.11, TMS provisioning services are off by default in the Expressway for new systems (if you are upgrading an existing system to X8.11 or later, your current settings are retained). To enable TMS provisioning, services follow the steps below:

Note Although provisioning is supported on both the Cisco Expressway-C and the Cisco Expressway-E, for deployments with a paired Expressway-C and Expressway-E, we recommend that you use it on the Cisco Expressway-C.

1. (One-time only) If not already enabled, you need to enable provisioning services on the Expressway:
   a. Go to **System** > **Administration**.
   b. In the **Services** area, set **Provisioning services** to *On*.

      This makes the **System** > **TMS Provisioning Extension services** page accessible in the interface. From here you can connect to the Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) and its provisioning services for users, devices, FindMe and phone books.
2. Go to **System** > **TMS Provisioning Extension services**.
3. Specify your connection details for the Cisco TMSPE (for assistance, see Configuring TMS Provisioning Extension Services).

4. Enable one or more provisioning services (users, devices, FindMe and phone books). For each service you want:
   a. Set **Connect to this service** to *Yes*.
   b. If you don't want the default values, optionally define a **Polling interval** or **Connection**.

      For Devices, you need to specify a **Base Group**. An ID which identifies the Expressway or cluster in the Cisco TMSPE.

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 Even if the Cluster License Usage and Capacity Guidelines of your system is greater, you are 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 used for provisioning

When TMS provisioning is enabled, Expressway uses the following Cisco TMSPE services (hosted on Cisco TMS) to provide the Expressway / Expressway cluster with data:

Service	Description
User Preference	Provides data that enables the Expressway to configure a device with settings that apply to a specific user (a user is essentially a SIP URI). Devices such as Jabber Video are configured entirely using this service. Also provides connection details to a TURN server; typically the Expressway-E.
FindMe	Provides details of user 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	Provides data that allows users to search for contacts in 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).

Service	Description
Devices	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). If the Devices service is not active, the Expressway's Provisioning Server will not be able to provision any devices.

Status information for Cisco TMSPE services

Service status information is displayed on the TMS Provisioning Extension Service Status page.

- The Expressway periodically polls 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.

  With clustered 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.

- You can do an immediate resynchronization of data between Expressway and Cisco TMS at any time by clicking **Perform full synchronization** on the **TMS Provisioning Extension services** page. This will result in a few seconds lack of service on the Expressway while data is deleted and refreshed. If you only need to apply recent updates in Cisco TMS to the Expressway, click **Check for updates** instead.

Changing configuration settings for Cisco TMSPE services

We strongly recommend using Cisco TMS to make any changes to Cisco TMSPE services settings. Although you can configure the services on the Expressway (**TMS Provisioning Extension services** page), changes made through this page **are not applied in Cisco TMS**.

Expressway Provisioning Server

If device provisioning is enabled, the Expressway Provisioning Server provides provisioning-related services to provisioned devices, using data supplied by Cisco TMS through the Cisco TMS Provisioning (Including FindMe) mechanism.

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 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.

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 for more information.

Hybrid Services and Connector Management

If you want to register Expressways for Hybrid Services, see the Hybrid Services documentation to get more detailed information, including how to do first time deployments of Hybrid Services.

What are Hybrid Services and what do they do?

Cisco Webex Hybrid Services tie your premises-based solutions into the Cisco Collaboration cloud to deliver a more capable, better integrated collaboration user experience.

Which services can I use?

When you purchase Hybrid Services, you get access to Cisco Webex Control Hub - an administrative interface to the Cisco Webex cloud. From the Control Hub you can walk through deployment aids for each hybrid service, 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 Expressway to the cloud. When you register, the management connector is automatically downloaded, installed, and upgraded if a newer version is available.

The Expressway then downloads any other connectors that you selected using Control Hub. They are not started by default and you need to do some configuration before they'll work.

After this configuration, the connectors automatically download and upgrade based on the software upgrade schedule that you set in Control Hub. No manual intervention is required.

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 interface pages that the connectors install on the Expressway.

Connector upgrades are made available through Control Hub, 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 Cisco Webex and removes all connectors and related configuration.

Note Because cloud-delivered services are constantly in development to deliver new features and functionality, the minimum supported Expressway version for Hybrid Services may also change. You must ensure that your registered Expressways are up to date so that your Hybrid Services deployment remains functional and can be officially supported. See the Expressway version support statement for more information.

Where can I read more about Hybrid Services?

Hybrid Services are continuously developed and may be published more frequently than Expressway. This means that information about Hybrid Services is maintained in the Hybrid Services documentation, and several Expressway interface pages link out to that site.

Connector Proxy

If you want to register Expressways for Hybrid Services, see the Hybrid Services documentation to get more detailed information, including how to do first time deployments of Hybrid Services.

What is this proxy for?

Use the **Applications** > **Hybrid Services** > **Connector Proxy** page if this Expressway needs a proxy to connect to Cisco Webex. 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).

Cisco Webex CA Root Certificates on Expressway-E

The Cisco Webex cloud CA root certificates are packaged in the Expressway software and you can click **Get certificates** to start using them to validate incoming certificates. 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 Cisco Webex 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=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2
- O=QuoVadis Limited, CN=QuoVadis Root CA 2
- O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority
- O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA
- O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
- O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA

If you prefer to manually maintain the trusted CA list, go to **Maintenance** > **Security** > **Trusted CA certificate** page. See Managing the Trusted CA Certificate List for more help.

Related Reading

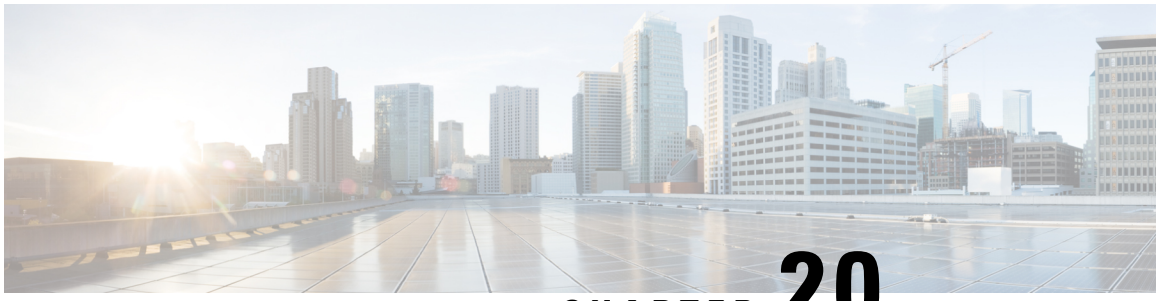
- Cisco Webex Signing CAs
- Supported Certificate Authorities for Cisco Webex

Cisco Webex Edge

Using Webex Edge Connect - and no Expressway-C

For business to business cases (not for MRA) from X12.5.5 we successfully tested using Cisco Webex Edge Audio with the Webex Edge Connect product, and without an Expressway-C. So Expressway-E connects to Cisco Unified Communications Manager without Expressway-C. No traversal or firewall is required for this scenario, and Expressway E connects the Webex Cloud directly to Cisco Unified Communications Manager. The tested configuration uses standard Webex Edge Audio over the internet, with a Neighbor zone between Cisco Unified Communications Manager and Expressway -E. The Webex zone media encryption mode needs to be “On” (the default is “Auto”).

This scenario requires inbound connections to be opened on the internal firewall. So it is **not** supported for standard Expressway deployments with the usual dual firewall configuration - only for use with WebEx Edge Connect.



CHAPTER 20

User Accounts

- About User Accounts, on page 395
- Configuring Password Security, on page 397
- Password Encryption, on page 399
- Forbidden Password Dictionary, on page 400
- Configuring Administrator Accounts, on page 402
- Configuring Remote Account Authentication Using LDAP, on page 406
- Resetting Forgotten Passwords, on page 412
- Using the Root Account, on page 414
- Setting the Pwrec Account Password, on page 415
- Managing SSO tokens, on page 415

About User Accounts

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. (FindMe account configuration via Expressway does not apply if the Expressway is using Configuring TMS Provisioning Extension Services to provide FindMe data.)

Account Authentication

Administrator and FindMe accounts must be authenticated before access is allowed to the Expressway.

Expressway can authenticate accounts locally, or against a remote directory service using LDAP (currently, Windows Active Directory is supported), or using 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 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 Expressway with the following:

- 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 and Configuring user groups).

The Expressway can also be configured to use Configuring Certificate-Based Authentication. This would typically be required if the Expressway is deployed in a highly-secure environment.

Password complexity

Complexity requirements can be specified for locally-managed passwords, from the Configuring Password Security page (**Users** > **Password security**).

All passwords and usernames are case sensitive.

Account Types

Administrator accounts

Administrator accounts are used to configure the Expressway.

The Expressway has a default **admin** local administrator account with full read-write access. It can be used to access the Expressway using the web interface, the API interface or the CLI.

Note 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 also be used to access the Expressway, using the web interface, the API interface, or the CLI.

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.

Configuration log

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.

Multiple admin sessions

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. Be aware that if each administrator session attempts to modify the same configuration settings, changes made in one session will overwrite changes made in another session.

Session limits and timeouts

You can configure account session limits and inactivity timeouts, as described in Network Services.

Login history page (advanced account security)

If the system is in advanced account security mode, a **Login history** page is displayed immediately after logging in. This page shows the recent activity of the currently logged in account.

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 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 section for more information.

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.

More Information

See Configuring Administrator Accounts.

Configuring Password Security

The **Password security** page (**Users** > **Password security**) controls whether or not passwords for *local* accounts must meet a minimum level of complexity before they are accepted.

- If **Enforce strict passwords** is set to *On*, all subsequently configured passwords for qualifying accounts 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 passwords. The default is *Off*.

The minimum number of bits of entropy in generated passphrases is also configurable on this page, in the range 0 to 255 (the default is 6).

Note You can never set a blank password for any administrator account, regardless of this setting.

Scope of strict passwords

The **Enforce strict passwords** setting applies only to local accounts that are managed in Expressway itself:

- Local administrator accounts
- Local FindMe user 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)

It does not affect any other passwords used on Expressway, such as LDAP/remotely stored administrator and FindMe credentials.

Note 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*, and they cannot be configured:

- 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”

While creating or modifying passwords for administrator accounts, FindMe user accounts, and the local authentication database, if **Enforce strict passwords** is *On*, and the password has the same letters as the username in straight or reverse order in lower or upper case, an error message displays at the top of the page.

Configurable rules for strict passwords

The following properties of the password policy can be configured:

If **Enable custom forbidden password dictionary** is set to *On*, it allows the use of a custom forbidden password dictionary to perform strict password checks.

If **Enable custom forbidden password dictionary** is set to *Off*, no custom dictionary is utilized when performing strict password checks. Default is *Off*.

- 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, for example, (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.

  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. Or, if you set the minimum number of character classes to 2, and 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 the other criteria).

Password Encryption

All passwords configured on Expressway are stored securely in an encrypted or hashed form. This applies to the following items, which all have usernames and passwords associated with them:

- 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)

Local administrator account passwords are hashed using SHA512. Other passwords are stored in an encrypted format.

Web interface and CLI compared

When entering or viewing passwords using the web interface, you see placeholder characters instead of the characters you are typing.

When entering passwords using the command line interface, you type the password in plain text. However, after the command is 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
FindMe accounts	1024

Note When a password is encrypted and stored, it uses more characters than the original plain text version.

Forbidden Password Dictionary

Note If you have not configured the Forbidden password dictionary, clicking it displays a warning message,

```
This Expressway is not currently configured to use a custom forbidden password
dictionary.
```

Downloading Forbidden Password Dictionary

Step 1 Go to **Users** > **Forbidden password**.

Step 2 Click **Download dictionary** to download the current version of the dictionary to your local drive.

Uploading Forbidden Password Dictionary

Note

- Only **.txt** file is supported.
- Make sure you upload files along **/tmp/** path to keep the file upload process secure.

  For example, Consider the following command:

  ```
  xcommand Passworddictionarywrite
  ```

  Use **/tmp/** at the beginning of the path:

  ```
  xcommand Passworddictionarywrite /tmp/random_file
  ```

  If **/tmp/** is not specified, the following error message is displayed.

  ```
  PasswordDictionaryWriteCommandError: Forbidden password dictionary file
  path must start with /tmp/
  ```

Step 1 Go to **Users** > **Forbidden password**.

Step 2 Click **Choose File**.

Step 3 Select the dictionary file you want to upload from your local drive and click **Upload dictionary**.
Result: The new dictionary is uploaded and integrated into the application.

Updating Forbidden Password Dictionary

Step 1 Go to **Users** > **Forbidden password**.

Step 2 Click **Download dictionary**.

Download the current version of the dictionary and make necessary changes.

Step 3 Click **Choose File** and select the updated file.

Step 4 Click **Upload dictionary**.

The updated dictionary is uploaded and integrated into the application.

Generating Passphrase

Generate passphrase provides a random secure passphrase that is longer than a password and contains spaces in between words which increases security, without the cryptic series of letters, numbers, and symbols, improving usability. It prevents unauthorized users from decrypting them. The default length of the generated passphrase is 64.

Step 1 Go to **Maintenance** > **Tools** > **Generate Passphrase**

Step 2 A new **Generated passphrase** displays.

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.

Step 1 Go to **Users** > **Administrator accounts**.

Step 2 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.

Changing the Password

Step 1 Go to **Users** > **Administrator accounts**.

Step 2 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 account.

Step 3 Go to **Related tasks** section and click **Generate passphrase**.

A new passphrase displays on the **Generated passphrase** page.

Step 4 Enter or copy paste the newly generated passphrase in **New password** field and **Confirm new password** field text box.

Step 5 Enter your **Current password** to authorize the password change process.

Step 6 Click **Save**.

A message `Password changed successfully` displays.

About the Administrator Account and Field References

This default local administrator "admin" 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).

Note Presently, only the built-in **admin** user has access to CLI. From 14.0.1 and later, Multiple Admin Accounts and Groups can have CLI access. Administrator Users can provide this access through a User Interface. Similarly, it also allows Administrator Users to toggle access between the CLI and REST API.

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 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.

Field	Description	Usage tips
Access level	The access level of the administrator account: *Read-write*: Allows all configuration information to be viewed and changed. This provides the same rights as the default **admin** account. *Read-only*: 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. *Auditor*: Allows access to the **Event Log**, **Configuration Log**, **Network Log**, **Alarms** and **Overview** pages only. Default: *Read-write*	The access permissions of the currently logged in user are shown in the system information bar at the bottom of each web page. The access level of the default **admin** account cannot be changed from *Read-write*.
Password	The password that this administrator will use to log in to the Expressway.	All passwords on the Expressway are encrypted, so you only see placeholder characters here. 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 Configuring Password Security page (**Users** > **Password security**). You cannot set blank passwords. **Note** While creating or modifying a password, for Administrator Accounts, Local authentication database, and FindMe users, if "**Enforce strict passwords**" is ON, and the password has the same letters as the username in straight or reverse order (in lower or upper case), an error message displays at the top of the page.
New password	Enter a new password for the account.	This field only appears when you are changing a password.
Confirm password	Re-enter the password for the account.	This field only appears when you create an account or when you change its password.

Field	Description	Usage tips
Emergency account	Select *Yes* to use this account as the emergency account. You must use an enabled local administrator account that has read-write access and web access.	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. The purpose of this account is to help you work around being locked out of the system when remote authentication is not available.
Web access	Select whether this account is allowed to log in to the system using the web interface. Default: *Yes*	
Force password reset	If you select Yes, then the new user must create a new password when they log in. Default: *No*	
API access	Select whether this account is allowed to access the system's status and configuration using the Application Programming Interface (API). Default: *Yes*	This controls access to the XML and REST APIs by systems such as Cisco TMS.
State	Select whether the account is *Enabled* or *Disabled*. 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.

Note Expressway supports Microsoft Active Directory's LDAP interface for remote authentication; other LDAP interfaces, such as Okta, are not currently supported configurations.

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	Defines where administrator login credentials are authenticated. *Local only*: Credentials are verified against a local database stored on the system. *Remote only*: Credentials are verified against an external credentials directory. *Both*: 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. The default is *Local only*.	*Both* allows you to continue to use locally-defined accounts. This is useful while troubleshooting any connection or authorization issues with the LDAP server. You cannot log in using a locally-configured administrator account, including the default **admin** account, if *Remote only* authentication is in use. **Note** Do not use *Remote only* if Expressway is managed by Cisco TMS.
LDAP server configuration: This section specifies the connection details to the LDAP server. Expressway looks for an attribute named **distinguishedName** to search the user in the LDAP server. **Note** Make sure LDAP server user records have a valid attribute named **distinguishedName**.		

Field	Description	Usage tips
FQDN address resolution	Defines how the LDAP server address is resolved. *SRV record*: DNS SRV record lookup. *Address record*: DNS A or AAAA record lookup. *IP address*: Entered directly as an IP address. The default is *Address record*. If you use SRV records, ensure that *_ldap._tcp.<domain> records* use the standard LDAP port 389. The Expressway does not support other port numbers for LDAP. To use LDAPS with SRV, the AD server must support the STARTTLS extension. (If you want to do LDAPS using port 636, you need to use an address record for FQDN resolution, and connect directly to port 636.)	The SRV lookup is for _ldap._tcp records. If multiple servers are returned, the priority and weight of each SRV record determines the order in which the servers are used.
Host name and **Domain** or **Server address**	The way in which the server address is specified depends on the **FQDN address resolution** setting: *SRV record*: Only the **Domain** portion of the server address is required. *Address record*: Enter the **Host name** and **Domain**. These are then combined to provide the full server address for the DNS address record lookup. *IP address*: The **Server address** is entered directly as an IP address.	If using TLS, the address entered here must match the CN (common name) contained within the certificate presented by the LDAP server.
Port	The IP port to use on the LDAP server.	The Expressway *only* supports ports 636 or 3269 for LDAP Encrypted connections.
Encryption	Determines whether the connection to the LDAP server is encrypted using Transport Layer Security (TLS). • *TLS*: Uses TLS encryption for the connection to the LDAP server. • *Off*: No encryption is used. The default is *TLS*. For more information, see Configuring Minimum TLS Version and Cipher Suites.	When TLS is enabled, the LDAP server's certificate must be signed by an authority within the Expressway's trusted CA certificates file. Click **Upload a CA certificate file for TLS** (in the **Related tasks** section) to go to the Managing the Trusted CA Certificate List page.

Field	Description	Usage tips
Certificate revocation list (CRL) checking	Specifies whether certificate revocation lists (CRLs) are checked when forming a TLS connection with the LDAP server. *None*: No CRL checking is performed. *Peer*: Only the CRL associated with the CA that issued the LDAP server's certificate is checked. *All*: All CRLs in the trusted certificate chain of the CA that issued the LDAP server's certificate are checked. The default is *None*.	If you are using revocation lists, any required CRL data must also be included within the CA certificate file.
Authentication configuration: This section specifies the Expressway's authentication credentials to use when binding to the LDAP server.		
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= **Note** Make sure that you provide LDAP users with the least possible privileges.	Any special characters within a name must be escaped with a backslash as per the LDAP standard (*RFC 4514*). 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. *None*: No mechanism is used. *DIGEST-MD5*: The DIGEST-MD5 mechanism is used. The default is *DIGEST-MD5*.	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.		

Field	Description	Usage tips
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.
Nested subgroup search depth	Used to limit the depth of groups for the LDAP search.	For optimal search performance, define the top-level group for the remote administrator as an (administrator) group in Expressway and set the search depth to "1".
Skip looking up all the members	Used to disable or enable member lookup of an administrator group during the authentication search process. The default is "*Yes*" - skip the member lookup.	We recommend keeping this setting as "*Yes*" if the configured groups have relatively high numbers of members. However, for deployments where the configured groups have relatively few members, setting it to "*No*" (do member lookup) may help to reduce authentication latency.

Checking the LDAP Server Connection Status

The status of the connection to LDAP server is displayed at the bottom of the page.

State = **Available**

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. **Note** To facilitate reverse lookup, give the domain in the form of 152.50.10.in-addr.arpa (the subnet of addresses would be 10.50.152.0/24) and the target DNS server in the address. This sends all requests in the subnet to the target DNS server instead of the default server.

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 *DIGEST-MD5* when it should be set to *None*.
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 Configuring Remote Account Authentication Using LDAP 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.

Note LDAP users can now login to Expressway using CLI if they have configured CLI access for their group.

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.
Access level	The access level given to members of the administrator group: *Read-write*: Allows all configuration information to be viewed and changed. This provides the same rights as the default **admin** account. *Read-only*: 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. *Auditor*: Allows access to the **Event Log, Configuration Log**, **Network Log**, **Alarms** and **Overview** pages only . *None*: No access is allowed. Default: *Read-write*	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 below for more information.
Web access	Determines whether members of this group are allowed to log in to the system using the web interface. Default: *Yes*	
API access	Determines whether members of this group are allowed to access the system's status and configuration using the Application Programming Interface (API). Default: *Yes*	This controls access to the XML and REST APIs by systems such as Cisco TMS.
State	Indicates if the group is enabled or disabled. Access will be denied to members of disabled groups.	If an administrator account belongs to more than one administrator group with a combination of both *Enabled* and *Disabled* states, their access will be *Enabled*.

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
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 Through the Web Interface

You can change the password for the default administrator account and for additional local administrator accounts.

Step 1 Go to **Users** > **Administrator accounts**.

Step 2 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.

Step 3 Enter the new password and confirm it.

Note You must also enter the password for the administrator account with which you are currently logged in to authorize the password change.

Resetting the Root or Admin Password Through a Serial Connection

On a hardware Expressway, reset the **admin** or **root** password as follows:

Step 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.

Step 2 Restart the Expressway.

Step 3 Log in from the PC with the username **`pwrec`**. No password is required.

Step 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.

Step 5 Select the account to be changed (**root** or **admin**).

Step 6 You are prompted for a new password.

What to do next

The **pwrec** account is only active for one minute following a restart. After that time you will need 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:

Step 1 Open the vSphere client.

Step 2 Click on the link **Launch Console**.

Step 3 Reboot the Expressway.

Step 4 In the vSphere console log in with the username **`pwrec`**. No password is required.

Step 5 When prompted, select the account (*root* or the username of the administrator account) whose password you want to change.

Step 6 You are prompted for a new password.

What to do next

The **pwrec** account is only active for one minute following a reboot. After that time you will need 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 set the password of your choice when prompted. 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

Step 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.

Step 2 Type the command **`passwd`**.

You will be asked for the new password.

Step 3 Enter the new password and when prompted, retype the password.

Step 4 Type **`exit`** to log out of the root account.

Accessing the Root Account Over SSH

Note
- The root account can be accessed over a serial connection or SSH only.
- 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.

You can enable and disable access to the root account using SSH.

Step 1 Log in to the Expressway as **root**.

Step 2 Type one of the following commands:

- **rootaccess --ssh on** - To enable access using SSH
- **rootaccess --ssh off** - To disable access using SSH

Step 3 Type **`exit`** to log out of the root account.

Setting the Pwrec Account Password

As of X14.0 release, you can set a password for pwrec account through command line interface only.

Important Once a password is set, the account will always require a password. Currently, there's no way to reset the password.

To set a password:

- Log in as root via SSH, or through the physical appliance
- Set the password using "passwd pwrec".
- You'll be prompted to enter a new password and retype it to confirm.
- If both the passwords match a message, "passwd: password updated successfully" displays.
    - If the passwords don't match a message, Sorry ", passwords don't match" displays.

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**).

1. **View the list of users who currently hold SSO tokens**: Go to **Users** > **SSO token holders** to view the list of users who currently hold SSO tokens. This page can help you troubleshoot issues related to single sign-on for a particular user.
2. **Purge tokens from all holders**: 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.

Managing the tokens of a particular user

Step 1 [Optional] Filter by a substring of the username to return a smaller list.

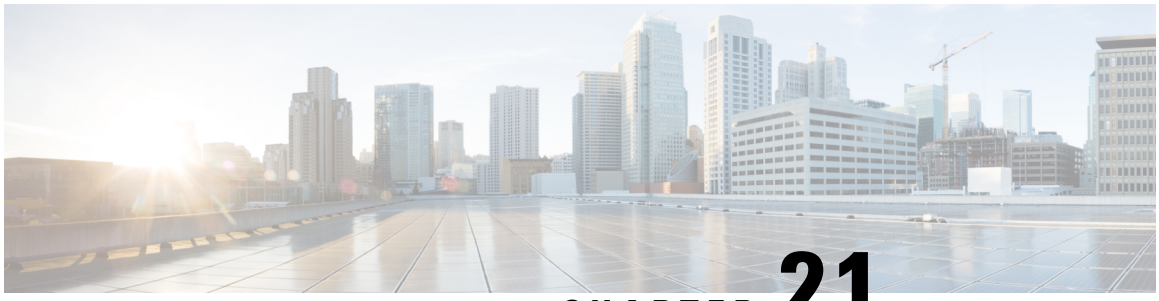
You may need this if there are many usernames in the list, because a long list spans multiple pages of up to 200 usernames each.

Step 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.

Step 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.



CHAPTER 21

Status and System Information

- Status Overview, on page 417
- System Information, on page 419
- Ethernet Status, on page 420
- IP Status, on page 420
- Resource Usage, on page 422
- Registration Status, on page 422
- Call Status, on page 424
- B2BUA Calls, on page 426
- Search History, on page 427
- Search Details, on page 428
- Local Zone Status, on page 429
- Zone Status, on page 430
- Bandwidth, on page 431
- Policy Server Status and Resiliency, on page 431
- TURN Relay Usage, on page 433
- Unified Communications Status, on page 434
- Microsoft Interoperability, on page 435
- TMS Provisioning Extension Service Status, on page 436
- Managing Alarms, on page 440
- Logs, on page 442
- Hardware Status, on page 446

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.	

Field	Description
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
IPv6 address	Expressway's IPv6 addresses
Options	Maximum limits for calls and registrations are controlled by option keys. Depending on the software version, a few additional features may also be controlled by option keys, although we are phasing out this approach

Resource usage

This section provides statistics about current and cumulative license usage for calls and registrations.

Shows current and peak usage broken down by:

- Rich media sessions
- Registrations (including Unified CM remote sessions)

  Registrations shows the total count of devices registered with Expressway, which includes TelePresence Room, Desktop System, and Conference System.

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.

To view details of current calls or registrations, click the relevant item in the section.

Note All statistics are based on data since the system was last restarted; values are set to zero after a restart. The information auto-refreshes every 5 seconds.

You can go to the **Resource usage** page to see more details, including total usage statistics.

MRA deployments

If you deploy the Cisco Unified Communications Mobile and Remote Access feature with Expressway, from Expressway X12.6.1 the Expressway-E also displays usage information about SIP devices that are currently

registered over MRA. (The MRA service must be enabled for the Expressway in question.) The information shows the count of current active MRA devices, and the peak count for MRA registrations since the last Expressway restart.

Clustered systems

If the Expressway is part of a cluster, then details for each peer are shown as well as totals for the entire cluster.

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
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 some additional Expressway features are controlled through option keys. This section shows any optional features currently installed.
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
VM size	(Virtual machine-based systems only) Size of the VM hardware platform - small, medium or large
Time information section	
Up time	The time that has elapsed since the system last restarted

Field	Description
System time (UTC)	The time as determined by the NTP server.If no NTP server is configured, this shows *Time Not Set*.
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 Settings 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	

Field	Description
Protocol	Indicates the IP protocol supported by the Expressway: • *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.
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 Configuring IP Settings page.

Resource Usage

The **Resource usage** page (**Status** > **System** > **Resource usage**) provides statistics about the current and cumulative license usage for calls and registrations.

Shows current and peak usage broken down by:

- Rich media sessions
- Registrations (including Unified CM remote sessions)

  Registrations shows the total count of devices registered with Expressway, which includes TelePresence Room, Desktop System, and Conference System.

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.

To view details of current calls or registrations, click the relevant item in the section.

Note All statistics are based on data since the system was last restarted; values are set to zero after a restart. The information auto-refreshes 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. See About Clusters 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 *Time not set*.
Address	For SIP UAs this is the Contact address presented in the REGISTER request.
Device type	Indicates the type of the registered device. The possible types are: *TelePresence Room*, *Desktop System*, or *Conference Systems*.
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.
Action	Click **View** to go to **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 Configuring 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 Configuring the Registration 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*.)

Note If your Expressway is part of a cluster you have to be logged into the peer to which the device is registered, 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 calls currently taking place to or from devices registered with the Expressway, or passing through the Expressway.
- **Completed calls:** The **Call history** page (**Status** > **Calls** > **History**) lists all calls that are no longer active. The list is limited to the most recent 500 calls--or less if calls used multiple components (see below). It 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).

Field	Description
Type	Indicates the type of call.
SIP variant	*Standards-based*, *Microsoft AV*, *Microsoft SIP IM&P*, or *Microsoft Share* 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:

- *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

To view full details of a call component, click **Local call serial number** associated with it. This opens the **Call details** page for 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.

Call history may reflect fewer than 500 calls

Some calls use multiple components, particularly calls invoked through the B2BUA. In these cases each individual call is actually counted as *three* calls due to the multiple components involved. This means that the number of entries actually listed in the call history may be significantly less than the theoretical 500 limit.

Identifying Mobile and Remote Access (MRA) calls

The call status and call history pages show all call types: Unified CM remote sessions (if MRA is enabled) as well as Expressway RMS sessions.

To distinguish between the call types, you need to drill down into the call components. MRA 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 (RMA)

If your system has an RMA 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 provides overview information about a call routed through the B2BUA. To access this page, go to **Status** > **Calls** > **Calls** or **Status** > **Calls** > **History** and click **View** for a particular B2BUA call.

Calls are routed through the B2BUA in the following cases:

- A Configuring Media Encryption Policy applies to the call (any encryption setting other than Auto).
- Expressway is load balancing calls for Cisco Meeting Server. The Expressway B2BUA processes the INVITE messages from the Meeting Server when load balancing is enabled. Note that support for Meeting Server load balancing **may be provided in Preview mode only**, as detailed in the release notes for your current Expressway version.
- Configuring ICE Messaging Support is triggered.
- About Microsoft Interoperability is enabled and the call routed through the **To Microsoft destination via B2BUA** neighbor zone.

For Microsoft interoperability calls, you can click the **Corresponding Expressway call** link to see details of the leg passing through the Expressway.

Known Limitation

The Send empty INVITE for interworked calls (configured on advanced custom zone profile) is not supported for call that involve B2BUA.

Viewing B2BUA Call Media Details

The **B2BUA call media** page is accessed from the B2BUA Calls page by clicking **View media statistics for this call**. It shows information about the audio and video media channels 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 any external transcoder (if applicable).

Note B2BUA debug tool connects to media process over ports 13997, 13998 and 13999 on local loopback to get the media statistics. These ports are open for connection and are strictly for internal use only. This is accessible from root only.

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** appears in the **Search history** page.
- SIP: a single message is sent to place a call: this is either a SIP **INVITE** or SIP **OPTIONS**.

Note An individual call can have one or more searches associated with it, and can be of different types. Each search has an individual Search ID; each call has an individual Call Tag (see Identifying Calls).

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.

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 **Subzone name** takes you to the configuration page for that subzone.
Calls	The number of calls currently passing through the subzone. **Note** A single call may pass through more than one subzone, depending on the route it takes. For example, calls from a locally registered endpoint 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:

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: • *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, for example, 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
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** 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.
Calls	The total number of calls currently traversing the pipe. **Note** 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 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 is not queried for policy service requests until it returns to an active state. Its availability is not 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 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 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 This method provides resiliency but not load balancing i.e. all requests are 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.

Field	Description
URL	The address of the service. **Note** 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 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 Mobile and Remote Access Overview services including:

- The number of configured Unified CM and IM&P servers (Expressway-C only)
- The current number of active provisioning sessions (Expressway-C only)
- The number of current calls
- All the domains and zones that have been configured for Unified Communications services
- Statistics about SSO access requests and responses

If any configuration or connectivity problems are detected, appropriate messages are displayed with either links or guidelines as to how to resolve the issue.

You can also view some advanced status information, including:

- A list of all current and recent (shown in red) provisioning sessions (Expressway-C only)
- A list of the automatically-generated SSH tunnels servicing requests through the traversal zone

Checking 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 About Microsoft Interoperability.

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 Configuring Microsoft Interoperability 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** 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.

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 About Microsoft Interoperability.

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 Configuring TMS Provisioning Extension Services page (**System** > **TMS Provisioning Extension services**).

See the Expressway 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.

If device provisioning is enabled, the Expressway Provisioning Server provides provisioning-related services to provisioned devices, using data supplied by Cisco TMS through the Cisco TMS Provisioning (Including FindMe) mechanism.

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:

- 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 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 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 Checking 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:

- **Accounts**
- **Locations**
- **Devices**

All the records in the chosen table are listed.

Note 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 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 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**.

Only those records that match all of the selected filter options are shown.

Note 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 Expressway 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**).

Step 1 Verify that the **User account name** is displaying the name of the user account you want to check.

Step 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.

Step 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
9nnnn	Significant Event 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 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 Reference 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 Configure Logging 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 and Events and Levels.

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.
- **Contains any of the words**: Includes any events that contain at least one 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 Configure Logging will not affect their presence in the Configuration Log.

Configuration Log events

Changes to the Expressway configuration made by administrators using the web interface have an Event field of *System Configuration Changed*.

The **Detail** field of each of these events shows:

- The configuration item that was affected

- What it was changed from and to
- The name of the administrator user who made the change, and their IP address
- The date and time that the change was made

Network Log

The **Network Log** page (**Status** > **Logs** > **Network Log**) provides a list of the call signaling messages that have been logged on this Expressway.

The Network Log holds a maximum of 2GB of data; when this size is reached, the oldest entries are overwritten. However, only the first 50MB of Network Log data can be displayed through the web interface.

Filtering the Network Log

The **Filter** section lets you filter the Network Log. It is displayed only if there is more than one page of information to display. Log pages show 1000 records per page.

Enter the words you want to search for and click **Filter**. Only those events that contain all the words you entered are shown.

To do more advanced filtering, click **more options**. This gives you additional filtering methods:

- **Contains the string**: Only includes events containing the exact phrase entered here.
- **Contains any of the words**: Includes any events that contain at least one of the words entered here.
- **Not containing any of the words**: Filters out any events containing any of the words entered here.

Note Use spaces to separate each word you want to filter by.

Click **Filter** to reapply any modified filter conditions. To return to the complete log listing, click **Reset**.

Reconfiguring the log settings

Clicking **Configure the log settings** takes you to the Configuring Network Log Levels 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 Configuring Network Log Levels page.

Hardware Status

The **Hardware** page (**Status** > **Hardware**) provides information about the physical status of your Expressway appliance.

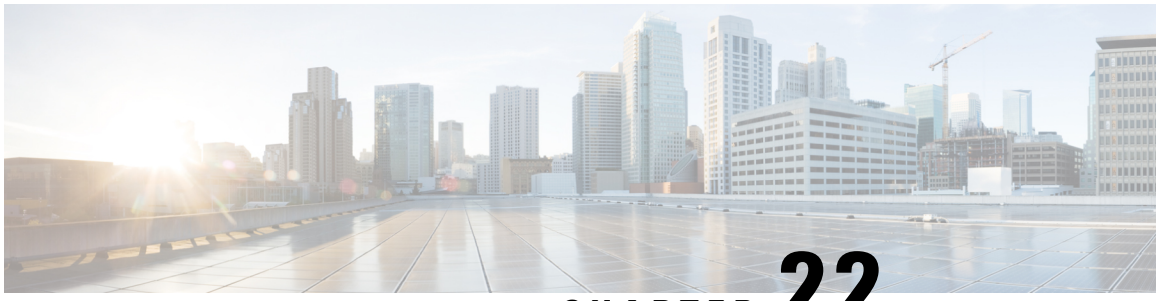
Information displayed includes:

- 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 Hardware status information is not displayed if the Expressway is running on VMware.



CHAPTER 22

Maintenance

- Enable Maintenance Mode, on page 447
- Enabling SSH Access to Expressway, on page 448
- Upgrading Expressway Software, on page 449
- Configuring Language Settings, on page 459
- Backing Up and Restoring Expressway Data, on page 460
- Creating a System Backup, on page 461
- Restoring a Previous Backup, on page 463
- Checking the Effect of Pattern, on page 464
- Locating an Alias, on page 465
- Port Usage, on page 466
- Restarting, Rebooting, and Shutting Down, on page 467

Enable 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.

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.

When a peer is in maintenance mode, its workload is handled by the other cluster nodes. For large multitenant deployments or MRA deployments therefore, we recommend that you only enable maintenance mode on one peer at a time, to avoid overloading the other nodes.

Impact on Active Calls and Registrations

Standard Expressway sessions (not MRA)

- New calls and registrations will be handled by another peer in the cluster.

- Existing registrations are allowed to expire and then should reregister 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 continue until the call is terminated.

Unified CM MRA sessions

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.

Process to Enable Maintenance Mode

1. Log to 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 Maintenance mode is automatically disabled if the peer is restarted.

How to Manually Remove Calls or Registrations

To manually remove any calls or registrations that don't clear automatically:

- Go to **Status** > **Calls**, click **Select all** and then click **Disconnect** (SIP calls may not disconnect immediately).
- Go to **Status** > **Registrations** > **By device**, click **Select all** and then click **Unregister**.

You can leave the Conference Factory registration. This will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration (if enabled).

Enabling SSH Access to Expressway

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`.

Step 1 Use SSH to log in as `root`.

Step 2 Enter `mkdir /tandberg/.ssh` to create `.ssh` directory if it is not already present.

Step 3 Copy your public key to `/tandberg/.ssh`.

Step 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)

Step 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`.

Upgrading Expressway Software

This section describes how to install new releases of Expressway software components onto an existing system. Component upgrades can be performed in one of two ways:

- **Using the Web Interface** - Recommended approach using the **Maintenance** > **Upgrade** page.
- **Using Secure Copy** (SCP/PSCP) - Alternative approach. This method may be useful in specific cases such as with a slow or unstable network connection.
- **Using APIs** – Only single node upgrade is supported as of now. So, we are introducing another alternative approach which is useful in specific cases of automated deployment. For upgrading a clustered system, start with the primary peer.

Downgrading Support

Downgrading to an older version is NOT supported.

