Cisco TelePresence Video Communication Server

Administrator Guide

Last Updated: April 2020

X12.5.6

Preface

Change History

Table 1 Administrator Guide Change History

Date	Change	Reason
April 2020	Reinstate section "License Usage within a Cluster".	Document correction
January 2020	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
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). Fix incorrect naming of "Certification logging mode" option in the *Maintenance* section.	X12.5.2 maintenance release Document correction
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
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	X8.11.3 maintenance release (withdrawn)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 and X8.11.1 release.	X8.11.1 release (withdrawn)
July 2018	Updates for X8.11.	X8.11 release (withdrawn)

Table 1 Administrator Guide Change History (continued)

Date	Change	Reason
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

Contents

Preface 2
Change History 2
Contents 4
Introduction 9
About the Cisco TelePresence Video Communication Server 9
About This Guide 13
About the Service Setup Wizard 20
Network and System Settings 22
Network Settings 22
Intrusion Protection 28
Network Services 34
Configuring External Manager Settings 43
Configuring TMS Provisioning Extension Services 44
Firewall Traversal 47
About Firewall Traversal 47
Firewall Traversal Configuration Overview 49
Configuring a Traversal Client and Server 50
Configuring Ports for Firewall Traversal 52
Firewall Traversal and Authentication 54
Configuring VCS Expressway and Traversal Endpoint Communications 54
About ICE and TURN Services 55
Configuring TURN Services 56
Unified Communications 59
Unified Communications Prerequisites 59
Mobile and Remote Access Overview 69
XMPP Federation through VCS 72
Delayed Cisco XCP Router Restart 75
Jabber Guest Services Overview 76
Meeting Server Web Proxy on VCS 77
Protocols 79
About H.323 79
Configuring H.323 80
About SIP 81
Configuring SIP 84

Configuring Domains 88
Configuring SIP and H.323 Interworking 89
Registration Control 91
About Registrations 91
About Allow and Deny Lists 94
Configuring Registration Policy to Use an External Service 96
Device Authentication 99
About Device Authentication 99
Authenticating with External Systems 125
Zones and Neighbors 127
Video Network Fundamentals 127
Structuring the Dial Plan 128
About Zones 130
Configuring ICE Messaging Support 130
About the Local Zone and Subzones 132
Configuring the Default Zone 133
Configuring Default Zone Access Rules 134
Configuring Zones (Non-Default Zones) 135
Clustering and Peers 157
About Clusters 157
License Usage Within a Cluster 159
Managing Clusters and Peers 160
Troubleshooting Cluster Replication Problems 167
Dial Plan and Call Processing 169
Call Routing Process 169
Configuring Hop Counts 172
Configuring Dial Plan Settings 172
About Transforms and Search Rules 173
Example Searches and Transforms 180
Configuring Search Rules to Use an External Service 189
About Call Policy 191
Supported Address Formats 196
Dialing by IP Address 197
About URI Dialing 198
About ENUM Dialing 205
Configuring DNS Servers for ENUM and URI Dialing 210

Configuring Call Routing and Signaling 210
Identifying Calls 211
Disconnecting Calls 212
Bandwidth Control 215
About Bandwidth Control 215
Configuring Bandwidth Controls 216
About Subzones 217
Links and Pipes 223
Bandwidth Control Examples 226
Applications 229
Configuring Conference Factory 230
Presence 232
B2BUA (Back-to-Back User Agent) Overview 236
FindMe™ 246
Cisco TMS Provisioning (Including FindMe) 250
Hybrid Services and Connector Management 253
User Accounts 257
About User Accounts 257
Configuring Password Security 259
Configuring Administrator Accounts 260
Configuring Remote Account Authentication Using LDAP 262
Configuring FindMe Accounts 268
Resetting Forgotten Passwords 271
Using the Root Account 272
Managing SSO tokens 273
Maintenance 275
Enabling SSH access 275
Enabling Maintenance Mode 276
Upgrading Software Components 276
Upgrading Firmware (Physical Appliances Only) 279
Configuring Logging 279
Managing Option Keys 284
About Security 286
Managing Domain Certificates and Sever Name Indication for Multitenancy 301
Domain Certificates and Clustered Systems 304
Advanced Security 305

Configuring Language Settings 309
Backing Up and Restoring VCS Data 310
Diagnostics Tools 313
Incident Reporting 316
Checking the Effect of a Pattern 318
Locating an Alias 319
Serviceability 319
Port Usage 320
Network Utilities 321
Restarting, Rebooting and Shutting Down 326
Developer Resources 327
Overview and Status Information 329
Status Overview 329
System Information 330
Ethernet Status 331
IP Status 332
Resource Usage 332
Registration Status 333
Call Status 334
B2BUA Calls 336
Search History 337
Search Details 337
Local Zone Status 338
Zone Status 338
Bandwidth 339
Policy Server Status and Resiliency 340
TURN Relay Usage 340
Unified Communications Status 341
Presence 342
Microsoft interoperability 343
TMS Provisioning Extension Service Status 344
Starter Pack Provisioning Server Status 347
Managing Alarms 348
Logs 349
Hardware Status 352
Reference Material 353
About Event Log Levels 354

CPL Reference 364
LDAP Server Configuration for Device Authentication 374
DNS Configuration Examples 379
Changing the Default SSH Key 380
Restoring the Default Configuration (Factory Reset) 380
Password Encryption 383
Pattern Matching Variables 384
Port Reference 385
Regular expressions 386
Supported Characters 388
Call Types and Licensing 389
Product Identifiers and Corresponding Keys 390
Allow List Rules File Reference 392
Allow List Tests File Reference 393
VCS Multitenancy Overview 394
Multitenant VCS Sizing 395
Alarms 397
Command Reference – xConfiguration 434
Command Reference – xCommand 511
Command Reference – xStatus 549
External Policy Overview 551
Flash Status Word Reference Table 554
Supported RFCs 555
Software Version History 557
Legal Notices 562
Cisco Legal Information 564
Cisco Trademark 564

Introduction

About the Cisco TelePresence Video Communication Server 9
About This Guide 13
About the Service Setup Wizard 20

About the Cisco TelePresence Video Communication Server

IMPORTANT! New features in software version X12.5 and later are not supported for the Cisco TelePresence Video Communication Server product (VCS). They apply only to the Cisco Expressway Series product (Expressway). This software version is provided for the VCS for maintenance and bug fixing purposes only.

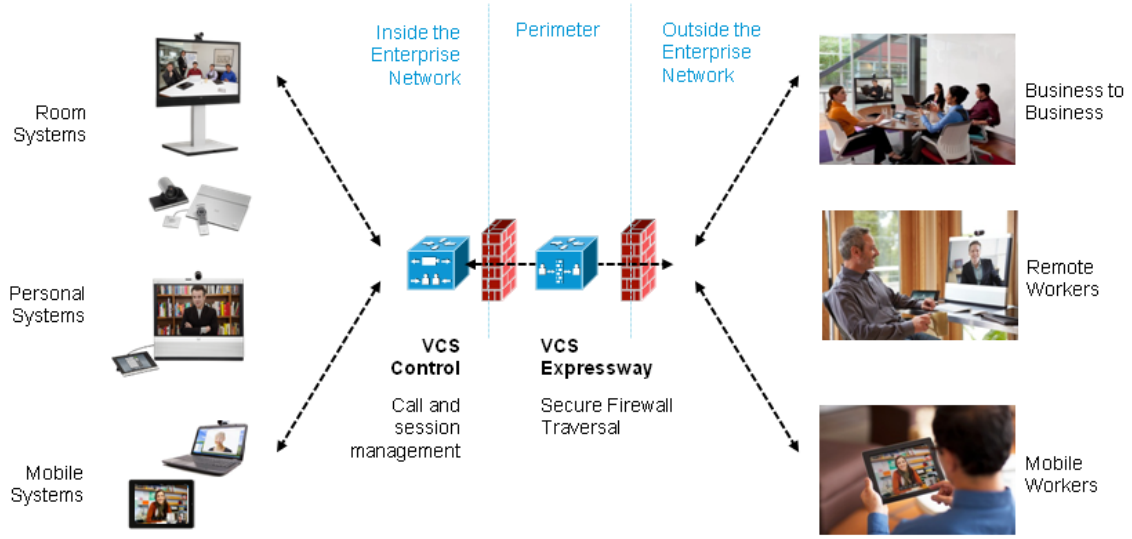
The Cisco TelePresence Video Communication Server (VCS) software simplifies session management and control of telepresence conferences. It provides flexible and extensible conferencing applications, enabling organizations to benefit from increased employee productivity and enhanced communication with partners and customers.

The VCS delivers exceptional scalability and resiliency, secure communications, and simplified large-scale provisioning and network administration in conjunction with Cisco TelePresence Management Suite (Cisco TMS).

The VCS interworks transparently with Cisco Unified Communications Manager (Unified CM), bringing rich telepresence services to organizations with Unified CM. It also offers interoperability with third-party unified communications, IP telephony networks, and voice-over-IP (VoIP) systems.

The VCS 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.

You can deploy the VCS as the VCS Control for use within an enterprise and as the VCS Expressway for business-to-business and remote and mobile worker external communication. An alternative solution, suited to small to medium-sized businesses (SMBs), is the VCS Starter Pack Express.



The VCS is available on a dedicated appliance (CE1100) and also runs on VMware on a range of Cisco UCS servers.

VCS Types

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

VCS Control

VCS Control 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. VCS Control 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.

VCS Expressway

The VCS Expressway deployed with the VCS Control 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 VCS Expressway 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 VCS 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. The maximum registrations listed here are global system capacities; the **capacity for individual deployments depends on the product licensing**:
  - Small systems support up to 2000 registrations on a standard M5-based small system, or 2500 registrations on a standard M4-based small system.
  - Medium systems support up to 2500 registrations.
  - Large systems support up to 5000 registrations. For Mobile and Remote Access registrations the limit is 2500.
- SIP Proxy

  Note: The SIP and H.323 protocols are disabled by default on new installs of X8.9.2 or later versions. Use the **Configuration > Protocols** page to enable them.
- SIP Registrar
- SIP Presence Server
- SIP Presence User Agent
- 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
- Up to 500 non-traversal calls
- Up to 75 traversal calls on an M5-based small system. Up to 100 traversal calls on a standard M4-based small system or medium system. Up to 500 traversal calls on a large system
- 1000 external zones with up to 2000 matches
- 1000 subzones and supporting up to 3000 membership rules
- Flexible zone configuration with prefix, suffix and regex support
- Can function as a standalone VCS, or be neighbored with other systems such as other VCSs, gatekeepers and SIP proxies
- Can be clustered with up to 6 VCSs to provide n+1 redundancy, and up to 4 x individual capacity.
- Intelligent Route Director for single number dialing and network failover facilities
- Optional endpoint authentication
- Control over which endpoints are allowed to register
- Call Policy (also known as Administrator Policy) including support for CPL
- Support for external policy servers
- Can be managed with Cisco TelePresence Management Suite (Cisco TMS) 13.2 or later
- AD authentication for administrators of the VCS
- Pre-configured defaults for:
  - Cisco Unified Communications Manager neighbor zones
  - Cisco TelePresence Advanced Media Gateway

    The Cisco Advanced Media Gateway (AM Gateway) is supported only with Expressway X8.x software versions; support for the AM Gateway is deprecated from Expressway version X12.5.
  - Nortel Communication Server neighbor zones
- Embedded setup wizard using a serial port for initial configuration
- System administration using a web interface or SSH, or via the CIMC port for a CE*nnnn* physical appliance
- Intrusion protection

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

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

Hardware Appliance and Virtual Machine Options

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

Virtual Machine Options

The VCS 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)

Hardware CE Series Appliances

The VCS is also available as a dedicated CE Series appliance based on UCS hardware. For example, the CE1100 appliance based on a UCS C220 M4L, operates as a medium capacity or large capacity VCS.

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

Changing the default system size

For CE1100 appliances deployed as VCS Expressway and running version X8.11.4 or later, 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 Video Communication Server CE1100 Appliance Installation Guide* on the VCS installation guides page.

Legacy Appliance

The VCS was also previously available on a legacy hardware appliance, now known as VCS appliance (1st generation). These have an LCD panel, keypad, and a black faceplate, and their serial numbers start with 52A.

1st generation appliances have the equivalent capabilities of a standard Medium VM or CE500 appliance.

Installation and initial configuration instructions for the VCS legacy appliance are contained in *VCS Getting Started Guide*.

Software Versions Supported by Hardware Platforms

Table 2 VCS Software Versions Supported by Platform

Platform name	Serial Numbers	Scope of software version support
VCS appliance (1st generation)	52A0#####	All features in versions up to and including X8.6.1. Critical fixes only in X8.7.x No support for X8.8 or later versions on this hardware.
VCS appliance (1st generation)	52A1####-52A4#####	All features in versions up to and including X8.6.1. Critical fixes only in later versions, up to and including X8.8.3*. No support for any versions after X8.8.3 on this hardware.

Table 2 VCS Software Versions Supported by Platform (continued)

Platform name	Serial Numbers	Scope of software version support
Small VM (OVA)	(Auto-generated)	X8.1 onwards. For VCS, support for versions after X8.11.x is for maintenance and bug fixing purposes only. New features are not supported.
Medium VM (OVA)	(Auto-generated)	X8.1 onwards. For VCS, support for versions after X8.11.x is for maintenance and bug fixing purposes only. New features are not supported.
Large VM (OVA)	(Auto-generated)	X8.1 onwards. For VCS, support for versions after X8.11.x is for maintenance and bug fixing purposes only. New features are not supported.
CE1100‡ (VCS pre-installed on UCS C220 M4L)	52D######	X8.6.1 onwards. For VCS, support for versions after X8.11.x is for maintenance and bug fixing purposes only. New features are not supported.
CE1000 (VCS pre-installed on UCS C220 M3L)	52B######	X8.1.1 to X8.10.x No support for any versions after X8.10.x on this hardware.
CE500 (VCS pre-installed on UCS C220 M3L)	52C######	X8.1.1 to X8.10.x No support for any versions after X8.10.x on this hardware.

‡ As of 13th November 2018, you cannot order the CE1100 appliance from Cisco. See the End-of-sale announcement for other important dates in the lifecycle of this platform.

About This Guide

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

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

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

Where CLI commands are included, they are shown in the format:

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

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 TelePresence Video Communication Server is available here:

www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html#telepresence

You can find more information about accessibility here:

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

Using the Web Interface

System configuration is normally carried out through the web interface.

To use the web interface:

1. Open a browser window and in the address bar type either:
   - the IP address of the system
   - the FQDN of the system
2. Click **Administrator Login**.

   (This step only applies if you are using "standalone FindMe" i.e. FindMe without Cisco TMSPE.)
3. Enter a valid administrator **Username** and **Password** and click **Login** (see the user accounts section for details on setting up administrator accounts). You are presented with the **Overview** page.

Note that when logging in using the VCS web interface, you may receive a warning message regarding the VCS's security certificate. You can ignore this until you are ready to secure the system.

A command line interface is also available.

Field Markers

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

Supported Browsers

The VCS 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 VCS web interface.

HTTP Methods

The VCS 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 VCS web interface.
POST	Yes	Yes	Apply data to a web resource. For example, when an administrator saves changes to a setting using the VCS web interface.
OPTIONS	No	Yes	For a specified URL, returns the HTTP methods supported by the server. For example, the VCS 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 VCS 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 VCS is running in advanced account security mode, then API access is automatically disabled for all users.
- API access for individual administrators can be disabled through their user configuration options.

Using the Command Line Interface (CLI)

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

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

To use the CLI:

1. Start an SSH session.
2. Enter the IP address or FQDN of the VCS.
3. Log in with your administrator username and password.

   See Enabling SSH access, page 275 if you prefer to use your private key to authenticate.
4. You can now start using the CLI by typing the appropriate commands.

Command Types

Commands are divided into the following groups:

- **`xStatus`**: these commands return information about the current status of the system. Information such as current calls and registrations is available through this command group. See Command Reference – xStatus, page 549 for a full list of **`xStatus`** commands.
- **`xConfiguration`**: these commands allow you to add and edit single items of data such as IP address and zones. See Command Reference – xConfiguration, page 434 for a full list of **`xConfiguration`** commands.
- **`xCommand`**: these commands allow you to add and configure items and obtain information. See Command Reference – xCommand, page 511 for a full list of **`xCommand`** commands.
- **`xHistory`**: these commands provide historical information about calls and registrations.
- **`xFeedback`**: these commands provide information about events as they happen, such as calls and registrations.

Note that:

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

Web Page Features and Layout

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

Figure 1 Example list page

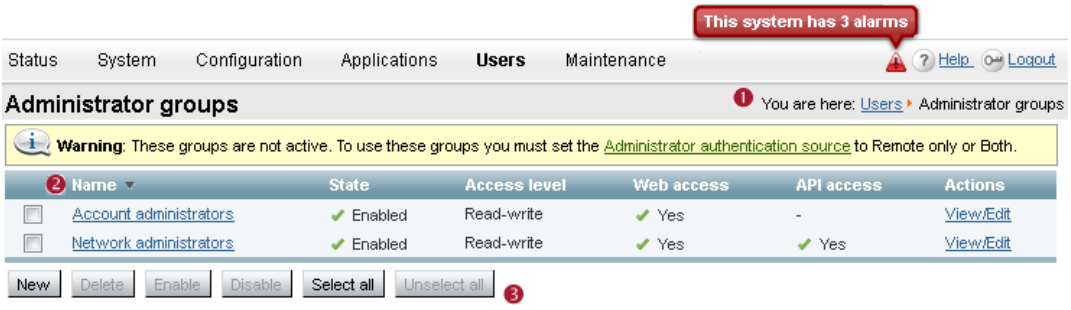
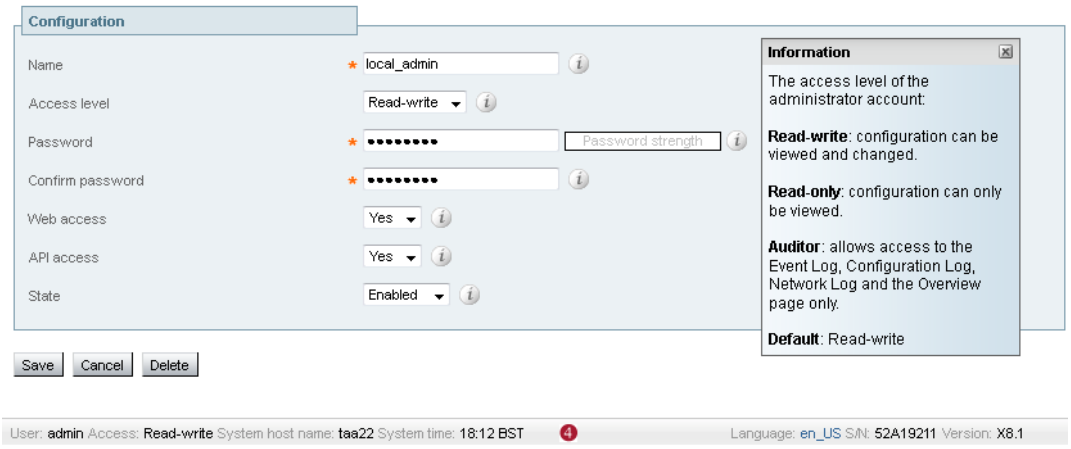


Figure 2 Example configuration page



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

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

Page element		Description
Field level information		An information box appears on the configuration pages whenever you either click on the Information icon or click inside a field. This box gives you information about the particular field, including where applicable the valid ranges and default value. To close the information box, click on the X at its top right corner.
Information bar		The VCS 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.
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 a VCS 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 VCS software version are shown at the bottom of the page.

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

Related Documentation

Table 3 Links to Related Documents and Videos

Support videos	Videos provided by Cisco TAC engineers about certain common VCS configuration procedures are available on the Expressway/VCS Screencast Video List page
Installation - virtual machines	*Cisco Expressway Virtual Machine Installation Guide* on the Expressway installation guides page
Installation - physical appliances	*Cisco Video Communication Server CE1100 Appliance Installation Guide* on the VCS installation guides page
Basic configuration for registrar / single systems	*Cisco Expressway Registrar Deployment Guide* on the Expressway configuration guides page
Basic configuration for firewall traversal / paired systems	*Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide* on the Expressway configuration guides page
Administration and maintenance	*Cisco TelePresence VCS Administrator Guide* on the VCS maintain and operate guides page *Cisco TelePresence VCS Serviceability Guide* on the VCS maintain and operate guides page

Table 3 Links to Related Documents and Videos (continued)

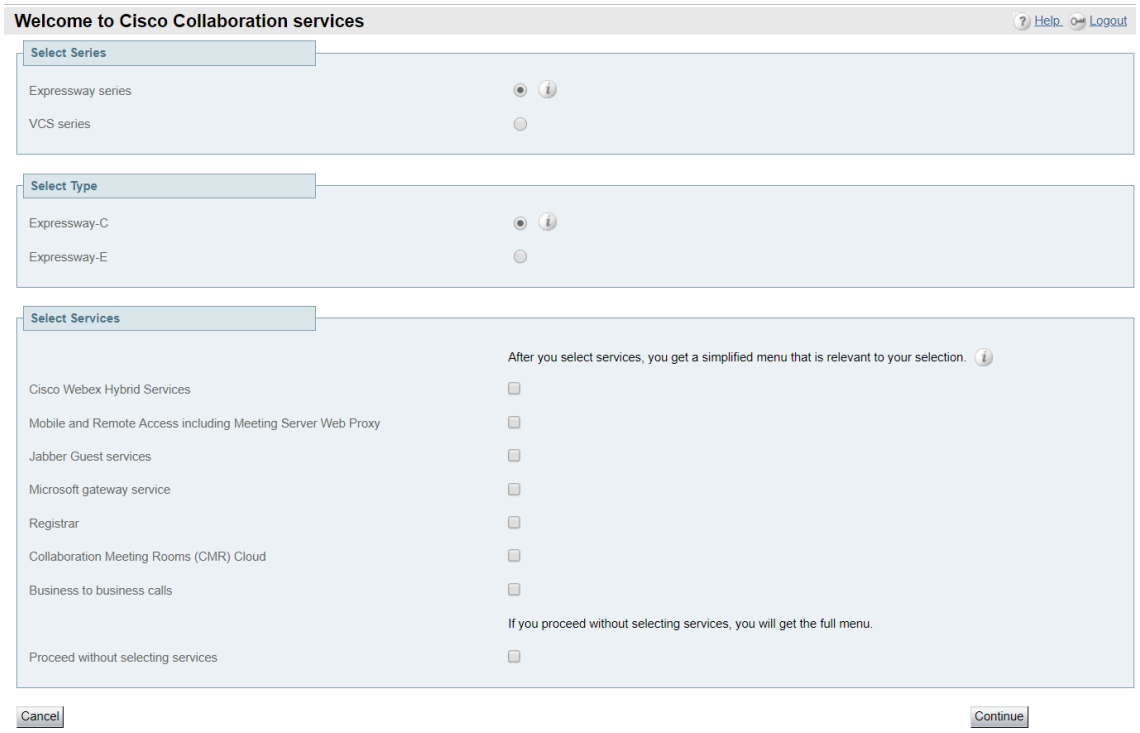
Clustering	*Cisco Expressway Cluster Creation and Maintenance Deployment Guide* on the Expressway configuration guides page
Certificates	*Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page
Ports	*Cisco Expressway IP Port Usage Configuration Guide* 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

The Service Setup Wizard makes it easier to configure and license the Expressway or VCS system for its chosen purpose in your environment. It also simplifies the user interface.

For details about using the Services Setup Wizard, see *Cisco Expressway-E and Expressway-C - Basic Configuration guide* on the Expressway configuration guides page. The guide describes how to access and navigate the wizard and apply option keys for licenses, and settings specific to CE physical appliances.

Figure 3 Service Setup Wizard - Selection Page



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 Guest Services	Microsoft gateway service	Registrar	CMR Cloud	Business to Business calling (incl. 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 Cisco Webex Hybrid Call Service)	Y	Y*	Y	N	Y	Y	Y

Key to Table

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

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

Rules

- Hybrid Services connectors may co-reside with the VCS Control 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 VCS Control. This is because we do not support the connectors being hosted on the VCS Control 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 VCS traversal pair, the VCS Expressway and VCS Control must both be in dual stack mode.

Network and System Settings

This section describes network services and settings related options that appear under the **System** menu of the web interface. These options enable you to configure the VCS 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 VCS (for example DNS, NTP and SNMP).

Network Settings 22

Intrusion Protection 28

Network Services 34

Configuring External Manager Settings 43

Configuring TMS Provisioning Extension Services 44

Network Settings

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 VCS and the Ethernet networks to which it is connected. As the VCS only supports auto-negotiation, the **Speed** is always *Auto*. The VCS 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 VCS.

IP Protocol Configuration

You can configure whether the VCS 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 VCS 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 VCS. Which protocol it uses is determined by the format used to specify the IP address of the VCS on the endpoint. After the endpoint has registered using either IPv4 or IPv6, the VCS 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 VCS.

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

IPv4 to IPv6 Interworking

The VCS 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 VCS is acting as an IPv4 to IPv6 gateway are traversal calls and require a traversal call license.

IP Gateways

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

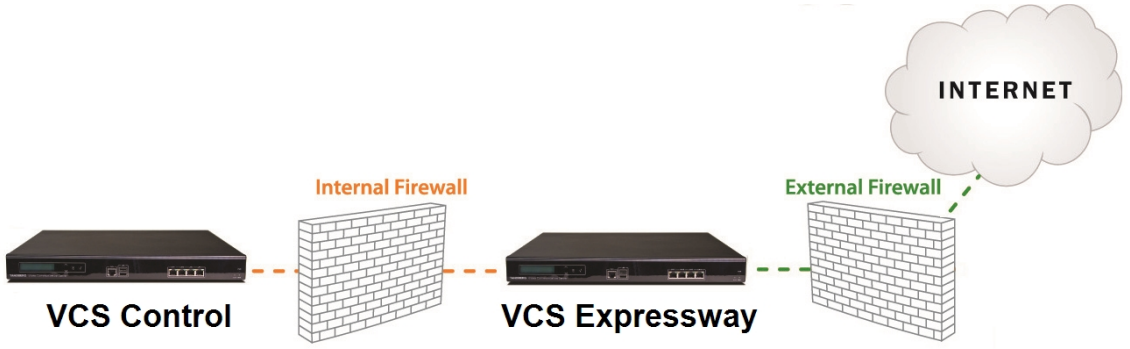
LAN Configuration

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

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

About Advanced Networking

The Advanced Networking feature enables the LAN 2 Ethernet port on the VCS Expressway, to allow a secondary IP address for the VCS. It also includes support for deployments where the VCS Expressway 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 intended for deployments where the VCS Expressway 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 VCS Expressway.

To enable the use of dual network interfaces:

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

Notes:

- Configure the LAN 1 port and restart the VCS before you configure the LAN 2 port.
- The LAN 1 and LAN 2 interfaces must be on different, non-overlapping subnets.
- If you have Advanced Networking enabled but only want to configure one of the Ethernet ports, switch **Use dual network interfaces** to *No*.
- If the VCS Expressway is in the DMZ, the outside IP address of the VCS Expressway must be a public IP address, or if static NAT mode is enabled, the static NAT address must be publicly accessible.
- The VCS Expressway may also be used to traverse internal firewalls within an enterprise. In this case the "public" IP address may not be publicly accessible, but is an IP address accessible to other parts of the enterprise.
- If you need to change the IP addresses on one or both interfaces, you can do it via the UI or the CLI. You can change both at the same time if required, and the new addresses take effect after a restart.

Configuring Static NAT

You can deploy the VCS Expressway 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 VCS Expressway 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 VCS Expressway.

To enable the use of a static NAT:

1. For the externally-facing LAN port:
   a. In the **IPv4 address** field, enter the port's private IP address.
   b. Set **IPv4 static NAT mode** to *On*.
   c. In the **IPv4 static NAT address** field, enter the port's public IP address - this is the IP address as it appears after translation (outside the NAT element).

IPv6 Mode Features and Limitations

When you set the IP interfaces of the VCS 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).

We test and support VCS in IPv6 mode when it is operating as the call control agent of an IPv6 only, on-premises, video conferencing deployment.

Explicit IPv6 Supported Features

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

Supported RFCs

- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification (partially implemented: static global addresses only).
- RFC 2464: Transmission of IPv6 Packets over Ethernet Networks.
- RFC 3596: DNS Extensions to Support IP Version 6.
- 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 VCS when you change its IP address or its gateway's IP address.
- Mobile and Remote Access (MRA) is not tested or supported in IPv6 mode. For MRA, the primary call control agent is Unified CM which does not support IPv6.
- Getting revocation status from distributed Certificate Revocation Lists is not supported in IPv6 mode.

Configuring DNS Settings

The **DNS** page (**System > DNS**) is used to configure DNS servers and DNS settings on the VCS.

Configuring the System Host Name and Domain Name

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

- It must be unique for each peer in a cluster.
- It is used to identify the VCS 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 VCS 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 VCS 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 VCS in SIP messaging, where an endpoint has configured the VCS as its SIP proxy in the form of an FQDN (as opposed to an IP address, which is

not recommended).

In this case the VCS 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 VCS. (Note that this check occurs because the SIP proxy FQDN is included in the route header of the SIP request sent by the endpoint to the VCS.)

Custom domain searches

The **Search domains** setting is relevant for Edge deployments where the external hosts are in a different DNS domain from VCS Control, and are configured with non-qualified hostnames. You can optionally use this setting to specify one or more DNS domains. The VCS 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 that setting a small source port range will increase your vulnerability to DNS spoofing attacks.

Configuring DNS Server Addresses

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

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

Default DNS servers

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

The order that the servers are specified is not significant. The VCS 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 VCS 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 VCS cannot process the UDP response. This is not usually a problem, because the VCS 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 VCS 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 VCS 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 VCS.
- Traffic type "Video" is assigned by default if the media type cannot be identified. (For example, if different media types are multiplexed on the same port.)

Existing QoS/DSCP Commands and API are Discontinued

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

What if I currently use these commands?

When you upgrade the VCS, 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 VCS 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 VCS in a DMZ. They may also be required in other complex network deployments.

To add a static route:

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

   For example, enter `203.0.113.0` or `2001:db8::`
2. Enter the prefix length that defines the range

   Extending the example, you could enter `24` to define the IPv4 range 203.0.113.0 – 203.0.113.255, or `32` to define the IPv6 range 2001:db8:: to 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff.

   The address range field shows the range calculated by the VCS from the IP address and Prefix length.
3. Enter the IP address of the gateway for your new route
4. Select an ethernet interface for your new route

   This option is only available if the second ethernet interface is enabled. Select *LAN 1* or *LAN 2* to force the route via that interface, or select *Auto* to allow the VCS to make this route on either interface.
5. Click **Create route**

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

Notes

- IP routes can also be configured using the CLI, using xCommand RouteAdd and the xConfiguration IP Route commands.
- You can configure routes for up to 50 network and host combinations.
- Do not configure IP routes by logging in as `root` and using `ip route` statements.

Intrusion Protection

Configuring Firewall Rules

Firewall rules provide the ability to configure IP table rules to control access to the VCS at the IP level. On the VCS, 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 VCS. There is a final rule in this group that allows all traffic destined for the VCS 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 VCS is allowed access, but that traffic will be dropped if the VCS is not explicitly listening for it. You have to actively configure extra rules to lock down the system to your specifications.

Note that return traffic from outbound connections is always accepted.

User-configured rules

The user-configured rules are typically used to restrict what can access the VCS. 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 that the built-in rules are not shown in this list.

You can change the set of firewall rules by adding new rules, or by modifying or deleting existing ones. Changes to the current active rules are held in a pending state. When you finish making changes, you activate the new rules to replace the previous set. For UDP-related rules, note that new rules only take effect at the next system reboot (although if you delete UDP rules, they become inactive as soon as you activate the rule set).

To configure and activate rules:

1. Go to **System > Protection > Firewall rules > Configuration**.
2. Make your changes by adding, modifying, or deleting rules as required.

   To change the order of the rules, use the up/down arrows and to swap the priorities of adjacent rules.

   - New or modified rules are shown as **Pending** (in the **State** column).
   - Deleted rules are shown as **Pending delete**.
3. When you finish configuring the new set of firewall rules, click **Activate firewall rules**.
4. Confirm that you want to activate the new rules. This will replace the existing set of active rules with the set you have just configured.
   After confirming that you want to activate the new rules, they are validated and any errors reported.

5. If there are no errors, the new rules are temporarily activated and you are taken to the **Firewall rules confirmation** page.
   You now have 15 seconds to confirm that you want to keep the new rules:
   - Click **Accept changes** to permanently apply the rules.
   - If the 15 seconds time limit expires or you click **Rollback changes**, the previous rules are reinstated and you are taken back to the configuration page.

     The automatic rollback mechanism provided by the 15 seconds time limit ensures that the client system that activated the changes is still able to access the system after the new rules have been applied. If the client system is unable to confirm the changes (because it can no longer access the web interface) then the rollback will ensure that its ability to access the system is reinstated.
6. This step only applies if you add UDP rules. That is, one or more custom rules with **Transport**=*UDP*. New UDP rules do not take effect until the next system reboot. In this special case, activating the firewall rules is not sufficient by itself. Deleted UDP rules do not have this requirement, and become inactive as soon as you activate the rule set.

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

Rule settings

The configurable options for each rule are:

Field	Description	Usage tips
Priority	The order in which the firewall rules are applied.	The rules with the highest priority (1, then 2, then 3 and so on) are applied first. Firewall rules must have unique priorities. Rule activation will fail if there are multiple rules with the same priority.
Interface	The LAN interface on which you want to control access.	This only applies if the **Advanced Networking** option key is installed.
IP address and **Prefix length**	These two fields together determine the range of IP addresses to which the rule applies.	The **Address range** field shows the range of IP addresses to which the rule applies, based on the combination of the **IP address** and **Prefix length**. The prefix length range is 0-32 for an IPv4 address, and 0-128 for an IPv6 address.
Service	Choose the service to which the rule applies, or choose *Custom* to specify your own transport type and port ranges.	Note that if the destination port of a service is subsequently reconfigured on the VCS, 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 VCS from dictionary-based attempts to breach login security.

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

You can configure ranges of addresses that are exempted from one or more categories (see Configuring Exemptions, page 33 below).

You should use automated protection in combination with firewall rules; automated protection to dynamically detect and temporarily block specific threats, and firewall rules to permanently block a range of known host addresses.

About protection categories

The set of available protection categories on your VCS 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 onwards, automated intrusion protection is enabled, by default, for the following categories:

- http-ce-auth
- http-ce-intrusion
- sshpfwd-auth
- sshpfwd-intrusion
- xmpp-intrusion

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

To enable intrusion protection on your VCS:

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

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

Configuring Protection Categories

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

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

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

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

Enabling and disabling categories

To enable or disable one or more protection categories:

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

Configuring a category's blocking rules

To configure a category's specific blocking rules:

1. Go to **System > Protection > Automated detection > Configuration**.
2. Click on the name of the category you want to configure.

   You are taken to the configuration page for that category.

3. Configure the category as required:
   - **State**: whether protection for that category is enabled or disabled.
   - **Description**: a free-form description of the category.
   - **Trigger level** and **Detection window**: these settings combine to define the blocking threshold for the category. They specify the number of failed access attempts that must occur before the block is triggered, and the time window in which those failures must occur.
   - **Block duration**: the period of time for which the block will remain in place.
4. Click **Save**.

Configuring Exemptions

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

To configure exempted addresses:

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

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

Managing Blocked Addresses

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

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

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

Investigating Access Failures and Intrusions

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

1. Go to **System > Protection > Automated detection > Configuration**.
2. Click on the name of the category you want to investigate.
3. Click **View all matching intrusion protection triggers for this category**.

   The system will display all the relevant events for that category. You can then search through the list of triggering events for the relevant event details such as a user name, address or alias.

Automated Protection Service and Clustered Systems

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

- Each peer maintains its own count of connection failures and the trigger threshold must be reached on each peer for the intruder's address to be blocked by that peer.

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

Automated Protection in MRA Deployments

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

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

Additional Information

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

Network Services

Configuring System Name and Access Settings

The **System administration** page (**System > Administration**) is used to configure the following:

- Name of the Cisco TelePresence Video Communication Server system.
- Methods by which the system may be accessed by administrators. Although you can administer the Cisco TelePresence Video Communication Server 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.

The configurable options are described in the table:

Table 5 Settings for the System Administration Page

Field	Description	Usage tips
System name	Used to identify the VCS. 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). Also used by Cisco TMS.	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 VCS 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 VCS can be accessed via SSH and SCP. Default is *On*.	
Web interface (over HTTPS)	Whether the VCS can be accessed via the web interface. Default is *On*.	Cisco TMS accesses the VCS via the web server. If HTTPS mode is turned off, Cisco TMS will not be able to access it.
Provisioning services	Whether the **System > TMS Provisioning Extension services** page is accessible in the VCS 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*.	
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 VCS.	This includes web, SSH and serial sessions. Session limits are not enforced on FindMe accounts or the root account. A value of 0 turns session limits off.

Table 5 Settings for the System Administration Page (continued)

Field	Description	Usage tips
System session limit	The maximum number of concurrent administrator sessions allowed on each VCS.	This includes web, SSH and serial sessions. Session limits are not enforced on FindMe accounts or the root account; however active root account sessions do count towards the total number of current administrator sessions. A value of 0 turns session limits off.
System protection		
Automated protection service	Whether the automated protection service is active. Default is *On*.	After enabling the service you must go and configure the specific protection categories.
Automatic discovery protection	Controls how management systems such as Cisco TMS can discover this VCS. *Off*: automatic discovery is allowed. *On*: Cisco TMS has to be manually configured to discover this VCS and must provide administrator account credentials. Default is *Off*.	You must restart the system for any changes to take effect.
Web server configuration		
Redirect HTTP requests to HTTPS	Determines whether HTTP requests are redirected to the HTTPS port. Default is *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, the VCS redirects your 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.

Table 5 Settings for the System Administration Page (continued)

Field	Description	Usage tips
Web administrator port	Sets the https listening port for administrators to access the VCS web interface. We strongly recommend using a non-default port for web administration on the VCS Expressway if you enable any features that need TCP 443, eg. Meeting Server Web Proxy. Restart the VCS 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 VCS denies access. Web access to the VCS 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.
Client certificate-based security	Controls the level of security required to allow client systems (typically web browsers) to communicate with the VCS 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 that a 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*	**Important**: Enabling *Certificate validation* means that your browser (the client system) can use the VCS 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 VCS'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 287 page, and test client certificates on the Testing Client Certificates, page 297 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 VCS extracts credentials from the browser certificate on the Certificate-based authentication configuration page. This setting does not affect client verification of the VCS's server certificate.

Table 5 Settings for the System Administration Page (continued)

Field	Description	Usage tips
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		

Table 5 Settings for the System Administration Page (continued)

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, VCS **automatically converts the appliance to a Large system**. As a result, VCS Expressway listens for multiplexed RTP/RTCP traffic on default demultiplexing ports for Large systems (36000 to 36011). In this case, VCS 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 CE1100 appliances that are deployed as VCS Expressways, and with the following specification or higher: ■ VCS version X8.11.3 or later ■ 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 VCS in a physically secure environment.

HTTP Strict Transport Security (HSTS)

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

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

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

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

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

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

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

Configuring SNMP Settings

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

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

The VCS supports the most basic MIB-II tree (.1.3.6.1.2.1) as defined in *RFC 1213*.

The information made available by the VCS includes:

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

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

Field	Description	Usage tips
SNMP mode	Controls the level of SNMP support. *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 VCS's SNMP community name. The default is *public*.	Only applies when using *v2c* or *v3 plus TMS support*.
System contact	The name of the person who can be contacted regarding issues with the VCS. 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 VCS.	
Username	The VCS'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*
v3 Authentication settings (only applicable to SNMPv3)		

Field	Description	Usage tips
Authentication mode	Enables or disables SNMPv3 authentication.	
Type	The algorithm used to hash authentication credentials. *SHA*: Secure Hash Algorithm. *MD5*: Message-Digest algorithm 5. The default is *SHA*.	
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.	
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 VCS 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 VCS 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 VCS's NTP servers and to specify the local time zone.

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

Accurate time is necessary for correct system operation.

Configuring the NTP Servers

To configure the VCS 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 VCS 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.
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 VCS is shown in the **Status** area as follows:

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

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

Other status information available includes:

Field	Description
NTP server	The actual NTP server that has responded to the request. This may be different to the NTP server in the NTP server address field.
Condition	Gives a relative ranking of each NTP server. All servers that are providing accurate time are given a status of *Candidate*; of those, the server that the VCS 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, page 554 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*.
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 VCS 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 VCS's time.

Field	Description
Delay	The network delay between the NTP server and the VCS.
Stratum	The degree of separation between the VCS 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.

VCS Time Display and Time Zone

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

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

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

Specifying your local **Time zone** lets the VCS 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 for both users and administrators. The **Welcome message title** and **text** appears to administrators when they log in using the CLI, and to FindMe users and administrators when they log in using 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 VCS is using the TMS Provisioning Extension services to provide FindMe account data, then users log into their FindMe accounts through Cisco TMS, not through VCS.

Note that this feature is not configurable using the CLI.

Configuring External Manager Settings

The **External manager** page (**System > External manager**) is used to configure the VCS 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 VCS, for example call attempts, connections and disconnections, and as a place for where the VCS can send alarm information. The use of an external manager is optional.

Note: Cisco TMS identifies the VCS as a "TANDBERG VCS".

The VCS will continue to operate without loss of service if its connection to Cisco TMS fails. This applies even if the VCSs are clustered. No specific actions are required as the VCS 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 VCS with the IP address or host name and path of the external manager to be used.	If you are using Cisco TMS as your external manager, use the default path of **tms/public/external/management/SystemManagementService.asmx**.
Protocol	Determines whether communications with the external manager are over *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 VCS's trusted CA certificates. This is done from the Managing the Trusted CA Certificate List, page 287 page (**Maintenance > Security > Trusted CA certificate**).

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 VCS's Provisioning Server to service provisioning requests from endpoint devices. They also provide the VCS 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.

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 VCS 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 VCS **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 6 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 use for the connection to the Cisco TMSPE service. *Off*: no encryption is used. *TLS*: TLS encryption is used. Default is *TLS*.	A TLS connection is recommended.
Verify certificate	Controls whether the certificate presented by the Cisco TMSPE service is verified against the VCS'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 VCS's trusted CA certificates. Do this from the Managing the Trusted CA Certificate List, page 287 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 VCS. 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.
Base group	The ID used to identify this VCS (or VCS 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 VCS to authenticate itself with the Cisco TMSPE service.	If TLS encryption is not enabled, the authentication password is sent in the clear.

Table 6 Configurable Options for Provisioning Services (continued)

Field	Description	Usage tips
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 VCS 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 **details** to view full status information.)
Polling interval	The frequency with which the VCS 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 VCS 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 VCS while data is deleted and refreshed. If you only need to apply recent updates in Cisco TMS to the VCS, click **Check for updates** instead.

Firewall Traversal

This section describes how to configure your VCS Control and VCS Expressway in order to traverse firewalls.

About Firewall Traversal 47
Firewall Traversal Configuration Overview 49
Configuring a Traversal Client and Server 50
Configuring Ports for Firewall Traversal 52
Firewall Traversal and Authentication 54
Configuring VCS Expressway and Traversal Endpoint Communications 54
About ICE and TURN Services 55
Configuring TURN Services 56

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:

- A VCS Expressway located outside the firewall on the public network or in the DMZ, which acts as the firewall traversal server.
- A VCS Control 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

Recommendations and Prerequisites

We recommend that both the VCS Expressway and the VCS Control run the same software version.

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

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 VCS Expressway 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 VCS Expressway; the settings for these connections are configured in a different way). Likewise, each VCS client must have one traversal client zone configured on it for each server that it is connecting to.

The ports and protocols configured for each pair of client-server zones must be the same. See the Configuring a Traversal Client and Server, page 50 for a summary of the required configuration on each system. Because the VCS Expressway listens for connections from the client on a specific port, you are recommended to create the traversal server zone on the VCS Expressway before you create the traversal client zone on the VCS Control.

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

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 VCS to send messages to that endpoint. The VCS 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 VCS 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 VCS Expressway or they can just send calls to the VCS Expressway as the local "DMZ" firewall has relevant ports open to allow communication to the VCS Expressway over SIP and H.323 ports.

Endpoints can also use 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 VCS supports ICE for calls where the VCS 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 a VCS Expressway cluster.
- The VCS Expressway has its own built-in TURN server to support ICE-enabled endpoints.

H.323 Firewall Traversal Protocols

The VCS 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 VCS 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 VCS Expressway uses media demultiplexing in the following call scenarios:

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

The VCS Expressway 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 VCS Expressway 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 VCS Control at **Configuration > Local Zones > Traversal Subzone**. In Large VCS systems the first 12 ports in the range – 36000 to 36011 by default – are always reserved for multiplexed traffic. The VCS Expressway 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 VCS Expressway (**Configuration > Traversal > Ports**). If you choose not to configure a particular pair of ports (**Use configured demultiplexing ports** = *No*), then the VCS Expressway 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 a VCS Control/VCS Expressway pair, the only demultiplexing that would occur would be on the VCS Expressway ports facing the VCS Control:

Enterprise endpoint	⟷	**VCS Control**		⟷	**VCS Expressway**		⟷	**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 VCS Control/VCS Expressway would perform demultiplexing on both sides of the VCS Expressway:

Enterprise endpoint	⟷	**VCS Control**		⟷	**VCS Expressway**		⟷	**Home endpoint**
		Non-demuxed	**Non-demuxed**		**Demuxed**	**Demuxed**		
RTP ports		36002	36004		36000	36000		
RTCP ports		36003	36005		36001	36001		

If the VCS Expressway 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 VCS can act as a traversal server or as a traversal client.

VCS as a Firewall Traversal Client

The VCS 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 VCS 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 VCS client (**Configuration > Zones > Zones**) and configuring it with the details of the traversal server. See Configuring Traversal Client Zones, page 139 for more information. You can create more than one traversal client zone if you want to connect to multiple traversal servers.

Note that:

- In most cases, you will use a VCS Control as a firewall traversal client. However, a VCS Expressway can also act as a firewall traversal client.
- The firewall traversal server used by the VCS client must be a VCS Expressway.

VCS as a Firewall Traversal Server

The VCS Expressway has all the functionality of a VCS Control (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 VCS Expressway to act as a firewall traversal server for Cisco systems, you must create a traversal server zone on the VCS Expressway (**Configuration > Zones > Zones**) and configure it with the details of the traversal client. See Configuring Traversal Server Zones, page 142 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 VCS Expressway 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 VCS Expressway and Traversal Endpoint Communications, page 54 for more information.
- To enable TURN relay services and find out more about ICE, see About ICE and TURN Services, page 55.
- To reconfigure the default ports used by the VCS Expressway, see Configuring Ports for Firewall Traversal, page 52.

Firewall Traversal and Advanced Networking

The Advanced Networking option key enables the LAN 2 interface on the VCS Expressway (the option is not available on a VCS Control). The LAN 2 interface is used in situations where the VCS Expressway 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.

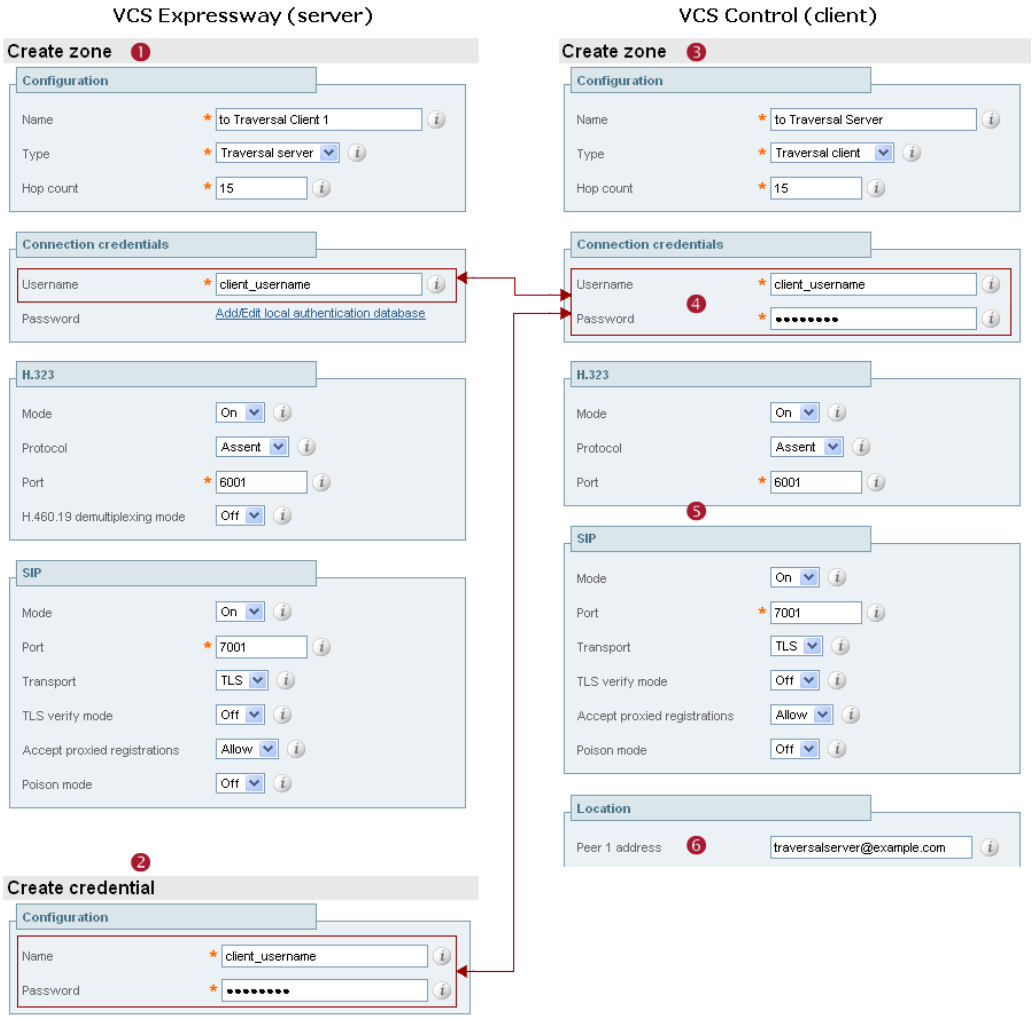
With the LAN 2 interface enabled, you can configure the VCS with two separate IP addresses, one for each network in the DMZ. Your VCS then acts as a proxy server between the two networks, allowing calls to pass between the internal and outer firewalls that make up your DMZ.

When Advanced Networking is enabled, all ports configured on the VCS, 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 VCS Expressway, create a traversal server zone (this represents the incoming connection from the VCS Control). In the **Username** field, enter the VCS Control's authentication username.
2	On the VCS Expressway, add the VCS Control's authentication username and password as credentials into the local authentication database.
3	On the VCS Control, create a traversal client zone (this represents the connection to the VCS Expressway).
4	Enter the same authentication **Username** and **Password** as specified on the VCS Expressway.
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 VCS Expressway.
6	Enter the VCS Expressway'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 VCS Expressway, traversal client and firewall in order for connections to be permitted.

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

The Port Usage, page 320 pages (under **Maintenance > Tools > Port usage**) list all the IP ports that are being used on the VCS, 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 VCS, 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 VCS Expressway.
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 VCS Expressway to keep the connection alive.
4. When the VCS Expressway 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 VCS Expressway.
- Allow return traffic from those ports on the VCS Expressway 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 VCS Expressway 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 type of appliance or VM:

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

Configuring Ports for Connections From Traversal Clients

Each traversal server zone specifies an H.323 port and a SIP port to use for the initial connection from the traversal client. Each time you configure a new traversal server zone on the VCS Expressway, 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 VCS Expressway, matching ports must be configured on the corresponding traversal client. Note that:

- The default port used for the initial connections from MXP endpoints is the same as that used for standard RAS messages, that is UDP/1719. While you can change this port on the VCS Expressway, 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 VCS Expressway'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 VCS Expressway 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 VCS Control and VCS Expressway.

Configuring TURN Ports

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

The ports used by these services are configurable via **Configuration > Traversal > TURN**.

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

Configuring Ports for Connections Out to the Public Internet

In situations where the VCS Expressway 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 VCS Expressway only after the server has located the endpoint on the public internet. This may cause problems if your VCS Expressway is located within a DMZ (where there is a firewall between the VCS Expressway 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 VCS Expressway 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 VCS Expressway allows only authenticated client systems to use it as a traversal server.

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

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

Traversal client	VCS Expressway traversal server
VCS Control (or VCS Expressway) The VCS 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 VCS client must be configured with the client's authentication **Username**. This is set on the VCS Expressway by using **Configuration > Zones > Zones > Edit zone**, in the **Connection credentials** section. There must also be an entry in the VCS Expressway'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 VCS Expressway's authentication database with the corresponding client username and password.

Note that all VCS traversal clients must authenticate with the VCS Expressway, even if the VCS Expressway is not using device authentication for endpoint clients.

Authentication and NTP

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

Configuring VCS Expressway and Traversal Endpoint Communications

Traversal-enabled H.323 endpoints can register directly with the VCS Expressway 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 VCS Expressway 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.

Field	Description
H.460.19 demux mode	Determines whether the VCS Expressway 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 VCS Expressway 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 VCS Expressway.
UDP probe retry count	The number of times locally registered endpoints attempt to send a UDP probe to the VCS Expressway.
UDP probe keep alive interval	The interval (in seconds) with which locally registered endpoints send a UDP probe to the VCS Expressway 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 VCS Expressway.
TCP probe retry count	The number of times locally registered endpoints attempt to send a TCP probe to the VCS Expressway.
TCP probe keep alive interval	The interval (in seconds) with which locally registered endpoints send a TCP probe to the VCS Expressway 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 VCS Expressway 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 VCS also takes the media and thus requires a traversal license.

For more information about ICE, see *RFC 5245*.

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.

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 that the signaling always goes via the VCS, regardless of the final media communication path chosen by the endpoints.

Capabilities and limitations

- Small or Medium 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 Large system supports up to 6000 relays, spread evenly across 6 ports where each port is limited to handling 1000 relays. This limit is not strictly enforced, so we recommend adding an SRV record for each port to enable round robin.
- On a Large system, if TCP 443 TURN service is enabled, the external port does not multiplex the TCP TURN requests due to a technical limitation. So in this case, only 1000 TCP TURN relays are supported.
- Clustered VCSs: 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 VCS'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 VCS's externally facing LAN interface.
- VCS Expressway's TURN server does not support Microsoft ICE (which is not standards-based). To enable communications between the VCS and Microsoft clients that are registered through a Microsoft Edge Server you need to use the Microsoft interoperability service.
- The TURN server does not support bandwidth requests. Traversal zone bandwidth limits do not apply.
- The VCS Expressway 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 VCS Expressway TURN server supports UDP relays over TCP. It does not currently support TCP relays.

Configuring TURN Services

TURN relay services are only available on the VCS Expressway. To use TURN services you need the TURN Relay option key. This TURN Relay option key controls the number of TURN relays that can be simultaneously allocated by the TURN server.

The **TURN** page (**Configuration > Traversal > TURN**) is used to configure the VCS Expressway's TURN settings. If you are configuring your VCS Expressway 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 VCS 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.
TURN requests port	The listening port for TURN requests. The default port is 3478.	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).
Delegated credential checking	Controls whether the credential checking of TURN server requests is delegated, via a traversal zone, to another VCS. 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 VCS performing the authentication challenge. *On*: delegate the credential checking to a traversal client. The default is *Off*.	See delegated credential checking for more information.

Field	Description	Usage tips
Authentication realm	The realm sent by the server in its authentication challenges. ▪ When **Delegated credential checking** is *Off*, this is a free-form text field. ▪ When **Delegated credential checking** is *On*, you choose from the set of configured SIP domains. The chosen domain also determines the traversal zone through which credential checking is delegated.	When **Delegated credential checking** is *Off*, ensure that the client's credentials are stored in the relevant device 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 VCS. You can also review further details of each TURN relay including permissions, channel bindings and counters.

Unified Communications

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

Unified Communications Prerequisites 59
Mobile and Remote Access Overview 69
XMPP Federation through VCS 72
Delayed Cisco XCP Router Restart 75
Jabber Guest Services Overview 76
Meeting Server Web Proxy on VCS 77

Unified Communications Prerequisites

Configuring a Secure Traversal Zone Connection for Unified Communications

Unified Communications features such as Mobile and Remote Access or Jabber Guest, require a Unified Communications traversal zone connection between the VCS Control and the VCS Expressway. This involves:

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

Note: Configure only one *Unified Communications traversal* zone per VCS traversal pair. That is, one *Unified Communications traversal* zone on the VCS Control cluster, and one corresponding *Unified Communications traversal* zone on the VCS Expressway cluster.

Installing VCS Security Certificates

You must set up trust between the VCS Control and the VCS Expressway:

1. Install a suitable server certificate on both the VCS Control and the VCS Expressway.
   - 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 VCS includes a built-in mechanism to generate a certificate signing request (CSR) and is the recommended method for generating a CSR:
     - Ensure that the CA that signs the request does not strip out the client authentication extension.
     - The generated CSR includes the client authentication request and any relevant subject alternate names for the Unified Communications features that have been enabled (see Server Certificate Requirements for Unified Communications, page 61).
   - To generate a CSR and /or to upload a server certificate to the VCS, go to **Maintenance > Security > Server certificate**. You must restart the VCS for the new server certificate to take effect.

2. Install on both VCSs the trusted Certificate Authority (CA) certificates of the authority that signed the VCS's server certificates.

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

   For Mobile and Remote Access deployments:

   - The VCS Control must trust the Unified CM and IM&P tomcat certificate.
   - If appropriate, both the VCS Control and the VCS Expressway 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 VCS Control 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 VCS, go to **Maintenance > Security > Trusted CA certificate**. You must restart the VCS 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 VCS Traversal Zones

To support Unified Communications features via a secure traversal zone connection between the VCS Control and the VCS Expressway:

- The VCS Control and VCS Expressway must be configured with a zone of type *Unified Communications traversal*. This automatically configures an appropriate traversal zone (a traversal client zone when selected on VCS Control or a traversal server zone when selected on VCS Expressway) that uses SIP TLS with **TLS verify mode** set to *On*, and **Media encryption mode** set to *Force encrypted*.
- Both VCSs must trust each other's server certificate. As each VCS acts both as a client and as a server you must ensure that each VCS's certificate is valid both as a client and as a server.
- Be aware that VCS uses the SAN attribute (Subject Alternative Name) to validate the received certificate, not the CN (Common Name).
- If an H.323 or a non-encrypted connection is also required, a separate pair of traversal zones must be configured.

To set up a secure traversal zone, configure your VCS Control and VCS Expressway as follows:

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.

3. Configure the fields as follows (leave all other fields with default values):

	VCS Control	VCS Expressway
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
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		
Authentication policy	*Do not check credentials*	*Do not check credentials*
Location section		
Peer 1 address	Enter the FQDN of the VCS Expressway. Note that if you use an IP address (not recommended), that address must be present in the VCS Expressway server certificate.	Not applicable
Peer 2...6 address	Enter the FQDNs of additional peers if it is a cluster of VCS Expressways.	Not applicable

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 VCS 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 VCS's trusted CA list, the VCS can only trust one of them. This means that either secure HTTP or secure SIP, between VCS Control 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 *VCS 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 VCS does not allow two self-signed certificates with the same CN. If the *cup-xmpp* and *tomcat* (self-signed) certificates have the same CN, VCS only trusts one of them, and some TLS attempts between VCS Expressway and IM and Presence Service servers will fail. For more details, see CSCve56019.

VCS Certificates

The VCS 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 VCS.

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 VCS Expressway only	–	–	–
XMPP federation domains	–	–	Required on VCS Expressway only	–
IM and Presence chat node aliases (federated group chat)	–	–	Required	–
Unified CM phone security profile names	Required on VCS Control only	–	–	–

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
(Clustered systems only) VCS cluster name	Required on VCS Control only	Required on VCS Control only	Required on VCS Control only	

Note:

- You may need to produce a new server certificate for the VCS Control 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 VCS Expressway 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 VCS for any new uploaded server certificate to take effect.

More details about the individual feature requirements per VCS Control / VCS Expressway are described below.

VCS Control server certificate requirements

The VCS Control server certificate must include the elements listed below in its list of subject alternative names (SAN).

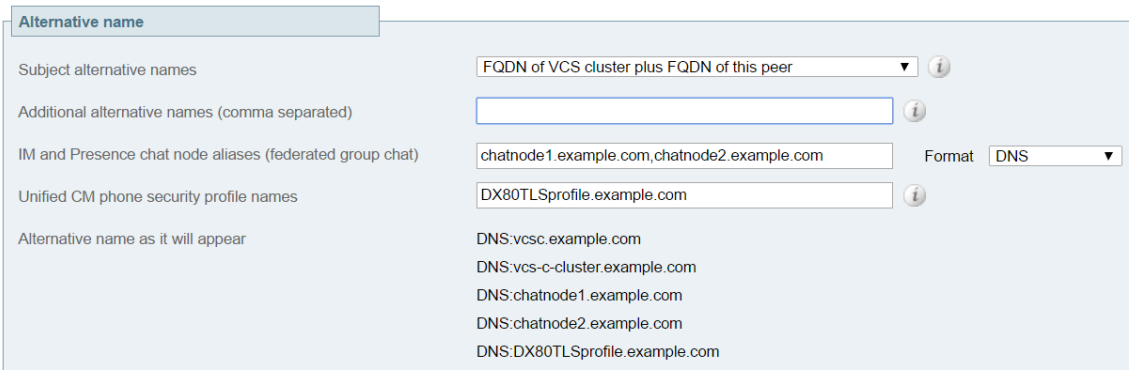
- **Unified CM phone security profile names**: the names of the **Phone Security Profiles** in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. Use the FQDN format and separate multiple entries with commas.

  Having the secure phone profiles as alternative names means that Unified CM can communicate via TLS with the VCS Control 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 VCS Control 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 VCS Expressway server certificate's alternative names.

Figure 4 Entering subject alternative names for security profiles and chat node aliases on the VCS Control's CSR generator



VCS Expressway server certificate requirements

The VCS Expressway 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 VCS Control for Unified CM registrations. Required for secure communications between endpoint devices and VCS Expressway.

  The Unified CM registration domains used in the VCS configuration and VCS Expressway 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.

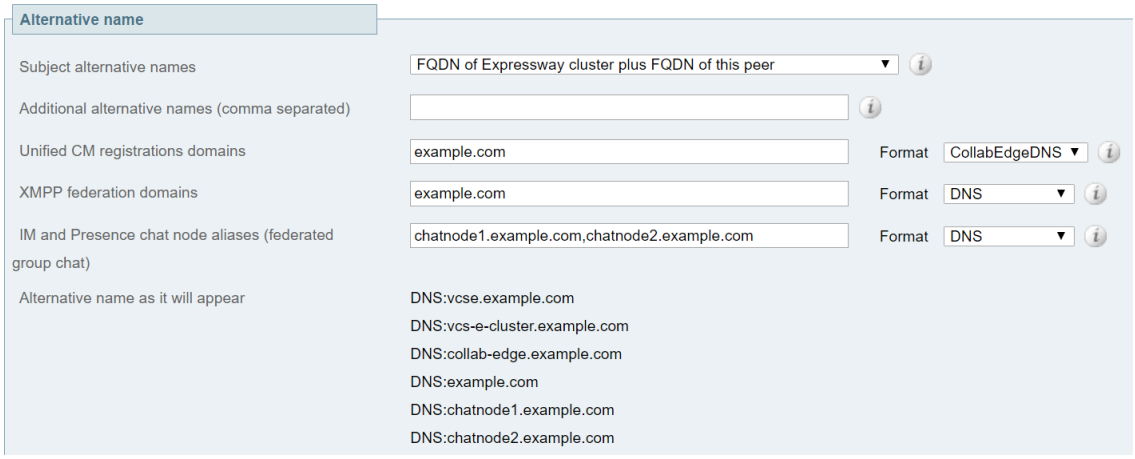
  These service discovery domains may or may not match the SIP registration domains. It depends on the deployment, and they don't have to match. One example is a deployment that uses a .local or similar private domain with Unified CM on the internal network, and public domain names for the VCS Expressway FQDN and service discovery. In this case, you need to include the public domain names in the VCS Expressway 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 VCS Control as domains for XMPP federation.

  Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. Do not use the *XMPPAddress* format as it may not be supported by your CA, and may be discontinued in future versions of the VCS software.
- **IM and Presence chat node aliases (federated group chat)**: the same set of **Chat Node Aliases** as entered on the VCS Control's certificate. They are only required for voice and presence deployments which will support group chat over TLS with federated contacts.

  Note that you can copy the list of chat node aliases from the equivalent **Generate CSR** page on the VCS Control.

Figure 5 Entering subject alternative names for Unified CM registration domains, XMPP federation domains, and chat node aliases, on the VCS Expressway's CSR generator



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 for Multitenancy

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

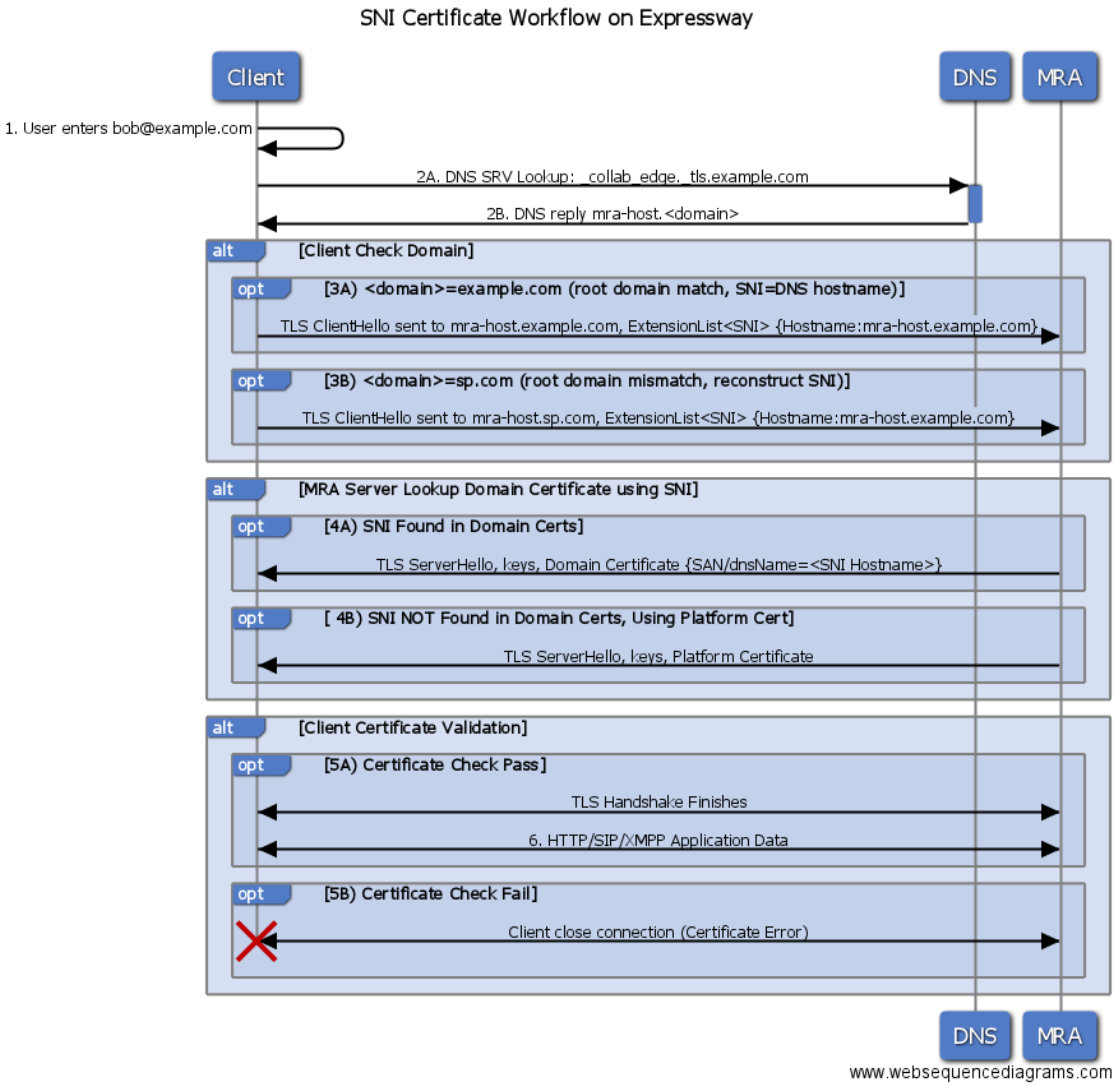
Using the Server Name Indication (SNI) protocol extension within TLS, the VCS can now store and use domain-specific certificates that can be offered to a client during the TLS handshake. This capability allows seamless integration of endpoints registering through MRA in a multitenant environment, and 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 VCS 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 VCS Expressway 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 VCS Expressway searches its certificate store to find a certificate matching the SNI hostname.
      - If a match is found, the VCS Expressway 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 VCS's Domain Certificates

You manage the VCS'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 VCS Expressway 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 VCS in all scenarios. Use the **Trusted CA certificate** page to manage the list of certificates for the Certificate Authorities (CAs) trusted by this VCS.

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 VCS.

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 VCS from being able to connect to those systems.

Adding a New Domain

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

Generating a Certificate Signing Request

The VCS can generate domain CSRs, which removes the need to use an external mechanism to generate and obtain certificate requests.

To generate a CSR:

1. Go to **Maintenance > Security > Domain certificates**.
2. Click on the domain for which you wish to generate a CSR.
3. Click **Generate CSR** to go to the **Generate CSR** page.
4. Enter the required properties for the certificate.
   - See Domain Certificates and Clustered Systems, page 68 if your VCS is part of a cluster.
5. Click **Generate CSR**. The system will produce a signing request and an associated private key. The private key is stored securely on the VCS and cannot be viewed or downloaded. **Never disclose your private key, not even to the certificate authority**.
6. You are returned to the **Domain certificate** page. From here you can:
   - Download the request to your local file system so that it can be sent to a certificate authority. You are prompted to save the file (the exact wording depends on your browser).
   - View the current request (click **Show (decoded)** to view it in a human-readable form, or click **Show (PEM file)** to view the file in its raw format).

Notes

- Only one signing request can be in progress at any one time. This is because the VCS 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. VCS supports a key length of 1024, 2048 and 4096.

Uploading a New Domain Certificate

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

To upload a domain certificate:

1. Go to **Maintenance > Security > Domain certificates**.
2. Use the **Browse** button in the **Upload new certificate** section to select and upload the domain certificate PEM file.
3. If you used an external system to generate the CSR you must also upload the server private key PEM file that was used to encrypt the domain certificate. (The private key file will have been automatically generated and stored earlier if the VCS was used to produce the CSR for this domain certificate.)
   - The server private key PEM file must not be password protected.
   - You cannot upload a server private key if a certificate signing request is in progress.
4. Click **Upload domain certificate data**.

ACME (Automated Certificate Management Environment) Service

The 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 VCSs, 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.

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.

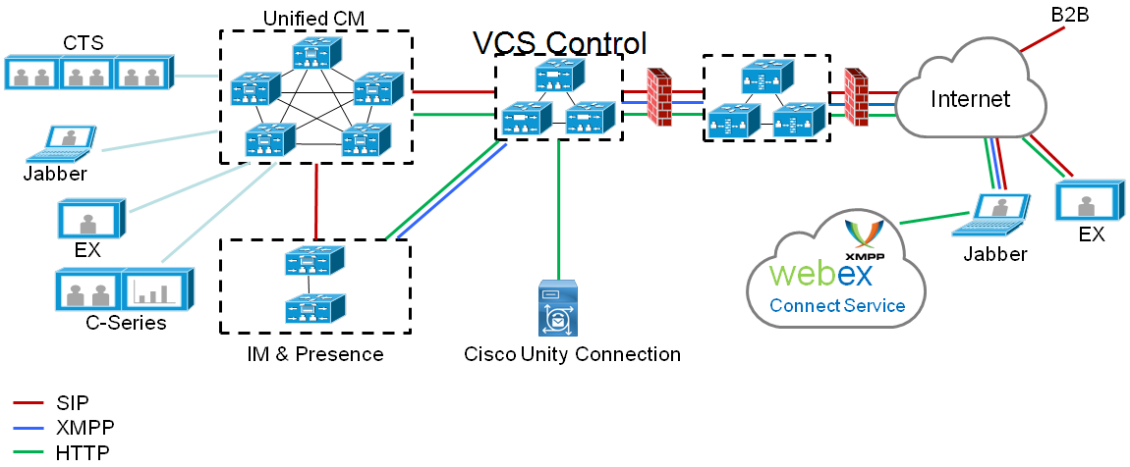
Mobile and Remote Access Overview

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 VCS provides secure firewall traversal and line-side support for Unified CM registrations.

The overall solution provides the following functions:

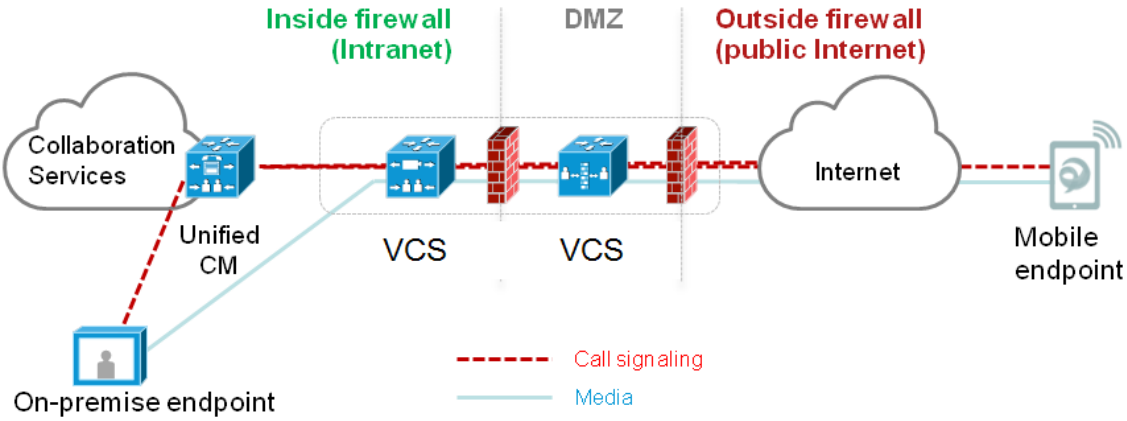
- **Off-premises access**: a consistent experience outside the network for Jabber and EX/MX/SX Series clients
- **Security**: secure business-to-business communications
- **Cloud services**: enterprise grade flexibility and scalable solutions providing rich Cisco Webex integration and service provider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

Figure 6 Unified Communications: Mobile and Remote Access



Note: Third-party SIP or H.323 devices can register to the VCS Control and, if necessary, interoperate with Unified CM-registered devices over a SIP trunk.

Figure 7 Typical call flow - signaling and media paths



Unified CM provides call control for both mobile and on-premises endpoints.

Signaling traverses the Expressway solution between the mobile endpoint and Unified CM. Media traverses the Expressway solution and is relayed between endpoints directly.

All media is encrypted between the VCS Control and the mobile endpoint.

Deployment Scope

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

- Mobile and Remote Access
- Microsoft interoperability, using the VCS Control-based B2BUA
- Jabber Guest services

Mobile & 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

Note: Cisco Jabber Video for TelePresence (Jabber Video) does not work with MRA, although it is supported as a general client registered to VCS.