Upgrading Using Web Interface

Upgrading Expressway

This section describes how to install the software on Expressway using the web user interface, which is the method we recommend. If you prefer to use a secure copy program such as SCP or PSCP to do the install, please use the *Cisco Expressway Administrator Guide* instead.

Summary

Table 22: Summary of tasks in a typical upgrade process

Stage	Task	Where
1	Review the *Prerequisites and Software Dependencies* and *Before You Begin* sections below	Release Notes
2	Back up the system	**Maintenance** > **Backup and restore**
3	Enable maintenance mode and wait for current calls and registrations to end	**Maintenance** > **Maintenance mode**
4	Upload the new software image (**"Upgrade"** option)	**Maintenance** > **Upgrade**
5	Install the new software ("**Continue with upgrade**" option)	**Maintenance** > **Upgrade**
6	Reboot	From the **Upgrade** page
7	In clustered deployments repeat for each peer in sequence	-

Prerequisites and Software Dependencies

This section has important information about issues that may prevent the system working properly after an upgrade. Before you upgrade, please review this section and complete any tasks that apply to your deployment.

Expressway and Cisco VCS systems before X8.11.4 need a two-stage upgrade

If you are upgrading a system which is running software earlier than version X8.11.4, you must first upgrade to an **intermediate release** before you install X14.2 software (this requirement applies to all upgrades X8.11.x and later versions). Depending on the existing system version, the upgrade will fail. We recommend upgrading to X8.11.4 as the intermediate release.

All deployments

If you are upgrading from X12.6 or X12.6.1 and use the alarm-based email notifications feature

Note In X12.6.2 the email ID length is limited to 254 characters maximum. Before you upgrade make sure that all destination email IDs are no longer than 254 characters.

We do not support downgrades. Do not install a previous Expressway/Cisco VCS version onto a system that is running a newer version; the system configuration will be lost.

Note From X8.11.x, when the system restarts after the upgrade it uses a new encryption mechanism. This is due to a unique root of trust for every software installation that was introduced in that release.

X8.8 and later versions are more secure than earlier versions. Upgrading could cause your deployments to stop working as expected, and you must check for the following environmental issues before you upgrade to X8.8 or later:

- **Certificates**: Because certificate validation was tightened up in X8.8, you must verify the following items to avoid validation failures:
  - Try the secure traversal test before and after upgrade (**Maintenance** > **Security** > **Secure traversal test**) to validate TLS connections.
  - If Unified Communications nodes are deployed, do they use valid certificates that were issued by a CA in the Expressway-C/Cisco VCS Control trust list?
  - If you use self-signed certificates, are they unique? Does the trusted CA list on Expressway/Cisco VCS have the self-signed certificates of all the nodes in your deployment?
  - Are all entries in the Expressway/Cisco VCS trusted CA list unique? Remove any duplicates.
  - If **TLS verify mode** is enabled on connections to other infrastructure (always on by default for Unified Communications traversal zone, and optional for zones to Unified Communications nodes), make sure that the hostname is present in the CN or SAN field of the host's certificate. We do not recommend disabling TLS verify mode, even though it may be a quick way to resolve a failing deployment.
- **DNS entries**: Do you have forward and reverse DNS lookups for all infrastructure systems that the Expressway/Cisco VCS interacts with? From X8.8, you need forward and reverse DNS entries for all Expressway-E/Cisco VCS Expressway systems, so that systems making TLS connections to them can resolve their FQDNs and validate their certificates. If the Expressway/Cisco VCS cannot resolve system hostnames and IP addresses, complex deployments like MRA may not work as expected after the upgrade.
- **Cluster peers**: Do they have valid certificates? If they are using default certificates you should replace them with (at least) internally generated certificates and update the peers trust lists with the issuing CA. From X8.8, clustering communications use TLS connections between peers instead of IPSec. By default, TLS verification is not enforced after the upgrade, and an alarm will remind you to enforce it.

How and when rebooting is necessary as part of the upgrade

Upgrading the *System platform* component is a two-stage process. First, the new software image is uploaded onto the Expressway/Cisco VCS. 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/Cisco VCS 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. Any **configuration changes made between the software upload and the reboot will be lost when the system restarts** with the new software version.

Upgrades for components other than the *System platform* do not involve a system reboot, although the services provided by that component are temporarily stopped while the upgrade process completes.

Deployments that use MRA

This section only applies if you use the Expressway/Cisco VCS for MRA (mobile and remote access with Cisco Unified Communications products).

- Minimum versions of Unified Communications infrastructure software apply - some versions of Unified CM, IM and Presence Service, and Cisco Unity Connection have been patched with CiscoSSL updates. Before you upgrade Expressway/Cisco VCS check that you are running the minimum versions listed in the *Mobile and Remote Access Through Expressway Deployment Guide*.

  IM and Presence Service 11.5 is an exception. You must upgrade Expressway/Cisco VCS to X8.8 or later before you upgrade IM and Presence Service to 11.5.

- Expressway-C/Cisco VCS Control and Cisco Expressway-E/VCS Expressway **should both be upgraded** in the same upgrade "window"/timescale (this is also a general recommendation for non-MRA deployments). We don't recommend operating with Expressway-C/Cisco VCS Control and Expressway-E/Cisco VCS Expressway on different versions for an extended period.

- This item applies if you are upgrading a Expressway/Cisco VCS that is used for MRA, with clustered Unified CMs and endpoints running TC or Collaboration Endpoint (CE) software. In this case you must install the relevant TC or CE maintenance release listed below (or later) before you upgrade the Expressway/Cisco VCS. This is required to avoid a known problem with failover. If you do not have the recommended TC/CE maintenance release, an endpoint will not attempt failover to another Unified CM if the original Unified CM to which the endpoint registered fails for some reason. Bug ID CSCvh97495 refers.

  - TC7.3.11
  - CE8.3.3
  - CE9.1.2

From X8.10.x, the MRA authentication (access control) settings are configured on Expressway-C/Cisco VCS Control and not on Expressway-E/Cisco VCS Expressway as in earlier releases, and default values are applied if it is not possible to retain the existing settings. To ensure correct system operation, after the upgrade reconfigure the access control settings on the Expressway/Cisco VCS, as described later in these instructions.

Deployments that use FIPS mode cryptography

If the Expressway/Cisco VCS has FIPS mode enabled, after the upgrade, manually change the default SIP TLS Diffie-Hellman key size from the default 1024 bits, to 2048 or greater, as described later in these instructions.

Deployments that use X8.7.x or earlier with Cisco Unified Communications Manager IM and Presence Service 11.5(1)

X8.7.x (and earlier versions) of Expressway/Cisco VCS are not interoperable with Cisco Unified Communications Manager IM and Presence Service 11.5(1) and later. This is caused by a deliberate change in that version of IM and Presence Service, which has a corresponding change in Expressway/Cisco VCS X8.8 and later. To ensure continuous interoperability, upgrade the Expressway/Cisco VCS systems before you upgrade the IM and Presence Service systems. The following error on Expressway/Cisco VCS is a symptom of this issue: `Failed Unable to Communicate with <IM&P node address>. AXL query HTTP error "'HTTPError:500'"`

Deployments that use Cisco Webex Hybrid Services

The Management Connector must be up to date before you upgrade Expressway/Cisco VCS. Authorize and accept any Management Connector upgrades advertised by the Cisco Webex cloud before you try to upgrade Expressway/Cisco VCS. Failure to do so may cause issues with the connector after the upgrade. For details about which versions of Expressway/Cisco VCS are supported for hybrid connector hosting, see Connector Host Support for Cisco Webex Hybrid Services.

Upgrade Instructions

Before You Begin

- Do the upgrade when the system has low levels of activity.
- A system upgrade needs a system reboot to complete the process. The reboot will terminate any active calls and registrations.
- For clustered systems, allocate enough time to upgrade all peers in the same upgrade "window". The cluster will not re-form correctly until the software versions match on all peers.
- Check the **Alarms** page (**Status** > **Alarms**) and make sure that all alarms are acted upon and cleared. Do this for each peer if you are upgrading a cluster.
- If you are upgrading a VM-based system, use the standard *.tar.gz* software image file. The *.ova* file is only needed for the initial install of Expressway software onto VMware.
- If you use the Expressway for MRA and you upgrade from X8.9.x or earlier to X8.10 or later, note your MRA authentication settings before you upgrade. From version X8.10 the MRA authentication (access control) settings moved from the Expressway-E to the Expressway-C. The upgrade does not preserve the existing Cisco Expressway-E settings, so after the upgrade you need to review them on the Expressway-C and adjust as necessary for your deployment. To access existing MRA authentication settings:

  a. On the Expressway-E, go to **Configuration** > **Unified Communications** > **Configuration** and locate **Single Sign-on support**.

Note The existing value (On, Exclusive, or Off)

  b. If **Single Sign-on support** is set to *On* or *Exclusive*.

Note The current values of these related fields:

- Check for internal authentication availability.
- Allow Jabber iOS clients to use embedded Safari.

- Make sure that all relevant tasks in Prerequisites and Software Dependencies are complete.

Upgrading Expressway-C and Expressway-E systems connected over a traversal zone

In all cases we recommend that Expressway-C (traversal client) and Expressway-E (traversal server) systems that are connected over a traversal zone **both run the same software version**. For some services such as Mobile and Remote Access, we *require* both systems to run the same version.

However, we do support a traversal zone link from one Expressway system to another that is running the previous feature release of Expressway (for example, from an X12.6 system to an X12.5 system). This means that you do not have to simultaneously upgrade your Expressway-C and Expressway-E systems.

Process to Upgrade a Standalone System

Note Do not use this process if you are upgrading a clustered Expressway/Cisco VCS; instead use the Process to Upgrade a Clustered System.

Step 1 Sign in to the Expressway/Cisco VCS web user interface as *admin*.

Step 2 Back up the Expressway/Cisco VCS system before you upgrade (**Maintenance** > **Backup and restore**).

Step 3 Enable maintenance mode so that Expressway/Cisco VCS does not process any new incoming calls (**Maintenance** > **Maintenance mode**). Existing calls continue until the call is terminated.

Step 4 Wait for all calls to clear and registrations to timeout.

To manually remove any calls or registrations that don't clear automatically, use the **Status** > **Calls** page or the **Status** > **Registrations** > **By device** page respectively (SIP calls may not clear immediately).

Note You can leave the registration for Conference Factory (if enabled) – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration.

Step 5 Go to **Maintenance** > **Upgrade** to access the **Upgrade** page.

Step 6 Click **Browse** and select the software image file for the component you want to upgrade.

The Expressway/Cisco VCS automatically detects which component you are upgrading based on the selected software image file.

Step 7 Click **Upgrade**. This step uploads the software file but does not install it. The upload may take a few minutes to finish.

Step 8 For upgrades to the **System platform** component, the **Upgrade confirmation** page is displayed:

a. Check the following details:

- **New software version** number is as expected.
- **MD5 hash** and **SHA1 hash** values match the values displayed on the cisco.com page, where you downloaded the software image file.

b. Click **Continue with upgrade**. This step installs the new software.

The **System upgrade** page opens and displays a progress bar while the software installs.

A summary of any active calls and registrations is displayed when the software completes installing (the calls and registrations will be lost when you reboot the system in the next step).

c. Click **Reboot system**. Any configuration changes made between uploading the software tar file and rebooting, will be lost when the system restarts.

   Sometimes the web browser interface times out during the restart process, after the progress bar reaches the end. This may occur if the Expressway/Cisco VCS carries out a disk file system check – approximately once every 30 restarts.

   After the reboot is complete the **Login** page is displayed.

Step 9 For upgrades to other components (not System platform) the software is automatically installed and no reboot is required.

What Next?

If you don't use MRA, the upgrade is now complete, and the Expressway configuration should be as expected. The **Overview** and **Upgrade** pages show the upgraded software version numbers.

If you do use MRA, and you are upgrading from X8.9.x or earlier, reconfigure your MRA access control settings as described in "Appendix 2: Post-Upgrade Tasks for MRA Deployments" in the *Mobile and Remote Access Deployment Guide*.

If you have components that require option keys to enable them, do this from the **Maintenance** > **Option keys** page.

If the Expressway has FIPS mode enabled (that is, it's a FIPS140-2 cryptographic system) then from X12.6 you must manually change the default SIP TLS Diffie-Hellman key size from the default 1024 bits, to 2048 or greater. To do this type the following command in the Expressway command line interface (change the value in the final element if you want a key size higher than 2048): ***xconfiguration SIP Advanced SipTlsDhKeySize: "2048"***

This step does **not** apply to most systems. It only affects systems with advanced account security configured and FIPS enabled.

Process to Upgrade a Clustered System

Caution To avoid the risk of configuration data being lost and to maintain service continuity, UPGRADE THE PRIMARY PEER FIRST and then upgrade the subordinate peers ONE AT A TIME in sequence.

We recommend upgrading the Expressway-E cluster first, followed by the Expressway-C (in each case start with the primary peer). This ensures that when Expressway-C starts a new traversal session toward Expressway-E, the Expressway-E is ready to process it. Starting with the primary peer, upgrade the cluster peers in sequence as follows:

Step 1 Sign in to the Expressway/Cisco VCS web user interface as *admin*.

Step 2 Back up the Expressway/Cisco VCS before you upgrade (**Maintenance** > **Backup and restore**).

Note If the cluster peers are running different versions of the Expressway/Cisco VCS, do not make any configuration changes other than the settings required to upgrade. The cluster does not replicate any configuration changes to the subordinate peers that are running on different versions from the primary Expressway/Cisco VCS.

Step 3 Enable maintenance mode so that the peer does not process any new incoming calls (**Maintenance** > **Maintenance mode**). Existing calls continue until the call is terminated. Other peers in the cluster continue to process calls.

Step 4 Wait for all calls to clear and registrations to timeout.

To manually remove any calls or registrations that don't clear automatically, use the **Status** > **Calls** page or the **Status** > **Registrations** > **By device** page respectively (SIP calls may not clear immediately).

Note You can leave the registration for Conference Factory (if enabled) – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration.

Step 5 Go to **Maintenance** > **Upgrade** to access the **Upgrade** page.

Step 6 Click **Browse** and select the software image file for the component you want to upgrade. The Expressway/Cisco VCS automatically detects which component you are upgrading based on the selected software image file.

Step 7 Click **Upgrade**. This step uploads the software file but does not install it. The upload may take a few minutes to finish.

Step 8 For upgrades to the **System platform** component, the **Upgrade confirmation** page is displayed:

a. Check the following details:

- **New software version** number is as expected.
- **MD5 hash** and **SHA1 hash** values match the values displayed on the cisco.com page, where you downloaded the software image file.

b. Click **Continue with upgrade**. This step installs the new software.

The **System upgrade** page opens and displays a progress bar while the software installs.

A summary of any active calls and registrations is displayed when the software completes installing (the calls and registrations will be lost when you reboot the system in the next step).

c. Click **Reboot system**. Any configuration changes made between uploading the software tar file and rebooting, will be lost when the system restarts.

Sometimes the web browser interface times out during the restart process, after the progress bar reaches the end. This may occur if the Expressway/Cisco VCS carries out a disk file system check – approximately once every 30 restarts.

Ignore any cluster-related alarms and warnings that occur during the upgrade process, such as cluster communication failures or cluster replication errors. These are expected and will resolve when all cluster peers are upgraded and after cluster data synchronization (typically within 10 minutes of the complete upgrade).

After the reboot is complete the **Login** page displays.

Step 9 For upgrades to other components (not the System platform) the software is automatically installed and no reboot is required.

Step 10 Repeat the previous steps for each peer in sequence until all peers are on the new software version.

What Next?

1. Verify the new status of each Expressway (including the primary):
   a. Go to **System** > **Clustering** and check that the cluster database status reports as **Active**.

b. Check the configuration for items from the System, Configuration, and Application menus.

2. Backup the Expressway again (**Maintenance** > **Backup and restore**).
3. If you use MRA, and you are upgrading from X8.9.x or earlier, reconfigure the MRA access control settings as described in "Appendix 2: Post-Upgrade Tasks for MRA Deployments" in the *Mobile and Remote Access Deployment Guide*.
4. If you have components that require option keys to enable them, do this from the **Maintenance** > **Option keys** page.
5. If the Expressway has FIPS mode enabled (that is, it's a FIPS140-2 cryptographic system) then from X12.6 you must manually change the default SIP TLS Diffie-Hellman key size from the default 1024 bits, to 2048 or greater. To do this type the following command in the Expressway command line interface (change the value in the final element if you want a key size higher than 2048): ***xconfiguration SIP Advanced SipTlsDhKeySize: "2048"***

   This step does **not** apply to most systems. It only affects systems with advanced account security configured and FIPS enabled.
6. (Optional) If for any reason you want to change the default TLS version, the *Cisco Expressway Certificate Creation and Use Deployment Guide* explains how to set the TLS version on each peer.

The software upgrade on the Expressway cluster is now complete.

Upgrading Using Secure Copy (SCP/PSCP)

Optionally use this process to upgrade using a secure copy program such as SCP or PSCP (part of the PuTTY free package) to transfer the file containing the software image onto the system.

Before you begin

The process requires the software image file to be manually renamed to the filename expected by the system. We recommend that you upload the file with its default name (similar to *s42700xXX_XX_XX.tar.gz*) and rename it only when you are ready to start (install) the upgrade. This provides better control of the process and also lets you check the file size before you proceed.

Depending on the software version, you may also need to install the *release-key* file.

Step 1 Upload the software image file.

- For the **System platform** component, upload to the /tmp folder on the system. For example: *scp s42700x12_5_7.tar.gz root@10.0.0.1:/tmp/s42700x12_5_7.tar.gz*
- For other components, upload to the */tmp/pkgs/new/* folder on the system, keeping the file name and extension unchanged. For example: *scp root@10.0.0.1:/tmp/pkgs/new/vcs-lang-es-es_8.1_amd64.tlp*

Step 2 Wait for the file upload to complete and then check the file size.

Note The default */tmp/tandberg-image.tar.gz* file entry in */tmp* will be 0 bytes.

Step 3 When you are ready to start the upgrade, rename (or move) the file to the required filename of */tmp/tandberg-image.tar.gz* (this will start the upgrade process).

For example: *mv /tmp/s42700x12_5_7.tar.gz /tmp/tandberg-image.tar.gz*

Step 4 Enter the root password when prompted. The software installation begins automatically and you see "*Software upgrade in progress*" on the SSH/console.

Step 5 Wait until the software has installed completely and you see "*Upgrade complete! The new software will be used on the next reboot*".

Step 6 We recommend that you reboot the system immediately, because any further configuration changes made before the reboot **will be lost when the system restarts**.

Upgrading Using APIs

Before you begin

The process requires the software image file to be placed manually in a SFTP server.

For request parameters and more information, refer to *REST API Summary Guide*.

Step 1 Add SFTP details with the following API

PUT https://<Expressway FQDN or IPaddress>/api/v1/provisioning/common/sftpconfig

Step 2 Trigger Upgrade with the following API

POST https://<Expressway FQDN or IPaddress>/api/v1/provisioning/common/upgrade

Step 3 Check UpgradeStatus with the following API

GET https://<Expressway FQDN or IPaddress>/api/v1/status/common/upgradestatus

Upgrading Firmware (Physical Appliances Only)

This section applies if Expressway is deployed on a physical appliance, and you need to upgrade the firmware for some reason.

Use the Cisco Host Upgrade Utility (HUU) to perform the upgrade. This is Cisco's dedicated tool for upgrading firmware components on a UCS C-Series server. Detailed instructions about using the HUU are available in the latest *Cisco Host Upgrade Utility User Guide* on the Cisco UCS C-Series Rack Servers documentation page.

Known Issues and Workarounds

Upgrade failure due to "Unique index collision" error

From X14.2.1 release, duplicate entries are not allowed in the CDB table **serviceConfiguration**. Due to this, upgrades from a previous version (which have duplicate entries in 'serviceConfiguration' table) fail with the below error.

Error: Upgrade fails with the following error in developer logs.

```
"Unique index collision: The value already exists in the table"
Table="serviceConfiguration""
```

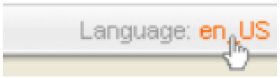
Cause: A 'UNIQUE' qualifier is introduced on the 'name' field of the table.

Due to this, upgrades from any previous version (which have duplicate entries in the 'serviceConfiguration' table) to a version higher or equal to X14.2.1 fails with a unique index collision error.

Solution: For technical assistance, contact Cisco Technical Assistance Center (TAC) team for a workaround script to delete duplicate entries before retrying the upgrade (bug ID CSCwd38155 refers).

Configuring Language Settings

The **Language** page (**Maintenance** > **Language**) controls which language is used for text displayed in the web user interface.

 453657	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.

For the list of available languages, see the relevant release notes for your software version.

Note

- 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.

To install a .tlp language pack file:

Step 1 Go to **Maintenance** > **Language**.

Step 2 Click **Browse** and select the **.tlp** language pack you want to upload.

Step 3 Click **Install**.

The selected language pack is then verified and uploaded. This may take several seconds.

Step 4 Repeat steps 2 and 3 for any other languages you want to install.

Removing Language Packs

To remove a language pack:

Step 1 Go to the **Language** page (**Maintenance** > **Language**).

Step 2 From the list of installed language packs, select the language packs you want to remove.

Step 3 Click **Remove**.

Step 4 Click **Yes** when asked to confirm.

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:

- Bootstrap key (from X8.11)
- 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)

Log files are not included in backup files.

For detailed backup and restore procedures, see Creating a System Backup, and Restoring a Previous Backup.

Clustered Systems

For more details about backing up and restoring peers in a cluster, see

Cluster Upgrades, Backup, and Restore.

Creating a System Backup

Before you Begin

- Backup files are always encrypted (from X8.11). In particular because they include the bootstrap key, and authentication data and other sensitive information.
- Backups can only be restored to a system that is running the **same version of software from which the backup was made**.
- You can create a backup on one Expressway and restore it to a different Expressway. For example if the original system has failed. 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

- All backups must be password protected.
- If you restore to a previous backup, and the administrator account password has changed since the backup was done, you must also provide the old account 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:

Step 1 Go to **Maintenance** > **Backup and restore**.

Step 2 Enter an **Encryption password** to encrypt the backup file.

Caution The password will be required in future if you ever want to restore the backup file.

Step 3 Click **Create system backup file**.

Step 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.

Step 5 When the backup is ready, you are prompted to save it. The default filename uses format: **<software version>_<hardware serial number>_<date>_<time>_backup.tar.gz.enc**. Or if you use Internet Explorer, the default extension is **.tar.gz.gz**. (These different filename extensions have no operational impact, and you can create and restore backups using any supported browser.)

Step 6 Save the backup file to a secure location.

Restoring a Previous Backup

Before you Begin

Caution When you restore an Expressway-E onto a CE1200 appliance from a CE1100 or earlier appliance backup, the CE1200 appliance may restore as Expressway-C. This issue occurs if the service setup wizard was used in the CE1100 or earlier appliance to change the type to Expressway-C and you skipped the wizard without completing the entire configuration. To avoid this issue, before you back up the appliance, run the service setup wizard, change the type to Expressway-E, and ensure that you complete the wizard.

- You need the password for the backup file from which you intend to restore.
- If you are restoring a backup file from a different Expressway, you need to apply the same set of license keys as exist on the system from which you intend to restore.
- 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**.
- 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:
  1. Upgrade the software version to the required later version.
  2. 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.

Passwords

- Backups must be password protected.
- If you restore to a previous backup, and the administrator account password has changed since the backup was done, you must also provide the old account 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:

Step 1 First do a factory reset, as described in Restoring the Default Configuration (Factory Reset) (Factory Reset). 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.

Step 2 Upgrade the system to the software version that was running when you made the backup.

- For standalone systems, see *Upgrade instructions*.
- For clustered systems, see the *Expressway Cluster Creation and Maintenance Deployment Guide*.

Step 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.

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 and registrations 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.

Step 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).

Checking the Effect of 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:

- Configuring Pre-Search Transforms to specify aliases to be transformed before any searches take place

- Configuring 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:

Step 1 Enter an **Alias** against which you want to test the transform.

Step 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.

Step 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.

Step 1 Enter the **Alias** you want to locate.

Step 2 Enter the **Hop count** for the search.

Step 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.

Step 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.

Step 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).

Step 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.)

Step 7 Click **Locate** to start to 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 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
- Local Outbound Ports
- Remote Listening Ports

On Expressway-E you can also configure the specific listening ports used for firewall traversal via **Configuration** > **Traversal** > **Ports**.

See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series configuration guides page.

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.

Note This firewall configuration is particularly important if this Expressway is a traversal client or traversal server, in order for Expressway firewall traversal to function correctly.

See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series configuration guides page.

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.

Note This firewall configuration is particularly important if this Expressway is a traversal client or traversal server, in order for Expressway firewall traversal to function correctly.

See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series configuration guides page.

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.

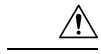
Your firewall must be configured to allow traffic originating from the local Expressway to the remote devices identified by the IP addresses and IP ports listed on this page.

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.

See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series configuration guides page.

Restarting, Rebooting, and Shutting Down

The **Restart options** page (**Maintenance** > **Restart options**) allows you to restart, reboot, or shut down the Expressway without having physical access to the hardware.



Caution Do not restart, reboot or shut down the Expressway while the red ALM LED on the front of the unit is on. This indicates a hardware fault. Contact your Cisco customer support representative.

Restarting

The restart function shuts down and restarts the Expressway application software, but not the operating system or hardware. A restart takes approximately 3 minutes.

A restart is typically required in order for some configuration changes to take effect, or when the system is being added to, or removed from, a cluster. In these cases a system alarm is raised and will remain in place until the system is restarted.

If the Expressway is part of a cluster and other peers in the cluster also require a restart, we recommend that you wait until each peer has restarted before restarting the next peer.

Rebooting

The reboot function shuts down and restarts the Expressway application software, operating system and hardware. A reboot takes approximately 5 minutes.

Reboots are normally only required after software upgrades and are performed as part of the upgrade process. A reboot may also be required when you are trying to resolve unexpected system errors.

Shutting down

A shutdown is typically required if you want to unplug your unit, prior to maintenance or relocation for example. The system must be shut down before it is unplugged. Avoid uncontrolled shutdowns, in particular the removal of power to the system during normal operation.

Effect on active calls

Any of these restart options will cause all active calls to be terminated. (If the Expressway is part of a cluster, only those calls for which the Expressway is taking the signaling will be terminated.)

For this reason, the **System status** section displays the number of current calls so you can check these before you restart the system. If you do not restart the system immediately, you should refresh this page before restarting to check the current status of calls.

If **Mobile and remote access** is enabled, the number of currently provisioned sessions is displayed (Expressway-C only).

Restarting, rebooting or shutting down using the web interface

To restart the Expressway using the web interface:

1. Go to **Maintenance** > **Restart options**.
2. Check the number of calls currently in place.
3. Click **Restart**, **Reboot**, or **Shutdown** as appropriate and confirm the action.

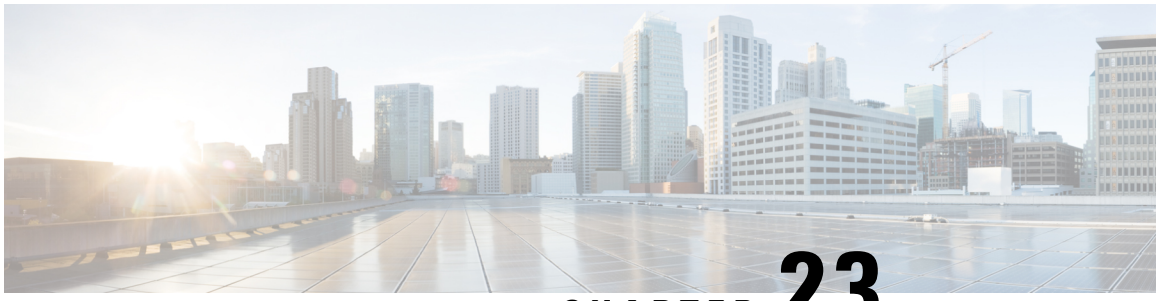
   Sometimes only one of these options, such as **Restart** for example, may be available. This typically occurs when you access the **Restart options** page after following a link in an alarm or a banner message.

   - Restart/reboot: the **Restarting/Rebooting** page appears, with an orange bar indicating progress.

After the system has successfully restarted or rebooted, you are automatically taken to the **Login** page.

- Shutdown: the **Shutting down** page appears.

  This page remains in place after the system has successfully shut down but any attempts to refresh the page or access the Expressway will be unsuccessful.



CHAPTER 23

Diagnostics and Troubleshooting

- Network Utilities, on page 471
- Diagnostics Tools, on page 478
- Incident Reporting, on page 484
- Developer Resources, on page 487

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.
- SRV Connectivity Tester: allows you to check DNS for specific service records, and verify connectivity to the returned hosts.

Ping

The **Ping** tool (**Maintenance** > **Tools** > **Network utilities** > **Ping**) can be used to assist in troubleshooting system issues.

It allows you to check that a particular host system is contactable and that your network is correctly configured to reach it. It reports details of the time taken for a message to be sent from the Expressway to the destination host system.

To use this tool:

1. In the **Host** field, enter the IP address or hostname of the host system you want to try to contact.
2. Click **Ping**.

A new section will appear showing the results of the contact attempt. If successful, it will display the following information:

Host	The hostname and IP address returned by the host system that was queried.
Response time (ms)	The time taken (in ms) for the request to be sent from the Expressway to the host system and back again.

Traceroute

The **Traceroute** tool (**Maintenance** > **Tools** > **Network utilities** > **Traceroute**) can be used to assist in troubleshooting system issues.

It allows you to discover the route taken by a network packet sent from the Expressway to a particular destination host system. It reports the details of each node along the path, and the time taken for each node to respond to the request.

To use this tool:

1. In the **Host** field, enter the IP address or hostname of the host system to which you want to trace the path.
2. Click **Traceroute**.

A new section will appear with a banner stating the results of the trace, and showing the following information for each node in the path:

TTL	(Time to Live). This is the hop count of the request, showing the sequential number of the node.
Response	This shows the IP address of the node, and the time taken (in ms) to respond to each packet received from the Expressway. *** 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)

Note To facilitate proper reverse lookup, give the domain in the form of 152.50.10.in-addr.arpa (the subnet of addresses would be 10.50.152.0/24) and the target DNS server in the address. This sends all requests in the subnet to the target DNS server instead of the default server.

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>**.

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	`IN` (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**.

Transport protocols

The Expressway uses UDP and TCP to do DNS resolution, and DNS servers usually send both UDP and TCP responses. If the UDP response exceeds the UDP message size limit of 512 bytes, then the Expressway cannot process the UDP response. This is not usually a problem, because the Expressway can process the TCP response instead.

However, if you block TCP inbound on port 53, and if the UDP response is greater than 512 bytes, then the Expressway cannot process the response from the DNS. In this case you won't see the results using the DNS lookup tool, and any operations that need the requested addresses will fail.

However, if you block TCP inbound on port 53, and if the UDP response is greater than 512 bytes, then the Expressway cannot process the response from the DNS. In this case you won't see the results using the DNS lookup tool, and any operations that need the requested addresses will fail.

SRV Connectivity Tester

The SRV connectivity tester is a network utility that tests whether the Expressway can connect to particular services on a given domain. You can use this tool to proactively test your connectivity while configuring Expressway-based solutions such as Cisco Webex Hybrid Call Service or business-to-business video calling.

You specify the DNS Service Record Domain and the Service Record Protocols you want to query for that domain. The Expressway does a DNS SRV query for each specified protocol, and then attempts TCP connections to the hosts returned by the DNS. If you specify TLS, the Expressway only attempts a TLS connection after the TCP succeeds.

The Expressway connectivity test page shows the DNS response and the connection attempts. For any connection failures, the reason is provided along with advice to help with resolving specific issues.

To troubleshoot connectivity, you can download the TCP data from your test in *.pcap* format. You can selectively download a dump of the DNS query, or a specific connection attempt, or you can get a single *.pcap* file showing the whole test.

To use this tool:

1. Go to **Maintenance** > **Tools** > **Network utilities** > **Connectivity test**
2. Enter a **Service Record Domain** you want to query, for example, `callservice.webex.com`.
3. Enter the **Service Record Protocols** you want to test, for example, `_sips._tcp`.

   Use commas to delimit multiple protocols, for example, `_sip._tcp,_sips._tcp`.
4. Click **Run**

The Expressway queries DNS for SRV records comprised of the service, protocol and domain combinations, for example: `_sip._tcp.callservice.webex.com` and `_sips._tcp.callservice.webex.com`.

By default the system will submit the query to all of the system's default DNS servers (**System** > **DNS**).

Service Record Options

Here are some of the _service._protocol combinations you might need to test in your deployments:

- _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>
- _cms-web._tls.<domain>
- _sipfederationtls._tcp.<domain>

Test Results

A section at the bottom of the page shows the query results and the connectivity test results. Test results will have some or all of the following information:

Table 23: Connectivity Test Results - DNS SRV Lookup

Result field	Description
Stage	The stage of the test; there is one stage for each response to your query and another one for the overall query result.
Service Record	The SRV records that were found, from the set that you queried.
Result	The hosts mapped by the DNS SRV record, if the test succeeded. Also shows the priority, weight, and port of each entry, if they are defined in the DNS record.
Hint	This field holds no value in this table of results.
TCP Dump	For the overall result, you can download a .pcap file that contains the TCP record of the SRV query.

Table 24: Connectivity Test Results - TCP Connections

Result	Description
Stage	The stage of the test; there is one test for each host that was returned for the queried service on TCP protocol. There is also a collective result of all tests.
Target	The hostname returned by DNS SRV query.
Result	Shows that the test completed successfully, or gives the reason for failure, if known.
Hint	A pointer that might help you troubleshoot unsuccessful tests.
TCP Dump	You can download a .pcap file that contains the TCP record of the specific connection attempt.

Table 25: Connectivity Test Results - TLS Connections

Result field	Description
Stage	The stage of the test. For each host, one to three tests are returned for the queried service on TLS protocol. The test is performed using each TLS version that is supported by the host, in the following order: • TLS 1.2 • TLS 1.1 • TLS 1 For example, if the host supports all three versions and the connection is successful using the TLS 1.1 version then the check returns two tests. There is also a collective result of all tests. **Note** If the Expressway cannot establish a TCP connection to a host, it does not attempt a TLS connection to that host.
Target	The hostname returned by DNS SRV query.
Result	Shows that the test completed successfully, or gives the reason for failure, if known.
Hint	A pointer that might help you troubleshoot unsuccessful tests.
TCP Dump	You can download a .pcap file that contains the TCP record of the specific connection attempt.

Diagnostics Tools

This section provides information about how to use Expressway diagnostics tools:

- Configuring Diagnostic Logging
- Creating a System Snapshot
- Configuring Network Log Levels and Configuring Support Log Levels advanced logging configuration tools
- Incident Reporting

Expressway supports 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 assist with troubleshooting. You can generate a diagnostic log of system activity over a period of time, and download it to send to your Cisco customer support representative. You can also obtain and download a *tcpdump* while logging is in progress.

Before You Begin

- Only one diagnostic log can be generated at a time. Creating a new diagnostic log replaces any previously produced log.
- Expressway continually logs relevant system activity. The diagnostic logging function extracts the activity from the start of the diagnostic logging time to when diagnostic logging is stopped and provides a convenient web-based download facility.
- **Restart/Reboot:** Only diagnostic log will be collected; other files will be missing from the bundle.
- When you start a diagnostic log, the relevant system modules have their log levels automatically set to "debug". Ignore any resulting *Verbose log levels configured* alarms, as the log levels will get reset to their original values when you stop logging.
- Diagnostic logging is controlled through the web interface. There is no CLI option.
- When tcpdump option is selected, a maximum of 2 packet 3 packet capture files are created per network interface, each with a maximum size of 20MB (i.e., up to 4 files with a total size of 80MB could be created on an Expressway with dual network interfaces).

Note From X14.0, the number of .pcap files are increased up to 20 per network interface so, the tcpdump can run continuously through web UI. Maximum file size is still 20 MB.

Caution Enabling diagnostic logging can affect the performance of your system. You should only collect diagnostic logs on the advice of Cisco customer support or during periods of lighter traffic load.

Process to Generate the Diagnostic Log

1. Go to **Maintenance** > **Diagnostics** > **Diagnostic logging**
2. (Optional) Select *Take tcpdump while logging*. You can select this option to take a tcpdump while diagnostic logging is in progress. The tcpdump can be downloaded as a separate file on logging completion.

Note Now administrator can provide **IP address** and **Port** filters if tcpdump is enabled on the user interface.

The tcpdump filters are used if the administrator wants to see packets coming from a specific host (IP address or Fully Qualified Domain Name (FQDN)) and/or port in pcap files. The administrator can provide the values in the fields identified to get the filtered packets. From version X14.0, tcpdump captures 20 pcap files per LAN and every pcap file is 20MB in size.

The table represents the average time (in seconds) taken to generate 1 pcap file (20MB max) and 20 pcap files depending upon the number of registrations.

Expressway C:

	20MB	**400MB**
5 users	2	40
20 users	2	40
2500 users	10	200

Expressway E:

	20MB	**400MB**
5 users	1	20
20 users	1	20
2500 users	2	40

These numbers are specific to the environment used for troubleshooting. We have used 1 node and Mobile and Remote Access (MRA) video while running this performance test.

3. Enter **Filter tcpdump by IP address**.
4. Enter **Filter tcpdump by port**. Range is 1 to 65536.
5. Click **Start new log**.
6. (Optional) Enter some **Marker** text and click **Add marker**.

- You can use the marker facility to add comment text to the log file before certain activities are performed. This helps to subsequently identify specific sections in the diagnostic log file. Marker text has a `DEBUG_MARKER` tag in the log file.
- You can add as many markers as required, at any time while the diagnostic logging is in progress.

7. Reproduce the system issue you want to trace in the diagnostic log.
8. Click **Stop logging**.
9. Click **Collect log**.
10. When the log collection completes, 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).

Files contained in the diagnostic log archive

- 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) eth *n*_diagnostic_logging_tcpdump x_<*system host name*>_<*timestamp*>.pcap - containing the packets captured during the logging period
- ca_<*system host name*>_<*timestamp*>.pem
- server_<*system host name*>_<*timestamp*>.pem

These files can be sent to your Cisco support representative if you are asked 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.

Link to Collaboration Solutions Analyzer tool

You can optionally use the **Analyze log**, to open a link to the Collaboration Solutions Analyzer troubleshooting tool.

To download logs again

To download the logs again, you can re-collect them by using the **Collect log** button. If the button is grayed out, refresh the browser page.

Clustered Systems

If the Expressway is part of a cluster, 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 *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**.

XCP Routing Information

This improvement displays content of the Extensible Communications Platform (XCP) routing table. This content is a complete data dump of the XCP routing information contained in Cisco Jabber. This information is useful for debugging from the XCP point of view. It is made available both in the **routing.xml** file on the VCS device and in the **developer.xcp.jabber logs**.

Additionally, the ConnectionManager information is also available as a data dump through developer logs. This information displays the state of ConnectedSockets and FailedRequests counters.

All this information will help administrators to check the routing information, the number of connections, and details of each Jabber client connection.

Implementation

Information is made available in the following files -

- **routing.xml** file under `/tmp/xml` location which contains XCP route information.
- Additional logging for XCP route information in developer logs in **developer.xcp.jabber logs**.

XCP Routing Graph Representation

This section details the structure of the **routing.xml** file. It contains multiple structures. For more information, see Table 26: List of Element(s) and their Description.

XML Syntax

```
> <RoutingGraph>
             > <Edges>
               ...
               </Edges>
             > <RealmsToEdges>
               ...
               </RealmsToEdges>
             > <VersionsToEdges>
               ...
               </VersionsToEdges>
             > <BestHops>
               ...
               </BestHops>
             > <LastHops>
               ...
               </LastHops>
               <Orphans/>
               <from>vmx144-032-p-extend1-corpb-rd-rusc1abs-cisco-com</from>
               <num_edges>2</num_edges>
               <num_vertices>3</num_vertices>
             > <Connections>
               ...
               </Connections>
             > <RealmsToConnections>
               ...
               </RealmsToConnections>
             > <CompToDomains>
               ...
               </CompToDomains>
              > <DomainToComps>
                ...
                </DomainToComps>
              > <IdRealms>
                ...
                </IdRealms>
           </RoutingGraph>
```

The table describes the various elements used in the *routing.xml* file.

Table 26: List of Element(s) and their Description

Element(s)	Description
Edges	Associate JIDs of local and remote Realms
RealmsToEdges	Multimap of JID to Edges
VersionsToEdges	Multimap of Version to Edges
BestHops	Hash map of Realm JID to JID distance
LastHops	The result when BestHops was last computed successfully
Orphans	Vertices without edges
from	The last vertex that BestHops are computed from
num_edges	Number of edges
num_vertices	Number of nodes
Connections	Associate remote Realm JID and corresponding component
RealmsToConnections	Map of connection JID to component that supports it
CompToDomains	Map of component JID to set of routable JIDs
DomainToComps	Map of routable JID to set of component JIDs
IdRealms	Map of component JID to pair of Realm JID and available type

Incident Reporting

The incident reporting feature for Expressway automatically saves information about critical system issues such as application failures. This section describes how to view incident reports.

It also describes how to send incident reports to Cisco customer support, either manually or automatically. The information in the 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 Report Details 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 Viewing Incident Reports page.

Enabling Automatic Incident Reporting

Read the Incident Reporting Caution: Privacy-Protected Personal Data 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 Viewing Incident Reports from the **Incident detail** page.

Sending Incident Reports Manually

Read the Incident Reporting Caution: Privacy-Protected Personal Data before you decide whether to send an incident report manually to Cisco.

To send an incident report manually to Cisco customer support:

1. Go to **Maintenance** > **Diagnostics** > **Incident reporting** > **View**.
2. Click on the incident you want to send. You will be taken to the **Incident detail** page.

3. Scroll down to the bottom of the page and click **Download incident report**. You will be given the option to save the file.
4. Save the file in a location from where it can be forwarded to Cisco customer support.

Removing Sensitive Information from a Report

The details in the downloaded incident report are Base64-encoded, so you will not be able to meaningfully view or edit the information within the file.

If you need to edit the report before sending it to Cisco (for example, if you need to remove any potentially sensitive information) you must copy and paste the information from the **Incident detail** page into a text file, and edit the information in that file before sending it to Cisco.

Viewing Incident Reports

The **Incident view** page (**Maintenance** > **Diagnostics** > **Incident reporting** > **View**) shows a list of all incident reports that have occurred since the Expressway was last upgraded. A report is generated for each incident, and the information contained in these reports can then be used by Cisco customer support to diagnose the cause of the failures.

For each report the following information is shown:

Field	Description
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: *Pending*: indicates that the incident has been saved locally but not sent. *Sent*: indicates that details of the incident have been sent to the URL specified in the Incident Reporting page.

To view the information contained in a particular incident report, click on the report's **Time**. You will be taken to the Incident Report Details 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.
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).
Username	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 Incident Reporting Caution: Privacy-Protected Personal Data regarding privacy-protected personal data before you decide whether to enable automatic incident reporting.

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
- Experimental Menu

Debugging and System Administration Tools

Caution These features are not intended for customer use unless on the advice of a Cisco support representative. Incorrect usage of these features could cause the system operation to become unstable, cause performance problems and cause persistent corruption of system configuration.

The Expressway includes a number of debugging and system admin tools that allow administrators to inspect what is happening at a detailed level on a live system, including accessing and modifying configuration data and accessing network traffic.

To access these tools:

1. Open an SSH session.
2. Log in as admin or root as required.
3. Follow the instructions provided by your Cisco support representative.

Experimental Menu

The Expressway web interface contains a number of pages that are not intended for use by customers. These pages exist for the use of Cisco support and development teams only. Do not access these pages unless it is under the advice and supervision of your Cisco support representative.

Caution Incorrect usage of the features on these pages could cause the system operation to become unstable, cause performance problems and cause persistent corruption of system configuration.

To access these pages:

1. Go to `https://<Expressway host name or IP address>/setaccess`.

   The **Set access** page appears.
2. In the **Access password** field, enter `qwertsys`.
3. Click **Enable access**.

A new top-level **Experimental** menu will appear to the right of the existing menu items.

Enabling or Disabling CDB API Access

Considering the Security of the Expressway product, access to CDB API has been disabled by default. They can be enabled or disabled using the Web User Interface or through REST API. Enabling or Disabling of CDB API Access is implemented across the cluster.

Caution Enabling this feature provides access to numerous experimental Database Rest APIs with exposure to Security vulnerabilities. These are not intended for use on a production system. Use of this feature will be at your own risk.

CDB REST APIs are available in the **Experimental** menu -> **API** -> **DATABASE REST API**. Here the status of CDB REST API Access is displayed which is disabled by default.

Enable CDB API Access

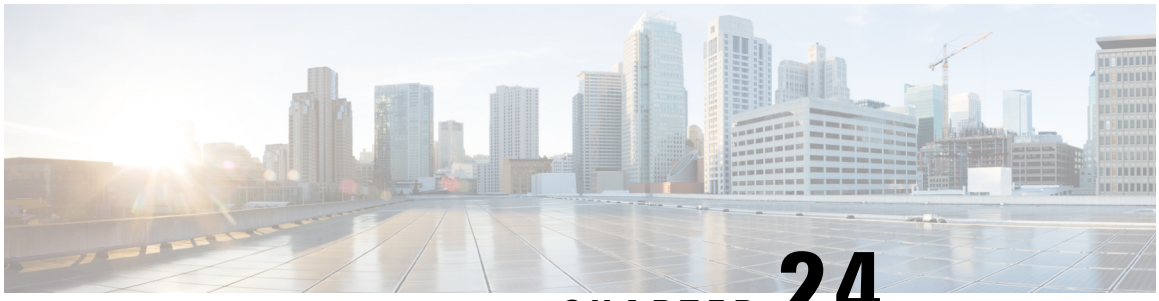
In the **Experimental** menu -> **API** -> **DATABASE REST API** page, click **Enable CDB API Access**.

This will enable the CDB API Access (across the cluster if applicable).

Disable CDB API Access

In the **Experimental** menu -> **API** -> **DATABASE REST API** page, click **Disable CDB API Access**.

This will disable the CDB API Access (across the cluster if applicable).



CHAPTER 24

Reference Material

- About Event Log Levels, on page 491
- CPL Reference, on page 502
- LDAP Server Configuration for Device Authentication, on page 512
- Using the Collaboration Solutions Analyzer Tool, on page 517
- Changing the Default SSH Key, on page 518
- Restoring the Default Configuration (Factory Reset), on page 518
- Pattern Matching Variables, on page 520
- Port Reference, on page 522
- Regular Expressions, on page 522
- Supported Characters, on page 524
- Product Identifiers and Corresponding Keys, on page 525
- Allow List Rules File Reference, on page 530
- Allow List Tests File Reference, on page 532
- Expressway Multitenancy Overview, on page 533
- Multitenant Expressway Sizing, on page 534
- Alarms Reference, on page 536
- Command Reference — xConfiguration, on page 602
- Command Reference — xCommand, on page 685
- Command Reference — xStatus, on page 722
- External Policy Overview, on page 724
- Flash Status Word Reference Table, on page 727
- Supported RFCs, on page 728
- Software Version History, on page 731
- Legal Notices, on page 740

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: • 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: • protocol keepalives • call-related SIP signaling messages
4	The most verbose level: all Level 1, Level 2 and Level 3 events, plus: • 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: • **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.

Field	Description
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 Message Details 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.

Name	Description
Protocol	Specifies which protocol was used for the communication. Valid values are: • 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: • H.323 • SIP • H.225 • H.245 • LDAP • Q.931 • NeighbourGatekeeper • Clustering • ConferenceFactory
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.

Name	Description
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	• 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.
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.

Name	Description
Level	The level of the event as defined in the About Event Log Levels section.
UTC Time	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

Event	Description	Level
Authorization Failure	The user has either entered invalid credentials, does not belong to an access group, or belongs to a group that has an access level of "None". Applies when remote authentication is enabled.	1
Beginning System Backup	A system backup has started.	1
Beginning System Restore	A system restore has started.	1
Call Answer Attempted	An attempt to answer a call has been made.	1
Call Attempted	A call has been attempted.	1
Call Bandwidth Changed	The endpoints in a call have renegotiated call bandwidth.	1
Call Connected	A call has been connected.	1
Call Diverted	A call has been diverted.	1
Call Disconnected	A call has been disconnected.	1
Call Inactivity Timer	A call has been disconnected due to inactivity.	1
Call Rejected	A call has been rejected. The **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 *On* 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

Event	Description	Level
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.	
External Server Communication Failure	Communication with an external server failed unexpectedly. The **Detail** event parameter should differentiate between “no response” and “request rejected”. Servers concerned are: • DNS • LDAP Servers • Neighbor Gatekeeper • NTP servers • Peers	
Hardware Failure	There is an issue with the Expressway hardware. If the problem persists, contact your Cisco support representative.	
License Limit Reached	Licensing limits for a given feature have been reached. The **Detail** event parameter specifies the facility/limits concerned. If this occurs frequently, you may want to contact your Cisco representative to purchase more licenses.	
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

Event	Description	Level
Message Rejected	This could be for one of two reasons: • 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.	
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
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

Event	Description	Level
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: • 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
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

Event	Description	Level
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
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

Event	Description	Level
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 Configuring Call Policy Using a CPL Script and used to validate your script before uploading to the Expressway.

The following example shows the correct use of namespaces to make the syntax acceptable:

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="destination">
   <address is="reception@example.com">
    <proxy/>
   </address>
  </address-switch>
 </taa:routed>
</cpl>
```

Source and destination address formats

When the descriptions in this section refer to the source or destination aliases of a call, this means all supported address formats (URIs, IP addresses, E.164 aliases and so on).

CPL Address-Switch Node

The `address-switch` node allows the script to run different actions based on the source or destination aliases of the call. It specifies which fields to match, and then a list of address nodes contains the possible matches and their associated actions.

The address-switch has two node parameters: `field` and `subfield`.

Address

The `address` construct is used within an `address-switch` to specify addresses to match. It supports the use of Regular Expressions.

Valid values are:

`is=string`	Selected field and subfield exactly match the given string.
`contains=string`	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.
`subdomain-of=string`	If the selected field is numeric (for example, the tel subfield) then this matches as a prefix; so `address subdomain-of="555"` matches `5556734` and so on. If the field is not numeric then normal domain name matching is applied; so `address subdomain-of="company.com"` matches `nodeA.company.com` and so on.
`regex="regular expression"`	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
`unauthenticated-origin`	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.

Field parameter attributes	SIP	H.323
`authenticated-origin` and `origin`	The "From" and "ReplyTo" fields of the message, if it authenticates correctly (or where the relevant **Authentication Policy** is *Treat as authenticated*), otherwise `not-present`.	The source aliases from the original LRQ or ARQ that started the call if it authenticated correctly (or where the relevant **Authentication Policy** is *Treat as authenticated*) otherwise `not-present`. Because SETUP messages are not authenticated, if the Expressway receives a SETUP without a preceding RAS message the origin will always be `not-present`.
`originating-zone`	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".	
`originating-user`	If the relevant **Authentication Policy** is *Check credentials* or *Treat as authenticated* this is the username used for authentication, otherwise `not-present`.	
`registered-origin`	If the call originates from a registered endpoint this is the list of all aliases it has registered, otherwise `not-present`.	
`destination`	The destination aliases.	
`original-destination`	The destination aliases.	

Note that any Authentication Policy settings that apply are those configured for the relevant zone according to the source of the incoming message.

If the selected field contains multiple aliases then the Expressway will attempt to match each address node with all of the aliases before proceeding to the next address node, that is, an address node matches if it matches any alias.

Subfield

Within the address-switch node, the optional subfield parameter specifies which part of the address is to be considered. The following table gives the definition of subfields for each alias type.

If a subfield is not specified for the alias type being matched then the `not-present` action is taken.

`address-type`	Either `h323` or `sip`, based on the type of endpoint that originated the call.
`user`	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.

`host`	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.
`tel`	For E.164 numbers this selects the entire string of digits.
`alias-type`	Gives a string representation of the type of alias. The type is inferred from the format of the alias. Possible types are: • 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.

`Clear = "yes" | "no"`	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.

`url=string`	The new location to be added to the location set. The given string can specify a URL (for example, `user@domain.com`), H.323 ID or an E.164 number.
`priority=<0.0..1.0> | "random"`	Specified either as a floating point number in the range 0.0 to 1.0, or `random`, which assigns a random number within the same range. 1.0 is the highest priority. Locations with the same priority are searched in parallel.
`regex="<regular expression>"` `replace="<string>"`	Specifies the way in which a location matching the regular expression is to be changed.
`source-url-for-message="<string>"`	Replaces the From header (source alias) with the specified string.
`source-url-for-message-regex="<regular expression>"` together with `source-url-for-message-replace="<string>"`	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 CPL Address-Switch Node section.

The `message-regex` parameter allows a regular expression to be matched against the entire incoming SIP message.

Note Any rule containing a message-regex parameter will never match an H.323 call.

Proxy

On executing a proxy node the Expressway attempts to forward the call to the locations specified in the current location set. If multiple entries are in the location set then this results in a forked call. If the current location set is empty the call is forwarded to its original destination.

The proxy node supports the following optional parameters:

`timeout=<1..86400>`	Timeout duration, specified in seconds
`stop-on-busy = "yes" | "no"`	Whether to stop searching if a busy response is received

The proxy action can lead to the results shown in the table below:

`failure`	The proxy failed to route the call
busy	Destination is found but is busy
`noanswer`	Destination is found but does not answer
`redirection`	Expressway is asked to redirect the call
`default`	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.

In this example, only calls from users with authenticated source addresses are allowed. See About Device Authentication, 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.

In this example, user ceo will only accept calls from users `vpsales`, `vpmarketing` or `vpengineering`.

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|vpengineering">
      <!-- Allow the call -->
      <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.

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>
     <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

Note In this example, the administrator only wants to allow calls that originate from locally registered endpoints.

```
<?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.

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.

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.

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:

- Downloading the H.350 Schemas that must be installed on the LDAP server
- Install and configure two common types of LDAP servers for use with the Expressway:
  - Configuring a Microsoft Active Directory LDAP Server
  - Configuring an OpenLDAP Server

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 Downloading 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:

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.
- 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:

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.

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**.

Using the Collaboration Solutions Analyzer Tool

The *Collaboration Solutions Analyzer* is created by Cisco Technical Assistance Center (TAC) to help you with validating your deployment, and to assist with troubleshooting by analyzing Expressway log files. For example, you can use the Business to Business Call Tester to validate and test calls, including Microsoft interworked calls.

You need a customer or partner account to use the Collaboration Solutions Analyzer.

Getting started

1. If you plan to use the log analysis tool, first collect the Expressway logs.
2. Sign in to https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/

   From X12.6 you can use the **Analyze log** button on the **Diagnostic logging** page (**Maintenance** > **Diagnostics**) to open a link to the Collaboration Solutions Analyzer troubleshooting tool.
3. Click the tool you want to use. For example, to work with logs:
   a. Click **Log analysis**.
   b. Upload the log file(s).
   c. Select the files you want to analyze.

d. Click **Run analysis**.

The tool analyzes the log files and displays the information in a format which is much easier to understand than the raw logs. For example, you can generate ladder diagrams to show SIP calls.

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.

Before You Begin

If you've upgraded since the system was first set up, be aware that the reset reinstalls your latest software version.

The factory reset procedure is intended for system recovery after a serious failure. **It is NOT designed as a security mechanism to erase information from physical storage.** Do not rely on a reset to return the system

to a “clean” or “blank” secure state. The reset is intended just to return the system to a minimum configuration state.

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.)

Prerequisites

- As the virtual machine console is required to complete this process, **you need appropriate VMware access in order to open the VM console**.
- 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. 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.
  - 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*. You need to manually rename the downloaded version-specific tar file to *tandberg-image.tar.gz*.

Process to Reset to the Default Configuration

You must do this procedure from the console (or for hardware-based CE appliances you can optionally use 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

Prompt	Recommended response
Keep server certificate, associated key and CA trust store [YES/NO]? This option does *not* preserve SNI / domain certificates, which are always deleted regardless of what you respond. Only the server certificate and associated key and CA trust store are saved (if you respond YES).	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 VM boots, you are taken to the Install Wizard. You must complete the wizard through the VM console. Some of the questions in the wizard may be skipped depending on your responses in step 3, but even if you preserved the IP configuration and password, you still need to complete the Install Wizard through the VM console.

Note If you were using FIPS140 and you want to enable it again, see the section in this guide about Configuring FIPS140-2 Cryptographic Mode.

Resetting via USB Stick - CE Hardware Appliances

This section does not apply to virtualized, VM-based Expressways.

Cisco TAC may suggest an alternative reset method, to download the software image onto a USB stick and then reboot 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.

Note Reset functionality comes built in with the CE hardware appliances, through the Internal Recovery Partition (IRP). See the *CEnnnn Appliance Installation Guide* on the Install and Upgrade Guides page for more information.

Pattern Matching Variables

The Expressway makes use of pattern matching in a number of its features, namely About Allow and Deny Lists 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.

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 Checking the Effect of Pattern tool (**Maintenance** > **Tools** > **Check pattern**).

Port Reference

See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series configuration guides page.

Regular Expressions

Regular expressions can be used in conjunction with a number of Expressway features such as alias transformations, zone transformations, CPL policy and ENUM. The Expressway uses POSIX format regular expression syntax. The table below provides a list of commonly used special characters in regular expression syntax. This is only a subset of the full range of expressions available. For a detailed description of regular expression syntax see the publication *Regular Expression Pocket Reference*.

Character	Description	Example
.	Matches any single character.	
\d	Matches any decimal digit, i.e. 0-9.	
*	Matches 0 or more repetitions of the previous character or expression.	.* matches against any sequence of characters
+	Matches 1 or more repetitions of the previous character or expression.	
?	Matches 0 or 1 repetitions of the previous character or expression.	`9?123` matches against 9123 and 123
{n}	Matches n repetitions of the previous character or expression	`\d{3}` matches 3 digits
{n,m}	Matches n to m repetitions of the previous character or expression	`\d{3,5}` matches 3, 4 or 5 digits
[...]	Matches a set of specified characters. Each character in the set can be specified individually, or a range can be specified by giving the first character in the range followed by the - character and then the last character in the range. 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 (*)

Character	Description	Example
(...)	Groups a set of matching characters together. Groups can then be referenced in order using the characters \1, \2, etc. as part of a replace string.	A regular expression can be constructed to transform a URI containing a user's full name to a URI based on their initials. The regular expression `(.).*_(.).*(@example.com)` would match against the user `john_smith@example.com` and with a replace string of `\1\2\3` would transform it to `js@example.com`
|	Matches against one expression or an alternate expression.	`.*@example.(net|com)` matches against any URI for the domain `example.com` or the domain `example.net`
\	Escapes a regular expression special character.	
^	Signifies the start of a line. 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 Configuring Administrator Groups 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.

Product Identifiers and Corresponding Keys

Cisco PIDs (Product Identifiers) are also sometimes known as a product name, model name, or product number. These are examples of PIDs that can apply to Expressway, depending on the software version. Many have been phased out in later software versions - for example, a Release Key is no longer used from X12.5.4 for Cisco Expressway products.

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.

Feature or License Option	PID (Product Identifier)	Key Pattern	Valid On	Required For
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 Cisco Webex Hybrid Services)

Feature or License Option	PID (Product Identifier)	Key Pattern	Valid On	Required For
Rich Media Session licenses	LIC-EXP-RMS	116341Yn-m-#########	Expressway-C Expressway-E	Calls enabled by Expressway where the Expressway must process the media streams (also known as 'traverse' or 'handle' the media). RMS licenses are used by calls that require: • IPv4-IPv6 interworking • H.323-SIP interworking • Media encryption on behalf of another entity • Microsoft SIP to standards-based SIP interworking **Note:** If both endpoints are registered to the Cisco infrastructure RMS license is not required. RMS licenses are not used by CMR Cloud calls

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	Calls enabled by VCS where the VCS must process the media streams (also known as 'traverse' or 'handle' the media). Traversal call licenses are used by calls that require: • IPv4-IPv6 interworking • H.323-SIP interworking • Media encryption on behalf of another entity • Microsoft SIP to standards-based SIP interworking Traversal call licenses are not used by CMR Cloud calls
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 Expressway-E	Registering TelePresence rooms to Expressway-C.
Desktop system registration licenses	LIC-EXP-DSK	116341Bn-m-########	Expressway-C Expressway-E	Registering desktop endpoints to Expressway-C.

Feature or License Option	PID (Product Identifier)	Key Pattern	Valid On	Required For
TURN relay licenses	LIC-EXP-TURN	116341In-m-########	VCS Expressway Expressway-E	Jabber Guest, Microsoft Interoperability (offsite MS clients)
Traversal Server feature (not used in X12.6 and later)	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 Expressway-C	Multiple aliases managed by Cisco TMS. This key is not explicitly required, but does not interfere with operation if loaded.
Interworking H.323 to SIP feature	LIC-EXP-GW	116341G00-m-########	VCS Control VCS Expressway Expressway-C Expressway-E	This key is not explicitly required, but does not interfere with operation if loaded.
Device Provisioning feature	LIC-VCS-DEVPROV	116341P00-m-########	VCS Control Expressway-C	Provisioning endpoints with configuration and phonebook data from Cisco TMS. This key is not explicitly required, but does not interfere with operation if loaded.
Advanced Networking feature	LIC-EXP-AN	116341L00-m-########	VCS Expressway Expressway-E	Enabling second NIC and static NAT. This key is not explicitly required, but does not interfere with operation if loaded.

Feature or License Option	PID (Product Identifier)	Key Pattern	Valid On	Required For
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 27: Allow List Rule Arguments

Argument index	Parameter name	Required/Optional	Sample value
0	Url	Required	`protocol://host[:port][/path]` Where: • protocol is `http` or `https` • host may be a DNS name or IP address • :port is optional, and may only be : followed by one number in the range 0-65535, eg. `:8443` If the port is not specified, then the Expressway uses the default port for the supplied protocol (80 or 443) • /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. `"GET,PUT"`
3	MatchType	Optional	`exact` or `prefix` . Default is `prefix`
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 28: Allow List Test Arguments

Argument index	Parameter name	Required/Optional	Sample value
0	Url	Required	`protocol://host[:port][/path]` Where: • protocol is `http` or `https` • host may be a DNS name or IP address • :port is optional, and may only be : followed by one number in the range 0-65535 • /path is optional and must conform to HTTP specification
1	ExpectedResult	Required	`allow` or `block`. 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.

Argument index	Parameter name	Required/Optional	Sample value
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. `PUT`. Defaults to `GET` 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.
- Cisco Webex Hybrid Services links on-premises equipment with the Cisco Collaboration cloud for an integrated Cisco Webex experience.

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.

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)

More Information

For detailed information about multitenancy, please refer to the following documents on the Cisco Hosted Collaboration Solution documentation page:

- Cisco Hosted Collaboration Solution Reference Network Design Guide
- Cisco Hosted Collaboration Customer Onboarding Guide
- Cisco Hosted Collaboration Solution Capacity Planning Guide
- Cisco Hosted Collaboration Solution Troubleshooting Guide

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.

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. Note that the figures for video and audio-only calls are for either one or the other call type; not both.

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.

Table 29: Deployment scenarios

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 Reference

These tables list the alarms that can be raised on the Expressway:

- Table 30: Hardware Alarms
- Table 31: Software Alarms
- Table 32: Cluster Alarms
- Table 33: Network Alarms
- Table 34: License Alarms
- Table 35: External Applications / Services Alarms
- Table 36: Security Alarms
- Table 37: Misconfiguration Alarms
- Table 38: Back to Back User Agent Alarms
- Table 39: Management Connector Alarms
- Table 40: Calendar Connector Alarms
- Table 41: Call Connector Alarms
- Table 42: Significant Event Alarms
- Table 43: Telemetry Alarms

Table 30: Hardware Alarms

ID	Title	Description	Solution	Severity
10001	Hardware failure	Raised when the following hardware issues occur: • Fan speed below the threshold. • System temperature higher than the threshold. • System input voltage below the threshold. • System input voltage higher than the threshold.	Follow your Cisco RMA process to obtain replacement parts. For information about how to replace server components, see *Cisco UCS C220 M4 Server Installation and Service Guide* on the Cisco UCS C220 M4 Rack Server page.	Critical
10002	RAID degraded	<problem description>	Follow your Cisco RMA process to obtain replacement parts. For information about how to replace server components, see *Cisco UCS C220 M4 Server Installation and Service Guide* on the Cisco UCS C220 M4 Rack Server page.	Critical

ID	Title	Description	Solution	Severity
10003	PSU redundancy lost	<problem description>	Follow your Cisco RMA process to obtain replacement parts. For information about how to replace server components, see *Cisco UCS C220 M4 Server Installation and Service Guide* on the Cisco UCS C220 M4 Rack Server page.	Critical
10004	RAID rebuilding	<problem description>	Wait for the rebuild to complete. On successful completion, all RAID-related alarms will be automatically lowered.	Critical
10005	Unsuitable hardware warning	Your current hardware does not meet supported VM configuration requirements for this version of Expressway.	Contact your Cisco representative for an upgrade to a supported hardware version. For information on supported versions, refer to *Cisco Expressway on Virtual Machine Installation Guide* on Expressway Install Guides page.	Warning

Table 31: Software Alarms

ID	Title	Description	Solution	Severity
15004	Application failed	An unexpected software error was detected in <module>	View the Viewing Incident Reports page	Error

ID	Title	Description	Solution	Severity
15005	Database failure	Please remove database and restore from backup, then reboot the system	Reboot the system	Warning
15006	Restart required	A language pack has been installed, however a restart is required for this to take effect	Restart 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
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

ID	Title	Description	Solution	Severity
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
15023	Restore failed	Backup was not restored. The system is restored onto the previous configuration.	Check the error log for more information and retry the operation; if the problem persists, contact your Cisco support representative	Error

ID	Title	Description	Solution	Severity
15024	Crypto device failure	A failure was detected while testing encrypt/decrypt cycle with the configured crypto device.	Please refer to the HSM configuration page for details	Critical
15025	HSM disenrollment failure	Disenrollment of peer to HSM failed.	Please refer to the HSM configuration page for details	Error
15026	HSM enrollment failure	Enrollment of peer to HSM failed.	Please refer to the HSM configuration page for details	Error
15027	HSM failure	An HSM failure needs administrator attention.	Please refer to the HSM configuration page for details	Critical
15028	Restart required	Server certificate and private key have been changed, however a restart is required for this to take effect.	Restart the Expressway to make this change effective	Warning
15029	Failed to send Crash Report	Failed to send Crash Report to the Server.	Check the network connectivity between Expressway and the Crash Reporting Server. Make sure the Crash Reporting Server certificate is not expired or revoked and the certificates in the CA chain were updated in the trust store.	

ID	Title	Description	Solution	Severity
15030	Unified CM data crosscheck failure	Unified CM configuration data on Expressway is inconsistent.	Please delete all Unified CM servers and then add them again. For details see the Mobile and Remote Access Through Cisco Expressway Deployment Guide, section " Discover Unified CM Servers"	Error
15031	HSM TLP not installed	An HSM failure needs administrator attention.	Please refer to the Upgrade page for details.	Error
15032	Unified CM server unavailable	Unified CM configuration for publisher includes unavailable servers	See event log for further details. Correct the issue and refresh. For details see the Mobile and Remote Access Through Cisco Expressway Deployment Guide, section Discover Unified CM Servers.	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

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
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

ID	Title	Description	Solution	Severity
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
20014	Cluster replication error	Cannot find primary or this subordinate's peer configuration file	Restart the node	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
20019	Cluster name not configured	If FindMe or clustering are in use a cluster name must be defined.	Configure the cluster name	Warning

ID	Title	Description	Solution	Severity
20024	Cluster configuration error	Cluster is in inconsistent state	View Cisco Expressway Cluster Creation and Maintenance Deployment Guide to recreate the cluster	Warning
20025	Failed to synchronize database	Database synchronization failed on node <nodename>, reboot node <nodename> from CLI Here, <nodename> is either the IP address or Fully Qualified Domain Name (FQDN)	Reboot the affected node from Command Line Interface (CLI)	Critical
20026	Failed to recover ClusterDB log server	ClusterDB log server is frozen and CDB log messages are not processed.	If the problem persists, contact your Cisco representative.	Critical

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

ID	Title	Description	Solution	Severity
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
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

ID	Title	Description	Solution	Severity
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

ID	Title	Description	Solution	Severity
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
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
25026	Restart required	Web administration port has been changed, however, a restart is required for this to take effect	Restart the system	Warning
25027	SSLH failure	The protocol multiplexing service cannot start because the configuration file was not written. The Expressway-E is not able to listen on TCP 443 for TURN and WebRTC requests.	Reconfigure the TURN service	Critical

ID	Title	Description	Solution	Severity
25028	HSM box connectivity issue	There is an issue with HSM modules	Please refer to the HSM configuration page for details	Alert
25029	Restart required	TURN Protocol Mode changed to UDP. Due to this, the TCP 443 TURN service has been turned OFF, however a restart is required for this to take effect	Restart the system	
25030	Reverse DNS Lookup failed	Failed to do reverse DNS Lookup for address <*IP Address of E server*>. This can cause MRA login to fail.	Ensure your DNS server is configured with valid PTR record for that address <*IP Address of E server*>.	Error
25031	Certificate verification failed	FQDN in PTR record for address <*IP Address of E server*> does not match with SAN entries presented in certificate of that Server with IP <*IP Address of E server*>.	Ensure a valid PTR record (only one) is created for address <*IP Address of E server*> with an FQDN which is present as a SAN entry in the Expressway-E's server certificate.	Error

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

ID	Title	Description	Solution	Severity
30003	Capacity warning	The number of concurrent non-traversal calls has approached the unit's physical limit	Contact your Cisco representative	Warning
30004	Capacity warning	The number of concurrent non-traversal calls has approached the licensed limit	Contact your Cisco representative	Warning
30005	Capacity warning	TURN relays usage has approached the unit's physical limit	Contact your Cisco representative	Warning
30007	Capacity warning	TURN relays usage has approached the licensed limit	Contact your Cisco representative	Warning
30009	TURN relays installed	TURN services are only available on Expressway-E; TURN option key ignored	Add/Remove opton keys	Warning
30010	Capacity warning	The number of concurrent registrations has approached the licensed limit	Contact your Cisco representative	Warning
30011	TURN relay licenses required	TURN services are enabled but no TURN relay license option keys are installed	Add option keys or disable Configuring 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

ID	Title	Description	Solution	Severity
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

ID	Title	Description	Solution	Severity
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
30019	Call license limit reached	You have reached your license limit of <n> concurrent non-traversal call licenses	If the problem persists, contact your Cisco representative to buy more call licenses	Warning
30020	Call license limit reached	You have reached your license limit of <n> concurrent traversal call licenses	If the problem persists, contact your Cisco representative to buy more call licenses	Warning
30021	TURN relay license limit reached	You have reached your license limit of <n> concurrent TURN relay licenses	If the problem persists, contact your Cisco representative to buy more TURN relay licenses	Warning
30022	Call capacity limit reached	The number of concurrent non-traversal calls has reached the unit's physical limit	Add more capacity to your system; contact your Cisco representative	Warning
30023	Call capacity limit reached	The number of concurrent traversal calls has reached the unit's physical limit	Add more capacity to your system; contact your Cisco representative	Warning
30024	TURN relay capacity limit reached	The number of concurrent TURN relay calls has reached the unit's physical limit	Add more capacity to your system; contact your Cisco representative	Warning
30025	Restart required	An option key or the type has been changed, however a restart is required for this to take effect	Restarting, Rebooting, and Shutting Down	Warning

ID	Title	Description	Solution	Severity
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
30035	Smart license in Eval	The system is operating in Evaluation Mode that will expire in 30, 7, 3 , 2, 1 days	Register the system with Cisco Smart Software Manager or satellite	Warning

ID	Title	Description	Solution	Severity
30036	Smart license in overage out of compliance	The system is operating with an insufficient number of licenses	Configure additional licenses in Cisco Smart Software Manager	Alert
30037	Smart license no provision out of compliance	The system is operating with an insufficient number of licenses	Configure additional licenses in Cisco Smart Software Manager in order to restore the ability to provision users and devices	Critical
30038	Smart license no provision Eval expired	The license evaluation period has expired and the product is in enforced mode	Please check the network connection and renew the license authorization in order to restore the ability to provision users and devices	Critical
30039	Smart license in overage authorization expired	The license authorization has expired	Please check the network connection and renew the license authorization to avoid losing the ability to provision users and devices	Alert
30040	Smart license no provision authorization expired	The license authorization has expired and the product is in enforced mode	Please check the network connection and renew the license authorization in order to restore the ability to provision users and devices	Critical

ID	Title	Description	Solution	Severity
30041	Smart license registration expired	The license registration has expired and the system is unregistered with Cisco Smart Software Manager or satellite	Please check the network connectivity to Cisco Smart Software manager or satellite. Also verify your system clock is correct and then register the system with Cisco Smart Software Manager or satellite. If the issue still persists, please raise a TAC case	Error
30042	Smart license communication error	The system failed to communicate with cloud-based Cisco Smart Software Manager or On-Prem	Please check the network connectivity to cloud-based Cisco Smart Software manager or On-Prem	Error
30043	Smart license authorization expiring soon	The license authorization period will expire soon	Please initiate an authorization renewal	Warning
30044	Smart license renew auth failed	The license authorization renewal failed	Please retry an authorization renewal. If the problem persists please raise a TAC case	Error
30045	Smart license renew registration failed	The license registration renewal failed	Please retry a registration renewal. If the problem persists please raise a TAC case	Error
30046	Smart license registration expiring soon	The registration with Cisco Smart Software Manager or satellite will expire soon	Please initiate a registration renewal to avoid losing ability to provision users or devices	Warning

ID	Title	Description	Solution	Severity
30047	Capacity warning	The system has reached the licensed limit to support the number of devices for encrypted signaling sessions due to the Export Control Classification	Contact your Cisco representative	Warning
30048	Approaching Capacity warning	The system is reaching the licensed limit to support the number of devices for encrypted signaling sessions due to Export Control Classification	Contact your Cisco representative	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 Configuring DNS Settings	Warning
35002	Configuration warning	Active Directory mode has been enabled but the NTP server has not been configured	Configure Configuring Time Settings server	Warning
35003	Configuration warning	Active Directory mode has been enabled but no DNS servers have been configured	Configure a Configuring DNS Settings server	Warning

ID	Title	Description	Solution	Severity
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 Configuring Remote Account Authentication Using LDAP	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

ID	Title	Description	Solution	Severity
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 TMS Provisioning Extension Service Status 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 TMS Provisioning Extension Service Status after the data has been corrected in TMS	Warning
35012	Failed to connect to LDAP server	Failed to connect to the LDAP server for H.350 device authentication	Ensure that your H.350 directory service is correctly configured	Warning
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

ID	Title	Description	Solution	Severity
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 Managing Certificate Revocation Lists (CRLs)	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 Using the Root Account	Warning

ID	Title	Description	Solution	Severity
40004	Certificate-based authentication required	Your system is recommended to have client certificate-based security set to *Certificate-based authentication* when in advanced account security mode	Configure Network Services	Warning
40005	Insecure password in use	The admin user has the default password set	Change the Configuring Administrator Accounts	Error
40006	Security alert	Unable to download CRL update	Check Managing Certificate Revocation Lists (CRLs) and the Logs	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 Changing 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	Restarting, Rebooting, and Shutting Down	Warning
40011	Per-account session limit required	A non-zero per-account session limit is required when in advanced account security mode	Configure Network Services	Warning
40012	External manager connection is using HTTP	You are recommended to use HTTPS connections to the external manger when in advanced account security mode	Configure Configuring External Manager Settings	Warning

ID	Title	Description	Solution	Severity
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 Network Services	Warning
40014	Time out period required	A non-zero system session time out period is required when in advanced account security mode	Configure Network Services	Warning
40015	System session limit required	A non-zero system session limit is required when in advanced account security mode	Configure Network Services	Warning
40016	Encryption required	Your login account LDAP server configuration is recommended to have encryption set to *TLS* when in advanced account security mode	Configure Configuring Remote Account Authentication Using LDAP	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 Configuring External Manager Settings	Warning