Detailed Configuration Information

For details about using VCS for MRA, see *Mobile and Remote Access Through Cisco Expressway* on the Expressway configuration guides page. The guide describes:

- How to enable and configure MRA features on VCS Control and VCS Expressway.
- 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 the Apple Push Notification Service (APNS).

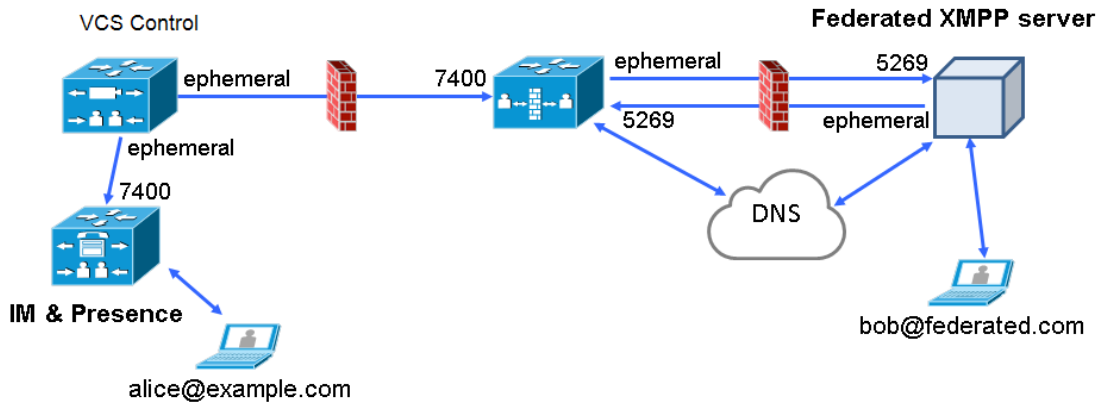
XMPP Federation through VCS

External XMPP federation enables users registered to Cisco Unified Communications Manager IM and Presence Service, to communicate via the VCS Expressway with users from a different XMPP deployment.

Note: This section describes XMPP federation as managed through VCS, 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 VCS Control and VCS Expressway 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 8 Message routing for XMPP federation



Supported Systems

VCS Expressway supports XMPP federation with the following products:

- VCS 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 VCS for XMPP federation, the VCS Expressway 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 VCS 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 VCS Expressway. 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 VCS 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 VCS).
  - 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 VCS:
  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.
- A VCS Control (cluster) and VCS Expressway (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 that 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 VCS.
- If you deploy external XMPP federation through VCS, 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 VCS Control and VCS Expressway 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 that the VCS Control 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 VCS Expressway we recommend that you copy-paste the chat node aliases from the equivalent **Generate CSR** page on the VCS Control.

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 VCS, 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 VCS Expressway is in multitenant mode. The VCS Expressway 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 VCS Expressway 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 VCS Expressway cluster among multiple tenants. Each tenant has a dedicated VCS Control cluster that connects to the shared VCS Expressway cluster.

Certain configuration changes on the VCS Expressway cluster, or a customer's VCS Control cluster, require a restart of the Cisco XCP Router on each VCS Expressway in the shared cluster. The restart is required for Cisco XCP Router configuration changes to take effect across all nodes in a multitenant VCS Expressway 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.

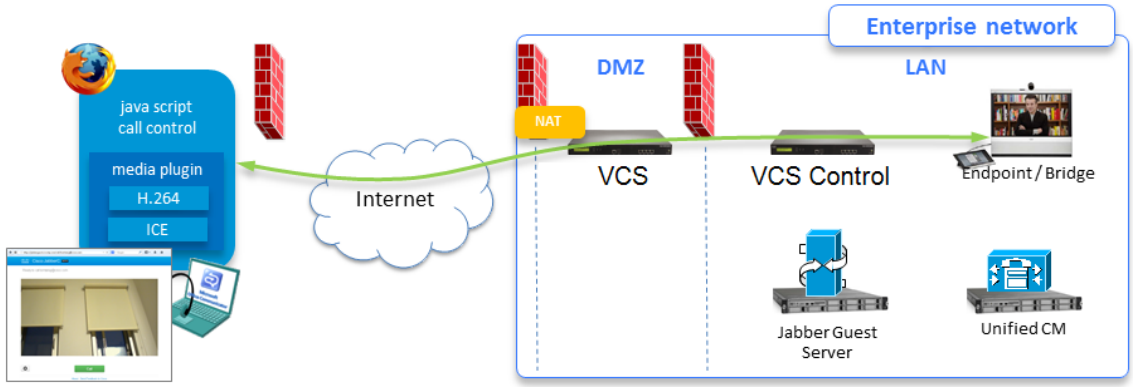
Jabber Guest Services Overview

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 VCS Control and VCS Expressway) 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 9 Jabber Guest Components



Information Scope

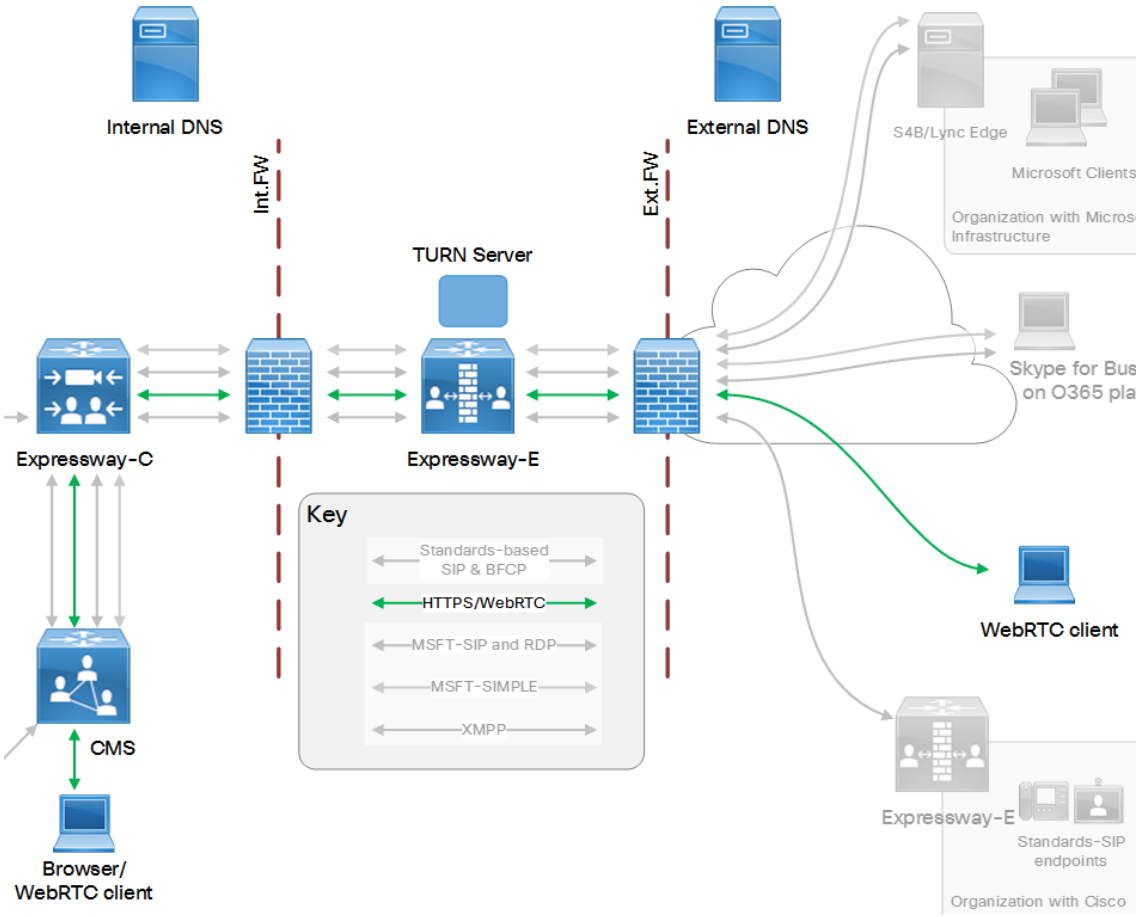
In versions X8.7 and earlier, all VCS configuration required for deployment with Jabber Guest was contained in the Administrator Guide. From X8.8 onwards, that information is kept in a separate deployment guide. You can read more detailed information about Jabber Guest in the following documents:

- *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 VCS

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 10 Meeting Server web proxy on VCS



Cisco Meeting Server with Cisco Expressway Deployment Guide on the Expressway configuration guides page (previously called the *Cisco Expressway Traffic Classification Deployment Guide*).

Protocols

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

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

About H.323 79

Configuring H.323 80

About SIP 81

Configuring SIP 84

Configuring Domains 88

Configuring SIP and H.323 Interworking 89

About H.323

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

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

Using the VCS as an H.323 Gatekeeper

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

To enable the VCS 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 VCS in order to use it as their gatekeeper.

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

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

Preventing Automatic H.323 Registrations

You can prevent H.323 endpoints being able to register automatically with the VCS by disabling **Auto Discovery** on the VCS (**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 VCS performance.

Configuring H.323

Go to **Configuration > Protocols > H.323** to configure the H.323 settings on the VCS.

The configurable options are:

Field	Description	Usage tips
H.323 mode	Enables or disables H.323 on the VCS. H.323 support is *Off* by default.	You must enable H.323 mode if you are clustering the VCS, even if there are no H.323 endpoints in your deployment.
Registration UDP port	The listening port for H.323 UDP registrations.	The default VCS configuration uses standard port numbers so you can use H.323 services out of the box without having to first set these up.
Registration conflict mode	Determines how the system behaves if an endpoint attempts to register an alias currently registered from another IP address. *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 VCS using an alias that has already been registered on the VCS 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 that in a cluster a registration conflict is only detected if the registration requests are received by the same peer.
Call signaling TCP port	The listening port for H.323 call signaling.	
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.

Field	Description	Usage tips
Time to live	The interval (in seconds) at which an H.323 endpoint must re-register with the VCS 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 VCS with registration requests, which will severely impact performance. This impact is proportional to the number of endpoints, so you should balance the need for occasional quick failover against the need for continuous good performance.
Call time to live	The interval (in seconds) at which the VCS polls the endpoints in a call to verify that they are still in the call. Default is 120.	If the endpoint does not respond, the call is disconnected. The system polls endpoints in a call, whether the call type is traversal or non-traversal.
Auto discover	Determines whether it will respond to Gatekeeper Discovery Requests sent out by endpoints. The default is *On*.	To prevent H.323 endpoints being able to register automatically with the VCS, set **Auto discover** to *Off*. This means that endpoints can only register with the VCS if their **Gatekeeper Discovery** setting is *Manual* and they have been configured with the VCS'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 VCS supports the SIP protocol. It can act as a SIP registrar, SIP proxy and as a SIP Presence Server. VCS 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:

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

VCS as a SIP Registrar

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

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

A SIP registrar only accepts registrations for domains for which it is authoritative. The VCS can act as a SIP registrar for up to 200 domains. To make the VCS act as a SIP registrar, you must configure it with the SIP domains for which it will be authoritative . It will then handle registration requests for any endpoints attempting to register against that domain. Note that the VCS will also accept registration requests where the domain portion of the AOR is either the

FQDN or the IP address of the VCS. Whether or not the VCS accepts a registration request depends on its registration control settings.

In a Unified Communications deployment, endpoint registration for SIP devices may be provided by Unified CM. In this scenario, the VCS 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 VCS 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 (VCS or VCS cluster) with which they want to register, and the endpoint will attempt to register with that registrar only.

The VCS is a SIP server and a SIP registrar.

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

Registration refresh intervals

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

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

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

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

SIP registration resiliency

The VCS 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 VCS 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.

VCS as a SIP Proxy Server

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

endpoint.

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

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

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 VCS, it adds a path header component to the request. This signals that calls to that endpoint should be routed through the VCS. 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 VCS 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 VCS 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 VCS 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 VCS receives a registration request for a domain for which it is not acting as a Registrar (the VCS does not have that SIP domain configured), then the VCS may proxy the registration request onwards. This depends on the **SIP registration proxy mode** setting, as follows:

- *Off*: the VCS does not proxy any registration requests. They are rejected with a "403 Forbidden" message.
- *Proxy to known only*: the VCS 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.

If your network is set up to proxy registration requests, we recommend that you disable GRUU on the VCS systems that are acting as a Registrar for those proxied requests. If GRUU is left enabled, Presence may not work properly for the proxy registered endpoints.

GRUU can only be disabled via the CLI (`xConfiguration SIP GRUU Mode: Off`).

Accepting proxied registration requests

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

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

VCS as a SIP Presence Server

The VCS 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 VCS as a SIP Presence server, see the Presence section.

Configuring SIP

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

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

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 VCS. Default is *Off*.	This mode must be enabled to use either the Presence Server or the Presence User Agent.
SIP protocols and ports	The VCS 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 VCS 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 VCS 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 VCS 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 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 VCS, downloaded automatically from preconfigured URIs (see Managing Certificate Revocation Lists (CRLs), page 291), 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 VCS never returns a value higher than what was requested. This applies only to endpoints registered with the VCS. It does not apply to endpoints whose registrations are proxied through the VCS.
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, page 82
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.
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.	

Field	Description	Usage tips
Outbound registration refresh maximum	The maximum allowed value for a SIP registration refresh period for an outbound registration. Requests for a value greater than this will result in a lower value being returned (calculated according to the **Outbound registration refresh strategy**). The default is 3600 seconds.	
SIP registration proxy mode	Specifies how proxied registrations and requests containing Route Sets are handled when the VCS 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 VCS 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, page 83 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 VCS. *Off*: use the relevant credential checking mechanisms (local database, Active Directory Service or H.350 directory via LDAP) on the VCS performing the authentication challenge. *On*: delegate the credential checking to a traversal client. The default is *Off*.	Note that 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 VCS (in bytes). Default is 32768 bytes.	If you use Microsoft interop with dual-homed conferencing through VCS 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 Messages (CLI)

From X8.11, a CLI command (not the web user interface) is available to optionally configure the VCS 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>, page 499.

Configuring Domains

The **Domains** page (**Configuration > Domains**) lists the SIP domains managed by this VCS.

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

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

You can configure up to 200 domains.

Configuring the Supported Services for Unified Communications (VCS Control Only)

When the VCS Control has been enabled for Unified Communications mobile and remote access, you must select the services that each domain will support. The options are:

- **SIP registrations and provisioning on VCS**: the VCS is authoritative for this SIP domain. The VCS 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 VCS 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 VCS Control and VCS Expressway.

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 (VCS Expressway 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 VCS 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 VCS Expressway to perform the credential checking.

Testing the credential checking service

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

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

   The system displays a **Results** section and reports whether the receiving VCS 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 VCS 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 VCS 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 VCS 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 VCS 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 VCS does not act as a SIP–H.323 gateway.
- *Registered only*: the VCS acts as a SIP–H.323 gateway but only if at least one of the endpoints is locally registered.
- *On*: the VCS acts as a SIP–H.323 gateway regardless of whether the endpoints are locally registered.

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

Calls for which the VCS acts as a SIP to H.323 gateway are traversal calls. The VCS 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 VCS 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 VCS is in the media path it will close and open logical channels to the H.323 device as the media changes (as required) so that media is passed correctly.

Searching by protocol

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

- If the request has come from a neighboring system and **Interworking mode** is set to *Registered only*, the VCS 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 VCS 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 VCS 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 VCS that strips the `@domain` portion of the alias for those URIs that are in the form of `number@domain`.
  See the pre-search transforms section for information about how to configure pre-search transforms, and the stripping @domain for dialing to H.323 numbers section for an example of how to do this.

Interworking DTMF signals

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

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

When the VCS 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".

Registration Control

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

About Registrations 91

About Allow and Deny Lists 94

Configuring Registration Policy to Use an External Service 96

About Registrations

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

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

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

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

- the **Registration conflict mode** and **Auto discover** settings for H.323 registrations
- the **SIP registration proxy mode** for SIP registrations

For specific information about how registrations are managed across peers in a cluster, see the Sharing Registrations Across Peers, page 164 section.

In a Unified Communications deployment, endpoint registration for SIP devices may be provided by Unified CM. In this scenario, the VCS 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 VCS provides registration and provisioning services for the domain.

Finding a VCS With Which to Register

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

Registrations on a VCS Expressway

If a traversal-enabled endpoint registers directly with a VCS Expressway, the VCS Expressway will provide the same services to that endpoint as a VCS Control, with the addition of firewall traversal. Traversal-enabled endpoints include all Cisco TelePresence Expressway™ endpoints and third-party endpoints which support the ITU H.460.18 and H.460.19 standards.

Endpoints that are not traversal-enabled can still register with a VCS Expressway, but they may not be able to make or receive calls through the firewall successfully. This will depend on a number of factors:

- whether the endpoint is using SIP or H.323
- the endpoint's position in relation to the firewall
- whether there is a NAT in use
- whether the endpoint is using a public IP address

For example, if an endpoint is behind a NAT or firewall, it may not be able to receive incoming calls and may not be able to receive media for calls it has initiated. SIP endpoints can also work behind a NAT but can only receive video if they send it as well.

To ensure firewall traversal will work successfully for H.323 endpoints behind a NAT, the endpoint must be traversal-enabled.

MCU, Gateway and Content Server Registration

H.323 systems such as gateways, MCUs and Content Servers can also register with a VCS. They are known as locally registered services. These systems are configured with their own prefix, which they provide to the VCS when registering. The VCS 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 VCS manages its registrations.

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

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

The default is *None*.

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

The *Policy service* option is used if you want to refer all registration restriction policy decisions out to an external service. If you select this option an extra set of configuration fields appear so that you can specify the connection details of the external service. See Configuring Registration Policy to Use an External Service, page 96.

Registering Aliases

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

H.323

When registering, the H.323 endpoint presents the VCS 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 VCS 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 VCS 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, page 117 for more information.

Attempts to register using an existing alias

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

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

Blocking registrations

If you have configured the VCS to use a Deny List, you will have an option to block the registration. This will add all the aliases used by that endpoint to the Deny List.

Removing existing registrations

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

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

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

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

Re-registrations

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

- H.323 endpoints may use "light" re-registrations which do not contain all the aliases presented in the initial registration, so the re-registration may not get filtered by the restriction policy. If this is the case, the registration will not expire at the end of the registration timeout period and must be removed manually.

- SIP re-registrations contain the same information as the initial registrations so will be filtered by the restriction policy. This means that, after the list has been activated, all SIP registrations will disappear at the end of their registration timeout period.

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

Note: By reducing the registration time to live too much, you risk flooding the VCS 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 VCS it presents a list of aliases. One of the methods provided by the VCS to control which endpoints are allowed to register is to set the **Restriction policy** (on the Configuring Registration Restriction Policy, page 92 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 subzone level. Each subzone's registration policy can be configured to allow or deny registrations assigned to it via the subzone membership rules.

Configuring the Registration Allow List

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

To use the Allow List, you must select a **Restriction policy** of *Allow List* on the Registration configuration page.

The configurable options are:

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

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 expression.	You can test whether a pattern matches a particular alias by using the **Check pattern** tool (**Maintenance > Tools > Check pattern**).
Pattern string	The pattern against which an alias is compared.	

Configuring the Registration Deny List

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

To use the Deny List, you must select a **Restriction policy** of *Deny List* on the Registration configuration page.

The configurable options are:

Field	Description	Usage tips
Description	An optional free-form description of the entry.	
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 expression.	You can test whether a pattern matches a particular alias by using the **Check pattern** tool (**Maintenance > Tools > Check pattern**).
Pattern string	The pattern against which an alias is compared.	

Configuring Registration Policy to Use an External Service

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

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

Field	Description	Usage tips
Protocol	The protocol used to connect to the policy service. The default is *HTTPS*.	The VCS 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 VCS to connect to a policy server over HTTPS, the VCS 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 VCS'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 VCS 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 VCS 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 VCS 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, page 340.
Username	The username used by the VCS to log in and query the service.	
Password	The password used by the VCS to log in and query the service.	The maximum plaintext length is 30 characters (which is subsequently encrypted).

Field	Description	Usage tips
Default CPL	This is the fallback CPL used by the VCS if the service is not available.	You can change it, for example, to redirect to an answer service or recorded message. For more information, see Default CPL for Policy Services, page 553.

4. Click **Save**.

   The VCS should connect to the policy service server and start using the service for Registration Policy decisions.

   Any connection problems will be reported on this page. Check the **Status** area at the bottom of the page and check for additional information messages against the **Server address** fields.

Device Authentication

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

About Device Authentication 99

Authenticating with External Systems 125

About Device Authentication

Device authentication is the verification of the credentials of an incoming request to the Cisco TelePresence Video Communication Server (VCS) from a device or external system. It is used so that certain functionality may be reserved for known and trusted users, for example the publishing of presence status, collection of provisioning data, or the ability to use resources that cost money like ISDN gateway calling.

When device authentication is enabled on a VCS, any device that attempts to communicate with the VCS is challenged to present its credentials (typically based on a username and password). The VCS will then verify those credentials, or have them verified, according to the authentication method, and then accept or reject the message accordingly.

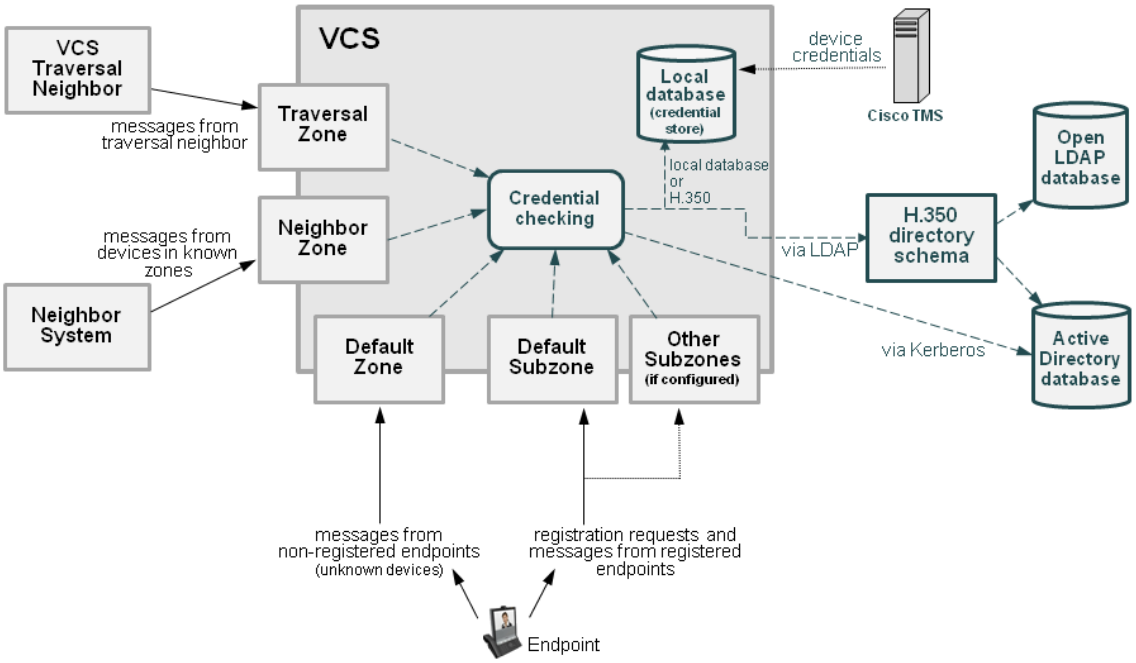
VCS authentication policy can be configured separately for each zone and subzone. This means that both authenticated and unauthenticated devices could be allowed to register to, and communicate with, the same VCS if required. Subsequent call routing decisions can then be configured with different rules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

The VCS attempts to verify the credentials presented to it by first checking against its on-box local database of usernames and passwords. If the username is not found in the local database, the VCS may then attempt to verify the credentials via a real-time LDAP connection to an external H.350 directory service. The directory service, if configured, must have an H.350 directory schema for either a Microsoft Active Directory LDAP server or an OpenLDAP server.

You can also configure a VCS Expressway so that the credential checking of SIP messages is delegated, via a traversal zone, to another VCS.

Along with one of the above methods, for those devices that support NTLM challenges, the VCS can alternatively verify credentials via direct access to an Active Directory server using a Kerberos connection.

The various VCS authentication entry points and credential checking methods are shown below:



Mobile and Remote Access devices

You do not have to make any explicit configuration on the VCS regarding the authentication of devices that are registering to Unified CM via the VCS. If the VCS 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.

Configuring VCS Authentication Policy

Authentication policy is applied by the VCS at the zone and subzone levels. It controls how the VCS challenges incoming messages (for provisioning, registration, presence, phone books, and calls) from that zone or subzone and whether those messages are rejected, treated as authenticated, or treated as unauthenticated within the VCS.

Each zone and subzone can set its **Authentication policy** to *Check credentials*, *Do not check credentials*, or *Treat as authenticated*.

- Registration authentication is controlled by the Default Subzone configuration (or the relevant alternative subzone).
- Initial provisioning subscription request authentication is controlled by the Default Zone configuration.
- Call, presence, and phone book request authentication is controlled by the Default Subzone (or relevant alternative subzone) if the endpoint is registered, or by the Default Zone if the endpoint is not registered.

Note that the exact authentication policy behavior depends on whether the messages are H.323 messages, SIP messages received from local domains, or SIP messages received from non-local domains. See Authentication Policy Configuration Options, page 102 for a full description of the various authentication policy behaviors.

Zone-level authentication policy

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.

Subzone-level authentication policy

Authentication policy is configurable for the Default Subzone and any other configured subzone.

To configure a subzone's **Authentication policy**, go to **Configuration > Local Zone > Subzones**, then click View/Edit or the name of the subzone. The policy is set to *Do not check credentials* by default when a new subzone is created.

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 VCS. The Provisioning Server does not do its own authentication challenge and will reject any unauthenticated messages.

See Device Provisioning and Authentication Policy, page 109 for more information.

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 VCS 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, page 111 for more information.

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 VCS itself. You can configure the VCS to use policy services in the following areas:

- Registration Policy
- Search rules (dial plan)
- Call Policy
- User Policy (FindMe)

When the VCS 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 VCS External Policy Deployment Guide* at the Cisco TelePresence Video Communication Server (VCS) Configuration Guides page.

CPL

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

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

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

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

Authentication Policy Configuration Options

Authentication policy behavior varies for H.323 messages, SIP messages received from local domains and SIP messages from non-local domains.

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

- **Check credentials**: verify the credentials using the relevant authentication method. Note that in some scenarios, messages are not challenged, see below.
- **Do not check credentials**: do not verify the credentials and allow the message to be processed.
- **Treat as authenticated**: do not verify the credentials and allow the message to be processed as if it 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 that in some scenarios, messages are allowed but will still be treated as though they are unauthenticated, see below.

The following tables summarize the policy behavior when applied at the zone and subzone level, and how it varies depending on the message protocol.

Zone-Level Authentication Policy

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.
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 VCS 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 VCS 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.
	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 VCS'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.

Policy	Trust	In local domain	Outside local domain
	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.

Subzone-Level Authentication Policy

Authentication policy is configurable for the Default Subzone and any other configured subzone.

To configure a subzone's **Authentication policy**, go to **Configuration > Local Zone > Subzones**, then click View/Edit or the name of the subzone. The policy is set to *Do not check credentials* by default when a new subzone is created.

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. Messages that pass authentication are classified as authenticated. If no credentials are supplied, the message is always classified as unauthenticated. Note that unauthenticated registration requests are rejected.
Do not check credentials	Message credentials are not checked and all messages are classified as unauthenticated.
Treat as authenticated	Message credentials are not checked and all messages are classified as authenticated.

SIP

The behavior for SIP messages depends upon whether the message was received from a local domain (a domain for which the VCS is authoritative) or a non-local domain.

Policy	In local domain	Outside local domain
Check credentials	Messages are challenged for authentication and those that pass are classified as authenticated. Messages (including registration requests) that fail authentication are rejected.	SIP messages received from non-local domains are all treated in the same manner, regardless of the subzone's **Authentication policy** setting: Messages are not challenged for authentication. All messages are classified as unauthenticated.
Do not check credentials	Messages are not challenged for authentication. All messages are classified as unauthenticated.	
Treat as authenticated	Messages are not challenged for authentication. All messages are classified as authenticated.	

SIP Authentication Trust

If the VCS is configured to use device authentication it will authenticate incoming SIP registration and INVITE requests. If the VCS then forwards the request on to a neighbor zone such as another VCS, 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 VCS. Pre-authenticated SIP requests are identified by the presence of a P-Asserted-Identity field in the SIP message header as defined by *RFC 3325*.

The **Authentication trust mode** settings are:

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

Note:

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

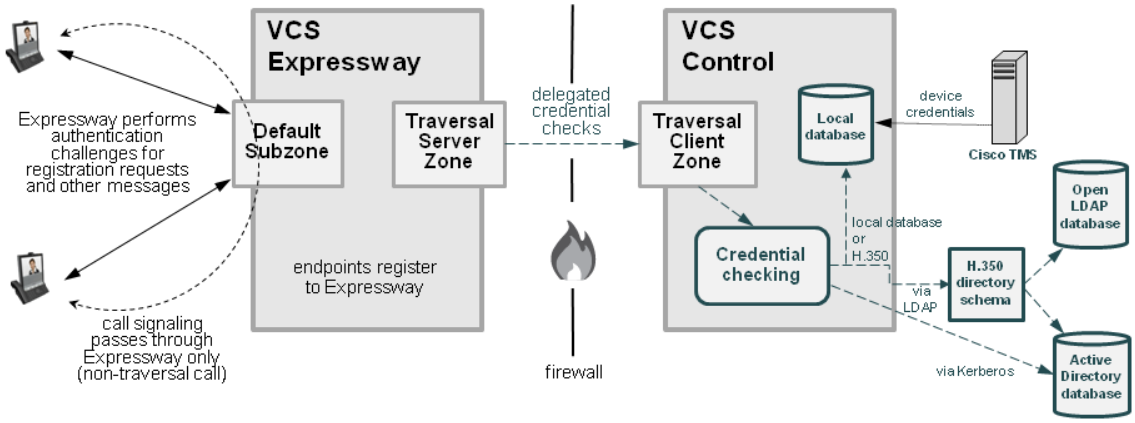
Configuring Delegated Credential Checking (SIP Only)

By default, the VCS uses the relevant credential checking mechanisms (local database, Active Directory Service or H.350 directory via LDAP) on the same VCS that is performing the authentication challenge.

Alternatively you can configure the VCS that is performing the authentication challenges to delegate the credential checking of SIP messages, via a traversal zone, to another VCS (typically a VCS Control). Delegated credential checking is useful in deployments where you want to allow devices to register on the VCS Expressway (so that, for example, calls may be made without having to use a traversal license), but for security you want all communications with authentication systems (such as an Active Directory server) to be performed inside the enterprise.

- Credential checking for both SIP Digest and NTLM messages may be delegated.
- All messages must be for locally-defined SIP domains. You can delegate credential checking to different traversal clients on a per domain basis if required.

The following diagram shows how incoming SIP messages (calls, registrations and so on) are challenged by the VCS Expressway, but the checking of the credentials presented in response to those challenges is delegated to the VCS Control.



Configuring Your Video Communications Network for Delegated Credential Checking

Several configuration steps are involved, on both your VCS Expressway and your VCS Control, in setting up your video network for delegated credential checking.

It is likely that much of this configuration, such as the set of local SIP domains, will already be in place, however the sections below list all of the necessary configuration requirements.

VCS Expressway and VCS Control

There must be a secure traversal zone connection between the VCS Control and the VCS Expressway:

- The VCS Control and VCS Expressway must be configured with a zone of type *Unified Communications traversal*. This automatically configures an appropriate traversal zone (a traversal client zone when selected on VCS Control or a traversal server zone when selected on VCS Expressway) that uses SIP TLS with **TLS verify mode** set to *On*, and **Media encryption mode** set to *Force encrypted*.
- Both VCSs must trust each other's server certificate. As each VCS acts both as a client and as a server you must ensure that each VCS's certificate is valid both as a client and as a server.
- Be aware that VCS uses the SAN attribute (Subject Alternative Name) to validate the received certificate, not the CN (Common Name).
- If an H.323 or a non-encrypted connection is also required, a separate pair of traversal zones must be configured.

VCS Control

1. Configure SIP domains (**Configuration > Domains**).

   It must be configured with all of the domains for which it will receive delegated authentication checks.
2. Configure the relevant authentication mechanisms (local database, Active Directory Service or H.350 directory via LDAP).
3. Enable **Delegated credential checking** (**Configuration > Protocols > SIP**).
4. Ensure that the traversal client zone is configured to **Accept delegated credential checks**.

VCS Expressway

1. Configure SIP domains (**Configuration > Domains**).

   It must be configured with all of the domains for which it will delegate authentication checks.
2. For each domain, choose the traversal zone over which the credential checks are to be delegated.
3. If NTLM / Active Directory Service authentication is required, ensure that **NTLM protocol challenges** (**Configuration > Authentication > Devices > Active Directory Service**) is set to *Auto*.
4. Enable **Delegated credential checking** on the **SIP** page (**Configuration > Protocols > SIP**).
5. Ensure that the relevant zone and subzone authentication policies are set to *Check credentials*.

   Note that any H.323 messages that arrive at the zones or subzones that are now configured to *Check credentials* will still have those credentials checked via the relevant mechanisms (such as the local database or H.350 directory) on that local VCS and they will not be delegated.
6. If required as part of your dial plan, configure search rules that forward SIP call signaling messages to the relevant traversal client zones.

   (Note that no specific search rules are required to support the delegation of authentication messages to the VCS Control.

The credential checking of authentication challenges made by the VCS Expressway should now be delegated through the traversal zone to the VCS Control.

Testing the credential checking service

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

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

   The system displays a **Results** section and reports whether the receiving VCS 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 VCS is not configured with a connection to an Active Directory Service, then the NTLM check will be expected to fail.

TURN services

If TURN services are enabled on the VCS Expressway and you also want to delegate the credential checking of TURN server requests:

1. Go to **Configuration > Traversal > TURN**.
2. Set **Delegated credential checking** to *On*.
3. For the **Authentication realm**, choose from the set of configured SIP domains to determine the traversal zone through which credential checking is delegated.

Additional information

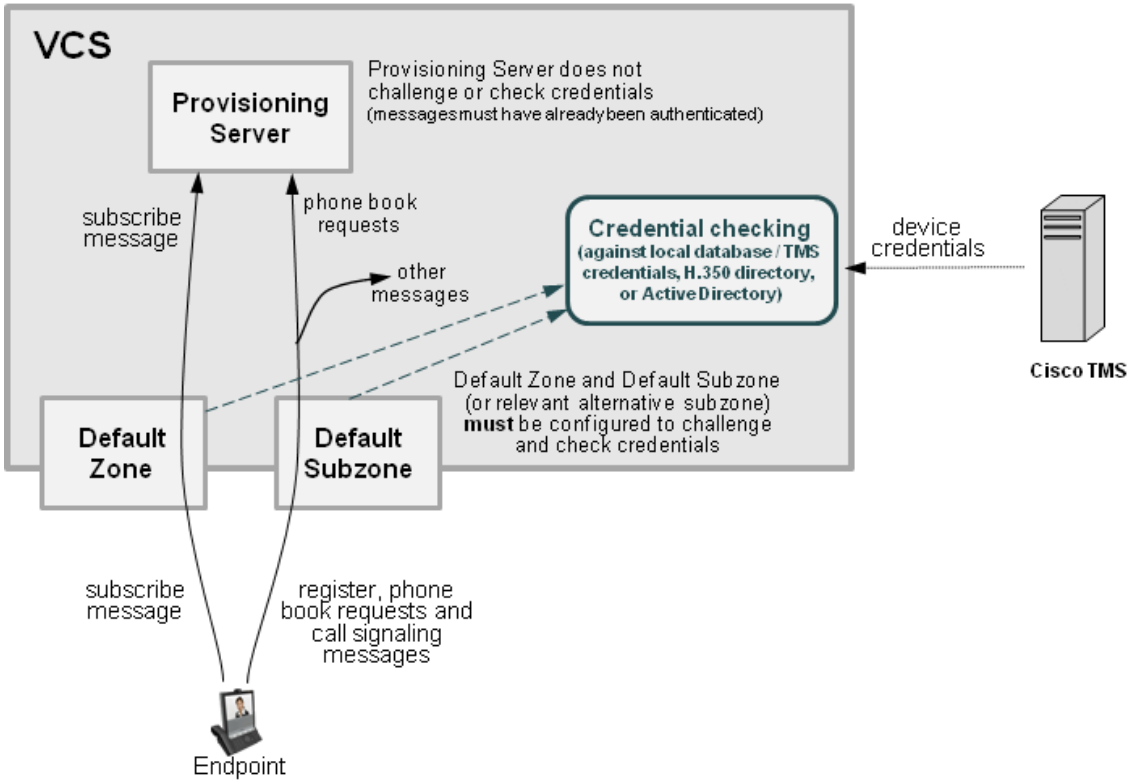
- The system clocks on the VCS Control and the VCS Expressway must be within 100 seconds of each other. We recommend that all VCSs are configured to use a common NTP server.
- The VCS Expressway can still perform "local" non-delegated authentication for specific domains. If this is required, ensure that:
  - Those domains have **Traversal zone for delegated credential checking** set to *Do not delegate*.
  - The relevant authentication mechanisms are configured on the VCS Expressway.
- The VCS Control can still perform authentication in the normal manner, as well as providing a delegated credential checking service for the VCS Expressway. Note that:
  - The **NTLM protocol challenges** setting on the VCS Control only applies if the VCS Control itself is making an authentication challenge.
  - The authentication policy configuration on the traversal client on the VCS Control has no effect on the delegated credential checking requests received by the VCS Control.

  Enabling delegated credential checking does not affect any other message routing; there is no need to amend any existing transforms, search rules and so on.

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 VCS. The Provisioning Server does not do its own authentication challenge and will reject any unauthenticated messages.

The following diagram shows the flow of provisioning messages from an endpoint to the Provisioning Server, together with the credential checking processes:



The VCS 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.
- The authentication of subsequent messages, including registration requests, phone book requests and call signaling messages 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 phone book requests will fail.

In each case, the VCS performs its authentication checking against the appropriate credential store, according to whichever authentication methods are configured. Note that if the VCS is using the local database, this will include all credentials supplied by Cisco TMS.

For more information about provisioning configuration in general, see *Cisco TMS Provisioning Extension Deployment Guide*.

VCS Starter Pack Express

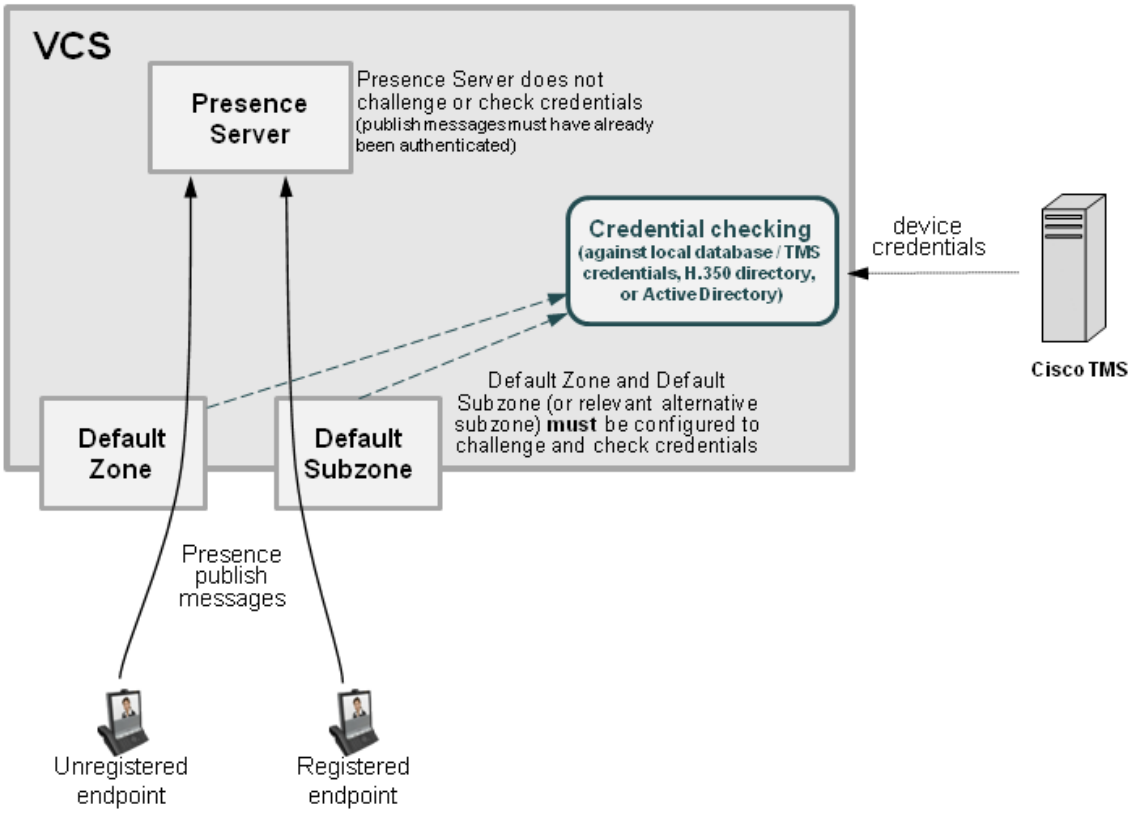
The Provisioning Server on a VCS Starter Pack Express operates in the same manner as when using Cisco TMS provisioning – it does not challenge provisioning requests. It provisions devices only if the request has already been authenticated by the VCS (at the zone or subzone entry point).

Presence and Authentication Policy

The Presence Server accepts presence PUBLISH messages only if they have already been authenticated:

- The authentication of presence messages by the VCS 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.

The following diagram shows the flow of presence messages from an endpoint to the Presence Server:



In each case, the VCS performs its authentication checking against the appropriate credential store, according to whichever authentication methods are configured. Note that if the VCS is using the local database, this will include any credentials supplied by Cisco TMS.

Hierarchical Dial Plans and Authentication Policy

Hierarchical dial plan (directory VCS) deployments and device authentication

When introducing authentication into video networks which have a hierarchical dial plan with a directory VCS, authentication problems can occur if:

- any VCS in the network uses a different authentication database from any other VCS in the network, and
- credential checking is enabled on the Default Zone of any VCS (as is needed, for example, when using Cisco TMSPE), and
- the directory VCS or any other VCS in a signaling path can optimize itself out of the call routing path

In such deployments, each VCS must be configured with a neighbor zone between itself and every other VCS in the network. Each zone must be configured with an **Authentication policy** of *Do not check credentials*. (No search rules are required for these neighbor zones; the zones purely provide a mechanism for trusting messages between VCSs.)

This is required because, otherwise, some messages such as SIP RE-INVITES, which are sent directly between VCSs (due to optimal call routing), will be categorized as coming from the Default Zone. The VCS will then attempt to authenticate the message and this may fail as it may not have the necessary credentials in its authentication database. This means that the message will be rejected and the call may be dropped. However, if the node VCSs have a neighbor zone relationship then the message will be identified as coming through that neighbor zone, the VCS will not perform any credential checking (as the neighbor zone is set to *Do not check credentials*) and the message will be accepted.

Deployments with multiple regional / subnetwork directory VCSs

If your deployment is segmented into multiple regional subnetworks, each with their own directory VCS, it is not feasible (or recommended) to set up neighbor zones between each and every VCS across the entire network.

In this scenario you should configure each subnetwork as described above – i.e. set up neighbor zones between each of the VCSs managed by the same directory VCS – and then configure the neighbor zones between each directory VCS so that they stay in the call signaling path on calls crossing subnetworks between those directory VCSs. To do this:

1. On the directory VCS, go to **Configuration > Zones > Zones** and then click on the relevant zone to the other directory VCS.
2. On the **Edit zones** page, scroll down to the **Advanced** section and set **Zone profile** to *Custom*.
3. Set **Call signaling routed mode** to *Always*.
4. Click **Save**.
5. Repeat this for the equivalent zone definition on the "other" directory VCS, and then repeat the entire process for any other zone configurations between any other directory VCSs.

Note: do not modify the directory VCS's primary **Call signaling routed mode** setting on the **Calls** page.

This means that the each directory VCS will stay in the call signaling path for calls that go between subnetworks. Each directory VCS will still be able to optimize itself out of the call signaling path for calls entirely within each subnetwork.

You must also ensure that you have sufficient call licenses (traversal and non-traversal) on each directory VCS to handle those calls going between each subnetwork.

Practical Configuration of Authentication Policy

VCS Control

The table below contains practical guidelines for configuring authentication policy on a VCS Control.

Authentication point	Guideline
Default Zone	Use *Check credentials*.
Default Subzone	Use *Check credentials*.
Specific local subzones	For known local subnets, to avoid having to configure all local endpoints with credentials, use *Treat as authenticated*. Although this is a practical solution, we recommend that no *Treat as authenticated* subzones are used, and that every endpoint is populated with appropriate and unique credentials and that *Check credentials* is used.
Other subzones	Use *Check credentials*.
Traversal zone	Use *Check credentials*. Always check the credentials of requests coming from the VCS Expressway.
Neighbor zone	Use *Do not check credentials* and set **SIP authentication trust mode** to *On*.

VCS Expressway

Ideally, VCS Expressway authentication policy, should follow exactly the same guidelines as for the VCS Control. However if AD Direct or H.350 access is required, many security policies will not allow a device in a DMZ access to those resources. Practicality therefore recommends that authentication is left to the VCS Control. For SIP devices you can use delegated credential checking; this allows SIP devices to register to the VCS Expressway but be authenticated via a device authentication mechanism configured on the VCS Control.

You can also use registration allow and deny lists to limit what can register to the VCS Expressway. If it is required that outbound calls may only be made by authenticated users, ensure that all call requests are routed to the VCS Control and it only forwards requests back that it can authenticate.

Infrastructure devices

You are recommended to configure your VCS so that infrastructure products, such as MCUs, register to a dedicated subzone with an authentication policy set to *Treat as authenticated*.

Configuring VCS Authentication Methods

The VCS supports 3 different methods of verifying authentication credentials:

- against the system's local database (which includes any Cisco TMS-supplied credentials)
- via an LDAP connection to an external H.350 directory service
- via direct access to an Active Directory server using a Kerberos connection (NTLM challenges only)

The VCS attempts to verify the credentials presented to it by first checking against its on-box local database of usernames and passwords. If the username is not found in the local database, the VCS may then attempt to verify the credentials via a real-time LDAP connection to an external H.350 directory service. The directory service, if configured, must have an H.350 directory schema for either a Microsoft Active Directory LDAP server or an OpenLDAP server.

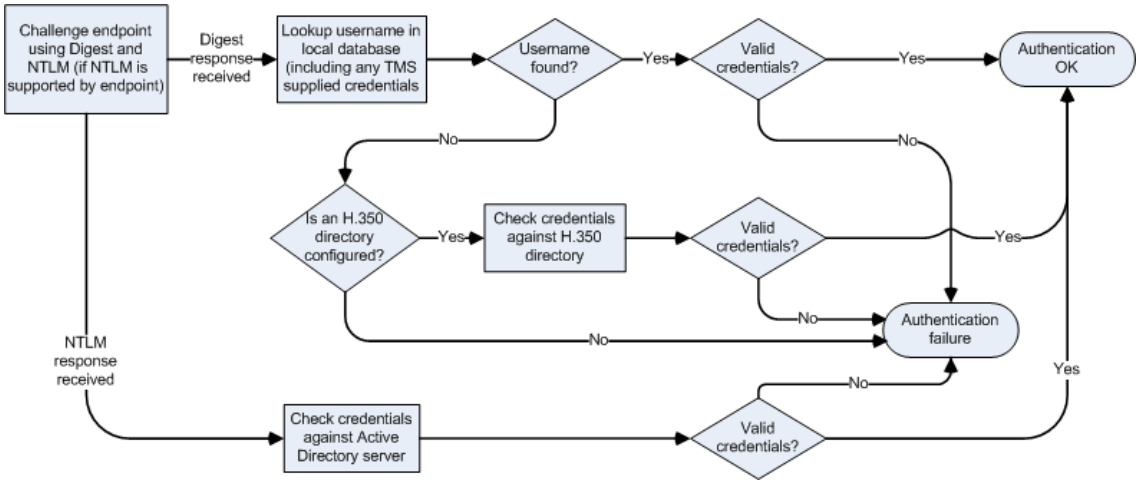
Along with one of the above methods, for those devices that support NTLM challenges, the VCS can alternatively verify credentials via direct access to an Active Directory server using a Kerberos connection. The direct Active Directory authentication via Kerberos method is only supported by a limited range of endpoints – at the time of

writing, only Cisco Jabber for iPad and Jabber Video. If used, other non-supported endpoint devices will continue to authenticate using one of the other two authentication methods.

Note that the VCS always challenges an endpoint with a standard Digest challenge. The VCS will additionally send an NTLM challenge if the VCS has NTLM protocol challenges enabled and it recognizes that the endpoint supports NTLM.

If the endpoint receives both challenges, it is the endpoint's decision as to whether to respond to the Digest challenge or to the NTLM challenge. At the time of writing, all supported endpoints respond to an NTLM challenge in preference to a Digest challenge.

The following diagram shows the process followed by the VCS when authenticating credentials:



Note that accurate timestamps play an important part in authentication of H.323 devices, helping to guard against replay attacks. For this reason, if you are using device authentication with H.323 devices, both the VCS and the endpoints must use an NTP server to synchronize their system time.

Authentication Mechanism

The authentication process uses a username and password-based challenge-response scheme to check a device's credentials.

The actual mechanism used by the device to supply its credentials to the VCS depends on the protocol being used:

- **H.323**: any necessary credentials are contained within the incoming request. (The VCS supports the *ITU H.235 specification* for authenticating the identity of H.323 network devices with which it communicates.)
- **SIP**: credentials are not contained within the initial request. Instead the VCS sends a challenge back to the sender that asks for its credentials. However, if a SIP message has already been authenticated (for example by another VCS on a previous hop), that system may insert information into the SIP message to show that it has been authenticated. You can control whether the VCS chooses to trust any authentication carried out at an earlier stage by configuring a zone's SIP authentication trust setting.

Note that if the VCS is acting as a traversal server, you must ensure that each traversal client's authentication credentials are entered into the selected database.

Endpoint Credentials Used for Authentication

An endpoint must supply the VCS with a username and password if it is required to authenticate with the VCS, for example when attempting to register and the relevant subzone's **Authentication policy** is set to *Check credentials*.

For Cisco endpoints using H.323, the username is typically the endpoint's **Authentication ID**; for Cisco endpoints using SIP it is typically the endpoint's **Authentication username**.

See the relevant endpoint manual for details about how to configure the endpoint's credentials.

Configuring Authentication to Use the Local Database

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

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

Adding credentials to the local database

To enter a set of device credentials:

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

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

Credentials managed within Cisco TMS (for device provisioning)

When the VCS 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 VCS 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 VCS to use both the local database and an H.350 directory.

If an H.350 directory is configured, the VCS 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 VCS will attempt to authenticate that NTLM response.

Starter Pack

If the **Starter Pack** option key is installed, the local authentication database will include a pre-configured set of authentication credentials. To ensure correct operation of the TURN server in conjunction with the Starter Pack, do not delete or modify the **StarterPackTURNUser** entry in the local authentication database.

All other credentials that are required to support Starter Pack provisioned devices have to be added manually for each user account.

Using an H.350 Directory Service Lookup via LDAP

The **Device authentication H.350 configuration** page (**Configuration > Authentication > Devices > H.350 directory service**) is used to configure a connection via LDAP to an H.350 directory service. An H.350 directory service lookup can be used for authenticating any endpoint, SIP and H.323.

H.350 directory authentication and registration process

If the VCS is using an H.350 directory service to authenticate registration requests, the process is as follows:

1. The endpoint presents its username and authentication credentials to the VCS, and the aliases with which it wants to register.
2. The VCS then determines which aliases the endpoint is allowed to attempt to register with, based on the **Source of aliases for registration** setting.

   For H.323 endpoints, you can use this setting to override the aliases presented by the endpoint with those in the H.350 directory, or you can use them in addition to the endpoint's aliases.

   For SIP endpoints, you can use this setting to reject a registration if the endpoint's AOR does not match that in the H.350 directory.

   The options are:

   - *H.350 directory*: for SIP registrations the AOR presented by the endpoint is registered providing it is listed in the H.350 directory for the endpoint's username.

     For H.323 registrations:

     - At least one of the aliases presented by the endpoint must be listed in the H.350 directory for that endpoint's username. If none of the presented aliases are listed it is not allowed to register.
     - The endpoint will register with all of the aliases (up to a maximum of 20) listed in the H.350 directory. Aliases presented by the endpoint that are not in the H.350 directory will not be registered.
     - If no aliases are listed in the H.350 directory, the endpoint will register with all the aliases it presented.
     - If no aliases are presented by the endpoint, it will register with all the aliases listed in the H.350 directory for its username.
   - *Combined*: the aliases presented by the endpoint are used in addition to any listed in the H.350 directory for the endpoint's username. In other words, this is the same as for *H.350 directory*, except that if an endpoint presents an alias that is not in the H.350 directory, it will be allowed to register with that alias.
   - *Endpoint*: the aliases presented by the endpoint are used; any in the H.350 directory are ignored. If no aliases are presented by the endpoint, it is not allowed to register.

   The default is *H.350 directory*.

Note that if the authentication policy is *Do not check credentials* or *Treat as authenticated*, then the **Source of aliases for registration** setting is ignored and the aliases presented by the endpoint are used.

Configuring the LDAP server directory

The H.350 directory on the LDAP server should be configured to implement the *ITU H.350 specification*. It should store credentials for devices with which the VCS communicates, and the aliases of endpoints that will register with the VCS.

1. Download the required H.350 schemas from the VCS (**Configuration > Authentication > Devices > H.350 directory schemas**) and install them on the LDAP server.
2. Configure the directory with the aliases of endpoints that will register with the VCS.

   See LDAP Server Configuration for Device Authentication, page 374 for instructions on configuring LDAP servers.

Configuring the LDAP server settings

1. Go to **Configuration > Authentication > Devices > H.350 directory service**.

2. Configure the fields as follows:

Field	Description	Usage tips
H.350 device authentication	Enables or disables the use of an H.350 directory for device authentication.	The H.350 directory can be used in combination with other authentication mechanisms.
Source of aliases for registration	Determines how aliases are checked and registered.	See **H.350 directory authentication and registration process** above for a description of each setting. When **Source of aliases for registration** is *H.350 directory*, MCUs are treated as a special case. They register with the presented aliases and ignore any aliases in the H.350 directory. (This is to allow MCUs to additively register aliases for conferences.)
Server address	The IP address or FQDN (or server address, if a DNS **Domain name** has also been configured) of the LDAP server.	The LDAP server must have the H.350 schemas installed. If using TLS, the address entered here must match the CN (common name) contained within the certificate presented by the LDAP server.
FQDN address resolution	Defines how the LDAP **Server address** is resolved if it is specified as an FQDN. *Address record*: DNS A or AAAA record lookup. *SRV record*: DNS SRV record lookup. The default is *Address record*. If you use SRV records, ensure that *_ldap._tcp.<domain>* records use the standard LDAP port 389. The VCS 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.)	DNS SRV lookups enable the VCS to authenticate devices against multiple remote H.350 directory servers. This provides a seamless redundancy mechanism in the event of reachability problems to an H.350 directory server. 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.
Port	The IP port of the LDAP server.	LDAP connections use port *389*. Note that to do LDAPS with SRV records, VCS requires the AD server to support the STARTTLS extension.

Field	Description	Usage tips
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*.	When TLS is enabled, the LDAP server's certificate must be signed by an authority within the VCS'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 287 page.
Bind DN	The user distinguished name used by the VCS when binding to the LDAP server.	For example, uid=admin, ou=system
Bind password	The password used by the VCS when binding to the LDAP server.	
Base DN for devices	The area of the directory on the LDAP server to search for credential information. This should be specified as the Distinguished Name (DN) in the LDAP directory under which the H.350 objects reside.	For example, ou=H350,dc=example,dc=com

3. Click **Save**.

The current status of the connection to the specified LDAP server is displayed at the bottom of the page.

Using an H.350 Directory with Other Authentication Mechanisms

Local database authentication in combination with H.350 directory authentication

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

If an H.350 directory is configured, the VCS 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.

H.350 directory service 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. Devices that do not support NTLM will continue to receive a standard Digest challenge.

Using Active Directory Database (Direct)

Active Directory database (direct) authentication uses NTLM protocol challenges and authenticates credentials via direct access to an Active Directory server using a Kerberos connection.

It can be enabled at the same time as local database and H.350 directory service authentication. This is because NTLM authentication is only supported by certain endpoints. Therefore, for example, you could use the Active Directory (direct) server method for Jabber Video, and the local database or H.350 directory service authentication for the other devices that do not support NTLM.

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. Devices that do not support NTLM will continue to receive a standard Digest challenge.

Note that the VCS embeds NTLMv2 authentication protocol messages within standard SIP messages when communicating with endpoint devices, and uses a secure RPC channel when communicating with the AD Domain Controller. Users' Windows domain credentials and the AD domain administrator credentials are not stored on the VCS.

Configuration Prerequisites

Active Directory

- A username and password of an AD user account with either “account operator” or “administrator” access rights must be available for the VCS to use for joining and leaving the domain.
- Entries must exist in the Active Directory server for all devices that are to be authenticated through this method. Each entry must have an associated password.
- The device entries (in all domains) must be accessible by the user account that is used by VCS to join the domain. If the VCS is in a domain that is part of a forest, and there is trust between domains in the forest, the VCS can authenticate device entries from different domains providing the user account has appropriate rights to authenticate devices against the other domains.

Kerberos Key Distribution Center

The KDC (Kerberos Key Distribution Center) server must be synchronized to a time server.

DNS server

If a DNS name or DNS SRV name is used to identify the AD servers, a DNS server must be configured with the relevant details. (Note that the VCS must be configured to use a DNS server even if you are not using DNS / DNS SRV to specify the AD servers.)

VCS

- The VCS must be configured to use a DNS server (**System > DNS**).
  - The VCS’s **System host name** (**System > DNS**) must be 15 or fewer characters long.

    (Microsoft NetBIOS names are capped at 15 characters.)
  - When part of a cluster, ensure that each VCS peer has a unique **System host name**.
- Ensure that an NTP server (**System > Time**) has been configured and is active.
- If the connection is going to use TLS encryption, a valid CA certificate, private key and server certificate must be uploaded to the VCS.
- The VCS must be configured to challenge for authentication on the relevant zones and subzones:
  - The Default Zone (**Configuration > Zones > Zones**, then select Default Zone) must be configured with an **Authentication policy** of *Check credentials*. This ensures that provisioning requests (and any call requests from non-registered devices) are challenged.
  - The Default Subzone (**Configuration > Local Zone > Default Subzone**) – or the relevant subzones - must be configured with an **Authentication policy** of *Check credentials*. This ensures that registration, presence, phone book and call requests from registered devices are challenged.

Setting up your authentication policy to check credentials will affect any device that sends provisioning, registration, presence, phone book, and call requests to the VCS.

Endpoint

The PC on which Jabber Video runs must use settings which match the settings of the AD server.

Configuring the Connection to Active Directory Service (ADS)

The **Active Directory Service** page (**Configuration > Authentication > Devices > Active Directory Service**) is used to configure a connection to an Active Directory Service for device authentication of Jabber Video endpoints (version 4.2 or later).

Configuring the Active Directory Service Settings

To configure Active Directory (direct) and join the AD domain:

1. Go to **Configuration > Authentication > Devices > Active Directory Service**.
2. Configure the fields as follows:

Field	Description	Usage tips
Connect to Active Directory Service	Enables or disables the connection between the VCS and the Active Directory Service. When the connection is enabled, the VCS includes NTLM protocol challenges when authenticating endpoints, according to the **NTLM protocol challenges** setting.	Turning **Connect to Active Directory Service** to *Off* does not cause the VCS to leave the AD domain.
NTLM protocol challenges	Controls whether or not the VCS sends NTLM protocol challenges (in addition to Digest challenges) when authenticating devices over SIP. *Auto*: the VCS decides, based on the device type, whether to send NTLM challenges. *Off*: NTLM challenges are never sent. *On*: NTLM challenges are always sent. The default is *Auto*.	Normally, this should be set to *Auto*. If you are migrating from an existing authentication mechanism to ADS then select *Off* while the connection to the AD server is being configured; select *Auto* later, when you have an active connection and are ready to switch over to this authentication mechanism. Never use *On*, as this will send NTLM challenges to devices that may not support NTLM (and therefore they may crash or otherwise misbehave). The VCS must be connected to an Active Directory Service to send NTLM challenges.
AD domain	This must be the fully qualified domain name (FQDN) of the AD domain that the VCS will join. It must be entered in upper case, such as, EXAMPLE.COM.	Typically the domain is the same as the DNS name of the Kerberos server. Upper case entry is enforced due to case sensitivity issues with Active Directory.
Short domain name	The short domain name used by the VCS when it joins the AD domain.	It is also known as the NetBIOS domain name.

Field	Description	Usage tips
NetBIOS machine name (override)	By default the system uses the **System host name** as the NetBIOS machine name when joining the AD domain. If required, you can enter a different name here to override the default name.	An override must be specified if the **System host name** exceeds 15 characters.
Secure channel mode	Indicates if data transmitted from the VCS to an AD Domain Controller is sent over a secure channel. *Auto*: automatically adapts to the domain controller's settings. *Enabled*: always attempts to use a secure channel. *Disabled*: does not use a secure channel. The default is *Auto*.	You are recommended to use *Auto*.
Encryption	Sets the encryption to use for the LDAP connection to the Active Directory Service. *Off*: no encryption is used. *TLS*: TLS encryption is used. The default is *TLS*.	If encryption is set to TLS, a valid CA certificate, private key and server certificate must be uploaded to the VCS. Click **Upload a CA certificate file for TLS** (in the **Related tasks** section) to go to the Managing the Trusted CA Certificate List, page 287 page.
Clockskew	The maximum allowed clockskew (in seconds) between the VCS and the KDC before the Kerberos message is assumed to be invalid. The default is 300 seconds.	It should be kept in step with the clock skew setting on the KDC. Ensure that VCS and KDC are synchronized to time servers.
Use DNS SRV lookup to obtain Domain Controller addresses	*Yes* is the recommended setting. This means that VCS will use a DNS SRV lookup of the **AD domain** to obtain the address details of the AD domain controllers. If the lookup cannot provide the addresses then set this field to *No* and enter the IP address of the primary Domain Controller into the **Address 1** field that will be displayed.	

Field	Description	Usage tips
Use DNS SRV lookup to obtain Kerberos Key Distribution Center addresses	*Yes* is the recommended setting. This means that VCS will use a DNS SRV lookup of the **AD domain** to obtain the address details of the Kerberos Key Distribution Center servers. If the lookup cannot provide the addresses then set this field to *No* and enter the IP address of the primary Key Distribution Center servers into the **Address 1** field that will be displayed. Typically, **Port 1** can be left as its default value of 88.	Typically, the KDC addresses are the same as the Domain Controller addresses.
Username and **Password**	The AD domain administrator username and password. The password is case sensitive.	The domain administrator's credentials are required only when you attempt to join a domain. The VCS only needs to join the domain once, after which the connection can be enabled or disabled as required.

3. Click **Save** to store the configuration and join the AD domain.

   The VCS should join the AD domain. If you receive an error message, check the following:

   - the configuration settings on this page, including the username and password
   - the VCS's CA certificate, private key and server certificate
   - the **Status** area at the bottom of the Active Directory Service page for more information about the status of the connection to the AD domain

Note that:

- The domain administrator username and password are not stored in VCS; they are only required to join an AD domain (or to leave a domain).
- The VCS only needs to join the AD domain once, even if the connection to the Active Directory Service is disabled and turned back on again. The only time a join is needed again is if the VCS leaves the domain or needs to join a different domain.

Adding non-primary Domain Controllers and Kerberos Key Distribution Center servers (optional)

This procedure is only required if you are not using DNS SRV lookups of the **AD domain** to obtain the address details of the Domain Controller servers and the Kerberos Key Distribution Center servers.

1. Go to **Configuration > Authentication > Devices > Active Directory Service**.
2. Enter up to 4 further Domain Controller server addresses (up to 5 in total).
3. Enter up to 4 further Kerberos Key Distribution Center server addresses and port numbers (up to 5 in total).
4. Click **Save**.
5. If the VCS is part of a cluster, check that the configuration entered on the primary peer has been replicated to each other peer.

Clustered VCS Systems

In a clustered system, each VCS must join the AD domain separately. To do this:

On the primary peer:

1. Follow the instructions as above to configure Active Directory (direct) and join the AD domain.
2. Ensure that the primary peer has successfully joined the AD domain before continuing.

On each other peer in turn:

1. Go to **Configuration > Authentication > Devices > Active Directory Service**.
2. Check that the configuration entered on the primary peer has been replicated to the current peer.
3. Enter the AD domain administrator **Username** and **Password**.
   (These credentials are not stored by the VCS and so have to be entered each time.)
4. Click **Save**.

   The VCS should join the AD domain. If you receive an error message, check the following:

   - the configuration settings on this page, including the username and password
   - the VCS's CA certificate, private key and server certificate (CA certificate information is not replicated across cluster peers)

Enabling NTLM Authentication Challenges

When Active Directory details have been configured and the VCS has been joined into the AD domain, VCS can now be configured to challenge Jabber Video (4.2 or later) with NTLM authentication challenges.

1. Go to **Configuration > Authentication > Devices > Active Directory Service**.
2. Ensure that **NTLM protocol challenges** is set to *Auto*.

   Never use *On*, as this will send NTLM challenges to devices that may not support NTLM (and therefore they may crash or otherwise misbehave).
3. Click **Save** if required.
4. If the VCS is part of a cluster, check that any configuration changes entered on the primary peer have been replicated to each other peer.

Configuring Jabber Video and Testing Active Directory Database (Direct) Authentication

We recommend that you use a Jabber Video configuration that already authenticates successfully using either provisioning or VCS authentication. This means that Jabber Video's Advanced settings (**Internal Server**, **External Server** and **SIP Domain** entries) are correctly configured.

1. Sign in to Jabber Video:
2. In the **Username** field, configure `<AD Short Domain Name>\username`

   (this field is not case sensitive).
3. In the **Password** field, enter the password as configured in the Active Directory database for the chosen user.
4. Click **Sign in**.

A successful registration confirms that authentication of provisioning and registration of Jabber Video to VCS now works using Active Directory database (direct) authentication.

Ports

See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series configuration guides page.

SPNEGO

SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism) is a mechanism used by client applications when they seek to authenticate with a remote server. It allows the client and server to identify which authentication protocols they both support and decide which protocol to use.

By default the VCS uses SPNEGO when communicating with an AD Domain Controller. It can only be enabled or disabled through the CLI by using the command **`xConfiguration Authentication ADS SPNEGO`**.

Authenticating with External Systems

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

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

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

Zones and Neighbors

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

Video Network Fundamentals 127
Structuring the Dial Plan 128
About Zones 130
Configuring ICE Messaging Support 130
About the Local Zone and Subzones 132
Configuring the Default Zone 133
Configuring Default Zone Access Rules 134
Configuring Zones (Non-Default Zones) 135

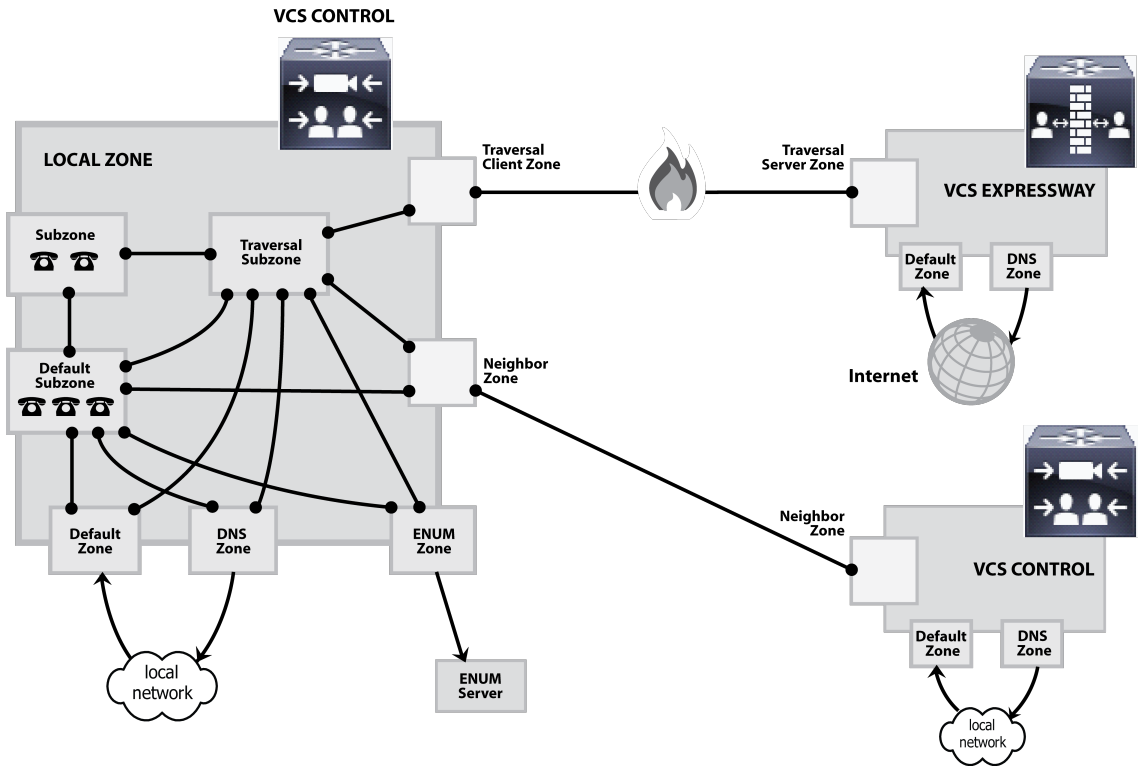
Video Network Fundamentals

This section summarizes the different parts of a video communications network that uses VCS, and the ways to connect them.

The most basic implementation is a single VCS connected to the internet with one or more endpoints registered to it. Depending on the size and complexity of your enterprise the VCS may be part of a network of endpoints, other VCSs and other network infrastructure devices, and with one or more firewalls between the VCS 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 following diagram shows the different subzones and zones for an example VCS deployment. It uses a VCS Control 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 VCSs and to the internet via particular types of zones.

Figure 11 Example network diagram



Structuring the Dial Plan

As you start deploying more than one VCS, 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 VCSs 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 VCSs. Each VCS is then configured with all the other VCS as neighbor zones. When one VCS receives a call for an endpoint which is not registered with it, it will send out a Location Request to all the other neighbor VCSs.

While conceptually simple, this sort of flat dial plan does not scale very well. Adding or moving a VCS requires changing the configuration of every VCS, 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 VCSs 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 VCS would be assigned an area code. When the VCSs 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 VCSs in your deployment. A hierarchical dial plan can simplify this.

Hierarchical Dial Plan

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

- The directory VCS is configured with each VCS as a neighbor zone, and search rules for each zone that have a **Mode** of *Alias pattern match* and the target VCS's prefix (as with the structured dial plan) as the **Pattern string**.
- Each VCS is configured with the directory VCS as a neighbor zone, and a search rule with a **Mode** of *Any alias* and a **Target** of the directory VCS.

Unless your deployment uses device authentication, there's no need to neighbor every VCS with each other. Adding a new VCS now only requires changing configuration on the new VCS and the directory VCS. It may be necessary to neighbor the VCSs to each other if you use device authentication (see below).

Failure of the directory VCS in this situation could cause significant disruption to communications. Consideration should be given to the use of clustering for increased resilience.

H.323 calls and optimal call routing

For H.323 calls, if *Optimal* call routing is enabled you must ensure that all search rules are configured with a **Source** of *Any*. If the **Source** is configured to *All zones*, H.323 calls will fail to connect. This is because the H.323 SETUP message, having followed the optimized route established by the original LRQ or ARQ, will appear to the target VCS as coming from an unknown zone. SIP calls, however, are successfully routed if the search rule **Source** is *All zones* (because in SIP the search and call setup is combined into one message).

Hierarchical dial plan (directory VCS) deployments and device authentication

See Hierarchical Dial Plans and Authentication Policy, page 112 for important information about how to configure your authentication policy within a hierarchical dial plan.

About Zones

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

- Control through links whether calls can be made between your local subzones and these other zones
- Manage the bandwidth of calls between your local subzones and endpoints in other zones
- Search for aliases that are not registered locally
- Control the services available to endpoints within that zone by setting up its authentication policy
- Control the media encryption and ICE capabilities for SIP calls to and from a zone

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

- *Neighbor*: a connection to a neighbor system of the local VCS.
- *Traversal client*: the local VCS is a traversal client of the system being connected to, and there is a firewall between the two.
- *Traversal server*: the local VCS is a traversal server for the system being connected to, and there is a firewall between the two.
- *ENUM*: the zone contains endpoints discoverable by ENUM lookup.
- *DNS*: the zone contains endpoints discoverable by DNS lookup.
- *Unified Communications traversal*: a traversal client or traversal server zone used for Unified Communications features such as mobile and remote access or Jabber Guest.

The VCS also has a pre-configured Default Zone.

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

Automatically generated neighbor zones

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

- A VCS Control automatically generates neighbor zones between itself and each discovered Unified CM node when the system is configured for mobile and remote access.
- A VCS automatically generates a neighbor zone named "To Microsoft destination via B2BUA" when the 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 and per-subzone configuration setting that controls how the VCS supports ICE messages to and from SIP devices within that zone or subzone.

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

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

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

Note that:

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

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 VCS. This allows you to configure your system so that, for example, all traffic arriving or leaving a VCS Expressway 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 VCS).

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 VCS. Media encryption is purely dependent on the target system/endpoint requests. This is the default behavior and is equivalent to how the VCS 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 VCS.

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

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

Configuring the B2BUA for Media Encryption

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

About the Local Zone and Subzones

The collection of all devices registered with the VCS 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 VCS, 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 VCS also has two special types of subzones:

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

Bandwidth management

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

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

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

Registration, authentication and media encryption policies

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

See Configuring Subzones, page 219 for more information about how to configure these settings.

Local Zone searches

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

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

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 VCS comes preconfigured with the Default Zone and default links between it and both the Default Subzone and the Traversal Subzone. The Default Zone cannot be deleted.

Default Zone Settings

By configuring the Default Zone you can control how the VCS 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 VCS challenges incoming messages to the Default Zone.	See Authentication Policy Configuration Options, page 102 for more information.
Media encryption mode	The **Media encryption mode** setting controls the media encryption capabilities for SIP calls flowing through the Default Zone.	See Configuring Media Encryption Policy, page 131 for more information.
ICE support	Controls whether ICE messages are supported by the devices in this zone.	See Configuring ICE Messaging Support, page 130 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 VCS 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 7 Default Zone Access Rule Parameters

Field	Description	Usage tips
Name	The name assigned to the rule.	
Description	An optional free-form description of the rule.	
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 expression.	You can test whether a pattern matches a particular name by using the **Check pattern** tool (**Maintenance > Tools > Check pattern**).
Pattern string	The pattern against which the name is compared.	
Action	The action to take if the certificate matches this access rule. *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 zones configured on the VCS, 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, eg. DNS and ENUM zones)
- *Failed*: the protocol is enabled for the zone but its connection has failed
- *Checking*: the protocol is enabled for the zone and the system is currently trying to establish a connection

You configure a zone on the local VCS to neighbor with another system (such as another VCS 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:

- *Neighbor*: connects the local VCS to a neighbor system
- *Traversal client*: connects the local VCS to a traversal server
- *Traversal server*: connects the local VCS Expressway to a traversal client
- *ENUM*: enables ENUM dialing via the local VCS
- *DNS*: enables the local VCS to locate endpoints and other systems by using DNS lookups
- *Unified Communications traversal*: a traversal client or traversal server zone used for Unified Communications features such as mobile and remote access or Jabber Guest.
- *Hybrid*: 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, page 130 for more information about zones and the different zone types.