ID	Title	Description	Solution	Severity
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 Configure 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 *All* when in advanced account security mode	Configure Configuring Remote Account Authentication Using LDAP	Warning
40025	SNMP enabled	You are recommended to disable SNMP when in advanced account security mode	Configure Configuring SNMP Settings	Warning
40026	Reboot required	The advanced account security mode has changed, however a reboot is required for this to take effect	Restarting, Rebooting, and Shutting Down	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

ID	Title	Description	Solution	Severity
40028	Insecure password in use	The root user's password is hashed using MD5, which is not secure enough	View instructions on Using the Root Account	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 Intrusion Protection, fix any rejected rules and re-try the activation	Warning
40031	Security alert	Unable to restore previous firewall configuration	Check your Intrusion Protection, 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	Restarting, Rebooting, and Shutting Down; 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 Configuring SIP to enforce certificate identity checking using TLS, or disable the access rules for the Configuring the Default Zone.	Warning

ID	Title	Description	Solution	Severity
40034	Security alert	Firewall rules activation failed; the firewall configuration contains rules with duplicated priorities	Check your Intrusion Protection, ensure all rules have a unique priority and re-try the activation	Warning
40036	Delegated credential checking error	The traversal server zone associated with SIP domain <domain> cannot connect to the traversal client system	Check that the domain and its associated traversal server zone are configured correctly. You may also need to check the remote traversal client system	Warning
40037	Delegated credential checking error	There is a communication problem with the traversal client zone <zone> used to receive delegated credential checking requests	Check that the traversal client zone is configured correctly. You may also need to check the remote traversal server system	Warning
40038	Delegated credential checking configuration error	TLS verify mode is not enabled on the traversal server zone associated with SIP domain <domain>	Check the domain and ensure that TLS verify mode is enabled on the associated traversal server zone	Warning
40039	Delegated credential checking configuration error	TLS verify mode is not enabled on the traversal client zone (<zone>) that has been configured to accept delegated authentication requests	Ensure that TLS verify mode is enabled on the traversal client zone	Warning
40040	Unified Communications configuration error	TLS verify mode is not enabled on a traversal zone configured for Unified Communications services	Ensure that TLS verify mode is enabled on the traversal zone; you may also need to check the remote traversal system	Warning

ID	Title	Description	Solution	Severity
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	Restarting, Rebooting, and Shutting Down	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

ID	Title	Description	Solution	Severity
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 Intrusion Protection and rate limits configuration, fix any rejected rules; Do not restart your system; if the problem persists, contact your Cisco representative	
40051	CMS not Identified by Server Certificate	CMS address <*address*> 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 Managing the Expressway Server Certificate 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: <*List*>	Please reconfigure the affected cipher entries at Configuring Minimum TLS Version and Cipher Suites	

ID	Title	Description	Solution	Severity
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
40055	Failed to update key file	Failed to update system key file due to inconsistent state	Restart the system. If that doesn't clear the problem, contact your Cisco representative	Warning
40061	ACME auto-sign failure	A failure was detected while running the auto-sign command for the server certificate	Please refer to the server certificate page for details	Warning
40062	ACME auto-sign failure	A failure was detected while running the auto-sign command for SNI domains [<*domain*>]	Please refer to the domain certificates page for details	Warning
40063	ACME auto-deploy failure	A failure was detected while running the auto-deploy command for the server certificate	Please refer to the server certificate page for details	Warning
40064	ACME auto-deploy failure	A failure was detected while running the auto-deploy command for SNI domains [*domain*]	Please refer to the domain certificates page for details	Warning
40066	HSM certificate is not used	An HSM certificate is installed but not in use	Please refer to the HSM configuration page for details	Alert
40068	Server certificate validity	Server certificate expired *or* Server certificate expires today	Create and upload a new server certificate	Critical

ID	Title	Description	Solution	Severity
40069	Server certificate validity	Server certificate expires in <*n*> days	You are recommended to create and upload a new server certificate	Alert
40100	Security alert	Firewall rules are not synchronized with network interfaces	Restart the system. If that doesn't clear the problem, contact your Cisco representative	Warning
40101	Absolute Time out period required	A non-zero system absolute time out period is required when in advanced account security mode	Configure absolute time out period	Warning

Table 37: Misconfiguration Alarms

ID	Title	Description	Solution	Severity
45001	Failed to load Call Policy file	<failure details>	Configure Configuring 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 Configuring H.323 and/or Configuring 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

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
45009	Configuration warning	For provisioning to work correctly, authentication policy must be enabled on the Default Zone and any other relevant zone that receives provisioning requests	Set authentication policy to either "Check credentials" or "Treat as authenticated" for each relevant zone	Warning
45012	Configuration warning	For Presence services to work correctly, authentication policy must be enabled on the Default Subzone and any other relevant subzone; authentication must also be enabled on the Default Zone if the endpoints are not registered	Set authentication policy to either "Check credentials" or "Treat as authenticated" for the Default Subzone and each relevant subzone and zone	Warning
45013	Configuration warning	For phone book requests to work correctly, authentication policy must be enabled on the Default Subzone and any other relevant subzone; authentication must also be enabled on the Default Zone if the endpoints are not registered	Set authentication policy to either "Check credentials" or "Treat as authenticated" for the Default Subzone and each relevant subzone and zone	Warning

ID	Title	Description	Solution	Severity
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
45017	Configuration warning	A subzone has a SIP media encryption mode of “Best effort” or “Force encrypted” but TLS is not enabled. TLS is required for encryption.	Either enable TLS on the SIP configuration page or select a different SIP media encryption mode for the relevant subzone or Default Subzone	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
45021	HSM server configuration issue	There is an issue with the HSM server configuration	Please refer to the HSM configuration page for details	Alert

ID	Title	Description	Solution	Severity
45022	Restart required	DMI administration configuration has been changed; however a restart is required for this to take effect.	Restarting, Rebooting, and Shutting Down	Warning
45023	Configuration error	Attempt to share host/port tuple among multiple connections.	Review zones and correct any hostname or port conflict	Error
45024	SSLH failure	As *Administration DMI only* mode is not set and Web Administration is using port 443, the protocol multiplexing service cannot start. The Expressway is unable to listen on TCP 443 for TURN and WebRTC requests.		Critical

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

ID	Title	Description	Solution	Severity
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
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

ID	Title	Description	Solution	Severity
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
55026	B2BUA misconfiguration	TURN services are enabled, but there are no valid TURN servers configured	Configure the TURN server address	Warning
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

ID	Title	Description	Solution	Severity
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

ID	Title	Description	Solution	Severity
55104	B2BUA misconfiguration	Invalid Expressway ICE mode	Restart the service; contact your Cisco representative if the problem persists	Warning
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

ID	Title	Description	Solution	Severity
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
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

ID	Title	Description	Solution	Severity
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

ID	Title	Description	Solution	Severity
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
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: <*string*>	Check <*string*>, or <*string*>, or use network utilities <*string*>, to verify this address.	error
60051	[Hybrid services] Communication error	HTTP error code <*string*> from Cisco Collaboration Cloud (address: <*string*>)	Check Hybrid Services status. Contact your Cisco Collaboration Cloud administrator if the issue persists.	error
60052	[Hybrid services] Communication error	<*string*>	Verify your <*string*>, <*string*>, <*string*> the address. Contact your Cisco Collaboration Cloud administrator if you have ruled these out.	error
60053	[Hybrid services] Access error	<*string*>	Contact your Cisco Collaboration Cloud administrator.	error
60054	[Hybrid services] Connector install error	<*string*>	Contact your Cisco Collaboration Cloud administrator.	error
60055	[Hybrid services] Download failed because the certificate was not valid	<*string*>	Check the Expressway's trusted CA list for the CA that signed the received certificate.	error
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

ID	Title	Description	Solution	Severity
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

ID	Title	Description	Solution	Severity
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
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

ID	Title	Description	Solution	Severity
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
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

ID	Title	Description	Solution	Severity
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
60073	[Hybrid services] Unsupported Expressway version	A new version of Cisco Expressway was released. We advise that you upgrade to this version at your earliest convenience to use the latest features and avoid an unsupported Hybrid Services deployment when the next Expressway version is released. Your current version will be supported until the next Expressway release.	Please upgrade to the latest Expressway version, available on cisco.com.	alert
60074	[Hybrid services] Connectivity error	Unable to reach the Cisco Collaboration Cloud.	Check Network requirements for Teams Service and follow the proxy guidelines as highlighted.	error

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 <*string*>. The last known error is: <*string*>	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 <*string*>. The last known error is: <*string*>	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 <*string*>. The last known error is: <*string*>	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: <*string*>	Microsoft Exchange Server must be upgraded to supported version	critical

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 <*string*>. The last known error is: <*string*>	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 <*string*>. The last known error is: <*string*>	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 <*string*>. The last known error is: <*string*>	Verify the server certificate is valid	critical

ID	Title	Description	Solution	Severity
60113	Redirected Microsoft Exchange Autodiscovery URL not trusted	The redirected Microsoft Exchange Autodiscovery URL is changed and not trusted. Detailed info: <*string*>	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 <*string*>. The last known error is: <*string*>	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 <*string*>. The last known error is: <*string*>	Verify that the service account has valid credentials and correct permissions, and is not locked out	critical
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

ID	Title	Description	Solution	Severity
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

ID	Title	Description	Solution	Severity
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
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 <*string*>	Verify the encryption service is on	error

ID	Title	Description	Solution	Severity
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 <*string*>	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 <*string*>	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 <*string*>	Verify network connectivity and configured account credentials to CMR service	error
60161	WebEx user account not available	<*string*> 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 <*string*>	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

ID	Title	Description	Solution	Severity
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 <*string*>	Change the expired or invalid administrator password on affected WebEx server	error
60163	Cisco WebEx administrator password expiring	Cisco WebEx administrator password for <*string*> site(s) will expire soon. Detailed info: the WebEx service site with expiring administrator password includes <*string*>	Change the expiring administrator password on affected WebEx server	warning
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 <*string*>	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

ID	Title	Description	Solution	Severity
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[<*string*>]: <*string*>	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[<*string*>]: <*string*>	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[<*string*>]: <*string*>	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[<*string*>]: <*string*>	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[<*string*>]: <*string*>	Verify that the user's email and directory URI are identical in Unified CM	warning

ID	Title	Description	Solution	Severity
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[<*string*>]: <*string*>	Verify that the user's directory URI and line URI on an associated device are identical in Unified CM	warning
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	Webex SIP address cannot be routed to the Webex cloud.	The user's Webex SIP address cannot be routed to the Webex cloud - user[<*string*>]: <*string*>	Check the rerouting calling search space on Unified CM and the partition configured for the Webex SIP address pattern.	error
60308	Webex SIP address is already in use.	The User's Webex SIP address is assigned to another user - user[<*string*>]: <*string*>	In Cisco Unified CM administration, check whether the user's remote destination is already used by a device.	error
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*>	In Cisco Unified CM administration, check whether the user's remote destination is already used by a device. Remove the remote destination from the user's CTI remote device in Unified CM.	warning

ID	Title	Description	Solution	Severity
60310	Unable to add the user's Webex SIP address in Unified CM.	Unable to add the user's Webex SIP address in Unified CM - user[<*string*>]: <*string*>	In Cisco Unified CM Administration, delete a manually created remote destination if it exists. Then call connector will recreate the remote destination automatically.	error
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 nam <*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

ID	Title	Description	Solution	Severity
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 Remote Device for Webex - user[<*string*>]: <*string*>	Check whether the Unified CM user is enabled for mobility.	warning
60319	Connectivity to Unified CM AXL Service lost	Connectivity to Unified CM AXL Service lost - for Unified CM [<*string*>]	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 [<*string*>]	Check whether the CTIManager service is running on Unified CM and resolve any networking issues.	error
60321	Certificate verification failed	Call Connector stopped as it could not verify the certificate provided by the Webex cloud.	Download the certificate as part of the Expressway registration process and reregister the Expressway-C. If the error remains, update the Webex certificate in the Expressway-C trust store.	error
60322	Fully Qualified Domain Name is not valid	Fully Qualified Domain Name is Empty - user[<*string*>]: <*string*>	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[<*string*>]: <*string*>	Add a new fully qualified domain name without wildcards in the Unified CM enterprise parameter.	warning

ID	Title	Description	Solution	Severity
60324	Unable to reach the Unified CM AXL server.	Unable to reach the Unified CM AXL server - server[<*string*>]	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 - [<*string*>]	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 [<*string*>]	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[<*string*>]: <*string*>	Check the user's home cluster setting on all Unified CMs configured on this call connector.	warning
60329	Call connector received an invalid Webex SIP Address.	Invalid Spark SIP Address - for user[<*string*>]: <*string*>	Check the user and device configuration. Follow the documentation to reconfigure these, and if needed, reconfigure to create a valid Webex SIP address.	error
60330	The user is configured with more than one CTI remote device.	The user is configured with more than one CTI remote device - user[<*string*>]: <*string*>	Remove extra devices from the user's control list in Unified CM.	warning

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

ID	Title	Description	Solution	Severity
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 Webex SIP address.	warning
60339	The user exceeds the remote destination limit.	Unable to create a Webex SIP address. The user exceeds the remote destination limit in Cisco Unified CM.	Remove any unused remote destinations or increase the limit.	error
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
60342	Call connector version mismatch with the Webex cloud	Invalid message received in state [<*string*>], potential version mismatch with the Webex cloud	Go to admin.webex.com > Services > Hybrid Call > View all to open the resources, and then upgrade to the latest Call Connector software.	error
60343	Webex SIP Address exceeds the 48 character limit.	Unable to add Webex SIP address for a user. Unified CM does not support remote destinations that are longer than 48 characters.	Change device names so Webex SIP addresses don't exceed the character limit.	error
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[<*string*>]: <*string*> has domain list = <*string*>	Check the user's directory URI and list of verified domains for this user	warning

ID	Title	Description	Solution	Severity
60345	Failed to Build Unified CM Cluster Data-Cache	Failed to Build Unified CM Cluster Data-Cache - server[<*string*>]	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

ID	Title	Description	Solution	Severity
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
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

Table 42: Significant Event Alarms

ID	Title	Description	Solution	Severity
90001	Emergency call	Emergency call has been made by ([*user@example.com*]), from zone (*zone name*), source IP (*IP address*).	NA	emergency

Table 43: Telemetry Alarms

ID	Title	Description	Solution	Severity
60800	CollectD Service Down	Core Telemetry Service is not operational	Disable and enable the Telemetry Connector and check for network issues. If the problem persists, contact your Cisco support representative.	Critical

ID	Title	Description	Solution	Severity
60801	Cloud-Connected UC Connection Down	Connection to Cloud-Connected UC is broken	Disable and enable the Telemetry Connector and check for network issues. If the problem persists, contact your Cisco support representative.	Critical
60802	Configuration Error	Configuration Update or Configuration Fetch Failed	Disable and enable the Telemetry Connector and check for network issues. Also, check if the cluster or node is authorized, and onboarded properly. If the problem still persists, contact your Cisco support representative.	Error
60803	Authentication Error	Authentication Failed on one or all the Telemetry Connector Connections or Transactions Processing	Disable and enable the Telemetry Connector and check for network issues. Also, check if the cluster or node is authorized, onboarded properly and the necessary certificates are installed. If the problem still persists, contact your Cisco support representative.	Error

ID	Title	Description	Solution	Severity
60804	CA Certificate Read Error	Failed to Read or include CA Certificate	• Check if the cluster or node is authorized, onboarded properly and the necessary certificates are installed. • Reinstall the required certificates. • Disable and Enable Telemetry Connector and check for network issues. If the problem persists, contact your Cisco support representative.	Error
60805	Invalid Certificate Error	Invalid Certificate Loaded	• Check if the cluster or node is authorized, onboarded properly and the valid certificates are installed. • Reinstall the correct and valid certificates. • Disable and Enable Telemetry Connector and check for network issues. If the problem persists, contact your Cisco support representative.	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 44: 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 `IP Route [1..50] Address <S: 0,39>` 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 45: xConfiguration CLI reference

xConfiguration Administration DeviceProvisioning: <On/Off> Determines whether the **System** > **TMS Provisioning Extension services** page is accessible in the Expressway web user interface. From there you can connect to the Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) and its provisioning services for users, devices, FindMe and phone books. Default: Off. *On*: the **System** > **TMS Provisioning Extension services** page is accessible and provisioning services can be configured for this Expressway. *Off*: the **System** > **TMS Provisioning Extension services** page is not accessible. Example: `xConfiguration Administration DeviceProvisioning: On`
xConfiguration Administration HTTP Mode: <On/Off> Determines whether HTTP calls will be redirected to the HTTPS port. You must restart the system for any changes to take effect. Default: On. *On*: calls will be redirected to HTTPS. *Off*: no HTTP access will be available. Example: `xConfiguration Administration HTTP Mode: On`
xConfiguration Administration HTTPS Mode: <On/Off> 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. Example: `xConfiguration Administration HTTPS Mode: On`
xConfiguration Administration LCDPanel Mode: <On/Off> Controls whether the LCD panel on the front of the Expressway identifies the system. Default: On. *On*: the system name and first active IP address are shown. *Off*: the LCD panel reveals no identifying information about the system. Example: `xConfiguration Administration LCDPanel Mode: On`
xConfiguration Administration SSH Mode: <On/Off> Determines whether the Expressway can be accessed via SSH and SCP. You must restart the system for any changes to take effect. Default: On. Example: `xConfiguration Administration SSH Mode: On`
xConfiguration Alarm Notification Email Custom Alarm ID: <String> If one or more customized alarm notifications is configured. The alarm Id for customized or disabled notifications.

xConfiguration Alarm Notification Email Custom Disable Notify: <Off>

If one or more customized alarm notifications is configured.

xConfiguration Alarm Notification Email Custom Email: <String>

If one or more customized alarm notifications is configured. The email id to which the selected alarm notifications are to be sent (maximum length 254).

xConfiguration Alarm Notification Email Destination Alert: <S: 0, 254>

The email destination for alarms with severity attribute “Alert”.

Example: `xConfiguration Alarm Notification Email Destination Alert: "ucadmin@example.com"`

xConfiguration Alarm Notification Email Destination Critical: <S: 0, 254>

The email destination for alarms with severity attribute “Critical”.

Example: `xConfiguration Alarm Notification Email Destination Alert: "ucadmin@example.com"`

xConfiguration Alarm Notification Email Destination Debug: <S: 0, 254>

The email destination for alarms with severity attribute “Debug”.

Example: `xConfiguration Alarm Notification Email Destination Debug: "uctech@example.com"`

xConfiguration Alarm Notification Email Destination Emergency: <S: 0, 254>

The email destination for alarms with severity attribute “Emergency”.

Example: `xConfiguration Alarm Notification Email Destination Emergency: "ert@example.com"`

xConfiguration Alarm Notification Email Destination Error: <S: 0, 254>

The email destination for alarms with severity attribute “Error”.

Example: `xConfiguration Alarm Notification Email Destination Error: "ucadmin@example.com"`

xConfiguration Alarm Notification Email Destination Info: <S: 0, 254>

The email destination for alarms with severity attribute “Info”.

Example: `xConfiguration Alarm Notification Email Destination Info: "ucadmin@example.com"`

xConfiguration Alarm Notification Email Destination Notice: <S: 0, 254>

The email destination for alarms with severity attribute “Notice”.

Example: `xConfiguration Alarm Notification Email Destination Notice: "ucadmin@example.com"`

xConfiguration Alarm Notification Email Destination Warning: <S: 0, 254>

The email destination for alarms with severity attribute “Warning”.

Example: `xConfiguration Alarm Notification Email Destination Warning: "ucadmin@example.com"`

xConfiguration Alarm Notification SMTP Mode: <On/Off>

Determines whether or not alarm-based email notifications will be used. The default is Off.

Example: `xConfiguration Alarm Notification SMTP Mode: On`

xConfiguration Alarm Notification SMTP Server Email: <S: 0, 254>

The source email from which alarm-based email notifications are sent to the configured destination address.

Example: `Alarm Notification SMTP Server Email: "ucadmin@example.com"`

xConfiguration Alarm Notification SMTP Server Host: <S: 0, 128>

IP address or FQDN of the SMTP server to be used to send alarm-based email notifications.

Example: `xConfiguration Alarm Notification SMTP Server Host: "email.example.com"`

xConfiguration Alarm Notification SMTP Server Password: <Password>

Password for the SMTP server to be used to send alarm-based email notifications.

Example: `xConfiguration Alarm Notification SMTP Server Password: "{cipher}$NNxx1xxx-xxxx-xxxx-xxxn-fnxnxNNNxxxN$1$xX+xnXnnXxnnxxnnnXXXnxnXXxnxXxxx/XXxnxnxxxx="`

xConfiguration Alarm Notification SMTP Server Port:

Port number of the SMTP server to be used to send alarm-based email notifications. Default is 587.

Example: `xConfiguration Alarm Notification SMTP Server Port: 587`

xConfiguration Alternates Cluster Name: <S: 0,128>

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.

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.

Example: `xConfiguration Alternates Cluster Name: "Regional"`

xConfiguration Alternates ConfigurationPrimary: <1..6>

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.

Example: `xConfiguration Alternates ConfigurationPrimary: 1`

xConfiguration Alternates Peer [1..6] Address: <S: 0, 128>

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.

Example: `xConfiguration Alternates 1 Peer Address: "cluster1peer3.example.com"`

xConfiguration ApacheModReqTimeOut

You can set all available properties for the request timeout using a single shorthand command.

Example: `xConfiguration ApacheModReqTimeout Apachehead:20 Apachebody:20 Status:On`

xConfiguration ApacheModReqTimeOut Apachebody: <0..120>

Modifes 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.

Example: `xConfiguration ApacheModReqTimeout Apachebody:20`

xConfiguration ApacheModReqTimeOut Apacheheader: <0..120>

Modifes 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.

Example: `xConfiguration ApacheModReqTimeout Apacheheader:20`

xConfiguration ApacheModReqTimeOut Status: <On/Off>

Toggles the custom Apache request timeout. Displays the status of the timeout if you omit the switch.

On: The default Apache request timeout is superseded with your settings (or the defaults) for `Apachebody` and `Apacheheader`.

Off: `Apachebody` and `Apacheheader` have no effect. The Apache request timeout defaults to 300 seconds.

Example: `xConfiguration ApacheModReqTimeout Status:On`

xConfiguration Applications ConferenceFactory Alias: <S:0,60>

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.

Example: `xConfiguration Applications ConferenceFactory Alias: "multiway@example.com"`

xConfiguration Applications ConferenceFactory Mode: <On/Off>

The Mode option allows you to enable or disable the Conference Factory application. Default: Off.

Example: `xConfiguration Applications ConferenceFactory Mode: Off`

xConfiguration Applications ConferenceFactory Range End: <1..65535>

The last number of the range that replaces %% in the template used to generate a conference alias. Default: 65535.

Example: `xConfiguration Applications ConferenceFactory Range End: 30000`

xConfiguration Applications ConferenceFactory Range Start: <1..65535>

The first number of the range that replaces %% in the template used to generate a conference alias. Default: 65535.

Example: `xConfiguration Applications ConferenceFactory Range Start: 10000`

xConfiguration Applications ConferenceFactory Template: <S:0,60>

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

Example: `xConfiguration Applications ConferenceFactory Template: "563%%@example.com"`

xConfiguration Applications External Status [1..10] Filename: <S:0,255>

XML file containing status that is to be attached for an external application.

Example: `xConfiguration Applications External Status 1 Filename: "foo.xml"`

xConfiguration Applications External Status [1..10] Name: <S:0,64>

Descriptive name for the external application whose status is being referenced.

Example: `xConfiguration Applications External Status 1 Name: "foo"`

xConfiguration Authentication ADS ADDomain: <S: 0,255>

The Kerberos realm used when the Expressway joins the AD domain. Note: this field is case sensitive.

Example: `xConfiguration Authentication ADS ADDomain: "CORPORATION.INT"`

xConfiguration Authentication ADS Clockskew: <1..65535>

Maximum allowed clockskew between the Expressway and the KDC before the Kerberos message is assumed to be invalid (in seconds). Default: 300.

Example: `xConfiguration Authentication ADS Clockskew: 300`

xConfiguration Authentication ADS CipherSuite: <S:1,2048>

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/man1.0.2/apps/ciphers.html#CIPHER-LIST-FORMAT).

Example: `xConfiguration Authentication ADS CipherSuite: "HIGH:MEDIUM:!ADH:!aNULL:!eNULL:-AES128-SHA256:@STRENGTH"`

xConfiguration Authentication ADS DC [1..5] Address: <S: 0,39>

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.

Example: `xConfiguration Authentication ADS DC 1 Address: "192.168.0.0"`

xConfiguration Authentication ADS Encryption: <Off/TLS>

Sets the encryption to use for the LDAP connection to the ADS server.

Note Removed the weak ciphers, but retained one cipher (eTYPE-ARCFOUR-HMAC-MD5) to allow for backward compatibility.

Default: TLS.

Off: no encryption is used.

TLS: TLS encryption is used.

Example: `xConfiguration Authentication ADS Encryption: TLS`

xConfiguration Authentication ADS KDC [1..5] Address: <S: 0,39>

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.

Example: `xConfiguration Authentication ADS KDC 1 Address: "192.168.0.0"`

xConfiguration Authentication ADS KDC [1..5] Port: <1..65534>

Specifies the port of a KDC that can be used when the Expressway joins the AD domain. Default: 88.

Example: `xConfiguration Authentication ADS KDC 1 Port: 88`

xConfiguration Authentication ADS MachineName: <S: 0..15>

This overides the default NETBIOS machine name used when the Expressway joins the AD domain.

Example: `xConfiguration Authentication ADS MachineName: "short_name"`

xConfiguration Authentication ADS MachinePassword Refresh: <On/Off>

Determines if this samba client should refresh its machine password every 7 days, when joined to the AD domain. Default: On.

Example: `xConfiguration Authentication ADS MachinePassword Refresh: On`

xConfiguration Authentication ADS Mode: <On/Off>

Indicates if the Expressway should attempt to form a relationship with the AD. Default: Off.

Example: `xConfiguration Authentication ADS Mode: On`

xConfiguration Authentication ADS SPNEGO: <Enabled/Disabled>

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.

Example: `xConfiguration Authentication ADS SPNEGO: Enabled`

xConfiguration Authentication ADS SecureChannel: <Auto/Enabled/Disabled>

Indicates if data transmitted from the Expressway to an AD domain controller is sent over a secure channel. Default: Auto.

Example: `xConfiguration Authentication ADS SecureChannel: Auto`

xConfiguration Authentication ADS Workgroup: <S: 0,15>

The workgroup used when the Expressway joins the AD domain.

Example: `xConfiguration Authentication ADS Workgroup: "corporation"`

xConfiguration Authentication Account Admin Account [1..n] AccessAPI: <On/Off>

Determines whether this account is allowed to access the system's status and configuration via the Application Programming Interface (API). Default: On.

Example: `xConfiguration Authentication Account Admin Account 1 AccessAPI: On`

xConfiguration Authentication Account Admin Account [1..n] AccessWeb: <On/Off>

Determines whether this account is allowed to log in to the system using the web interface. Default: On.

Example: `xConfiguration Authentication Account Admin Account 1 AccessWeb: On`

xConfiguration Authentication Account Admin Account [1..n] Enabled: <On/Off>

Indicates if the account is enabled or disabled. Access will be denied to disabled accounts. Default: On.

Example: `xConfiguration Authentication Account Admin Account 1 Enabled: On`

xConfiguration Authentication Account Admin Account [1..n] Name: <S: 0, 128>

The username for the administrator account.

Example: `xConfiguration Authentication Account Admin Account 1 Name: "bob_smith"`

xConfiguration Authentication Account Admin Account [1..n] Password: <Password>

The password that this administrator will use to log in to the Expressway.

Example: `xConfiguration Authentication Account Admin Account 1 Password: "abcXYZ_123"`

xConfiguration Authentication Account Admin Group [1..n] AccessAPI: <On/Off>

Determines whether members of this group are allowed to access the system's status and configuration using the Application Programming Interface (API). Default: On.

Example: `xConfiguration Authentication Account Admin Group 1 AccessAPI: On`

xConfiguration Authentication Account Admin Group [1..n] AccessWeb: <On/Off>

Determines whether members of this group are allowed to log in to the system using the web interface. Default: On.

Example: `xConfiguration Authentication Account Admin Group 1 AccessWeb: On`

xConfiguration Authentication Account Admin Group [1..n] Enabled: <On/Off>

Indicates if the group is enabled or disabled. Access will be denied to members of disabled groups. Default: On.

Example: `xConfiguration Authentication Account Admin Group 1 Enabled: On`

xConfiguration Authentication Account Admin Group [1..n] Name: <S: 0, 128>

The name of the administrator group.

Example: `xConfiguration Authentication Account Admin Group 1 Name: "administrators"`

xConfiguration Authentication Certificate Crlcheck: <None/Peer/All>

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.

None: no CRL checking is performed.

Peer: only the CRL associated with the CA that issued the client's certificate is checked.

All: all CRLs in the trusted certificate chain of the CA that issued the client's certificate are checked.

Example: `xConfiguration Authentication Certificate Crlcheck: All`

xConfiguration Authentication Certificate Crlinaccessible: <Ignore/Fail>

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.

Ignore: treat the certificate as not revoked.

Fail: treat the certificate as revoked (and thus do not allow the TLS connection).

Example: `xConfiguration Authentication Certificate Crlinaccessible: Ignore`

xConfiguration Authentication Certificate Mode: <NotRequired/Validation/Authentication>

Controls the level of security required to allow client systems (typically web browsers) to communicate with the Expressway over HTTPS. Default: NotRequired.

NotRequired: the client system does not have to present any form of certificate.

Validation: 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.

Authentication: 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.

Example: `xConfiguration Authentication Certificate Mode: NotRequired`

xConfiguration Authentication Certificate UsernameRegex: <String>

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

Example: `xConfiguration Authentication Certificate UsernameRegex: "/Subject:.*CN= (? ([^,\]|(\,))*)/m"`

xConfiguration Authentication Certificate UsernameTemplate: <String>

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#

Example: `xConfiguration Authentication Certificate UsernameTemplate: "#captureCommonName#"`

xConfiguration Authentication H350 BindPassword: <S: 0, 60>

Sets the password to use when binding to the LDAP server.

Example: `xConfiguration Authentication H350 BindPassword: "abcXYZ_123"`

xConfiguration Authentication H350 BindSaslMode: <None/DIGEST-MD5>

The SASL (Simple Authentication and Security Layer) mechanism to use when binding to the LDAP server. Default: DIGEST-MD5.

None: no mechanism is used.

DIGEST-MD5: the DIGEST-MD5 mechanism is used.

Example: `xConfiguration Authentication H350 BindSaslMode: DIGEST-MD5`

xConfiguration Authentication H350 BindUserDn: <S: 0, 500>

Sets the user distinguished name to use when binding to the LDAP server.

Example: `xConfiguration Authentication H350 BindUserDn: "manager"`

xConfiguration Authentication H350 BindUserName: <S: 0, 500>

Sets the username to use when binding to the LDAP server. Only applies if using SASL.

Example: `xConfiguration Authentication H350 BindUserName: "manager"`

xConfiguration Authentication H350 DirectoryBaseDn: <S: 0, 500>

Sets the Distinguished Name to use when connecting to an LDAP server.

Example: `xConfiguration Authentication H350 DirectoryBaseDn: "dc=example,dc=company,dc=com"`

xConfiguration Authentication H350 LdapEncryption: <Off/TLS>

Sets the encryption to use for the connection to the LDAP server. Default : TLS.

Off: no encryption is used.

TLS: TLS encryption is used.

Example: `xConfiguration Authentication H350 LdapEncryption: TLS`

xConfiguration Authentication H350 LdapServerAddress: <S: 0, 256>

The IP address or Fully Qualified Domain Name of the LDAP server to use when making LDAP queries for device authentication.

Example: `xConfiguration Authentication H350 LdapServerAddress: "ldap_server.example.com"`

xConfiguration Authentication H350 LdapServerAddressResolution: <AddressRecord/ServiceRecord>

Sets how the LDAP server address is resolved if specified as an FQDN. Default: AddressRecord.

Address record: DNS A or AAAA record lookup.

SRV record: DNS SRV record lookup.

Example: `xConfiguration Authentication H350 LdapServerAddressResolution: AddressRecord`

xConfiguration Authentication H350 LdapServerPort: <1..65535>

Sets the IP port of the LDAP server to use when making LDAP queries for device authentication. Typically, non-secure connections use 389. Default : 389

Example: `xConfiguration Authentication H350 LdapServerPort: 389`

xConfiguration Authentication H350 Mode: <On/Off>

Enables or disables the use of an H.350 directory for device authentication. Default: Off.

Example: `xConfiguration Authentication H350 Mode: Off`

xConfiguration Authentication LDAP AliasOrigin: <LDAP/Endpoint/Combined>

Determines how aliases are checked and registered. Default: LDAP.

LDAP: the aliases presented by the endpoint are checked against those listed in the LDAP database.

Endpoint: the aliases presented by the endpoint are used; any in the LDAP database are ignored.

Combined: the aliases presented by the endpoint are used in addition to any listed in the LDAP database.

Example: `xConfiguration Authentication LDAP AliasOrigin: LDAP`

xConfiguration Authentication Password: <S: 0, 215>

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.

Example: `xConfiguration Authentication Password: "password123"`

xConfiguration Authentication Remote Digest Cache ExpireCheckInterval: <0..65535>

The interval between digest authentication cache expiration checks in seconds. Default: 600

Example: `xConfiguration Authentication Remote Digest Cache ExpireCheckInterval: 600`

xConfiguration Authentication Remote Digest Cache Lifetime: <0..43200>

The lifetime of digest authentication interim hashes in seconds. Default: 600

Example: `xConfiguration Authentication Remote Digest Cache Lifetime: 600`

xConfiguration Authentication Remote Digest Cache Limit: <0..65535>

The interval between digest authentication cache expiration checks in seconds. Default: 10000

Example: `xConfiguration Authentication Remote Digest Cache Limit: 10000`

xConfiguration Authentication Remote Digest Cache Mode: <On/Off>

Controls whether the digest authentication cache is enabled. Default: On

Example: `xConfiguration Authentication Remote Digest Cache Mode: On`

xConfiguration Authentication StrictPassword Enabled: <On/Off>

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.

On: local administrator account passwords must meet the complexity requirements.

Off: passwords are not checked for complexity.

Example: `xConfiguration Authentication StrictPassword Enabled: Off`

xConfiguration Authentication StrictPassword MaximumConsecutiveRepeated: <0..255>

The maximum number of times the same character can be repeated consecutively. A value of 0 disables this check. Default: 0

Example: `xConfiguration Authentication StrictPassword MaximumConsecutiveRepeated: 0`

xConfiguration Authentication StrictPassword MinimumClasses: <0..4>

The minimum number of character classes that must be present. There are four character classes: digit, upper case, lower case and special. Use this setting if you want to mandate the use of 2-3 different character classes without requiring all of them to be present. A value of 0 disables this check. Default: 0.

Example: `xConfiguration Authentication StrictPassword MinimumClasses: 0`

xConfiguration Authentication StrictPassword MinimumDigits: <0..255>

The minimum number of digits that must be present. A value of 0 disables this check. Default: 2.

Example: `xConfiguration Authentication StrictPassword MinimumDigits: 2`

xConfiguration Authentication StrictPassword MinimumLength: <6..255>

The minimum length of the password. Default: 15.

Example: `xConfiguration Authentication StrictPassword MinimumLength: 15`

xConfiguration Authentication StrictPassword MinimumLowerCase: <0..255>

The minimum number of lower case characters that must be present. A value of 0 disables this check. Default: 2.

Example: `xConfiguration Authentication StrictPassword MinimumLowerCase: 2`

xConfiguration Authentication StrictPassword MinimumOther: <0..255>

The minimum number of special characters that must be present. A special character is anything that is not a letter or a digit. A value of 0 disables this check. Default: 2

Example: `xConfiguration Authentication StrictPassword MinimumOther: 2`

xConfiguration Authentication StrictPassword MinimumUpperCase: <0..255>

The minimum number of upper case characters that must be present. A value of 0 disables this check. Default : 2

Example: `xConfiguration Authentication StrictPassword MinimumUpperCase: 2`

xConfiguration Authentication UserName: <S: 0, 128>

The username used by the Expressway when authenticating with another system. Note: this does not apply to traversal client zones.

Example: `xConfiguration Authentication UserName: "user123"`

xConfiguration Bandwidth Default: <64..65535>

The bandwidth (in kbps) to use on calls managed by the Expressway where no bandwidth has been specified by the endpoint. Default: 384.

Example: `xConfiguration Bandwidth Default: 384`

xConfiguration Bandwidth Downspeed PerCall Mode: <On/Off>

Determines whether the Expressway attempts to downspeed a call if there is insufficient per-call bandwidth available to fulfill the request. Default: On.

On: the Expressway will attempt to place the call at a lower bandwidth.

Off: the call will be rejected.

Example: `xConfiguration Bandwidth Downspeed PerCall Mode: On`

xConfiguration Bandwidth Downspeed Total Mode: <On/Off>

Determines whether the Expressway attempts to downspeed a call if there is insufficient total bandwidth available to fulfill the request. Default: On.

On: the Expressway will attempt to place the call at a lower bandwidth.

Off: the call will be rejected.

Example: `xConfiguration Bandwidth Downspeed Total Mode: On`

xConfiguration Bandwidth Link [1..3000] Name: <S: 1, 50>

Assigns a name to this link.

Example: `xConfiguration Bandwidth Link 1 Name: "HQ to BranchOffice"`

xConfiguration Bandwidth Link [1..3000] Node1 Name: <S: 0, 50>

Specifies the first zone or subzone to which this link will be applied.

Example: `xConfiguration Bandwidth Link 1 Node1 Name: "HQ"`

xConfiguration Bandwidth Link [1..3000] Node2 Name: <S: 0, 50>

Specifies the second zone or subzone to which this link will be applied.

Example: `xConfiguration Bandwidth Link 1 Node2 Name: "BranchOffice"`

xConfiguration Bandwidth Link [1..3000] Pipe1 Name: <S: 0, 50>

Specifies the first pipe to be associated with this link.

Example: `xConfiguration Bandwidth Link 1 Pipe1 Name: "512Kb ASDL"`

xConfiguration Bandwidth Link [1..3000] Pipe2 Name: <S: 0, 50>

Specifies the second pipe to be associated with this link.

Example: `xConfiguration Bandwidth Link 1 Pipe2 Name: "2Gb Broadband"`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth PerCall Limit: <1..100000000>

If this pipe has limited per-call bandwidth, sets the maximum amount of bandwidth (in kbps) available for any one call. Default: 1920.

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Limit: 256`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth>

Determines whether or not this pipe is limiting the bandwidth of individual calls. Default: Unlimited.

NoBandwidth: no bandwidth available. No calls can be made on this pipe.

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Mode: Limited`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth Total Limit: <1..100000000>

If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe. Default: 500000.

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth Total Limit: 1024`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Determines whether or not this pipe is enforcing total bandwidth restrictions. Default: Unlimited.

NoBandwidth: no bandwidth available. No calls can be made on this pipe.

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth Total Mode: Limited`

xConfiguration Bandwidth Pipe [1..1000] Name: <S: 1, 50>

Assigns a name to this pipe.

Example: `xConfiguration Bandwidth Pipe 1 Name: "512Kb ASDL"`

xConfiguration Call Loop Detection Mode: <On/Off>

Specifies whether the Expressway will check for call loops. Default: On.

Example: `xConfiguration Call Loop Detection Mode: On`

xConfiguration Call Routed Mode: <Always/Optimal>

Specifies whether the Expressway routes the signaling for calls. Default: Always.

Always: the Expressway will always route the call signaling.

Optimal: if possible, the Expressway will remove itself from the call signaling path, which may mean the call does not consume a call license.

Example: `xConfiguration Call Routed Mode: Always`

xConfiguration Call Services CallsToUnknownIPAddresses: <Off/Direct/Indirect>

The way in which the Expressway attempts to call systems that are not registered with it or one of its neighbors. Default: Indirect.

Direct: allows an endpoint to make a call to an unknown IP address without the Expressway querying any neighbors. The call setup would occur just as it would if the far end were registered directly to the local system.

Indirect: upon receiving a call to an unknown IP address, the Expressway will query its neighbors for the remote address and if permitted will route the call through the neighbor.

Off: endpoints registered directly to the Expressway may only call an IP address of a system also registered directly to that Expressway.

Example: `xConfiguration Call Services CallsToUnknownIPAddresses: Indirect`

xConfiguration Call Services Fallback Alias: <S: 0, 60>

Specifies the alias to which incoming calls are placed for calls where the IP address or domain name of the Expressway has been given but no callee alias has been specified.

Example: `xConfiguration Call Services Fallback Alias: "reception@example.com"`

xConfiguration CollaborationEdge AllowEmbeddedSafari: <Yes/No>

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.

Select *Yes* to allow Jabber on iOS devices to display the authentication page in the native Safari browser.

Select *No* to have Jabber on iOS devices display the authentication page in the WebView browser, rather than in the Safari browser.

Note If you toggle this option, also make the corresponding selection for **SSO Login Behavior for iOS** in Cisco Unified Communications Manager.

Example: `xConfiguration CollaborationEdge AllowEmbeddedSafari: No`

xConfiguration CollaborationEdge AllowList DefaultMethods: <String>

Configure one or more default HTTP methods for the HTTP allow list.

Configuration Parameters:

Methods: <OPTIONS/GET/HEAD/POST/PUT/DELETE> - A comma-delimiting set of one or more http methods

Example: `xConfiguration CollaborationEdge AllowList DefaultMethods: PUT,GET,POST`

xConfiguration CollaborationEdge AllowOnboardingOverMra: <On/Off>

Enables or disables activation code onboarding for MRA devices. If enabled/disabled, mTLS is automatically enabled/disabled on the MRA port. The necessary CA certificates for mTLS are auto-generated.

Example: `xConfiguration CollaborationEdge AllowOnboardingOverMra: On`

xConfiguration CollaborationEdge AllowRedirectUri: <On/Off>

Enables or disables Redirect URI. Allows the client to use Embedded browser for (and MRA) OAuth flow. Default value is *No*. Set the value to *Yes* to enable this option.

Example: `xConfiguration CollaborationEdge AllowRedirectUri: Off`

xConfiguration CollaborationEdge Enabled: <On/Off>

Enables or disables Mobile and Remote Access on this Expressway.

Example: `xConfiguration CollaborationEdge Enabled: On`

xConfiguration CollaborationEdge InternalCheck: <No/Yes>

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.

Select *Yes* to allow the Expressway-C to check on the user's home node before the Expressway-E responds to the client.

Example: `xConfiguration CollaborationEdge InternalCheck: No`

xConfiguration CollaborationEdge JabbercEnabled: <On/Off>

Enables or disables Jabber Guest services on this Expressway.

Example: `xConfiguration JabbercEnabled: Off`

xConfiguration CollaborationEdge JabbercProxyProtocol: <http/https>

Selects the protocol used to proxy Jabber Guest services requests through the Expressway.

Example: `xConfiguration JabbercProxyProtocol: https`

xConfiguration CollaborationEdge LegacyCred: <On/Off>

Select On if Unified Communications services authorize MRA clients based on the username and password they supply to the Expressway.

Example: `xConfiguration CollaborationEdge LegacyCred: Off`

xConfiguration CollaborationEdge LegacySso: <On/Off/Exclusive>

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.

Example: `xConfiguration CollaborationEdge LegacySso: Off`

xConfiguration CollaborationEdge OauthLocal: <On/Off>

Enables or disables OAuth local authentication for mobile and remote access to Unified Communications services.

Example: `xConfiguration CollaborationEdge OauthLocal: Off`

xConfiguration CollaborationEdge OauthSso: <On/Off>

Enables or disables OAuth Single Sign-On for mobile and remote access to Unified Communications services.

Example: `xConfiguration CollaborationEdge OauthSso: Off`

xConfiguration CollaborationEdge RFC3327Enabled: <On/Off>

Changes Path header support for registrations going through automatically generated neighbor zones to Unified CM nodes.

On: The Expressway-C inserts its address into the Path header of the REGISTER message, and into the response to that message.

Off: The Expressway-C overwrites the address in the Contact header of the REGISTER message.

Example: `xConfiguration CollaborationEdge rfc3327Enabled: On`

xConfiguration CollaborationEdge SSO Scope: <PEER/CLUSTER>

Use PEER if you wish to use a SAML agreement, with your chosen IdP, for each Expressway peer. Use CLUSTER if you wish to use a single SAML agreement for the cl uster.

Example: `xConfiguration CollaborationEdge SSO Scope: CLUSTER`

xConfiguration CollaborationEdge SSO IdP <index> Digest: <sha1/sha256>

Changes the hash algorithm that the Expressway uses when signing SAML authentication requests given to the client.

<*index*> is an integer distinguishing a particular IdP from the list that is configured on the Expressway.

Example: `xConfiguration CollaborationEdge SSO IdP 1 Digest: sha256`

xConfiguration CollaborationEdge SsoAlwaysAvailable: <On/Off>

Determines whether the Expressway-C will check if the user's home node has SSO available.

On: The Expressway-E always tells the client that SSO is available, without actually checking the home node.

Off: Allow the Expressway-C to check if SSO is available on the user's home node before the Expressway-E responds to the client.

Example: `xConfiguration CollaborationEdge SsoAlwaysAvailable: Off`

Note The default value *Off* corresponds to the following default on the web UI: **Check for internal SSO availability**: *Yes*

xConfiguration CollaborationEdge SsoEnabled: <On/Off>

Toggles Single Sign-On for mobile and remote access to UC services.

Example: `xConfiguration CollaborationEdge SsoEnabled: Off`

xConfiguration CollaborationEdge SsoSipTokenExtraTtl: <0..172800>

Extends the lifetime of the SIP authorization token by the supplied number of seconds.

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.

Example: `xConfiguration CollaborationEdge SsoSipTokenExtraTtl: 0`

xConfiguration CollaborationEdgeDeployments <index> DeploymentId: <1..65535>

Changes the deployment ID of a particular deployment.

<*index*> is an integer distinguishing a particular IdP from the list that is configured on the Expressway.

Example: `xConfiguration CollaborationEdgeDeployments 1 DeploymentId: 5`

xConfiguration CollaborationEdgeDeployments <index> UserReadableName: <String>

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.

<*index*> is an integer distinguishing a particular IdP from the list that is configured on the Expressway.

Example: `xConfiguration CollaborationEdgeDeployments 1 UserReadableName: StagingDeployment`

xConfiguration Ciphers SIPTLSCiphers Value: <S:0,2048>

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: `EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH`

Example: `xConfiguration Ciphers SIPTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH"`

To change SIP TLS protocol value, see: *SIP Advanced SipTlsVersions*.

xConfiguration Ciphers HTTPSCiphers Value: <S:0,2048>

Specifies the HTTPS cipher suite to use in 'OpenSSL ciphers' format (See https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT).

Default: `EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

Example: `xConfiguration Ciphers HTTPSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"`

xConfiguration Ciphers HTTPSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

Specifies the HTTPS TLS protocol minimum version.

Default: `minTLSv1.2`

Example: `xConfiguration Ciphers HTTPSProtocol Value: "minTLSv1.2"`

xConfiguration Ciphers SMTPTLSCiphers Value: <S:0,2048>

Specifies the SMTP TLS cipher suite to use in 'OpenSSL ciphers' format (see https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT

Default: `EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

Example: `xConfiguration Ciphers SMTPTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"`

xConfiguration Ciphers SMTPTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

Specifies the SMTP TLS protocol minimum version.

Default: `minTLSv1.2`

Example: `xConfiguration Ciphers SMTPTLSProtocol Value: "minTLSv1.2"`

xConfiguration Ciphers ReverseProxyTLSCiphers Value: <S:0,2048>

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).

Default: `EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

Example: `xConfiguration Ciphers ReverseProxyTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"`

xConfiguration Ciphers ReverseProxyTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

Specifies the Reverse Proxy TLS protocol minimum version.

Default: `minTLSv1.2`

Example: `xConfiguration Ciphers ReverseProxyTLSProtocol Value: "minTLSv1.2"`

xConfiguration Ciphers UcClientTLSCiphers Value: <S:0,2048>

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).

Default: `EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

Example: `xConfiguration CiphersUcClientTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"`

xConfiguration Ciphers UcClientTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

Specifies the UC Client TLS protocol minimum version.

Default: `minTLSv1.2`

Example: `xConfiguration Ciphers UcClientTLSProtocol Value: "minTLSv1.2"`

xConfiguration Ciphers XCPTLSCiphers Value: <S:0,2048>

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.

Default: `EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

Example: `xConfiguration Ciphers XCPTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"`

xConfiguration Ciphers XCPTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

Specifies the XCP TLS protocol minimum version.

Default: `minTLSv1.2`

Example: `xConfiguration Ciphers XCPTLSProtocol Value: minTLSv1.2`

xConfiguration Ciphers sshd_ciphers Value: <S:0,2048>

Configures the available ciphers for admin/root SSH connections (TCP/22) in "openssh" format.

Default: `aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr`

Example: `xConfiguration Ciphers sshd_ciphers Value: "aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr"`

xConfiguration Ciphers sshd_kex Value: <S:0,2048>

Configures key exchange algorithms for admin/root SSH connections (TCP/22) in "openssh" format.

Default: `ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1`

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"`

xConfiguration Ciphers sshd_macs Value: <S:0,2048>

Configures the message authentication code digests for admin/root SSH connections (TCP/22) in "openssh" format.

Default: `hmac-sha2-512,hmac-sha2-256,hmac-sha1`

Example: `xConfiguration Ciphers sshd_macs Value: "hmac-sha2-512,hmac-sha2-256,hmac-sha1"`

xConfiguration Ciphers sshd_pfwd_ciphers Value: <S:0,2048>

The ciphers available for the SSH tunnels used for the forward and reverse HTTP proxies (i.e. APNS and MRA HTTP traffic).

Default: `aes256-ctr`

Example: `xConfiguration Ciphers sshd_pfwd_ciphers Value: "aes256-ctr"`

xconfiguration Ciphers sshd_pfwd_pubkeyalgorithms

Configure the available public key algorithms.

Default values:
`"x509v3-rsa2048-sha256,x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384,x509v3-ecdsa-sha2-nistp521"`

Only following values are allowed:
`x509v3-rsa2048-sha256,x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384,x509v3-ecdsa-sha2-nistp521`

Example: `xconfiguration Ciphers sshd_pfwd_pubkeyalgorithms Value: "x509v3-rsa2048-sha256,x509v3-ecdsa-sha2-nistp256"`

Note You must use the default value for the **sshd_pfwd_pubkeyalgorithms** configuration (All four types of public key configured).

Configure all public key types that the server certificate of this node uses in case you plan to customize this configuration. Similarly, configure all other nodes that are connecting to this node using ssh tunnel.

For example, One node Expressway-C has a server certificate created using ECDSA with 256 size and this is connecting to another node Expressway-E over ssh tunnel which has a server certificate created using ECDSA with 384 size. Configure **sshd_pfwd_pubkeyalgorithms** to values `"x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384"` for both the nodes.

xConfiguration DNS PerDomainServer [1..5] Address: <S: 0, 39>

The IP address of the DNS server to use only when resolving hostnames for the associated domain names.

Example: `xConfiguration DNS PerDomainServer 1 Address: "192.168.12.1"`

xConfiguration DNS PerDomainServer [1..5] Domain1: <S: 0, 39>

The first domain name to be resolved by this particular DNS server.

Example: `xConfiguration DNS PerDomainServer 1 Domain1: "dept.example.com"`

xConfiguration DNS PerDomainServer [1..5] Domain2: <S: 0, 39>

The second domain name to be resolved by this particular DNS server.

Example: `xConfiguration DNS PerDomainServer 1 Domain2: "other.example.com"`

xConfiguration DNS Server [1..5] Address: <S: 0, 39>

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.

Example: `xConfiguration DNS Server 1 Address: "192.168.12.0"`

xConfiguration EdgeConfigServer CredentialTtl: <0..604800>

Does not apply to SSO authentications.

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.

Example: `xConfiguration EdgeConfigServer CredentialTtl: 28800`

xConfiguration EdgeConfigServer PurgeInterval: <0..604800>

Does not apply to SSO authentications.

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.

Example: `xConfiguration EdgeConfigServer PurgeInterval: 43200`

xConfiguration EdgeConfigServer RateLimitLogins: <0..100>

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.

After the limit is reached, any further attempts to use these credentials are rejected until the current rate control period expires.

Enter 0 to disable the rate control feature.

Example: `xConfiguration EdgeConfigServer RateLimitLogins: 3`

xConfiguration EdgeConfigServer RateLimitPeriod: <0..86400>

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.

Enter 0 to disable the rate control feature.

Example: `xConfiguration EdgeConfigServer RateLimitPeriod: 300`

xConfiguration ErrorReport Contact: <S: 0, 128>

An optional contact email address for follow up on incident reports if required.

Example: `xConfiguration ErrorReport Contact: "bob smith"`

xConfiguration ErrorReport CoreDump: <On/Off>

Determines whether diagnostic core dump files are created. Default: On.

Example: `xConfiguration ErrorReport CoreDump: On`

xConfiguration ErrorReport Mode: <On/Off>

Determines whether details of application failures are automatically sent to a web service. Default: Off.

Example: `xConfiguration ErrorReport Mode: Off`

xConfiguration ErrorReport Proxy: <S: 0, 128>

An optional proxy server to use for the HTTP/HTTPS connections to the incident reporting server.

Example: `xConfiguration ErrorReport Proxy: https://proxy_address/submiterror/`

xConfiguration ErrorReport Url: <S: 0, 128>

The URL of the web service to which details of application failures are sent. Default: https://cc-reports.cisco.com/submitapplicationerror/

Example: `xConfiguration ErrorReport Url: https://cc-reports.cisco.com/submitapplicationerror/`

xConfiguration Ethernet [1..2] IP V4 Address: <S: 7,15>

Specifies the IPv4 address of the specified LAN port. Note: you must restart the system for any changes to take effect.

Example: `xConfiguration Ethernet 1 IP V4 Address: "192.168.10.10"`

xConfiguration Ethernet [1..2] IP V4 StaticNAT Address: <S:7,15>

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.

Example: `xConfiguration Ethernet 1 IP V4 StaticNAT Address: "64.22.64.85"`

xConfiguration Ethernet [1..2] IP V4 StaticNAT Mode: <On/Off>

Specifies whether the Expressway is located behind a static NAT. You must restart the system for any changes to take effect. Default: Off.

Example: `xConfiguration Ethernet 1 IP V4 StaticNAT Mode: On`

xConfiguration Ethernet [1..2] IP V4 SubnetMask: <S: 7,15>

Specifies the IPv4 subnet mask of the specified LAN port. You must restart the system for any changes to take effect.

Example: `xConfiguration Ethernet 1 IP V4 SubnetMask: "255.255.255.0"`

xConfiguration Ethernet [1..2] IP V6 Address: <S: 0, 39>

Specifies the IPv6 address of the specified LAN port. You must restart the system for any changes to take effect.

Example: `xConfiguration Ethernet 1 IP V6 Address: "2001:db8::1428:57ab"`

xConfiguration Ethernet [1..2] Speed: <Auto/10half/10full/100half/100full/1000full

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.

Example: `xConfiguration Ethernet 1 Speed: Auto`

xConfiguration ExternalManager Address: <S: 0, 128>

Sets the IP address or Fully Qualified Domain Name (FQDN) of the external manager.

Example: `xConfiguration ExternalManager Address: "192.168.0.0"`

xConfiguration ExternalManager Path: <S: 0, 255>

Sets the URL of the external manager. Default: tms/public/external/management/SystemManagementService.asmx

Example: `xConfiguration ExternalManager Path: "tms/public/external/management/SystemManagementService.asmx"`

xConfiguration ExternalManager Protocol: <HTTP/HTTPS>

The protocol used to connect to the external manager. Default: HTTPS.

Example: `xConfiguration ExternalManager Protocol: HTTPS`

xConfiguration ExternalManager Server Certificate Verification Mode: <On/Off>

Controls whether the certificate presented by the external manager is verified. Default: On.

Example: `xConfiguration ExternalManager Server Certificate Verification Mode: On`

xConfiguration H323 Gatekeeper AutoDiscovery Mode: <On/Off>

Determines whether or not the Expressway responds to gatekeeper discovery requests from endpoints. Default: On.

Example: `xConfiguration H323 Gatekeeper AutoDiscovery Mode: On`

xConfiguration H323 Gatekeeper CallSignaling PortRange End: <1024..65534>

Specifies the upper port in the range to be used by calls once they are established. Default: 19999.

Example: `xConfiguration H323 Gatekeeper CallSignaling PortRange End: 19999`

xConfiguration H323 Gatekeeper CallSignaling PortRange Start: <1024..65534>

Specifies the lower port in the range to be used by calls once they are established. Default: 15000.

Example: `xConfiguration H323 Gatekeeper CallSignaling PortRange Start: 15000`

xConfiguration H323 Gatekeeper CallSignaling TCP Port: <1024..65534>

Specifies the port that listens for H.323 call signaling. Default: 1720.

Example: `xConfiguration H323 Gatekeeper CallSignaling TCP Port: 1720`

xConfiguration H323 Gatekeeper CallTimeToLive: <60..65534>

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.

Example: `xConfiguration H323 Gatekeeper CallTimeToLive: 120`

xConfiguration H323 Gatekeeper Registration RIPAllRequests: <On/Off>

Determines whether the Expressway will respond to H.323 registration request with a Request In Progress message.

Enable this setting if you are experiencing registration timeouts when authenticating registration requests with a remote LDAP directory service. Default: Off

Example: `xConfiguration H323 Gatekeeper Registration RIPAllRequests: Off`

xConfiguration H323 Gatekeeper Registration ConflictMode: <Reject/Overwrite>

How the system behaves if an endpoint attempts to register an alias currently registered from another IP address. Default: Reject.

Reject: denies the registration.

Overwrite: deletes the original registration and replaces it with the new registration.

Example: `xConfiguration H323 Gatekeeper Registration ConflictMode: Reject`

xConfiguration H323 Gatekeeper Registration UDP Port: <1024..65534>

Specifies the port to be used for H.323 UDP registrations. Default: 1719.

Example: `xConfiguration H323 Gatekeeper Registration UDP Port: 1719`

xConfiguration H323 Gatekeeper TimeToLive: <60..65534>

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.

Example: `xConfiguration H323 Gatekeeper TimeToLive: 1800`

xConfiguration H323 Gateway CallerId: <IncludePrefix/ExcludePrefix>

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.

IncludePrefix: inserts the ISDN gateway's prefix into the source E.164 number.

ExcludePrefix: only displays the source E.164 number.

Example: `xConfiguration H323 Gateway CallerId: ExcludePrefix`

xConfiguration H323 Mode: <On/Off>

Determines whether or not the Expressway will provide H.323 gatekeeper functionality. Default: Off.

Example: `xConfiguration H323 Mode: On`

xConfiguration Interworking BFCP Compatibility Mode: <Auto/TAA/Draft>

Controls the compatibility settings of the SIP to H.323 interworking BFCP component. Default: Auto.

Example: `xConfiguration Interworking BFCP Compatibility Mode: Auto`

xConfiguration Interworking Encryption KeySize2048: <On/Off>

Determines whether or not the Expressway includes 2048-bit Diffie-Hellman keys for encryption of H.323-SIP interworking. Default: On.

On: Expressway will offer both 1024-bit and 2048-bit encryption key lengths.

Off: Expressway will not offer 2048-bit encryption key length.

Example: `xConfiguration Interworking Encryption KeySize2048: On`

xConfiguration Interworking Encryption Mode: <Auto/Off>

Determines whether or not the Expressway will allow encrypted calls between SIP and H.323 endpoints. Default: Auto.

Off: interworked calls will never be encrypted.

Auto: interworked calls will be encrypted if the endpoints request it.

Example: `xConfiguration Interworking Encryption Mode: Auto`

xConfiguration Interworking Encryption Replay Protection Mode: <On/Off>

Controls whether the Expressway will perform replay protection for incoming SRTP packets when interworking a call. Default: Off.

On: replayed SRTP packets will be dropped by the Expressway.

Off: the Expressway will not check for replayed SRTP packets.

Example: `xConfiguration Interworking Encryption Replay Protection Mode: Off`

xConfiguration Interworking Mode: <On/Off/RegisteredOnly>

Determines whether or not the Expressway will act as a gateway between SIP and H.323 calls. Default: RegisteredOnly.

Off: the Expressway will not act as a SIP-H.323 gateway.

On: the Expressway will act as SIP-H.323 gateway regardless of whether the endpoints are locally registered.

RegisteredOnly: the Expressway will act as a SIP-H.323 gateway but only if at least one of the endpoints is locally registered.

Example: `xConfiguration Interworking Mode: On`

xConfiguration Interworking Require Invite Header Mode: <On/Off>

Controls whether the SIP to H.323 interworking function sends com.tandberg.sdp.duo.enable and com.tandberg.sdp.bfcp.udp in the require header for dialog forming INVITEs. Default: Off.

Example: `xConfiguration Interworking Require Invite Header Mode: Off`

xConfiguration IP DNS Domain Name: <S: 0, 128>

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.

Example: `xConfiguration IP DNS Domain Name: "example.com"`

xConfiguration IP DNS Hostname : <S: 0, 63>

The DNS host name that this system is known by. This is not the fully-qualified domain name, just the host label portion. The name can only contain letters, digits, hyphens and underscores. The first character must be a letter and the last character must be a letter or a digit.

Example: `xConfiguration IP DNS Hostname: "localsystem"`

xConfiguration IP DNS MaxPort: <1024..65535>

The upper source port in the range used for sending DNS queries. Requests choose a random port from this range. Warning: setting a small source port range increases your vulnerability to DNS spoofing attacks. Default: 65535.

Example: `xConfiguration IP DNS MaxPort: 65535`

xConfiguration IP DNS MinPort: <1024..65535>

The lower source port in the range used for sending DNS queries. Requests choose a random port from this range. Warning: setting a small source port range increases your vulnerability to DNS spoofing attacks. Default: 1024.

Example: `xConfiguration IP DNS MinPort: 1024`

xConfiguration IP DNS SearchDomains: <S: 0, 1024>

Space separated list of extra domain names to be searched when 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 local System host name to identify references to this system in SIP messaging. (Peer-specific)

Example: `xConfiguration IP DNS SearchDomains: "example1.int" "example2.int" "example3.int"`

xConfiguration IP DNS UseEphemeralPortRange: <On/Off>

Determines whether outgoing DNS queries use the system's normal ephemeral port range, or a custom port range that you can configure. Default: On.

Example: `xConfiguration IP DNS UseEphemeralPortRange: On`

xConfiguration IP Ephemeral PortRange End: <1024..65534>

The highest port in the range used for ephemeral outbound connections not otherwise constrained by Expressway call processing. Default: 35999.

Example: `xConfiguration IP Ephemeral PortRange End: 35999`

xConfiguration IP Ephemeral PortRange Start: <1024..65534>

The lowest port in the range used for ephemeral outbound connections not otherwise constrained by Expressway call processing. Default: 30000.

Example: `xConfiguration IP Ephemeral PortRange Start: 30000`

xConfiguration IP External Interface: <LAN1/LAN2>

Defines which LAN interface is externally facing. Default: LAN1.

Example: `xConfiguration IP External Interface: LAN1`

xConfiguration IP Gateway: <S: 7,15>

Specifies the IPv4 gateway of the Expressway. Note: you must restart the system for any changes to take effect. Default: 127.0.0.1

Example: `xConfiguration IP Gateway: "192.168.127.0"`

xConfiguration IP QoS Mode: <None/DiffServ>

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.

None: no specific QoS tagging is applied.

DiffServ: 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.

Example: `xConfiguration IP QoS Mode: DiffServ`

Important This command is discontinued from Version X8.9 and replaced by commands `QoS Audio`, `QoS Video`, `QoS XMPP`, and `QoS Signaling`.

xConfiguration IP QoS Value: <0..63>

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.

Example: `xConfiguration IP QoS Value: 16`

Important This command is discontinued from Version X8.9 and replaced by commands `QoS Audio`, `QoS Video`, `QoS XMPP`, and `QoS Signaling`.

xConfiguration IP RFC4821 Mode: <Auto/Enabled/Disabled>

Determines when RFC4821 Packetization Layer Path MTU Discovery is used by the Expressway network interface. You must restart the system for any changes to take effect. Default: Disabled.

Enabled: Packetization layer MTU probing is always performed.

Auto: Disabled by default, enabled when an ICMP black hole is detected.

Disabled: Packetization layer MTU probing is not performed.

Example: `xConfiguration IP RFC4821 Mode: Disabled`

xConfiguration IP Route [1..50] Address: <S: 0, 39>

Specifies an IP address used in conjunction with the Prefix Length to determine the network to which this route applies.

Example: `xConfiguration IP Route 1 Address: "128.168.0.0"`

xConfiguration IP Route [1..50] Gateway: <S: 0, 39>

Specifies the IP address of the Gateway for this route.

Example: `xConfiguration IP Route 1 Gateway: "192.168.0.0"`

xConfiguration IP Route [1..50] Interface: <Auto/LAN1/LAN2>

Specifies the LAN interface to use for this route. Auto: The Expressway will select the most appropriate interface to use. Default: Auto.

Example: `xConfiguration IP Route 1 Interface: Auto`

xConfiguration IP Route [1..50] PrefixLength: <0..128>

The number of bits of the IP address which must match when determining the network to which this route applies. Default: 32.

Example: `xConfiguration IP Route 1 PrefixLength: 16`

xConfiguration IP V6 Gateway: <S: 0, 39>

Specifies the IPv6 gateway of the Expressway. You must restart the system for any changes to take effect.

Example: `xConfiguration IP V6 Gateway: "3dda:80bb:6::9:144"`

xConfiguration IPProtocol: <Both/IPv4/IPv6>

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.

Example: `xConfiguration IPProtocol: IPv4`

xConfiguration Language Default: <S: 0, 128>

The default language used on the web interface. Default: "en_US".

Example: `xConfiguration Language Default: "en_US"`

xConfiguration Log CDR Service: <off/serviceonly/serviceandlogging>

Select how to log Call Detail Records produced by this Expressway.

Off: Call Detail Records are not logged.

serviceonly: Call Detail Records are stored locally for 7 days and then deleted. The logged records are not accessible via the user interface.

serviceandlogging: As for serviceonly, 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.

Default: *off*

Example: `xConfiguration Log CDR Service: serviceonly`

xConfiguration Log Level: <1..4>

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

Example: `xConfiguration Log Level: 1`

xConfiguration Log MediaStats Logging: <On/Off>

Toggles media statistics logging. Default: Off

Example: `xConfiguration Log MediaStats Logging: On`

xConfiguration Log SystemMetrics Interval: <30..600>

Sets the number of seconds to wait between metrics collection events.

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.

Default: 60

Example: `xConfiguration Log SystemMetrics Interval: 60`

xConfiguration Log SystemMetrics Mode: <On/Off>

Toggles the System Metrics Collection service. Enter On to start collecting metrics for this system.

Default: *Off*

Example: `xConfiguration Log SystemMetrics Mode: On`

xConfiguration Log SystemMetrics Network Address: <S: 0,1024>

Enter the address of the listening server. You may use IP address, hostname, or FQDN.

Default: *Empty*

Example: `xConfiguration log SystemMetrics Network Address: "192.168.0.5"`

xConfiguration Log SystemMetrics Network Port: <1..65535>

Enter the port on which the listening server is expecting System Metrics traffic.

Default: *25826*

Example: `xConfiguration log SystemMetrics Network Port: 25826`

xConfiguration Logger Network [1..n] Level: <FATAL/ERROR/WARN/INFO/DEBUG/TRACE>

The logging level for the nominated module. Default : INFO.

Example: `xConfiguration Logger Developer 1 Level: INFO`

xConfiguration Login Remote LDAP BaseDN Accounts: <S: 0,255>

Sets the Distinguished Name to use as the base when searching for administrator and user accounts.

Example: `xConfiguration Login Remote LDAP BaseDN Accounts: "ou=useraccounts,dc=corporation,dc=int"`

xConfiguration Login Remote LDAP BaseDN Groups: <S: 0,255>

Sets the Distinguished Name to use as the base when searching for administrator and user groups.

Example: `xConfiguration Login Remote LDAP BaseDN Groups: "ou=groups,dc=corporation,dc=int"`

xConfiguration Login Remote LDAP CRLCheck: <None/Peer/All>

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.

None: no CRL checking is performed.

Peer: only the CRL associated with the CA that issued the LDAP server's certificate is checked.

All: all CRLs in the trusted certificate chain of the CA that issued the LDAP server's certificate are checked.

Example: `xConfiguration Login Remote LDAP CRLCheck: Peer`

xConfiguration Login Remote LDAP DirectoryType: <ActiveDirectory>

Defines the type of LDAP directory that is being accessed. Default: ActiveDirectory.

ActiveDirectory: directory is Windows Active Directory.

Example: `xConfiguration Login Remote LDAP DirectoryType: ActiveDirectory`

xConfiguration Login Remote LDAP Encryption: <Off/TLS>

Sets the encryption to use for the connection to the LDAP server. Default: TLS.

Off: no encryption is used.

TLS: TLS encryption is used.

Example: `xConfiguration Login Remote LDAP Encryption: Off`

xConfiguration Login Remote LDAP SASL: <None/DIGEST-MD5>

The SASL (Simple Authentication and Security Layer) mechanism to use when binding to the LDAP server. Default: DIGEST-MD5.

None: no mechanism is used.

DIGEST-MD5: The DIGEST-MD5 mechanism is used.

Example: `xConfiguration Login Remote LDAP SASL: DIGEST-MD5`

xConfiguration Login Remote LDAP SearchOptimize NestedDepth: <1..16>

Sets the subgroup search depth level for LDAP authentication. Default: 16

Example: `xConfiguration Login Remote LDAP SearchOptimize NestedDepth: "1"`

xConfiguration Login Remote LDAP SearchOptimize SkipMembers: <Yes/No>

Defines whether to skip group member lookup when searching groups for LDAP authentication. Default: Yes

Example: `xConfiguration Login Remote LDAP SearchOptimize SkipMembers: "No"`

xConfiguration Login Remote LDAP Server Address: <S: 0,128>

Sets the IP address or Fully Qualified Domain Name (FQDN) of the LDAP server to use when making LDAP queries.

Example: `xConfiguration Login Remote LDAP Server Address: "server.example.com"`

xConfiguration Login Remote LDAP Server FQDNResolution: <AddressRecord/SRVRecord>

Sets how the LDAP server address is resolved if specified as an FQDN. Default: AddressRecord.

AddressRecord: DNS A or AAAA record lookup.

SRVRecord: DNS SRV record lookup.

Example: `xConfiguration Login Remote LDAP Server FQDNResolution: AddressRecord`

xConfiguration Login Remote LDAP Server Port: <1..65534>

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.

Example: `xConfiguration Login Remote LDAP Server Port: 389`

xConfiguration Login Remote LDAP VCS BindDN: <S: 0,255>

Sets the user distinguished name to use when binding to the LDAP server.

Example: `xConfiguration Login Remote LDAP VCS BindDN: "systemmanager"`

xConfiguration Login Remote LDAP VCS BindPassword: <S: 0,122>

Sets the password to use when binding to the LDAP server. The maximum plaintext length is 60 characters, which is then encrypted.

Example: `xConfiguration Login Remote LDAP VCS BindPassword: "password123"`

xConfiguration Login Remote LDAP VCS BindUsername: <S: 0,255>

Sets the username to use when binding to the LDAP server. Only applies if using SASL.

Example: `xConfiguration Login Remote LDAP VCS BindUsername: "systemmanager"`

xConfiguration Login Remote Protocol: <LDAP>

The protocol used to connect to the external directory. Default: LDAP.

Example: `xConfiguration Login Remote Protocol: LDAP`

xConfiguration Login Source Admin: <LocalOnly/RemoteOnly/Both>

Defines where administrator login credentials are authenticated before access is allowed. Default: LocalOnly.

LocalOnly: credentials are verified against a local database stored on the Expressway.

RemoteOnly: credentials are verified against an external credentials directory, for example Windows Active Directory. Note that this disables login access via the default admin account.

Both: 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.

Example: `xConfiguration Login Source Admin: LocalOnly`

xConfiguration Login User [1..n] Name: <S: 0,60>

Defines the name for this entry in the local authentication database.

Example: `xConfiguration Login User 1 Name: "alice"`

xConfiguration Login User [1..n] Password: <S: 0,128>

Defines the password for this entry in the local authentication database.

Example: `xConfiguration Login User 1 Password: "abcXYZ_123"`

xConfiguration Management Interface HstsMode: <On/Off>

Determines whether web browsers are instructed to only ever use a secure connection to access this server. Enabling this feature gives added protection against man-in-the-middle (MITM) attacks. Default: On.

On: the Strict-Transport-Security header is sent with all responses from the web server, with a 1 year expiry time.

Off: the Strict-Transport-Security header is not sent, and browsers work as normal. Note: you must restart the system for any changes to take effect.

Example: `xConfiguration Management Interface HstsMode: On`

xConfiguration Management Interface Port: <1..65535>

Sets the https listening port for administrators to access the Expressway web interface. Default: 443.

Example: `xConfiguration Management Interface Port: 7443`

Warning Check if you can access the Expressway Web Interface port using your Browser. If the Browser is unresponsive, it means that you cannot administer using the Web Interface. Ensure that the Firewall or any other security equipment in your network do not block the specified port. The ports offered in the Web Interface (443, 445, 7443, 9000) are likely to work in most networks.

xConfiguration Management Session InactivityTimeout: <0..65535>

Sets the number of minutes that an administration session (serial port, HTTPS or SSH) may be inactive before the session is timed out. A value of 0 turns session time outs off. Default: 30.

Example: `xConfiguration Management Session InactivityTimeout: 30`

xConfiguration Management Session MaxConcurrentSessionsTotal: <0..65535>

The maximum number of concurrent administrator sessions allowed on the system. This includes web, SSH and serial sessions. A value of 0 turns session limits off. Default: 0.

Example: `xConfiguration Management Session MaxConcurrentSessionsTotal: 0`

xConfiguration Management Session MaxConcurrentSessionsUser: <0..65535>

The number of concurrent sessions that each individual administrator account is allowed on the system. This includes web, SSH and serial sessions. A value of 0 turns session limits off. Default: 0.

Example: `xConfiguration Management Session MaxConcurrentSessionsUser: 0`

xConfiguration NetworkLimits

Configures the experimental rate limiting feature. Enter `xconfig networklimits ?` to read the help.

Example: `xConfiguration NetworkLimits Configuration GarbageCollectSecs: 5`

xConfiguration NTP Server [1..5] Address: <S: 0, 128>

Sets the IP address or Fully Qualified Domain Name (FQDN) of up to 5 NTP servers to be used when synchronizing system time.

Example: `xConfiguration NTP Server 1 Address: "ntp.server.example.com"`

xConfiguration Option [1..64] Key: <S: 0, 90>

Specifies the option key of your software option. These are added to the system in order to add extra functionality, such as increasing the system's capacity. Contact your Cisco support representative for further information.

Example: `xConfiguration Option 1 Key: "1X4757T5-1-60BAD5CD"`

xConfiguration Policy AdministratorPolicy Mode: <Off/LocalCPL/LocalService/PolicyService>

Enables and disables use of Call Policy. Default: Off.

Off: Disables call policy.

LocalCPL: uses policy from an uploaded CPL file.

LocalService: uses group policy information and a local file.

PolicyService: uses an external policy server.

Example: `xConfiguration Policy AdministratorPolicy Mode: Off`

xConfiguration Policy AdministratorPolicy Service DefaultCPL: <S: 0,255>

The CPL used by the Expressway when the remote service is unavailable. Default: <reject status='403' reason='Service Unavailable'/>

Example: `xConfiguration Policy AdministratorPolicy Service DefaultCPL: "<reject status='403' reason='Service Unavailable'/>"`

xConfiguration Policy AdministratorPolicy Service Password: <S: 0,82>

Specifies the password used by the Expressway to log in and query the remote service. The maximum plaintext length is 30 characters, which will then be encrypted.

Example: `xConfiguration Policy AdministratorPolicy Service Password: "password123"`

xConfiguration Policy AdministratorPolicy Service Path: <S: 0,255>

Specifies the URL of the remote service.

Example: `xConfiguration Policy AdministratorPolicy Service Path: "service"`

xConfiguration Policy AdministratorPolicy Service Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote service. Default: HTTPS.