The VCS also has a preconfigured 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 VCS 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. In software versions prior to X5.1 a connection could be established if one system was configured to use TLS and the other used TCP. Any connection failures due to transport type mismatches are recorded in the Event Log.

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

Configuring Neighbor Zones

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

You create a neighbor relationship with the other system by adding it as a neighbor zone on your local VCS. 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 VCS and the neighbor zone.

Notes:

- Neighbor zone relationship definitions are one-way; adding a system as a neighbor to your VCS does not automatically make your VCS 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 8 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 VCS. 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 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 VCS.	Must be the same port number as that configured on the neighbor system as its H.323 UDP port. If the neighbor is a VCS acting as a gatekeeper, this corresponds to the **Registration UDP Port** on **Configuration > Protocols > H.323** page.
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 VCS.	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).

Table 8 Neighbor zone settings (continued)

Field	Description	Usage tips
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 VCS performs X.509 certificate checking against the neighbor system when communicating over TLS.	If the neighbor system is another VCS, both systems can verify each other's certificate (known as mutual authentication). See TLS Certificate Verification of Neighbor Systems, page 156 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 VCS 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 VCS for SIP calls (including interworked calls) to and from this zone.	See Configuring Media Encryption Policy, page 131 for more information.
ICE support	Controls whether ICE messages are supported by the devices in this zone.	See Configuring ICE Messaging Support, page 130 for more information.
Multistream mode	Controls whether the VCS B2BUA allows multistream calls to be negotiated between calling parties. *On*: VCS allows the calling parties to negotiate and set up a multistream call through this zone *Off*: VCS 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.
Authentication section:		

Table 8 Neighbor zone settings (continued)

Field	Description	Usage tips
Authentication policy	Controls how the VCS authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected.	The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. See Authentication Policy Configuration Options, page 102 for more information.
SIP authentication trust mode	Controls whether authenticated SIP messages (ones containing a P-Asserted-Identity header) from this zone are trusted without further challenge.	See SIP Authentication Trust, page 105 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 VCS does the lookup for the addresses. ■ *Service record* produces a field to enter the Service Domain. When you click **Save**, the VCS 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 VCS 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 VCS can register against is 15. 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.
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 a VCS cluster, in which case you must specify all of the peers in the cluster ■ the neighbor is a resilient non-VCS system, in which case you must enter the addresses of all of the resilient elements in that system	Calls to a VCS cluster are routed to whichever peer in that neighboring cluster has the lowest resource usage. See Neighboring Between VCS Clusters, page 167 for more information. For connections to non-VCS systems, the VCS uses a round-robin selection process to decide which peer to contact if no resource usage information is available.
Advanced section:		

Table 8 Neighbor zone settings (continued)

Field	Description	Usage tips
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: ▪ *Cisco Unified Communications Manager* ▪ *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, page 150 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 VCS Deployment Guide* for more information about the *Cisco Unified Communications Manager* profiles.

Configuring Traversal Client Zones

To traverse a firewall, the VCS must be connected with a traversal server (typically, a VCS Expressway). In this situation your local VCS is a traversal client, so you create a connection with the traversal server by creating a traversal client zone on your local VCS. 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 VCS 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 VCS and the traversal server.

Note: An NTP server 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, page 47.

Traversal client zone settings

The configurable options for a traversal client zone are described in the table.

Table 9 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 VCS. 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 Hop counts section for more information). This field specifies the hop count to use when sending a search request to this particular zone.	If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used.
Connection credentials section:		
Username and **Password**	Traversal clients must always authenticate with traversal servers by providing their authentication credentials. Each traversal client zone must specify a **Username** and **Password** to be used for authentication with the traversal server.	Multiple traversal client zones can be configured, each with distinct credentials, to connect to one or more service providers.
H.323 section:		
Mode	Determines whether H.323 calls are allowed to and from the traversal server.	
Protocol	Determines which of the two firewall traversal protocols (*Assent* or *H.460.18*) to use for calls to the traversal server.	See Configuring Ports for Firewall Traversal, page 52 for more information.
Port	The port on the traversal server to use for H.323 calls to and from the local VCS.	For firewall traversal to work via H.323, the traversal server must have a traversal server zone configured on it to represent this VCS, 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 VCS. 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 VCS, 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*.	

Table 9 Traversal client zone settings (continued)

Field	Description	Usage tips
TLS verify mode	Controls X.509 certificate checking and mutual authentication between this VCS and the traversal server when communicating over TLS.	See TLS Certificate Verification of Neighbor Systems, page 156 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 VCS 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 VCS for SIP calls (including interworked calls) to and from this zone.	See Configuring Media Encryption Policy, page 131 for more information.
ICE support	Controls whether ICE messages are supported by the devices in this zone.	See Configuring ICE Messaging Support, page 130 for more information.
Multistream mode	Controls whether the VCS B2BUA allows multistream calls to be negotiated between calling parties. *On*: VCS allows the calling parties to negotiate and set up a multistream call through this zone *Off*: VCS 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 VCS 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.	

Table 9 Traversal client zone settings (continued)

Field	Description	Usage tips
SIP parameter preservation	Determines whether the VCS'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.
Authentication section:		
Authentication policy	Controls how the VCS authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains.	See Authentication Policy Configuration Options, page 102 for more information.
Accept delegated credential checks	Controls whether this zone accepts delegated authentication requests.	See Configuring Delegated Credential Checking (SIP Only), page 106 for more information.
Client settings section:		
Retry interval	The interval in seconds with which a failed attempt to establish a connection to the traversal server should be retried.	
Location section:		
Peer 1 to Peer 6 address	The IP address or FQDN of the traversal server. If the traversal server is a VCS Expressway cluster, this should include all of its peers.	See Neighboring Between VCS Clusters, page 167 for more information.

Configuring Traversal Server Zones

A VCS Expressway can act as a traversal server, providing firewall traversal on behalf of traversal clients (a VCS Control).

For firewall traversal to work, the traversal server (VCS Expressway) must have a special type of two-way relationship with each traversal client. To create this connection between a VCS Expressway and a VCS Control, see Configuring a Traversal Client and Server, page 50. For full details on how traversal client zones and traversal server zones work together to achieve firewall traversal, see About Firewall Traversal, page 47.

Note: You must synchronize with an NTP server to make sure that traversal zones to work.

After you have neighbored with the traversal client you can:

- provide firewall traversal services to the traversal client
- query the traversal client about its endpoints
- apply transforms to any queries before they are sent to the traversal client
- control the bandwidth used for calls between your local VCS 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 10 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 VCS. 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 Hop counts section for more information). This field specifies the hop count to use when sending a search request to this particular zone.	If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used.
Connection credentials section:		
Username	Traversal clients must always authenticate with traversal servers by providing their authentication credentials. The authentication username is the name that the traversal client must provide to the VCS Expressway. (It is configured as the connection credentials **Username** in its traversal client zone.)	There must also be an entry in the VCS Expressway'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, page 52 for more information.
Port	The port on the local VCS Expressway to use for H.323 calls to and from the traversal client.	

Table 10 Traversal server zone configuration reference (continued)

Field	Description	Usage tips
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 VCS Expressway 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*.	
Unified Communications services	Controls whether this traversal zone provides Unified Communications services, such as mobile and remote access.	If enabled, this zone must also be configured to use TLS with **TLS verify mode** enabled. This setting only applies when Unified Communications mode is set to *Mobile and remote access*.
TLS verify mode and **subject name**	Controls X.509 certificate checking and mutual authentication between this VCS and the traversal client. If **TLS verify mode** is enabled, a **TLS verify subject name** must be specified. This is the certificate holder's name to look for in the traversal client's X.509 certificate.	If the traversal client is clustered, the **TLS verify subject name** must be the FQDN of the cluster. See TLS Certificate Verification of Neighbor Systems, page 156 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 VCS 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 VCS for SIP calls (including interworked calls) to and from this zone.	See Configuring Media Encryption Policy, page 131 for more information.
ICE support	Controls whether ICE messages are supported by the devices in this zone.	See Configuring ICE Messaging Support, page 130 for more information.

Table 10 Traversal server zone configuration reference (continued)

Field	Description	Usage tips
Multistream mode	Controls whether the VCS B2BUA allows multistream calls to be negotiated between calling parties. *On*: VCS allows the calling parties to negotiate and set up a multistream call through this zone *Off*: VCS 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 VCS 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 VCS'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.
Authentication section:		

Table 10 Traversal server zone configuration reference (continued)

Field	Description	Usage tips
Authentication policy	Controls how the VCS authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains.	See Authentication Policy Configuration Options, page 102 for more information.
UDP / TCP probes section:		
UDP retry interval	The frequency (in seconds) with which the client sends a UDP probe to the VCS Expressway 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 VCS Expressway during call setup.	
UDP keep alive interval	The interval (in seconds) with which the client sends a UDP probe to the VCS Expressway 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 VCS Expressway 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 VCS Expressway during call setup.	
TCP keep alive interval	The interval (in seconds) with which the traversal client sends a TCP probe to the VCS Expressway 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 VCS and each group of ENUM endpoints

Full details of how to use and configure ENUM zones are given in the About ENUM Dialing, page 205 section.

The configurable options for an ENUM zone are described in the table.

Table 11 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 VCS. 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 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 VCS and each group of DNS endpoints. See About URI Dialing, page 198 for more information on configuring and using DNS zones.

The configurable options for a DNS zone are described in the table.

Table 12 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 VCS. 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 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.	

Table 12 DNS zone settings (continued)

Field	Description	Usage tips
TLS verify mode and **subject name**	Controls whether the VCS performs X.509 certificate checking against the destination system server returned by the DNS lookup. If **TLS verify mode** is enabled, a **TLS verify subject name** must be specified. This is the certificate holder's name to look for in the destination system server's X.509 certificate.	This setting only applies if the DNS lookup specifies TLS as the required protocol. If TLS is not required then the setting is ignored. See TLS Certificate Verification of Neighbor Systems, page 156 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 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 VCS from attempting to map inbound TLS connections to this zone.
Fallback transport protocol	The transport type to use for SIP calls from the DNS zone, when DNS NAPTR records and SIP URI parameters do not provide the preferred transport information. The default is *UDP* (if enabled).	
Media encryption mode	Controls the media encryption policy applied by the VCS for SIP calls (including interworked calls) to the internet.	See Configuring Media Encryption Policy, page 131 for more information.
ICE support	Controls whether ICE messages are supported by the devices in this zone.	See Configuring ICE Messaging Support, page 130 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.

Table 12 DNS zone settings (continued)

Field	Description	Usage tips
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		
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 VCS. *On*: pre-authenticated messages are trusted without further challenge and subsequently treated as authenticated within the VCS. 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 VCS 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 VCS believing the search was successful and forwarding calls to this zone, and the call will fail. *On*: the VCS queries for A or AAAA records. If any are found, the VCS will not then query any lower priority zones. *Off*: (default) the VCS will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.	

Table 12 DNS zone settings (continued)

Field	Description	Usage tips
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, page 150 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. It is for connecting the VCS Expressway to Cisco Webex. You can use this zone to enable Cisco Webex Hybrid Call Service or Webex Meetings, or both.

To enable this zone:

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.
3. Select *Webex* from the **Type** dropdown.

   The VCS creates the new zone. It has a pre-configured name and other 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.

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 VCS 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 VCS believing the search was successful and forwarding calls to this zone, and the call will fail. *On*: the VCS queries for A or AAAA records. If any are found, the VCS will not then query any lower priority zones. *Off*: the VCS will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.	Off	DNS

Setting	Description	Default	Zone types
Monitor peer status	Specifies whether the VCS 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 VCS 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 VCS 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
Automatically respond to SIP searches	Determines what happens when the VCS 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

Setting	Description	Default	Zone types
Send empty INVITE for interworked calls	Determines whether the VCS 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 that 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.	On	Neighbor DNS
SIP parameter preservation	Determines whether the VCS'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
SIP poison mode	*On*: SIP requests sent to systems located via this zone are "poisoned" such that if they are received by this VCS again they will be rejected. *Off*: SIP requests sent out via this zone that are received by this VCS again will not be rejected; they will be processed as normal.	Off	Neighbor Traversal client Traversal server DNS

Setting	Description	Default	Zone types
SIP encryption mode	Determines whether or not the VCS 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 VCS.	Forward	Neighbor
Meeting Server load balancing	From X8.11, Cisco TelePresence Video Communication Server 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*: VCS B2BUA processes the INVITEs from the Meeting Server. Required to enable load balancing for endpoints that are registered to Unified CM or this VCS, or to a neighboring VCS or Expressway. *Off*: VCS B2BUA does not process the INVITEs from the Meeting Server.	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 VCS 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 VCS searches for SIP endpoints when interworking an H.323 call. *Options*: the VCS sends an OPTIONS request. *Info*: the VCS 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 VCS uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone. *IP*: uses the VCS's IP address. *Hostname*: uses the VCS'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	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 poison mode	Off	Off	Off	Off	Off	Off
SIP encryption mode	Auto	Auto	Auto	Auto	Auto	Auto
SIP REFER mode	Forward	Forward	Forward	Forward	Forward	Forward
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

Setting	Cisco Unified CM, 9.x or later	Cisco Unified CM, 8.6.1 or 8.6.2	Cisco Unified CM	Nortel Communication Server 1000	Infrastructure device	Default
SIP UDP/IX filter mode	On	On	Off	On	On	On
SIP record route address type	IP	IP	IP	IP	IP	IP
SIP Proxy-Require header strip list	<blank>	<blank>	<blank>	"com.nortelnetworks.firewall"	<blank>	<blank>

More information about configuring a SIP trunk between VCS and Unified CM:

See *Cisco VCS and CUCM via SIP Trunk Deployment Guide* on the VCS configuration guides page.

TLS Certificate Verification of Neighbor Systems

When a SIP TLS connection is established between a VCS and a neighbor system, the VCS 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 that for traversal server and DNS zones, the FQDN or IP address of the connecting traversal client is not configured, so the required certificate holder's name is specified separately.

If the neighbor system is another VCS, 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 VCS acts both as a client and as a server and therefore you must ensure that each VCS's certificate is valid both as a client and as a server.

See About Security, page 286 for more information about certificate verification and for instructions on uploading the VCS's server certificate and uploading a list of trusted certificate authorities.

Configuring a Zone for Incoming Calls Only

To configure a zone so that it is never sent an alias search request (for example if you only want to receive incoming calls from this zone), do not define any search rules that have that zone as its target.

In this scenario, when viewing the zone, you can ignore the warning indicating that search rules have not been configured.

Clustering and Peers

This section describes how to set up a cluster of VCS peers. Clustering is used to increase the capacity of your VCS deployment and to provide resiliency.

About Clusters 157

License Usage Within a Cluster 159

Managing Clusters and Peers 160

Troubleshooting Cluster Replication Problems 167

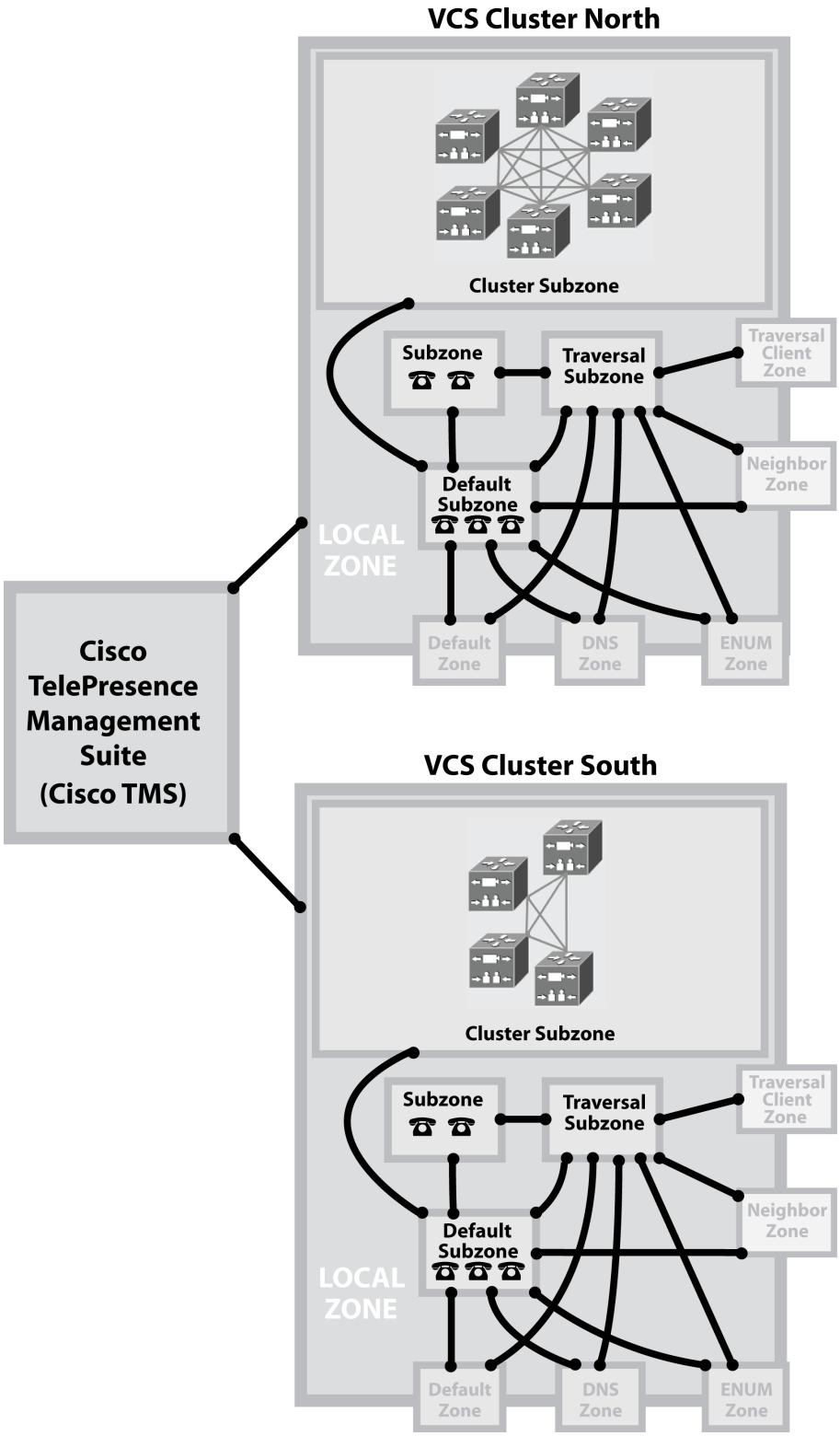
About Clusters

A VCS can be part of a cluster of up to six VCSs. Each VCS in the cluster is a peer of every other VCS 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 VCS deployment compared with a single VCS.
- Resilience. Provide redundancy while a VCS is in 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 VCSs 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 VCS Local Zone, as shown in this example:



About the configuration primary

All peers in a cluster must have identical configuration for subzones, zones, links, pipes, authentication, bandwidth control and Call Policy. To achieve this, you define a cluster name and nominate one peer as the configuration

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

You should only make configuration changes on the primary VCS.

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

Any changes made on other peers are not reflected across the cluster, and will be overwritten the next time the primary's configuration is replicated across the peers. The only exceptions to this are some peer-specific configuration items.

You may need to wait up to one minute before changes are updated across all peers in the cluster.

Secure communication between peers

The VCS uses TLS (Transport Layer Security) to secure the communications between cluster peers. Peers identify each other using certificates; if you wish to enforce TLS verification, a VCS must have a certificate that is trusted by all other peers, or it will be unable to join the cluster.

DNS resolution of peers

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

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

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

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

License Usage Within a Cluster

These license types are pooled for use by any peer in a cluster, irrespective of which peer the licenses are installed on:

- Traversal or non-traversal call licenses
- TURN relay licenses

You can cluster up to 6 VCS systems to increase capacity by a maximum factor of 4. For Small VMs, clustering is only for redundancy and not for scale and **there is no capacity gain from clustering**.

If a cluster peer becomes unavailable, the shareable licenses installed on that peer remain available to the rest of the cluster peers for two weeks from the time the cluster lost contact with the peer. This will maintain the overall license capacity of the cluster – however, note that each peer is limited by its physical capacity. After this two week period, the licenses associated with the unavailable peer are removed from the cluster. To maintain the same capacity for the cluster, ensure that the problem with the peer is resolved, or new option keys are installed on another peer in the cluster.

The maximum number of licenses that each VCS system can *use* depends on the type of appliance or VM:

Table 13 Maximum licenses that a peer can use

	Small / Medium systems	Large‡ / CE500/ CE1000/ CE1100/ CE1200 systems
Traversal calls	150†	500
Non-traversal calls	750	750
Registrations	2500	5000 (2500 for MRA registrations)
TURN relays*	1800	6000

‡ From X8.10, the requirement to have a 10 Gbps NIC to achieve the scalability of a Large system is removed. Subject to your bandwidth constraints, it is possible to have the capacity of a Large system with a 1 Gbps NIC.
The CE1200 is not available for the Cisco VCS, only for the Cisco Expressway Series.

† This is the maximum number of licenses the system can *use*. This limit specifically applies to the case where a peer becomes unavailable and the other peers must use that peer's licenses to honor the cluster's overall capacity. This is not intended as a production capacity limit, only as a temporary measure to allow the affected peer to be returned to normal service. **We strongly discourage installing more than 100 licenses on any Medium-capacity platform, or more than 75 licenses on a Small-capacity platform.**

* On a Large system, the total TURN capacity of 6000 relays is spread evenly across 6 ports. Each port is limited to handling 1000 relays. On a Small or Medium system, a single TURN port handles up to 1800 relays.

Note that each VCS comes pre-installed with 2,500 registration licenses, and that registration licenses are not shared across a cluster. If you want more than the default 2500 licenses, you need to install an option key for the number of additional registrations required (up to the maximum limit supported for the system).

To see a summary of all call, registration, and TURN relay licenses installed on each cluster peer, go to the **Option keys** page and scroll down to **Current licenses**.

Intracluster calls

This section describes license usage when endpoints are registered to different peers in the same cluster.

If the call media does not traverse the cluster peers:

- A SIP call between the endpoints consumes two non-traversal call licenses (one on each node).
- An H.323 call between the endpoints consumes one non-traversal license (on the node where the endpoint that initiated the call is registered).

If the call media traverses the cluster peers or if either endpoint is registered with ASSENT or H.460 capability:

- A SIP call between the endpoints consumes two traversal call licenses (one on each node).
- An H.323 call between the endpoints consumes two traversal call licenses (one on each node).

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 VCS 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 VCS belongs, and identifies the configuration primary peer.

Cluster configuration

- The **Cluster name** is used to identify one cluster of VCSs from another. Set it to the fully qualified domain name (FQDN) used in SRV records that address this VCS cluster, for example `cluster1.example.com`.

  The FQDN can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. A cluster name is required if FindMe is enabled.
- All peers must agree on which is the **Configuration primary**. Use the same number on each peer, and keep the **Peer N address** list in the same order on all peers.
- All peers must use the same IP version. Set the **Cluster IP version** to the same value on all peers.
- All peers must use the same **TLS verification mode**. Choose *Enforce* for better security, but be aware that the peers must be able to verify each others' certificates against their trusted CAs.
- The **Cluster Address Mapping** option allows you to map VCS Expressway peers' FQDNs to their private IP addresses. Cluster address mapping allows you to enforce TLS clustering of peers in an isolated network, because it does not require the use of the public DNS and the peers' public IP addresses.

Other configuration for the cluster

You should only make configuration changes on the primary VCS.

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

Any changes made on other peers are not reflected across the cluster, and will be overwritten the next time the primary's configuration is replicated across the peers. The only exceptions to this are some peer-specific configuration items.

You may need to wait up to one minute before changes are updated across all peers in the cluster.

Adding and Removing Peers From a Cluster

After a cluster has been set up you can add new peers to the cluster or remove peers from it (see See *Expressway Cluster Creation and Maintenance Deployment Guide* on the VCS Configuration Guides page.

Note that:

- Systems that are configured as peers must not also be configured as neighbors to each other, and vice versa.
- If peers are deployed on different LANs, there must be sufficient connectivity between the networks to ensure a low degree of latency between the peers.
- Cluster peers can be in separate subnets. Peers communicate with each other using H.323 messaging, which can be transmitted across subnet boundaries.
- Deploying all peers in a cluster on the same LAN means they can be configured with the same routing information such as local domain names and local domain subnet masks.

- To remove a peer from the cluster you must clear all peer address fields on that peer, save, then restart.

  CAUTION: If you clear all the peer address fields from the clustering page and save the configuration, then the VCS 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.

  The VCS displays a banner to remind you that it is pending a factory reset.

  If you need to prevent the factory reset, restore the clustering peer address fields exactly as they were. Replace the original peer addresses in the same order, and then save the configuration to clear the banner and prevent the reset.

Changing the Primary Peer

Typically you only need to change the **Configuration primary** in the following cases:

- If the original primary peer fails.
- To take the primary VCS unit out of service.

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 change the primary peer, log in to every other VCS in the cluster and change the configuration primary on each peer, as follows:

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

You may see alarms raised on some peers about inconsistent primary peer configuration. These alarms will be lowered when every peer in the cluster is configured with the new primary.

No further steps are required if you are using FQDNs, with valid cluster address mapping configured.

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.

Peer-Specific Items in Clustered Systems

Most items of configuration are applied via the primary peer to all peers in a cluster. However, the following items (marked with a † on the web interface) must be specified separately on each cluster peer.

Note: You should not modify configuration data that applies to all peers on any peer other than the primary peer. At best it will result in the changes being overwritten from the primary; at worst it will cause cluster replication to fail.

Cluster configuration (System > Clustering)

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

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

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

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 that the IP protocol is applied to all peers, because each peer must support the same protocols.

IP static routes (System > Network interfaces > Static routes)

Any static routes you add are peer-specific and you may create different routes on different peers if required. If you want all peers in the cluster to be able to use the same static route, you must create the route on each peer.

System name (System > Administration)

The **System name** must be different for each peer in the cluster.

DNS servers and DNS host name (System > DNS)

DNS servers are specific to each peer. Each peer can use a different set of DNS servers.

The **System host name** and **Domain name** are specific to each peer.

NTP servers and time zone (System > Time)

The **NTP servers** are specific to each peer. Each peer may use one or more different NTP servers.

The **Time zone** is specific to each peer. Each peer may have a different local time.

SNMP (System > SNMP)

SNMP settings are specific to each peer. They can be different for each peer.

Logging (Maintenance > Logging)

The Event Log and Configuration Log on each peer only report activity for that particular VCS. The **Log level** and the list of **Remote syslog servers** are specific to each peer. We recommend that you set up a remote syslog server to which the logs of all peers can be sent. This allows you to have a global view of activity across all peers in the cluster. See the logging section for further details.

Security certificates (Maintenance > Security)

The trusted CA certificate, server certificate and certificate revocation lists (CRLs) used by the VCS must be uploaded individually per peer.

Administration access (System > Administration)

The following system administration access settings are specific to each peer:

- Serial port / console
- SSH service
- Web interface (over HTTPS)
- Redirect HTTP requests to HTTPS
- Automated protection service

Option keys (Maintenance > Option keys)

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

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

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

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

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 LRQ, ARQ or 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 VCS.

Peers are periodically queried to ensure they are still functioning. To prevent delays during call setup, any nonfunctioning peers do not receive LRQs.

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 VCS, 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 VCS 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 VCS 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 VCS 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 VCS manages bandwidth, see the bandwidth control section.

Cluster Upgrades, Backup and Restore

Upgrading a cluster

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

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

Backing up a cluster

Use the backup and restore process to save cluster configuration information. The backup process saves *all* configuration information for the cluster, regardless of the VCS used to make the backup.

Caution: Do not take VMware snapshots of Cisco TelePresence Video Communication Server 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 a VCS that is part of a cluster. As described here, first remove the VCS peer from the cluster. Then do the restore. (After the restore you need to build a new cluster.)

1. Remove the VCS peer from the cluster so that it becomes a standalone VCS.
2. Restore the configuration data to the standalone VCS. See Restoring a Previous Backup, page 312 for details.
3. Build a new cluster using the VCS that now has the restored data.
4. Take each of the other peers out of their previous cluster and add them to the new cluster. See Setting Up a Cluster, page 160 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 Presence

Clustering supports the use of Presence.

- All peers in the cluster must have identical SIP domain, Presence Server and Presence User Agent (PUA) configuration.
- If peers in the cluster have the PUA enabled, each peer publishes information about its own local registrations.

This information is routed to a Presence Server authoritative for the cluster's domain.

- If peers have the Presence Server enabled, the Presence database is replicated across all peers in the cluster.

When viewing presence status on a peer in a cluster:

- **Publishers** shows all presentities across the cluster for whom presence information is being published.
- **Presentities** shows any presentity for whom a subscription request has been received on the local VCS only.
- **Subscribers** shows each endpoint from which a subscription request has been received on the local VCS only.

Clustering and Cisco TMS

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

From X8.1 onwards you must use Cisco TelePresence Management Suite Provisioning Extension.

Size limitations for clusters and provisioning

A VCS cluster of any size supports up to:

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

Note: Even if the device registration capacity limit 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 VCS 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 VCSs are clustered together, a new subzone is created within the cluster's Local Zone. This is the Cluster Subzone (see the diagram in the About Clusters, page 157 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 VCS for the Branch Office, which is neighbored to a cluster of 4 VCSs at the Head Office. A user in the Branch Office calls Endpoint A in the Head Office. Endpoint A is registered in the Default Subzone to Peer 1. The call is received by Peer 2, as it has the lowest resource usage at that moment. Peer 2 then searches for Endpoint A within the cluster's Local Zone, and finds that it is registered to Peer 1. Peer 2 then forwards the call to Peer 1, which forwards it to Endpoint A. In this case, on Peer 2 the call route will be shown as **Branch Office -> Default Subzone -> Cluster Subzone**, and on Peer 1 as **Cluster Subzone -> Default Subzone**.

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

Neighboring Between VCS Clusters

You can neighbor your local VCS (or VCS cluster) to a remote VCS cluster; this remote cluster could be a neighbor, traversal client, or traversal server to your local VCS. In this case, when a call is received on your local VCS and is passed via the relevant zone to the remote cluster, it will be routed to whichever peer in that neighboring cluster has the lowest resource usage. That peer will then forward the call as appropriate to one of its:

- locally registered endpoints (if the endpoint is registered to that peer)
- peers (if the endpoint is registered to another peer in that cluster)
- external zones (if the endpoint has been located elsewhere)

For Expressway: Lowest resource usage is determined by comparing the number of available media sessions (maximum – current use) on the peers, and choosing the peer with the highest number. Peers that are in maintenance mode are not considered.

For VCS: Lowest resource usage is determined by comparing the number of available traversal calls (maximum – current use) on the peers, and choosing the peer with the highest number. Peers that are in maintenance mode are not considered.

When configuring a connection to a remote cluster, you create a single zone and configure it with details of all the peers in the cluster. Adding this information to the zone ensures that the call is passed to that cluster regardless of the status of the individual peers.

You also need to enter the address of all peers in the remote cluster when the connection is via a **neighbor** or **traversal client** zone. You do not do this for **traversal server** zones, as these connections are not configured by specifying the remote system's address.

Note: Systems that are configured as peers must **not** also be configured as neighbors to each other, and vice versa.

Neighboring your clusters

To neighbor your local VCS (or VCS cluster) to a remote VCS cluster, you create a single zone to represent the cluster and configure it with the details of all the peers in that cluster:

1. On your local VCS (or, if the local VCS is a cluster, on the primary peer), create a zone of the appropriate type. This zone will represent the connection to the cluster.
2. In the **Location** section, enter the IP address or FQDN of each peer in the remote cluster in the **Peer 1** to **Peer 6** address fields.

Note that:

- Ideally you should use FQDNs in these fields. Each FQDN must be different and must resolve to a single IP address for each peer. With IP addresses, you may not be able to use TLS verification, because many CAs will not supply certificates to authenticate an IP address.
- The order in which the peers in the remote VCS cluster are listed here does not matter.
- Whenever you add an extra VCS to a cluster (to increase capacity or improve redundancy, for example) you will need to modify any VCSs which neighbor to that cluster to let them know about the new cluster peer.

Troubleshooting Cluster Replication Problems

Cluster replication can fail for a variety of reasons. This section describes the most common problems and how to resolve them. For more detailed information:

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

Some peers have a different primary peer defined

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

Unable to reach the cluster configuration primary peer

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

- Network access problems
- VCS 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 VCSs

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 VCS peer's configuration and force it to update its configuration from the primary VCS.

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

Incorrect IP to FQDN mappings

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

Firewall preventing the cluster communicating

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

Dial Plan and Call Processing

This section provides information about the pages that appear under the Calls, Dial plan, Transforms and Call Policy sub-menus of the **Configuration** menu. These pages are used to configure the way in which the VCS receives and processes calls.

Call Routing Process 169
Configuring Hop Counts 172
Configuring Dial Plan Settings 172
About Transforms and Search Rules 173
Example Searches and Transforms 180
Configuring Search Rules to Use an External Service 189
About Call Policy 191
Supported Address Formats 196
Dialing by IP Address 197
About URI Dialing 198
About ENUM Dialing 205
Configuring DNS Servers for ENUM and URI Dialing 210
Configuring Call Routing and Signaling 210
Identifying Calls 211
Disconnecting Calls 212

Call Routing Process

One of the functions of the VCS is to route calls to their appropriate destination. It does this by processing incoming search requests in order to locate the given target alias. These search requests are received from:

- locally registered endpoints
- neighboring systems, including neighbors, traversal clients and traversal servers
- endpoints on the public internet

There are a number of steps involved in determining the destination of a call, and some of these steps can involve transforming the alias or redirecting the call to other aliases.

It is important to understand the process before setting up your dial plan so you can avoid circular references, where an alias is transformed from its original format to a different format, and then back to the original alias. The VCS 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 VCS determines the destination of a call

The process followed by the VCS when attempting to locate a destination endpoint is described below.

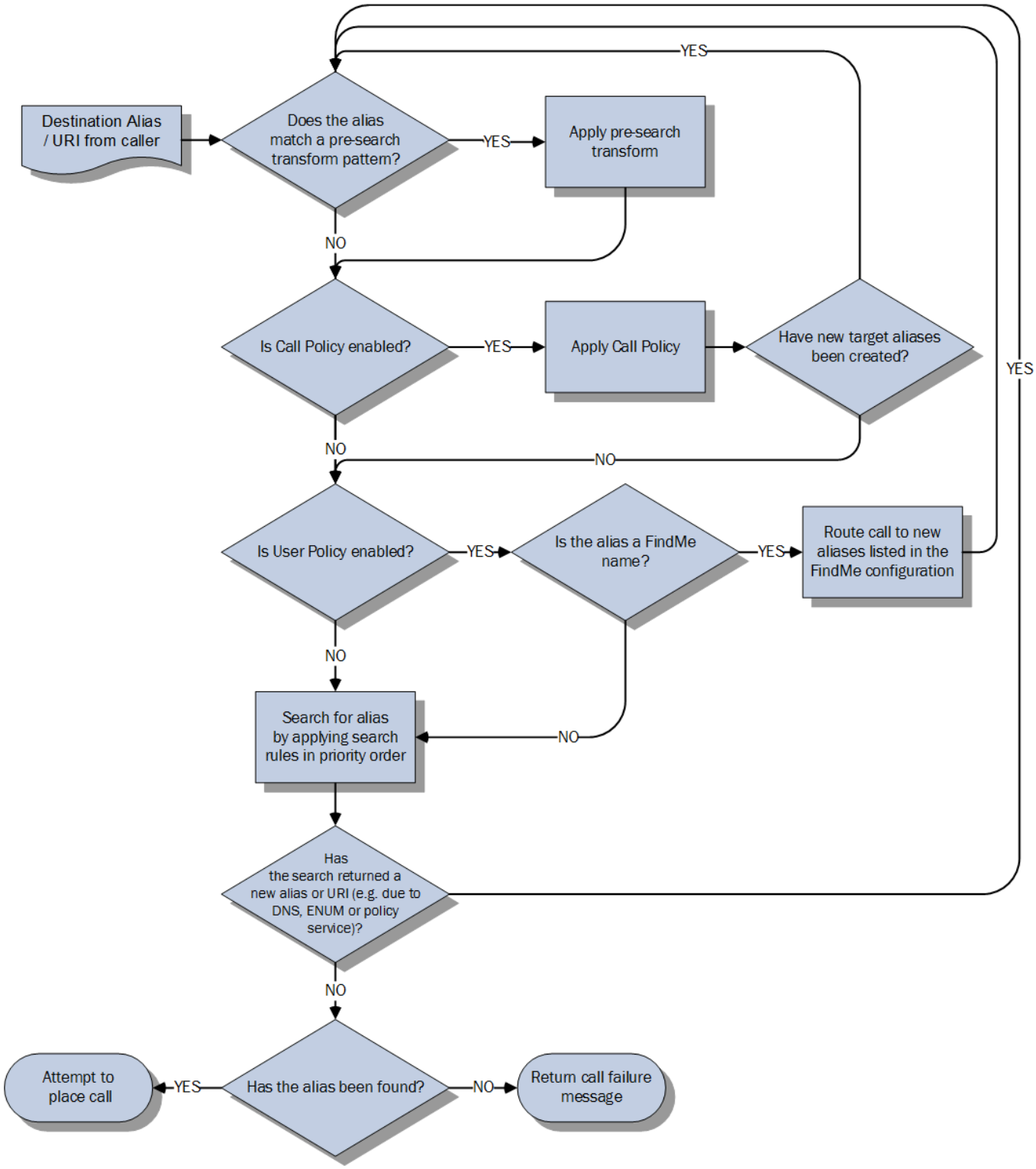
1. The caller enters into their endpoint the alias or address of the destination endpoint. This alias or address can be in a number of different address formats.
2. The destination address is received by the VCS.

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

   Note: The VCS 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 VCS.
     - **Neighbor zone**: one of the VCS's configured external neighbor zones, or a DNS or ENUM lookup zone.
     - **Policy service**: an external service or application, such as a Cisco TelePresence Conductor. 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 VCS 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 VCS attempts to place the call.
9. If the alias is not found, it responds with a message to say that the call has failed.

Figure 12 Call Routing Flowchart



Configuring Hop Counts

Each search request is assigned a hop count value by the system that initiates the search. Every time the request is forwarded to another neighbor gatekeeper or proxy, the hop count value is decreased by a value of 1. When the hop count reaches 0, the request will not be forwarded on any further and the search will fail.

For search requests initiated by the local VCS, 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 VCS that are sent to that zone.

Search requests received from another zone will already have a hop count assigned. When the request is subsequently forwarded on to a neighbor zone, the lower of the two values (the original hop count or the hop count configured for that zone) is used.

For H.323, the hop count only applies to search requests. For SIP, the hop count applies to all requests sent to a zone (affecting the Max-Forwards field in the request).

The hop count value can be between 1 and 255. The default is 15.

Note: if your hop counts are set higher than necessary, you may risk introducing loops into your network. In these situations a search request will be sent around the network until the hop count reaches 0, consuming resources unnecessarily. This can be prevented by setting the Call loop detection mode to *On*.

When dialing by URI or ENUM, the hop count used is that for the associated DNS or ENUM zone via which the destination endpoint (or intermediary SIP proxy or gatekeeper) was found.

Configuring hop counts for a zone

Hop counts are configured on a zone basis. To configure the hop count for a zone:

1. Go to the **Zones** page (**Configuration > Zones > Zones**).
2. Click on the name of the zone you want to configure. You are taken to the **Edit zone** page.
3. In the **Configuration** section, in the **Hop count** field, enter the hop count value you want to use for this zone.

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), page 135 section.

Configuring Dial Plan Settings

The **Dial plan configuration** page (**Configuration > Dial plan > Configuration**) is used to configure how the VCS 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 VCS 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 VCS 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 VCS will query its neighbors for the remote address and if permitted will route the call through the neighbor. *Off*: endpoints registered directly to the VCS may only call an IP address of a system also registered directly to that VCS. 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, page 197 for more information.
Fallback alias	The alias to which incoming calls are placed for calls where the IP address or domain name of the VCS 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 VCS 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 VCS directly
- the caller has dialed a domain name belonging to the VCS (either one of its configured SIP domains, or any domain that has an SRV record that points at the IP address of the VCS), without giving an alias as a prefix

Normally such calls would be disconnected. However, such calls will be routed to the **Fallback alias** if it is specified. Note that some endpoints do not allow users to enter an alias and an IP address to which the call should be placed.

Example usage

You may want to configure your fallback alias to be that of your receptionist, so that all calls that do not specify an alias are still answered personally and can then be redirected appropriately.

For example, Example Inc has the domain of `example.com`. The endpoint at reception has the alias `reception@example.com`. They configure their VCS 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 VCS 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, page 174 for more details).

- **Zone transforms** are applied during the search process by each individual search rule as required. After the search rule has matched an alias they can be used to change the target alias before the search request is sent to a target zone or policy service (see Search and Zone Transform Process, page 176 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 VCS's search rules are highly configurable. You can:

- define alias, IP address and pattern matches to filter searches to specific zones or policy services
- define the priority (order) in which the rules are applied and stop applying any lower-priority search rules after a match is found; this lets you reduce the potential number of search requests sent out, and speed up the search process
- set up different rules according to the protocol (SIP or H.323) or the source of the query (such as the Local Zone, or a specific zone or subzone)
- set up rules that only match specific traffic types, for example standards-based SIP or Microsoft SIP
- limit the range of destinations or network services available to unauthenticated devices by making specific search rules applicable to authenticated requests only
- use zone transforms to modify an alias before the query is sent to a target zone or policy service

Note that multiple search rules can refer to the same target zone or policy service. This means that you can specify different sets of search criteria and zone transforms for each zone or policy service.

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

- It applies to all incoming search requests received from locally registered endpoints, neighbor, traversal client and traversal server zones, and endpoints on the public internet.
- It does not apply to requests received from peers (which are configured identically and therefore will have already applied the same transform).

Each pre-search transform defines a string against which an alias is compared, and the changes to make to the alias if it matches that string.

After the alias has been transformed, it remains changed and all further call processing is applied to the new alias.

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

Pre-search transform process

Up to 100 pre-search transforms can be configured. Each transform must have a unique priority number between 1 and 65534.

Every incoming alias is compared with each transform in order of priority, starting with that closest to 1. If and when a match is made, the transform is applied to the alias and no further pre-search checks and transformations of the new alias will take place. The new alias is then used for the remainder of the call routing process.

- Further transforms of the alias may take place during the remainder of the search process. This may be as a result of Call Policy (also known as Administrator Policy) or User Policy (if FindMe is enabled). If this is the case, the pre-search transforms are re-applied to the new alias.
- If you add a new pre-search transform that has the same priority as an existing transform, all transforms with a lower priority (those with a larger numerical value) will have their priority incremented by one, and the new transform will be added with the specified priority. However, if there are not enough "slots" left to move all the priorities down, you will get an error message.

Configuring Pre-Search Transforms

The **Transforms** page (**Configuration > Dial plan > Transforms**) lists all the pre-search transforms currently configured on the VCS. It is used to create, edit, delete, enable and disable transforms.

Aliases are compared against each transform in order of **Priority**, until a transform is found where the alias matches the **Pattern** in the manner specified by the pattern **Type**. The alias is then transformed according to the **Pattern behavior** and **Replace string** rules before the search takes place (either locally or to external zones).

After the alias has been transformed, it remains changed. and all further call processing is applied to the new alias.

Note that transforms also apply to any Publication, Subscription or Notify URIs handled by the Presence Services, and to any Unified Communications messages.

The configurable options are:

Field	Description	Usage tips
Priority	The priority of the transform. Priority can be from 1 to 65534, with 1 being the highest priority. Transforms are applied in order of priority, and the priority must be unique for each transform.	
Description	An optional free-form description of the transform.	The description appears as a tooltip if you hover your mouse pointer over a transform in the list.
Pattern type	How the **Pattern string** must match the alias for the rule to be applied. Options are: *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 expression.	You can test whether a pattern matches a particular alias and is transformed in the expected way by using the **Check pattern** tool (**Maintenance > Tools > Check pattern**).

Field	Description	Usage tips
Pattern string	Specifies the pattern against which the alias is compared.	The VCS has a set of predefined pattern matching variables that can be used to match against certain configuration elements.
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 Transform Process

The search rules and zone transform process is applied after all pre-search transforms, Call Policy and User Policy have been applied.

The process is as follows:

1. The VCS applies the search rules in priority order (all rules with a priority of 1 are processed first, then priority 2 and so on) to see if the given alias matches the rules criteria based on the **Source** of the query and the rule **Mode**.
2. If the match is successful, any associated zone transform (where the **Mode** is *Alias pattern match* and the **Pattern behavior** is *Replace* or *Strip*) is applied to the alias.

3. The search rule's **Target** zone or policy service is queried (with the revised alias if a zone transform has been applied) using the same protocol (SIP or H.323) as the incoming call request. Note that if there are many successful matches for multiple search rules at the same priority level, every applicable **Target** is queried.
   - If the alias is found, the call is forwarded to that zone. If the alias is found by more than one zone, the call is forwarded to the zone that responds first.
   - If the alias is not found using the native protocol, the query is repeated using the interworked protocol, depending on the interworking mode.
   - If the search returns a new URI or alias (for example, due to an ENUM lookup, or the response from a policy service), the entire Call Routing Process, page 169 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 VCS from searching any other zones unnecessarily.

Configuring Search Rules

The **Search rules** page (**Configuration > Dial plan > Search rules**) is used to configure how the VCS routes incoming search requests to the appropriate target zones (including the Local Zone) or policy services.

The page lists all the currently configured search rules and lets you create, edit, delete, enable and disable rules. You can click on a column heading to sort the list, for example by **Target** or **Priority**. If you hover your mouse pointer over a search rule, the rule description (if one has been defined) appears as a tooltip.

You can also copy and then edit any existing search rule by clicking **Clone** in the **Actions** column.

Up to 2000 search rules can be configured. Priority 1 search rules are applied first, followed by all priority 2 search rules, and so on.

The configurable options are:

Field	Description	Usage tips
Rule name	A descriptive name for the search rule.	
Description	An optional free-form description of the search rule.	The description appears as a tooltip if you hover your mouse pointer over a rule in the list.
Priority	The order in the search process that this rule is applied, when compared to the priority of the other search rules. All Priority 1 search rules are applied first, followed by all Priority 2 search rules, and so on. More than one rule can be assigned the same priority, in which case any matching target zones are queried simultaneously. The default is 100.	The default configuration means that the Local Zone is searched first for all aliases. If the alias is not found locally, all neighbor, traversal client and traversal server zones are searched, and if they cannot locate the alias the request is sent to any DNS and ENUM zones.
Protocol	The source protocol for which the rule applies. The options are *Any*, *H.323* or *SIP*.	

Field	Description	Usage tips
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 VCS's Authentication Policy to limit the set of services available to unauthenticated devices.
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.	

Field	Description	Usage tips
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 expression.	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 **Check 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 VCS 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 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.
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 policy services to use as a target of search rules. This could be used, for example, to call out to an external service or application, such as a TelePresence Conductor. The service will return some CPL which could, for example, specify a new destination alias which would start the search process over again.

Field	Description	Usage tips
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 VCS can find an endpoint identified by a given alias, without actually placing a call to that endpoint, by using the Locate tool (**Maintenance > Tools > Locate**).
- You can test whether a pattern matches a particular alias and is transformed in the expected way by using the **Check pattern** tool (**Maintenance > Tools > Check pattern**).

Example Searches and Transforms

You can use pre-search transforms and search rules separately or together. You can also define multiple search rules that use a combination of **Any alias** and **Alias pattern match** modes, and apply the same or different priorities to each rule. This will give you a great deal of flexibility in determining if and when a target zone is queried and whether any transforms are applied.

This section gives the following examples that demonstrate how you might use pre-search transforms and search rules to solve specific use cases in your deployment:

- Filter queries to a zone using the original alias
- Always query a zone using the original alias
- Always query a zone using a transformed alias
- Query a zone using both the original and transformed alias
- Query a zone using two or more different transformed aliases
- Stripping the domain from an alias to allow dialing from SIP to H.323 numbers
- Stripping the domain from an alias to allow dialing from SIP to H.323 IDs
- Allow calls to IP addresses only if they come from known zones
- Forward Microsoft SIP Calls toCisco Meeting Server

Filter Queries to a Zone Without Transforming

You can filter the search requests sent to a zone so that it is only queried for aliases that match certain criteria. For example, assume all endpoints in your regional sales office are registered to their local Cisco VCS with a suffix of `@sales.example.com`. In this situation, it makes sense for your Head Office VCS 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 VCS will not apply any further (lower priority) search rules.

To achieve the example described above, on your Head Office VCS 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

Field	Value
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
Priority	100
Source	Any
Request must be authenticated	No
Mode	Any alias
On successful match	Continue
Target	Head office
State	Enabled

Query a Zone for a Transformed Alias

Note that the *Any alias* mode does not support alias transforms. If you want to always query a zone using a different alias to that received, you need to use a mode of *Alias pattern match* in combination with a regular expression.

You may want to configure your dial plan so that when a user dials an alias in the format `name@example.com` the VCS 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
Target zone	Head office
State	Enabled

Query a Zone for Original and Transformed Alias

You may want to query a zone for the original alias at the same time as you query it for a transformed alias. To do this, configure one search rule with a **Mode** of *Any alias*, and a second search rule with a **Mode** of *Alias pattern match* along with details of the transform to be applied. Both searches must be given the same **Priority** level.

For example, you may want to query a neighbor zone for both a full URI and just the name (the URI with the domain removed). To achieve this, on your local VCS 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
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 VCS 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 VCS queries the zone simultaneously for both `name@example.co.uk` and `name@example.net`.

To achieve this, from the **Create search rule** page (**Configuration > Dial plan > Search rules > New**) set up two search rules as follows:

Rule #1

Field	Value
Rule name	Transform to example.co.uk
Description	Transform example.com to example.co.uk
Priority	100
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Suffix
Pattern string	example.com
Pattern behavior	Replace

Field	Value
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 VCS 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

Field	Value
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
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

Field	Value
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 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
Pattern type	Regex
Pattern string	(.+)@domain
Pattern behavior	Replace
Replace string	\1
On successful match	Continue
Target zone	Local Zone
State	Enabled

Rule #2

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

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

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

Allowing Calls to IP Addresses Only if They Come From Known Zones

In addition to making calls to aliases, calls can be made to specified IP addresses. To pass on such calls to the appropriate target zones you must set up search rules with a **Mode** of *Any IP address*. To provide extra security you can set the rule's **Source** option to *All zones*. This means that the query is only sent to the target zone if it originated from any configured zone or the Local Zone.

To achieve the example described above, from the **Create search rule** page (**Configuration > Dial plan > Search rules > New**) set up a search rule as follows:

Field	Value
Rule name	IP addresses from known zones
Description	Allow calls to IP addresses only from a known zone
Priority	100
Source	All zones
Request must be authenticated	No
Mode	Any IP address
On successful match	Continue
Target zone	Overseas office
State	Enabled

Forward Microsoft SIP Calls to Cisco Meeting Server

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

Field	Value
Rule name	Route all to Meeting Server
Description	Send all inbound MS traffic to Meeting Server
Priority	100
Protocol	SIP
Traffic type	Any Microsoft
Source	Any
Request must be authenticated	No
Mode	Any alias
On successful match	Stop
Target	Cisco Meeting Server
State	Enabled

Configuring Search Rules to Use an External Service

The configuration process to set up the VCS to use an external policy service for search rules (dial plan) is broken down into the following steps:

- Configure the policy service to be used by search rules.
- Configure the relevant search rules to direct a search to the policy service.

Configuring a policy service to be used by search rules

1. Go to **Configuration > Dial plan > Policy services**.
2. Click **New**.
3. Configure the fields on the **Create policy service** page as follows:

Field	Description	Usage tips
Name	The name of the policy service.	
Description	An optional free-form description of the policy service.	The description appears as a tooltip if you hover your mouse pointer over a policy service in the list.
Protocol	The protocol used to connect to the policy service. The default is *HTTPS*.	The VCS 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 VCS to connect to a policy server over HTTPS, the VCS 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 VCS'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 VCS 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 VCS has an appropriate DNS configuration that allows the FQDN to be resolved. For resiliency, up to three server addresses can be supplied.
Path	Enter the URL of the service on the server.	

Field	Description	Usage tips
Status path	The **Status path** identifies the path from where the VCS 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, page 340.
Username	The username used by the VCS to log in and query the service.	
Password	The password used by the VCS 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 VCS if the service is not available.	You can change it, for example, to redirect to an answer service or recorded message. For more information, see Default CPL for Policy Services, page 553.

4. Click **Create policy service**.

Configuring a search rule to direct a search to the policy service

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.

3. Configure the fields on the **Create search rule** page as appropriate for the searches you want to direct to the external policy server.

   This example shows how to divert calls to aliases ending in .meet to the external policy server:

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
Pattern behavior	As required, for example *Leave*.
On successful match	As required. Note that if *Stop* is selected the VCS 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*.

4. Click **Create search rule**.

The VCS will direct all searches that match the specified pattern to the policy service server.

Your search rules must be configured in such a way that they will result in a match for the initial alias, and then either not match or not return a reject for any aliases to which the policy server has routed the call.

About Call Policy

You can set up rules to control which calls are allowed, which calls are rejected, and which calls are to be redirected to a different destination. These rules are known as Call Policy (or Administrator Policy).

If Call Policy is enabled and has been configured, each time a call is made the VCS 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 VCS.

You should:

- use Call Policy to determine which callers can make or receive calls via the VCS
- use Registration restriction policy to determine which aliases can or cannot register with the VCS

Configuring Call Policy

The **Call Policy configuration** page (**Configuration > Call Policy> Configuration**) is used to configure the VCS's Call Policy mode and to upload local policy files.

Call Policy Mode

The **Call Policy mode** controls from where the VCS 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 VCS. If you choose *Local CPL* you must then either:

- configure basic Call Policy through the **Call Policy rules** page (**Configuration > Call Policy > Rules**) – note that this only lets you allow or reject specified calls, or
- upload a Call Policy file that contains CPL script; however, due to the complexity of writing CPL scripts you are recommended to use an external policy service instead

Only one of these two methods can be used at any one time to specify Call Policy. If a CPL script has been uploaded, this takes precedence and you will not be able to use the **Call Policy rules** page; to use the page you must first delete the CPL script that has been uploaded.

If *Local CPL* is enabled but no policy is configured or uploaded, then a default policy is applied that allows all calls, regardless of source or destination.

The *Policy service* option is used if you want to refer all Call Policy decisions out to an external service. If you select this option an extra set of configuration fields appear so that you can specify the connection details of the external service. See Configuring Call Policy to Use an External Service, page 195 .

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 VCS, 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 VCS, or ■ registered and authenticated to a neighbor which in turn has authenticated with the local VCS	See About Device Authentication, page 99 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 VCS 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 VCS rejects the call.	
Rearrange	This field is only visible in the list of call policy rules (on the 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 VCS. However, due to the complexity of writing CPL scripts you are recommended to use an external policy service instead.

For information on the CPL syntax and commands that are supported by the VCS, see the CPL Reference, page 364 section.

Viewing existing CPL script

To view the Call Policy that is currently in place as an XML-based CPL script, go to the Call Policy configuration page (**Configuration > Call Policy > Configuration**) and click **Show Call Policy file**.

- If Call Policy is configured to use a CPL script, this shows you the script that was uploaded.
- If Call Policy is configured by the **Call Policy rules** page, this shows you the CPL version of those call policy rules.
- If **Call Policy mode** is *On* but a policy has not been configured, this shows you a default CPL script that allows all calls.

You may want to view the file to take a backup copy of the Call Policy, or, if Call Policy has been configured using the Call Policy rules page you could take a copy of this CPL file to use as a starting point for a more advanced CPL script.

If Call Policy has been configured using the **Call Policy rules** page and you download the CPL file and then upload it back to the VCS without editing it, the VCS 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 VCS. The **Call Policy configuration** page allows you to download the XML schemas which are used to check scripts that are uploaded to the VCS. 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 VCS.

Uploading a CPL script

To upload a new CPL file:

1. Go to **Configuration > Call Policy > Configuration**.
2. From the **Policy files** section, in the **Select the new Call Policy file** field, enter the file name or **Browse** to the CPL script you want upload.
3. Click **Upload file**.

The VCS polls for CPL script changes every 5 seconds, so the VCS will almost immediately start using the updated CPL script. CPL scripts cannot be uploaded using the command line interface.

Deleting an existing CPL script

If a CPL script has already been uploaded, a **Delete uploaded file** button will be visible. Click it to delete the file.

Configuring Call Policy to Use an External Service

To configure Call Policy to refer all policy decisions out to an external service:

1. Go to **Configuration > Call policy > Configuration**.
2. Select a **Call Policy mode** of *Policy service*.
3. Configure the fields that are presented as follows:

Field	Description	Usage tips
Protocol	The protocol used to connect to the policy service. The default is *HTTPS*.	The VCS 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 VCS to connect to a policy server over HTTPS, the VCS 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 VCS'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 VCS 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 VCS has an appropriate DNS configuration that allows the FQDN to be resolved. For resiliency, up to three server addresses can be supplied.
Path	Enter the URL of the service on the server.	

Field	Description	Usage tips
Status path	The **Status path** identifies the path from where the VCS 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, page 340.
Username	The username used by the VCS to log in and query the service.	
Password	The password used by the VCS 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 VCS if the service is not available.	You can change it, for example, to redirect to an answer service or recorded message. For more information, see Default CPL for Policy Services, page 553.

4. Click **Save**.

   The VCS 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 VCS follows when attempting to locate the destination endpoint. The address formats supported by the VCS are:

- IP address, for example `10.44.10.1` or `3ffe:80ee:3706::10:35`
- H.323 ID, for example `john.smith` or `john.smith@example.com` (note that an H.323 ID can be in the form of a URI)
- E.164 alias, for example `441189876432` or `6432`
- URI, for example `john.smith@example.com`
- ENUM, for example `441189876432` or `6432`

Each of these address formats may require some configuration of the VCS 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 (such as a VCS or other gatekeeper). See the Dialing by IP Address, page 197 section for more information.

Endpoints registered to a VCS Expressway

Calls made by dialing the IP address of an H.323 endpoint registered directly with a VCS Expressway are forced to route through the VCS Expressway. The call will therefore be subject to any restrictions configured on that system.

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 VCS follows the usual call routing process, applying any transforms and then searching the Local Zone and external zones for the alias, according to the search rules.

Note that SIP endpoints always register using an AOR in the form of a URI. You are recommended to ensure that H.323 endpoints also register with an H.323 ID in the form of a URI to facilitate interworking.

Dialing by H.323 or SIP URI

When a user places a call using URI dialing, they will typically dial `name@example.com`.

If the destination endpoint is locally registered or registered to a neighbor system, no special configuration is required for the call to be placed. The VCS follows the usual search process, applying any transforms and then searching the Local Zone and external zones for the alias, according to the search rules.

If the destination endpoint is not locally registered, URI dialing may make use of DNS to locate the destination endpoint. To support URI dialing via DNS, you must configure the VCS with at least one DNS server and at least one DNS zone.

Full instructions on how to configure the VCS to support URI dialing via DNS (both outbound and inbound) are given in the URI dialing section.

Dialing by ENUM

ENUM dialing allows an endpoint to be contacted by a caller dialing an E.164 number – a telephone number – even if that endpoint has registered using a different format of alias. The E.164 number is converted into a URI by the DNS system, and the rules for URI dialing are then followed to place the call.

The ENUM dialing facility allows you to retain the flexibility of URI dialing while having the simplicity of being called using just a number – particularly important if any of your callers are restricted to dialing using a numeric keypad.

To support ENUM dialing on the VCS you must configure it with at least one DNS server and the appropriate ENUM zones.

Full instructions on how to configure the VCS to support ENUM dialing (both outbound and inbound) are given in the ENUM dialing section.

Dialing by IP Address

Dialing by IP address is necessary when the destination endpoint is not registered with any system.

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

Calls to known IP addresses

VCS 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 VCS.

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 ExpresswayVCS 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 VCS supports dialing by IP address, it is sometimes undesirable for the VCS 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 VCS, or not allow such calls at all. The **Calls to unknown IP addresses** setting (on the **Dial plan configuration** page) configures how the VCS handles calls to IP addresses which are not on its local network, or registered with it or one of its neighbors.

VCS 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 VCS according to the **Calls to Unknown IP addresses** setting:

- *Direct*: the VCS attempts to place the call directly to the unknown IP address without querying any neighbors.
- *Indirect*: the VCS 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 VCS will pass the call to that neighbor for completion. This is the default setting.
- *Off*: the VCS 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 VCS 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 a VCS Expressway is neighbored with a VCS Control for firewall traversal, you should typically set **Calls to unknown IP addresses** to *Indirect* on the VCS Control and *Direct* on the VCS Expressway. 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 VCS Control with which it is registered.
2. As the IP address being called is not registered to that VCS, and its **Calls to unknown IP addresses** setting is *Indirect*, the VCS does not place the call directly. Instead, it queries its neighbor VCS Expressway to see if that system is able to place the call on the VCS Control's behalf. You must configure a search rule for *Any IP Address* against the traversal server zone.
3. The VCS Expressway receives the call, and because its **Calls to unknown IP addresses** setting is *Direct*, it will make the call directly to the called IP address.

About URI Dialing

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

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

URI Dialing Without DNS

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

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

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

If a DNS zone and a DNS server have not been configured on the local VCS, calls to endpoints that are not registered locally or to a neighbor system could still be placed if the local VCS is neighbored (either directly or indirectly) with another VCS 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 a VCS Expressway.

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 VCS will query its local zone and neighbors for that URI.

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

- the H.323 endpoints should register with the VCS using an address in the format of a URI

  Or
- an appropriate transform should be written to convert URIs into the format used by the H.323 registrations. An example would be a deployment where H.323 endpoints register with an `alias`, and incoming calls are made to `alias@domain.com`. A local transform is then configured to strip the `@domain`, and the search is made locally for `alias`. See Stripping @domain for Dialing to H.323 Numbers, page 184 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 VCS uses a DNS lookup to locate the domain in the URI address and then queries that domain for the alias. See the URI Resolution Process Using DNS, page 200 section for more information.

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

Outgoing calls

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

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

This is described in the URI Dialing via DNS for Outgoing Calls, page 201 section.

Incoming calls

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

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

This is described in the URI Dialing via DNS for Incoming Calls, page 203 section.

Firewall traversal calls

To configure your system so that you can place and receive calls using URI dialing through a firewall, see the URI Dialing and Firewall Traversal, page 205 section.

URI Resolution Process Using DNS

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

H.323

1. The VCS 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 VCS, the query will be sent to all servers at the same time, and all responses will be prioritized by the VCS 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 VCS will send an A/AAAA record query for each name record returned. These will resolve to one or more IP addresses, and the VCS 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 VCS will send an A/AAAA record query for each name record returned. These will resolve to one or more IP addresses, and the VCS 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 that if the A and AAAA records that are found at this domain are for systems other than those that support SIP or H.323, the VCS 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 VCS will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.

SIP

The VCS supports the SIP resolution process as outlined in *RFC 3263*. An example of how the VCS implements this process is as follows:

1. The VCS 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 VCS 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 VCS sends SRV queries for each result returned from the NAPTR record lookup. A prioritized list of A/AAAA records returned is built.
   - The VCS sends an A/AAAA record query for each name record returned by the SRV record lookup.

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

2. If the search process does not return a relevant SRV record:
   - If the **Include address record** setting for the DNS zone being queried is set to *On*, the system will fall back to looking for an A or AAAA record for the domain in the URI. If such a record is found, the call will be routed to that IP address and the search will terminate. Note that if the A and AAAA records that are found at this domain are for systems other than those that support SIP or H.323, the VCS 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 VCS 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 VCS, or received as a query from a neighbor system:

1. The VCS checks its search rules to see if any of them are configured with a **Mode** of either:
   - *Any alias*, or
   - *Alias pattern match* with a pattern that matches the URI address
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 VCS attempts to locate the endpoint through a DNS lookup. It does this by querying the DNS server configured on the VCS for the location of the domain as per the URI resolution process via DNS. If the domain part of the URI address is resolved successfully the request is forwarded to those addresses.
   - If one of the target zones is a neighbor, traversal client or traversal server zones, those zones are queried for the URI. If that system supports URI dialing via DNS, it may route the call itself.

Adding and configuring DNS zones

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

1. Go to **Configuration > Zones > Zones**.
2. Click **New**. You are taken to the **Create zone** page.
3. Enter a **Name** for the zone and select a **Type** of *DNS*.

4. Configure the DNS zone settings as follows:

Field	Guidelines
Hop count	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 VCS 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 VCS 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 VCS 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*.

5. Click **Create zone**.

Configuring search rules for DNS zones

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

- configure the DNS servers used by the VCS 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 VCS 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 VCS is hosting.

These records can be of various types including:

- A records, which provide the IPv4 address of the VCS
- AAAA records, which provide the IPv6 address of the VCS
- Service (SRV) records, which specify the FQDN of the VCS 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 VCS.

Incoming call process

When an incoming call has been placed using URI dialing via DNS, the VCS will have been located by the calling system using one of the DNS record lookups described above. The VCS will receive the request containing the dialed URI in the form user@example.com. This will appear as coming from the Default Zone. The VCS 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 VCS, 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 VCS is hosting (such as `example.com`)
- `Port` is the IP port on the VCS that has been configured to listen for that particular service and protocol combination
- `Target` is the FQDN of the VCS.

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 VCS 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 VCS. For each domain hosted by the VCS, 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 VCS, 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 VCS. For each domain hosted by the VCS, 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 VCS to be contactable using SIP URI dialing, you should configure an SRV record for each SIP transport protocol enabled on the VCS (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 VCS hosting the domain has the FQDN `vcs.example.com`.

Their DNS records would typically be as follows:

- SRV record for `_h323ls._udp.example.com` returns `vcs.example.com`
- SRV record for `_h323cs._tcp.example.com` returns `vcs.example.com`
- SRV record for `_h323rs._tcp.example.com` returns `vcs.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 `vcs.example.com`
- SRV record for `_sips._tcp.example.com` returns `vcs.example.com`

- A record for `vcs.example.com` returns the IPv4 address of the VCS
- AAAA record for `vcs.example.com` returns the IPv6 address of the VCS

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 Examples, page 379 section.

For locally registered H.323 endpoints to be reached using URI dialing, either:

- the H.323 endpoints should register with the VCS using an address in the format of a URI
- an appropriate transform should be written to convert URIs into the format used by the H.323 registrations. An example would be a deployment where H.323 endpoints register with an alias, and incoming calls are made to alias@domain.com. A local transform is then configured to strip the @domain, and the search is made locally for alias. See Stripping @domain for Dialing to H.323 Numbers, page 184 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 VCS. You may want to enable calls placed to `user@<IP_address>` to be routed to an existing registration for `user@example.com`. In this case you would configure a pre-search transform that would strip the IP_address suffix from the incoming URI and replace it with the suffix of `example.com`.

URI Dialing and Firewall Traversal

If URI dialing via DNS is being used in conjunction with firewall traversal, DNS zones should be configured on the VCS Expressway and any VCSs on the public network only. VCSs behind the firewall should not have any DNS zones configured. This will ensure that any outgoing URI calls made by endpoints registered with the VCS will be routed through the VCS Expressway.

In addition, the DNS records for incoming calls should be configured with the address of the VCS Expressway as the authoritative gatekeeper/proxy for the enterprise (the DNS Configuration Examples, page 379 section for more information). This ensures that incoming calls placed using URI dialing enter the enterprise through the VCS Expressway, 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 VCS 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 VCS supports outward ENUM dialing by allowing you to configure ENUM zones on the VCS. When an ENUM zone is queried, this triggers the VCS 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 VCS 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 VCS 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 VCS begins the search again, this time for the converted URI as per the URI dialing process. Note that this is considered to be a completely new search, and so pre-search transforms and Call Policy will therefore apply.

Enabling ENUM Dialing

ENUM dialing is enabled separately for incoming and outgoing calls.

Outgoing calls

To allow outgoing calls to endpoints using ENUM, you must:

- configure at least one ENUM zone, and
- configure at least one DNS Server

This is described in the ENUM Dialing for Outgoing Calls, page 206 section.

Incoming calls

To enable endpoints in your enterprise to receive incoming calls from other endpoints via ENUM dialing, you must configure a DNS NAPTR record mapping your endpoints' E.164 numbers to their SIP/H.323 URIs. See the ENUM dialing for incoming calls, page 209 section for instructions on how to do this.

Note: if an ENUM zone and a DNS server have not been configured on the local VCS, calls made using ENUM dialing could still be placed if the local VCS is neighbored with another VCS 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 VCS, the following conditions must be met:

- There must be a NAPTR record available in DNS that maps the called endpoint's E.164 number to its URI. It is the responsibility of the administrator of the enterprise to which the called endpoint belongs to provide this record, and they will only make it available if they want the endpoints in their enterprise to be contactable via ENUM dialing.
- You must configure an ENUM zone on your local VCS. 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 VCS with the address of at least one DNS server that it can query for the NAPTR record (and if necessary any resulting URI).

After the ENUM process has returned one or more URIs, a new search will begin for each of these URIs in accordance with the URI dialing process. If the URIs belong to locally registered endpoints, no further configuration is required. However, if one or more of the URIs are not locally registered, you may also need to configure a DNS zone if they are to be located using a DNS lookup.

Calling process

The VCS follows this process when searching for an ENUM (E.164) number:

1. The VCS 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 VCS checks its search rules to see if any of them are configured with a **Mode** of either:
   - *Any alias*, or
   - *Alias pattern match* with a pattern that matches the E.164 number

3. The target zones associated with any matching search rules are queried in rule priority order.
   - If a target zone is a neighbor zone, the neighbor is queried for the E.164 number. If the neighbor supports ENUM dialing, it may route the call itself.
   - If a target zone is an ENUM zone, the VCS attempts to locate the endpoint through ENUM. As and when each ENUM zone configured on the VCS is queried, the E.164 number is transformed into an ENUM domain as follows:
     1. The digits are reversed and separated by a dot.
     2. The **DNS suffix** configured for that ENUM zone is appended.
4. DNS is then queried for the resulting ENUM domain.
5. If the DNS server finds at that ENUM domain a NAPTR record that matches the transformed E.164 number (that is, after it has been reversed and separated by a dot), it returns the associated URI to the VCS.
6. The VCS then initiates a new search for that URI (maintaining the existing hop count). The VCS starts at the beginning of the search process (applying any pre-search transforms, then searching local and external zones in priority order).From this point, as it is now searching for a SIP/H.323 URI, the process for URI dialing is followed.

In this example, we want to call Fred at Example Corp. Fred's endpoint is actually registered with the URI `fred@example.com`, but to make it easier to contact him his system administrator has configured a DNS NAPTR record mapping this alias to his E.164 number: `+44123456789`.

We know that the NAPTR record for `example.com` uses the DNS domain of `e164.arpa`.

1. We create an ENUM zone on our local VCS 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 VCS initiates a search for a registration of `44123456789` and the search rule of *Any alias* means the ENUM zone is queried. (Note that other higher priority searches could potentially match the number first.)
5. Because the zone being queried is an ENUM zone, the VCS 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 VCS that the E.164 number we have dialed is mapped to the SIP URI of `fred@example.com`.
8. The VCS then starts another search, this time for `fred@example.com`. From this point the process for URI dialing is followed, and results in the call being forwarded to Fred's endpoint.

Configuring Zones and Search Rules for ENUM Dialing

To support ENUM dialing, you must configure an ENUM zone and related search rules for each ENUM service used by remote endpoints.

Adding and configuring ENUM zones

To set up an ENUM zone:

1. Go to **Configuration > Zones > Zones**.
2. Click **New**. You are taken to the **Create zone** page.
3. Enter a **Name** for the zone and select a **Type** of *ENUM*.

4. Configure the ENUM zone settings as follows:

Field	Guidelines
Hop count	The hop count specified for an ENUM zone is applied in the same manner as hop counts for other zone types. The currently applicable hop count is maintained when the VCS initiates a new search process for the alias returned by the DNS lookup.
DNS suffix	The suffix to append to a transformed E.164 number to create an ENUM host name. It represents the DNS zone (in the domain name space) to be queried for a NAPTR record.
H.323 mode	Controls if H.323 records are looked up for this zone.
SIP mode	Controls if SIP records are looked up for this zone.

5. Click **Create zone**.

Note that:

- Any number of ENUM zones may be configured on the VCS. You should configure at least one ENUM zone for each DNS suffix that your endpoints may use.
- Normal search rule pattern matching and prioritization rules apply to ENUM zones.
- You must also configure the VCS with details of DNS servers to be used when searching for NAPTR records.

Configuring search rules for ENUM zones

If you want locally registered endpoints to be able to make ENUM calls via the VCS, 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 VCS, and then an associated search rule with:

- **Mode** of *Alias pattern match*
- **Pattern string** of `44`
- **Pattern type** of *Prefix*

This results in an ENUM query being sent to that zone only when someone dials a number starting with `44`.

Configuring transforms for ENUM zones

You can configure transforms for ENUM zones in the same way as any other zones (see the Search and Zone Transform Process, page 176 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 VCS and then an associated search rule with:

- **Mode** of *Alias pattern match*
- **Pattern string** of `8(\d{4})`
- **Pattern type** of *Regex*
- **Pattern behavior** of *Replace*
- **Replace string** of `44123123(\1)`

With this configuration, it is the resulting string (`44123123xxxx`) that is converted into an ENUM domain and queried for via DNS.

To verify you have configured your outward ENUM dialing correctly, use the Locate tool (**Maintenance > Tools > Locate**) to try to resolve an E.164 alias.

ENUM dialing for incoming calls

For your locally registered endpoints to be reached using ENUM dialing, you must configure a DNS NAPTR record that maps your endpoints' E.164 numbers to their URIs. This record must be located at an appropriate DNS domain where it can be found by any systems attempting to reach you by using ENUM dialing.

About DNS domains for ENUM

ENUM relies on the presence of NAPTR records to provide the mapping between E.164 numbers and their URIs.

RFC 3761, which is part of a suite of documents that define the ENUM standard, specifies that the domain for ENUM – where the NAPTR records should be located for public ENUM deployments – is `e164.arpa`. However, use of this domain requires that your E.164 numbers are assigned by an appropriate national regulatory body. Not all countries are yet participating in ENUM, so you may want to use an alternative domain for your NAPTR records. This domain could reside within your corporate network (for internal use of ENUM) or it could use a public ENUM database such as `http://www.e164.org`.

Configuring DNS NAPTR records

ENUM relies on the presence of NAPTR records, as defined by *RFC 2915*. These are used to obtain an H.323 or SIP URI from an E.164 number.

The record format that the VCS 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 VCS and should be set to `.` (the full stop character).

Non-terminal rules in ENUM are not currently supported by the VCS. 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 VCS for DNS queries:

1. Go to the **DNS** page (**System > DNS**).
2. Enter in the **Address 1** to **Address 5** fields the IP addresses of up to 5 DNS servers that the VCS 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 VCS's call routing and signaling functionality.

Call Signaling Optimization

Calls are made up of two components – signaling and media. For traversal calls, the VCS always handles both the media and the signaling. For non-traversal calls, the VCS does not handle the media, and may or may not need to handle the signaling.

The **Call signaling optimization** setting specifies whether the VCS 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 VCS always handles the call signaling.
  - The call consumes either a traversal call license or a local (non-traversal) call license on the VCS.