Example: `xConfiguration Policy AdministratorPolicy Service Protocol: HTTPS`

xConfiguration Policy AdministratorPolicy Service Server [1..3] Address: <S: 0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.

Example: `xConfiguration Policy AdministratorPolicy Service Server 1 Address: "service.server.example.com"`

xConfiguration Policy AdministratorPolicy Service Status Path: <S: 0..255>

Specifies the path for obtaining the remote service status. Default: status

Example: `xConfiguration Policy AdministratorPolicy Service Status Path: status`

xConfiguration Policy AdministratorPolicy Service TLS CRLCheck Mode: <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.

Example: `xConfiguration Policy AdministratorPolicy Service TLS CRLCheck Mode: Off`

xConfiguration Policy AdministratorPolicy Service TLS Verify Mode: <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.

Example: `xConfiguration Policy AdministratorPolicy Service TLS Verify Mode: On`

xConfiguration Policy AdministratorPolicy Service UserName: <S: 0,30>

Specifies the user name used by the Expressway to log in and query the remote policy service.

Example: `xConfiguration Policy AdministratorPolicy Service UserName: "user123"`

xConfiguration Policy FindMe CallerID: <FindMeID/IncomingID>

Determines how the source of an incoming call is presented to the callee. Default: IncomingID.

IncomingID: displays the address of the endpoint from which the call was placed.

FindMeID: displays the FindMe ID associated with the originating endpoint's address.

Example: `xConfiguration Policy FindMe CallerId: FindMeID`

xConfiguration Policy FindMe Mode: <Off/On/ThirdPartyManager>

Configures how the FindMe application operates. Default: Off.

Off: disables FindMe.

On: enables FindMe.

ThirdPartyManager: uses an off-box, third-party FindMe manager.

Example: `xConfiguration Policy FindMe Mode: On`

xConfiguration Policy FindMe Server Address: <S: 0, 128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote FindMe Manager.

Example: `xConfiguration Policy FindMe Server Address: "userpolicy.server.example.com"`

xConfiguration Policy FindMe Server Password: <S: 0, 82>

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.

Example: `xConfiguration Policy FindMe Server Password: "password123"`

xConfiguration Policy FindMe Server Path: <S: 0, 255>

Specifies the URL of the remote FindMe Manager.

Example: `xConfiguration Policy FindMe Server Path: "service"`

xConfiguration Policy Services Service [1..20] DefaultCPL: <S: 0,255>

The CPL used by the Expressway when the remote service is unavailable. Default: <reject status='504' reason='Policy Service Unavailable'/>

Example: `xConfiguration Policy Services Service 1 DefaultCPL: "<reject status='403' reason='Service Unavailable'/>"`

xConfiguration Policy Services Service [1..20] Description: <S: 0,64>

A free-form description of the Policy Service.

Example: `xConfiguration Policy Services Service 1 Description: "Conference management service"`

xConfiguration Policy Services Service [1..20] HTTPMethod: <POST/GET>

Specifies the HTTP method type to use for the remote service. Default: POST.

Example: `xConfiguration Policy Services Service 1 HTTPMethod: POST`

xConfiguration Policy Services Service [1..20] Name: <S: 0,50>

Assigns a name to this Policy Service.

Example: `xConfiguration Policy Services Service 1 Name: "Conference handler"`

xConfiguration Policy Services Service [1..20] Password: <S: 0,82>

Specifies the password used by the Expressway to log in and query the remote service. The maximum plaintext length is 30 characters, which will then be encrypted.

Example: `xConfiguration Policy Services Service 1 Password: "password123"`

xConfiguration Policy Services Service [1..20] Path: <S: 0,255>

Specifies the URL of the remote service.

Example: `xConfiguration Policy Services Service 1 Path: "service"`

xConfiguration Policy Services Service [1..20] Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote service. Default: HTTPS.

Example: `xConfiguration Policy Services Service 1 Protocol: HTTPS`

xConfiguration Policy Services Service [1..20] Server [1..3] Address: <S: 0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.

Example: `xConfiguration Policy Services Service 1 Server 1 Address: "192.168.0.0"`

xConfiguration Policy Services Service [1..20] Status Path: <S: 0..255>

Specifies the path for obtaining the remote service status. Default: status

Example: `xConfiguration Policy Services Service 1 Status Path: status`

xConfiguration Policy Services Service [1..20] TLS CRLCheck Mode: <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.

Example: `xConfiguration Policy Services Service 1 TLS CRLCheck Mode: Off`

xConfiguration Policy Services Service [1..20] TLS Verify Mode: <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.

Example: `xConfiguration Policy Services Service 1 TLS Verify Mode: On`

xConfiguration Policy Services Service [1..20] UserName: <S: 0,30>

Specifies the user name used by the Expressway to log in and query the remote service.

Example: `xConfiguration Policy Services Service 1 UserName: "user123"`

xConfiguration QoS Audio <0..63>

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.

You must restart the system for any changes to take effect.

Example: `xConfiguration QoS Audio: 30`

xConfiguration QoS Video <0..63>

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.

You must restart the system for any changes to take effect.

Example: `xConfiguration QoS Video: 43`

xConfiguration QoS XMPP <0..63>

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.

You must restart the system for any changes to take effect.

Example: `xConfiguration QoS XMPP: 34`

xConfiguration QoS Signaling <0..63>

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.

You must restart the system for any changes to take effect.

Example: `xConfiguration QoS Signaling: 34`

xConfiguration Registration AllowList [1..2500] Description: <S: 0,64>

A free-form description of the Allow List rule.

Example: `xConfiguration Registration AllowList 1 Description: "Everybody at @example.com"`

xConfiguration Registration AllowList [1..2500] Pattern String: <S: 0, 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.

Example: `xConfiguration Registration AllowList 1 Pattern String: "john.smith@example.com"`

xConfiguration Registration AllowList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Allow List is a prefix, suffix, regular expression, or must be matched exactly. Default: Exact.

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.

Example: `xConfiguration Registration AllowList 1 Pattern Type: Exact`

xConfiguration Registration AllowList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Allow List is a prefix, suffix, regular expression, or must be matched exactly. Default: Exact.

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.

Example: `xConfiguration Registration AllowList 1 Pattern Type: Exact`

xConfiguration Registration DenyList [1..2500] Description: <S: 0,64>

A free-form description of the Deny List rule.

Example: `xConfiguration Registration DenyList 1 Description: "Anybody at @nuisance.com"`

xConfiguration Registration DenyList [1..2500] Pattern String: <S: 0, 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.

Example: `xConfiguration Registration DenyList 1 Pattern String: "john.jones@example.com"`

xConfiguration Registration DenyList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Deny List is a prefix, suffix, regular expression, or must be matched exactly. Default: Exact.

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.

Example: `xConfiguration Registration DenyList 1 Pattern Type: Exact`

xConfiguration Registration RestrictionPolicy Mode: <None/AllowList/DenyList/Directory/PolicyService>

Specifies the policy to be used when determining which endpoints may register with the system. Default: None.

None: no restriction.

AllowList: only endpoints attempting to register with an alias listed on the Allow List may register.

DenyList: all endpoints, except those attempting to register with an alias listed on the Deny List, may register.

Directory: only endpoints who register an alias listed in the local Directory, may register.

PolicyService: only endpoints who register with details allowed by the Policy Service, may register.

Example: `xConfiguration Registration RestrictionPolicy Mode: None`

xConfiguration Registration RestrictionPolicy Service DefaultCPL: <S: 0,255>

The CPL used by the Expressway when the remote service is unavailable. Default: <reject status='504' reason='Policy Service Unavailable'/>

Example: `xConfiguration Registration RestrictionPolicy Service DefaultCPL: "<reject status='403' reason='Service Unavailable'/>"`

xConfiguration Registration RestrictionPolicy Service Password: <S: 0,82>

Specifies the password used by the Expressway to log in and query the remote service. The maximum plaintext length is 30 characters, which will then be encrypted.

Example: `xConfiguration Registration RestrictionPolicy Service Password: "password123"`

xConfiguration Registration RestrictionPolicy Service Path: <S: 0,255>

Specifies the URL of the remote service.

Example: `xConfiguration Registration RestrictionPolicy Service Path: "service"`

xConfiguration Registration RestrictionPolicy Service Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote service. Default: HTTPS.

Example: `xConfiguration Registration RestrictionPolicy Service Protocol: HTTPS`

xConfiguration Registration RestrictionPolicy Service Server [1..3] Address: <S: 0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.

Example: `xConfiguration Registration RestrictionPolicy Service Server 1 Address: "192.168.0.0"`

xConfiguration Registration RestrictionPolicy Service Status Path: <S: 0..255>

Specifies the path for obtaining the remote service status. Default: status

Example: `xConfiguration Registration RestrictionPolicy Service Status Path: status`

xConfiguration Registration RestrictionPolicy Service TLS CRLCheck Mode: <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.

Example: `xConfiguration Registration RestrictionPolicy Service TLS CRLCheck Mode: Off`

xConfiguration Registration RestrictionPolicy Service TLS Verify Mode: <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.

Example: `xConfiguration Registration RestrictionPolicy Service TLS Verify Mode: On`

xConfiguration Registration RestrictionPolicy Service UserName: <S: 0,30>

Specifies the user name used by the Expressway to log in and query the remote service.

Example: `xConfiguration Registration RestrictionPolicy Service UserName: "user123"`

xConfiguration Remote Syslog [1..4] Address: <S: 0..128>

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.

Example: `xConfiguration Remote Syslog 1 Address: "remote_server.example.com"`

xConfiguration Remote Syslog [1..4] Crlcheck: <On/Off>

Controls whether the certificate supplied by the syslog server is checked against the certificate revocation list (CRL). Default: Off.

Example: `xConfiguration Remote Syslog 1 Crlcheck: Off`

xConfiguration Remote Syslog [1..4] Format: <bsd/ietf>

The format in which remote syslog messages are written. Default: bsd.

Example: `xConfiguration Remote Syslog 1 Format: bsd`

xConfiguration Remote Syslog [1..4] Loglevel: <emergency/alert/critical/error/warning/notice/informational/debug>

Select the minimum severity of log messages to send to this syslog server. Default: informational.

Example: `xConfiguration Remote Syslog 1 Loglevel: informational`

xConfiguration Remote Syslog [1..4] Mode: <bsd/ietf/ietf_secure/user_defined>

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.

Example: `xConfiguration Remote Syslog 1 Mode: bsd`

xConfiguration Remote Syslog [1..4] Port: <1..65535>

The UDP/TCP destination port to use. Suggested ports: UDP=514 TCP/TLS=6514. Default : 514.

Example: `xConfiguration Remote Syslog 1 Port: 514`

xConfiguration Remote Syslog [1..4] Transport: <udp/tcp/tls>

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.

Example: `xConfiguration Remote Syslog 1 Transport: udp`

xConfiguration ResourceUsage Warning Activation Level: <0..100>

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.

Example: `xConfiguration ResourceUsage Warning Activation Level: 90`

xConfiguration SIP Advanced BibInviteDelay: <1..5000>

Specifies the maximum delay of a SIP BIB invite message that the server must handle (in milliseconds).

Default: 0

Example: `xConfiguration SIP Advanced BibInviteDelay: 1000`

xConfiguration SIP Advanced BusytoneReferDelay: <0..2000>

Specifies the maximum delay of a SIP REFER message . It contains DtLineBusyTone during initial call dialog (ensure SIP messages proceeds in a sequence) that the server can handle (in milliseconds).

Expressway processes and sends SIP messages (REFER contain DtLineBusyTone parameter and 183 Session Progress), which causes Jabber Over MRA to intermittently play Ringing Tone instead of Busy Tone

Default: 0

Recommend adjust delay between 100-200 milliseconds.

Example: `xConfiguration SIP Advanced BusytoneReferDelay: <0..2000>`

xConfiguration SIP Advanced SipMaxSize: <1..1048576>

Specifies the maximum size of a SIP message that can be handled by the server (in bytes). Default: `32768`

Example: `xConfiguration SIP Advanced SipMaxSize: 32768`

xConfiguration SIP Advanced SipTcpConnectTimeout: <1..150>

Enter the maximum number of seconds to wait for an outgoing SIP TCP connection to be established. Default: 10.

Example: `xConfiguration SIP Advanced SipTcpConnectTimeout: 10`

xConfiguration SIP Advanced SipTlsDhKeySize: <1024/2048/3072>

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.

Example: `xConfiguration SIP Advanced SipTlsDhKeySize: 1024`

xConfiguration SIP Advanced SipTlsVersions: <TLSv1/TLSv1.1/TLSv1.2/TLSv1:TLSv1.1/TLSv1:TLSv1.2/TLSv1.1:TLSv1.2/TLSv1:TLSv1.1:TLSv1.2>

Specifies the supported SIP TLS protocol versions. Default: TLSv1:TLSv1.1:TLSv1.2

Example: `xConfiguration SIP Advanced SipTlsVersions: TLSv1.1:TLSv1.2`

xConfiguration SIP Authentication Digest Nonce ExpireDelta: <30..3600>

Specifies the maximum time (in seconds) that a nonce may be re-used for. Default: 300.

Example: `xConfiguration SIP Authentication Digest Nonce ExpireDelta: 300`

xConfiguration SIP Authentication Digest Nonce Length: <32..512>

Length of nonce or cnonce to generate for use in SIP Digest authentication. Default: 60.

Example: `xConfiguration SIP Authentication Digest Nonce Length: 60`

xConfiguration SIP Authentication Digest Nonce Limit: <1..65535>

Maximum limit on the number of nonces to store. Default: 10000.

Example: `xConfiguration SIP Authentication Digest Nonce Limit: 10000`

xConfiguration SIP Authentication Digest Nonce Maximum Use Count: <1..1024>

Maximum number of times that a nonce generated by the Expressway may be used by a client. Default: 128.

Example: `xConfiguration SIP Authentication Digest Nonce Maximum Use Count: 128`

xConfiguration SIP Authentication NTLM Mode: <On/Off/Auto>

Controls when the Expressway will challenge endpoints using the NTLM protocol. Default: Auto.

Off: the Expressway will never send a challenge containing the NTLM protocol.

On: the Expressway will always include NTLM in its challenges.

Auto: the Expressway will decide based on endpoint type whether to challenge with NTLM.

Example: `xConfiguration SIP Authentication NTLM Mode: Auto`

xConfiguration SIP Authentication NTLM SA Lifetime: <30..43200>

Specifies the lifetime of NTLM security associations in seconds. Default: 28800.

Example: `xConfiguration SIP Authentication NTLM SA Lifetime: 28800`

xConfiguration SIP Authentication NTLM SA Limit: <1..65535>

Maximum number of NTLM security associations to store. Default: 10000.

Example: `xConfiguration SIP Authentication NTLM SA Limit: 10000`

xConfiguration SIP Authentication Retry Limit: <1..16>

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.

Example: `xConfiguration SIP Authentication Retry Limit: 3`

xConfiguration SIP Domain [1..200] Authzone: <S: 0,128>

The traversal zone to use when delegating credential checks for SIP messages for this domain.

Example: `xConfiguration SIP Domain 1 Authzone: "traversalzone"`

xConfiguration SIP Domain [1..200] Edge: <On/Off>

Whether remote and mobile collaboration features are enabled. Default Off.

Example: `xConfiguration SIP Domain 1 Edge: On`

xConfiguration SIP Domain [1..200] Name: <S: 0,128>

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

Example: `xConfiguration SIP Domain 1 Name: "100.example-name.com"`

xConfiguration SIP Domain [1..200] Sip: <On/Off>

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.

Example: `xConfiguration SIP Domain 1 Sip: On`

xConfiguration SIP GRUU Mode: <On/Off>

Controls whether GRUU (RFC5627) support is active. Default: On.

Example: `xConfiguration SIP GRUU Mode: On`

xConfiguration SIP MediaRouting ICE Mode: <On/Off>

Controls whether the Expressway takes the media for an ICE to non-ICE call where the ICE participant is thought to be behind a NAT device. Default: Off.

Example: `xConfiguration SIP MediaRouting ICE Mode: Off`

xConfiguration SIP Mode: <On/Off>

Determines whether or not the Expressway will provide SIP registrar and SIP proxy functionality. Default: Off.

Example: `xConfiguration SIP Mode: On`

xConfiguration SIP PreRoutedRouteHeader: <S:0,128>

Controls which Request Messages are allowed to go through the new pre-routed route header path.

As at X12.5, this flag is available only for the SIP REGISTER message.

Example: `xConfiguration SIP PreRoutedRouteHeader: "REGISTER"`

xConfiguration SIP Registration Call Remove: <Yes/No>

Specifies whether associated calls are dropped when a SIP registration expires or is removed. Default: No.

Example: `xConfiguration SIP Registration Call Remove: No`

xConfiguration SIP Registration Mode: <Off/On>

Determines whether or not the Expressway provides SIP registration. Default: On

Example: `xConfiguration SIP Registration Mode: Off`

xConfiguration SIP Registration Outbound Flow Timer: <0..600>

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).

Example: `xConfiguration SIP Registration Outbound Flow Timer: 0`

xConfiguration SIP Registration Outbound Refresh Maximum: <30..7200>

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.

Example: `xConfiguration SIP Registration Outbound Refresh Maximum: 3600`

xConfiguration SIP Registration Outbound Refresh Minimum: <30..7200>

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.

Example: `xConfiguration SIP Registration Outbound Refresh Minimum: 300`

xConfiguration SIP Registration Outbound Refresh Strategy: <Maximum/Variable>

The method used to generate the SIP registration expiry period for Outbound registrations. Default: Variable.

Maximum: uses the lesser of the configured maximum refresh value and the value requested in the registration.

Variable: 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.

Example: `xConfiguration SIP Registration Outbound Refresh Strategy: Variable`

xConfiguration SIP Registration Proxy Mode: <Off/ProxyToKnownOnly/ProxyToAny>

Specifies how proxied registrations should be handled. Default: Off.

Off: registration requests will not be proxied.

ProxyToKnownOnly: registration requests will be proxied to neighbors only.

ProxyToAny: registration requests will be proxied in accordance with the Expressway's existing call processing rules.

Example: `xConfiguration SIP Registration Proxy Mode: Off`

xConfiguration SIP Registration Standard Refresh Maximum: <30..7200>

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.

Example: `xConfiguration SIP Registration Standard Refresh Maximum: 60`

xConfiguration SIP Registration Standard Refresh Minimum: <30..3600>

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.

Example: `xConfiguration SIP Registration Standard Refresh Minimum: 45`

xConfiguration SIP Registration Standard Refresh Strategy: <Maximum/Variable>

The method used to generate the SIP registration expiry period for standard registrations. Default: Maximum.

Maximum: uses the lesser of the configured maximum refresh value and the value requested in the registration.

Variable: 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.

Example: `xConfiguration SIP Registration Standard Refresh Strategy: Maximum`

xConfiguration SIP Require Duo Video Mode: <On/Off>

Controls whether the Expressway requires the use of the com.tandberg.sdp.duo.enable extension for endpoints that support it. Default: On.

Example: `xConfiguration SIP Require Duo Video Mode: On`

xConfiguration SIP Require UDP BFCP Mode: <On/Off>

Controls whether the Expressway will require the use of the com.tandberg.udp.bfcp extension for endpoints that support it. Default: On.

Example: `xConfiguration SIP Require UDP BFCP Mode: On`

xConfiguration SIP Routes Route [1..20] Address: <S:0,39>

Specifies the IP address of the next hop for this route, where matching SIP requests will be forwarded. Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Address: "127.0.0.1"`

xConfiguration SIP Routes Route [1..20] Authenticated: <On/Off>

Whether to forward authenticated requests. Default: Off. Note: this command is intended for developer use only.

On: only forward requests along route if incoming message has been authenticated.

Off: always forward messages that match this route.

Example: `xConfiguration SIP Routes Route 1 Authenticated: On`

xConfiguration SIP Routes Route [1..20] Header Name: <S:0,64>

Name of SIP header field to match (e.g. Event). Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Header Name: "Event"`

xConfiguration SIP Routes Route [1..20] Header Pattern: <S:0,128>

Regular expression to match against the specified SIP header field. Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Header Pattern: "(my-event-package)(.*)"`

xConfiguration SIP Routes Route [1..20] Method: <S:0,64>

SIP method to match to select this route (e.g. INVITE, SUBSCRIBE). Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Method: "SUBSCRIBE"`

xConfiguration SIP Routes Route [1..20] Port: <1..65534>

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.

Example: `xConfiguration SIP Routes Route 1 Port: 22400`

xConfiguration SIP Routes Route [1..20] Request Line Pattern: <S:0,128>

Regular expression to match against the SIP request line. Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Request Line Pattern: ".*@(%localdomains%|%ip%)"`

xConfiguration SIP Routes Route [1..20] Tag: <S:0,64>

Tag value specified by external applications to identify routes that they create. Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Tag: "Tag1"`

xConfiguration SIP Routes Route [1..20] Transport: <UDP/TCP/TLS>

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.

Example: `xConfiguration SIP Routes Route 1 Transport: TCP`

xConfiguration SIP Service SipRegistrationMode: <Off/On>

Determines whether or not the Expressway provides SIP Service registration. Default: On

Example: `xConfiguration SIP Service SipRegistrationMode: Off`

Important The following command is discontinued from Version X14.0.1.

`xConfiguration SIP Registration Mode: <Off/On>`

xConfiguration SIP Session Refresh Minimum: <90..7200>

The minimum value the Expressway will negotiate for the session refresh interval for SIP calls. For more information see the definition of Min-SE header in RFC 4028. Default: 500.

Example: `xConfiguration SIP Session Refresh Minimum: 500`

xConfiguration SIP Session Refresh Value: <90..86400>

The maximum time allowed between session refresh requests for SIP calls. For more information see the definition of Session-Expires in RFC 4028. Default: 1800.

Example: `xConfiguration SIP Session Refresh Value: 1800`

xConfiguration SIP TCP Mode: <On/Off>

Determines whether incoming and outgoing SIP calls using the TCP protocol will be allowed. Default: Off.

Example: `xConfiguration SIP TCP Mode: On`

xConfiguration SIP TCP Outbound Port End: <1024..65534>

Specifies the upper port in the range to be used by outbound TCP/TLS SIP connections. Default: 29999.

Example: `xConfiguration SIP TCP Outbound Port End: 29999`

xConfiguration SIP TCP Outbound Port Start: <1024..65534>

Specifies the lower port in the range to be used by outbound TCP/TLS SIP connections. Default: 25000.

Example: `xConfiguration SIP TCP Outbound Port Start: 25000`

xConfiguration SIP TCP Port: <1024..65534>

Specifies the listening port for incoming SIP TCP calls. Default: 5060.

Example: `xConfiguration SIP TCP Port: 5060`

xConfiguration SIP TLS Certificate Revocation Checking CRL Mode: <On/Off>

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.

Example: `xConfiguration SIP TLS Certificate Revocation Checking CRL Mode: On`

xConfiguration SIP TLS Certificate Revocation Checking CRL Network Fetch Mode: <On/Off>

Controls whether the download of CRLs from the CDP URIs contained in X.509 certificates is allowed. Default: On.

Example: `xConfiguration SIP TLS Certificate Revocation Checking CRL Network Fetch Mode: On`

xConfiguration SIP TLS Certificate Revocation Checking Mode: <On/Off>

Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment. Default: Off.

Example: `xConfiguration SIP TLS Certificate Revocation Checking Mode: Off`

xConfiguration SIP TLS Certificate Revocation Checking OCSP Mode: <On/Off>

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.

Example: `xConfiguration SIP TLS Certificate Revocation Checking OCSP Mode: On`

xConfiguration SIP TLS Certificate Revocation Checking Source Inaccessibility Behavior: <Ignore/Fail>

Controls the revocation checking behavior if the revocation source cannot be contacted. Default: Fail.

Fail: treat the certificate as revoked (and thus do not allow the TLS connection).

Ignore: treat the certificate as not revoked.

Example: `xConfiguration SIP TLS Certificate Revocation Checking Source Inaccessibility Behavior: Fail`

xConfiguration SIP TLS Mode: <On/Off>

Determines whether incoming and outgoing SIP calls using the TLS protocol will be allowed. Default: On.

Example: `xConfiguration SIP TLS Mode: On`

xConfiguration SIP TLS Port: <1024..65534>

Specifies the listening port for incoming SIP TLS calls. Default: 5061.

Example: `xConfiguration SIP TLS Port: 5061`

xConfiguration SIP UDP Mode: <On/Off>

Determines whether incoming and outgoing SIP calls using the UDP protocol will be allowed. Default: Off.

Example: `xConfiguration SIP UDP Mode: On`

xConfiguration SIP UDP Port: <1024..65534>

Specifies the listening port for incoming SIP UDP calls. Default: 5060.

Example: `xConfiguration SIP UDP Port: 5060`

xConfiguration SNMP CommunityName: <S: 0, 16>

The Expressway's SNMP community name. Default: public

Example: `xConfiguration SNMP CommunityName: "public"`

xConfiguration SNMP SystemContact: <S: 0, 70>

The name of the person who can be contacted regarding issues with the Expressway. Default: Administrator.

Example: `xConfiguration SNMP SystemContact: Administrator`

xConfiguration SNMP SystemLocation: <S: 0, 70>

The physical location of the system.

Example: `xConfiguration SNMP SystemLocation: "Server Room 128"`

xConfiguration SNMP V1Mode: <On/Off>

Enables or disables SNMP Version 1 support. Default: Off.

Example: `xConfiguration SNMP V1Mode: Off`

xConfiguration SNMP V2cMode: <On/Off>

Enables or disables SNMP Version 2c support. Default: On.

Example: `xConfiguration SNMP V2cMode: On`

xConfiguration SNMP V3AuthenticationMode: <On/Off>

Enables or disables SNMP Version 3 authentication. Default: On.

Example: `xConfiguration SNMP V3AuthenticationMode: On`

xConfiguration SNMP V3AuthenticationPassword: <S: 0,215>

Sets SNMP Version 3 authentication password. It must be at least 8 characters.

Example: `xConfiguration SNMP V3AuthenticationPassword: "password123"`

xConfiguration SNMP V3Mode: <On/Off>

Enables or disables SNMP Version 3 support. Default: On.

Example: `xConfiguration SNMPV3 Mode: On`

xConfiguration SNMP V3PrivacyMode: <On/Off>

Enables or disables SNMP Version 3 privacy. Default: On.

Example: `xConfiguration SNMP V3PrivacyMode: On`

xConfiguration SNMP V3PrivacyPassword: <S: 0,215>

Sets SNMP Version 3 privacy password. It must be at least 8 characters.

Example: `xConfiguration SNMP V3PrivacyPassword: "password123"`

xConfiguration SNMP V3PrivacyType: <AES>

Sets SNMP Version 3 privacy type. Default: AES.

Example: `xConfiguration SNMP V3PrivacyType: AES`

xConfiguration SNMP V3UserName: <S: 0,70>

Sets the username to use when using SNMP V3.

Example: `xConfiguration SNMP V3UserName: "user123"`

xConfiguration SystemUnit Maintenance Mode: <On/Off>

Sets the Expressway into maintenance mode. New calls and registrations are disallowed and existing calls and registrations are allowed to expire. Default: Off.

Example: `xConfiguration SystemUnit Maintenance Mode: Off`

xConfiguration SystemUnit Name: <S:, 0, 50>

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.

Example: `xConfiguration SystemUnit Name: "MainHQ"`

xConfiguration TimeZone Name: <S: 0, 64>

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.

Example: `xConfiguration TimeZone Name: "GMT"`

xConfiguration Transform [1..100] Description: <S: 0,64>

A free-form description of the transform.

Example: `xConfiguration Transform [1..100] Description: "Change example.net to example.com"`

xConfiguration Transform [1..100] Pattern Behavior: <Strip/Replace>

How the alias is modified. Default: Strip.

Strip: removes the matching prefix or suffix from the alias.

Replace: substitutes the matching part of the alias with the text in replace string.

AddPrefix: prepends the replace string to the alias.

AddSuffix: appends the replace string to the alias.

Example: `xConfiguration Transform 1 Pattern Behavior: Replace`

xConfiguration Transform [1..100] Pattern Replace: <S: 0, 60>

The text string to use in conjunction with the selected Pattern behavior.

Example: `xConfiguration Transform 1 Pattern Replace: "example.com"`

xConfiguration Transform [1..100] Pattern String: <S: 0, 60>

The pattern against which the alias is compared.

Example: `xConfiguration Transform 1 Pattern String: "example.net"`

xConfiguration Transform [1..100] Pattern Type: <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the transform to be applied. Default: Prefix.

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.

Example: `xConfiguration Transform 1 Pattern Type: Suffix`

xConfiguration Transform [1..100] 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 .

Example: `xConfiguration Transform 1 Priority: 10`

xConfiguration Transform [1..100] State: <Enabled/Disabled>

Indicates if the transform is enabled or disabled. Disabled transforms are ignored.

Example: `xConfiguration Transform 1 State: Enabled`

xConfiguration Traversal Media Port End: <1025..65533>

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 .

Example: `xConfiguration Traversal Media Port End: 59999`

xConfiguration Traversal Media Port Start: <1024..65532>

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 .

Example: `xConfiguration Traversal Media Port Start: 36000`

xConfiguration Traversal Server H323 Assent CallSignaling Port: <1024..65534>

The port on the Expressway to use for Assent signaling. Default: 2776 .

Example: `xConfiguration Traversal Server H323 Assent CallSignaling Port: 2777`

xConfiguration Traversal Server H323 H46018 CallSignaling Port: <1024..65534>

The port on the Expressway to use for H460.18 signaling. Default: 2777 .

Example: `xConfiguration Traversal Server H323 H46018 CallSignaling Port: 2777`

xConfiguration Traversal Server TURN Authentication Realm: <S: 1,128>

The realm sent by the server in its authentication challenges. Default: TANDBERG .

Example: `xConfiguration Traversal Server TURN Authentication Realm: "TANDBERG"`

xConfiguration Traversal Server TURN Authentication Remote Mode: <On/Off>

Determines whether the server requires requests to be authenticated. When enabled the server will also authenticate its responses. Default: On.

Example: `xConfiguration Traversal Server TURN Authentication Remote Mode: On`

xConfiguration Traversal Server TURN Media Port End: <1024..65534>

The upper port in the range used for TURN relays. Default: 61799.

Example: `xConfiguration Traversal Server TURN Media Port End: 61799`

xConfiguration Traversal Server TURN Media Port Start: <1024..65534>

The lower port in the range used for TURN relays. Default: 60000.

Example: `xConfiguration Traversal Server TURN Media Port Start: 60000`

xConfiguration Traversal Server TURN Mode: <On/Off>

Determines whether the Expressway offers TURN services to traversal clients. Default: Off .

Example: `xConfiguration Traversal Server TURN Mode: Off`

xConfiguration Traversal Server TURN Port: <1024..65534>

The listening port for TURN requests. Default: 3478.

Example: `xConfiguration Traversal Server TURN Port: 3478`

xConfiguration Traversal Server TURN PortRangeEnd: <1024..65534>

The upper port in the range used for TURN requests. Default: 3483

Example: `xConfiguration Traversal Server TURN PortRangeEnd: 3483`

xConfiguration Traversal Server TURN PortRangeStart: <1024..65534>

The lower port in the range used for TURN requests. Default: 3478.

Example: `xConfiguration Traversal Server TURN PortRangeStart: 3478`

xConfiguration Traversal Server TURN ProtocolMode: <TCP/UDP/Both>

The permitted protocols for TURN requests. Default: Both.

Example: `xConfiguration Traversal Server TURN ProtocolMode: Both`

xConfiguration xConfiguration Traversal Server TURN Authentication Mode: <On/Off>>

Determines whether the server will require requests to be authenticated. When enabled the server will also authenticate its responses. Default: On

Example: `xConfiguration Traversal Server TURN Authentication Mode: On`

xConfiguration XCP Config FcmService: <On/Off>

Controls whether FCM Push Notifications for Jabber Android Devices over MRA are enabled. Default: Off.

Example: `xConfiguration XCP Config FcmService: On`

xConfiguration XCP DelayedRestart EnableDelayedRestart: <On/Off>

Controls whether the Delayed Cisco XCP Router restart feature is enabled. Default: Off.

Example: `xConfiguration DelayedRestart EnableDelayedRestart: On`

xConfiguration XCP DelayedRestart EnableScheduledRestart: <On/Off>

Controls whether a scheduled restart of the Cisco XCP Router is enabled. Default: Off.

Example: `xConfiguration XCP DelayedRestart EnableScheduledRestart: On`

xConfiguration XCP DelayedRestart MultitenancyEnabled: <On/Off>

Turn on multitenancy to configure the delayed Cisco XCP Router restart. Default: Off.

Example: `xConfiguration XCP DelayedRestart MultitenancyEnabled: On`

xConfiguration XCP DelayedRestart ScheduledTime:

The time each day that the scheduled restart takes place.

Example: `xConfiguration XCP DelayedRestart ScheduledTime: 01.00`

xConfiguration XCP DelayedRestartNotify RestartTime:

Set the notification for the restart time.

Example: `xConfiguration DelayedRestartNotify RestartTime: 01.00`

xConfiguration XCP TLS Certificate CVS CertificateRevocationCheck: <On/Off>

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.

Example: `xConfiguration XCP TLS Certificate CVS CertificateRevocationCheck: Off`

xConfiguration XCP TLS Certificate CVS ConvertIpToHostname: <On/Off>

Controls whether Expressway automatically converts XCP peer's IP address to FQDN for certificate verification. Default: On.

Example: `xConfiguration XCP TLS Certificate CVS ConvertIpToHostname: On`

xConfiguration XCP TLS Certificate CVS CrlNetworkFetchEnabled: <On/Off>

Controls whether the Expressway is allowed to download CRLs from the CDP URIs contained in its X.509 certificate. Default: On.

Example: `xConfiguration XCP TLS Certificate CVS CrlNetworkFetchEnabled: On`

xConfiguration XCP TLS Certificate CVS EnableCvs: <On/Off>

Controls whether or not to verify XCP peers' certificates during XCP TLS connection. When *Off*, all other XCP TLS Certificate CVS configuration options will have no effect. Default: On.

Example: `xConfiguration XCP TLS Certificate CVS EnableCvs: On`

xConfiguration XCP TLS Certificate CVS FailOnInaccessibleSource: <On/Off>

Controls the certificate verification behavior if the revocation source cannot be contacted.

On: treat the certificate as revoked (and thus do not allow the TLS connection).

Off: treat the certificate as not revoked.

Default: On.

Example: `xConfiguration XCP TLS Certificate CVS FailOnInaccessibleSource: On`

xConfiguration XCP TLS Certificate CVS UseCrl: <On/Off>

Controls whether Expressway checks its own CRL for revocation of certificates exchanged during establishment of XCP TLS connections. Default: On.

Example: `xConfiguration XCP TLS Certificate CVS UseCrl: On`

xConfiguration XCP TLS Certificate CVS UseOcsp: <On/Off>

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.

Example: `xConfiguration XCP TLS Certificate CVS UseOcsp: On`

xConfiguration XCP TLS Certificate CVS VerifyHostname: <On/Off>

Controls whether the Expressway verifies the hostname from the XCP host's certificate against its own peer configuration. Default: On.

Example: `xConfiguration XCP TLS Certificate CVS VerifyHostname: On`

xConfiguration Zones DefaultZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials.

Example: `xConfiguration Zones DefaultZone Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones DefaultZone SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto.

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones DefaultZone SIP Media Encryption Mode: Auto`

xConfiguration Zones DefaultZone SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off

On: This zone supports ICE.

Off: This zone does not support ICE.

Example: `xConfiguration Zones DefaultZone SIP Media ICE Support: On`

xConfiguration Zones DefaultZone SIP Multistream Mode: <Off/On>

Controls if the Expressway allows Multistream to and from devices in this zone. Default: On

On: allow Multistream

Off: disallow Multistream.

Example: `xConfiguration Zones DefaultZone SIP Multistream Mode: Off`

xConfiguration Zones DefaultZone SIP Record Route Address Type: <IP/Hostname>

Controls whether the Expressway uses its IP address or host name in the Record-Route or Path headers of outgoing SIP requests to this zone. Note: setting this value to hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.

Example: `xConfiguration Zones DefaultZone SIP Record Route Address Type: IP`

xConfiguration Zones DefaultZone SIP SipUpdateRefresh Support: <On/Off>

Determines whether session refresh by SIP UPDATE message is supported in this zone.

On: This zone sends SIP UPDATE messages for SIP session refresh.

Off: This zone does not send SIP UPDATE messages for SIP session refresh.

Default: Off.

Example: `xConfiguration Zones DefaultZone SIP SipUpdateRefresh Support: Off`

xConfiguration Zones DefaultZone SIP TLS Verify Mode: <On/Off>

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.

Example: `xConfiguration Zones DefaultZone SIP TLS Verify Mode: Off`

xConfiguration Zones LocalZone DefaultSubZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

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.

Example: `xConfiguration Zones LocalZone DefaultSubZone Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: <1..100000000>

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.

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: 1920`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth>

Controls if there is a limit on the bandwidth for any one call to or from an endpoint in the Default Subzone.

NoBandwidth: no bandwidth available. No calls can be made to or from the Default Subzone.

Default: Unlimited.

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: Limited`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: <1..100000000>

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.

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: 1920`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth>

Controls if there is a limit on the bandwidth for any one call between two endpoints within the Default Subzone.

NoBandwidth: no bandwidth available. No calls can be made within the Default Subzone.

Default: Unlimited.

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: Limited`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Limit: <1..100000000>

Sets the total bandwidth limit (in kbps) of the Default Subzone (applies only if Mode is set to Limited). Default: 500000 .

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Limit: 500000`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Controls if the Default Subzone has a limit on the total bandwidth being used by its endpoints at any one time.

NoBandwidth: no bandwidth available. No calls can be made to, from, or within the Default Subzone.

Default: Unlimited.

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: Limited`

xConfiguration Zones LocalZone DefaultSubZone Registrations: <Allow/Deny>

Controls whether registrations assigned to the Default Subzone are accepted. Default: Allow.

Example: `xConfiguration Zones LocalZone DefaultSubZone Registrations: Allow`

xConfiguration Zones LocalZone DefaultSubZone SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this subzone. Default: Auto

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones LocalZone DefaultSubZone SIP Media Encryption Mode: Auto`

xConfiguration Zones LocalZone DefaultSubZone SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off

On: This zone supports ICE.

Off: This zone does not support ICE.

Example: `xConfiguration Zones LocalZone DefaultSubZone SIP Media ICE Support: On`

xConfiguration Zones LocalZone DefaultSubZone SIP Multistream Mode: <Off/On>

Controls if the Expressway allows Multistream to and from devices in this zone. Default: On

On: allow Multistream

Off: disallow Multistream.

Example: `xConfiguration Zones LocalZone DefaultSubZone SIP Multistream Mode: Off`

xConfiguration Zones LocalZone DefaultSubZone SIP SipUpdateRefresh Support: <On/Off>

Determines whether session refresh by SIP UPDATE message is supported in this zone.

On: This zone sends SIP UPDATE messages for SIP session refresh.

Off: This zone does not send SIP UPDATE messages for SIP session refresh.

Default: Off.

Example: `xConfiguration Zones LocalZone DefaultSubZone SIP SipUpdateRefresh Support: On`

xConfiguration Zones LocalZone SIP Record Route Address Type: <IP/Hostname>

Controls whether the Expressway uses its IP address or host name in the Record-Route or Path headers of outgoing SIP requests to this zone. Note: setting this value to hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.

Example: `xConfiguration Zones LocalZone SIP Record Route Address Type: IP`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Description: <S: 0,64>

A free-form description of the membership rule.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Description: "Office-based staff"`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Name: <S: 0,50>

Assigns a name to this membership rule.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Name: "Office Workers"`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Pattern String: <S: 0,60>

Specifies the pattern against which the alias is compared.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Pattern String: "@example.com"`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Pattern Type: <Exact/Prefix/Suffix/Regex>

The way in which the pattern must match the alias.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Pattern Type: Suffix`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Priority: <1..65534>

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.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Priority: 100`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] State: <Enabled/Disabled>

Indicates if the membership rule is enabled or disabled. Disabled membership rules are ignored. Default: Enabled.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 State: Enabled`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] SubZoneName: <S: 0,50>

The subzone to which an endpoint is assigned if its address satisfies this rule.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 SubZoneName: "Branch Office"`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Subnet Address: <S: 0,39>

Specifies an IP address used (in conjunction with the prefix length) to identify this subnet.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Subnet Address: "192.168.0.0"`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Subnet PrefixLength: <1..128>

The number of bits of the subnet address which must match for an IP address to belong in this subnet. Default: 32.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Subnet PrefixLength: 32`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Type: <Subnet/AliasPatternMatch>

The type of address that applies to this rule.

Subnet: assigns the device if its IP address falls within the configured IP address subnet.

AliasPatternMatch: assigns the device if its alias matches the configured pattern.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Type: Subnet`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

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.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Inter Limit: <1..100000000>

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.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Inter Limit: 1920`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth for any one call to or from an endpoint in this subzone. Default: Unlimited.

NoBandwidth: no bandwidth available. No calls can be made to or from this subzone.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Inter Mode: Limited`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Intra Limit: <1..100000000>

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.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Intra Limit: 1920`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth for any one call between two endpoints within this subzone. Default: Unlimited.

NoBandwidth: no bandwidth available. No calls can be made within this subzone.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Intra Mode: Limited`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth Total Limit: <1..100000000>

Sets the total bandwidth limit (in kbps) of this subzone (applies only if the mode is set to Limited). Default: 500000.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth Total Limit: 500000`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Controls if this subzone has a limit on the total bandwidth of calls being used by its endpoints at any one time. Default: Unlimited.

NoBandwidth: no bandwidth available. No calls can be made to, from, or within this subzone.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth Total Mode: Limited`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Name: <S: 0, 50>

Assigns a name to this subzone.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Name: "BranchOffice"`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Registrations: <Allow/Deny>

Controls whether registrations assigned to this subzone are accepted. Default: Allow.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Registrations: Allow`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this subzone. Default: Auto

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 SIP Media Encryption Mode: Auto`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off

On: This zone supports ICE.

Off: This zone does not support ICE.

Example: `xConfiguration Zones LocalZone SubZones Subzone 1 SIP Media ICE Support: On`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] SIP Multistream Mode: <Off/On>

Controls if the Expressway allows Multistream to and from devices in this zone. Default: On

On: allow Multistream

Off: disallow Multistream.

Example: `xConfiguration Zones LocalZone SubZones Subzone 1 SIP Multistream Mode: Off`

xConfiguration Zones LocalZone Traversal H323 Assent Mode: <On/Off>

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 .

Example: `xConfiguration Zones LocalZone Traversal H323 Assent Mode: On`

xConfiguration Zones LocalZone Traversal H323 H46018 Mode: <On/Off>

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 .

Example: `xConfiguration Zones LocalZone Traversal H323 H46018 Mode: On`

xConfiguration Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: <On/Off>

Controls whether the Expressway operates in Demultiplexing mode for calls from traversal-enabled endpoints registered directly with it. Default: Off .

On: allows use of the same two ports for all calls.

Off: each call will use a separate pair of ports for media.

Example: `xConfiguration Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: Off`

xConfiguration Zones LocalZone Traversal H323 Preference: <Assent/H46018>

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.

Example: `xConfiguration Zones LocalZone Traversal H323 Preference: Assent`

xConfiguration Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: <1..65534>

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 .

Example: `xConfiguration Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: 20`

xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryCount: <1..65534>

Sets the number of times traversal-enabled endpoints registered directly with the Expressway will attempt to send a TCP probe. Default: 5 .

Example: `xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryCount: 5`

xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the Expressway will send a TCP probe. Default: 2 .

Example: `xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryInterval: 2`

xConfiguration Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: <1..65534>

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 .

Example: `xConfiguration Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: 20`

xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryCount: <1..65534>

Sets the number of times traversal-enabled endpoints registered directly with the Expressway will attempt to send a UDP probe. Default: 5 .

Example: `xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryCount: 5`

xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the Expressway will send a UDP probe. Default: 2 .

Example: `xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryInterval: 2`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: <1..100000000>

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 .

Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: 1920`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth of any one traversal call being handled by the Expressway. Default: Unlimited.

NoBandwidth: no bandwidth available. No traversal calls can be made.

Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: Limited`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Limit: <1..100000000>

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 .

Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Limit: 500000`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Determines whether or not there is a limit to the total bandwidth of all traversal calls being handled by the Expressway. Default: Unlimited.

NoBandwidth: no bandwidth available. No traversal calls can be made.

Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: Limited`

xConfiguration Zones Policy Mode: <SearchRules/Directory>

The mode used when attempting to locate a destination. Default: SearchRules.

SearchRules: use the configured search rules to determine which zones are queried and in what order.

Directory: use the facilities of a directory service to direct the request to the correct zones.

Example: `xConfiguration Zones Policy Mode: SearchRules`

xConfiguration Zones Policy SearchRules Rule [1..2000] Authentication: <Yes/No>

Specifies whether this search rule applies only to authenticated search requests. Default: No.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Authentication: No`

xConfiguration Zones Policy SearchRules Rule [1..2000] Description: <S: 0,64>

A free-form description of the search rule.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Description: "Send query to the DNS zone"`

xConfiguration Zones Policy SearchRules Rule [1..2000] Mode: <AliasPatternMatch/AnyAlias/AnyIPAddress>

Determines whether a query is sent to the target zone. Default: AnyAlias.

AliasPatternMatch: queries the zone only if the alias matches the corresponding pattern type and string.

AnyAlias: queries the zone for any alias (but not IP address).

AnyIPAddress: queries the zone for any given IP address (but not alias).

Example: `xConfiguration Zones Policy SearchRules Rule 1 Mode: AnyAlias`

xConfiguration Zones Policy SearchRules Rule [1..2000] Name: <S: 0,50>

Descriptive name for the search rule.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Name: "DNS lookup"`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern Behavior: <Strip/Leave/Replace>

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.

Leave: the alias is not modified.

Strip: the matching prefix or suffix is removed from the alias.

Replace: the matching part of the alias is substituted with the text in the replace string.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Pattern Behavior: Strip`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern Replace: <S: 0,60>

The string to substitute for the part of the alias that matches the pattern. (Applies to Replace pattern behavior only.)

Example: `xConfiguration Zones Policy SearchRules Rule 1 Pattern Replace: "@example.net"`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern String: <S: 0,60>

The pattern against which the alias is compared. (Applies to Alias Pattern Match mode only.)

Example: `xConfiguration Zones Policy SearchRules Rule 1 Pattern String: "@example.com"`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern Type: <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the rule to be applied. (Applies to Alias Pattern Match mode only.) Default: Prefix.

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.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Pattern Type: Suffix`

xConfiguration Zones Policy SearchRules Rule [1..2000] Priority: <1..65534>

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.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Priority: 100`

xConfiguration Zones Policy SearchRules Rule [1..2000] Progress: <Continue/Stop>

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.

Continue: continue applying the remaining search rules (in priority order) until the endpoint identified by the alias is found.

Stop: do not apply any more search rules, even if the endpoint identified by the alias is not found in the target zone.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Progress: Continue`

xConfiguration Zones Policy SearchRules Rule [1..2000] Protocol: <Any/H323/SIP>

The source protocol required for the rule to match.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Protocol: Any`

xConfiguration Zones Policy SearchRules Rule [1..2000] Source Mode: <Any/AllZones/LocalZone/Named>

The sources of the requests for which this rule applies. Default: Any.

Any: locally registered devices, neighbor or traversal zones, and any non-registered devices.

All zones: locally registered devices plus neighbor or traversal zones.

Local Zone: locally registered devices only.

Named: A specific Zone or SubZone.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Source Mode: Any`

xConfiguration Zones Policy SearchRules Rule [1..2000] Source Name: <S: 0..50>

The name of the source (Sub)Zone for which this rule applies.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Source Name: "Local Office"`

xConfiguration Zones Policy SearchRules Rule [1..2000] State: <Enabled/Disabled>

Indicates if the search rule is enabled or disabled. Disabled search rules are ignored. Default: Enabled .

Example: `xConfiguration Zones Policy SearchRules Rule 1 State: Enabled`

xConfiguration Zones Policy SearchRules Rule [1..2000] Target Name: <S: 0,50>

The zone or policy service to query if the alias matches the search rule.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Target Name: "Sales Office"`

xConfiguration Zones Policy SearchRules Rule [1..2000] Target Type: <Zone/PolicyService>

The type of target this search rule applies to.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Target Type: Zone`

xConfiguration Zones Zone [1..1000] DNS IncludeAddressRecord: <On/Off>

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 .

Example: `xConfiguration Zones Zone 1 DNS IncludeAddressRecord: Off`

xConfiguration 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>`

Specifies which audio codec to use when empty INVITEs are not allowed. Default: G711u .

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP Audio DefaultCodec: G711u`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP EmptyInviteAllowed: <On/Off>

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.

On: SIP INVITEs with no SDP will be generated and sent to this neighbor.

Off: SIP INVITEs will be generated and a pre-configured SDP will be inserted before the INVITEs are sent to this neighbor.

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP EmptyInviteAllowed: On`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Video DefaultBitrate: <64..65535>

Specifies which video bit rate to use when empty INVITEs are not allowed. Default: 384 .

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultBitrate: 384`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264>

Specifies which video codec to use when empty INVITEs are not allowed. Default: H263 .

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultCodec: H263`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>

Specifies which video resolution to use when empty INVITEs are not allowed. Default: CIF .

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultResolution: CIF`

xConfiguration Zones Zone [1..1000] DNS SIP Default Transport: <UDP/TCP/TLS>

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.

Example: `xConfiguration Zones Zone [1..1000] DNS SIP Default Transport: UDP`

xConfiguration Zones Zone [1..1000] DNS SIP Media AesGcm Support: <Off/On>

Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. Default: Off.

Example: `xConfiguration Zones Zone 1 DNS SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] DNS SIP SipUpdateRefresh Support: <Off/On>

Determines whether session refresh by SIP UPDATE message is supported in this zone.

On: This zone sends SIP UPDATE messages for SIP session refresh.

Off: This zone does not send SIP UPDATE messages for SIP session refresh.

Default: Off.

Example: `xConfiguration Zones Zone 1 DNS SIP SipUpdateRefresh Support: On`

xConfiguration Zones Zone [1..1000] DNS SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto.

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones Zone 1 DNS SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] DNS SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off.

On: This zone supports ICE.

Off: This zone does not support ICE.

Example: `xConfiguration Zones Zone 1 DNS SIP Media ICE Support: Off`

xConfiguration Zones Zone [1..1000] DNS SIP Media ICEPassThrough Support: <On/Off>

Controls whether ICE Pass Through is supported by the devices in the zone. Default: Off

On: This zone supports ICE Pass Through.

Off: This zone does not support ICE Pass Through.

Example: `xConfiguration Zones Zone 1 DNS SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] DNS SIP Poison Mode: <On/Off>

Determines whether SIP requests sent out to this zone will be "poisoned" such that if they are received by the local Expressway again they will be rejected. Default: Off .

On: SIP requests sent out via this zone that are received again by this Expressway will be rejected.

Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.

Example: `xConfiguration Zones Zone 1 DNS SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] DNS SIP PreloadedSipRoutes Accept: <Off/On>

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.

Example: `xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] DNS SIP Record Route Address Type: <IP/Hostname>

Controls whether the Expressway uses its IP address or host name in the Record-Route or Path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.

Example: `xConfiguration Zones Zone 1 DNS SIP Record Route Address Type: IP`

xConfiguration Zones Zone [1..1000] DNS SIP SearchAutoResponse: <On/Off>

Controls what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. Default: Off .

Off: a SIP OPTION message will be sent to the zone.

On: searches will be responded to automatically, without being forwarded to the zone.

Example: `xConfiguration Zones Zone 1 DNS SIP SearchAutoResponse: Off`

xConfiguration Zones Zone [1..1000] DNS SIP TLS Verify Mode: <On/Off>

Controls X.509 certificate checking between this Expressway and the destination system server returned by the DNS lookup. When enabled, the domain name submitted to the DNS lookup must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes).

Default: Off.

Example: `xConfiguration Zones Zone 1 DNS SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] DNS SIP TLS Verify Subject Name: <S: 0..128>

The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). If empty then the domain portion of the resolved URI is used.

Example: `xConfiguration Zones Zone 1 DNS SIP TLS Verify Subject Name: "example.com"`

xConfiguration Zones Zone [1..1000] DNS SIP UDP BFCP Filter Mode: <On/Off>

Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. Default: Off .

On: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled.

Off: INVITE requests are not modified.

Example: `xConfiguration Zones Zone 1 DNS SIP UDP BFCP Filter Mode: Off`

xConfiguration Zones Zone [1..1000] DNS ZoneProfile:

`<Default/Custom/CiscoUnifiedCommunicationsManager/CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDevice/LocalB2BUAService>`

Determines how the zone's advanced settings are configured.

Default: uses the factory defaults.

Custom: allows you to configure each setting individually.

Preconfigured profiles: alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.

Example: `xConfiguration Zones Zone 1 DNS ZoneProfile: Default`

xConfiguration Zones Zone [1..1000] ENUM DNSSuffix: <S: 0, 128>

The DNS zone to append to the transformed E.164 number to create an ENUM host name which this zone is then queried for.

Example: `xConfiguration Zones Zone 2 ENUM DNSSuffix: "e164.arpa"`

xConfiguration Zones Zone [1..1000] H323 Mode: <On/Off>

Determines whether H.323 calls will be allowed to and from this zone. Default: On .

Example: `xConfiguration Zones Zone 2 H323 Mode: On`

xConfiguration Zones Zone [1..1000] HopCount: <1..255>

Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used. Default: 15 .

Example: `xConfiguration Zones Zone 2 HopCount: 15`

xConfiguration Zones Zone [1..1000] Name: <S: 1, 50>

Assigns a name to this zone.

Example: `xConfiguration Zones Zone 3 Name: "UK Sales Office"`

xConfiguration Zones Zone [1..1000] Neighbor Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials.

Example: `xConfiguration Zones Zone 3 Neighbor Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones Zone [1..1000] Neighbor H323 CallSignaling Port: <1024..65534>

The port on the neighbor to use for H.323 calls to and from this Expressway. Default: 1720 .

Example: `xConfiguration Zones Zone 3 Neighbor H323 CallSignaling Port: 1720`

xConfiguration Zones Zone [1..1000] Neighbor H323 Port: <1024..65534>

The port on the neighbor to use for H.323 searches to and from this Expressway. Default: 1719 .

Example: `xConfiguration Zones Zone 3 Neighbor H323 Port: 1719`

xConfiguration Zones Zone [1..1000] Neighbor H323 SearchAutoResponse: <On/Off>

Determines what happens when the Expressway receives a H323 search, destined for this zone. Default: Off.

Off: an LRQ message will be sent to the zone.

On: searches will be responded to automatically, without being forwarded to the zone.

Example: `xConfiguration Zones Zone 3 Neighbor H323 SearchAutoResponse: Off`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Audio DefaultCodec:

`<G711u/G711a/G722_48/G722_56/G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48/G723_1/G728/G729/AACLD_48/AACLD_56/AACLD_64/AMR>`

Specifies which audio codec to use when empty INVITEs are not allowed. Default: G711u .

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Audio DefaultCodec: G711u`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP EmptyInviteAllowed: <On/Off>

Determines whether the Expressway will generate a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. Default: On .

On: SIP INVITEs with no SDP will be generated and sent to this neighbor.

Off: SIP INVITEs will be generated and a pre-configured SDP will be inserted before the INVITEs are sent to this neighbor.

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP EmptyInviteAllowed: On`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Encryption EncryptSRTCP: <Yes/No>

Controls if the Expressway offers encrypted SRTCP in calls to this zone. The Expressway will send an INFO request. Default: No.

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Encryption EncryptSRTCP: No`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Search Strategy: <Options/Info>

Determines how the Expressway will search for SIP endpoints when interworking an H.323 call. Default: Options .

Options: the Expressway will send an OPTIONS request.

Info: the Expressway will send an INFO request.

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Search Strategy: Options`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultBitrate: <64..65535>

Specifies which video bit rate to use when empty INVITEs are not allowed. Default: 384 .

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultBitrate: 384`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264>

Specifies which video codec to use when empty INVITEs are not allowed. Default: H263 .

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultCodec: H263`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>

Specifies which video resolution to use when empty INVITEs are not allowed. Default: CIF .

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultResolution: CIF`

xConfiguration Zones Zone [1..1000] Neighbor Monitor: <Yes/No>

Specifies whether the zone monitors the aliveness of its neighbor peers. H323 LRQs and/or SIP OPTIONS will be periodically sent to the peers. If any peer fails to respond, that peer will be marked as inactive. If no peer manages to respond the zone will be marked as inactive. Default: Yes.

Example: `xConfiguration Zones Zone 3 Neighbor Monitor: Yes`

xConfiguration Zones Zone [1..1000] Neighbor Peer [1..6] Address: <S:0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the neighbor. If the neighbor zone is an Expressway cluster, this will be one of the peers in that cluster.

Example: `xConfiguration Zones Zone 3 Neighbor Peer 1 Address: "192.44.0.18"`

xConfiguration Zones Zone [1..1000] Neighbor Registrations: <Allow/Deny>

Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow .

Example: `xConfiguration Zones Zone 3 Neighbor Registrations: Allow`

xConfiguration Zones Zone [1..1000] Neighbor RetainConnectionOnParseErrorMode: <mode>

Controls how tolerant the system is of malformed or corrupt SIP messages.

DropAll: The system closes the SIP connection when it receives a malformed or corrupt SIP message.

RetainSome: The system maintains the SIP connection when it receives a SIP message with malformed, non-mandatory headers. It closes the connection if any mandatory headers are malformed.

RetainAll: The system maintains the SIP connection when it receives a SIP message with any malformed headers (including mandatory headers).

Default: DropAll.

Note

- The *Content-Length* header is an exception. If this header is missing or malformed, the connection is always closed, regardless of the mode.
- The connection is also always closed, regardless of the mode, if the Expressway receives more than 10 consecutive malformed messages.
- For CMR Cloud deployments, we recommend configuring RetainAll mode.

Example: `xConfiguration Zones Zone 3 RetainConnectionOnParseErrorMode: RetainSome`

xConfiguration Zones Zone [1..1000] Neighbor SIP Authentication Trust Mode: <On/Off>

Controls if authenticated SIP messages (ones containing a P-Asserted-Identity header) from this zone are trusted. Default: Off .

On: messages are trusted without further challenge.

Off: messages are challenged for authentication.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Authentication Trust Mode: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP B2BUA Refer Mode: <Forward/Terminate>

Determines how SIP REFER requests are handled.

Forward: SIP REFER requests are forwarded to the target.

Terminate: SIP REFER requests are terminated by the Expressway.

Default: Forward

Example: `xConfiguration Zones Zone 3 Neighbor SIP B2BUA Refer Mode: Terminate`

xConfiguration Zones Zone [1..1000] Neighbor SIP B2BUA Replaces Mode: <Forward/Terminate>

Enables the Expressway to process load balancing INVITE messages from Meeting Server call bridge groups. Default: Forward

Terminate: Expressway B2BUA processes the INVITEs from the Meeting Server. Required to enable load balancing for endpoints that are registered to this Expressway, or to a neighboring VCS or Expressway.

Forward: Expressway proxies the INVITEs from the Meeting Server. This is an option if your endpoints are registered to Unified CM, because Unified CM could process those INVITEs instead.

Example: `xConfiguration Zones Zone 3 Neighbor SIP B2BUA Replaces Mode: Terminate`

xConfiguration Zones Zone [1..1000] Neighbor SIP B2BUA Service Identifier: <0..64>

The identifier that represents an instance of a local SIP Back-to-Back User Agent service.

Example: `xConfiguration Zones Zone 3 Neighbor SIP B2BUA Service Identifier: 1`

xConfiguration Zones Zone [1..1000] Neighbor SIP ClassFiveResponseLiveness: <Yes/No>

Specifies whether Class 5 SIP responses from neighbor peers result in the zone being considered alive for use. Default: Yes.

Example: `xConfiguration Zones Zone 3 Neighbor SIP ClassFiveResponseLiveness: Yes`

xConfiguration Zones Zone [1..1000] Neighbor SIP Encryption Mode: <Auto/Microsoft/Off>

Determines how the Expressway handles encrypted SIP calls on this zone. Default: Auto.

Auto: SIP calls are encrypted if a secure SIP transport (TLS) is used.

Microsoft: SIP calls are encrypted using MS-SRTP.

Off: SIP calls are never encrypted.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SIP MIME Strip Mode: <On/Off>

Controls whether multipart MIME stripping is performed on requests from this zone. This must be set to On for connections to a Microsoft Office Communications Server 2007. Default: Off.

Example: `xConfiguration Zones Zone 3 Neighbor SIP MIME Strip Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media AesGcm Support: <Off/On>

Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. Default: Off.

Example: `xConfiguration Zones Zone 1 Neighbor SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off

On: This zone supports ICE.

Off: This zone does not support ICE.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Media ICE Support: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media ICEPassThrough Support: <On/Off>

Controls whether ICE Pass Through is supported by the devices in the zone. Default: Off

On: This zone supports ICE Pass Through.

Off: This zone does not support ICE Pass Through.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP MediaRouting Mode: <Auto/Signaled/Latching>

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. .

Signaled: media is always taken for calls to and from this neighbor. It will be forwarded as signaled in the SDP received from this neighbor.

Latching: 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.

Auto: 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).

Example: `xConfiguration Zones Zone 3 Neighbor SIP MediaRouting Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SIP Multistream Mode: <Off/On>

Controls if the Expressway allows Multistream to and from devices in this zone. Default: On

On: allow Multistream

Off: disallow Multistream.

Example: `xConfiguration Zones Zone 1 Neighbor SIP Multistream Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP Poison Mode: <On/Off>

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 .

On: SIP requests sent out via this zone that are received again by this Expressway will be rejected.

Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP Port: <1024..65534>

Specifies the port on the neighbor to be used for SIP calls to and from this Expressway. Default: 5061 .

Example: `xConfiguration Zones Zone 3 Neighbor SIP Port: 5061`

xConfiguration Zones Zone [1..1000] Neighbor SIP PreloadedSipRoutes Accept: <Off/On>

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.

Example: `xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP ProxyRequire Strip List: <S: 0,255>

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.

Example: `xConfiguration Zones Zone 3 Neighbor SIP ProxyRequire Strip List: "com.example.something,com.example.somethingelse"`

xConfiguration Zones Zone [1..1000] Neighbor SIP RFC3327 Enabled: <Yes/No>

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.

Example: `xConfiguration Zones Zone [1..1000] Neighbor SIP RFC3327 Enabled: Yes`

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 `xConfiguration CollaborationEdge RFC3327Enabled`.

xConfiguration Zones Zone [1..1000] Neighbor SIP Record Route Address Type: <IP/Hostname>

Controls whether the Expressway uses its IP address or host name in the Record-Route or Path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Record Route Address Type: IP`

xConfiguration Zones Zone [1..1000] Neighbor SIP SearchAutoResponse: <On/Off>

Controls what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. Default: Off .

Off: a SIP OPTION message will be sent to the zone.

On: searches will be responded to automatically, without being forwarded to the zone.

Example: `xConfiguration Zones Zone 3 Neighbor SIP SearchAutoResponse: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP SipUpdateRefresh Support: <On/Off>

Determines whether session refresh by SIP UPDATE message is supported in this zone.

On: This zone sends SIP UPDATE messages for SIP session refresh.

Off: This zone does not send SIP UPDATE messages for SIP session refresh.

Default: Off

Example: `xConfiguration Zones Zone 3 Neighbor SIP SipUpdateRefresh Support: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication for inbound and outbound connections between this Expressway and the neighbor system. When enabled, the neighbor system's FQDN or IP address, as specified in the Peer address field, must be contained within the neighbor's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: Off .

Example: `xConfiguration Zones Zone 3 Neighbor SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP Transport: <UDP/TCP/TLS>

Determines which transport type will be used for SIP calls to and from this neighbor. Default: TLS .

Example: `xConfiguration Zones Zone 3 Neighbor SIP Transport: TLS`

xConfiguration Zones Zone [1..1000] Neighbor SIP UDP BFCP Filter Mode: <On/Off>

Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. Default: Off .

On: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled.

Off: INVITE requests are not modified.

Example: `xConfiguration Zones Zone 3 Neighbor SIP UDP BFCP Filter Mode: Off`

xConfiguration Zones Zone 1 Neighbor SIP UDP IX Filter Mode: <On/Off>

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. Default: Off.

On: any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled.

Off: INVITE requests are not modified.

Example: `xConfiguration Zones Zone 1 neighbor SIP UDP IX Filter Mode: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP UPDATE Strip Mode: <On/Off>

Determines whether the Expressway strips the UPDATE method from the Allow header of all requests and responses going to and from this zone. Default: Off .

Example: `xConfiguration Zones Zone 3 Neighbor SIP UPDATE Strip Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SignalingRouting Mode: <Auto/Always>

Specifies how the Expressway handles the signaling for calls to and from this neighbor. Default: Auto.

Auto: Signaling will be taken as determined by the Call Routed Mode configuration.

Always: Signaling will always be taken for calls to or from this neighbor, regardless of the Call Routed Mode configuration.

Example: `xConfiguration Zones Zone 3 Neighbor SignalingRouting Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SRV MaxPeers: <1..30>

Specifies the maximum number of peers the Expressway can register with when the given neighbor zone is configured with an SRV record lookup.

Examples: `xConfiguration Zones Zone 1 Neighbor SRV MaxPeers: 30`

xConfiguration Zones Zone [1..1000] Neighbor ZoneProfile:

`<Default/Custom/CiscoUnifiedCommunicationsManager/CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDevice/LocalB2BUAService>`

Determines how the zone's advanced settings are configured.

Default: uses the factory defaults.

Custom: allows you to configure each setting individually.

Preconfigured profiles: alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.

Example: `xConfiguration Zones Zone 3 Neighbor ZoneProfile: Default`

xConfiguration Zones Zone [1..1000] SIP Mode: <On/Off>

Determines whether SIP calls will be allowed to and from this zone. Default: On.

Example: `xConfiguration Zones Zone 3 SIP Mode: On`

xConfiguration Zones Zone [1..1000] TraversalClient Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials.

Example: `xConfiguration Zones Zone 4 TraversalClient Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones Zone [1..1000] TraversalClient Authentication Password: <S: 0,215>

The password used by the Expressway when connecting to the traversal server. The maximum plaintext length is 128 characters, which is then encrypted.

Example: `xConfiguration Zones Zone 4 TraversalClient Authentication Password: "password123"`

xConfiguration Zones Zone [1..1000] TraversalClient Authentication UserName: <S: 0,128>

The user name used by the Expressway when connecting to the traversal server.

Example: `xConfiguration Zones Zone 4 TraversalClient Authentication UserName: "clientname"`

xConfiguration Zones Zone [1..1000] TraversalClient DisconnectOnFailInterval: <10>

When a peer fails to respond to an OPTIONS ping, the Traversal Client zone enters an error state. If the DISCONNECT_ON_FAIL_INTERVAL is configured, then, while in the error state the expressway node disconnects the connection before sending the OPTIONS ping to ensure connectivity robustness. The disconnect occurs at intervals according to the DISCONNECT_ON_FAIL_INTERVAL.

By default, this flag is disabled. To enable, set the value range from 0 to 3600 seconds

Min Value = 0.

Max Value = 3600.

Default: 0 (Disabled)

Example: `xConfiguration Zones Zone 1 TraversalClient DisconnectOnFailInterval: "10"`

xConfiguration Zones Zone [1..1000] TraversalClient H323 Port: <1024..65534>

The port on the traversal server to use for H.323 firewall traversal calls from this Expressway. If the traversal server is an Expressway-E, this must be the port number that is configured on the Expressway-E's traversal server zone associated with this Expressway.

Example: `xConfiguration Zones Zone 4 TraversalClient H323 Port: 2777`

xConfiguration Zones Zone [1..1000] TraversalClient H323 Protocol: <Assent/H46018>

Determines which of the two firewall traversal protocols will be used for calls to and from the traversal server. Note: the same protocol must be set on the server for calls to and from this traversal client. Default: Assent.

Example: `xConfiguration Zones Zone 4 TraversalClient H323 Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalClient Peer [1..6] Address: <S:0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the traversal server. If the traversal server is an Expressway-E cluster, this will be one of the peers in that cluster.

Example: `xConfiguration Zones Zone 4 TraversalClient Peer 1 Address: "10.192.168.1"`

xConfiguration Zones Zone [1..1000] TraversalClient Registrations: <Allow/Deny>

Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow.

Example: `xConfiguration Zones Zone 4 TraversalClient Registrations: Allow`

xConfiguration Zones Zone [1..1000] TraversalClient RetryInterval: <1..65534>

The interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. Default: 120.

Example: `xConfiguration Zones Zone 4 TraversalClient RetryInterval: 120`

xConfiguration Zones Zone [1..1000] TraversalClient SIP SipUpdateRefresh Support: <Off/On>

Determines whether session refresh by SIP UPDATE message is supported in this zone.

On: This zone sends SIP UPDATE messages for SIP session refresh.

Off: This zone does not send SIP UPDATE messages for SIP session refresh.

Default: Off

Example: `xConfiguration Zones Zone 1 TraversalClient SIP SipUpdateRefresh Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media AesGcm Support: <Off/On>

Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. Default: Off.

Example: `xConfiguration Zones Zone 1 TraversalClient SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto.

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off

On: This zone supports ICE.

Off: This zone does not support ICE.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Media ICE Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media ICEPassThrough Support: <On/Off>

Controls whether ICE Pass Through is supported by the devices in the zone. Default: Off

On: This zone supports ICE Pass Through.

Off: This zone does not support ICE Pass Through.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Multistream Mode: <Off/On>

Controls if the Expressway allows Multistream to and from devices in this zone. Default: On

On: allow Multistream

Off: disallow Multistream.

Example: `xConfiguration Zones Zone 1 TraversalClient SIP Multistream Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Poison Mode: <On/Off>

Controls whether SIP requests sent out to this zone are "poisoned" such that if they are received by the local Expressway again they will be rejected. Default: Off .

On: SIP requests sent out via this zone that are received again by this Expressway will be rejected.

Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Port: <1024..65534>

Specifies the port on the traversal server to be used for SIP calls from this Expressway. If your traversal server is an Expressway-E, this must be the port number that has been configured in the traversal server zone for this Expressway.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Port: 5061`

xConfiguration Zones Zone [1..1000] TraversalClient SIP PreloadedSipRoutes Accept: <Off/On>

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.

Example: `xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Protocol: <Assent/TURN/ICE>

Determines which firewall traversal protocol will be used for SIP calls to and from the traversal server. Note: the same protocol must be set on the server for calls to and from this traversal client. Default: Assent.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalClient SIP TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal server. When enabled, the server's FQDN or IP address, as specified in the Peer address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: Off.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Transport: <TCP/TLS>

Determines which transport type will be used for SIP calls to and from the traversal server. Default: TLS .

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Transport: TLS`

xConfiguration Zones Zone [1..1000] TraversalServer Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials.

Example: `xConfiguration Zones Zone 5 TraversalServer Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones Zone [1..1000] TraversalServer Authentication UserName: <S: 0,128>

The name used by the traversal client when authenticating with the traversal server. If the traversal client is an Expressway, this must be the Expressway's authentication user name. If the traversal client is a gatekeeper, this must be the gatekeeper's System Name.

Example: `xConfiguration Zones Zone 5 TraversalServer Authentication UserName: "User123"`

xConfiguration Zones Zone [1..1000] TraversalServer H323 H46019 Demultiplexing Mode: <On/Off>

Determines whether the Expressway will operate in demultiplexing mode for calls from the traversal client. Default: Off .

On: allows use of the same two ports for all calls.

Off: each call will use a separate pair of ports for media.

Example: `xConfiguration Zones Zone 5 TraversalServer H323 H46019 Demultiplexing Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalServer H323 Port: <1024..65534>

Specifies the port on the Expressway being used for H.323 firewall traversal from this traversal client. Default: 6001, incrementing by 1 for each new zone.

Example: `xConfiguration Zones Zone 5 TraversalServer H323 Port: 2777`

xConfiguration Zones Zone [1..1000] TraversalServer H323 Protocol: <Assent/H46018>

Determines which of the two firewall traversal protocols will be used for calls to and from the traversal client. Note: the same protocol must be set on the client for calls to and from this traversal server. Default: Assent .

Example: `xConfiguration Zones Zone 5 TraversalServer H323 Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalServer Registrations: <Allow/Deny>

Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow .

Example: `xConfiguration Zones Zone 5 TraversalServer Registrations: Allow`

xConfiguration Zones Zone [1..1000] TraversalServer SIP SipUpdateRefresh Support: <Off/On>

Determines whether session refresh by SIP UPDATE message is supported in this zone.

On: This zone sends SIP UPDATE messages for SIP session refresh.

Off: This zone does not send SIP UPDATE messages for SIP session refresh.

Default: Off.

Example: `xConfiguration Zones Zone 1 TraversalServer SIP SipUpdateRefresh Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media AesGcm Support: <Off/On>

Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. Default: Off.

Example: `xConfiguration Zones Zone 1 TraversalServer SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off

On: This zone supports ICE.

Off: This zone does not supports ICE.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Media ICE Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media ICEPassThrough Support: <On/Off>

Controls whether ICE Pass Through is supported by the devices in the zone. Default: Off

On: This zone supports ICE Pass Through.

Off: This zone does not supports ICE Pass Through.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Multistream Mode: <Off/On>

Controls if the Expressway allows Multistream to and from devices in this zone. Default: On

On: allow Multistream

Off: disallow Multistream.

Example: `xConfiguration Zones Zone 1 TraversalServer SIP Multistream Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Poison Mode: <On/Off>

Controls whether SIP requests sent out to this zone are "poisoned" such that if they are received by the local Expressway again they will be rejected. Default: Off .

On: SIP requests sent out via this zone that are received again by this Expressway will be rejected.

Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Port: <1024..65534>

The port on the Expressway being used for SIP firewall traversal from this traversal client. Default: 7001, incrementing by 1 for each new zone.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Port: 5061`

xConfiguration Zones Zone [1..1000] TraversalServer SIP PreloadedSipRoutes Accept: <Off/On>

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.

Example: `xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Protocol: <Assent/TURN/ICE>

Determines which firewall traversal protocol will be used for SIP calls to and from the traversal client. Note: the same protocol must be set on the client for calls to and from this traversal server. Default: Assent.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalServer SIP TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified. Default: Off.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP TLS Verify Subject Name: <S: 0,128>

The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes).

Example: `xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Subject Name: "myclientname"`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Transport: <TCP/TLS>

Determines which of the two transport types will be used for SIP calls between the traversal client and Expressway. Default: TLS .

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Transport: TLS`

xConfiguration Zones Zone [1..1000] TraversalServer TCPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which the traversal client will send a TCP probe to the Expressway once a call is established, in order to keep the firewall's NAT bindings open. Default: 20.

Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe KeepAliveInterval: 20`

xConfiguration Zones Zone [1..1000] TraversalServer TCPProbe RetryCount: <1..65534>

Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway. Default: 5 .

Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryCount: 5`

xConfiguration Zones Zone [1..1000] TraversalServer TCPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway. Default: 2 .

Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryInterval: 2`

xConfiguration Zones Zone [1..1000] TraversalServer UDPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which the traversal client will send a UDP probe to the Expressway once a call is established, in order to keep the firewall's NAT bindings open. Default: 20.

Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe KeepAliveInterval: 20`

xConfiguration Zones Zone [1..1000] TraversalServer UDPProbe RetryCount: <1..65534>

Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway. Default: 5.

Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryCount: 5`

xConfiguration Zones Zone [1..1000] TraversalServer UDPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway. Default: 2.

Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryInterval: 2`

xConfiguration Zones Zone [1..1000] Type: <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>

Determines the nature of the specified zone, in relation to the local Expressway.

Neighbor: the new zone will be a neighbor of the local Expressway.

TraversalClient: there is a firewall between the zones, and the local Expressway is a traversal client of the new zone.

TraversalServer: there is a firewall between the zones and the local Expressway is a traversal server for the new zone.

ENUM: the new zone contains endpoints discoverable by ENUM lookup.

DNS: the new zone contains endpoints discoverable by DNS lookup.

Example: `xConfiguration Zones Zone 3 Type: Neighbor`

xConfiguration license smart debug: <error/trace/debug/all>

Enables debugging for Smart Licensing. Default: Error.

Error: Logs errors encountered in Smart Licensing.

Trace: Logs trace messages during normal Smart Licensing operations.