- *On*: the VCS 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 VCS removes itself from the call signaling path after the call has been set up. The VCS 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 VCS. In such deployments the directory VCS is used to look up and locate endpoints and it does not have any endpoints registered directly to it.

Call Loop Detection Mode

Your dial plan or that of networks to which you are neighbored may be configured in such a way that there are potential signaling loops. An example of this is a structured dial plan, where all systems are neighbored together in a mesh. In such a configuration, if the hop counts are set too high, a single search request may be sent repeatedly around the network until the hop count reaches 0, consuming resources unnecessarily.

The VCS 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 VCS 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 VCS 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 VCS 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 VCS 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 VCS will assign that call the lowest available Call ID number. For example, if there is already a call in progress with a Call ID of 1, the next call will be assigned a Call ID of 2. If Call 1 is then disconnected, the third call to be made will be assigned a Call ID of 1.

The Call ID is not therefore a unique identifier: while no two calls in progress at the same time will have the same Call ID, the same Call ID will be assigned to more than one call over time.

Note that the VCS web interface does not show the Call ID.

Call Serial Number

The VCS assigns a unique Call Serial Number to every call passing through it. No two calls on a VCS will ever have the same Call Serial Number. A single call passing between two or more VCSs 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 VCSs. When the VCS receives a call, it checks to see if there is a Call Tag already assigned to it. If so, the VCS 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 VCSs will be assigned a different Call Serial Number each time it arrives at a VCS (including one it has already passed through) but can be identified as the same call by use of the Call Tag. This is particularly useful if you are using a remote syslog server to collate events across a number of VCSs in your network.

The Call Tag also helps identify loops in your network – it is used as part of the automatic call loop detection feature, and you can also search the Event Log for all events relating to a single call tag. Loops occur when a query is sent to a neighbor zone and passes through one or more systems before being routed back to the original VCS. 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 a VCS or TelePresence Conductor then the Call Tag information will be lost.

Identifying Calls in the CLI

To control a call using the CLI, you must reference the call using either its Call ID or Call Serial Number. These can be obtained using the command:

```
xStatus Calls
```

This returns details of each call currently in progress in order of their Call ID. The second line of each entry lists the Call Serial Number, and the third lists the Call Tag.

Disconnecting Calls

Disconnecting a call using the web interface

To disconnect one or more existing calls using the web interface:

1. Go to the **Calls** page (**Status > Calls**).
2. If you want to confirm the details of the call, including the Call Serial Number and Call Tag, click **View**. Click the back button on your browser to return to the **Calls** page.
3. Select the box next to the calls you want to terminate and click **Disconnect**.

Note that if your VCS is part of a cluster you have to be logged into the peer through which the call is associated to be able to disconnect the call.

Disconnecting a call using the CLI

To disconnect an existing call using the CLI, you must first obtain either the call ID number or the call serial number (see Identifying Calls, page 211). 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 VCS also allows you to reference the call using the longer but unique call serial number.

Note that when disconnecting a call, only the call with that Call Serial Number is disconnected. Other calls with the same Call Tag but a different Call Serial Number may not be affected.

Limitations when disconnecting SIP calls

Call disconnection works differently for H.323 and SIP calls due to differences in the way the protocols work.

For H.323 calls, and interworked calls, the `Disconnect` command actually disconnects the call.

For SIP calls, the `Disconnect` command causes the VCS to release all resources used for the call; the call will appear as disconnected on the VCS. However, endpoints will still consider themselves to be in the call. SIP calls are peer-to-peer, and as the VCS is a SIP proxy it has no authority over the endpoints. Releasing the resources on the VCS means that the next time there is any signaling from the endpoint to the VCS, the VCS will respond with a '481 Call/Transaction Does Not Exist' causing the endpoint to clear the call.

Note that endpoints that support SIP session timers (see RFC 4028) have a call refresh timer which allows them to detect a hung call (signaling lost between endpoints). The endpoints will release their resources after the next session-timer message exchange.

Bandwidth Control

This section describes how to control the bandwidth that is used for calls within your Local Zone, as well as calls out to other zones (**Configuration > Local Zone** and **Configuration > Bandwidth**).

About Bandwidth Control 215

Configuring Bandwidth Controls 216

About Subzones 217

Links and Pipes 223

Bandwidth Control Examples 226

About Bandwidth Control

The VCS allows you to control the amount of bandwidth used by endpoints on your network. This is done by grouping endpoints into subzones, and then using links and pipes to apply limits to the bandwidth that can be used:

- within each subzone
- between a subzone and another subzone
- between a subzone and a zone

Bandwidth limits may be set on a call-by-call basis and/or on a total concurrent usage basis. This flexibility allows you to set appropriate bandwidth controls on individual components of your network.

Calls will fail if links are not configured correctly. You can check whether a call will succeed, and what bandwidth will be allocated to it, using the command `xCommand CheckBandwidth`.

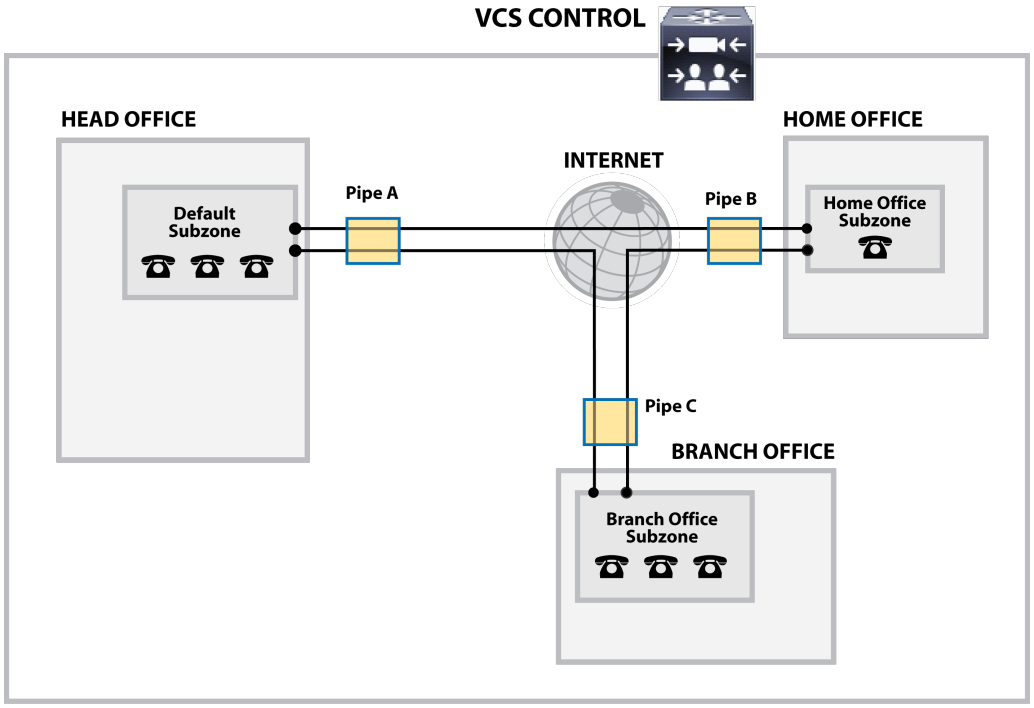
For specific information about how bandwidth is managed across peers in a cluster, see Sharing Bandwidth Across Peers, page 165.

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 VCS 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.
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 VCS 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 VCS's registration, authentication and media encryption policies.

When an endpoint registers with the VCS it is allocated to an appropriate subzone, determined by subzone membership rules based on endpoint IP address ranges or alias pattern matches.

You can create and configure subzones through the **Subzones** page (**Configuration > Local Zone > Subzones**).

The VCS automatically creates the following special subzones, which you cannot delete:

- Default Subzone
- Traversal Subzone
- Cluster Subzone (if VCS is in a cluster)

The VCS is shipped with the Default Subzone and Traversal Subzone (and Default Zone) already created, and with links between them. If the VCS 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 VCS will perform at any one time. These limitations can be applied on a total concurrent usage basis, and on a per-call basis.

See Applying Bandwidth Limitations to Subzones, page 222 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 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 therefore 48*500 = 24000 ports.

If you want to reduce the range, be aware that VCS 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 traversal calls. You may need to increase the range again if you add new licenses.

Why are 48 ports required for each call?

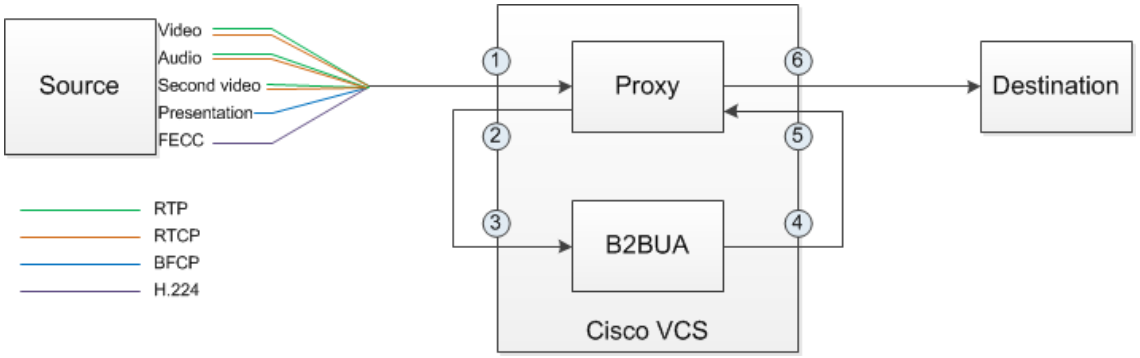
The nominal maximum number of ports allocated per call = max number of ports per allocation * max number of allocation instances. This is 8 * 6 = 48, and those numbers are derived as follows:

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 VCS and outbound from VCS), requiring two instances of port allocation. A further four instances of allocation are required if the call is routed via the B2BUA. In this case, ports are allocated at the following points:

1. Inbound to the local proxy from the source
2. Outbound from the local proxy to the local B2BUA
3. Inbound to the local B2BUA from the local proxy
4. Outbound from the local B2BUA to the local proxy
5. Inbound to the local proxy from the local B2BUA
6. Outbound from the local proxy to the destination

Figure 13 Maximum port allocation for a media traversal call



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 VCS 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 VCS Control at **Configuration > Local Zones > Traversal Subzone**. In Large VCS systems the first 12 ports in the range – 36000 to 36011 by default – are always reserved for multiplexed traffic. The VCS Expressway 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 VCS Expressway (**Configuration > Traversal > Ports**). If you choose not to configure a particular pair of ports (**Use configured demultiplexing ports** = *No*), then the VCS Expressway 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 VCS, its IP address and alias is checked against the subzone membership rules and it is assigned to the appropriate subzone. If no subzones have been created, or the endpoint's IP address or alias does not match any of the subzone membership rules, it is assigned to the Default Subzone (subject to the Default Subzone's **Registration policy** and **Authentication policy**).

The use of a Default Subzone on its own (without any other manually created subzones) is suitable only if you have uniform bandwidth available between all your endpoints. Note that if your Local Zone contains two or more different networks with different bandwidth limitations, you should configure separate subzones for each different part of the network.

Default Subzone configuration options

The Default Subzone can be configured in the same manner as any other manually created subzone.

Configuring Subzones

The **Subzones** page (**Configuration > Local Zone > Subzones**) lists all the subzones that have been configured on the VCS, and allows you to create, edit and delete subzones. For each subzone, it shows how many membership rules it has, how many devices are currently registered to it, and the current number of calls and bandwidth in use. Up to 1000 subzones can be configured.

After configuring a subzone you should set up the Subzone membership rules which control which subzone an endpoint device is assigned to when it registers with the VCS as opposed to defaulting to the Default Subzone.

The configurable options are:

Field / section	Description
Registration policy	When an endpoint registers with the VCS, 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 registration restriction policy to control whether an endpoint can register with the VCS, 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 that 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 VCS challenges incoming messages to the Default Subzone. See Authentication Policy Configuration Options, page 102 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, page 131 for more information. Note that 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, page 222 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 subzone an endpoint is assigned when it registers with the VCS.

The page lists all the subzone membership rules that have been configured on the VCS, 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 that if an endpoint's IP address or registration alias does not match any of the membership rules, it is assigned to the Default Subzone.

Up to 3000 subzone membership rules can be configured.

The configurable options are:

Field	Description	Usage tips
Rule name	A descriptive name for the membership rule.	
Description	An optional free-form description of the rule.	The description appears as a tooltip if you hover your mouse pointer over a rule in the list.
Priority	The order in which the rules are applied (and thus to which subzone the endpoint is assigned) if an endpoint's address satisfies multiple rules.	The rules with the highest priority (1, then 2, then 3 and so on) are applied first. If multiple *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.
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 expression.	Applies only if the **Type** is *Alias pattern match*.

Field	Description	Usage tips
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
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 VCS will perform the bandwidth calculations using the one with the fewest links.

The **Links** page (**Configuration > Bandwidth > Links**) lists all existing links and allows you to create, edit and delete links.

The following information is displayed:

Field	Description
Name	The name of the link. Automatically created links have names based on the nodes that the link is between.
Node 1 and **Node 2**	The Traversal Subzone and the zone that the link is between. The two subzones, or one subzone and one zone, that the link is between.
Pipe 1 and Pipe 2	Any pipes that have been used to apply bandwidth limitations to the link. See Applying Pipes to Links, page 225 for more information. Note that in order to apply a pipe, you must first have created it via the Pipes page.
Calls	Shows the total number of calls currently traversing the link.
Bandwidth used	Shows the total amount of bandwidth currently being consumed by all calls traversing the link.

You can configure up to 3000 links. Some links are created automatically when a subzone or zone is created.

Default Links

If a subzone has no links configured, then endpoints within the subzone are only able to call other endpoints within the same subzone. For this reason, the VCS 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 VCS 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 VCS 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, page 225 for more information.

The **Pipes** page (**Configuration > Bandwidth > Pipes**) lists all the pipes that have been configured on the VCS and allows you to create, edit and delete pipes.

The following information is displayed:

Field	Description
Name	The name of the pipe.
Total bandwidth	The upper limit on the total bandwidth used at any one time by all calls on all links to which this pipe is applied.
Per call bandwidth	The maximum bandwidth of any one call on the links to which this pipe is applied.
Calls	Shows the total number of calls currently traversing all links to which the pipe is applied.
Bandwidth used	Shows the total amount of bandwidth currently being consumed by all calls traversing all links to which the pipe is applied.

You can configure up to 1000 pipes.

See Applying Bandwidth Limitations to Subzones, page 222 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

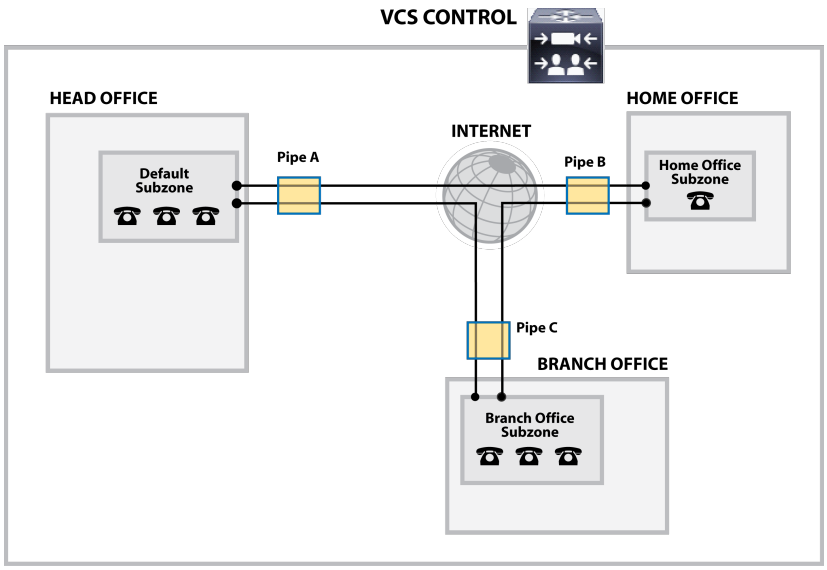
Each pipe may be applied to multiple links. This is used to model the situation where one site communicates with several other sites over the same broadband connection to the Internet. A pipe should be configured to represent the broadband connection, and then applied to all the links. This allows you 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

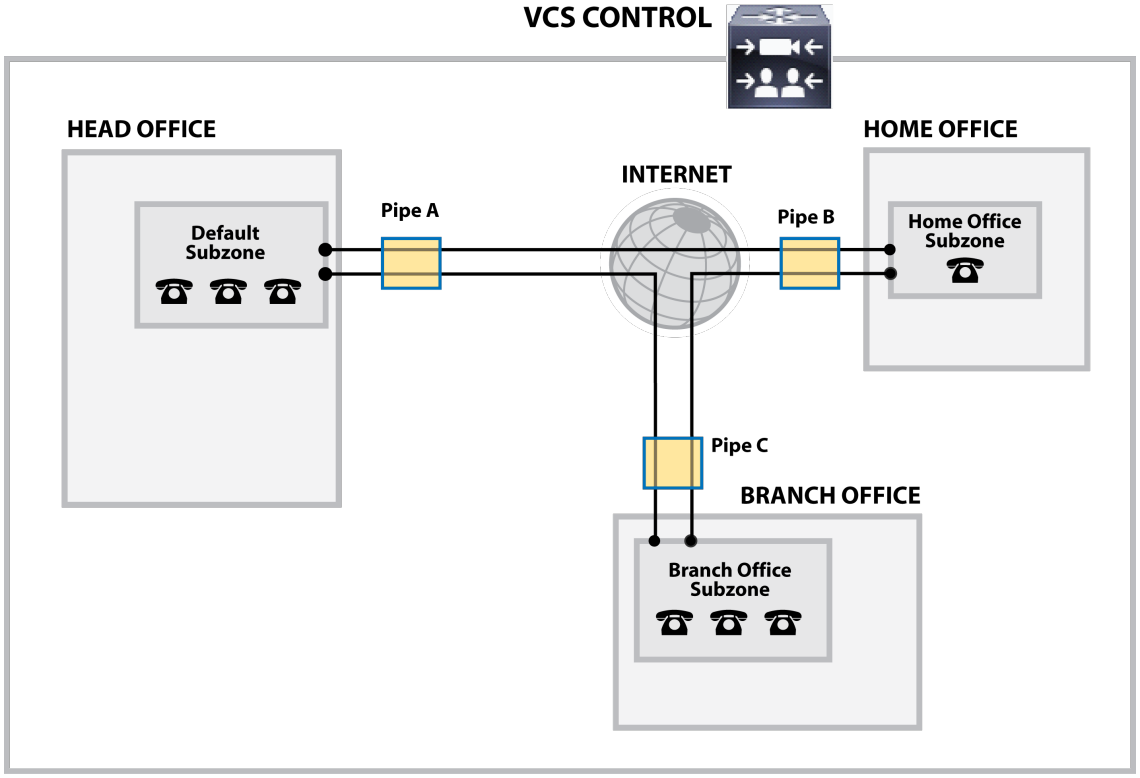
In the example below, there are three geographically separate offices: Head, Branch and Home. All endpoints in the Head Office register with the VCS Control, as do those in the Branch and Home offices.

Each of the three offices is represented as a separate subzone on the VCS, 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.



With a Firewall

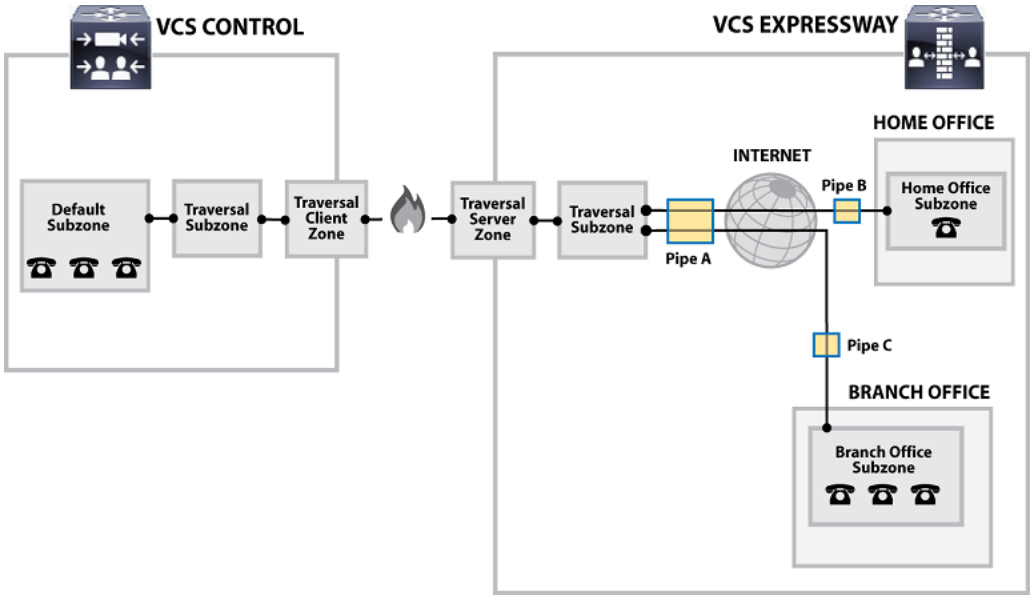
If the example deployment above is modified to include firewalls between the offices, we can use Cisco's Expressway firewall traversal solution to maintain connectivity. We do this by adding a VCS Expressway outside the firewall on the public internet, which will work in conjunction with the VCS Control and Home and Branch office endpoints to traverse the firewalls.

In this example, shown below, the endpoints in the Head Office register with the VCS Control, while those in the Branch and Home offices register with the VCS Expressway. The introduction of the firewalls means that there is no longer any direct connectivity between the Branch and Home offices. All traffic must be routed through the VCS Expressway. This is shown by the absence of a link between the Home and Branch subzones.

The VCS Expressway has subzones configured for the Home Office and Branch Office. These are linked to the VCS Expressway's Traversal Subzone, with pipes placed on each link. All calls from the VCS Expressway to the VCS Control must go through the Traversal Subzone and will consume bandwidth from this subzone. Note also that calls from the Home Office to the Branch Office must also go through the Traversal Subzone, and will also consume bandwidth from this subzone as well as the Home and Branch subzones and Home Office, Branch Office and Head Office pipes.

This example assumes that there is no bottleneck on the link between the VCS Expressway and the Head Office network, so a pipe has not been placed on this link. If you want to limit the amount of traffic flowing through your firewall, you could provision a pipe on this link.

Because the VCS Control is only managing endpoints on the Head Office LAN, its configuration is simpler. All of the endpoints in the Head Office are assigned to the Default Subzone. This is linked to the Traversal Subzone, through which all calls leaving the Head Office must pass.



Applications

This section provides information about each of the additional services that are available under the **Applications** menu of the VCS.

Configuring Conference Factory 230

Presence 232

B2BUA (Back-to-Back User Agent) Overview 236

FindMe™ 246

Cisco TMS Provisioning (Including FindMe) 250

Hybrid Services and Connector Management 253

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 VCS 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 VCS.
2. The VCS 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 VCS 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 VCS 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 that the %% represents a fixed number of digits – with leading zeroes where required – based upon the length of the upper range limit.)

Notes:

- Use a different **Template** on each VCS in your network that has the Conference Factory application enabled. If your VCS 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 VCSs) in order to use Multiway in your deployment.

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 VCS 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 VCS 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 VCS supports the SIP-based SIMPLE standard and is made up of two separate services. These are the Presence Server and the Presence User Agent (PUA). These services can be enabled and disabled 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 that 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. For specific information about how Presence information is managed across peers in a cluster, see Clustering and Presence, page 165.

Presence Server

The Presence Server application on the VCS is responsible for managing the presence information for all presentities in the SIP domains for which the VCS 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 VCS).

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 (PUA).
- **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 VCS 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 VCS 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, page 111 for more information.

Presence User Agent (PUA)

Endpoints that do not support presence can have status published on their behalf by the VCS. 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 VCS, 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 VCS, 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 a VCS 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 VCS.

These services can be enabled and disabled separately from each other, depending on the nature of your deployment. Both are disabled by default.

Note that **SIP mode** must be enabled for the Presence services to function.

Presence User Agent (PUA)

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 that:

- 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 VCS 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 VCS is authoritative. All other PUBLISH messages will be proxied on in accordance with the VCS's SIP routing rules. Note that 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 VCS will proxy on all PUBLISH messages to one or more of its neighbor zones in accordance with its locally configured call routing rules. The local VCS 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 VCS 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 that Presence Server is automatically enabled when the **Starter Pack** option key is installed.

Recommendations

- **VCS Expressway and VCS Control**: the recommended configuration for a VCS Expressway when acting as a traversal server for a VCS Control is to enable the PUA and disable the Presence Server on the VCS Expressway, and enable the Presence Server on the VCS Control. This will ensure that all PUBLISH messages generated by the PUA are routed to the VCS Control.
- **VCS neighbors**: if you have a deployment with two or more VCSs 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.
- **VCS clusters**: for information about how Presence works within a cluster, see Clustering and Presence, page 165.

Note: any defined 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 VCS. They are used in the following scenarios:

- To apply media encryption policy. This usage does not require any explicit B2BUA configuration.
- To support ICE messaging. The only B2BUA-related configuration required is to define the set of TURN servers required to support ICE calls.
- To route SIP calls between the VCS and a Microsoft SIP domain. This requires manual configuration of Microsoft Interoperability and the set of TURN servers available for use by the B2BUA.

Configuring B2BUA TURN Servers

Go to **Applications > B2BUA > B2BUA TURN servers** to enter details of the TURN servers that are needed by the VCS B2BUA instances. The page lists the currently configured TURN servers and lets you create, edit and delete them.

The B2BUA chooses which TURN server to offer via random load-balancing between all of the available servers. There is no limit to the number of servers that can be configured for the B2BUA to choose from.

The TURN servers are automatically used by B2BUA instances for ICE messaging when it is enabled on a zone or subzone.

If you want to use the TURN servers for Microsoft interoperability, you must enable **Offer TURN services** (See Configuring Microsoft Interoperability, page 238).

Table 14 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 a VCS Expressway 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.

Microsoft Interoperability

VCS interoperability with Microsoft is based on a back-to-back user agent (B2BUA) which handles SIP calls between the VCS and the Microsoft Skype for Business infrastructure.

Note: From version X8.9, you can interoperate with Microsoft infrastructure without using the B2BUA on the VCS. You can use session classification search rules to route calls to Cisco Meeting Server which does the transcoding instead. 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, eg. IM and Presence Service nodes, while handling the voice/video traffic on the VCS.

Configuration Summary

- Selecting the Microsoft interoperability service on a dedicated VCS.
- Adding the *Microsoft Interoperability* key.
- Configuring Microsoft Interoperability, page 238.
- Configuring the B2BUA's Trusted Hosts, page 242 – the devices that may send signaling messages to the B2BUA.
- Configuring B2BUA TURN Servers, page 236 – 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 VCS 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, page 245, 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 VCS Control (on each peer if the VCS Control is clustered) if you are using the VCS 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 VCS to route Microsoft traffic without modifying it. For example, if you are using the VCS 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 VCS.
- 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 VCS to B2BUA leg will implicitly apply to the B2BUA to Microsoft leg.
- The non-configurable neighbor zone (named "**To Microsoft destination via B2BUA**") uses a special zone profile of *Microsoft interoperability*. You cannot select this profile for any manually configured zones.

For more information about configuring VCS 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 VCS and Microsoft Infrastructure Deployment Guide* on the VCS configuration guides page.
- See *Microsoft Lync 2010, Cisco AM GW and VCS Deployment Guide*

Configuring Microsoft Interoperability

Go **Applications > B2BUA > Microsoft interoperability > Configuration** configure and enable and the B2BUA's connection to the Microsoft environment.

The configurable options are:

Field	Description	Usage tips
Configuration section:		
Microsoft interoperability	Enables or disables the Microsoft interoperability service.	
Destination address	The IP address or Fully Qualified Domain Name (FQDN) of the Hardware Load Balancer, Director or Front End Processor to which the VCS sends the signaling messages.	You must also configure the IP addresses of the trusted hosts. These are the Microsoft systems that may send signaling messages to the VCS.
Listening port	The IP port on the Hardware Load Balancer, Director or Front End Processor to which the VCS sends the signaling messages.	
Signaling transport	The transport type used for connection to the Microsoft infrastructure. The default is *TLS*.	
FindMe integration section:		

Field	Description	Usage tips
Register FindMe users as clients to Microsoft server	Controls whether to register FindMe users to the Microsoft registrar so that it can forward calls to FindMe aliases and share FindMe presence information. Default is *Yes*.	This feature only applies if FindMe is enabled. Note that FindMe users can only register to Microsoft infrastructure if the FindMe ID is a valid user in the Active Directory (in the same way that Microsoft clients can only register if they have a valid account enabled in AD).
Microsoft domain	The SIP domain in use on the Microsoft server. This must be selected from one of the SIP domains already configured on the VCS.	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.
External transcoders section:		
Enable external transcoders for this B2BUA	Controls whether calls may be routed through an external transcoder.	You should enable this option if you need to use a transcoder to transcode between standard codecs (such as H.264) and Microsoft RT Video and RT Audio.
Port on B2BUA for transcoder communications	The IP port used on the B2BUA for communicating with the transcoders.	All transcoder communications are carried out over TLS.
Use transcoder policy rules	Specifies whether the transcoder policy rules are used to control access to the transcoders. Default is No.	If **Enable transcoders for this B2BUA** is *Yes*, then all calls are routed via the transcoders by default. If transcoder resources need to be reserved for specific types of calls, you can use this option to limit the types of calls that are routed via the transcoders. Set this option to *Yes* and then define the required policy rules.
SIP broker section:		
Enable broker for inbound SIP	Toggles the SIP broker, and opens a list of destination presence servers. The broker inspects Microsoft SIP, and routes the SIP SIMPLE to IM and Presence Service nodes that you enter.	If the broker is not enabled, then the B2BUA attempts to process all inbound SIP from Microsoft. If it receives SIP SIMPLE, it tries to route it as if it were SIP audio/video traffic. The SIP SIMPLE will probably be rejected by the call control infrastructure in this case.

Field	Description	Usage tips
Listening port on presence destination servers	This is the port configured on the IM and Presence Service nodes.	
Destination presence server 1..6	IP address, hostname, or FQDN of the IM and Presence Service node.	Enter up to 6. The VCS 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 **Configure B2BUA TURN servers**.
Advanced settings: you should only modify the advanced settings on the advice of Cisco customer support.		
Encryption	Controls how the B2BUA handles encrypted and unencrypted call legs. *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.
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 VCS or this VCS'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 VCS communications	The port used on the B2BUA for communicating with the VCS.	

Field	Description	Usage tips
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.

<table>
<tr><th>Field</th><th>Description</th><th>Usage tips</th></tr>
<tr><td>Maximum RDP transcode sessions</td><td>Limits the number of simultaneous RDP transcoding sessions on this VCS. Default is 10.

Note: Save the page and restart the Microsoft interoperability service to apply your changes.

Table 15 Recommended Number of Desktop Transcode Sessions by Platform
<table>
<tr><th>On this platform:</th><th>Set Maximum RDP transcode sessions to:</th></tr>
<tr><td>1st generation VCS appliance</td><td>1</td></tr>
<tr><td>Medium OVA</td><td>10</td></tr>
<tr><td>‡ Large OVA
CE500/
CE1000/
CE1100</td><td>20</td></tr>
<tr><td>Clusters</td><td>Same as the individual platform setting. The Maximum RDP transcode sessions you enter on the primary applies to each peer in the cluster.</td></tr>
</table>
‡ From X8.10, the requirement to have a 10 Gbps NIC to achieve the scalability of a Large system is removed. Subject to your bandwidth constraints, it is possible to have the capacity of a Large system with a 1 Gbps NIC.</td><td>Higher values will mean that more system resources can be consumed by RDP transcoding, which could impact other services. Maximum is 100.</td></tr>
<tr><td>Port for FindMe presence integration with Microsoft server</td><td>The port used on the B2BUA for presence communications with the Microsoft server.

Default is 10011.</td><td></td></tr>
</table>

Configuring the B2BUA's Trusted Hosts

Go to **Applications > B2BUA > Microsoft Interoperability > Trusted hosts**) to specify the Microsoft hosts from which the VCS will trust SIP signaling.

The interoperability service does not accept messages from any addresses that are not on the trusted hosts list.

Note that trusted host verification only applies to calls initiated by Microsoft clients that are inbound to the VCS video network. It is not necessary to configure trusted hosts if calls are only ever to be initiated from the VCS video network.

The VCS currently has a nominal limit of 25 trusted hosts. If there are more than 25 trusted hosts, the VCS 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 VCS.

The configurable options are:

Field	Description	Usage tips
Name	An optional free-form description of the trusted host.	The name is not used as part of the "trusted" criteria. It is only to help you distinguish between multiple hosts without relying on the IP addresses.
IP address	The IP address of the trusted host.	
Type	The type of device that may send signaling messages to the B2BUA. *Microsoft infrastructure*: this includes Hardware Load Balancers, Directors and Front End Processors *External transcoder*: a transcoder device	

Configuring External Transcoder Policy Rules

Go to **Applications > B2BUA > Microsoft Interoperability > Transcoder policy rules**) to define rules that control which Microsoft interoperability calls are routed via a transcoder.

The Cisco Advanced Media Gateway (AM Gateway) is supported only with Expressway X8.x software versions; support for the AM Gateway is deprecated from Expressway version X12.5.

The page lists all the currently configured rules and lets you create, edit, delete, enable and disable rules. Note that you can click on a column heading to sort the list, for example by **Rule name** or **Priority**.

If **Enable external transcoders for this B2BUA** is *Yes* (configured on the **Microsoft interoperability configuration** page), then all calls are routed via the external transcoders by default. If you want to reserve transcoder resources for specific types of calls, then you can specify rules to control which calls are routed to the external transcoders.

- The rules on this page only apply if **Use transcoder policy rules** is set to *Yes*(on the **Microsoft interoperability configuration** page).
- A rule is applied if it matches either the source or destination alias of a call.
- If call aliases do not match any policy rules, the call will be routed via the external transcoder.

  You should set a general, low priority rule to match all aliases and deny transcoder resources – and then have more specific, higher priority rules to allow specific aliases to use the transcoder resources.

The configurable options are:

Field	Description	Usage tips
Name	The name assigned to the rule.	
Description	An optional free-form description of the rule.	The description appears as a tooltip if you hover your mouse pointer over a rule in the list.
Priority	Sets the order in which the rules are applied. The rules with the highest priority (1, then 2, then 3 and so on) are applied first.	Multiple rules with the same priority are applied in configuration order. For clarity you are recommended to use unique priority settings for each rule.

Field	Description	Usage tips
Pattern type	The way in which the **Pattern string** must match either the source or destination alias of the call. *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 expression.	You can test whether a pattern matches a particular alias and is transformed in the expected way by using the **Check pattern** tool (**Maintenance > Tools > Check pattern**).
Pattern string	The pattern against which the alias is compared.	
Action	The action to take if the source or destination alias of the call matches this policy rule. *Allow*: the call can connect via the transcoder. *Deny*: the call can connect but it will not use transcoder resources.	
State	Indicates if the rule is enabled or not.	Use this setting to test configuration changes, or to temporarily disable certain rules. Any disabled rules still appear in the rules list but are ignored.

Configuring External B2BUA Transcoders

Transcoders are used to convert digital media from one format to another. The only transcoder currently supported by the Microsoft interoperability service is the Cisco TelePresence Advanced Media Gateway (Cisco AM GW).

The Cisco Advanced Media Gateway (AM Gateway) is supported only with Expressway X8.x software versions; support for the AM Gateway is deprecated from Expressway version X12.5.

The B2BUA can use the Cisco AM GW to transcode between standard codecs (such as H.264) and Microsoft RT Video and RT Audio to allow high definition calls between Microsoft clients and Cisco endpoints.

Go to **Applications > B2BUA > Microsoft Interoperability > External transcoders** to manage the set of transcoders available to the B2BUA.

- Multiple transcoders can be configured for load balancing purposes; the B2BUA automatically manages which transcoder to use.
- The status of each transcoder is shown, this includes:
  - whether the transcoder is accessible or not
  - the number of available connections; note that Cisco AM GW calls require 2 connections per call
- Go to Configuring Microsoft Interoperability, page 238 to control whether the B2BUA uses transcoder resources and whether specific policy rules are used to filter which calls are allowed to be routed through the transcoders. Note that the B2BUA can operate without any associated transcoders (calls will still connect but will not be transcoded).

The configurable options are:

Field	Description	Usage tips
Name	An optional free-form description of the transcoder.	
Address	The IP address or Fully Qualified Domain Name (FQDN) of the transcoder.	If you have several transcoders you are recommended to either use their IP addresses or to give each device a different FQDN. You may encounter problems if you use an FQDN that resolves to multiple transcoders (via DNS-based load balancing). This is because the B2BUA will first use DNS to discover the number of available ports on a transcoder, and then use DNS again to route a call to the transcoder. If the DNS lookup can resolve to different transcoders there is no guarantee that the call will be directed to the same transcoder that provided the resource information.
Port	The listening port on the transcoder.	

Restarting the Microsoft Interoperability Service

Sometimes you need a restart to apply changes to the Microsoft interoperability service. The system raises an alarm if you need a restart.

When you restart this service, the VCS does not restart, but it does drop any calls that are being managed by the B2BUA.

1. Go to **Applications > B2BUA > Microsoft interoperability > Restart service...**.
2. Check the number of active calls currently in place.
3. Click **Restart**.

The service restarts after a few seconds. You can check the service status on the Microsoft Interoperability page.

Clustered VCS systems

You must restart the Microsoft interoperability service on every peer. Configure, restart and verify the service on the primary before restarting the service on other peers.

FindMe™

FindMe is a form of User Policy, which is the set of rules that determines what happens to a call for a particular user or group when it is received by the VCS.

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 the **FindMe** option key. Standard operation is to use the VCS's own FindMe manager. However, you can use an off-box FindMe manager; this feature is intended for future third-party integration.

End-User FindMe Account Configuration

From VCS version X7.1, how users configure their FindMe settings depends on whether the VCS is using Cisco TMS provisioning:

- If Cisco TMS provisioning is enabled:
  - Users manage their FindMe settings by logging in to Cisco TMS using their FindMe account.
  - User account and FindMe data is provided from Cisco TMS to VCS by the TMS Provisioning Extension services.
- If you are using FindMe without Cisco TMS (known as "standalone FindMe") then users manage their FindMe settings by logging in to their FindMe account through VCS.

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 VCS 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 VCS 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 VCS continues to search for the alias in the usual manner.

Note that User Policy is invoked after any Call Policy configured on the VCS has been applied. See Call Routing Process, page 169 for more information.

Recommendations when Deploying FindMe

- The FindMe ID should be in the form of a URI, and should be the individual's primary URI.
- Endpoints should not register with an alias that is the same as an existing FindMe ID. You can prevent this by including all FindMe IDs on the Deny List.

Example

Users at Example Corp. have a FindMe ID in the format `john.smith@example.com`. Each of the user's endpoints are registered with a slightly different alias that identifies its physical location. For example their office endpoint is registered with an alias in the format `john.smith.office@example.com` and their home endpoint as `john.smith.home@example.com`.

Both of these endpoints are included in the list of devices to ring when the FindMe ID is dialed. The alias `john.smith@example.com` is added to the Deny List, to prevent an individual endpoint registering with that alias.

Configuring FindMe

The **FindMe configuration** page (**Applications > FindMe**) is used to enable and configure FindMe User Policy.

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. *On*: enables FindMe and uses the VCS's local FindMe manager. *Remote service*: enables FindMe and uses a FindMe manager located on an off-box system (eg.TMS).	Call Policy is always applied regardless of the FindMe mode. If you enable FindMe, you must ensure a **Cluster name** is specified (you do this on the Clustering page).

Field	Description	Usage tips
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. For H.323 calls placed through an ISDN gateway, the E.164 phone number associated with the FindMe account is signaled instead as that is a more appropriate number to dial when returning the call. Note that the ISDN gateway must be registered to the same VCS as the call recipient. The FindMe ID is only displayed if the source endpoint has been authenticated (or treated as authenticated). If it is not authenticated the Incoming ID is displayed. See About Device Authentication, page 99 for more details.
Restrict users from configuring their devices	Controls if users are restricted from adding, deleting or modifying their own devices. The default is *Off*.	By default FindMe users are allowed to configure further devices in addition to any principal or provisioned devices assigned to them by the system administrator. This setting can be used to stop users from adding their own devices and restrict them to being able to only maintain their locations and their associated devices. This setting only applies if you are using FindMe without Cisco TMS (known as "standalone FindMe").

Device creation message	Only applies when **FindMe mode** is *On*.
	
	The text entered here is displayed to users when they add a device to their FindMe configuration.
	
	A limited set of HTML markup is supported in the message which is previewed in the window at the bottom of the page when you click **Save**. The following tags (without any attributes) are allowed:
	
	`b i tt big small strike s u em strong cite dfn samp kbd var abbr acronym sub sup ins del br`
	
	`<a href="…">` is also supported, but the URL can only contain A-Z 0-9, dot, "?" "=" and "%"; note that the URL is relative to the current page so you must prefix it with, for example, http:// if you want to refer to an external site.
		It can be used to provide information about how to format the device address or number, for example any dial prefixes that must be included.
		
		An example message could be:
		
		`Phone numbers: use the prefix <b>9</b>`
		
		`Endpoints: use the suffix <b>@video.test.com</b>`
		
		This setting only applies if you are using FindMe without Cisco TMS (known as "standalone FindMe").

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 VCS to log in and query the remote service.
Password	The password used by the VCS to log in and query the remote service.

If the **Starter Pack** option key is installed the Presence Server and FindMe are automatically enabled.

Management and Storage of FindMe Data

If you use FindMe without Cisco TMS (known as "standalone FindMe") or the **Starter Pack** option key is installed, the VCS's local database is used to store FindMe data and share it across all peers in a cluster.

If you use FindMe and want to use Cisco TMS to manage your FindMe data, you must configure Cisco TMSPE services to provide the VCS with FindMe data.

Note that if you have the **Device Provisioning** feature enabled, you must use Cisco TMSPE services to obtain FindMe configuration data from Cisco TMS.

Cisco TMS Provisioning (Including FindMe)

Cisco TMS provisioning is the mechanism through which the VCS uses provisioning data for the following services:

- User account, device, and phone book data used by VCS to service provisioning requests from endpoint devices
- FindMe account configuration data used by VCS to provide FindMe services

How to enable TMS provisioning services

From X8.11, TMS provisioning services are off by default in the VCS 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 VCS Control and the VCS Expressway, for deployments with a paired VCS Control and VCS Expressway, we recommend that you use it on the VCS Control.

1. (One-time only) If not already enabled, you need to enable provisioning services on the VCS:
   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, page 44).
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 VCS or cluster in the Cisco TMSPE.

Size limitations for clusters and provisioning

A VCS cluster of any size supports up to:

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

Note: Even if the device registration capacity limit 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 VCS 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 VCS.

Cisco TMSPE services used for provisioning

When TMS provisioning is enabled, VCS uses the following Cisco TMSPE services (hosted on Cisco TMS) to provide the VCS / VCS cluster with data:

Service	Description
User Preference	Provides data that enables the VCS 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 VCS Expressway.
FindMe	Provides details of user FindMe accounts, in particular the locations and devices associated with each FindMe ID. This allows the VCS 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).
Devices	Exchanges provisioning licensing information between the VCS and Cisco TMS. Information is exchanged every 30 seconds – the VCS is provided with the current number of free licenses available across the range of VCS clusters being managed by Cisco TMS, and the VCS updates Cisco TMS with the status of provisioning licenses being used by this VCS (or VCS cluster). If the Devices service is not active, the VCS'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 VCS periodically polls Cisco TMSPE services to ensure the data held on VCS 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 VCSs, 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 VCS's cluster replication mechanism.
- You can do an immediate resynchronization of data between VCS 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 VCS while data is deleted and refreshed. If you only need to apply recent updates in Cisco TMS to the VCS, 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 VCS (**TMS Provisioning Extension services** page), changes made through this page **are not applied in Cisco TMS**.

Using FindMe without Cisco TMS

If you use FindMe without TMS (known as "standalone FindMe"), then all FindMe account information is stored and managed locally on the VCS. See *FindMe Deployment Guide* for more information.

VCS Provisioning Server

If device provisioning is enabled, the VCS Provisioning Server provides provisioning-related services to provisioned devices, using data supplied by Cisco TMS through the Cisco TMS provisioning mechanism.

As from version X8.1 , the VCS supports only the Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) services to provide the VCS 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. VCS 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 VCS's Provisioning Server will not be able to provision any devices.

The VCS is provided with the current number of free licenses available across the range of VCS clusters being managed by Cisco TMS, and the VCS updates Cisco TMS with the status of provisioning licenses being used by this VCS (or VCS cluster). License limits can be managed at a per device type basis.

Some devices, including Jabber Video 4.x, do not inform the VCS when they sign out (unsubscribe) from being provisioned. The VCS 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 VCS. The Provisioning Server does not do its own authentication challenge and will reject any unauthenticated messages.

See Device Provisioning and Authentication Policy, page 109 for more information.

Starter Pack Provisioning

The VCS's Starter Pack Provisioning Server provides basic device provisioning, including phone book support, for a range of endpoint device types without the need for Cisco TMS.

The **Starter Pack** option key must be installed to use basic device provisioning. It cannot be used in combination with device provisioning managed through TMS. Note that the **Starter Pack** option key is designed for single box deployments and is only available as a pre-configured factory setting.

Starter Pack

The Starter Pack is suitable for small enterprises. It provides basic VCS functionality and includes Expressway and FindMe functionality automatically.

The following license restrictions apply by default:

- 50 registrations
- 5 traversal calls (extra traversal call license option keys can be added if required)
- 900 TURN relays

Note that:

- non-traversal calls are supported (a traversal license is used when one occurs)
- the Starter Pack has a maximum limit of 25 calls

When the **Starter Pack** option key is installed the Presence Server and FindMe are automatically enabled.

Configuring Starter Pack Provisioning

The **Provisioning** page (**Applications > Provisioning**) is used to configure the VCS's Provisioning Server when the VCS is running in Starter Pack mode.

The Starter Pack Provisioning Server provides basic device provisioning and is automatically enabled when the **Starter Pack** option key is installed. It can be monitored on the Starter Pack status page.

Bandwidth limits

The **Bandwidth limits** section lists each supported device type and lets you choose whether or not to enable the provisioning of bandwidth limits for that device. If you enable the bandwidth limits option for a device type you can then configure the maximum incoming and outgoing bandwidth (in kbps) values to set on the provisioned devices.

ClearPath

The **ClearPath** section lists each supported device type and lets you choose whether or not to enable the provisioning of ClearPath for that device.

Provisioning Users

To provision individual users, you must set up FindMe accounts. When you configure a FindMe account, you can choose the devices to provision for that user. The FindMe account is also used to configure the user's FindMe settings.

See *VCS Starter Pack Express Deployment Guide* for full details on setting up Starter Pack provisioning.

Hybrid Services and Connector Management

If you want to register VCSs 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 VCS software contains a management connector to manage registration and other connectors.

The management connector is dormant until you register VCS to the cloud. When you register, the management connector is automatically downloaded, installed, and upgraded if a newer version is available.

The VCS 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 VCS.

Connector upgrades are made available through Control Hub, and the management connector will download the new versions to VCS when you have authorized the upgrade.

You can also deregister, which disconnects your VCS 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 VCS version for Hybrid Services may also change. You must ensure that your registered VCSs 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 VCS. This means that information about Hybrid Services is maintained in the Hybrid Services documentation, and several VCS interface pages link out to that site.

Connector Proxy

If you want to register VCSs 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 VCS needs a proxy to connect to Cisco Webex. This proxy is not used by the VCS 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 VCS 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 VCS Expressway

The Cisco Webex cloud CA root certificates are packaged in the VCS 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 VCS Expressway needs to trust these CAs so that it can authenticate the server certificates from Collaboration Cloud, to make the encrypted connections needed by some VCS-based hybrid services.

Note: The VCS Expressway cannot register for hybrid services. It must be connected by a secure traversal zone to the VCS (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=QuoVadis Limited, CN=QuoVadis Root CA 2
- O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority

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, page 287 for more help.

Related Reading

- Cisco Webex Signing CAs
- Supported Certificate Authorities for Cisco Webex

User Accounts

This section provides information about how to configure administrator and FindMe user accounts, and how to display the details of all active administrator and FindMe sessions.

About User Accounts 257
Configuring Password Security 259
Configuring Administrator Accounts 260
Configuring Remote Account Authentication Using LDAP 262
Configuring FindMe Accounts 268
Resetting Forgotten Passwords 271
Using the Root Account 272
Managing SSO tokens 273

About User Accounts

The VCS has two types of user account for normal operation:

- **Administrator accounts**: used to configure the VCS.
- **FindMe accounts**: used by individuals in an enterprise to configure their FindMe profile. They can also be used to enable basic device provisioning when the **Starter Pack** option key is installed.

Note that FindMe account configuration via VCS does not apply if the VCS is using the TMS Provisioning Extension services to provide FindMe data.

Account Authentication

Administrator and FindMe accounts must be authenticated before access is allowed to the VCS.

VCS can authenticate accounts either locally or against a remote directory service using LDAP (currently, only Windows Active Directory is supported), or it can use a combination of local and remotely managed accounts. The remote option allows administration groups to be set up in the directory service for all VCSs in an enterprise, removing the need to have separate accounts on each VCS.

See Configuring Remote Account Authentication Using LDAP, page 262 and *Authenticating VCS Accounts using LDAP Deployment Guide* for more information about setting up remote authentication.

If a remote source is used for either administrator or FindMe account authentication, you also need to configure the VCS with:

- appropriate LDAP server connection settings
- administrator groups and/or FindMe groups that match the corresponding group names already set up in the remote directory service to manage administrator and FindMe access to this VCS (see Configuring Administrator Groups, page 266 and Configuring FindMe Groups, page 268)

The VCS can also be configured to use certificate-based authentication. This would typically be required if the VCS was deployed in a highly-secure environment.

Account Types

Administrator accounts

Administrator accounts are used to configure the VCS.

- The VCS has a default **admin** local administrator account with full read-write access. It can be used to access the VCS using the web interface, the API interface or the CLI. Note that you cannot access the VCS 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 VCS using the web and API interfaces only.
- Remotely managed administrator accounts can be used to access the VCS using the web and API interfaces only.
- You can configure one administrator account to be the emergency account. This special account gives access to the VCS even when it disallows local authentication, in case remote authentication is not possible.

You can configure the complexity requirements for local administrator passwords on the Password security page (**Users > Password security**). All passwords and usernames are case sensitive.

Note that:

- The Configuration Log records all login attempts and configuration changes made using the web interface, and can be used as an audit trail. This is particularly useful when you have multiple administrator accounts.
- More than one administrator session can be running at the same time. These sessions could be using the web interface, command line interface, or a mixture of both. This may cause confusion if each administrator session attempts to modify the same configuration settings – changes made in one session will overwrite changes made in another session.
- You can configure account session limits and inactivity timeouts (see Network Services, page 34).
- If the system is in advanced account security mode, a **Login history** page is displayed immediately after logging in. It shows the recent activity of the currently logged in account.

See the Configuring Administrator Accounts, page 260 section for more information.

FindMe accounts

FindMe accounts are used by individuals in an enterprise to configure the devices and locations on which they can be contacted through their FindMe ID.

Each FindMe account is accessed using a username and password.

- If local FindMe account authentication is selected, each FindMe account must be created locally by the VCS administrator.
- If remote FindMe account authentication is selected, the VCS administrator must set up FindMe groups to match the corresponding group names in the remote directory service. Note that only the username and password details are managed remotely. All other properties of the FindMe account, such as the FindMe ID, devices and locations are stored in the local VCS database.

See the Configuring FindMe Accounts, page 268 section for more information about defining FindMe account details and their associated FindMe devices and locations, and for enabling basic **Starter Pack** provisioning.

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 VCS provides a root account which can be used to log in to the VCS operating system. The **root** account should not be used in normal operation, and in particular system configuration should not be conducted using this account. Use an administrator account instead.

See the Using the Root Account, page 272 section for more information.

SECURITY CAUTION: The pre-X8.9 default passwords of the **admin** and **root** accounts are well known. You must use strong passwords for these accounts. If your new system is on X8.9 or later, you must supply non-default passwords on startup.

Configuring Password Security

The **Password security** page (**Users > Password security**) controls whether or not local administrator account passwords must meet a minimum level of complexity before they are accepted.

If **Enforce strict passwords** is set to *On*, all subsequently configured local administrator account passwords must conform to the following rules for what constitutes a strict password.

If **Enforce strict passwords** is set to *Off*, no extra checks are made on local administrator account passwords.

Notes:

- You can never set a blank password for any administrator account, regardless of this setting.
- This setting affects only local administrator account passwords. It does not affect any other passwords used on the VCS, such as in the local authentication database, LDAP server, external registration credentials, user account passwords, or administrator account passwords stored on remote credential directories.
- All passwords and usernames are case sensitive.

Non-configurable rules for strict passwords

The following password rules always apply when **Enforce strict passwords** is set to *On*. There is no way to configure them:

- Avoid multiple instances of the same characters (non-consecutive instances are checked)
- Avoid three or more consecutive characters such as "abc" or "123"
- Avoid dictionary words, or reversed dictionary words
- Avoid palindromes, such as "risetovotesir"

Configurable rules for strict passwords

The following properties of the password policy can be configured:

- Length must be at least 6 ASCII characters, but can be up to 255 (default 15)
- Number of numeric digits [0-9] may be between 0 and 255 (default 2)
- Number of uppercase letters [A-Z] may be between 0 and 255 (default 2)
- Number of lowercase letters [a-z] may be between 0 and 255 (default 2)
- Number of special characters [printable characters from 7-bit ASCII, eg. (space), @, $ etc.)] may be between 0 and 255 (default 2)
- Number of consecutive repeated characters allowed may be between 1 and 255 (the default 0 disables the check, so consecutive repeated characters are allowed by default; set it to 1 to prevent a password from containing any consecutive repeats)

- The minimum number of character classes may be between 0 and 4 (the default 0 disables the check). Character classes are digits, lowercase letters, uppercase letters, and special characters.

  Note: You may experience precedence effects between the required number of character classes and the number of characters per class.

  For example, if you leave the default requirements of 2 characters of each class, there is an *implied* rule that 4 character classes are required. In this case, any setting of **Minimum number of character classes** is irrelevant.

  For another example, if you set the minimum number of character classes to 2, and set the minimum number of characters required from each class to 0, then a password that contains characters from any two of the classes will suffice (presuming it meets all the other criteria as well).

Configuring Administrator Accounts

The **Administrator accounts** page (**Users > Administrator accounts**) lists all the local administrator accounts on the VCS.

In general, local administrator accounts are used to access the VCS on its web interface or API interface, but are not permitted to access the CLI.

On this page you can:

- Create a new administrator account
- Change an administrator password
- Change the access level of an account: *Read-write*, *Read-only*, or *Auditor*
- Change the access scope of an account: *Web access*, *API access*, or both
- Delete, enable, or disable individual or multiple administrator accounts
- Nominate an emergency account

Editing administrator account details

You can edit the details for the default administrator account and for additional local administrator accounts.

Go to **Users > Administrator accounts**. Under **Actions** for the relevant administrator account, click **Edit user**.

A new page is displayed, where you can edit all fields for the selected administrator account except for the password. To change the password, see below.

About the "admin" account

This default local administrator account has full *Read-write* access and can access the VCS using the web UI, the API interface, or the CLI.

The username for this account is **admin** (all lower case).

Before X8.9, the default password was TANDBERG (all upper case). From X8.9 onwards, new systems run a secure install wizard on startup, so that you can provide new passwords before the system is connected to the network.

You cannot delete, rename, or disable **admin** and you cannot change its access level from *Read-write*, but you can disable its web and API access.

If your system was upgraded from a pre-X8.9 version, you may need to change the password. Choose a strong password, particularly if administration over IP is enabled.

If you forget the password for the **admin** account, you can log in as another administrator account with read-write access and change the password for the **admin** account. If there are no other administrator accounts, or you have forgotten those passwords as well, you can still reset the password for the **admin** account providing you have physical access to the VCS. See Resetting Forgotten Passwords, page 271 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.
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 VCS.	All passwords on the VCS 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 Password security page (**Users > Password security**). You cannot set blank passwords.
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.
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 VCS 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*	

Field	Description	Usage tips
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 VCS.

It displays details of their session including their login time, session type, IP address and port, and when they last accessed this VCS.

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 VCS.

Login History

The **Login history** page is displayed immediately after logging in, when the system is in advanced account security mode. It shows the recent activity of the currently logged in account.

This session

This section shows the login date and time of the currently logged in account, and the IP address from where the login originated.

Previous sessions (for this account)

This section shows the date, time and source IP address of the last successful login for this account. If applicable it also shows details of the last failed login attempt for this account, and the number of failed login attempts since the last successful login.

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. It can also provide user account authentication if you are using FindMe without Cisco TMS.

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 VCS is managed by Cisco TMS.
FindMe authentication source	Defines where FindMe account credentials are authenticated: *Remote*: credentials are verified against an external credentials directory (the VCS currently supports only Windows Active Directory). *Local*: credentials are verified against a local database stored on the VCS. The default is *Local*.	This option applies only if you are using FindMe without Cisco TMS.
LDAP server configuration: this section specifies the connection details to the LDAP server.		
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 VCS 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.

Field	Description	Usage tips
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.	
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*.	When TLS is enabled, the LDAP server's certificate must be signed by an authority within the VCS'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 287 page.
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 VCS's authentication credentials to use when binding to the LDAP server.		
Bind DN	The distinguished name (case insensitive) used by the VCS when binding to the LDAP server. It is important to specify the DN in the order cn=, then ou=, then dc=	Any special characters within a name must be escaped with a backslash as per the LDAP standard (*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 VCS when binding to the LDAP server.	The maximum plaintext length is 60 characters, which is then encrypted.

Field	Description	Usage tips
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 VCS will use to log in to the LDAP server (case sensitive). Only required if SASL is enabled.	Configure this to be the sAMAccountName; Security Access Manager Account Name (in AD this is the account's user logon name).
Directory configuration: this section specifies the base distinguished names to use when searching for account and group names.		
Base DN for accounts	The ou= and dc= definition of the Distinguished Name where a search for user accounts should start in the database structure (case insensitive). It is important to specify the DN in the order ou=, then dc=	This is for authentication of both administrator login and user login requests. 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=	This is for authorization of an authenticated user to log in as an administrator or to log in to a user account. If no **Base DN for groups** is specified, then the Base DN for accounts will be used for both groups and accounts.

Checking the LDAP Server Connection Status

The status of the connection to LDAP server is displayed at the bottom of the page.

State = 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.
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.

Error message	Reason / resolution
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 VCS using a valid group name. If VCS reports "saved" then there is not a problem (the VCS 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 VCS, and lets you add, edit and delete groups.

Administrator groups only apply if remote account authentication is enabled.

When you log in to the VCS web interface, your credentials are authenticated against the remote directory service and you are assigned the access rights associated with the group to which you belong. If the administrator account belongs to more than one group, the highest level permission is assigned.

The configurable options are:

Field	Description	Usage tips
Name	The name of the administrator group. It cannot contain any of the following characters: / \ [ ] : ; | = , + * ? > < @ "	The group names defined in the VCS must match the group names that have been set up in the remote directory service to manage administrator access to this VCS.

Field	Description	Usage tips
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, page 267 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

Configuring FindMe Groups

The **FindMe groups** page (**Users > FindMe groups**) lists all the FindMe groups that have been configured on the VCS, and lets you add, edit and delete groups.

Note that this page does not apply if the VCS is using TMS Provisioning Extension services to provide FindMe account data; in this case, FindMe accounts are maintained through Cisco TMS.

- FindMe groups are only active when remote FindMe authentication is enabled.
- FindMe groups determine which access rights members of the group have after they have been successfully authenticated to use the VCS.

When a FindMe user logs in to the VCS their credentials are authenticated against the remote directory service and they are assigned the access rights associated with the group to which that user belongs. If the user account belongs to more than one group, the highest level permission is assigned.

The configurable options are:

Field	Description	Usage tips
Name	The name of the FindMe group. It cannot contain any of the following characters: / \ [ ] : ; | = , + * ? > < @ "	The group names defined in the VCS must match the group names that have been set up in the remote directory service to manage FindMe accounts.
State	Indicates if the group is enabled or disabled. *Enabled*: users can view and modify their personal FindMe details, devices and locations. *Disabled*: users are not allowed to log in to their account. Default: *Enabled*	

Configuring FindMe Accounts

The **FindMe accounts** page (**Users > FindMe accounts**) lists all the FindMe accounts that have been configured on the VCS, and lets you add, edit and delete accounts.

Note that this page does not apply if the VCS is using TMS Provisioning Extension services to provide FindMe account data; in this case, FindMe accounts are maintained through Cisco TMS.

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 local FindMe account authentication is selected, each FindMe account must be created locally by the VCS administrator.
- If remote FindMe account authentication is selected, the VCS administrator must set up FindMe groups to match the corresponding group names in the remote directory service.

Filtering the view

The **Filter** section lets you filter the set of records. Enter the word or phrase you want to search for and click **Filter**. Only those records that contain the word or phrase you entered are shown.

Configuring an account

Click **New** to set up a new account, or click **View/Edit** (or the username) to edit an existing FindMe account.

The configurable options for a FindMe account are:

Field	Description	Usage tips
Username	The account name. It is used (along with a password) by the user to log in to the VCS and configure their FindMe details. The username cannot be changed after the account has been created.	If remote authentication is enabled, the username defined in the VCS must match the username set up in the remote directory service.
Display name	A free-form display name for the user (rather than the user's **Username** or **FindMe ID**).	The **Display name** is used in phone books and as the caller display name in SIP calls.
Phone number	The numeric caller ID presented when making an outbound call through an ISDN gateway.	To allow call return, this number could be configured to route to the associated FindMe ID by mapping incoming numbers to the FindMe ID using ENUM, search rules or CPL. See *FindMe Deployment Guide* for more information.
FindMe ID	The FindMe alias – the dialable address – by which the user can be contacted.	The **FindMe ID** can be any string of up to 60 characters. However, not all endpoints are able to dial aliases with spaces or other non-alphanumeric characters so we recommend that these are not used in your FindMe IDs.
Principal device address	The address or alias of the user's first principal device. An administrator (or FindMe users themselves) can add more endpoint addresses after an account has been created.	After the account has been created any non-principal devices (including any devices added by FindMe users themselves) can be set as principal devices. This has the effect of stopping the user from being able to delete that device. To do this, click **Edit principal devices** from the **Edit FindMe account** page. If the **Starter Pack** option key is installed, there is a separate section for specifying the user's principal devices (see below).
Password	The password to be used, along with the **Username**, when logging into this account. You must confirm any new or modified password.	FindMe users can change their password after they have logged in. Note that passwords are case sensitive, and that the password fields are not shown if remote authentication is enabled.

Field	Description	Usage tips
FindMe type	Specifies if the account is for an individual person or a group of people, and affects how calls are diverted when endpoints in the user's primary list are busy. *Individual*: calls immediately divert if any primary endpoint is busy. *Group of people*: calls immediately divert only if all primary endpoints are busy.	If the **Starter Pack** option key is installed all FindMe IDs are created as *Individual* accounts.

You can control general FindMe behavior, including whether users are allowed to add their own devices, on the Configuring FindMe, page 247 page.

Principal devices (Starter Pack)

The **Principal devices** section is used to specify the principal devices that are associated with the FindMe profile and to enable provisioning for those devices. This section only displays if the **Starter Pack** option key is installed.

Principal devices are devices assigned to the profile by the system administrator and cannot be deleted by the FindMe user. Note that users can add other, non-principal, devices to their FindMe profiles.

To assign a principal device, select *On* for the relevant device type. The page will then display the URI that will be assigned for that user and device type. You can assign as many devices as required.

The device URI is based on a combination of the **Username**, **FindMe ID** and device type. It takes the format `<username>.<device type>@<domain portion of FindMe ID>`.

For example, if the **Username** is `Alice.Smith` and the **FindMe ID** is `asmith@example.com`, then the URI for an E20 device would be `alice.smith.e20@example.com`.

- Each selected device is automatically provisioned (with bandwidth limits and phone book information, for example) when that device registers to the VCS.
- You can specify an additional principal device by setting **Other device** to *On* and then specifying the required **URI** of the device. If required, you can add further non-principal devices by clicking **Edit user** from the **Edit FindMe account** page.

Note that the VCS only sends provisioning information to the pre-configured device types (Jabber Video, E20 and so on). Other principal devices added by the administrator or any other devices added by the FindMe user are not provisioned by the VCS.

If your system's authentication policy is configured to check credentials, then authentication credentials for the provisioned devices must be set up in the relevant credential store (typically the local database). The credential name must be the same as account username and the credential password must be the same as the password configured on the provisioned devices. See About Device Authentication, page 99 for more information.

Note: all device address URIs are converted to lower case.

Configuring a FindMe Account's Principal Devices

The **Edit principal devices** page (**Users > FindMe accounts**, click **View/Edit** or the username to open the **Edit FindMe account** page, and then click **Edit principal devices**) is used to configure which of the user's devices are their principal devices associated with their FindMe ID.

Note that this page does not apply if the VCS is using TMS Provisioning Extension services to provide FindMe account data; in this case, FindMe accounts are maintained through Cisco TMS.

Users are not allowed to delete or change the address of their principal devices; they can only change the **Device name**. This is to stop users from unintentionally changing their basic FindMe configuration. Principal devices are also

used by the VCS to decide which FindMe name to display as a **Caller ID** if the same device address is associated with more than one account.

The page lists all of the devices currently associated with the selected user. The **Principal device** column indicates each device's current status as a principal device or not.

- To set devices as a principal device, select the box next to the required devices and click **Set as principal device**.
- To set devices so they are no longer principal devices, select the required devices and click **Unset as principal device**.

Note that only an administrator (and not users themselves) can configure which of a user's devices are their principal devices.

Active FindMe Sessions

Note that this page does not apply if the VCS is using TMS Provisioning Extension services to provide FindMe account data; in this case, FindMe accounts are maintained through Cisco TMS.

The **Active FindMe sessions** page (**Users > Active FindMe sessions**) lists all FindMe accounts that are currently logged in to this VCS.

It displays details of their session including their login time, IP address and port, and when they last accessed this VCS.

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 a user ends their session by closing down their browser without first logging out of the VCS.

Resetting Forgotten Passwords

You can reset any account password by logging in to the VCS as the default **admin** account or as any other administrator account that has read-write access. If this is not possible you can reset the **admin** or **root** password via the console.

Note: Stored configuration and data will not be affected when you reset your password.

Changing an Administrator Account Password via GUI

You can change the password for the default administrator account and for additional local administrator accounts.

Go to **Users > Administrator accounts**. Under **Actions** for the relevant administrator account, click **Change password**.

A new page is displayed, where you can change the password for the selected administrator. Enter the new password and confirm it. You must also enter the password for the administrator account with which you are currently logged in to authorize the password change.

Resetting Root or Admin Password via Serial Connection

On a hardware VCS, reset the **admin** or **root** password as follows:

1. Connect a PC to the VCS using the serial cable as per the instructions in *VCS Getting Started Guide*. Serial port / console access is always enabled for one minute following a restart, even if it is normally disabled.
2. Restart the VCS.
3. Log in from the PC with the username **pwrec**. No password is required.
4. If the administrator account authentication source is set to *Remote*, you are given the option to change the setting to *Both*; this will allow local administrator accounts to access the system.

5. Select the account (**root** or **admin**) whose password you want to change.
6. You will be prompted for a new password.

The **pwrec** account is only active for one minute following a restart. After that time you will have to restart the system again to change the password.

Resetting Root or Admin Password via vSphere

If you have forgotten the password for either an administrator account or the **root** account and you are using a VM (Virtual Machine) VCS, you can reset it using the following procedure:

1. Open the vSphere client.
2. Click on the link **Launch Console**.
3. Reboot the VCS.
4. In the vSphere console log in with the username `pwrec`. No password is required.
5. When prompted, select the account (*root* or the username of the administrator account) whose password you want to change.
6. You will be prompted for a new password.

The **pwrec** account is only active for one minute following a reboot. After that time you will have to reboot the system again to reset the password.

Resetting FindMe Account Passwords

To change a password on behalf of a FindMe user without knowing their existing password (for example, when a user forgets their password):

1. Go to the **Edit FindMe account** page (**Users > FindMe accounts**, then click **View/Edit** or the username) for the account whose password you want to reset.
2. Enter the new password to be used when logging into this account into the **New password** and **Confirm password** fields and click **Save**.

This procedure only applies if local FindMe account authentication is enabled. If remote authentication is enabled, passwords are managed through your remote directory server instead.

Using the Root Account

The VCS provides a root account which can be used to log in to the VCS operating system. This account has a username of **root** (all lower case) and a default password of **TANDBERG** (all upper case). For security reasons you must change the password as soon as possible. An alarm is displayed on the web interface and the CLI if the **root** account has the default password set.

Note: the **root** account may allow access to sensitive information and it should not be used in normal operation, and in particular system configuration should not be conducted using this account. Use the **admin** account instead.

Changing the Root Account Password

To change the password for the **root** account:

1. Log in to the VCS as **root** using the existing password. By default you can only do this using a serial connection or SSH.
2. Type the command `passwd`.
   You will be asked for the new password.
3. Enter the new password and when prompted, retype the password.
4. Type `exit` to log out of the root account.

Accessing the Root Account Over SSH

The root account can be accessed over a serial connection or SSH only.

To enable and disable access to the root account using SSH:

1. Log in to the VCS as **root**.
2. Type one of the following commands:
   - `rootaccess --ssh on` to enable access using SSH
   - `rootaccess --ssh off` to disable access using SSH
3. Type `exit` to log out of the root account.

If you have disabled SSH access while logged in using SSH, your current session will remain active until you log out, but all future SSH access will be denied.

Managing SSO tokens

Note: This page applies to standard OAuth tokens configured by the **Authorize by OAuth token** setting. It does not apply to self-describing OAuth tokens (configured by **Authorize by OAuth token with refresh**).

Go to **Users > SSO token holders** to view the list of users who currently hold SSO tokens. This page can help you troubleshoot issues related to single sign-on for a particular user.

You can also use this page to **Purge tokens from all holders**. This option is probably disruptive for your users so make sure you need it before you proceed. You may need it, for example, if you know your security is compromised, or if you are upgrading internal or edge infrastructure.

To manage the tokens of a particular user:

1. [Optional] Filter by a substring of the username to return a smaller list.

   You may need this if there are many usernames in the list, because a long list spans multiple pages of up to 200 usernames each.
2. Click a username to see the detail of the tokens held by that user.

   The **SSO tokens for user *<Username>*** page appears, listing details of the tokens issued to that user. The details include the token issuer and expiry.
3. [Optional] Click **Delete these tokens** if you want the user's identity to be confirmed before they continue to access the UC services.

   The next time the user's client attempts to access UC services via this VCS Control, 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 VCS Control. The user can then be issued with new tokens where authorized.

Maintenance

This section describes the pages that appear under the **Configuration > Maintenance** menu of the VCS web interface.

Enabling SSH access 275
Enabling Maintenance Mode 276
Upgrading Software Components 276
Upgrading Firmware (Physical Appliances Only) 279
Configuring Logging 279
Managing Option Keys 284
About Security 286
Managing Domain Certificates and Sever Name Indication for Multitenancy 301
Domain Certificates and Clustered Systems 304
Advanced Security 305
Configuring Language Settings 309
Backing Up and Restoring VCS Data 310
Diagnostics Tools 313
Incident Reporting 316
Checking the Effect of a Pattern 318
Locating an Alias 319
Serviceability 319
Port Usage 320
Network Utilities 321
Restarting, Rebooting and Shutting Down 326
Developer Resources 327

Enabling SSH access

You may want to enable SSH access to the VCS 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 VCS that you want to access in this way.

Caution: You will use root access to authorize your public key. Take care not to increase your security exposure or cause any unsupported configuration. We strongly discourage using `root`.

1. Use SSH to log in as `root`
2. Enter `mkdir /tandberg/.ssh` to create `.ssh` directory if it is not already present

3. Copy your public key to `/tandberg/.ssh`
4. Append your public key to the `authorized_keys` file with `cat /tandberg/.ssh/id_rsa.pub >> /tandberg/.ssh/authorized_keys`

   where *id_rsa.pub* is substituted with the name of your public key. Do not place your key anywhere else because the key could be lost on upgrade (`authorized_keys` file does persist)
5. Log off and test SSH access using your own key

   If you cannot access the VCS with your key, you may need to connect as `root` and restart the SSH daemon with `/etc/init.d/sshd restart`

Enabling Maintenance Mode

Maintenance mode is typically used when you need to upgrade or take out of service a VCS peer that is part of a cluster. It allows the other cluster peers to continue to operate normally while the peer that is in maintenance mode is upgraded or serviced.

Putting a peer into maintenance mode provides a controlled method of stopping any further registrations or calls from being managed by that peer:

- Standard VCS sessions:
  - New calls and registrations will be handled by another peer in the cluster.
  - Existing registrations are allowed to expire and they then should re-register to another peer (see *VCS Cluster Creation and Maintenance Deployment Guide* for more information about endpoint configuration and setting up DNS SRV records).
  - Existing calls will continue until the call is terminated. If necessary, you can manually remove any calls on this peer that do not clear automatically by going to **Status > Calls**, selecting the check box next to the calls you want to terminate and clicking **Disconnect** (note that SIP calls may not disconnect immediately).
- Unified CM mobile and remote access sessions:
  - Any existing calls passing through that VCS will be dropped.
  - Jabber clients will failover automatically and re-register through another peer in the cluster.
  - Clients running TC software will not failover automatically will have to be restarted.

To maintain capacity, we recommend that you only enable maintenance mode on one peer at a time.

To enable maintenance mode:

1. Log in the relevant peer.
2. Go to the **Maintenance mode** page (**Maintenance > Maintenance mode**).
3. Set **Maintenance mode** to *On*.
4. Click **Save** and click **OK** on the confirmation dialog.

Note that:

- An alarm is raised while the peer is in maintenance mode.
- You can monitor the **Resource usage** page (**Status > System > Resource usage**) to check how many registrations and calls are currently being handled by that peer.
- Maintenance mode is automatically disabled if the peer is restarted.
- Maintenance mode is not supported by Cisco DX Series endpoints. The Expressway drops MRA calls from these endpoints when you enable maintenance mode.

Upgrading Software Components

You can install new releases of the VCS software components on your existing hardware. Component upgrades can be performed in one of two ways:

- Using the web interface – this is the recommended process.
- Using secure copy (SCP/PSCP).

This guide describes how both of these methods are used to perform upgrades. You can also upgrade the **System platform** component using Cisco TMS (see the Cisco TMS documentation for more information).

- We recommended that you upgrade VCS components while the system is inactive.
- From X8.8 onwards, the VCS release packages are signed to give you confidence in their integrity.
- If your VCS is registered for Hybrid Services: **Important! Your Management Connector must be up to date before you upgrade your VCS. You must authorize and accept any Management Connector upgrades advertised by the Cisco Collaboration Cloud before attempting to upgrade your VCS. Failure to do so may cause issues with the connector once you have upgraded your VCS.**
- If you are upgrading a cluster:

  See *VCS Cluster Creation and Maintenance Deployment Guide* on the VCS Configuration Guides page.
- If you are currently running non-clustered VCS X5.1, X5.1.1 or X5.2, you must first upgrade to X6.1, then upgrade from X6.1 to X8.n.
- If you are currently running non-clustered VCS X5.0 or earlier, you must first upgrade to X5.2, then upgrade from X5.2 to X6.1, and then upgrade from X6.1 to X8.n.

VCS software components

All existing installed components are listed on the **Upgrade** page (**Maintenance > Upgrade**), showing their current version and associated release key where appropriate.

The main component is the **System platform**, and when upgraded this will typically include automatic upgrades of some or all of the other components. However, you can independently upgrade the other components if required to do so. The upgrade process ensures that compatibility is maintained across all components.

Upgrade prerequisites

The upgrade requires you to have:

- a valid **Release key**, if you are upgrading to the next major release of the **System platform**, for example from X7.2 to X8.1; it is not required for dot releases, for example X8.1 to X8.2
- a software image file for the component you want to upgrade, and it is stored in a network location that is locally accessible from your client computer; use the standard .tar.gz software image file when upgrading a virtual machine (the .ova file is only required for the initial install of the VCS software on VMware)
- release notes for the software version you are upgrading to – additional manual steps may be required

Contact your Cisco representative for more information on how to obtain these.

Backing up before upgrading

You should backup your system configuration before upgrading. Click **System backup** to go to the Backup and restore page.

Upgrading and option keys

All existing option keys are retained through the upgrade from one version of the **System platform** to the next, including upgrades to the next major release. However, you are recommended to take note of your existing option keys before performing the upgrade.

New features may also become available with each major release of the **System platform** component, and you may need to install new option keys to take advantage of these new features. Contact your Cisco representative for more information on all the options available for the latest release of VCS software.

Installing and rebooting

Upgrading the **System platform** component is a two-stage process. First, the new software image is uploaded onto the 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 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.

Note: Any configuration changes you make between the software upload and the reboot will be lost when the system restarts using the new software version.

The upgrade of components other than the **System platform** does not involve a system reboot, however the services provided by that component will be temporarily stopped while the upgrade process completes.

Upgrading VCS Software

The **Upgrade** page (**Maintenance > Upgrade**) is used to install new versions of VCS software components. (Downgrading to an older version is not supported.)

As well as these instructions, a video demonstration of the process – provided by Cisco TAC engineers – is available on the Expressway/VCS Screencast Video List page.

To upgrade a component using the web interface:

1. Review the relevant release notes to see if any special steps are required either before or after installing the software image file.
2. Go to the **Upgrade** page (**Maintenance > Upgrade**).
3. Click **Browse** and select the software image file for the component you want to upgrade.
   The VCS automatically detects which component you are upgrading based upon the selected software image file.
4. Enter the **Release key** if required.
5. Click **Upgrade**.
   The VCS will start loading the file. This may take a few minutes.
6. For upgrades to the **System platform** component, the **Upgrade confirmation** page is displayed:
   a. Check that:
      - the expected **New software version** number is displayed
      - the **MD5 hash** and **SHA1 hash** values match the values displayed on the cisco.com page, where you have downloaded the software image file

   b. Click **Continue with upgrade**.
      The **System upgrade** page opens and displays a progress bar while the software installs.
      When the software has installed, a summary of active calls and registrations is displayed. These will be lost when you reboot the system.

   c. Click **Reboot system**.
      Note that if you make any configuration changes between uploading the software and rebooting, those changes will be lost when the system restarts.
      After the reboot is complete you are taken to the **Login** page.
7. For upgrades to other components, the software is automatically installed. No reboot is required.

The upgrade is now complete. The **Overview** and **Upgrade** pages now show the upgraded software component version numbers.

Note that some components may require option keys to enable them; this is done through the Option keys page (**Maintenance > Option keys**).

Upgrading Using Secure Copy (SCP/PSCP)

To upgrade using a secure copy program such as SCP or PSCP (part of the PuTTY free package) you need to transfer two files to the VCS:

- A text file containing just the 16-character Release Key (required for the **System platform** component only). Ensure there is no extraneous white space in this file.
- The file containing the software image.

To transfer these files:

1. If you are upgrading the **System platform** component, upload the Release Key file using SCP/PSCP to the **/tmp/** folder on the system. The target name must be **release-key**, for example:
   `scp release-key root@10.0.0.1:/tmp/release-key`
   - Enter the root password when prompted.
   - The Release Key file must be uploaded before the image file.
2. Upload the software image using SCP/PSCP.
   - For the **System platform** component:

     Upload to the **/tmp** folder on the system. The target name must be **/tmp/tandberg-image.tar.gz**, for example: `scp s42700x8_1_0.tar.gz root@10.0.0.1:/tmp/tandberg-image.tar.gz`
   - For other components:

     Upload to the **/tmp/pkgs/new/** folder on the system, preserving the file name and extension, for example:
     `scp root@10.0.0.1:/tmp/pkgs/new/vcs-lang-es-es_8.1_amd64.tlp`
3. Enter the root password when prompted.
   The software installation begins automatically. Wait until the software has installed completely. This should not take more than five minutes.
4. If you have upgraded the **System platform** component, log in to the VCS, either using the web interface or CLI, and reboot the VCS. After about five minutes the system will be ready to use.

Note: if you make any further configuration changes before rebooting, those changes will be lost when the system restarts, so you are recommended to reboot your system immediately.

Upgrading Firmware (Physical Appliances Only)

This section applies if VCS 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.

Configuring Logging

The VCS provides syslogging features for troubleshooting and auditing purposes.

The Event Log is a rotating local log that records information about such things as calls, registrations, and messages sent and received.

The VCS's logging options are configured on the **Logging** page (**Maintenance > Logging**) where you can:

- specify the Local event log verbosity to change the depth of event information recorded locally
- toggle Media statistics logging
- toggle Call Detail Records
- toggle Certification-compliant logging

- define one or more remote syslog server addresses
- filter the events sent to each remote syslog server by severity
- toggle System Metrics Collection

Changing Event Log Verbosity

Control the local log verbosity by setting the **Local event log verbosity** between *1* and *4*.

All events have an associated level in the range 1–4, with Level 1 Events considered the most important. The table below gives an overview of the levels assigned to different events.

Level	Assigned events
1	High-level events such as registration requests and call attempts. Easily human readable. For example: ■ 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 VCS, and the level at which they are logged.

Notes:

- Events are always logged locally (to the Event Log) regardless of whether or not remote logging is enabled.
- Logging at level 3 or level 4 is not recommended for normal operation, because such detailed logging may cause the 2GB log to rotate too quickly. You may need to record this level of detail while troubleshooting.
- Changes to the log level affect both the Event Log that you can view via the web interface, and the information that is copied to any remote log server.
- Changes to the log level are not retrospective – they only affect what is logged after you change the level.
- The VCS uses the following facilities for local logging. The software components / logs that map to the (local) facilities are emphasised:
  - 0 (kern)
  - 3 (daemon)
  - 16 (local0) *Administrator*
  - 17 (local1) *Config*
  - 18 (local2) *Mediastats*
  - 19 (local3) *Apache error*
  - 20 (local4) *etc/opt/apache2*
  - 21 (local5) *Developer*
  - 22 (local6) *Network*

Media Statistics Logging for Calls

How to Enable Media Statistics

To optionally enable media statistics collection on the VCS, 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 VCS 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.

Call Detail Records (CDRs)

Subject to enabling the service (which is off by default) VCS 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

1. Go to **Maintenance > Logging**.
2. In the **Logging options** section, set the **Call Detail Records (CDR)** field to your required option:

CDR mode	Description
Off	CDRs are not logged locally (default).
Service Only	CDRs are stored locally for 7 days and then deleted. The records are not accessible through the web GUI and can only be read through the REST API to the VCS.

Services and Logging	CDRs are stored locally for 7 days and then deleted. The records are accessible from the local Event Log and the external syslog server (sent as INFO messages to the syslog host).

For more information about CDRs:

See the *Cisco VCS Serviceability Guide* on the VCS Maintain and Operate Guides page.

Certification-compliant Logging

In some environments you may want to ensure that the VCS 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; in the certification-compliant modes it may be impossible to establish the exact cause of a problem call.

How to Configure Certification-compliant Logging

1. Go to **Maintenance > Logging**.
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 VCS to publish log messages to up to 4 remote syslog servers.
- The syslog servers must support one of the following standard protocols:
  - BSD (as defined in *RFC 3164*)
  - IETF (as defined in *RFC 5424*)

Configuring Remote Syslog Servers

1. Go to **Maintenance > Logging**, and enter the IP addresses or Fully Qualified Domain Names (FQDNs) of the **Remote syslog servers** to which this system will send log messages.
2. Click on the **Options** button for each server.
3. Specify the **Transport** protocol and **Port** you wish to use. If you choose to use TLS, you will see the option to enable Certificate Revocation List (CRL) checking for the syslog server.
4. In the **Message Format** field, select the writing format for remote syslog messages. The default is *Legacy BSD*.
5. Use the **Filter by Severity** option to select how much detail to send. The VCS sends messages of the selected severity and all of the more severe messages.
6. Use the **Filter by Keywords** option if you only want to send messages with certain keywords.
7. Click **Save**.

Notes:

- The **Filter by Keywords** option is applied to messages already filtered by severity.
- You can use up to five keywords, which includes groups of words (for example 'login successful'), separated by commas.
- You can use a maximum of 256 characters in the keyword search.
- We recommend that you search for the most relevant keywords first to avoid any impact on system performance. This ensures the system pushes the relevant log messages to the syslog server at the earliest opportunity.

What are the Typical Values used for my Syslog Server?

The following table should help you select the format that best matches your logging server(s) and network configuration and shows the typical values used.

Table 16 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

Notes:

- The UDP protocol is stateless. If reliability of syslog messages is very important in your environment, you should use a different transport protocol.
- If there is a firewall between the VCS and the syslog server, you must open the appropriate port to allow the messages through.
- If you select TLS transport, the VCS must trust the syslog server's certificate. Upload the syslog server's CA certificate to the local trust store if necessary.
- CRL checking when using TLS is disabled by default. To enable CRL, set **CRL checking** to *On* and ensure that relevant certificate revocation lists (CRLs) are loaded.

  See About Security, page 286 for more information.
- The remote server cannot be another VCS.
- A VCS cannot act as a remote log server for other systems.
- The VCS uses the following facilities for remote logging. The software components / logs that map to the (local) facilities are emphasised:
  - 0 (kern)
  - 3 (daemon)
  - 16 (local0) *Administrator*
  - 17 (local1) *Config*
  - 18 (local2) *Mediastats*
  - 19 (local3) *Apache error*
  - 20 (local4) *etc/opt/apache2*
  - 21 (local5) *Developer*
  - 22 (local6) *Network*

Configure System Metrics Collection on VCS

In the following procedure you'll use the web interface to configure the VCS to collect statistics and publish them to a specified server.

1. Log on to the VCS and go to **Maintenance > Logging**.
2. Toggle **System Metrics Collection** to *On*.
3. Enter the **Collection server address**.

   You can use IP address, hostname or FQDN to identify the remote server.
4. Change the **Collection Interval** and **Collection server port** if necessary.

   You may need to change the port if the collection server is listening on a non-default port. You may need to change the collection interval if your policy requires finer-grained metrics than the default interval (*60*s).
5. Click **Save**.

Managing Option Keys

Options are used to add additional features to the VCS. Option keys can be valid for a fixed time period or for an unlimited duration. The VCS may have been shipped with one or more optional features pre-installed. To purchase further options, contact your Cisco representative.

The **Option keys** page (**Maintenance > Option keys**) lists the existing options currently installed on the VCS, and allows you to add new options.

The **System information** section summarizes the existing features installed on the VCS and displays the **Validity period** of each installed key. The options that you may see here include:

- **Traversal Server**: enables the VCS to work as a firewall traversal server.
- **H.323 to SIP Interworking gateway**: enables H.323 calls to be translated to SIP and vice versa.
- **Starter Pack**: allows the VCS to offer basic device provisioning without the need for Cisco TMS (see Provisioning (Starter Pack)).
- **Traversal calls**: determines the number of traversal calls allowed on the VCS (or VCS cluster) at any one time. Note that traversal calls that are passing through the VCS from one neighbor to another but where neither endpoint in the call is locally registered will still be counted as one traversal call. See the Call Types and Licensing, page 389 section for more information.
- **Non-traversal calls**: determines the number of non-traversal calls allowed on the VCS (or VCS cluster) at any one time. Note that non-traversal calls that are passing through the VCS from one neighbor to another but where neither endpoint in the call is locally registered may or may not require a non-traversal call license, depending on the Call signaling optimization setting. Note that a non-traversal call on a VCS Expressway will consume a traversal license if there are no non-traversal call licenses available.
- **Registrations**: the number of concurrent registrations allowed on the VCS. An endpoint can register with more than one alias and this will be considered to be a single registration. However, an endpoint that supports both SIP and H.323 and registers using both protocols will count as two registrations. H.323 systems such as gateways, MCUs and Content Servers can also register with the VCS, and these will each count as one registration.
- **Encryption**: indicates that AES encryption is supported by this software build.
- **Advanced account security**: enables advanced security features and restrictions for high-security installations.
- **Microsoft Interoperability**: enables encrypted calls to and from Microsoft Lync 2010 Server (for both native SIP calls and calls interworked from H.323). It is also required by the Lync B2BUA when establishing ICE calls to Lync 2010 clients. It is required for all types of communication with Lync 2013.

See License Usage Within a Cluster, page 159 for more information about how traversal call, non-traversal call and TURN relay option key licenses are shared across all peers in the cluster.

See Product Identifiers and Corresponding Keys, page 390, for all option keys and associated PIDs.

Adding Keys

You can add option keys through the web UI or the CLI.

As well as these instructions, a video demonstration of the process – provided by Cisco TAC engineers – is available on the Expressway/VCS Screencast Video List page.

65 option key limit

If you try to add more than 65 option keys (licenses), they appear as normal on the **Option keys** page. However, only the first 65 keys take effect. Additional keys from 66 onwards appear to be added, but actually the VCS does not process them. CDETS CSCvf78728 refers.

Before you start

1. Have the option keys available.
2. Remove any demo option keys you already have on the system for the options in question, and restart the system. Otherwise the feature may stop working when the time-limited demo key expires.

Adding option keys using the web UI

1. In the **Add option key** field, enter the key for the option you want to add.
2. Click **Add option**.

Some option keys need a system restart before they take effect, including:

- Traversal Server
- Starter Pack
- Expressway Series
- Advanced Account Security (if moved into FIPS mode)

If a restart is required, you get an alarm on the web interface, which remains as a notification until you restart. You can continue to use and configure the VCS in the meantime.

Adding option keys using the CLI

To return the indexes of all the option keys that are already installed on your system:

```
xStatus Options
```

To add a new option key to your system:

```
xConfiguration Option [1..64] Key
```

Note: when using the CLI to add an extra option key, you can use any unused option index. If you chose an existing option index, that option will be overwritten and the extra functionality provided by that option key will no longer exist. To see which indexes are currently in use, type `xConfiguration option`.

About Security

Data at Rest

From X8.11, every software installation has a unique root of trust. Each VCS system, including hardware versions and VM versions has a unique key that is used to encrypt data local to that system. This improves the security of your 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 VCS key can decrypt this system's data.
- The key is never exposed on the UI. It is never logged, either locally or remotely.

TLS and Certificates

For extra security, you may want to have the VCS communicate with other systems (such as LDAP servers, neighbor VCSs, or clients such as SIP endpoints and web browsers) using TLS encryption.

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

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

The VCS lets you install a certificate that can represent the VCS as either a client or a server in connections using TLS. The VCS can also authenticate client connections (typically from a web browser) over HTTPS. You can also upload certificate revocation lists (CRLs) for the CAs used to verify LDAP server and HTTPS client certificates.

The VCS can generate server certificate signing requests (CSRs). This removes the need to use an external mechanism to generate certificate requests.

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

Table 17 VCS Role in Different Connection Types

In connections...	The VCS acts as...
To an endpoint.	TLS server.
To an LDAP server.	Client.
Between two VCS systems.	Either VCS may be the client. The other VCS is the TLS server.
Over HTTPS.	Web browser is the client. VCS is the server.

TLS can be difficult to configure. For example, when using it with an LDAP server we recommend verifying that the system works correctly over TCP, before you attempt to secure the connection with TLS. We also recommend using a third-party LDAP browser to verify that your LDAP server is correctly configured for TLS.

Note: Be careful not to allow your CA certificates or CRLs to expire. This may cause certificates signed by those CAs to be rejected.

Certificate and CRL files can only be managed via the web interface. They cannot be installed using the CLI.

More Information

For detailed information about working with certificates see the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page.

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 VCS. When a TLS connection to VCS mandates certificate verification, the certificate presented to the VCS must be signed by a trusted CA in this list and there must be a full chain of trust (intermediate CAs) to the root CA.

- To upload a new file containing one or more CA certificates, **Browse** to the required PEM file and click **Append CA certificate**. This will append any new certificates to the existing list of CA certificates. If you are replacing existing certificates for a particular issuer and subject, you have to manually delete the previous certificates.
- To replace all of the currently uploaded CA certificates with the system's original list of trusted CA certificates, click **Reset to default CA certificate**.
- To view the entire list of currently uploaded trusted CA certificates, click **Show all (decoded)** to view it in a human-readable form, or click **Show all (PEM file)** to view the file in its raw format.
- To view an individual trusted CA certificate, click on **View (decoded)** in the row for the specific CA certificate.
- To delete one or more CA certificates, tick the box(es) next to the relevant CA certificate(s) and click **Delete**.

Note: if you have enabled certificate revocation list (CRL) checking for TLS encrypted connections to an LDAP server (for account authentication), you must add the PEM encoded CRL data to your trusted CA certificate file.

Managing the VCS's Server Certificate

You manage the VCS's server certificate through the **Server certificate** page (**Maintenance > Security > Server certificate**). This certificate is used to identify the VCS when it communicates with client systems using TLS encryption, and with web browsers over HTTPS. You can use the **Server certificate** page to:

- View details about the currently loaded certificate.
- Generate a certificate signing request.
- Upload a new server certificate.

  Note: We highly recommend using certificates based on RSA keys. Other types of certificate, such as those based on DSA keys, are not tested and may not work with the VCS in all scenarios.
- (On Expressway-E) Configure the Automated Certificate Management Environment (ACME) service to automatically submit a CSR to an ACME provider, and automatically deploy the resulting server certificate.

Viewing the currently uploaded certificate

The **Server certificate data** section shows information about the server certificate currently loaded on the VCS.

- To view the currently uploaded server certificate file, click **Show (decoded)** to view it in a human-readable form, or click **Show (PEM file)** to view the file in its raw format.
  If a certificate contains SRV-ID or XMPP-ID formatted entries, when that certificate is viewed those entries will show as '<unsupported>'. That does not mean the certificate is invalid, but that the openssl code does not know how to display those identifiers.
- To replace the currently uploaded server certificate with the VCS's original certificate, click **Reset to default server certificate**.

Note: Do not allow your server certificate to expire as this may cause other external systems to reject your certificate and prevent the VCS from being able to connect to those systems.

Generating a certificate signing request (CSR)

The VCS can generate server certificate signing requests. This removes the need to use an external mechanism to generate and obtain certificate requests.

To generate a CSR:

1. Go to **Maintenance > Security > Server certificate**.
2. Click **Generate CSR** to go to the **Generate CSR** page.
3. Enter the required properties for the certificate.
   - See Server Certificates and Clustered Systems, page 289 if your VCS is part of a cluster.
   - See Server Certificate Requirements for Unified Communications, page 61 if this VCS is part of a Unified Communications solution.
   - The certificate request includes automatically the public key that will be used in the certificate, and the client and server authentication Enhanced Key Usage (EKU) extension.
4. Click **Generate CSR**. The system will produce a signing request and an associated private key.

   The private key is stored securely on the VCS and cannot be viewed or downloaded. You must never disclose your private key, not even to the certificate authority.
5. You are returned to the **Server certificate** page. From here you can:
   - **Download** the request to your local file system so that it can be sent to a certificate authority. You are prompted to save the file (the exact wording depends on your browser).
   - View the current request (click **Show (decoded)** to view it in a human-readable form, or click **Show (PEM file)** to view the file in its raw format).
   - Use ACME to manually or automatically submit the CSR to a CA that signs ACME certificates.

Note:

- Only one signing request can be in progress at any one time. This is because the VCS has to keep track of the private key file associated with the current request. To discard the current request and start a new request, click **Discard CSR**.
- From version X8.5.1 the user interface provides an option to set the Digest algorithm. The default is set to SHA-256, with options to change to SHA-1, SHA-384, or SHA-512.
- From version X8.10, you cannot select SHA-1.
- The Issuer and Subject fields of certificates returned by Let's Encrypt do not include attributes like State, Country, and Organisation. The Expressway UI still requires you to complete these fields in the CSR, even though the authority ignores them.

Uploading a new server certificate

When the signed server certificate is received back from the certificate authority it must be uploaded to the VCS. Use the **Upload new certificate** section to replace the VCS's current server certificate with a new certificate.

To upload a server certificate:

1. Go to **Maintenance > Security > Server certificate**.
2. Use the **Browse** button in the **Upload new certificate** section to select and upload the **server certificate** PEM file.
3. If you used an external system to generate the Certificate Signing Request (CSR) you must also upload the **server private key** PEM file that was used to encrypt the server certificate. (The private key file will have been automatically generated and stored earlier if the VCS was used to produce the CSR for this server certificate.)
   - The **server private key** PEM file must not be password protected.
   - You cannot upload a server private key if a certificate signing request is in progress.
4. Click **Upload server certificate data**.

ACME (Automated Certificate Management Environment) 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 VCS Expressway from a certificate

authority such as Let's Encrypt. The main benefit of this feature is to generate low-cost server certificates to identify the VCS Expressway, thereby reducing the cost of Expressway-based deployments like MRA (Mobile and Remote Access).

Due to the underlying validation mechanism this feature is most likely to be useful for MRA deployments. For Business to Business (B2B) applications, it's not always practical to include your primary domain in ACME certificates.

The configuration process is simple. You enter some information on the VCS Expressway to create a certificate signing request (CSR), then the Expressway's ACME client interacts with the certificate authority to request the certificate. The Expressway downloads the certificate and you click a button to deploy it. After this manual step, you can schedule renewal so that the certificate does not expire—because ACME certificates are deliberately short-lived.

One compromise of the ACME protocol is that it requires an inbound HTTP connection to port 80 on the VCS Expressway. You can manage this risk with the Expressway's security features or, for highly secure environments, you can disable ACME and use the traditional CSR procedure with your preferred certificate authority.

No Jabber Guest support with ACME

Currently Expressway does not support ACME with Jabber Guest deployments.

See *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page.

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 VCSs, you must generate a separate signing request on each peer. Those requests must then be sent to the certificate authority and the returned server certificates uploaded to each relevant peer.

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

Server Certificates and Unified Communications

VCS Control server certificate requirements

The VCS Control server certificate must include the elements listed below in its list of subject alternative names (SAN).

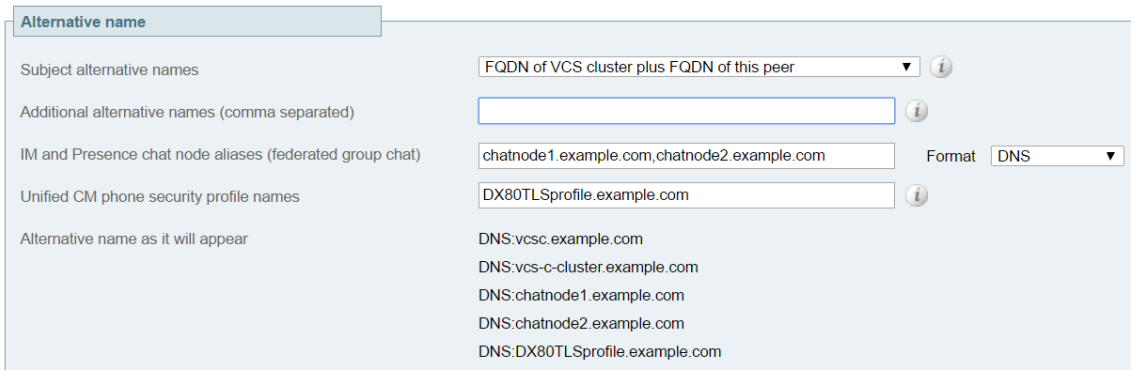
- **Unified CM phone security profile names**: the names of the **Phone Security Profiles** in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. Use the FQDN format and separate multiple entries with commas.

  Having the secure phone profiles as alternative names means that Unified CM can communicate via TLS with the VCS Control 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 VCS Control 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 VCS Expressway server certificate's alternative names.

Figure 14 Entering subject alternative names for security profiles and chat node aliases on the VCS Control's CSR generator



VCS Expressway server certificate requirements

The VCS Expressway 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 VCS Control for Unified CM registrations. Required for secure communications between endpoint devices and VCS Expressway.

  The Unified CM registration domains used in the VCS configuration and VCS Expressway 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.

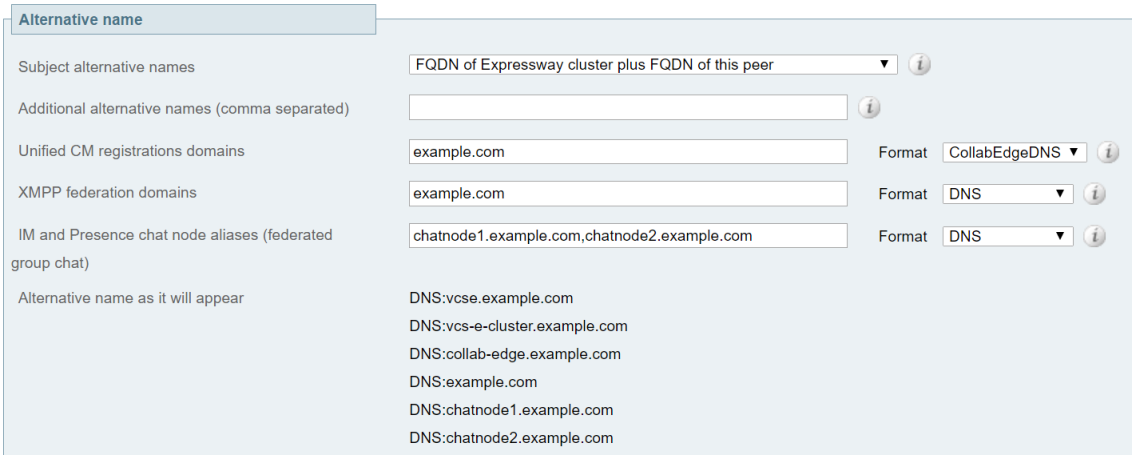
  These service discovery domains may or may not match the SIP registration domains. It depends on the deployment, and they don't have to match. One example is a deployment that uses a .local or similar private domain with Unified CM on the internal network, and public domain names for the VCS Expressway FQDN and service discovery. In this case, you need to include the public domain names in the VCS Expressway 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 VCS Control as domains for XMPP federation.

  Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. Do not use the *XMPPAddress* format as it may not be supported by your CA, and may be discontinued in future versions of the VCS software.
- **IM and Presence chat node aliases (federated group chat)**: the same set of **Chat Node Aliases** as entered on the VCS Control's certificate. They are only required for voice and presence deployments which will support group chat over TLS with federated contacts.

  Note that you can copy the list of chat node aliases from the equivalent **Generate CSR** page on the VCS Control.

Figure 15 Entering subject alternative names for Unified CM registration domains, XMPP federation domains, and chat node aliases, on the VCS Expressway's CSR generator



Managing Certificate Revocation Lists (CRLs)

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

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 VCS 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 VCS'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 VCS uses manually loaded CRLs only.
- When validating TLS connections with an LDAP server for remote login account authentication, the VCS only uses CRL data that has been embedded into the **Trusted CA certificate** (**Tools > Security > Trusted CA certificate**).

  For LDAP connections, VCS 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

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

To configure the VCS to use automatic CRL updates:

1. Go to **Maintenance > Security > CRL management**.
2. Set **Automatic CRL updates** to *Enabled*.
3. Enter the set of **HTTP(S) distribution points** from where the VCS 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 VCS will determine the underlying file type for itself; however, typical URLs could be in the format:
     - http://example.com/crl.pem
     - http://example.com/crl.der
     - http://example.com/ca.crl
     - https://example.com/allcrls.zip
     - https://example.com/allcrls.gz
4. Enter the **Daily update time** (in UTC). This is the approximate time of day when the VCS will attempt to update its CRLs from the distribution points.
5. Click **Save**.

Manual CRL Updates

You can upload CRL files manually to the VCS. Certificates presented by external policy servers can only be validated against manually loaded CRLs.

To upload a CRL file:

1. Go to **Maintenance > Security > CRL management**.
2. Click **Browse** and select the required file from your file system. It must be in PEM encoded format.
3. Click **Upload CRL file**.
   This uploads the selected file and replaces any previously uploaded CRL file.

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

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

Online Certificate Status Protocol (OCSP)

The VCS can establish a connection with an OCSP responder to query the status of a particular certificate.The VCS 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 VCS Expressway 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 VCS Expressway.

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 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 VCS, downloaded automatically from preconfigured URIs (see Managing Certificate Revocation Lists (CRLs), page 291), 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.

Configuring Certificate-Based Authentication

The **Certificate-based authentication configuration** page (**Maintenance > Security > Certificate-based authentication configuration**) is used to configure how the VCS retrieves authorization credentials (the username) from a client browser's certificate.

This configuration is required if **Client certificate-based security** (as defined on the System page) has been set to *Certificate-based authentication.* This setting means that the standard login mechanism is no longer available and that administrators (and FindMe accounts, if accessed via the VCS) can log in only if they present a valid browser certificate – typically provided via a smart card (also referred to as a Common Access Card or CAC) – and the certificate contains appropriate credentials that have a suitable authorization level.

Enabling Certificate-Based Authentication

The recommended procedure for enabling certificate-based authentication is described below:

1. Add the VCS's trusted CA and server certificate files (on the **Trusted CA certificate** and **Server certificate** pages, respectively).
2. Configure certificate revocation lists (on the **CRL management** page).
3. Use the **Client certificate testing** page to verify that the client certificate you intend to use is valid.
4. Set **Client certificate-based security** to *Certificate validation* (on the **System administration** page).
5. Restart the VCS.
6. Use the **Client certificate testing** page again to set up the required regex and format patterns to extract the username credentials from the certificate.
7. Only when you are sure that the correct username is being extracted from the certificate, set **Client certificate-based security** to *Certificate-based authentication*.

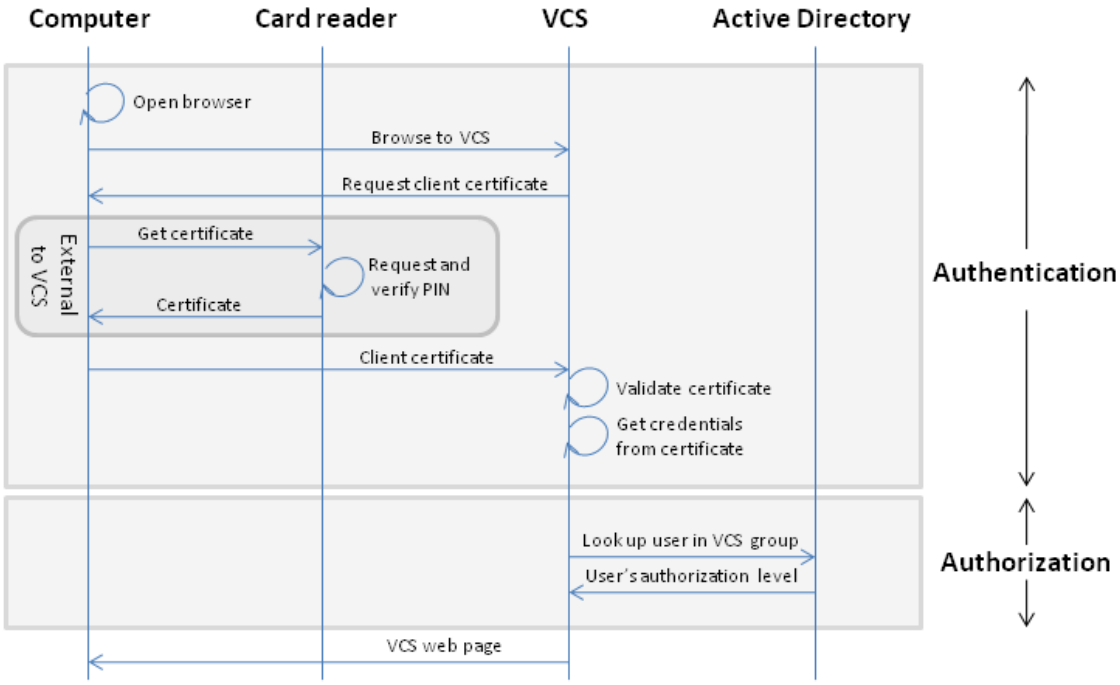
Authentication Versus Authorization

When the VCS is operating in certificate-based authentication mode, user authentication is managed by a process external to the VCS.

When a user attempts to log in to the VCS, the VCS 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 VCS 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 VCS must extract the user's authorization username from the certificate and present it to the relevant local or remote authorization mechanism.

The following diagram shows an example authorization and authentication process. It shows how a certificate is obtained from a card reader and then validated by the VCS. It then shows how the VCS obtains the user's authorization level from an Active Directory service.



Note that if the client certificate is not protected (by a PIN or some other mechanism) then unauthenticated access to the VCS may be possible. This lack of protection may also apply if the certificates are stored in the browser, although some browsers do allow you to password protect their certificate store.

Obtaining the Username from the Certificate

The username is extracted from the client browser's certificate according to the patterns defined in the **Regex** and **Username format** fields on the **Certificate-based authentication configuration** page:

- In the **Regex** field, use the `(?<name>regex)` syntax to supply names for capture groups so that matching sub-patterns can be substituted in the associated **Username format** field, for example,

  `/(Subject:.*, CN=(?<Group1>.*))/m`.

  The regex defined here must conform to *PHP regex guidelines*.
- The **Username format** field can contain a mixture of fixed text and the capture group names used in the **Regex**. Delimit each capture group name with `#`, for example, `prefix#Group1#suffix`. Each capture group name will be replaced with the text obtained from the regular expression processing.

You can use the Client certificate testing page to test the outcome of applying different **Regex** and **Username format** combinations to a certificate.

Emergency Account and Certificate-based Authentication

Advanced account security mode requires that you use only remote authentication, but also mandates that you have an emergency account in case the authentication server is unavailable. See Configuring Advanced Account Security Mode, page 305.

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 mTLS Client Certificate Verification for MRA Onboarding

Although this feature is in the Cisco Expressway Series from X12.5, **it has external software dependencies and cannot currently be used** until these dependencies are satisfied and the feature is fully implemented in the solution.

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 VCS 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 client certificate validation. You can:

- Test whether a client certificate is valid when checked against the VCS's current trusted CA list and, if loaded, the revocation list (see Managing Certificate Revocation Lists (CRLs), page 291).
- Test the outcome of applying the regex and template patterns that retrieve a certificate's authorization credentials (the username).

You can test against:

- a certificate on your local file system
- the browser's currently loaded certificate

To test if a certificate is valid:

1. Select the **Certificate source**. You can choose to:
   - upload a test file from your file system in either PEM or plain text format; if so click **Browse** to select the certificate file you want to test
   - test against the certificate currently loaded into your browser (only available if the system is already configured to use *Certificate validation* and a certificate is currently loaded)
2. Ignore the **Certificate-based authentication pattern** section – this is only relevant if you are extracting authorization credentials from the certificate.
3. Click **Check certificate**.
4. The results of the test are shown in the **Certificate test results** section.

To retrieve authorization credentials (username) from the certificate:

1. Select the **Certificate source** as described above.
2. Configure the **Regex** and **Username format** fields as required. Their purpose is to extract a username from the nominated certificate by supplying a regular expression that will look for an appropriate string pattern within the certificate. The fields default to the currently configured settings on the **Certificate-based authentication configuration** page but you can change them as required.
   - In the **Regex** field, use the `(?<name>regex)` syntax to supply names for capture groups so that matching sub-patterns can be substituted in the associated **Username format** field, for example,

     `/(Subject:.*, CN=(?<Group1>.*))/m`.

     The regex defined here must conform to *PHP regex guidelines*.
   - The **Username format** field can contain a mixture of fixed text and the capture group names used in the **Regex**. Delimit each capture group name with `#`, for example, `prefix#Group1#suffix`. Each capture group name will be replaced with the text obtained from the regular expression processing.
3. Click **Check certificate**.
   The results of the test are shown in the **Certificate test results** section. The **Resulting string** item is the username credential that would be checked against the relevant authorization mechanism to determine that user's authorization (account access) level.

4. If necessary, you can modify the **Regex** and **Username format** fields and repeat the test until the correct results are produced.
   Note that if the **Certificate source** is an uploaded PEM or plain text file, the selected file is temporarily uploaded to the VCS when the test is first performed:
   - if you want to keep testing different **Regex** and **Username format** combinations against the same file, you do not have to reselect the file for every test
   - if you change the contents of your test file on your file system, or you want to choose a different file, you must click **Browse** again and select the new or modified file to upload
5. If you have changed the **Regex** and **Username format** fields from their default values and want to use these values in the VCS'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 VCS 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 VCS Control to the VCS Expressway. A secure connection is required for a Unified Communications traversal zone, and is optional (recommended) for a normal traversal zone.

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

1. On the VCS Control, go to **Maintenance > Security > Secure traversal test**.
2. Enter the FQDN of the VCS Expressway that is paired with this VCS Control.
3. Enter the TLS verify name of this VCS Control, as it appears on the paired VCS Expressway.
   This setting is in the SIP section of the VCS Expressway's traversal zone configuration page.
4. Click **Test connection**.
   The secure traversal test utility checks whether the hosts on either side of the traversal zone recognize each other and trust each others' certificate chains.

Configuring Minimum TLS version and Cipher Suites

For improved security, TLS 1.2 or later is recommended for all encrypted sessions. If required (typically for compatibility reasons with legacy equipment), the minimum TLS versions can be configured to use versions 1.0 or 1.1.

The **Maintenance > Security > Ciphers** page allows you to configure the minimum supported TLS version for each service.

From X8.10, VCS defaults to TLS version 1.2 when establishing secure connections for the following services:

- HTTPS
- SIP
- XMPP
- UC server discovery
- Reverse proxy

On upgrade, previous behavior and defaults persist so you won't be defaulted to TLS version 1.2. However, new installations will use the new defaults. So for new installations you should check that all browsers and other equipment that must connect to VCS supports TLS version 1.2.

Cipher Suites

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

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

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

SIP Behavior – Disable ADH Recommendation

Some endpoints, for example E20, only support ADH when you connect to them, so ADH is enabled in the default cipher suites. However, if it's an inbound connection, for security reasons you should always add `!ADH` to disable it. If you remove the `ADH` from SIP then the outbound connections to some legacy endpoints will fail.

Known Issues

See the Release Notes for this release for the latest information on TLS version 1.2 support on other products.

Restarts Required

– SIP currently requires a restart after changing the cipher suite configuration. TLS protocol version continues to require a restart.

– XCP requires a restart after changing the cipher suite configuration or TLS protocol version.

SSH Configuration

The VCS pair uses SSH tunnels to securely transfer data from the VCS Expressway to the VCS Control without requiring VCS Expressway to open the connection. The VCS Control opens a TCP session with the VCS Expressway 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.

To configure the cipher and algorithms that the pair use to encrypt the tunnels:

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

Setting	Description
Ciphers	*aes256-ctr*: Advanced Encryption Standard using the CTR (counter) mode to encipher 256 bit blocks. (Default) *aes256-cbc*: Advanced Encryption Standard using the CBC (cipher-block-chaining) mode to encipher 256 bit blocks.
Public Key Algorithms	*X509v3-sign-rsa* (Default) *X509v3-ssh-rsa*
Key Exchange Algorithms	*ecdh-sha2-nistp256* *ecdh-sha2-nistp384* (Default)

3. Click **Save**.

Managing Domain Certificates and Sever Name Indication for Multitenancy

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

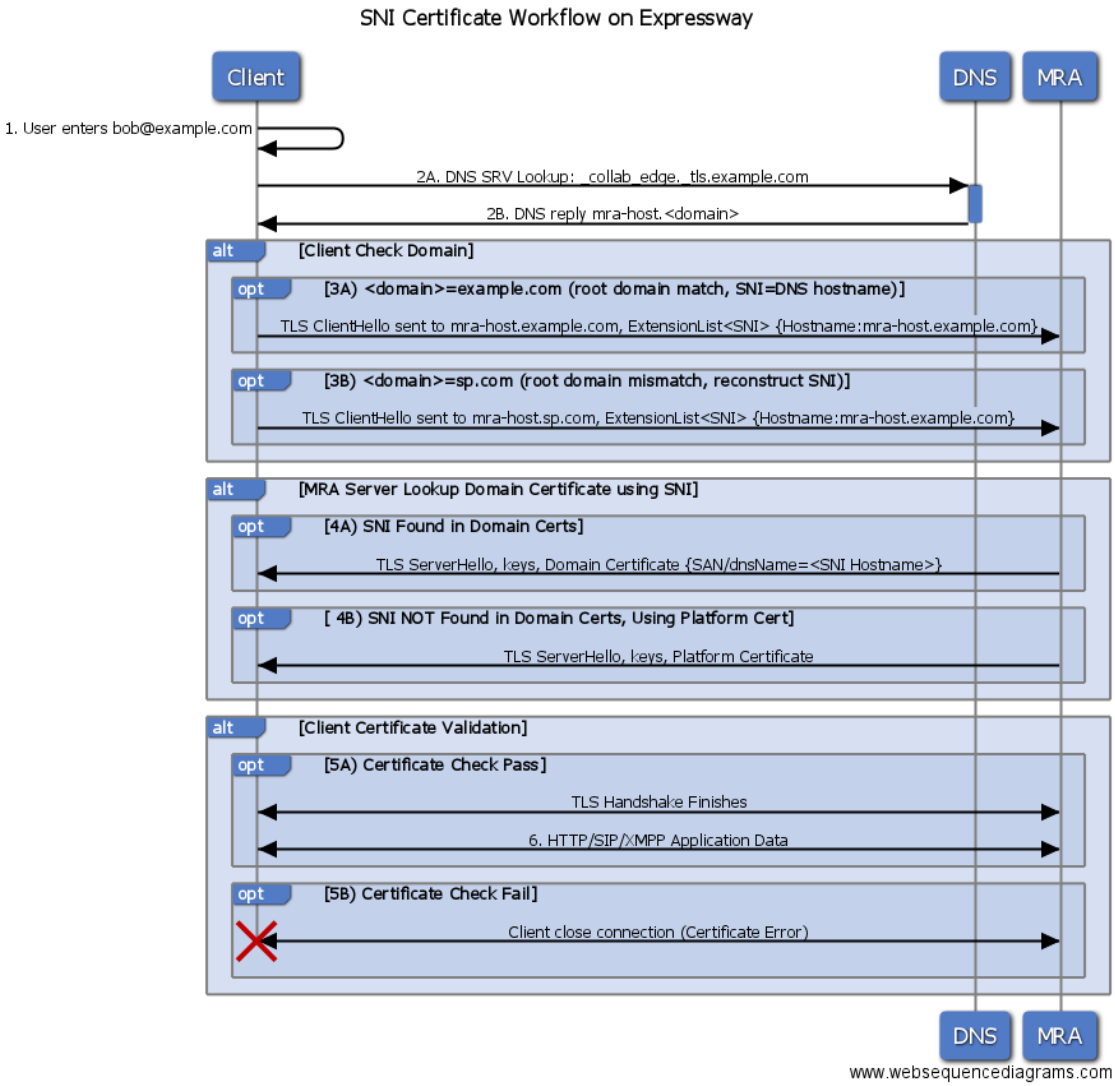
Using the Server Name Indication (SNI) protocol extension within TLS, the VCS can now store and use domain-specific certificates that can be offered to a client during the TLS handshake. This capability allows seamless integration of endpoints registering through MRA in a multitenant environment, and 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 VCS 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 VCS Expressway 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 VCS Expressway searches its certificate store to find a certificate matching the SNI hostname.
      - If a match is found, the VCS Expressway 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 VCS's Domain Certificates

You manage the VCS'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 VCS Expressway 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 VCS in all scenarios. Use the **Trusted CA certificate** page to manage the list of certificates for the Certificate Authorities (CAs) trusted by this VCS.

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 VCS.

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 VCS from being able to connect to those systems.

Adding a New Domain

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

Generating a Certificate Signing Request

The VCS can generate domain CSRs, which removes the need to use an external mechanism to generate and obtain certificate requests.

To generate a CSR:

1. Go to **Maintenance > Security > Domain certificates**.
2. Click on the domain for which you wish to generate a CSR.
3. Click **Generate CSR** to go to the **Generate CSR** page.
4. Enter the required properties for the certificate.
   - See Domain Certificates and Clustered Systems, page 304 if your VCS is part of a cluster.
5. Click **Generate CSR**. The system will produce a signing request and an associated private key. The private key is stored securely on the VCS and cannot be viewed or downloaded. **Never disclose your private key, not even to the certificate authority**.
6. You are returned to the **Domain certificate** page. From here you can:
   - Download the request to your local file system so that it can be sent to a certificate authority. You are prompted to save the file (the exact wording depends on your browser).
   - View the current request (click **Show (decoded)** to view it in a human-readable form, or click **Show (PEM file)** to view the file in its raw format).

Notes

- Only one signing request can be in progress at any one time. This is because the VCS 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. VCS supports a key length of 1024, 2048 and 4096.

Uploading a New Domain Certificate

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

To upload a domain certificate:

1. Go to **Maintenance > Security > Domain certificates**.
2. Use the **Browse** button in the **Upload new certificate** section to select and upload the domain certificate PEM file.
3. If you used an external system to generate the CSR you must also upload the server private key PEM file that was used to encrypt the domain certificate. (The private key file will have been automatically generated and stored earlier if the VCS was used to produce the CSR for this domain certificate.)
   - The server private key PEM file must not be password protected.
   - You cannot upload a server private key if a certificate signing request is in progress.
4. Click **Upload domain certificate data**.

ACME (Automated Certificate Management Environment) Service

The 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 VCSs, 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.

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.

Advanced Security

The **Advanced security** page (**Maintenance > Advanced security**) is used to configure the VCS for use in highly secure environments. You need to install the **Advanced Account Security** option key to see this page.

You can configure the system for:

- Advanced account security mode
- FIPS140-2 cryptographic mode

Configuring Advanced Account Security Mode

Enabling advanced account security limits login access to remotely authenticated users using the web interface only, and also restricts access to some system features. To indicate that the VCS 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 VCS 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 VCS web interface.
POST	Yes	Yes	Apply data to a web resource. For example, when an administrator saves changes to a setting using the VCS web interface.
OPTIONS	No	Yes	For a specified URL, returns the HTTP methods supported by the server. For example, the VCS 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 VCS 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 VCS is running in advanced account security mode, then API access is automatically disabled for all users.
- API access for individual administrators can be disabled through their user configuration options.

Prerequisites

Before you can enable advanced account security mode, the following items are required:

- The system must be configured to use remote account authentication for administrator accounts.
- The **Advanced Account Security** option key must be installed.
- You must create a local administrator account and nominate it as the emergency account, so that you can get in if remote authentication is unavailable. You cannot use a remote account for this purpose.

  Do not use the built in *admin* account.

Caution: The VCS will disallow local authentication by all accounts except the emergency account. Ensure that the remote directory service is working properly before you enable the mode.

You are also recommended to configure your system so that:

- SNMP is disabled.
- The session time out period is set to a non-zero value.
- HTTPS client certificate validation is enabled.
- User account LDAP server configuration uses TLS encryption and has certificate revocation list (CRL) checking set to *All*.
- Remote logging is disabled.
- Incident reporting is disabled.
- Any connection to an external manager uses HTTPS and has certificate checking enabled.

Alarms are raised for any non-recommended configuration settings.

Enabling Advanced Account Security

To enable advanced account security:

1. Go to **Maintenance > Advanced security**.
2. Enter a **Classification banner**.

   The text entered here is displayed on every web page.
3. Set **Advanced account security mode** to *On*.
4. Click **Save**.
5. Reboot the VCS (**Maintenance > Restart options**).

VCS Functionality: Changes and Limitations

When in secure mode, the following changes and limitations to standard VCS functionality apply:

- Access over SSH and through the serial port is disabled and cannot be turned on (the pwrec password recovery function is also unavailable).
- Access over HTTPS is enabled and cannot be turned off.
- The command line interface (CLI) and API access are unavailable.
- Administrator account authentication source is set to *Remote only* and cannot be changed.
- Local authentication is disabled. There is no access using the root account or any local administrator account except the emergency account.
- Only the emergency account may change the emergency account.
- If you are using certificate-based authentication, the emergency account must be authenticated by credentials in the client's certificate. See Emergency Account and Certificate-based Authentication, page 296
- If there are three consecutive failed attempts to log in (by the same or different users), login access to the VCS 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.
- Downgrades to version X5.0 or below are not allowed.

The Event Log, Configuration Log, Network Log, call history, search history and registration history are cleared whenever the VCS is taken out of advanced account security mode. Note that if intrusion protection is enabled, this will cause any existing blocked addresses to become unblocked.

Disabling Advanced Account Security

Note: This operation wipes all configuration. You cannot maintain any configuration or history when exiting this mode. The system returns to factory state.

1. Sign in with the emergency account.
2. Disable Advanced Account Security mode (**Maintenance > Advanced security**).
3. Sign out.
4. Connect to the console.
5. Sign in as **root** and run `factory-reset`.

   See Restoring the Default Configuration (Factory Reset), page 380 for details.

Configuring FIPS140-2 Cryptographic Mode

FIPS140 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. FIPS140-1 became a mandatory standard for the protection of sensitive data in 1994 and was superseded by FIPS140-2 in 2001.

VCS X8.1 or later implements FIPS140-2 compliant features. The scope of functionality that is FIPS140-2 compliant has increased in VCS X8.8.

When in FIPS140-2 cryptographic mode, system performance may be affected due to the increased cryptographic workload.

You can cluster VCSs that have FIPS140-2 mode enabled.

Prerequisites

Before you enable FIPS140-2 mode:

- Ensure that the system is not using NTLM protocol challenges with a direct Active Directory Service connection for device authentication; NTLM cannot be used while in FIPS140-2 mode.
- If login authentication via a remote LDAP server is configured, ensure that it uses TLS encryption if it is using SASL binding.
- The **Advanced Account Security** option key must be installed.

FIPS140-2 compliance also requires the following restrictions:

- System-wide SIP transport mode settings must be TLS: *On*, TCP: *Off* and UDP: *Off*.
- All SIP zones must use TLS.
- SNMP and NTP server connections should use strong hashing and encryption. Use these settings:

  System > SNMP > v3 Authentication > Type = *SHA*

  System > SNMP > v3 Privacy > Type = *AES*

  System > Time > NTP server *n* > Authentication= *Symmetric key*

  System > Time > NTP server *n* > Hash= *SHA-1*

If your system is running as a virtualized application and has never been through an upgrade process:

1. Ensure it has a valid release key (check this via **Maintenance > Option keys**).
2. Perform a system upgrade. You can upgrade the system to the same software release version that it is currently running.

   If you do not complete this step, the activation process described below will fail.

Enable FIPS140-2 Cryptographic Mode

Caution: The transition to FIPS140-2 cryptographic mode requires a system reset to be performed. This will remove all existing configuration data. To preserve your data you should take a backup immediately prior to performing the reset, and then restore the backup file when the reset has completed.
The reset removes all administrator account information and reinstates the default security certificates. To log in after the reset has completed you will have to first complete the Install Wizard.

To turn your system into a compliant FIPS140-2 cryptographic system:

1. Enable FIPS140-2 cryptographic mode:
   a. Go to **Maintenance > Advanced security**.
   b. Set **FIPS140-2 cryptographic mode** to *On*.
   c. Click **Save**.
2. Fix any alarms that have been raised that report non-compliant configuration.
3. Take a system backup if you want to preserve your current configuration data. Note that all backups require password protection.
4. Reset the system and complete the activation of FIPS140-2 mode:

   a. Log in to VCS as **root**.
   b. Type `fips-activate`

   The reset takes up to 30 minutes to complete.
5. Follow the prompts to complete the Install Wizard.
6. When the system has applied the configuration and restarted, log in as `admin` using the password you set.

   You may see alarms related to non-compliance with FIPS 140-2. Ignore these alarms if you intend to restore the backup taken prior to the reset. You must take action if they persist after restoring the backup.
7. Restore your previous data, if required.

   Note that while in FIPS140-2 mode, you can only restore backup files that were taken when **FIPS140-2 cryptographic mode** was set *On*. Any previous administrator account information and passwords will be restored, however the previous **root** account password will not be restored. If the data you are restoring contains untrusted security certificates, the restart that occurs as part of the restore process may take up to 6 minutes to complete.

FIPS140-2 Compliant Features

The following VCS 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)

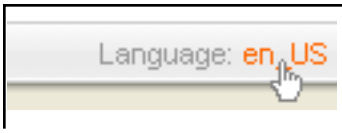
- NTP (NTP server authentication using symmetric key is restricted to SHA1)
- Device authentication against the local database
- SIP connections to/from the VCS providing they use TLS
- H.323 connections to/from the VCS
- Delegated credential checking
- SRTP media encryption
- SIP/H.323 interworking
- 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 VCS 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

Configuring Language Settings

The **Language** page (**Maintenance > Language**) controls which language is used for text displayed in the web user interface.



You can also get to the **Language** page by clicking on the **Language** link at the bottom of every page.

Changing the Language

You can configure both the default language and the language to use on an individual browser:

Field	Description	Usage tips
System default language	The default language used on the web interface.	This applies to administrator and user (FindMe) sessions. You can select from the set of installed language packs.
This browser	The language used by the current browser on the current client computer. It can be set to use either the system default language or a specific alternative language.	This setting applies to the browser currently in use on the client computer. If you access the VCS 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 VCS software files. All available languages are contained in one language pack zip file. Download the appropriate language pack version that matches your software release.

After downloading the language pack, unzip the file to extract a set of .tlp files, one per supported language.

To install a .tlp language pack file:

1. Go to **Maintenance > Language**.
2. Click **Browse** and select the **.tlp** language pack file you want to upload.
3. Click **Install**.

   The selected language pack is then verified and uploaded. This may take several seconds.
4. Repeat steps 2 and 3 for any other languages you want to install.

For the list of available languages, see the relevant release notes for your software version.

Note that:

- English (en_us) is installed by default and is always available.
- You cannot create your own language packs. Language packs can be obtained only from Cisco.
- If you upgrade to a later version of VCS software you will see a "Language pack mismatch" alarm. You may need to install a later version of the associated language pack to ensure that all text is available in the chosen language.

Removing Language Packs

To remove a language pack:

1. Go to the **Language** page (**Maintenance > Language**).
2. From the list of installed language packs, select the language packs you want to remove.
3. Click **Remove**.
4. Click **Yes** when asked to confirm their removal.

   The selected language packs are then removed. This may take several seconds.

Backing Up and Restoring VCS Data

Use the **Backup and restore** page (**Maintenance > Backup and restore**) to create backup files of VCS data, and to restore the VCS 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 VCS 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 VCS is enabled)

Note: Log files are not included in backup files.

Clustered Systems

For extra information about backing up and restoring peers in a cluster, see Cluster Upgrades, Backup and Restore, page 165

Creating a System Backup

Before You Begin

- From X8.11, backup files are always encrypted. 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 VCS and restore it to a different VCS. 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 VCS, 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 VCSs. 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

- From X8.11, 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 VCS system data:

1. Go to **Maintenance > Backup and restore**.
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.
3. Click **Create system backup file**.

4. Wait for the backup file to be created. This may take several minutes. Do not navigate away from this page while the file is being prepared.
5. When the backup 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.)
6. Save the backup file to a secure location.

Restoring a Previous Backup

Before You Begin

- You need the password for the backup file from which you intend to restore.
- We recommend that you take the VCS 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:
  a. Upgrade the software version to the required later version.
  b. Manually redo any configuration changes made since the backup was taken.
- (If you use FIPS140-2 cryptographic mode) You can't restore a backup made on a non-FIPS system, onto a system that's running in FIPS mode. You can restore a backup from a FIPS-enabled system onto a non-FIPS system.
- You can't restore data to a VCS while it's part of a cluster. You must first remove it from the cluster. For details, see Cluster Upgrades, Backup and Restore, page 165.

Passwords

- From X8.11, 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 restore the VCS to a previous configuration of system data:

1. First do a factory reset, as described in Restoring the Default Configuration (Factory Reset), page 380. This removes your configuration data, and reverts the system back to its original state. The reset maintains your current software version if you've upgraded since the system was first set up.
2. Upgrade the system to the software version that was running when you made the backup.
   - For standalone systems, see Upgrade Instructions, page 1.
   - For clustered systems, see the *VCS Cluster Creation and Maintenance Deployment Guide*.

3. Now you can restore the system from the backup, as follows:
   a. Go to **Maintenance > Backup and restore**.
   b. In the **Restore** section, click **Browse** and navigate to the backup file that you want to restore.
   c. In the **Decryption password** field, enter the password used to create the backup file.
   d. Click **Upload system backup file**.
   e. The VCS 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.
4. This step only applies if the backup file is out of date. That is, the software version was upgraded, or system configuration changes were made after the backup was done. In this case:
   a. Upgrade the system again, this time to the required software version for the system.
   b. Redo any configuration changes made after the backup (assuming you still need them on the restored system).

Diagnostics Tools

This section provides information about how to use the diagnostics tools:

- Diagnostic logging
- System snapshot
- Network Log and Support Log advanced logging configuration tools
- Incident reporting

From X8.10 the VCS can support SIP "session identifiers". Assuming all devices in the call use session identifiers, the mechanism uses the *Session-ID* field in SIP headers to maintain a unique code through the entire transit of a call. Session identifiers are useful for investigating issues with calls that involve multiple components, as they can be used to find and track a specific call on the VCS server. Support for session identifiers includes the SIP side of interworked SIP/H.323 calls, and calls to and from Microsoft systems. Session identifiers are defined in RFC 7989.

Configuring Diagnostic Logging

The **Diagnostic logging** tool (**Maintenance > Diagnostics > Diagnostic logging**) can be used to assist in troubleshooting system issues.

It allows you to generate a diagnostic log of system activity over a period of time, and then to download the log so that it can be sent to your Cisco customer support representative. You can also take and subsequently download a tcpdump while logging is in progress.

To use this tool:

1. Go to **Maintenance > Diagnostics > Diagnostic logging**.
2. Optionally, select **Take tcpdump while logging**.
3. Click **Start new log**.

4. (Optional) Enter some **Marker** text and click **Add marker**.
   - The marker facility can be used to add comment text to the log file before certain activities are performed. This helps to subsequently identify the relevant sections in the downloaded diagnostic log file.
   - You can add as many markers as required, at any time while the diagnostic logging is in progress.
   - Marker text is added to the log with a "DEBUG_MARKER" tag.
5. Reproduce the system issue you want to trace in the diagnostic log.
6. Click **Stop logging**.
7. Click **Collect log**.
8. 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).

To download logs again

If you want to download the logs again, you can re-collect them by using the **Collect log** button. If the button is grayed out, first refresh the page in your browser.

The downloaded diagnostic log archive contains the following files:

- loggingsnapshot_*<system host name>*_*<timestamp>*.txt – containing log messages in response to the activities performed during the logging period
- xconf_dump_*<system host name>*_*<timestamp>*.txt – containing information about the configuration of the system at the time the logging was started
- xconf_dump_*<system host name>*_*<timestamp>*.xml – more complete version of xconfig, in XML format
- xstat_dump_*<system host name>*_*<timestamp>*.txt – containing information about the status of the system at the time the logging was started
- xstat_dump_*<system host name>*_*<timestamp>*.xml – more complete version of xstatus, in XML format
- (if relevant) eth*n*_diagnostic_logging_tcpdump*x*_*<system host name>*_*<timestamp>*.pcap – containing the packets captured during the logging period

These files can be sent to your Cisco support representative, if you have been requested to do so.

Caution: tcpdump files may contain sensitive information. Only send tcpdump files to trusted recipients. Consider encrypting the file before sending it, and also send the decrypt password out-of-band.

Note that:

- Only one diagnostic log can be produced at a time; creating a new diagnostic log will replace any previously produced log.
- The VCS continually logs all system activity to a unified log file. The diagnostic logging facility works by extracting a portion of this unified log. On busy systems the unified log file may become full over time and will discard historic log data so that it can continue logging current activity. This means that all or part of your diagnostic log could be overwritten. The system will warn you if you attempt to download a partial diagnostic log file.
- The diagnostic log will continue logging all system activity until it is stopped, including over multiple login sessions and system restarts.
- When starting a diagnostic log, the relevant system modules have their log levels automatically set to "debug". You can ignore any "Verbose log levels configured" alarms; the log levels are reset to their original values when you stop logging.
- Diagnostic logging can only be controlled through the web interface; there is no CLI option.
- The tcpdump has a maximum file size limit of 50 MB.

Clustered Systems

Diagnostic logging can also be used if your VCS is a part of a cluster, however some activities only apply to the "current" peer (the peer to which you are currently logged in to as an administrator):

- The start and stop logging operations are applied to every peer in the cluster, regardless of the current peer.
- The taking a tcpdump operation is applied to every peer in the cluster, regardless of the current peer.
- Each cluster peer maintains its own unified log, and logs activity that occurs only on that peer.
- Marker text is only applied to log of the current peer.
- You can only download the diagnostic log from the current peer.
- To add markers to other peers' logs, or to download diagnostic logs from other peers, you must log in as an administrator to that other peer.

To collect comprehensive information for debugging purposes, we recommend that you extract the diagnostic log for each peer in a cluster.

Creating a System Snapshot

The **System snapshot** page (**Maintenance > Diagnostics > System snapshot**) lets you create files that can be used for diagnostic purposes. The files should be sent to your support representative at their request to assist them in troubleshooting issues you may be experiencing.

You can create several types of snapshot file:

- **Status snapshot**: contains the system's current configuration and status settings.
- **Logs snapshot**: contains log file information (including the Event Log, Configuration Log and Network Log).
- **Full snapshot**: contains a complete download of all system information. The preparation of this snapshot file may take several minutes to complete and may lead to a drop in system performance while the snapshot is in progress.

To create a system snapshot file:

1. Click one of the snapshot buttons to start the download of the snapshot file. Typically your support representative will tell you which type of snapshot file is required.
   - The snapshot creation process will start. This process runs in the background. If required, you can navigate away from the snapshot page and return to it later to download the generated snapshot file.
   - When the snapshot file has been created, a **Download snapshot** button will appear.
2. Click **Download snapshot**. A pop-up window appears and prompts you to save the file (the exact wording depends on your browser). Select a location from where you can easily send the file to your support representative.

Configuring Network Log Levels

The **Network Log configuration** page (**Maintenance > Diagnostics > Advanced > Network Log configuration**) is used to configure the log levels for the range of Network Log message modules.

Caution: changing the logging levels can affect the performance of your system. You should only change a log level on the advice of Cisco customer support.

To change a logging level:

1. Click on the **Name** of the module whose log level you want to modify.
2. Choose the required **Level** from the drop-down list.
   - A log level of *Fatal* is the least verbose; *Trace* is the most verbose.
   - Each message category has a log level of *Info* by default.

3. Click **Save**.

Configuring Support Log Levels

The **Support Log configuration** page (**Maintenance > Diagnostics > Advanced > Support Log configuration**) is used to configure the log levels for the range of Support Log message modules.

Caution: changing the logging levels can affect the performance of your system. You should only change a log level on the advice of Cisco customer support.

To change a logging level:

1. Click on the **Name** of the module whose log level you want to modify.
2. Choose the required **Level** from the drop-down list.
   - A log level of *Fatal* is the least verbose; *Trace* is the most verbose.
   - Each message category has a log level of *Info* by default.
3. Click **Save**.

Incident Reporting

The incident reporting feature of the VCS automatically saves information about critical system issues such as application failures. You can:

- Configure the VCS to send the reports automatically to Cisco customer support
- View the reports from the VCS web interface
- Download and send the reports manually to Cisco (usually at the request of Cisco customer support)

The information contained in these reports can then be used by Cisco customer support to diagnose the cause of the failures. All information gathered during this process will be held in confidence and used by Cisco personnel for the sole purpose of issue diagnosis and problem resolution.

Incident Reporting Caution: Privacy-Protected Personal Data

IN NO EVENT SHOULD PRIVACY-PROTECTED PERSONAL DATA BE INCLUDED IN ANY REPORTS TO CISCO.

Privacy-Protected Personal Data means any information about persons or entities that the Customer receives or derives in any manner from any source that contains any personal information about prospective, former, and existing customers, employees or any other person or entity. Privacy-Protected Personal Data includes, without limitation, names, addresses, telephone numbers, electronic addresses, social security numbers, credit card numbers, customer proprietary network information (as defined under 47 U.S.C. § 222 and its implementing regulations), IP addresses or other handset identifiers, account information, credit information, demographic information, and any other information that, either alone or in combination with other data, could provide information specific to a particular person.

PLEASE BE SURE THAT PRIVACY-PROTECTED PERSONAL DATA IS NOT SENT TO CISCO WHEN THE VCS IS CONFIGURED TO AUTOMATICALLY SEND REPORTS.

IF DISCLOSURE OF SUCH INFORMATION CANNOT BE PREVENTED, PLEASE DO NOT USE THE AUTOMATIC CONFIGURATION FEATURE. Instead, copy the data from the Incident detail page and paste it into a text file. You can then edit out any sensitive information before forwarding the file on to Cisco customer support.

Incident reports are always saved locally, and can be viewed via the Incident view page.

Enabling Automatic Incident Reporting

Read the privacy-protected personal data caution before you decide whether to enable automatic incident reporting.

To configure the VCS to send incident reports automatically to Cisco customer support:

1. Go to **Maintenance > Diagnostics > Incident reporting > Configuration**.
2. Set the **Incident reports sending mode** to *On*.
3. Specify the **Incident reports URL** of the web service to which any error reports are to be sent.
   The default is `https://cc-reports.cisco.com/submitapplicationerror/`.
4. Optional. Specify a **Contact email address** that can be used by Cisco customer support to follow up any error reports.
5. Optional. Specify a **Proxy server** to use for the connection to the incident reporting server.
   Use the format (http|https)://address:port/ such as `http://www.example.com:3128/`
6. Ensure that **Create core dumps** is *On*; this is the recommended setting as it provides useful diagnostic information.

Note: If the **Incident reports sending mode** is *Off*, incidents will not be sent to any URL but they will still be saved locally and can be viewed and downloaded from the **Incident detail** page.

Sending Incident Reports Manually

Read the privacy-protected personal data caution before you decide whether to send an incident report manually to Cisco.

To send an incident report manually to Cisco customer support:

1. Go to **Maintenance > Diagnostics > Incident reporting > View**.
2. Click on the incident you want to send. You will be taken to the **Incident detail** page.
3. Scroll down to the bottom of the page and click **Download incident report**. You will be given the option to save the file.
4. Save the file in a location from where it can be forwarded to Cisco customer support.

Removing Sensitive Information from a Report

The details in the downloaded incident report are Base64-encoded, so you will not be able to meaningfully view or edit the information within the file.

If you need to edit the report before sending it to Cisco (for example, if you need to remove any potentially sensitive information) you must copy and paste the information from the **Incident detail** page into a text file, and edit the information in that file before sending it to Cisco.

Viewing Incident Reports

The **Incident view** page (**Maintenance > Diagnostics > Incident reporting > View**) shows a list of all incident reports that have occurred since the VCS 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 VCS software version running when the incident occurred.
Build	The internal build number of the VCS software version running when the incident occurred.

Field	Description
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 configuration page.

To view the information contained in a particular incident report, click on the report's **Time**. You will be taken to the Incident detail page, from where you can view the report on screen, or download it as an XML file for forwarding manually to Cisco customer support.

Incident Report Details

The **Incident detail** page (**Maintenance > Diagnostics > Incident reporting > View**, then click on a report's **Time**) shows the information contained in a particular incident report.

This is the information that is sent to the external web service if you have enabled **Incident reports sending mode** (via **Maintenance > Diagnostics > Incident reporting > Configuration**). It is also the same information that is downloaded as a Base64-encoded XML file if you click **Download incident report**.

The information contained in the report is:

Field	Description
Time	The date and time when the incident occurred.
Version	The VCS software version running when the incident occurred.
Build	The internal build number of the VCS 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 VCS application had when the incident occurred.
Release	A true/false flag indicating if this is a release build (rather than a development build).
User name	The name of the person that built this software. This is blank for release builds.
Stack	The trace of the thread of execution that caused the incident.
Debug information	A full trace of the application call stack for all threads and the values of the registers.

Caution: for each call stack, the Debug information includes the contents of variables which may contain some sensitive information, for example alias values and IP addresses. If your deployment is such that this information could contain information specific to a particular person, read the caution regarding privacy-protected personal data before you decide whether to enable automatic incident reporting.

Checking the Effect of a Pattern

The **Check pattern** tool (**Maintenance > Tools > Check pattern**) lets you test whether a pattern or transform you intend to configure on the VCS will have the expected result.

Patterns can be used when configuring:

- Allow lists and Deny lists to specify aliases to be included in the lists
- Transforms to specify aliases to be transformed before any searches take place

- Search rules to filter searches based on the alias being searched for, and to transform an alias before the search is sent to a zone
- Subzone membership rules to determine, based on the address of the device, to which subzone an endpoint is assigned when it registers with the VCS

To use this tool:

1. Enter an **Alias** against which you want to test the transform.
2. In the **Pattern** section, enter the combination of **Pattern type** and **Pattern behavior** for the **Pattern string** being tested.
   - If you select a **Pattern behavior** of *Replace*, you also need to enter a **Replace string**.
   - If you select a **Pattern behavior** of *Add prefix* or *Add suffix*, you also need to enter an **Additional text** string to append/prepend to the **Pattern string**.
   - The VCS has a set of predefined pattern matching variables that can be used to match against certain configuration elements.
3. Click **Check pattern** to test whether the alias matches the pattern.
   The **Result** section shows whether the alias matched the pattern, and displays the resulting alias (including the effect of any transform if appropriate).

Locating an Alias

The **Locate** tool (**Maintenance > Tools > Locate**) lets you test whether the VCS can find an endpoint identified by the given alias, within the specified number of "hops", without actually placing a call to that endpoint.

This tool is useful when diagnosing dial plan and network deployment issues.

To use this tool:

1. Enter the **Alias** you want to locate.
2. Enter the **Hop count** for the search.
3. Select the **Protocol** used to initiate the search, either *H.323* or *SIP*. The search may be interworked during the search process, but the VCS always uses the native protocol first to search those target zones and policy services associated with search rules at the same priority, before searching those zones again using the alternative protocol.
4. Select the **Source** from which to simulate the search request. Choose from the *Default Zone* (an unknown remote system), the *Default Subzone* (a locally registered endpoint) or any other configured zone or subzone.
5. Select whether the request should be treated as **Authenticated** or not (search rules can be restricted so that they only apply to authenticated messages).
6. Optionally, you can enter a **Source alias**. Typically, this is only relevant if the routing process uses CPL that has rules dependent on the source alias. (If no value is specified a default alias of `xcom-locate` is used.)
7. Click **Locate** to start the search.

   The status bar shows **Searching...** followed by **Search completed**. The results include the list of zones that were searched, any transforms and Call Policy that were applied, and if found, the zone in which the alias was located.

The locate process performs the search as though the VCS received a call request from the selected **Source zone**. For more information, see the Call Routing Process, page 169 section.

Serviceability

The **Serviceability** page (**Maintenance > Serviceability**) is used to configure Smart Call Home on the VCS.

About Smart Call Home

This feature is deprecated from VCS X12.5, and **support will be withdrawn in a subsequent release**.

Smart Call Home is an embedded support capability for VCS. It offers proactive diagnostics and real-time alerts, enabling higher network availability and increased operational efficiency. Smart Call Home notifies users of Schedule- and Event-based notifications.

- Schedule-based notifications: inventory, telemetry and configuration messages used to generate a Device Report and improve hardware and software quality by identifying failure trends. You can find these notifications posted on the first day of every month.
- Event-based notifications: ad hoc events already supported by VCS such as alarms and ACRs. You will find these notifications posted to the Smart Call Home server as and when they occur.

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 VCS.

The information shown on these pages is specific to that particular VCS and varies depending on the VCS'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 VCS. 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 VCS configuration.

The port information is split into the following pages:

- Local Inbound Ports, page 320
- Local Outbound Ports, page 321
- Remote Listening Ports, page 321

On VCS Expressway 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 VCS that are used to receive inbound communications from other systems.

For each port listed on this page, if there is a firewall between the VCS and the source of the inbound communications, your firewall must allow:

- inbound traffic to the IP port on the VCS from the source of the inbound communications, and
- return traffic from that same VCS IP port back out to the source of the inbound communication.

Note: this firewall configuration is particularly important if this VCS 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 VCS that are used to send outbound communications to other systems.

For each port listed on this page, if there is a firewall between the VCS and the destination of the outbound communications, your firewall must allow:

- outbound traffic out from the IP port on the VCS to the destination of the outbound communications, and
- return traffic from that destination back to the same VCS IP port.

Note: this firewall configuration is particularly important if this VCS 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 VCS communicates.

Your firewall must be configured to allow traffic originating from the local VCS 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 VCS will be sending media and signaling, but the ports on which these devices receive traffic from the VCS 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 VCS 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.

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 VCS 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 VCS to a particular destination host system.
- Tracepath: allows you to discover the path taken by a network packet sent from the VCS 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 test: 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 VCS 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 VCS 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 VCS 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 VCS. *** indicates that the node did not respond to the request.

The route taken between the VCS 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 VCS 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 VCS and a particular host may vary for each tracepath request.

DNS Lookup

The **DNS lookup** tool (**Maintenance > Tools > Network utilities > DNS lookup**) can be used to assist in troubleshooting system issues.

It allows you to query DNS for a supplied hostname and display the results of the query if the lookup was successful.

To use this tool:

1. In the **Host** field, enter either:
   - the name of the host you want to query, or
   - an IPv4 or IPv6 address if you want to perform a reverse DNS lookup
2. In the **Query type** field, select the type of record you want to search for:

   (for reverse lookups the **Query type** is ignored – the search automatically looks for PTR records)

Option	Searches for...
All	any type of record
A (IPv4 address)	a record that maps the hostname to the host's IPv4 address
AAAA (IPv6 address)	a record that maps the hostname to the host's IPv6 address
SRV (services)	SRV records (which includes those specific to H.323, SIP, Unified Communications and TURN services, see below)
NAPTR (Name authority pointer)	a record that rewrites a domain name (into a URI or other domain name for example)

3. By default the system will submit the query to all of the system's default DNS servers (**System > DNS**). To query specific servers only, set **Check against the following DNS servers** to *Custom* and then select the DNS servers you want to use.
4. Click **Lookup**.

A separate DNS query is performed for each selected **Query type**. The domain that is included within the query sent to DNS depends upon whether the supplied **Host** is fully qualified or not (a fully qualified host name contains at least one "dot"):

- If the supplied **Host** is fully qualified:
  - DNS is queried first for **Host**
  - If the lookup for **Host** fails, then an additional query for **Host.<system_domain>** is performed (where **<system_domain>** is the **Domain name** as configured on the **DNS** page)
- If the supplied **Host** is not fully qualified:
  - DNS is queried first for **Host.<system_domain>**
  - If the lookup for **Host.<system_domain>** fails, then an additional query for **Host** is performed

For SRV record type lookups, multiple DNS queries are performed. An SRV query is made for each of the following _ service._protocol combinations:

- _h323ls._udp.<domain>
- _h323rs._udp.<domain>
- _h323cs._tcp.<domain>
- _sips._tcp.<domain>
- _sip._tcp.<domain>
- _sip._udp.<domain>
- _collab-edge._tls
- _cisco-uds._tcp
- _turn._udp.<domain>
- _turn._tcp.<domain>

In each case, as for all other query types, either one or two queries may be performed for a <domain> of either **Host** and/or **Host.<system_domain>**.