Debug: Logs debug messages.

All: Enables all three levels. (Peer-specific)

Example: `xConfiguration license smart debug: all`

xConfiguration license smart deregister: <On/Off>

The product reverts to evaluation mode providing the evaluation period has not expired. All license entitlements used for the product are released immediately to the virtual account and are available for other product instances to use it. (Peer-specific)

Example: `xConfiguration license smart deregister: On`

xConfiguration license smart privacy: <none/all/hostname/version>

Use if hostname and IP address of this product instance must not be exchanged with the Cisco Smart Software Manager or Cisco Smart Software Manager Satellite. (Peer-specific)

Example: `xConfiguration license smart privacy: all`

xConfiguration license smart register idtoken: <String>

Use the Product Instance Registration token that you generated from Smart Software Manager or your Smart Software Manager satellite to register the product. (Peer-specific)

Example: `xConfiguration license smart register idtoken: <Token>`

xConfiguration license smart renew ID: <On/Off>

Perform this operation if automatic registration renewal fails due to network connectivity issues with Cisco Smart Software Manager. (Peer-specific)

Example: `xConfiguration license smart renew ID: On`

xConfiguration license smart renew auth: <On/Off>

Perform this operation if automatic authorization status renewal failed due to network connectivity issues with Cisco Smart Software Manager. (Peer-specific)

Example: `xConfiguration license smart renew auth: On`

xConfiguration license smart transport: <direct/satellite>

Determines how this product instance communicate with Cisco Smart Software Manager to send and receive usage information.

Direct: Communicates directly over the internet to the Cisco Smart Software Manager.

Satellite: Communicates through a Smart Software Manager satellite deployed on your premises.

Example: `xConfiguration license smart transport: direct`

xConfiguration license smart reregister: <String>

Perform this operation to reregister the product instance in the following cases: Previous registration attempt of this product instance failed due to network connectivity issue and you want to reregister after resolving this issue. To reregister the product instance, already registered with a virtual account, to a different virtual account. (Peer-specific)

Example: `xConfiguration license smart reregister: <Token>`

xConfiguration license smart url: <String>

Enter the URL of the Cisco Smart Software Manager satellite server. (Peer-specific)

Example: `xConfiguration license smart url: http://www.alpha.crate.cisco.com/Transport gateway`

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)	Indicates that this is a required parameter. Note that the (r) is not part of the command itself.

To obtain information about using each of the **xCommand** commands from within the CLI, type:

- **xCommand** or **xCommand ?** to return a list of all available **xCommand** commands.
- **xCommand ??** to return all current **xCommand** commands, along with a description of each command, a list of its parameters, and for each parameter its valuespaces and description.
- **xCommand <command> ?** to return a description of the command, a list of its parameters, and for each parameter its valuespaces and description.

About the set-access command (experimental)

The set-access command enables access to Expressway internal system commands. **These commands exist for the use of Cisco support and development teams only.** Do not access the commands unless it is under the advice and supervision of your Cisco support representative.

Caution Incorrect usage of these commands could cause the system operation to become unstable, cause performance problems, and cause persistent corruption of system configuration.

To use set-access:

1. Log into the CLI as administrator.
2. Type `set-access qwertsys`

   This enables the system commands ("sys-") that are associated with set-access.
3. Enter `?` to list the available commands.

xCommand Commands

All the available **xCommand** commands are listed in the table below:

Table 46: xCommand CLI reference

xCommand ACME Delete Pending Cert Deletes a pending certificate. *Domain: <String>* A pending certificate is one that has been signed by an ACME provider and which may have/not have been deployed to the Expressway. If passed no arguments or empty string, the command deletes the pending server certificate, otherwise it will delete pending certificate for the specified domain. Examples: `xCommand ACME Delete Pending Cert` `xCommand ACME Delete Pending Cert Domain:"example.com"`
xCommand ACME Deploy Deploys a pending certificate. *Domain: <String>* *ReloadCerts: <On/Off>* If passed no arguments, the command deploys the pending server certificate and reloads the certificate for the required processes. Otherwise it deploys the certificate for the specified domain and reloads the certificate if specified by ReloadCerts parameter. Examples: `xCommand ACME Deploy` `xCommand ACME Deploy Domain:"example.com" ReloadCerts:"On"`

xCommand ACME Get Pending Cert

Fetches a pending certificate.

Domain: <String>

A pending certificate is one that has been signed by an ACME provider and which may have/not have been deployed to the Expressway.

If passed no arguments the command fetches the server certificate, otherwise it fetches the certificate for the specified domain.

Examples: `xCommand ACME Get Pending Cert`

`xCommand ACME Get Pending Cert Domain:"example.com"`

xCommand ACME Providers Read

Reads information about the ACME provider.

ProviderUuid: <"Default"/String>

If passed no arguments the command will return information about all providers in the database. The string "Default" returns information about the default provider. Provide a UUID to return information about that specific provider.

Examples: `xCommand ACME Providers Read`

`xCommand ACME Providers Read ProviderUuid: "Default"`

`xCommand ACME Providers Read ProviderUuid: "Provider-UUID"`

xCommand ACME Providers Write

Updates information about the provider.

Default: <On/Off>

Email(r): <String>

Name: <String>

ProviderUuid(r): <"Default"/String>

TermsOfService(r): <Accepted>

Url: <String>

You must supply ProviderUuid, Email, and TermsOfService arguments. The command only allows you to update the Email address and Terms Of Service for a particular provider. It ignores all other arguments that you supply.

Example: `xCommand ACME Providers Write ProviderUuid: "Default" Email: "new-email@example.com" TermsOfService: "Accepted"`

xCommand ACME Reset

Resets the ACME service on the Expressway-E, removing all configuration issued through CLI, Rest API, or web interface.

Action: <execute>

The command can only be invoked on Expressway-E. It cannot run if SIGN, DISCARD, or DEPLOY commands are in progress. Acmereset cannot run unless ACME service is disabled for all domain certificates and the server certificate.

Example: `xCommand ACME Reset execute`

```
xCommand ACME Reset Action: "execute"
```

xCommand ACME Revoke

Revokes an ACME certificate.

CertPath: <String>

Provider: <String>

Before you can revoke an ACME certificate, you must prove to the provider that you control the domain name/SAN entries in that certificate.

To validate this control, you must use the normal submit and sign process to generate a new certificate containing the same domain name/SAN entries as the original certificate.

After you receive the new certificate, revoke the old one using `acmerevoke` with the path to the certificate

Example, using the default ACME provider: `xCommand ACME Revoke "/path_to_cert_to_be_revoked"`

Example, using a specific ACME provider:

```
xCommand ACME Revoke CertPath:"/path_to_cert_to_be_revoked" Provider:"ACME_Provider_Name"
```

xCommand ACME Settings Read

Reads ACME settings.

Domain: <String>

Enter this command without parameters to read the ACME settings for the server certificate. Otherwise, supply the domain to read ACME settings for a specified domain.

Examples: `xCommand ACME Settings Read`

```
xCommand ACME Settings Read "example.com"
```

xCommand ACME Settings Write

Writes ACME settings.

AcmeManaged(r): <Disabled/Manual/Automated>

Domain: <String>

ProviderUuid: <String>

RenewKey: <Retain/Rotate>

RenewalSchedule: <String>

If you do not specify a domain, the command writes the settings for the ACME service managing the server certificate. Otherwise it writes settings for the specified domain.

If the specified domain does not yet have ACME settings, the command writes the settings for that domain using the default provider's UUID.

If the specified domain already has ACME settings, the command updates the settings that you supply, and does not change any settings you did not specify.

You must supply the AcmeManaged parameter. If you set AcmeManaged to Automated, then you must also supply RenewalSchedule and RenewKey.

Examples: `xCommand ACME Settings Write AcmeManaged: "Manual"`

```
xCommand ACME Settings Write AcmeManaged: "Automated" Domain: "example.com" RenewalSchedule:
"{"DaysOfWeek":["Mon"],"TimeOfDay":"04:00"}" RenewKey: "Rotate"
```

xCommand ACME Sign

Signs a CSR.

Domain: <String>

NumSanEntries: <-2147483648..2147483647>

Enter the command with no parameters to submit the CSR for the server certificate to its ACME provider. Supply a domain to submit the CSR for a domain certificate to its ACME provider.

Do not supply the `NumSanEntries` parameter. It has no user-modifiable purpose.

Example: `xCommand Acme Sign`

```
xCommand ACME Sign Domain: "example.com"
```

xCommand Admin Account Add

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 Admin Account Add Name: "bob_smith" Password: "abcXYZ_123" AccessAPI: On AccessWeb: On Enabled: On`

xCommand Admin Account Delete

Deletes a local administrator account.

Name(r): <S: 0, 128>

The username of the account to delete.

Example: `xCommand Admin Account Delete: "bob_smith"`

xCommand Admin Group Add

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 Admin Group Add Name: "administrators" AccessAPI: On AccessWeb: On Enabled: On`

xCommand Admin Group Delete

Deletes an administrator group.

Name(r): <S: 0, 128>

The name of the group to delete.

Example: `xCommand Admin Group Delete: "administrators"`

xCommand Allow List Add

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 Allow List Add PatternString: "John.Smith@example.com" PatternType: Exact Description: "Allow John Smith"`

xCommand Allow List Delete

Deletes an entry from the Allow List.

AllowListId(r): <1..2500>

The index of the entry to be deleted.

Example: `xCommand Allow List Delete AllowListId: 2`

xCommand Boot

Reboots the Expressway.

This command has no parameters.

Example: `xCommand Boot`

xcommand Certs Command for Server CSR

Allows to generate Server Certificate Signing Request (CSR)

Default value of Publickeyalgorithm parameter is “RSA”

The following are the Supported Keysize(s) for

- ECDSA: 256, 384, 521
- RSA: 2048, 4096

Example: `xcommand Certs Command csr_create subjectfields: '{"CN": "www.cisco.com", "C": "US", "OU": "expressway" }' Keysize: 256 Publickeyalgorithm: ECDSA`

xcommand Certs Command for Domain CSR

Allows to generate Domain Certificate Signing Request (CSR)

Deafult value of Publickeyalgorithm parameter is “RSA”

The following are the Supported Keysize(s) for

- ECDSA: 256, 384, 521
- RSA: 2048, 4096

Example: `xcommand Certs Command: csr_create subjectfields: '{"CN": "www.cisco.com", "C": "US", "OU": "expressway" }' Keysize: 256 Publickeyalgorithm: ECDSA Domain: cisco.com`

xCommand Check Bandwidth

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 Check Bandwidth Node1: “DefaultSubzone” Node2: “UK Sales Office” Bandwidth: 512 CallType: nontraversal`

xCommand Check Pattern

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 Check Pattern Target: "bob@a.net" Pattern: "@a.net" Type: "suffix" Behavior: replace Replace: "@a.com"`

xCommand Clear All Status

Clears all status and history on the system.

Example: `xCommand Clear All Status`

xCommand Cluster Address Mapping Add

Fqdn(r): <Value>

IpAddress(r): <Value>

Adds an FQDN/IP mapping entry to the cluster address mapping table.

xCommand Cluster Address Mapping Delete

Fqdn(r): <Value>

IpAddress(r): <Value>

Deletes an FQDN/IP mapping entry from the cluster address mapping table.

xCommand CMS Add

Manage Cisco Meeting Server web bridges. Add a Guest account client URI

Name: <Value>

Example: `xCommand CMS Add name: "join.example.com"`

xCommand CMS Delete

Manage Cisco Meeting Server web bridges. Delete a Guest account client URI

Name: <Value>

Example: `xCommand CMS Delete name: "join.example.com"`

xCommand Credential Add

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 Credential Add Name: "alice" Password: "abcXYZ_123"`

xCommand Credential Delete

Deletes an entry from the local authentication database.

Name(r): <String>

The name of the entry to delete.

Example: `xCommand Credential Delete Name: "alice"`

xCommand CUCM Config Add

Performs a lookup on a Unified CM publisher.

Address(r): <Value>

The FQDN or IP address of the Unified CM publisher.

Axlpassword(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 CUCM Config Add Address: "cucm.example.com" Axlpassword: "xyz" Axlusername: "abc"`

xCommand CUCM Config Delete

Deletes the details of a Unified CM publisher.

Address(r): <Value>

The FQDN or IP address of the Unified CM publisher.

Example: `xCommand CUCM Config delete Address: "cucm.example.com"`

xCommand CUCM Mixed Mode Check

Address(r): <Value>

The FQDN or IP address of the Unified CM publisher.

Axlpassword(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.

xCommand Custom Notification Add

Adds a customized entry for alarm-based email notifications. Per alarm id, either to disable notifications for the alarm ID or to direct them to a specified email address.

alarm_id: <String> Enter the alarm Id for which you want to customize or disable notifications.

custom_email: <S: 0, 254> If the Notification is "Custom", enter the email id to which the selected alarm notifications are to be sent.

disable_notify: <on/off> Choose the action you want for the selected alarm:

- On : No notification regarding the selected alarm will be sent.
- Off : Notification regarding the selected alarm will be sent to the email id entered in the Email field.

Default: On

To add a custom notification, specify disable_notify as "Off".

After a custom notification is added, it will be listed in the xconfiguration command "Alarm Notification Email".

xCommand Custom Notification Delete

Removes a customized entry for alarm-based email notifications.

alarm_id(r): <String> Enter the alarm Id for which you want to customize or disable notifications.

xCommand Default Links Add

Restores links between the Default Subzone, Traversal Subzone and the Default Zone.

This command has no parameters.

Example: `xCommand Default Links Add`

xCommand Default Values Set

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 Default Values Set Level: 1`

xCommand Deny List Add

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 Deny List Add PatternString: "sally.jones@example.com" PatternType: exact Description: "Deny Sally Jones"`

xCommand Deny List Delete

Deletes an entry from the Deny List.

DenyListId(r): <1..2500>

The index of the entry to be deleted.

Example: `xCommand Deny List Delete DenyListId: 2`

xCommand Disconnect Call

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 Disconnect Call CallSerialNumber: "6d843434-211c-11b2-b35d-0010f30f521c"`

xCommand DNS Lookup

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 DNS Lookup Hostname: "example.com" RecordType: all`

xCommand DNS Per Domain Server Add

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 DNS Server Add Address: "192.168.12.0" Index: 1`

xCommand DNS Per Domain Server Delete

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 DNS Per Domain Server Delete Address: "192.168.12.0"`

xCommand DNS Server Add

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 DNS Server Add Address: "192.168.12.0" Index: 1`

xCommand DNS Server Delete

Deletes a DNS server

Address: <Value>

The IP address of the DNS server to delete.

Example: `xCommand DNS Server Delete Address: "192.168.12.0"`

xCommand Domain Add

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 and Presence Serverfor 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 Domain Add Name: "100.example-name.com" Authzone: "Traversal zone" Edge: Off Sip: On`

xCommand Domain Delete

Deletes a domain.

DomainId(r): <1..200>

The index of the domain to be deleted.

Example: `xCommand Domain Delete DomainId: 2`

xCommand Domain Certs

Manage multidomain certificates for Server Name Indication (SNI).

Each Domain Certs xCommand requires a 'command' parameter specifying an operation to be performed, followed by any additional parameters required for the specific command.

Domain Certs commands and associated parameters:

domain_list: Lists domains for which certificates are managed for SNI.

parameters: (none)

Example: `xCommand Domain Certs command: domain_list`

domain_create: Creates a new domain for managing certificates for SNI.

parameters: domain

Example: `xCommand Domain Certs command: domain_create domain: a.com`

domain_delete: Deletes the specified certificate domain.

parameters: domain

Example: `xCommand Domain Certs 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 Domain Certs 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 Domain Certs 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" }'`

Note

- 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 Domain Certs command: csr_get domain: a.com`

csr_delete: Deletes a pending certificate signing request.

parameters: domain

Example: `xCommand Domain Certs command: csr_delete domain: a.com`

is_cert_set: Returns true if a certificate has been set for the domain.

parameters: domain

Example: `xCommand Domain Certs command: is_cert_set domain: a.com`

cert_put: Uploads a certificate and private key.

parameters: domain, certpath, keypath

Example: `xCommand Domain Certs command: cert_put domain: a.com certpath: /tmp/cert.pem keypath: /tmp/key.pem`

Note
- 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 Domain Certs command: cert_get domain: a.com`

cert_delete: Deletes a domain's certificate and private key.

parameters: domain

Example: `xCommand Domain Certs 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>

xCommand Edge SSO Delete Tokens

Deletes all tokens issued to a particular user.

Username(r): <String>

Specifes which user's tokens will be deleted.

Example: `xCommand Edge SSO Delete Tokens Username: "APerson"`

xCommand Edge SSO Purge Tokens

Deletes all tokens issued to all users.

Example: `xCommand Edge SSO Purge Tokens`

xCommand Edge SSO Status Clear

Resets the SSO request/response counters to 0.

Example: `xCommand Edge SSO Status Clear`

xCommand Feedback Deregister

Deactivates a particular feedback request.

ID: <1..3>

The index of the feedback request to be deactivated.

Example: `xCommand Feedback Deregister ID: 1`

xCommand Feedback Register

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 Feedback Register ID: 1 URL: "http://192.168.0.1/feedback/" Expression.1: "Status/Calls" Expression.2: "Event/CallAttempt"`

xCommand Find Registration

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 want to find out about.

Example: `xCommand Find Registration Alias: "john.smith@example.com"`

Important This command is applicable **only** to Cisco TelePresence Video Communication Server (VCS) Series.

xCommand Fips

Sets FIPS140-2 cryptographic mode.

Command: <leave/enter/status>

Either enters, leaves or provides the current status of the system's FIPS140-2 cryptographic mode.

Example: `xCommand Fips Command: enter`

xCommand Force Config Update

Forces the relevant configuration on this peer to be updated to match that of the cluster primary.

This command has no parameters.

Example: `xCommand Force Config Update`

Important HSM functionality may be a Preview feature only, depending on the Expressway software version. For example, it is a Preview feature in version X12.6.

Please check the release notes for your Expressway version before you use HSM and if its status is Preview for your software version, **only enable HSM and use these HSM-related commands if you are willing to implement it as a Preview feature, and subject to the Preview disclaimer contained in the Expressway Release Notes**.

xCommand HSM Mode Read

Returns the current HSM mode set on the Expressway.

Example: `xCommand HSM Mode Read`

xCommand HSM Mode Write

Changes the HSM mode on Expressway. Can only be used if HSM settings and at least one HSM module is already configured on the Expressway.

Mode: <enabled, disabled>

Example: `xCommand HSM Mode Write Mode: enabled`

xCommand HSM Module Add

Adds a new HSM module to the Expressway configuration. HSM provider settings must be configured before using this command.

Ip(r): <S: 0, 1024>

The IP address of the HSM device to be added.

Port: <1..65535>

The port being used to communicate with an nShield HSM. Optional. Default is 9004.

Esn: <S: 0, 1024>

The serial number of an nShield HSM. Required.

Kneti: <S: 0, 1024>

The security hash used to verify an nShield HSM. Required.

Example: `xCommand HSM Module Add Ip: 1.1.1.1 Port: 9004 Esn: abcd-abcd-abcd Kneti: abcd1234abcd1234a`

xCommand HSM Module Remove

Removes an HSM module from the list of modules used by the Expressway.

Ip(r): <S: 0, 1024>

This command requires an IP address of an already configured HSM module.

Example: `xCommand HSM Module Remove Ip: 1.1.1.1`

xCommand HSM Modules

Returns a list of the HSM modules to be used by the Expressway.

Example: `xCommand HSM Modules`

xCommand HSM Settings Read

Returns the currently configured HSM settings.

Example: `xCommand HSM settings Read`

xCommand HSM Settings Write

Configures the HSM provider to be used (see the *Expressway Release Notes* for details of which providers are supported; support may be on a Preview basis only).

Provider(r): <nShield>

The HSM provider to be configured.

Rfsip: <S: 0, 1024>

The IP address of the Thales RFS (Remote File System). Required when nShield HSMs are used.

Rfsport: <1..65535>

The port being used to communicate with the RFS. Required when nShield HSMs are used. Default 9004

Example: `xCommand HSM Settings Write Provider: "nShield" Rfsip: "1.1.1.1" Rfsport: "9004"`

xCommand HTTP Allow List Export

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. The file path should start with '/tmp/'.

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.

xCommand HTTP Allow List Export Test

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. The file path should start with '/tmp/'.

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.

xCommand HTTP Allow List Rule Add

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.

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 HTTP Allow List Rule Add URLfile: "/tmp/rules.csv"`

Example 2: `xCommand HTTP Allow List Rule Add 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"`

xCommand HTTP Allow List Rule Delete

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 HTTP Allow List Rule Delete URLfile: "/tmp/rules.csv"`

Example 2: `xCommand HTTP Allow List Rule Delete 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"`

xCommand HTTP Allow List Rules Test

(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.

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.

Example: `xCommand HTTP Allow List Rules Test Tests: "/tmp/tests.csv" Rules: "/tmp/rules.csv"`

xCommand HTTP Allow List Test Add

(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.

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 HTTP Allow List Test Add URLfile: "/tmp/tests.csv"`

Example 2: `xCommand MRA Allow List Test Add URL: "https://cucm2.example.com:8443/partial/path" ExpectedResult: block Description: "https access to write to partial/path/ on cucm2.example.com" HttpMethod: "POST"`

xCommand HTTP Allow List Test Delete

(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 HTTP Allow List Test Delete URLfile: "/tmp/tests.csv"`

Example 2: `xCommand HTTP Allow List Test Delete URL: "https://cucm2.example.com:8443/partial/path" ExpectedResult: allow HttpMethod: "get"`

xCommand HTTP Proxy Jabber CTargets Add

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 HTTP Proxy Jabber CTargets Add DomainIndex: 2 Host: jabberguest.example.com`

xCommand HTTP Proxy Jabber CTargets Delete

Deletes the configured Jabber Guest Server from the Expressway.

Host(r): <S:1,1024> The FQDN of the Jabber Guest Server to delete.

xCommand IMP Server Add

Adds an external messaging server to which to route Microsoft SIP Simple messages.

IMP(r): <Value> configuration/b2bua/imp/imp

xCommand IMP Server Delete

Deletes an external messaging server.

IMP(r): <Value> configuration/b2bua/imp/imp

xCommand License Smart Deregister

The product reverts to evaluation mode providing the evaluation period has not expired. License entitlements used for the product are released immediately to the virtual account and are available for other product instances to use it.

xCommand License Smart Register Idtoken: <String>

Use the Product Instance Registration token that you generated from Smart Software Manager or your Smart Software Manager satellite to register the product.

xCommand License Smart Renew Auth

Perform this operation if automatic authorization status renewal failed due to network connectivity issues with Cisco Smart Software Manager.

xCommand License Smart Renew ID

Perform this operation if automatic registration renewal failed due to network connectivity issues with Cisco Smart Software Manager.

xCommand License Smart Reregister: <String>

Perform this operation to reregister the product instance in the following cases:

- Previous registration attempt of this product instance failed due to network connectivity issue and you want to reregister after resolving this issue.
- To reregister the product instance, already registered with a virtual account, to a different virtual account.

xCommand Link Add

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 Link Add LinkName: "Subzone1 to UK" Node1: "Subzone1" Node2: "UK Sales Office" Pipe1: "512Kb ASDL"`

xCommand Link Delete

Deletes a link.

LinkId(r): <1..3000>

The index of the link to be deleted.

Example: `xCommand Link Delete LinkId: 2`

xCommand 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`

xCommand Network Interface

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 LAN 2 port.

Example: `xCommand Networkinterface DualInterfaces: enable`

DedicatedManagementInterface: <enable/disable/status>

If enabled, the Dedicated Management Interface (DMI) uses the LAN3 port for management traffic. (If you try to disable the DMI and a management service is using it as its only interface, the command will fail.)

Example: `xCommand Network Interface DedicatedManagementInterface: enable`

xCommand Network Limits

Controls the experimental rate limiting feature.

Enter `xCommand Network Limits ?` to read the help.

xCommand NTP Server Add

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 NTP Server Add Address: ntp.server.example.com`

xCommand NTP Server Delete

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the NTP server to delete.

Example: `xCommand NTP Server Delete Address: "ntp.server.example.com"`

xCommand Option Key Add

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 Option Key Add Key: "1X4757T5-1-60BAD5CD"`

xCommand Option Key Delete

Deletes a software option key from the Expressway.

OptionKeyId(r): <1..64>

Specifies the ID of the software option to be deleted.

Example: `xCommand Option Key Delete OptionKeyId: 2`

xCommand 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"`

xCommand Pipe Add

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 Pipe Add PipeName: "512k ADSL" TotalMode: Limited Total: 512 PerCallMode: Limited PerCall: 128`

xCommand Pipe Delete

Deletes a pipe.

PipeId(r): <1..1000>

The index of the pipe to be deleted.

Example: `xCommand Pipe Delete PipeId: 2`

xCommand Policy Service Add

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 Policy Service Add 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'/>”`

xCommand Policy Service Delete

Deletes a policy service.

PolicyServiceId(r): <1..20>

The index of the policy service to be deleted.

Example: `xCommand Policy Service Delete PolicyServiceId: 1`

xCommand Remote Syslog Add

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 Remote Syslog Add Address: "remote_server.example.com" Crlcheck: Off Format: bsd Loglevel: warning Mode: bsd Port: 514 Transport: udp`

xCommand Remote Syslog Delete

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 Remote Syslog Delete Address: "remote_server.example.com" Port: 514 Transport: udp`

xCommand Remove Registration

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 Remove Registration RegistrationSerialNumber: "a761c4bc-25c9-11b2-a37f-0010f30f521c"`

xCommand Restart

Restarts the Expressway without a full system reboot.

This command has no parameters.

Example: `xCommand Restart`

xCommand Route Add

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 selects the most appropriate interface to use. Default: Auto

Example: `xCommand Route Add Address: "10.13.8.0" PrefixLength: 32 Gateway: "192.44.0.1"`

xCommand Route Delete

Deletes a route.

RouteId(r): <1..50>

The index of the route to be deleted.

Example: `xCommand Route Delete RouteId: 1`

Important This command is applicable **only** to Cisco TelePresence Video Communication Server (VCS) Series.

xCommand Secure Mode

Controls Advanced Account Security options.

Command(r): <on/off/status>

The index of the route to be deleted.

Example: `xCommand Secure Mode Command: off`

xCommand Search Rule Add

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 Search Rule Add Name: "DNS lookup" ZoneName: "Sales Office Description": "Send query to the DNS zone"`

xCommand Search Rule Delete

Deletes a search rule.

SearchRuleId(r): <1..2000>

The index of the search rule to be deleted.

Example: `xCommand Search Rule Delete SearchRuleId: 1`

xCommand Trace Path

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 Trace Path Hostname: "example.com"`

xCommand Trace Route

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 Trace Route Hostname: "example.com"`

xCommand Transform Add

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 Transform Add Pattern: "example.net" Type: suffix Behavior: replace Replace: "example.com" Priority: 3 Description: "Change example.net to example.com" State: Enabled`

xCommand Transform Delete

Deletes a transform.

TransformId(r): <1..100>

The index of the transform to be deleted.

Example: `xCommand Transform Delete TransformId: 2`

xCommand Ucxn Config Add

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 Expressway to access the Unity Connection publisher. For example, System Administrator role in UC publisher.

xCommand Ucxn Config Delete

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.

xCommand XMPP Delete

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 XMPP Delete Address: "imp_server.example.com"`

xCommand XMPP Discovery

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 XMPP Discovery Address: "imp.example.com" Axlpassword: "xyz" Axlusername: "abc"`

xCommand Zone Add

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 Zone Add ZoneName: "UK Sales Office" Type: Neighbor`

xCommand Zone Delete

Deletes a zone.

ZoneId(r): <1..1000>

The index of the zone to be deleted.

Example: `xCommand Zone Delete ZoneId: 2`

xCommand Zone List

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 Zone List 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
- 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 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			√	√

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 / TURNSERVER / TURNCLIENT / ICE]		√	√
UNAUTHENTICATED_SOURCE_ALIAS			√	√
UTCTIME		√	√	√

Parameter name	Values	Registration policy	Search rules	Call policy
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.

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

Code	Tag	Message	Description
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 47: 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

RFC	Description
2976	SIP INFO method
3164	The BSD syslog Protocol
3261	Session Initiation Protocol
3263	Locating SIP Servers
3264	An Offer/Answer Model with the Session Description Protocol (SDP)
3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
3326	The Reason Header Field for the Session initiation Protocol (SIP)
3265	Session Initiation Protocol (SIP) – Specific Event Notification
3327	Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
3489	STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
3515	The Session Initiation Protocol (SIP) Refer Method
3550	RTP: A Transport Protocol for Real-Time Applications
3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
3596	DNS Extensions to Support IP Version 6
3761	The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)
3880	Call Processing Language (CPL): A Language for User Control of Internet Telephony Services
3891	Replaces header
3892	Referred-by header
3903	Session Initiation Protocol (SIP) Extension for Event State Publication
3944	H.350 Directory Services
3986	Uniform Resource Identifier (URI): Generic Syntax

RFC	Description
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 in earlier software releases, starting from version X8.7. For information about a particular feature, see Release Notes for the relevant software version.

New features from software version X12.5 and later are not supported for the Cisco VCS product, and apply only to the Cisco Expressway product. For VCS systems, this version is provided for maintenance and bug fixing purposes only.

X12.6 Features

Table 48: Feature History by Release Number - Cisco Expressway Series

Feature/ change	Status
Whisper Coaching / Whisper Announcements over MRA	Supported from X12.6.2
Customizable Alarm-based Email Notifications	Supported from X12.6.2
Agent Greeting over MRA	Supported from X12.6.2
Display Active MRA Registrations Count	Supported from X12.6.1
Silent Monitoring Over MRA	Supported from X12.6.1
Security Enhancements	Supported from X12.6
Smart Licensing	Supported from X12.6
Type and Series Configuration by UI Setting not by Option Key	Supported from X12.6
Alarm-based Email Notifications	Supported from X12.6
Hardware Security Module (HSM) Support	Preview
Android Push Notifications for IM&P	Preview (disabled by default from X12.6.2)
Headset Capabilities for Cisco Contact Center	Preview
Multiple Presence Domains over MRA	Preview
Expressway Forward Proxy	Removed from X12.6.2
Smart Call Home	Removed from X12.6.2
Advanced Media Gateway	Removed from X12.6

X12.5 Features

Table 49: Feature History by Release Number - Cisco Expressway Series

Feature/ change	X12.5	X12.5.1	X12.5.2, X12.5.3	X12.5.4, X12.5.5, X12.5.6, X12.5.9 (X12.5.7 & X12.5.8 withdrawn)
Direct 9-1-1 Calls for “Kari's Law” (for Applicable B2B Deployments)	NA	NA	NA	Supported from X12.5.7 onwards
Virtualized Systems - ESXi Qualification and version support	Please see the *Cisco Expressway on Virtual Machine Installation Guide* for details			
ACME (Automated Certificate Management Environment) support on Expressway-E	Supported	Supported	Supported	Supported
Single SAML for Clusters	Supported	Supported	Supported	Supported
SIP Proxy to Multiple Meeting Server Conference Bridges - Support for Cisco Meeting Server Load Balancing (Not new in X12.5. Included for information due to its preview status)	Preview	Supported	Supported	Supported
MRA: Media Path Optimization for ICE	Supported	Supported	Supported	Supported
MRA: Improved Handling of Dual Network Domains with no Split DNS	Supported	Supported	Supported	Supported

Feature/ change	X12.5	X12.5.1	X12.5.2, X12.5.3	X12.5.4, X12.5.5, X12.5.6, X12.5.9 (X12.5.7 & X12.5.8 withdrawn)
MRA: OAuth with Refresh (Self-Describing) on Unified CM SIP Lines	Preview	Supported	Supported	Supported
MRA: Device Onboarding with Activation Codes	Preview	Preview	Preview	Supported
MRA: Support for Encrypted iX	Preview	Preview	Preview	Supported
MRA: Support for Headset Management	Preview	Preview	Preview	Supported
Features which are not new in X12.5 but included for information due to their former preview status:				
Cisco Meeting App can use the Expressway-E TURN Server	Preview	Supported	Supported	Supported
Multiple Presence Domains over MRA	Preview	Preview	Preview	Preview
Smart Call Home	Deprecated and Preview	Deprecated and Preview	Deprecated and Preview	Deprecated and Preview

X8.11 Features

Table 50: Feature History by Release Number

Feature/ change	X8.11 (withdrawn)	X8.11.1 (withdrawn)	X8.11.2 (withdrawn)	X8.11.3 (withdrawn)	X8.11.4
System Size Selection for Appliances	—	—	—	Supported	Supported

Feature/ change	X8.11 (withdrawn)	X8.11.1 (withdrawn)	X8.11.2 (withdrawn)	X8.11.3 (withdrawn)	X8.11.4
Finesse Agent Support over MRA	—	—	Supported	Supported	Supported
First Software Release for the CE1200 Appliance	—	Supported	Supported	Supported	Supported
Device Registration to Expressway-E (SIP and H.323)	Supported	Supported	Supported	Supported	Supported
Changes to Cisco TMS Provisioning Access	Supported	Supported	Supported	Supported	Supported
Multiway Conferencing on Cisco Expressway Series	Supported	Supported	Supported	Supported	Supported
SIP Proxy to Multiple Meeting Server Conference Bridges (Support for Cisco Meeting Server Load Balancing)	Preview	Preview	Preview	Preview	Preview
Web Proxy to Multiple Meeting Server Web Bridges	Supported	Supported	Supported	Supported	Supported
Cisco Meeting App can use Expressway-E TURN Server	Preview	Preview	Preview	Preview	Preview
TURN on TCP 443	Supported	Supported	Supported	Supported	Supported

Feature/ change	X8.11 (withdrawn)	X8.11.1 (withdrawn)	X8.11.2 (withdrawn)	X8.11.3 (withdrawn)	X8.11.4
TURN Port Multiplexing on Large Expressway-E	Supported	Supported	Supported	Supported	Supported
Improved Security of Data at Rest	Supported	Supported	Supported	Supported	Supported
Common Criteria Preparation	Supported	Supported	Supported	Supported	Supported
Mandatory Password on Backups	Supported	Supported	Supported	Supported	Supported
Custom Domain Search	Supported	Supported	Supported	Supported	Supported
Built-in-Bridge Recording over MRA (Not new in X8.11. Included for information due to its former preview status) Information about BiB over MRA is now available in the *Mobile and Remote Access Through Cisco Expressway* guide	Supported (formerly preview)	Supported	Supported	Supported	Supported
Access Policy Support over MRA (Not new in X8.11. Included for information due to its former preview status)	Supported (formerly preview) Requires Cisco Jabber 12.0	As for X8.11	As for X8.11	As for X8.11	As for X8.11

Feature/ change	X8.11 (withdrawn)	X8.11.1 (withdrawn)	X8.11.2 (withdrawn)	X8.11.3 (withdrawn)	X8.11.4
Multiple Presence Domains over MRA (Not new in X8.11. Included for information due to its preview status)	Preview	Preview	Preview	Preview	Preview
License Key Consolidation	Supported	Supported	Supported	Supported	Supported
Factory Reset of Peer Leaving Cluster	Supported	Supported	Supported	Supported	Supported
Smart Call Home (Not new in X8.11. Included for information due to its preview status)	Preview	Preview	Preview	Preview	Preview
SRV Connectivity Tester Tool	Supported	Supported	Supported	Supported	Supported
REST API Expansion	Supported	Supported	Supported	Supported	Supported

X8.10 Features

Table 51: Feature History by Release Number

Feature / change	X8.10	X8.10.1	X8.10.2	X8.10.3 (no change)	X8.10.4 (no change)
Built-in-Bridge Recording over MRA	Not supported	Not supported	Preview	Preview	Preview
Improved Push Notification Support for MRA	Preview	Supported	Supported	Supported	Supported

Feature / change	X8.10	X8.10.1	X8.10.2	X8.10.3 (no change)	X8.10.4 (no change)
Self-Describing Tokens Support for MRA (OAuth tokens with refresh)	Preview	Supported	Supported	Supported	Supported
Access Control Configuration Changes for MRA	Supported	Supported	Supported	Supported	Supported
Access Policy Support for MRA	Preview	Preview	Preview	Preview	Preview
Changes to TLS and Cipher Suite Defaults	Supported	Supported	Supported	Supported	Supported
AES-GCM Cipher Mode for Media Encryption	Supported	Supported	Supported	Supported	Supported
Delayed Cisco XCP Router Restart for Multitenancy	Supported	Supported	Supported	Supported	Supported
Server Name Indication for Multitenancy	Supported	Supported	Supported	Supported	Supported
Session Identifier Support	Supported	Supported	Supported	Supported	Supported
REST API Expansion	Supported	Supported	Supported	Supported	Supported
Smart Call Home (Not new in X8.10. Included for information due to its preview status)	Preview	Preview	Preview	Preview	Preview

X8.9 Features

Table 52: Feature History by Release Number

Feature / change	X8.9	X8.9.1	X8.9.2
Apple Push Notifications Service Pass Through to Cisco Jabber for iPhone and iPad	Not supported	Supported	Supported
Edge Traversal of Microsoft SIP Traffic for Cisco Meeting Server	Supported	Supported	Supported
Web Proxy for Meeting Server	Not supported	Not supported	Supported
IM and Presence Service Federation With Skype for Business or Office 365 Organizations	Preview	Supported	Supported
Cisco Expressway as H.323 Gatekeeper	Supported	Supported	Supported
REST API Expansion	Supported	Supported	Supported
Allow Jabber for iPhone and iPad to Use Safari for SSO Over MRA	Supported	Supported	Supported
Shared Line / Multiple Line Support for MRA Endpoints	Preview	Supported	Supported
Smart Call Home	Preview	Preview	Preview
Secure Install Wizard	Supported	Supported	Supported
DiffServ Code Point Marking	Supported	Supported	Supported
Maintenance Mode For MRA	Supported	Supported	Supported

X8.8 Features

Table 53: Feature History by Release Number

Feature / change	X8.8
Registrations On Expressway	Supported
Skype for Business 2016 and Skype for Business Mobile Support	Supported
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

X8.7 Features

Table 54: 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 Supported Cisco IP Phones	Supported
Hybrid Services and Expressway/VCS Rebranding	Supported
Hosting on VMWare vSphere® 6.0	Supported
Keyword Filter for Syslog Output	Supported

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