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 VCS.
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 VCS.
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 VCS 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 VCS cannot process the UDP response. This is not usually a problem, because the VCS 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 VCS 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 VCS 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 VCS can connect to particular services on a given domain. You can use this tool to proactively test your connectivity while configuring VCS-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 VCS 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 VCS only attempts a TLS connection after the TCP succeeds.

The VCS 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 VCS 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 18 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 19 Connectivity Test Results - TCP Connections

Result field	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.

Table 19 Connectivity Test Results – TCP Connections (continued)

Result field	Description
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 20 Connectivity Test Results – TLS Connections

Result field	Description
Stage	The stage of the test. For each host, returns one to three tests for the queried service on TLS protocol. The test is performed using each TLS version that is supported by the Expressway, in the following order, and stops when a successful connection is made: ▪ 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 VCS 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.

Restarting, Rebooting and Shutting Down

The **Restart options** page (**Maintenance > Restart options**) allows you to restart, reboot or shut down the VCS without having physical access to the hardware.

Caution: do not restart, reboot or shut down the VCS 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 VCS 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 VCS 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 VCS 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.

After the system has been shut down, the only way it can be restarted (unless it is a virtual appliance) is by pressing the soft power button on the unit itself. You must therefore have physical access to the unit if you want to restart it after it has been shut down.

Effect on active calls and registrations

Any of these restart options will cause all active calls and registrations to be terminated. (If the VCS is part of a cluster, only those calls for which the VCS is taking the signaling will be terminated.)

For this reason, the **System status** section displays the number of current calls and registrations, 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 and registrations.

If **Mobile and remote access** is enabled, the number of currently provisioned sessions is displayed (VCS Control only).

Restarting, rebooting or shutting down using the web interface

To restart the VCS using the web interface:

1. Go to **Maintenance > Restart options**.
2. Check the number of calls and registrations 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 VCS will be unsuccessful.

Developer Resources

The VCS includes some features that are intended for the use of Cisco support and development teams only. Do not access these pages unless it is under the advice and supervision of your Cisco support representative.

Caution: **incorrect usage of the features on these pages could cause the system operation to become unstable, cause performance problems and cause persistent corruption of system configuration.**

These features are:

- Debugging and System Administration Tools, page 328
- Experimental Menu, page 328

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 VCS 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 VCS 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://<VCS host name or IP address>/setaccess`.
   The **Set access** page appears.
2. In the **Access password** field, enter `qwertsys`.
3. Click **Enable access**.

A new top-level **Experimental** menu will appear to the right of the existing menu items.

Overview and Status Information

You can view information about the current status, registrations, current calls and call history, and configuration of the VCS by using the **Status** menu options.

Status Overview 329
System Information 330
Ethernet Status 331
IP Status 332
Resource Usage 332
Registration Status 333
Call Status 334
B2BUA Calls 336
Search History 337
Search Details 337
Local Zone Status 338
Zone Status 338
Bandwidth 339
Policy Server Status and Resiliency 340
TURN Relay Usage 340
Unified Communications Status 341
Presence 342
Microsoft interoperability 343
TMS Provisioning Extension Service Status 344
Starter Pack Provisioning Server Status 347
Managing Alarms 348
Logs 349
Hardware Status 352

Status Overview

The **Overview** page (**Status > Overview**) provides an overview of the current status of the VCS (or VCS cluster, if applicable). This page is displayed by default after logging in to the VCS as an administrator.

The following information is displayed:

Field	Description
System information: many of the items in this section are configurable. Click on an item name to go to its configuration page.	
System name	Name assigned to the VCS.
Up time	Time elapsed since the system last restarted.
Software version	Software version currently installed on the VCS.
IPv4 address	VCS's IPv4 addresses.
IPv6 address	VCS's IPv6 addresses.
Options	Maximum limits for calls and registrations, and availability of additional VCS features like TURN Relays, FindMe™, Device Provisioning and Advanced Networking, are controlled by option keys.

Resource usage

This section provides statistics about current and cumulative license usage for calls and registrations.

It shows current and peak (highest concurrent) usage broken down by:

- Unified CM remote session calls (if Unified Communications **Mobile and remote access** is enabled)
- Traversal calls
- Non-traversal calls
- SIP traversal audio-only calls

It also displays resource and license usage information:

- Monitored resource usage, expressed as a percentage of the system capacity.
- Current and peak license usage, expressed as a percentage of the available licenses for each license type. **For Expressway:** 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. **For VCS:** Each traversal call license allows either 1 video call or 2 audio-only SIP calls. Hence, a 100 traversal call 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 standard video call license (traversal or non-traversal as appropriate).

You can view details of current calls or registrations by clicking on the relevant item in the section.

All statistics are based on data since the system was last restarted. The information on this page refreshes automatically every 5 seconds.

Total usage statistics are also shown (unless Unified Communications **Mobile and remote access** is enabled, in which case this data is shown on the **Resource usage** page only).

Clustered VCS systems

If the VCS is part of a cluster, then details for each peer are shown as well as totals for the entire cluster.

See About Clusters, page 157 for more information.

System Information

The **System information** page (**Status > System > Information**) provides details of the software, hardware, and time settings of the VCS.

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 VCS.
Product	This identifies the VCS.
Software version	The version of software that is currently installed on the VCS.
Software build	The build number of this software version.
Software release date	The date on which this version of the software was released.
Software name	The internal reference number for this software release.
Software options	The maximum number of calls, and the availability of additional VCS features such as FindMe™, Device Provisioning and Advanced Networking, are controlled through the use of option keys. This section shows all the optional features currently installed on the VCS.
Hardware version	The version number of the hardware on which the VCS software is installed.
Serial number	The serial number of the hardware or virtual machine on which the VCS 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 amount of time that has elapsed since the system last restarted.
System time (UTC)	The time as determined by the NTP server. If no NTP server is configured, this shows *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 VCS'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.
FindMe sessions	The number of current active FindMe sessions. Click on the link to see the list of active sessions.

Ethernet Status

The **Ethernet** page (**Status > System > Ethernet**) shows the MAC address and Ethernet speed of the VCS.

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 VCS's Ethernet device for that LAN port.
Speed	The speed of the connection between the LAN port on the VCS and the Ethernet switch.

The Ethernet speed can be configured via the Ethernet page.

IP Status

The **IP status** page (**Status > System > IP**) shows the current IP settings of the VCS.

The following information is displayed:

Field	Description
IP section:	
Protocol	Indicates the IP protocol supported by the VCS: ▪ *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 VCS acts as an IPv4 to IPv6 gateway. It communicates with other systems via either protocol.
IPv4 gateway	The IPv4 gateway used by VCS.
IPv6 gateway	The IPv6 gateway used by VCS.
Advanced Networking	Indicates whether the second LAN port has been enabled. This is done by installing the **Advanced Networking** option key.
LAN 1	Shows the IPv4 address and subnet mask, and IPv6 address of the LAN 1 port.
LAN 2	If the **Advanced Networking** option key has been installed, this shows the IPv4 address and subnet mask, and IPv6 address of the LAN 2 port.
DNS section:	
Server 1..5 address	The IP addresses of each of the DNS servers that are queried when resolving domain names. Up to 5 DNS servers may be configured.
Domain	Specifies the name to be appended to the host name before a query to the DNS server is executed.

The IP settings can be configured via the IP page.

Resource Usage

The **Resource usage** page (**Status > System > Resource usage**) provides statistics about the current and cumulative license usage for calls and registrations.

It shows current and peak (highest concurrent) usage broken down by:

- Unified CM remote session calls (if Unified Communications **Mobile and remote access** is enabled)
- Traversal calls
- Non-traversal calls
- SIP traversal audio-only calls

It also displays resource and license usage information:

- Monitored resource usage, expressed as a percentage of the system capacity.
- Current and peak license usage, expressed as a percentage of the available licenses for each license type. **For Expressway:** 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.**For VCS:** Each traversal call license allows either 1 video call or 2 audio-only SIP calls. Hence, a 100 traversal call 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 standard video call license (traversal or non-traversal as appropriate).

You can view details of current calls or registrations by clicking on the relevant item in the section.

All statistics are based on data since the system was last restarted. The information on this page refreshes automatically every 5 seconds.

Clustered VCS systems

If the VCS is part of a cluster, details for each peer are shown as well as totals for the entire cluster. See About Clusters, page 157 for more information.

Registration Status

Registration status information can be displayed for both current and historic registrations. If the VCS 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 VCS, and allows you to remove a device's registration. If the VCS is part of a cluster, all registrations across the cluster are shown. Note that an H.323 device can register with more than one alias; in such cases this page will show only one alias and (when present) one E.164 number for that device. Note also that a single device can support both the SIP and H.323 protocols; in such a case the SIP registration and the H.323 registration will appear as separate entries on this page.
- 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 VCS. Note that a single H.323 device can register with more than one alias, and each will appear as a separate entry on this page.
- The **Registration history** page (**Status > Registrations > History**) lists all the registrations that are no longer current. It contains all historical registrations since the VCS was last restarted.

The following information is displayed:

Field	Description
Name	For H.323 devices, this is one of its aliases. If the device has registered with more than one alias, this will be (in order of preference) its H.323 ID, URI or email address. For MCUs and Gateways this will be its alias or, if it has not registered an alias, one of its prefixes. For SIP devices, this is its SIP AOR.
Number	For H.323 devices that have registered one or more E.164 numbers, the first will be shown here. 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 H.323 alias, E.164 number, prefix or SIP AOR registered by a device. (Registration by alias view only.)

Field	Description
Type	Indicates the nature of the registration. This will most commonly be Endpoint, MCU, Gateway, or SIP UA. The registration by alias view shows whether the alias is an H.323 ID, E.164 number, prefix or SIP AOR.
Protocol	Indicates whether the registration is for a SIP or H.323 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 H.323 devices this is its RAS address, and for SIP UAs it is the Contact address presented in the REGISTER request.
End time	The date and time at which the registration was terminated. (Registration history view only.)
Duration	The length of time that the registration was in place. (Registration history view only.)
Reason	The reason why the registration was terminated. (Registration history view only.)
Peer	Identifies the cluster peer to which the device is registered.
Actions	Click **View** to go to the **Registration details** page to see further detailed information about the registration.

Registration details

The information shown on the **Registration details** page depends on the device's protocol, and whether the registration is still current. For example, SIP registrations include the AOR, contact and, if applicable, public GRUU details. H.323 registration details include all of the registered aliases. It also provides related tasks that let you **View active calls involving this registration** and **View previous calls involving this registration**; these options take you to the **Calls by registration** page, showing the relevant current or historic call status information filtered for that particular registration.

Unregistering and blocking devices

The registration status pages provide options to manually unregister and block devices.

- Click **Unregister** to unregister the device. Note that the device may automatically re-register after a period of time, depending on its configuration. To prevent this, you must also use a registration restriction policy such as an Allow List or Deny List.
- Click **Unregister and block** to unregister the device and add the alias to the Deny List page, thus preventing the device from automatically re-registering. (This option is only available if the **Restriction policy** is set to *Deny List*.)

Note that if your VCS is part of a cluster you have to be logged into the peer to which the device is registered to be able to unregister it.

Call Status

Call status information can be displayed for both current and completed calls:

- **Current calls**: the **Call status** page (**Status > Calls > Calls**) lists all the calls currently taking place to or from devices registered with the VCS, or that are passing through the VCS.
- **Completed calls**: the **Call history** page (**Status > Calls > History**) lists all the calls that are no longer active. The list is limited to the most recent 500 calls, and only includes calls that have taken place since the VCS 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 VCS 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 VCS and User Policy is enabled, the caller's FindMe ID may be displayed instead.)
Destination	The alias dialed from the device. This may be different from the alias to which the call was placed, which may have been transformed (due to pre-search transforms, zone transforms or User Policy).
Type	Indicates either a traversal or non-traversal 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 VCS. 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:

- *VCS*: a standard VCS call
- *B2BUA*: a call component that is routed through the B2BUA to apply a media encryption policy or ICE messaging support
- *Microsoft Lync B2BUA*: a call component that is routed through the Microsoft Lync B2BUA

You can view full details of each call component by clicking on the **Local call serial number** associated with each component. This will open the **Call details** page which lists full information about that component, including all call legs and sessions. It also provides further links to the **Call media** page which lists the individual media channels (audio, video, data and so on) for the most relevant session for a traversal call.

If the VCS 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.

Identifying Mobile and Remote Access calls

The call status and call history pages show all call types. Unified CM remote sessions (if Mobile and Remote Access is enabled) as well as VCS traversal and non-traversal calls, or Expressway RMS sessions.

To distinguish between the call types, you must drill down into the call components. Mobile and Remote Access calls have different component characteristics depending on whether the call is being viewed on the VCS Control or VCS Expressway:

- On the VCS Control, a Unified CM remote session has three components (as it uses the B2BUA to enforce media encryption). One of the VCS components routes the call through one of the automatically generated neighbor zones (with a name prefixed by either **CEtcp** or **CEtls**) between VCS and Unified CM.
- On the VCS Expressway, 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 (for Expressway only)

If your system has a rich media session key installed and thus supports business-to-business calls, and interworked or gatewayed calls to third-party solutions and so on, those calls are also listed on the call status and call history pages.

Disconnecting Calls

Click **Disconnect** to disconnect the selected calls. Note that if your VCS 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 VCS 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 VCS 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 to **Status > Calls > History** and then click **View** for a particular B2BUA call.

Calls are routed through the B2BUA in the following cases:

- A media encryption policy applies to the call (any encryption setting other than *Auto*).
- VCS is load balancing calls for Cisco Meeting Server. The VCS 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 VCS version.
- ICE messaging support is triggered.
- Microsoft interoperability service is enabled and the call routed through the **To Microsoft destination via B2BUA** neighbor zone.

For Microsoft interoperability calls, you can click the **Corresponding VCS call** link to see details of the leg passing through the VCS.

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 VCS, the Microsoft server and any external transcoder (if applicable).

Search History

The **Search history** page (**Status > Search history**) lists the most recent 255 searches that have taken place since the VCS was last restarted.

About searches

Before a call can be placed, the endpoint being called must be located. The VCS sends and receives a series of messages during its attempt to locate the endpoint being called; these messages are each known as searches. An individual call can have one or more searches associated with it, and these searches can be of different types.

The type of search message that is sent depends on whether the call is for SIP or H.323, and whether the call request was received locally or from an external zone, as follows:

- H.323 calls that are placed locally: two messages are sent – the first is an **ARQ** which locates the device being called, and the second is the call **Setup** which sends a request to the device asking it to accept the call. Each message shows up as a separate search in the **Search history** page, but only the **Setup** message is associated with a particular call.
- H.323 searches originating from external zones: an **LRQ** will appear in the **Search history** page.
- SIP: a single message is sent in order to place a call: this is either a SIP **INVITE** or a SIP **OPTIONS**.

Note that an individual call can have one or more searches associated with it, and these searches can be of different types. Each search has an individual *Search ID*; each call has an individual *Call Tag* (see Identifying Calls, page 211).

The VCS 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 all of the subzones on the VCS that together make up the Local Zone. This always includes the Default Subzone and the Traversal Subzone, plus any other subzones that have been configured.

The following information is displayed:

Field	Description
Subzone name	The names of each subzone currently configured on this VCS. Clicking on a **Subzone name** takes you to the configuration page for that subzone.
Registrations	The number of devices currently registered within the subzone. Note that devices cannot be registered to the Traversal Subzone.
Calls	The number of calls currently passing through the subzone. Note that a single call may pass through more than one subzone, depending on the route it takes. For example, traversal calls from a locally registered endpoint will always pass through the Traversal Subzone, so they will show up twice; once in the originating subzone and once in the Traversal Subzone. .
Bandwidth used	The total amount of bandwidth used by all calls passing through the subzone.

Zone Status

The **Zone status** page (**Status > Zones**) lists all of the external zones on the VCS. 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 VCS. 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, eg. DNS and ENUM zones) ■ *Failed*: the protocol is enabled for the zone but its connection has failed ■ *Checking*: the protocol is enabled for the zone and the system is currently trying to establish a connection
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 VCS, along with the number of calls and the bandwidth being used by each link.

The following information is displayed:

Field	Description
Name	The name of each link. Clicking on a link **Name** takes you to the configuration page for that link.
Calls	The total number of calls currently traversing the link. Note that a single call may traverse more than one link, depending on how your system is configured.
Bandwidth used	The total bandwidth of all the calls currently traversing the link.

Pipe Status

The **Pipe status** page (**Status > Bandwidth > Pipes**) lists all of the pipes currently configured on the VCS, 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 that a single call may traverse more than one pipe, depending on how your system is configured.
Bandwidth used	The total bandwidth of all the calls currently traversing the pipe.

Policy Server Status and Resiliency

You must specify a **Status path** when configuring the VCS'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 VCS polls each address on the specified path every 60 seconds to test the reachability of that address. The VCS accepts standard HTTP(S) response status codes. (Note that the developers of the policy service must ensure that this provides the appropriate status of the service.)

If a server does not respond to status requests, VCS will deem that server's status to be in a failed state and it will not be queried for policy service requests until it returns to an active state. Its availability will not be checked again until after the 60 second polling interval has elapsed.

When the VCS needs to make a policy service request, it attempts to contact the service via one of the configured server addresses. It will try each address in turn, starting with **Server 1 address**, and then if necessary – and if configured – via the **Server 2 address** and then the **Server 3 address**. The VCS only tries to use a server address if it is in an active state, based on its most recent status query.

The VCS has a non-configurable 30 seconds timeout value for each attempt it makes to contact a policy server. However, if the server is not reachable, the connection failure will occur almost instantaneously. (Note that the TCP connection timeout is usually 75 seconds. Therefore, in practice, a TCP connection timeout is unlikely to occur as either the connection will be instantly unreachable or the 30 second request timeout will occur first.)

The VCS uses the configured **Default CPL** if it fails to contact the policy service via any of the configured addresses.

Note that this method provides resiliency but not load balancing i.e. all requests will be sent to **Server 1 address**, providing that server address is functioning correctly.

Viewing Policy Server Status via the VCS

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 if a remote service has been selected for either Call Policy or for registration restriction policy it will also display a **Call Policy** or a **Registration restriction** service respectively.

The following information is displayed:

Field	Description
Name	The name of the policy service. Clicking on a **Name** takes you to the configuration page for that service where you can change any of the settings or see the details of any connection problems.
URL	The address of the service. Note that each service can be configured with multiple server addresses for resiliency. This field displays the server address currently selected for use by the VCS.
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 VCS.

TURN Relay Usage

The **TURN relay usage** page (**Status > TURN relay usage**) provides a summary list of all the clients that are connected to the TURN server.

Note that TURN services are available on VCS Expressway systems only; they are configured via **Configuration > Traversal > TURN**.

The following information is displayed:

Field	Description
Client	The IP address of the client that requested the relay.
Media destinations	The address of destination system the media is being relayed to.
Connection protocol	Indicates if the client is connected over TCP or UDP.
Relays	Number of current relays being used by the client.

Viewing TURN relay details for a client connection

You can click on a specific client to see all of the relays and ports that it is using.

For each relay, its associated relay peer address/port is displayed. It also displays each relay's associated peer address/port (the TURN server relay port from which the media is being sent to the destination system). To see specific statistics about a relay, click **View** to go to the **TURN relay summary** page.

TURN Relay Summary

The **TURN relay summary** page provides overview information about a particular relay, including a summary count of the permissions, channels and requests associated with that relay.

To access this page, go to **Status > TURN relay usage**, then click **View** for a TURN client, and then **View** again for the required relay.

Further detailed information about the relay can be viewed by using the links in the **Related tasks** section at the bottom of the page. These let you:

- **View permissions for this relay**: information about the permissions that have been defined on this relay.
- **View channels for this relay**: information about the channel bindings that have been defined on this relay.
- **View counters for this relay**: information about the number of TURN requests received, and the number of TURN success or error responses sent. It also shows counts of the number of packets forwarded to and from the client that allocated this relay.

Unified Communications Status

The **Unified Communications status** page (**Status > Unified Communications**) shows the current status of the Unified Communications services including:

- the number of configured Unified CM and IM&P servers (VCS Control only)
- the current number of active provisioning sessions (VCS Control 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 (VCS Control 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 VCS and its "traversal partner". You can view this status from either side of the tunnel, that is, on the VCS Control or the VCS Expressway.

Here are some reasons why SSH tunnels could fail:

- The VCS Control cannot find the VCS Expressway:
  - Is there a firewall between them? Is TCP 2222 open from the VCS Control to the VCS Expressway?
  - Are there forward and reverse DNS entries for the VCS Control and VCS Expressway?

  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 VCS Expressway?
  - Is the same authentication account entered on the VCS Control?

  Try a secure traversal test from the VCS Control (**Maintenance > Security > Secure traversal test** and enter the FQDN of the VCS Expressway).

Presence

Presence Publishers

The **Publishers** page (**Status > Applications > Presence > Publishers**) lists each presentity whose presence information is being managed by (that is, published to) the local Presence Server.

All presentities are listed here regardless of whether or not anyone is requesting their presence information. If there are no publishers listed, this could mean that the presence server is not enabled on this VCS.

Note: FindMe users are not listed here as they do not have their status individually published. The status of a FindMe user is based on the published status of the endpoints and/or presentities that make up the FindMe user, and is determined by the presentity manager.

URI

The address of the presentity whose presence information is being published.

Publisher count

The number of sources of information that are being published for this particular presentity. All endpoints that are registered to the VCS have information published on their behalf by the PUA (as long as they are registered with an alias in the form of a URI). If an endpoint supports presence, it may also publish its own presence information. This means that some presentities have more than one source of information about their presence. It is the job of the presentity manager to aggregate this information and determine the actual status of the presentity.

Presence Presentities

The **Presentities** page (**Status > Applications > Presence > Presentities**) lists each presentity whose presence information is being managed by (that is, published to) the local Presence Server and whose presence information has been requested by a subscriber. Presentities are listed here whether or not there is any information currently available about that presentity. If a presentity has been subscribed to but there is no information being published about it, then it will be listed here if the local presence server is authoritative for the presentity's domain.

Presentities are listed here regardless of whether the subscriber that requested the information is registered locally or to a remote system.

Note: FindMe users are listed here if their presence information has been requested by a subscriber.

URI

The address of the presentity whose presence information has been requested.

Subscriber count

The number of endpoints who have requested information about that particular presentity.

To view the list of all subscribers who are requesting information about a particular presentity, click on the presentity's URI.

Presence Subscribers

The **Subscribers** page (**Status > Applications > Presence > Subscribers**) lists each endpoint that has requested information about one or more presentities whose information is managed by (that is, published to) the local Presence Server.

Endpoints requesting this information are listed here regardless of whether they are registered locally or to a remote server.

Note that FindMe users are not listed here as a FindMe entity cannot subscribe to presence information. However, one or more of the endpoints that make up a FindMe user may be requesting presence information, in which case that endpoint will be listed here.

URI

The address of the endpoint that has requested presence information.

Subscription count

The number of local presentities about whom this endpoint is requesting information.

To view the list of all local presentities whose information is being requested by a particular endpoint, click on the endpoint's URI.

Microsoft interoperability

Microsoft-registered FindMe User Status

The **Status > Applications > Microsoft-registered FindMe users** page lists the current status of all FindMe IDs being handled by the Microsoft Interoperability service.

It applies to deployments that use both Microsoft clients and FindMe, if they both use the same SIP domain. To enable this feature, **Register FindMe users as clients to Microsoft server** must be set to *Yes* on the Microsoft Interoperability configuration page.

The following information is displayed:

Field	Description
URI	The FindMe ID being handled by the B2BUA Presence Relay application.
Presence state	Shows the presence information currently being published for the FindMe ID.
Registration state	Indicates whether the FindMe ID has registered successfully with a Microsoft Front End server. Doing so allows Microsoft infrastructure to forward calls to the FindMe ID. Note that FindMe users can only register to Microsoft infrastructure if the FindMe ID is a valid user in the Active Directory (in the same way that Microsoft clients can only register if they have a valid account enabled in AD).
Subscription state	Indicates whether the B2BUA Presence Relay application has subscribed successfully to the FindMe ID's presence information. Doing so allows Lync clients to view the presence information of FindMe users.
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 Microsoft interoperability service.

This service routes SIP calls between the VCS 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 VCS 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 VCS in the cluster has the actual connection to the Cisco TMSPE services (only displayed if the VCS 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 VCS from the **TMS Provisioning Extension services** page (**System > TMS Provisioning Extension services**).

See the Provisioning Server section for more information.

Provisioning Server Device Requests Status (Cisco TMSPE)

The **Device requests status** page (**Status > Applications > TMS Provisioning Extension services > Device requests**) shows the status of the VCS Provisioning Server when using Cisco TMSPE.

If device provisioning is enabled, the VCS Provisioning Server provides provisioning-related services to provisioned devices, using data supplied by Cisco TMS through the Cisco TMS provisioning mechanism.

As from version X8.1 , the VCS supports only the Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) services to provide the VCS 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 VCS 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 VCS (or VCS cluster); this information is broken down by the device types that can be provisioned by this VCS

License information is exchanged between Cisco TMS and VCS by the Cisco TMSPE Devices service. If the Devices service is not active, the VCS'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 VCSs or VCS 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 VCS or VCS 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 VCS was last restarted.

User Records Provided by Cisco TMSPE Services

You can view the data records provided by the Cisco TMSPE **Users** service by going to **Status > Applications > TMS Provisioning Extension services > Users > ...** and then the relevant table:

- **Accounts**
- **Groups**
- **Templates**

All the records in the chosen table are listed. Note that some tables can contain several thousand records and you may experience a delay before the data is displayed.

Filtering the view

The **Filter** section lets you filter the set of records that are shown. It is displayed only if there is more than one page of information to display. Status pages show 200 records per page.

Enter a text string or select a value with which to filter each relevant field, and then click **Filter**.

Only those records that match all of the selected filter options are shown. Note that text string filtering is case insensitive.

Viewing more details and related records

You can click **View** to display further details about the selected record. Many views also allow you to click on related information to see the data records associated with that item. For example, when viewing user groups, you can also access the related user templates. When viewing user accounts you can check the data that would be provisioned to that user by clicking Check provisioned data.

FindMe Records Provided by Cisco TMSPE Services

You can view the data records provided by the Cisco TMSPE **FindMe** service by going to **Status > Applications > TMS Provisioning Extension services > FindMe > ...** and then the relevant table:

- **Accounts**
- **Locations**
- **Devices**

All the records in the chosen table are listed. Note that some tables can contain several thousand records and you may experience a delay before the data is displayed.

Filtering the view

The **Filter** section lets you filter the set of records that are shown. It is displayed only if there is more than one page of information to display. Status pages show 200 records per page.

Enter a text string or select a value with which to filter each relevant field, and then click **Filter**.

Only those records that match all of the selected filter options are shown. Note that text string filtering is case insensitive.

Viewing more details and related records

You can click **View** to display further details about the selected record. Many views also allow you to click on related information to see the data records associated with that item. For example, when viewing a FindMe user, you can also access the related location and device records.

Phone Book Records Provided by Cisco TMSPE Services

You can view the data records provided by the Cisco TMSPE **Phone books** service by going to **Status > Applications > TMS Provisioning Extension services > Phone book > ...** and then the relevant table:

- **Folders**
- **Entries**
- **Contact methods**
- **User access**

All the records in the chosen table are listed. Note that some tables can contain several thousand records and you may experience a delay before the data is displayed.

Filtering the view

The **Filter** section lets you filter the set of records that are shown. It is displayed only if there is more than one page of information to display. Status pages show 200 records per page.

Enter a text string or select a value with which to filter each relevant field, and then click **Filter**.

Only those records that match all of the selected filter options are shown. Note that text string filtering is case insensitive.

Viewing more details and related records

You can click **View** to display further details about the selected record. Many views also allow you to click on related information to see the data records associated with that item. For example, when viewing a phone book entry, you can also access the related contact method or folder.

Provisioned Devices

The **Provisioned device status** page (**Status > Applications > TMS Provisioning Extension services > Provisioned device status**) displays a list of all of the devices that have submitted provisioning requests to the VCS'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 that text string filtering is case insensitive.

The list shows all current and historically provisioned devices. A device appears in the list after it has made its first provisioning request. The **Active** column indicates if the device is currently being provisioned (and is thus consuming a provisioning license).

Checking Provisioned Data

The **Check provisioned data** page is used to check the configuration data that the VCS's Provisioning Server will provision to a specific user and device combination.

You can get to this page only through the **User accounts** status page (**Status > Applications > TMS Provisioning Extension services > Users > Accounts**, locate the user you want to check and then click **Check provisioned data**).

To check provisioned data:

1. Verify that the **User account name** is displaying the name of the user account you want to check.
2. Select the **Model** and **Version** of the user's endpoint device.
   If the actual **Version** used by the endpoint is not listed, select the nearest earlier version.
3. Click **Check provisioned data**.

The **Results** section will show the data that would be provisioned out to that user and device combination.

Starter Pack Provisioning Server Status

The **Starter Pack status** page (**Status > Applications > Starter Pack > Starter Pack status**) shows the status of the VCS's Provisioning Server when running as a Starter Pack.

The Starter Pack Provisioning Server provides basic provisioning-related services to provisioned devices, without the need for Cisco TMS.

Provisioning server

This section displays the server's status and summarizes the subscription requests received by the server since the VCS 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 number of licenses currently being used by devices that are registered to this VCS. This information is broken down by the device types that can be provisioned by this VCS.

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 VCS was last restarted.

Managing Alarms

Alarms occur when an event or configuration change has taken place on the VCS 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 VCS, 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 VCS configuration issues
55nnn	B2BUA issues
6nnnn	Hybrid Services alarms
60000-60099	Management Connector alarms
60100-60199	Calendar Connector alarms
60300-60399	Call Connector alarms

All alarms raised on the VCS 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 VCS only after the required action or configuration change has been made.
- After a restart of the VCS, any *Acknowledged* alarms that are still in place on the VCS 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 VCS was last restarted.
- If your VCS is a part of a cluster, the **Alarms** page shows all of the alarms raised by any of the cluster peers. However, you can acknowledge only those alarms that have been raised by the "current" peer (the peer to which you are currently logged in to as an administrator).
- You can click the Alarm ID to generate a filtered view of the Event Log, showing all occurrences of when that alarm has been raised and lowered.

See the alarms list for further information about the specific alarms that can be raised.

Logs

Event Log

The **Event Log** page (**Status > Logs > Event Log**) lets you view and search the Event Log, which is a list of the events that have occurred on your system since the last upgrade.

The Event Log holds a maximum of 2GB of data; when this size is reached, the oldest entries are overwritten. However, only the first 50MB of Event Log data can be displayed through the web interface.

Filtering the Event Log

The **Filter** section lets you filter the Event Log. It is displayed only if there is more than one page of information to display. Log pages show 1000 records per page.

Enter the words you want to search for and click **Filter**. Only those events that contain all the words you entered are shown.

To do more advanced filtering, click **more options**. This gives you additional filtering methods:

- **Contains the string**: only includes events containing the exact phrase entered here.
- **Contains any of the words**: includes any events that contain at least one of the words entered here.
- **Not containing any of the words**: filters out any events containing any of the words entered here.

Note: use spaces to separate each word you want to filter by.

Click **Filter** to reapply any modified filter conditions. To return to the complete log listing, click **Reset**.

Reconfiguring the log settings

Clicking **Configure the log settings** takes you to the Logging configuration page. From this page, you can set the level of events that are recorded in the Event Log, and also set up a remote server to which the Event Log can be copied.

Saving the results to a local disk

Click **Download this page** if you want to download the contents of the results section to a text file on your local PC or server.

Results section

The **Results** section shows all the events matching the current filter conditions, with the most recent being shown first.

Most **tvcs** events contain hyperlinks in one or more of the fields (such fields change color when you hover over them). You can click on the hyperlink to show only those events that contain the same text string. For example, clicking on the text that appears after **Event=** filters the list to show all the events of that particular type. Likewise, clicking on a particular **Call-Id** shows just those events that contain a reference to that particular call.

Event Log color coding

Certain events in the Event Log are color-coded so that you can identify them more easily. These events are as follows:

Green events:

- System Start
- Admin Session Start/Finish
- Installation of <item> succeeded
- Registration Accepted
- Call Connected
- Request Successful
- Beginning System Restore
- Completed System Restore

Orange events:

- System Shutdown
- Intrusion Protection Unblocking

Purple events:

- Diagnostic Logging

Red events:

- Registration Rejected
- Registration Refresh Rejected
- Call Rejected
- Security Alert
- License Limit Reached
- Decode Error
- TLS Negotiation Error
- External Server Communications Failure
- Application Failed
- Request Failed
- System Backup Error
- System Restore Error
- Authorization Failure
- Intrusion Protection Blocking

For more information about the format and content of the Event Log see Event Log Format, page 354 and Events and Levels, page 357.

Configuration Log

The **Configuration Log** page (**Status > Logs > Configuration Log**) provides a list of all changes to the VCS configuration.

The Configuration Log holds a maximum of 30MB of data; when this size is reached, the oldest entries are overwritten. The entire Configuration Log can be displayed through the web interface.

Filtering the Configuration Log

The **Filter** section lets you filter the Configuration Log. It is displayed only if there is more than one page of information to display. Log pages show 1000 records per page.

Enter the words you want to search for and click **Filter**. Only those events that contain all the words you entered are shown.

To do more advanced filtering, click **more options**. This gives you additional filtering methods:

- **Contains the string**: only includes events containing the exact phrase entered here.
- **Contains any of the words**: includes any events that contain at least one of the words entered here.
- **Not containing any of the words**: filters out any events containing any of the words entered here.

Note: use spaces to separate each word you want to filter by.

Click **Filter** to reapply any modified filter conditions. To return to the complete log listing, click **Reset**.

Results section

The **Results** section shows all the web-based events, with the most recent being shown first.

Most events contain hyperlinks in one or more of the fields (such fields change color when you hover over them). You can click on the hyperlink to show only those events that contain the same text string. For example, clicking on the text that appears after **Event=** filters the list to show all the events of that particular type. Likewise, clicking on a particular **user** shows just those events relating to that particular administrator account.

All events that appear in the Configuration Log are recorded as Level 1 Events, so any changes to the logging levels will not affect their presence in the Configuration Log.

Configuration Log events

Changes to the VCS 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 VCS.

The Network Log holds a maximum of 2GB of data; when this size is reached, the oldest entries are overwritten. However, only the first 50MB of Network Log data can be displayed through the web interface.

Filtering the Network Log

The **Filter** section lets you filter the Network Log. It is displayed only if there is more than one page of information to display. Log pages show 1000 records per page.

Enter the words you want to search for and click **Filter**. Only those events that contain all the words you entered are shown.

To do more advanced filtering, click **more options**. This gives you additional filtering methods:

- **Contains the string**: only includes events containing the exact phrase entered here.
- **Contains any of the words**: includes any events that contain at least one of the words entered here.

- **Not containing any of the words**: filters out any events containing any of the words entered here.

Note: use spaces to separate each word you want to filter by.

Click **Filter** to reapply any modified filter conditions. To return to the complete log listing, click **Reset**.

Reconfiguring the log settings

Clicking **Configure the log settings** takes you to the Network Log configuration page. From this page, you can set the level of events that are recorded in the Network Log.

Saving the results to a local disk

Click **Download this page** if you want to download the contents of the results section to a text file on your local PC or server.

Results Section

The **Results** section shows the events logged by each of the Network Log modules.

Most events contain hyperlinks in one or more of the fields (such fields change color when you hover over them). You can click on the hyperlink to show only those events that contain the same text string. For example, clicking on the text that appears after **Module=** filters the list to show all the events of that particular type.

The events that appear in the Network Log are dependent on the log levels configured on the Network Log configuration page.

Hardware Status

The **Hardware** page (**Status > Hardware**) provides information about the physical status of your VCS appliance.

Information displayed includes:

- fan speeds
- component temperatures
- component voltages

Any appropriate minimum or maximum levels are shown to help identify any components operating outside of their standard limits.

Warning: do not attempt to service the apparatus yourself as opening or removing covers may expose you to dangerous voltages or other hazards, and will void the warranty. Refer all servicing to qualified service personnel.

Note that hardware status information is not displayed if the VCS is running on VMware.

Reference Material

This section provides supplementary information about the features and administration of the VCS.

About Event Log Levels 354
CPL Reference 364
LDAP Server Configuration for Device Authentication 374
DNS Configuration Examples 379
Changing the Default SSH Key 380
Restoring the Default Configuration (Factory Reset) 380
Password Encryption 383
Pattern Matching Variables 384
Port Reference 385
Regular expressions 386
Supported Characters 388
Call Types and Licensing 389
Product Identifiers and Corresponding Keys 390
Allow List Rules File Reference 392
Allow List Tests File Reference 393
VCS Multitenancy Overview 394
Multitenant VCS Sizing 395
Alarms 397
Command Reference – xConfiguration 434
Command Reference – xCommand 511
Command Reference – xStatus 549
External Policy Overview 551
Flash Status Word Reference Table 554
Supported RFCs 555
Software Version History 557
Legal Notices 562

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 VCS, 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.

Field	Description
process_name	The name of the program generating the log message. This could include: ▪ **tvcs** for all messages originating from VCS processes ▪ **web** for all web login and configuration events ▪ **licensemanager** for messages originating from the call license manager ▪ **provisioning** for provisioning server events ▪ **b2bua** for B2BUA events ▪ **presencerelay** for B2BUA Presence Relay application events ▪ **portforwarding** for internal communications between the VCS Control and the VCS Expressway ▪ **ssh** for ssh tunnels between the VCS Control and the VCS Expressway but will differ for messages from other applications running on the VCS.
message_details	The body of the message (see the Message details field section for further information).

Administrator and FindMe User Events

Administrator session related events are:

- Admin Session Start
- Admin Session Finish
- Admin Session Login Failure

FindMe user session related events are:

- User Session Start
- User Session Finish
- User Session Login Failure

For both administrator and FindMe user related events, the Detail field includes:

- the name of the administrator or FindMe 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 VCS, and the level at which they are logged.

Name	Description
User	The username that was entered when a login attempt was made.
ipaddr	The source IP address of the user who has logged in.
Protocol	Specifies which protocol was used for the communication. Valid values are: ■ 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: ■ H323 ■ 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.
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.

Name	Description
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 a VCS network for all forks of a call.
Call-routed	Indicates if the VCS 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.
Level	The level of the event as defined in the About Event Log levels section.
UTCTime	Time the event occurred, shown in UTC format.

Events and Levels

The following table lists the events that can appear in the Event Log.

Event	Description	Level
Alarm acknowledged	An administrator has acknowledged an alarm. The **Detail** event parameter provides information about the nature of the issue.	1
Alarm lowered	The issue that caused an alarm to be raised has been resolved. The **Detail** event parameter provides information about the nature of the issue.	1
Alarm raised	The VCS 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 VCS is configured to use certificate-based authentication.	1

Event	Description	Level
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 VCS application has been exited. Further information may be provided in the **Detail** event parameter.	1
Application Failed	The VCS application is out of service due to an unexpected failure.	1
Application Start	The VCS has started. Further detail may be provided in the **Detail** event parameter.	1
Application Warning	The VCS application is still running but has experienced a recoverable problem. Further detail may be provided in the **Detail** event parameter.	1
Authorization Failure	The user has either entered invalid credentials, does not belong to an access group, or belongs to a group that has an access level of "None". Applies when remote authentication is enabled.	1
Beginning System Backup	A system backup has started.	1
Beginning System Restore	A system restore has started.	1
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 VCS 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

Event	Description	Level
Completed System Backup	A system backup has completed.	1
Completed System restore	A system restore has completed.	1
Configlog Cleared	An operator cleared the Configuration Log.	1
Decode Error	A syntax error was encountered when decoding a SIP or H.323 message.	1
Diagnostic Logging	Indicates that diagnostic logging is in progress. The **Detail** event parameter provides additional details.	1
Error Response Sent	The TURN server has sent an error message to a client (using STUN protocol).	3
Eventlog Cleared	An operator cleared the Event Log.	1
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	1
FindMe Search Failed	A search of the FindMe database has failed, for example due to no alias being provided.	1
Hardware Failure	There is an issue with the VCS hardware. If the problem persists, contact your Cisco support representative.	1
License Limit Reached	Licensing limits for a given feature have been reached. The **Detail** event parameter specifies the facility/limits concerned. Possible values for the detail field are: ■ Non Traversal Call Limit Reached ■ Traversal Call Limit Reached If this occurs frequently, you may want to contact your Cisco representative to purchase more licenses.	1
Message Received	An incoming RAS message has been received.	2
Message Received	An incoming RAS NSM Keepalive, H.225, H.245 or a RAS message between peers has been received.	3
Message Received	(SIP) An incoming message has been received.	4

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 VCS. This could be either because the endpoint has not supplied any authentication credentials, or because its credentials do not match those expected by the VCS. ■ Clustering is enabled but bandwidth across the cluster has not been configured identically, and the VCS has received a message relating to an unknown peer, link, pipe, subzone or zone.	1
Message Sent	An outgoing RAS message has been sent.	2
Message Sent	An outgoing RAS NSM Keepalive, H.225, H.245 or a RAS message between peers has been sent.	3
Message Sent	(SIP) An outgoing message has been sent.	4
Operator Call Disconnect	An administrator has disconnected a call.	1
Outbound TLS Negotiation Error	The VCS 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
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

Event	Description	Level
Registration Removed	A registration has been removed by the VCS. 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
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 VCS is in **Call loop detection** mode and has identified and terminated a looped branch of a search.	2

Event	Description	Level
Secure mode disabled	The VCS has successfully exited **Advanced account security** mode.	1
Secure mode enabled	The VCS has successfully entered **Advanced account security** mode.	1
Security Alert	A potential security-related attack on the VCS has been detected.	1
Source Aliases Rewritten	A source alias has been changed to indicate the caller's FindMe ID.	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
System Start	The operating system has started. The **Detail** event parameter may contain additional information if there are startup problems.	1

Event	Description	Level
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
User session finish	A FindMe user has logged out of the system.	1
User session Login failure	An unsuccessful attempt has been made to log in as a FindMe user. This could be because either an incorrect username or password (or both) was entered.	1
User session start	A FindMe user has logged on to the system.	1

CPL Reference

Call Processing Language (CPL) is an XML-based language for defining call handling. This section gives details of the VCS's implementation of the CPL language and should be read in conjunction with the CPL standard *RFC 3880*.

The VCS has many powerful inbuilt transform features so CPL should be required only if advanced call handling rules are required.

The VCS 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 VCS, the script is checked against an XML schema to verify the syntax. There are two schemas - one for the basic CPL specification and one for the TANDBERG extensions. Both of these schemas can be downloaded from the web interface and used to validate your script before uploading to the VCS.

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 VCS 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.
`authenticated-origin` and `origin`	The "From" and "ReplyTo" fields of the message if it authenticated 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 VCS 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 or subzone according to the source of the incoming message.

If the selected field contains multiple aliases then the VCS 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 VCS 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. Note that this will override any User Policy that may have been applied.
`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. Note that this will override any User Policy that may have been applied.

If the source URL of a From header is modified, any corresponding display name is also modified to match the username part of the modified source URL.

Rule-Switch

This extension to CPL is provided to simplify Call Policy scripts that need to make decisions based on both the source and destination of the call. A `taa:rule-switch` can contain any number of rules that are tested in sequence; as soon as a match is found the CPL within that rule element is executed.

Each rule must take one of the following forms:

```
<taa:rule-switch>
  <taa:rule origin="<regular expression>" destination="<regular expression>" message-regex="<regular
expression>">
  <taa:rule authenticated-origin="<regular expression>" destination="<regular expression>" message-
regex="<regular expression>">
  <taa:rule unauthenticated-origin="<regular expression>" destination="<regular expression>" message-
regex="<regular expression>">
  <taa:rule registered-origin="<regular expression>" destination="<regular expression>" message-
regex="<regular expression>">
  <taa:rule originating-user="<regular expression>" destination="<regular expression>" message-
regex="<regular expression>">
  <taa:rule originating-zone="<regular expression>" destination="<regular expression>" message-
regex="<regular expression>">
</taa:rule-switch>
```

The meaning of the various `origin` selectors is as described in the field section.

The `message-regex` parameter allows a regular expression to be matched against the entire incoming SIP message.

Note that any rule containing a message-regex parameter will never match an H.323 call.

Proxy

On executing a proxy node the VCS 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`	VCS 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 VCS 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 VCS 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 VCS 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 alias
- 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
- Redirecting failed calls based on status code
- Reject attempts to subscribe to a presentity

CPL Example: Call Screening of Authenticated Users

Note: You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See About Call Policy, page 191.

In this example, only calls from users with authenticated source addresses are allowed. See About Device Authentication, page 99 for details on how to enable authentication.

If calls are coming in through VCS Expressway, then we recommend screening on the VCS Expressway to prevent unwelcome calls from progressing into the network.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
  xmlns:taa="http://www.tandberg.net/cpl-extensions"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
  <taa:routed>
    <address-switch field="authenticated-origin">
      <not-present>
        <!-- Reject call with a status code of 403 (Forbidden) -->
        <reject status="403" reason="Denied by policy"/>
      </not-present>
    </address-switch>
  </taa:routed>
</cpl>
```

CPL Example: Call Screening Based on Alias

Note: You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See About Call Policy, page 191.

In this example, user `ceo` will only accept calls from users `vpsales`, `vpmarketing` or `vpengineering`.

If calls are coming in through VCS Expressway, then we recommend screening on the VCS Expressway 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, page 191.

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 VCS Expressway, then we recommend screening on the VCS Expressway 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

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 VCS"/>
      </not-present>
    </address-switch>
  </taa:routed>
</cpl>
```

CPL Example: Block Calls From Default Zone and Default Subzone

Note: You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See About Call Policy, page 191.

The script to allow calls from locally registered endpoints only can be extended to also allow calls from configured zones but not from the Default Zone or Default Subzone.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
  xmlns:taa="http://www.tandberg.net/cpl-extensions"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
  <taa:routed>
    <address-switch field="registered-origin">
      <not-present>
        <address-switch field="originating-zone">
          <address is="DefaultZone">
            <!-- Reject call with a status code of 403 (Forbidden) -->
            <reject status="403" reason="Denied by policy"/>
          </address>
          <address is="DefaultSubZone">
            <!-- Reject call with a status code of 403 (Forbidden) -->
            <reject status="403" reason="Denied by policy"/>
          </address>
          <otherwise>
            <proxy/>
          </otherwise>
        </address-switch>
      </not-present>
    </address-switch>
  </taa:routed>
</cpl>
```

CPL Example: Restricting Access to a Local Gateway

Note: You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See About Call Policy, page 191.

In these examples, a gateway is registered to the VCS 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.

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>
```

CPL Example: Redirecting Failed Calls Based on Status Code

The output from a `proxy` node allow actions to be taken based on the result of the proxy operation. In base CPL a single failure output is allowed which is invoked if the call attempt fails for any reason (see section 6.1 of *RFC 3880* for details).

The VCS supports an extension to the base CPL specification that allows a status code to be specified so that the failure action is only invoked if the call attempt fails for the specified reason. In addition the VCS allows multiple failure outputs to be specified within a single proxy node. This allows a script to redirect the call to different locations (such as different recorded messages) based on the exact reason for call failure.

For example:

```
<?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>
    <!-- Proxy the call normally, but redirect to different recorded messages based on -->
    <!-- the particular error response we get -->
    <proxy>
      <failure status="403">
        <!-- Call attempt failed with 403 (Forbidden) -->
        <taa:location url="forbidden-message@example.com" clear="yes">
          <proxy/>
        </taa:location>
      </failure>
      <failure status="404">
        <!-- Call attempt failed with 404 (Not Found) -->
        <taa:location url="notfound-message@example.com" clear="yes">
          <proxy/>
        </taa:location>
      </failure>
      <failure>
        <!-- General catch-all failure handler for all other error responses -->
        <taa:location url="failed-message@example.com" clear="yes">
          <proxy/>
        </taa:location>
      </failure>
    </proxy>
  </taa:routed>
</cpl>
```

CPL Example: Reject Attempts to Subscribe to a Presentity

In this example, attempts to subscribe to the presence of `user@example.com` are rejected.

```
<?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 origin=".*" destination="user@example.com" message-regex="^SUBSCRIBE.*">
        <!-- Cannot subscribe to user@example.com -->
        <!-- Reject call with a status code of 403 (Forbidden) -->
        <reject status="403" reason="Denied by policy"/>
      </taa:rule>
    </taa:rule-switch>
  </taa:routed>
</cpl>
```

LDAP Server Configuration for Device Authentication

The VCS can be configured to authenticate devices against an H.350 directory service on an LDAP server.

This section describes how to:

- download the schemas that must be installed on the LDAP server
- install and configure two common types of LDAP servers for use with the VCS:
  - Microsoft Active Directory
  - OpenLDAP

Downloading the H.350 Schemas

The following ITU specifications describe the schemas which are required to be installed on the LDAP server:

H.350	Directory services architecture for multimedia conferencing – an LDAP schema to represent endpoints on the network.
H.350.1	Directory services architecture for H.323 – an LDAP schema to represent H.323 endpoints.
H.350.2	Directory services architecture for H.235 – an LDAP schema to represent H.235 elements.
H.350.4	Directory services architecture for SIP – an LDAP schema to represent SIP endpoints.

The schemas can be downloaded from the web interface on the VCS. To do this:

1. Go to **Configuration > Authentication > Devices > H.350 directory schemas**. You are presented with a list of downloadable schemas.
2. Click on the **Download** button next to each file to open it.
3. Use your browser's **Save As** command to store it on your file system.

Configuring a Microsoft Active Directory LDAP Server

Prerequisites

These instructions assume that Active Directory has already been installed. For details on installing Active Directory please consult your Windows documentation.

The following instructions are for Windows Server 2003 Enterprise Edition. If you are not using this version of Windows, your instructions may vary.

Installing the H.350 Schemas

After you have downloaded the H.350 schemas, install them as follows:

Open an elevated command prompt by right-clicking Command Prompt and selecting 'Run as administrator'. For each file execute the following command:

```
ldifde -i -c DC=X <ldap_base> -f filename.ldf
```

where:

`<ldap_base>` is the base DN for your Active Directory server.

Adding H.350 Objects

Create the organizational hierarchy:

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 VCS 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 Using an H.350 Directory Service Lookup via LDAP, page 117 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 VCS 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 VCS 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 VCS (**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 VCS 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 VCS 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 Using an H.350 Directory Service Lookup via LDAP, page 117 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 VCS 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 VCS 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 VCS by going to: **Maintenance > Security > Trusted CA certificate**.

DNS Configuration Examples

This section gives examples of DNS configuration using Microsoft DNS Server and BIND 8 & 9.

These examples show how to set up an SRV record to handle H.323 URIs of the form `user@example.com`. These are handled by the system with the fully qualified domain name of `vcs.example.com` which is listening on port 1719, the default registration port.

It is assumed that both A and AAAA records already exist for `vcs.example.com`. If not, you will need to add them.

Verifying the SRV Record

There are a range of tools available to investigate DNS records. One commonly found on Microsoft Windows and UNIX platforms is `nslookup`. Use this to verify that everything is working as expected. For example:

```
nslookup -querytype=srv_h323ls._udp.example.com
```

and check the output.

Microsoft DNS Server

Using Microsoft DNS Server you can add the SRV record using either the command line or the MMC snap-in.

To use the command line, on the DNS server open a command window and enter:

```
dnscmd . /RecordAdd domain service_name SRV Priority Weight Port Target
```

where:

domain	is the domain into which you want to insert the record
service_name	is the name of the service you are adding
Priority	is the priority as defined by *RFC 2782*
Weight	is the weight as defined by *RFC 2782*
Port	is the port on which the system hosting the domain is listening
Target	is the FQDN of the system hosting the domain

For example:

```
dnscmd . /RecordAdd example.com_h323ls._udp SRV 1 0 1719 vcs.example.com
```

BIND 8 & 9

BIND is a commonly used DNS server on UNIX and Linux systems. Configuration is based around two sets of text files: **named.conf** which describes which zones are represented by the server, and a selection of zone files which describe the detail of each zone.

BIND is sometimes run chrooted for increased security. This gives the program a new root directory, which means that the configuration files may not appear where you expect them to be. To see if this is the case on your system, run

```
ps aux | grep named
```

This will give the command line that named (the BIND server) was invoked with. If there is a `-t` option, then the path following that is the new root directory and your files will be located relative to that root.

In **/etc/named.conf** look for a directory entry within the options section. This will give the directory in which the zone files are stored, possibly relative to a new root directory. In the appropriate zone section, a file entry will give the name of the file containing the zone details.

For more details of how to configure BIND servers and the DNS system in general see the publication *DNS and BIND*.

Changing the Default SSH Key

Using the default key means that SSH sessions established to the VCS may be vulnerable to "man-in-the-middle" attacks, so we recommend that you generate new SSH keys that are unique to your VCS.

An alarm message "Security alert: the SSH service is using the default key" is displayed if your VCS is still configured with its factory default SSH key.

To generate a new SSH key for the VCS:

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 VCS 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 VCS over SSH you may receive a warning that the key identity of the VCS has changed. Please follow the appropriate process for your SSH client to suppress this warning.

If your VCS is subsequently downgraded to an earlier version of VCS 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**

Process to Reset to the Default Configuration

You must do this procedure from the console (or via a direct connection to the appliance with a keyboard and monitor). Because the network settings are rewritten, all calls and any SSH session used to initiate the reset will be dropped and you won't be able to see the procedure output.

The process takes approximately 20 minutes.

1. Log in to the system as **root**.
2. Type `factory-reset`
3. Answer the questions as required. The recommended responses will reset the system completely to a factory default state:

Prompt	Recommended response
Keep option keys [YES/NO]?	NO
Keep FIPS140 configuration [YES/NO]?	NO
Keep IP configuration [YES/NO]?	NO
Keep ssh keys [YES/NO]?	NO
Keep server certificate, associated key and CA trust store [YES/NO]? 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

Cisco TAC may also suggest an alternative reset method. This involves downloading the software image onto a USB stick and then rebooting the system with the USB stick plugged in.

If you use this method you must clear down and rebuild the USB stick after use. Do not reset one system and then take the USB stick and re-use it on another system.

Note: Reset functionality comes built in with the CE1100 and later hardware appliances, through the Internal Recovery Partition (IRP). See the *CEnnnn Appliance Installation Guide* on the Install and Upgrade Guides page for more information.

Password Encryption

All passwords configured on the VCS are stored securely in either an encrypted or hashed form. This applies to the following items, which all have usernames and passwords associated with them:

- the default admin administrator account
- any additional administrator accounts
- local authentication database credentials (a list of valid usernames and passwords that are used when other devices are required to authenticate with the VCS)
- outbound connection credentials (used by the VCS when required to authenticate with another system)
- LDAP server (used by the VCS when binding to an LDAP server)

Web interface

When entering or viewing passwords using the web interface, you will see placeholder characters (e.g. dots or stars, depending on your browser) instead of the characters you are typing.

Command line interface (CLI)

When entering passwords using the command line interface (CLI), you type the password in plain text. However, after the command has been executed, the password is displayed in its encrypted form with a `{cipher}` prefix, for example:

```
xConfiguration Authentication Password: "{cipher}xcy6k+4NgB025vYEgoEXXw=="
```

Note that FindMe is a standalone application that can be hosted by the VCS or by another remote server. This means that FindMe account information is not configured or accessible using the CLI of the VCS. However, FindMe account passwords are still stored securely.

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 that:

- local administrator account passwords are hashed using SHA512; other passwords are stored in an encrypted format
- when a password is encrypted and stored, it uses more characters than the original plain text version of the password

Pattern Matching Variables

The VCS makes use of pattern matching in a number of its features, namely Allow Lists and Deny Lists, pre-search transforms and when configuring search rules and zone transforms.

For each of these pattern matches, the VCS 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 VCS 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 VCS 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 VCS is part of a cluster.	Replaces the string with the LAN 1 IPv4 address. If the VCS 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 VCS is part of a cluster.	Replaces the string with the LAN 2 IPv4 address. If the VCS is part of a cluster, the address of the local peer is always used.
%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 VCS is part of a cluster.	not applicable

String	Represents value returned by…	When used in a Pattern field	When used in a Replace field
%ipv6_1%	xConfiguration Ethernet 1 IP V6 Address	Matches the IPv6 address currently configured for LAN 1. Applies to all peer addresses if the VCS is part of a cluster.	Replaces the string with the LAN 1 IPv6 address. If the VCS 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 VCS is part of a cluster.	Replaces the string with the LAN 2 IPv6 address. If the VCS is part of a cluster, the address of the local peer is always used.
%localdomains%	xConfiguration SIP Domains Domain 1 Name … xConfiguration SIP Domains Domain 200 Name	Matches all the SIP domains currently configured on the VCS.	not applicable
%localdomain1% … %localdomain200%	xConfiguration SIP Domains Domain 1 Name … xConfiguration SIP Domains Domain 200 Name	Matches the specified SIP domain. Up to 200 SIP domains can be configured on the VCS, and they are identified by an index number between 1 and 200.	Replaces the string with the specified SIP domain.
%systemname%	xConfiguration SystemUnit Name	Matches the VCS's System Name.	Replaces the string with the VCS's System Name.

You can test whether a pattern matches a particular alias and is transformed in the expected way by using the **Check pattern** tool (**Maintenance > Tools > Check pattern**).

Port Reference

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 VCS features such as alias transformations, zone transformations, CPL policy and ENUM. The VCS 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 (*)
(...)	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 VCS 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
- FindMe account names additionally allow the use of all uppercase and lowercase Unicode characters

The following characters are specifically not allowed:

- tabs
- angle brackets (< and >)
- ampersand (&)
- caret (^)

Note that some specific text fields (including Administrator and user groups) have different restrictions and these are noted in the relevant sections of this guide.

Case sensitivity

Text items entered through the CLI and web interface are case insensitive. The only exceptions are passwords and local administrator account names which are case sensitive.

Call Types and Licensing

The VCS distinguishes between the following types of call:

- **Unified CM remote sessions**: these are "Mobile and Remote Access" 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. These calls do not require any type of call license, although they do contribute to traversal load.
- **VCS traversal calls**: these are standard VCS video or audio calls, including business-to-business calls, B2BUA calls (for media encryption or ICE), and interworked or gatewayed calls to third-party solutions where the VCS takes both the call signaling and the call media. Each call consumes a traversal call license.

  Audio-only SIP traversal calls are treated distinctly from video SIP traversal calls. **For Expressway:** 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.**For VCS:** Each traversal call license allows either 1 video call or 2 audio-only SIP calls. Hence, a 100 traversal call 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 standard video call license (traversal or non-traversal as appropriate).
- **VCS non-traversal calls**: these are standard VCS video or audio calls where the signaling passes through the VCS but the media goes directly between the endpoints, or between an endpoint and another system in the call route. Each call consumes a non-traversal call license. Note that Microsoft interoperability calls are classified as non-traversal calls (even though the media does traverse the VCS).

Each VCS also allows up to 750 concurrent non-traversal calls.

Note that:

- VCS defines an "audio-only" SIP call as one that was negotiated with a single “m=” line in the SDP. Thus, for example, if a person makes a “telephone” call but the SIP UA includes an additional m= line in the SDP, the call will consume a video call license.
- While an "audio-only" SIP call is being established, it is treated (licensed) as a video call. It only becomes licensed as "audio-only" when the call setup has completed. This means that if your system approaches its maximum licensed limit, you may be unable to connect some "audio-only" calls if they are made simultaneously.

What are Traversal Calls?

A traversal call is any call passing through the VCS that includes both the signaling (information about the call) and media (voice and video). The only other type of call is a non-traversal call, where the signaling passes through the VCS but the media goes directly between the endpoints (or between one endpoint and another VCS in the call route, or between two VCSs in the call route).

A call is "traversal" or "non-traversal" from the point of view of the VCS through which it is being routed at the time. A call between two endpoints may pass through two or more VCSs. Some of these VCSs may just take the signaling, in which case the call will be a non-traversal call for that VCS. Other VCSs in the route may need to take the media as well, and so the call will count as a traversal call on that particular VCS.

The following types of calls require the VCS to take the media. They are classified as traversal calls, require a traversal call license, and always pass through the Traversal Subzone:

- Unified CM remote sessions (these do not require a traversal call license).
- All other firewall traversal calls that are not Unified CM remote sessions, where the local VCS is either the traversal client or traversal server.
- Calls that are gatewayed (interworked) between H.323 and SIP on the local VCS.
- Calls that are gatewayed (interworked) between IPv4 and IPv6 on the local VCS.

- For a VCS Expressway with Advanced Networking enabled, calls that are inbound from one LAN port and outbound on the other.
- A SIP to SIP call when one of the participants is behind a NAT (unless both endpoints are using ICE for NAT traversal).
- Calls that invoke the B2BUA to apply a media encryption policy or for ICE messaging support.

Note that for calls via the Microsoft interoperability service, the B2BUA application always takes the media but the call is not classified as a VCS traversal call and does not consume a traversal call license (it may still consume a non-traversal license if the VCS takes the call signaling).

Traversal calls use more resource than non-traversal calls, and the numbers of each type of call are licensed separately. The VCS has one license for the maximum number of concurrent traversal calls it can take, and another for the maximum number of concurrent non-traversal calls. You can increase the number of each type of call available on your VCS (or VCS cluster, see License Usage Within a Cluster, page 159 for more information) by purchasing and installing the appropriate option key. While every deployment is different, as a guideline we recommend that your system has a 10:1 ratio of registrations to concurrent call licenses.

Note that a non-traversal call on a VCS Expressway will consume a traversal license if there are no non-traversal call licenses available (in this situation, the call will remain a non-traversal call – the VCS Expressway will not take the media, even though it is using a traversal license).

License Bypass for Calls to Collaboration Meeting Rooms (CMRs)

The VCS no longer requires traversal call licenses for calls to and from cloud-based CMRs. This includes SIP calls between Collaboration Cloud and the CMR Hybrid solution.

Note: This only applies when the dialed string does not need transformation on the VCS (for example, user@sitename.webex.com).

Although untransformed SIP calls to cloud-based CMRs do not consume licenses, they do consume resources and may not progress if the VCS 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 traversal licenses.

Product Identifiers and Corresponding Keys

Feature or License Option	PID (Product Identifier)	Key Pattern	Valid On	Required For
Release Key	`LIC-SW-VMVCS-K9`	16 digit number	VCS Control VCS Expressway	Enabling the system. The key is unique to a serial number and a particular base version of software. Most features will not work permanently without this key.
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 RMS licenses are not used by CMR Cloud calls
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	Registering TelePresence rooms to Expressway-C.
Desktop system registration licenses	LIC-EXP-DSK	116341Bn-m-#########	Expressway-C	Registering desktop endpoints to Expressway-C.
TURN relay licenses	LIC-EXP-TURN	116341In-m-#########	VCS Expressway Expressway-E	Jabber Guest, Microsoft Interoperability (offsite MS clients)
Traversal Server feature	LIC-EXP-E	116341T00-m-#########	VCS Expressway Expressway-E	Firewall traversal: MRA, B2B, CMR Cloud, CMR Hybrid, Proxy registrations, Jabber Guest, MS interop (offsite MS clients)

Feature or License Option	PID (Product Identifier)	Key Pattern	Valid On	Required For
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.
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 VCS 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 21 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 VCS 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 22 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.
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

VCS Multitenancy Overview

The VCS 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 VCS 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 VCS Expressway cluster and VCS Control 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 VCS Expressway cluster across up to 50 customers while a dedicated VCS Control cluster is deployed per customer.

This dedicated VCS Control 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) VCS Expressway cluster to meet the customer's scale and performance requirements.

Multitenant VCS Restrictions

Multitenant VCS has some restrictions relative to the standard VCS 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 VCS Sizing

In previous VCS releases, VCS Expressway and VCS Control cluster deployments are restricted to matching cluster and OVA sizes. The number of nodes in the VCS Expressway cluster must match the number of nodes in the VCS Control 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 VCS Expressway cluster, and dedicated 2-node medium OVA VCS Control cluster per customer.

For customers who need more capacity than a 2-node medium OVA cluster affords, we recommend deploying a dedicated VCS Expressway 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 VCS section of this chapter discusses the sizing and capacity of VCS clusters.

In a multitenant deployment, the VCS Expressway's capacity is shared across all of the customers, whereas the VCS Control cluster's capacity is dedicated to the customer. The following tables provide the recommended capacity per customer.

Shared VCS Expressway 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 VCS Control 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 VCS Expressway cluster, the maximum average concurrent MRA registrations per customer is 200, well below the VCS Control cluster's capacity.

Likewise, the maximum average concurrent video calls per customer is 40, again below the capacity of the VCS Control cluster. This spare capacity in the VCS Control 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 VCS Expressway. In both of these use cases, the VCS Expressway cluster is the limiting factor; there is plenty of capacity in the VCS Control.

Use Case 1

Most customers are using MPLS for in-office connectivity and only using MRA at home or when mobile. In this case, only a small percentage (10-20%) of users are registered with MRA at any given time. Maximum users per customer should be around 500.

Use Case 2

Most customers are not using MPLS and are using MRA for all connectivity. In this case, 100% of users are registered with MRA. Maximum users per customer must not exceed 200.

The following table summarizes these deployment options.

Deployment scenarios

Use case	Average maximum users per customer	Percentage of users that can register via MRA at once	Notes
1	500	40%	Use this when most customers are using MPLS for in-office connectivity.
2	200	100%	Use this when most customers are using MRA for in-office connectivity.

See *Multitenancy with Cisco Expressway* on the Cisco Hosted Collaboration Solution page.

Alarms

Alarms occur when an event or configuration change has taken place on the VCS 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 VCS, 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 VCS configuration issues
55nnn	B2BUA issues
6nnnn	Hybrid Services alarms
60000-60099	Management Connector alarms
60100-60199	Calendar Connector alarms
60300-60399	Call Connector alarms

All alarms raised on the VCS are also raised as Cisco TMS tickets. All the attributes of an alarm (its ID, severity and so on) are included in the information sent to Cisco TMS.

Alarms Reference

These tables list the alarms that can be raised on the VCS:

- Table 23 Hardware Alarms, page 398
- Table 24 Software Alarms, page 398
- Table 25 Cluster Alarms, page 400
- Table 26 Network Alarms, page 402
- Table 27 License Alarms, page 404
- Table 28 External Applications / Services Alarms, page 407
- Table 29 Security Alarms, page 409
- Table 30 Misconfiguration Alarms, page 414
- Table 31 Back to Back User Agent Alarms, page 416
- Table 32 Management Connector Alarms, page 421

- Table 33 Calendar Connector Alarms, page 424
- Table 34 Call Connector Alarms, page 428

Table 23 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
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

Table 24 Software Alarms

ID	Title	Description	Solution	Severity
15004	Application failed	An unexpected software error was detected in <module>	View the incident reporting page	Error

Table 24 Software Alarms (continued)

ID	Title	Description	Solution	Severity
15005	Database failure	Please remove database and restore from backup, then reboot the system	Reboot the system	Warning
15007	The system is busy	The system is shutting down, or starting		Alert
15008	Failed to load database	The database failed to load; some configuration data has been lost	Restore system data from backup	Warning
15009	Factory reset started	Factory reset started		Alert
15010	Application failed	An unexpected software error was detected in <module>	View the incident reporting page	Error
15011	Application failed	An unexpected software error was detected in <module>	View the incident reporting page	Error
15012	Language pack mismatch	Some text labels may not be translated	Contact your Cisco representative to see if an up-to-date language pack is available	Warning
15013	Factory reset failed	Factory reset failed		Alert
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 VCS is in Maintenance mode and will no longer accept calls and registrations		Warning
15016	Directory service database failure	The directory service database is not running	Restart the system	Warning
15017	Application failed	The OpenDS service has stopped unexpectedly and has been restarted	If the problem persists, contact your Cisco representative	Warning
15018	Boot selection mismatch	Booted system does not match expected configuration; this may be caused by user input or spurious characters on the serial console during the boot	Reboot the system	Critical

Table 24 Software Alarms (continued)

ID	Title	Description	Solution	Severity
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
15024	HSM enrollment failure	A failure was detected while trying to enroll peer to HSM.		Error
15025	HSM disenrollment failure	A failure was detected while trying to disenroll peer from HSM.		Error
15026	Crypto device failure	A failure was detected while trying to change the configured crypto device.		Error
15028	Restart required	Server certificate and private key have been changed, however a restart is required for this to take effect.	Restart the system.	Warning
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

Table 25 Cluster Alarms

ID	Title	Description	Solution	Severity
20020	Restart required	TLS verification configuration does not match active status.	Restart the system.	Warning

Table 25 Cluster Alarms (continued)

ID	Title	Description	Solution	Severity
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
20004	Cluster communication failure	The system is unable to communicate with one or more of the cluster peers	Check the clustering configuration	Warning
20005	Invalid peer address	One or more peer addresses are invalid	Check the Clustering page and ensure that all Peer fields use a valid IP address	Warning
20006	Cluster database communication failure	The database is unable to replicate with one or more of the cluster peers	Check the clustering configuration and restart	Warning
20007	Restart required	Cluster configuration has been changed, however a restart is required for this to take effect	Restart the system	Warning
20008	Cluster replication error	Automatic replication of configuration has been temporarily disabled because an upgrade is in progress	Please wait until the upgrade has completed	Warning
20009	Cluster replication error	There was an error during automatic replication of configuration	View cluster replication instructions	Warning
20010	Cluster replication error	The NTP server is not configured	Configure an NTP server	Warning
20011	Cluster replication error	This peer's configuration conflicts with the primary's configuration, manual synchronization of configuration is required	View cluster replication instructions	Warning
20012	Cluster replication error	This peer's cluster configuration settings do not match the configuration primary peer's settings	Configure this peer's cluster settings	Warning
20014	Cluster replication error	Cannot find primary or this peer's configuration file, manual synchronization of configuration is required	View cluster replication instructions	Warning
20015	Cluster replication error	The local VCS does not appear in the list of peers	Check the list of peers for this cluster	Warning

Table 25 Cluster Alarms (continued)

ID	Title	Description	Solution	Severity
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

Table 26 Network Alarms

ID	Title	Description	Solution	Severity
25001	Restart required	Network configuration has been changed, however a restart is required for this to take effect	Restart the system	Warning
25002	Date and time not validated	The system is unable to obtain the correct time and date from an NTP server	Check the time configuration	Warning
25003	IP configuration mismatch	IP protocol is set to both IPv4 and IPv6, but the system does not have any IPv4 addresses defined	Configure IP settings	Warning
25004	IP configuration mismatch	IP protocol is set to both IPv4 and IPv6, but the system does not have an IPv4 gateway defined	Configure IP settings	Warning
25006	Restart required	Advanced Networking option key has been changed, however a restart is required for this to take effect	Configure your required LAN and static NAT settings on the IP page and then restart the system.	Warning
25007	Restart required	QoS settings have been changed, however a restart is required for this to take effect	Restart the system	Warning
25008	Restart required	Port configuration has been changed, however a restart is required for this to take effect	Restart the system	Warning

Table 26 Network Alarms (continued)

ID	Title	Description	Solution	Severity
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
25014	Configuration warning	IP protocol is set to both IPv4 and IPv6, but the VCS 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

Table 26 Network Alarms (continued)

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 VCS address for XMPP federation	Check that the IM and Presence Service servers are running, and that the AXL service is running on them, then refresh the servers.	Warning
25024	XMPP configuration error	Invalid configuration of XMPP network address	Check that the IPv4 addresses are correct. You may not use 127.0.0.1 (loopback address)	Error
25025	Smart Call Home connection failed	VCS could not send information to Smart Call Home. This could be a transient network condition, a misconfiguration, or a certificate mismatch	Check the Smart Call Home and DNS configuration	Critical
25026	Restart required	Web administration port has been changed, however, a restart is required for this to take effect	Restart the system	Warning
25027	SSLH failure	The protocol multiplexing service cannot start because the configuration file was not written. The VCS Expressway is not able to listen on TCP 443 for TURN and WebRTC requests.	Reconfigure the TURN service	Critical

Table 27 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

Table 27 License Alarms (continued)

ID	Title	Description	Solution	Severity
30002	Capacity warning	The number of concurrent traversal calls has approached the unit's physical limit	Contact your Cisco representative	Warning
30003	Capacity warning	The number of concurrent non-traversal calls has approached the unit's physical limit	Contact your Cisco representative	Warning
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
30006	Restart required	The release key has been changed, however a restart is required for this to take effect	Restart the system	Warning
30007	Capacity warning	TURN relays usage has approached the licensed limit	Contact your Cisco representative	Warning
30008	Invalid release key	The release key is not valid; if you do not have a valid key, contact your Cisco support representative	Add/Remove option keys	Warning
30009	TURN relays installed	TURN services are only available on VCS Expressway; TURN option key ignored	Add/Remove option 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 key or disable TURN services	Warning
30012	License usage of lost cluster peer	Cluster peer <n> has been unavailable for more than <n> hours. Its licenses will be removed from the total available for use across the cluster on <date>.	Resolve the issue with this peer, or remove it from the cluster configuration	Warning
30013	License usage of lost cluster peer	Several cluster peers have been unavailable for more than <n> hours. Their licenses will be removed from the total available for use across the cluster as follows: <details>.	Resolve the issue with this peer, or remove it from the cluster configuration	Warning
30014	License usage of lost cluster peer	Cluster peer <n> has been unavailable for more than <n> days. Its licenses will be removed from the total available for use across the cluster on <date>.	Resolve the issue with this peer, or remove it from the cluster configuration	Warning

Table 27 License Alarms (continued)

ID	Title	Description	Solution	Severity
30015	License usage of lost cluster peer	Several cluster peers have been unavailable for more than <n> days. Their licenses will be removed from the total available for use across the cluster as follows: <details>.	Resolve the issue with this peer, or remove it from the cluster configuration	Warning
30016	Licenses of lost cluster peer have been taken off the license pool	Cluster peer <n> has been unavailable for more than <n> days. Its licenses have been removed from the total available for use across the cluster on <date>.	Resolve the issue with this peer, or remove it from the cluster configuration	Warning
30017	Licenses of lost cluster peer have been taken off the license pool	Several cluster peers have been unavailable for more than <n> days. Their licenses have been removed from the total available for use across the cluster as follows: <details>.	Resolve the issue with this peer, or remove it from the cluster configuration	Warning
30018	Provisioning licenses limit reached	The number of concurrently provisioned devices has reached the licensed limit	Provisioning limits are set by Cisco TMS; contact your Cisco representative if you require more licenses	Warning
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	Ensure that your registrations are distributed evenly across all peers	Warning
30023	Call capacity limit reached	The number of concurrent traversal calls has reached the unit's physical limit	Ensure that your registrations are distributed evenly across all peers	Warning

Table 27 License Alarms (continued)

ID	Title	Description	Solution	Severity
30024	TURN relay capacity limit reached	The number of concurrent TURN relay calls has reached the unit's physical limit	Ensure that your registrations are distributed evenly across all peers	Warning
30025	Restart required	An option key or the type has been changed, however a restart is required for this to take effect	Restart the system	Warning

Table 28 External Applications / Services Alarms

ID	Title	Description	Solution	Severity
35001	Configuration warning	Active Directory mode has been enabled but the DNS hostname has not been configured	Configure DNS hostname	Warning
35002	Configuration warning	Active Directory mode has been enabled but the NTP server has not been configured	Configure NTP server	Warning
35003	Configuration warning	Active Directory mode has been enabled but no DNS servers have been configured	Configure a DNS server	Warning
35004	LDAP configuration required	Remote login authentication is in use for administrator or FindMe accounts but a valid LDAP Server address, Port, Bind_DN and Base_DN have not been configured	Configure LDAP parameters	Warning
35005	Configuration warning	Active Directory mode has been enabled but a domain has not been configured	Configure domain on Active Directory Service page	Warning
35007	Configuration warning	Active Directory SPNEGO disabled; you are recommended to enable the SPNEGO setting	Enable SPNEGO	Warning
35008	Configuration warning	Active Directory mode has been enabled but a workgroup has not been configured	Configure workgroup on Active Directory Service page	Warning
35009	TMS Provisioning Extension services communication failure	The VCS 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

Table 28 External Applications / Services Alarms (continued)

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 VCS to exceed internal table limits	See the VCS Event Log for details, then check the corresponding data within TMS; you must perform a full synchronization after the data has been corrected in TMS	Warning
35011	TMS Provisioning Extension services data import failure	One or more records imported from the TMS Provisioning Extension services have been dropped due to unrecognized data format	See the VCS Event Log for details, then check the corresponding data within TMS; you must perform a full synchronization after the data has been corrected in TMS	Warning
35012	Failed to connect to LDAP server	Failed to connect to the LDAP server for H.350 device authentication	Ensure that your H.350 directory service is correctly configured	Warning
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 VCS Control and the VCS Expressway 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 VCS Control ephemeral ports to 2222 TCP on the VCS Expressway	Warning
35015	Unified CM port conflict	There is a port conflict on Unified CM <name> between neighbor zone <name> and Unified Communications (both are using port <number>)	The same port on Unified CM cannot be used for line side (Unified Communications) and SIP trunk traffic. Review the port configuration on Unified CM and reconfigure the <zone> if necessary	Warning
35016	SAML metadata has been modified	Configuration changes have modified the local SAML metadata, which is now different to any copies on Identity Provider(s). This metadata may have been modified by changing the server certificate or the SSO-enabled domains, or by changing the number of traversal server peers or their addresses	Export the SAML metadata so you can import it on the Identity Provider	Warning

Table 29 Security Alarms

ID	Title	Description	Solution	Severity
40001	Security alert	No CRL distribution points have been defined for automatic updates	Check CRL configuration	Warning
40002	Security alert	Automatic updating of CRL files has failed	If the problem persists, contact your Cisco representative	Warning
40003	Insecure password in use	The root user has the default password set	View instructions on changing the root password	Warning
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 client certificate-based security	Warning
40005	Insecure password in use	The admin user has the default password set	Change the admin password	Error
40006	Security alert	Unable to download CRL update	Check CRL distribution points and the Event Log	Warning
40007	Security alert	Failed to find configuration file for CRL automatic updates	If the problem persists, contact your Cisco representative	Warning
40008	Security alert	The SSH service is using the default key	View instructions on replacing the default SSH key	Warning
40009	Restart required	HTTPS client certificates validation mode has changed, however a restart is required for this to take effect	Restart the system	Warning
40011	Per-account session limit required	A non-zero per-account session limit is required when in advanced account security mode	Configure per-account session limit	Warning
40012	External manager connection is using HTTP	You are recommended to use HTTPS connections to the external manger when in advanced account security mode	Configure external manager	Warning

Table 29 Security Alarms (continued)

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 HTTPS client certificate validation	Warning
40014	Time out period required	A non-zero system session time out period is required when in advanced account security mode	Configure session time out period	Warning
40015	System session limit required	A non-zero system session limit is required when in advanced account security mode	Configure system session limit	Warning
40016	Encryption required	Your login account LDAP server configuration is recommended to have encryption set to *TLS* when in advanced account security mode	Configure login account LDAP server	Warning
40017	Incident reporting enabled	You are recommended to disable incident reporting when in advanced account security mode	Configure incident reporting	Warning
40018	Insecure password in use	One or more users has a non-strict password		Warning
40019	External manager has certificate checking disabled	You are recommended to enable external manager certificate checking when in advanced account security mode	Configure external manager	Warning
40020	Security alert	The connection to the Active Directory Service is not using TLS encryption	Configure Active Directory Service connection settings	Warning
40021	Remote logging enabled	You are recommended to disable the remote syslog server when in advanced account security mode	Configure remote logging	Warning

Table 29 Security Alarms (continued)

ID	Title	Description	Solution	Severity
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 login account LDAP server	Warning
40025	SNMP enabled	You are recommended to disable SNMP when in advanced account security mode	Configure SNMP mode	Warning
40026	Reboot required	The advanced account security mode has changed, however a reboot is required for this to take effect	Reboot the VCS	Warning
40027	Security alert	The connection to the TMS Provisioning Extension services is not using TLS encryption	Configure TMS Provisioning Extension services connection settings	Warning
40028	Insecure password in use	The root user's password is hashed using MD5, which is not secure enough	View instructions on changing the root password	Warning
40029	LDAP server CA certificate is missing	A valid CA certificate for the LDAP database has not been uploaded; this is required for connections via TLS	Upload a valid CA certificate	Warning
40030	Security alert	Firewall rules activation failed; the firewall configuration contains at least one rejected rule	Check your firewall rules configuration, fix any rejected rules and re-try the activation	Warning
40031	Security alert	Unable to restore previous firewall configuration	Check your firewall rules configuration, fix any rejected rules, activate and accept the rules; if the problem persists, contact your Cisco representative	Warning

Table 29 Security Alarms (continued)

ID	Title	Description	Solution	Severity
40032	Security alert	Unable to initialize firewall	Restart the system; if the problem persists, contact your Cisco representative	Warning
40033	Configuration warning	The Default Zone access rules are enabled, but leaving SIP over UDP or SIP over TCP enabled offers a way to circumvent this security feature	Either disable UDP and TCP on the SIP page to enforce certificate identity checking using TLS, or disable the access rules for the Default Zone.	Warning
40034	Security alert	Firewall rules activation failed; the firewall configuration contains rules with duplicated priorities	Check your firewall rules configuration, ensure all rules have a unique priority and re-try the activation	Warning
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
40041	Security alert	Automated intrusion protection rules are not available	Disable and then re-enable the failed services	Warning

Table 29 Security Alarms (continued)

ID	Title	Description	Solution	Severity
40042	FIPS140-2 compliance restriction	Some SIP configuration is not using TLS transport; FIPS140-2 compliance requires TLS	Ensure that TLS is the only enabled system-wide SIP transport mode on the SIP page, and that all zones are using TLS. Alternatively, if you are transitioning into FIPS140-2 you may want to restore a FIPS-compliant backup of your data.	Warning
40043	Unified Communications configuration error	Media encryption is not enforced on a traversal zone configured for Unified Communications services	Ensure that media encryption is set to 'Force encrypted' on the traversal zone	Warning
40044	System reset required	FIPS140-2 mode has been enabled; a system reset is required to complete this process	Ensure that all alarms are cleared, then take a system backup before performing a system reset	Warning
40045	Restart required	FIPS140-2 mode has been disabled; a system restart is required to complete this process	Restart the system	Warning
40046	FIPS140-2 compliance restriction	Clustered systems are not FIPS140-2 compliant	Disband the cluster	Warning
40048	Unified Communications configuration error	Unified Communications services are enabled but SIP TLS is disabled	Ensure that SIP TLS mode is set to 'On' on SIP configuration page	Warning
40049	Cluster TLS permissive	Cluster TLS verification mode permits invalid certificates	Change the cluster's TLS verification mode to Enforcing	Notice
40050	Security alert	Unable to install new firewall configuration	Check your firewall configuration and rate limits configuration, fix any rejected rules; Do not restart your system; if the problem persists, contact your Cisco representative	
40051	CMS not Identified by Server Certificate	CMS address *<address>* has been entered on the VCS Control but is not identified by the VCS Expressway server certificate	Check that the CMS address on the VCS Control matches the SAN entry on the VCS Expressway server. You may need to generate a CSR for a new server certificate that includes the CMS as a SAN, or edit (or remove) the CMS on the VCS Control	
40052	Certificate error	Server certificate does not have a Common Name (CN) attribute. Some services do not work without the CN	Update certificate	

Table 29 Security Alarms (continued)

ID	Title	Description	Solution	Severity
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 ciphers	
40054	Token decryption failure	The VCS Control 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
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

Table 30 Misconfiguration Alarms

ID	Title	Description	Solution	Severity
45001	Failed to load Call Policy file	<failure details>	Configure Call Policy	Warning
45002	Configuration warning	Expected default link between the Default Subzone and the Default Zone is missing	Configure default links	Warning
45003	Configuration warning	H.323 and SIP modes are set to Off; one or both of them should be enabled	Configure H.323 and/or SIP modes	Warning

Table 30 Misconfiguration Alarms (continued)

ID	Title	Description	Solution	Severity
45004	Configuration conflict	The FindMe mode is set to *On* or *Remote service* but the FindMe option key has been deleted	Reconfigure FindMe mode or reinstall the option key	Warning
45005	Configuration conflict	H323-SIP Protocol Interworking mode is set to "On" but the H323-SIP Interworking Gateway option key has been deleted	Reconfigure Interworking mode or reinstall the option key	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
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
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

Table 30 Misconfiguration Alarms (continued)

ID	Title	Description	Solution	Severity
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

Table 31 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 VCS communications is misconfigured	Check B2BUA configuration (advanced settings)	Warning
55003	B2BUA misconfiguration	Invalid trusted host IP address of Microsoft device	Check configured addresses of trusted hosts	Warning
55004	B2BUA misconfiguration	The port on B2BUA for Microsoft call communications is misconfigured	Check B2BUA configuration (advanced settings)	Warning
55005	B2BUA misconfiguration	The Microsoft destination address is misconfigured	Check B2BUA configuration	Warning
55005	B2BUA misconfiguration	The Microsoft destination address is misconfigured	Check B2BUA configuration	Warning
55006	B2BUA misconfiguration	The Microsoft destination port is misconfigured	Check B2BUA configuration	Warning
55007	B2BUA misconfiguration	The Microsoft transport type is misconfigured	Check B2BUA configuration	Warning
55008	B2BUA misconfiguration	Missing or invalid FQDN of service	Check the VCS's system host name and domain name	Warning
55009	B2BUA misconfiguration	Invalid IP address of service	Check the VCS's LAN 1 IPv4 address	Warning

Table 31 Back to Back User Agent Alarms (continued)

ID	Title	Description	Solution	Severity
55010	B2BUA misconfiguration	The B2BUA media port range end value is misconfigured	Check B2BUA configuration (advanced settings)	Warning
55011	B2BUA misconfiguration	The B2BUA media port range start value is misconfigured	Check B2BUA configuration (advanced settings)	Warning
55012	B2BUA misconfiguration	Invalid Microsoft interoperability mode	Check B2BUA configuration	Warning
55013	B2BUA misconfiguration	Invalid option key	Check option keys	Warning
55014	B2BUA misconfiguration	Invalid hop count	Check B2BUA configuration (advanced settings)	Warning
55015	B2BUA misconfiguration	Invalid trusted host IP address of transcoder	Check configured addresses of trusted hosts	Warning
55016	B2BUA misconfiguration	The setting to enable transcoders for this B2BUA is misconfigured	Check B2BUA configuration (transcoder settings)	Warning
55017	B2BUA misconfiguration	The port on B2BUA for transcoder communications is misconfigured	Check B2BUA configuration (transcoder settings)	Warning
55018	B2BUA misconfiguration	Transcoder address and/or port details are misconfigured	Check B2BUA configuration (transcoder settings) and the configured addresses of trusted hosts	Warning
55019	B2BUA misconfiguration	Invalid TURN server address	Check B2BUA configuration (TURN settings)	Warning
55021	B2BUA misconfiguration	The setting to offer TURN services for this B2BUA is misconfigured	Check B2BUA configuration (TURN settings)	Warning
55023	B2BUA misconfiguration	The transcoder policy rules are misconfigured	Check transcoder policy rules configuration	Warning
55024	B2BUA misconfiguration	The setting to use transcoder policy rules is misconfigured	Check B2BUA configuration (transcoder settings)	Warning
55025	B2BUA misconfiguration	The B2BUA has been enabled to use transcoders, but there are no transcoders configured	Configure one or more transcoders	Warning
55026	B2BUA misconfiguration	TURN services are enabled, but there are no valid TURN servers configured	Configure the TURN server address	Warning
55028	B2BUA misconfiguration	The start and end media port ranges are misconfigured	Check the B2BUA media port range settings	Warning

Table 31 Back to Back User Agent Alarms (continued)

ID	Title	Description	Solution	Severity
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 VCS communications is also used by <module>	Check the port configuration for both services	Warning
55031	B2BUA misconfiguration	The port used by the B2BUA for Microsoft call communications is also used by <module>	Check the port configuration for both services	Warning
55032	B2BUA misconfiguration	The port used by the B2BUA for transcoder communications is also used by <module>	Check the port configuration for both services	Warning
55033	B2BUA misconfiguration	No valid Microsoft trusted hosts have been configured	Configure at least one trusted host device	Warning
55034	B2BUA misconfiguration	No valid transcoder trusted hosts have been configured	Configure at least one transcoder trusted host	Warning
55035	B2BUA connectivity problem	The B2BUA cannot connect to the transcoders	Restart the B2BUA service	Warning
55036	B2BUA connectivity problem	The B2BUA cannot connect to the VCS	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 VCS authorized host IP address	Restart the service; contact your Cisco representative if the problem persists	Warning
55102	B2BUA misconfiguration	Invalid URI format of VCS contact address	Restart the service; contact your Cisco representative if the problem persists	Warning
55103	B2BUA misconfiguration	Invalid VCS encryption mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55104	B2BUA misconfiguration	Invalid VCS ICE mode	Restart the service; contact your Cisco representative if the problem persists	Warning

Table 31 Back to Back User Agent Alarms (continued)

ID	Title	Description	Solution	Severity
55105	B2BUA misconfiguration	Invalid VCS next hop host configuration	Restart the service; contact your Cisco representative if the problem persists	Warning
55106	B2BUA misconfiguration	Invalid VCS next hop liveness mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55107	B2BUA misconfiguration	Invalid VCS next hop mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55108	B2BUA misconfiguration	Invalid VCS next hop port	Restart the service; contact your Cisco representative if the problem persists	Warning
55109	B2BUA misconfiguration	Invalid VCS transport type	Restart the service; contact your Cisco representative if the problem persists	Warning
55110	B2BUA misconfiguration	Invalid URI format of B side contact address	Restart the service; contact your Cisco representative if the problem persists	Warning
55111	B2BUA misconfiguration	Invalid B side encryption mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55112	B2BUA misconfiguration	Invalid B side ICE mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55113	B2BUA misconfiguration	Invalid B side next hop liveness mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55114	B2BUA misconfiguration	Invalid B side next hop mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55115	B2BUA misconfiguration	Invalid command listening port	Restart the service; contact your Cisco representative if the problem persists	Warning
55116	B2BUA misconfiguration	Invalid debug status path	Restart the service; contact your Cisco representative if the problem persists	Warning
55117	B2BUA misconfiguration	Invalid service	Restart the service; contact your Cisco representative if the problem persists	Warning
55118	B2BUA misconfiguration	Invalid software string	Restart the service; contact your Cisco representative if the problem persists	Warning

Table 31 Back to Back User Agent Alarms (continued)

ID	Title	Description	Solution	Severity
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
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 VCS next hop host configuration	Restart the service; contact your Cisco representative if the problem persists	Warning
55126	B2BUA misconfiguration	Invalid VCS 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

Table 31 Back to Back User Agent Alarms (continued)

ID	Title	Description	Solution	Severity
55132	B2BUA misconfiguration	Invalid call resource limit	Restart the service; contact your Cisco representative if the problem persists	Warning
55133	B2BUA misconfiguration	The B2BUA session refresh interval is smaller than the minimum session refresh interval	Check both settings on the B2BUA configuration (advanced settings) and then restart the B2BUA service	Warning
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 32 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

Table 32 Management Connector Alarms (continued)

ID	Title	Description	Solution	Severity
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
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

Table 32 Management Connector Alarms (continued)

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
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

Table 32 Management Connector Alarms (continued)

ID	Title	Description	Solution	Severity
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
60072	[Hybrid services] Unsupported Expressway version	Your version of Expressway is no longer supported for Hybrid Services. To continue using Hybrid Services, you must upgrade to a newer version.	Please upgrade to the latest Expressway version, available on cisco.com.	alert

Table 33 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

Table 33 Calendar Connector Alarms (continued)

ID	Title	Description	Solution	Severity
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
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

Table 33 Calendar Connector Alarms (continued)

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
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

Table 33 Calendar Connector Alarms (continued)

ID	Title	Description	Solution	Severity
60150	Cisco Collaboration Cloud Monitor Service unreachable	A required cloud service currently cannot be reached. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: *<string>*	Verify connectivity to Internet	critical
60151	Cisco Collaboration Cloud Monitor Service access denied	Access to Cisco Collaboration Cloud services was denied. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: *<string>*	Contact tech support	critical
60152	Cisco Collaboration Cloud API Service unreachable	A required cloud service currently cannot be reached. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: *<string>*	Verify connectivity to Internet	critical
60153	Cisco Collaboration Cloud API Service access denied	Access to Cisco Collaboration Cloud services was denied. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: *<string>*	Contact tech support	critical
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
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

Table 33 Calendar Connector Alarms (continued)

ID	Title	Description	Solution	Severity
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
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
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 34 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

Table 34 Call Connector Alarms (continued)

ID	Title	Description	Solution	Severity
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
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
60310	Unable to add the user's Webex Teams 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

Table 34 Call Connector Alarms (continued)

ID	Title	Description	Solution	Severity
60315	Automatic Spark Remote Device created with truncated name	The Automatic Spark Remote Device name was shortened during Call Service Connect activation. - user[*<string>*]: *<string>* has device with name *<string>*	To avoid this issue, user IDs must not exceed 15 characters.	warning
60316	Unable to delete Spark Remote Device	Call connector cannot delete the Spark remote device after Call Service Connect was deactivated - user[*<string>*]: *<string>*	Check error messages in Unified CM.	warning
60317	Call connector is unable to create a CTI Remote Device in Unified CM.	Call connector is unable to create a CTI Remote Device in Unified CM - user[*<string>*]: *<string>*	Check for any potentially conflicting device names.	warning
60318	Users must have mobility enabled for call connector to create a CTI remote device.	Users must have mobility enabled for call connector to create a Remote Device for Webex Teams - 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
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

Table 34 Call Connector Alarms (continued)

ID	Title	Description	Solution	Severity
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
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

Table 34 Call Connector Alarms (continued)

ID	Title	Description	Solution	Severity
60336	A device exists with the same name as the CTI remote device tried to create for the user.	A device exists with the same name as the CTI remote device tried to create - for user [*<string>*]: *<string>*	Check the device names and configuration in Unified CM.	warning
60337	CTI remote device successfully created for the user, but the device subscription to receive call events failed.	CTI remote device successfully created for the user, but the device subscription to receive call events failed - for user [*<string>*]: *<string>*	Check the configuration in Unified CM and retry.	warning
60338	Invalid remote destination on Unified CM.	Invalid remote destination on Unified CM - for user[*<string>*]: *<string>*	Follow the user and remote device configuration in the documentation to create a valid 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
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

Table 34 Call Connector Alarms (continued)

ID	Title	Description	Solution	Severity
60347	Authorization Failure with Cisco Collaboration Cloud Services.	Invalid role or access scope for this Expressway to access Cisco Collaboration Cloud Services.	Go to the Expressway, and then reregister it to the cloud under Applications > Hybrid Services > Connector Management.	error
60348	Connection from the Cisco Collaboration Cloud is down.	Connection from the Cisco Collaboration Cloud is down.	Check your network DNS or proxy settings and then try again.	error
60349	Connection to the Cisco Collaboration Cloud is down.	Connection to the Cisco Collaboration Cloud is down.	Check your network DNS or proxy settings and then try again.	error
60350	Cannot enable hybrid voicemail for your organization.	Cannot enable hybrid voicemail for your organization.	If this error persists, work with your trials team or contact support by submitting feedback through the Cisco Spark app.	warning
60351	Call connector detected an invalid hybrid voicemail configuration.	Call connector detected an invalid hybrid voicemail configuration.	Check the Hybrid Voicemail deployment steps. If this error persists, work with your trials team or contact support by submitting feedback through the Cisco Spark app.	error
60352	No Directory Number exists in UCM with this directory URI	No Directory Number exists in UCM with this directory URI	Configure a Directory Number in UCM with this directory URI	error
60353	AXL Change Notification is not started at Unified CM.	AXL Change Notification is not started at Unified CM – server [*<string>*]	Enable AXL Change Notification in Enterprise Parameters of Unified CM.	error

Command Reference – xConfiguration

The `xConfiguration` group of commands are used to set and change individual items of configuration. Each command is made up of a main element followed by one or more sub-elements.

To obtain information about existing configuration, type:

- `xConfiguration` to return all current configuration settings
- `xConfiguration <element>` to return configuration for that element and all its sub-elements
- `xConfiguration <element> <subelement>` to return configuration for that sub-element

To obtain information about using each of the `xConfiguration` commands, type:

- `xConfiguration ?` to return a list of all elements available under the `xConfiguration` command
- `xConfiguration ??` to return a list of all elements available under the `xConfiguration` command, along with the valuespace, description and default values for each element
- `xConfiguration <element> ?` to return all available sub-elements and their valuespace, description and default values
- `xConfiguration <element> <sub-element> ?` to return all available sub-elements and their valuespace, description and default values

To set a configuration item, type the command as shown. The valid values for each command are indicated in the angle brackets following each command, using the following notation:

Table 35 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 36 xConfiguration CLI reference

Administration DeviceProvisioning: <On/Off> Determines whether the **System > TMS Provisioning Extension services** page is accessible in the VCS 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 VCS. *Off*: the **System > TMS Provisioning Extension services** page is not accessible. Example: `xConfiguration Administration DeviceProvisioning: On`
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`
Administration HTTPS Mode: <On/Off> Determines whether the VCS 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`
Administration LCDPanel Mode: <On/Off> Controls whether the LCD panel on the front of the VCS 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`
Administration SSH Mode: <On/Off> Determines whether the VCS 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`
Alternates Cluster Name: <S: 0,128> The fully qualified domain name used in SRV records that address this VCS 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 VCS, you may need to reconfigure your user accounts to use the new cluster name. Example: `xConfiguration Alternates Cluster Name: "Regional"`

Table 36 xConfiguration CLI reference (continued)

Alternates ConfigurationMaster: <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 VCS. Example: `xConfiguration Alternates ConfigurationMaster: 1`
Alternates Peer [1..6] Address: <S: 0, 128> Specifies the address of one of the peers in the cluster to which this VCS belongs. A cluster consists of up to 6 peers, including the local VCS. We recommend using FQDNs, but these can be IP addresses. Example: `xConfiguration Alternates 1 Peer Address: "cluster1peer3.example.com"`
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`
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`
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`
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`
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"`
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`

Table 36 xConfiguration CLI reference (continued)

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`
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`
Applications ConferenceFactory Template: <S:0,60> The alias that the VCS 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: `Applications ConferenceFactory Template: "563%%@example.com"`
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"`
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"`
Applications Presence Server Mode: <On/Off> Enables and disables the SIMPLE Presence Server. SIP must also be enabled for the Presence Server to function. Default: Off. Example: `xConfiguration Applications Presence Server Mode: On`
Applications Presence Server Publication ExpireDelta: <30..7200> Specifies the maximum time (in seconds) within which a publisher must refresh its publication. Default: 1800 Example: `xConfiguration Applications Presence Server Publication ExpireDelta: 1800`
Applications Presence Server Subscription ExpireDelta: <30..7200> Specifies the maximum time (in seconds) within which a subscriber must refresh its subscription. Default: 3600. Example: `xConfiguration Applications Presence Server Subscription ExpireDelta: 3600`
Applications Presence User Agent ExpireDelta: <1..65534> Specifies the lifetime value (in seconds) the Presence User Agent will advertise in the PUBLISH messages it sends to the Presence Server. The Presence User Agent will refresh its PUBLISH messages at 75% of this value (to keep them active). The Presence Server may reduce this value in its responses. Default: 3600 Example: `xConfiguration Applications Presence User Agent ExpireDelta: 3600`

Table 36 xConfiguration CLI reference (continued)

Applications Presence User Agent Mode: <On/Off> Enables and disables the SIMPLE Presence User Agent (PUA). The PUA provides presence information on behalf of registered endpoints. SIP mode must also be enabled for the PUA to function. Default: Off. Example: `xConfiguration Applications Presence User Agent Mode: Off`
Applications Presence User Agent Presentity Idle Status: <Offline/Online> Default presentity status published by the Presence User Agent. Default: Online. *Online*: publish registered endpoints as online. *Offline*: publish registered endpoints as offline. Example: `xConfiguration Applications Presence User Agent Presentity Idle Status: Online`
Applications Presence User Agent RetryDelta: <1..65534> Specifies the time (in seconds) after which the Presence User Agent will attempt to resend a PUBLISH to the Presence Server. This will occur if the original attempt failed due to resource issues or other transitory errors. Default: 1800. Example: `xConfiguration Applications Presence User Agent RetryDelta: 1800`
Authentication ADS ADDomain: <S: 0,255> The Kerberos realm used when the VCS joins the AD domain. Note: this field is case sensitive. Example: `xConfiguration Authentication ADS ADDomain: "CORPORATION.INT"`
Authentication ADS Clockskew: <1..65535> Maximum allowed clockskew between the VCS and the KDC before the Kerberos message is assumed to be invalid (in seconds). Default: 300. Example: `xConfiguration Authentication ADS Clockskew: 300`
Authentication ADS CipherSuite: <S:1,2048> Specifies the cipher suite to use when the VCS 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"`
Authentication ADS DC [1..5] Address: <S: 0,39> The address of a domain controller that can be used when the VCS 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"`

Table 36 xConfiguration CLI reference (continued)

Authentication ADS Encryption: <Off/TLS> Sets the encryption to use for the LDAP connection to the ADS server. Default: TLS. *Off*: no encryption is used. *TLS*: TLS encryption is used. Example: `xConfiguration Authentication ADS Encryption: TLS`
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"`
Authentication ADS KDC [1..5] Port: <1..65534> Specifies the port of a KDC that can be used when the VCS joins the AD domain. Default: 88. Example: `xConfiguration Authentication ADS KDC 1 Port: 88`
Authentication ADS MachineName: <S: 0..15> This overides the default NETBIOS machine name used when the VCS joins the AD domain. Example: `xConfiguration Authentication ADS MachineName: "short_name"`
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`
Authentication ADS Mode: <On/Off> Indicates if the VCS should attempt to form a relationship with the AD. Default: Off. Example: `xConfiguration Authentication ADS Mode: On`
Authentication ADS SPNEGO: <Enabled/Disabled> Indicates if SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism) is used when the client (the VCS) authenticates with the server (the AD domain controller). Default: Enabled. Example: `xConfiguration Authentication ADS SPNEGO: Enabled`
Authentication ADS SecureChannel: <Auto/Enabled/Disabled> Indicates if data transmitted from the VCS to an AD domain controller is sent over a secure channel. Default: Auto. Example: `xConfiguration Authentication ADS SecureChannel: Auto`
Authentication ADS Workgroup: <S: 0,15> The workgroup used when the VCS joins the AD domain. Example: `xConfiguration Authentication ADS Workgroup: "corporation"`

Table 36 xConfiguration CLI reference (continued)

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`
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`
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`
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"`
Authentication Account Admin Account [1..n] Password: <Password> The password that this administrator will use to log in to the VCS. Example: `xConfiguration Authentication Account Admin Account 1 Password: "abcXYZ_123"`
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`
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`
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`
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"`

Table 36 xConfiguration CLI reference (continued)

Authentication Certificate Crlcheck: <None/Peer/All> Specifies whether HTTPS client certificates are checked against certificate revocation lists (CRLs). CRL data is uploaded to the VCS 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`
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`
Authentication Certificate Mode: <NotRequired/Validation/Authentication> Controls the level of security required to allow client systems (typically web browsers) to communicate with the VCS 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`
Authentication Certificate UsernameRegex: <String> The regular expression to apply to the client certificate presented to the VCS. 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"`
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#"`
Authentication H350 BindPassword: <S: 0, 60> Sets the password to use when binding to the LDAP server. Example: `xConfiguration Authentication H350 BindPassword: "abcXYZ_123"`

Table 36 xConfiguration CLI reference (continued)

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`
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"`
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"`
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"`
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`
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"`
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`
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`

Table 36 xConfiguration CLI reference (continued)

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`
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`
Authentication Password: <S: 0, 215> The password used by the VCS 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"`
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`
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`
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`
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`
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`

Table 36 xConfiguration CLI reference (continued)

Authentication StrictPassword MaximumConsecutiveRepeated: <0..255> The maximum number of times the same character can be repeated consecutively. A value of 0 disables this check. Default: 0 Example: `xConfiguration Authentication StrictPassword MaximumConsecutiveRepeated: 0`
Authentication StrictPassword MinimumClasses: <0..4> The minimum number of character classes that must be present. There are four character classes: digit, upper case, lower case and special. Use this setting if you want to mandate the use of 2–3 different character classes without requiring all of them to be present. A value of 0 disables this check. Default: 0. Example: `xConfiguration Authentication StrictPassword MinimumClasses: 0`
Authentication StrictPassword MinimumDigits: <0..255> The minimum number of digits that must be present. A value of 0 disables this check. Default: 2. Example: `xConfiguration Authentication StrictPassword MinimumDigits: 2`
Authentication StrictPassword MinimumLength: <6..255> The minimum length of the password. Default: 15. Example: *xConfiguration Authentication StrictPassword MinimumLength: 15*
Authentication StrictPassword MinimumLowerCase: <0..255> The minimum number of lower case characters that must be present. A value of 0 disables this check. Default: 2. Example: `xConfiguration Authentication StrictPassword MinimumLowerCase: 2`
Authentication StrictPassword MinimumOther: <0..255> The minimum number of special characters that must be present. A special character is anything that is not a letter or a digit. A value of 0 disables this check. Default: 2 Example: `xConfiguration Authentication StrictPassword MinimumOther: 2`
Authentication StrictPassword MinimumUpperCase: <0..255> The minimum number of upper case characters that must be present. A value of 0 disables this check. Default : 2 Example: *xConfiguration Authentication StrictPassword MinimumUpperCase: 2*
Authentication UserName: <S: 0, 128> The username used by the VCS when authenticating with another system. Note: this does not apply to traversal client zones. Example: `xConfiguration Authentication UserName: "user123"`
Bandwidth Default: <64..65535> The bandwidth (in kbps) to use on calls managed by the VCS where no bandwidth has been specified by the endpoint. Default: 384. Example: `xConfiguration Bandwidth Default: 384`

Table 36 xConfiguration CLI reference (continued)

Bandwidth Downspeed PerCall Mode: <On/Off> Determines whether the VCS attempts to downspeed a call if there is insufficient per-call bandwidth available to fulfill the request. Default: On. *On*: the VCS will attempt to place the call at a lower bandwidth. *Off*: the call will be rejected. Example: `xConfiguration Bandwidth Downspeed PerCall Mode: On`
Bandwidth Downspeed Total Mode: <On/Off> Determines whether the VCS attempts to downspeed a call if there is insufficient total bandwidth available to fulfill the request. Default: On. *On*: the VCS will attempt to place the call at a lower bandwidth. *Off*: the call will be rejected. Example: `xConfiguration Bandwidth Downspeed Total Mode: On`
Bandwidth Link [1..3000] Name: <S: 1, 50> Assigns a name to this link. Example: `xConfiguration Bandwidth Link 1 Name: "HQ to BranchOffice"`
Bandwidth Link [1..3000] Node1 Name: <S: 0, 50> Specifies the first zone or subzone to which this link will be applied. Example: `xConfiguration Bandwidth Link 1 Node1 Name: "HQ"`
Bandwidth Link [1..3000] Node2 Name: <S: 0, 50> Specifies the second zone or subzone to which this link will be applied. Example: `xConfiguration Bandwidth Link 1 Node2 Name: "BranchOffice"`
Bandwidth Link [1..3000] Pipe1 Name: <S: 0, 50> Specifies the first pipe to be associated with this link. Example: `xConfiguration Bandwidth Link 1 Pipe1 Name: "512Kb ASDL"`
Bandwidth Link [1..3000] Pipe2 Name: <S: 0, 50> Specifies the second pipe to be associated with this link. Example: `xConfiguration Bandwidth Link 1 Pipe2 Name: "2Gb Broadband"`
Bandwidth Pipe [1..1000] Bandwidth PerCall Limit: <1..100000000> If this pipe has limited per-call bandwidth, sets the maximum amount of bandwidth (in kbps) available for any one call. Default: 1920. Example: `xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Limit: 256`

Table 36 xConfiguration CLI reference (continued)

Bandwidth Pipe [1..1000] Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth> Determines whether or not this pipe is limiting the bandwidth of individual calls. Default: Unlimited. *NoBandwidth*: no bandwidth available. No calls can be made on this pipe. Example: `xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Mode: Limited`
Bandwidth Pipe [1..1000] Bandwidth Total Limit: <1..100000000> If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe. Default: 500000. Example: `xConfiguration Bandwidth Pipe 1 Bandwidth Total Limit: 1024`
Bandwidth Pipe [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth> Determines whether or not this pipe is enforcing total bandwidth restrictions. Default: Unlimited. *NoBandwidth*: no bandwidth available. No calls can be made on this pipe. Example: `xConfiguration Bandwidth Pipe 1 Bandwidth Total Mode: Limited`
Bandwidth Pipe [1..1000] Name: <S: 1, 50> Assigns a name to this pipe. Example: `xConfiguration Bandwidth Pipe 1 Name: "512Kb ASDL"`
Call Loop Detection Mode: <On/Off> Specifies whether the VCS will check for call loops. Default: On. Example: `xConfiguration Call Loop Detection Mode: On`
Call Routed Mode: <Always/Optimal> Specifies whether the VCS routes the signaling for calls. Default: Always. *Always*: the VCS will always route the call signaling. *Optimal*: if possible, the VCS will remove itself from the call signaling path, which may mean the call does not consume a call license. Example: `xConfiguration Call Routed Mode: Always`
Call Services CallsToUnknownIPAddresses: <Off/Direct/Indirect> The way in which the VCS 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 VCS 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 VCS will query its neighbors for the remote address and if permitted will route the call through the neighbor. *Off*: endpoints registered directly to the VCS may only call an IP address of a system also registered directly to that VCS. Example: `xConfiguration Call Services CallsToUnknownIPAddresses: Indirect`

Table 36 xConfiguration CLI reference (continued)

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 VCS has been given but no callee alias has been specified. Example: `xConfiguration Call Services Fallback Alias: "reception@example.com"`
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`
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`
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`
CollaborationEdge Enabled: <On/Off> Enables or disables Mobile and Remote Access on this VCS. Example: `xConfiguration CollaborationEdge Enabled: On`
CollaborationEdge InternalCheck: <No/Yes> This switch determines whether the VCS Control will check the user's home node for available authentication modes. If you select No , the VCS tells the client that the authentication modes enabled on the VCS Control 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 VCS Control to check on the user's home node before the VCS Expressway responds to the client. Example: `xConfiguration CollaborationEdge InternalCheck: No`
CollaborationEdge JabbercEnabled: <On/Off> Enables or disables Jabber Guest services on this VCS. Example: `xConfiguration JabbercEnabled: Off`

Table 36 xConfiguration CLI reference (continued)

CollaborationEdge JabbercProxyProtocol: <http/https> Selects the protocol used to proxy Jabber Guest services requests through the VCS. Example: `xConfiguration JabbercProxyProtocol: https`
CollaborationEdge LegacyCred: <On/Off> Select On if Unified Communications services authorize MRA clients based on the username and password they supply to the VCS. Example: `xConfiguration CollaborationEdge LegacyCred: Off`
CollaborationEdge LegacySso: <On/Off/Exclusive> Select On if Unified Communications services authorize MRA clients based on the OAuth token they supply to the VCS. This is not the self-describing OAuth token type. Example: `xConfiguration CollaborationEdge LegacySso: Off`
CollaborationEdge OauthLocal: <On/Off> Enables or disables OAuth local authentication for mobile and remote access to Unified Communications services. Example: `xConfiguration CollaborationEdge OauthLocal: Off`
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`
CollaborationEdge RFC3327Enabled: <On/Off> Changes Path header support for registrations going through automatically generated neighbor zones to Unified CM nodes. *On*: The VCS Control inserts its address into the Path header of the REGISTER message, and into the response to that message. *Off*: The VCS Control overwrites the address in the Contact header of the REGISTER message. Example: `xConfiguration CollaborationEdge rfc3327Enabled: On`
CollaborationEdge SSO Scope: <PEER/CLUSTER> Use PEER if you wish to use a SAML agreement, with your chosen IdP, for each VCS peer. Use CLUSTER if you wish to use a single SAML agreement for the cl uster. Example: `xConfiguration CollaborationEdge SSO Scope: CLUSTER`
CollaborationEdge SSO IdP <index> Digest: <sha1/sha256> Changes the hash algorithm that the VCS 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 VCS. Example: `xConfiguration CollaborationEdge SSO IdP 1 Digest: sha256`

Table 36 xConfiguration CLI reference (continued)

CollaborationEdge SsoAlwaysAvailable: <On/Off> Determines whether the VCS Control will check if the user's home node has SSO available. *On*: The VCS Expressway always tells the client that SSO is available, without actually checking the home node. *Off*: Allow the VCS Control to check if SSO is available on the user's home node before the VCS Expressway responds to the client. Example: `xConfiguration CollaborationEdge SsoAlwaysAvailable: Off` **Note:** The default value *Off* corresponds to the following default on the web UI: **Check for internal SSO availability**: *Yes*
CollaborationEdge SsoEnabled: <On/Off> Toggles Single Sign-On for mobile and remote access to UC services. Example: `xConfiguration CollaborationEdge SsoEnabled: Off`
CollaborationEdge SsoSipTokenExtraTtl: <0..172800> Extends the lifetime of the SIP authorization token by the supplied number of seconds. **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`
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 VCS. Example: `xConfiguration CollaborationEdgeDeployments 1 DeploymentId: 5`
CollaborationEdgeDeployments <index> UserReadableName: <String> Enter a name for this deployment. You can use multiple deployments to partition the Unified Communications services provided via this VCS. See Using deployments to partition Unified Communications services. *<index>* is an integer distinguishing a particular IdP from the list that is configured on the VCS. Example: `xConfiguration CollaborationEdgeDeployments 1 UserReadableName: StagingDeployment`
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.

Table 36 xConfiguration CLI reference (continued)

Ciphers ForwardProxyTLSCiphers Value: <S:0,2048> **CAUTION: Although the built-in forward proxy is in the VCS interface, it is not currently supported and it should not be used.** Specifies the Forward Proxy TLS cipher suite to use in 'OpenSSL ciphers' format (See https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT). Default: `EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL` Example: `xConfiguration Ciphers ForwardProxyTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"`
Ciphers ForwardProxyTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2> **CAUTION: Although the built-in forward proxy is in the VCS interface, it is not currently supported and it should not be used.** Specifies the Forward Proxy TLS protocol minimum version. Default: `minTLSv1.2` Example: `xConfiguration Ciphers ForwardProxyTLSProtocol Value: "minTLSv1.2"`
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"`
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"`
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"`
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"`

Table 36 xConfiguration CLI reference (continued)

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"`
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"`
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"`
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"`
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"`
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"`

Table 36 xConfiguration CLI reference (continued)

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"`
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"`
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"`
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"`
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"`
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"`
EdgeConfigServer CredentialTtl: <0..604800> Does not apply to SSO authentications. Specifies the lifetime of the authentication token issued by the VCS 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: `EdgeConfigServer CredentialTtl: 28800`
EdgeConfigServer PurgeInterval: <0..604800> Does not apply to SSO authentications. Specifies how long the VCS 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: `EdgeConfigServer PurgeInterval: 43200`

Table 36 xConfiguration CLI reference (continued)

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`
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`
ErrorReport Contact: <S: 0, 128> An optional contact email address for follow up on incident reports if required. Example: `xConfiguration ErrorReport Contact: "bob smith"`
ErrorReport CoreDump: <On/Off> Determines whether diagnostic core dump files are created. Default: On. Example: `xConfiguration ErrorReport CoreDump: On`
ErrorReport Mode: <On/Off> Determines whether details of application failures are automatically sent to a web service. Default: Off. Example: `xConfiguration ErrorReport Mode: Off`
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/`
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/`
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"`

Table 36 xConfiguration CLI reference (continued)

Ethernet [1..2] IP V4 StaticNAT Address: <S:7,15> If the VCS 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"`
Ethernet [1..2] IP V4 StaticNAT Mode: <On/Off> Specifies whether the VCS 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`
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"`
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"`
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`
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"`
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"`
ExternalManager Protocol: <HTTP/HTTPS> The protocol used to connect to the external manager. Default: HTTPS. Example: `xConfiguration ExternalManager Protocol: HTTPS`
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`

Table 36 xConfiguration CLI reference (continued)

H323 Gatekeeper AutoDiscovery Mode: <On/Off> Determines whether or not the VCS responds to gatekeeper discovery requests from endpoints. Default: On. Example: `xConfiguration H323 Gatekeeper AutoDiscovery Mode: On`
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`
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`
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`
H323 Gatekeeper CallTimeToLive: <60..65534> Specifies the interval (in seconds) at which the VCS polls the endpoints in a call to verify that they are still in the call. Default: 120. Example: `xConfiguration H323 Gatekeeper CallTimeToLive: 120`
H323 Gatekeeper Registration RIPAllRequests: <On/Off> Determines whether the VCS 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`
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`
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`
H323 Gatekeeper TimeToLive: <60..65534> The interval (in seconds) at which an H.323 endpoint must re-register with the VCS to confirm that it is still functioning. Default: 1800. Example: `xConfiguration H323 Gatekeeper TimeToLive: 1800`

Table 36 xConfiguration CLI reference (continued)

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`
H323 Mode: <On/Off> Determines whether or not the VCS will provide H.323 gatekeeper functionality. Default: Off. Example: `xConfiguration H323 Mode: On`
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`
Interworking Encryption Mode: <Auto/Off> Determines whether or not the VCS 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`
Interworking Encryption Replay Protection Mode: <On/Off> Controls whether the VCS will perform replay protection for incoming SRTP packets when interworking a call. Default: Off. *On*: replayed SRTP packets will be dropped by the VCS. *Off*: the VCS will not check for replayed SRTP packets. Example: `xConfiguration Interworking Encryption Replay Protection Mode: Off`
Interworking Mode: <On/Off/RegisteredOnly> Determines whether or not the VCS will act as a gateway between SIP and H.323 calls. Default: RegisteredOnly. *Off*: the VCS will not act as a SIP–H.323 gateway. *On*: the VCS will act as SIP–H.323 gateway regardless of whether the endpoints are locally registered. *RegisteredOnly*: the VCS 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`
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"`

Table 36 xConfiguration CLI reference (continued)

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 VCS in SIP messaging. Example: `xConfiguration IP DNS Domain Name: "example.com"`
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"`
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`
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`
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"`
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`
IP Ephemeral PortRange End: <1024..65534> The highest port in the range used for ephemeral outbound connections not otherwise constrained by VCS call processing. Default: 35999. Example: `xConfiguration IP Ephemeral PortRange End: 35999`
IP Ephemeral PortRange Start: <1024..65534> The lowest port in the range used for ephemeral outbound connections not otherwise constrained by VCS call processing. Default: 30000. Example: `xConfiguration IP Ephemeral PortRange Start: 30000`

Table 36 xConfiguration CLI reference (continued)

IP External Interface: <LAN1/LAN2> Defines which LAN interface is externally facing. Default: LAN1. Example: `xConfiguration IP External Interface: LAN1`
IP Gateway: <S: 7,15> Specifies the IPv4 gateway of the VCS. 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"`
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`.
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`.
IP RFC4821 Mode: <Auto/Enabled/Disabled> Determines when RFC4821 Packetization Layer Path MTU Discovery is used by the VCS network interface. 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`
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"`
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"`

Table 36 xConfiguration CLI reference (continued)

IP Route [1..50] Interface: <Auto/LAN1/LAN2> Specifies the LAN interface to use for this route. Auto: The VCS will select the most appropriate interface to use. Default: Auto. Example: `xConfiguration IP Route 1 Interface: Auto`
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`
IP V6 Gateway: <S: 0, 39> Specifies the IPv6 gateway of the VCS. You must restart the system for any changes to take effect. Example: `xConfiguration IP V6 Gateway: "3dda:80bb:6::9:144"`
IPProtocol: <Both/IPv4/IPv6> Selects whether the VCS 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`
Language Default: <S: 0, 128> The default language used on the web interface. Default: "en_US". Example: `xConfiguration Language Default: "en_US"`
Log CDR Service: <off/serviceonly/serviceandlogging> Select how to log Call Detail Records produced by this VCS. *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: `xconfig Log CDR Service: serviceonly`
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`
Log MediaStats Logging: <On/Off> Toggles media statistics logging. Default: Off Example: `xConfiguration Log MediaStats Logging: On`

Table 36 xConfiguration CLI reference (continued)

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: `xconfig Log SystemMetrics Interval: 60`
Log SystemMetrics Mode: <On/Off> Toggles the System Metrics Collection service. Enter On to start collecting metrics for this system. Default: Off Example: `xconfig Log SystemMetrics Mode: On`
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: `xconfig log SystemMetrics Network Address: "192.168.0.5"`
Log SystemMetrics Network Port: <1..65535> Enter the port on which the listening server is expecting System Metrics traffic. Default: 25826 Example: `xconfig log SystemMetrics Network Port: 25826`
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`
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"`
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"`

Table 36 xConfiguration CLI reference (continued)

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 VCS 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`
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`
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`
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`
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"`
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`

Table 36 xConfiguration CLI reference (continued)

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`
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"`
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"`
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"`
Login Remote Protocol: <LDAP> The protocol used to connect to the external directory. Default: LDAP. Example: `xConfiguration Login Remote Protocol: LDAP`
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 VCS. *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 VCS, and then if no matching account is found the external credentials directory is used instead. Example: `xConfiguration Login Source Admin: LocalOnly`
Login Source User: <Local/Remote> Defines where FindMe login credentials are authenticated before access is allowed. Default : Local. *Remote*: credentials are verified against an external credentials directory, for example Windows Active Directory. *Local*: credentials are verified against a local database stored on the VCS. Example: `xConfiguration Login Source User: Local`
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"`

Table 36 xConfiguration CLI reference (continued)

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"`
Management Interface HstsMode: <On/Off> Determines whether web browsers are instructed to only ever use a secure connection to access this server. Enabling this feature gives added protection against man-in-the-middle (MITM) attacks. Default: On. *On*: the Strict-Transport-Security header is sent with all responses from the web server, with a 1 year expiry time. *Off* : the Strict-Transport-Security header is not sent, and browsers work as normal. Note: you must restart the system for any changes to take effect. Example: `xConfiguration Management Interface HstsMode: On`
Management Interface Port: <1..65535> Sets the https listening port for administrators to access the VCS web interface. Default: 443. Example: `xConfiguration Management Interface Port: 7443`
Management Session InactivityTimeout: <0..65535> Sets the number of minutes that an administration session (serial port, HTTPS or SSH) or a user (FindMe) session may be inactive before the session is timed out. A value of 0 turns session time outs off. Default: 30. Example: `xConfiguration Management Session InactivityTimeout: 30`
Management Session MaxConcurrentSessionsTotal: <0..65535> The maximum number of concurrent administrator sessions allowed on the system. This includes web, SSH and serial sessions. A value of 0 turns session limits off. Default: 0. Example: `xConfiguration Management Session MaxConcurrentSessionsTotal: 0`
Management Session MaxConcurrentSessionsUser: <0..65535> The number of concurrent sessions that each individual administrator account is allowed on the system. This includes web, SSH and serial sessions. A value of 0 turns session limits off. Default: 0. Example: `xConfiguration Management Session MaxConcurrentSessionsUser: 0`
NetworkLimits Configures the experimental rate limiting feature. Enter `xconfig networklimits ?` to read the help. Example: `xConfiguration NetworkLimits Configuration GarbageCollectSecs: 5`
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"`

Table 36 xConfiguration CLI reference (continued)

Option [1..64] Key: <S: 0, 90> Specifies the option key of your software option. These are added to the system in order to add extra functionality, such as increasing the system's capacity. Contact your Cisco support representative for further information. Example: `xConfiguration Option 1 Key: "1X4757T5-1-60BAD5CD"`
Policy AdministratorPolicy Mode: <Off/LocalCPL/LocalService/PolicyService> Enables and disables use of Call Policy. Default: Off. *Off*: Disables call policy. *LocalCPL*: uses policy from an uploaded CPL file. *LocalService*: uses group policy information and a local file. *PolicyService*: uses an external policy server. Example: `xConfiguration Policy AdministratorPolicy Mode: Off`
Policy AdministratorPolicy Service DefaultCPL: <S: 0,255> The CPL used by the VCS when the remote service is unavailable. Default: <reject status='403' reason='Service Unavailable'/> Example: `xConfiguration Policy AdministratorPolicy Service DefaultCPL: "<reject status='403' reason='Service Unavailable'/>"`
Policy AdministratorPolicy Service Password: <S: 0,82> Specifies the password used by the VCS 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"`
Policy AdministratorPolicy Service Path: <S: 0,255> Specifies the URL of the remote service. Example: `xConfiguration Policy AdministratorPolicy Service Path: "service"`
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`
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"`
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`

Table 36 xConfiguration CLI reference (continued)

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`
Policy AdministratorPolicy Service TLS Verify Mode: <On/Off> Controls X.509 certificate checking and mutual authentication between this VCS 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`
Policy AdministratorPolicy Service UserName: <S: 0,30> Specifies the user name used by the VCS to log in and query the remote policy service. Example: `xConfiguration Policy AdministratorPolicy Service UserName: "user123"`
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`
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`
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"`
Policy FindMe Server Password: <S: 0, 82> Specifies the password used by the VCS 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"`
Policy FindMe Server Path: <S: 0, 255> Specifies the URL of the remote FindMe Manager. Example: `xConfiguration Policy FindMe Server Path: "service"`

Table 36 xConfiguration CLI reference (continued)

Policy FindMe Server Protocol: <HTTP/HTTPS> Specifies the protocol used to connect to the remote FindMe Manager. Default: HTTPS. Example: `xConfiguration Policy FindMe Server Protocol: HTTPS`
Policy FindMe Server UserName: <S: 0, 30> Specifies the user name used by the VCS to log in and query the remote FindMe Manager. Example: `xConfiguration Policy FindMe Server UserName: "user123"`
Policy FindMe UserDeviceRestriction: <Off/On> Controls if users are restricted from adding, deleting or modifying their own devices. Default: Off. Example: `xConfiguration Policy FindMe UserDeviceRestriction: Off`
Policy Services Service [1..20] DefaultCPL: <S: 0,255> The CPL used by the VCS 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'/>"`
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"`
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`
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"`
Policy Services Service [1..20] Password: <S: 0,82> Specifies the password used by the VCS 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"`
Policy Services Service [1..20] Path: <S: 0,255> Specifies the URL of the remote service. Example: `xConfiguration Policy Services Service 1 Path: "service"`

Table 36 xConfiguration CLI reference (continued)

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`
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"`
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`
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`
Policy Services Service [1..20] TLS Verify Mode: <On/Off> Controls X.509 certificate checking and mutual authentication between this VCS 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`
Policy Services Service [1..20] UserName: <S: 0,30> Specifies the user name used by the VCS to log in and query the remote service. Example: `xConfiguration Policy Services Service 1 UserName: "user123"`
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 VCS, 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`
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 VCS, 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`

Table 36 xConfiguration CLI reference (continued)

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 VCS, 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`
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 VCS, 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`
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"`
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"`
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`
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"`
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"`

Table 36 xConfiguration CLI reference (continued)

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`
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`
Registration RestrictionPolicy Service DefaultCPL: <S: 0,255> The CPL used by the VCS 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'/>"`
Registration RestrictionPolicy Service Password: <S: 0,82> Specifies the password used by the VCS 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"`
Registration RestrictionPolicy Service Path: <S: 0,255> Specifies the URL of the remote service. Example: `xConfiguration Registration RestrictionPolicy Service Path: "service"`
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`

Table 36 xConfiguration CLI reference (continued)

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"`
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`
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`
Registration RestrictionPolicy Service TLS Verify Mode: <On/Off> Controls X.509 certificate checking and mutual authentication between this VCS 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`
Registration RestrictionPolicy Service UserName: <S: 0,30> Specifies the user name used by the VCS to log in and query the remote service. Example: `xConfiguration Registration RestrictionPolicy Service UserName: "user123"`
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"`
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`
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`
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`

Table 36 xConfiguration CLI reference (continued)

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`
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`
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`
ResourceUsage Warning Activation Level: <0..100> Controls if and when the VCS 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`
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`
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`
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`
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`
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`

Table 36 xConfiguration CLI reference (continued)

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`
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`
SIP Authentication Digest Nonce Maximum Use Count: <1..1024> Maximum number of times that a nonce generated by the VCS may be used by a client. Default: 128. Example: `xConfiguration SIP Authentication Digest Nonce Maximum Use Count: 128`
SIP Authentication NTLM Mode: <On/Off/Auto> Controls when the VCS will challenge endpoints using the NTLM protocol. Default: Auto. *Off*: the VCS will never send a challenge containing the NTLM protocol. *On*: the VCS will always include NTLM in its challenges. *Auto*: the VCS will decide based on endpoint type whether to challenge with NTLM. Example: `xConfiguration SIP Authentication NTLM Mode: Auto`
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`
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`
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`
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"`
SIP Domain [1..200] Edge: <On/Off> Whether remote and mobile collaboration features are enabled. Default Off. Example: `xConfiguration SIP Domain 1 Edge: On`

Table 36 xConfiguration CLI reference (continued)

SIP Domain [1..200] Name: <S: 0,128> Specifies a domain for which this VCS is authoritative. The domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is "100.example-name.com". Example: `xConfiguration SIP Domain 1 Name: "100.example-name.com"`
SIP Domain [1..200] Sip: <On/Off> Specifies whether the VCS will act as a SIP registrar and Presence Server 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`
SIP GRUU Mode: <On/Off> Controls whether GRUU (RFC5627) support is active. Default: On. Example: `xConfiguration SIP GRUU Mode: On`
SIP MediaRouting ICE Mode: <On/Off> Controls whether the VCS takes the media for an ICE to non-ICE call where the ICE participant is thought to be behind a NAT device. Default: Off. Example: `xConfiguration SIP MediaRouting ICE Mode: Off`
SIP Mode: <On/Off> Determines whether or not the VCS will provide SIP registrar and SIP proxy functionality. This mode must be enabled in order to use either the Presence Server or the Presence User Agent. Default: Off. Example: `xConfiguration SIP Mode: On`
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"`
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`
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`

Table 36 xConfiguration CLI reference (continued)

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`
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`
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`
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 VCS's existing call processing rules. Example: `xConfiguration SIP Registration Proxy Mode: Off`
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`
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`

Table 36 xConfiguration CLI reference (continued)

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`
SIP Require Duo Video Mode: <On/Off> Controls whether the VCS requires the use of the com.tandberg.sdp.duo.enable extension for endpoints that support it. Default: On. Example: `xConfiguration SIP Require Duo Video Mode: On`
SIP Require UDP BFCP Mode: <On/Off> Controls whether the VCS will require the use of the com.tandberg.udp.bfcp extension for endpoints that support it. Default: On. Example: `xConfiguration SIP Require UDP BFCP Mode: On`
SIP Routes Route [1..20] Address: <S:0,39> Specifies the IP address of the next hop for this route, where matching SIP requests will be forwarded. Note: this command is intended for developer use only. Example: `xConfiguration SIP Routes Route 1 Address: "127.0.0.1"`
SIP Routes Route [1..20] Authenticated: <On/Off> Whether to forward authenticated requests. Default: Off. Note: this command is intended for developer use only. *On*: only forward requests along route if incoming message has been authenticated. *Off*: always forward messages that match this route. Example: `xConfiguration SIP Routes Route 1 Authenticated: On`
SIP 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"`
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)(.*)"`
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"`

Table 36 xConfiguration CLI reference (continued)

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`
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%)"`
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"`
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`
SIP Session Refresh Minimum: <90..7200> The minimum value the VCS will negotiate for the session refresh interval for SIP calls. For more information see the definition of Min-SE header in RFC 4028. Default: 500. Example: `xConfiguration SIP Session Refresh Minimum: 500`
SIP Session Refresh Value: <90..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`
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`
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`
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`

Table 36 xConfiguration CLI reference (continued)

SIP TCP Port: <1024..65534> Specifies the listening port for incoming SIP TCP calls. Default: 5060. Example: `xConfiguration SIP TCP Port: 5060`
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 VCS, 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`
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`
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`
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`
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`
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`
SIP TLS Port: <1024..65534> Specifies the listening port for incoming SIP TLS calls. Default: 5061. Example: `xConfiguration SIP TLS Port: 5061`

Table 36 xConfiguration CLI reference (continued)

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`
SIP UDP Port: <1024..65534> Specifies the listening port for incoming SIP UDP calls. Default: 5060. Example: `xConfiguration SIP UDP Port: 5060`
SNMP CommunityName: <S: 0, 16> The VCS's SNMP community name. Default: public Example: `xConfiguration SNMP CommunityName: "public"`
SNMP SystemContact: <S: 0, 70> The name of the person who can be contacted regarding issues with the VCS. Default: Administrator. Example: `xConfiguration SNMP SystemContact: Administrator`
SNMP SystemLocation: <S: 0, 70> The physical location of the system. Example: `xConfiguration SNMP SystemLocation: "Server Room 128"`
SNMP V1Mode: <On/Off> Enables or disables SNMP Version 1 support. Default: Off. Example: `Configuration SNMP V1Mode: Off`
SNMP V2cMode: <On/Off> Enables or disables SNMP Version 2c support. Default: On. Example: `xConfiguration SNMP V2cMode: On`
SNMP V3AuthenticationMode: <On/Off> Enables or disables SNMP Version 3 authentication. Default: On. Example: `xConfiguration SNMP V3AuthenticationMode: On`
SNMP V3AuthenticationPassword: <S: 0,215> Sets SNMP Version 3 authentication password. It must be at least 8 characters. Example: `xConfiguration SNMP V3AuthenticationPassword: "password123"`
SNMP V3AuthenticationType: <MD5/SHA> Sets SNMP Version 3 authentication type. Default: SHA. Example: `xConfiguration SNMP V3AuthenticationType: SHA`

Table 36 xConfiguration CLI reference (continued)

SNMP V3Mode: <On/Off> Enables or disables SNMP Version 3 support. Default: On. Example: `xConfiguration SNMPV3 Mode: On`
SNMP V3PrivacyMode: <On/Off> Enables or disables SNMP Version 3 privacy. Default: On. Example: `xConfiguration SNMP V3PrivacyMode: On`
SNMP V3PrivacyPassword: <S: 0,215> Sets SNMP Version 3 privacy password. It must be at least 8 characters. Example: `xConfiguration SNMP V3PrivacyPassword: "password123"`
SNMP V3PrivacyType: <AES> Sets SNMP Version 3 privacy type. Default: AES. Example: `xConfiguration SNMP V3PrivacyType: AES`
SNMP V3UserName: <S: 0,70> Sets the username to use when using SNMP V3. Example: `xConfiguration SNMP V3UserName: "user123"`
SystemUnit Maintenance Mode: <On/Off> Sets the VCS 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`
SystemUnit Name: <S:, 0, 50> Defines the name of the VCS. 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"`
TimeZone Name: <S: 0, 64> Sets the local time zone of the VCS. Time zone names follow the POSIX naming convention e.g. Europe/London or America/New_ York. Default: GMT. Example: `xConfiguration TimeZone Name: "GMT"`
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"`

Table 36 xConfiguration CLI reference (continued)

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`
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"`
Transform [1..100] Pattern String: <S: 0, 60> The pattern against which the alias is compared. Example: `xConfiguration Transform 1 Pattern String: "example.net"`
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`
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`
Transform [1..100] State: <Enabled/Disabled> Indicates if the transform is enabled or disabled. Disabled transforms are ignored. Example: `xConfiguration Transform 1 State: Enabled`
Traversal Media Port End: <1025..65533> For traversal calls (where the VCS 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`

Table 36 xConfiguration CLI reference (continued)

Traversal Media Port Start: <1024..65532> For traversal calls (where the VCS 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`
Traversal Server H323 Assent CallSignaling Port: <1024..65534> The port on the VCS to use for Assent signaling. Default: 2776 . Example: `xConfiguration Traversal Server H323 Assent CallSignaling Port: 2777`
Traversal Server H323 H46018 CallSignaling Port: <1024..65534> The port on the VCS to use for H460.18 signaling. Default: 2777 . Example: `xConfiguration Traversal Server H323 H46018 CallSignaling Port: 2777`
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`
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"`
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`
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`
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`
Traversal Server TURN Mode: <On/Off> Determines whether the VCS offers TURN services to traversal clients. Default: Off . Example: `xConfiguration Traversal Server TURN Mode: Off`

Table 36 xConfiguration CLI reference (continued)

Traversal Server TURN Port: <1024..65534> The listening port for TURN requests. Default: 3478. Example: `xConfiguration Traversal Server TURN Port: 3478`
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`
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`
Traversal Server TURN ProtocolMode: <TCP/UDP/Both> The permitted protocols for TURN requests. Default: Both. Example: `xConfiguration Traversal Server TURN ProtocolMode: Both`
XCP DelayedRestart EnableDelayedRestart: <On/Off> Controls whether the Delayed Cisco XCP Router restart feature is enabled. Default: Off. Example: `xConfiguration DelayedRestart EnableDelayedRestart: On`
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`
XCP DelayedRestart MultitenancyEnabled: <On/Off> Turn on multitenancy to configure the delayed Cisco XCP Router restart. Default: Off. Example: `xConfiguration XCP DelayedRestart MultitenancyEnabled: On`
XCP DelayedRestart ScheduledTime: The time each day that the scheduled restart takes place. Example: `xConfiguration XCP DelayedRestart ScheduledTime: 01.00`
XCP DelayedRestartNotify RestartTime: Set the notification for the restart time. Example: `xConfiguration DelayedRestartNotify RestartTime: 01.00`

Table 36 xConfiguration CLI reference (continued)

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`
XCP TLS Certificate CVS ConvertIpToHostname: <On/Off> Controls whether VCS automatically converts XCP peer's IP address to FQDN for certificate verification. Default: On. Example: `xConfiguration XCP TLS Certificate CVS ConvertIpToHostname: On`
XCP TLS Certificate CVS CrlNetworkFetchEnabled: <On/Off> Controls whether the VCS 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`
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`
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`
XCP TLS Certificate CVS UseCrl: <On/Off> Controls whether VCS 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`
XCP TLS Certificate CVS UseOcsp: <On/Off> Controls whether the VCS 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`
XCP TLS Certificate CVS VerifyHostname: <On/Off> Controls whether the VCS verifies the hostname from the XCP host's certificate against its own peer configuration. Default: On. Example: `xConfiguration XCP TLS Certificate CVS VerifyHostname: On`

Table 36 xConfiguration CLI reference (continued)

Zones DefaultZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials> Controls how the VCS 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`
Zones DefaultZone SIP Media Encryption Mode: <Off/On/BestEffort/Auto> The media encryption policy applied by the VCS 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`
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: `Zones DefaultZone SIP Media ICE Support: On`
Zones DefaultZone SIP Multistream Mode: <Off/On> Controls if the VCS 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`
Zones DefaultZone SIP Record Route Address Type: <IP/Hostname> Controls whether the VCS 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 VCS. Default: IP. Example: `xConfiguration Zones DefaultZone SIP Record Route Address Type: IP`
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`

Table 36 xConfiguration CLI reference (continued)

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 VCS. 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`
Zones LocalZone DefaultSubZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials> Controls how the VCS 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`
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`
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. Default: Unlimited. *NoBandwidth*: no bandwidth available. No calls can be made to or from the Default Subzone. Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: Limited`
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`
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. Default: Unlimited. *NoBandwidth*: no bandwidth available. No calls can be made within the Default Subzone. Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: Limited`
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`
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. Default: Unlimited. *NoBandwidth*: no bandwidth available. No calls can be made to, from, or within the Default Subzone. Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: Limited`

Table 36 xConfiguration CLI reference (continued)

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`
Zones LocalZone DefaultSubZone SIP Media Encryption Mode: <Off/On/BestEffort/Auto> The media encryption policy applied by the VCS 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`
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`
Zones LocalZone DefaultSubZone SIP Multistream Mode: <Off/On> Controls if the VCS 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`
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`
Zones LocalZone SIP Record Route Address Type: <IP/Hostname> Controls whether the VCS 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 VCS. Default: IP. Example: `xConfiguration Zones LocalZone SIP Record Route Address Type: IP`
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"`

Table 36 xConfiguration CLI reference (continued)

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"`
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"`
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`
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`
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`
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"`
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"`
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`
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`

Table 36 xConfiguration CLI reference (continued)

Zones LocalZone SubZones SubZone [1..1000] Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials> Controls how the VCS 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`
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`
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`
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: `Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Intra Limit: 1920`
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`
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`
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`
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"`

Table 36 xConfiguration CLI reference (continued)

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`
Zones LocalZone SubZones SubZone [1..1000] SIP Media Encryption Mode: <Off/On/BestEffort/Auto> The media encryption policy applied by the VCS 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`
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`
Zones LocalZone SubZones SubZone [1..1000] SIP Multistream Mode: <Off/On> Controls if the VCS 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`
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 VCS. Default: On . Example: `xConfiguration Zones LocalZone Traversal H323 Assent Mode: On`
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 VCS. Default: On . Example: `xConfiguration Zones LocalZone Traversal H323 H46018 Mode: On`

Table 36 xConfiguration CLI reference (continued)

Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: <On/Off> Controls whether the VCS 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`
Zones LocalZone Traversal H323 Preference: <Assent/H46018> If an endpoint that is registered directly with the VCS supports both Assent and H460.18 protocols, this setting determines which the VCS uses. Default: Assent. Example: `xConfiguration Zones LocalZone Traversal H323 Preference: Assent`
Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: <1..65534> Sets the interval (in seconds) with which a traversal-enabled endpoint registered directly with the VCS will send a TCP probe to the VCS 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`
Zones LocalZone Traversal H323 TCPProbe RetryCount: <1..65534> Sets the number of times traversal-enabled endpoints registered directly with the VCS will attempt to send a TCP probe. Default: 5 . Example: `xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryCount: 5`
Zones LocalZone Traversal H323 TCPProbe RetryInterval: <1..65534> Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the VCS will send a TCP probe. Default: 2 . Example: `xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryInterval: 2`
Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: <1..65534> Sets the interval (in seconds) with which a traversal-enabled endpoint registered directly with the VCS will send a UDP probe to the VCS 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`
Zones LocalZone Traversal H323 UDPProbe RetryCount: <1..65534> Sets the number of times traversal-enabled endpoints registered directly with the VCS will attempt to send a UDP probe. Default: 5 . Example: `xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryCount: 5`
Zones LocalZone Traversal H323 UDPProbe RetryInterval: <1..65534> Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the VCS will send a UDP probe. Default: 2 . Example: `xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryInterval: 2`

Table 36 xConfiguration CLI reference (continued)

Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: <1..100000000> The bandwidth limit (in kbps) applied to any one traversal call being handled by the VCS (applies only if the mode is set to Limited). Default: 1920 . Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: 1920`
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 VCS. Default: Unlimited. *NoBandwidth*: no bandwidth available. No traversal calls can be made. Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: Limited`
Zones LocalZone TraversalSubZone Bandwidth Total Limit: <1..100000000> The total bandwidth (in kbps) allowed for all traversal calls being handled by the VCS (applies only if the mode is set to Limited). Default: 500000 . Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Limit: 500000`
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 VCS. Default: Unlimited. *NoBandwidth*: no bandwidth available. No traversal calls can be made. Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: Limited`
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`
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`
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"`

Table 36 xConfiguration CLI reference (continued)

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`
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"`
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`
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"`
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"`
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`

Table 36 xConfiguration CLI reference (continued)

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`
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`
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`
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`
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"`
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`
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"`
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`

Table 36 xConfiguration CLI reference (continued)

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 VCS will then query for A and AAAA DNS Records. Default: Off . Example: `xConfiguration Zones Zone 1 DNS IncludeAddressRecord: Off`
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`
Zones Zone [1..1000] DNS Interworking SIP EmptyInviteAllowed: <On/Off> Controls if the VCS 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`
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`
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`
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`
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`

Table 36 xConfiguration CLI reference (continued)

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`
Zones Zone [1..1000] DNS SIP Media Encryption Mode: <Off/On/BestEffort/Auto> The media encryption policy applied by the VCS for SIP calls (including interworked calls) to and from this zone. Default: Auto. *On*: All media must be encrypted. *Off*: All media must be unencrypted. *BestEffort*: Use encryption if available otherwise fallback to unencrypted media. *Auto*: No media encryption policy is applied. Example: `xConfiguration Zones Zone 1 DNS SIP Media Encryption Mode: Auto`
Zones Zone [1..1000] DNS SIP 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`
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`
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 VCS again they will be rejected. Default: Off . *On*: SIP requests sent out via this zone that are received again by this VCS will be rejected. *Off*: SIP requests sent out via this zone that are received by this VCS again will be processed as normal. Example: `xConfiguration Zones Zone 1 DNS SIP Poison Mode: Off`
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`

Table 36 xConfiguration CLI reference (continued)

Zones Zone [1..1000] DNS SIP Record Route Address Type: <IP/Hostname> Controls whether the VCS 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 VCS. Default: IP. Example: `xConfiguration Zones Zone 1 DNS SIP Record Route Address Type: IP`
Zones Zone [1..1000] DNS SIP SearchAutoResponse: <On/Off> Controls what happens when the VCS receives a SIP search that originated as an H.323 search, destined for this zone. Default: Off . *Off*: a SIP OPTION message will be sent to the zone. *On*: searches will be responded to automatically, without being forwarded to the zone. Example: `xConfiguration Zones Zone 1 DNS SIP SearchAutoResponse: Off`
Zones Zone [1..1000] DNS SIP TLS Verify Mode: <On/Off> Controls X.509 certificate checking between this VCS and the destination system server returned by the DNS lookup. When enabled, the domain name submitted to the DNS lookup must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: Off . Example: `xConfiguration Zones Zone 1 DNS SIP TLS Verify Mode: On`
Zones Zone [1..1000] DNS SIP TLS Verify Subject Name: <S: 0..128> The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). If empty then the domain portion of the resolved URI is used. Example: `xConfiguration Zones Zone 1 DNS SIP TLS Verify Subject Name: "example.com"`
Zones Zone [1..1000] DNS SIP UDP BFCP Filter Mode: <On/Off> Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. Default: Off . *On*: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled. *Off*: INVITE requests are not modified. Example: `xConfiguration Zones Zone 1 DNS SIP UDP BFCP Filter Mode: Off`
Zones Zone [1..1000] DNS ZoneProfile: <Default/Custom/CiscoUnifiedCommunicationsManager/ CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDevice/LocalB2BUAService> Determines how the zone's advanced settings are configured. *Default*: uses the factory defaults. *Custom*: allows you to configure each setting individually. *Preconfigured profiles*: alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. Example: `xConfiguration Zones Zone 1 DNS ZoneProfile: Default`

Table 36 xConfiguration CLI reference (continued)

Zones Zone [1..1000] ENUM DNSSuffix: <S: 0, 128> The DNS zone to append to the transformed E.164 number to create an ENUM host name which this zone is then queried for. Example: `xConfiguration Zones Zone 2 ENUM DNSSuffix: "e164.arpa"`
Zones Zone [1..1000] H323 Mode: <On/Off> Determines whether H.323 calls will be allowed to and from this zone. Default: On . Example: `xConfiguration Zones Zone 2 H323 Mode: On`
Zones Zone [1..1000] HopCount: <1..255> Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used. Default: 15 . Example: `xConfiguration Zones Zone 2 HopCount: 15`
Zones Zone [1..1000] Name: <S: 1, 50> Assigns a name to this zone. Example: `xConfiguration Zones Zone 3 Name: "UK Sales Office"`
Zones Zone [1..1000] Neighbor Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/ CheckCredentials> Controls how the VCS authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials. Example: `xConfiguration Zones Zone 3 Neighbor Authentication Mode: DoNotCheckCredentials`
Zones Zone [1..1000] Neighbor H323 CallSignaling Port: <1024..65534> The port on the neighbor to use for H.323 calls to and from this VCS. Default: 1720 . Example: `xConfiguration Zones Zone 3 Neighbor H323 CallSignaling Port: 1720`
Zones Zone [1..1000] Neighbor H323 Port: <1024..65534> The port on the neighbor to use for H.323 searches to and from this VCS. Default: 1719 . Example: `xConfiguration Zones Zone 3 Neighbor H323 Port: 1719`
Zones Zone [1..1000] Neighbor H323 SearchAutoResponse: <On/Off> Determines what happens when the VCS 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`

Table 36 xConfiguration CLI reference (continued)

Zones Zone [1..1000] Neighbor Interworking SIP Audio DefaultCodec: <G711u/G711a/G722_48/G722_56/ G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48/G723_1/G728/G729/AACLD_48/AACLD_56/AACLD_64/AMR> Specifies which audio codec to use when empty INVITEs are not allowed. Default: G711u . Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Audio DefaultCodec: G711u`
Zones Zone [1..1000] Neighbor Interworking SIP EmptyInviteAllowed: <On/Off> Determines whether the VCS will generate a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. Default: On . *On*: SIP INVITEs with no SDP will be generated and sent to this neighbor. *Off*: SIP INVITEs will be generated and a pre-configured SDP will be inserted before the INVITEs are sent to this neighbor. Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP EmptyInviteAllowed: On`
Zones Zone [1..1000] Neighbor Interworking SIP Encryption EncryptSRTCP: <Yes/No> Controls if the VCS offers encrypted SRTCP in calls to this zone. The VCS will send an INFO request. Default: No. Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Encryption EncryptSRTCP: No`
Zones Zone [1..1000] Neighbor Interworking SIP Search Strategy: <Options/Info> Determines how the VCS will search for SIP endpoints when interworking an H.323 call. Default: Options . *Options*: the VCS will send an OPTIONS request. *Info*: the VCS will send an INFO request. Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Search Strategy: Options`
Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultBitrate: <64..65535> Specifies which video bit rate to use when empty INVITEs are not allowed. Default: 384 . Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultBitrate: 384`
Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264> Specifies which video codec to use when empty INVITEs are not allowed. Default: H263 . Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultCodec: H263`
Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA> Specifies which video resolution to use when empty INVITEs are not allowed. Default: CIF . Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultResolution: CIF`
Zones Zone [1..1000] Neighbor Monitor: <Yes/No> Specifies whether the zone monitors the aliveness of its neighbor peers. H323 LRQs and/or SIP OPTIONS will be periodically sent to the peers. If any peer fails to respond, that peer will be marked as inactive. If no peer manages to respond the zone will be marked as inactive. Default: Yes. Example: `xConfiguration Zones Zone 3 Neighbor Monitor: Yes`

Table 36 xConfiguration CLI reference (continued)

Zones Zone [1..1000] Neighbor Peer [1..6] Address: <S:0,128> Specifies the IP address or Fully Qualified Domain Name (FQDN) of the neighbor. If the neighbor zone is a VCS cluster, this will be one of the peers in that cluster. Example: `xConfiguration Zones Zone 3 Neighbor Peer 1 Address: "192.44.0.18"`
Zones Zone [1..1000] Neighbor Registrations: <Allow/Deny> Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow . Example: `xConfiguration Zones Zone 3 Neighbor Registrations: Allow`
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. **Notes:** ■ 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 VCS receives more than 10 consecutive malformed messages. ■ For CMR Cloud deployments, we recommend configuring RetainAll mode. Example: `xConfiguration Zones Zone 3 RetainConnectionOnParseErrorMode: RetainSome`
Zones Zone [1..1000] Neighbor SIP Authentication Trust Mode: <On/Off> Controls if authenticated SIP messages (ones containing a P-Asserted-Identity header) from this zone are trusted. Default: Off . *On*: messages are trusted without further challenge. *Off*: messages are challenged for authentication. Example: `xConfiguration Zones Zone 3 Neighbor SIP Authentication Trust Mode: On`
Zones Zone [1..1000] Neighbor SIP B2BUA Refer Mode: <Forward/Terminate> Determines how SIP REFER requests are handled. Default: *Forward* *Forward*: SIP REFER requests are forwarded to the target. *Terminate*: SIP REFER requests are terminated by the VCS. Example: `xConfiguration Zones Zone 3 Neighbor SIP B2BUA Refer Mode: Terminate`

Table 36 xConfiguration CLI reference (continued)

Zones Zone [1..1000] Neighbor SIP B2BUA Replaces Mode: <Forward/Terminate> Enables the VCS to process load balancing INVITE messages from Meeting Server call bridge groups. Default: *Forward* *Terminate*: VCS B2BUA processes the INVITEs from the Meeting Server. Required to enable load balancing for endpoints that are registered to this VCS, or to a neighboring VCS or Expressway. *Forward*: VCS 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`
Zones Zone [1..1000] Neighbor SIP B2BUA Service Identifier: <0..64> The identifier that represents an instance of a local SIP Back-to-Back User Agent service. Example: `xConfiguration Zones Zone 3 Neighbor SIP B2BUA Service Identifier: 1`
Zones Zone [1..1000] Neighbor SIP ClassFiveResponseLiveness: <Yes/No> Specifies whether Class 5 SIP responses from neighbor peers result in the zone being considered alive for use. Default: Yes. Example: `xConfiguration Zones Zone 3 Neighbor SIP ClassFiveResponseLiveness: Yes`
Zones Zone [1..1000] Neighbor SIP Encryption Mode: <Auto/Microsoft/Off> Determines how the VCS handles encrypted SIP calls on this zone. Default: Auto. *Auto*: SIP calls are encrypted if a secure SIP transport (TLS) is used. *Microsoft*: SIP calls are encrypted using MS-SRTP. *Off*: SIP calls are never encrypted. Example: `xConfiguration Zones Zone 3 Neighbor SIP Encryption Mode: Auto`
Zones Zone [1..1000] Neighbor SIP MIME Strip Mode: <On/Off> Controls whether multipart MIME stripping is performed on requests from this zone. This must be set to On for connections to a Microsoft Office Communications Server 2007. Default: Off . Example: `xConfiguration Zones Zone 3 Neighbor SIP MIME Strip Mode: Off`
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`

Table 36 xConfiguration CLI reference (continued)

Zones Zone [1..1000] Neighbor SIP Media Encryption Mode: <Off/On/BestEffort/Auto> The media encryption policy applied by the VCS 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`
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`
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`
Zones Zone [1..1000] Neighbor SIP MediaRouting Mode: <Auto/Signaled/Latching> How the VCS 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 VCS 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`
Zones Zone [1..1000] Neighbor SIP Multistream Mode: <Off/On> Controls if the VCS 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`

Table 36 xConfiguration CLI reference (continued)

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 VCS again they will be rejected. Default: Off . *On*: SIP requests sent out via this zone that are received again by this VCS will be rejected. *Off*: SIP requests sent out via this zone that are received by this VCS again will be processed as normal. Example: `xConfiguration Zones Zone 3 Neighbor SIP Poison Mode: Off`
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 VCS. Default: 5061 . Example: `xConfiguration Zones Zone 3 Neighbor SIP Port: 5061`
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`
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"`
Zones Zone [1..1000] Neighbor SIP RFC3327 Enabled: <Yes/No> Controls whether the VCS will insert RFC3327 Path headers when proxying REGISTER messages toward this zone. If disabled the VCS 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`.
Zones Zone [1..1000] Neighbor SIP Record Route Address Type: <IP/Hostname> Controls whether the VCS 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 VCS. Default: IP. Example: `xConfiguration Zones Zone 3 Neighbor SIP Record Route Address Type: IP`
Zones Zone [1..1000] Neighbor SIP SearchAutoResponse: <On/Off> Controls what happens when the VCS 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`

Table 36 xConfiguration CLI reference (continued)

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`
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 VCS and the neighbor system. When enabled, the neighbor system's FQDN or IP address, as specified in the Peer address field, must be contained within the neighbor's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: Off . Example: `xConfiguration Zones Zone 3 Neighbor SIP TLS Verify Mode: On`
Zones Zone [1..1000] Neighbor SIP Transport: <UDP/TCP/TLS> Determines which transport type will be used for SIP calls to and from this neighbor. Default: TLS . Example: `xConfiguration Zones Zone 3 Neighbor SIP Transport: TLS`
Zones Zone [1..1000] Neighbor SIP UDP BFCP Filter Mode: <On/Off> Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. Default: Off . *On*: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled. *Off*: INVITE requests are not modified. Example: `xConfiguration Zones Zone 3 Neighbor SIP UDP BFCP Filter Mode: Off`
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`
Zones Zone [1..1000] Neighbor SIP UPDATE Strip Mode: <On/Off> Determines whether the VCS 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`

Table 36 xConfiguration CLI reference (continued)

Zones Zone [1..1000] Neighbor SignalingRouting Mode: <Auto/Always> Specifies how the VCS handles the signaling for calls to and from this neighbor. Default: Auto. *Auto*: Signaling will be taken as determined by the Call Routed Mode configuration. *Always*: Signaling will always be taken for calls to or from this neighbor, regardless of the Call Routed Mode configuration. Example: `xConfiguration Zones Zone 3 Neighbor SignalingRouting Mode: Auto`
Zones Zone [1..1000] Neighbor ZoneProfile: <Default/Custom/CiscoUnifiedCommunicationsManager/ CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDevice/LocalB2BUAService> Determines how the zone's advanced settings are configured. *Default*: uses the factory defaults. *Custom*: allows you to configure each setting individually. *Preconfigured profiles*: alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. Example: `xConfiguration Zones Zone 3 Neighbor ZoneProfile: Default`
Zones Zone [1..1000] SIP Mode: <On/Off> Determines whether SIP calls will be allowed to and from this zone. Default: On. Example: `xConfiguration Zones Zone 3 SIP Mode: On`
Zones Zone [1..1000] TraversalClient Accept Delegated Credential Checks: <On/Off> Controls whether this traversal client accepts delegated credential checking requests from the VCS Expressway. Default: Off. *Off*: reject the requests. *On*: accept the requests and perform the credential checking using the authentication methods configured on this VCS. Example: `xConfiguration Zones Zone [1..1000] TraversalClient Accept Delegated Credential Checks: Off`
Zones Zone [1..1000] TraversalClient Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials> Controls how the VCS authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials. Example: `xConfiguration Zones Zone 4 TraversalClient Authentication Mode: DoNotCheckCredentials`
Zones Zone [1..1000] TraversalClient Authentication Password: <S: 0,215> The password used by the VCS when connecting to the traversal server. The maximum plaintext length is 128 characters, which is then encrypted. Example: `xConfiguration Zones Zone 4 TraversalClient Authentication Password: "password123"`
Zones Zone [1..1000] TraversalClient Authentication UserName: <S: 0,128> The user name used by the VCS when connecting to the traversal server. Example: `xConfiguration Zones Zone 4 TraversalClient Authentication UserName: "clientname"`

Table 36 xConfiguration CLI reference (continued)

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 VCS. If the traversal server is a VCS Expressway, this must be the port number that is configured on the VCS Expressway's traversal server zone associated with this VCS. Example: `xConfiguration Zones Zone 4 TraversalClient H323 Port: 2777`
Zones Zone [1..1000] TraversalClient H323 Protocol: <Assent/H46018> Determines which of the two firewall traversal protocols will be used for calls to and from the traversal server. Note: the same protocol must be set on the server for calls to and from this traversal client. Default: Assent. Example: `xConfiguration Zones Zone 4 TraversalClient H323 Protocol: Assent`
Zones Zone [1..1000] TraversalClient Peer [1..6] Address: <S:0,128> Specifies the IP address or Fully Qualified Domain Name (FQDN) of the traversal server. If the traversal server is a VCS Expressway cluster, this will be one of the peers in that cluster. Example: `xConfiguration Zones Zone 4 TraversalClient Peer 1 Address: "10.192.168.1"`
Zones Zone [1..1000] TraversalClient Registrations: <Allow/Deny> Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow. Example: `xConfiguration Zones Zone 4 TraversalClient Registrations: Allow`
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`
Zones Zone [1..1000] TraversalClient SIP Media Encryption Mode: <Off/On/BestEffort/Auto> The media encryption policy applied by the VCS 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`

Table 36 xConfiguration CLI reference (continued)

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`
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`
Zones Zone [1..1000] TraversalClient SIP Multistream Mode: <Off/On> Controls if the VCS 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`
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 VCS again they will be rejected. Default: Off . *On*: SIP requests sent out via this zone that are received again by this VCS will be rejected. *Off*: SIP requests sent out via this zone that are received by this VCS again will be processed as normal. Example: `xConfiguration Zones Zone 4 TraversalClient SIP Poison Mode: Off`
Zones Zone [1..1000] TraversalClient SIP Port: <1024..65534> Specifies the port on the traversal server to be used for SIP calls from this VCS. If your traversal server is a VCS Expressway, this must be the port number that has been configured in the traversal server zone for this VCS. Example: `xConfiguration Zones Zone 4 TraversalClient SIP Port: 5061`
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`
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`

Table 36 xConfiguration CLI reference (continued)

Zones Zone [1..1000] TraversalClient SIP TLS Verify Mode: <On/Off> Controls X.509 certificate checking and mutual authentication between this VCS and the traversal server. When enabled, the server's FQDN or IP address, as specified in the Peer address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: Off . Example: `xConfiguration Zones Zone 4 TraversalClient SIP TLS Verify Mode: On`
Zones Zone [1..1000] TraversalClient SIP Transport: <TCP/TLS> Determines which transport type will be used for SIP calls to and from the traversal server. Default: TLS . Example: `xConfiguration Zones Zone 4 TraversalClient SIP Transport: TLS`
Zones Zone [1..1000] TraversalServer Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials> Controls how the VCS authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials. Example: `xConfiguration Zones Zone 5 TraversalServer Authentication Mode: DoNotCheckCredentials`
Zones Zone [1..1000] TraversalServer Authentication UserName: <S: 0,128> The name used by the traversal client when authenticating with the traversal server. If the traversal client is a VCS, this must be the VCS's authentication user name. If the traversal client is a gatekeeper, this must be the gatekeeper's System Name. Example: `xConfiguration Zones Zone 5 TraversalServer Authentication UserName: "User123"`
Zones Zone [1..1000] TraversalServer H323 H46019 Demultiplexing Mode: <On/Off> Determines whether the VCS will operate in demultiplexing mode for calls from the traversal client. Default: Off . *On*: allows use of the same two ports for all calls. *Off*: each call will use a separate pair of ports for media. Example: `xConfiguration Zones Zone 5 TraversalServer H323 H46019 Demultiplexing Mode: Off`
Zones Zone [1..1000] TraversalServer H323 Port: <1024..65534> Specifies the port on the VCS being used for H.323 firewall traversal from this traversal client. Default: 6001, incrementing by 1 for each new zone. Example: `xConfiguration Zones Zone 5 TraversalServer H323 Port: 2777`
Zones Zone [1..1000] TraversalServer H323 Protocol: <Assent/H46018> Determines which of the two firewall traversal protocols will be used for calls to and from the traversal client. Note: the same protocol must be set on the client for calls to and from this traversal server. Default: Assent . Example: `xConfiguration Zones Zone 5 TraversalServer H323 Protocol: Assent`
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`

Table 36 xConfiguration CLI reference (continued)

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`
Zones Zone [1..1000] TraversalServer SIP Media Encryption Mode: <Off/On/BestEffort/Auto> The media encryption policy applied by the VCS for SIP calls (including interworked calls) to and from this zone. Default: Auto *On*: All media must be encrypted. *Off*: All media must be unencrypted. *BestEffort*: Use encryption if available otherwise fallback to unencrypted media. *Auto*: No media encryption policy is applied. Example: `xConfiguration Zones Zone 5 TraversalServer SIP Media Encryption Mode: Auto`
Zones Zone [1..1000] TraversalServer SIP 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`
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`
Zones Zone [1..1000] TraversalServer SIP Multistream Mode: <Off/On> Controls if the VCS 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`

Table 36 xConfiguration CLI reference (continued)

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 VCS again they will be rejected. Default: Off . *On*: SIP requests sent out via this zone that are received again by this VCS will be rejected. *Off*: SIP requests sent out via this zone that are received by this VCS again will be processed as normal. Example: `xConfiguration Zones Zone 5 TraversalServer SIP Poison Mode: Off`
Zones Zone [1..1000] TraversalServer SIP Port: <1024..65534> The port on the VCS being used for SIP firewall traversal from this traversal client. Default: 7001, incrementing by 1 for each new zone. Example: `xConfiguration Zones Zone 5 TraversalServer SIP Port: 5061`
Zones Zone [1..1000] TraversalServer SIP 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`
Zones Zone [1..1000] TraversalServer SIP Protocol: <Assent/TURN/ICE> Determines which firewall traversal protocol will be used for SIP calls to and from the traversal client. Note: the same protocol must be set on the client for calls to and from this traversal server. Default: Assent. Example: `xConfiguration Zones Zone 5 TraversalServer SIP Protocol: Assent`
Zones Zone [1..1000] TraversalServer SIP TLS Verify Mode: <On/Off> Controls X.509 certificate checking and mutual authentication between this VCS and the traversal client. If enabled, a TLS verify subject name must be specified. Default: Off. Example: `xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Mode: On`
Zones Zone [1..1000] TraversalServer SIP TLS Verify Subject Name: <S: 0,128> The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). Example: `xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Subject Name: "myclientname"`
Zones Zone [1..1000] TraversalServer SIP Transport: <TCP/TLS> Determines which of the two transport types will be used for SIP calls between the traversal client and VCS. Default: TLS . Example: `xConfiguration Zones Zone 5 TraversalServer SIP Transport: TLS`
Zones Zone [1..1000] TraversalServer TCPProbe KeepAliveInterval: <1..65534> Sets the interval (in seconds) with which the traversal client will send a TCP probe to the VCS 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`

Table 36 xConfiguration CLI reference (continued)

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 VCS. Default: 5 . Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryCount: 5`
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 VCS. Default: 2 . Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryInterval: 2`
Zones Zone [1..1000] TraversalServer UDPProbe KeepAliveInterval: <1..65534> Sets the interval (in seconds) with which the traversal client will send a UDP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open. Default: 20. Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe KeepAliveInterval: 20`
Zones Zone [1..1000] TraversalServer UDPProbe RetryCount: <1..65534> Sets the number of times the traversal client will attempt to send a UDP probe to the VCS. Default: 5. Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryCount: 5`
Zones Zone [1..1000] TraversalServer UDPProbe RetryInterval: <1..65534> Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the VCS. Default: 2. Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryInterval: 2`
Zones Zone [1..1000] Type: <Neighbor/TraversalClient/TraversalServer/ENUM/DNS> Determines the nature of the specified zone, in relation to the local VCS. *Neighbor*: the new zone will be a neighbor of the local VCS. *TraversalClient*: there is a firewall between the zones, and the local VCS is a traversal client of the new zone. *TraversalServer*: there is a firewall between the zones and the local VCS is a traversal server for the new zone. *ENUM*: the new zone contains endpoints discoverable by ENUM lookup. *DNS*: the new zone contains endpoints discoverable by DNS lookup. Example: `xConfiguration Zones Zone 3 Type: Neighbor`

Command Reference – xCommand

The `xCommand` group of commands are used to add and delete items and issue system commands.

The following section lists all the currently available `xCommand` commands.

To issue a command, type the command as shown, followed by one or more of the given parameters and values. The valid values for each parameter are indicated in the angle brackets following each parameter, using the following notation:

Format	Meaning
<0..63>	Indicates an integer value is required. The numbers indicate the minimum and maximum value. In this example the value must be in the range 0 to 63.
<S: 7,15>	An **S** indicates a string value, to be enclosed in quotation marks, is required. The numbers indicate the minimum and maximum number of characters for the string. In this example the string must be between 7 and 15 characters long.
<Off/Direct/Indirect>	Lists the set of valid values for the command. Do not enclose the value in quotation marks
(r)	(r) indicates that this is a required parameter. Note that the (r) is not part of the command itself.

To obtain information about using each of the `xCommand` commands from within the CLI, type:

- `xCommand` 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 VCS 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 of the available `xCommand` commands are listed in the table below:

acmedeletependingcert

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 acmedeletependingcert`**

`xCommand acmedeletependingcert Domain:"example.com"`

acmedeploy

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 acmedeploy`**

`xCommand acmedeploy Domain:"example.com" ReloadCerts:"On"`

acmegetpendingcert

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 Acmegetpendingcert`**

`xCommand Acmegetpendingcert Domain:"example.com"`

acmeprovidersread

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 Acmeprovidersread`**

`xCommand Acmeprovidersread ProviderUuid: "Default"`

`xCommand Acmeprovidersread ProviderUuid: "Provider-UUID"`

acmeproviderswrite

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 Acmeproviderswrite ProviderUuid: "Default" Email: "new-email@example.com" TermsOfService: "Accepted"`**

acmereset

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 Acmereset execute`**

`xCommand Acmereset Action: "execute"`

acmerevoke

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 Acmerevoke "/path_to_cert_to_be_revoked"`**

Example, using a specific ACME provider: **`xCommand Acmerevoke CertPath:"/path_to_cert_to_be_revoked" Provider:"ACME_Provider_Name"`**

acmesettingsread

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 Acmesettingsread`**

`xcommand Acmesettingsread "example.com"`

acmesettingswrite

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 Acmesettingswrite AcmeManaged: "Manual"`**

`xCommand Acmesettingswrite AcmeManaged: "Automated" Domain: "example.com" RenewalSchedule: "{"DaysOfWeek": ["Mon"],"TimeOfDay":"04:00"}" RenewKey: "Rotate"`

acmesign

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 Acmesign`**

`xcommand Acmesign Domain:"example.com"`

AdminAccountAdd

Adds a local administrator account.

Name(r): <S: 0, 128>

The username for this account.

Password(r): <Password>

The password for this account.

AccessAPI: <On/Off>

Whether this account is allowed to access the system's status and configuration via the API. Default: On.

AccessWeb: <On/Off>

Whether this account is allowed to log in to the system using the web interface. Default: On.

Enabled: <On/Off>

Indicates if the account is enabled or disabled. Access is denied to disabled accounts. Default: On.

Example: `xCommand AdminAccountAdd Name: "bob_smith" Password: "abcXYZ_123" AccessAPI: On AccessWeb: On Enabled: On`

AdminAccountDelete

Deletes a local administrator account.

Name(r): <S: 0, 128>

The username of the account to delete.

Example: `xCommand AdminAccountDelete: "bob_smith"`

AdminGroupAdd

Name(r): <S: 0, 128>

The name of the administrator group.

AccessAPI: <On/Off>

Whether members of this group are allowed to access the system's status and configuration using the API. Default: On.

AccessWeb: <On/Off>

Whether members of this group are allowed to log in to the system using the web interface. Default: On.

Enabled: <On/Off>

Indicates if the group is enabled or disabled. Access is denied to members of disabled groups. Default: On.

Example: `xCommand AdminGroupAdd Name: "administrators" AccessAPI: On AccessWeb: On Enabled: On`

AdminGroupDelete

Deletes an administrator group.

Name(r): <S: 0, 128>

The name of the group to delete.

Example: `xCommand AdminGroupDelete: "administrators"`

AdsDcAdd

Adds a new Active Directory server.

ActiveDirectoryAddress(r): <S: 0,39>

The address of a domain controller that can be used when the VCS joins the AD domain. Not specifying a specific AD will result the use of DNS SRV queries to find an AD.

Example: `xCommand AdsDcAdd ActiveDirectoryAddress: "192.168.0.0"`

AdsDcDelete

Deletes an Active Directory server.

ActiveDirectoryId(r): <1..5>

The index of the Active Directory server to be deleted.

Example: `xCommand AdsDcDelete ActiveDirectoryId: 1`

AdsKdcAdd

Adds a new Kerberos KDC.

KerberosKDCAddress(r): <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.

KerberosKDCPort: <1..65534>

Specifies the port of a KDC that can be used when the VCS joins the AD domain. Default: 88

Example: `xCommand AdsKdcAdd KerberosKDCAddress: "192.168.0.0" KerberosKDCPort: 88`

AdsKdcDelete

Deletes a configured Kerberos KDC.

KerberosKDCId(r): <1..5>

The index of the Kerberos KDC to be deleted.

Example: `xCommand AdsKdcDelete KerberosKDCId: 1`

AllowListAdd

Adds an entry to the Allow List.

PatternString(r): <S: 1, 60>

Specifies an entry to be added to the Allow List. If one of an endpoint's aliases matches one of the patterns in the Allow List, the registration will be permitted.

PatternType: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Allow List is a prefix, suffix, regular expression, or must be matched exactly. *Exact*: the string must match the alias character for character. *Prefix*: the string must appear at the beginning of the alias. *Suffix*: the string must appear at the end of the alias. *Regex*: the string will be treated as a regular expression.
Default: Exact.

Description: <S: 0,64>

A free-form description of the Allow List rule.

Example: `xCommand AllowListAdd PatternString: "John.Smith@example.com" PatternType: Exact Description: "Allow John Smith"`

AllowListDelete

Deletes an entry from the Allow List.

AllowListId(r): <1..2500>

The index of the entry to be deleted.

Example: `xCommand AllowListDelete AllowListId: 2`

Boot

Reboots the VCS.

This command has no parameters.

Example: `xCommand boot`

CheckBandwidth

A diagnostic tool that returns the status and route (as a list of nodes and links) that a call of the specified type and bandwidth would take between two nodes. Note that this command does not change any existing system configuration.

Node1(r): <S: 1, 50>

The subzone or zone from which the call originates.

Node2(r): <S: 1, 50>

The subzone or zone at which the call terminates.

Bandwidth(r): <1..100000000>

The requested bandwidth of the call (in kbps).

CallType(r): <Traversal/NonTraversal>

Whether the call type is Traversal or Non-traversal.

Example: `xCommand CheckBandwidth Node1: "DefaultSubzone" Node2: "UK Sales Office" Bandwidth: 512 CallType: nontraversal`

CheckPattern

A diagnostic tool that allows you to check the result of an alias transform (local or zone) before you configure it on the system.

Target(r): <S: 1, 60>

The alias you want to use to test the pattern match or transform.

Pattern(r): <S: 1, 60>

The pattern against which the alias is compared.

Type(r): <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the pattern behavior to be applied.

Behavior(r): <Strip/Leave/Replace/AddPrefix/AddSuffix>

How the alias is modified.

Replace: <S: 0, 60>

The text string to use in conjunction with the selected Pattern behavior.

Example: `xCommand CheckPattern Target: "bob@a.net" Pattern: "@a.net" Type: "suffix" Behavior: replace Replace: "@a.com"`

ClearAllStatus

Clears all status and history on the system.

Example: `xCommand ClearAllStatus`

ClusterAddressMappingAdd

Fqdn(r): <Value>

IpAddress(r): <Value>

Adds an FQDN/IP mapping entry to the cluster address mapping table.

ClusterAddressMappingDelete

Fqdn(r): <Value>

IpAddress(r): <Value>

Deletes an FQDN/IP mapping entry from the cluster address mapping table.

Cmsadd

Manage Cisco Meeting Server web bridges. Add a Guest account client URI

Name: <Value>

Example: `xCommand Cmsadd name: "join.example.com"`

Cmsdelete

Manage Cisco Meeting Server web bridges. Delete a Guest account client URI

Name: <Value>

Example: `xCommand Cmsdelete name: "join.example.com"`

CredentialAdd

Adds an entry to the local authentication database.

Name(r): <String>

Defines the name for this entry in the local authentication database.

Password(r): <Password>

Defines the password for this entry in the local authentication database.

The maximum plaintext length is 128 characters, which will then be encrypted.

Example: `xCommand CredentialAdd Name: "alice" Password: "abcXYZ_123"`

CredentialDelete

Deletes an entry from the local authentication database.

Name(r): <String>

The name of the entry to delete.

Example: `xCommand CredentialDelete Name: "alice"`

Cucmconfigadd

Performs a lookup on a Unified CM publisher.

Address(r): <Value>

The FQDN or IP address of the Unified CM publisher.

Axlpassword(r): <Value>

The password used by the VCS to access the Unified CM publisher.

Axlusername(r): <Value>

The user name used by the VCS to access the Unified CM publisher.

CertValidationDisabled: <On/Off>

Controls X.509 certificate checking against the certificate presented by the Unified CM publisher. Default: On

Example: `xCommand Cucmconfigadd Address: "cucm.example.com" Axlpassword: "xyz" Axlusername: "abc"`

Cucmconfigdelete

Deletes the details of a Unified CM publisher.

Address(r): <Value>

The FQDN or IP address of the Unified CM publisher.

Example: `xCommand Cucmconfigdelete Address: "cucm.example.com"`

Cucmmixedmodecheck

Address(r): <Value>

The FQDN or IP address of the Unified CM publisher.

Axlpassword(r): <Value>

The password used by the VCS to access the Unified CM publisher.

Axlusername(r): <Value>

The user name used by the VCS to access the Unified CM publisher.

DefaultLinksAdd

Restores links between the Default Subzone, Traversal Subzone and the Default Zone.

This command has no parameters.

Example: `xCommand DefaultLinksAdd`

DefaultValuesSet

Resets system parameters to default values. Level 1 resets most configuration items to their default value, with the exception of the Level 2 and Level 3 items. Level 2 resets configuration items related to remote authentication, plus Level 1 items to their default value. Level 3 resets all critical configuration items, plus Level 1 and Level 2 items to their default value.

Level(r): <1..3>

The level of system parameters to be reset.

Example: `xCommand DefaultValuesSet Level: 1`

DenyListAdd

Adds an entry to the Deny List.

PatternString(r): <S: 1, 60>

Specifies an entry to be added to the Deny List. If one of an endpoint's aliases matches one of the patterns in the Deny List, the registration will not be permitted.

PatternType: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Deny List is a prefix, suffix, regular expression, or must be matched exactly. *Exact*: the string must match the alias character for character. *Prefix*: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. *Regex*: the string will be treated as a regular expression.
Default: Exact.

Description: <S: 0, 64>

A free-form description of the Deny List rule.

Example: `xCommand DenyListAdd PatternString: "sally.jones@example.com" PatternType: exact Description: "Deny Sally Jones"`

DenyListDelete

Deletes an entry from the Deny List.

DenyListId(r): <1..2500>

The index of the entry to be deleted.

Example: `xCommand DenyListDelete DenyListId: 2`

DisconnectCall

Disconnects a call.

Call: <1..1000>

The index of the call to be disconnected.

CallSerialNumber: <S: 1, 255>

The serial number of the call to be disconnected. You must specify either a call index or a call serial number.

Example: `xCommand DisconnectCall CallSerialNumber: "6d843434-211c-11b2-b35d-0010f30f521c"`

Dnslookup

Queries DNS for a supplied hostname.

Hostname: <Value>

The name of the host you want to query.

RecordType: <all/a/aaaa/srv/naptr>

The type of record you want to search for. If not specified, all record types are returned.

Example: `xCommand Dnslookup Hostname: "example.com" RecordType: all`

DNSPerDomainServerAdd

Adds a DNS server to use only for resolving hostnames for specific domains.

Address(r): <Value>

The IP address of the DNS server to use when resolving hostnames for the associated domain names.

Domain1(r): <Value>

The domain to associate with the specific DNS server.

Domain2(r): <Value>

An optional second domain to associate with the specific DNS server.

Index: <0..5>

The index of the server to add.

Example: `xCommand DNSServerAdd Address: "192.168.12.0" Index: 1`

DNSPerDomainServerDelete

Deletes a DNS server used for resolving hostnames for a specific domain.

Address: <Value>

The IP address of the DNS server to delete.

Example: `xCommand DNSPerDomainServerDelete Address: "192.168.12.0"`

DNSServerAdd

Adds a default DNS server. Default servers are used if there is no per-domain DNS server defined for the domain being looked up.

Address(r): <Value>

The IP address of a default DNS server to use when resolving domain names.

Index: <0..5>

The index of the server to add.

Example: `xCommand DNSServerAdd Address: "192.168.12.0" Index: 1`

DNSServerDelete

Deletes a DNS server

Address: <Value>

The IP address of the DNS server to delete.

Example: `xCommand DNSServerDelete Address: "192.168.12.0"`

DomainAdd

Adds a domain for which this VCS 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.

Authzone: <S: 1, 128>

The name of the traversal zone to use when delegating credential checks for SIP messages for this domain. Leave this parameter unspecified if you want this VCS Expressway to perform the credential checking.

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 VCS is authoritative for this domain. The VCS 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 DomainAdd Name: "100.example-name.com" Authzone: "Traversal zone" Edge: Off Sip: On`

DomainDelete

Deletes a domain.

DomainId(r): <1..200>

The index of the domain to be deleted.

Example: `xCommand DomainDelete DomainId: 2`

Domaincerts

Manage multidomain certificates for Server Name Indication (SNI).

Each Domaincerts xCommand requires a 'command' parameter specifying an operation to be performed, followed by any additional parameters required for the specific command.

Domaincerts commands and associated parameters:

domain_list: Lists domains for which certificates are managed for SNI.

parameters: (none)

Example: `xCommand Domaincerts command: domain_list`

domain_create: Creates a new domain for managing certificates for SNI.

parameters: domain

Example: `xCommand domaincerts command: domain_create domain: a.com`

domain_delete: Deletes the specified certificate domain.

parameters: domain

Example: `xCommand domaincerts command: domain_delete domain: a.com`

is_csr_pending: Returns true if a certificate signing request is pending for the domain.

parameters: domain

Example: `xCommand domaincerts command: is_csr_pending domain: a.com`

csr_create: Creates a certificate signing request for a domain.

parameters: domain, subjectfields, sans, digestalgorithm, keysize

Example: `xCommand domaincerts command: csr_create domain: a.com keysize: 4096 digestalgorithm: sha256 sans: 'DNS:host1.a.com, DNS:host2.a.com' subjectfields: '{ "CN": "www.a.com", "C": "US", "ST": "North Carolina", "L": "RTP", "O": "a", "OU": "example org unit", "emailAddress": "admin@a.com" }'`

Notes:

- xCommand parameter values can be contained in single quotes so that space can be included.
- sans is an optional, comma-separated list of hostnames, each hostname prefixed by 'DNS:', see RFC5280.
- subjectfields is a JSON object containing a list of name: value pairs for each Subject Name field, see RFC5280.
- JSON names and values must be contained in double quotes as shown.
- keysize is the length in bits of the private key generated for the CSR.
- digestalgorithm is the name of the message digest algorithm used to sign the CSR, see 'openssl dgst'.

csr_get: Returns a pending certificate signing request in PEM format.

parameters: domain

Example: `xCommand domaincerts command: csr_get domain: a.com`

csr_delete: Deletes a pending certificate signing request.

parameters: domain

Example: `xCommand domaincerts command: csr_delete domain: a.com`

is_cert_set: Returns true if a certificate has been set for the domain.

parameters: domain

Example: **`xCommand domaincerts command: is_cert_set domain: a.com`**

cert_put: Uploads a certificate and private key.

parameters: domain, certpath, keypath

Example: **`xCommand domaincerts command: cert_put domain: a.com certpath: /tmp/cert.pem keypath: /tmp/key.pem`**

Notes:

- When a certificate and key have not been uploaded yet, both must be specified.
- When a certificate signing request is in progress, only a certificate can be uploaded.

cert_get: Returns a domain's certificate in PEM format.

parameters: domain

Example: **`xCommand domaincerts command: cert_get domain: a.com`**

cert_delete: Deletes a domain's certificate and private key.

parameters: domain

Example: **`xCommand domaincerts command: cert_delete domain: a.com`**

default command help:"

Certpath: <String>

Command: <domain_list/domain_create/domain_delete/csr_create/csr_get/csr_delete/cert_put/cert_get/cert_delete/is_csr_pending/is_cert_set>

Digestalgorithm: </sha256/sha384/sha512>

Domain: <String>

Keypath: <String>

Keysize: <Value>

Sans: <String>

Subjectfields: <String>

Edgessodeletetokens

Deletes all tokens issued to a particular user.

Username(r): <String>

Specifes which user's tokens will be deleted.

Example: **`xCommand Edgessodeletetokens Username: "APerson"`**

Edgessopurgetokens

Deletes all tokens issued to all users.

Example: **`xCommand Edgessopurgetokens`**

Edgessostatusclear

Resets the SSO request/response counters to 0.

Example: `xCommand Edgessostatusclear`

ExtAppStatusAdd

Allows another application running on the VCS to attach xstatus to the VCS XML xstatus tree.

Note: this command is intended for developer use only.

Name(r): <S:1, 64>

Descriptive name for the external application whose status is being referenced.

Filename(r): <S:0, 255>

XML file containing status that is to be attached for an external application.

Example: `xCommand ExtAppStatusAdd Name: "foo" Filename: "foo.xml"`

ExtAppStatusDelete

Deletes an external application status entry.

Note: this command is intended for developer use only.

Name(r): <S:1, 64>

Descriptive name for the external application whose status is being referenced.

Example: `xCommand ExtAppStatusDelete Name: foo`

Fail2banExemptionAdd

Adds an automated intrusion protection exemption.

Address(r): <String>

The IP address / range that is exempted from Fail2ban intrusion protection.

Jail(r): <ssh-auth/sshpfwd-auth/web-auth/apache-auth/snmp-auth/http-ce-auth/xmpp-intrusion/http-ce-intrusion/http-ce-resource_access/ssh-intrusion/sshpfwd-intrusion/web-intrusion/snmp-intrusion/sip-auth/sip-reg/sip-calls/sip-violations/h323-auth/h323-adm/h323-calls/h323-violations/generic-tcp-intrusion/generic-udp-intrusion>

The exempted categories for the corresponding address range

Example: `xCommand Fail2banExemptionAdd Address: "192.0.0.18/32" Jail: "ssh-auth"`

Fail2banExemptionDelete

Removes an automated intrusion protection exemption.

Address(r): <String>

The IP address / range that is exempted from Fail2ban intrusion protection.

Jail(r): <ssh-auth/sshpfwd-auth/web-auth/apache-auth/snmp-auth/http-ce-auth/xmpp-intrusion/http-ce-intrusion/http-ce-resource_access/ssh-intrusion/sshpfwd-intrusion/web-intrusion/snmp-intrusion/sip-auth/sip-reg/sip-calls/sip-violations/h323-auth/h323-adm/h323-calls/h323-violations/generic-tcp-intrusion/generic-udp-intrusion>

The exempted categories for the corresponding address range

Example: `xCommand Fail2banExemptionDelete Address: "192.0.0.18/32" Jail: "ssh-auth"`

FeedbackDeregister

Deactivates a particular feedback request.

ID: <1..3>

The index of the feedback request to be deactivated.

Example: `xCommand FeedbackDeregister ID: 1`

FeedbackRegister

Activates notifications on the event or status changes described by the expressions. Notifications are sent in XML format to the specified URL. Up to 15 expressions may be registered for each of 3 feedback IDs.

ID: <1..3>

The ID of this particular feedback request.

URL(r): <S: 1, 256>

The URL to which notifications are to be sent.

Expression.1..15: <S: 1, 256>

The events or status change to be notified. Valid Expressions are:

`Status/Ethernet`	`Status/Calls`	`Event/CallDisconnected`
`Event/`	`Status/NTP`	`Status/Registrations`
`Event/CallFailure`	`Event/Bandwidth`	`Status/LDAP`
`Status/Zones`	`Event/RegistrationAdded`	`Event/Locate`
`Status/Feedback`	`Event/CallAttempt`	`Event/RegistrationRemoved`
`Event/ResourceUsage`	`Status/ExternalManager`	`Event/CallConnected`
`Event/RegistrationFailure`	`Event/AuthenticationFailure`	

Example: `xCommand FeedbackRegister ID: 1 URL: "http://192.168.0.1/feedback/" Expression.1: "Status/Calls" Expression.2: "Event/CallAttempt"`

FindRegistration

Returns information about the registration associated with the specified alias. The alias must be registered on the VCS on which the command is issued.

Alias(r): <S: 1, 60>

The alias that you wish to find out about.

Example: `xCommand FindRegistration Alias: "john.smith@example.com"`

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`

ForceConfigUpdate

Forces the relevant configuration on this peer to be updated to match that of the cluster primary.

This command has no parameters.

Example: `xCommand ForceConfigUpdate`

Httpallowlistexport

Export the HTTP allow list rules in CSV format from the database.

File: <S>

Specifies the path to a file where the rules will get exported in CSV format.

Deployment: <S>

Use with URL to specify which of your deployments uses this rule. Not required unless you have multiple deployments. If you have multiple deployments, the rule will use the default deployment if you don't specify the deployment.

Httpallowlistexporttest

Export the HTTP allow list tests in CSV format from the database.

File: <S>

Specifies the path to a file where the tests will get exported in CSV format.

Deployment: <S>

Use with URL to specify which of your deployments uses this test. Not required unless you have multiple deployments. If you have multiple deployments, the rule will use the default deployment if you don't specify the deployment.

HTTPAllowListRuleAdd

Adds one or more rules to the HTTP allow list. You must specify at least URL or URLFile.

URL(r): <S>

Specifies the URL of a resource that HTTP clients will be allowed to access. IPv6 addresses must use RFC 2732 format.

For example: **`https://[2001:DB8::1]:8443/path`** or **`https://www.example.com:8443/resource`**

Do not supply URL if you are supplying URLFile.

URL must contain the protocol, either **`http://`** or **`https://`**, and the hostname. It should also contain domain, port, and path to make the URL more specific. If you omit some portions of the URL, VCS will supply its defaults. eg. **`http://hostname`** allows clients to access to everything included by **`http://hostname.SystemDNSDomain:80`**. The default ports are 80 for http and 443 for https.

URLFile(r): <S>

Specifies the path to a CSV file that contains multiple rules. See Allow List Rules File Reference, page 392.

Do not supply URLFile if you are supplying URL.

MatchType: <exact/starts-with/startswith/prefix>

Use with URL to specify whether the rule matches exactly what is in URL, or uses it as a base for a prefix match. Defaults to **`exact`** if not supplied. The other options are all equivalent.

Deployment: <S: "Your Deployment 1"/"Your Deployment 2">

Use with URL to specify which of your deployments uses this rule. Not required unless you have multiple deployments. If you have multiple deployments, the rule will use the default deployment if you don't specify the deployment.

Description: <S:128>

A text description of the rule.

HttpMethods: <OPTIONS/GET/HEAD/POST/PUT/DELETE>

A comma-delimited set of methods to allow with this rule. If you do not specify the methods, the rule will use the default methods configured on **Configuration > Unified Communications > HTTP allow list > Editable inbound rules**.

Example 1: **`xCommand HTTPAllowListRuleAdd URLfile: "/tmp/rules.csv"`**

Example 2: **`xCommand HTTPAllowListRuleAdd URL: "https://cucm2.example.com:8443/partial/path" MatchType: starts-with Description: "https access to read everything below partial/path/ on cucm2.example.com" HttpMethods: "OPTIONS,GET"`**

HTTPAllowListRuleDelete

Deletes one or more rules from the HTTP allow list. You must specify at least URL or URLFile. You may need to specify other parameters if you have multiple rules for a single host.

URL(r): <S>

Specifies the URL of the rule you are deleting.

Do not supply URL if you are supplying URLFile.

URL must contain the protocol, either **`http://`** or **`https://`**, and the hostname. It should also contain domain, port, and path to make the URL more specific. If you omit some portions of the URL, VCS will supply its defaults. eg. **`http://hostname`** will delete the rule **`http://hostname.SystemDNSDomain:80`**. The default ports are 80 for http and 443 for https.

URLFile(r): <S>

Specifies the path to a CSV file that contains multiple rules that you want to delete.

Do not supply URLFile if you are supplying URL.

MatchType: <exact/starts-with/startswith/prefix>

Use with URL to specify whether the rule matches exactly what is in URL, or uses it as a base for a prefix match. Defaults to **`exact`** if not supplied. The other options are all equivalent.

Deployment: <S>

Use with URL to specify which of your deployments uses this rule. Not required unless you have multiple deployments. If you have multiple deployments, the rule will use the default deployment if you don't specify the deployment.

Description: <S:128>

A text description of the rule.

HttpMethods: <OPTIONS/GET/HEAD/POST/PUT/DELETE>

A comma-delimited set of methods to allow with this rule. If you do not specify the methods, the rule will use the default methods configured on **Configuration > Unified Communications > HTTP allow list > Editable inbound rules**.

Example 1: **`xCommand HTTPAllowListRuleDelete URLfile: "/tmp/rules.csv"`**

Example 2: **`xCommand HTTPAllowListRuleDelete URL: "https://cucm2.example.com:8443/partial/path" MatchType: starts-with Description: "https access to read everything below partial/path/ on cucm2.example.com" HttpMethods: "OPTIONS,GET"`**

HTTPAllowListRulesTest

(Experimental)

Tests a collection of URLs (defined in a CSV file) against a list of rules (defined in a CSV file). This enables you to test rules before you apply them, or to test that existing rules are working as expected.

You can provide either the tests, or the rules, or both, as CSV files. If you provide both, the tests in the Tests CSV file are run against the rules in the Rules CSV file. If you omit one or both parameters, this command uses the rules or tests (or both) that are already on the VCS. (Use **`xstatus collaborationedge httpallowlist`** to see the current rules).

Tests: <S>

Specifies the path to a CSV file that contains multiple tests, eg. **`/tmp/tests.csv`**. See Allow List Tests File Reference, page 393.

Rules: <S>

Specifies the path to a CSV file that contains multiple rules you want to test, eg. **`/tmp/rules.csv`**. See Allow List Rules File Reference, page 392.

Example : **`xCommand HTTPAllowListRulesTest Tests: "/tmp/tests.csv" Rules: "/tmp/rules.csv"`**

HTTPAllowListTestAdd

(Experimental)

Adds one or more URLs to test against the HTTP allow list. You must specify at least URL or URLFile; if you specify URL, you must specify ExpectedResult.

URL(r): <S>

Specifies the test URL. IPv6 addresses must use RFC 2732 format.

For example: **`https://[2001:DB8::1]:8443/path`** or **`https://www.example.com:8443/resource`**

Do not supply URL if you are supplying URLFile.

URL must contain the protocol, either **`http://`** or **`https://`**, and the hostname. It should also contain domain, port, and path to make the URL more specific. If you omit some portions of the URL, VCS will supply its defaults. eg. **`http://hostname`** tests the URL **`http://hostname.SystemDNSDomain:80`**. The default ports are 80 for http and 443 for https.

URLFile(r): <S>

Specifies the path to a CSV file that contains multiple tests. See Allow List Tests File Reference, page 393.

Do not supply URLFile if you are supplying URL.

ExpectedResult(r): <allow/block>

Required with URL to specify whether the URL should be allowed or blocked by the allow list.

Deployment: <S>

Use with URL to specify which of your deployments uses this test. Not required unless you have multiple deployments. If you have multiple deployments, the test will use the default deployment unless you specify the deployment.

Description: <S:128>

A text description of the test.

HttpMethod: <OPTIONS/GET/HEAD/POST/PUT/DELETE>

Specify one method to test. If you do not specify the method, the test will use GET.

Example 1: **`xCommand HTTPAllowListTestAdd URLfile: "/tmp/tests.csv"`**

Example 2: **`xCommand MRAAllowListTestAdd URL: "https://cucm2.example.com:8443/partial/path"`**
`ExpectedResult: block Description: "https access to write to partial/path/ on cucm2.example.com"`
`HttpMethod: "POST"`

HTTPAllowListTestDelete

(Experimental)

Deletes one or more test URLs from the HTTP allow list. You must specify at least URL or URLFile; if you specify URL, you must specify ExpectedResult.

URL(r): <S>

Specifies the test URL you are deleting.

Do not supply URL if you are supplying URLFile.

URLFile(r): <S>

Specifies the path to a CSV file that contains multiple tests you want to delete.

Do not supply URLFile if you are supplying URL.

ExpectedResult(r): <allow/block>

Specify the result expected by the test you are deleting. Required for deleting the test.

Deployment: <S>

Specify which deployment use the test you are deleting. Not required unless you have multiple deployments.

Description: <S:128>

A text description of the test. Not required for deleting the test unless you have multiple tests that cannot otherwise be distinguished from each other.

HttpMethod: <OPTIONS/GET/HEAD/POST/PUT/DELETE>

Specify which method is used in the test you are deleting. If you omit the methods, the VCS uses the current default methods with this command. This means the delete could fail unless the test was created with the corresponding methods.

Example 1: `xCommand HTTPAllowListTestDelete URLfile: "/tmp/tests.csv"`

Example 2: `xCommand HTTPAllowListTestDelete URL: "https://cucm2.example.com:8443/partial/path" ExpectedResult: allow HttpMethod: "get"`

HTTPProxyJabberCTargetsAdd

Configures a Jabber Guest Server and associates it with a Jabber Guest domain.

DomainIndex(r): <0..200>

Index of the domain with which this Jabber Guest Server is associated

Host(r): <S:1,1024>

The FQDN of a Jabber Guest Server to use for the selected domain. This must be an FQDN, not an unqualified hostname or an IP address.

Note that you can specify alternative addresses for the same domain, each with different priorities.

Priority: <0..9>

The order in which connections to this hostname are attempted for this domain. All priority 1 hostnames for the domain are attempted first, followed by all priority 2 hostnames, and so on.

Example: `xCommand HTTPProxyJabberCTargetsAdd DomainIndex: 2 Host: jabberguest.example.com`

HTTPProxyJabberCTargetsDelete

Deletes the configured Jabber Guest Server from the VCS.

Host(r): <S:1,1024> The FQDN of the Jabber Guest Server to delete.

IMPServerAdd

Adds an external messaging server to which to route Microsoft SIP Simple messages.

IMP(r): <Value> configuration/b2bua/imp/imp

IMPServerDelete

Deletes an external messaging server.

IMP(r): <Value> configuration/b2bua/imp/imp

LinkAdd

Adds and configures a new link.

LinkName(r): <S: 1, 50>

Assigns a name to this link.

Node1: <S: 1, 50>

Specifies the first zone or subzone to which this link will be applied.

Node2: <S: 1, 50>

Specifies the second zone or subzone to which this link will be applied.

Pipe1: <S: 1, 50>

Specifies the first pipe to be associated with this link.

Pipe2: <S: 1, 50>

Specifies the second pipe to be associated with this link.

Example: `xCommand LinkAdd LinkName: "Subzone1 to UK" Node1: "Subzone1" Node2: "UK Sales Office" Pipe1: "512Kb ASDL"`

LinkDelete

Deletes a link.

LinkId(r): <1..3000>

The index of the link to be deleted.

Example: `xCommand LinkDelete LinkId: 2`

ListPresentities

Returns a list of all the presentities being watched by a particular subscriber.

Subscriber(r): <S:1, 255>

The URI of the subscriber who is watching.

Example: `xCommand ListPresentities Subscriber: "john.smith@example.com"`

ListSubscribers

Returns a list of all subscribers who are watching for the presence information of a particular presentity.

Presentity(r): <S:1, 255>

The URI of the presentity being watched.

Example: `xCommand ListSubscribers Presentity: "mary.jones@example.com"`

Locate

Runs the VCS's location algorithm to locate the endpoint identified by the given alias, searching locally, on neighbors, and on systems discovered through the DNS system, within the specified number of 'hops'. Results are reported back through the xFeedback mechanism, which must therefore be activated before issuing this command (e.g. xFeedback register event/locate).

Alias(r): <S: 1, 60>

The alias associated with the endpoint you wish to locate.

HopCount(r): <0..255>

The hop count to be used in the search.

Protocol(r): <H323/SIP>

The protocol used to initiate the search.

SourceZone: <S: 1, 50>

The zone from which to simulate the search request. Choose from the Default Zone (an unknown remote system), the Local Zone (a locally registered endpoint) or any other configured neighbor, traversal client or traversal server zone.

Authenticated: <Yes/No>

Whether the search request should be treated as authenticated or not.

SourceAlias: <S: 0, 60>

The source alias to be used for the search request. Default: xcom-locate

Example: `xCommand Locate Alias: "john.smith@example.com" HopCount: 15 Protocol: SIP SourceZone: LocalZone Authenticated: Yes SourceAlias: alice@example.com`

Networkinterface

Controls whether the LAN 2 port is enabled for management and call signaling.

DualInterfaces(r): <enable/disable/status>

Sets or reports on the current status of the the LAN 2 port.

Example: `xCommand Networkinterface DualInterfaces: enable`

Networklimits

Controls the experimental rate limiting feature. Enter `xcom networklimits ?` to read the help.

NTPServerAdd

Adds an NTP server to be used when synchronizing system time.

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the NTP server to add.

Example: `xCommand NTPServerAdd Address: "ntp.server.example.com"`

NTPServerDelete

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the NTP server to delete.

Example: `xCommand NTPServerDelete Address: "ntp.server.example.com"`

OptionKeyAdd

Adds a new option key to the VCS. These are added to the VCS in order to add extra functionality, such as increasing the VCS's capacity. Contact your Cisco representative for further information.

Key(r): <S: 0, 90>

Specifies the option key of your software option.

Example: `xCommand OptionKeyAdd Key: "1X4757T5-1-60BAD5CD"`

OptionKeyDelete

Deletes a software option key from the VCS.

OptionKeyId(r): <1..64>

Specifies the ID of the software option to be deleted.

Example: `xCommand OptionKeyDelete OptionKeyId: 2`

Ping

Checks that a particular host system is contactable.

Hostname: <Value>

The IP address or hostname of the host system you want to try to contact.

Example: `xCommand Ping Hostname: "example.com"`

PipeAdd

Adds and configures a new pipe.

PipeName(r): <S: 1, 50>

Assigns a name to this pipe.

TotalMode: <Unlimited/Limited/NoBandwidth>

Controls total bandwidth restrictions for the pipe. *NoBandwidth*: no calls can be made using this pipe. Default: Unlimited.

Total: <1..100000000>

If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe. Default: 500000.

PerCallMode: <Unlimited/Limited/NoBandwidth>

Controls bandwidth restrictions of individual calls. *NoBandwidth*: no calls can be made using this pipe. Default: Unlimited.

PerCall: <1..100000000> For limited per-call mode, sets the maximum bandwidth (in kbps) available per call. Default: 1920.

Example: **`xCommand PipeAdd PipeName: "512k ADSL" TotalMode: Limited Total: 512 PerCallMode: Limited PerCall: 128`**

PipeDelete

Deletes a pipe.

PipeId(r): <1..1000>

The index of the pipe to be deleted.

Example: **`xCommand PipeDelete PipeId: 2`**

PolicyServiceAdd

Adds a policy service.

Name(r): <S: 0, 50>

Assigns a name to this Policy Service.

Description: <S: 0, 64>

A free-form description of the Policy Service.

Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote service. Default: HTTPS

Verify: <On/Off>

Controls X.509 certificate checking and mutual authentication between this VCS 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 VCS to log in and query the remote service.

Password: <S: 0, 82>

The password used by the VCS to log in and query the remote service. The maximum plaintext length is 30 characters.

DefaultCPL: <S: 0, 255>

The CPL used when the remote service is unavailable. Default: <reject status='403' reason='Service Unavailable'/>

Example: `xCommand PolicyServiceAdd Name: "Conference" Description: "Conference service" Protocol: HTTPS Verify: On CRLCheck: On Address: "service.example.com" Path: "service" StatusPath: "status" UserName: "user123" Password: "password123" DefaultCPL: "<reject status='403' reason='Service Unavailable'/>"`

PolicyServiceDelete

Deletes a policy service.

PolicyServiceId(r): <1..20>

The index of the policy service to be deleted.

Example: `xCommand PolicyServiceDelete PolicyServiceId: 1`

RemoteSyslogAdd

Adds the address of a remote syslog server.

Address(r): <Value>

The IP address or FQDN of the remote syslog server.

CrlCheck: <On/Off>

Controls whether the certificate supplied by the syslog server is checked against the certificate revocation list (CRL). Default : Off

Format: <bsd/ietf>

The format in which remote syslog messages are written. Default : bsd

Loglevel: <emergency/alert/critical/error/warning/notice/informational/debug>

The minimum severity of log messages to send to this syslog server. Default: informational.

Mode: <bsd/ietf/ietf_secure/user_defined>

The syslog protocol to use when sending messages to the syslog server. Default: bsd.

Port: <1..65535>

The UDP/TCP destination port to use. Suggested ports: UDP=514 TCP/TLS=6514 Default : 514

Transport: <udp/tcp/tls>

The transport protocol to use when communicating with the syslog server. Default: udp

Example: `xCommand RemoteSyslogAdd Address: "remote_server.example.com" Crlcheck: Off Format: bsd Loglevel: warning Mode: bsd Port: 514 Transport: udp`

RemoteSyslogDelete

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the remote syslog server to delete.

Port(r): <1..65535>

The port used by the remote syslog server to be deleted.

Transport(r): <udp/tcp/tls>

The transport protocol used by the remote syslog server to be deleted.

Example: `xCommand RemoteSyslogDelete Address: "remote_server.example.com" Port: 514 Transport: udp`

RemoveRegistration

Removes a registration from the VCS.

Registration: <1..3750>

The index of the registration to be removed.

RegistrationSerialNumber: <S: 1, 255>

The serial number of the registration to be removed.

Example: `xCommand RemoveRegistration RegistrationSerialNumber: "a761c4bc-25c9-11b2-a37f-0010f30f521c"`

Restart

Restarts the VCS without a full system reboot.

This command has no parameters.

Example: `xCommand Restart`

RouteAdd

Adds and configures a new IP route (also known as a static route).

Address(r): <S: 1, 39>

Specifies an IP address used in conjunction with the prefix length to determine the network to which this route applies. Default: 32

PrefixLength(r): <1..128>

Specifies the number of bits of the IP address which must match when determining the network to which this route applies.

Gateway(r): <S: 1, 39>

Specifies the IP address of the gateway for this route.

Interface: <Auto/LAN1/LAN2>

The LAN interface to use for this route. *Auto*: the VCS will select the most appropriate interface to use. Default: Auto

Example: `xCommand RouteAdd Address: "10.13.8.0" PrefixLength: 32 Gateway: "192.44.0.1"`

RouteDelete

Deletes a route.

RouteId(r): <1..50>

The index of the route to be deleted.

Example: `xCommand RouteDelete RouteId: 1`

Securemode

Controls Advanced Account Security options.

Command(r): <on/off/status>

The index of the route to be deleted.

Example: `xCommand Securemode Command: off`

SearchRuleAdd

Adds a new search rule to route searches and calls toward a zone or policy service.

Name(r): <S: 0, 50>

Descriptive name for the search rule.

ZoneName: <S: 0, 50>

The zone or policy service to query if the alias matches the search rule.

Description: <S: 0, 64>

A free-form description of the search rule.

Example: `xCommand SearchRuleAdd Name: "DNS lookup" ZoneName: "Sales Office" Description: "Send query to the DNS zone"`

SearchRuleDelete

Deletes a search rule.

SearchRuleId(r): <1..2000>

The index of the search rule to be deleted.

Example: `xCommand SearchRuleDelete SearchRuleId: 1`

SIPRouteAdd

Adds a route that will cause SIP messages matching the given criteria to be forwarded to the specified IP address and port.

Note: this command is intended for developer use only.

Method(r): <S:0, 64>

SIP method to match to select this route (e.g. INVITE, SUBSCRIBE).

RequestLinePattern(r): <S:0, 128>

Regular expression to match against the SIP request line.

HeaderName(r): <S:0, 64>

Name of SIP header field to match (e.g. Event).

HeaderPattern(r): <S:0, 128>

Regular expression to match against the specified SIP header field.

Authenticated(r): <On/Off>

Whether to forward authenticated requests. *On*: only forward requests along route if incoming message has been authenticated. *Off*: always forward messages that match this route. Default: Off

Address(r): <S:0, 39>

Specifies the IP address of the next hop for this route, where matching SIP requests will be forwarded.

Port(r): <1..65534>

Specifies the port on the next hop for this route to which matching SIP requests will be routed. Default: 5060

Transport(r): <UDP/TCP/TLS>

Determines which transport type will be used for SIP messages forwarded along this route.

Tag(r): <S:0, 64>

Tag value specified by external applications to identify routes that they create.

Example: `xCommand SIPRouteAdd Method: "SUBSCRIBE" RequestLinePattern: ".*@(%localdomains%|%ip%)" HeaderName: "Event" HeaderPattern: "(my-event-package)(.*)" Authenticated: On Address: "127.0.0.1" Port: 22400 Transport: TCP Tag: "Tag1"`

SIPRouteDelete

Deletes an existing SIP route, identified either by the specified index or tag.

Note: this command is intended for developer use only.

SipRouteId: <1..20>

The index of the SIP route to be deleted.

Tag: <S:0, 64>

Tag value specified by external applications to uniquely identify routes that they create.

Example: `xCommand SIPRouteDelete SipRouteId: Tag: "Tag1"`

SubZoneAdd

Adds and configures a new subzone.

SubZoneName(r): <S: 1, 50>

Assigns a name to this subzone.

TotalMode: <Unlimited/Limited/NoBandwidth>

Determines whether this subzone has a limit on the total bandwidth of calls being used by its endpoints at any one time. *NoBandwidth*: no bandwidth available. No calls can be made to, from, or within this subzone. Default: Unlimited.

Total: <1..100000000>

Sets the total bandwidth limit (in kbps) of this subzone (applies only if the mode is set to *Limited*). Default: 500000.

PerCallInterMode: <Unlimited/Limited/NoBandwidth>

Sets bandwidth limits for any one call to or from an endpoint in this subzone. *NoBandwidth*: no bandwidth available. No calls can be made to or from this subzone. Default: Unlimited.

PerCallInter: <1..100000000>

Specifies the bandwidth limit (in kbps) on any one call to or from an endpoint in this subzone (applies only if the mode is set to *Limited*). Default: 1920.

PerCallIntraMode: <Unlimited/Limited/NoBandwidth>

Sets bandwidth limits for any one call between two endpoints within this subzone. *NoBandwidth*: no bandwidth available. No calls can be made within this subzone. Default: Unlimited.

PerCallIntra: <1..100000000>

Specifies 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: `xCommand SubZoneAdd SubZoneName: "BranchOffice" TotalMode: Limited Total: 1024 PerCallInterMode: Limited PerCallInter: 512 PerCallIntraMode: Limited PerCallIntra: 512`

SubZoneDelete

Deletes a subzone.

SubZoneId(r): <1..1000>

The index of the subzone to be deleted.

Example: `xCommand SubZoneDelete SubZoneId: 2`

SubZoneMembershipRuleAdd

Adds and configures a new membership rule.

Name(r): <S: 1, 50>

Assigns a name to this membership rule.

Type(r): <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. *Alias Pattern Match*: assigns the device if its alias matches the configured pattern.

SubZoneName(r): <S: 1, 50>

The subzone to which an endpoint is assigned if its address satisfies this rule.

Description: <S: 0, 64>

A free-form description of the membership rule.

Example: `xCommand SubZoneMembershipRuleAdd Name: "Home Workers" Type: Subnet SubZoneName: "Home Workers" Description: "Staff working at home"`

SubZoneMembershipRuleDelete

Deletes a membership rule.

SubZoneMembershipRuleId(r): <1..3000>

The index of the membership rule to be deleted.

Example: `xCommand SubZoneMembershipRuleDelete SubZoneMembershipRuleId: 1`

Tracepath

Discover the path taken by a network packet sent to a particular destination host system.

Hostname: <Value>

The IP address or hostname of the host system to which you want to trace the path.

Example: `xCommand Tracepath Hostname: "example.com"`

Traceroute

Discover the route taken by a network packet sent to a particular destination host system. It reports the details of each router along the path, and the time taken for each router to respond to the request.

Hostname: <Value>

The IP address or hostname of the host system to which you want to trace the route.

Example: `xCommand Traceroute Hostname: "example.com"`

TransformAdd

Adds and configures a new transform.

Pattern(r): <S: 1, 60>

Specifies the pattern against which the alias is compared.

Type: <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the transform to be applied. *Exact*: the entire string must exactly match the alias character for character. *Prefix*: the string must appear at the beginning of the alias. *Suffix*: the string must appear at the end of the alias. *Regex*: the string is treated as a regular expression. Default: Prefix

Behavior: <Strip/Replace/AddPrefix/AddSuffix>

How the alias is modified. *Strip*: removes the matching prefix or suffix from the alias. *Replace*: substitutes the matching part of the alias with the text in the replace string. *AddPrefix*: prepends the replace string to the alias. *AddSuffix*: appends the replace string to the alias. Default: Strip

Replace: <S: 0, 60>

The text string to use in conjunction with the selected Pattern behavior.

Priority: <1..65534>

Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform. Default: 1

Description: <S: 0, 64>

A free-form description of the transform.

State: <Enabled/Disabled>

Indicates if the transform is enabled or disabled. Disabled transforms are ignored. Default: Enabled

Example: `xCommand TransformAdd Pattern: "example.net" Type: suffix Behavior: replace Replace: "example.com" Priority: 3 Description: "Change example.net to example.com" State: Enabled`

TransformDelete

Deletes a transform.

TransformId(r): <1..100>

The index of the transform to be deleted.

Example: `xCommand TransformDelete TransformId: 2`

UcxnConfigAdd

Configures a link to a Cisco Unity Connection server, for use with Mobile and Remote Access.

Address(r): <S:0,1024>

The FQDN or IP address of a Unity Connection publisher.

CertValidationDisabled: <On/Off>

If CertValidationDisabled is Off, the Cisco Unity Connection system's FQDN or IP address must be contained within the X.509 certificate presented by that system (in either the Subject Common Name or the Subject Alternative Name attributes of the certificate). The certificate itself must also be valid and signed by a trusted certificate authority.

DeploymentId: <1..65535>

This Unity Connection publisher is associated with the selected deployment and can only communicate with other members of the selected deployment. It cannot communicate with members of other deployments.

Password(r): <S:1,1024>

The password used by the VCS Control to access the Cisco Unity Connection publisher.

Username(r): <S:1,1024>

The username used by the VCS to access the Unity Connection publisher.

UcxnConfigDelete

Removes a link to a Cisco Unity Connection server from the VCS.

Address(r): <S:0,1024>

The FQDN or IP address of a Unity Connection publisher.

WarningAcknowledge

Acknowledges an existing warning.

Note: this command is intended for developer use only.

WarningID(r): <S:36, 36>

The warning ID

Example: `xCommand WarningAcknowledge WarningID: "ab3d63f6-c0bb-4a9c-a121-e683abfedff0"`

WarningLower

Lowers a warning.

Note: this command is intended for developer use only.

WarningID(r): <S:36, 36>

The warning ID.

Example: `xCommand WarningLower WarningID: "ab3d63f6-c0bb-4a9c-a121-e683abfedff0"`

WarningRaise

Raises a warning.

Note: this command is intended for developer use only.

WarningID(r): <S:36, 36>

The warning ID.

WarningText(r): <S:0, 255>

The description of the warning.

Example: `xCommand WarningRaise WarningID: "ab3d63f6-c0bb-4a9c-a121-e683abfedff0" WarningText: "Module foo is malfunctioning"`

Xmppdelete

Deletes the details of IM and Presence servers.

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the IM and Presence server to delete.

Example: `xCommand Xmppdelete Address: "imp_server.example.com"`

Xmppdiscovery

Discovers the details of IM and Presence servers.

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the IM and Presence server to discover.

AxlpasswordAxlpassword(r): <Password>

The password used to access the IM and Presence publisher.

Axlusername(r): <String>

The username used to access the IM and Presence publisher.

CertValidationDisabled: <On/Off>

Controls X.509 certificate checking against the certificate presented by the IM and Presence publisher. Default: On

Example: `xCommand Xmppdiscovery Address: "imp.example.com" Axlpassword: "xyz" Axlusername: "abc"`

ZoneAdd

Adds and configures a new zone.

ZoneName(r): <S: 1, 50>

Assigns a name to this zone.

Type(r): <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>

Determines the nature of the specified zone, in relation to the local VCS. *Neighbor*: the new zone will be a neighbor of the local VCS. *TraversalClient*: a firewall exists between the zones, and the local VCS is a traversal client of the new zone. *TraversalServer*: a firewall exists between the zones and the local VCS is a traversal server for the new zone. *ENUM*: the new zone contains endpoints discoverable by ENUM lookup. *DNS*: the new zone contains endpoints discoverable by DNS lookup.

Example: `xCommand ZoneAdd ZoneName: "UK Sales Office" Type: Neighbor`

ZoneDelete

Deletes a zone.

ZoneId(r): <1..1000>

The index of the zone to be deleted.

Example: `xCommand ZoneDelete ZoneId: 2`

ZoneList

A diagnostic tool that returns the list of zones (grouped by priority) that would be queried, and any transforms that would be applied, in a search for a given alias.

Note that this command does not change any existing system configuration.

Alias(r): <S: 1, 60>

The alias to be searched for.

Example: `xCommand ZoneList Alias: "john.smith@example.com"`

Command Reference – xStatus

The **xStatus** group of commands are used to return information about the current status of the system. Each **xStatus** element returns information about one or more sub-elements.

The following section lists all the currently available **xStatus** commands, and the information that is returned by each command.

To obtain information about the existing status, type:

- **xStatus** to return the current status of all status elements
- **xStatus <element>** to return the current status for that particular element and all its sub-elements
- **xStatus <element> <sub-element>** to return the current status of that group of sub-elements

To obtain information about the **xStatus** commands, type:

- **xStatus ?** to return a list of all elements available under the **xStatus** command

xStatus elements

The current xStatus elements are:

- Alarm
- Alternates
- Applications
- Authentication
- Authzkeys
- B2BUACalls
- B2buapresencerelayservice
- B2buapresencerelayuser
- CDR
- Cafe
- Calls
- Cloud
- Cluster
- CollaborationEdge
- Edgeauth
- Edgecmsserver
- EdgeConfigProvisioning
- Edgeconfigprovisioning
- Edgedomain
- Edgeexternalfqdn
- Edgeauthcodecache
- Edgesso
- ExternalManager
- Fail2ban
- Feedback
- FindMeManager

- Fips
- Firewall
- Gwtunnels
- H323
- HTTPProxy
- Hardware
- IntrusionProtection
- Iptablesacceptedrule
- Iptablesrule
- License
- Links
- Mediastatistics
- MicrosoftContent
- MicrosoftIMP
- NetworkInterface
- NetworkLimits (experimental)
- Ntpcertificates
- Options
- PhonebookServer
- Pipes
- Policy
- PortUsage
- ProvisioningServer
- Provisioningdevice
- Provisioningdevicestatussynch
- Provisioningservice
- RateLimits
- Registrations
- ResourceUsage
- Resourceusage
- SIP
- SipServiceDomains
- SipServiceZones
- SystemMetrics
- SystemUnit
- TURN
- Teststatus
- Time
- Traversalserverresourceusage
- Tunnels
- Warnings
- XMPP

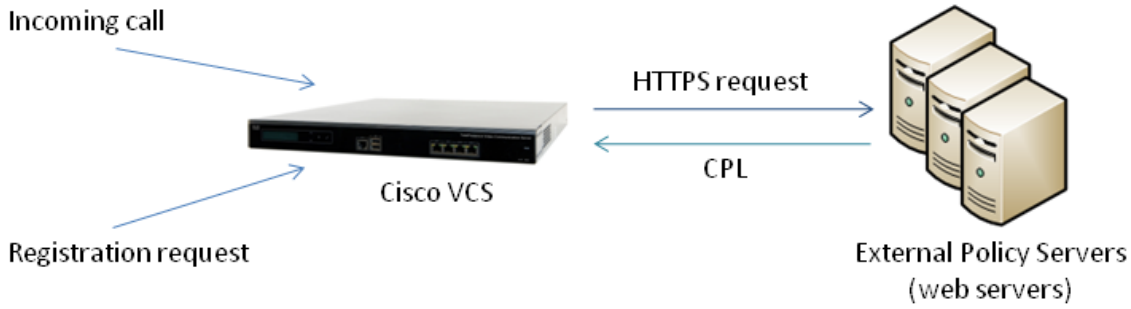
- Xcps2s
- Zones

External Policy Overview

The Cisco TelePresence Video Communication Server (VCS) has built in support for Registration Policy, User Policy (FindMe), 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 VCS can be loaded with CPL to implement advanced call policy decisions, complex CPL is difficult to write and maintain.

The VCS's external policy feature allows policy decisions to be taken by an external system which can then instruct the VCS 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 VCS, and can implement features that are unavailable on the VCS. 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 VCS is configured to use an external policy server the VCS 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 VCS will then execute.



Using an External Policy Server

The main areas where the VCS 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 VCS.

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 VCS as a fallback, if the service is not available.
- The status and reachability of the service can be queried via a status path.

If you require FindMe functionality beyond that provided by VCS / Cisco TMS, we recommend that you implement it through Call Policy.

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

External Policy Request Parameters

When the VCS 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	User Policy
ALIAS		✓			
ALLOW_INTERWORKING	TRUE / FALSE		✓	✓	✓
AUTHENTICATED	TRUE / FALSE	✓	✓	✓	✓
AUTHENTICATED_SOURCE_ALIAS			✓	✓	✓
AUTHENTICATION_USER_NAME			✓	✓	✓
CLUSTER_NAME		✓	✓	✓	✓
DESTINATION_ALIAS			✓	✓	✓
DESTINATION_ALIAS_PARAMS			✓	✓	✓
GLOBAL_CALL-SERIAL_NUMBER	GUID		✓	✓	✓
LOCAL_CALL_SERIAL_NUMBER	GUID		✓	✓	✓
METHOD	INVITE / ARQ / LRQ / OPTIONS / SETUP / REGISTER / SUBSCRIBE / PUBLISH	✓	✓	✓	✓
NETWORK_TYPE	IPV4 / IPV6		✓	✓	✓
POLICY_TYPE	REGISTRATION / SEARCH / ADMIN / USER	✓	✓	✓	✓
PROTOCOL	SIP / H323	✓	✓	✓	✓
REGISTERED_ALIAS			✓	✓	✓
SOURCE_ADDRESS		✓	✓	✓	✓
SOURCE_IP		✓	✓	✓	✓
SOURCE_PORT		✓	✓	✓	✓
TRAVERSAL_TYPE	TYPE_[UNDEF / ASSENTSERVER / ASSENTCLIENT / H460SERVER / H460CLIENT / TURNSERVER / TURNCLIENT / ICE]		✓	✓	✓

Parameter name	Values	Registration Policy	Search rules	Call Policy	User Policy
UNAUTHENTICATED_SOURCE_ALIAS			✓	✓	✓
UTCTIME		✓	✓	✓	✓
ZONE_NAME			✓	✓	✓

Cryptography support

External policy servers should support TLS and AES-256/AES-128/3DES-168.

SHA-1 is required for MAC and Diffie-Hellman / Elliptic Curve Diffie-Hellman key exchange; the VCS 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 VCS 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
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

VCS supports the following RFCs:

Table 37 Supported RFCs

RFC	Description
791	Internet Protocol
1213	Management Information Base for Network Management of TCP/IP-based internets
1305	Network Time Protocol (Version 3) Specification, Implementation and Analysis
2327	SDP: Session Description Protocol
2460	Internet Protocol, Version 6 (IPv6) Specification (partial, static global addresses only)
2464	Transmission of IPv6 Packets over Ethernet Networks
2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
2782	A DNS RR for specifying the location of services (DNS SRV)
2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
2915	The Naming Authority Pointer (NAPTR) DNS Resource Record
2976	SIP INFO method
3164	The BSD syslog Protocol
3261	Session Initiation Protocol
3263	Locating SIP Servers
3264	An Offer/Answer Model with the Session Description Protocol (SDP)
3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
3326	The Reason Header Field for the Session initiation Protocol (SIP)
3265	Session Initiation Protocol (SIP) – Specific Event Notification
3327	Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
3489	STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
3515	The Session Initiation Protocol (SIP) Refer Method
3550	RTP: A Transport Protocol for Real-Time Applications
3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
3596	DNS Extensions to Support IP Version 6
3761	The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)
3856	A Presence Event Package for the Session Initiation Protocol (SIP)
3863	Presence Information Data Format (PIDF)
3880	Call Processing Language (CPL): A Language for User Control of Internet Telephony Services

Table 37 Supported RFCs (continued)

RFC	Description
3891	Replaces header
3892	Referred-by header
3903	Session Initiation Protocol (SIP) Extension for Event State Publication
3944	H.350 Directory Services
3986	Uniform Resource Identifier (URI): Generic Syntax
4028	Session Timers in the Session Initiation Protocol
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers
4291	IP Version 6 Addressing Architecture
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
4479	A Data Model for Presence
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 earlier releases that are not listed here, see the previous versions of this document or online help.

X8.11 Features

Table 38 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
Finesse Agent Support over MRA	–	–	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
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

Table 38 Feature History by Release Number (continued)

Feature / change	X8.11 (withdrawn)	X8.11.1 (withdrawn)	X8.11.2 (withdrawn)	X8.11.3 (withdrawn)	X8.11.4
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
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 39 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
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
X8.10 Minor Changes and Enhancements	Supported	Supported	Supported	Supported	Supported

More information

For details about a particular feature in X8.10.*n*, please see the Release Notes for the relevant software version.

X8.9 Features

Table 40 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
REST API Expansion	Supported	Supported	Supported

Table 40 Feature History by Release Number (continued)

Feature / change	X8.9	X8.9.1	X8.9.2
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
X8.9 Minor Changes and Enhancements	Supported	Supported	Supported

More information

For details about a particular feature in X8.9.*n*, please see the Release Notes for the relevant software version.

X8.8 Features

Table 41 Feature History by Release Number

Feature / change	X8.8
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
X8.8 Minor Changes and Enhancements	Supported

More information

For details about a particular feature in X8.8, please see the latest X8.8 Release Notes.

X8.7 Features

Table 42 Feature History by Release Number

Feature / change	X8.7
Dial via Office-Reverse (DVO-R)	Supported
Lync Screen Sharing Through a Gateway Cluster	Supported

Table 42 Feature History by Release Number (continued)

Feature / change	X8.7
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
X8.7 Minor Changes and Enhancements	Supported

More information

For details about a particular feature in X8.7, please see the latest X8.7 Release Notes.

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.

The terms and conditions of use can be found at:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/license_info/Cisco_VCS_EULA.pdf

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/telepresence-video-communication-server-vcs/products-licensing-information-listing.html

This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/).

This product includes software developed by the University of California, Berkeley and its contributors.

IMPORTANT: USE OF THIS PRODUCT IS SUBJECT IN ALL CASES TO THE COPYRIGHT RIGHTS AND THE TERMS AND CONDITIONS OF USE REFERRED TO ABOVE. USE OF THIS PRODUCT CONSTITUTES AGREEMENT TO SUCH TERMS AND CONDITIONS.

AVC Video License

With respect to each AVC/H.264 product, we are obligated to provide the following notice:

This product is licensed under the AVC patent portfolio license for the personal use of a consumer or other uses in which it does not receive remuneration to (i) encode video in compliance with the AVC standard ("AVC video") and/or (ii) decode AVC video that was encoded by a consumer engaged in a personal activity and/or was obtained from a video provider licensed to provide AVC video. No license is granted or shall be implied for any other use. Additional information may be obtained from MPEG LA, L.L.C.

See http://www.mpegla.com.

Accordingly, please be advised that service providers, content providers, and broadcasters are required to obtain a separate use license from MPEG LA prior to any use of AVC/H.264 encoders and/or decoders.

Patent Information

This product is covered by one or more of the following patents:

- US7,512,708
- EP1305927
- EP1338127

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies 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.

© 2016–2020 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)